PERANAN MOBILE ADHOC DALAM KOMUNIKASI DATA

2023

LAKSAMANA RAJENDRA HAIDAR AZANI FAJRI

YAYASAN PRIMA AGUS TEKNIK

PERANAN MOBILE ADHOC DALAM KOMUNIKASI DATA

2023

PENULIS:

LAKSAMANA RAJENDRA HAIDAR AZANI FAJRI

PENERBIT:
YAYASAN PRIMA AGUS TEKNIK

YAYASAN PRIMA AGUS TEKNIK

PERANAN MOBILE ADHOC DALAM KOMUNIKASI DATA

Penulis:
Laksamana Rajendra Haidar Azani Fajri .,M.T.,M.Kom
ISBN: ***978-623-8120-09-3 (PDF)***

Editor:
Teguh Setiadi.,M.Kom

Penyunting :
Dr. MIFTAHURROHMAN, M.Si

Desain Sampul dan Tata Letak:
Moh. Muthohir.,M.Kom

Yayasan :
Yayasan Prima Agus Teknik bekerja sama dengan
Universitas Sains dan Teknologi Komputer (Universitas STEKOM)

Redaksi:
Jalan Majapahit no 605. Semarang
Telp. (024) 6723456
Fax. 024-6710144
email:penerbit_ypat@stekom.ac.id
Distributor tunggal:
Universitas STEKOM
Jalan Majapahit no 605. Semarang
Telp. (024) 6723456
Fax. 024-6710144
email:info@stekom.ac.id

KATA PENGANTAR

Puji syukur penulis panjatkan atas terselesaikannya buku yang berjudul “Peranan Mobile ad Hoc dalam Komunikasi Data”. Dalam Bab pertama, kita membahas beberapa isu dasar dalam peranan mobile ad hoc dalam komunikasi data. Penulis menyadari bahwa masih banyak kekurangan pada perancangan dan pembuatan buku peranan mobile adhoc ini. Oleh karena itu, besar harapan penulis untuk menerima saran dan kritik dari pembaca. Saran dan kritik dapat didiskusikan melalui email penulis laksamanahaidar@gmail.com Semoga buku ini dapat memberikan manfaat bagi para mahasiswa Universitas STEKOM pada khususnya dan dapat memberikan nilai lebih untuk para pembaca pada umumnya. Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak-pihak yang telah memberikan bantuan baik secara moril maupun materiil, dukungan serta do’a selama proses penyelesaian penulisan Buku ini untuk itu, penulis ingin mengucapkan terima kasih kepada Allah SWT yang telah memberikan berbagai macam nikmat , mulai dari nikmat iman ,nikmat islam dan nikmat sehat wal’afiat.Atas kehendak-Mu Proyek Akhir ini dapat terselesaikan.Dan Nabi Muhammad SAW yang telah menjadi panutan bagi seluruh umat di dunia. Bapakku Sulistyono Sofyan dan Ibu Yayah Ratikah yang selalu memberikan semangat baik secara moril maupun materiil dan selalu mendoakanku di setiap ibadah nya.Dan terima kasih untuk Istriku Afria Afria Alfitri Rizqi dan anakku Alisha Alfathunnisa dan adik-adikku Haikal dan Baron yang telah menemani dalam suka ataupun duka.Sukses juga buat kalian kelak.

Semarang, 3 Januari 2023

Penulis

Daftar Isi

CHAPTER 1 JARINGAN AD HOC MULTIHOP:JALUR EVOLUSIONER

1.1 PENDAHULUAN

Pada akhir 1990-an, proliferasi perangkat komputasi dan komunikasi seluler (misalnya ponsel, laptop, perangkat digital genggam, perangkat digital pribadi) asisten, atau komputer yang dapat dikenakan) memicu ledakan pertumbuhan pasar komputasi seluler dan jaringan seluler, dan hot spot WiFi dengan cepat menggantikan jaringan akses kabel. Meskipun jaringan berbasis infrastruktur menawarkan cara terbaik bagi perangkat seluler untuk mendapatkan layanan jaringan, dibutuhkan waktu dan biaya yang berpotensi tinggi untuk menyiapkan infrastruktur yang diperlukan di mana saja. Biaya dan penundaan ini mungkin tidak dapat diterima untuk lingkungan yang dinamis di mana

orang dan/atau kendaraan perlu saling terhubung untuk sementara di area tanpa infrastruktur komunikasi yang sudah ada sebelumnya (misalnya, jaringan antarkendaraan dan bencana), atau di mana biaya infrastruktur tidak dapat dibenarkan (misalnya, di -membangun jaringan, jaringan masyarakat perumahan, dll). Dalam kasus ini, jaringan tanpa infrastruktur, sering disebut sebagai jaringan ad hoc atau jaringan self-organizing, memberikan solusi yang lebih efisien [1,2]. Jaringan ad hoc single-hop adalah bentuk paling sederhana dari jaringan self- organizing yang diperoleh dengan menghubungkan perangkat yang berada dalam jangkauan transmisi yang sama. Beberapa standar jaringan nirkabel mendukung paradigma jaringan

ad hoc single-hop: IEEE 802.15.4 untuk jaringan kecepatan data rendah jarak pendek (<250 kbps) (juga dikenal sebagai Zigbee), Bluetooth (IEEE 802.15.1) untuk jaringan area pribadi berfungsi, dan keluarga standar 802.11 untuk jaringan ad hoc LAN berkecepatan tinggi (lihat Bab 2 dalam buku ini). Node terdekat dapat berkomunikasi secara langsung dengan mengeksploitasi teknologi jaringan nirkabel dalam mode ad hoc. Dalam jaringan multihop, sering disebut sebagai Mobile Ad hoc Networks (MANETs), node jaringan (misalnya, perangkat seluler pengguna) harus secara kooperatif menyediakan fungsionalitas yang biasanya disediakan oleh infrastruktur jaringan (misalnya, router, sakelar, server) . Dalam MANET, perangkat pengguna dengan antarmuka nirkabel (biasanya 802.11 dalam mode ad hoc) mengaktifkan sesi komunikasi dengan perangkat seluler lain untuk melakukan operasi transfer data tanpa memerlukan infrastruktur jaringan apa pun. Potensi paradigma jaringan ini membuat jaringan ad hoc menjadi pilihan yang menarik untuk membangun jaringan nirkabel 4G, dan karenanya MANET segera memperoleh momentum dan ini menghasilkan upaya penelitian yang luar biasa dalam komunitas jaringan seluler (lihat, misalnya, referensi 1 dan 2). Namun, terlepas dari upaya penelitian yang sangat besar, setelah lebih dari 15 tahun kegiatan penelitian yang intens, teknologi MANET hanya memiliki peran kecil dalam bidang jaringan nirkabel: Ini diterapkan hanya dalam skenario yang sangat khusus. Memang, seperti yang ditunjukkan dalam referensi 3, sementara dari sudut pandang akademik MANET telah menjadi bidang penelitian yang sangat produktif, dampak paradigma jaringan pada komunikasi komputer sipil telah diabaikan. Lebih tepatnya, sementara penelitian MANET menghasilkan literatur yang luas yang sangat mempengaruhi pengembangan jaringan ad hoc multihop generasi berikutnya, dari sudut pandang penggunaan, penelitian MANET telah gagal. Hal ini terutama disebabkan oleh kurangnya realisme dalam pendekatan / tujuan penelitian yang menghasilkan banyak makalah ilmiah tetapi hanya penyebaran nyata dalam jumlah yang sangat terbatas, dengan keterlibatan pengguna nyata yang terbatas dan tidak ada aplikasi pembunuh. Namun, dengan memanfaatkan pembelajaran dalam penelitian MANET, bersama dengan

hasil ilmiah yang dihasilkan, komunitas ilmiah telah mampu mengubah paradigma jaringan multihop ad hoc menjadi paradigma jaringan yang sukses dengan menerapkannya di beberapa kelas jaringan yang sedang merambah. pasar massal.

Seperti yang dibahas dalam bab ini, contoh yang relevan dari teknologi ini termasuk jaringan mesh

Dalam bab ini kita membahas evolusi paradigma jaringan multihop ad hoc. Secara khusus, Bagian 1.2 dikhususkan untuk menganalisis dan mendiskusikan penelitian MANET dengan terlebih dahulu menyajikan pencapaian ilmiah utama di bidang penelitian ini (dengan perhatian khusus pada konsep lintas lapisan yang sangat inovatif) dan kemudian mendiskusikan pelajaran yang dipetik dari "kegagalan" MANET. Kemudian, di Bagian 1.3 kami mengulas paradigma jaringan yang paling sukses berdasarkan jaringan ad hoc multihop, dengan membahas hasil yang telah dicapai dan tantangan terbuka. Bagian 1.4 menyimpulkan bab ini.

1.2 PENELITIAN MANET: PENCAPAIAN UTAMA DAN PELAJARAN YANG DIPEROLEH

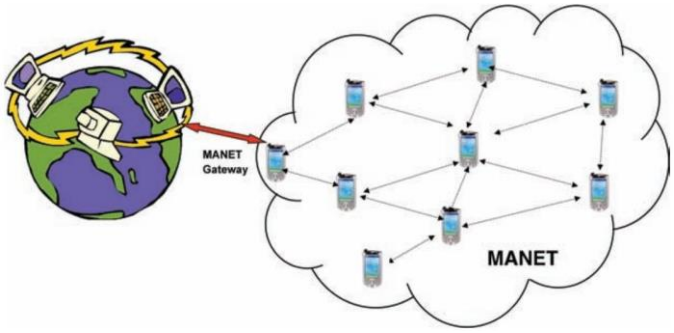
Pada bagian ini kami meninjau hasil ilmiah dalam penelitian MANET dan kemudian kami

membahas alasan mengapa paradigma ini tidak berdampak besar pada bidang jaringan nirkabel, dan kami menyimpulkan dengan serangkaian pembelajaran dari penelitian MANET.

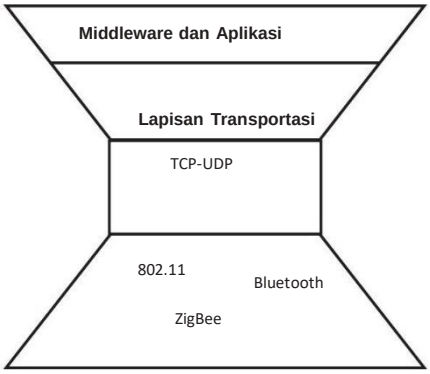
1.2.1 Pencapaian Utama dalam Riset MANET

Penelitian MANET berfokus pada apa yang kita sebut MANET tujuan umum murni , di mana murni menunjukkan bahwa tidak ada infrastruktur yang diasumsikan untuk mengimplementasikan fungsi jaringan dan tidak ada otoritas yang bertanggung jawab untuk mengelola dan mengendalikan jaringan. Tujuan umum menunjukkan bahwa jaringan ini tidak dirancang dengan aplikasi khusus apa pun, melainkan untuk mendukung aplikasi TCP/IP warisan apa pun. Secara khusus, para peneliti memusatkan upaya mereka untuk merancang dan mengevaluasi algoritma dan protokol untuk mengimplementasikan komunikasi yang efisien dalam skenario seperti yang ditunjukkan pada Gambar 1.1. Di sini, perangkat pengguna secara kooperatif menyediakan fungsionalitas

yang biasanya disediakan oleh infrastruktur jaringan (misalnya router, switch, server).



Gambar 1. Topologi Manet



Gambar 1.2 Stack berlapis MANET

tidak hanya dapat berkomunikasi satu sama lain, tetapi juga dapat mengakses Internet dengan mengeksploitasi layanan yang ditawarkan oleh node gateway MANET, sehingga secara efektif memperluas layanan Internet ke area non-infrastruktur (misalnya, lihat referensi 4 dan 5).

MANET dengan tujuan umum yang murni merupakan perubahan besar dari paradigma jaringan komputer tradisional yang memerlukan desain ulang lengkap dari arsitektur dan protokol jaringan. Ini telah menghasilkan kegiatan penelitian yang intens. Gambaran mendalam tentang kegiatan penelitian MANET dapat ditemukan di referensi 2, sedangkan referensi 1 merangkum hasil dan tantangan utama dalam penelitian MANET.

Kelompok kerja IETF MANET telah menjadi titik referensi untuk kegiatan penelitian MANET tujuan umum murni. MANET IETF WG mengadopsi tampilan IP-centric dari MANET (lihat Gambar 1.2) yang mewarisi lapisan tumpukan protokol TCP/IP dengan tujuan mendesain ulang tumpukan protokol jaringan untuk merespons karakteristik baru, kompleksitas, dan kendala desain MANET [6]. Semua lapisan tumpukan protokol adalah subjek dari kegiatan penelitian intensif. Selanjutnya, menurut tampilan berlapis tumpukan protokol (lihat Gambar 1.2), kami akan meringkas secara singkat arah/hasil penelitian utama, dari teknologi yang memungkinkan hingga middleware dan aplikasi.

1.2.1.1 Mengaktifkan Teknologi.

Mengaktifkan teknologi adalah blok dasar MANET yang menjamin komunikasi single-hop langsung antara perangkat pengguna.

Oleh karena itu, kegiatan penelitian intensif difokuskan pada menyelidiki kesesuaian standar jaringan nirkabel yang ada untuk mendukung jaringan ad hoc multihop dengan perhatian khusus pada keluarga IEEE 802.11 (misalnya, lihat referensi 7-10), untuk Bluetooth (misalnya, lihat referensi 7, 11). , dan 12), dan, baru-baru ini, ke ZigBee (misalnya, lihat referensi 13 dan 14). Biasanya, standar jaringan nirkabel ini tidak dirancang untuk mendukung jaringan ad hoc multihop; karenanya beberapa peningkatan, baik pada MAC dan lapisan fisik telah diusulkan dan dievaluasi untuk meningkatkan teknologi ini saat beroperasi dalam mode ad hoc. Perangkat tambahan pada lapisan fisik termasuk penggunaan antena directional dan kontrol daya [15], penggunaan OFDM, skema pemrosesan

sinyal yang ditingkatkan, radio yang ditentukan perangkat lunak, dan teknologi MIMO; ketika pada lapisan MAC telah ada beberapa usulan untuk mengendalikan tabrakan dan interferensi antar node tetap menjamin konsumsi energi yang efisien [1].

Analisis terbaru dari teknologi yang memungkinkan untuk jaringan ad hoc multihop disajikan dalam Bab 2 buku ini.

1.2.1.2 Lapisan Jaringan.

Upaya penelitian MANET terutama difokuskan pada lapisan jaringan, dengan perhatian khusus pada perutean dan penerusan, karena ini adalah layanan jaringan dasar untuk membangun jaringan ad hoc multihop. Routing adalah fungsi untuk mengidentifikasi jalur antara pengirim dan penerima, dan untuk menangkal, fungsi selanjutnya mengirimkan paket di sepanjang jalur ini. Fungsi- fungsi ini sangat terkait dengan karakteristik topologi jaringan. Karena sifat topologi MANET yang tidak dapat diprediksi dan dinamis, protokol perutean lama yang dikembangkan untuk jaringan kabel tidak cocok untuk jaringan ad hoc multihop, dan ini merangsang aktivitas penelitian intensif yang menghasilkan jumlah usulan protokol perutean yang mengesankan (dan terus meningkat). lihat referensi 16 untuk daftar yang diperbarui). Protokol perutean dan penerusan dapat diklasifikasikan menurut properti cast—yaitu, apakah mereka menggunakan Unicast, Geocast, Multicast, atau Broad cast forwarding. Siaran adalah mode dasar operasi melalui saluran nirkabel; setiap pesan yang ditransmisikan pada saluran nirkabel umumnya diterima oleh semua tetangga yang berada dalam satu lompatan dari pengirim. Implementasi paling sederhana dari operasi broadcast ke semua node jaringan adalah dengan flooding, tetapi hal ini dapat menyebabkan masalah broad cast storm karena redundant re- broadcast [17]. Skema telah diusulkan untuk mengatasi masalah ini dengan mengurangi penyiaran yang berlebihan. Diskusi tentang skema penyiaran yang efisien disajikan dalam referensi 18. Protokol perutean multicast berperan ketika sebuah node perlu mengirim pesan yang sama, atau aliran data, ke subset dari tujuan node jaringan. Penerusan geocast adalah kasus khusus multicast yang digunakan untuk mengirimkan paket data ke sekelompok node yang terletak di dalam area geografis tertentu. Dari sudut pandang implementasi, geocasting adalah bentuk penyiaran "terbatas": Pesan dikirimkan ke semua node yang berada di dalam wilayah tertentu. Ini dapat dicapai dengan mengarahkan paket dari sumber ke node di dalam wilayah geocasting dan kemudian menerapkan transmisi siaran di dalam wilayah tersebut. Algoritma perutean berbasis posisi atau sadar lokasi, dengan memberikan solusi yang efisien untuk meneruskan paket ke posisi geografis, merupakan dasar untuk membangun layanan pengiriman geocasting [19]. Protokol perutean sadar lokasi menggunakan posisi node (yaitu, koordinat geografis) untuk penerusan data.

Sebuah node memilih hop berikutnya untuk meneruskan paket dengan menggunakan

posisi fisik tetangganya, bersama dengan posisi fisik node tujuan: Paket dikirim menuju koordinat Penerusan unicast berarti komunikasi satu-ke-satu; yaitu, satu sumber

mentransmisikan paket data ke satu tujuan. Ini adalah mekanisme penerusan dasar dalam jaringan komputer; untuk alasan ini, protokol routing unicast terdiri dari kelas terbesar dari protokol routing MANET. Menurut WG MANET, protokol perutean unicast diklasifikasikan menjadi dua kategori utama: protokol perutean proaktif dan protokol perutean reaktif (sesuai permintaan). Protokol perutean proaktif diturunkan dari protokol jarak-vektor Internet dan status-tautan warisan. Mereka berusaha untuk memelihara informasi perutean yang konsisten dan diperbarui untuk setiap pasangan node jaringan dengan menyebarkan, secara proaktif, pembaruan rute pada interval waktu yang tetap. Sebaliknya, protokol perutean reaktif menetapkan rute ke tujuan hanya jika diminta (node sumber biasanya memulai proses penemuan rute dengan mengirimkan pesan permintaan rute). Setelah rute ditetapkan, rute tersebut dipertahankan hingga tujuan menjadi tidak dapat diakses atau hingga rute tidak lagi digunakan. Secara khusus, tiga protokol routing utama muncul dari bidang MANET dan

merupakan referensi untuk jaringan ad hoc multihop lainnya: dua protokol routing reaktif, AODV (dan penggantinya DYMO) dan DSR, dan satu protokol proaktif, OLSR. Sebuah survei tentang protokol

perutean MANET disajikan dalam referensi 21, sedangkan referensi 1 merangkum arah penelitian utama di bidang ini.

Selain protokol proaktif dan reaktif, kelas protokol lain telah diidentifikasi untuk meningkatkan kinerja jaringan setidaknya dalam skenario tertentu. Protokol hibrid menggabungkan pendekatan proaktif dan reaktif, sehingga mencoba untuk mendapatkan keuntungan dari keduanya. Protokol perutean sadar-energi mempertimbangkan energi yang tersedia di node jaringan untuk memilih jalur untuk penerusan data.

Ini mungkin berarti (a) untuk meminimalkan konsumsi energi untuk meneruskan paket dari sumber ke tujuan atau (b) untuk memaksimalkan seumur hidup jaringan dengan melestarikan sebanyak mungkin konektivitas jaringan. Perutean hierarkis bertujuan untuk mengurangi overhead dengan menyusun jaringan pada lebih banyak level dan memungkinkan komunikasi multihop hanya di antara beberapa node, yang mewakili sekelompok node pada level yang lebih rendah. Perutean berbasis cluster adalah contoh yang relevan dari perutean hierarkis. Ide dasar di balik clustering adalah untuk mengelompokkan node jaringan ke dalam sejumlah cluster yang tumpang tindih. Jalur dicatat hanya antar cluster (bukan antar node); ini memungkinkan agregasi informasi perutean dan akibatnya meningkatkan skalabilitas algoritma perutean. Dalam definisi aslinya, di dalam cluster, satu node bertugas mengkoordinasikan kegiatan cluster (clusterhead). Di luar clusterhead, di dalam cluster, kami memiliki node biasa yang memiliki akses langsung hanya ke clusterhead dan gateway mereka—yaitu, node yang dapat mendengarkan dua atau lebih clusterhead dan yang meneruskan lalu lintas di antara cluster yang berbeda. Routing berbasis cluster telah diadopsi secara luas dalam

jaringan ad hoc multihop, dan akibatnya definisi cluster dan routing berbasis cluster telah berkembang s

1.2.1.3 highest Layer.

Di atas protokol jaringan, MANET umumnya mengasumsikan protokol transportasi Internet. Sayangnya, Transmission Control Protocol (TCP) tidak berfungsi dengan baik dalam skenario ini, sebagaimana dibahas secara luas dalam

literatur (lihat, misalnya, referensi 1). Untuk meningkatkan kinerja protokol TCP dalam MANET, beberapa proposal telah diajukan. Sebagian besar proposal ini adalah versi modifikasi dari protokol TCP lama yang digunakan di Internet. Namun, solusi berbasis TCP mungkin bukan pendekatan terbaik saat beroperasi di lingkungan MANET, dan karenanya beberapa penulis telah mengusulkan protokol transport baru yang disesuaikan dengan fitur MANET (misalnya, lihat referensi 22 dan referensi di dalamnya).

Middleware dan aplikasi merupakan area yang kurang diselidiki di bidang MANET. Memang, MANET tujuan umum telah dirancang untuk mendukung aplikasi TCP/IP warisan tanpa pemahaman yang jelas tentang aplikasi yang multihop iklan jaringan hoc adalah peluang dan dengan demikian dapat mewakili aplikasi pembunuh untuk paradigma jaringan ini. Kurangnya perhatian pada aplikasi mungkin merupakan salah satu penyebab utama dampak MANET yang dapat diabaikan di bidang jaringan nirkabel.

Kurangnya perhatian terhadap aplikasi juga membatasi minat untuk mengembangkan solusi middleware yang disesuaikan dengan MANET. Namun, kesamaan antara MANET dan peer to-peer

(p2p) sistem (seperti distribusi dan kerjasama) telah mendorong beberapa kegiatan penelitian menggunakan model komputasi p2p untuk MANET (misalnya, lihat referensi

23-25 dan referensi di dalamnya). Memang dengan mengintegrasikan sistem p2p di atas jaringan ad hoc membuat beragam aplikasi dan layanan p2p tersedia untuk pengguna MANET juga.

1.2.1.4 Isu Penelitian Lintas Lapisan.

Selain analisis ulang mendalam dari semua lapisan tumpukan protokol, penelitian MANET juga berfokus pada topik penelitian cross-layering dengan perhatian khusus pada efisiensi energi [26], keamanan [27] dan kerjasama [28,29]. Memang, masalah efisiensi energi dan keamanan tidak terkait dengan lapisan tertentu, tetapi mempengaruhi desain seluruh tumpukan protokol. Efisiensi energi muncul sebagai kendala desain utama dengan pengembangan perangkat seluler, yang mengandalkan baterai untuk energi [30]. Dalam MANET batasan ini menjadi yang dominan karena perangkat seluler tidak hanya beroperasi sebagai perangkat pengguna tetapi mereka harus mengimplementasikan semua fungsi dasar jaringan (seperti perutean dan penerusan); oleh karena itu kebijakan hemat daya (sederhana) yang diimplementasikan dalam jaringan berbasis infrastruktur [30,31], yang menempatkan perangkat dalam keadaan tidur ketika tidak memiliki data untuk dikirim/diterima, tidak efektif/cukup di MANET. Dalam jaringan nirkabel infrastruktur, strategi manajemen energi bersifat lokal untuk setiap node dan ditujukan untuk meminimalkan konsumsi energi node [30,32]. Metrik ini tidak cocok untuk jaringan ad hoc di mana node juga harus bekerja sama dengan operasi jaringan untuk menjamin konektivitas jaringan. Node serakah yang sebagian besar tetap dalam keadaan

tidur, tanpa berkontribusi pada perutean dan penerusan, akan memaksimalkan masa pakai baterainya teta Oleh karena itu, di MANET kita dapat mengidentifikasi (setidaknya) dua kelas strategi hemat

daya: strategi lokal, yang biasanya beroperasi pada rentang waktu kecil (misalnya milidetik), dan strategi global yang beroperasi pada rentang waktu yang lebih lama. Strategi lokal beroperasi di dalam node, dan mencoba menempatkan antarmuka jaringan dalam mode hemat daya dengan dampak minimum pada operasi pengiriman dan penerimaan. Kebijakan ini, yang telah diwariskan oleh penelitian komputasi seluler, biasanya beroperasi pada lapisan fisik dan MAC, dengan tujuan memaksimalkan masa pakai baterai node tanpa mempengaruhi protokol lapisan yang lebih tinggi [30]. Di sisi lain, penelitian MANET secara ekstensif menyelidiki strategi global yang bertujuan untuk memaksimalkan masa hidup jaringan melalui kebijakan yang mencoba untuk menempatkan jumlah maksimum node jaringan dalam keadaan hemat daya tanpa mengorbankan jangkauan jaringan. Kegiatan penelitian di bidang ini, yang dapat kita sebut sebagai kontrol topologi, telah menjadi salah satu bidang penelitian MANET yang paling produktif [33]. Riset kontrol topologi meliputi kontrol daya node transmisi karena mempengaruhi baik jumlah energi yang terkuras dari baterai untuk setiap transmisi, dan jumlah link yang layak (yaitu, topologi jaringan).

Pengurangan daya transmisi memungkinkan penggunaan kembali frekuensi secara spasial

—yang dapat membantu meningkatkan throughput total dan meminimalkan interferensi—namun melompat menuju tujuan. Di sisi lain, dengan meningkatkan daya transmisi, kami meningkatkan biaya transmisi per-paket (efek negatif), tetapi kami mengurangi jumlah lompatan untuk mencapai tujuan (efek positif) karena semakin banyak tautan yang tersedia. Menemukan keseimbangan bukanlah usaha yang mudah. Bagian penting lain dari literatur yang berkaitan dengan efisiensi energi dalam jaringan ad hoc terkonsentrasi pada perutean hemat energi di mana tingkat daya transmisi merupakan variabel tambahan dalam desain protokol perutean [26].

Keamanan dan Kerjasama adalah tantangan lintas lapisan utama lainnya dalam jaringan multihop. Lingkungan swakelola memperkenalkan masalah keamanan baru yang tidak ditangani oleh layanan keamanan lama yang disediakan untuk jaringan berbasis infrastruktur. Memang, selain tantangan khas lingkungan nirkabel seperti kerentanan saluran dan node, tidak adanya infrastruktur, bersama dengan topologi yang berubah secara dinamis, membuat keamanan MANET menjadi tugas yang menantang, baik di jaringan (misalnya, perutean aman untuk mengatasi ancaman berbahaya). node yang dapat mengganggu fungsi yang benar dari protokol routing dengan memodifikasi informasi routing dan/atau menghasilkan informasi routing yang salah) dan memungkinkan tingkat teknologi (misalnya, mekanisme kriptografi diimplementasikan untuk mencegah akses yang tidak sah) [27]. Namun, di MANET, mekanisme keamanan yang hanya menegakkan kebenaran atau integritas operasi jaringan tidak cukup. Memang persyaratan dasar untuk menjaga operasional jaringan adalah untuk menegakkan kontribusi dari setiap node untuk operasi jaringan, meskipun ada kecenderungan konflik dari node menuju keegoisan (misalnya, termotivasi oleh kelangkaan energi) [34].

Oleh karena itu, jaringan yang mengatur dirinya sendiri harus didasarkan pada insentif bagi pengguna untuk berkolaborasi, sehingga menghindari perilaku egois (lihat referensi 29).

Beberapa solusi, yang diusulkan dalam literatur MANET, menyajikan pendekatan yang mirip dengan masalah kerjasama: Mereka bertujuan untuk mendeteksi dan mengisolasi node nakal melalui mekanisme berdasarkan pengawas dan sistem reputasi. Kelas pendekatan lain didasarkan pada pengenalan model ekonomi untuk menegakkan kerja sama. Secara khusus, karya-karya ini mengasumsikan pengenalan mata uang virtual, yang digunakan oleh node jaringan untuk meminta layanan dari node lain. Ketika sebuah node ingin mengirim paket, ia harus menggunakan mata uang virtual untuk membayar transmisi. Di sisi lain, sebuah node mendapatkan hadiah mata uang virtual saat meneruskan paket untuk kepentingan node lain. Kerjasama antar node adalah hasil dari keseimbangan antara kepentingan pribadi yang saling bertentangan, dan oleh karena itu model teori permainan telah banyak digunakan untuk mengevaluasi algoritma kerjasama MANET.

1.2.1.5 Arsitektur Lintas Lapisan.

IETF MANET WG mengusulkan pandangan jaringan ad hoc seluler sebagai evolusi Internet [6]. Ini terutama menyiratkan tampilan IP-sentris dari jaringan, bersama dengan penggunaan arsitektur berlapis (lihat Gambar 1.2). Penggunaan protokol IP memiliki dua keuntungan utama: Menyederhanakan interkoneksi MANET ke Internet, dan menjamin independensi dari teknologi nirkabel.

Paradigma berlapis telah sangat menyederhanakan desain jaringan komputer dan telah menghasilkan arsitektur Internet yang kuat dan dapat diskalakan. Namun, hasil menunjukkan bahwa dalam jaringan nirkabel, di mana beberapa sumber daya langka (misalnya, energi dan bandwidth), pendekatan berlapis tidak sama validnya dalam hal kinerja [35]. Memang, dengan pendekatan berlapis, setiap lapisan dalam tumpukan protokol dirancang dan dioptimalkan secara independen dari lapisan lain, dan ini mengarah pada pemanfaatan sumber daya jaringan yang kurang optimal. Ini mungkin penting dalam lingkungan terbatas sumber daya seperti jaringan ad hoc multihop. Selain itu, di MANET beberapa fungsi tidak dapat ditugaskan ke satu lapisan. Misalnya, seperti dibahas di atas, manajemen energi, keamanan, dan kerja sama tidak dapat sepenuhnya diimplementasikan dalam satu lapisan, tetapi diimplementasikan dengan menggabungkan dan memanfaatkan mekanisme yang diterapkan di beberapa lapisan, dan ini memerlukan desain bersama dari lapisan-lapisan ini untuk memanfaatkannya. saling ketergantungan mereka [36]. Misalnya, dari sudut pandang manajemen energi, kontrol daya dan beberapa antena pada lapisan tautan digabungkan dengan penjadwalan pada

lapisan MAC, serta perutean dengan pembatasan energi dan pembatasan penundaan pada lapisan jaringan. Ini jelas menunjukkan bahwa peningkatan kinerja yang signifikan dapat diharapkan dengan beralih dari pendekatan berlapis yang ketat dalam merancang tumpukan protokol MANET.

Di sisi lain, pendekatan berlapis menjamin arsitektur jaringan yang fleksibel, dan pendukung pendekatan ini menunjukkan bahwa optimalisasi lintas lapisan dapat membahayakan desain modular tumpukan protokol (yang telah menjadi elemen utama dalam keberhasilan TCP/IP). Arsitektur); ini dapat menimbulkan masalah parah [37]:

• Sebagai konsekuensi dari optimasi cross-layer, protokol mungkin menjadi ketat

digabungkan, dan perubahan dalam protokol menyebar ke yang lain.

• Menggabungkan beberapa optimisasi lintas-lapisan secara bersamaan dapat menyebabkan interferensi timbal balik di antara lapisan-lapisan tersebut, yang dapat menghasilkan desain tumpukan-protokol “spaghetti”, membuat pemeliharaan arsitektur menjadi tugas yang menantang.

Oleh karena itu, masalah utamanya adalah menemukan keseimbangan antara pengoptimalan kinerja dan fleksibilitas tumpukan protokol. Pertanyaan utamanya adalah sejauh mana pendekatan berlapis-murni perlu dimodifikasi. Pada satu titik ekstrim kami memiliki solusi berdasarkan pemicu lapisan. Secara khusus, pemicu lapisan adalah sinyal yang telah ditentukan sebelumnya untuk memberi tahu beberapa peristiwa ke lapisan yang lebih tinggi (misalnya, kegagalan dalam pengiriman data), yang dengan

demikian meningkatkan kerja sama antar lapisan dengan tetap mempertahankan prinsip pemisahan antar lapisan.

Sebuah desain cross-layer penuh merupakan ekstrim lainnya, yang mengoptimalkan kinerja jaringan secara keseluruhan dengan mengeksploitasi saling ketergantungan lapisan pada tingkat maksimum. Misalnya, lapisan fisik dapat mengadaptasi laju, daya, dan pengkodean untuk memenuhi persyaratan aplikasi dengan kondisi saluran dan jaringan saat ini; lapisan MAC dapat menyesuaikan perilakunya dengan kondisi interferensi tautan dasar serta kendala penundaan dan prioritas lapisan yang lebih tinggi. Protokol perutean adaptif dapat dikembangkan berdasarkan tautan saat ini, jaringan, dan kondisi dan persyaratan lalu lintas.

Akhirnya, middleware dapat menggunakan gagasan kualitas layanan lunak (QoS), yang menyesuaikan dengan kondisi jaringan yang mendasarinya untuk memberikan QoS setinggi mungkin ke aplikasi [35].

Spektrum yang luas dari kemungkinan alternatif untuk mengeksploitasi MANET cross-layering untuk meningkatkan kinerja jaringan telah menghasilkan banyak literatur. Kriteria yang berbeda dapat digunakan untuk mengklasifikasikan pendekatan lintas lapisan yang ada (misalnya, lihat referensi 38). Selanjutnya, kami mengklasifikasikan pendekatan cross-layering menjadi empat kategori utama:

• Komunikasi Antar Lapisan. Beberapa saluran komunikasi dibuat di antara protokol milik lapisan yang berbeda. Biasanya, organisasi berlapis dari arsitektur dipertahankan, tetapi antarmuka baru ditentukan untuk memungkinkan komunikasi di antara lapisan yang tidak berdekatan.

• Penyetelan Interlayer. Protokol pada lapisan yang berbeda diimplementasikan dengan cara yang tergantung, tetapi parameternya dioptimalkan bersama untuk meningkatkan kinerja sistem secara keseluruhan. Dalam kasus paling sederhana, penyetelan protokoldilakukan secara offline sebelum jaringan dimulai. Dalam hal ini arsitektur berlapis warisan dipertahankan sepenuhnya. Ekstrem lainnya dalam rangkaian solusi ini diwakili oleh penyetelan bersama online dari parameter protokol. Dalam hal

ini arsitektur berlapis dimodifikasi dengan penyisipan loop kontrol di antara protokol milik lapisan yang berbeda.

• Desain Interlayer. Desain bersama dari dua (atau lebih) protokol milik lapisan yang berbeda menghancurkan modularitas arsitektur, karena independensi lapisan tidak dipertahankan. Ketika sebuah protokol dimodifikasi/diganti juga, semua protokol lain dari stack, yang desainnya bergantung pada protokol yang dimodifikasi, perlu dimodifikasi/ diganti. • Desain Tanpa Lapisan. Dalam hal ini organisasi berlapis tidak digunakan dan

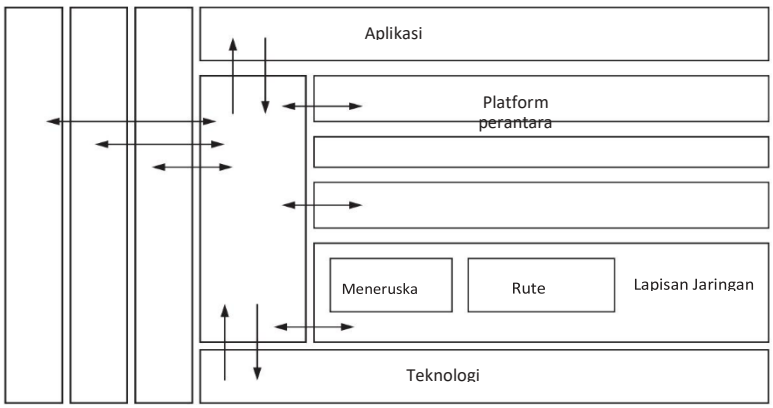
organisasi baru digunakan untuk memproses dan meneruskan paket yang berjalan melalui node jaringan. Arsitektur Haggle adalah contoh matang dari pendekatan ini [39].

Kategori di atas mencakup seluruh spektrum solusi, mulai dari arsitektur berlapis yang disempurnakan dengan pemicu lapisan hingga arsitektur tanpa lapisan. Memang, dalam tiga kasus pertama, organisasi berlapis dari arsitektur dipertahankan, tetapi independensi lapisan dan modularitas arsitektur tidak selalu dijamin. Umumnya, komunikasi interlayer masih mempertahankan modularitas arsitektur, sedangkan desain interlayer menghancurkan modularitas dengan mengeksploitasi desain bersama dari lapisan. Penyesuaian antar lapisan adalah penengah antara komunikasi antar lapisan dan desain antar lapisan. Terakhir, dalam pendekatan tanpa lapisan, konsep lapisan menghilang.

Meskipun ada beberapa proposal untuk memperkenalkan pengoptimalan lintas-lapisan dalam jaringan ad hoc seluler, sebagian besar dari pekerjaan ini hanya berfokus untuk menunjukkan peningkatan kinerja yang mungkin dilakukan dengan memperkenalkan lapisan- silang di antara dua hingga tiga lapisan tumpukan protokol, dan mereka tidak menanganinya. bagaimana interaksi lintas lapisan dapat diperkenalkan secara efektif dalam arsitektur jaringan. Hanya sejumlah kecil karya yang telah mendefinisikan arsitektur lintas-lapisan penuh; di antaranya, hanya dalam beberapa kasus implementasi arsitektur cross-layer telah disediakan, sedangkan proposal yang tersisa hanya divalidasi oleh simulasi.

Arsitektur MobileMAN [36] adalah salah satu dari sedikit (dan mungkin yang pertama) jenis arsitektur cross-layer untuk jaringan ad hoc yang telah diuji dan dievaluasi tidak hanya melalui simulasi tetapi juga diimplementasikan dalam prototipe nyata melalui pengukuran ekstensif kinerja telah dilakukan [25].

Gambar 1.3 menunjukkan arsitektur cross-layer MobileMAN. Dalam arsitektur ini, interaksi lintas lapisan diimplementasikan melalui berbagi data. Memang, seperti yang ditunjukkan pada Gambar 1.3, elemen kunci dari arsitektur adalah memori bersama, "Status jaringan"



Gambar **1.3** Arsitektur MobileMAN

pada gambar, yang merupakan tempat penyimpanan semua informasi status jaringan yang dikumpulkan oleh protokol jaringan—misalnya, nilai parameter protokol dan variabel status. Semua protokol dapat mengakses memori ini untuk menulis informasi untuk membaginya dengan protokol lain dan (b) membaca informasi yang dihasilkan/dikumpulkan oleh protokol lain. Ini menghindari duplikasi upaya lapisan untuk mengumpulkan informasi status jaringan, sehingga mengarah ke desain sistem yang lebih efisien. Selain itu, kerjasama antar lapisan dapat dengan mudah diimplementasikan oleh variabel bersama. Setiap protokol masih sepenuhnya diimplementasikan dalam satu lapisan, seperti pada arsitektur berlapis penuh

[40]. Oleh karena itu, pendekatan cross-layer MobileMAN dapat diklasifikasikan di antara solusi komunikasi interlayer; itu menggunakan memori bersama untuk mengimplementasikan komunikasi antar lapisan, yang menjamin tingkat kemandirian yang tinggi di antara lapisan.

Pendekatan MobileMAN untuk cross-layering, berdasarkan pembagian informasi antar

layer, telah diadops´i oleh arsitektur berturut-turut: WIDENS [41], GRACE [42], CrossTalk [43], ECLAIR [44], dan XIAN [45]. Perbedaan utama di antara arsitektur ini adalah cara berbagi informasi diimplementasikan dan jenis optimisasi lintas lapisan. Secara khusus, sementara WIDENS, CrossTalk, dan XIAN mengimplementasikan interaksi lintas-lapisan dengan (terutama) mengeksploitasi komunikasi antarlapisan, di GRACE dan ÉCLAIR parameter dari beberapa protokol dioptimalkan bersama (yaitu, penyetelan antarlapisan). Tabel 1.1 memberikan perbandingan dalam hal efisiensi dan fleksibilitas dari berbagai arsitektur cross- layer. Kami mengeksploitasi isi Tabel 1 dalam referensi 43 untuk mengisi baris kompleksitas/ overhead dan fleksibilitas Tabel 1.1.

Hasil yang disajikan pada Tabel 1.1 menunjukkan bahwa pendekatan MobileMAN menghadirkan kompleksitas terendah dan fleksibilitas tertinggi, menjadikan solusi MobileMAN salah satu arah yang paling menjanjikan untuk memperkenalkan interaksi lintas-lapisan dalam arsitektur mobile ad hoc dengan tetap mempertahankan prinsip-prinsip dasar (pemisahan lapisan). dan modularitas) dari arsitektur berlapis warisan.

1.2.2 Permasalahan dan Pembelajaran dari Penelitian MANET

Dari sudut pandang penelitian, penelitian MANET menghasilkan beberapa hasil penting (seperti yang dirangkum dalam Bagian 1.2.1), tetapi dalam hal implementasi dunia nyata dan penerapan industri, paradigma MANET tujuan umum yang murni mengalami eksploitasi yang langka dan minat yang rendah di antara pengguna. . Pembahasan yang luas tentang masalah utama dalam penelitian MANET disajikan dalam referensi 3, di mana ditunjukkan bahwa penelitian MANET pada umumnya kurang memiliki “realisme” baik dari perspektif teknis maupun sosial ekonomi.

Penelitian MANET terutama didorong oleh tantangan penelitian militer sementara penggunaannya untuk mendukung aplikasi sipil ditinggalkan. Memang, skenario MANET tujuan umum murni sangat cocok untuk skenario medan perang di mana paradigma komunikasi tanpa infrastruktur sepenuhnya—berdasarkan kerja sama di antara sejumlah besar node untuk menyampaikan lalu lintas melalui beberapa lompatan perantara dengan mengadopsi perangkat keras komunikasi khusus—sangat bermakna dan berharga. Di sisi lain, skenario ini tampaknya terlalu ambisius untuk aplikasi sipil di mana teknologi jaringan nirkabel off-the-shelf "terbatas" digunakan, dan kerja sama antar node tidak dapat diasumsikan secara apriori. Tidak ada upaya yang dilakukan untuk menyesuaikan skenario berbasis militer dengan skenario sipil yang realistis; akademisi hanya mengambil MANET tujuan umum murni

sebagai skenario yang relevan (juga untuk jaringan sipil) dan telah mencoba untuk mengatasi semua tantangan penelitian yang relevan terkait dengan skenario ini. Selain itu, penelitian MANET ditandai dengan terus munculnya tantangan penelitian baru (misalnya, keamanan dan kerjasama, manajemen energi, protokol transportasi) mengatasi masalah teoritis yang relevan, sedangkan rencana eksploitasi untuk teknologi ini telah ditinggalkan. Di sisi lain, untuk berhasil mem-bootstrap teknologi seperti MANET (berdasarkan kerja sama pengguna), sangat penting untuk membangun komunitas pengguna dengan menyediakan prototipe MANET dengan layanan komunikasi yang sederhana namun efektif (misalnya, berbagi file dan pengiriman pesan), di mana pengguna dapat merasakan fitur teknologi ini dengan tujuan untuk menguji penerimaan pengguna dan mungkin mengidentifikasi skenario aplikasi ios di mana paradigma jaringan ini dapat memiliki nilai tambah. Pada tahap awal ini, fitur jaringan tingkat lanjut (misalnya, mekanisme hemat energi dan/atau kerja sama dan keamanan) tidak berkontribusi pada pengalaman pengguna yang lebih baik; sebaliknya mereka membuat desain sistem lebih kompleks dan karenanya tidak stabil (karena kemampuan kemungkinan kesalahan

meningkat selama penerapannya), sehingga berdampak negatif pada pengalaman pengguna. Singkatnya, kelemahan utama dalam penelitian MANET adalah kurangnya implementasi, integrasi, dan eksperimen [46]. Kecuali untuk beberapa upaya dalam testbed APE

Universitas Uppsala, 1 testbed Eksperimental Dartmouth College, 2 dan proyek MobileMAN, 3 semua upaya penelitian berkonsentrasi pada pemecahan masalah teoritis yang sangat menarik untuk MANET tujuan umum murni dan menguji solusi yang diusulkan hanya melalui simulasi. Selain itu, studi simulasi MANET umumnya kurang akurasi, dan ini semakin mengurangi kredibilitas penelitian MANET. Memang, seperti yang dibahas secara luas dalam referensi 3 dan referensi di dalamnya, sementara penggunaan teknik simulasi dalam evaluasi kinerja jaringan komunikasi adalah area penelitian terkonsolidasi, sebagian besar studi simulasi MANET tidak menerapkan metodologi yang ditetapkan dengan benar. Masalah telah ditunjukkan dalam semua aspek studi simulasi, mulai dari model simulasi (misalnya, model mobilitas, karakterisasi saluran komunikasi nirkabel, dll.) hingga solusi model (misalnya, transient vs. steady-state). simulasi, alat simulasi, dll.) hingga analisis keluaran simulasi. Kurangnya akurasi, dalam satu atau lebih poin di atas, telah secara drastis mengurangi kredibilitas penelitian MANET.

Penelitian MANET juga lemah dari sudut pandang sosial ekonomi, bahkan jika dimensi sosial ekonomi dimasukkan dalam desain awal [47]. Umumnya, penggunaan paradigma MANET dilatarbelakangi oleh kemungkinan untuk membangun jaringan ketika tidak ada infrastruktur, atau untuk memiliki jaringan "bebas" di mana pengguna dapat berkomunikasi tanpa biaya asalkan kepadatan node cukup. Namun, beberapa laporan yang tersedia tentang persepsi MANET dari sudut pandang pengguna (lihat, misalnya, penyampaian proyek MobileMAN4) menunjukkan bahwa pengguna MANET potensial mengalami kesulitan besar

dalam melihat bagaimana jaringan ad hoc dapat membantu mereka dalam kehidupan sehari-hari.

Kemungkinan layanan komunikasi tanpa biaya tidak cukup untuk mengkompensasi kurangnya keandalan dalam komunikasi dan kesulitan tambahan dalam menggunakan jenis jaringan ini. Selain itu, pengguna mengatakan perlunya menggunakan teknologi ini untuk lebih memahami potensinya, sementara (seperti yang dikatakan sebelumnya) masih ada kekurangan penyebaran MANET yang dapat digunakan oleh pengguna yang tidak ahli.

Terakhir, pengguna ahli TIK (yaitu, mahasiswa Ph.D. ilmu komputer) yang memiliki kesempatan untuk secara langsung menguji teknologi MANET tidak dapat menunjukkan skenario di mana mereka dapat memperoleh manfaat yang jelas dari MANET tujuan umum

murni. Memang, aplikasi yang paling menarik dari teknologi ad hoc multihop yang mereka tunjukkan adalah dekat dengan definisi jaringan mesh.

1.3 JARINGAN AD HOC MULTIHOP: DARI TEORI KE REALITAS

Pada bagian sebelumnya kita telah meninjau penelitian MANET, menunjukkan bahwa, sementara dari sudut pandang penelitian beberapa hasil penting telah dicapai, MANET tujuan umum murni memiliki penetrasi yang langka di pasar nirkabel. Pada bagian ini kami menunjukkan bahwa dengan belajar dari pelajaran MANET, dan dengan mengeksploitasi hasil teoretis MANET dalam skenario jaringan yang realistis, komunitas ilmiah telah mampu merancang satu set paradigma jaringan ad hoc multihop baru yang saat ini menembus pasar massal. Secara khusus, seperti yang dibahas dalam referensi 48 untuk mengubah MANET menjadi komoditas, kita harus beralih ke pendekatan yang lebih pragmatis di mana beberapa kondisi berikut berlaku:

• Paradigma jaringan ad hoc multihop diperluas untuk menyertakan beberapa elemen infrastruktur

(misalnya, router mesh) untuk menyediakan ekstensi broadband Internet tanpa kabel yang hemat biaya. Jaringan mesh merupakan contoh yang paling relevan dari pendekatan ini. • Mobilitas

node tidak dianggap sebagai masalah untuk ditutup-tutupi (untuk mendukung tumpukan protokol

TCP/IP lama) tetapi sebagai peluang untuk dieksploitasi dengan merancang paradigma jaringan yang benar-benar baru. Jaringan oportunistik merupakan contoh yang paling relevan dari pendekatan ini.

• Paradigma jaringan ad hoc multihop diterapkan pada bidang-bidang khusus di mana sifat self-organizing dari paradigma ini dan tidak adanya infrastruktur yang digunakan sebelumnya merupakan nilai plus dan bukan batasan. Contoh penting dari pendekatan ini adalah jaringan berbasis aplikasi seperti, jaringan kendaraan dan jaringan sensor.

Pada bagian selanjutnya kita akan membahas secara singkat paradigma kerja jaringan ad hoc multihop yang muncul ini yang akan dianalisis secara mendalam pada bab-bab selanjutnya dari buku ini.

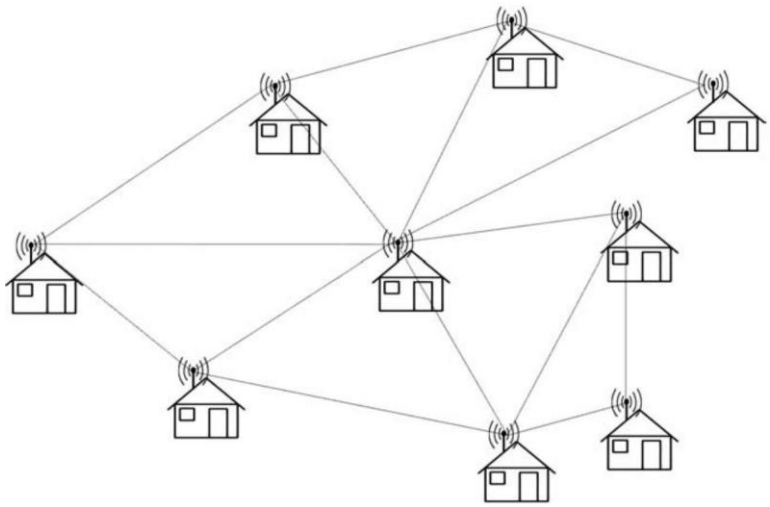
1.3.1 Jaringan Mesh

Paradigma mesh-network adalah contoh yang bermakna tentang bagaimana kita dapat mengubah paradigma MANET yang murni dan bertujuan umum (dan hasil penelitian terkait) menjadi pendekatan jaringan pragmatis yang segera mendapatkan pengguna dan penerimaan pasar.

Secara khusus, pendukung utama jaringan mesh adalah (i) serangkaian skenario aplikasi yang terdefinisi dengan baik untuk mendorong/memotivasi desainnya (yaitu, menyediakan ekstensi Internet yang fleksibel dan “berbiaya rendah”) dan (ii) pengurangan kompleksitas MANET dengan pengenalan backbone (tetap), yang membatasi dampak mobilitas node ke hop terakhir, menyediakan infrastruktur perutean yang tidak memerlukan kerja sama pengguna, melonggarkan batasan energi dalam desain protokol, dan seterusnya [49].

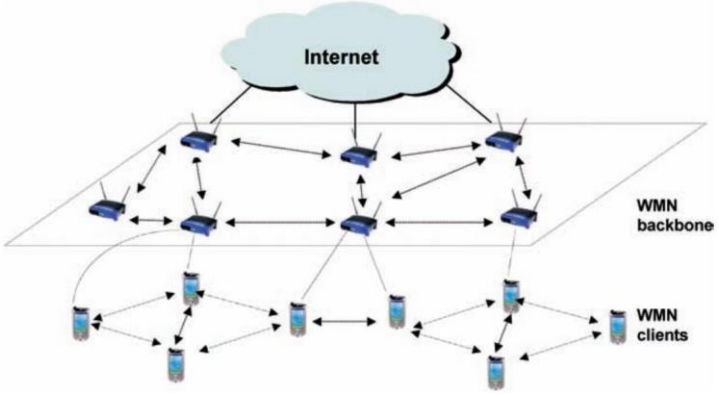
Penelitian pada jaringan wireless mesh (WMN), berbeda dengan MANET, sejak awal difokuskan pada implementasi, integrasi, dan eksperimen, untuk menguji solusi WMN pada jaringan nyata dengan pengguna nyata. Pada awalnya, WMN terutama dikembangkan sebagai hasil dari inisiatif komunitas

pengguna yang memasang tautan nirkabel IEEE 802.11 di antara rumah mereka untuk membentuk jaringan mesh komunitas (lihat Gambar 1.4) yang mendukung aplikasi seperti berbagi file atau VoIP. atau berbagi akses Internet kecepatan tinggi. WMN sekarang merupakan teknologi terkonsolidasi untuk perluasan Internet berbiaya rendah dengan tautan nirkabel beberapa hop, terutama menggunakan teknologi WiFi (lihat Gambar 1.5). WMN skala metropolitan sekarang menjadi kenyataan di banyak daerah perkotaan modern yang didukung oleh kotamadya dan organisasi pemerintah [50]. Memang, solusi telah dikembangkan untuk menyiapkan tulang punggung WMN yang kokoh (misalnya, lihat referensi 51 dan 52) dan untuk meneruskan data pengguna secara andal baik di dalam WMN dan ke/ dari Internet (misalnya, lihat referensi 53 dan 54). Namun, beberapa aspek dari teknologi ini masih dalam penyelidikan intensif agar teknologi ini lebih kuat dan mampu mendukung layanan yang lebih maju.



Gambar 1.4 Jaringan mesh komunitas

Masalah penelitian terbuka termasuk paradigma perutean baru [55], dukungan QoS [56– 58], keamanan [59], dan studi eksperimental versus simulasi [60]. Dua bab dari buku ini didedikasikan untuk beberapa topik penelitian hangat di bidang WMN. Secara khusus, Bab 7 menyajikan dan membahas penggunaan solusi multiradio dan multichannel untuk meningkat



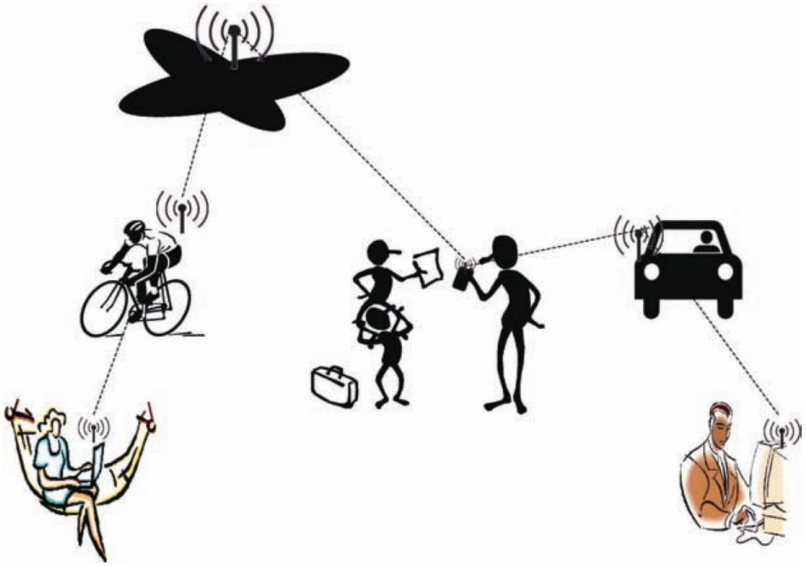
Gambar 1.5 Organisasi jaringan jala nirkabel.

1.3.2 Jaringan Oportunistik

Paradigma jaringan oportunistik adalah salah satu generalisasi paling inovatif dari paradigma MANET. Memang, sementara MANET mewakili pendekatan teknik untuk menutupi mobilitas node dengan membangun jalur end-to-end yang "stabil" seperti di Internet kabel, jaringan oportunistik tidak menganggap mobilitas node sebagai masalah (untuk menutupi) tetapi sebagai peluang untuk mengeksploitasi. Dalam jaringan oportunistik, mobilitas node menciptakan peluang kontak antar node, yang dapat digunakan untuk menghubungkan bagian jaringan yang tidak terhubung. Secara khusus, menurut paradigma ini (yang juga disebut sebagai jaringan yang toleran tunda atau tertantang), node dapat secara fisik membawa data yang di-buffer saat mereka bergerak di sekitar area jaringan, hingga mereka berhubungan dengan node next-hop yang sesuai—yaitu, sampai ada peluang penerusan. Dengan cara ini, ketika sebuah node tidak memiliki hop berikutnya

yang baik untuk meneruskan data, ia hanya menyimpan data secara lokal tanpa membuangnya, seperti y Selain itu, dengan paradigma oportunistik, data dapat dikirimkan antara sumber dan tujuan

meskipun jalur end-to-end antara dua node tidak pernah keluar dengan mengeksploitasi urutan grafik konektivitas yang dihasilkan oleh pergerakan node (lihat Gambar 1.6) . Oleh karena itu, paradigma jaringan oportunistik merupakan generalisasi dari paradigma Internet lama (di mana komunikasi dapat terjadi hanya jika



Gambar 1.6 Jaringan oportunistik

jalur end-to-end ada), dan tampaknya sangat cocok untuk komunikasi di lingkungan pervasif di mana lingkungan jenuh dengan perangkat (dengan teknologi nirkabel jarak pendek) yang dapat mengatur sendiri dalam jaringan untuk interaksi lokal di antara pengguna. Dalam skenario ini, jaringan umumnya

akan dipartisi dalam pulau-pulau yang terputus, yang mungkin saling terhubung dengan mengeksploitasi mobilitas node.

Jejaring oportunistik adalah bidang minat yang berkembang dengan beberapa masalah penelitian yang menantang. Sifat topologi jaringan yang dinamis dan sering tidak dapat diprediksi membuat perutean dalam jaringan oportunistik menjadi salah satu tantangan yang paling menarik. Hal ini telah menghasilkan kegiatan penelitian yang intensif di daerah tersebut, yang telah menghasilkan beberapa proposal untuk routing dan forwarding dalam jaringan oportunistik [61,62]. Saat ini, minat penelitian berfokus pada protokol perutean (seperti Bubble Rap [63], HiBOp [64], Propicman [65], dan SimBet [66]) yang mencoba mengeksploitasi konteks sosial node untuk perutean yang dioptimalkan.

Sementara perutean dalam jaringan oportunistik adalah area yang diselidiki dengan baik, area lain, seperti penyebaran data dan keamanan serta privasi, masih memerlukan aktivitas penelitian yang lebih intensif. Penyebaran data adalah tindak lanjut alami dari penelitian tentang perutean dan algoritma penangkalan. Salah satu kasus penggunaan yang paling menarik untuk jaringan oportunistik memang berbagi konten yang tersedia di perangkat pengguna seluler. Untuk alasan

ini, diseminasi konten sekarang menjadi area penelitian yang hangat di mana beberapa hasil menarik dapat ditemukan di referensi 67–69.

Privasi saat ini menjadi salah satu perhatian utama dalam jaringan oportunistik karena informasi konteks yang dipertukarkan di antara node (untuk memilih penerusan terbaik) mungkin menyertakan informasi yang masuk akal. Hasil yang sangat menjanjikan untuk mengatasi masalah disajikan dalam referensi 70. Keamanan adalah tantangan panas dan utama untuk jaringan oportunistik, karena pengguna seluler beroperasi saat bepergian di lingkungan terbuka, mungkin musuh. Pembahasan awal tentang enkripsi, dan ketangguhan terhadap penolakan serangan layanan untuk operasi protokol oportunistik dapat ditemukan di referensi 39. Masalah keamanan jaringan lainnya terkait dengan pencegahan babi sumber daya yang tidak terkendali (yaitu, individu yang tingkat pembuatan pesannya jauh lebih tinggi daripada rata-rata), yang secara signifikan dapat mengurangi kinerja jaringan [71].

Di dalam bidang jaringan oportunistik perlu diingat kegiatan penelitian yang dilakukan di dalam Kelompok Riset Jejaring Toleran-Tunda (DTNRG).

DTNRG adalah grup riset IRTF,5 yang mengembangkan arsitektur dan protokol untuk memperluas tumpukan protokol Internet agar dapat mengatasi partisi yang sering terjadi, yang dapat merusak perilaku protokol Internet lama (misalnya, TCP). Untuk tujuan ini, DTNRG telah mengembangkan overlay, bernama Bundle Layer Protocol, yang diimplementasikan di beberapa node jaringan (bernama node DTN) yang, selama fase pemutusan, menggunakan penyimpanan persisten untuk menyimpan paket yang akan diteruskan [72] . Lapisan bundel diimplementasikan di atas transportasi dan di bawah aplikasi dan bertujuan untuk menutupi pemutusan jaringan ke lapisan yang lebih tinggi. Alih-alih paket "kecil", lapisan bundel menggunakan unit data "panjang" untuk transfer data yang disebut "bundel". Gambaran umum kegiatan penelitian DTN disajikan pada referensi 73.

Jaringan oportunistik mengeksploitasi mobilitas perangkat untuk operasinya. Karena manusia biasanya membawa perangkat, mobilitas manusialah yang menghasilkan peluang komunikasi. Oleh karena itu, memahami dan memodelkan sifat-sifat mobilitas manusia merupakan area penelitian penting untuk jaringan oportunistik. Mempelajari jejak mobilitas manusia merupakan titik awal untuk memahami sifat-sifat mobilitas manusia. Tujuannya adalah untuk memberikan karakterisasi sifat temporal mobilitas perangkat/manusia dengan perhatian khusus pada waktu kontak (yaitu, distribusi durasi kontak antara dua perangkat) dan waktu antar-kontak (TIK) (yaitu, distribusi waktu antara dua kontak berurutan antar perangkat).

Karakterisasi distribusi TIK telah menimbulkan perdebatan besar dalam komunitas ilmiah di mana kelompok penelitian yang berbeda telah mengklaim hasil yang sama sekali berbeda mulai dari fungsi distribusi berekor berat—dengan [74] atau tanpa [75] batas eksponensial—hingga distribusi eksponensial. [76]. Dalam referensi 77, penulis telah menunjukkan hasil mendasar yang membantu menjelaskan perbedaan antara distribusi TIK yang diklaim oleh kelompok penelitian yang berbeda. Secara khusus, dalam makalah itu penulis menurunkan kondisi di mana, dengan memulai dari waktu antar-kontak eksponensial di antara beberapa node individu, kita dapat memperoleh distribusi TIK agregat berekor berat (yaitu, distribusi TIK antara beberapa node). Memahami sifat-sifat distribusi TIK merupakan masalah kritis karena distribusi ini mengontrol keefektifan beberapa protokol routing untuk jaringan oportunistik. Misalnya, dalam referensi 75 penulis telah menunjukkan bahwa untuk skema penerusan sederhana, seperti skema Dua-Hop, penundaan yang diharapkan untuk penerusan pesan mungkin tidak terbatas, tergantung pada sifat distribusi TIK. Hasil ini telah digeneralisasikan dalam referensi 78.

Menggunakan jejak dunia nyata sangat penting untuk evaluasi kinerja solusi jaringan oportunistik. Padahal, hanya dengan jejak seperti itu hubungan sosial antar pengguna dapat diperhitungkan dengan baik untuk analisis kontak antar pengguna dalam formasi. Misalnya, dalam referensi 79, penulis melakukan eksperimen penambangan data sosial yang menunjukkan bahwa kesamaan dalam profil pengguna dan informasi konteks yang terkandung di dalamnya meningkatkan kemungkinan kontak.

Mulai dari sifat mobilitas manusia yang diamati, beberapa model telah diusulkan untuk memberikan karakterisasi sintetik mobilitas manusia untuk digunakan dalam studi evaluasi kinerja yang digunakan untuk membandingkan dan membedakan mekanisme dan protokol yang dikembangkan untuk jaringan oportunistik. Beberapa model mobilitas, selain sifat antar kontak, juga merepresentasikan dampak hubungan sosial dalam mobilitas manusia [80,81]. Survei terbaru tentang model mobilitas manusia disajikan dalam referensi 82.

Pemodelan dan evaluasi kinerja saat ini merupakan salah satu bidang penelitian paling aktif dalam studi jaringan oportunistik. Contoh pekerjaan yang sedang berlangsung termasuk pemodelan protokol perutean (sadar sosial) dalam pengaturan heterogen [83,84], skema perutean berbasis konteks yang mempertimbangkan dimensi spasial dan temporal dari aktivitas node seluler untuk memprediksi pola mobilitas node [85] model teoretis baru untuk menyelidiki sifat grafik konektivitas yang mencirikan sifat konektivitas jaringan oportunistik [86].

Jaringan oportunistik saat ini merupakan bidang penelitian yang sangat aktif, dan oleh karena itu beberapa bab dari buku ini didedikasikan untuk menyajikan dan membahas berbagai aspek penelitian jaringan oportunistik: skenario aplikasi (Bab 9 dan 13), model mobilitas (Bab 8), oportunistik routing (Bab 11), dan penyebaran data (Bab 12).

1.3.3 Jaringan Ad Hoc Kendaraan (VANET)

Vehicular Ad hoc NETworks (VANETs) adalah contoh penting lainnya dari paradigma jaringan yang sukses yang muncul sebagai spesialisasi MANET (murni). Penelitian VANET dilatarbelakangi dengan baik oleh nilai sosial ekonomi dari sektor transportasi, yang mendorong pengembangan Intelligent Transportation System (ITS) canggih yang bertujuan untuk mengurangi kemacetan lalu lintas, jumlah kecelakaan lalu lintas, dan sebagainya. Sistem ITS lanjutan memerlukan komunikasi kendaraan-ke-jalan (V2R) dan kendaraan-ke-kendaraan (V2V). Dalam komunikasi V2R, kendaraan biasanya mengeksploitasi teknologi nirkabel berbasis infrastruktur, seperti jaringan seluler,

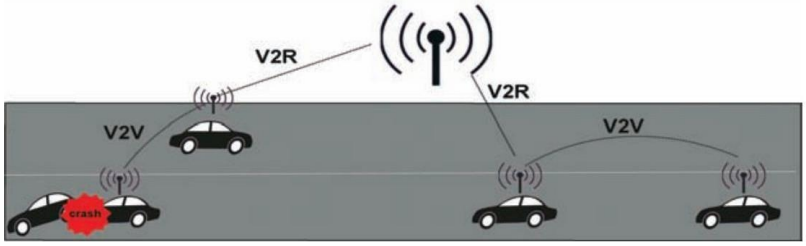
WiMAX, dan WiFi, untuk berkomunikasi dengan stasiun pangkalan/titik akses pinggir jalan.

VANET didasarkan pada paradigma jaringan multihop ad hoc. Secara khusus, menurut paradigma ini (lihat Gambar 1.7), kendaraan di jalan secara dinamis mengatur dirinya sendiri dalam VANET dengan mengeksploitasi antarmuka komunikasi nirkabelnya (misalnya, 802.11p; lihat Bab 2 dalam buku ini).

Bidang penelitian V2V mewarisi hasil MANET terkait dengan protokol routing/ forwarding ad hoc multihop [87], yang telah disetel dan dimodifikasi untuk menyesuaikannya dengan fitur khusus bidang kendaraan [88]. Perhatian khusus telah disediakan untuk pengembangan protokol penyiaran yang dioptimalkan karena beberapa aplikasi yang dikembangkan untuk jaringan ad hoc kendaraan menggunakan layanan komunikasi siaran [89,90]. Namun, tingkat mobilitas kendaraan yang tinggi dan kemungkinan skenario jaringan yang jarang (yang terjadi ketika intensitas lalu lintas rendah) membuat paradigma komunikasi store-and-forward yang digunakan di MANET menjadi tidak efisien, dan mereka mendorong ke arah adopsi yang lebih paradigma

store-carry-and forward yang fleksibel dan kuat yang diadopsi oleh jaringan oportunistik (lihat Bagian 1.3.2). Paradigma oportunistik yang diterapkan pada jaringan kendaraan

baru-baru ini menghasilkan banyak literatur terutama tentang protokol perutean dan penyebaran data



Gambar 1.7 VANET.

jaringan (misalnya, referensi 91 dan 92). Namun, masih ada beberapa isu yang menarik dan menantang untuk ditangani (misalnya, privasi [93]); perhatian khusus harus diberikan untuk mengembangkan model realistis untuk mengkarakterisasi mobilitas node VANET

[94] dan untuk mempelajari kinerja VANET secara analitis [95].

Sistem komunikasi V2R dan V2V dapat mendukung sejumlah besar aplikasi termasuk aplikasi keselamatan (misalnya, penghindaran tabrakan, peringatan hambatan jalan, penyebaran pesan keselamatan, dll.), informasi lalu lintas, dan layanan infotainment (misalnya, game, streaming multimedia, dll.) . Sebuah survei ekstensif aplikasi kendaraan disajikan dalam referensi 96.

Beberapa bab dalam buku ini dikhususkan untuk menganalisis tantangan penelitian terpanas dalam penelitian VANET. Bab 14 menyajikan taksonomi protokol komunikasi data untuk VANET. Bab 15 dan 16 masing-masing membahas simulasi dan eksperimen VANET. Bab 17 dan 18 fokus pada protokol dan teknologi VANET dengan menyajikan protokol MAC dan penggunaan teknologi radio Kognitif untuk membangun VANET. Bab 19 membahas evolusi dari VANET menjadi awan kendaraan.

1.3.4 Jaringan Sensor

Jaringan sensor dan aktuator memiliki peran besar terhadap konvergensi dunia maya/ fisik. Memang, informasi tentang realitas fisik, yang dikumpulkan melalui node sensor, diuraikan di dunia maya untuk menyempurnakan aplikasi dan layanan dunia maya ke konteks fisik, dan mungkin mengubah/menyesuaikan dunia fisik itu sendiri melalui aktuator [97]. Jaringan sensor nirkabel (dengan [98] atau tanpa aktuator [99]) karenanya memiliki peran utama dalam mengendalikan/menghubungkan dunia fisik dari/ke dunia maya [97]. Wireless Sensor Networks (WSNs) mewakili kelas "khusus" dari jaringan ad hoc multihop yang dikembangkan untuk mengontrol dan memantau peristiwa dan fenomena. Untuk tujuan ini, sejumlah node sensor (dengan antarmuka nirkabel) dikerahkan di dalam area pemantauan. Jika jaringan sensor cukup padat untuk menjamin jaringan yang terhubung, informasi yang dikumpulkan oleh node sensor dikirimkan, dengan mengikuti paradigma multihop melalui node sensor lainnya, ke sink node dan melalui itu ke Internet. Jika kepadatan sensor-node rendah, dan karenanya jaringan sensor terputus, elemen seluler (juga dirujuk sebagai bagal data atau feri pesan) digunakan untuk mengumpulkan data yang dirasakan dan mengirimkannya ke sink [100]. Memang desain jaringan ini sangat bergantung pada skenario aplikasi dan persyaratan aplikasi dalam hal keandalan, ketepatan waktu, dan sebagainya. WSN berhasil baik di akademi maupun industri, karena dikembangkan untuk menangani persyaratan aplikasi tertentu. Jadi, dalam sepuluh tahun terakhir mereka memicu kegiatan ilmiah intensif, yang telah menghasilkan banyak literatur untuk mengatasi beberapa tantangan penelitian WSN: efisiensi energi [101], protokol MAC [102], protokol routing [103], algoritma pengelompokan [101] 104], waktu [105] dan sinkronisasi jam [106], keamanan [107–109] jangkauan dan konektivitas [110.111], jaringan dengan mobile node [100], dan seterusnya. Literatur yang ada meninggalkan ruang yang sangat terbatas untuk menghasilkan karya ilmiah asli tambahan pada masalah warisan WSN seperti perutean, pengelompokan, protokol MAC, sinkronisasi, jangkauan, dan sebagainya. Di sisi lain,

penelitian lebih lanjut masih diharapkan untuk mengatasi (i) masalah mulai dari QoS hingga privasi. keamanan dan kepercayaan [112–117], (ii) topologi dan transmisi jaringan ([118.119]), (iii) simulasi dan eksperimen realistis ([120–122]), (v) skenario jaringan khusus [123.124], dan (vi) penggunaan jaringan sensor di lingkungan yang menantang seperti di bawah air [125.126] di bawah tanah [127], lingkungan industri [13], dan sebagainya. Buku ini mencakup beberapa topik penelitian

WSN tingkat lanjut, termasuk jaringan sensor bawah air (Bab 22 dan 23), sensor nirkabel dan jaringan robot (Bab 21), dan WSN dengan node pemanen energi (Bab 20).

Dalam waktu dekat, bidang penelitian yang sangat menjanjikan di bidang jaringan sensor terkait dengan tantangan baru yang muncul dari penggunaan ponsel sebagai alat penginderaan sentris manusia [128,129]. Secara khusus, kita dapat berpikir untuk mengeksploitasi miliaran perangkat/telepon seluler pengguna sebagai instrumen pengumpulan data sadar lokasi untuk pengamatan dunia nyata. Dengan cara ini kita dapat merasakan dunia fisik tanpa menggunakan jaringan sensor kita sendiri. Paradigma baru ini dikenal sebagai penginderaan partisipatif ketika orang mengambil peran aktif ke dalam tahap keputusan dari sistem penginderaan [130].

Desain sistem partisipatif berfokus pada alat yang membantu orang untuk berbagi, menerbitkan, mencari, menafsirkan, dan memverifikasi informasi yang dikumpulkan menggunakan perangkat kustodian [131]. Di sisi lain, dalam penginderaan oportunistik penjaga mungkin tidak menyadari aplikasi aktif; dalam hal ini kegiatan penginderaan dilakukan dengan eksploitasi (oportunistik) dari semua perangkat penginderaan yang tersedia di lingkungan setiap kali ada kecocokan dengan persyaratan aplikasi. Memang di dunia maya fisik yang konvergen, berbagai macam perangkat pintar yang tersebar di dunia fisik (seperti Tag RFID, Sensor dan Aktuator, Ponsel Pintar yang kaya Sensor,

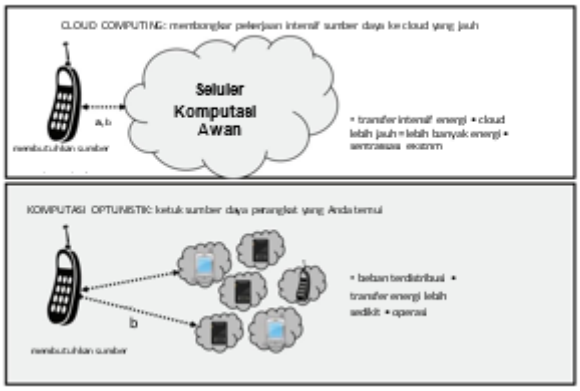
atau Teknologi Penginderaan Jarak Dekat) mengarah pada munculnya TIK yang sangat padat. infrastruktur untuk memantau dunia fisik dan mengumpulkan informasi tentang

perilaku dan persyaratan pengguna. Secara khusus, sensor multimodal yang tersebar di lingkungan dapat dieksploitasi secara oportunistik untuk menyimpulkan informasi yang tepat tentang perilaku sosial pengguna dan lingkungan sosial di sekitar mereka. Memang, penginderaan partisipatif dan oportunistik menawarkan peluang yang belum pernah terjadi sebelumnya untuk penginderaan perkotaan yang meluas [132]: untuk secara efektif mengumpulkan dan memproses jejak digital yang dihasilkan oleh manusia ketika berinteraksi dengan dunia fisik di sekitarnya dan dengan aktivitas sosial di dalamnya. Tujuan utama dari kegiatan penginderaan ini adalah untuk menyelidiki kota hibrida (yaitu, sebuah kota yang beroperasi secara bersamaan di dunia maya/digital dan fisik) dan untuk menyelidiki perilaku manusia dan hubungan sosial ekonominya [133]. Ini adalah tujuan penelitian yang sangat menantang dan inovatif yang dapat mengarah pada pengembangan

aplikasi perkotaan baru yang bermanfaat bagi warga, perencana kota, dan pembuat kebijakan.

Mempertahankan privasi individu yang menyumbangkan data penginderaan mereka merupakan tantangan utama untuk maju menuju penginderaan perkotaan yang meluas [134.135].

Solusi arsitektur untuk sistem penginderaan ponsel masih menjadi subjek penelitian terbuka [128]. Eksekusi lokal (eksklusif) dari tugas intensif komputasi tentu saja merupakan pendekatan yang kurang optimal. Sebaliknya, komputasi awan menawarkan sumber daya kelas atas dengan biaya energi yang tidak dapat diabaikan. Komputasi oportunistik [39.136] mungkin menawarkan yang terbaik dari kedua dunia [137]. Secara khusus, seperti yang ditunjukkan pada Gambar 1.8, perangkat individu dapat menggabungkan dan mengeksploitasi satu sama lain sumber daya untuk meningkatkan daya komputasi mereka dan mengatasi keterbatasan sumber daya mereka sendiri, tanpa jejak energi komunikasi dan sentralisasi ekstrim komputasi awan.



Gambar 1.8 Komputasi awan versus komputasi oportunistik dalam penginderaan ponsel.

1.4 RINGKASAN DAN KESIMPULAN

Dalam bab ini kita telah membahas evolusi paradigma jaringan ad hoc multihop dari perspektif penelitian dan penggunaan. Secara khusus, kami mulai dari paradigma MANET—yang diidentifikasi selama bertahun-tahun dengan paradigma jaringan multihop ad hoc—dan kami meninjau badan penting literatur ilmiah yang dihasilkan di bidang ini, dan yang diselidiki secara ekstensif dalam referensi 2.

Perhatian khusus telah diberikan dicadangkan untuk konsep cross-layer yang awalnya diselidiki di bidang MANET, sekarang menjadi konsep luas dalam literatur jaringan. Kami telah menyimpulkan analisis literatur MANET ini, menunjukkan bahwa paradigma MANET tidak berdampak signifikan pada pasar jaringan nirkabel karena beberapa kelemahan dalam desain aslinya. Secara khusus, kami telah mencatat bahwa penyebab utama kegagalan MANET adalah kurangnya realisme dalam desain jaringan ad hoc multihop murni skala besar dan tujuan umum. Selain

itu, kurangnya kredibilitas dalam studi simulasi MANET dan kurangnya implementasi, integrasi, dan eksperimen semakin membatasi dampak paradigma MANET. Namun, seperti yang dibahas dalam bab ini, pelajaran yang dipetik dari penelitian MANET telah mendorong evolusi pragmatis dari konsep jaringan multihop ad hoc yang

telah menghasilkan teknologi jaringan baru yang memiliki efek transformatif pada bidang jaringan tanpa kabel. Teknologi baru ini, yang meliputi jaringan mesh, oportunistik, kendaraan, dan sensor, telah menghasilkan beberapa tantangan penelitian baru yang saat ini menghasilkan kegiatan penelitian yang luas. Oleh

karena itu, sementara di referensi 2 kami menyajikan analisis mendalam tentang arsitektur dan bab dari buku ini didedikasikan untuk tantangan penelitian yang terkait dengan teknologi jaringan ad hoc multihop baru ini.

CHAPTER 2 TEKNOLOGI PENGUNGKAPAN DAN STANDAR UNTUK MULTIHOP MOBILE JARINGAN NIRKABEL

2.1 PENDAHULUAN

Standar memainkan peran penting dalam evolusi pasar dan teknologi komunikasi. Faktanya, pengguna peralatan jaringan yang sudah mapan—yaitu, telekomunikasi dan operator seluler lebih memilih untuk menggunakan teknologi standar karena (i) hal ini menghindari "vendor lock-in," yang dapat terjadi ketika pabrikan memonopoli komunikasi. mersialisasi teknologi tertentu dan dapat menyebabkan harga menjadi (jauh) lebih tinggi daripada nilai sebenarnya dari produk, dan (ii) standar mendukung diversifikasi pasar, sehingga mereka dapat memilih dari berbagai sumber, yang biasanya menghasilkan harga yang lebih rendah. Di sisi lain, produsen peralatan jaringan mendapat manfaat dari standar karena mereka memberikan referensi untuk apa yang ingin dibeli pengguna di masa mendatang dan, dengan demikian, membantu membuat investasi penelitian dan pengembangan lebih aman. Faktanya, banyak standar yang paling sukses (misalnya, GSM) lahir dengan kontribusi langsung yang signifikan dari pengguna akhir. Namun, sementara interoperabilitas adalah masalah yang tidak dapat diperdebatkan dalam pengembangan standar, produsen tidak dapat menerima bahwa semua perangkat bekerja persis sama, karena persaingan akan didasarkan pada tingkat harga saja. Oleh karena itu, standar biasanya meninggalkan beberapa aspek kunci yang tidak ditentukan yang tidak mempengaruhi interoperabilitas untuk menciptakan ruang tambahan bagi persaingan di antara pabrikan. Salah satu contohnya adalah alokasi/penjadwalan sumber

daya pada bidang data, di mana kinerja dapat ditingkatkan secara signifikan dengan pilihan "cerdas", tetapi komunikasi yang benar antar perangkat tidak terpengaruh.

Kami memulai survei kami tentang teknologi dan standar yang memungkinkan untuk jaringan nirkabel multihop seluler dengan mempertimbangkan yang telah diusulkan untuk mendukung transmisi multihop di jaringan BWA. Secara historis, fitur seperti itu terus-menerus diabaikan dalam grup standardisasi yang menangani BWA, karena yang terakhir biasanya bergantung pada stasiun pangkalan (BS) yang mengoordinasikan akses ke media. Koordinasi terpusat menghasilkan penggunaan kapasitas saluran yang lebih efisien dan memungkinkan penyediaan jaminan kualitas layanan (QoS) yang ketat, tetapi membuat multihop secara inheren menjadi tugas yang kompleks. Ini berbeda dengan banyak teknologi untuk WLAN

dan WPAN, seperti IEEE 802.11 [1] dan IEEE 802.15.4 [2], di mana akses media tidak terkoordinasi, untuk menjaga kompleksitas perangkat tetap rendah dan karena penggunaan pita frekuensi tanpa izin, yang dengan mudah mendukung penyebaran jaringan adhoc dan multihop. Oleh karena itu, kami melaporkan dua variasi standar untuk BWA di bawah ini, yaitu

IEEE 802.16, yang menambahkan dukungan multihop: mode mesh [3] dan amandemen IEEE 802.16j [4].

Kedua, kami meninjau kecanggihan teknologi WLAN dengan dukungan multihop. Karena penyebarannya yang luas, IEEE 802.11 mendominasi di area ini. Dalam beberapa tahun terakhir, standar terbukti serbaguna dalam mengadaptasi aplikasi yang berbeda dan kasus penggunaan melalui berbagai amandemennya, termasuk berikut ini yang disurvei dalam bab ini: IEEE 802.11s [5], IEEE

802.11z [6], IEEE 802.11n [7], dan IEEE 802.11p [8].1 Secara umum, dukungan multihop di domain WLAN memiliki catatan yang lebih panjang dan lebih gemilang daripada di BWA. Mungkin, ini karena teknologi WLAN, menurut definisinya, memiliki jangkauan terbatas dan, karenanya, biasanya dioperasikan dalam pita bebas lisensi. Dalam konteks ini, skema Medium Access Control (MAC) terdistribusi selalu lebih disukai daripada protokol terpusat, yang khas untuk jaringan seluler dan BWA. Faktanya, upaya untuk menambahkan koordinasi terpusat dalam IEEE 802.11 selalu gagal memenuhi penerimaan industri. Ini adalah kasus (i) fungsi koordinasi titik (PCF) [9], berdasarkan polling dan yang sudah termasuk dalam versi pertama dari standar yang dirilis pada tahun 1999 sebagai alternatif dari fungsi koordinasi terdistribusi (DCF) berbasis di mana- mana pada CSMA/CA, dan (ii) fungsi koordinasi hibrid (HCF) controlled channel access (HCCA) [10], yang ditambahkan dalam amandemen “e” yang dirilis pada tahun 2005 [11] dan menawarkan sarana untuk memberikan jaminan QoS deterministik , berbeda dengan akses saluran terdistribusi yang ditingkatkan (EDCA), yang sekarang menjadi arus utama dan hanya menyediakan layanan yang berbeda.

Ketiga, kami meninjau teknologi paling canggih yang mendukung komunikasi multihop (seluler) di WPAN. Jaringan ini umumnya dicirikan oleh jangkauan komunikasi pendek (yaitu, ÿ10 m) dan serangkaian kecepatan data yang luas, tergantung pada skenario penggunaan, mulai dari kecepatan tinggi, seperti yang dibutuhkan oleh aplikasi multi media yang berjalan pada perangkat elektronik konsumen di jaringan rumah [12], ke tingkat yang sangat rendah misalnya, untuk sensor nirkabel atau jaringan area tubuh yang terbuat dari perangkat berbiaya rendah dan konsumsi daya rendah [13,14]. Kami fokus khususnya pada WPAN tingkat rendah (LR-WPANs), yang kemampuan untuk mendukung topologi multihop/mesh sebagian besar diinginkan karena jangkauan komunikasi yang sangat terbatas, dibandingkan dengan area cakupan yang diperlukan dalam banyak penyebaran tipikal, seperti besar - skala pemantauan lingkungan [15]. Selain itu, topologi multihop/mesh juga memungkinkan kami untuk memenuhi persyaratan layanan tertentu seperti (a) meningkatkan keandalan melalui multipath routing dan (b) mendukung mobilitas node. Pada Bagian 2.4 bab ini, pertama-tama kami mengilustrasikan ekstensi IEEE 802.15.5 yang baru dirilis [16], memungkinkan topologi mesh di atas WPAN IEEE 802.15.4, dan kemudian kami fokus pada solusi multihop yang disediakan oleh Aliansi ZigBee [17]. Akhirnya, didorong oleh relevansi visi Internet of Things dalam perdebatan tentang evolusi Internet Masa Depan, kami menutup bagian ini dengan survei solusi berbasis IPv6 untuk WPAN yang saat ini sedang dikejar oleh IETF dan aliansi industri IPSO [18].

Akhirnya, kami menyimpulkan bab ini dengan membahas masalah dukungan mobilitas yang dapat dioperasikan dalam skenario heterogen di mana teknologi akses nirkabel yang berbeda (mungkin multihop) dilibatkan. Hal ini dilakukan dengan memperkenalkan standar IEEE 802.21 [19], yang mengusulkan serangkaian pesan dan prosedur netral teknologi untuk memungkinkan penyerahan media-independen (MIH) antara teknologi yang sama atau

berbeda dan dapat memfasilitasi mobilitas di lingkungan dengan tumpang tindih sebagian jaringan nirkabel,

terutama kombinasi dari BWA (misalnya, di tingkat kota atau kota) dan jaringan WLAN/WPAN (misalnya, di rumah atau kantor). Meskipun IEEE 802.21 tidak terkait langsung dengan komunikasi multihop, kami menganggapnya relevan dengan bab ini karena mewakili pendekatan yang berguna menuju integrasi dan interoperabilitas berbagai teknologi yang dijelaskan dalam bab ini.

2.2 TEKNOLOGI AKSES NIRKABEL BROADBAND

Pada bagian ini kami mensurvei standar yang paling relevan untuk multihop seluler di jaringan utama BWA: IEEE 802.16 mesh [3] dan penggantinya IEEE 802.16j [4]. Perlu disebutkan bahwa standar baru telah diterbitkan baru-baru ini oleh IEEE dan 3GPP untuk mobile BWA, juga termasuk dukungan relay

[20]: IEEE 802.16m [21] dan LTE-Advanced (LTE-A) [22]. Kedua standar tersebut telah disetujui sebagai sistem International Mobile Telecommunications- Advanced (IMT-Advanced) [23], yang memiliki persyaratan yang sangat menantang dalam hal tingkat kinerja yang ditawarkan—misalnya, laju data nominal 100 Mb/s ke pengguna bergerak dengan kecepatan tinggi dan 1 Gb/dtk ke pengguna statis atau nomaden. Namun, IEEE 802.16m dan LTE-A hanya mencakup sebagian dari fitur relai IEEE 802.16j dan karenanya tidak dibahas di sini.

2.2.1 IEEE 802.16 Jala

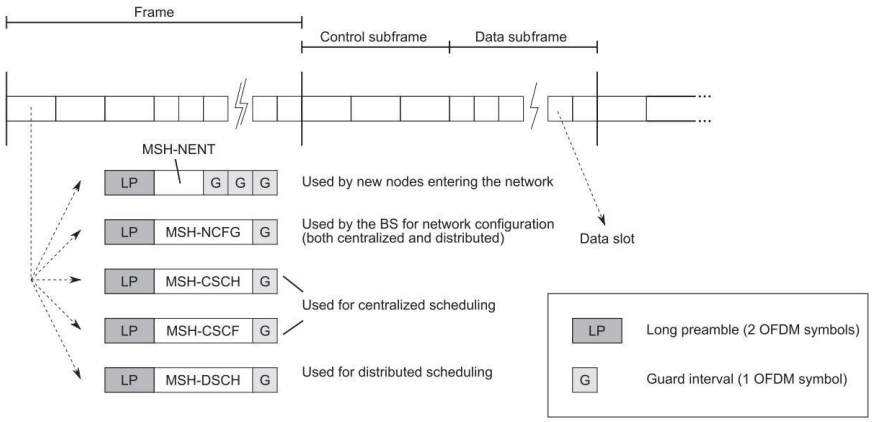
Standar IEEE 802.16 awalnya dirilis pada tahun 2001 [24], dengan fokus yang kuat pada penerapan fixed point-to-multipoint (PMP) sebagai alternatif kabel untuk konektivitas broadband, terutama di daerah pedesaan dan pinggiran kota [25]. Antarmuka udara yang didukung hanya didasarkan pada transmisi single carrier (SC), yang membutuhkan line-of-sight (LOS), yaitu peralatan mahal dan instalasi profesional. Sejak itu standar telah berkembang berkali-kali, termasuk rilis tahun 2004 [3], yang menyertakan antarmuka udara orthogonal frequency division multiplexing (OFDM), yang tidak memerlukan LOS karena ketahanan alaminya terhadap efek propagasi multipath.

Dalam rilis yang sama, mode mesh ditambahkan ke mode PMP untuk mengaktifkan multihop. Antarmuka udara tetap sama, tetapi ada perbedaan signifikan pada lapisan kontrol akses menengah (MAC) antara PMP dan mesh, sehingga kedua mode tersebut tidak dapat dioperasikan. Untuk yang pertama, kami merujuk pembaca yang tertarik ke salah satu dari banyak makalah survei tentang topik tersebut (misalnya, referensi 26), sedangkan kami menjelaskan mode mesh berikut ini.

Dalam IEEE 802.16-2004 ada dua mode jaring koordinasi: terpusat dan terdistribusi. Dalam

mode terpusat , BS bertanggung jawab untuk menentukan jadwal transmisi di seluruh jaringan. Dalam mode terdistribusi , transmisi dijadwalkan dengan cara terdistribusi penuh tanpa memerlukan interaksi apa pun dengan BS. Mode terdistribusi lebih fleksibel dan responsif daripada mode terpusat, karena keputusan dibuat secara lokal oleh node sesuai dengan beban lalu lintas dan status saluran fisik saat ini.

Waktu dipartisi menjadi bingkai dengan durasi tetap. Setiap frame terdiri dari subframe kontrol dan subframe data, seperti yang diilustrasikan pada Gambar 2.1. Kontrol subframe



Gambar 2.1 Struktur rangka.

dipartisi ke dalam slot dengan durasi tetap (selanjutnya disebut slot kontrol), yang terdiri dari tujuh simbol OFDM, dua di antaranya digunakan sebagai pembukaan fisik untuk menyinkronkan penerima, dan satu digunakan sebagai simbol penjaga. Hingga 16 slot kontrol dapat ditentukan per frame, tergantung pada konfigurasi jaringan. Slot kontrol diakses oleh node berdasarkan prosedur pemilihan terdistribusi yang ditentukan oleh standar. Ini memastikan bahwa, dalam keadaan stabil, setiap node mendapat kesempatan untuk mengirimkan pesan kontrol secara teratur, meskipun tidak berkala [27]. Prosedur ini menjamin bahwa tidak ada tabrakan yang terjadi dalam lingkungan dua-hop mana pun: Di satu sisi, ini agak konservatif dan dapat menyebabkan saluran kontrol kurang dimanfaatkan; di sisi lain, mekanisme tersebut tidak melindungi pesan kontrol dari interferensi kumulatif dari beberapa transmisi yang terjadi di

luar lingkungan dua-hop dalam slot kontrol yang sama, berpotensi menyebabkan kerusakan paket pada penerima. Versi yang lebih baik dari mekanisme akses slot kontrol telah diusulkan dalam literatur, (misalnya, referensi 28 dan 29), tetapi belum dimasukkan dalam rilis standar mana pun.

Subframe data terdiri dari slot mini data dalam jumlah tetap (selanjutnya disebut slot), hingga 256. Jumlah byte yang disampaikan oleh slot bergantung pada skema modulasi dan pengkodean (MCS) yang digunakan oleh pengirim untuk mengirimkan data ke penerima . Setiap node secara dinamis menyesuaikan MCS dari tetangga ke tetangga berdasarkan pengukuran kualitas sinyal yang diterima pada lapisan fisik. Namun, pesan kontrol ditransmisikan menggunakan modulasi dan skema pengkodean yang paling kuat—yaitu, QPSK dengan laju kode 1/2. Jaringan mesh IEEE 802.16 dapat menggunakan hingga 16 saluran noninterfering untuk transmisi data guna meningkatkan kapasitas transmisi yang tersedia untuk node terdekat yang tidak dapat mengeksploitasi penggunaan kembali spasial.

Namun, pesan kontrol ditransmisikan oleh semua node di jaringan pada saluran yang sama, yang diumumka Untuk mode terpusat dan mode terdistribusi, masalah alokasi bandwidth dibiarkan tidak

terpecahkan oleh standar IEEE 802.16, kecuali untuk menyediakan beberapa pesan kontrol

yang dapat digunakan untuk tujuan ini. Pembaca yang tertarik dapat menemukan diskusi teknis terperinci tentang masalah ini di referensi 30 dan dapat menemukan survei komprehensif pada algoritma penjadwalan yang telah dikemukakan dalam literatur untuk mengatasi masalah dalam referensi 31. Dalam mode terpusat, BS secara berkala menyebarkan ke tetangganya informasi konfigurasi pohon penjadwalan dalam konfigurasi penjadwalan terpusat mesh (MSH-CSCF) pesan, yang disiarkan ulang oleh node perantara, di masing- masing slot kontrol, hingga mencapai seluruh jaringan. Periode penjadwalan diadaptasi oleh

BS dari waktu ke waktu, bergantung pada waktu aktual yang diperlukan untuk prosedur flooding, yang, pada gilirannya, bergantung pada jumlah node dan topologinya serta konfigurasi jaringan—misalnya, jumlah slot kontrol per bingkai. Pohon penjadwalan ditentukan oleh BS berdasarkan proses permintaan/hibah, menggunakan pesan penjadwalan terpusat mesh (MSH- CSCH): SS mengirimkan permintaan kapasitas ke simpul induknya (yaitu, lompatan berikutnya menuju BS) menggunakan MSH-CSCH: Pesan permintaan; setelah BS menentukan alokasi sumber daya, pesan MSH-CSCH:Grant dikirim sebagai tanggapan. Mode terpusat tidak terlalu fleksibel, terutama karena alasan berikut: (i) tidak memungkinkan komunikasi SS-SS langsung dan, oleh karena itu, hanya cocok untuk skenario di mana

BS adalah pintu gerbang ke Internet, oleh karena itu semua lalu lintas di mesh diharapkan terjadi antara SS dan BS; dan (ii) alokasi sumber daya terjadi pada skala waktu yang agak lama, yaitu dalam urutan puluhan hingga ratusan frame (50–500 mdtk), yang mungkin tidak dapat beradaptasi dengan baik untuk aplikasi yang menghasilkan lalu lintas yang meledak (misalnya, transmisi video) atau aplikasi elastis tapi interaktif menggunakan TCP (misalnya, web browsing).

Algoritma untuk meningkatkan throughput jaringan dengan bersama-sama mempertimbangkan interferensi dan penghitungan hop untuk membangun pohon perutean

telah diuraikan dalam referensi 32, bersama dengan skema kontrol daya terdistribusi. Konstruksi pohon rute juga dipelajari dalam referensi 33, di mana throughput rute yang efektif ditingkatkan dengan membagi tautan panjang. Baru-baru ini, penulis dalam referensi 34 mengusulkan konstruksi pohon perutean bersama dan algoritme alokasi slot yang ditujukan untuk memaksimalkan penggunaan kembali spektral sambil memberikan jaminan QoS dan pembagian sumber daya tingkat MAC yang adil. Akhirnya, kami mengutip karya dalam referensi 35, di

mana kerangka optimisasi umum untuk WMN diusulkan, dengan algoritme perkiraan yang layak secara numerik terkait, yang cocok untuk konfigurasi jaringan mesh IEEE 802.16.

Mode terdistribusi menyelesaikan kedua masalah yang ditemukan dalam mode terpusat.

Pada kenyataannya, pengiriman data dikoordinasikan melalui prosedur jabat tangan tiga arah:

(i) sebuah node, yaitu peminta, meminta node tetangga, yaitu pemberi, untuk mengalokasikan beberapa bandwidth; (ii) pemberi mengiklankan satu set slot sebagai "diberikan" kepada pemohon; dan (iii) pemohon menegaskan bahwa ia benar-benar akan menggunakan rangkaian slot tersebut (atau bagiannya) untuk mengirimkan data. Ini dilakukan melalui pesan jadwal terdistribusi mesh (MSH DSCH), yang berisi daftar elemen informasi (IE), yang diklasifikasikan oleh standar IEEE 802.16 ke dalam empat jenis berikut. Sebuah permintaan IE menunjukkan

bahwa pemohon memiliki data yang ditujukan kepada pemberi yang menunggu pengiriman (yaitu backlog).

Pemberi mencadangkan bandwidth untuk pemohon menggunakan IE hibah, masing-masing berisi rentang slot pada rentang bingkai dalam saluran tertentu. Hibah dengan demikian dinyatakan sebagai tiga <rentang slot, rentang bingkai, saluran>; misalnya, < [3, 8], [4, 5], 1 > mewakili slot bernomor dari 3 hingga 8 dalam subframe data dari frame keempat dan kelima sejak hibah dikeluarkan, di saluran 1. Set yang sama dari parameter juga digunakan dalam IE konfirmasi, yang digunakan oleh pemohon untuk menyelesaikan tiga arah prosedur jabat tangan. Terakhir, IE ketersediaan dapat digunakan untuk melaporkan slot yang tidak dapat digunakan oleh pemohon untuk mengirimkan atau menerima data. Negosiasi bandwidth dalam mode terdistribusi secara implisit didasarkan pada asumsi bahwa hanya tetangga satu-hop penerima yang dapat mengganggu penerimaan data yang sedang berlangsung, kadang-kadang disebut sebagai "model protokol" [36]. Dengan kata lain, diasumsikan bahwa interferensi kumulatif node yang berjarak dua atau lebih lompatan dari penerima dapat diabaikan. Perlu disebutkan bahwa mode terdistribusi jauh lebih kompleks pada level SS daripada mode terpusat, di mana semua keputusan diambil oleh BS. Faktanya, pada yang pertama, node perlu melacak semua kombinasi <slot, frame, channel> yang tidak dapat diberikan kepada pemohon jika salah satu dari kondisi berikut ini benar: (i) pemberi mentransmisikan/menerima di <slot, bingkai>; (ii) pemohon mengirim/menerima dalam <slot, frame>; (iii) salah satu tetangga pemohon mengirimkan di <slot, frame, channel>.

Kondisi i dan ii diperlukan karena node memiliki satu radio, sehingga mereka dapat menerima dari atau mengirimkan pada satu saluran pada waktu tertentu, sedangkan kondisi iii hasil dari asumsi "model protokol".

Dalam referensi 37 penulis mengusulkan hibah bersama dan strategi penjadwalan paket yang ditujukan untuk memberikan keadilan proporsional, hanya mengandalkan informasi yang dipertukarkan oleh node sesuai dengan protokol MAC mesh IEEE 802.16. Ide dasarnya adalah bahwa setiap node menyimpan penghitung berapa banyak hibah yang diberikan untuk setiap aliran, yang diidentifikasi oleh pasangan sumber dan tujuan, dan menggunakan informasi tersebut untuk menyamakan alokasi sumber daya lokal. Strategi yang berbeda dicari dalam referensi 38, di mana penulis mengusulkan solusi untuk mencapai keadilan dengan menyetel parameter konfigurasi untuk mengakses slot kontrol oleh node. Terakhir, gabungan pendekatan terpusat dan terdistribusi diusulkan dalam referensi 39.

Terlepas dari strategi penjadwalan yang digunakan, unit data protokol MAC (PDU) digunakan untuk mengenkapsulasi dan mengirimkan data tingkat tinggi dalam slot yang dialokasikan. Setiap PDU menyertakan header MAC IEEE 802.16 dengan pengidentifikasi node (Node ID) dari pemohon dan pemberi, dan panjang PDU, prioritas (3 bit) dan prioritas jatuh (2 bit). Selain itu, kode redundansi siklik (CRC) 32-bit ditambahkan untuk memastikan keandalan data. Jika diperlukan, pemohon dapat memecah unit data layanan MAC (SDU) yang diterima dari lapisan atas menjadi beberapa PDU untuk membatasi pemborosan kapasitas. Fragmen SDU menimbulkan penalti overhead kecil, yaitu, 13 byte/fragmen, karena header MAC, termasuk subheader fragmentasi, harus ditambahkan ke setiap fragmen.

2.2.2 IEEE 802.16j

Seperti yang telah disebutkan, penetrasi industri dari mode mesh IEEE 802.16 dapat diabaikan; sebenarnya, itu telah dihapus dari standar sejak revisi tahun 2009 [40]. Hal ini terjadi terlepas dari potensi komunikasi multihop, yang telah terbukti menawarkan peluang tambahan untuk penerapan jaringan BWA yang efisien dalam banyak skenario praktis. Yang terakhir mencakup daerah berpenduduk jarang, di mana apa yang disebut stasiun relai (RS) membantu mencapai jangkauan yang luas, dan daerah perkotaan yang padat, di mana penghalang dan pantulan bangunan sering kali menciptakan banyak titik hitam, yang dapat dihilangkan dengan menggunakan RS ad hoc. Dalam kedua kasus, yang terbesar keuntungan dari multihop adalah pengurangan belanja modal (CAPEX) untuk penyebaran peralatan jaringan, dengan asumsi bahwa biaya RS secara signifikan lebih rendah daripada BS karena kompleksitasnya yang berkurang.

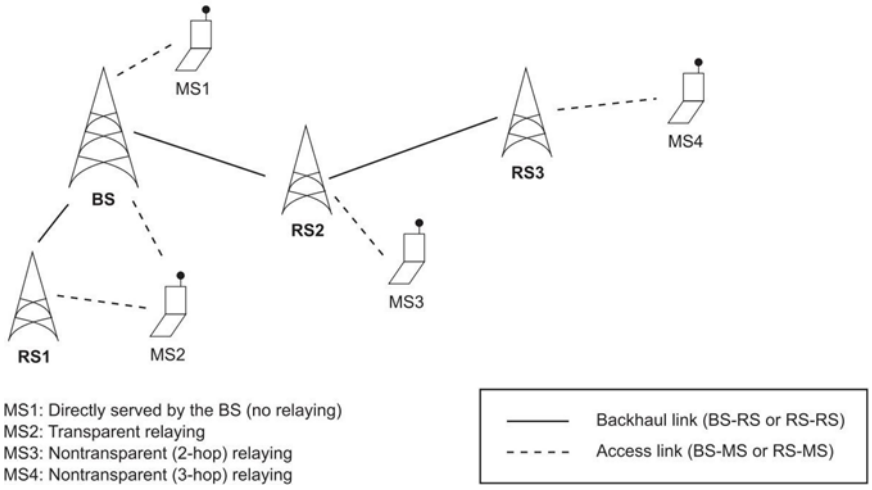
Untuk alasan ini, pada tahun 2006 kelompok tugas "j" dari Kelompok Kerja IEEE 802.16 mulai menyiapkan amandemen untuk pengenalan transmisi multihop sedemikian rupa sehingga keunggulan biaya dipertahankan. Dengan kata lain, mereka mempelajari pelajaran dari mode mesh IEEE 802.16 dan mendefinisikan mode multihop yang kompatibel dengan operasi point-to-point biasa, tidak hanya pada tingkat fisik tetapi juga pada lapisan atas.

Amandemen tersebut selesai pada tahun 2009 [4]; pada kenyataannya, sangat mungkin untuk mengoperasikan jaringan yang disusun oleh campuran mode point-to-point dan multihop. Hal ini pada akhirnya memungkinkan perlindungan investasi ke dalam lisensi spektrum operator sekaligus memungkinkan penetrasi IEEE 802.16j RS secara bertahap ke pasar. Fitur pembeda menonjol lainnya dari IEEE 802.16j sehubungan dengan mode mesh IEEE 802.16 adalah: (i) dukungan Mobile Stations (MSs) melalui antarmuka udara OFDMA dan dengan penggunaan teknik Hybrid Automatic Repeat reQuest (H-ARQ); dan (ii) penyediaan QoS dengan jaminan yang sama seperti dalam mode point-to-point. Perlu dicatat bahwa amandemen memungkinkan tingkat sewenang-wenang menyampaikan

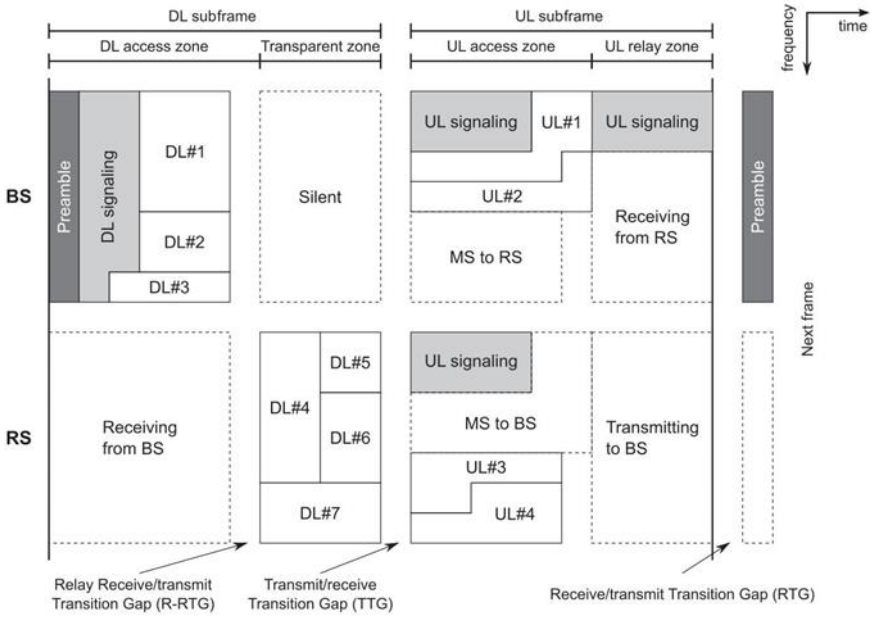
dari BS ke MS melalui satu atau lebih RS. Namun, keunggulan teknis dan ekonomis menjadi semakin tidak terlihat ketika lebih dari satu RS ditempatkan di antaranya.

IEEE 802.16j menetapkan dua tipe utama relaying, tergantung pada apakah MS dapat mendekode informasi kontrol dari BS atau tidak, masing-masing disebut transparan dan tidak transparan. Skenario ringkasan dengan berbagai mode operasi diilustrasikan pada Gambar 2.2.

Dalam penyampaian transparan , MS berada dalam jangkauan jangkauan BS, dari mana ia menerima semua informasi sinkronisasi dan kontrol. Namun, data pengguna disampaikan di kedua arah oleh RS dalam porsi khusus dari frame OFDMA, seperti



Gambar 2.2 Contoh skenario dengan semua mode operasi utama di IEEE 802.16j.



Gambar 2.3 Contoh struktur rangka (BS dan RS) dengan relai transparan.

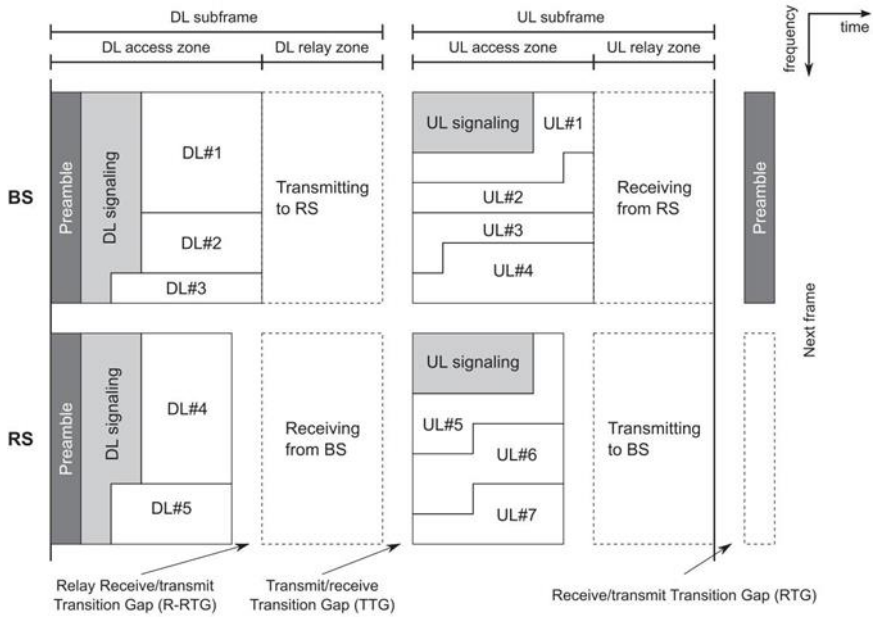
diilustrasikan pada Gambar 2.3. Mode ini disebut transparan karena MS bahkan tidak tahu bahwa ia sedang berkomunikasi dengan RS daripada BS, tetapi dapat menggunakan skema modulasi dan pengkodean (MCS) yang lebih efisien daripada yang mungkin dengan BS karena kedekatannya dengan relai . Dengan demikian, jenis moda ini menghasilkan peningkatan kapasitas, sedangkan jangkauan tidak ditingkatkan.

Di sisi lain, cakupan ditangani oleh mode relai lainnya, yaitu tidak transparan. Dalam mode ini, MS diasumsikan berada di luar jangkauan BS; karenanya, RS harus menghasilkan sinyal sinkronisasi dan kontrolnya sendiri, yang tumpang tindih dalam waktu dan frekuensi dengan sinyal dari BS, seperti yang ditunjukkan pada Gambar 2.4.

Perhatikan bahwa dengan relai nontransparan, RS diperlukan untuk menyediakan banyak fungsi lapisan MAC dari BS; karenanya kompleksitasnya (dan, karenanya, biaya) lebih tinggi daripada hanya menyampaikan transparan. Jenis relai opsional didefinisikan sebagai tambahan dari dua jenis relai wajib yang dijelaskan sejauh ini, yang bertujuan untuk mengeksploitasi keragaman kooperatif transmisi yang terjadi dari BS dan RS pada saat yang sama untuk

meningkatkan kinerja. Mode ini tidak dilaporkan di sini karena masalah kerumitan dan kebutuhan sinkronisasi yang ketat, yang membuat dampak praktisnya tidak pasti.

Dengan relai transparan, seluruh beban alokasi sumber daya berada di BS, karena RS hanya mendekode dan meneruskan MAC PDU. Ini disebut penjadwalan terpusat dan memfasilitasi penyediaan QoS karena BS memiliki semua data untuk dimasukkan ke algoritme internalnya. Mode ini juga dimungkinkan dengan relai tidak transparan, yang, bagaimanapun, juga memungkinkan penjadwalan terdistribusi. Dengan yang terakhir, data



Gambar 2.4 Contoh struktur rangka (BS dan RS) dengan relai tidak transparan. diarahkan ke/berasal dari kumpulan MS yang dilayani oleh relai digabungkan olehnya. BS kemudian "melihat" RS saja dan, karenanya, menerapkan algoritme alokasi sumber dayanya dengan cara yang kasar. RS kemudian memiliki tanggung jawab untuk membagi total bandwidth yang diberikan oleh BS di antara MS yang dilayani sedemikian rupa sehingga konsisten dengan jaminan QoS yang disepakati. Sementara mode ini menambah kompleksitas lebih lanjut ke dalam RS, ini berpotensi mengarah pada pemanfaatan spektrum yang lebih baik karena keputusan lokal yang dibuat oleh

RS dapat mengikuti perubahan saluran dan kondisi lalu lintas jangka pendek dengan lebih baik.

2.3 TEKNOLOGI WIRELESS LOCAL AREA NETWORKS

Pada bagian ini kami meninjau amandemen IEEE 802.11 terkait dengan evolusi menuju konektivitas

multihop seluler. Secara historis, karena sifat terdistribusi dari IEEE 802.11 MAC dan untuk mengatasi keterbatasan konektivitas dari jangkauannya yang rendah, multihop tampaknya merupakan pilihan yang sangat masuk akal untuk dikejar sejak awal standar. Pertama, kami meninjau amandemen "s" untuk IEEE 802.11 untuk jaringan mesh nirkabel. Kemudian, kami

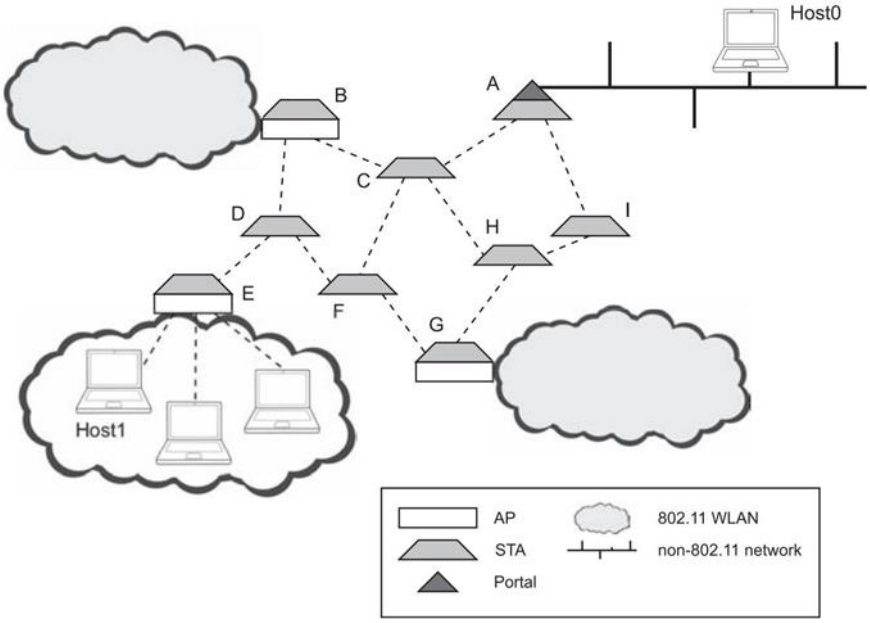
merangkum pencapaian yang paling relevan dari amandemen "n" dan "z" untuk IEEE 802.11. Semua amandemen IEEE 802.11 yang akan dijelaskan dalam bab ini telah dimasukkan dalam rilis

standar IEEE 802.11-2012 [1]. Kami menyimpulkan bagian ini dengan mengilustrasikan IEEE 802.11p untuk lingkungan jaringan kendaraan [8]. 2.3.1 IEEE 802.11s

Meskipun versi asli dari IEEE 802.11 tidak menyertakan dukungan untuk transmisi multihop, standar tersebut telah dipilih sejak awal (misalnya, referensi 41) sebagai kunci teknologi yang memungkinkan untuk berbagai jenis jaringan ad hoc, termasuk jaringan ad hoc seluler (MANET) dan jaringan mesh nirkabel (WMN). Selama bertahun-tahun, solusi eksklusif telah diajukan oleh industri dan sejumlah besar penelitian telah dilakukan pada topik tersebut, tetapi masih belum ada upaya standardisasi yang terungkap.

Ini sampai Task Group "s" telah dibentuk, dengan tujuan memperluas IEEE 802.11 untuk memberikan dukungan jaringan mesh. Standardisasi memakan waktu yang sangat lama, dibandingkan dengan amandemen lain di IEEE 802, dan berakhir pada September 2011. Implementasi awal open source dari IEEE 802.11s sedang dikembangkan dengan nama "open80211s" [42].

IEEE 802.11 memperkenalkan tipe baru jaringan 802.11, yang disebut mesh basic service set (MBSS), yang dibentuk oleh mesh station (STA) yang mampu mendukung pengiriman data melalui jalur multihop. Ketika MBSS digunakan sebagai backhaul nirkabel untuk LAN nirkabel yang diperluas (yaitu, sistem distribusi dari set layanan yang diperluas, menurut terminologi IEEE 802.11), titik akses tradisional (AP) dapat digabungkan dengan mesh STA, yang dengan demikian bertindak sebagai gerbang mesh untuk menyediakan akses jaringan ke STA nonmesh. Selain itu, portal juga dapat digabungkan dengan mesh gate untuk menghubungkan MBSS dengan segmen LAN 802.x lainnya. MBSS muncul untuk yang terakhir sebagai domain siaran tunggal — misalnya, untuk tujuan protokol spanning tree dan resolusi alamat L2. Contoh skenario jaringan diilustrasikan pada Gambar 2.5, dengan



Gambar 2.5 Contoh IEEE 802.11s WMN.

tiga AP dan satu portal. Dalam contoh ini, sangat mungkin bagi Host0 dan Host1 untuk menukar frame L2—misalnya, melalui rute A–C–F–D–E di dalam MBSS.

Untuk tujuan ini, total enam alamat MAC harus dibawa oleh frame di dalam MBSS: sumber dan tujuan akhir (Host0–Host1), sumber dan tujuan di dalam MBSS (A–E) yang digunakan untuk perutean, dan per-hop pemancar dan penerima (A–C, C–F, F–D, D–E). Karena header MAC pra-802.11 hanya memiliki ruang untuk empat alamat MAC, yang baru dihosting oleh subheader kontrol mesh khusus, yang memiliki ukuran variabel dari 6 hingga 24 byte dan juga mencakup bidang berguna lainnya (mis. MBSS untuk mendeteksi loop perutean).

Berikut ini kami memberikan pengantar halus untuk dua inovasi terpenting yang dibawa oleh IEEE 802.11 sehubungan dengan perutean dan MAC. Pembaca yang tertarik dirujuk ke makalah tutorial baru-baru ini [43] untuk panduan tambahan dan standar [1] untuk detail selengkapnya.

2.3.1.1 Perutean

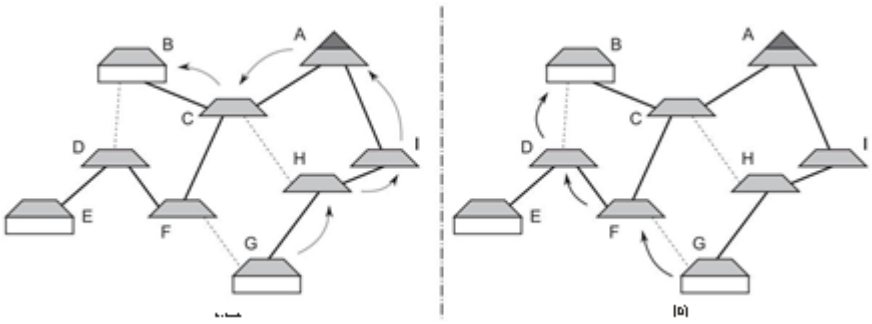
Dalam literatur ilmiah telah terjadi perdebatan panjang yang merupakan protokol routing terbaik untuk WMN (misalnya, referensi 44-47), dengan banyak fokus pada definisi yang tepat dari metrik tersebut mampu menangkap kualitas nyata dari jalur tanpa disesatkan oleh variasi saluran sementara dan ketidaknyamanan lain yang khas

dari jaringan nirkabel (misalnya, referensi 48 dan 49). IEEE 802.11 mengambil pendekatan agnostik, dengan mengizinkan vendor untuk menggunakan protokol routing dan metrik tautan pilihan mereka sendiri, satu-satunya kendala adalah bahwa semua STA mesh dalam MBSS menggunakan hal yang sama pada waktu tertentu. Bahkan, ketika dua STA mesh berada dalam jangkauan komunikasi satu sama lain, mereka memulai prosedur yang disebut manajemen peering mesh, di mana mereka bertukar kemampuan mereka, termasuk daftar protokol routing dan metrik yang didukung. Tautan antara mesh STA dibuat hanya jika ada kesepakatan bersama tentang konfigurasi dan aturan keamanan.

Namun, standar ini menyediakan protokol dan metrik perutean default untuk memungkinkan komunikasi dasar dan mempromosikan interoperabilitas, yang harus didukung oleh semua STA mesh di MBSS. Protokol perutean disebut Hybrid Wireless Mesh Protocol (HWMP) dan merupakan kombinasi dari protokol perutean proaktif berbasis pohon dan yang reaktif. Protokol proaktif adalah protokol di mana setiap node mengetahui jalur terbaik ke node lain dalam jaringan, terlepas dari kebutuhan di masa lalu atau masa depan yang dapat diperkirakan untuk berkomunikasi dengannya. Untuk tujuan ini, node secara periodik bertukar informasi link state, seperti protokol gateway interior (misalnya Open Shortest Path First—OSPF) yang dilakukan di Internet. Salah satu protokol routing proaktif yang paling awal adalah Destination Sequenced Distance-Vector (DSDV) [50],

dan ada banyak derivasi yang dioptimalkan, seperti Optimized Link State Routing Protocol (OLSR) yang banyak digunakan [51]. Di sisi lain, protokol perutean reaktif hanya menentukan jalur ke tujuan tertentu saat diperlukan. Protokol yang paling relevan dalam kategori ini adalah Dynamic Source Routing Protocol (DSR) [52] dan protokol routing Ad hoc On-Demand Distance Vector (AODV) [53]. Perbedaan utama antara keduanya adalah bahwa yang pertama (yaitu, DSR) membawa di setiap paket yang ditransmisikan rute lengkap ke tujuan, sedangkan yang terakhir (yaitu, AODV) menyimpulkan informasi semacam itu di node perantara dengan menyimpan tabel perutean sementara yang

diperoleh selama fase penemuan. Keuntungan utama dari protokol routing proaktif adalah jalur ke tujuan



Gambar 2.6 Contoh pohon routing dengan HWMP.

Pertukaran bingkai antara mesh STA G dan B ditunjukkan dengan (a) protokol routing proaktif dan (b) protokol routing reaktif. bila diperlukan (yaitu, pengurangan latensi), tetapi mereka melakukannya dengan (berpotensi) biaya tinggi untuk menjaga agar tabel perutean tetap mutakhir—yaitu, peningkatan overhead, yang, sebaliknya, tidak diperlukan dengan protokol reaktif.

Dengan HWMP, STA mesh diharapkan menggunakan perutean proaktif untuk mempertahankan rute ke/dari gerbang mesh dan portal—khususnya, ketika sejumlah besar lalu lintas diharapkan berasal dari dan ditujukan ke luar MBSS. Namun, jika STA jala mana pun ingin mengirimkan data ke yang lain tanpa melewati portal, ia dapat melakukannya dengan menemukan jalur terbaik melalui pendamping protokol perutean reaktif di HWMP, yaitu AODV. Pohon routing yang mungkin dari jaringan pada Gambar 2.5, sebagaimana ditentukan oleh protokol routing proaktif, diilustrasikan pada Gambar 2.6.

Jika mesh STA G ingin mengirim bingkai ke mesh STA B, ia dapat mengirimkannya melalui portal [misalnya, sepanjang jalur G–H–I–A–C–B yang berpotensi suboptimal (lihat sisi kiri gambar)] atau

memulai prosedur penemuan AODV, kemungkinan menemukan jalur yang lebih baik [misalnya, G– F– D–B (lihat sisi kanan gambar)]. Dalam kasus reaktif, STA perantara (yaitu, F dan D dalam contoh) harus melacak penemuan semacam itu untuk meneruskan frame yang dipertukarkan dengan benar antara mesh STA G dan B.

Akhirnya, sehubungan dengan metrik perutean default, IEEE 802.11s menggunakan apa yang disebut metrik airtime, yang merupakan turunan akhir dari waktu transmisi yang diharapkan (ETT) yang diusulkan dalam referensi 54. Gagasan utama metrik airtime adalah untuk mewakili biaya untuk melintasi tautan yang diberikan, dengan mempertimbangkan kecepatan data saat ini, overhead, dan perkiraan tingkat kesalahan bingkai, untuk bingkai nominal 1 kbyte.

2.3.1.2 MAC. IEEE 802.11s

menggunakan dua skema berbeda untuk mengakses media: EDCA, yang wajib dan diwariskan dari rilis standar konsolidasi industri sebelumnya, dan akses saluran terkoordinasi mesh baru (MCCA), yang bersifat opsional dan dijelaskan dalam pengikut.

MCCA mengizinkan dua tetangga mana pun untuk menegosiasikan interval waktu berkala, yang disebut peluang MCCA (MCCAOP), selama akses saluran dilakukan dengan pertentangan yang lebih rendah daripada selama interval non-MCCA. Secara khusus, akses ke media di IEEE 802.11 didasarkan pada CSMA/CA, yang parameter dasarnya adalah: minimum contention window (CWmin), maximum contention window (CWmax), dan arbitration inter- frame space (AIFS). Sejauh menyangkut MCCA, standar menentukan nilai khusus CWmin, CWmax, dan AIFS, yang dimaksudkan untuk membuat akses saluran jauh lebih efisien. Mesh STA sebenarnya diizinkan untuk memulai transmisi lebih awal, setelah periode diam terdeteksi, dan dengan backoff yang lebih kecil. Ini dapat dilakukan karena transmisi selama MCCAOP seharusnya dilindungi oleh prosedur MCCA untuk negosiasi slot (lihat di bawah). Perhatikan bahwa MCCA membutuhkan sarana untuk semua mesh STA untuk disinkronkan pada batas waktu tetap, yang disebut interval pengiriman pesan indikasi lalu lintas (DTIM). Hal ini dapat dicapai melalui prosedur IEEE 802.11s untuk sinkronisasi waktu dalam MBSS, yang menetapkan bahwa STA dapat mengadopsi aturan fungsi sinkronisasi waktu bersama (TSF) lebar mesh, menggunakan referensi waktu yang disertakan dalam beacon yang ditransmisikan secara berkala oleh setiap mesh STA.

Prosedur MCCA untuk negosiasi slot adalah sebagai berikut. Ketika STA, yang disebut pemohon, ingin membuat MCCAOP ke tetangga, yang disebut pemberi, ia mengirimkan pesan permintaan pengaturan MCCAOP (MREQ) yang merupakan bingkai kontrol MAC unicast dan mencakup bidang-bidang berikut: ID set MCCAOP, yang digunakan untuk secara unik mengidentifikasi MCCAOP dalam kombinasi dengan alamat MAC pemohon dan pemberi; durasi MCCAOP dalam slot; dan offset MCCAOP, dalam slot sehubungan dengan awal interval DTIM. Slot adalah unit alokasi waktu minimum dan sama dengan 32 ÿs. Opsional, periodisitas juga dapat dimasukkan untuk menentukan berapa banyak MCCAOP yang akan dialokasikan dalam interval DTIM. Misalnya, jika interval DTIM adalah 120 slot, durasi 10, dan offset 15, periodisitas 3 menyiratkan bahwa MCCAOP dialokasikan pada offset 15, 55, dan 95 sehubungan dengan permulaan interval DTIM. Pemberi balasan kepada pemohon melalui pesan unicast MCCA setup reply (MREP), yang dapat digunakan untuk menerima indikasi MCCAOP atau menolaknya. Dalam kasus terakhir, MCCAOP alternatif dapat diberikan secara opsional sebagai petunjuk kepada pemohon jika ingin mengulangi permintaan tersebut.

Baik MREQ dan MREP bersifat unicast; dengan demikian mereka hanya dipertukarkan antara dua STA yang terlibat dalam penyiapan MCCAOP. Informasi tentang MCCAOP yang aktif kemudian

disebarluaskan melalui pesan iklan MCCAOP (MADV) yang disiarkan secara berkala oleh seluruh STA. MADV mencakup waktu TX-RX dan laporan waktu yang mengganggu , yang merupakan dua daftar terpisah dari MCCAOP, dan fraksi akses menengah (MAF). Set waktu TX-RX adalah daftar MCCAOP yang STA periklanannya adalah pemohon atau pemberi. Set waktu yang mengganggu adalah daftar MCCAOP yang salah satu tetangga dari STA periklanan adalah pemohon atau pemberi, tetapi dirinya sendiri bukan keduanya. Daftar ini dapat dengan mudah diperbarui dengan menyalin MCCAOP di waktu TX-RX yang diterima oleh tetangga. Terakhir, MAF yang ditunjukkan oleh STA adalah rasio antara jumlah waktu TX-RX dan waktu interferensi, dengan interval DTIM. Jumlah kapasitas saluran yang dicadangkan untuk transmisi MCCA dinaikkan per dibatasi oleh parameter sistem yang disebut batas MAF, yang harus diterapkan oleh semua STA saat menegosiasikan MCCAOP baru. Sementara standar menentukan prosedur yang tepat untuk menegosiasikan MCCAOP, tidak ada algoritme

penjadwalan yang diamanatkan untuk menentukan durasi dan jadwal periodiknya, yang diserahkan kepada implementasi. Contoh algoritma untuk kondisi lalu lintas yang dinamis dapat dilihat pada referensi 55.

2.3.2 IEEE 802.11n dan IEEE 802.11z

Pada bagian ini kami menjelaskan secara singkat dua amandemen terbaru, yang tidak menambahkan fitur khusus untuk komunikasi multihop tetapi ditujukan untuk meningkatkan throughput. Oleh

karena itu, mereka mungkin mendukung difusi IEEE 802.11 dan memungkinkan dalam jangka panjang untuk mengeksploitasi peluang bisnis yang saat ini diremehkan dengan lebih baik atau menciptakan yang baru. Salah satu contohnya adalah penggunaan WMN dalam skenario rumah tangga untuk transmisi audio dan video definisi tinggi (HD)—misalnya, antara PC yang tersambung

ke Internet dan perangkat TV, yang memerlukan jumlah bandwidth yang tidak dapat dicapai. dengan rilis IEEE 802.11 saat ini.

Kami menjelaskan amandemen IEEE 802.11n [1] terlebih dahulu, yang membawa perubahan pada MAC dan lapisan fisik, semuanya bertujuan untuk meningkatkan throughput yang dapat dicapai. Pada lapisan MAC, pencapaian utamanya adalah spesifikasi agregasi bingkai opsional, yang merupakan proses menggabungkan beberapa bingkai MAC ke dalam semburan lapisan fisik yang sama yang ditransmisikan melalui udara. Meskipun teknik ini tidak mengubah kapasitas saluran mentah, dalam hal modulasi bit/s, teknik ini dapat secara signifikan meningkatkan QoS yang dirasakan dengan meningkatkan throughput bersih pada lapisan MAC.

Bergantung pada konfigurasi dan kemampuan perangkat, beberapa unit data layanan MAC (MSDU) dapat diagregasi menjadi satu agregat MAC SDU (A-MSDU), atau beberapa unit data protokol MAC (MPDU) dapat diagregasi menjadi satu agregat MAC PDU (A-MPDU). Penerima diperlukan untuk mendukung fitur spesifik yang diaktifkan untuk membongkar A-MSDU (atau A-MPDU) agregat dan meneruskan urutan MSDU (atau MPDU) nonagregat yang benar ke lapisan atas yang sesuai.

Dalam kasus agregasi tingkat PDU, penerima juga diharuskan untuk mengakui secara eksplisit setiap MPDU dalam burst, yang dapat dilakukan per grup untuk lebih mengurangi overhead pensinyalan. Teknik seperti itu sudah diusulkan, meskipun dalam bentuk yang sedikit berbeda, dalam amandemen “e” untuk IEEE 802.11 [11]. Agregasi bingkai tipikal di sebagian besar sistem telekomunikasi canggih, termasuk rilis awal IEEE 802.16, yang disebut "pengepakan", dan teknologi berbasis paket 3GPP—misalnya, Sistem Telekomunikasi Seluler Universal (UMTS) dan Evolusi Jangka Panjang (LTE), dimana fungsi ini dijalankan oleh layer yang sesuai di atas MAC, yang disebut Radio Link Control (RLC).

Namun, perubahan paling penting dari IEEE 802.11n, yang mendorong adopsi sangat awal di pasar konsumen bahkan sebelum standardisasi diselesaikan, berada di lapisan fisik dan berada di bawah antarmuka udara baru yang disebut High Throughput (HT). HT didasarkan pada orthogonal frequency division multiplexing (OFDM) dan dapat beroperasi pada frekuensi pembawa yang paling umum pada 2,4 GHz dan 5 GHz. Berbeda dengan perubahan pada MAC, fitur lapisan fisik baru meningkatkan kapasitas saluran mentah , dalam bit/dtk. Ini dilakukan dengan dua cara. Pertama, lebar saluran maksimum telah ditingkatkan dari 20 MHz menjadi 40 MHz, yang menggandakan kapasitas saluran maksimum.

Kedua, multiple input multiple output (MIMO) [56] digunakan untuk mengeksploitasi keragaman spasial, dengan perangkat yang dilengkapi dengan dua hingga empat antena untuk transmisi dan/atau

penerimaan. Kombinasi dari beberapa teknik MIMO berbeda yang didefinisikan dalam standar dapat digunakan di antara dua perangkat IEEE 802.11n, tergantung pada kecocokan sebenarnya dari kemampuan fisik dan perangkat lunaknya, yang meliputi space time block coding (STBC) dan beamforming. Terakhir, untuk meningkatkan kekokohan transmisi, adalah opsional untuk menggunakan kode pemeriksaan paritas rendah (LDPC) tingkat lanjut, yang diketahui memberikan kinerja lebih baik daripada kode konvolusional tradisional, dalam hal tingkat kesalahan bit, di bawah kondisi saluran yang sama. , tetapi lebih kompleks untuk diimplementasikan dan dieksekusi secara real time [57].

Seperti pendahulunya, antarmuka udara HT yang ditentukan oleh IEEE 802.11n menganut tradisi mendukung kompatibilitas mundur dengan antarmuka udara sebelumnya yang berperforma lebih rendah. Ini selalu karena volume besar perangkat yang telah diproduksi dan dijual di seluruh dunia menciptakan penghalang untuk setiap perubahan yang akan menyebabkannya menjadi usang terlalu cepat. Jelas, dari segi teknis, desain brownfield seperti itu kurang optimal. Untuk mengatasi dilema komersial versus teknis seperti itu, IEEE 802.11n secara opsional memungkinkan jaringan dioperasikan di bawah mode HT-Greenfield, di mana kendala yang berasal dari kompatibilitas ke belakang tidak berlaku. Namun, mode ini hanya diperbolehkan jika semua perangkat yang berkomunikasi (setidaknya) mampu IEEE 802.11n.

Oleh karena itu, pada hari-hari awal adopsi, HT-Greenfield mungkin akan jarang digunakan, tetapi kita dapat memperkirakan bahwa dalam jangka panjang akan ada lebih banyak jaringan HT- Greenfield, yang akan sepenuhnya mengeksploitasi peningkatan pada MAC dan lapisan fisik. dengan pengurangan overhead dan efisiensi spektral yang sangat ditingkatkan.

Kami mengakhiri bagian ini dengan survei IEEE 802.11z. Sejak amandemen “e” diterbitkan pada tahun 2005, mode pengaturan tautan langsung (DLS) telah ditambahkan ke standar.

Hal ini memungkinkan setiap dua stasiun dalam satu set layanan dasar (BSS), yaitu, dilayani oleh titik akses umum (AP), untuk membangun komunikasi langsung antara mereka, tanpa harus menyampaikan data melalui AP. Keuntungan dari mode tersebut ada dua: Di satu sisi, setiap frame hanya ditransmisikan sekali (stasiun-stasiun) daripada dua kali (stasiun-AP-stasiun), yang mengurangi latensi transmisi dan beban jaringan; di sisi lain, dua stasiun dapat menggunakan bit rate yang lebih tinggi daripada yang digunakan oleh AP, terutama jika mereka berdekatan satu sama lain, tetapi pasangan tersebut agak jauh dari AP. Setelah link langsung dibuat, stasiun masih harus mematuhi aturan yang biasa untuk mengakses media. AP harus mengetahui pembuatan

dan penghentian semua tautan langsung di BSS-nya. Amandemen “z” untuk IEEE 802.11 [1], yang dirilis pada tahun 2010, memberdayakan konsep tautan langsung dengan melonggarkan batasan terakhir ini. Untuk tujuan ini, ia menetapkan prosedur baru, yang disebut pengaturan tautan langsung terowongan

(tunneled direct link setup, TDLS), yang berbeda dan terpisah dari DLS, dan dilakukan antara dua stasiun dalam BSS tanpa intervensi/pemantauan AP.

Selain pengurangan overhead pensinyalan, salah satu keuntungan TDLS dibandingkan DLS adalah bahwa dua stasiun yang membuat tautan langsung dapat memiliki seperangkat kemampuan bersama yang berbeda dari AP yang terkait. Misalnya, mereka mungkin mendukung dan menggunakan saluran 40-MHz, sedangkan AP, maka BSS, dibatasi hingga 20 MHz. Selain itu, prosedur pengalihan saluran ditentukan, yang memungkinkan stasiun untuk memindahkan tautan langsungnya ke saluran frekuensi lain yang kurang ditempati. Bahkan dalam kasus ini, AP tidak mengetahui adanya bongkar muat sementara kedua stasiun tersebut dari BSS-nya.

2.3.3 IEEE 802.11p/GELOMBANG

Salah satu bidang penting di mana penggunaan teknologi nirkabel diharapkan tumbuh secara substansial, dan membawa manfaat yang signifikan bagi ekonomi dan masyarakat luas, adalah sistem transportasi cerdas (ITS). Secara umum, ini mengacu pada kontrol lalu lintas otomatis, berdasarkan data yang dikumpulkan secara real time dan model prediksi yang berasal dari informasi historis, untuk mencapai tingkat efisiensi transportasi yang baru.

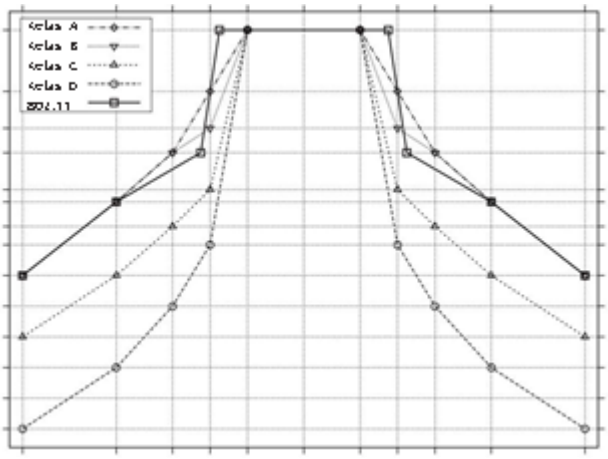
ITS akan meningkatkan kualitas hidup pengemudi, penumpang, dan warga negara, melalui pengurangan kecelakaan dan emisi CO2 yang signifikan [58]. Blok bangunan ITS adalah (a) unit sisi jalan (RSU), yang ditempatkan di sepanjang jalan untuk mengumpulkan pengukuran, menggerakkan umpan balik, dan bertindak sebagai gerbang untuk komunikasi kendaraan, dan

(b) unit di kapal (OBU), yang berada di mobil dan dilengkapi dengan sensor dan peralatan jaringan nirkabel untuk komunikasi dengan mobil lain, dengan cara kendaraan-ke-kendaraan (V2V), dan unit sisi jalan, dengan cara kendaraan ke infrastruktur (V2I). . Di tingkat internasional, ada kesepakatan umum bahwa versi modifikasi dari IEEE 802.11, yang disebut IEEE 802.11p [8], akan menjadi penentu tak terbantahkan sebagai teknologi untuk akses nirkabel di lingkungan kendaraan (WAVE) untuk memungkinkan komunikasi V2V dan V2I. Modifikasi utama IEEE 802.11p sehubungan dengan warisan IEEE 802.11 dijelaskan berikut ini.

Basis informasi manajemen (MIB) pada lapisan MAC telah diperluas untuk mendukung komunikasi antar node di luar konteks BSS. Padahal, di lingkungan perkotaan yang posisi kendaraan berubah dengan cepat, waktu yang digunakan untuk berkomunikasi bisa sangat singkat. Untuk alasan ini, sebuah node IEEE 802.11p dapat segera berkomunikasi dengan node lain, tanpa harus terhubung ke BSS tertentu, menggunakan identifikasi set layanan dasar khusus (BSSID) yang disebut wildcard BSSID [59]. Modifikasi ini menghindari latensi tambahan karena autentikasi dan asosiasi.

Lapisan fisik pada dasarnya didasarkan pada spesifikasi OFDM PHY dari IEEE 802.11. Namun, IEEE 802.11p mendefinisikan nilai penolakan saluran yang berdekatan dan tidak berdekatan yang lebih ketat, yang dapat diimplementasikan secara opsional dalam chip baru untuk mengurangi interferensi lintas saluran. Modifikasi ini tentunya meningkatkan kinerja komunikasi terutama dalam skenario yang padat, tetapi mungkin akan menyebabkan perangkat menjadi lebih mahal. Pita frekuensi yang dialokasikan untuk komunikasi di Eropa adalah spektrum 5,855 hingga 5,925 GHz. Meskipun standar IEEE 802.11 mendefinisikan tiga mode OFDM PHY (yaitu, 5, 10, dan 20 MHz), transmisi node dalam spektrum ini umumnya akan menggunakan operasi setengah jam dengan jarak saluran 10-MHz. Dengan cara ini, menggunakan panjang simbol OFDM dua kali lipat, sinyal akan lebih kuat terhadap

pemudaran—misalnya, mengurangi efek penyebaran Doppler dan interferensi antar simbol (ISI). Selanjutnya, node IEEE 802.11p diklasifikasikan ke dalam empat kelas daya, untuk membatasi daya pancar maksimum setiap stasiun. Selain laju jam, topeng emisi spektrum (SEM) juga diubah; faktanya, empat SEM tambahan ditentukan untuk setiap kelas daya. Gambar 2.7 menunjukkan perbandingan antara topeng spektrum yang digunakan dalam IEEE 802.11 dan yang digunakan dalam IEEE 802.11p, di mana kerapatan spektral daya maksimum yang diukur dalam saluran digunakan sebagai daya referensi dalam sinyal.

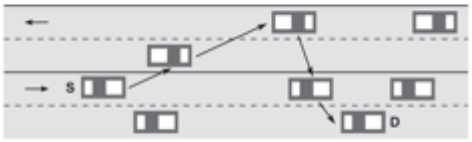


Gambar 2.7 Perbandingan antara mask spektrum pancar dengan jarak kanal 10 MHz.

IEEE 802.11p hanya mengalamatkan MAC dan lapisan fisik, seperti yang selalu terjadi pada standar dalam keluarga IEEE 802. Namun, untuk memiliki sistem komunikasi yang lengkap untuk V2V dan V2I, lapisan atas juga perlu distandarisasi. Upaya tersebut saat ini sedang dilakukan oleh badan standardisasi yang berbeda, yang saat ini dalam status mendefinisikan arsitektur-misalnya, IEEE dalam Kelompok Kerja Komunikasi Jarak Pendek Terdedikasi [60] dan ETSI dalam Komite Teknis ITS [61]. Berikut ini kami sketsa protokol GeoNetworking [62] awalnya diusulkan oleh proyek Eropa GEONET2 [63] dan kemudian distandarisasi oleh ETSI, yang menyediakan komunikasi di lingkungan bergerak tanpa memerlukan infrastruktur koordinasi dan memanfaatkan posisi geografis untuk penyebaran informasi dan pengangkutan paket data. Di ITS, GeoNetworking menyediakan komunikasi nirkabel di antara kendaraan dan di antara kendaraan dan stasiun tetap di sepanjang jalan, dan bekerja dengan cara tanpa koneksi dan terdistribusi penuh. Implementasi protokol open source baru-baru ini dirilis [64], yang juga telah diuji secara eksperimental [65] dan memungkinkan penerapan penemuan layanan sadar lokasi [66].

GeoNetworking pada dasarnya menyediakan dua fungsi [67]: pengalamatan geografis dan penerusan geografis. Tidak seperti pengalamatan di jaringan konvensional, kerja GeoNet dapat mengirim paket data ke sebuah node berdasarkan posisinya atau ke beberapa node dalam area geografis (melingkar, persegi panjang, atau ellipsoidal). Untuk penerusan, diasumsikan

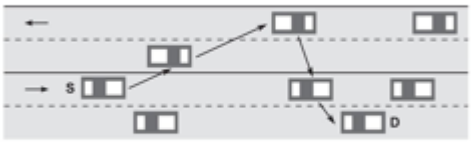
bahwa setiap node memiliki pandangan sebagian dari topologi jaringan terdekat dan bahwa setiap



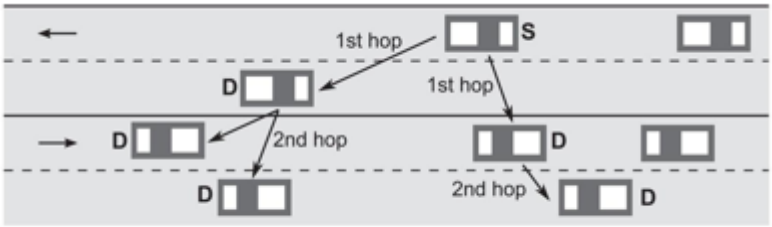
Gambar 2.8 Contoh GeoUnicast.

paket membawa alamat geografis. Ketika sebuah node menerima sebuah paket, ia membandingkan alamat-geo dalam paket data dan tampilan node pada topologi jaringan dan membuat keputusan penerusan yang otonom.

Perutean geografis terdiri dari skema penerusan berikut: GeoUnicast, GeoBroadcast, dan Siaran cakupan topologi. Gambar 2.8 menunjukkan contoh pengiriman paket antara dua node melalui beberapa hop nirkabel. Ketika sebuah node (S dalam contoh) ingin mengirim paket unicast ke tujuan (D dalam contoh), pertama-tama ia menentukan posisi tujuan dan kemudian meneruskan paket data ke sebuah node menuju tujuan, yang, pada gilirannya, kembali. -meneruskan paket di sepanjang jalur hingga paket mencapai tujuan.



Gambar 2.9 menunjukkan contoh siaran geografis. Sebuah paket diteruskan hop-by- hop hingga mencapai area tujuan yang ditentukan oleh paket, dan node menyiarkan ulang paket jika mereka berada di dalam area tujuan. GeoAnycast berbeda dari siaran geografis di mana node di dalam area tujuan tidak akan menyiarkan ulang paket yang diterima. GeoAnycast memiliki banyak aplikasi terkait keselamatan praktis; misalnya, kecelakaan mobil yang tiba-tiba harus diketahui hanya oleh mobil-mobil di area bahaya. Akhirnya, siaran cakupan topologi adalah ketika node sumber mentransmisikan paket yang disiarkan ulang untuk sejumlah lompatan tertentu. Pada Gambar 2.10 kami menunjukkan contoh penyiaran ulang di lingkungan 2-hop.



Gambar 2.10 Contoh siaran cakupan topologi. 2.4

2.4 TEKNOLOGI JARINGAN AREA PERSONAL

Teknologi referensi untuk LR-WPAN adalah standar IEEE 802.15.4 yang terkenal [2], yang revisi terakhirnya dirilis pada tahun 2011. MAC IEEE 802.15.4 mendukung port topologi jaringan bintang dan peer-to-peer. Yang terakhir berbeda dari yang pertama karena memungkinkan komunikasi langsung antara perangkat rekan tanpa melewati koordinator. Meskipun koordinator PAN unik ditunjuk juga dalam kasus ini, tidak ada batasan topologi tertentu yang dikenakan pada struktur jaringan peer-to-peer, yang karenanya dapat menjangkau banyak hop. Kemampuan routing multihop diperlukan untuk memungkinkan komunikasi end-to-end. Namun, penyediaan kemampuan tersebut, serta prosedur khusus untuk pembentukan jaringan, dianggap berada di luar cakupan spesifikasi IEEE 802.15.4, dan penerapannya didelegasikan ke lapisan di atas MAC. Berikut ini, kami menjelaskan bagaimana hal ini dicapai dalam teknologi canggih paling relevan yang dibangun di atas IEEE 802.15.4 untuk menyediakan kemampuan multihop seluler. Untuk perincian lebih lanjut tentang operasi MAC IEEE.802.15.4 yang mendasari fungsionalitas mesh yang akan dijelaskan berikut ini, kami merujuk pembaca ke standar [2,68].

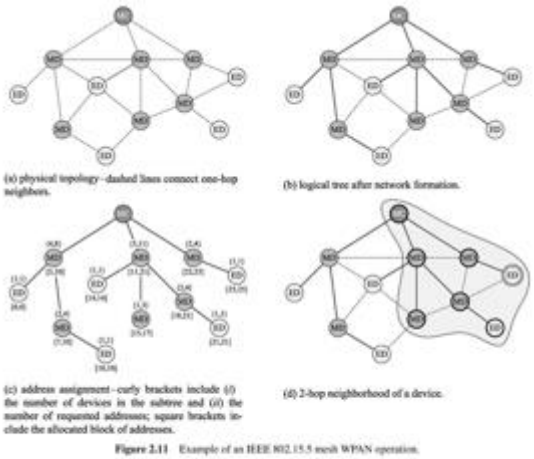
2.4.1 Standar IEEE 802.15.5

Standar IEEE 802.15.5 [16], dirilis pada tahun 2009, mendefinisikan sublapisan mesh di atas sublapisan MAC IEEE 802.15.4. Alasan di balik solusi mesh IEEE 802.15.5 adalah untuk memungkinkan tradeoff (dapat disesuaikan) antara perutean stateless, yang sebagian besar diinginkan untuk perangkat terbatas dengan penyimpanan terbatas, perhitungan, dan kemampuan energi, dan perutean stateful, yang sebaliknya memungkinkan untuk optimal routing melalui jalur berkualitas tinggi. Ini dicapai dengan melengkapi perutean implisit, diperoleh dari alamat logis yang mengikat ke topologi jaringan berbasis pohon, dengan pertukaran dan penyimpanan informasi status tautan lokal yang terbatas. Yang terakhir memungkinkan untuk memilih di antara jalur yang berbeda untuk mencapai tujuan tertentu, dan dengan demikian untuk mengatasi keterbatasan ketersediaan jalur tunggal dalam topologi berbasis pohon, yang dapat menjadi

tidak efisien dalam hal kualitas rute dan/atau sangat rentan terhadap partisi jaringan karena kegagalan tautan

IEEE 802.15.5 mendukung topologi jaringan mesh umum, seperti yang digambarkan pada Gambar 2.11a. Node diklasifikasikan menjadi perangkat mesh, yang mampu

menyampaikan frame, dan perangkat akhir, yang sebaliknya tidak mampu bertindak sebagai relai data.



(a) physical topology—dashed lines connect one-hop neighbors.

(b) logical tree after network formation.

(c) address assignment—curly brackets include (i) the number of devices in the subtree and (ii) the number of requested addresses; square brackets include the allocated block of addresses.

(d) 2-hop neighborhood of a device.

Figure 2.11 Example of an IEEE 802.15.5 mesh WPAN operation.

Di antara perangkat mesh dalam jaringan, terdapat mesh coordinator (MC), yang bertanggung jawab untuk mengelola jaringan mesh dan memainkan peran kunci, khususnya untuk tujuan pembentukan jaringan.

Semua perangkat di jaringan berbagi id PAN yang sama. Selain itu, dalam rilis IEEE 802.15.5 saat ini, hanya mode non-beacon-enabled yang diizinkan untuk komunikasi antar perangkat tetangga.

Sebelum perangkat dalam WPAN mesh IEEE 802.15.5 berhasil berkomunikasi satu sama lain secara end-to-end, prosedur pembentukan jaringan harus dijalankan. Ini diprakarsai oleh MC, yang memilih saluran dan id PAN yang sesuai, dan kemudian memulai pembentukan pohon logika yang menjangkau semua perangkat yang berpartisipasi dalam jaringan. MC secara default adalah root dari pohon, dan menjadi siap untuk mengirimkan pesan suar yang mengumumkan mesh PAN baru atas permintaan dari perangkat tetangga lain yang bersedia bergabung dengan jaringan. Operasi berikut kemudian diimplementasikan pada setiap perangkat non-MC sampai pohon diatur:

Perangkat memulai proses penemuan dengan melakukan pemindaian aktif pada rentang saluran yang berbeda sesuai dengan prosedur IEEE 802.15.4 standar. Secara khusus, pada setiap saluran dalam rentang yang ditentukan dan untuk durasi yang dapat dikonfigurasi, perangkat mengirimkan permintaan suar dan menunggu satu atau lebih perangkat mesh untuk membalas dengan pesan suar yang mengumumkan jaringan mesh tempat mereka terhubung.

Beacon mencakup informasi yang berguna untuk terhubung ke jaringan mesh, seperti id PAN,

tingkat pohon pengirim beacon, kualitas tautan yang diukur dengan penerimaan beacon, dan parameter jaringan lain yang terkait, misalnya hemat energi fitur. • Setelah proses penemuan selesai, perangkat penyambung memilih jaringan mesh untuk dihubungkan, jika lebih dari satu, dan

perangkat induk terbaik untuk bergabung dalam jaringan. Tingkat pohon dan kualitas tautan adalah metrik yang tersedia untuk memandu pilihan ini; namun, standar tidak menentukan kriteria khusus apa pun untuk menimbangnya, juga tidak mengecualikan faktor lain yang dapat diperhitungkan tergantung pada persyaratan spesifik aplikasi. Perangkat kemudian dikaitkan ke induk yang dipilih, sehingga bergabung dengan pohon. • Setelah bergabung dengan pohon, sebuah perangkat dapat memutuskan untuk bertindak sebagai perangkat mesh. Kemudian menjadi siap untuk membalas permintaan suar dari perangkat lain yang belum bergabung, dan akhirnya menerima permintaan

asosiasi mereka, jika dipilih sebagai simpul induk.Tidak ada batasan jumlah anak yang mungkin dimiliki perangkat mesh. Nomor tersebut dapat terikat secara administratif, tergantung pada kemampuan perangkat, atau dapat ditentukan dengan mengatur pengatur waktu yang sesuai setelah perangkat bergabung dengan jaringan. Saat penghitung waktu berakhir, perangkat jala akan berhenti menerima anak baru; jika tidak ada perangkat lain yang bergabung dengan jaringan melaluinya, perangkat mesh menjadi daun pohon. Perhatikan bahwa, dengan mengizinkan perangkat menerima asosiasi hanya setelah bergabung dengan pohon, loop apa pun dapat dihindari.

Hasil dari prosedur pembentukan jaringan terdistribusi yang dijelaskan di atas adalah, pada titik tertentu, sebuah pohon yang menghubungkan semua perangkat yang telah bergabung dalam jaringan, seperti pada WPAN IEEE 802.15.5 yang digambarkan pada Gambar 2.11b. Jaringan mesh, bagaimanapun, belum berfungsi sampai alokasi alamat dilakukan.

Yang terakhir dilakukan secara adaptif untuk memungkinkan pencocokan alokasi ruang alamat dengan distribusi aktual perangkat di sepanjang pohon yang dipertimbangkan, dan ini terdiri dari dua langkah. Langkah pertama adalah prosedur pelaporan dari bawah ke atas: Setiap perangkat melaporkan kepada induknya (i) jumlah perangkat di subpohon di mana perangkat tersebut adalah root (termasuk perangkat itu sendiri) dan (ii) jumlah alamat yang diminta, yang dapat harus benar-benar lebih besar dari yang sebelumnya, untuk mengakomodasi pertumbuhan subtree di masa mendatang.

Perangkat di tingkat menengah di pohon menunggu untuk menerima laporan dari semua anaknya masing- masing, dan kemudian mereka menghitung informasi untuk dilaporkan ke orang tua mereka sendiri. Proses tersebut berlanjut hingga akhirnya perangkat MC di akar seluruh pohon menerima informasi dari semua anaknya. Pada titik ini, langkah kedua dimulai, di mana alamat pendek 16-bit dialokasikan secara iteratif dengan cara top-down. Prosesnya dimulai oleh perangkat MC, yang mengalokasikan blok alamat pendek

16-bit berturut-turut ke masing-masing anaknya. Ukuran setiap blok tidak boleh lebih kecil dari ukuran subtree yang sesuai, tetapi bisa lebih kecil, atau bahkan lebih besar, dari jumlah alamat yang diminta selama

langkah sebelumnya, tergantung pada ketersediaan ruang alamat secara keseluruhan. Setiap perangkat mesh pada tingkat menengah akan mengulangi operasi yang sama dengan mengalokasikan ke dirinya sendiri dan anak-anaknya blok alamat yang ditetapkan oleh induknya, hingga akhirnya semua daun tercapai. Lihat Gambar 2.11c untuk contoh informasi yang dilaporkan selama fase alokasi alamat dan kemungkinan alokasi yang sesuai dalam WPAN mesh IEEE 802.15.5.

Sebagai hasil dari operasi ini, setiap perangkat mesh di pohon dialokasikan untuk penggunaan eksklusifnya satu blok alamat berturut-turut, yang mana yang pertama adalah alamat unicastnya sendiri. Selain itu, perangkat mengetahui blok alamat yang diberikan ke masing-masing anaknya. Karena itu, jaringan sekarang beroperasi, karena setiap perangkat mesh dapat merutekan frame secara implisit di sepanjang jalur, tanpa perlu mengumpulkan status perutean lebih lanjut. Faktanya, jika frame tidak dialamatkan ke perangkat mesh, maka alamat tujuan termasuk dalam blok alamat yang ditetapkan ke salah satu anaknya, atau tidak. Dalam kasus sebelumnya, lompatan berikutnya untuk menyampaikan frame adalah anak yang sesuai; jika tidak, dalam kasus terakhir, frame diteruskan ke perangkat induk pada rute default.

Seperti yang telah disebutkan di atas, pendekatan tanpa kewarganegaraan seperti itu dapat menghasilkan perutean yang sangat tidak efisien, tergantung pada bagaimana pohon logika disiapkan

selama pembentukan jaringan. Selain itu, setiap kegagalan tautan di sepanjang pohon akan menghasilkan partisi jaringan.

Oleh karena itu, informasi status tautan lokal juga dipertukarkan segera setelah alokasi alamat, untuk membangun pengetahuan lengkap tentang konektivitas tautan di dalam lingkungan (meshTTLOfHello+1)- hop , di mana meshTTLOfHello adalah parameter IEEE 802.15.5 yang dapat dikonfigurasi yang nilai default ke 2. Lebih khusus lagi, setiap perangkat mesh mulai menyiarkan pesan halo ke semua tetangganya. Setiap sage hello mes menyertakan blok alamat yang ditetapkan ke perangkat, tingkat hierarki, dan daftar blok alamat yang ditetapkan ke setiap tetangga satu lompatannya (seperti yang dipelajari oleh sage hello mes yang diterima sejauh ini). Pesan Hello kemudian diteruskan dengan menerima perangkat hingga meshTTLOfHello melompat dari pengirim aslinya. Dengan cara ini, setelah sejumlah pertukaran pesan halo, setiap perangkat dapat merekonstruksi matriks konektivitas penuh dari jaringan mesh di dalam lingkungan (meshTTLOfHello+1)-hopnya . Apalagi untuk

setiap perangkat di lingkungan, ia mengetahui blok alamat yang ditetapkan—yaitu, alamat yang mungkin dari setiap perangkat di subpohon yang sesuai. Lihat Gambar 2.11d untuk contoh lingkungan perangkat yang dipelajari melalui pertukaran informasi status tautan lokal.

Algoritme penerusan data sekarang dapat memanfaatkan informasi tambahan ini untuk meningkatkan kualitas perutean. Faktanya, jika frame yang akan diteruskan sekarang dialamatkan ke salah satu (meshTTLOfHello+1)-hop tetangganya, maka perangkat dapat dengan mudah menentukan hop berikutnya dari matriks konektivitas. Di sisi lain, jika alamat tujuan disertakan dalam blok alamat yang ditetapkan ke salah satu (meshTTLOfHello+1)- hop tetangganya (mungkin lebih dari satu), maka frame harus diteruskan ke tujuan melalui salah satu tetangga jangkar tersebut , dan hop berikutnya ditentukan sesuai. Jika tidak, perangkat dapat terus meneruskan frame ke induknya sebagai rute default, atau "menebak" perangkat jangkar yang mungkin lebih baik berdasarkan level pohon dan jarak lompatan setiap tetangga dari perangkat relai. Selain menyediakan peningkatan kualitas routing, mekanisme ini dapat dengan mudah menghasilkan ketersediaan beberapa perangkat next-hop menuju tujuan, yang juga meningkatkan ketahanan mesh routing.

Terakhir, mobilitas perangkat yang mulus hanya didukung sebagian oleh IEEE 802.15.5, dan terbatas pada perangkat daun. Mekanisme ini memang disebut oleh standar sebagai dukungan portabilitas . Ini didasarkan pada memungkinkan perangkat seluler untuk mempertahankan blok alamat asli yang ditetapkan, bahkan jika itu bergabung kembali dengan pohon melalui induk yang berbeda. Tujuannya adalah untuk memungkinkan perangkat mempertahankan konektivitas saat bergerak, dan bergantung pada induk sebelumnya dan lingkungan terkaitnya, yang bertindak sebagai semacam agen rumah terdistribusi untuk perangkat bergerak.

Selain yang dijelaskan di bagian ini, standar IEEE 802.15.5 mendefinisikan fitur tambahan

yang sangat penting dalam jaringan mesh WPAN, seperti siaran multicast dan andal, serta penghematan daya sinkron dan asinkron untuk perangkat mesh. Kami merujuk pembaca yang tertarik ke makalah tutorial terbaru [69,70] untuk informasi lebih lanjut tentang fitur tersebut, dan ke standar [16] untuk detail selengkapnya.

2.4.2 Standar Industri ZigBee

Ada beberapa standar industri untuk wireless mesh PAN, di antaranya yang paling penting adalah yang dipromosikan oleh HART Communication Foundation, dengan standar WirelessHART [71], International Society for Automation (ISA), dengan standar ISA 100.11a [72] , dan, yang tak kalah pentingnya, aliansi ZigBee, yang merilis versi pertama dari spesifikasinya pada tahun 2004 dan tentunya merupakan teknologi komunikasi nirkabel paling luas yang diadopsi dalam WPAN tingkat rendah yang digunakan dalam uji coba industri atau lingkungan bisnis. Berikut ini, kami fokus pada solusi mesh yang didefinisikan dalam versi terbaru ZigBee, yang telah dirilis pada 2007. ZigBee mendefinisikan lapisan jaringan di atas lapisan MAC IEEE 802.15.4. Tiga topologi yang berbeda diperbolehkan: bintang, pohon, dan mesh. Hanya dua yang terakhir yang memungkinkan komunikasi multihop, dan oleh karena itu mereka dipertimbangkan sebagai berikut. Prosedur pembentukan jaringan ditentukan, di mana pohon dibuat dengan koordinator ZigBee di akarnya.

Penemuan jaringan dan mekanisme asosiasi sangat mirip dengan yang didefinisikan oleh IEEE

802.15.5 (meskipun, tentu saja, yang ZigBee didefinisikan terlebih dahulu)

dan dijelaskan pada bagian sebelumnya. Penetapan alamat, bagaimanapun, dilakukan bersamaan dengan pembentukan jaringan dan bukan pada langkah selanjutnya, seperti yang diperlukan oleh spesifikasi IEEE 802.15.5. Secara khusus, dua alternatif skema penugasan alamat pendek 16-bit didefinisikan, yaitu skema penetapan alamat terdistribusi dan skema penetapan alamat stokastik .

Dengan skema penetapan alamat terdistribusi, blok alamat ditetapkan ke perangkat termediasi seperti pada IEEE 802.15.5. Penugasan, bagaimanapun, tidak adaptif tergantung pada bentuk pohon yang sebenarnya, tetapi secara statis ditentukan oleh set parameter yang telah dikonfigurasi sebelumnya — yaitu, kedalaman pohon maksimum, jumlah anak maksimum per node, dan jumlah maksimum perangkat router di antara anak- anak—yang juga membatasi struktur pohon selama pembentukan jaringan. Dengan menerapkan angka seperti itu, ukuran blok alamat yang akan ditugaskan ke perangkat router ditentukan dengan mempertimbangkan kasus terburuk dan hanya bergantung pada levelnya di pohon. Oleh karena itu, setelah perangkat router perantara bergabung dengan pohon dan telah diberi alamat awal bloknya, ia dapat segera menetapkan sub-blok alamat ke perangkat yang baru bergabung yang bersedia mengasosiasikannya sebagai induknya

di pohon. . Seperti pada IEEE 802.15.5, alamat pertama dari blok adalah alamat unicast dari akar subpoh

Selain itu, karena pengikatan antara hierarki ruang alamat dan struktur pohon yang sesuai, perutean stateless langsung diaktifkan: Ketika perangkat router harus menyampaikan sebuah frame, baik itu meneruskannya ke salah satu dari setiap router anak, jika alamat tujuan disertakan dalam sub-blok alamat yang sesuai, atau mengarahkannya sepanjang pohon ke induknya. Di sisi lain, karena ukuran blok alamat ditentukan secara apriori terlepas dari struktur pohon yang sebenarnya, dan sub-blok alamat tidak dapat dibagi antar perangkat, mungkin saja salah satu induk menghabiskan blok alamatnya sementara induk kedua memiliki alamat yang tetap tidak terpakai, meskipun pada prinsipnya mungkin ada pohon logika lain yang membentang di atas topologi fisik yang sama [73].

Jika perutean hirarkis stateless adalah satu-satunya mekanisme perutean yang diizinkan, maka MAC yang mendukung beacon, dan komunikasi CSMA/CA yang ditempatkan, juga diperbolehkan,

berdasarkan mekanisme MAC IEEE 802.15.4 yang mendasarinya. Di sisi lain, perangkat router mungkin memiliki kemampuan perutean stateful dan memelihara

tabel perutean untuk menentukan jalur penerusan ranjau. Entri tabel diperbarui melalui protokol AODVjr [74], versi sederhana dari spesifikasi protokol AODV [53], yang mempertahankan elemen penting AODV, termasuk mekanisme penemuan rute reaktifnya. Dalam hal ini, topologi jala penuh diperbolehkan untuk tujuan penerusan data, yang meningkatkan ketahanan dan pengoptimalan jalur, meskipun dengan biaya overhead yang meningkat dan kemungkinan konsumsi energi. Perutean hierarkis berdasarkan pohon yang dibuat selama pembentukan jaringan secara opsional masih dapat digunakan — misalnya, untuk mengakomodasi perangkat yang tidak memiliki kemampuan memelihara tabel perutean. Namun, operasi yang mengaktifkan suar tidak lagi diizinkan dalam kasus ini.

Skema penugasan alamat stokastik telah diperkenalkan pada rilis terakhir untuk mengatasi sebagian masalah kekurangan alamat yang mungkin terjadi karena alokasi inefisien yang inheren dilakukan dengan mekanisme terdistribusi. Sederhananya, dengan skema penetapan stokastik, saat perangkat bergabung dengan jaringan, induknya memilih alamat acak dan menetapkannya ke anak baru. Perangkat juga dapat menetapkan sendiri alamat acak. Dengan cara ini, ruang alamat menjadi sepenuhnya tersedia untuk jaringan,

terlepas dari topologi sebenarnya, dan, faktanya, jumlah maksimum parameter router anak dan kedalaman pohon tidak ada artinya dalam kasus ini. Di sisi lain, dengan skema seperti itu, perutean hierarkis tanpa kewarganegaraan tidak lagi diizinkan, dan juga diperlukan mekanisme tambahan untuk mendeteksi dan menyelesaikan kemungkinan konflik alamat.

Akhirnya, sejauh menyangkut manajemen mobilitas, dengan penetapan alamat terdistribusi tidak ada dukungan eksplisit untuk mobilitas perangkat akhir yang mulus. Faktanya, dalam kasus seperti itu, alamatnya sangat bergantung pada titik pohon tempat perangkat terpasang. Menjauh dari satu induk dan berasosiasi dengan node lain di PAN yang sama tentu menyiratkan perubahan alamat. Oleh karena itu, komunikasi terputus hingga prosedur penemuan perangkat dijalankan pada lapisan aplikasi. Di sisi lain, dengan penetapan alamat stokastik, alamat dapat ditetapkan sendiri. Oleh karena itu, saat perangkat akhir berpindah, perangkat tersebut mungkin mempertahankan alamat yang sama saat digunakan saat dikaitkan dengan induk baru. Prosedur penemuan dan pemeliharaan rute, didukung oleh perutean berbasis tabel, kemudian membantu mencapai mobilitas yang mulus.

2.4.3 WPAN Berbasis IPv6

Kebutuhan untuk mengintegrasikan jaringan area pribadi nirkabel berdaya rendah ke dalam jaringan tradisional baru-baru ini mendapatkan banyak perhatian menyusul keberhasilan

visi Internet of Things (IoT) dari Internet di mana-mana di masa depan, yang menghubungkan orang dan objek dengan mulus, sehingga memungkinkan pengembangan layanan cerdas baru tersedia kapan saja, di mana saja, oleh siapa saja dan apa saja. Rumah dan kota

pintar, sistem transportasi cerdas, e-health, otomasi industri, dan jaringan pintar adalah beberapa contoh area aplikasi di mana minat industri dan pemangku kepentingan terkait dalam menerapkan konsep IoT berkembang pesat.

Realisasi konsep tersebut, bagaimanapun, menimbulkan beberapa tantangan dalam hal interoperabilitas, keragaman aplikasi, dan skalabilitas. Untuk memenuhi persyaratan tersebut, IPv6 telah didorong sebagai solusi global, karena menyediakan arsitektur end-to- end yang independen dari

beragam teknologi komunikasi yang mendasarinya. Terlebih lagi, ini mencakup skema pengalamatan unik dengan ukuran ruang yang sesuai dan juga memberikan dukungan langsung untuk konfigurasi dan manajemen otomatis. Minat untuk solusi berbasis IPv6 untuk WPAN dibuktikan dengan meningkatnya perhatian seputar aktivitas standardisasi terkait dalam IETF, yang mengembangkan serangkaian solusi berbasis IPv6 untuk objek yang dibatasi (didukung oleh IPSO—IP untuk Smart Object— aliansi industri) , dan ETSI, yang mengembangkan arsitektur umum untuk komunikasi mesin- ke-mesin (M2M) yang dapat dioperasikan [75]. Selain itu, pada tahun 2009 ZigBee Alliance mengumumkan bahwa ZigBee akan mulai mengintegrasikan standar IETF seperti 6LoWPAN dan ROLL ke dalam portofolio spesifikasi masa depannya.

Mengadopsi IPv6 di LR-WPAN, bagaimanapun, tidak mudah. Faktanya, overhead protokol perlu dikelola secara efisien. Selain itu, perutean multihop harus berurusan dengan node yang dibatasi sumber daya dan sifat tautan nirkabel yang hilang. Mobilitas juga perlu didukung dengan cara yang sangat terukur. Dalam subbagian berikut, kami akan memberikan ulasan tentang bagaimana masalah tersebut saat ini sedang ditangani oleh pekerjaan yang dilakukan oleh IETF.

2.4.3.1 6LoWPAN.

Kelompok Kerja 6LoWPAN (IPv6 over Low-power WPAN) telah disewa oleh IETF pada tahun 2005 untuk menentukan lapisan adaptasi untuk IPv6 di

jaringan area pribadi nirkabel dengan perangkat terbatas dalam hal energi dan kemampuan pemrosesan. Meskipun secara khusus ditujukan untuk komunikasi nirkabel, dan

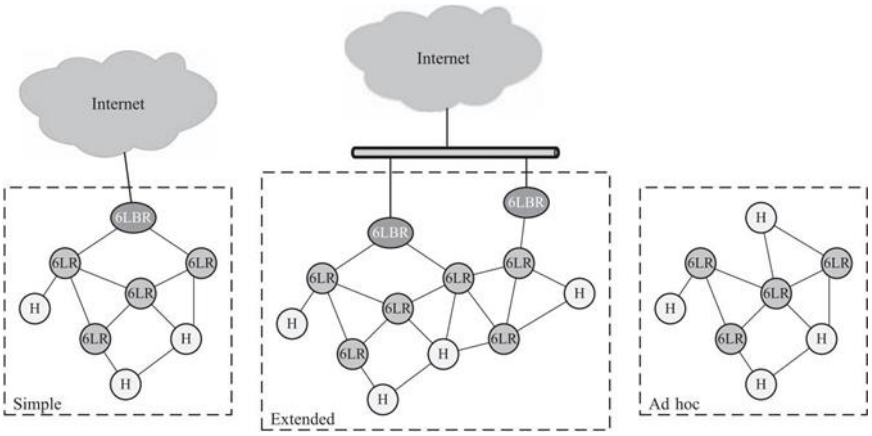
khususnya IEEE 802.15.4, minat 6LoWPAN, bagaimanapun, bergerak ke arah penyediaan dukungan untuk jaringan berdaya rendah dan lossy (LLN) yang lebih umum berdasarkan teknologi lapisan tautan lainnya, seperti, misalnya, Power-Line Communication (PLC) tingkat rendah. 6LoWPAN sejauh ini telah menetapkan lapisan adaptasi untuk IPv6 di

atas tumpukan IEEE 802.15.4 [76,77] dan operasi IPv6 Neighbor Discovery (6LoWPAN- ND) yang dioptimalkan dan diperluas di LLNs [78].

Jaringan 6LoWPAN adalah jaringan rintisan IPv6 dengan tiga jenis node: host (H), router (6LR), dan router perbatasan (6LBR), dengan alamat IPv6 unik yang terkait dengan antarmuka 6LoWPAN. 6LBR diasumsikan terpasang ke Internet melalui link backhaul atau backbone. Jaringan 6LoWPAN dapat bersifat ad hoc, sederhana, atau diperluas (lihat Gambar 2.12), tergantung pada jumlah router perbatasan: masing-masing nol, satu, atau lebih dari satu. Dalam kasus terakhir, semua router perbatasan diasumsikan terhubung juga melalui link backbone untuk bertukar pesan koordinasi terkait dengan operasi 6LoWPAN-ND [78]. Bagaimanapun, semua node dalam 6LowPAN yang sama berbagi awalan jaringan IPv6 yang sama; yaitu, sebuah node mengubah alamat IPv6 yang ditugaskan hanya ketika ia berpindah dari satu 6LoWPAN ke yang lain yang mungkin tumpang tindih (lihat Bagian 2.4.3.3). Mengenai operasi MAC IEEE 802.15.4

yang mendasarinya, tidak ada asumsi khusus yang dibuat; yaitu, mode yang mendukung suar dan non-

Konfigurasi otomatis alamat stateless tersedia: alamat IPv6 yang terkait dengan setiap node, baik tautan-lokal atau global, disusun oleh awalan 64-bit dan ID Antarmuka (IID) 64- bit. Untuk alamat global, awalan jaringan IPv6 diperoleh di bootstrap dari router tetangga melalui protokol 6LoWPAN-ND [78]. IID malah langsung



Gambar 2.12 Arsitektur jaringan 6LoWPAN. Garis solid yang menghubungkan node menunjukkan bahwa mereka berada dalam jangkauan komunikasi radio masing-masing.

dipetakan ke alamat lapisan tautan IEEE 802.15.4 yang mendasarinya, agar resolusi alamat menjadi tugas yang mudah. Fungsi pemetaan alamat ditentukan baik untuk alamat tambahan 64-bit IEEE 802.15.4, yang ditetapkan secara statis ke perangkat oleh pabrikan, dan untuk alamat pendek 16-bit. Dalam kasus sebelumnya, operasi 6LoWPAN-ND yang dioptimalkan memungkinkan untuk tidak melakukan deteksi alamat duplikat. Di sisi lain, karena alamat 16- bit diberikan oleh koordinator lapisan tautan menurut prosedur yang tidak standar—kita membahas di Bagian 2.4.1 dan 2.4.2 bagaimana hal ini dilakukan dengan cara yang berbeda oleh IEEE 802.15.4 dan ZigBee, masing-masing, sebagai bagian dari spesifikasinya— pendeteksian alamat duplikat IPv6 diperlukan dalam kasus ini, dan implementasinya di beberapa hop didukung dengan bantuan node 6LR dan 6LBR. Terakhir, DHCPv6 standar

[79] dapat digunakan untuk penugasan alamat dinamis; Node 6LR diharapkan menyampaikan pesan DHCPv6 ke node 6LBR bila diperlukan. Untuk detail lebih lanjut tentang optimalisasi dan ekstensi IPv6 ND untuk 6LoWPAN, kami merujuk pembaca ke referensi 78.

6LoWPAN mendukung routing dan forwarding multihop layer-2 dan layer-3, masing- masing disebut sebagai mesh-under dan route-over. Dengan konfigurasi mesh-under, perutean multihop dilakukan pada lapisan tautan melalui, misalnya, sublapisan jala IEEE 802.15.5, dan karenanya sepenuhnya tersembunyi ke IPv6. Dalam hal ini, semua node 6LoWPAN dilampirkan ke tautan IPv6 yang sama pada jarak satu lompatan satu sama lain. Oleh karena itu, hanya ada 6LBR dan host, dan tidak ada node 6LR. Di sisi lain, dengan konfigurasi route-over, perutean dan penerusan terjadi pada lapisan IPv6, dan protokol perutean khusus dapat dirancang untuk mengoptimalkan operasi tersebut dengan mempertimbangkan sifat spesifik jaringan 6LoWPAN — misalnya, protokol perutean RPL dijelaskan dalam Bagian 2.4.3.2. Alternatif ketiga juga tersedia, serupa dengan konfigurasi mesh-under, yang terdiri dari melakukan perutean dan penerusan di dalam lapisan adaptasi 6LoWPAN. Untuk tujuan ini, subheader mesh didefinisikan untuk membawa alamat link-layer tujuan akhir dan originator, serta batas hop. Namun, tidak ada protokol perutean khusus yang ditentukan oleh 6LoWPAN untuk kasus ini, maupun prosedur pembentukan jaringan IEEE

802.15.4. Perhatikan bahwa, dalam kasus di atas, tidak ada asumsi tentang kemungkinan pengikatan antara ruang alamat pendek 16-bit dan topologi 6LoWPAN [80].

Terakhir, 6LoWPAN mendefinisikan format bingkai untuk memungkinkan enkapsulasi pesan IPv6 ke dalam bingkai IEEE 802.15.4. Yang terakhir diperlukan untuk mendukung fragmentation dan reassembly, karena ukuran minimum MTU IPv6 adalah 1280 byte,

sedangkan IEEE 802.15.4 hanya dapat mengangkut paket hingga 127 byte, termasuk overhead. Selain itu, kompresi header yang efisien diimplementasikan untuk mengurangi overhead protokol IPv6 (lihat referensi 76 dan 77 untuk detail lebih lanjut).

2.4.3.2 Perutean.

ROLL IETF (Perutean Melalui Jaringan Berdaya Rendah dan Rugi) Kelompok Kerja berfokus pada persyaratan perutean dan solusi untuk LLN. Beberapa skenario aplikasi dipertimbangkan untuk jaringan seperti itu, termasuk otomatisasi industri, bangunan pintar, jaringan pintar, dan seterusnya, dan persyaratan perutean khusus telah ditentukan untuk subsetnya [81–84]. Sejauh menyangkut solusi, ROLL WG hanya mempertimbangkan solusi perutean IPv6; dan khususnya protokol perutean IPv6, bernama RPL [85], telah ditentukan untuk LLN di salah satu

skenario aplikasi yang disebutkan di atas. Sehubungan dengan alternatif konfigurasi perutean 6LoWPAN, RPL mengklasifikasikan dirinya sebagai solusi rute-over murni, yang lebih disukai daripada yang lain karena meniru domain siaran tunggal pada lapisan tautan dalam jaringan nirkabel multihop dianggap sebagai tugas yang menantang dan mahal. Untuk pembahasan lebih lanjut tentang debat route-over versus mesh-under, kami merujuk pembaca ke referensi 86 dan 87, Bagian 5.3.

Sama halnya dengan solusi mesh IEEE 802.15.5 dan ZigBee, RPL membangun topologi jaringan di atas beberapa domain broadcast link-layer yang tumpang tindih dalam LLN.

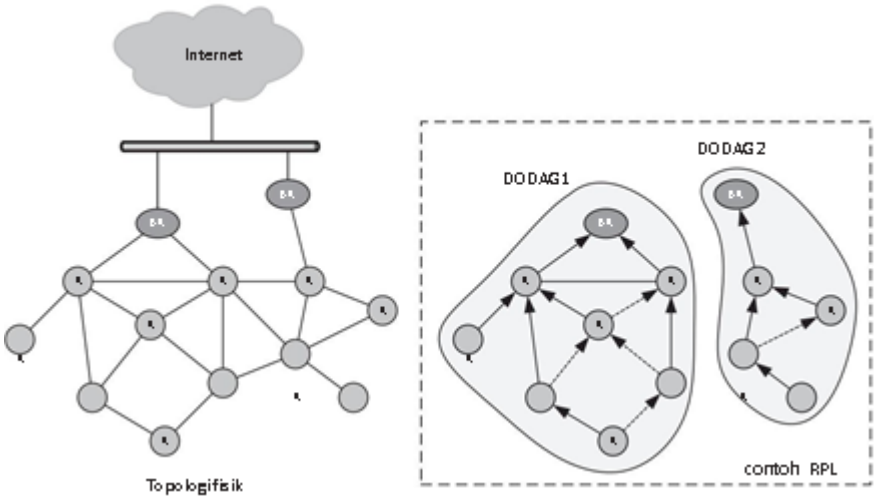
Rute multihop kemudian dihitung berdasarkan protokol vektor jarak. Juga diasumsikan bahwa rute tersebut harus dioptimalkan untuk pengiriman lalu lintas ke sejumlah sink node yang dipilih (yaitu MP2P routing). Alih-alih mempertimbangkan topologi pohon minimal, RPL membangun grafik asiklik terarah (DAG) yang terdiri dari DAG berorientasi tujuan (DODAG) sebanyak jumlah sink node, masing-masing di akar DODAG yang sesuai. Namun, setiap simpul RPL dapat dimiliki oleh paling banyak satu DODAG, artinya, jika beberapa DODAG didefinisikan—misalnya, dalam kasus perluasan 6LoWPAN (lihat Gambar 2.12)—kumpulan DODAG akan mempartisi seluruh jaringan. Namun diharapkan sink node akan dapat berkomunikasi melalui link backbone umum, yang juga memungkinkan untuk mengatur satu DODAG dengan root virtual dalam kasus beberapa sink.

Untuk memperhitungkan persyaratan perutean yang berbeda dalam LLN yang sama, RPL memperkenalkan konsep instans RPL, yang secara unik mengidentifikasi DAG (terbuat dari kumpulan DODAG) seperti yang dijelaskan sebelumnya. Semua DODAG dalam instance yang sama berbagi metrik dan batasan perutean yang sama [88], dan cara mereka digunakan untuk memilih simpul induk dan oleh karena itu DAG terbentuk. Yang terakhir disebut sebagai fungsi tujuan (OF) dari contoh RPL [89]. Beberapa instans RPL dengan OF yang berbeda diperbolehkan dalam LLN yang sama dan beroperasi secara independen satu sama lain.

Setiap node RPL, bagaimanapun, dapat berpartisipasi dalam lebih dari satu contoh, sehingga memungkinkan untuk membedakan penerusan lalu lintas di jaringan yang sama tergantung, misalnya, pada jenis layanan yang dibutuhkan oleh aplikasi asal. Yang terakhir ini dimungkinkan karena diasumsikan bahwa setiap paket data IPv6 akan mengangkut beberapa informasi terkait RPL, termasuk contoh RPL mana yang dimaksudkan untuk diteruskan oleh paket tersebut. Contoh instance RPL dengan banyak DODAG digambarkan pada Gambar 2.13.

Dalam setiap DODAG, simpul RPL dicirikan oleh peringkatnya, yang merupakan ukuran skalar dari jarak simpul tersebut dari akar. Peringkat harus menurun secara monoton pada setiap jalur yang diidentifikasi oleh DODAG menuju akarnya. Properti ini juga digunakan untuk mendeteksi loop ketika

lalu lintas diteruskan: Jika paket data diteruskan ke root tetapi peringkatnya tidak berkurang, prosedur perbaikan lokal dimulai untuk menyesuaikan DODAG. Peringkat node RPL pengirim termasuk dalam informasi terkait RPL yang diangkut oleh setiap paket data. OF yang terkait dengan instance RPL (yang disiarkan selama pembentukan DAG) menentukan cara menghitung peringkat node. Meskipun perhitungan seperti itu kemungkinan besar akan bergantung pada metrik dan batasan yang dikonfigurasikan untuk instans RPL (selain peringkat induk yang dipilih), nilainya tidak dimaksudkan sebagai biaya jalur dari simpul RPL ke akar DODAG , melainkan sebagai jarak relatif node tersebut dari root sehubungan dengan tetangganya sendiri. Bahkan, demi stabilitas routing, diharapkan



Gambar 2.13 Contoh instance RPL dengan banyak DODAG. Panah solid menghubungkan node ke induk pilihannya, panah putus-putus terhubung ke node di set induk, garis solid terhubung ke node lebih lanjut di set kandidat tetangga.

peringkat simpul RPL akan bervariasi di berbagai versi DODAG3 jauh lebih lambat daripada biaya jalur yang sesuai. Selain itu, peringkat harus diturunkan secara monoton ke arah akar, yang tidak selalu demikian—misalnya, untuk metrik tautan nonadditif.

DODAG dalam instance RPL dibuat berdasarkan algoritme terdistribusi. Akar DODAG mulai mengiklankan keberadaan mereka dengan mengirimkan paket kontrol DODAG Information Object (DIO) secara berkala ke alamat multicast link-local IPv6. Pesan DIO mencakup ID instance dan DODAG, peringkat node pengirim, dan parameter konfigurasi lain yang relevan. Semua node RPL mendengarkan DIO dan meneruskannya ke alamat multicast link-local untuk mengiklankan kehadiran mereka dan berkontribusi untuk menyebarkan informasi ini ke seluruh jaringan. Untuk menghindari banjir paket, penyiaran DIO dikendalikan oleh algoritma Trickle [90,91], yang mengatur kecepatan pengiriman pada setiap node tergantung pada apakah informasi yang diterima konsisten dengan statusnya sendiri atau tidak. Dengan menerima pesan DIO, sebuah simpul RPL mempelajari sekumpulan simpul yang secara langsung dapat dijangkau melalui multicast tautan-lokal (yakni, mereka berada pada tautan IP yang sama). Di dalam set seperti itu, didorong oleh instance OF dan batasan dan metrik perutean yang sesuai, node menentukan set kandidat tetangganya dan memilih satu atau lebih induk, sehingga bergabung dengan DODAG. Induk pilihan juga harus dipilih dari set induk sebagai lompatan berikutnya untuk rute default ke atas ke akar. Saat menerima pesan DIO dari

induknya, node menghitung peringkatnya sendiri, dan memperbarui bidang pesan DIO yang sesuai Meskipun dioptimalkan untuk perutean MP2P melalui DODAG, RPL secara opsional mendukung perutean P2MP dan P2P dengan menemukan rute ke bawah dengan bantuan pesan objek iklan tujuan (DAO). Yang terakhir dipancarkan oleh node RPL segera setelah mereka bergabung dengan DODAG, dan mereka menyertakan alamat IPv6 target atau perbaikan awal yang dimiliki oleh node tersebut. Perbanyakan ke atas ke akar kemudian dilakukan dengan cara yang sedikit berbeda, tergantung pada cara mempertahankan dan mengoperasikan rute ke bawah. Secara khusus, dua mode alternatif didefinisikan untuk contoh RPL yang diberikan: baik menyimpan (stateful) atau nonstoring (berbasis sumber-perutean). Dalam kasus penyimpanan, pesan DAO dikirim secara unicast ke (kemungkinan subset dari) set induk. Setiap induk menyimpan informasi yang diterima dalam tabel perutean ke bawah, dan meneruskan pesan DAO ke induknya sendiri ke akar. Lalu lintas kemudian diarahkan ke hilir berdasarkan informasi hop berikutnya yang disimpan dalam tabel routing di setiap hop. Di sisi lain, dalam kasus nonstoring, pesan DAO dialamatkan secara unicast ke root DODAG dan disebarkan oleh leluhur perantara di sepanjang rute default, seperti paket data lainnya. Tidak ada informasi yang disertakan dalam pesan DAO yang dikumpulkan dan disimpan dalam tabel perutean di setiap node, melainkan informasi tentang jalur yang dilalui ke root disimpan dalam pesan DAO. Oleh karena itu root dapat mengirim paket data ke hilir ke tujuan yang diiklankan melalui perutean sumber IPv6.

Adapun perutean P2P, secara implisit didukung dengan menggabungkan kemampuan MP2P dan P2MP. Sebuah paket yang dialamatkan ke node lain dalam jaringan RPL yang sama diteruskan ke hulu menuju nenek moyang yang sama dari sumber dan tujuan, dan kemudian ke hilir ke tujuan akhir. Dalam kasus nonstoring, satu-satunya leluhur umum yang mampu merutekan paket ke hilir adalah akar DODAG. Di sisi lain, RPL juga memungkinkan pembentukan DODAG lokal, yang berakar pada node sumber dari jalur P2P tertentu. Dengan cara ini, sumber dapat menemukan rute

yang dioptimalkan ke tujuan akhir tanpa dibatasi oleh topologi DAG yang terkait dengan instans RPL.

Akhirnya, RPL juga mendefinisikan prosedur yang sesuai, baik global maupun lokal, untuk

memperbaiki DODAG ketika topologi fisik yang mendasarinya berubah. Kami merujuk pembaca yang tertarik ke referensi 85 untuk perincian lebih lanjut.

2.4.3.3 Manajemen Mobilitas.

Mobilitas intra-pan — yaitu, mobilitas node dalam 6LoWPAN — transparan, karena semua node berbagi satu awalan tunggal di seluruh jaringan 6LoWPAN. Sebenarnya protokol routing yang menangani pengelolaan mobilitas host dan node router, dengan menjalankan prosedur pemulihan rute yang sesuai. Di sisi lain, mobilitas antarpan dianggap berada di luar cakupan 6LoWPAN. Kami merujuk di sini untuk mobilitas tanpa batas, yang membutuhkan sebuah node untuk berpindah dari satu 6LoWPAN ke 6LoWPAN lainnya tanpa mengganggu sesi data yang sedang berlangsung di lapisan yang lebih tinggi. Protokol manajemen mobilitas berbasis IP umum dapat menangani masalah ini di lapisan jaringan. Secara khusus, ini adalah kasus mobile IPv6 (MIPv6) [92], yang memelihara alamat rumah untuk mobile node melalui agen rumah, dan mengelola komunikasi antara yang terakhir dan node saat bergerak melintasi jaringan yang berbeda. MIPv6, bagaimanapun, memerlukan keterlibatan yang kuat dari mobile node untuk menjaga agar protokol tetap berjalan dengan benar, yang merupakan beban yang terlalu berat untuk perangkat yang dibatasi, seperti biasanya host dalam 6LoWPAN.

Alternatif yang menarik adalah protokol proxy MIPv6 (PMIPv6) [93], yang telah ditentukan oleh kelompok kerja manajemen mobilitas lokal berbasis jaringan (NETLMM) di IETF. PMIPv6 memanfaatkan fungsi jangkar mobilitas lokal (LMA), yang mengelola mobilitas dalam domain PMIPv6, dan sejumlah gerbang akses seluler (MAG) dalam domain, yang bertindak sebagai proksi atas nama node seluler untuk menjalankan semua protokol -tindakan terkait. Dengan mendeteksi mobilitas secara implisit melalui pesan protokol ND, PMIPv6 adalah solusi murni berbasis jaringan yang memungkinkan host untuk mempertahankan alamatnya sendiri saat bergerak di seluruh domain PMIPv6. Namun, PMIPv6 tidak langsung berlaku untuk 6LoWPAN. Secara khusus, ini mengasumsikan mobile host berada pada jarak one-hop ke MAG yang dilampirkan, sehingga tidak kompatibel dengan solusi route-over, atau membutuhkan node router 6LoWPAN untuk bertindak sebagai MAG. Selain itu, mobile node diasumsikan disediakan dengan awalan jaringannya sendiri di dalam domain, yang tidak sesuai dengan hipotesis perpindahan melalui 6LoWPAN yang berbeda.

2.5 DUKUNGAN MOBILITAS DALAM SKENARIO HETEROGEN

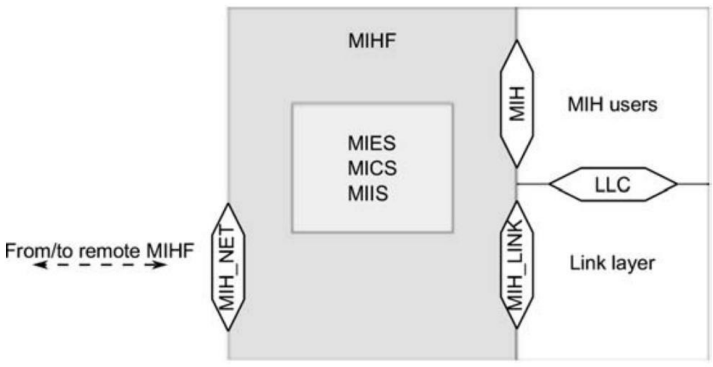
Banyak jaringan akses didasarkan pada teknologi nirkabel, dan popularitasnya meningkat pesat sementara pengguna menjadi semakin akrab dengan layanan di mana-mana. Sayangnya, kami tidak dapat melihat dalam waktu dekat konvergensi menuju satu teknologi nirkabel, karena karakteristik jaringan WPAN, WLAN, dan BWA yang sangat berbeda, dalam hal kecepatan bit (dari kbit/s ke Mbit/s), cakupan (dari meter ke kilometer), dan konsumsi energi (dari mW ke W). Selain itu, perangkat seluler yang mendukung banyak teknologi radio sekarang sudah umum [94], dan mencapai kualitas pengalaman terbaik (QoE) memerlukan sarana untuk mengalami prosedur serah terima yang mulus baik intra-teknologi (horizontal) dan antar-teknologi (vertikal) sehingga dapat menjaga agar perangkat seluler tetap terhubung ke jaringan akses yang paling sesuai pada waktu dan tempat tertentu. Selain itu, karena karakteristik propagasi dan koeksistensi beberapa operator jaringan, baik di pita berlisensi maupun tidak, sangat umum untuk memiliki banyak peluang koneksi, bahkan dalam satu teknologi.

Untuk alasan ini, juga disorot oleh Internet Engineering Task Force (IETF) dalam referensi 95, standar IEEE 802.21 [19] untuk layanan MIH telah diterbitkan pada Januari 2009. Dokumen ini bertujuan untuk menentukan mekanisme untuk mengaktifkan dan mengoptimalkan handover antara jaringan IEEE 802 yang heterogen, termasuk di mana penyerahan tidak ditentukan lain, dan memfasilitasi penyerahan antara jaringan IEEE 802 dan jaringan seluler, serta jaringan nirkabel 4G [96]. Tujuan ini dicapai

dengan mendefinisikan entitas dan layanan baru yang harus diimplementasikan ke perangkat seluler dan jaringan serta protokol komunikasi yang dapat diperluas [97]. Namun, seperti yang sering terjadi pada standar komunikasi, prosedur dan algoritme

dibiarkan tidak ditentukan untuk mempromosikan persaingan dengan diferensiasi kemampuan dan layanan peralatan.

Standar tersebut terdiri dari (i) kerangka kerja yang memungkinkan transisi mulus dari sebuah mobile node (MN) antara jaringan dengan (mungkin) teknologi yang berbeda; (ii) entitas baru yang disebut fungsi MIH (MIHF); (iii) titik akses layanan MIH



Gambar 2.14 model referensi MIH dan SAP.

(SAP), disebut MIH SAP, dan primitif terkaitnya; (iv) SAP lapisan tautan, yang disebut MIH LINK SAP, untuk setiap teknologi jaringan; (v) antarmuka yang bergantung pada media abstrak yang menyediakan layanan transportasi melalui bidang data pada node lokal, yang disebut MIH NET SAP; dan (vi) entitas baru yang disebut pengguna MIH (MIH USR), yang merupakan entitas fungsional yang menggunakan layanan MIH.

Model referensi MIH diilustrasikan pada Gambar 2.14. MIH LINK SAP digunakan untuk mengumpulkan informasi tautan dan mengontrol perilaku tautan selama serah terima. Untuk setiap teknologi jaringan yang ada, amandemen diperlukan untuk berinteraksi dengan primitif dasar yang didefinisikan dalam standar IEEE 802.21. Pekerjaan tersebut sedang dilakukan untuk IEEE 802.3, IEEE 802.11, IEEE 802.16, 3GPP dan 3GPP2 di masing-masing kelompok tugas atau komite teknis. Untuk teknologi baru, diperkirakan bahwa mereka akan menggabungkan primitif yang cocok secara native untuk IEEE 802.21.

MIHF menyediakan layanan berikut:

• Layanan Acara Independen Media (MIES). Peristiwa adalah pemberitahuan yang dihasilkan oleh lapisan tautan, biasanya melibatkan kualitas dan status tautan. Seorang pengguna MIH dapat berlangganan untuk menerima pemberitahuan tersebut, baik dari lapisan bawah lokal maupun dari entitas jarak jauh, melalui MIHF lokal. Beberapa

pengguna dapat mendaftar ke acara yang sama, dalam hal ini pemberitahuan dikirim ke semua pelanggan.

• Layanan Komando Media-Independen (MICS). Perintah dikirim dari pengguna MIH ke lapisan bawah. Perintah digunakan untuk mengonfigurasi, mengontrol, dan mengambil informasi dari lapisan bawah. Seperti acara, perintah juga dapat diarahkan ke entitas jarak jauh melalui MIHF lokal. • Layanan Informasi Media-Independen (MIIS). Ini

mendefinisikan kerangka kerja untuk memperoleh, menyimpan, dan mengambil informasi yang berguna untuk keputusan serah terima dalam wilayah geografis. Dukungan untuk banyak elemen informasi (IE) disertakan untuk mencakup berbagai jenis mobilitas dan teknologi yang didukung. IE dapat dikodekan baik dalam bentuk biner, menggunakan struktur tipe-panjang-nilai (TLV), atau dengan representasi resource description framework (RDF) [98]. Dengan

RDF skema dasar disediakan dalam Lampiran H [19], yang dapat dengan mudah diperluas untuk menyertakan potongan informasi khusus pengguna atau vendor.

Pengambilan data dilakukan dengan cara query TLV atau SPARQL [99], untuk masing- masing metode pengkodean.

MIEC dan MICS adalah blok bangunan untuk memungkinkan komunikasi antarlapisan, baik lokal maupun jarak jauh, dan karenanya penting untuk implementasi MIH apa pun. Untuk fleksibilitas

maksimum, protokol komunikasi antara entitas MIHF ditentukan oleh standar untuk lapisan 2 dan lapisan 3: Transport lapisan 2 diperbolehkan dengan nilai EtherType yang ditetapkan untuk Protokol MIH; transport layer 3 didukung untuk Transmission Control Protocol (TCP), User Datagram Protocol (UDP), dan Stream Control Transmission Protocol (SCTP).

Layanan pengakuan dapat diaktifkan untuk menambah keandalan pertukaran pesan jika metode transportasi yang diadopsi belum menyediakan ini. Rancangan kerangka kerja untuk layanan mobilitas dan mekanisme lapisan transportasi yang andal untuk IEEE 802.21 telah ditetapkan oleh Grup Jaringan IETF [100].

Di sisi lain, kehadiran MIIS bersifat opsional, dan ditujukan untuk mengaktifkan fungsi lanjutan untuk antar-teknologi dan serah terima yang dikendalikan jaringan dalam satu domain penyedia. Karena standar tidak menentukan konten pesan yang dapat dipertukarkan oleh node seluler dengan MIIS, MIIS dapat digunakan untuk berbagai tujuan. Misalnya, dalam referensi 101 penulis mengusulkan peningkatan dukungan mobilitas yang menerapkan protokol Location-to- Service Translation (LoST) [102], yang bergantung pada arsitektur terdistribusi yang sangat skalabel untuk menyelesaikan lokasi fisik perangkat yang diidentifikasi dengan pencari sumber daya . Sebagai gantinya, prosedur serah terima netral teknologi berbantuan jaringan diusulkan dalam referensi 103, yang memungkinkan MIIS untuk secara mandiri memaksa keputusan pada pengguna seluler tentang antarmuka radio mana yang akan digunakan, sambil mematikan semua yang lain untuk mengurangi konsumsi energi.

2.6 KESIMPULAN

Dalam bab ini kami telah menyajikan teknologi dan standar terkini untuk jaringan nirkabel multihop/mesh seluler. Kami telah mempertimbangkan cakupan tipikal untuk membedakannya, dan kami berfokus pada aspek spesifikasi tersebut yang khususnya terkait dengan memungkinkan penerusan multihop. Tabel 2.1 memberikan ringkasan umum dan skema fitur utama dari berbagai teknologi yang dipertimbangkan. Meskipun mereka pada dasarnya ditargetkan untuk tujuan yang berbeda, dan oleh karena itu mereka tidak dapat dianggap sebagai solusi alternatif yang bersaing satu sama lain, namun bermanfaat untuk melihat sekilas pilihan desain yang diadopsi secara komparatif, untuk lebih menghargai perbedaan dan persamaan di antara mereka.

Ada banyak skenario aplikasi saat ini di mana teknologi komunikasi mobile multi-hop/mesh wireless merupakan salah satu solusi yang paling efektif. Akses broadband bisnis publik di seluruh kota, pedesaan, dan swasta, serta komunitas lingkungan, hanya untuk menyebutkan beberapa, adalah semua kasus di mana infrastruktur jaringan

Table 2.1 Main Features of the Technologies Presented in This Chapter

	PHY	MAC Protocol	Scheduling/ Coordination	Routing Protocol	Routing Metric(s)
IEEE 802.16 mesh	802.16-OFDM	TDMA	Centralized or distributed	Tree-based	Unspecified
IEEE 802.16j	802.16-OFDMA	TDMA	Centralized	Tree-based	Unspecified
IEEE 802.11s	—	CSMA/CA	None (EDCA) or distributed (MCCA)	Mixed (tree-based + AODV)	Airtime (additive) as a function of the data transmission rate and the frame error rate
IEEE 802.11p/ WAVE	802.11a modified	CSMA/CA	None	Geo-Networking	Physical distance or hop count (additive)
IEEE 802.15.5	802.15.4	Unslotted CSMA/CA	None	Mixed (tree-based + k-hop link-state)	Hop count (additive) or link quality (min)
ZigBee	802.15.4	Unslotted and slotted CSMA/CA	None or distributed	Mixed (tree-based + AODV)	Link cost (additive), as a function of the number of expected transmissions attempts before successful reception
RPL	—	—	—	Distance vector, DAG-based	Rank (additive), as a function of different combinations of metrics and constraints

ditandai dengan seringnya perubahan topologi, kesalahan pada peralatan, dan/atau kondisi lingkungan yang keras. Selain itu, dalam situasi darurat, jaringan mesh nirkabel adalah solusi ideal untuk beroperasi secara mandiri dalam keadaan apa pun saat tidak ada akses ke jaringan eksternal. Di sisi konsumen, kamera digital, ponsel pintar, tablet, dan gadget elektronik lainnya difungsikan untuk berkomunikasi guna berbagi data pengguna, terutama di lingkungan rumah.

Ini membutuhkan solusi nirkabel multihop di mana perangkat dapat secara spontan berkomunikasi satu sama lain tanpa memerlukan topologi yang dikelola secara terpusat. Akhirnya merupakan taruhan yang aman untuk membayangkan bahwa skenario penerapan seperti itu untuk jaringan nirkabel multihop akan meningkat secara eksponensial karena Internet akan membuat langkah evolusioner berikutnya untuk terhubung kapan saja dan di mana saja tidak hanya siapa pun, tetapi apa saja, seperti yang diramalkan oleh visi Internet of Things.

Ini akan menuntut cakupan jaringan kapiler dan pervasif, di mana teknologi komunikasi nirkabel dan penerusan multihop dapat memainkan peran utama.

Ketersediaan teknologi standar adalah kunci untuk memungkinkan skenario seperti itu dalam skala besar, dengan memungkinkan perangkat dari manufaktur yang berbeda untuk berhasil saling beroperasi dan dengan demikian membuka persaingan pasar dan mendukung produksi skala besar. Teknologi canggih yang disajikan dalam bab ini pasti akan menjadi dasar bagi evolusi jaringan nirkabel multihop seluler standar berikutnya, yang diperlukan untuk menghadapi tantangan baru yang ditimbulkan oleh skenario aplikasi masa depan yang disebutkan di atas.

Kami juga berpendapat bahwa difusi besar-besaran dari teknologi semacam itu hanya akan mungkin terjadi jika mereka dapat hidup berdampingan dengan sarana komunikasi nirkabel “tradisional” lainnya, seperti jaringan seluler, semata-mata karena alasan ekonomis. Oleh karena itu, semua upaya mendorong menuju tingkat interoperabilitas yang lebih tinggi di antara teknologi yang berbeda, seperti yang diwakili oleh standar IEEE 802.21 yang dijelaskan di bagian terakhir bab ini, secara

otomatis akan menciptakan peluang baru bagi jaringan nirkabel multihop untuk menunjukkan potensinya dan menjadi yang utama. pemain dalam ekosistem jaringan nirkabel.

CHAPTER 3 SKENARIO APLIKASI

3.1 PENDAHULUAN

Selama beberapa tahun terakhir telah terjadi peningkatan minat penelitian dalam jaringan ad hoc seluler nirkabel (MANET) terutama didorong oleh munculnya perangkat portabel murah seperti smartphone, tablet, netbook dan berbagai modalitas komunikasi nirkabel kecil dan murah. misalnya, Bluetooth, WiFi, Zigbee, NFC).

Para peneliti membayangkan masa depan di mana setiap orang, kendaraan, dan alat dapat berkomunikasi melalui pita radio tanpa izin jarak pendek, sehingga membentuk jaringan peer-to-peer tanpa infrastruktur (misalnya, mirip dengan Internet of Things [1]). Tujuan utamanya adalah untuk membangun jaringan ad hoc yang mengatur dirinya sendiri di mana setiap perangkat dapat berpartisipasi secara bebas dan menawarkan/menerima semua jenis layanan. Untuk berkomunikasi dengan node yang jauh, paradigma multihop (store-and- forward) digunakan, artinya pesan dapat disampaikan melalui sejumlah node penerusan perantara (hop). MANET tujuan umum ini bertujuan untuk menyatukan perangkat heterogen dan untuk mendukung berbagai aplikasi yang dapat dibangun di atasnya.

Paradigma komunikasi seperti itu menawarkan banyak keuntungan. Pertama-tama, ini memiliki biaya awal yang lebih rendah karena tidak perlu memasang perangkat keras tambahan atau membayar untuk melisensikan bagian mana pun dari spektrum frekuensi. Selain itu, MANET dapat digunakan dengan cepat: secara teori hanya dengan merilis aplikasi di pasar smartphone mana pun (misalnya, Apple AppStore). Mereka juga akan sangat tahan

terhadap gangguan karena tidak ada satu pun titik kegagalan dan tidak memerlukan infrastruktur apa pun untuk berfungsi.

Meskipun infrastruktur seluler dapat digunakan untuk menghubungkan host seluler secara nirkabel, solusi ini dapat menimbulkan masalah. Pertama, penyedia seluler di setiap negara memberlakukan aturan dan batasan yang berbeda mengenai jenis data apa yang dapat ditransmisikan melalui jaringan mereka atau bahkan jenis aplikasi apa yang dapat mengaksesnya, sehingga mempersulit aplikasi untuk diterapkan secara global (berpotensi per negara). diperlukan kesepakatan). Selain itu, biaya komunikasi data seluler sangat tinggi, karena bisa mencapai beberapa sen per kilobyte. Bahkan paket "tak terbatas" yang mahal saat ini biasanya dibatasi hingga beberapa ratus megabita per bulan, membuat komunikasi data yang signifikan antar perangkat tidak dapat dilakukan. Selain itu, dalam koneksi 3G/4G bandwidth dibagi antara semua pengguna di dalam sel; dan bahkan saat ini, ketika 3G tidak digunakan secara luas, jaringan dibanjiri oleh lalu lintas, sehingga menghasilkan throughput yang sangat rendah di daerah padat penduduk. Di sisi lain, penggunaan teknologi jaringan perangkat-ke-perangkat seperti WiFi atau Bluetooth tidak memerlukan lisensi apa pun atau penerapan infrastruktur apa pun dan sangat ideal untuk membuat jaringan berskala kecil, bandwidth tinggi dari perangkat terdekat sekalipun. di daerah di mana layanan seluler terbatas.

Tidak adanya pihak ketiga dalam proses komunikasi dapat menjadi sangat penting jika informasi tersebut bersifat sensitif.

Meskipun MANET tujuan umum memiliki banyak keuntungan, dalam praktiknya mereka belum mencapai dampak yang diharapkan dalam penerapan dunia nyata dan adopsi uji coba industri. Meningkatnya ketersediaan konektivitas infrastruktur seluler (misalnya, jaringan 3G, hotspot WiFi) seringkali menyediakan konektivitas tujuan umum yang sesuai, terlepas dari keterbatasannya sendiri. Sementara para peneliti menganggap sistem swa-kelola yang

sepenuhnya terdesentralisasi cukup menarik, model ini juga menunjukkan beberapa hal yang melekat keterbatasan. Pertama, sistem hanya berfungsi jika ada cukup banyak peserta yang berkolaborasi. Ini dapat menjadi masalah jika sumber daya perangkat dikonsumsi melalui partisipasi, dan dapat menyebabkan orang dengan egois hanya berpartisipasi ketika mereka membutuhkan layanan. Selain itu, mungkin tidak jelas siapa yang bertanggung jawab atas tanggung jawab dan masalah kualitas layanan—misalnya, jika kecelakaan kendaraan disebabkan oleh informasi yang diberikan oleh sistem tersebut (atau kekurangannya). Tidak

adanya otoritas tunggal untuk mengontrol dan mengelola jaringan juga dapat membuat sistem menantang bagi industri untuk menghasilkan uang.

Meskipun MANET tujuan umum mungkin tidak tersebar luas, jaringan khusus yang dikelola oleh satu otoritas dan disesuaikan untuk memecahkan masalah tertentu sudah menjadi

kenyataan. Misalnya, jaringan militer telah digunakan untuk (a) menyediakan komunikasi di lingkungan yang tidak bersahabat di mana tidak tersedia infrastruktur tepercaya dan (b)

mengoordinasikan perangkat otonom (seperti ranjau pintar, kendaraan tak berawak, dll.). MANET yang tahan tunda telah digunakan untuk menyediakan konektivitas di area di mana komunikasi tidak selalu tersedia, seperti komunikasi antarplanet, atau bahkan menyediakan koneksi Internet di area yang kekurangan. Jaringan sensor nirkabel telah digunakan untuk menyebarkan perangkat berbiaya rendah dan berdaya rendah dengan cepat. Jaringan pemulihan bencana dapat menyelamatkan nyawa dalam kasus ekstrim di mana infrastruktur mungkin runtuh karena bencana alam atau karena persyaratan konektivitas yang tinggi.

Terakhir, jaringan kendaraan dapat menghubungkan kendaraan dan infrastruktur untuk mendukung aplikasi keselamatan, meningkatkan kapasitas jalan, menyebarkan pemberitahuan, atau bahkan mendukung sistem transportasi cerdas yang dapat mengurangi kemacetan jalan.

Di bagian berikut, kami akan memeriksa beberapa sistem ini dan menjelaskan penerapannya di dunia nyata.

3.2 APLIKASI MILITER

Relai multihop pada awalnya digunakan untuk mendukung kebutuhan komunikasi dan koordinasi antara tentara, kendaraan militer, dan markas informasi. Alasan yang membuat MANET cocok untuk aplikasi militer bermacam-macam: Pertama-tama, jaringan terdistribusi seperti itu tidak memiliki titik kegagalan tunggal, dibandingkan dengan sistem infrastruktur. Kedua, operasi

militer terjadi di daerah di mana tidak ada infrastruktur yang tersedia atau infrastruktur yang ada tidak dapat dipercaya dan oleh karena itu jaringan swakelola yang dapat dikerahkan dengan cepat sangat penting. Akhirnya, bahkan dalam kasus di mana infrastruktur tersedia (misalnya, komunikasi satelit),

MANET dapat digunakan untuk menghubungkan perangkat lokal dengan cepat (misalnya, tambang) untuk mendukung koordinasi kelompok dan agregasi informasi tanpa menggunakan sumber daya satelit yang terbatas. Pada bagian ini kami akan menjelaskan beberapa sistem militer berbasis MANET yang telah digunakan selama bertahun-tahun.

3.2.1 Komunikasi

Awalnya, MANET diterapkan untuk mendukung komunikasi di daerah di mana infrastruktur tidak tersedia. Ini termasuk menyampaikan informasi dari medan perang ke markas besar, menyediakan komunikasi dalam kelompok tentara, kendaraan militer, dan menghubungkan kelompok yang berbeda, bahkan jika mereka tidak saling berhadapan (LOS).

Faktanya, penggunaan komunikasi semacam itu yang pertama kali didokumentasikan berasal dari tahun 1184 SM: Aeschylus melaporkan bahwa garis sinyal api digunakan untuk mengirim pesan dari Troy ke kota Argos yang menandakan kemenangan oleh orang Yunani [2]. Sistem tersebut diduga lebih dari 25 kali lebih cepat daripada messenger normal yang tersedia saat itu. Metode serupa digunakan di banyak masyarakat kuno/suku dengan rangkaian pengulang gendang, terompet, terompet, pesan asap, dan sebagainya.

Baru-baru ini, pada tahun 1972, Departemen Pertahanan Amerika (DoD) dan DARPA memprakarsai program penelitian di Packet Radio Networks (PRNet) [3] dengan maksud untuk menciptakan teknologi komunikasi multihop untuk medan perang yang dapat beroperasi di wilayah yang luas dan mungkin bermusuhan. . Tujuan utamanya adalah untuk membuat jaringan yang dapat diatur sendiri, dapat diterapkan dengan cepat, dan kuat terhadap kegagalan dan serangan. Dalam PRNet kombinasi ALOHA [4] dan carrier sense multiple access (CSMA) digunakan dengan cara store-and-forward untuk memungkinkan jaringan perangkat yang padat untuk berbagi frekuensi tertentu dan berkomunikasi melintasi area geografis yang sangat luas.

PRNet adalah penerapan pertama yang menghadapi masalah mempertahankan topologi dinamis untuk menangani tautan yang rusak dan konfigurasi ulang jalur. Protokol perutean yang digunakan dalam PRNet dirancang untuk memungkinkan keandalan dengan mengukur kondisi tautan secara konstan dan beradaptasi secara dinamis dengan kondisi jaringan.

Pada 1980-an generasi kedua dari sistem semacam itu muncul. Survivable Radio Networks (SURAN) [5] bertujuan untuk mengatasi masalah terbuka di PRNet seperti ukuran perangkat, biaya, skalabilitas, kecepatan komunikasi, dan keamanan. Selama program ini, protokol baru dirancang yang dapat mendukung jaringan yang dapat menskalakan hingga puluhan ribu node dan menahan serangan keamanan, serta menggunakan radio portabel kecil, berbiaya rendah, dan berdaya rendah. Modulasi baru digunakan seperti bentuk gelombang spread-spectrum menggunakan urutan pseudo-noise untuk meningkatkan ketahanan terhadap interferensi dan untuk meminimalkan kemungkinan penyadapan. Transmisi dan penerimaan omnidirectional, spread-spectrum, half-duplex ini memungkinkan kecepatan masing-masing 400 kbit/s dan 100 kbit/s, membuat jaringan ini lebih praktis. Selanjutnya, lapisan manajemen jaringan yang memungkinkan operator PRNet memantau jaringan muncul untuk pertama kalinya.

Pada awal 1990-an, DARPA memprakarsai program Sistem Informasi Global Mobile (GloMo).

Hal ini bertujuan untuk mendukung konektivitas berbasis IP di antara perangkat nirkabel yang heterogen dalam berbagai kemungkinan skenario. Munculnya komputer portabel dan perangkat komunikasi nirkabel yang layak melahirkan konsep arsitektur ad hoc peer-to-peer yang tidak terstruktur di mana tentara dan bahkan perangkat yang lebih kecil seperti drone atau bahkan ranjau dapat menjadi bagian dari jaringan ini.

Baru-baru ini, pertumbuhan kelaparan akan bandwidth dan gagasan "perang sentris jaringan," di mana kendaraan tak berawak dan tentara adalah bagian dari jaringan, mengarah pada penciptaan Internet Taktis (TI) dan versi selulernya M@TIS [6]. M@TIS memungkinkan pengaturan jaringan komunikasi seluler nirkabel yang menyediakan layanan komunikasi tipe Internet hingga ke prajurit yang diturunkan. Selain itu, mendukung jaringan radio heterogen (HF,

VHF, UHF, dll.) dan berbagai layanan seperti VOIP, akses ke jaringan backbone, dan sebagainya.

3.2.2 Coordination

Selain mendukung komunikasi, MANET telah diterapkan untuk mengoordinasikan perangkat otonom yang dapat digunakan di medan perang.

Contoh pertama dari sistem tersebut adalah Ladang Ranjau Penyembuhan Sendiri[7]. Ladang Ranjau Self-Healing adalah penghalang cerdas dan dinamis yang merespons upaya musuh menerobos dengan mengatur ulang secara fisik: ranjau antitank yang tersebar dapat mendeteksi serangan musuh di ladang ranjau dan merespons secara mandiri, dengan membuat sebagian kecil ranjau bergerak untuk menyembuhkan pelanggaran . Tambang berkomunikasi dengan mentransmisikan sinyal periodik untuk menunjukkan statusnya ke seluruh jaringan. Tidak adanya transmisi yang diharapkan dari satu atau lebih tambang terdekat digunakan untuk menunjukkan upaya pelanggaran. Ranjau yang tersisa menggunakan tautan radio mereka untuk memberi tahu ranjau yang lebih jauh tentang upaya pelanggaran dan untuk mengoordinasikan tanggapan.

Selanjutnya, MANET telah digunakan untuk mengoordinasikan kendaraan militer tak berawak.

Misalnya, dalam referensi 8 kendaraan tak berawak digunakan untuk menjaga perimeter dengan cara membunyikan alarm dari sensor deteksi intrusi. Saat tidak memperhatikan alarm, kendaraan

mendistribusikan dirinya secara merata di sepanjang perimeter. Komunikasi radio multihop digunakan untuk menyiarkan lokasi setiap kendaraan dan mengoordinasikan keputusan mereka.

Demikian pula, kendaraan udara tak berawak (UAV) [9] dapat berjejaring satu sama lain untuk memaksimalkan jangkauan pengintaian dan hasil agregat sebelum mengirimkannya melalui tautan satelit. Selain itu, jaringan memungkinkan kendaraan ini berkumpul bersama, atau terbang dalam berbagai formasi. Akhirnya, kendaraan-kendaraan ini dapat berkoordinasi untuk menyediakan jalur komunikasi ke unit-unit darat (yaitu, mempertahankan barisan drone yang digunakan untuk menyampaikan pesan dari suatu area kembali ke pangkalan).

Akhirnya, militer menggunakan MANET untuk penginderaan terdistribusi. Misalnya, sebuah sistem yang dapat melokalkan penembak jitu [10] menggunakan sejumlah perangkat yang dapat dipakai oleh tentara (misalnya, PDA) yang saling berjejaring. Pendekatan ini bergantung pada pengukuran perbedaan waktu antara ledakan moncong dan gelombang kejut untuk memperkirakan jarak penembak jitu.

Komunikasi radio digunakan karena beberapa deteksi diperlukan untuk trilaterate posisi penembak; oleh karena itu, informasi yang dirasakan dari banyak tentara digabungkan untuk memberikan perkiraan yang akurat. Di lingkungan yang ekstrim, sensor jaringan bersama-sama dapat memberikan lebih banyak informasi daripada saat sendirian, meskipun hal ini bisa sangat menantang saat tidak ada infrastruktur.

3.3 KONEKTIVITAS JARINGAN

Selain aplikasi militer, MANET telah digunakan untuk menyediakan komunikasi antar perangkat atau dengan Internet di area dengan infrastruktur terbatas atau terputus-putus.

mengakses.

3.3.1 IPN

Konsep Interplanetary Internet (IPN) dimulai pada tahun 1982 oleh Consultative Committee for Space Data Systems (CCSDS), tetapi baru belakangan ini digunakan. Tautan radio antarplanet, yang berpotensi beroperasi pada skala tata surya kita, bisa dibilang merupakan salah satu lingkungan paling ekstrem untuk komunikasi. Saluran komunikasi antara satelit, pesawat ulang-alik, dan stasiun permukaan masih jauh dari sempurna.

Jarak ekstrim yang menyebabkan penundaan propagasi yang lama, penerimaan daya rendah, pelemahan sinyal, dan sumber gangguan lainnya semuanya berpotensi menyebabkan kurangnya jalur komunikasi end-to-end. Ini mungkin karena oklusi planet atau hanya dua titik komunikasi yang terlalu jauh untuk berkomunikasi dengan andal. Rotasi planet, orbit satelit, dan interferensi atmosfer lokal semuanya menciptakan situasi yang kompleks untuk mencapai konektivitas. Solusi alami untuk masalah ini melibatkan komunikasi multihop antar perangkat yang berada dalam jangkauan, memindahkan data antar tetangga yang saat ini memiliki konektivitas.

Delay-tolerant networking (DTN) awalnya dikembangkan saat mempertimbangkan jaringan terplanet. DTN adalah model komunikasi yang secara fundamental berbeda dari perilaku jaringan tradisional. Asumsi biasa konektivitas dengan anggota lain dari jaringan santai, memungkinkan fungsi jaringan yang akan dibangun melalui link terputus-putus dan tidak dapat diandalkan, di mana pemutusan diperlakukan sebagai kasus umum. Oleh karena itu, mereka menggunakan mekanisme untuk secara cerdas memanfaatkan konektivitas ketika tersedia.

Data untuk mengirimkan dipartisi menjadi bundel dan ditujukan ke tujuan. Node kemudian menunggu sampai mereka dapat berkomunikasi dengan orang lain di jaringan, dengan bundel “melompati” melalui node perantara hingga mencapai tujuan. Perilaku ini mungkin menimbulkan penundaan yang signifikan, tetapi sangat tahan terhadap masalah jaringan. Sebagian besar pekerjaan akademis dan standar untuk bidang ini dikaitkan dengan Delay-Tolerant Networking Research Group (DTNRG) http://www.dtnrg.org, yang menyediakan analisis dan penerapan banyak sistem DTN.

Otomatisasi entitas luar angkasa yang memilih kapan dan dengan siapa memindahkan data mengarah ke asal-usul DTN. DTN memungkinkan perangkat tersebut hanya mencoba komunikasi ketika tautan tersedia. Mereka tidak perlu merencanakan seluruh rute secara eksplisit; mereka hanya mengirimkan bundel lebih dekat ke tujuan, memungkinkan perangkat secara mandiri membuat pilihan terbaik untuk kondisi saat ini. Salah satu penyebaran ruang angkasa paling awal dari DTN adalah pada tahun 2003 di

satelit UK-DMC I [11], yang merupakan bagian dari sistem pemantauan bencana yang dibangun untuk Badan Antariksa Inggris. Satelit berisi sensor untuk memantau planet dan router Cisco dalam sistem Low Earth Orbit (CLEO) untuk berpartisipasi dalam Internet Antarplanet. CLEO mengoperasikan Protokol Bundel sebagaimana ditentukan dalam RFC 5050 [12].

Komunikasi DTN juga telah diperluas melampaui orbit geostasioner ke luar angkasa (melampaui 2 juta kilometer dari Bumi). Ini pertama kali dicapai pada proyek Deep Impact/ EPOXI NASA, menggunakan Deep Space Network mereka selama tahun 2008.

Satelit EPOXI sedang dalam misi mempelajari Komet Hartley 2; selama perjalanannya itu digunakan sebagai pengorbit relai data untuk peralatan di Mars. Mars Exploration Rovers telah menggunakan satelit Mars Odyssey sebagai relai karena visibilitas Bumi yang lebih baik. Setelah sukses dengan proyek tersebut, NASA mulai menyematkan teknologi DTN pada perangkat keras satelitnya [13]. Mereka bahkan telah membuat implementasi DTN Interplanetary Overlay Network mereka tersedia sebagai Open Source melalui Open Channel Foundation.1 Keunggulan utama teknologi ini adalah perutean otomatis antara satelit dan stasiun bumi yang relevan, tetapi ini memulai proses perluasan Internet dari planet kita dan memungkinkan kita untuk mengukur dan memahami tata surya kita.

3.3.2 Perdesaan

Negara-negara berkembang menderita kekurangan infrastruktur dan karena itu kurangnya konektivitas Internet, khususnya di daerah pedesaan mereka. Namun, banyak anggota populasi ini memiliki perangkat elektronik, baik milik pribadi (misalnya ponsel) maupun milik masyarakat, yang mampu menyediakan layanan komputer yang penting. Salah satu upaya paling terkenal untuk menghadirkan akses komputer ke wilayah berkembang adalah proyek One Laptop per Child [14], yang bertujuan untuk menyediakan banyak laptop tangguh dan murah dengan antarmuka jaringan kepada anak-anak untuk memberi mereka pengalaman komputer. Membawa konektivitas yang lebih besar ke perangkat tersebut menawarkan prospek peningkatan pendidikan dan keterlibatan dengan komunitas lain.

Terlepas dari pengalaman banyak orang tentang koneksi Internet yang "selalu aktif", konektivitas tenda yang terputus-putus masih dapat bermanfaat. Komunikasi permintaan/ respons asinkron cocok untuk penelusuran situs web, email, dan banyak aplikasi lainnya. Analisis oleh proyek SARI India

[15] menyatakan bahwa “dalam jangka pendek hanya email, scan-mail, voice-over-e-mail, dan obrolan yang cenderung menjadi aplikasi penghasil pendapatan” di area tersebut. Selama dekade terakhir, berbagai upaya telah dilakukan untuk membawa gagasan Internet yang sedikit lebih terbatas ini kepada orang-orang di wilayah berkembang ini untuk memungkinkan pengembangan infrastruktur dan layanan komunitas mereka lebih lanjut.

Penduduk desa berkembang dapat mengajukan permintaan ke komputer (berpotensi publik).

Kemudian sistem "backhaul mekanis" digunakan, di mana kendaraan yang mendukung DTN melakukan perjalanan antar desa untuk mengumpulkan dan menyebarkan data yang relevan. Ini mungkin hanya terjadi setiap minggu untuk lokasi yang sangat terpencil, tetapi waktu pulang pergi mingguan masih dapat menawarkan beberapa manfaat bagi penduduk. Yang penting, layanan ini bisa sangat murah berdasarkan per pengguna, dan dapat menghadirkan Internet bahkan ke wilayah paling terpencil di planet ini.

Sistem Kiosknet [16] telah diterapkan di Anandapuram, sebuah desa di India Selatan pada tahun 2006, dan juga di Ada, sebuah desa di Ghana Tenggara selama tahun 2008. Feri di Kiosknet hanya membutuhkan satu papan komputer sederhana, yang dapat diberi daya oleh baterai kendaraan.

Menggunakan WiFi untuk terhubung dengan kios komunitas, feri mengumpulkan permintaan dan mengembalikan hasil permintaan sebelumnya, yang sebelumnya dikeluarkan ke Internet dalam periode konektivitas yang sebenarnya. Yang diperlukan hanyalah kios umum dan kapal feri memiliki penyimpanan yang cukup untuk permintaan yang tertunda dan respons pengembalian, yang diperkirakan berukuran 40 GB. Ada banyak proyek lain di pedesaan India [15] dan di tempat yang

lebih ekstrim, seperti Arktik Swedia untuk penduduk asli nomaden Sami [17]. 3.3.3 Sistem Kota/Komunitas

Bahkan di negara maju, meskipun infrastruktur nirkabel mungkin tersedia untuk pengguna, masih diinginkan untuk berkomunikasi dalam toleransi penundaan dengan sekelompok rekannya. Penyebaran awal jaringan nirkabel kolaboratif adalah RoofNet di kampus perguruan tinggi Massachusetts Institute of Technology (MIT). RoofNet adalah proyek dari banyak siswa yang membentuk jaringan nirkabel multihop menggunakan perangkat di atap mereka.2 Jalinan perangkat memungkinkan komunikasi tidak langsung antara setiap anggota jaringan ini.

Dengan beberapa gateway yang terhubung ke Internet, dimungkinkan untuk menyediakan akses Internet untuk semua anggota jaringan. Sistem berbasis komunitas lainnya adalah Athens Wireless Metropolitan Network (AWMN), sistem nirkabel berbasis mesh nirlaba serupa. Beroperasi sejak tahun 2002 di Athena, lebih dari 2000 peserta dapat menerima konektivitas Internet.3 Model ini sangat berguna jika peer berkomunikasi satu sama lain, menerima penundaan singkat dan tidak membebani gerbang Internet mereka dengan lalu lintas lokal.

Ini menarik ketika data bersifat lokal, sensitif, atau besar. Itu juga dapat digunakan untuk menyediakan akses Internet murah ke lebih banyak pengguna daripada yang saat ini dapat mengakses koneksi kabel.

3.4 JARINGAN SENSOR NIRKABEL

Selain penyebaran militer dan antarplanet, MANET juga digunakan untuk aplikasi komersial: Jaringan sensor nirkabel (WSN) dapat dilihat sebagai kehadiran MANET di ruang fisik di sekitar kita. Mereka terdiri dari perangkat berbiaya rendah dan berdaya rendah yang digunakan di lingkungan atau, alternatifnya, dibawa oleh manusia atau hewan. Perangkat ini biasanya memiliki beberapa memori, CPU, dan radio jarak pendek untuk berkomunikasi satu sama lain. Tertanam di lingkungan kita, kita jarang menyadarinya saat mereka melacak kita dan mencatat lingkungan kita, bahkan mungkin menghidupkan atau mematikan mesin. Salah satu kelemahan dari jaringan sensor awal adalah kesulitan yang terlibat dalam penggelaran sistem tersebut.

Pengguna harus memasang kabel, saluran listrik, dan mungkin komputer yang lebih kecil untuk mengelola sistem. Dalam beberapa kasus, di mana beberapa infrastruktur sudah ada (misalnya daya), jaringan besar dapat digunakan; namun, di daerah terpencil, penyebaran seperti itu tidak mungkin dan tidak sepadan secara finansial.

Dengan diperkenalkannya perangkat nirkabel, batasan ini telah dihapus; oleh karena itu

menjadi mungkin untuk memasangnya hampir di mana-mana: bangunan, jalan, jembatan, pada hewan, hutan, dan gunung, hanya untuk beberapa daftar. Sifat nirkabel dari jaringan memungkinkan

penerapan yang mudah, tetapi juga menghadirkan tantangan: Transmisi melalui udara jauh lebih tidak dapat diandalkan daripada transmisi melalui kabel. Tautan radio sangat dipengaruhi oleh kondisi lingkungan, atau penghalang fisik; oleh karena itu protokol komunikasi yang digunakan harus dapat menangani hal ini. Dalam banyak kasus, untuk memungkinkan fleksibilitas terbesar, bahkan jaringan statis diperlakukan sebagai jaringan seluler, karena seringnya perubahan topologi.

Pada bagian ini, beberapa area aplikasi jaringan sensor nirkabel yang paling penting akan dicantumkan, menjelaskan proyek untuk masing-masing area tersebut. Kita akan mulai dengan sistem di sekitar kita

dan kemudian perlahan beralih ke sistem yang digunakan di hutan dan pegunungan terpencil.

3.4.1 Pemantauan Tubuh dan Kesehatan

Daftar skenario akan dimulai dengan sistem pemantauan kesehatan . Beberapa jenis perangkat sensor telah digunakan untuk memantau kesehatan pasien selama beberapa dekade. Sayangnya, sebagian besar sistem ini memerlukan sensor fisik yang ditempatkan di tubuh untuk disambungkan ke komputer besar di samping tempat tidur pasien di rumah sakit. Pada saat itu, ini bukanlah tindakan pencegahan, melainkan upaya untuk memantau fungsi vital tubuh orang tersebut.

Namun, karena perangkat menjadi lebih kecil, dan kebutuhan akan kabel menghilang, dan sensor dapat dipakai hampir tanpa disadari; dengan demikian, dokter dapat memantau kesehatan pasien dan memperingatkan mereka sebelum terjadi sesuatu yang serius. Salah satu tantangan utama dalam sistem ini adalah menghasilkan sensor yang cukup kecil sehingga dapat dipakai dengan nyaman sekaligus menghasilkan pengukuran yang andal. Sensor detak jantung sederhana telah dibuat pada jam tangan sejak lama, dan beberapa proyek melibatkan sensor yang dibuat pada gaun atau sepatu khusus.

Perangkat sekarang dapat terhubung secara nirkabel ke smartphone (melalui Bluetooth) untuk memberikan informasi kesehatan kepada pengguna. Contoh komersialnya adalah sepatu lari Nike yang dapat mengirimkan informasi ke iPhone dan menunjukkan seberapa banyak pengguna berlari/berjalan.

Sensor sekarang dapat digabungkan dengan setelan. Sebuah studi yang sangat menarik dibuat di mana petugas pemadam kebakaran "dilengkapi" dengan sensor yang dapat dipakai untuk memantau detak jantung, tekanan darah, dan sebagainya, dan data dikumpulkan dan kemudian dikirim kembali ke stasiun pangkalan [18]. Motivasi dari proyek ini adalah untuk melihat bagaimana pekerjaan yang penuh tekanan fisik dan mental ini memengaruhi petugas pemadam kebakaran dan apakah umpan balik waktu nyata dapat membantu menjaga kesehatan mereka.

Sistem terkait lainnya adalah karya Lorincz et al. [19] dari situs Universitas Harvard. Tujuan mereka adalah memberikan solusi jangka panjang untuk memantau kondisi fisiologis seseorang menggunakan platform sensor yang dirancang khusus. Perangkat berisi CPU, radio yang kompatibel dengan Zigbee, kartu micro-SD, giroskop, dan antarmuka untuk menghubungkan sensor eksternal. Mereka merancang protokol pengiriman data yang efisien, serta protokol untuk mengekstraksi fitur dari data beresolusi tinggi. Intinya adalah untuk menghindari pengiriman seluruh data sepanjang waktu, melainkan hanya mengirim peristiwa penting (seperti tanda serangan epilepsi) secara real time, sehingga menghemat banyak energi.

FluPhone [20] adalah sistem yang dirancang untuk nonprofesional untuk memantau penyebaran penyakit menggunakan ponsel. Perangkat menggunakan antarmuka Bluetooth untuk melihat apa perangkat lain (yaitu, orang) di sekitar. Suar membawa informasi tentang kesehatan pengguna; dengan demikian seseorang dapat melihat apakah dia telah ditempatkan bersama seseorang yang membawa virus. Jenis data ini bisa sangat berguna bagi ahli epidemiologi.

3.4.2 Rumah Pintar

Setelah membahas berbagai metode untuk memantau tubuh kita, sekarang kita beralih ke rumah pintar.

Di rumah pintar, lingkungan menyesuaikan dengan pemiliknya sambil mengoptimalkan energy penggunaan dengan mematikan peralatan yang tidak digunakan seperti pemanas. Ini dicapai dengan menggunakan detektor gerak bawaan, sensor suhu dan cahaya, dan sejumlah aktuator.

Sistem yang lebih kompleks memprediksi kapan pengguna akan kembali ke rumah, dan mereka mempersiapkan rumah terlebih dahulu. Demikian pula, beberapa sistem dapat melacak orang tersebut di rumah dan dapat menyalakan/mematikan lampu saat dia berjalan di sekitar rumah.

Lingkungan rumah pintar membuat perbedaan besar dalam perawatan lansia di rumah. “Rumah” dapat memberi tahu perawat atau dokter jika orang di rumah tidak bergerak atau tersandung, serta memastikan bahwa orang tersebut aman dan nyaman di dalam rumah. Proyek SM4ALL [21] menyediakan kerangka kerja untuk perangkat tertanam dalam jaringan sentris orang. Ini didasarkan pada teknologi P2P dan dikatakan mudah diskalakan.

Kamilaris dkk. [22] melangkah lebih jauh dan menghubungkan semuanya ke Internet.

Inilah yang disebut Internet of things, di mana semua perangkat berkomunikasi melalui antarmuka umum (dalam hal ini HTTP) dan dengan demikian dapat dengan mudah dikendalikan dari jarak jauh. Makalah ini menjelaskan bukti konsep yang dibangun dari perangkat sensor off-the-shelf yang menjalankan TinyOS dan dengan demikian menunjukkan kelayakan gagasan tersebut.

3.4.3 Pemantauan Industri

Sekarang kita beralih dari lingkungan rumah ke skala yang lebih besar, di mana bangunan atau struktur besar perlu dipantau untuk tujuan keamanan atau pemeliharaan . Jaringan sensor nirkabel ideal untuk skenario seperti itu, karena dapat digunakan tanpa harus memodifikasi bangunan yang akan dipantau. Pada bagian ini, kami akan menjelaskan sistem untuk memantau menara bersejarah di Italia, terowongan, dan jembatan, tetapi daftar ini masih jauh dari lengkap—sensor dapat dipasang di jalan untuk memantau lalu lintas, di tiang lampu untuk memantau tingkat polusi, dan segera. Semua jaringan ini memerlukan arsitektur perangkat lunak dan perangkat keras yang berbeda karena persyaratannya untuk operasi yang dioptimalkan. Mereka memiliki persyaratan data yang berbeda: Sistem pemantauan kesehatan struktur jembatan harus menyediakan data waktu nyata untuk menghindari kecelakaan, sementara data tentang kondisi lingkungan di bangunan bersejarah tidak mengancam jiwa, dan dengan demikian berpotensi tertunda, jika mengarah ke untuk penggunaan sumber daya yang lebih efisien.

Sensor nirkabel digunakan untuk memantau Torre Aquila, sebuah menara bersejarah di Trento, Italia [23]. Menara ini berisi lukisan dinding abad pertengahan yang terkenal secara internasional, sangat

rentan terhadap variasi kelembaban dan suhu. Pelestarian lukisan dinding ini menjadi perhatian utama, terutama selama pembangunan terowongan di dekat menara. Untuk memastikan lukisan dinding disimpan di lingkungan yang paling ideal, sensor digunakan untuk mengumpulkan data waktu nyata tentang suhu, kelembapan, dan getaran. Ilmuwan dan konservasionis juga tertarik dengan potensi deformasi dinding menara. Untuk mencapai tujuan tersebut, tim merancang sejumlah sensor yang berbeda, semuanya terhubung dalam jaringan yang heterogen. Berbagai jenis sensor dikendalikan oleh middleware umum untuk menyederhanakan parameterisasi sistem.

Terowongan pemantauan adalah area penting lain dari jaringan sensor: Sangat mudah untuk melihat mengapa pemerintah dan perusahaan bersedia mengeluarkan uang dan upaya ke dalam sistem semacam itu. Bahkan retakan kecil dapat menyebabkan kerusakan serius pada struktur terowongan, menyebabkan kecelakaan. Sensor telah dipasang di terowongan Metro [24] dan terowongan mobil [25]. Dalam kasus pertama, dinding dimonitor untuk deformasi dan retakan, sementara di kasus kedua sistem dikerahkan untuk mengoptimalkan tingkat cahaya di dalam terowongan (perubahan kondisi pencahayaan yang tiba-tiba saat keluar dari terowongan dapat menyebabkan kecelakaan mobil). Kedua sistem menggunakan jaringan multihop, di mana data dikirim pertama kali ke node terdekat dan kemudian ke stasiun pangkalan lokal, yang kemudian meneruskan data ke dunia luar. Menarik untuk dicatat bagaimana perilaku propagasi sinyal radio berubah berdasarkan kondisi di dalam terowongan.

Protokol perutean yang mengirimkan data harus dapat mengadopsi perubahan ini dengan terus memantau kualitas tautan dan kemudian merutekan data yang sesuai.

Aplikasi yang agak mirip adalah pemantauan jembatan: Mereka dibangun dengan angin kencang

dan kondisi cuaca normal; namun, ini harus dipantau, jika terjadi badai atau panas yang parah. Pekerjaan Ian Wassel dan timnya memantau Jembatan Humber di Inggris [26]. Ada masalah dengan pendinginan

struktur penahan jembatan: Mereka memiliki jadwal perbaikan, yang ternyata tidak efisien; oleh karena itu mereka menggunakan jaringan untuk mengontrol pendinginan secara mandiri, berdasarkan suhu sebenarnya di dalam ruangan.

Meskipun sistem ini masih jauh lebih mudah diakses oleh pengontrol daripada sistem yang akan diikuti, mereka berbagi masalah dan keuntungan umum dari WSN, seperti kemudahan penerapan, pengumpulan dan transfer data yang andal, kendala daya, dan tantangan komunikasi radio.

3.4.4 Pemantauan Lingkungan

Aplikasi jaringan sensor nirkabel yang paling menantang adalah aplikasi di mana infrastruktur pendukung tidak tersedia. Yang kami maksud dengan infrastruktur pendukung adalah daya, cakupan GSM atau

Wifi, atau bahkan aksesibilitas fisik. Pada bagian ini, kita akan fokus pada pemantauan lingkungan alam, dimana tugas jaringan adalah memantau kondisi di alam liar. Infrastruktur tidak tersedia dalam banyak kasus; oleh karena itu nirkabel, perangkat mandiri harus digunakan. Kurangnya infrastruktur juga berarti

komunikasi antara sensor dan stasiun pangkalan perlu direncanakan dengan hati-hati. Karena node tidak dapat selalu mengirimkan langsung ke base station, mereka perlu menggunakan jaringan multihop;

sehingga mereka perlu memutuskan ke mana harus mengirim data, tanpa membanjiri jaringan. Dalam banyak kasus, data tidak memiliki persyaratan waktu yang ketat, oleh karena itu node dapat dengan mudah menyimpannya, menunggu kesempatan yang baik untuk ditransmisikan—seperti kualitas tautan yang kuat atau sink seluler yang lewat.

Salah satu aplikasi yang menantang adalah pemantauan gletser di sistem GlacsWeb [27] yang diterapkan di Norwegia dan Islandia. Sistem tersebut terdiri dari probe yang dibenamkan ke dalam es dan stasiun pangkalan yang menyampaikan data kembali ke pengguna menggunakan GSM/GPRS. Probe termasuk sensor tekanan, suhu, kelembaban, dan orientasi, serta jam waktu nyata dan baterai besar. Base station pada dasarnya adalah komputer sederhana berbasis UNIX (berdasarkan platform

Gumstix). Sistem ini juga mengalami beberapa transisi, di mana board dan perangkat lunak yang berjalan di board diperbarui menggunakan pengalaman yang diperoleh dari penerapan sebelumnya.

PermaSense [28] adalah proyek serupa, mengumpulkan data real-time di lingkungan pegunungan tinggi, di Swiss. Dalam hal ini, sensor diharapkan bekerja selama 3 tahun secara mandiri dan bertahan di lingkungan yang keras (kisaran suhu antara ÿ40 ÿC dan +65 ÿC), pengambilan sampel antara 1 dan 60 menit, dan memiliki kapasitas penyimpanan untuk menyimpan data selama 6 bulan. Sensor menyampaikan data (bila memungkinkan) kembali ke

stasiun pangkalan secara nirkabel. Proyek ini membuktikan bahwa penyebaran sensor otonom jangka panjang bukanlah fiksi ilmiah.

3.4.5 Pemantauan Hewan

Langkah selanjutnya dari pemantauan lingkungan alam adalah memantau hewan secara langsung. Selalu sulit untuk mengamati dan mempelajari mereka di habitat aslinya, karena secara alami mereka tidak menyukai kehadiran manusia. Ada upaya untuk memasang kamera infra merah atau menggunakan teknik pengawasan lainnya; namun, selalu sulit untuk melacak individu tersebut. Dengan kemajuan teknologi sensor, menjadi mungkin untuk membuat perangkat yang cukup kecil untuk dibawa oleh hewan. Sensor dapat mengumpulkan data tentang hewan secara langsung, tetapi ini juga menimbulkan banyak tantangan bagi perancang sistem: Perangkat harus kecil dan ringan, sementara harus bertahan selama mungkin (hewan mungkin tidak mudah ditangkap kembali). Kapasitas baterai saat ini sangat terbatas; oleh karena itu perangkat lunak pada perangkat harus menggunakan sumber daya yang terbatas ini dengan bijak.

Banyak upaya dilakukan untuk merancang protokol jaringan yang efisien, karena transmisi data adalah salah satu tugas sistem yang paling menghabiskan energi: Semakin sedikit transmisi, semakin lama jaringan bertahan. Untuk mengurangi jumlah transmisi, node cenderung menggunakan semacam

logika untuk mengagregasi atau memfilter lompatan data berikutnya, mungkin berdasarkan riwayat colocation, jarak ke stasiun pangkalan, dan sebagainya.

Tugas menjadi lebih sulit karena sifat hewan yang bergerak, dan sulit untuk memprediksi ke mana mereka akan bergerak. Kami akan mempresentasikan beberapa karya awal tentang pemantauan satwa liar menggunakan sensor selanjutnya.

Salah satu sistem pertama yang digunakan adalah proyek Great Duck Island [29]. Pada tahun 2002, 43 sensor yang dirancang khusus dikerahkan untuk memantau burung laut Storm Petrel milik Leach.

Tujuan proyek ini adalah mempelajari kebiasaan bersarang burung-burung ini; oleh karena itu sensor ditempatkan di liang sarang bawah tanah dan di pintu masuk sarang. Alat tersebut dilengkapi dengan cahaya, suhu, tekanan, dan sensor infra merah (untuk mendeteksi keberadaan burung). Mereka dikurung dalam wadah tahan cuaca dan ditempatkan di lingkungan sekitar 120 hari. Node gateway ditempatkan di antara node sensor ini, dan membentuk jaringan transit untuk menyediakan konektivitas ke stasiun pangkalan. Selain mengumpulkan data tentang burung, proyek ini memberikan banyak wawasan tentang penerapan sensor jangka panjang. Mereka mencatat informasi tentang sensor (misalnya, level voltase dan memori) dan tautan radio yang menghubungkan perangkat.

Seperti yang diharapkan dari penerapan di dunia nyata, tidak semua sensor selamat: Banyak yang tidak berfungsi, sementara beberapa mati sepenuhnya, terutama karena kelembapan. Proyek ini berhasil menggambarkan pelajaran yang didapat dari jaringan sensor nirkabel, serta merancang jaringan yang kuat dengan struktur kompleks yang memungkinkan akses hampir secara real-time.

Proyek ZebraNet adalah yang pertama memasang sensor pada hewan [30]. Tujuan dari proyek ini adalah untuk memantau sekitar 30 zebra di Pusat Penelitian Mpala di Kenya, dan persyaratannya termasuk mencatat lokasi GPS setiap 3 menit, setiap jam.

“sampel aktivitas”, operasi satu tahun tanpa campur tangan manusia, bekerja tanpa infrastruktur apa pun, dan pengiriman data secara nirkabel ke stasiun pangkalan. Perangkat tersebut dilengkapi dengan chip GPS, radio jarak jauh dan pendek, dan memori dalam jumlah terbatas, dan dipasang pada kalung yang dikenakan oleh hewan. Protokol perutean khusus dirancang, memanfaatkan pola mobilitas hewan untuk meningkatkan pengiriman data.

Proyek berbeda yang berfokus pada possum Brushtail. Data dikumpulkan di Selandia Baru menggunakan kerah GPS yang melekat pada possum Brushtail [31]. Tag ini berusaha mengambil lokasi GPS paling banyak setiap 16 menit. Karena tag GPS agak haus daya, tag tersebut dimatikan pada malam hari untuk menghemat daya—bahkan dalam kasus ini, tag tersebut perlu diambil kembali setiap 3 minggu untuk mengganti baterai serta membongkar data. Pencapaian utama dari proyek ini adalah keberhasilan penggunaan GPS pada hewan, bersama dengan kumpulan data besar tentang mobilitas posum.

Proyek WildSensing [32] ditujukan untuk menyebarkan sistem hibrid WSN-RFID untuk memantau secara mandiri Badgers Eurasia (Meles meles) di Wytham Woods, hutan dekat Oxford. Proyek ini berlangsung dari tahun 2007 hingga 2010, termasuk penyebaran selama 14 bulan, menghasilkan lebih dari 2 juta penampakan hewan dan banyak pelajaran yang didapat tentang penerapan di kehidupan nyata. Meskipun musang memiliki ukuran yang mirip dengan possum, tag GPS tidak mungkin: Pertama-tama, musang hanya dapat dijebak dua kali setahun, dan oleh karena itu tag tersebut harus bekerja setidaknya selama 6 bulan. Kedua, penerimaan GPS ditemukan sangat buruk di dekat tanah. Pendekatan berbeda diambil: Tag RFID aktif digunakan pada hewan, dan sistem sensor RFID hibrida

dirancang untuk mengumpulkan penampakan hewan. Sekitar 70 hewan diberi tag RFID, sementara 29 pembaca RFID ditempatkan di lokasi tertentu di hutan. Pembaca ini dapat mendeteksi suar reguler yang dikirim oleh tag dalam jangkauan, sehingga mencatat "penampakan" hewan tersebut.

Tujuan dari teknologi ini tentu saja untuk menempatkan sensor nyata pada hewan. Meskipun kami mencapainya dengan lambat, masih sangat sulit untuk mencapai seumur hidup yang sebanding dengan tag VHF atau RFID. Ahli zoologi dan biologi, di sisi lain, dapat membahayakan masa pakai perangkat untuk mendapatkan lebih banyak data: Sensor dapat memberikan data berkelanjutan secara langsung tentang hewan. Dengan tren saat ini, ini akan menjadi mungkin dalam waktu dekat, dan para ilmuwan akan dapat memantau satwa liar secara mandiri dari kantor mereka.

3.5 PENCARIAN DAN PENYELAMATAN

MANET juga dapat dikerahkan dalam situasi bencana karena dapat mendukung upaya pencarian dan penyelamatan. Selain menyediakan komunikasi darurat antara penyelamat, mereka juga dapat digunakan untuk menyebarkan perangkat mandiri dengan cepat seperti kendaraan udara tak berawak (UAV) atau robot otonom, untuk meminimalkan waktu respons, meningkatkan keselamatan penyelamat, dan memaksimalkan efisiensi. dari sumber daya yang tersedia.

3.5.1 Pencarian dan Penyelamatan dengan UAV

Dalam operasi pencarian dan penyelamatan, waktu sangat penting. Untuk memaksimalkan kesempatan menemukan korban selamat, operasi pencarian harus dilakukan secepat mungkin. Dalam pencarian untuk bukti kemungkinan lokasi korban, kendaraan udara tak berawak (UAV) telah didemonstrasikan sebagai alat yang efisien karena mereka dapat dengan cepat memperoleh citra udara dari beberapa titik pandang secara bersamaan bahkan di lingkungan yang berbahaya [33]. Saat ini, sebagian besar sistem dilengkapi dengan kamera dan dikendalikan oleh operator UAV yang menerbangkan UAV dan operator sensor yang mengontrol kamera dan menginterpretasikan data. Tetapi untuk mengamati, menilai, dan mengintegrasikan semua informasi yang diterima dari sensor adalah proses yang sulit dan rawan kesalahan. Sumber daya manusia yang dibutuhkan untuk mengoperasikan UAV bisa sangat mahal. Salah satu cara untuk mengurangi kesulitan ini adalah mengotomatisasi pengoperasian UAV. Jika UAV dapat melakukan pengaturan mandiri kolaboratif dalam penerbangan, mereka dapat mengoptimalkan operasinya. Mereka juga dapat responsif terhadap kegagalan sistem dan sensor.

Jika mereka melakukan deteksi objek dalam penerbangan, operator sensor hanya perlu diberi tahu tentang kejadian kritis.

Komunikasi antar UAV terjadi pada setiap langkah operasi pencarian dan penyelamatan.

Pertama UAV harus merencanakan jalur mereka untuk sampai ke area eksplorasi dengan cara yang aman (misalnya, menghindari hambatan lingkungan dan UAV lainnya) [34]. Jika peta lingkungan diketahui, perencanaan jalur deterministik dapat diimplementasikan. Masalah perutean UAV melalui area yang akan dijelajahi kemudian dapat dinyatakan sebagai variasi dari Masalah Traveling Salesman dengan beberapa agen, masalah yang ada heuristik [35]. Jika sedikit atau tidak ada informasi yang diketahui tentang lingkungan, maka perencanaan jalur probabilistik adalah pendekatan yang lebih masuk akal. UAV kemudian dapat mengadaptasi jalur pencarian mereka karena lebih banyak data tentang lingkungan diperoleh melalui pengamatan selanjutnya. Ketika berada dalam jangkauan

komunikasi satu sama lain, UAV dapat bertukar hasil pengamatan mereka dan memadukan informasi ini, yang akibatnya dapat digunakan sebagai input dalam strategi pencarian mereka.

Setelah UAV mencapai area eksplorasi mereka, mereka secara individual melakukan operasi pencarian sesuai dengan strategi yang telah ditentukan sebelumnya. Heuristik serakah berdasarkan algoritme yang diilhami secara biologis (misalnya, algoritme feromon semut) telah menunjukkan hasil yang efektif dalam situasi di mana banyak agen kolaboratif hadir [36,37]. Jika informasi tambahan tentang lingkungan diketahui seperti adanya halangan, atau jika beberapa informasi tentang posisi korban dapat diperoleh, pencarian berdasarkan grid hunian merupakan pendekatan yang efektif dan terukur karena dapat mengintegrasikan informasi sebelumnya dan berbagi informasi yang diperoleh dari UAV tetangga [38,39]. Namun, penting juga untuk menyadari bahwa kesalahan dapat terjadi selama operasi penginderaan.

Ini mungkin akibat dari kualitas perangkat keras yang digunakan, dari cara analisis data dilakukan, atau bisa saja akibat dari kondisi lingkungan yang buruk selama operasi penginderaan. Untuk menjelaskannya, Chung et al. mengusulkan kerangka kerja probabilistik di mana banyak UAV mencari banyak target dalam lingkungan statis yang telah ditentukan sebelumnya.

Setelah setiap pengamatan atau setelah bertukar hasil pengamatan dengan UAV lain, setiap UAV memperbarui petanya, menunjukkan keyakinannya di mana korban berada sambil mempertimbangkan kemungkinan kesalahan pengamatan [40-43]. Bertuccelli dan How telah memperluas pekerjaan ini dengan mempertimbangkan bahwa target dapat bergerak dan lingkungan juga dapat berubah dari waktu ke waktu [44]. Dengan pengetahuan tentang probabilitas kesalahan penginderaan, juga memungkinkan untuk memodelkan operasi pencarian menggunakan Proses Keputusan Markov yang Dapat Diamati Sebagian. Sebuah UAV kemudian dapat memperkirakan apa yang akan menjadi tindakan terbaik untuk diambil (misalnya, terbang ke depan menuju area tertentu) untuk memaksimalkan hadiahnya Hadiah ini dapat didasarkan pada informasi maksimum tentang lokasi korban yang diharapkan diperolehnya. Meskipun ini merupakan jalan penelitian yang menjanjikan, biaya komputasi tinggi yang diperlukan untuk saat ini membatasi penerapannya pada skenario yang ruang keadaannya terbatas [45,46].

Terakhir, UAV harus melaporkan informasi ini ke stasiun pangkalan. Ada dua opsi potensial: UAV kembali ke lokasi di mana ia dapat mencapai stasiun pusat dan mengirimkan datanya, atau UAV membuat jembatan komunikasi nirkabel untuk mentransfer data yang dikumpulkan dalam waktu dekat [47]. Jika ada beberapa tim darat, satu masalah yang muncul adalah menentukan di mana posisi UAV untuk membuat jaringan yang terhubung. Metode yang diusulkan bergantung pada (a) pada fakta bahwa ground node secara berkala mentransmisikan pesan suar sehingga UAV dapat menyesuaikan lintasannya agar jaringan tetap terhubung [48], atau (b) mencoba mengoptimalkan posisi UAV berdasarkan lokasi yang dipilih set kemungkinan posisi dan arus lalu lintas yang diketahui [49].

3.5.2 Eksplorasi Multiagen di Area Tak Dikenal

Jika terjadi keadaan darurat di dalam gedung, sangat penting bagi responden pertama untuk memperoleh informasi sebanyak mungkin tentang situasi yang sedang berlangsung, untuk mengidentifikasi dan mengatasi bahaya dan mengoordinasikan penyelamatan korban. Dalam banyak kasus, sangat berbahaya mengirim petugas tanggap manusia untuk melakukan tugas ini. Sebaliknya, banyak penelitian baru-baru ini berfokus pada pengiriman robot otonom, juga disebut sebagai agen

dalam literatur, untuk menutupi area secepat mungkin dan melaporkan kembali temuan menarik kepada personel manusia di luar gedung.

Namun, ada sejumlah tantangan dalam mengoordinasikan agen otonom di dalam gedung— misalnya, kemungkinan kurangnya peta, kegagalan jaringan yang dibuat sebelumnya, dan komunikasi dalam ruangan nirkabel jarak pendek dan seringkali tidak dapat diandalkan. Selain itu, mungkin sulit untuk menggunakan pemosisian GPS di dalam gedung, sehingga agen tidak dapat mengandalkan pengetahuan tentang lokasi persisnya saat berada di dalam. Untuk semua alasan ini, MANET baru-baru ini menemukan banyak aplikasi dalam eksplorasi multiagen di area yang tidak diketahui.

Saat agen memasuki area darurat, mereka dapat secara dinamis menyebarkan jaringan node sensor stasioner (terkadang disebut sebagai tag) dan membangun jaringan ad hoc langsung di lapangan. Dengan membaca dan memperbarui status tag lokal, agen dapat berkoordinasi secara tidak langsung satu sama lain, tanpa bergantung pada komunikasi agen-ke-agen langsung. Varietas MANET khusus ini disebut "Stigmergy" [50] dan terinspirasi oleh pengamatan koloni serangga sosial, yang memodifikasi lingkungan mereka untuk berkomunikasi satu sama lain. menutupi seluruh medan asalkan semua sel dapat diakses oleh agen. Meskipun algoritmenya sederhana dan kuat, tidak ada cara untuk mengetahui kapan lingkungan dieksplorasi sepenuhnya, dan agen melanjutkan fase eksplorasi hingga kehabisan energi. Dengan demikian, pendekatan ini tidak sesuai dalam skenario darurat, di mana pertimbangan utamanya adalah untuk mencakup keseluruhan area secepat mungkin dan diberitahukan segera setelah tugas selesai. Keterbatasan lain menyangkut penggunaan kemampuan agen yang tidak memadai: Dalam skenario dengan banyak ruangan, sebagian besar agen sibuk menyapu

beberapa ruangan pertama berulang kali sementara hanya beberapa dari mereka yang berangkat untuk mendapatkandaerah baru.

Solusi untuk masalah ini adalah algoritma Brick&Mortar [53], dimana agen dapat dengan mudah menentukan kapan tugas eksplorasi selesai. Algoritme menghindari menjelajahi area yang sama beberapa kali, memanfaatkan semua agen dengan baik, dan mampu menyelesaikan loop. Hasil eksperimen menunjukkan bahwa Brick&Mortar secara signifikan lebih cepat

daripada dua algoritma yang bersaing, Ants [51] dan Multiple Depth First Search [53], dalam

berbagai skenario. Pekerjaan yang lebih baru [54,55] memperluas model sebelumnya dan memanfaatkan MANET untuk menggabungkan dua mode komunikasi: antara agen dan tag

(agent-to-tag) dan komunikasi multihop dalam jaringan stasioner dari tag (tag -untuk-menandai). Dalam algoritme ini, yang disebut HybridExploration, tag bertukar informasi lokal secara nirkabel dengan tag terdekat untuk lebih membantu agen dalam tugas eksplorasi mereka.

Penggunaan suar radio untuk memandu navigasi robot dan membantu mereka dalam jangkauan medan yang tidak diketahui telah diusulkan sebagai aplikasi MANET lainnya

[56-59]. Secara khusus, robot dapat mendeteksi suar (yang telah ditempatkan sebelumnya di lingkungan), memilih salah satunya, dan bergerak ke sana. Suar dapat memberi tahu robot ke arah mana (Utara, Timur, Selatan, atau Barat) letak suar tetangga yang terakhir dikunjungi.

Beacon dan robot keduanya dilengkapi dengan kompas 2-bit, sehingga yang pertama dapat

memberikan indikasi yang terakhir tentang arah mana yang harus diambil untuk mencapai suar berikutnya. Penggunaan jaringan tertanam pra-disebarkan untuk membantu navigasi robot di lingkungan juga telah dipelajari secara ekstensif [60-63]. Secara khusus, platform jaringan tertanam

yang kecil dan relatif murah, yang disebut GNAT, mampu memandu navigasi robot LEGO Mindstorm/RCX menggunakan pemancar dan penerima inframerah. Kekuatan utama dari pekerjaan ini bergantung pada eksperimen dunia nyata yang ekstensif (hingga 156 node dikerahkan), yang membuktikan kelayakan pendekatan mereka dan mode komunikasi agen- ke-lingkungan secara umum.

Meskipun algoritme eksplorasi memungkinkan robot menjelajahi area yang tidak diketahui secepat mungkin, mereka tidak menjelaskan cara memandu korban menuju pintu keluar darurat atau cara memandu petugas tanggap manusia menuju lokasi korban dan bahaya.

Kebutuhan tambahan ini telah diatasi dalam pekerjaan lain [64], di mana penemuan dinamis dan pemeliharaan rute yang efisien dilakukan, sehingga pintu keluar darurat terhubung ke sel- sel kritis di area tempat kejadian menarik diidentifikasi. Tujuan dari pendekatan ini ada dua:

(1) untuk menemukan jalur evakuasi sedini mungkin dalam proses eksplorasi dan (2) untuk menjaga jalur evakuasi sependek mungkin untuk memungkinkan akses yang mudah bagi para penanggap manusia ke korban dan bahaya. Idenya adalah untuk mengaktifkan pencarian jalur evakuasi secara paralel dengan tugas eksplorasi wilayah

3.6 JARINGAN KENDARAAN

Tren terbaru dalam Sistem Transportasi Cerdas menunjukkan bahwa semakin banyak kendaraan akan dilengkapi dengan transceiver nirkabel yang akan memungkinkan mereka berkomunikasi satu sama lain (V2V) atau dengan infrastruktur tetap sisi jalan (V2I). Kendaraan ini kemudian dapat membentuk kelas khusus jaringan nirkabel, yang dikenal sebagai jaringan ad hoc kendaraan atau VANET. Para peneliti dan industri otomotif membayangkan penerapan spektrum besar aplikasi yang berjalan di VANET, termasuk sistem keselamatan jalan, platform koordinasi kendaraan, dan layanan notifikasi untuk memperingatkan pengemudi tentang kecelakaan dan kemacetan lalu lintas.

Untuk mengakomodasi konektivitas V2V IEEE mengembangkan standar 802.11p atau Dedicated Short-Range Communications (DSRC) [65]. Standar ini menetapkan peningkatan ke 802.11a yang diperlukan untuk mendukung aplikasi Sistem Transportasi Cerdas (ITS) yang mendukung pertukaran data antara kendaraan berkecepatan tinggi dan antara kendaraan dan infrastruktur pinggir jalan. Selain itu, pemerintah di seluruh dunia secara aktif mendukung konektivitas kendaraan-ke-kendaraan dengan melisensikan sebagian besar (dan mahal) spektrum nirkabel untuk penggunaan ini (5,9 GHz di AS dan 5,8 GHz di Eropa dan Jepang), sehingga mendorong sistem ini selangkah lebih maju mendekati realisasi.

Ada banyak minat penelitian di VANET karena banyaknya variasi aplikasi menarik mulai dari sistem pendukung mengemudi hingga koordinasi kendaraan otonom, penyebaran informasi, dan sistem transportasi cerdas.

3.6.1 Sistem Pendukung Keselamatan Berkendara

Sistem Pendukung Keselamatan Berkendara (DSSS) bertujuan untuk mengurangi kecelakaan lalu lintas, mengurangi beban pengemudi dalam membuat keputusan, dan meningkatkan kesadaran pengemudi dengan memungkinkan kendaraan berkomunikasi satu sama lain dan dengan infrastruktur yang dipasang (misalnya, lampu lalu lintas cerdas). Sistem tersebut saat ini sedang digunakan di Jepang sebagai bagian dari proyek UTMS [66]. Perusahaan otomotif besar mengambil bagian dalam inisiatif ini: Toyota [67,68] telah mengembangkan sistem navigasi on-board yang kompatibel dengan DSSS

yang bertujuan untuk mengurangi kecelakaan dengan memberikan peringatan audio dan visual melalui sistem navigasi on-board. Fitur utama dari sistem ini adalah untuk memperingatkan pengemudi

(i) ketika kendaraan mendekati lampu merah atau tanda berhenti tanpa niat berhenti, (ii) tentang kendaraan yang diam atau lebih lambat di depan, (iii) tentang kemungkinan tabrakan dengan kendaraan. atau pejalan kaki di titik buta atau sudut (atau saat kendaraan berada di jalur tabrakan di persimpangan), dan (iv) tentang kemungkinan bahaya lain di depan (misalnya kecelakaan). Melalui sistem DSSS, sistem navigasi kendaraan menerima informasi infrastruktur dari suar pinggir jalan dan kendaraan di sekitarnya. Sehubungan dengan informasi kendaraan real-time, seperti kecepatan dan posisi pedal akselerator, informasi ini digunakan untuk meningkatkan keselamatan dengan memberikan peringatan audio dan visual bila perlu. Selain memberi peringatan kepada pengemudi, sistem ini dapat mengintervensi secara aktif dengan menginjak rem atau bahkan memanggil layanan darurat. Nissan juga menerapkan sistem seperti itu, yang saat ini sedang diuji menggunakan 20.000 kendaraan di Kanagawa (sebuah prefektur di selatan Tokyo) [69].

3.6.2 Koordinasi Kendaraan

Kopling radio nirkabel digunakan untuk mengoordinasikan kendaraan untuk membentuk peleton otonom: kendaraan yang mempercepat atau mengerem secara bersamaan, sehingga memungkinkan peleton bergerak sebagai satu unit seperti kereta. Dalam peleton seperti itu, kendaraan dapat melaju dengan kecepatan tinggi hingga 70 mph sambil menjaga jarak sesedikit 21 kaki di antaranya.

Pengelompokan kendaraan dapat melipatgandakan kapasitas jalan, menghemat bahan bakar hingga 25% dan bahkan meningkatkan keselamatan [70]. Selain itu, sistem ini mampu mengotomatisasi berbagai prosedur berkendara seperti penggabungan jalur jalan raya, koordinasi persimpangan,

prioritas lampu lalu lintas, dan penghindaran rintangan kolaboratif sehingga semakin meningkatkan kapasitas dan kesel Komunikasi nirkabel multihop digunakan yang memungkinkan kendaraan bertukar informasi

penting ratusan kali per detik dengan penundaan minimum. Untuk mendukung persyaratan ini, protokol komunikasi berbasis DSRC seperti AVCS [71] telah dirancang khusus untuk mencapai latensi rendah dan rasio pengiriman yang tinggi.

Implementasi pertama dari sistem semacam itu adalah bagian dari program “California Partners for Advanced Transit and Highways” (PATH) [70], di mana prototipe paling awal diuji di San Diego County, California di sepanjang Interstate 15. Versi yang lebih baru dari ini sistem saat ini diuji oleh perusahaan besar seperti Mercedes, BMW, Volkswagen dan Toyota. Di Eropa, Volvo saat ini sedang menguji sistem tersebut sebagai bagian dari proyek “Safe Road Trains for the Environment" (SARTRE) [72].

3.6.3 Sistem Notifikasi

Kendaraan dapat dianggap sebagai sensor bergerak yang mengumpulkan semua jenis informasi (misalnya, kondisi lalu lintas real-time, lokasi lubang, gambar terkini, pengukuran polusi, lokasi tempat parkir yang tersedia, kecelakaan terdekat). Setelah itu, kendaraan dapat mengirimkan informasi ini ke lokasi pusat untuk diproses melalui stasiun informasi terdekat yang diketahui atau hanya menukarnya satu sama lain secara oportunistik untuk memberi tahu pengemudi lain di sekitarnya tentang peristiwa tertentu.

Demikian pula, kendaraan individu atau titik keputusan pusat (misalnya, badan jalan raya) dapat menghasilkan pemberitahuan (misalnya, peringatan lalu lintas) mengenai ruas jalan tertentu untuk memperingatkan kendaraan lain yang mendekati area tersebut. Perutean multihop dalam hubungannya dengan teknik penyebaran pesan lokal dapat digunakan untuk menyebarkan informasi ke kendaraan di sekitarnya.

Awalnya, sistem tersebut didasarkan pada penyebaran epidemi [73]: Sebuah kendaraan yang menyimpan sepotong informasi (misalnya, tentang kecelakaan terdekat) akan bertukar informasi ini dengan kendaraan lain yang kontak saat mengemudi. Hal ini menyebabkan penyebaran informasi yang sangat cepat yang menimbulkan biaya tinggi dalam hal kemacetan jaringan.

Oleh karena itu, sistem Publish/Subscribe [74] digunakan untuk menyebarkan notifikasi hanya ke kendaraan yang tertarik. Langganan kendaraan menunjukkan minat pengemudi tentang jenis konten dan digunakan untuk memfilter dan merutekan informasi ke kendaraan yang terpengaruh (perutean berbasis konteks). Sistem navigasi satelit kendaraan selanjutnya dapat digunakan untuk menyimpulkan minat (misalnya, kendaraan hanya berlangganan untuk menerima informasi mengenai rute navigasi mereka). Publikasi, dihasilkan oleh kendaraan lain atau oleh server pusat, pertama-tama diarahkan ke area tersebut, dan kemudian disebarluaskan ke pelanggan dengan cara berbasis konteks. Demikian pula, proyek FleetNet dan CarTalk [75,76] menggunakan pendekatan store-and-forward untuk mendistribusikan data yang relevan secara lokal untuk memenuhi kebutuhan akan informasi yang bergantung pada lokasi.

MANET juga digunakan untuk membantu pengemudi menemukan tempat parkir gratis [77]. Kendaraan dapat mengumpulkan informasi ini, dan mekanisme epidemi dapat digunakan untuk menyebarluaskannya sementara redundansi dapat diminimalkan dengan mengumpulkan informasi: Karena informasi tempat parkir bersifat spatiotemporal, distribusi spasialnya mungkin dibatasi dengan mempertimbangkan relevansi lokalnya dan usia. Pada intinya, informasi rinci disebarluaskan untuk daerah lokal sementara informasi yang lebih kasar (agregat) lebih disukai untuk daerah yang lebih jauh.

Selanjutnya, konektivitas internet dapat disediakan melalui jaringan kendaraan multihop. Di DieselNet [78], yang saat ini terdiri dari 40 bus, mereka menggunakan kebijakan DTN untuk merutekan informasi dari/ke penumpang dan Internet. Selain itu, mereka menggunakan "throwbox" [79] untuk meningkatkan jumlah kontak DTN. CarView [80,81] mengeksploitasi sistem

navigasi untuk mengarahkan informasi secara efisien dari kendaraan ke/dari Internet dengan bantuan sistem navigasi. Protokol carry-and-forward diusulkan untuk pengiriman pesan yang andal antar kendaraan dalam partisi jaringan yang berubah secara dinamis [82,83]. Protokol penerusan data ini memanfaatkan pengetahuan statistik lalu lintas di lingkungan perkotaan untuk memungkinkan pengiriman pesan secara tepat waktu dari kendaraan ke gateway stasioner sambil meminimalkan transmisi pesan dan mengoptimalkan pemanfaatan bandwidth. Untuk melakukannya, mereka secara proaktif berganti-ganti antara dua strategi penerusan: penerusan multihop, yang mengacu pada penerusan pesan yang agresif ke kendaraan yang memiliki posisi lebih baik untuk mengantarkannya ke gateway, dan muling data, yang mengacu pada pesan penyangga di memori lokal dan membawa mereka dengan kecepatan kendaraan.

Rambu lalu lintas virtual juga diimplementasikan menggunakan MANET. Idenya adalah bahwa informasi tertentu dapat dipertahankan di area tertentu (misalnya, di dekat persimpangan) yang mewakili rambu virtual; kendaraan yang mendekati area yang dipilih akan diberitahukan. Bertahan Geocast [84] adalah protokol pertama yang mengirimkan pesan dengan waktu stabil di wilayah

geografis tertentu. Meskipun pekerjaan ini tidak dioptimalkan untuk jaringan kendaraan, penulis menggunakan Geocast Ad Hoc tradisional (misalnya, banjir yang dibatasi secara geografis secara berkala) dan teknik epidemi untuk menyebarkan pesan di sisi area yang dipilih. Dalam referensi 85 dan 86, penulis lebih lanjut mengeksploitasi peta dan informasi navigasi kendaraan untuk lebih menyempurnakan sistem tersebut dengan hati-hati memilih operator yang dapat menyimpan informasi di dekat rambu virtual.

3.6.4 Sistem Transportasi Cerdas

Sistem berbasis VANET dapat membantu pengemudi dan otoritas jalan raya untuk memantau dan

mengelola kemacetan lalu lintas, mengawasi infrastruktur mereka, dan mengontrol layanan transportasi.

Awalnya, sistem tersebut digunakan untuk memperkirakan waktu kedatangan bus. Sebagai contoh, Portsmouth Real-Time Travel Information System (PORTAL) [87] lebih dari 300 jaringan bus satu sama lain untuk memberikan informasi transportasi secara real-time.

layanan, seperti di mana bus berada, tujuan akhir mereka, dan perkiraan waktu kedatangan mereka. Demikian pula, di DieselNet [78] sistem juga digunakan untuk terus memantau lokasi bus.

Proyek CarTel [88] menganggap kendaraan sebagai platform penginderaan terdistribusi yang dirancang untuk mengumpulkan, memproses, mengirim, dan memvisualisasikan data dari sensor yang dapat dipasang di atasnya. Idenya adalah kendaraan dapat mengukur dan geolokasi berbagai informasi seperti tingkat CO2, lubang (melalui akselerometer), titik akses WiFi gratis, kemacetan lalu lintas, dan sebagainya. Saat kendaraan mengumpulkan informasi yang diperlukan, protokol toleransi- penundaan digunakan untuk menyampaikan informasi tersebut ke salah satu titik akses pinggir jalan. Penyebaran CarTel 27 mobil saat ini digunakan sebagai testbed.

VANET juga dapat membantu mengurangi kemacetan lalu lintas. Kemacetan jalan menghasilkan pemborosan waktu dan produktivitas yang sangat besar bagi jutaan orang. Cara yang mungkin untuk mengatasi masalah ini adalah meminta otoritas transportasi mendistribusikan informasi lalu lintas kepada pengemudi dan penumpang, yang pada gilirannya dapat memutuskan rute di sekitar area padat atau memilih platform transportasi yang sesuai. Informasi lalu lintas tersebut dapat

dikumpulkan dengan mengandalkan sensor statis yang ditempatkan di lokasi jalan tertentu (misalnya,

loop induksi, kamera video, infrastruktur bus) atau dengan memiliki satu kendaraan sendiri untuk melaporkan informasi ini. VANET dapat digunakan untuk mengumpulkan informasi ini dan

membagikannya dengan orang lain di area tersebut atau bahkan mengunggahnya ke otoritas pusat menggunakan protokol perutean DTN seperti pada referensi 81.

Dalam proyek TIME-EACM, penggunaan kendaraan yang dilengkapi dengan GPS sebagai sensor bergerak untuk memantau lalu lintas diselidiki [82,83,89]. Mereka memanfaatkan konektivitas antara kendaraan yang berjalan di daerah perkotaan untuk menyebarkan informasi lalu lintas yang dihasilkan oleh kendaraan ke gateway stasioner yang tersebar di seluruh kota. Masalah data untuk menangkal kemudian dieksplorasi bersama dengan masalah akuisisi data (memutuskan tingkat di mana kendaraan memperoleh data), dan optimasi bersama dari dua aspek pemantauan lalu lintas yang saling terkait ini diselidiki dalam referensi 89.

Terakhir, CATE [90] memungkinkan kendaraan untuk mengumpulkan informasi lalu lintas dan mengubah rute secara dinamis. Kendaraan yang dilengkapi dengan sistem komputerisasi dapat dibantu navigasinya dengan terus menilai dan mengoreksi prediksi rute terbaik ke suatu tujuan. Untuk melakukannya, setiap kendaraan harus mampu (i) merasakan informasi lalu lintas, (ii) membaginya dengan kendaraan tetangga (secara ad hoc), dan (iii) secara dinamis menghitung ulang rute terbaik ke tujuan dari posisi saat ini berdasarkan informasi yang dikumpulkan. Oleh karena itu, Sistem Navigasi (NavSys) menjadi elemen dari sistem terdistribusi yang secara kooperatif mengumpulkan dan bertukar kondisi lalu lintas dan, pada saat yang sama, penaksir lalu lintas yang canggih, berdasarkan informasi real-time.

3.7 DISEMINASI KONTEN PRIBADI

Terlepas dari pentingnya aplikasi yang terlihat sebelumnya, tautan ad hoc nirkabel sering digunakan untuk fungsi yang lebih santai—misalnya, berbagi media digital. Perangkat seperti ponsel, laptop, dan tablet dengan Bluetooth dan Wifi telah berpartisipasi dalam penyebaran MANET terbesar yang digunakan untuk penyebaran konten digital. Misalnya, mereka seringkali merupakan cara paling sederhana untuk memindahkan foto/lagu/film favorit dari ponsel seseorang ke ponsel teman. Namun, transfer ini dilakukan secara manual dan jarang menjadi bagian dari jaringan yang lebih besar atau persisten. Jika infrastruktur tidak tersedia, nirkabel jarak pendek sebenarnya bisa menjadi satu-satunya cara untuk mentransfer data. Aliansi Wifi sekarang juga telah mengembangkan WiFi Direct, yang menghadirkan lebih banyak tantangan terhadap sifat tanpa infrastruktur Bluetooth. WiFi Direct memungkinkan host normal untuk bertindak sebagai titik akses WiFi, menyederhanakan proses penemuan dan perilaku tingkat jaringan mode ad hoc WiFi, yang berpotensi menawarkan metode superior untuk berbagi melalui WiFi.

Bahkan dengan ketersediaan infrastruktur nirkabel, mungkin terlalu mahal untuk digunakan atau datanya mungkin tidak sesuai untuk jaringan. Meskipun pemikiran untuk menggunakan jaringan seluler untuk memungkinkan perangkat seluler bertindak sebagai simpul Internet lainnya menarik, ia memiliki beberapa batasan penting. Paket telepon konsumen yang mengenakan biaya untuk volume data seluler yang ditransfer seringkali sangat mahal, sedangkan penawaran biaya tetap sering membatasi penggunaan [91]. Ini berkisar dari batas volume data hingga pelarangan eksplisit lalu lintas jaringan massal dalam persyaratan layanan. Pembatasan layanan oleh Penyedia Layanan Internet (ISP) kabel komersial adalah umum dan bahkan dapat menjadi lebih penting bagi penyedia seluler, karena kendala teknologi dari jenis pekerjaan jaringan. Selain itu, penggunaan tautan nirkabel peer-to-peer langsung tidak memerlukan penggunaan pihak ketiga untuk menyediakan tautan jaringan. Ini menghilangkan kemampuan untuk memantau atau menyensor transfer antar rekan dengan mudah. Kerusuhan politik 2009 di Iran menyebabkan penangguhan jaringan seluler yang menunjukkan bagaimana ketersediaan dan kerja sama tidak selalu dapat diharapkan dari infrastruktur. Radio jarak pendek bahkan digunakan para aktivis untuk menyebarkan pesan-pesan koordinasi tanpa takut diawasi. Transfer Bluetooth juga telah digunakan dalam pemasaran untuk mendorong trailer film ke konsumen dari papan reklame jaringan. Itu bahkan telah digunakan oleh otoritas kota di London untuk mengirimkan peringatan kepada publik tentang tempat berbahaya. Namun, melakukan berbagi konten secara otomatis, cerdas, dan efisien akan diperlukan untuk mendapatkan partisipasi aktif pengguna dalam jaringan ad hoc tersebut.

Investigasi interkoneksi perangkat seluler pribadi, dan komunikasi apa yang dapat dicapai di antara mereka, telah menerima minat penelitian akademis yang signifikan, dengan bidang-bidang seperti jaringan pocket-switched (PSN) mulai dibangun.

Proyek Haggle menemukan pendekatan bersih untuk jaringan antar-perangkat, dan telah merilis implementasi untuk banyak perangkat seluler yang berbeda [92]. Haggle menggunakan pendekatan konten-sentris , di mana data dikirim melalui tautan oportunistik sesuai dengan minat terdaftar perangkat. Ada banyak minat dalam menggunakan perangkat seluler yang dibawa secara pribadi dan koneksi oportunistik di antara mereka untuk menyebarkan informasi melalui banyak lompatan. Beberapa pekerjaan telah difokuskan terutama pada penyebaran konten berpasangan di jaringan tersebut [93], menggunakan langganan eksplisit oleh node untuk mendaftarkan minat mereka pada jenis konten.

Dalam sistem terdesentralisasi seperti itu, membuat keputusan penerusan seringkali didasarkan pada informasi statistik historis. Asumsikan bahwa jika host A bertemu B berkali-kali sebelumnya, kemungkinan akan melakukannya lagi. Beberapa penelitian baru menggunakan informasi eksplisit tentang tautan sosial orang untuk memandu keputusan penerusan ini. Pengetahuan tentang komunitas, interaksi sosial dan colocation juga telah digunakan untuk meningkatkan DTN multihop [94,95].

Bluetorrent [96] adalah sistem berbagi file peer-to-peer menggunakan Bluetooth. Ini mirip dalam operasinya dengan Bittorrent, di mana file dipecah menjadi potongan-potongan kecil dan kemudian diunduh

dan dibagikan oleh klien. Tujuan mereka adalah untuk mendukung pengunduhan konten melalui beberapa sesi, sehingga menghindari masalah pemindahan host secara independen, dengan pola konektivitas yang pendek. AP digunakan untuk menyemai dan menyebarkan konten terpilih, membutuhkan pembuatan infrastruktur ini dan pengelolaan injeksi konten ke dalam sistem.

Pekerjaan itu bergantung pada cukup banyak orang yang melayani versi file yang sama untuk mendapatkan keuntungan dari kerumunan dan mencakup overhead komunikasi untuk memberi tahu rekan lain tentang kemajuan file individu.

Penawaran komersial di bidang ini sering dikaitkan dengan masalah lisensi dan pembajakan, meskipun ada keinginan pengguna potensial untuk berbagi musik dan video secara ad hoc dengan mudah. Telah muncul aplikasi streaming musik P2P nirkabel di "App Store" Apple, seperti MyStream dan Eavesdrop. Namun, penawaran ini perlu mendapatkan penetrasi pasar yang besar untuk mencapai kegunaan dari mana-mana. Salah satu penerapan perangkat distribusi konten peer-to-peer terbesar adalah pemutar musik Microsoft Zune. Pertama kali dirilis pada tahun 2003, perangkat ini mempromosikan distribusi konten berpasangan secara manual melalui tautan nirkabel, tanpa memerlukan infrastruktur apa pun. Sayangnya, interaksi ini terbatas fungsinya dan hanya berfungsi di antara dua Zune, yang membatasi fleksibilitasnya. Meskipun tanggapan komersial yang lemah terhadap Zune, kemampuan berbagi pengguna-ke-pengguna yang mudah masih merupakan nilai jual baru untuk pemutar media pribadi. Kurangnya sistem penyebaran konten skala besar tampaknya bukan disebabkan oleh keterbatasan teknis atau kurangnya minat pengguna, melainkan oleh masalah perizinan dan monetisasi sistem yang dihasilkan.

3.8 KESIMPULAN

Bab ini telah menunjukkan bahwa MANET tidak hanya merupakan pilihan yang layak untuk media komunikasi, terkadang MANET juga merupakan satu-satunya pilihan, khususnya di lingkungan khusus atau terbatas. Ketika infrastruktur langka atau aksesnya dibatasi, gagasan jaringan yang lebih konservatif seringkali diperlukan. Aplikasi yang muncul seperti jaringan sensor nirkabel, jaringan kendaraan, dan kendaraan tak berawak membuat sistem seperti itu semakin menarik bagi industri dan pengguna akhir karena ketahanan dan fiturnya yang unik.

Tingkat partisipasi dan/atau altruisme yang diperlukan untuk memfasilitasi jenis sistem ini terbukti menantang untuk dicapai di kalangan masyarakat umum. Namun, daya baterai perangkat yang meningkat pesat dan pengurangan biaya komunikasi radio akan mengurangi hambatan masuk ke realisasi tersebut. Dalam waktu dekat, kemajuan antarmuka komunikasi, pertumbuhan pesat perangkat di mana-mana, dan meningkatnya kebutuhan bandwidth pada akhirnya dapat mendorong realisasi Internet of Things, di mana setiap perangkat atau kendaraan pribadi dapat melakukan internetwork secara alami.

CHAPTER 4 KEAMANAN DALAM NIRKABEL JARINGAN AD HOC

4.1 PENDAHULUAN

Jaringan nirkabel memanfaatkan sinyal radio untuk bertukar data antara dua atau lebih perangkat fisik, juga disebut "node". Kurangnya kabel memungkinkan penggelaran jaringan ini juga di lingkungan yang tidak bersahabat atau skenario seluler. Ketika node tidak mengandalkan infrastruktur yang sudah ada sebelumnya, jaringan nirkabel mengambil nama jaringan ad hoc nirkabel. Dengan demikian, node harus berkomunikasi satu sama lain dengan membentuk jaringan radio multihop. Secara umum, beberapa kerentanan dapat diidentifikasi dalam jaringan ad hoc, dan pada tingkat yang sangat abstrak, kerentanan tersebut dapat dikaitkan dengan salah satu masalah berikut:

Kerentanan Saluran. Pesan dapat disadap dan pesan palsu dapat disuntikkan atau diputar ulang ke dalam jaringan tanpa kesulitan memiliki akses fisik ke komponen jaringan.

Kerentanan Node. Karena node jaringan mungkin tidak berada di tempat yang terlindungi secara fisik, mereka dapat lebih mudah ditangkap dan dirusak oleh penyerang. Dalam praktiknya, musuh dapat mencuri informasi sensitif dari mereka, mengubah perilakunya, atau merusak perangkat keras secara fisik untuk mengakhiri node.

Dalam kasus terakhir ini, serangan juga dapat dianggap termasuk dalam domain toleransi

kesalahan, yang merupakan kemampuan untuk mempertahankan fungsi jaringan tanpa gangguan akibat kegagalan node.

Tidak adanya Infrastruktur. Jaringan ad hoc seharusnya beroperasi secara independen dari infrastruktur tetap apa pun. Ini membuat solusi keamanan klasik berdasarkan otoritas sertifikasi dan server online tidak dapat diterapkan. Asumsi umumnya adalah bahwa node yang memiliki kunci rahasia yang valid dapat dipercaya.

Konsekuensinya, skema manajemen kunci yang aman dan efisien menjadi sangat penting.1 Selanjutnya, karena kurangnya infrastruktur, kerjasama node menjadi penting. Kami dapat mengidentifikasi dua jenis node yang tidak kooperatif: node yang salah atau berbahaya dan node yang egois. Dalam bab ini kita akan fokus pada node berbahaya. Pembaca yang tertarik dengan keegoisan dapat merujuk ke [1] untuk mendapatkan ide tentang masalah yang diperkenalkan oleh node tersebut.

Mengubah Topologi Secara Dinamis. Seringkali, topologi jaringan berubah dengan cepat.

Dengan demikian, diperlukan protokol perutean yang canggih, yang keamanannya merupakan tantangan tambahan. Memang, informasi perutean yang salah dapat dihasilkan oleh node yang dikompromikan atau sebagai akibat dari beberapa perubahan topologi.

Beberapa protokol routing telah diperkenalkan untuk jaringan ad hoc, dan beberapa versi aman dan modifikasi dari protokol ini telah diusulkan (ARIADNE [2], SAODV [3], ARAN [4], SAR [5], SRP [6], SEAD [7], dll.).

Dalam literatur, ada beberapa karya yang mensurvei protokol tersebut, di antaranya [8] dan [9].

Dalam bab ini kami tidak bermaksud mensurvei literatur yang ada tentang jaringan ad hoc, tetapi kami ingin fokus pada tantangan keamanan yang muncul dalam lima subset berbeda dari jaringan ad hoc: jaringan sensor nirkabel (WSN), jaringan sensor nirkabel tanpa pengawasan

(UWSN), jaringan mesh nirkabel (WMN), jaringan toleran tunda (DTN), dan jaringan ad hoc kendaraan (VANET). Jaringan ini berbagi banyak fitur, tetapi masing-masing menghadirkan tantangan baru yang harus ditangani secara khusus. Demi kejelasan dan kelengkapan, berikut ini kami akan memperkenalkan keamanan utama tantangan umum untuk semua jaringan ad hoc nirkabel, dan kemudian kami akan memperkenalkan fitur khas WSN, UWSN, WMN, DTN, dan VANET. Setelah itu, untuk masing-masing teknologi jaringan ini, kami akan merinci masalah keamanan yang dibahas sejauh ini dalam literatur.

4.1.1 Tantangan Keamanan di Jaringan Ad Hoc Nirkabel

Sebelum menjelaskan serangan keamanan dan penanggulangan yang tersedia untuk berbagai

jenis jaringan ad hoc, kami meninjau secara singkat persyaratan utama yang biasanya harus dipenuhi dalam jaringan ad hoc nirkabel:

Ketersediaan. Layanan yang diberikan harus tersedia tepat waktu meskipun ada masalah dalam sistem. Penting bahwa layanan yang disediakan oleh jaringan tersedia bahkan ketika diserang. Serangan penipisan sumber daya bertujuan menumbangkan properti ini.

Integritas. Informasi yang dipertukarkan antar node tidak boleh diubah, baik sengaja maupun tidak sengaja. Oleh karena itu, node berbahaya tidak boleh memodifikasi pesan yang telah dikirim oleh node yang sah.

Kerahasiaan. Informasi rahasia yang dipertukarkan dalam jaringan tidak boleh dibocorkan kepada entitas yang tidak sah. Kerahasiaan dapat dicapai dengan menggunakan beberapa teknik enkripsi sehingga hanya node yang sah yang dapat memahami isi dari sebuah paket. Dalam beberapa kasus, penting untuk menyembunyikan keberadaan komunikasi antara dua titik akhir. Otorisasi. Hanya node yang berwenang yang harus dapat memperoleh akses ke jaringan, dan hanya entitas yang berwenang yang dapat menggunakan layanan yang disediakan oleh jaringan.

Autentikasi. Harus dimungkinkan untuk memverifikasi bahwa data benar-benar dikirim oleh pengirim yang diklaim. Dengan cara ini, penyerang tidak dapat memalsukan pesan dan membuat jaringan percaya bahwa itu adalah pesan yang sah.

Non-penolakan. Pengirim tidak boleh berpura-pura bahwa dia tidak mengirimkan informasi yang sebenarnya dia kirimkan. Properti ini berharga untuk menemukan dan memisahkan node yang disusupi dalam jaringan.

Kesegaran. Data harus segar sedemikian rupa sehingga musuh tidak dapat menggunakan kembali yang lama pesan untuk menyesatkan layanan jaringan.

Ketika node dapat bergabung atau meninggalkan jaringan, kerahasiaan maju dan mundur juga penting. Kerahasiaan ke depan berarti kompromi kunci saat ini tidak boleh mengkompromikan

kunci masa depan. Kerahasiaan mundur berarti kompromi kunci saat ini tidak boleh membahayakan kunci sebelumnya. Dengan kata lain, yang pertama memastikan bahwa sebuah node tidak dapat memahami pesan yang dikirim setelah meninggalkan jaringan, sedangkan yang kedua memastikan

bahwa node baru tidak dapat memahami pesan apa pun yang dikirim sebelum bergabung dengan jaringan.

Klasifikasi pertama serangan terhadap jaringan ad hoc dapat dibuat dengan mempertimbangkan keanggotaan penyerang dalam jaringan: Kita dapat membedakan antara serangan berasal dari orang luar dan yang berasal dari orang dalam. Yang pertama adalah serangan yang dihasilkan oleh entitas yang bukan milik jaringan tetapi ingin mengganggu layanan yang disediakan, sedangkan yang terakhir terjadi ketika node yang sah berperilaku jahat. Serangan dapat diklasifikasikan lebih lanjut menjadi serangan pasif dan aktif : Sementara serangan pasif bertujuan memantau dan menganalisis perilaku jaringan tanpa mengganggunya, serangan aktif mengubah perilaku normal jaringan. Kategorisasi ketiga lebih fokus pada tujuan serangan daripada sifat penyerang atau perilakunya. Menurut klasifikasi ketiga ini, kita dapat membedakan tiga jenis serangan:

• Serangan terhadap ketersediaan jaringan dan integritas layanan. Serangan ini bertujuan untuk mengganggu layanan yang disediakan oleh jaringan. Banyak penolakan layanan, perutean, dan serangan fisik termasuk dalam kategori ini.

• Serangan terhadap privasi dan kerahasiaan. Ini adalah serangan yang mencoba untuk mendapatkan wawasan

pertukaran data dalam jaringan dan pada topologi jaringan.

• Serangan terhadap integritas data. Serangan ini mencoba mengubah data yang dikirimkan. Node berbahaya dapat menyuntikkan pesan palsu, memodifikasi yang sudah ada, mereplikasi paket lama atau seluruh node, dan seterusnya.

4.1.2 WSN, UWSN, WMN, DTN, dan VANET

Jaringan sensor nirkabel, jaringan sensor nirkabel tanpa pengawasan, jaringan mesh nirkabel, jaringan toleran tunda, dan jaringan ad hoc kendaraan berbagi banyak fitur. Namun, masing-masing teknologi jaringan tersebut memiliki ciri khas yang dirangkum dalam Tabel 4.1. Secara khusus, WSN terdiri dari kumpulan node sensor yang merasakan informasi di lapangan, bersama dengan satu atau lebih sink yang mengumpulkan data ini. Node sensor memiliki daya komputasi yang sangat terbatas dan daya yang terbatas.

Jumlah sensor di dalam WSN bisa beberapa kali lipat lebih besar daripada di jaringan sensor ad hoc lainnya. Unattended WSNs (UWSNs) dicirikan oleh keberadaan wastafel yang terputus-putus. Oleh karena itu, sensor mungkin tidak dapat segera mengirimkan data yang dikumpulkan ke sink, dan oleh karena itu muncul banyak masalah keamanan baru. Jaringan mesh nirkabel malah dicirikan oleh tujuannya: interaksi berbagai jenis jaringan.

Mereka harus memberikan tingkat keamanan tertentu meskipun harus berurusan dengan banyak teknologi pada saat yang sama. Jaringan toleran tunda, aktif di sisi lain, dicirikan oleh kontak oportunistik dan konektivitas intermiten dari node mereka.

Akhirnya, VANET adalah jaringan ad hoc seluler yang dirancang untuk memiliki kendaraan sebagai node seluler.

Pada bagian berikut kami akan memperkenalkan fitur-fitur utama dari jaringan ini, dan kami akan menyoroti tantangan keamanan mereka yang khas dan penanggulangan yang sesuai. Kami awalnya akan fokus pada WSN. Memang, karena kendala sumber daya yang parah dan akses fisik yang mudah

ke perangkat di lapangan, WSN dapat dianggap sebagai salah satu skenario yang paling menantang. Kami akan menganalisis secara detail masalah

yang muncul dalam pengaturan ini, dan kemudian kami akan beralih ke UWSN, WMN, DTN, dan VANET.

Pembaca harus mencatat bahwa banyak masalah yang akan kita diskusikan untuk WSN juga dapat diterapkan di jaringan ad hoc lainnya. Namun, alih-alih mensurvei literatur keamanan jaringan ad hoc, kami memutuskan untuk mengadopsi pendekatan holistik: Kami memperkenalkan masalah khusus dalam skenario khusus seperti WSN, UWSN, dan seterusnya.

Jaringan	Ciri khas
WSN	Jumlah node sangat tinggi, daya komputasi terbatas
UWSN	Wastafel berselang
WMN	
DTN	Integrasi banyak jaringan

4.2 JARINGAN SENSOR NIRKABEL

Sebuah jaringan sensor nirkabel (WSN) terdiri dari kumpulan besar node, bahkan beberapa magnitudo lebih besar daripada jaringan sensor lainnya. Node milik WSN sering disebut "motes." Mereka memiliki daya komputasi yang terbatas, memori yang terbatas, dan daya yang terbatas. Pengisian ulang biasanya tidak dianggap layak; dan bahkan jika banyak metode pemberian daya telah diusulkan, mote masih dianggap sebagai perangkat "sekali pakai". Mereka ditempatkan di area geografis yang luas, dan mengatur diri sendiri ke dalam jaringan ad hoc. Kegagalan adalah hal biasa, karena sumber dayanya yang terbatas dan bidang yang kedap air tempat mereka digunakan, dan memaksimalkan masa pakai dan produktivitas adalah hal yang sangat penting. WSN pada dasarnya adalah jaringan ad hoc dengan batasan tambahan dan lebih ketat. Mereka harus lebih hemat energi dan dapat diskalakan daripada jaringan ad hoc lainnya, yang memperburuk tantangan keamanan.

Saat ini, WSN menjadi sistem yang meresap, dan mereka menemukan aplikasi di beberapa bidang, mulai dari otomatisasi rumah hingga pemantauan perbatasan. Mungkin, dua aplikasi WSN yang paling berorientasi pada keamanan adalah solusi militer dan medis. Dalam kasus pertama, informasi sensitif harus dilindungi dari penyerang yang kuat, tetapi pada saat yang sama harus jelas dan dapat dimengerti oleh teman. Dalam kasus kedua, data tentang pasien harus dirahasiakan, dan protokol keamanan yang kuat harus disediakan.

Saat mendesain WSN, keamanan harus mencakup semua lapisan sistem. Desainer harus memperhitungkan serangan ke lapisan aplikasi serta lapisan fisik (yang sering dianggap aman dalam pengaturan konvensional). Selain itu, serupa dengan jaringan konvensional, sebagian besar aplikasi WSN menawarkan keamanan terhadap injeksi pesan, penyadapan, penyamaran, dan sebagainya. Namun, terutama karena sumber dayanya yang terbatas, teknik standar seperti perangkat keras anti rusak, perutean aman, kriptografi kunci publik, dan seterusnya, tidak sesuai dengan WSN. Oleh karena itu, solusi untuk WSN harus dirancang khusus dengan mempertimbangkan perangkat kelas bawah ini.

Ada dua spesifikasi yang tersedia untuk komunikasi WSN: IEEE 802.15.4 [11] dan ZigBee [12]. Yang pertama adalah standar untuk area pribadi nirkabel dengan tarif rendah jaringan yang dikembangkan oleh IEEE (Institute of Electrical and Electronics Engineers)

dan berisi sejumlah suite keamanan. Pada dasarnya, ini memberikan kontrol akses, integritas, kerahasiaan, dan perlindungan pemutaran ulang; namun, itu tidak berurusan dengan autentikasi atau pertukaran kunci. IEEE 802.15.4 mendefinisikan lapisan komunikasi pada level 2 dalam model OSI (Open System Interconnection), dan tujuan utamanya adalah untuk memungkinkan komunikasi antara dua perangkat. Namun dalam praktiknya, jaringan dapat memiliki lebih banyak topologi. ZigBee dibangun di atas IEEE 802.15.4. Standar ini mendefinisikan lapisan komunikasi pada level 3 ke atas dalam model OSI. Tujuan utamanya adalah untuk (a) membuat topologi jaringan (hierarki) untuk memungkinkan sejumlah perangkat berkomunikasi di antara mereka dan (b) menambahkan fitur komunikasi tambahan

seperti autentikasi, enkripsi, dan asosiasi. Lapisan jaringan ZigBee secara alami mendukung jaringan bintang, pohon, dan mesh umum.

Pada bagian berikut kami akan memberikan kategorisasi serangan yang dapat dipasang terhadap WSN. Kami akan menjelaskan secara rinci beberapa ancaman, dan kami akan menunjukkan tindakan pencegahan yang ada. Tabel 4.2 meringkas serangan yang akan kami pertimbangkan, kategorisasinya menurut klasifikasi yang disediakan di Bagian 4.1.1, dan penanggulangan yang sesuai.

4.2.1 Serangan Terhadap Ketersediaan Jaringan dan Integritas Layanan

Serangan terhadap ketersediaan jaringan dan integritas layanan sering disebut sebagai serangan denial-of-service (DoS): Musuh mencoba mengganggu, menumbangkan, atau menghancurkan layanan yang disediakan oleh jaringan. Serangan DoS dapat menargetkan setiap lapisan jaringan sensor. Memang, ada serangan yang dilakukan pada lapisan fisik, serta serangan pada data link, jaringan, dan lapisan transport. Pada bagian ini kita akan menganalisis serangan DoS yang ada lapis demi lapis.

4.2.1.1 Gangguan Lapisan

Fisik . Jammer adalah perangkat yang sebagian atau seluruhnya dapat mengganggu komunikasi suatu node dengan mengganggu frekuensi radio yang digunakan node tersebut. Bergantung pada daya transmisinya, jammer dapat menghancurkan seluruh jaringan atau sebagian kecilnya. Jika diabaikan dalam desain WSN awal, serangan jamming dapat dengan mudah mengganggu jaringan, meskipun menggunakan mekanisme keamanan tingkat tinggi. Jamming dapat dianggap sebagai kebisingan yang dibuat oleh penyerang dengan tujuan mengganggu sinyal yang sah. Memang, aktivitas gangguan hanya efektif jika rasio signal-to- noise kurang dari 1. Ada berbagai jenis gangguan [13]:

Spot Jamming. Ini adalah teknik jamming yang paling sederhana. Penyerang mengarahkan semua kekuatan kompromінya ke satu frekuensi. Biasanya efektif, tetapi dapat dihindari dengan mengubah frekuensi yang digunakan.

Sapu Jamming. Penyerang dengan cepat menggeser frekuensi target sedemikian rupa untuk mengganggu beberapa frekuensi secara berurutan. Karena aktivitas penyerang tidak terus menerus, efektivitas serangan jenis ini terbatas. Namun, dalam WSN dapat menyebabkan banyak transmisi ulang karena hilangnya paket.

Table 4.2 Attacks Against Wireless Sensor Networks

Target	Layer	Attack	Countermeasures	Attacker		Attack	
				Internal	External	Active	Passive
Network Availability and Service Integrity	Physical	Jamming	Detection techniques, proactive, reactive, and mobile agent-based countermeasures		×	×	
		Tampering	Tamper-proofing, software tamper detection, sensor monitoring		×	×	
	Link	Collision	Forward error-correcting codes		×	×	
		Exhaustion	Rate limitation		×	×	
		Unfairness	Error-correcting codes	×		×	
		Sleep Deprivation	Anti-replay protection, strong link-layer authentication, and broadcast attack protection		×	×	
	Network & Routing	Routing information	Authentication, MAC	×		×	
		Hello flooding	Authentication, bi-directionality checking, signal strength		×	×	
		Black hole	Authentication, REWARD, watchdog and pathrater		×	×	
		Sink hole attack	Authentication, monitoring, secure routing		×	×	
		Selective forwarding	Authentication, IDS, multi-hop acknowledgments, multipath routing		×	×	
		Wormhole attack	Authentication, packet leashes		×	×	
		Sybil	Authentication, radio resource testing, key validation for random key pre-distribution, position verification		×	×	
	Transport	Flooding	Client puzzles, cryptographic techniques	×		×	
		Desynchronization	Authentication		×	×	
Privacy and Secrecy	Physical	Eavesdropping	Cryptographic techniques		×		×
	Network	Traffic analysis	Randomized communications	×		×	
Data Integrity	Physical	Node replication	Emergent properties		×	×	
	Network	Packet injection	Data authentication	×	×	×	
		Packet duplication	Data authentication	×	×	×	
		Packet alteration	Data authentication	×	×	×	

Kemacetan Bertubi-tubi. Dalam jenis kemacetan ini, musuh macet pada saat yang sama pada rentang frekuensi. Namun, seiring bertambahnya jangkauan serangan, daya output gangguan berkurang secara proporsional.

Kemacetan yang Menipu. Penyerang memalsukan atau memutar ulang sinyal yang valid pada saluran tanpa henti, sehingga menempati bandwidth yang tersedia dan mencoba

menghancurkan layanan jaringan. Ini dapat diterapkan pada satu frekuensi atau satu set frekuensi.

Beberapa penanggulangan dapat digunakan terhadap berbagai serangan jamming. Fre quency-hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), hybrid FHSS/DSSS, teknologi ultrawide band (UWB), polarisasi antena, transmisi terarah, dan pengaturan daya transmisi adalah beberapa contohnya [14– 16]. Node sensor generasi sebelumnya menggunakan radio frekuensi tunggal, dan karena itu rentan terhadap derau pita sempit, baik yang tidak disengaja atau berbahaya. Misalnya, transceiver Chipcon CC1000 pada Mica2 dan motes sebelumnya beroperasi pada 433 atau 900 MHz. Motes yang lebih baru, seperti mote MICAz dan Telos, menggunakan Chipcon CC2420, yang beroperasi pada 2,45 GHz dan menggunakan spektrum penyebaran urutan langsung untuk mengurangi kerentanan terhadap noise. Penggunaan spektrum sebar ini mengurangi dampak derau pita sempit pada komunikasi, seperti yang berasal dari oven microwave dan jaringan nirkabel lainnya. Namun, mereka tidak mengalahkan musuh dengan pengetahuan tentang kode penyebaran atau urutan lompatan. Memang, ini bukan rahasia: Ini adalah standar (dalam IEEE 802.15.4) atau berasal dari alamat node (dalam Bluetooth).

Skema keamanan yang ada yang menangani serangan gangguan di WSN dapat diklasifikasikan dalam: teknik deteksi, penanggulangan proaktif, penanggulangan reaktif, dan penanggulangan berbasis agen seluler. Teknik deteksi bertujuan untuk mendeteksi serangan gangguan secara instan. Sebagai contoh, Xu et al. [17] mengeksplorasi berbagai teknik untuk mendeteksi serangan gangguan di WSN. Pengamatan utama adalah bahwa kekuatan sinyal, waktu penginderaan pembawa atau rasio pengiriman paket secara individual tidak dapat secara meyakinkan mendeteksi keberadaan jammer. Oleh karena itu, untuk meningkatkan pendeteksian, penulis memperkenalkan pengertian pengecekan konsistensi, dimana rasio pengiriman paket digunakan untuk mengklasifikasikan sebuah link radio memiliki utilitas yang buruk, dan kemudian pemeriksaan konsistensi dilakukan untuk mengklasifikasikan apakah kualitas link yang buruk disebabkan oleh jamming. Penanggulangan proaktif membuat WSN kebal terhadap serangan gangguan daripada secara reaktif menanggapi insiden semacam it Contohnya adalah DEEJAM, sebuah protokol yang diusulkan untuk bertahan melawan jammer

tersembunyi menggunakan perangkat keras berbasis IEEE 802.15.4 [18]. Ini menggunakan empat mekanisme pertahanan bersama-sama untuk mengalahkan atau mengurangi efektivitas jamming oleh musuh yang menggunakan perangkat keras dengan kemampuan yang sama dengan node yang dikerahkan: frame masking, channel hop ping, fragmentasi paket, dan pengkodean berlebihan.

Setiap mekanisme pertahanan mengatasi serangan gangguan yang berbeda. Secara khusus, frame masking bertahan dari serangan di mana jammer mentransmisikan hanya ketika radionya menangkap pembukaan multibyte dan memulai urutan frame delimiter (SFD). Channel hopping bertahan melawan penyerang yang mencoba mendeteksi aktivitas radio dengan mengambil sampel indikator kekuatan sinyal radio (RSSI) secara berkala dan yang memulai serangannya saat RSSI berada di atas ambang batas yang dapat diprogram. Fragmentasi paket adalah penanggulangan yang tepat terhadap penyerang yang mengambil sampel setiap saluran sesingkat mungkin untuk menentukan apakah aktivitas hadir. Jamming segera dimulai ketika dia menemukan aktivitas radio.

Fragmentasi paket memungkinkan pemecahan paket yang ditransmisikan menjadi fragmen yang ditransmisikan secara terpisah pada saluran yang berbeda dan dengan SFD yang berbeda. Ketika fragmen cukup pendek, penyerang tidak memiliki waktu untuk memulai serangannya sebelum pengirim menyelesaikan transmisinya dan melompat ke saluran lain. Encoding redundan diusulkan sebagai penanggulangan terhadap penyerang yang membabi buta macet satu saluran menggunakan pulsa pendek. Bahkan jika sebuah fragmen rusak, penerima dapat memulihkan paket tersebut. Namun, ada peningkatan biaya dalam penggunaan energi dan bandwidth. Penanggulangan reaktif memungkinkan reaksi hanya setelah insiden serangan jamming. Algoritme JAM yang diusulkan dalam referensi 19 termasuk dalam kategori ini. Ini memungkinkan deteksi dan pemetaan wilayah yang macet untuk meningkatkan efisiensi jaringan.

Dalam praktiknya, node di dekat perbatasan wilayah yang macet memberi tahu tetangga di luar wilayah yang macet. Tetangga mulai memetakan wilayah yang sedang macet dengan bertukar pesan pemetaan. Saat jammer bergerak atau hanya menghentikan serangan, node yang macet pulih dan mengirim pemberitahuan ke tetangganya untuk memberi tahu mereka

tentang perubahan ini. Di dalam kelas penanggulangan berbasis agen seluler kami menemukan pendekatan yang memungkinkan agen seluler (MA) untuk meningkatkan kemampuan bertahan WSN.

Istilah MA mengacu pada program otonom yang dapat berpindah dari host ke host dan bertindak atas nama pengguna menuju penyelesaian tugas yang diberikan. JAID adalah protokol yang termasuk dalam kategori ini [20]. Tujuannya adalah untuk (a) menghitung rute yang hampir optimal untuk MA yang

secara bertahap memadukan data saat mereka mengunjungi node dan (b) memodifikasi rencana perjalanan MA untuk menghindari area yang macet sementara tidak merusak penyebaran data yang efisien dari sensor bekerja. Tujuan pertama dipenuhi melalui desain algoritma baru yang memisahkan jaringan sensor menjadi beberapa kelompok node, menghitung rute yang hampir optimal melalui node masing-masing kelompok dan menugaskan rencana perjalanan ini ke objek agen individu. Tujuan kedua dicapai dengan menggunakan algoritma JAM. Rangkuman komprehensif dari karya lain untuk mengatasi solusi kemacetan di WSN dapat ditemukan di referensi 13.

Merusak. Ini adalah serangan aktif yang umumnya dilakukan oleh orang luar. Penyerang mendapatkan akses fisik ke node dan mencoba untuk mengkompromikan kerahasiaan komunikasi dengan mencuri data yang disimpan dalam memori. Teknik yang diperkenalkan dalam referensi 21–23 hanyalah beberapa contoh kemungkinan serangan yang dapat dilakukan musuh. Musuh juga dapat mencuri kunci kriptografi yang digunakan untuk mengautentikasi transmisi. Selain itu, ia dapat memodifikasi perilaku node, menggantikannya dengan sensor jahat di bawah kendali penyerang. Pertahanan utama terhadap perusakan fisik berfokus pada membangun sensor tahan perusakan [24]. Keberhasilan pertahanan terutama bergantung

pada tiga hal: (1) seberapa akurat dan lengkap perancang mempertimbangkan potensi ancaman pada waktu perancangan; (2) sumber daya yang tersedia untuk desain, konstruksi, dan pengujian; dan (3) kepintaran dan keteguhan at tacker. Meskipun perangkat keras tahan kerusakan menjadi lebih murah, dalam banyak kasus ini bukanlah pilihan yang tepat.

Mekanisme pertahanan lain yang mungkin terkait dengan penggunaan perangkat lunak khusus yang mampu mendeteksi upaya perusakan. Ketika kemungkinan serangan terdeteksi, data sensitif seperti kunci kriptografi dihapus, dan protokol penghentian diri dijalankan. Merusak perangkat keras node sensor saat ini telah diselidiki

referensi 25, memberikan perhatian khusus pada serangan yang dapat dilakukan langsung di area penempatan. Serangan semacam ini dapat dilakukan tanpa mengganggu operasi node biasa. Para penulis menunjukkan bahwa serangan yang paling serius, yang menghasilkan kontrol penuh atas sebuah node sensor, membutuhkan absennya node dari jaringan untuk waktu yang cukup lama. Oleh karena itu, memantau node sensor untuk periode tidak aktif yang lama dapat dianggap sebagai strategi pertahanan yang baik.

4.2.1.2 Lapisan Tautan.

Dalam WSN, sebagian besar konsumsi energi disebabkan oleh komunikasi. Untuk alasan ini, serangan DoS yang paling efektif menargetkan transceiver dan lapisan data-link. Tabrakan lapisan tautan, kelelahan lapisan tautan, dan ketidakadilan adalah tiga serangan tersebut.

Tabrakan Lapisan Tautan. Serangan ini sangat mirip dengan jamming di physical layer. Itu terjadi ketika penyerang mengirim sinyal pada waktu dan frekuensi yang sama dari transmisi pesan yang sah hanya untuk satu oktet (atau byte) untuk merusak seluruh pesan [26]. Dalam prakteknya, penyerang menggunakan radionya untuk mendengarkan frekuensi yang digunakan oleh WSN. Penyerang mulai mengirimkan sinyalnya segera setelah dia mendengar dimulainya pesan yang sah. Tidak mudah mendeteksi serangan ini karena satu-satunya bukti adalah penerimaan pesan yang salah. Memang, ketika bingkai lapisan tautan gagal dalam pemeriksaan kode redundansi siklik (CRC), lapisan tautan secara otomatis membuang seluruh paket, sehingga membuang energi dan bandwidth. Sebagai penanggulangan, dimungkinkan untuk menggunakan kode koreksi kesalahan maju (FEC) untuk memulihkan informasi yang hilang [27].

Kelelahan Lapisan Tautan. Serangan ini terjadi ketika penyerang memanipulasi langkah-langkah efisiensi protokol dan menyebabkan node mengeluarkan energi tambahan. Memberikan batasan kecepatan dengan mengizinkan node untuk mengabaikan permintaan jaringan yang berlebihan dari sebuah node merupakan penanggulangan yang efektif terhadap serangan ini.

Ketidakadilan. Dalam serangan yang tidak adil, musuh mentransmisikan sejumlah besar paket ketika medianya bebas, sehingga mencegah sensor yang sah untuk mentransmisikan paket mereka. Dengan cara ini, penyerang dapat menurunkan kualitas layanan, sehingga melewatkan tenggat waktu waktu nyata. Namun, serangan ini tidak sepenuhnya menghalangi akses ke layanan. Biasanya, ini dianggap sebagai bentuk serangan DoS yang lemah yang dapat dibatasi dengan menggunakan bingkai yang lebih kecil, sedemikian rupa sehingga saluran hanya ditangkap untuk waktu yang singkat.

Penyiksaan Kurang Tidur. Dalam WSN, mekanisme tidur digunakan oleh node untuk menyesuaikan mode operasinya dan memperpanjang umur jaringan sedemikian rupa. Dengan daya penuh, sebuah sensor hanya dapat bekerja selama dua minggu sebelum menghabiskan sumber dayanya.

Oleh karena itu, sebaiknya node tetap dalam mode tidur dan menjadi aktif sesedikit mungkin (biasanya sekitar 1% dari waktu). Serangan penyiksaan kurang tidur bertujuan untuk mencegah sensor dari tidur. Istilah serangan "penyiksaan kurang tidur" pertama kali digunakan dalam referensi 28, di mana masalah

keamanan utama yang muncul dalam jaringan nirkabel perangkat seluler ad hoc diperhitungkan. Dalam beberapa kasus, serangan ini disebut juga serangan “denial-of-sleep”. Penolakan tidur utama

serangan dapat diklasifikasikan menjadi tiga kategori [29]: serangan daya permintaan layanan, serangan daya jinak, dan serangan daya ganas. Serangan daya permintaan layanan mengulangi permintaan layanan yang valid dengan maksud yang disengaja untuk menguras daya; serangan be nign service memulai operasi intensif daya pada perangkat yang diserang untuk menguras sumber daya daya dengan cepat; dan serangan kekuatan ganas menembus perangkat yang diserang dan mengubah program yang ada untuk mengonsumsi lebih banyak daya daripada yang dibutuhkan. Sebagai cara untuk mengurangi efek serangan ini, autentikasi lapisan tautan yang kuat , perlindungan anti-replay, dan perlindungan serangan siaran diusulkan dalam referensi 30. Secara khusus, penulis mengklaim bahwa autentikasi lapisan tautan yang kuat adalah yang pertama dan paling penting komponen pertahanan denial-of- sleep. Umur jaringan dapat dikurangi dari satu tahun atau lebih menjadi kurang dari seminggu ketika penyerang dapat mengirim lalu lintas lapisan MAC yang tepercaya. Opsi yang ada untuk menerapkan autentikasi lapisan tautan di WSN termasuk TinySec, yang dimasukkan ke dalam rilis TinyOS saat ini, dan algoritme autentikasi yang dibangun ke dalam perangkat yang sesuai dengan IEEE 802.15.4. Perlindungan anti-replay biasanya dicapai dengan memelihara tabel

tetangga dari nomor urut paket. Sayangnya, persyaratan ini bisa menjadi berat bahkan dalam jaringan berukur Salah satu cara untuk membatasi ukuran tabel tetangga adalah dengan menggunakan

tetangga lapisan jaringan untuk membatasi jumlah tetangga yang harus dilacak dari mana lalu lintas yang sah diharapkan. Penulis referensi 31 menyarankan untuk menggunakan protokol yang disebut CARP yang membatasi ukuran tabel tetangga sesuai dengan derajat node maksimum dan jumlah cluster yang telah dikonfigurasi sebelumnya. Perlindungan serangan siaran didasarkan pada prinsip sederhana: Melacak rasio lalu lintas yang sah dan berbahaya, bersama dengan persentase waktu perangkat dapat tidur, cukup untuk mengidentifikasi serangan siaran denial-of-sleep.

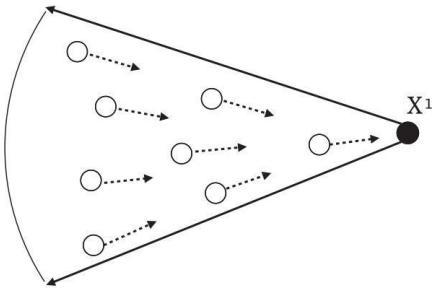
4.2.1.3 Lapisan Jaringan dan Perutean.

Pada lapisan jaringan, banyak serangan yang dapat mengganggu ketersediaan jaringan: hello flooding, black hole attack, sink hole attack, selective forwarding, dan wormhole attack adalah yang utama. Berikut ini kami akan uraikan satu per satu serangan-serangan tersebut dan penanggulangannya secara spesifik. Namun, perlu diperhatikan bahwa keamanan pada lapisan jaringan sangat bergantung pada autentikasi.

Di WSN, penggunaan kunci publik untuk otentikasi pesan biasanya dianggap tidak terjangkau. Zhang dan Subramanian [32] menyoroti bahwa kunci simetris dan fungsi hash efektif; tetapi ketika node sensor dikompromikan, kuncinya diketahui oleh musuh. Oleh karena itu, mereka mengusulkan pendekatan otentikasi pesan yang mengadopsi teknik berbasis polinomial yang terganggu untuk secara bersamaan mencapai tujuan ringan dan ketahanan terhadap sejumlah besar kompromi node, otentikasi langsung, skalabilitas, dan non-penolakan.

Serangan Langsung pada Informasi Routing. Informasi perutean adalah data paling sensitif yang dipertukarkan dalam protokol perutean. Dengan menumbangkan informasi ini, musuh akan dapat mengubah perutean normal sesuai keinginannya. Serangan langsung terhadap lapisan perutean dapat mencoba menipu, mengubah, atau memutar ulang informasi perutean.

Tindakan balasan yang efektif terhadap dua masalah pertama adalah dengan menggunakan kode otentikasi pesan (MAC). Penerima dapat memverifikasi apakah pesan telah dipalsukan atau diubah



Gambar 4.1 Halo Banjir.

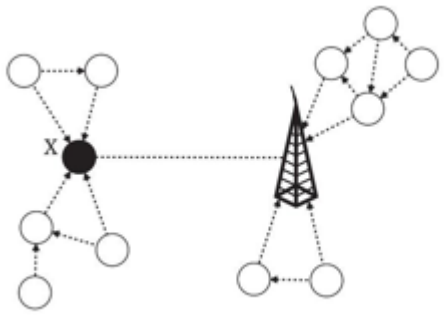
dengan memeriksa MAC. Penghitung atau stempel waktu dapat digunakan untuk bertahan melawan informasi yang diputar ulang [33].

Salam Banjir. Pesan halo sering digunakan untuk menemukan node tetangga dan secara otomatis membuat jaringan. Banyak protokol yang menggunakan mekanisme ini membuat asumsi naif bahwa pengirim berada dalam jangkauan radio. Namun, musuh dengan pemancar berkekuatan tinggi dapat mengirim pesan ini ke area node yang luas. Ketika menerima paket seperti itu, node akan percaya bahwa node berbahaya adalah tetangga dan akan menjawab dengan mengirimkan data ke sana, tetapi karena jaraknya jauh, paket akan dikirim terlupakan [34]. Sedemikian rupa, sensor dapat segera kehabisan energi. Selain itu, musuh dapat menumbangkan protokol perutean normal dan mencoba mengontrol aliran data di WSN, sehingga mengarah ke serangan lubang hitam atau sejenisnya. Gambar 4.1 mengilustrasikan serangan semacam itu. Umumnya, penanggulangan sederhana untuk serangan hello flooding adalah dengan memeriksa bidirectionality dari setiap link transmisi. Dalam referensi 35

metode berdasarkan kekuatan sinyal telah diusulkan untuk mendeteksi dan mencegah serangan hello flooding.

Serangan Lubang Hitam dan Tenggelam. Serangan lubang hitam bekerja dengan membuat simpul yang dikompromikan terlihat sangat menarik bagi simpul di sekitarnya sehubungan dengan algoritma perutean. Node kemudian akan merutekan semua lalu lintas melalui node yang dikompromikan, dan musuh akan dapat menjatuhkan semua paket yang dialihkan. REWARD [36] adalah algoritma perutean yang melawan serangan ini, juga saat musuh mengontrol tim node berbahaya. Serangan lubang hitam juga dapat dideteksi dengan mendengarkan dan memantau misi trans oleh tetangga. Dalam referensi 37, dua teknik yang mengurangi efek kesalahan perutean diusulkan: pengawas dan pembuat jalan. Yang pertama digunakan untuk mengidentifikasi node yang nakal, sedangkan yang kedua membantu perutean untuk menghindari node tersebut.

Serangan lubang hitam bisa menjadi lebih berbahaya ketika penyerang mengetahui posisi tenggelamnya. Gambar 4.2 menggambarkan serangan semacam itu. Musuh (yaitu, simpul hitam) mencoba menjadi simpul yang digunakan oleh semua simpul lain untuk mencapai wastafel. Dalam hal ini serangannya disebut sink hole attack. Pendekatan sederhana namun sayangnya mahal untuk mendeteksi lubang pembuangan telah diperkenalkan di referensi 38. Pada fase pertama, algoritme menemukan daftar node yang dicurigai. Kemudian, itu mengidentifikasi penyusup dalam daftar melalui grafik aliran jaringan. Tingginya biaya tergantung pada fakta bahwa sink membanjiri jaringan dengan tepat

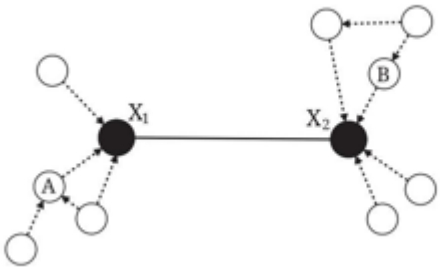


Gambar 4.2 Serangan lubang tenggelam.

pesan permintaan yang berisi ID dari node yang terpengaruh, dan kemudian node ini harus menjawab dengan informasi spesifik mengenai jalur yang benar. Penulis mengusulkan untuk meningkatkan enkripsi dan redundansi jalur untuk menghindari perubahan paket selama transmisi. Dalam referensi 39 dan 40, dua protokol routing lain terhadap serangan sink hole telah diusulkan. Namun, mereka masing-masing didasarkan pada Ad hoc On- demand Distance Vector Protocol (AODV) dan Protokol Dynamic Source Routing (DSR), yang merupakan protokol yang dibuat untuk, dan biasanya digunakan dalam, jaringan ad hoc. Dalam referensi 41, sistem deteksi intrusi yang mendeteksi serangan lubang pembuangan dan yang dapat digunakan dengan protokol perutean yang paling banyak digunakan dalam penyebaran jaringan sensor (MintRoute) diusulkan.

Serangan Lubang Cacing. Untuk menjalankan serangan wormhole, musuh perlu mengontrol setidaknya dua node yang disusupi di dua lokasi jaringan yang berbeda. Gambar 4.3 menunjukkan serangan ini. Dengan memanfaatkan koneksi yang cepat dan kuat (seringkali kabel), dua node yang disusupi (simpul hitam pada gambar) akan membuat jaringan berpikir bahwa mereka mengetahui jalur tercepat untuk mencapai sisi lain jaringan. Dalam praktiknya, musuh merekam paket (atau bit) di satu lokasi di jaringan, menyalurkannya ke lokasi lain, dan mentransmisikannya kembali ke jaringan. Sebagian besar protokol perutean

jaringan ad hoc yang ada, tanpa beberapa mekanisme untuk mempertahankan diri dari serangan ini,



Gambar 4.3 Serangan lubang cacing.

akan sangat terganggu oleh serangan sederhana ini. Sebuah mekanisme umum yang didasarkan pada pengikat paket untuk mendeteksi dan melawan serangan wormhole telah diperkenalkan di referensi 42. Pengikat adalah setiap informasi yang ditambahkan ke sebuah paket untuk membatasi jarak transmisi maksimum yang diperbolehkan dari paket itu sendiri. Dua jenis kalung anjing diusulkan: geografis dan temporal. Yang pertama memastikan bahwa penerima paket berada dalam jarak tertentu dari pengirim, sementara yang kedua memastikan bahwa paket tersebut memiliki batas atas pada masa pakainya, yang membatasi jarak perjalanan maksimum.

Penerusan Selektif. Ketika node jahat tidak mengikuti protokol perutean dan mulai menjatuhkan paket, kami menghadapi serangan penerusan selektif. Node jahat dapat bertindak sebagai filter yang meneruskan pesan tertentu dan menjatuhkan yang lain [34]. Serangan lubang hitam dapat dilihat sebagai bentuk khusus dari serangan ini, di mana semua paket dijatuhkan.

Sebagai penanggulangan, dalam referensi 43 skema deteksi intrusi terpusat berdasarkan Support Vector Machines

(SVMs) dan jendela geser diusulkan. Deteksi dilakukan di stasiun pangkalan dan karenanya sensor tidak mengeluarkan energi untuk mendukung fitur keamanan tambahan ini. Sebuah skema di mana deteksi terjadi baik di stasiun pangkalan dan node sumber disajikan dalam referensi 44. Ini menggunakan pengakuan multihop dari

node perantara untuk meningkatkan alarm di jaringan. Penanggulangan lain untuk melawan penerusan selektif adalah multipath routing [34,45]. Paket yang sama dikirim menggunakan beberapa jalur, sedemikian rupa untuk meningkatkan kemungkinan mencapai tujuannya.

Sybil. Serangan Sybil dilakukan ketika node jahat mengklaim banyak identitas.

Ini pertama kali diperkenalkan di jaringan peer-to-peer [46], tapi kemudian Karlof dan Wagner menyoroti ancaman juga di WSNs [34]. Skema toleransi kesalahan, perutean, dan algoritme penyimpanan terdistribusi dapat dengan mudah terpengaruh oleh serangan semacam itu. Taksonomi dari berbagai jenis serangan Sybil di jaringan sensor nirkabel disajikan dalam referensi 47. Penulis juga mengusulkan beberapa pertahanan, termasuk pengujian sumber daya radio, validasi kunci untuk pra-distribusi kunci acak, dan verifikasi posisi.

• Pengujian sumber daya radio adalah pemeriksaan keamanan probabilistik yang dijalankan dengan bertanya

semua node untuk mengirimkan pada waktu yang sama di saluran yang berbeda.

• Validasi kunci untuk pra-distribusi kunci acak adalah teknik yang secara langsung atau tidak langsung memeriksa kumpulan kunci yang biasanya didistribusikan sebelumnya ke sensor. Ini didasarkan pada dua gagasan utama: (1) menghubungkan identitas simpul dengan kunci yang ditetapkan ke simpul; (2) validasi kunci, yaitu, jaringan dapat memverifikasi sebagian atau seluruh kunci yang diklaim dimiliki oleh suatu identitas.

• Serangan Sybil juga dapat dikalahkan dengan memverifikasi posisi node. Node Sybil akan muncul persis di posisi yang sama. Namun, masih menjadi masalah terbuka bagaimana memverifikasi posisi tepat node dengan aman.

Skema tanda tangan ambang batas juga dapat digunakan sebagai penanggulangan. Kunci parsial ditetapkan untuk setiap sensor, dan jumlah ambang tanda tangan parsial diperlukan untuk itu menghasilkan tanda tangan lengkap. Sebuah sensor saja paling baik dapat menghasilkan tanda tangan sebagian, tetapi tidak sepenuhnya.

4.2.1.4 Lapisan Transportasi.

Beberapa protokol lapisan transport telah secara eksplisit dirancang untuk WSN: Fusion [48], CODA [49], CCF [50], Siphon [51], ARC [52], Trickle [53], STCP [54], ESRT [55], GARUDA [56], PSFQ [57], DTC [58], dan RBC [59] adalah di antaranya. Di luar cakupan bab ini untuk menyajikan deskripsi terperinci dari semua protokol yang ada. Pembaca yang tertarik dapat merujuk ke referensi terkait atau referensi 60 dan 61 untuk survei ini dan protokol lapisan transport lainnya untuk WSN.

Semua protokol yang dikutip sebelumnya dapat diklasifikasikan menjadi protokol yang menyediakan mekanisme kontrol kemacetan dan protokol yang menyediakan keandalan [60] transfer data.

Beberapa dari protokol ini menjamin keandalan paket (setiap kehilangan paket terdeteksi dan paket yang hilang ditransmisikan ulang hingga mencapai tujuannya) dan yang lain memberikan keandalan acara (yaitu, deteksi peristiwa yang berhasil, bukan transmisi yang berhasil dari setiap paket). Sayangnya, kebanyakan dari mereka memastikan komunikasi yang andal dan konsumsi energi yang rendah hanya di lingkungan yang ramah. Memang, mereka gagal memberikan keandalan end-to-end dan tunduk pada peningkatan konsumsi energi di hadapan musuh yang dapat memutar ulang atau memalsukan paket kontrol protokol.

Ketika musuh mampu menghapus kontrol dan paket data (misalnya, dengan jamming), secara teori tidak mungkin untuk memastikan komunikasi yang handal [62]. Oleh karena itu, ketika mengevaluasi protokol lapisan transport, model musuh dianggap hanya dapat memutar ulang dan menyuntikkan paket kontrol. Serangan terhadap lapisan ini dikatakan berhasil jika kehilangan paket tetap tidak terdeteksi atau penyerang dapat menolak pengiriman paket secara permanen. Protokol lapisan transport yang andal hanya dapat mendeteksi kehilangan paket jika ada semacam umpan balik dalam sistem. Biasanya, dua jenis ucapan terima kasih digunakan: ACK dan NACK . ACK bisa eksplisit (node yang menerima paket mengirimkan kembali konfirmasi eksplisit) atau implisit (jika sebuah node sengaja mendengar bahwa tetangganya adalah untuk menangkal paket yang awalnya dikirim dengan sendirinya, ia tahu bahwa pengiriman paket ke tetangga itu berhasil.). Protokol menggunakan acknowledgment negatif (NACKs) jika sebuah node entah bagaimana menyadari fakta bahwa ia tidak menerima paket, dan secara eksplisit mengirimkan permintaan untuk transmisi ulang.

Baik skema berbasis ACK maupun NACK rentan terhadap paket kontrol yang disuntikkan, tetapi secara umum skema berbasis ACK rentan terhadap serangan terhadap keandalan, sementara protokol berbasis NACK hanya rentan terhadap serangan yang menguras energi. Dalam praktiknya, serangan terhadap keandalan lebih penting daripada serangan yang menghabiskan energi; karena itu skema NACK (yaitu, PSFQ [57], [56]) mungkin lebih disukai daripada skema ACK (yaitu, referensi 58 dan 59). Skema NACK juga lebih cocok untuk komunikasi multihop. Namun, mereka memiliki dua kelemahan yang diwariskan: Satu melibatkan hilangnya bagian terakhir dari sebuah pesan, dan yang lainnya melibatkan hilangnya seluruh pesan. Relatif mudah untuk memecahkan masalah fragmen terakhir yang hilang dengan menginformasikan node tujuan tentang jumlah fragmen dalam pesan pada awal komunikasi (misalnya, pada fragmen pertama yang ditransmisikan). Untuk masalah pesan penuh yang hilang, belum ada solusi yang memuaskan saat ini [63].

Memberikan autentikasi pada lapisan bawah dapat menyelesaikan banyak masalah yang disebutkan di atas. Setidaknya, dengan mengautentikasi paket kontrol, akan lebih sulit bagi penyerang untuk menghabiskan baterai sensor, dan dengan demikian, mengurangi masa pakai jaringan. Serangan banjir dan desinkronisasi adalah dua serangan yang memiliki target lapisan transport [24]. Kami akan menganalisisnya di paragraf berikut.

Banjir. Serangan flooding digunakan untuk menghabiskan sumber daya memori dari sistem korban. Dalam praktiknya, musuh mengirimkan banyak permintaan pembuatan koneksi kepada korban. Setiap permintaan menyebabkan korban mengalokasikan sumber daya yang mempertahankan status untuk koneksi tersebut. Serangan ini dapat dijalankan setiap kali protokol diperlukan untuk mempertahankan status tain di kedua ujung koneksi. Untuk mengurangi keparahan serangan ini, teka-teki klien telah diperkenalkan [64]: Ketika klien membutuhkan akses ke sumber daya, server menjawab dengan teka-teki yang harus dipecahkan klien untuk mendapatkan akses yang diperlukan. Dengan cara ini, penyerang harus menghabiskan lebih banyak daya komputasi untuk membanjiri jaringan. Kelemahannya adalah node yang sah harus mengeluarkan sumber daya ekstra untuk bisa terhubung. Namun, bahkan jika teka-teki ini menyertakan overhead pemrosesan, teknik ini lebih diinginkan daripada komunikasi yang berlebihan. Sebuah protokol berdasarkan teka-teki klien dan cocok untuk WSN telah diusulkan dalam referensi 65. Ini mengurangi serangan DoS terhadap autentikasi siaran dengan memanfaatkan mekanisme autentikasi lemah yang menggunakan rantai kunci.

Desinkronisasi. Dalam serangan desinkronisasi, musuh mencoba mengganggu koneksi yang ada antara dua titik akhir. Untuk mencapai targetnya, musuh memalsukan pesan yang berisi nomor urut palsu atau bendera kontrol ke salah satu atau kedua titik akhir. Dengan terus- menerus menyebabkan permintaan pengiriman ulang pesan yang hilang, serangan ini mampu mencegah titik akhir bertukar informasi yang berguna. Secara alami, itu dapat dengan cepat menguras semua sumber daya dari titik akhir yang diserang. Penanggulangan tipikal dan efektif untuk serangan ini adalah otentikasi. Dengan mengautentikasi semua paket yang dipertukarkan, musuh tidak dapat memalsukan paket berbahaya lainnya . Otentikasi dapat dijalankan baik di header atau di seluruh paket.

4.2.2 Serangan Terhadap Privasi dan Kerahasiaan

Meluasnya WSN menimbulkan banyak keraguan tentang privasi dan kerahasiaan data yang dikumpulkan. Karena sensor mengumpulkan data (sensitif) yang kemudian dikirim ke sink, dan mungkin ke database terpusat, penting untuk memastikan akses yang tepat ke orang yang tepat. Yang pasti, kerahasiaan data harus ditegakkan melalui kebijakan kontrol akses yang mencegah penyalahgunaan informasi oleh pihak yang tidak diinginkan. Pada bagian ini, daripada berfokus pada aspek etika atau hukum dari masalah ini, kami akan berkonsentrasi pada solusi teknologi untuk menjamin kerahasiaan data dalam WSN.

Kerahasiaan data tidak selalu menjadi persyaratan: Misalnya, jika kita memantau cuaca, privasi data yang dikumpulkan tentu tidak penting. Namun jika kita menggunakan WSN untuk memantau kesehatan orang-orang di dalam rumah mereka, menjaga privasi data menjadi perhatian penting. Pemantauan kesehatan bukan satu-satunya aplikasi yang memerlukan kerahasiaan data. WSN dikerahkan untuk memantau hewan di dalam Negara

taman pada prinsipnya tidak memerlukan kerahasiaan data, tetapi jika layanan jaringan yang sama dapat digunakan oleh pemburu untuk menemukan hewan dengan cepat, kerahasiaan adalah suatu keharusan.

Dalam banyak aplikasi, node bertukar data yang sangat sensitif dan jaringan sensor tidak boleh membocorkan pembacaan sensor ke musuh eksternal. Kerahasiaan biasanya dicapai dengan mengenkripsi data dengan kunci rahasia yang hanya dimiliki oleh penerima yang dituju.

Karena daya komputasi sensor yang terbatas, mekanisme kunci simetris lebih disukai daripada kunci publik. Skema yang paling banyak digunakan dan dikutip berdasarkan kunci simetris diperkenalkan di referensi 33: SPINS. SPINS adalah rangkaian protokol keamanan yang dioptimalkan untuk WSN dan terdiri dari dua blok penyusun: Yang pertama memastikan kerahasiaan data, autentikasi data dua pihak, dan kesegaran data, sedangkan yang kedua menyediakan mekanisme autentikasi siaran yang efisien. Secara khusus, kerahasiaan data dicapai dengan menggunakan kunci rahasia bersama dan penghitung bersama antara pengirim dan penerima. Beberapa skema enkripsi didasarkan pada pra-distribusi kunci.

Saat dua sensor ingin berkomunikasi dengan aman, pertama-tama mereka harus mengetahui kunci mana yang mereka gunakan bersama dengan mengeksekusi fase penemuan kunci. Kemudian, mereka dapat membuat saluran aman dengan menghitung kunci umum sebagai fungsi dari kunci bersama [66,67].

Penting untuk mempertimbangkan kerahasiaan data saat menggunakan fungsi agregasi juga. Dalam WSN, agregasi data merupakan teknik penting untuk mencapai efisiensi daya dengan mengurangi redundansi data dan meminimalkan penggunaan bandwidth. Data yang dikumpulkan oleh node sensor

diproses dan dikumpulkan di setiap node perantara sebelum mencapai sink. Namun, kerahasiaan data dan agregasi data berada dalam konflik: Sementara kerahasiaan memerlukan enkripsi antara node asal dan sink, agregasi data mengharuskan node perantara memiliki akses ke cleartext untuk memproses data.

Dalam referensi 68, skema untuk WSN yang memberikan kerahasiaan dan integritas data agregat telah diusulkan. Ini didasarkan pada enkripsi homomorfik, dan juga dapat mendeteksi upaya injeksi data palsu.

Juga dalam referensi 69, skema lain diperkenalkan yang bergantung pada fungsi enkripsi homomorfik yang sederhana namun terbukti aman dan yang membahas kerahasiaan dan agregasi data yang efisien. Lihat referensi 70 untuk tinjauan teknik agregasi untuk data rahasia di WSN.

Namun, enkripsi saja tidak cukup untuk menjamin kerahasiaan dalam arti yang lebih luas.

Misalnya, musuh dapat melakukan analisis lalu lintas pada ciphertext yang didengar untuk mendapatkan informasi penting tentang topologi jaringan dan kejadian yang dirasakan. Pada fase kedua, musuh dapat menjalankan serangan yang ditargetkan untuk mengganggu bagian dari jaringan yang dipilih untuk efek terbesar. Jelas bahwa, dalam hal ini, tidak hanya kerahasiaan diperlukan untuk pertukaran data dalam jaringan (yang mungkin dienkripsi), tetapi juga fakta bahwa node bertukar beberapa informasi perlu disembunyikan juga. Pada Bagian 4.2.2.2, kami akan melaporkan tentang protokol yang dapat digunakan untuk menjamin kerahasiaan semacam ini.

4.2.2.1 Sniffing

Jika komunikasi end-to-end tidak dilindungi, musuh dapat menemukan konten komunikasi hanya dengan mendengarkan alirannya. Serangan pasif ini dapat dipasang bahkan oleh orang luar, yang dapat mencuri informasi pribadi atau sensitif dengan menguping rentang frekuensi radio jaringan. Jika penyerang mungkin langsung merasakan data yang sama sendiri dengan memasang sensornya sendiri di lapangan, menguping bukanlah masalah. Namun, jika tindakan sensor bersifat rahasia, seperti dalam aplikasi medis, penyadapan harus diatasi. Dalam hal ini, data sensitif dikirim melalui jaringan, dan oleh karena itu mekanisme keamanan yang dapat melindungi privasi data harus digunakan.

Kerentanan terhadap penyadapan telah dipelajari dalam referensi 71, tanpa solusi untuk kerahasiaan tetapi diskusi tentang pendekatan nonkriptografi. Namun, teknik keamanan standar dapat digunakan sebagai penanggulangan serangan ini; misalnya, kita dapat menggunakan kriptografi primitif untuk menjamin keaslian dan kerahasiaan komunikasi antara node yang sah. Masalahnya lagi-lagi berkurangnya sumber daya sensor. Oleh karena itu, diperlukan primitif kriptografi yang kompatibel dengan sumber daya node yang terbatas. SPINS [33] adalah protokol yang telah dirancang secara eksplisit dengan mempertimbangkan perangkat yang dibatasi sumber daya. Ini dapat digunakan untuk memastikan kerahasiaan data, otentikasi data dua pihak, dan kesegaran data.

4.2.2.2 Analisis Lalu Lintas. Analisis lalu lintas juga dapat digunakan oleh penyerang. Peningkatan jumlah paket yang ditransmisikan antara node tertentu dapat menandakan aktivitas di sensor tertentu. Melalui analisis lalu lintas, beberapa sensor dengan peran khusus atau yang bertanggung jawab atas aktivitas khusus dapat diidentifikasi secara efektif [72]. Ini berpotensi menjadi masalah besar di WSN karena memungkinkan penyerang melakukan serangan berbahaya dan terarah

untuk mengganggu bagian dari jaringan yang dipilih untuk memaksimalkan kerusakan. Musuh dapat menyimpulkan informasi penting dengan memantau volume lalu lintas dan informasi jalur lalu lintas meskipun konten paket data dienkripsi. Deng dkk. mengusulkan penanggulangan terhadap serangan analisis lalu lintas yang berusaha untuk menemukan base station [72]. Baru-baru ini, Wadaa et al. skema yang diusulkan untuk mengacak komunikasi selama fase pengaturan jaringan, untuk melindungi anonimitas infrastruktur jaringan sensor [73].

4.2.3 Serangan Terhadap Integritas Data

Ketika berbicara tentang integritas, kita perlu membedakan integritas data dan layanan. Sementara yang pertama bertujuan menjaga integritas informasi yang dirasakan oleh node, yang kedua bertujuan menjaga operasi layanan yang benar. Sebagai gantinya, di bagian ini kami akan menjelaskan hal-hal yang bertentangan dengan integritas data.

4.2.3.1 Replikasi Node

Terutama karena alasan biaya, sensor yang digunakan dalam WSN tipikal tidak dapat dirusak. Musuh dapat menangkap sebuah node, mereplikasi dan memasukkan node yang direplikasi di jaringan yang ada. Upaya yang diperlukan tergantung pada langkah-langkah balasan untuk anti-rusak yang diramalkan pada tahap desain. Namun, jika musuh mengkompromikan bahkan satu simpul saja, proses replikasi dapat berlanjut tanpa batas. Kelas serangan yang besar kemudian dapat digunakan: Dengan hanya menyuntikkan data palsu tingkat tinggi, penyerang dapat menumbangkan protokol pemungutan suara atau agregasi data.

Pemantauan terpusat biasanya digunakan untuk mencegah replikasi node. Mekanisme berdasarkan ide ini telah digunakan untuk mengatur pencabutan simpul terpusat dalam jaringan sensor bekerja [67,74]. Umumnya, skema ini membutuhkan semua node dalam jaringan untuk mentransfer daftar lokasi yang diklaim tetangga mereka ke entitas pusat. Dengan demikian, entitas ini dapat memeriksa daftar untuk klaim lokasi yang bertentangan. Namun, ada dua kelemahan dari pendekatan ini: (a) pengenalan satu titik kegagalan dan (b) overhead komunikasi yang dikeluarkan oleh node yang mengelilingi entitas pusat. Memang, musuh dapat mengkompromikan entitas pusat atau mengganggu komunikasinya, sehingga mengganggu pemantauan terpusat. Selain itu, node yang mengelilingi entitas terpusat ini tunduk pada beban komunikasi yang dapat mempersingkat harapan hidup jaringan. Properti yang muncul telah digunakan berbeda dengan pemantauan terpusat. Dalam referensi 75, dua protokol berdasarkan ide kunci ini telah diperkenalkan. Algoritme ini sangat tahan terhadap serangan aktif, dan kedua protokol berupaya meminimalkan konsumsi daya dengan membatasi komunikasi.

4.2.3.2 Paket Injeksi, Replikasi, dan Perubahan.

Injeksi paket atau pesan, replikasi dan perubahan adalah semua serangan aktif yang umumnya dijalankan oleh orang dalam. Namun, bila tidak ada autentikasi yang digunakan, serangan ini juga dapat dilakukan oleh pihak luar. Seringkali, tujuan penyerang adalah mengirimkan informasi palsu ke catatan yang korup, atau terkadang menjenuhkan jaringan. Replikasi paket digunakan saat musuh mengirimkan paket yang sebelumnya ditangkap ke sensor lain. Misalnya, penyerang dapat menangkap paket yang membunyikan alarm kebakaran, dan menggunakannya nanti untuk membuat jaringan percaya bahwa ada deteksi kebakaran baru. Musuh juga dapat mengubah isi paket yang diindera, yang dikenal sebagai serangan perubahan paket. Perubahan terdiri

dari mengganti data yang benar dengan data yang salah (khususnya, ini termasuk menghapus data ketika isi paket diganti dengan data null).

Peluang untuk menjalankan injeksi paket, replikasi, dan serangan perubahan sangat terkait dengan langkah-langkah otentikasi yang digunakan. Jika musuh tidak dapat mengkompromikan mekanisme autentikasi, sensor tidak akan menerima paket dan pesan yang coba dikirimnya. Memang, otentikasi data memungkinkan penerima untuk memverifikasi bahwa data benar-benar dikirim oleh pengirim yang diklaim. Umumnya, protokol autentikasi yang digunakan dalam jaringan ad hoc tidak cocok untuk WSN. Faktanya, kriptografi asimetris umumnya dihindari di WSN. Sebaliknya, mekanisme otentikasi data untuk WSN lebih memilih kunci simetris [67,74,76,77]. ÿTESLA [33] adalah versi "mikro" dari skema Timed Efficient Stream Loss-tolerant Authentication (TESLA) yang diusulkan dalam referensi 78. Ini didasarkan pada TESLA, tetapi dengan pembaruan kunci yang berbeda dan autentikasi awal, yang membuatnya cocok untuk nirkabel jaringan sensor. Gagasan utama ÿTESLA adalah menggunakan fungsi hash satu arah untuk membentuk gantungan kunci. Sebuah node dapat mengautentikasi kunci sebelumnya melalui kunci saat ini, sedangkan kunci saat ini tidak dapat dihitung dari kunci sebelumnya; pengumuman kunci tertunda setelah jangka waktu tertentu untuk pesan yang sesuai. Dengan cara ini, penyerang tidak dapat memalsukan kunci kuncinya harus diungkapkan. Node menyimpan paket dalam buffer, mengetahui bahwa kunci MAC hanya diketahui oleh stasiun pangkalan dan tidak ada musuh yang dapat mengubah paket selama transmisi. Saat kunci akan dibuka, stasiun pangkalan menyiarkan kunci ke semua penerima. Penerima kemudian dapat memverifikasi kebenaran kunci dan menggunakannya untuk mengautentikasi paket yang disimpan dalam buffer. Setiap kunci MAC adalah anggota dari rantai kunci, yang dihasilkan oleh fungsi satu arah F. Untuk menghasilkan rantai ini, pengirim memilih kunci terakhir Kn dari rantai secara acak dan menerapkan F berulang kali untuk menghitung semua yang lain. kunci; yaitu iterasi

Ki = F(Ki+1) untuk i = n ÿ 1 turun menjadi 1.

4.2.4 Rangkuman Ancaman Keamanan dan Penanggulangan di WSN

Pada bagian ini kita telah membahas ancaman dan penanggulangan keamanan utama yang terkait dengan WSN. Kami telah mengklasifikasikannya menggunakan tingkat abstraksi ganda: target musuh dan lapisan yang diserang . Sasaran musuh mungkin untuk mengkompromikan (1) ketersediaan jaringan atau integritas layanan, (2) privasi dan kerahasiaan protokol, (3) integritas data. Lapisan yang diserang dapat berupa (1) lapisan fisik, (2) lapisan tautan, dan (3) lapisan jaringan dan perutean. Secure WSN harus menyediakan mekanisme keamanan di setiap lapisan, dan, bergantung pada layanannya, mereka harus melindungi satu atau lebih target musuh.

4.3 WSN TANPA PENGAWASAN

Di WSN, data yang dirasakan oleh node dikirim secara real time (atau quasi real time) ke sink. Node mungkin bergantung pada protokol multihop untuk mencapai sink, yang terus tersedia. Sebaliknya, jaringan sensor nirkabel tanpa pengawasan (UWSNs) dicirikan oleh keberadaan wastafel yang terputus-putus. Dalam skenario seperti itu, node harus mengumpulkan informasi yang dirasakan di lapangan, serta mencoba untuk memindahkannya ke sink segera setelah tersedia. UWSN diperkenalkan pada tahun 2007 oleh Di Pietro et al. [79], salah satu penulis bab ini. Untuk alasan ini, bagian khusus ini mungkin tampak bias terhadap karya penulis itu sendiri meskipun kami berusaha untuk bersikap adil.

Alasan yang menyebabkan diperkenalkannya jenis jaringan sensor nirkabel ini terkait erat dengan tidak dapat diaksesnya lingkungan tempat node dapat digunakan. Sebagai contoh, pertimbangkan sistem monitor untuk mendeteksi perburuan liar di taman nasional. Kesulitan menyembunyikan wastafel, bersama dengan ukuran area yang dipantau, adalah alasan utama untuk mengadopsi WSN tanpa pengawasan. Ini juga kasus jaringan sensor bawah tanah, atau kapal selam: Tidak dapat diaksesnya area yang dipantau, bersama dengan masalah teknis yang muncul untuk menghubungkan bak cuci dengan sensor, tidak memungkinkan penggunaan bak cuci tradisional. Dalam semua kasus ini, wastafel intermiten adalah satu-satunya alternatif.

Karena sensor biasanya ditempatkan di lingkungan yang tidak bersahabat, dan karena wastafel tidak dapat terus-menerus memeriksa apakah sensor berfungsi dengan benar, UWSN mewakili target yang mudah dan menarik bagi musuh. Terutama karena alasan biaya, sensor tipikal adalah perangkat komoditas yang diproduksi secara massal tanpa perangkat keras khusus yang aman. Oleh karena

itu, saat wastafel pergi, musuh dapat membahayakan sensor, membaca, menghapus, atau mengubah

dan mengautentikasi pesan. Penulis menggunakan MD5 sebagai fungsi hash satu arah di TESLA dan ÿTES ÿTESLA membutuhkan stasiun pangkalan dan node untuk disinkronkan secara longgar,

serta setiap node mengetahui batas atas kesalahan sinkronisasi maksimum. Agar paket terotentikasi dikirim, stasiun pangkalan menghitung MAC pada paket dengan kunci rahasia pada saat itu. Ketika sebuah node mendapatkan paket, ia dapat mengonfirmasi bahwa stasiun pangkalan belum mengungkapkan kunci MAC yang sesuai, menggunakan jam yang disinkronkan secara longgar, kesalahan sinkronisasi maksimum, dan waktu di mana suatu informasi, dan menghilang tanpa meninggalkan bukti perilaku ilegalnya.

Pada bagian ini kami akan menjelaskan tantangan keamanan yang muncul saat berhadapan dengan fitur unik UWSN, dan kami akan menjelaskan solusi yang ada. Pertama, kami akan menawarkan kategorisasi tindakan keamanan ini berdasarkan kemampuan penyerang, teknik kriptografi yang digunakan, dan properti keamanan yang harus dipastikan.

Kemampuan Penyerang. Musuh yang biasanya dipertimbangkan dalam UWSN adalah bergerak atau diam. Musuh seluler "bergerak", sehingga membahayakan kumpulan node yang berbeda. Bergantung pada model yang diadopsi, dia dapat secara fisik bergerak di area tertentu dan mengkompromikan sensor yang dipasang di sekitarnya, atau berpindah dari satu set sensor ke set lainnya. Dalam kasus kedua, sensor dapat tersebar di semua jaringan, tetapi dalam setiap kerangka waktu musuh hanya dapat berkompromi dalam jumlah terbatas.

Penyerang stasioner malah mempertahankan posisi awalnya selama seluruh serangan.

Ini terjadi ketika dia memilih subset sensor di awal serangannya tanpa mengubah targetnya setelah itu, tetapi juga ketika dia memilih posisi fisik awal dan dia hanya mengkompromikan node yang ditempatkan di sekitarnya. Perhatikan bahwa dalam kasus terakhir ini subset dari node yang dapat dikompromikan berubah dari waktu ke waktu jika sensor bergerak.

Teknik Kriptografi. Solusi dan mekanisme yang dirancang secara eksplisit untuk UWSN dapat dikategorikan lebih lanjut, bergantung pada fungsi kriptografi yang digunakan.

Dalam banyak kasus, kunci simetris digunakan untuk mendapatkan kerahasiaan dan autentikasi data, tetapi dalam beberapa kasus, penggunaan kriptografi kunci publik juga dimungkinkan. Secara umum,

lebih baik menggunakan fungsi kriptografi sederhana, seperti fungsi hash satu arah [80] dan beberapa skema simetris yang efisien seperti AES [81] atau Skipjack [82].

Yang terakhir digunakan untuk WSN dalam skema TinySec [83] karena efisiensi dayanya.

Properti Yang Harus Dipastikan. Tiga properti keamanan utama yang harus dipastikan dalam UWSN adalah: kemampuan bertahan data, pemulihan kunci mandiri–ketahanan intrusi, dan autentikasi data. Kemampuan bertahan data merupakan aspek fundamental dalam UWSN. Karena data tidak dapat dipindahkan ke bak cuci secara real time, sensor perlu menanganinya hingga bak cuci muncul. Memang, tujuan utama musuh sering kali adalah menghapus data yang diindera sebelum mencapai sink. Mengenai penyembuhan diri sendiri–ketahanan intrusi, harus diperhitungkan bahwa interval antara kunjungan sink berturut-turut mewakili periode kerentanan, dan oleh karena itu memberikan dorongan untuk aktivitas musuh. Penyembuhan kunci sendiri dan mekanisme ketahanan intrusi bertujuan untuk memulihkan sensor yang disusupi.

Mengenai autentikasi data, jelas bahwa UWSN harus menggunakan mekanisme autentikasi data yang

tidak bergantung pada entitas terpusat mana pun; jika tidak, dengan waktu yang cukup antara kunjungan sink, musuh dapat dengan mudah mengkompromikan data yang dikumpulkan sensor. Dalam sekuelnya, kami akan menganalisis sifat-sifat ini dengan lebih baik dan menyoroti solusi yang diusulkan dalam literatur.

4.3.1 Ketahanan Data

Dalam UWSN, ketidakmampuan sensor untuk secara langsung memindahkan data ke sink memudahkan musuh untuk melakukan serangan terfokus yang ditujukan untuk menghapus data target tertentu. Di dalam pengaturan, seseorang biasanya mengasumsikan musuh seluler yang secara aktif memburu item data tertentu dan yang tidak takut untuk menghapus/menghapus item data lain yang dia temukan.

Kelangsungan hidup data dalam UWSNs pertama kali diperkenalkan pada referensi 79. Penulis mengusulkan teknik nonkriptografis sederhana yang ditujukan untuk menyembunyikan data dari musuh. Secara khusus, tiga strategi bertahan hidup telah diselidiki: Do-Nothing, Move-Once, dan Keep-Moving.

Tidak melakukan apapun. Ini adalah strategi bertahan hidup yang sepele yaitu, hanya meninggalkan data yang ada di sensor yang mengumpulkannya, menunggu kedatangan bak cuci. Bergerak-Sekali. Data dipindahkan ke sensor baru yang dipilih secara acak dari milik mereka ke jaringan. Terus bergerak. Data terus dipindahkan: Setiap sensor memindahkan setiap item data satu per satu ke sensor lain yang dipilih secara acak.

Juga, tiga strategi serangan telah diperhitungkan:

Malas. Ini adalah penyerang stasioner. Dia memilih k node untuk dikompromikan pada awal protokol dan tidak mengubah targetnya setelah itu.

Panik. Penyerang panik adalah penyerang seluler yang, dalam setiap interval, mengubah subset node yang disusupi dan berpindah ke k node lain yang dipilih secara acak.

Cerdas. Penyerang ini juga mobile, tetapi dia bergerak di antara dua set node yang telah dipilih sebelumnya, masing-masing berukuran k.

Penulis mempertimbangkan semua kombinasi strategi serangan-bertahan hidup yang masuk akal, dan mereka menyoroti bahwa (1) strategi bertahan hidup Do-Nothing tidak berguna, (2) strategi serangan terbaik terhadap strategi bertahan hidup Move-Once adalah strategi Frantic, dan (3) melawan strategi Keep-Moving, penyerang Cerdas adalah yang paling efektif.

Selanjutnya, penggunaan teknik kriptografi sederhana diklaim dalam makalah ini untuk lebih melindungi privasi data yang dikumpulkan. Namun, penulis meninggalkan studi lengkap tentang mekanisme ini untuk penyelidikan lebih lanjut.

Dalam referensi 84, musuh yang disebut Penghapus yang ingin menghapus informasi apa pun tanpa pandang bulu juga dianalisis. Anehnya, ternyata dalam hal ini strategi bertahan hidup terbaik adalah Do- Nothing. Dalam karya ini, efek replikasi data juga diselidiki, menunjukkan bahwa replikasi digabungkan dengan strategi Keep-Moving adalah solusi terbaik melawan Eraser. Replikasi juga digunakan dalam referensi 85. Di sana, teknik epidemi terkontrol murni digunakan untuk memberikan pertukaran antara kemampuan bertahan data, penggunaan sumber daya sensor yang optimal, dan waktu pengumpulan yang cepat dan dapat diprediksi. Penulis membuktikan bahwa dengan memperkirakan kekuatan maksimal penyerang, dimungkinkan untuk membuat batasan probabilistik pada daya tahan data. Ini adalah pekerjaan pertama di area yang menganggap waktu pengumpulan sebagai masalah; akibatnya, mungkin membuka baris baru penelitian. Dalam referensi 86, penulis menginvestigasi teknik yang dapat memaksimalkan ketahanan data di UWSN dengan adanya kegagalan acak dan kompromi simpul.

Mereka mengusulkan skema berbasis pembagian rahasia komputasi untuk memaksimalkan komunikasi

dan efisiensi penyimpanan dan tingkat kelangsungan hidup data. Selain itu, mereka memperkenalkan skema yang disempurnakan berdasarkan pengkodean jaringan untuk lebih meningkatkan efisiensi konsumsi daya komunikasi.

Dalam referensi 87, enkripsi digunakan untuk menyembunyikan asal paket, waktu pengumpulan, dan konten data penginderaan. Alasan di balik adopsi kriptografi adalah jika musuh tidak dapat mengenali data target, dia harus menghapus data secara membabi buta (seperti penyerang Eraser). Dengan kata lain, dia harus menebak ciphertext mana yang menyembunyikan data target. Hasil yang menarik dari analisis ini terkait dengan penggunaan kriptografi kunci publik: Data yang terus bergerak di sekitar jaringan memberikan keamanan yang sama dengan menggabungkan

data yang bergerak hanya sekali dan mengenkripsinya kembali.

4.3.2 Self-Key Healing dan Ketahanan Intrusi

Ada banyak skenario di mana autentikasi dan kerahasiaan data diperlukan untuk mengelola data penting atau bernilai tinggi. Mekanisme kriptografi sangat mendasar di sini. Ketika musuh mengkompromikan sebuah node, semua data dan kunci yang disimpan di node juga dikompromikan. Bergantung pada targetnya, musuh dapat mencoba menggunakan pengetahuan ini untuk memalsukan data baru (yang diautentikasi), atau mendapatkan beberapa pengetahuan di jaringan, terlepas dari skema kriptografi yang digunakan untuk autentikasi dan/atau kerahasiaan data. Di UWSN masalahnya bahkan lebih rumit. Memang, karena sink terputus-putus, tidak dapat mengambil tindakan cepat dan tepat untuk mencegah kompromi sensor, dan mendeteksi kompromi tersebut menjadi lebih sulit tanpa bantuan entitas pusat ini.

Penyembuhan kunci mandiri dan ketahanan intrusi berfokus pada teknik yang memungkinkan sensor tanpa pengawasan pulih dari intrusi dengan meminta bantuan dari sensor rekan. Jika kunci tetap dirahasiakan, tidak ada masalah yang dapat mengganggu kerahasiaan dan autentikasi data, tetapi, karena sensor biasanya tidak tahan terhadap kerusakan, penyerang dapat secara fisik membahayakan sensor dan membaca kunci yang saat ini disimpannya. Dalam UWSN, kami biasanya memperhatikan kerahasiaan ke belakang dan ke depan. Dalam hal ini, "backward" dan "forward secrecy" mengacu pada kerahasiaan kunci, yang kemudian dapat dimanfaatkan untuk memperoleh kerahasiaan data dan/atau autentikasi data. Menjamin kerahasiaan baik ke belakang maupun ke depan, adalah mungkin untuk menjamin bahwa sensor yang tidak berada di bawah kendali langsung musuh menggunakan kunci rahasia, yang tidak terpapar sepengetahuannya.

Kerahasiaan maju mudah diperoleh melalui evolusi kunci periodik [88]. Sebaliknya, kerahasiaan mundur jauh lebih sulit untuk dicapai karena bergantung pada sumber keacakan yang tidak boleh dikendalikan oleh Dalam referensi 89, DISH diperkenalkan. Ini adalah skema berdasarkan kunci simetris yang memanfaatkan kolaborasi sensor untuk pulih dari kompromi dan menjaga kerahasiaan data yang dikumpulkan. Ini memberikan kerahasiaan "mundur" dan "maju" menggunakan teknik "sponsor": Node yang sehat mensponsori node yang sakit untuk membuatnya sehat kembali.

Sponsorship dalam konteks ini berarti bahwa node sponsor memberikan nilai pseudorandom ke node sponsor, dan yang terakhir menggunakan nilai ini untuk memperbarui kunci kriptografi.

Secara lebih rinci, di setiap putaran, setiap node membutuhkan nilai dari sponsor t, dan menggunakan nilai ini di putaran berikutnya untuk memperbarui kunci simetrisnya sendiri. Penulis mempertimbangkan musuh seluler yang dapat berkompromi hingga k node dalam setiap interval waktu. Dua kemungkinan strategi dianalisis: Trivial Adversary dan Smart Adversary. Yang pertama mencoba untuk berkompromi di setiap interval waktu satu set sensor baru yang dipilih secara acak

yang belum dikompromikan. Yang terakhir memilih subset node yang akan dikompromikan sedemikian rupa untuk mengganggu mekanisme sponsor: Dia lebih memilih untuk mengkompromikan sponsor dari node yang sakit untuk mempertahankan status sakitnya. DISH berhasil mengurangi efek kompromi sensor. Namun, itu membutuhkan banyak pesan untuk ditukar di setiap putaran. Skema lain berdasarkan sponsor adalah POSH [90]. Idenya mirip dengan DISH, tetapi berbeda dalam satu masalah utama: Sponsor mendorong bukannya ditarik. Dengan kata lain, alih-alih node secara eksplisit membutuhkan kontribusi dari t node sponsor, yang terakhir secara sukarela mengirimkan kontribusinya. Dengan cara ini, pesan permintaan tidak lagi digunakan, sehingga mengurangi pemborosan energi yang sesuai.

Skema yang dikutip sebelumnya mempertimbangkan penyerang yang dapat berkompromi hingga sejumlah sensor di setiap putaran. Selain itu, sensor-sensor ini tidak bersebelahan, dalam artian dapat tersebar dalam skenario yang dipantau. Hipotesis yang lebih realistis adalah musuh yang hanya dapat membahayakan sensor dalam jangkauan komunikasi atau tindakannya. Musuh ini dianalisis dalam referensi 91, di mana ia dianggap mampu mengendalikan bagian tetap dari area penyebaran jaringan dan mengkompromikan semua sensor yang bergerak di dalamnya mengikuti model mobilitas tertentu, seperti titik jalan acak atau lompatan acak . Skema yang diusulkan didasarkan pada kriptografi kunci publik, tetapi menggunakan mekanisme evolusi berdasarkan kolaborasi node untuk menghasilkan kunci acak simetris satu kali. Secara khusus, skema memanfaatkan mobilitas node dengan cara yang mirip dengan mekanisme push yang digunakan di POSH. Di setiap putaran, node menyiarkan "kontribusi" yang kemudian digunakan oleh tetangganya untuk menghitung

kunci acak simetris satu kali berikutnya. Skema lain yang menggunakan mobilitas sensor adalah yang diusulkan dalam referensi 92. Namun, dalam karya ini musuh yang berbeda dianalisis. Dia tidak lagi diam di titik tetap area penyebaran jaringan, tetapi menjelajah jaringan dan memilih di setiap putaran bagian dari area penyebaran yang akan dikompromikan. Musuh jenis ini termasuk dalam kategori “musuh seluler” yang kami perkenalkan di Bagian 4.3. Protokol yang diusulkan mirip dengan yang ada di referensi 91, tetapi mobilitas musuh mengarah pada analisis baru. Penulis menunjukkan bahwa skema yang diusulkan bergantung pada (1) bagian dari permukaan penyebaran yang dikendalikan oleh musuh, (2) model mobilitas sensor, dan (3) jumlah rata-rata tetangga dari sebuah node. Analisis dan simulasi menunjukkan bahwa performa penyembuhan diri terbaik dicapai saat mengadopsi model mobilitas sensor yang memberikan variabilitas tinggi di lingkungan sensor.

4.3.3 Otentikasi

Otentikasi untuk sensor tanpa pengawasan pertama kali diselidiki dalam referensi 93, di mana teknik otentikasi agregat maju-aman diusulkan. Namun, dalam pekerjaan itu, sensor

tidak berkomunikasi satu sama lain, dan oleh karena itu solusi yang diusulkan tidak dapat dianggap sebagai skema otentikasi untuk jaringan sensor nirkabel tanpa pengawasan.

Skema pertama yang secara eksplisit menyediakan autentikasi dalam UWSN diusulkan dalam referensi 94. Penulis berfokus pada musuh seluler yang berupaya mengganti data autentik dengan data pilihannya. Mereka memperkenalkan dua teknik yang memanfaatkan kerja sama sensor, dan yang mengandalkan kriptografi simetris: Co-MAC dan ExCo.

Co-MAC adalah singkatan dari "Cooperative MAC", dan ini dapat dianggap sebagai skema berbasis "PUSH": setiap sensor menghitung MAC-nya sendiri, tetapi juga meminta satu set peer yang dipilih secara acak untuk mengotentikasi datanya dan menyimpan MAC yang

dihasilkan . Peer ini, yang disebut co-authenticators, dipilih berdasarkan hasil dari pseudorandom number generator (PRNG) yang diinisialisasi dengan secret seed yang diberikan oleh sink dan kemudian ditanyakan pada setiap putaran. Dengan cara ini, bak cuci tahu persis sensor mana yang akan berisi MAC yang sesuai dengan sensor dan putaran yang diberikan. ExCo, yang merupakan singkatan dari kerjasama yang luas, menggunakan pendekatan yang berbeda: Sensor tidak mengirimkan datanya, tetapi mengirimkan MAC datanya ke co-otentikator. Selain itu, semua MAC yang diterima oleh sensor digabungkan menjadi satu tag autentikasi, yang disimpan secara lokal. Dalam kedua kasus tersebut, untuk mengkompromikan item data yang

diautentikasi, musuh seluler harus mengkompromikan tidak hanya sensor asal, tetapi juga semua co-otentikat Penulis menunjukkan bahwa ini dapat terjadi dengan probabilitas terbatas yang bergantung

pada jumlah co-otentikator. Protokol ini kemudian diperluas dalam referensi 95, di mana mekanisme yang secara dinamis dapat mengadaptasi jumlah co-otentikator diusulkan.

4.3.4 Rangkuman Ancaman Keamanan dan Penanggulangan di UWSN

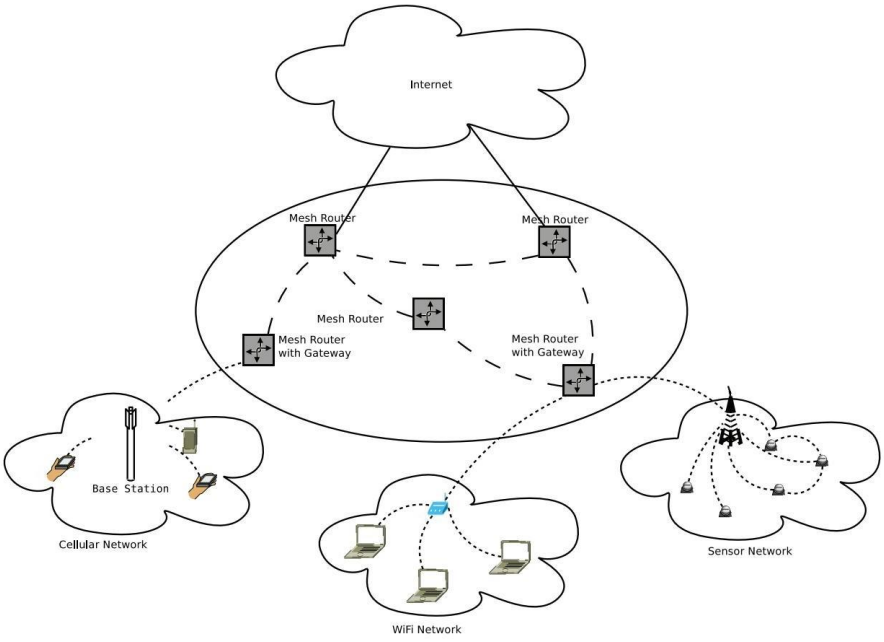
Pada bagian ini, beberapa masalah keamanan yang terkait dengan WSN tanpa pengawasan telah dilaporkan: kemampuan bertahan data, pemulihan kunci sendiri, dan otentikasi. Pertama, kami menawarkan kategorisasi tindakan keamanan yang diusulkan dalam literatur berdasarkan tiga ciri khas: kemampuan penyerang, teknik kriptografi yang digunakan, dan properti keamanan dipastikan. Terakhir, kami meninjau solusi yang telah dirancang secara eksplisit untuk UWSN.

4.4 JARINGAN NIRKABEL MESH

Jaringan mesh nirkabel (WMN) telah muncul sebagai paradigma baru untuk jaringan nirkabel masa depan. Mereka tidak hanya menyediakan konektivitas Internet nirkabel adaptif dan fleksibel untuk pengguna seluler, tetapi juga integrasi jaringan kabel dan nirkabel lainnya.

Self-healing, self-organization, autoconfiguration, dan penerapan yang mudah adalah fitur utama dari WMN. Dapat diperhatikan bahwa properti ini digunakan bersama dengan jaringan ad hoc nirkabel lainnya, dan inilah mengapa banyak solusi yang telah dirancang untuk jaringan ad hoc lainnya dapat digunakan untuk WMN juga.

Ciri khas WMN harus dicari dalam arsitekturnya. Gambar 4.4 menunjukkan komponen khas dari jaringan tersebut dan bagaimana mereka berkolaborasi bersama. Dapat dilihat bahwa node tidak homogen seperti pada skenario ad hoc pada umumnya, tetapi WMN terdiri dari dua set node: klien mesh dan router mesh. Klien mesh adalah perangkat yang mendapatkan akses ke jaringan menggunakan router mesh yang dilengkapi dengan gateway. Misalnya, klien mesh adalah ponsel cerdas di jaringan seluler, atau sensor di jaringan sensor. Router mesh menyusun semacam infrastruktur nirkabel yang digunakan sebagai tulang punggung jaringan. Melalui backbone ini, protokol multihop memungkinkan klien mesh untuk terhubung ke Internet dan mendapatkan akses ke jaringan lain.



Gambar 4.4 Arsitektur jaringan wireless mesh.

Router mesh memiliki mobilitas minimal, dan daya komputasi yang moderat dan seringkali tidak tunduk pada kendala energi. Router ini mungkin dilengkapi dengan beberapa antarmuka radio yang menggunakan teknologi akses nirkabel yang sama atau berbeda. Selain itu, mereka dapat memiliki fungsionalitas gateway/jembatan yang memungkinkan integrasi WMN dengan banyak jaringan seperti WiFi, seluler, WiMAX, atau jaringan sensor. Klien kabel juga dapat menggunakan router jala yang terhubung ke antarmuka Ethernet mereka. Arsitektur ini disusun oleh tulang punggung router jala dan banyak jaringan klien jala disebut sebagai WMN Tulang Punggung. Ketika klien mesh (tanpa bantuan

router mesh) berkomunikasi dalam mode peer-to-peer, dengan melakukan perutean dan menyediakan fungsionalitas konfigurasi serta menyediakan aplikasi pengguna akhir ke pengguna lain, WMN disebut Client WMN. Ada juga arsitektur hybrid yang merupakan kombinasi dari dua yang sebelumnya: Klien mesh dapat mengakses jaringan menggunakan router mesh, tetapi juga langsung terhubung dengan klien lain, sedangkan tulang punggung menyediakan konektivitas ke jaringan lain. Dalam kasus terakhir ini, cakupan dan konektivitas yang disediakan oleh backbone ditingkatkan dengan mekanisme mesh klien.

Karena tidak menggunakan koneksi kabel, WMN lebih mudah digunakan dan bahkan lebih murah daripada jaringan kabel. Selain itu, mereka dapat menyediakan konektivitas yang baik dan bandwidth yang besar kepada pengguna akhir. Untuk alasan ini mereka menjadi solusi yang menarik untuk banyak aplikasi komersial. Namun, ada dua masalah utama yang masih harus diselesaikan sepenuhnya: (i) kinerja saat jumlah lompatan

nirkabel meningkat dan (ii) keamanan. Yang pertama sedang diteliti dengan memperkenalkan baru protokol routing, serta multiradio, teknik multichannel [96], yang merupakan cara yang menjanjikan untuk memecahkan masalah ini. Namun, masalah kedua masih belum mendapat perhatian yang layak. Berikut ini kami akan menjelaskan tantangan keamanan utama, serta penanggulangan yang ada.

4.4.1 Tantangan Keamanan dan Penanggulangan yang Ada

Bahkan jika keamanan WMN merupakan topik yang masih belum sepenuhnya dibahas oleh para peneliti, banyak solusi yang tersedia untuk jaringan ad hoc nirkabel lainnya dapat diadopsi. Masalah otentikasi, misalnya, merupakan tantangan bersama yang telah dipelajari secara luas di jaringan sensor ad hoc dan nirkabel. Namun, di satu sisi, solusi berdasarkan infrastruktur kunci publik (PKI) dan otoritas sertifikasi tunggal (CA) harus dihindari di WMN. Memang, tidak praktis untuk menggunakan satu CA yang harus dipercaya oleh semua node jaringan. Di sisi lain, node WMN (setidaknya router mesh) cukup kuat untuk menggunakan kriptografi kunci publik, bertentangan dengan apa yang terjadi di jaringan sensor. Mekanisme cerdik yang dapat digunakan dalam WMN untuk mendistribusikan fungsionalitas CA terpusat ke seluruh jaringan adalah kriptografi ambang [97]. Dengan cara ini, satu titik kegagalan dihindari, dan subset dari t node masih dapat secara kolektif mengeluarkan sertifikat, tetapi tidak mungkin t ÿ 1 dari mereka dapat melakukan hal yang sama.

Perutean adalah masalah penting lainnya dalam WMN. Memang, terkadang diasumsikan bahwa semua node yang berpartisipasi bekerja sama satu sama lain tanpa mengganggu operasi reguler protokol. Namun, penyerang internal atau bahkan eksternal dapat mencoba mengubah perilaku satu atau lebih node dan memanfaatkan efek yang dapat dihasilkan oleh perilaku buruk tersebut. Perutean di WMN memerlukan tautan multihop nirkabel, konfigurasi mandiri, dan adaptasi mandiri: fitur yang persis sama diperlukan oleh jaringan ad hoc nirkabel lainnya. Faktanya, meskipun sangat sedikit protokol yang telah diusulkan untuk WMN, kesamaan antara mereka dan jaringan ad hoc membuat solusi yang diusulkan untuk jaringan terakhir ini layak untuk WMN juga.

Sebagai contoh, standar IEEE 802.11 untuk jaringan mesh LAN nirkabel (802.11s) mengusulkan protokol Ad hoc On Demand Distance Vector (AODV) yang terkenal [98] sebagai protokol routing dasar. Namun, ini menyarankan metrik baru yang disebut metrik tautan airtim Ketepatan informasi routing yang dipertukarkan antara node sangat penting. Sepertipada sensor dan jaringan ad hoc nirkabel lainnya, penyerang internal dan eksternal dapat mencoba menyuntikkan informasi perutean palsu atau dengan jahat mengubah konten pesan perutean. Seperti yang telah kita diskusikan di Bagian 4.2 ketika mengacu pada jaringan sensor nirkabel, serangan ini dapat dilakukan pada setiap lapisan

protokol komunikasi. Banyak algoritma yang diperkenalkan untuk jaringan ad hoc dan sensor dapat digunakan untuk mengamankan WMN juga: ARAN [4], ARIADNE [2], SEAD [7], SAR [5], SAODV [3], SRP [6], adalah hanya beberapa contoh. Juga, skema perutean geografis untuk WMN dapat diadopsi dari jaringan ad hoc dan sensor. Konsekuensinya, bahkan di WMN, penting untuk memastikan keakuratan lokasi router mesh untuk memastikan eksekusi yang benar dari skema perutean multihop. Perlu diperhatikan bahwa karena router mesh biasanya statis, tujuan ini dapat dicapai lebih baik daripada di jaringan lain. Protokol perutean aman yang dirancang secara eksplisit untuk WMN telah diusulkan dalam referensi 99. Penulis berfokus pada faktor kritis dalam merancang protokol perutean untuk WMN, dan dia mengusulkan protokol perutean yang efisien dan andal. Kontribusi utama dari pekerjaan ini adalah sebagai berikut: (i) Ini memberikan estimasi yang akurat dari delay end-to-end di jalur routing; nilai estimasi kemudian digunakan untuk memeriksa apakah routing dapat menjamin kualitas layanan aplikasi; (ii) menghitung penaksir kualitas tautan dan menggunakannya dalam pemilihan rute; (iii) ia menyediakan kerangka kerja untuk

perkiraan yang andal dari bandwidth yang tersedia dalam jalur perutean sehingga penerimaan aliran dengan kualitas layanan yang terjamin dapat dilakukan; (iv) membantu mengidentifikasi dan mengisolasi node egois. Untuk mengatasi masalah node egois di WMN dengan lebih baik, penulis yang sama mengusulkan skema yang menggunakan pengamatan lokal di node untuk mendeteksi perilaku buruk node [100]. Skema ini berlaku untuk protokol perutean sesuai permintaan seperti AODV, dan menggunakan teori statistik teknik inferensi dan pengelompokan untuk membuat klasifikasi yang kuat dan andal (kooperatif atau egois) dari node berdasarkan tetangganya.

Dengan menggunakan WMN, beberapa jaringan seperti WiFi, WiFi-MAX, jaringan sensor, dan jaringan seluler dapat bertukar lalu lintas dan informasi. Aplikasi baru yang mengeksploitasi integrasi ini dapat dikembangkan, memberikan manfaat besar bagi organisasi dan juga pengguna akhir. Namun, fitur ini juga membawa kekurangan: Jaringan heterogen mungkin memiliki perbedaan arsitektural yang signifikan. Seseorang hanya perlu memikirkan masalah otentikasi. Di banyak jaringan ad hoc dimungkinkan untuk memanfaatkan kriptografi kunci publik, tetapi umumnya tidak cocok untuk jaringan sensor. Oleh karena itu, WMN harus dapat menyesuaikan skema keamanan sesuai dengan fitur klien jaringan yang mendasarinya, tetapi tanpa mengorbankan tingkat keamanan secara keseluruhan.

Banyak aspek keamanan WMN tumpang tindih dengan sensor dan jaringan ad hoc nirkabel lainnya. Dalam referensi 101, misalnya, penulis membahas batasan umum dan fitur rentan dari WMN dan WSN, bersama dengan ancaman keamanan terkait dan kemungkinan penanggulangannya. Tantangan keamanan yang disoroti adalah kemacetan dan pengacakan, risiko terkait MAC, dan serangan perutean seperti blackhole dan kurang tidur untuk menghabiskan sumber daya daya. Dalam referensi 102, masalah keamanan di WMN diselidiki. Kendala jaringan tersebut disorot, seperti bandwidth terbatas, mobilitas tinggi, dan kendala energi dan komputasi dari node akhir. Selanjutnya, beberapa tujuan keamanan dibahas: perutean aman, sistem deteksi intrusi, dan manajemen kepercayaan dan kunci.

Bagaimanapun, solusi yang diusulkan adalah solusi yang awalnya diusulkan untuk WSN atau jaringan ad hoc lainnya. Untuk survei lengkap tentang protokol dan pendekatan ini, pembaca dapat merujuk ke referensi 103.

4.4.2 Rangkuman Ancaman Keamanan dan Penanggulangan di WMN

Banyak solusi yang diusulkan untuk WSN juga dapat diadopsi di WMN, tetapi saat ini banyak masalah terbuka yang perlu diselidiki lebih lanjut. Masalah-masalah ini terutama terkait dengan integrasi banyak teknologi dan perangkat di bawah jenis jaringan yang sama. Saat menggunakan klien meshing, keamanan harus ditegakkan tidak hanya antara gateway mesh dan jaringan klien yang heterogen, tetapi juga antara klien itu sendiri [104]. Di bagian ini, kami memperkenalkan tantangan keamanan utama WMN. Kami menyoroti elemen khas dari jaringan ini sehubungan dengan pekerjaan jaringan ad hoc lainnya. Selain itu, kami menjelaskan secara singkat solusi khusus yang dapat atau tidak dapat digunakan dalam WMN berdasarkan karakteristik dan batasan WMN yang diterapkan.

Sayangnya, keamanan di WMN merupakan topik yang belum sepenuhnya dibahas oleh para peneliti. Namun, banyak solusi yang tersedia untuk jaringan ad hoc lainnya dapat diadopsi: untuk memilih solusi yang layak, hal yang paling penting adalah mengenali masalah khusus yang muncul di WMN.

4.5 JARINGAN TOLERAN TUNDA

Delay-tolerant network (DTN), juga disebut jaringan yang toleran gangguan, adalah jaringan jaringan regional yang ditandai dengan kontak oportunistik (spontan) dan konektivitas intermiten.

Protokol perutean tradisional tidak dapat diterapkan secara langsung dalam skenario di mana koneksi end-to-end antara sumber dan tujuan tidak ada. Namun, meskipun pada saat tertentu jaringan mungkin tidak terhubung, masih mungkin untuk merutekan data dari sumber ke tujuan.

DTN pada awalnya dikembangkan untuk mendukung Interplanetary Internet (IPN), tetapi kemudian digeneralisasi agar dapat digunakan di banyak bidang lainnya. Jenis jaringan baru ini dimotivasi oleh fitur aktual dari Internet saat ini. Memang, berbagai lapisan komunikasi Internet didasarkan pada beberapa asumsi umum, seperti:

Jalur End-to-End Berkelanjutan, Dua Arah. Interaksi end-to-end didukung oleh koneksi dua arah yang terus tersedia antara sumber dan tujuan. Perjalanan Pulang Singkat. Penundaan jaringan dalam pengiriman paket data dan ucapan terima kasih yang sesuai dibatasi hingga beberapa detik atau bahkan milidetik.

Tarif Data Simetris. Tautan dua arah yang menghubungkan sumber dan tujuan mampu mengangkut jumlah data yang hampir sama di setiap interval waktu (asimetri dalam kecepatan data diperbolehkan, tetapi hampir sepanjang waktu terbatas).

Tingkat Kesalahan Rendah. Setiap tautan hanya menyebabkan sedikit kehilangan atau kerusakan data.

Sayangnya, baik IPN maupun banyak skenario jaringan sensor nirkabel tidak memenuhi satu atau banyak dari asumsi ini. Misalnya, tautan dengan satelit mungkin tidak tersedia sepanjang hari, atau sensor seluler mungkin hanya dapat dijangkau saat mendekati stasiun pangkalan.

Protokol TCP/IP yang digunakan di Internet tidak akan dapat mengirim pesan ke node sementara yang tidak tersedia ini, dan akan gagal melaporkan kesalahan koneksi. Memang, Internet adalah jaringan pertukaran paket: Paket diteruskan dari satu router ke router lainnya hingga mencapai tujuan. Jika jalur ke tujuan tidak dapat ditemukan atau jika penundaan terlalu lama, sambungan dibatalkan. Sebaliknya, DTN adalah overlay di atas jaringan regional, termasuk Internet, yang memungkinkan komunikasi dalam hal konektivitas intermiten, panjang atau variabel.

delay, kecepatan data asimetris, dan tingkat kesalahan yang tinggi. Untuk tujuan ini, ia menggunakan pengalihan pesan simpan dan teruskan: Node menggunakan penyimpanan persisten untuk menyimpan sementara pesan yang harus diteruskan ke hop berikutnya; ketika hop berikutnya tersedia, pesan ditransfer ke perangkat penyimpanan node berikutnya, hingga akhirnya mencapai tujuan. Perhatikan bahwa pesan dihapus dari perangkat penyimpanan sebuah node hanya jika yakin bahwa pesan tersebut telah ditransfer ke node berikutnya, atau ketika waktu aktifnya (biasanya beberapa jam atau hari) habis.

Daerah yang menyusun DTN dapat menggunakan protokol komunikasi yang berbeda, tetapi secara internal mereka menggunakan protokol yang sama. Mereka dapat berkomunikasi melalui penggunaan gateway khusus yang menghubungkan dua atau lebih jaringan dan menerjemahkan lalu lintas dari satu protokol ke protokol lainnya. Terjemahan ini, dan juga mekanisme simpan-dan-teruskan yang dijelaskan di atas, dimungkinkan dengan menggunakan lapisan bundel. Lapisan ini dapat dilihat sebagai lapisan komunikasi yang umum di semua wilayah DTN dan dibangun di atas lapisan transport khusus dari setiap wilayah. Bundel adalah pesan yang disusun oleh tiga bagian: (1) data pengguna aplikasi sumber; (2) mengontrol informasi, yang disediakan oleh aplikasi sumber untuk aplikasi tujuan, menjelaskan cara memproses, menyimpan, membuang, dan sebaliknya menangani data pengguna; dan (3) header bundel, disisipkan oleh lapisan bundel. Lapisan bundel DTN berkomunikasi di antara mereka sendiri menggunakan sesi sederhana dengan perjalanan bolak-balik minimal atau

tanpa. Pengakuan apa pun dari node penerima adalah opsional, tergantung pada kelas layanan yang dipilih.

4.5.1 Aplikasi DTN

Bahkan jika DTN pada awalnya dikembangkan untuk Internet Antarplanet, beberapa aplikasi dapat ditemukan saat ini, dan beberapa karya membahas topik ini di bidang jaringan sensor nirkabel. Dalam referensi 105, misalnya, DTN dirancang untuk memungkinkan pelacakan zebra menggunakan perangkat seluler. Dalam hal ini hewan mengenakan kalung yang didalamnya terdapat Global Positioning System (GPS) dan pemancar nirkabel. Mereka bergerak di dalam area yang luas dan liar, dan sayangnya tidak ada layanan seluler atau komunikasi siaran yang mencakup wilayah ini. Node harus menyimpan data secara lokal dan memindahkannya ke node lain atau ke stasiun pangkalan jika tersedia. Penulis menggunakan protokol berbasis riwayat untuk meneruskan data ke node yang terdaftar dengan kemungkinan lebih tinggi untuk bertemu stasiun pangkalan.

Pendekatan serupa digunakan dalam referensi 106. Node khusus yang disebut "bagal" mengambil data dari sensor saat dekat, menyangganya, dan kemudian mengirimkan data ke titik akses berkabel. Keledai juga digunakan dalam referensi 107, untuk menyediakan konektivitas Internet ke lima lokasi terpencil di pegunungan Swedia. Dalam hal ini, bagal data dipasang di atas dua helikopter yang bergerak setiap hari antara host yang terhubung ke Internet dan lima wilayah. Sebenarnya, ada beberapa proyek lain di mana ide spesifik DTN sedang diuji pada prototipe. Sebagian besar pekerjaan ini berfokus pada aspek perutean DTN. Survei protokol perutean untuk DTN dapat ditemukan di referensi 108 dan 109. Sayangnya, masalah keamanan tidak diperhitungkan dalam pekerjaan ini.

DTN dapat menggunakan mekanisme sadar konteks untuk bereaksi terhadap perubahan kondisi lingkungan. Secara khusus, kesadaran konteks menunjukkan semacam pengetahuan tentang status dan sumber daya yang terkait dengan node, tetangganya, dan mungkin

data yang ditransfer di antara mereka. Di antara informasi yang dapat digunakan adalah pendeteksian pemutusan sambungan dari tetangga yang diketahui, perkiraan probabilitas tetangga untuk mengirimkan pesan data ke tujuannya, pertimbangan sebelum meneruskan pesan sisa sumber daya dan penyimpanan energi tetangga. ruang, dan penetapan prioritas untuk pesan yang harus disampaikan oleh node. Informasi yang diperoleh atau diperkirakan ini dapat digunakan untuk mengoptimalkan perilaku mekanisme DTN sehubungan dengan metrik seperti penundaan pengiriman, rasio pengiriman, overhead lalu lintas, dan konsumsi energi [110–112].

4.5.2 Masalah Keamanan di DTN

Konektivitas terputus-putus, penundaan yang lama atau variabel, kecepatan data asimetris, dan tingkat kesalahan tinggi yang biasanya terlihat di DTN menimbulkan masalah keamanan yang penting. Lingkungan yang ditekankan dari jaringan dasar tempat Protokol Bundel beroperasi membuatnya penting bagi DTN untuk dilindungi dari penggunaan yang tidak sah. Selain itu, harus dipertimbangkan bahwa DTN sangat mungkin digunakan di lingkungan yang tidak bersahabat, di mana sebagian dari jaringan dapat disusupi, menimbulkan tantangan keamanan yang biasa terkait dengan kerahasiaan, integritas, dan ketersediaan.

Dalam DTN, semua node penerusan (router dan gateway) saling mengautentikasi satu sama lain, dan informasi pengirim diautentikasi dengan meneruskan node sedemikian rupa sehingga sumber daya jaringan dapat dihemat dengan mencegah lalu lintas terlarang sedini mungkin. Jika sebuah bundel tidak lulus pemeriksaan autentikasi, bundel tersebut langsung dibuang [113].

Kriptografi kunci publik biasanya digunakan untuk otentikasi timbal balik dari node DTN. Memang, pengguna dan node penerusan memiliki pasangan kunci dan sertifikat. Sertifikat pengguna juga menunjukkan hak kelas layanan pengguna: Bergantung pada hak ini, sertifikat dapat memerlukan tanda terima pengembalian, pemberitahuan transfer saat bundel diteruskan dari satu node ke node lainnya, dan seterusnya. Saat pengguna ingin mengirim bundel, ia menandatangani bundel itu sendiri dengan kunci privatnya. Tanda tangan kemudian diperiksa oleh node penerusan menggunakan kunci publik pengirim, untuk mengonfirmasi keaslian pengirim, integritas pesan, dan hak kelas layanan pengirim.

Pemeriksaan ini dijalankan secara berantai: Setiap node penerusan memeriksa tanda tangan yang diterima; dan jika itu asli, itu menggantikan tanda tangan ini dengan tanda tangannya sendiri sebelum meneruskan bundel tersebut. Dengan cara ini, setiap node penerusan berikutnya hanya memverifikasi identitas node penerusan sebelumnya. Dapat dilihat bahwa kombinasi sertifikat PKI yang diterbitkan oleh pihak ketiga yang terpercaya dan mekanisme Daftar Pencabutan Sertifikat diasumsikan. Namun, ini masih merupakan topik yang sulit dalam jaringan yang toleran tunda, yang perlu ditangani dengan lebih baik oleh para peneliti. Alasannya pasti lingkungan yang terputus khas DTN. Setiap kali tanda tangan harus diverifikasi, diperlukan perjalanan bolak-balik ujung ke ujung ke pusat atau basis data pencarian yang direplikasi, yang menunda transmisi data aktual. Saat beroperasi di wilayah yang berbeda, otoritas yang saling dipercaya diperlukan. Selain itu, pengelolaan daftar

pencabutan sertifikat sangat menderita karena pembaruan yang dapat ditunda secara berlebihan.

Kontribusi pertama untuk mengembangkan sistem kriptografi praktis untuk DTN didasarkan pada Kriptografi Berbasis Identitas Hierarki (HIBC) [114]. Sistem yang diusulkan adalah digunakan untuk membuat saluran aman, untuk menyediakan autentikasi timbal balik, dan untuk memungkinkan pencabutan kunci. Tidak seperti PKI konvensional, di mana pengguna memperoleh pasangan kunci publik/pribadi dari otoritas sertifikasi, kunci publik dalam Kriptografi Berbasis Identitas dapat berupa

string apa pun, tetapi kunci pribadi diperoleh dari otoritas tepercaya yang disebut Pembuat Kunci Pribadi (PKG). IBC hierarkis memperluas KPI dengan membentuk hierarki kooperatif PKG. Dalam referensi 114, penulis memperkenalkan prosedur untuk pembuatan kunci awal dan roaming di antara wilayah yang berbeda, dan mereka juga menjelaskan teknik sederhana untuk mencegah identitas pengguna disusupi karena kehilangan atau pencurian perangkat seluler. Kriptografi Berbasis Identitas juga digunakan dalam referensi 115 untuk menyediakan tidak hanya komunikasi yang aman tetapi juga anonimitas.

Dalam referensi 116, penggunaan PKI diintegrasikan dengan informasi sosial yang tersedia—pengetahuan tentang afiliasi saat ini dan sebelumnya serta kontak sosial teman sebaya. Gagasan utamanya adalah bahwa beberapa entitas memiliki lebih banyak peluang untuk mengetahui kunci publik entitas lain. Pengetahuan ini digunakan untuk menghubungkan pengguna ke entitas yang lebih menonjol (misalnya institusi atau sekelompok pengguna) yang mungkin memiliki kunci publik yang sudah diketahui oleh pengguna asal.

4.5.3 Ringkasan

Pada bagian ini kami telah memberikan ikhtisar tentang status keamanan saat ini untuk jaringan yang toleran tunda. Ada sejumlah masalah terbuka dalam keamanan DTN. Penerapan mekanisme kriptografi dapat menantang dalam skenario tertentu di mana node mungkin memiliki daya komputasi yang terbatas. Sama pentingnya, bekerja pada manajemen kunci baru benar-benar dimulai sekarang dan standardisasi masih jauh.

4.6 JARINGAN AD HOC KENDARAAN (VANETS)

Karena teknologi informasi dan komunikasi (TIK) semakin meluas, kendaraan diharapkan akan dilengkapi dalam waktu dekat [117.118] dengan perangkat cerdas dan antarmuka radio, yang dikenal sebagai unit on-board (OBU). OBU diizinkan untuk berbicara dengan OBU lain dan infrastruktur sisi jalan yang dibentuk oleh roadside unit (RSU).

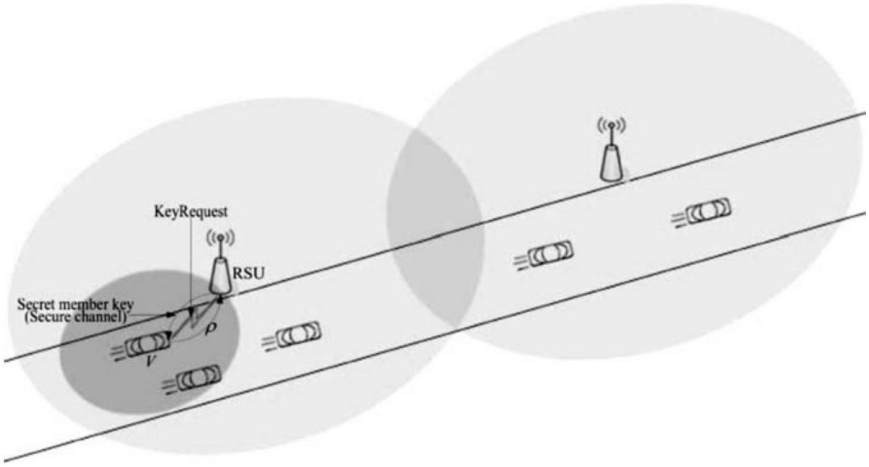
OBU dan RSU, dilengkapi dengan modul sensorik, pemrosesan, dan komunikasi nirkabel on-board, membentuk jaringan yang diatur sendiri dengan kendaraan sebagai node, biasanya disebut sebagai jaringan ad hoc kendaraan (VANET). Gambar 4.5 menggambarkan ruas jalan dengan peralatan VANET.

4.6.1 Kelebihan dan Masalah VANET

Sistem VANET bertujuan menyediakan platform untuk berbagai aplikasi yang dapat meningkatkan keselamatan dan efisiensi lalu lintas, bantuan pengemudi, regulasi transportasi, infotainment, dan sebagainya. Ada penelitian substansial dan upaya industri untuk mengembangkan pasar ini.

Komunikasi kendaraan didukung oleh standar Dedicated Short-Range Communica tions (DSRC)

[119] di AS dan Car2Car Communication Consortium [120] di Eropa. Departemen Perhubungan AS berinvestasi di Connected



Gambar 4.5 Ruas jalan yang mendukung VANET.

Program Penelitian Kendaraan (sebelumnya dikenal sebagai IntelliDrive [121]). Di Eropa, beberapa

proyek seperti SEVECOM [122] dan NoW [123] telah dilaksanakan. Diperkirakan pasar komunikasi kendaraan akan mencapai beberapa miliar euro di tahun-tahun mendatang.

Dorongan utama di balik VANET adalah untuk meningkatkan keamanan dan efisiensi lalu lintas. VANET mengizinkan kendaraan untuk secara otomatis memperingatkan kendaraan terdekat tentang pergerakannya (pengereman, perubahan jalur, dll.) untuk menghindari situasi berbahaya. Pesan peringatan ini hanya memerlukan penyebaran terbatas (kurang dari seratus meter) tetapi memiliki persyaratan waktu nyata yang sangat kuat (harus diproses dengan sangat cepat). VANET juga memungkinkan sebuah mobil mengirimkan pengumuman tentang kondisi jalan (kemacetan lalu lintas, kecelakaan) ke kendaraan lain sehingga kendaraan lain dapat memanfaatkan informasi tersebut untuk memilih rute menghindari titik-titik yang merepotkan. Pesan pengumuman semacam itu membutuhkan jangkauan penyebaran yang lebih panjang. Namun, persyaratan pemrosesan waktu nyata mereka jauh lebih ketat daripada dalam hal peringatan. Kendala waktu luang ini dan daya komputasi OBU memungkinkan penggunaan kriptografi canggih untuk membuat pesan pengumuman aman dan dapat dipercaya.

Sementara manfaat luar biasa yang diharapkan dari komunikasi kendaraan dan jumlah kendaraan yang sangat besar merupakan keunggulan VANET, masih ada masalah untuk menerapkan jaringan semacam itu dalam praktiknya. Yang sangat penting adalah untuk menjamin keamanan pengumuman yang dihasilkan kendaraan. Dalam hal keamanan, kendaraan yang mementingkan diri sendiri mungkin berusaha membersihkan jalan di depan atau mengacaukan jalan di belakang dengan pemberitahuan lalu lintas palsu; penjahat yang dikejar dapat menyebarkan pemberitahuan palsu ke kendaraan lain untuk memblokir mobil polisi. Serangan semacam itu dapat mengakibatkan bahaya serius, bahkan hilangnya nyawa. Masalah lainnya adalah untuk melindungi privasi kendaraan. VANET membuka

jendela besar bagi pengamat. Sangat mudah untuk mengumpulkan informasi tentang kecepatan, status, lintasan, dan keberadaan kendaraan di VANET. pengamat jahat dapat membuat kesimpulan tentang kepribadian pengemudi (misalnya, seseorang yang mengemudi dengan lambat kemungkinan besar adalah orang yang tenang), kebiasaan hidup, dan hubungan sosial (tempat yang dikunjungi menceritakan banyak hal tentang kehidupan orang). Informasi pribadi ini dapat diperdagangkan di pasar bawah tanah, mengekspos kendaraan dan pengemudi yang diamati untuk dilecehkan (misalnya, iklan sampah), ancaman (misalnya, pemerasan jika pengemudi sering mengunjungi tempat yang memalukan, seperti distrik lampu merah), dan bahaya. (misalnya pembajakan). Akhirnya, VANET sangat menarik di daerah perkotaan berpenduduk padat yang diliputi oleh kemacetan lalu lintas dan kecelakaan. Selain kerentanan versus serangan terhadap keamanan lalu lintas dan privasi pengemudi, VANET berskala besar di area metropolitan menimbulkan masalah skalabilitas dan manajemen.

4.6.2 Tujuan dan Tantangan Desain dalam VANET

Konsekuensi dari analisis di atas adalah bahwa tujuan desain VANET adalah sebagai berikut:

• Keamanan. Fungsi keamanan mendasar dalam komunikasi kendaraan terdiri dari memastikan tanggung jawab pencetus paket data. Tanggung jawab menyiratkan bahwa pembuat pesan bertanggung jawab atas pesan yang dihasilkan. Untuk menetapkan tanggung jawab tanpa perselisihan, otentikasi, integritas, dan non-penolakan harus disediakan dalam protokol kendaraan. Otentikasi memungkinkan verifikasi bahwa pesan itu dihasilkan oleh pembuatnya seperti yang diklaim, bukan oleh im personator. Integritas menjamin bahwa pesan tidak dirusak setelah dikirim. Non-repudiation menyiratkan bahwa pembuat pesan tidak dapat menolak kepenulisan pesan. • Privasi. Dalam jaringan nirkabel yang dijelaskan sebelumnya dalam bab ini, privasi sebagian besar mengacu pada kerahasiaan data yang dikirimkan. Di VANET, pesan yang dikirim tidak bersifat pribadi atau rahasia. Privasi dalam konteks VANET mengacu pada anonimitas pengirim pesan. Oleh karena itu, ada privasi jika, dengan memantau komunikasi di VANET, pembuat pesan tidak dapat diidentifikasi, kecuali mungkin oleh pihak yang ditunjuk. Karena autentikasi pesan memerlukan pengetahuan tentang identitas publik seperti kunci publik atau pelat nomor, jika tidak ada anonimitas yang diberikan, penyerang dapat dengan mudah melacak kendaraan apa pun dengan memantau komunikasi VANET. Hal ini tentunya tidak diinginkan oleh para pengendara.

Oleh karena itu, anonimitas harus dilindungi untuk kendaraan yang berperilaku jujur, yaitu tidak menghasilkan pesan yang tidak benar. Kami mencatat bahwa privasi/anonimitas sering diabaikan sebagai tujuan desain dalam jaringan semacam ini, fokus utamanya adalah pada keamanan dan skalabilitas (lihat di bawah).

• Manajemen Skalabel. Untuk VANET yang dikerahkan di area metropolitan padat penduduk, mengelola hingga (puluhan) juta kendaraan merupakan masalah besar.

Secara khusus, dalam VANET sebesar itu, setiap hari beberapa kendaraan terdaftar mungkin dicuri atau kunci rahasianya kadang-kadang bocor. Ini memerlukan beban ekstra untuk mengelola sistem sambil menjaga tanggung jawab dan anonimitas kendaraan. Oleh karena itu, penting untuk mempertimbangkan persyaratan manajemen yang dapat diskalakan saat sistem dirancang.

Menantang untuk secara bersamaan mencapai tujuan desain di atas. Tantangan pertama berasal dari fakta bahwa tanggung jawab dan anonimitas saling bertentangan.

Persyaratan pertanggungjawaban menyiratkan bahwa kendaraan curang yang mendistribusikan pesan palsu harus ditangkap. Di sisi lain, persyaratan anonimitas menyiratkan bahwa penyerang tidak dapat

melacak kendaraan asli yang membuat pengumuman. Oleh karena itu, harus ada pertukaran antara tanggung jawab dan anonimitas dalam VANET. Skema yang dirancang dengan baik harus melindungi privasi kendaraan yang jujur sambil membiarkan identitas kendaraan yang tidak jujur ditentukan.

Volatilitas jaringan adalah faktor lain yang meningkatkan kesulitan mengamankan VANET. Konektivitas antar kendaraan seringkali sangat sementara karena kecepatannya yang tinggi (misalnya, pikirkan tentang dua kendaraan yang saling bersilangan dalam arah yang berlawanan di jalan raya). Ini menyiratkan bahwa protokol yang membutuhkan banyak putaran atau kerja sama yang kuat seperti mekanisme pemungutan suara mungkin tidak praktis. Karena mobilitasnya yang tinggi, kendaraan mungkin tidak akan pernah lagi terhubung satu sama lain setelah satu kali koneksi. Hal ini menempatkan infrastruktur kunci publik yang diterapkan untuk mengamankan VANET di bawah tekanan: Jika sertifikat kunci publik digunakan, kendaraan dihadapkan pada banyak sertifikat yang mungkin dikeluarkan oleh beberapa otoritas sertifikasi (CA) yang berbeda; karena mobilitas, ada sedikit harapan bahwa menyimpan sertifikat kendaraan dan CA yang terverifikasi akan menghasilkan percepatan verifikasi berikutnya yang signifikan.

Kompleksitas VANET yang diterapkan di wilayah metropolitan merupakan tantangan lain.

Sistem transportasi diatur oleh konstelasi otoritas dengan kepentingan berbeda, yang memperumit banyak hal. Solusi yang meyakinkan secara teknis, dan mungkin politis, merupakan prasyarat untuk arsitektur keamanan apa pun.

Last but not least, skala besar jaringan kendaraan juga menantang: Sistem harus mengelola (puluhan) juta node yang beberapa mungkin bergabung atau meninggalkan VANET sesekali dan beberapa mungkin dikompromikan. Ini mengesampingkan protokol yang membutuhkan distribusi data besar-besaran ke semua node seluler. Selanjutnya, dalam kasus kepadatan kendaraan yang tinggi di wilayah metropolitan, setiap node dapat dibanjiri dengan sejumlah besar pesan masuk yang memerlukan verifikasi.

4.6.3 Skalabilitas dan Integritas Layanan di VANET

Seperti disebutkan di atas, skalabilitas merupakan tantangan dalam VANET dan memiliki sejumlah konsekuensi. Banyaknya jumlah kendaraan dan RSU dalam VANET berperilaku simultan sebagai sumber informasi dan tujuan. Cara untuk memastikan skalabilitas dengan bandwidth yang tersedia adalah dengan mengumpulkan informasi yang ditransmisikan saat berpindah antara sumber dan

tujuan. Dalam referensi 124 terbukti bahwa setiap skema agregasi yang sesuai harus mengurangi bandwidth di mana informasi tentang suatu area pada jarak diberikan ke mobil secara asimtotik lebih cepat dari 1/d2. Selain itu, penulis menunjukkan bahwa ikatan ini ketat: Untuk sembarang > 0, terdapat skema agregasi yang dapat diskalakan yang mereduksi informasi secara asimtotik seperti 1/d2+.

Saat menambahkan keamanan ke VANET (lihat Bagian 4.6.4 di bawah), bandwidth tambahan diperlukan, karena sejumlah tanda tangan digital perlu ditambahkan ke setiap pesan: satu tanda tangan untuk pembuat pesan dan mungkin tanda tangan lain untuk setiap kendaraan yang mendukung kebenaran pesan. isi pesan. Jika tanda tangan dan sertifikat kunci publik terkait digabungkan, seperti yang diusulkan dalam referensi 125, ukuran pesan VANET meningkat secara linier dengan jumlah endorser. Jika oversignatures digunakan—yaitu, setiap tanda tangan baru menandatangani tanda tangan sebelumnya alih-alih ditambahkan padanya—pemverifikasi hanya dapat memverifikasi tanda tangan oleh penanda tangan terakhir, tetapi bukan tanda tangan sebelumnya. Dalam referensi 126, sistem OBU berbasis kartu pintar diusulkan di mana tanda tangan dari originator dan endorser dapat

digabungkan untuk menghemat ruang. Dalam referensi 127, tanda tangan ambang digunakan yang memungkinkan penggabungan banyak tanda tangan pengesahan sebagian menjadi satu tanda tangan standar.

Meskipun demikian, tanda tangan yang dibahas sejauh ini memerlukan sertifikat kunci publik untuk ditambahkan ke tanda tangan, yang sebenarnya menyiratkan pertumbuhan linier dalam panjang pesan. Menggunakan kriptografi berbasis identitas adalah cara yang efektif untuk menghindari kebutuhan sertifikat kunci publik dan mendapatkan pesan dengan panjang tetap (lihat Bagian 4.6.4 di bawah dan referensi 128).

Di luar agregasi pesan, ada beberapa aturan sederhana untuk mengurangi jumlah pesan yang dibuat dan diverifikasi di VANET:

• Kendaraan tidak boleh menghasilkan pesan baru yang melaporkan informasi yang sama dengan pesan yang sebelumnya didukung oleh kendaraan yang sama. • Kendaraan tidak boleh memverifikasi pesan yang melaporkan informasi yang sama dengan pesan yang diverifikasi sebelumnya. Karena bandwidth adalah sumber daya yang langka di VANET, serangan DoS yang ditujukan untuk meruntuhkan kinerja jaringan dan mengalahkan integritas layanan menjadi perhatian khusus. Dalam serangan DoS, penyerang menghentikan media komunikasi utama dan jaringan tidak lagi tersedia untuk pengguna yang sah. Serangan DoS dapat diarahkan untuk mengganggu komunikasi dengan RSU tertentu (serangan kendaraan ke infrastruktur atau V2I DoS) atau untuk mengganggu media komunikasi antara kendaraan di suatu area (serangan kendaraan ke kendaraan atau V2V DoS). Serangan Denial of Service Terdistribusi (DDoS) adalah serangan DoS yang diluncurkan dari beberapa lokasi (biasanya beberapa kendaraan); mereka lebih berbahaya daripada DoS oleh satu kendaraan karena penyerang dapat mengoordinasikan dan mengirim pesan dari berbagai jenis pada waktu yang berbeda (lihat referensi 129 untuk detail lebih lanjut tentang serangan).

4.6.4 Keamanan dan Privasi di VANET

Agar VANET dapat berfungsi, persyaratan pertama adalah menjaganya dari informasi yang salah. Sebagai contoh, seorang penyerang dapat dengan mudah meletakkan sepotong es pada sensor suhu kendaraan dan kemudian suhu yang salah akan dilaporkan, bahkan jika sensor perangkat keras anti rusak. Untuk menangkal penipuan data, diperlukan mekanisme pendeteksian.

Skema umum yang bertujuan untuk mendeteksi dan mengoreksi data berbahaya diberikan oleh Golle et al. pada tahun 2004 [130]. Penulis berasumsi bahwa penjelasan paling sederhana dari beberapa

ketidakkonsistenan dalam informasi yang diterima kemungkinan besar adalah penjelasan yang benar.

..

Proposal khusus dibuat oleh Leinmuller et al. pada tahun 2006 [131] berfokus pada verifikasi data posisi yang dikirim oleh kendaraan. Semua informasi posisi yang diterima dari kendaraan disimpan untuk beberapa periode waktu; ini digunakan untuk melakukan pemeriksaan, yang hasilnya diberi bobot untuk membentuk metrik pada kepercayaan tetangga. Raya dkk. [125] dan Daza dkk. [127] memperkenalkan mekanisme ambang batas untuk mencegah generasi pesan penipuan: Sebuah pesan diberikan kredit hanya jika didukung oleh ambang batas kendaraan di sekitarnya.

Selain menjamin kebenaran pengumuman kendaraan, VANET juga harus memberikan otentikasi untuk menetapkan tanggung jawab untuk pencegahan, investigasi, deteksi, dan penuntutan tindak pidana berat. Untuk memenuhi persyaratan ini, komunikasi kendaraan harus ditandatangani untuk

memberikan otentikasi, integritas, dan non-penolakan sehingga dapat dikumpulkan sebagai bukti yudisial. Beberapa proposal (misalnya, referensi 132–136) menyarankan penggunaan infrastruktur kunci publik (PKI) dan tanda tangan digital untuk mengamankan VANET. Untuk mengusir kendaraan nakal, Raya et al. protokol yang diusulkan lebih lanjut bertujuan untuk mencabut sertifikasi kendaraan berbahaya [137]. Tantangan besar yang muncul dari skema berbasis PKI di VANET adalah beban berat pembuatan, penyimpanan, pengiriman, verifikasi, dan pencabutan sertifikat.

Untuk menjamin privasi kendaraan, beberapa proposal menyarankan otentikasi anonim di VANET. Di antara mereka ada dua jalur penelitian — yaitu, mekanisme nama samaran dan tanda tangan kelompok.

Nama samaran sebuah node adalah kunci publik berumur pendek yang diautentikasi oleh otoritas sertifikat (CA) dalam PKI kendaraan [138–140]. Pendekatan nama samaran terutama berfokus pada seberapa sering sebuah node harus mengubah nama samaran dan dengan siapa ia harus berkomunikasi. Sampigethaya dkk. [141] mengusulkan untuk menggunakan periode diam untuk menghambat keterkaitan antara nama samaran, atau sebagai alternatif untuk membuat grup kendaraan dan membatasi kendaraan dalam satu grup untuk mendengarkan pesan dari grup lain. Untuk menghindari pengiriman dan penyimpanan sejumlah besar nama samaran, Calandriello et al.

[142] mengusulkan nama samaran yang dihasilkan sendiri dengan bantuan tanda tangan kelompok yang diproduksi secara lokal oleh kendaraan.

Satu masalah dengan mekanisme anonimitas sederhana di VANET adalah apa yang disebut serangan Sybil atau "ilusi": satu kendaraan dapat menyalahgunakan anonimitas untuk meniru beberapa kendaraan dan menghasilkan serta memberikan beberapa dukungan untuk pesan yang melaporkan informasi palsu. Dalam referensi 127, tanda tangan ambang batas digunakan untuk memberikan anonimitas saat menggagalkan serangan Sybil: Setidaknya jumlah tanda tangan parsial yang berasal dari berbagai kelompok kendaraan diperlukan untuk mendukung pesan, sehingga satu kendaraan tidak dapat mendukung sendiri sebuah pesan . Mencatat bahwa tanda tangan grup dapat langsung digunakan untuk mengotentikasi komunikasi kendaraan secara anonim tanpa menghasilkan nama samaran tambahan, Guo et al. [143] mengusulkan kerangka kerja keamanan berbasis tanda tangan grup yang bergantung pada perangkat tahan gangguan (memerlukan akses kata sandi) untuk mencegah serangan permusuhan pada jaringan kendaraan. Namun, tidak ada instantiasi konkret maupun hasil simulasi yang disediakan. Lin dkk. [144]

memperkenalkan protokol keamanan dan pelestarian privasi untuk VANET dengan mengintegrasikan teknik tanda tangan grup. Dengan bantuan tanda tangan grup, komunikasi kendaraan-ke-kendaraan (V2V) diautentikasi dengan tetap menjaga privasi bersyarat. Wu dkk. [145] membedakan keterhubungan dan anonimitas tanda tangan grup untuk meningkatkan kepercayaan pesan yang dihasilkan oleh kendaraan.

Beberapa proposal terbaru menyediakan otentikasi untuk menetapkan kewajiban dan privasi kendaraan di VANET. Saat skema ini diimplementasikan dalam VANET skala besar

di daerah perkotaan yang padat penduduk, tantangan yang belum tertangani tetap ada. Skema berbasis samaran menghadapi tantangan untuk menghasilkan, mendistribusikan, memverifikasi, dan menyimpan sejumlah besar sertifikat. Skema berbasis tanda tangan kelompok dalam pengaturan PKI konvensional menghadapi masalah seperti bagaimana mengelola banyak kendaraan dan khususnya kendaraan yang disusupi. Perhatian umum dari kedua kelas skema ini adalah bagaimana memproses sejumlah besar pesan yang diterima setiap satuan waktu.

Pengamatan ini membutuhkan mekanisme baru untuk mengatasi tantangan ini dengan cara

yang efisien. Dengan mempertimbangkan tantangan ini, makalah baru-baru ini [128] mengusulkan seperangkat mekanisme untuk mengatasi persyaratan keamanan, privasi, dan manajemen

dalam VANET skala besar. Kekhawatiran yang saling bertentangan ini didamaikan dengan mengeksploitasi tanda tangan grup berbasis identitas (IBGS) dan membagi VANET berskala besar menjadi beberapa grup kecil yang mudah dikelola. Dalam sistem, masing-masing pihak, termasuk manajer grup (yaitu, kantor transportasi) dan penandatangan (yaitu, kendaraan), memiliki identitas unik yang dapat dikenali manusia sebagai kunci publiknya, bersama dengan kunci rahasia terkait yang dihasilkan oleh beberapa otoritas tepercaya. Sebagai contoh, kunci publik dari kantor administrasi, unit pinggir jalan [146] dan kendaraan masing-masing dapat berupa nama administrasi, alamat geografis RSU dan pelat nomor kendaraan tradisional.

Sertifikat tidak lagi diperlukan karena kunci publik masing-masing pihak adalah identitas yang dapat dikenali manusia. Fitur ini sangat mengurangi tantangan manajemen terkait keamanan.

Dalam referensi 128, setelah mendaftar ke kantor transportasi, kendaraan apa pun dapat mengautentikasi pesan apa pun secara anonim. Pesan yang dihasilkan oleh kendaraan ini dapat diverifikasi dengan identitas (misalnya, nama) dari kantor transportasi dan kunci publik dari otoritas escrow. Jika suatu pesan kemudian diketahui palsu, identitas pembuat pesan dapat dilacak oleh petugas polisi lalu lintas. Mempertimbangkan redundansi dalam komunikasi kendaraan, mekanisme verifikasi egois disajikan untuk mempercepat pemrosesan pesan di VANET. Dengan teknik ini, meskipun setiap kendaraan dapat menerima sejumlah besar pesan, kendaraan tersebut hanya memilih untuk verifikasi pesan-pesan yang mempengaruhi keputusan lalu lintasnya. Pesan yang dipilih dapat diverifikasi dalam satu batch seolah-olah itu adalah satu pesan. Mekanisme percepatan ini sangat penting untuk menyebarkan VANET di daerah perkotaan yang padat penduduk.

4.6.5 Ringkasan dan Informasi Lebih Lanjut

Kami telah menjelaskan secara singkat apa itu VANET dan kami telah memotivasi peluang dan masalah yang terkait dengan penerapannya. Meskipun jenis jaringan yang diatur sendiri ini memiliki potensi besar untuk meningkatkan keamanan lalu lintas, ini juga memerlukan tantangan keamanan, privasi, dan skalabilitas yang penting. Tidak seperti di jaringan ad hoc nirkabel lain sebelumnya, yang dibahas dalam bab ini, privasi VANET mengacu pada anonimitas pengirim daripada kerahasiaan data. Kami telah membahas skalabilitas dan integritas layanan, yaitu bagaimana menghemat bandwidth untuk meningkatkan skalabilitas dan bagaimana serangan denial-of-service dapat memengaruhi ketersediaan bandwidth di VANET. Terakhir, kami

mengakhiri bagian ini dengan ikhtisar solusi keamanan dan privasi untuk jaringan kendaraan yang diusulkan dalam literatur.

Lihat referensi 118 untuk survei perkembangan terkini pada jaringan area kendaraan, termasuk VANET dan juga komunikasi intra-kendaraan. Di http://vanet.info

informasi situs web tentang penelitian VANET saat ini dan tautan ke konferensi tahunan penting tentang topik ini dapat ditemukan (misalnya Konferensi Jaringan Kendaraan VNC- IEEE, ACM VANET, Keamanan Otomotif). Jurnal penting di bidang ini adalah Transaksi IEEE pada Teknologi Kendaraan dan Transaksi IEEE pada Sistem Transportasi Cerdas.

4.7 KESIMPULAN DAN MASALAH PENELITIAN TERBUKA

Jaringan ad hoc nirkabel adalah nama payung yang mengumpulkan teknologi jaringan yang sangat beragam dengan fitur umum yang dapat diatur sendiri dan nirkabel. Dua fitur yang menentukan ini adalah kekuatan dan kelemahan dari teknologi tersebut:

• Sisi positifnya, jaringan ad hoc nirkabel sangat fleksibel, relatif murah, dan sangat mudah digunakan, yang menjelaskan momentum dan popularitasnya yang besar baik untuk aplikasi sipil maupun militer.

• Sisi negatifnya, jaringan tersebut sangat rentan terhadap serangan terhadap ketersediaan, integritas

layanan, keamanan, dan privasi; memang, mengandalkan komunikasi radio memfasilitasi penyadapan, intersepsi dan serangan DoS dan topologi yang diatur sendiri tanpa kontrol terpusat rentan terhadap serangan terhadap autentikasi, seperti replikasi node, penekanan node, peniruan node, dan sebagainya.

Di luar pro dan kontra umum di atas, ada keragaman besar dalam teknologi ad hoc nirkabel. Di ujung bawah, kami menemukan jaringan sensor, yang simpulnya memiliki pasokan energi dan daya komputasi yang sangat terbatas. Di ujung atas, jaringan kendaraan memiliki kendaraan sebagai simpul dan unit terpasang kendaraan adalah komputer lengkap dengan catu daya yang besar. Terlepas dari keragaman di atas, agregasi data dan enkripsi berguna untuk mengurangi masalah skalabilitas dan kerentanan semua jaringan ad hoc nirkabel. Untuk jaringan low-end, kriptografi simetris adalah pilihan yang lebih disukai, sedangkan kriptografi kunci publik, termasuk kriptografi grup dan threshold, dapat diberikan pada jaringan high-end.

Tantangan penelitian bergantung pada masing-masing teknologi jaringan tertentu dan telah diidentifikasi di bagian terkait. Namun, ada beberapa masalah yang memerlukan penelitian lebih lanjut yang meliputi beberapa jaringan yang dijelaskan. Ini termasuk membuat keamanan dan privasi kompatibel dengan skalabilitas, meningkatkan efisiensi

bandwidth, melawan serangan DoS, menangani mobilitas node, dan juga mencapai standardisasi di seluruh dunia.

CHAPTER 5 SOLUSI ARSITEKTUR UNTUK MOBILITAS PENGGUNA AKHIR

5.1 PENDAHULUAN

Jaringan mesh nirkabel (WMN) semakin menjadi salah satu arsitektur jaringan yang fleksibel dan hemat biaya untuk menyediakan jangkauan jaringan nirkabel area luas.

Dalam WMN, titik akses dihubungkan oleh tulang punggung nirkabel dan, pada gilirannya, dapat terhubung ke jaringan berkabel atau nirkabel lain, atau langsung ke pengguna akhir. Ketika ponsel pengguna bergerak di luar area jangkauan titik akses dan terhubung ke titik yang lebih dekat, perubahan konektivitas melibatkan transisi (handoff atau handover), sebelum dapat merutekan lalu lintas secara mulus melalui titik akses baru. Selama perubahan rute, paket untuk aliran tertentu mungkin mengalami penundaan yang lama. Selain itu, paket mungkin hilang karena informasi perutean yang sudah ketinggalan zaman. Akibatnya, kualitas dan kinerja aplikasi pengguna mungkin menurun. Oleh karena itu, proses handoff melibatkan banyak lapisan jaringan. Meskipun mendukung mobilitas pengguna dalam WMN merupakan persyaratan penting, saat ini tidak ada solusi handoff standar yang efisien dan transparan untuk WMN. Standar saat ini, pada kenyataannya, hanya berfokus pada isu-isu tertentu atau tidak dioptimalkan untuk arsitektur WMN. Namun, dalam literatur beberapa solusi telah diusulkan untuk mendukung dan mengoptimalkan proses serah terima di WMN, dan beberapa di antaranya memanfaatkan standar.

Mobilitas juga telah dieksplorasi sejak awal penelitian jaringan sensor. Namun, masih sangat jarang untuk menemukan penerapan jaringan sensor tradisional di dunia nyata, dan potensinya masih belum dijelajahi. Oleh karena itu, hanya beberapa solusi arsitektur penggunaan umum untuk mobilitas yang telah diusulkan, dan sebagian besar penelitian telah dikonsentrasikan pada protokol dan algoritme untuk mendukung mobilitas.

Mobilitas juga merupakan fitur yang memungkinkan di OppNets, seperti yang diilustrasikan dengan baik di Bab 10 dan 11.

Pada bagian selanjutnya, pertama-tama kita berkonsentrasi pada protokol untuk mengoptimalkan fase spesifik dari proses serah terima dan arsitektur untuk dukungan handoff cepat mulus untuk WMN, lalu kita membahas mobilitas dalam jaringan sensor nirkabel (WSN) dan kita meninjau dua kerangka paling umum untuk dukungan mobilitas dalam WSN. Kami menggambarkan properti, kelebihan dan kekurangan mereka dan membandingkannya satu sama lain.

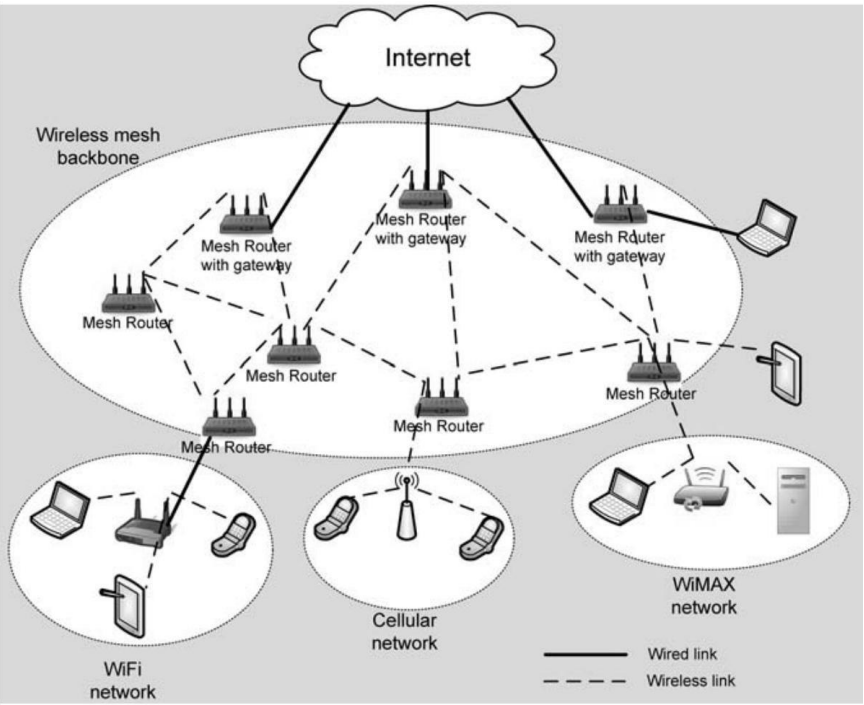
5.2 JARINGAN MESH

WMN adalah kombinasi dari node tetap dan seluler yang saling terhubung melalui tautan nirkabel

untuk membentuk jaringan ad hoc multihop (MANET), di mana perangkat pengguna adalah bagian aktif dari jaringan dan bergabung secara dinamis, bertindak sebagai terminal pengguna dan router untuk perangkat lain. Mereka berbeda dari MANET yang terisolasi dan dikonfigurasi sendiri karena jaringan tidak lagi terbuat dari perangkat pengguna tanpa infrastruktur, tetapi secara fleksibel dan hemat biaya memperluas jaringan infrastruktur kabel, hidup berdampingan dengan mereka [1].

WMN biasanya terdiri dari berbagai jenis entitas: gateway, router mesh, access point (AP), dan klien mesh [2] (Gambar 5.1). Gateway adalah titik koneksi ke jaringan kabel (biasanya Internet). Klien mesh adalah pengguna terminal yang tidak memiliki atau fungsi perutean terbatas. AP nirkabel adalah entitas yang bertanggung jawab atas akses nirkabel untuk klien mesh. Router mesh stasioner (MR), menyediakan layanan transportasi nirkabel ke data, membentuk tulang punggung multihop nirkabel dengan teknik nirkabel kecepatan tinggi jarak jauh (misalnya, WiMAX, 802.11s, atau 802.11a). Mereka dapat memiliki banyak antarmuka radio, beroperasi di saluran yang berbeda. Router mesh dan titik akses juga bisa bergerak: mobilitas stasiun mesh dibahas

lebih detail di Bab 2. MR sering menyediakan fungsi gateway dan bridge, sehingga memungkinkan



Gambar 5.1 Arsitektur jaringan mesh nirkabel.

integrasi WMN dengan jaringan nirkabel yang sudah ada (misalnya seluler, WiFi, jaringan sensor).

5.2.1 Teknologi Mesh dan Mobilitas Pengguna Akhir

Klien konvensional dengan antarmuka Ethernet dapat dihubungkan ke MR melalui tautan Ethernet. Untuk klien konvensional dengan teknologi radio yang sama dengan MR, mereka dapat langsung berkomunikasi dengan MR. Antarmuka WiMAX tidak tersedia untuk klien, sehingga teknologi ini tidak dapat digunakan untuk menangani mobilitas pengguna akhir.

WMN pada dasarnya mendiversifikasi kemampuan jaringan ad hoc. Fitur ini memberikan banyak keuntungan bagi WMN, seperti biaya instalasi yang rendah, pemeliharaan jaringan yang mudah, kekokohan, jangkauan layanan yang andal, dan sebagainya. Namun, untuk distribusi massal WMN, upaya penelitian yang cukup besar masih diperlukan. Ketika mobile client dari WMN stasioner, paket direlay melalui MR dan ke/dari gateway dengan dukungan dari backbone routing. Namun, masalah teknis mungkin muncul ketika ada kebutuhan klien mesh untuk bergerak melintasi area cakupan

jaringan mesh. Saat pengguna menjauh dari jangkauan node WMN, mungkin ada kekurangan dukungan sakelar otomatis di lapisan jaringan. Selain itu, bahkan jika beberapa solusi khusus untuk sakelar otomatis disediakan, tidak ada jaminan aplikasi tersebut akan tetap bekerja dengan baik. Oleh karena itu, tantangan utama terdiri dari penyediaan konektivitas tanpa batas dan berkelanjutan dengan QoS yang dibutuhkan oleh aplikasi pengguna, mengingat karakteristik yang berbeda (dalam hal cakupan, bandwidth, biaya, dll.) dari berbagai jaringan yang tersedia. Ini adalah aspek yang gagal ditangani oleh standar saat ini.

Misalnya, Mobile IP [3] hanya berfokus pada menjaga identitas IP klien seluler, sementara mengabaikan aspek lain dari proses handoff, seperti biaya komputasi yang rendah dan latensiyang singkat. Ekstensi IEEE 802.21 [4] untuk WMN masih terus dikerjakan. Versi standar untuk jaringan mesh WLAN saat ini—802.11s—tidak menentukan mekanisme protokol apa pun yang mendukung handoff cepat untuk klien seluler yang menjalankan aplikasi real-time seperti voice over IP (VoIP). Selain itu, ketika WLAN AP bersifat mobile, masalah fast handoff menjadi lebih menantang dan menuntut solusi yang efisien melalui IP (VoIP).

Untuk mengatasi keterbatasan ini, beberapa pendekatan telah diusulkan dalam literaturuntuk mendukung mobilitas tanpa batas di WMN. Berikut ini kami sajikan yang paling representatif.

5.2.2 Definisi dan Tantangan

Secara umum, dukungan mobilitas pengguna akhir yang mulus membutuhkan penyediaan mekanisme untuk terminal untuk mempertahankan identitas yang sama terlepas dari titik lampiran jaringannya, tanpa mengganggu sesi jaringan aktif apa pun dan menghindari atau meminimalkan intervensi pengguna. Ini menyiratkan mendukung penyerahan (atau penyerahan) antara penyedia jaringan dan teknologi yang berbeda.

Mobilitas mulus di WMN harus memperhitungkan pergerakan pada dua tingkat yang berbeda: intradomain atau mikromobilitas (antara AP/domain yang sama) dan interdomain atau mobilitas makro (antara AP yang terhubung ke Internet/domain yang berbeda). Selain itu, karena infrastruktur WMN dapat menyediakan konektivitas ke berbagai jenis jaringan seperti WiFi, WiMAX, seluler, dan jaringan sensor, mobilitas memerlukan dukungan serah terima vertikal (antar jenis jaringan yang berbeda) dan horizontal (antar jaringan dengan jenis yang sama) tanpa hambatan.

Proses serah terima secara praktis dapat dipecah menjadi tiga blok fungsional:

Inisiasi Handoff. Pemantauan proaktif koneksi saat ini dan/atau kemungkinan koneksi alternatif untuk (i) secara efektif mengantisipasi atau secara eksplisit menangani hilangnya konektivitas, (ii) memicu serah terima alternatif untuk mengoptimalkan biaya dan kinerja.

Pilihan jaringan. Pemilihan titik koneksi baru sesuai dengan metrik keputusan seperti kualitas sinyal, biaya, bandwidth, dan sebagainya. Informasi tentang metrik ini dapat dikumpulkan secara proaktif dan/atau reaktif.

Eksekusi serah terima. Serangkaian prosedur yang harus dilakukan untuk otentikasi dan reasosiasi klien seluler (prosedur switching).

Penyerahan klien seluler dikatakan dieksekusi jaringan jika sepenuhnya di bawah kendali jaringan (seperti halnya antara sel UMTS/GSM/GPRS).

Dalam serah terima yang dieksekusi seluler , keputusan serah terima diambil secara mandiri oleh klien seluler. Penyerahan dapat berupa (a) lunak saat dilakukan hanya untuk tujuan pengoptimalan biaya koneksi atau QoS atau (b) keras saat dilakukan karena hilangnya konektivitas dalam waktu dekat.

Manajemen mobilitas terkait erat dengan banyak lapisan protokol jaringan.

Sebagian besar pekerjaan pada mobilitas adalah skema handoff Layer-2 dan Layer-3. Skema handoff layer 2 bertujuan mengurangi waktu untuk inisiasi handover (biasanya, penundaan pemindaian) untuk membuat latensi handoff dapat ditoleransi untuk aplikasi real-time, sementara skema handoff Layer-3 mencoba mengurangi latensi pembaruan perutean dan memulihkan konektivitas Layer 3 hampir secara bersamaan ke konektivitas Layer-2 setelah handoff.

Sebagian besar skema yang diusulkan untuk manajemen mobilitas mengikuti pola umum: deteksi gerakan pada Layer-3 atau di bawahnya, pemilihan titik lampiran berikutnya, penemuan dan konfigurasi alamat IP baru, pensinyalan untuk pengalihan paket data yang masuk. Solusi yang efisien untuk WMN adalah solusi yang menyediakan transparansi dan latensi serah terima yang rendah, kokoh sehubungan dengan berbagai situasi, dapat diskalakan dengan baik, meminimalkan biaya pengguna dan penggunaan sumber daya, menyediakan dukungan QoS, dan dapat berdampingan dengan protokol dan teknologi saat ini.

Solusi yang kami sajikan selanjutnya dikelompokkan menurut klasifikasi mikro dan makromobilitas dan menggunakan definisi yang diberikan di atas. Pendekatan yang kami ikuti adalah mendeskripsikan fitur-fitur utama terlebih dahulu, kemudian membuat daftar keuntungan dan kerugian, dan terakhir, memberikan deskripsi solusi yang lebih mendetail.

5.2.3 Dukungan Mikromobilitas

Pada bagian ini kami menyajikan arsitektur pendukung mobilitas mikro. Kami memulai survei kami dengan menjelaskan SyncScan (Sinkronisasi Pemindaian) [5].

5.2.3.1 SyncScan

SyncScan mengusulkan pendekatan perangkat klien Layer-2 untuk handoff tradomain di jaringan mode infrastruktur 802.11. SyncScan berfokus pada minimalisasi waktu untuk inisiasi handoff. Ini dicapai dengan memindai secara berkala saluran 802.11 untuk suar dari titik akses. Dengan cara ini, jika klien memutuskan bahwa handoff diperlukan, ia memiliki daftar AP terbaru dan salurannya dan dapat melewati fase pemindaian. Ini menghasilkan minimalisasi latensi serah terima, karena biaya serah terima dikurangi menjadi biaya autentikasi dan reasosiasi.

SyncScan memerlukan sinkronisasi global waktu suar. Pendekatan yang sangat sederhana untuk mendapatkan akurasi jam yang tinggi di AP adalah dengan memanfaatkan layanan Network Time Protocol (NTP) [6] melalui Internet. Saat klien SyncScan pertama kali dimulai, secara eksplisit disinkronkan dengan semua AP yang tersedia dengan menunggu dua suar di setiap saluran dan mencatat waktu kedatangan dan frekuensi suar mereka. Dari waktu awal ini, ia menghitung jadwal waktu pemindaian.

Karena klien, saat melakukan pemindaian saluran berkala, tidak dapat menerima bingkai dari AP yang terhubung dengannya, klien menginformasikan kepada AP bahwa klien sedang memasuki mode hemat daya (PSM). Ini akan menyebabkan AP menyangga frame keluar ke klien sampaiklien kembali ke saluran. Demikian pula, klien menyangga bingkai keluarnya untuk AP hingga kembali ke saluran.

SyncScan memerlukan penginstalan daemon di sisi klien. Daemon ini, yang mengimplementasikan algoritme SyncScan itu sendiri, memberi tahu kartu antarmuka jaringan nirkabel (NIC) kapan harus berpindah saluran, mengumpulkan beacon, dan mencegat bingkai manajemen yang diperlukan untuk menyelesaikan handoff (misalnya, bingkai asosiasi dan autentikasi).

Selain manfaat paling nyata yang diperoleh dari pengurangan latensi handoff, pemindaian berkelanjutan SyncScan dapat menemukan keberadaan AP dengan SNR yang lebih kuat bahkan sebelum sinyal AP terkait menurun di bawah ambang batas.

Hal ini memungkinkan penyerahan dilakukan lebih awal, sehingga meningkatkan kualitas konektivitas klien.Syncscan diimplementasikan menggunakan perangkat keras komoditi 802.11, dan kinerjanya dievaluasi dengan Skype, yang menggunakan paket UDP untuk komunikasi suara.

Eksperimen menunjukkan bahwa dengan SyncScan tidak ada kehilangan paket selama penyerahan. Selain itu, tidak ada variasi yang signifikan dalam waktu antar kedatangan paket yang diterima saat klien melakukan handoff. Terakhir, transfer FTP dari file yang sama melalui SyncScan dan mode infrastruktur normal 802.11 menunjukkan bahwa dampak pemindaian Sinkronisasi terhadap throughput dapat diabaikan.

5.2.3.2 Handoff Berbasis Agen Seluler.

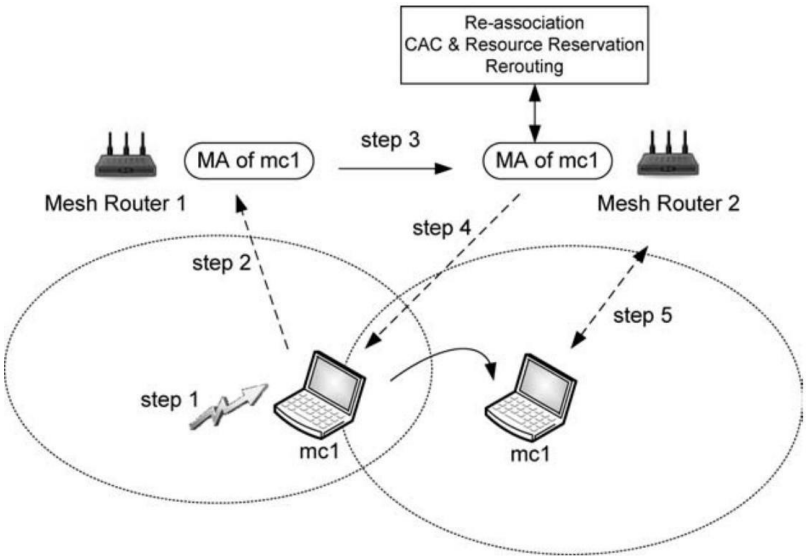
Skema mikromobilitas kedua disajikan dalam referensi 7, di mana penulis menjelaskan pendekatan handoff berbasis mobile agent (MA) untuk menangani mikromobilitas horizontal di WMN dan secara khusus mendukung panggilan VoIP dan aplikasi real- time lainnya. Skema mereka menetapkan setiap klien mesh MA yang berada di router mesh terpasang (MR). Jika klien mesh pindah ke lokasi baru dan mengubah MR-nya, MA juga bermigrasi. Khususnya, jika klien mesh bermaksud untuk melakukan handoff, klien MA akan pindah ke MR baru sebelumnya dan menyiapkan koneksi cadangan untuk panggilan handoff. Setelah itu, klien mesh akan menyelesaikan proses handoff dan melanjutkan panggilan pada koneksi cadangan. Untuk menjamin kualitas layanan (QoS) selama handoff, penulis mengembangkan kebijakan ambang proporsional optimal bandwidth efektif terstruktur (PTOEB) untuk kontrol penerimaan panggilan (CAC) [8] pada MR. Kebijakan ini mengadopsi struktur ambang batas proporsional, memberikan panggilan handoff dan panggilan baru prioritas yang berbeda, dan mendapatkan probabilitas pemblokiran rata-rata yang rendah. Karena sulit menemukan kebijakan secara tepat, algoritma genetika (GA) digunakan sebagai pendekatan komputasi tercepat untuk mencapai solusi yang hampir optimal.

Keuntungan utama dari pendekatan ini adalah penundaan handoff secara keseluruhan hanya melibatkan penundaan pendaftaran, yang dihabiskan untuk pertukaran informasi autentikasi antara klien mesh dan MR baru. Selain mengurangi delay handoff, handoff berbasis MA juga dapat mencapai efisiensi komputasi yang tinggi. MA klien mengeksekusi logika handoff pada MR di mana sumber daya komputasi jaringan berlimpah dan, dengan demikian, melepaskan beban pada klien mesh, yang didedikasikan untuk menjalankan aplikasi pengguna.

Pendekatan berbasis MA yang diusulkan dikombinasikan dengan skema pemindaian proaktif.

Seperti yang ditunjukkan pada Gambar 5.2, setiap klien mesh diberikan "klien MA". Klien mesh (mc1) menempatkan MA kliennya di MR yang didaftarkannya. Proses handoff terdiri dari lima langkah.

Pertama, pemicu pemindaian skema pemindaian proaktif mengaktifkan pemindaian saluran, yang menempatkan MR baru untuk handoff. Kedua, klien mesh akan menginformasikan MA kliennya tentang MR saat ini mana yang merupakan MR baru.



Gambar 5.2 Proses handoff berbasis MA.

MR mentransfer MA klien ke MR baru di lingkungan sekitar, dan MA klien akan melakukan pra-penyiapan koneksi cadangan pada MR baru untuk mempersiapkan handoff yang lancar. Pra-penyiapan koneksi cadangan biasanya melibatkan reasosiasi untuk pengalihan konteks antara titik akses lama (AP) dan AP baru oleh protokol titik akses antar [9], interaksi dengan modul CAC untuk reservasi sumber daya, dan negosiasi dengan perutean protokol untuk pembentukan kembali jalur lapisan jaringan. Keempat, setelah koneksi cadangan dibuat, MA klien akan memberi tahu klien mesh bahwa ia siap untuk handoff. Akhirnya, klien mesh menerima notifikasi dan menunggu api pemicu handoff untuk mendaftar ke MR baru dan menyelesaikan handoff.

Untuk memberikan layanan yang dijamin QoS kepada pengguna seluler, penulis mengusulkan kebijakan CAC. CAC adalah proses menerima/menolak panggilan baru yang berasal dari cakupan MR tertentu, atau panggilan handoff yang berpindah ke dalam cakupan MR tertentu, sambil memastikan layanan koneksi yang ada tidak terputus. Ini bertujuan untuk memaksimalkan jumlah sesi yang diterima sambil memenuhi persyaratan QoS mereka. Secara tradisional, CAC digunakan dalam jaringan seluler dan mempertimbangkan alokasi saluran. Di WMN, CAC terutama mempertimbangkan alokasi bandwidth. Selain itu, dalam lingkungan handoff WMN, masalah prioritas yang berbeda harus dipertimbangkan.

Artinya, panggilan handoff harus diberikan preferensi lebih dari panggilan baru dalam proses CAC, karena pengguna jauh lebih sensitif untuk menjatuhkan panggilan daripada memblokir panggilan. Untuk alasan ini, kebijakan CAC, bernama PTOEB, disajikan.

PTOEB mengadopsi struktur ambang batas proporsional untuk mengimplementasikan CAC, dan ini memberikan lebih banyak preferensi panggilan handoff daripada panggilan baru. Model yang digunakan untuk menghitung solusi kebijakan CAC mengasumsikan bahwa terdapat M kelas beban lalu

lintas yang berbeda dalam jaringan. Pada MR tertentu, semua beban lalu lintas berbagi unit B fisik secara keseluruhan bandwidth akses, dan setiap kelas beban lalu lintas terdiri dari panggilan baru dan panggilan handoff. Ini juga mengasumsikan bahwa klien mesh ingin memaksimalkan throughput jaringan dan memiliki akses Internet dengan bandwidth terluas (bandwidth efektif statistik maksimal). Untuk menyeimbangkan persyaratan prioritas yang dibedakan untuk handoff dan maksimalisasi bandwidth efektif statistik, PTOEB menggabungkan struktur ambang batas (setiap beban lalu lintas diberi batas kapasitas) dengan batasan proporsional (faktor x untuk setiap aliran) untuk memberikan lebih banyak panggilan handoff prioritas daripada panggilan baru. Tugas menemukan kebijakan CAC PTOEB dimodelkan sebagai masalah optimasi. Tujuannya adalah untuk mengoptimalkan nilai vektor ambang untuk mencapai bandwidth efektif statistik yang optimal. Untuk mengatasi masalah ini, GA digunakan untuk mencari solusi yang mendekati optimal [10].

GA adalah program pencarian heuristik adaptif yang menerapkan prinsip-prinsip evolusi yang ditemukan di alam. GA menggabungkan operator seleksi, persilangan, dan mutasi dengan tujuan menemukan solusi kesesuaian terbaik untuk suatu masalah. Di sini, fitness adalah istilah GA khusus yang mengacu pada fungsi objektif dari masalah optimisasi. Dalam masalah pengoptimalan yang ada, kebugaran didefinisikan sebagai fungsi bandwidth efektif statistik. Dalam GA, solusi untuk suatu masalah disebut kromosom. Kromosom terdiri dari kumpulan gen, yang merupakan parameter yang akan dioptimalkan.

GA menciptakan populasi awal dengan kumpulan kromosom, mengevaluasi populasi ini, dan mengembangkan populasi melalui beberapa generasi menggunakan operator genetik dalam mencari solusi yang baik dari masalah optimisasi, hingga kriteria terminasi yang ditentukan terpenuhi.

Mengacu pada kebijakan CAC struktur ambang batas proporsional, ruang pencarian dapat diwakili oleh vektor variabel M, yang mewakili ambang batas. Ruang pencarian tunduk pada kondisi bahwa

setiap ambang memiliki batas kapasitas yang diberikan sebanding dengan bandwidth aksesB. Vektor

ambang juga berfungsi sebagai kromosom dalam GA. Untuk mengatasi masalah optimalisasi bandwidth efektif statistik, operator genetik berikut ditentukan:

• Operator Seleksi. Pendekatan “Roulette” dipilih sebagai operator seleksi: kemungkinan sebuah kromosom terpilih sebanding dengan kebugarannya. • Operator Crossover. “One-point crossover” digunakan dalam pengoptimalan bandwidth efektif secara statistik. “Persilangan satu titik” secara acak memilih titik persilangan dalam kromosom dan kemudian menukar dua kromosom induk pada titik ini untuk menghasilkan dua keturunan baru (misalnya, memilih ambang pada posisi 2 pada dua induk a dan b, menukar kedua ambang ini, dan menghasilkan dua keturunan baru).

• Operator Mutasi. "Mutasi Gaussian" digunakan, yang menambahkan satu unit Gaussian mendistribusikan nilai acak (offset) ke gen yang dipilih sebelumnya.

• Metode Pemutusan. "Konvergensi kebugaran" adalah kriteria terminasi. Dia menghentikan evolusi ketika kebugaran dianggap konvergen.

Dengan menggunakan simulasi, penulis menunjukkan bahwa untuk x = 50% (faktor proporsional)

PTOEB dapat secara bersamaan mencapai bandwidth efektif statistik yang tinggi dan rasio prioritas panggilan handoff yang tinggi.

5.2.3.3 iMesh.

Pendekatan ketiga yang kami jelaskan adalah iMesh [11]. iMesh menyediakan pengurangan latensi handoff untuk handoff Layer-3 horizontal (khusus 802.11) di WMN.

Saat klien seluler berpindah dan bergabung kembali dengan AP 802.11 yang berbeda, peristiwa handoff Lapisan 2 terjadi. Hal ini menimbulkan masalah manajemen mobilitas - bagaimana mengirimkan frame yang ditujukan ke stasiun bergerak ketika titik lampirannya ke jaringan mesh (yaitu, AP) telah berubah. Di iMesh, ide dasarnya adalah menggunakan handoff apa pun sebagai pemicu untuk menghasilkan dan menyebarkan pembaruan perutean yang diperlukan di semua AP jaringan mesh. Ini memastikan bahwa jalur optimal ke klien seluler dapat dipertahankan setiap saat. Di iMesh, data disangga di AP yang saat ini menangani klien seluler. Data buffer dikirim ke AP baru saat pembaruan rute diberitahukan ke AP lama.

Kelemahan utama iMesh adalah bahwa dalam kasus di mana jumlah hop antara AP baru dan AP saat ini relatif besar, latensi pengiriman paket yang di-buffer di AP saat ini mungkin lama (yaitu, hasil percobaan iMesh telah menunjukkan bahwa latensi handoff Layer-3 dari jaringan topologi lima-hop lebih dari 40 ms).

Secara rinci, dalam jaringan mesh iMesh berbasis 802.11, protokol routing berbasis link- state OLSR [12] berjalan di semua antarmuka WDS (sistem distribusi nirkabel—jaringan tulang punggung nirkabel) di setiap AP. AP tidak menjalankan OLSR pada antarmuka sisi klien karena klien tidak mengetahui perutean.

Setiap kali klien seluler terhubung dengan AP baru, driver 802.11 yang berjalan di AP mengirimkan sinyal asosiasi ke daemon OLSR, yang menghapus semua rute yang sudah ada sebelumnya ke klien seluler dan menambahkan rute "langsung" ke klien melalui antarmuka logis 802.11. . Tautan antara AP dan klien seluler diperlakukan sebagai rute eksternal ke jaringan mesh. Pada tahap ini, klien seluler memiliki konektivitas uplink yang lengkap.

Informasi rute baru dikodekan sebagai pesan HNA [12] dan disiarkan di jaringan melalui protokol OLSR. Semua AP, saat menerima pesan HNA, hapus semua rute yang sudah ada sebelumnya ke klien seluler dan tambahkan rute baru melalui AP yang saat ini terkait. Selain itu, saat menerima HNA, AP menghapus informasi tentang klien seluler dari database lokal rute eksternalnya. Handoff layer-3 selesai ketika semua AP di jaringan memiliki rute khusus host ke klien seluler dengan AP baru sebagai node hop terakhir di rute. Penundaan handoff jelas bergantung pada jumlah perubahan rute dan jumlah node di sepanjang jalur antara AP baru dan yang lama.

Eksperimen menunjukkan bahwa latensi handoff Layer-2 tidak bergantung pada jumlah perubahan rute seperti yang diharapkan. Penundaan layer-3 sebanding dengan jumlah node di sepanjang jalur antara AP baru dan AP lama: latensi layer-3 maksimum tercatat untuk perubahan rute sepanjang lima lompatan, dan itu sekitar 40 md, dengan kurang dari 100 ms dari total latensi handoff.

5.2.3.4 Mekanisme Caching Data.

Fokus utama iMesh adalah meminimalkan latensi pembaruan perutean saat klien seluler terhubung ke AP baru. Pendekatan lain mengejar maksimalisasi ketersediaan data saat handoff sambil memenuhi batasan penundaan. Tujuan dari referensi 13 adalah untuk meminimalkan kehilangan paket saat menghubungkan dengan AP 802.11 yang baru. Ini memanfaatkan dua sifat unik dari jaringan mesh nirkabel: relai multi hop dan propagasi nirkabel omnidirectional. Minimalisasi kehilangan paket dicapai

melalui mekanisme caching data di node mesh di rute aliran saat ini dan/atau di node tetangga dalam keadaan promiscuous yang dapat menguping paket data.

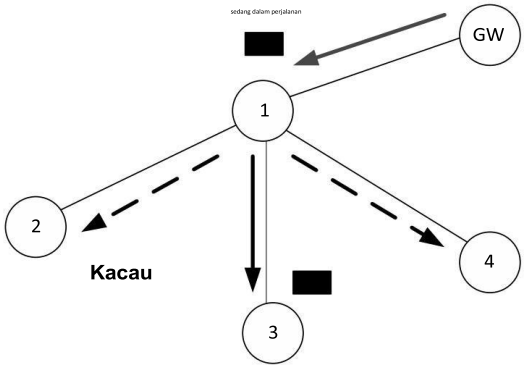
Skema ini tidak berfungsi dengan baik ketika ruang buffer pada node mesh terbatas (seperti yang selalu terjadi). Selanjutnya, ini menghasilkan overhead transmisi nirkabel tambahan ketika paket data yang disimpan diteruskan ke node baru. Akhirnya, caching promiscuous dapat menyebabkan overhead CPU tambahan dari pengintaian paket terus menerus; ini bisa menjadi perhatian jika node mesh tidak kuat.

Secara rinci, di bawah desain kerangka manajemen mobilitas, dua skema diusulkan untuk meminimalkan kehilangan paket selama handoff Layer-3: en-route caching dan promiscuous caching.

Skema caching pertama—caching en-route—memanfaatkan fakta bahwa paket data di WMN diteruskan melalui beberapa node perantara. MR perantara memeriksa tujuan di header paket data. Jika tujuan paket adalah salah satu tetangganya, paket data ini akan di cache. Akibatnya, setiap klien seluler yang melakukan handoff dari node tujuan ke node perantara dapat memiliki dukungan handoff yang mulus dari cache en-route di node perantara. Skema caching en-route ini menggunakan proses pencarian perutean multihop dan melakukannya tidak menimbulkan overhead transmisi nirkabel tambahan.

Skema caching kedua adalah promiscuous caching, yang memanfaatkan properti transmisi ad hoc nirkabel promiscuous. Dalam jaringan relai multihop nirkabel, protokol lapisan tautan (misalnya, 802.11) biasanya beroperasi dalam mode promiscuous, di mana node relai perantara mendengar semua transmisi nirkabel tetangga untuk melakukan perutean multihop dengan benar. Node perantara beroperasi dalam mode promiscuous dan memeriksa header paket dari transmisi paket nirkabel tetangga. Jika tujuan paket adalah tetangga dari node perantara, paket data ini akan di-cache. Pada contoh yang

ditunjukkan pada Gambar 5.3, Node 1 meneruskan paket data ke Node 3. Karena Node 2 dan Node 4 beroperasi dalam mode promiscuous, Node 2 dan Node 4 dapat menguping transmisi data dari Node 1 ke Node 3 dan



Gambar 5.3 Skema caching: en-route dan promiscuous mode caching.

5.2.3.5 BASH.

Pendekatan lain adalah BASH [14], yang berfokus pada desain horizontal—intradomain— Layer-2 skema handoff tanpa batas untuk 802.11 WMN, yang dapat dieksekusi seluler atau dieksekusi jaringan.

Tujuan BASH adalah untuk memanfaatkan fitur backhaul nirkabel WMN untuk mengurangi latensi pemindaian saluran dan kemudian mempersingkat latensi handoff secara keseluruhan. Di BASH, mobile station (MS) menggunakan saluran backhaul untuk menyiarkan pesan permintaan penyelidikan ke MR tetangga. Setelah itu, beralih kembali ke saluran sebelumnya. Setiap kandidat MR akan mengirimkan tanggapan probe ke MR yang saat ini terkait dengan MS. MR saat ini akan menentukan MR baru atas nama MS dan menginformasikan MS untuk memicu handoff Layer-2 ke MR baru. Ketika handoff Layer-2 selesai, MR baru dari MS dapat memulai handoff Layer-3 selanjutnya. Dengan skema ini, waktu untuk memindai saluran disimpan untuk MS, dan keseluruhan latensi handoff dapat dikurangi.

Hasil eksperimen menunjukkan bahwa BASH mencapai rata-rata handoff Layer-2 sebesar 8,7 ms. Latensi autentikasi juga dapat dikurangi. Karena MR saat ini telah mengatur hubungan kepercayaan dengan MS dan MR baru, ini dapat membantu menghasilkan kunci bersama untuk MS dan MR baru. Kunci ini kemudian digunakan oleh MS untuk mengautentikasi dengan MR baru. Di BASH, MS akan menyimpan alamat IP-nya setelah handoff; oleh karena itu, sesi lapisan atas yang sedang berlangsung tidak akan terganggu. Dalam lingkungan percobaan yang digunakan untuk evaluasi kinerja, total latensi handoff adalah 10,5 ms.

Kelemahan utama BASH adalah membutuhkan modifikasi di sisi MS untuk mengelola protokol handoff. Secara khusus, MS harus menangani pesan inisiasi yang dikirim oleh MR lama yang berisi informasi yang diperlukan dari backhaul untuk hand off. Setelah menerima pesan inisiasi handoff, MS harus beralih ke saluran backhaul dan menyiarkan pesan permintaan penyelidikan ke MR tetangga, yang berisi parameter lapisan fisik dan alamat MR saat ini. Hanya setelah itu, MS akan beralih kembali ke saluran sebelumnya dan melanjutkan komunikasi yang sedang berlangsung.

Berikut ini, kami menjelaskan secara rinci langkah-langkah fungsional BASH.

Deskripsi Rinci BASH. Di BASH, handoff dapat dimulai oleh MS atau MR. Jika SNR (signal-to-noise ratio) paket dari MR saat ini yang terkait dengan MS lebih rendah dari ambang batas yang telah ditentukan Tsig, MS akan memulai proses handoff. Alternatifnya, jika SNR paket dari MS lebih rendah dari Tsig, MR saat ini akan memulai handoff.

Pengoperasian BASH mungkin memiliki lima langkah atau enam langkah:

Langkah 0. Jika MS menginisiasi handoff, MS akan mengirimkan pesan permintaan handoff ke MR saat ini.

Langkah 1. Apakah MR saat ini memulai handoff atau menerima pesan permintaan handoff dari MS, itu akan mengirimkan pesan inisiasi handoff ke MS. Pesan ini berisi informasi backhaul yang diperlukan untuk handoff (misalnya frekuensi saluran dan BSSID backhaul) dan SNR yang diukur pada MR saat ini. Segera setelah mengirimkan pesan inisiasi handoff, MR saat ini memulai timertimerpresp, yang digunakan untuk menunggu pesan respons probe.

Alamat MAC dari MS dicatat dan disimpan ke dalam tabel konteks handoff MR untuk pencarian selanjutnya.

Langkah 2. Setelah menerima pesan inisiasi handoff, seperti dalam SyncScan, MS akan mengirim MR saat ini paket data fungsi nol yang bit manajemen dayanya diatur ke 1, untuk mengumumkan bahwa ia telah memasuki mode hemat daya dan menanyakan MR saat ini untuk buffer paket yang dikirimkan ke MS selama probing. Setelah itu, MS akan beralih ke saluran backhaul dan menyiarkan n(ÿ 2) pesan

permintaan probe ke semua MR dalam jangkauan transmisinya. Pesan permintaan pemeriksaan ini berisi teknik lapisan fisik (misalnya, 802.11a, 802.11b dan 802.11g) yang didukung oleh MS, SNR yang diukur pada MS atau MR saat ini yang lebih rendah dari Tsig, dan alamat IP dari saat ini PAK. Setelah MS beralih kembali ke saluran sebelumnya, ia akan mengirim MR saat ini paket data fungsi nol lainnya yang bit manajemen dayanya diatur ke 0, untuk mengumumkan bahwa ia telah meninggalkan mode hemat daya. MS melanjutkan komunikasi yang sedang berlangsung dengan MR saat ini, sampai dihubungi oleh yang terakhir untuk melakukan operasi terkait handoff.

Langkah 3. Ketika MR menerima pesan permintaan probe, itu akan merekam SNR dari paket itu. Jika MR ini bukan MR MS saat ini, ia akan memeriksa apakah saluran AP-nya didukung oleh MS dan jika SNR yang diukur secara lokal lebih tinggi daripada SNR yang terkandung dalam pesan permintaan probe setidaknya ÿ, yang digunakan untuk menghindari efek ping-pong [5]. Jika kedua kondisi tersebut terpenuhi, itu akan memulai pengatur waktu timerpreq beberapa milidetik, sebelum mengirim pesan respons probe ke MR saat ini, yang berisi alamat MAC dan frekuensi saluran dari antarmuka AP-nya dan alamat MAC dari MS yang dipelajari dari pesan permintaan probe. Saat timer habis, MR akan menghitung SNR rata-rata dari semua pesan permintaan probe yang diterima selama periode timerpreq. SNR rata-rata ini dilampirkan dalam pesan respons probe yang dikirim ke MR saat ini. Strategi ini dilakukan agar SNR yang dilaporkan ke MR saat ini lebih reliable. MR saat ini akan merekam informasi yang terkandung dalam pesan respons probe yang diterima ke dalam tabel konteks handoffnya.

Langkah 4. Saat timerpresp habis, currentMR berhenti mengumpulkan pesan respons probe. Jika MR saat ini belum menerima pesan respon probe apapun, itu akan mengirimkan pesan inisiasi handoff lain ke MS dan meminta MS untuk menggandakan n; proses ini dapat diulang jika belum ada pesan respons probe yang diterima dan tidak melebihi ambang batas Tprobe. MR saat ini kemudian akan memeriksa tabel konteks handoff dan menentukan MR baru untuk MS (dilambangkan sebagai MRnew) yang memiliki nilai SNR terbaik. Terakhir, MR saat ini mengirimkan pesan handoff execution ke MS, yang berisi informasi saluran AP MRnew. MS, pada gilirannya, beralih ke saluran AP dari MRnew dan mengirimkan probe unicast pesan ke MRnew. MRnew akan mengukur kualitas sinyal yang diterima dan mengirimkan umpan balik ke MR saat ini, yang akan menentukan apakah MR baru memenuhi syarat berdasarkan informasi ini. Jika ya, MR saat ini akan memberi tahu MS untuk menyerahkan ke MR baru ini. Jika tidak, MR saat ini mengirimkan MS informasi dari calon MR terbaik kedua untuk menyelidiki lagi.

Langkah 5. MS beralih ke saluran AP baru dan kemudian mengautentikasi dan menghubungkan kembali dengan MRnew dengan cara tradisional 802.11. Handoff Layer-2 selesai.

Karena di BASH, MR saat ini sudah mengetahui MRnew sebelum MS mengeksekusi handoff Layer-2, handoff Layer-3 dapat dimulai segera setelah pesan eksekusi handoff dikirim ke MS. Strategi ini tumpang tindih dengan latensi handoff Layer-2, dan latensi handoff Layer-3, sehingga meminimalkan penundaan handoff secara keseluruhan. Skema handoff Layer-3 yang digunakan oleh BASH mirip dengan skema perutean datar yang digunakan di iMesh. Setiap MR menjalankan server DHCP pada antarmuka AP-nya dan memiliki rentang subnet IP sendiri untuk menetapkan alamat IP ke MS yang terdaftar padanya. Ketika MS mendaftar ke MR di jaringan mesh, itu akan menetapkan gateway defaultnya sebagai MR itu. Setelah MS menyerahkan ke MR lain, MS menyimpan alamat IP gateway yang sama tetapi memperbarui tabel ARP menggunakan alamat MAC baru untuk gateway, yang diekstrak dari pesan eksekusi handoff. Mulai saat ini, handoff Layer-3 uplink selesai.

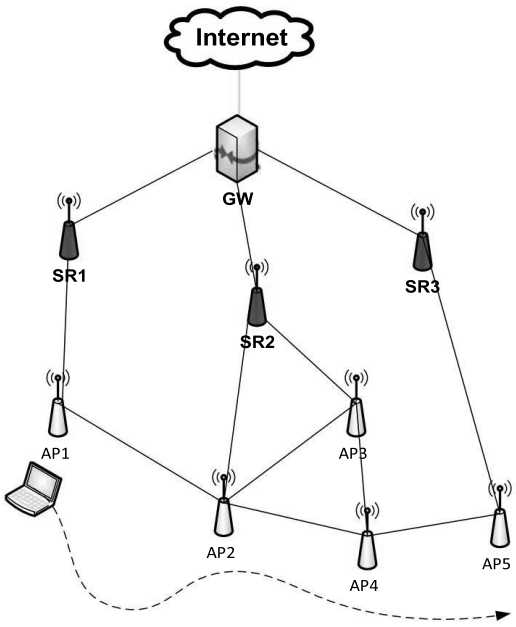
BASH dapat diperpanjang lebih lanjut untuk mengurangi latensi otentikasi yang diperlukan oleh metode otentikasi apa pun yang digunakan [15]. Hal ini dilakukan dengan memanfaatkan transitivitas

hubungan kepercayaan. Saat WMN diatur atau diperbarui dengan bergabungnya MR baru, MR mengatur hubungan kepercayaan satu sama lain. Ini dapat didasarkan pada kriptografi kunci publik/rahasia atau asosiasi keamanan lainnya. Ketika MS dikaitkan dengan MR saat ini, hubungan kepercayaan di antara mereka juga terbentuk. Karena di BASH, MR saat ini dapat mengetahui MRnew dari MS, berdasarkan hubungan kepercayaan yang ada dengan MRnew dan MS, MR saat ini dapat bernegosiasi dengan MRnew untuk menghasilkan kunci bersama untuk komunikasi antara MRnew dan MS. Ini dilakukan sebelum mengirim pesan eksekusi handoff ke MS. Kunci yang dibuat sebelumnya akan dienkripsi oleh kunci bersama antara MR saat ini dan MS, dan disampaikan oleh pesan eksekusi handoff. MS kemudian dapat menggunakan kunci ini untuk mengautentikasi dengan MRnew, mengurangi latensi autentikasi dan selanjutnya mengurangi laten

5.2.3.6 Manajemen Mobilitas Mesh

Metode terakhir diusulkan dalam referensi 16, dan menggabungkan teknik routing per-host dan tunneling. Skema yang diusulkan mencapai keuntungan dari kedua pendekatan dan memanfaatkan beberapa fitur WMN untuk mendukung mikromobilitas IP di WMN 802.11.

Sebuah WMN dimodelkan dengan struktur hirarki tiga tingkat yang terdiri dari satu gateway, beberapa router dengan fungsionalitas AP dan beberapa klien. Gateway terhubung dengan AP dengan status superior yang mengumpulkan informasi lokasi klien seluler di area cakupan AP bawahan (Gambar 5.4). AP status superior diberi nama "router superior" (SR). SR bertindak sebagai delegasi gateway dan berbagi lalu lintas pensinyalan. AP lainnya memiliki status yang setara. Gerbang



Gambar 5.4 Struktur hirarki tiga tingkat.

memberikan alamat IP unik dalam domainnya ke klien seluler. Skema mengasumsikan bahwa perutean di backbone (AP, SR, dan gateway) telah diatur. Ini juga mengasumsikan bahwa komunikasi terjadi di

sepanjang jalur yang ada di pohon, meskipun memungkinkan komunikasi di antara AP yang berdekatan secara geografis.

Ketika klien seluler dihidupkan, gateway mengaktifkan catatan yang berisi informasi pelanggan (otentikasi, otorisasi, dan akuntansi) yang terkait dengan klien seluler dan mendaftarkan informasi lokasi klien (AP yang terkait dengannya). AP yang melayani menyimpan salinan informasi langganan klien seluler, untuk menghindari mengunjungi database di gateway. Informasi lokasi dari semua klien seluler yang berada di sel AP bawahan dicatat dalam SR.

Paket hilir dikirim ke IP klien seluler dengan menggabungkan proses perutean dan proses tunneling. Pertama, paket dirutekan dari gateway ke SR sesuai dengan informasi lokasi klien. Kemudian, tunneling digunakan untuk meneruskan paket downstream ke alamat AP yang melayani. Paket-paket ini dilampirkan dengan header ekstra IP di mana alamat tujuan adalah alamat AP tujuan. Setelah menerima paket-paket yang disalurkan ini, AP tujuan mendekapsulasi dan meneruskannya ke klien seluler yang dituju.

Paket upstream malah diteruskan oleh AP ke gateway dengan menggunakan rute default.

Seperti di BASH, pengguna diharuskan memperbarui firmware di perangkat mereka untuk mendukung skema handoff. Handoff terjadi ketika mobile client berpindah ke sel AP yang baru.

Setelah menerima pesan permintaan handoff dari klien yang bergerak yang menunjukkan ID AP sebelumnya, AP baru mengirimkan pesan permintaan handoff ke AP sebelumnya.

Mantan AP mengirimkan kembali informasi pelanggan yang sesuai ke AP baru.

Sementara itu, ia menambahkan entri sementara di tabel perutean dengan alamat tujuan klien seluler. Jika paket hilir didekapsulasi oleh AP lama tetapi alamat klien seluler tidak ditemukan, paket ini dialihkan ke AP baru menggunakan entri perutean sementara. Entri perutean ini disimpan hingga penghitung waktu dengan panjang Tr kedaluwarsa. Untuk menjamin bahwa perutean ini dapat mencapai AP baru, entri perutean ditambahkan oleh setiap router di jalur dari AP lama ke AP baru. Saat klien seluler bergerak lagi, rantai rute hilir terus digabungkan.

Metode ini memperkenalkan masalah perutean segitiga (juga ada di IP seluler [3], protokol manajemen mobilitas standar). Masalah perutean segitiga terdiri dari pengiriman paket ke sistem proxy sebelum transmisi ke tujuan yang dituju. Untuk menghindari hal ini, pembaruan lokasi dipicu setelah interval waktu Tlu (pembaruan lokasi) kedaluwarsa. Pembaruan lokasi dipicu oleh setiap AP, yang melaporkan kumpulan klien seluler saat ini ke SR. SR, pada gilirannya, memilih interval lain Thu untuk secara berkala memperbarui set ke gateway. Thu harus tidak kurang dari Tlu. Setelah pembaruan lokasi berkala, paket downstream dapat disalurkan ke AP tempat klien seluler berada tepat tanpa melintasi semua AP yang telah dikunjungi klien seluler.

Seperti yang telah dikatakan, metode yang diperkenalkan di referensi 16 menggabungkan keuntungan dari tunneling dan perutean per-host, dan memanfaatkan beberapa fitur WMN.

Tunneling paket downstream di backbone overhead untuk routing di setiap AP perantara yang hadir dalam pendekatan lain (misalnya, BASH). Selain itu, struktur hirarkis tunneling WMNs lebih menarik. Di sisi lain, karena WMN memastikan cakupan yang berkelanjutan, perutean khusus seluler diterapkan dalam beberapa lompatan terakhir. Terakhir, menerapkan perutean per-host hanya di antara AP yang

bertetangga secara geografis tidak mengharuskan setiap AP mempertahankan terlalu banyak entri perutean perantara.

Kelemahan utama dari pendekatan ini terutama berkaitan dengan tunneling. Pertama, tunneling memperkenalkan penundaan ekstra untuk enkapsulasi/dekapsulasi paket. Kedua, tunneling memiliki fleksibilitas yang rendah: arsitektur mesh berubah (misalnya, AP baru ditambahkan), tunneling harus ditutup dan waktu yang lama diperlukan untuk ditayangkan setelah perubahan.

5.2.4 Dukungan Mikro dan Makromobilitas

Pada bagian ini pertama-tama kami menjelaskan algoritme keputusan serah terima dan kemudian menjelaskan dua pendekatan, untuk menyediakan dukungan serah terima intradomain dan interdomain.

5.2.4.1 Skema Keputusan Serah Terima Vertikal Menggunakan 802.21.

Sebuah algoritma keputusan untuk handover vertikal intra- dan interdomain, dalam jaringan berkemampuan IEEE 802.21 [17], disajikan dalam referensi 18. Keputusan handoff vertikal menggabungkan kekuatan evaluasi RSS tradisional dan berbasis pengambilan keputusan multi atribut (MADM) algoritma. Metode MADM digunakan untuk memaksimalkan QoS

dialami oleh setiap pengguna. Selain itu, skema memanfaatkan informasi jaringan yang disediakan oleh server informasi 802.21 MIH. Kinerja skema dalam hal waktu serah terima dan tingkat penurunan lebih baik dibandingkan dengan metode serah terima vertikal tradisional berbasis RSS dan berbasis fungsi biaya [19]. Hasil simulasi menunjukkan bahwa tingkat penurunan skema yang diusulkan memberikan peningkatan masing-masing sekitar 10% dan 5% untuk skema berbasis RSS dan berbasis fungsi biaya.

Secara rinci, karena masalah keputusan serah terima berkaitan dengan pemilihan di antara sejumlah kandidat jaringan yang terbatas sehubungan dengan kriteria yang berbeda, ini dimodelkan sebagai masalah MADM fuzzy. Logika fuzzy digunakan untuk mewakili informasi yang tidak tepat tentang kelas lalu lintas (yaitu, percakapan, streaming, latar belakang, dan interaktif). Metode fuzzy MADM terdiri dari dua langkah. Langkah pertama adalah mengubah

data fuzzy menjadi bilangan real. Proses hierarki analitik (AHP) [20] digunakan untuk menurunkan bobot parameter lalu lintas QoS (atribut) untuk jaringan alternatif yang berbeda. Ini dilakukan dengan melakukan perbandingan berpasangan dari parameter QoS ini sehubungan dengan kepentingannya untuk mencapai serah terima yang sukses.

Parameter yang dipertimbangkan adalah prioritas trafik, data rate, error rate, delay, dan jit ter. Skala perbandingan menggunakan rentang 1 sampai 9, masing-masing mewakili entri, sebagai berikut: 1 = sama pentingnya, 3 = cukup penting, 5 = sangat penting, 7 = sangat penting lebih penting, 9 = sangat penting.

Hasil perbandingan tersebut dimasukkan ke dalam matriks, seperti terlihat pada Tabel 5.1: matriks tersebut, jika bilangan yang menyatakan bobot lebih besar diletakkan pada posisi (i,j), kebalikan dari bilangan tersebut harus diletakkan pada posisi (j, saya). Matriks AHP dapat dihitung untuk setiap kelas lalu lintas (percakapan, streaming, latar belakang, dan inter aktif). Untuk memverifikasi konsistensi penilaian perbandingan, rasio konsistensi (CR) digunakan sebagai indikator. Matriks A dianggap konsisten jika kondisi berikut dipenuhi:

Ide penting dari AHP adalah bahwa matriks A dengan peringkat n hanya konsisten jika memiliki satu nilai eigen positif ÿmax = n sedangkan semua nilai eigen lainnya adalah nol. Selanjutnya, indeks konsistensi (CI) digunakan untuk mengukur penyimpangan dari matriks yang konsisten:

Rasio konsistensi (CR) kemudian didefinisikan sebagai rasio CI terhadap apa yang disebut indeks acak (RI), yang merupakan CI dari matriks yang dihasilkan secara acak:

Untuk n (rank matriks) = 3, CR harus kurang dari 0,05, untuk n = 4 harus kurang dari 0,08, dan untuk n ÿ 5 harus kurang dari 0,10. Bobot dihitung dengan menggunakan metode rata-rata geometris, yang merupakan akar n dari perkaliannya. Bobot yang dihasilkan untuk contoh pada Tabel 5.1 ditunjukkan pada Tabel 5.2.

Langkah kedua adalah menggunakan algoritma MADM klasik untuk menentukan urutan peringkat jaringan kandidat dengan menghitung skornya. Ada beberapa metode: dalam referensi 21, dua di antaranya disajikan, yaitu pembobotan aditif sederhana (SAW) dan pembobotan eksponen multiplikatif (MEM). Skor jaringan yang dipilih i oleh SAW adalah jumlah tertimbang dari semua nilai atribut:

di mana n adalah jumlah atribut, r adalah nilai atribut yang dinormalisasi, dan ÿ adalah nilai pembobotan. Normalisasi diperlukan untuk secara efisien membandingkan nilai atribut dari jaringan yang berbeda.

Dalam MEW, skor jaringan i ditentukan oleh produk tertimbang dari atribut:

dimana x adalah nilai atribut, n adalah jumlah atribut, dan ÿ adalah nilai pembobotan.

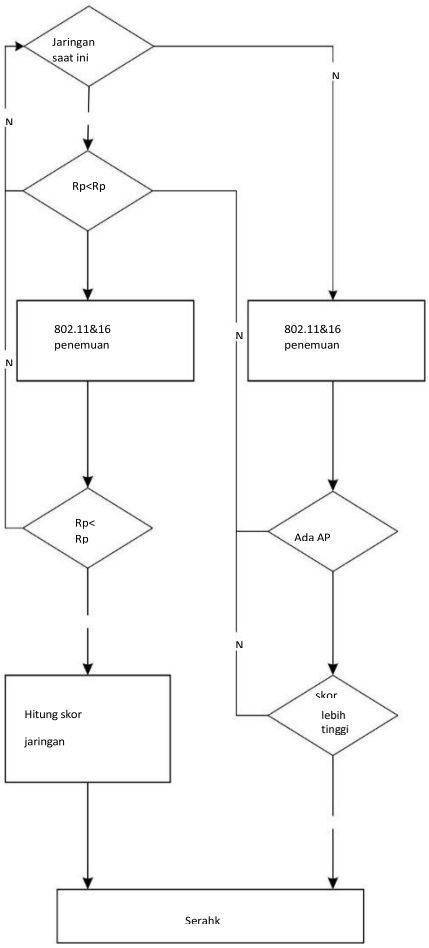
Skema keputusan serah terima yang diusulkan ditunjukkan pada Gambar 5.5 dan bekerja di jaringan WiFi dan WiMAX. Handover dipicu oleh informasi level RSS dari layer PHY. Setelah antarmuka jaringan WiFi atau WiMAX ditemukan dan sinyal yang diterima dapat diterima, terminal akan memulai proses pemilihan jaringan. Informasi jaringan diambil dengan meminta server informasi MI (MIIS) [17].

Informasi yang diberikan oleh MIIS termasuk tetangga, mode operasi, prioritas pengguna,

kecepatan data, penundaan, jitter, tingkat kesalahan paket, dan waktu pembaruan. Contoh basis informasi yang disimpan dalam MIIS ditunjukkan pada Tabel 5.3. Terminal berkemampuan IEEE

802.21 dapat memperoleh informasi ini secara berkala dengan menggunakan antarmuka jaringannya saat ini. Jika RSS lebih kecil dari ambang batas RSS yang ditentukan sebelumnya,

algoritme akan menghitung semua kemungkinan fungsi skor jaringan dan memilih yang terbaik. Istilah dari



Gambar 5.5 Usulan skema keputusan handover MADM untuk vertical handover antara WiFi dan WiMAX. prioritas, jaringan WiFi diasumsikan memiliki prioritas lebih tinggi daripada jaringan WiMAX karena memiliki kecepatan data yang tinggi dan hemat biaya. Untuk alasan ini, jika koneksi jaringan saat ini adalah WiMAX dan jaringan WiFi dengan skor lebih tinggi dari yang sekarang ditemukan di dekatnya, maka handover dipicu.

Kinerja skema keputusan serah terima dievaluasi dengan simulasi dan dibandingkan dengan dua skema lainnya: skema berbasis RSS dan skema berbasis fungsi biaya.

Algoritme handover vertikal berbasis RSS memicu handover jika titik akses 802.11 atau stasiun pangkalan WiMAX dengan RSS yang lebih kuat ditemukan di dekatnya. Algoritma berbasis fungsi biaya menghitung biaya jaringan i sebagaidi mana:

n adalah jumlah atribut.

Eij adalah faktor eliminasi. Ini menunjukkan apakah batasan minimum untuk atribut j dapat dipenuhi. Ini menghasilkan nilai yang besar jika kendala tidak dapat dipenuhi (1 jika kendala terpenuhi).

Qij adalah faktor QoS. Ini adalah nilai log alami yang dinormalisasi dari atribut j.

Algoritma berbasis fungsi biaya kemudian memilih jaringan dengan fungsi biaya terendah. Atribut termasuk prioritas pengguna, data rate, delay, jitter, error rate dan RSS.

Hasil simulasi menunjukkan bahwa skema yang diusulkan memberikan kinerja yang

lebih baik daripada RSS dan skema berbasis fungsi biaya dalam hal total waktu serah terima dan tingkat penurunan rata-rata.

5.2.4.2 Jaringan

Pendekatan pertama untuk penyediaan mikro dan makromobilitas adalah SMesh [22]. SMesh menyediakan arsitektur dan protokol jaringan mesh 802.11 yang mengoptimalkan perutean, untuk menyediakan handoff intradomain dan interdomain.

Handoff intradomain dicapai dengan bekerja dalam mode ad hoc (IBSS), mengendalikan handoff dari infrastruktur mesh, dan dengan menggunakan multicast di jaringan mesh untuk mengirim data melalui beberapa jalur ke klien seluler selama handoff. AP di sekitar klien memantau kualitas konektivitas dan menyinkronkan yang seharusnya menangani klien tersebut. Hingga hal ini terjadi, paket data dari gateway Internet ke klien digandakan oleh sistem di sekitar klien.

Handoff interdomain dicapai dengan menggunakan grup multicast melalui jaringan kabel untuk mengoordinasikan keputusan dan mentransfer koneksi secara mulus antara gateway Internet saat klien seluler berpindah antar AP.

Infrastruktur komunikasi SMesh bergantung pada sistem perpesanan overlay, yang digunakan oleh AP untuk meneruskan koneksi dan untuk koordinasi di antara keduanya.

SMesh mengasumsikan bahwa semua router mesh menggunakan saluran AP yang sama, yang merupakan strategi penerapan dominan di WLAN 802.11, di mana pengurangan interferensi diperoleh dengan menetapkan saluran yang tidak tumpang tindih ke saluran AP dari router mesh yang berdekatan. Ini menyiratkan bahwa stasiun seluler tidak perlu memindai saluran lain atau beralih ke saluran AP dari MR baru selama handoff Layer-2, sehingga mengurangi latensi handoff. Namun, asumsi ini dapat mewakili kendala yang sulit. Selain itu, SMesh meminimalkan latensi handoff dengan biaya pensinyalan yang tinggi: overhead dihasilkan untuk mengelola klien selama handoff dan untuk memelihara topologi jaringan.

Eksperimen menunjukkan bahwa overhead manajemen untuk penyerahan intradomain tumbuh secara linier dengan jumlah klien, dalam kasus terburuk dengan kecepatan sekitar 2 Kbps per klien. Overhead interdomain, sebaliknya, berbanding lurus dengan jumlah koneksi yang dimiliki setiap klien, dan ini bisa luar biasa.

Eksperimen menunjukkan bahwa overhead yang disebabkan oleh duplikasi paket selama serah terima rendah. Misalnya, ketika aliran VoIP dupleks penuh dikirim antara klien seluler dan host Internet, sebagian besar handoff mengalami sekitar dua duplikat ke klien seluler dan tidak ada di arah lain.

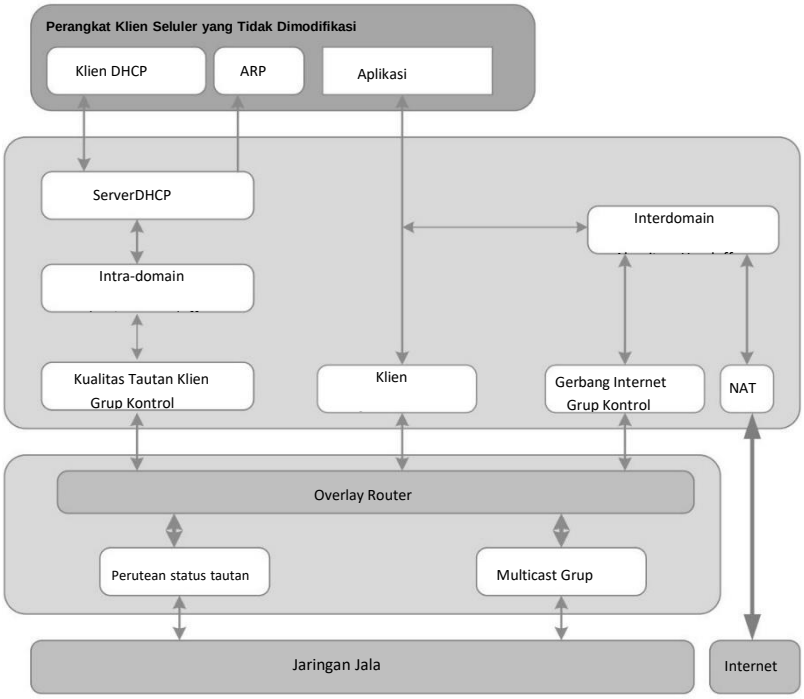
Deskripsi Rinci SMesh. Arsitektur perangkat lunak SMesh terdiri dari dua komponen utama: infrastruktur komunikasi dan antarmuka dengan klien seluler (Gambar 5.6).

Infrastruktur komunikasi SMesh bergantung pada sistem pesan Spines [23]. Jaringan overlay Spines menghubungkan semua node mesh melalui tautan langsung di jaringan nirkabel dan melalui tautan virtual di jaringan kabel. Setiap node jaringan nirkabel membuat daemon Spines untuk meneruskan pesan di dalam jaringan nirkabel. Spines juga memungkinkan untuk menggunakan fungsionalitas

multicast dan anycast. Setiap daemon Spines melacak tetangga langsungnya sendiri dengan mengirimkan pesan halo secara berkala. Berdasarkan konektivitas yang tersedia, setiap node membuat tautan nirkabel logis dengan tetangga langsungnya. Protokol link-state [24], yang didasarkan pada grafik konektivitas ke seluruh jaringan, digunakan oleh node untuk bertukar informasi routing dengan node lain. Node membanjiri informasi link-state (perubahan topologi) menggunakan link yang dapat diandalkan antara tetangga langsung.

Dalam arsitektur SMesh, klien seluler memelihara informasi jaringan yang sama (alamat IP, Netmask, dan Gateway Default). Informasi konektivitas disediakan oleh server DHCP, yang berjalan di setiap node mesh. Alamat IP yang ditetapkan untuk setiap klien seluler dihitung menggunakan fungsi hash pada alamat MAC klien (dipetakan ke alamat pribadi) dan diiklankan pada grup kontrol multicast (Grup Data Klien— CDG). Dalam kasus tabrakan hash, klien dengan MAC terkecil menyimpan IP saat ini dan klien lain dalam tabrakan tersebut mendapatkan IP terkelola. Gateway default diatur ke alamat IP virtual, yang dipetakan ke alamat perangkat keras node mesh.

Seperti dibahas di atas, setiap klien seluler dikaitkan dengan grup multicast (CDG), yang terdiri dari node mesh di lingkungannya. Node mesh bergabung dengan CDG jika dianggap memiliki konektivitas terbaik ke klien seluler berdasarkan metrik kualitas tautan



Gambar 5.6 Arsitektur SMesh.

diterima dari node lain. Jika tujuan paket adalah klien SMesh, paket dikirim oleh Spines ke node SMesh yang bergabung dengan Grup Data klien tersebut menggunakan pohon multicast. Dengan mekanisme ini, klien bisa menerima duplikasi paket IP.

Namun, duplikat paket IP dijatuhkan dengan anggun di penerima (duplikat TCP dijatuhkan di tingkat transportasi, dan aplikasi yang menggunakan UDP seharusnya menangani duplikat).

Jika tujuan paket adalah Internet, maka paket dikirim oleh titik akses klien asal ke gateway Internet terdekat dengan meneruskannya ke grup anycast tempat semua gateway Internet bergabung (pesan data anycast mengikuti satu jalur di pohon). kepada anggota kelompok terdekat).

Di SMesh, klien seluler dan AP dikonfigurasi dalam mode ad hoc (IBSS). Ini dilakukan untuk menghemat waktu pemindaian dan untuk menghubungkan ke AP baru. Selanjutnya, ini dipilih untuk benar-benar mengontrol penyerahan hanya dari AP.

Di SMesh, proses serah terima intradomain terdiri dari dua proses berbeda:

pemantauan klien seluler dan serah terima klien.

Pemantauan Klien Seluler (Detak Jantung Mulus). Setiap node SMesh secara berkala menghitung evaluasi kualitas tautan klien berdasarkan salah satu dari dua metrik berikut: hilangnya permintaan DHCP klien atau respons ARP yang teramati. Saat menggunakan monitor SMesh DHCP, setiap server DHCP menginstruksikan klien seluler untuk memperbarui alamat IP mereka secara berkala, sehingga berfungsi sebagai detak jantung untuk melacak klien. Hal ini dicapai dengan mengatur timer T 1 (Renew) dari protokol DHCP standar [25], yang menginstruksikan klien untuk memulai permintaan DHCP unicasting (DHCPREQUEST) setelah timer berakhir. Kelemahan utama dari metode ini adalah bahwa ia menggunakan overhead yang tidak dapat diabaikan karena paket DHCPREQUEST setidaknya memiliki panjang 300 byte, sebuah DHCPACK yang berukuran sekitar 548 byte. Kelemahan lainnya adalah ketika DHCPREQUEST pertama hilang, waktu antara permintaan ini dan berikutnya bergantung pada platform dan biasanya lebih dari beberapa detik [26].

Dalam skema pemantauan ARP, setiap node mesh dalam CDG secara berkala mengirimkan permintaan ARP ke klien, dan semua node di sekitarnya menggunakan balasan untuk menghitung metrik. Protokol ARP [27] digunakan untuk memetakan alamat IP ke alamat perangkat keras (MAC). ARP digunakan ketika sebuah host ingin berkomunikasi dengan host lain di dalam jaringan yang sama, tetapi tidak mengetahui alamat MAC-nya. Ketika sebuah host menerima permintaan ARP, itu membandingkan IP tujuan dengan alamat IP-nya sendiri: alamat IP cocok,

itu akan mengeluarkan balasan ARP (unicast), mengisi informasi yang terdapat di bidang MAC dengan alamat MAC-nya sendiri. Keuntungan menggunakan pendekatan ini adalah, tidak seperti DHCP, paket ARP sangat kecil (hanya 28 byte).

Metrik kualitas tautan klien yang dihitung oleh setiap node SMesh didasarkan pada hilangnya permintaan DHCP klien atau respons ARP yang teramati, menggunakan fungsi rata-rata tertimbang peluruhan:

Mnew = Cetakan ÿ Df + Arus ÿ (1 ÿ Df), 0 < Df < 1

di mana M adalah ukuran kualitas tautan dan Df adalah faktor peluruhan (nilai yang digunakan dalam SMesh adalah 0,8). Arus adalah nilai konstanta yang disetel ke 0 jika titik akses tidak menerima respons paket probe DHCP atau ARP dalam waktu yang diharapkan, atau disetel ke nilai maksimum (50) jika

paket probe diterima. Jika dua atau lebih titik akses memiliki metrik bilangan bulat yang sama, titik akses dengan IP terendah akan dipilih.

Untuk mendapatkan ukuran yang lebih andal dari kualitas tautan yang dipantau, fungsi peluruhan yang dijelaskan di atas digabungkan dengan RSSI (indikator kekuatan sinyal yang diterima) dan pengukuran tingkat kerugian. Pengukuran RSSI diperoleh dengan mengonfigurasi antarmuka nirkabel dari node mesh dalam mode monitor. Dalam konfigurasi tersebut, header tambahan ditambahkan oleh driver nirkabel, yang berisi informasi RSSI. Tingkat kerugian mengacu pada jumlah pengiriman ulang paket dari protokol 802.11. Setiap paket unicast yang ditransmisikan dalam 802.11 harus diakui oleh penerima. Jika paket hilang, pengirim mentransmisi ulang paket dan menyetel bendera pengiriman ulang di header 802.11.

Selain CDG yang dijelaskan sebelumnya, yang digunakan untuk meneruskan paket data di SMesh menuju AP yang melayani klien, AP di lingkungan klien bergabung dengan grup multicast yang berbeda khusus untuk klien tersebut, yang disebut Client Control Group (CCG).

CCG digunakan untuk berbagi dengan node mesh lain di sekitar klien metrik kualitas tautan untuk klien dan untuk memutuskan AP mana yang terbaik untuk melayani klien tersebut. Node

jala bergabung dengan Grup Kontrol klien saat menerima satu detak jantung dari klien, dan meninggalkan grup setelah tidak mendengar kabar dari klien selama beberapa waktu Penyerahan Intradomain. Untuk memberikan handoff yang transparan kepada klien, mesh nodes mengiklankan alamat IP gateway virtual untuk semua klien sebagai bagian dari penawaran dan pengakuan DHCP mereka (DHCPOFFER dan DHCPACK). Klien seluler mengatur gateway kesalahan mereka ke alamat IP virtual ini terlepas dari AP mana mereka terhubung. Alamat IP virtual ini kemudian dipetakan ke alamat MAC gateway sebenarnya dengan mekanisme yang dijelaskan berikut ini.

Proses handoff dimulai ketika mesh node yakin bahwa ia memiliki konektivitas terbaik ke klien dan metriknya setidaknya Ambang Batas lebih tinggi dari metrik AP saat ini yang

melayani klien tersebut (yaitu, Metrik > MetrikArusAP ÿ (1 + Ambang Batas)). Nilai tipikal untuk Ambang Batas adalah 12%.

Node mesh kemudian mengirimkan pesan ARP serampangan sebagai unicast, langsung ke klien. ARP serampangan adalah paket balasan ARP yang tidak dikirim sebagai balasan atas permintaan ARP, melainkan dikirim di jaringan lokal secara sukarela. Setelah menerima paket seperti itu, klien seluler akan memperbarui alamat MAC gateway defaultnya, dalam cache ARP-nya, dengan nilai yang terdapat dalam pesan ARP yang dikirim oleh node mesh.

Selain mengirimkan ARP serampangan ke klien seluler, node mesh bergabung dengan Grup Datanya sehingga paket yang ditujukan ke klien mulai mengalir melalui titik akses ini. Jika node lain juga merupakan anggota Grup Data, paket yang ditujukan ke klien ini diteruskan ke kedua node mesh, dan masing-masing meneruskan paket langsung ke klien seluler, yang mungkin menerima paket duplikat. Penggunaan multicast selama handoff memiliki keuntungan yang signifikan untuk mencapai konektivitas tanpa gangguan dengan

(1) mengirimkan paket melalui beberapa titik akses ke klien seluler, untuk menangani pergerakan klien yang tidak terduga sementara jalur akses terbaik untuk klien dipilih, dan (2) menghindari kerugian saat perubahan rute terjadi di jaringan nirkabel. Kelemahan utama dari mekanisme ini adalah pembangkitan overhead multicast lokal. Namun, seperti yang dijelaskan berikut ini, lalu lintas ini dapat dipersempit. Saat simpul jaring yang merupakan anggota CDG menerima pembaruan metrik kualitas tautan yang menunjukkan bahwa simpul berbeda di Grup Data terhubung dengan lebih baik, simpul

tersebut mengeluarkan Permintaan Keluar. Permintaan Cuti hanya dapat disetujui oleh node di Grup Data yang meyakini bahwa node tersebut memiliki konektivitas terbaik ke klien. Sebuah node dapat

meninggalkan Grup Data jika dan hanya jika permintaannya diakui oleh setidaknya satu node lainnya.

Kelemahan lain dari solusi ini adalah bahwa kinerja handoff bergantung pada nilai parameter untuk menunjukkan metrik kualitas tautan. Secara umum, semakin kecil faktor peluruhan dalam metrik kualitas tautan, semakin cepat klien dapat bereaksi terhadap perubahan kondisi. Namun, faktor peluruhan kecil dapat memicu handoff yang tidak perlu dan meningkatkan jumlah overhead dalam sistem. Sebaliknya, faktor peluruhan yang besar dapat menunda penyerahan terlalu lama dan menyebabkan kerugian. Singkatnya, pengorbanan ini harus seimbang untuk mencapai kinerja yang diinginkan.

Penyerahan Interdomain. Seperti disebutkan di atas, dalam komunikasi SMesh antara klien seluler dan Internet diteruskan melalui gateway Internet terdekat untuk meningkatkan penggunaan nirkabel. Ketika klien pindah ke pulau konektivitas yang berbeda, paket mungkin diteruskan ke gateway lain yang lebih dekat ke klien. Mengubah satu titik akhir koneksi (yaitu, alamat IP gateway Internet) seringkali tidak mungkin dilakukan tanpanya

memutuskan koneksi yang ada dan, oleh karena itu, diperlukan solusi untuk mempertahankan koneksi yang ada. Selain itu, klien seluler di SMesh berada di jaringan IP pribadi, dan Terjemahan Alamat Jaringan (NAT) diperlukan di gerbang Internet saat berkomunikasi dengan host eksternal. Solusi yang digunakan dalam SMesh untuk mendukung handoff interdomain memperlakukan koneksi UDP dan TCP secara terpisah.

Sesi TCP menuju host eksternal dimulai saat paket SYN pertama dikirim oleh gateway Internet. Acara ini menghasilkan entri di tabel NAT gateway.

Sejak saat itu, tujuan Internet menganggap alamat sumber paket sebagai gateway Internet. Jika gateway Internet menerima paket TCP yang bukan SYN dan tidak memiliki entri untuk koneksi tersebut dalam tabel NAT, gateway akan meneruskan paket tersebut ke grup IGMG (Internet Gateways Multicast Group). IGMG adalah grup multicast yang bergabung dengan gateway Internet SMesh, di mana gateway terhubung melalui tautan overlay kabel, membentuk grafik yang terhubung sepenuhnya. Pemilik asli koneksi (yang memilikinya di tabel NAT) selanjutnya menyampaikan paket ke tujuan dan mengirimkan pesan ke grup IGMG, yang menunjukkan bahwa itu adalah pemilik koneksi untuk entri NAT tersebut. Kemudian, setiap gateway yang bukan pemilik koneksi akan meneruskan paket koneksi tersebut ke masing-masing pemilik, menyelesaikan proses handoff koneksi. Kelemahan dari mekanisme ini adalah jika paket tiba di gateway Internet dengan kecepatan tinggi, beberapa paket dapat dikirim ke grup IGM sebelum pemilik koneksi dapat merespons, sehingga menghasilkan overhead lalu lintas lokal yang tinggi. Jika tidak ada gateway Internet yang mengklaim koneksi dalam batas waktu tertentu (tergantung implementasi), gateway baru mengklaim koneksi, meneruskan paket ke tujuan Internet.

Ini akan memutus koneksi TCP pada klien SMesh, karena host Internet akan menerima paket data TCP dari sumber tak terduga yang tidak terikat ke soket TCP yang ada, dan akan mengirimkan paket RST kembali ke pengirim paket tersebut.

Paket UDP diperlakukan berbeda di SMesh. Lalu lintas UDP pada nomor port diklasifikasikan sebagai tanpa koneksi dan berorientasi koneksi, dan berorientasi koneksi dipilih sebagai protokol default.

Lalu lintas DNS dan NTP termasuk dalam kategori tanpa koneksi. Lalu lintas UDP tanpa koneksi diteruskan langsung oleh gateway Internet setelah menerimanya dari jaringan mesh.

Ketika gateway Internet menerima paket UDP berorientasi koneksi baru, ia tidak dapat membedakan apakah itu paket pertama dari koneksi baru, atau paket milik koneksi yang ada yang dibuat melalui gateway Internet yang berbeda.

Gateway sama-sama menyampaikan paket itu ke tujuannya dan juga meneruskannya ke grup multicast IGMG. Jika paket UDP milik koneksi yang sudah dibuat, gateway Internet yang merupakan pemilik asli koneksi juga menyampaikan paket ke tujuan dan mengirimkan respons ke grup IGMG yang mengiklankan kepemilikannya untuk koneksi UDP tersebut. Setelah menerima respons, gateway awal akan meneruskan paket berikutnya langsung ke gateway asli dan tidak akan lagi menyampaikan paket UDP dari koneksi tersebut (dengan alamat sumber mesh dan alamat serta port tujuan yang sama) ke Internet. Jika respons tidak sampai dalam batas waktu tertentu (bergantung pada implementasi), gateway Internet akan mengklaim kepemilikan koneksi UDP, akan berhenti meneruskan paket-paket itu

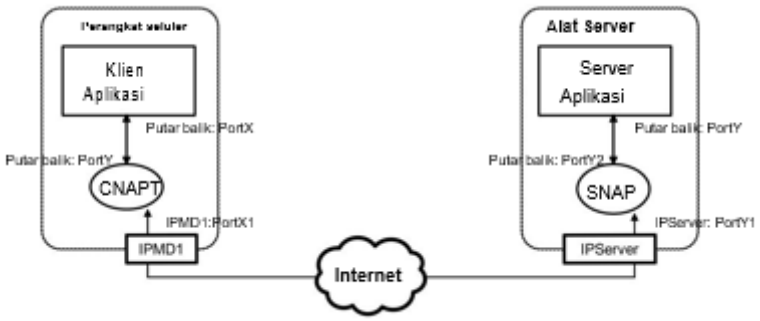
koneksi ke grup IGMG, dan akan terus menyampaikan paket ke Internet. Kelemahan utama dari pendekatan ini adalah bahwa overhead lalu lintas Internet dapat dihasilkan sebagai host akhir di Internet dapat melihat duplikasi paket UDP yang berasal dari alamat sumber IP yang berbeda selama handoff. Namun, duplikasi paket UDP pada akhirnya dijatuhkan oleh aplikasi (misalnya, beberapa mungkin hanya memproses muatan UDP dan melihat paket duplikat, sementara yang lain mungkin menjatuhkan paket dengan sumber yang salah).

5.2.4.3 WiOptiMo. Pendekatan terakhir untuk manajemen serah terima mulus yang kami hadirkan adalah WiOptiMo [28], yang mendukung serah terima horizontal/vertikal dan mikro/ makromobilitas. WiOptiMo memungkinkan serah terima yang diprakarsai oleh perangkat seluler dan jaringan. Desainnya sepenuhnya didasarkan pada penggunaan protokol dan driver jaringan yang saat ini digunakan. Ini tidak memerlukan modifikasi atau adaptasi ad hoc dalam standar 802.x saat ini, tetapi dapat dengan mudah diadaptasi untuk mengakomodasi dan mengeksploitasi peningkatan masa depan dalam standar ini.

WiOptiMo adalah solusi lapisan aplikasi yang mengeksploitasi pemantauan lintas lapisan untuk mengambil keputusan serah terima yang dioptimalkan, dan memungkinkan adaptasi efektif dari QoS yang dikirimkan ke kondisi jaringan variabel (misalnya, karena anomali operasional). WiOptiMo pada awalnya dirancang untuk manajemen serah terima mulus di Internet dengan jaringan WiFi, tetapi telah dioptimalkan untuk konteks mesh [29].

Selain itu, telah diberdayakan dengan mekanisme handoff reaktif dan proaktif berdasarkan kesadaran perilaku pengguna. Kinerjanya dalam konteks jaringan mesh dilaporkan dalam [30]. Uji coba yang dijalankan dalam penerapan jaring nyata menunjukkan keefektifan pendekatan WiOptiMo dalam hal waktu yang diperlukan untuk mengambil keputusan penyerahan, keseluruhan latensi penyerahan, tambahan penundaan end-to-end, dan persentase kehilangan paket selama penyerahan. Misalnya, penundaan end-to-end tambahan yang diperkenalkan oleh WiOptiMo dapat diabaikan (di bawah 1 mdtk) dan waktu yang diperlukan untuk mendeteksi sambungan yang terputus sedikit lebih dari 100 mdtk.

WiOptiMo menangani mobilitas dan serah terima yang mulus dengan menggunakan dua komponen utama: Alamat Jaringan Klien dan Penerjemah Port (CNAPT) dan Alamat Jaringan Server dan Penerjemah Port (SNAPT). CNAPT dan SNAPT secara bersama-sama bertindak sebagai middleware (Gambar 5.7), sehingga untuk aplikasi berbasis klien-server



Gambar 5.7 Komponen WiOptiMo: CNAPT dan SNAPT secara kolektif bertindak sebagai middleware

paradigma, klien percaya untuk berjalan baik pada mesin yang sama dengan server atau pada mesin dengan koneksi langsung yang stabil ke server.

CNAPT adalah aplikasi yang meniru perilaku server di sisi klien dan, pada saat yang sama, perilaku klien di sisi Internet. CNAPT dapat diinstal pada perangkat yang sama dengan pengguna seluler atau pada perangkat berbeda di jaringan seluler yang sama.

CNAPT meniru perilaku aplikasi klien dan server dengan menyediakan soket berikut:

• Soket server (SSESS) di sisi klien untuk setiap layanan yang dapat diminta klien dari Internet. Soket server ini mendengarkan port layanan server sebenarnya

• Soket Simulasi permintaan klien di sisi Internet untuk setiap permintaan layanan yang dikirim melalui Internet. Soket ini terikat ke alamat IP perangkat saat ini dan menyampaikan paket ke SSESS yang disediakan oleh SNAPT.

• Soket server (CSESS) di sisi Internet untuk setiap layanan klien (layanan yang dapat digunakan oleh server untuk model komunikasi publish/subscribe).

Soket ini mendengarkan port emulator layanan klien, yang berbeda dari port nyata layanan klien untuk menghindari kesalahan pengikatan. • Soket emulasi permintaan

server di sisi klien untuk setiap permintaan layanan klien. Soket ini menyampaikan paket ke soket server layanan klien sebenarnya.

SNAPT adalah aplikasi yang meniru perilaku klien di sisi server bersama dengan perilaku server di sisi Internet. Ini menyediakan:

• Soket server di sisi Internet untuk setiap layanan server. Soket server ini mendengarkan port emulator layanan server (SSESS). Port ini berbeda dari port nyata layanan server untuk menghindari kesalahan pengikatan jika SNAPT diinstal pada mesin yang sama dengan server.

• Soket emulasi permintaan klien di sisi server untuk setiap permintaan layanan server. Soket ini menyampaikan paket ke soket server layanan nyata.

• Soket server di sisi server untuk setiap layanan klien. Soket server ini mendengarkan port layanan klien nyata (CSESS). Soket server emulator layanan klien dikelompokkan berdasarkan ID CNAPT. Jika mereka menggunakan port yang sama, mereka terikat ke alamat IP virtual yang berbeda untuk menghindari kesalahan pengikatan.

• Soket emulasi permintaan server di sisi Internet untuk setiap permintaan layanan klien. Soket ini menyampaikan paket ke CSESS yang tepat yang disediakan oleh ID CNAPT yang sesuai.

• Soket kontrol di sisi Internet yang digunakan untuk komunikasi CNAPT–SNAPT. Soket ini digunakan untuk mentransmisikan paket jabat tangan selama serah terima.

Selama komunikasi normal, CNAPT meneruskan permintaan klien ke SNAPT yang mengelola server. Setelah menerima permintaan klien, SNAPT memprosesnya dan pada gilirannya menyampaikannya ke server yang sesuai. Jalur respons server mencerminkan jalur permintaan klien.

Selama fase serah terima, aliran data aplikasi terganggu di CNAPT, yang berhenti meneruskan paket IP keluar yang dihasilkan oleh klien. SNAPT juga berhenti meneruskan semua paket keluar yang dihasilkan oleh server. Paket-paket yang sudah disimpan dalam buffer transmisi dari soket CNAPT dan SNAPT akan diteruskan, masing-masing, ke SNAPT dan CNAPT setelah selesainya serah terima.

Mekanisme jendela TCP untuk kontrol aliran dieksploitasi untuk menjeda aplikasi, menghindari kebutuhan ruang buffer ekstra yang mungkin besar untuk paket keluar selama serah terima.

Untuk meningkatkan skalabilitas dalam WMN, beberapa SNAPT dapat diposisikan pada MR yang berbeda di seluruh jaringan. Komponen tambahan, Pengontrol, digunakan untuk

memilih SNAPT yang sesuai saat runtime. Metrik yang digunakan untuk pemilihan SNAPT adalah kombinasi dari:

• Bandwidth yang Tersedia. Jika SNAPT saat ini kelebihan beban, SNAPT dengan beban jaringan yang lebih kecil lebih disukai. • Latensi Jaringan. WiOptiMo mengklasifikasikan lalu lintas pengguna untuk meningkatkan pengalaman pengguna dengan menghubungkan

ke SNAPT yang lebih sesuai untuk fitur lalu lintas saat ini.

• Keterlambatan Paket. Prioritas diberikan kepada SNAPT yang memastikan paket terkecil

menunda.

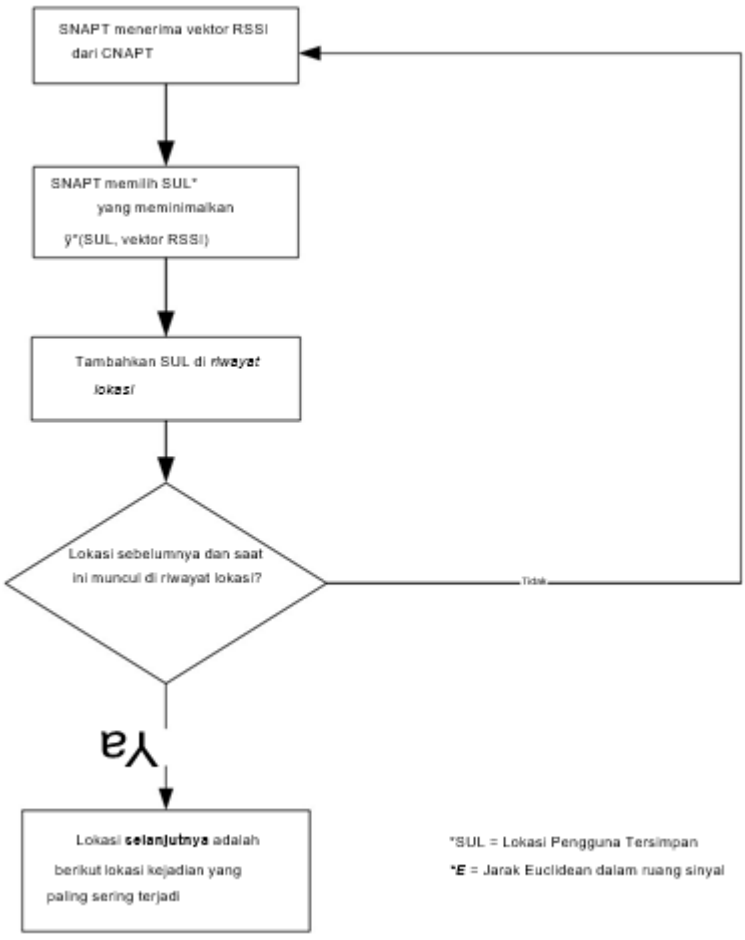
• Kehilangan Paket. Protokol mirip TCP menggunakan rasio kehilangan paket sebagai ukuran kemacetan dan oleh karena itu mengurangi throughput melalui saluran nirkabel yang berisik bahkan jika ketersediaan bandwidth tinggi.

WiOptiMo melakukan pemantauan pasif pada lapisan fisik dan pemantauan aktif pada lapisan jaringan/aplikasi untuk mengambil keputusan serah terima yang optimal. Dalam hal pengukuran lapisan fisik, WiOptiMo secara berkala mengambil sampel nilai kekuatan sinyal mentah yang diterima (RSSI) dari NIC nirkabel: nilai sampel di bawah ambang kritis, serah terima dimulai. Pemindaian terus-menerus juga dilakukan untuk menemukan keberadaan titik akses dengan RSSI yang lebih kuat bahkan sebelum sinyal titik akses terkait telah terdegradasi di bawah ambang batasnya. Layer-3 melaporkan keberadaan alamat IP saat ini. Selanjutnya, pemantauan lapisan aplikasi aktif diwujudkan dengan menyuntikkan beberapa paket kontrol dan mengamati perilakunya: paket ICMP ECHOREQUEST dikirim melalui tautan saat ini dan, jika tidak digaungkan dalam batas waktu yang diminta, tautan dianggap rusak, dan handoff dipicu .

Terakhir, dalam konteks mesh, WiOptiMo menggunakan teknik untuk lokalisasi perangkat seluler, untuk merampingkan serah terima yang dijalankan jaringan. Mekanisme ini memprediksi hilangnya konektivitas dengan melacak pergerakan perangkat berdasarkan RSSI pengukuran.

Secara khusus, CNAPT secara berkala membuat vektor RSSI dengan pengukuran RSSI dari semua AP tetangga. Jika jarak Euclidean [29] antara dua vektor RSSI yang berdekatan lebih tinggi dari ambang tetap, CNAPT mendeteksi bahwa pengguna telah pindah ke lokasi yang berbeda dan mengirimkan vektor RSSI saat ini ke SNAPT ke yang terhubung. SNAPT melacak rute pengguna, memelihara informasi mengenai lokasi pengguna saat ini dan sebelumnya. SNAPT juga memelihara grafik lokasi, yang berisi kumpulan vektor RSSI yang diukur di setiap lokasi yang ditetapkan. Itu juga menyimpan riwayat lokasi, yang merupakan urutan dari semua lokasi yang dikunjungi. SNAPT menghitung jarak Euclidean antara vektor RSSI yang dikirim oleh CNAPT dan daftar semua lokasi yang disimpan dalam grafik lokasi: lokasi dengan jarak Euclidean minimal diasumsikan bertepatan dengan lokasi CNAPT saat ini.

Kemudian, SNAPT jika lokasi sebelumnya dan saat ini terkait dengan CNAPT terjadi di riwayat lokasi, dan memprediksi lokasi berikutnya yang akan dikunjungi perangkat. Informasi ini digunakan untuk mempersiapkan serah terima secara proaktif, sehingga mengurangi latensi serah terima dan menyediakan mobilitas yang lancar bagi pengguna. Seluruh proses diilustrasikan pada Gambar 5.8.



5.3 JARINGAN SENSOR NIRKABEL

Mobilitas dalam jaringan sensor nirkabel (WSNs) belum dieksplorasi dengan baik dan masih menunjukkan banyak celah. Banyak peneliti membedakan antara mobilitas berbasis sink dan mobilitas berbasis node. Dalam mobilitas berbasis wastafel [31], WSN statis dieksplorasi oleh wastafel bergerak (dengan mobilitas yang terkontrol atau setidaknya dapat diprediksi) untuk meminimalkan penundaan dan konsumsi energi untuk node sensor. Ini adalah contoh pemanfaatan mobilitas untuk meningkatkan kinerja seluruh sistem, daripada menangani mobilitas yang ada.

Sebaliknya, mobilitas berbasis node mengasumsikan mobilitas node yang tidak terkontrol dan sudah ada sebelumnya, di mana jaringan perlu mengakomodasi dan menanganinya. Di sini, ada banyak pendekatan berbeda. Sebagian besar platform WSN berbasis IEEE802.14.5 [32], yang tidak menyediakan dukungan mobilitas default. Salah satu upaya untuk memecahkan masalah adalah dengan menangani mobilitas pada lapisan MAC dan banyak protokol MAC yang berbeda

telah diusulkan, kebanyakan dari mereka memiliki skema siklus tugas yang kompleks, seperti MS-MAC [33].

Namun, sepengetahuan kami, tidak ada protokol MAC yang mendukung mobilitas yang pernah diuji di lingkungan nyata dan pada perangkat keras nyata. Pendekatan lain berbagi penanganan mobilitas di beberapa lapisan, seperti Zigbee. Namun, telah ditunjukkan bahwa Zigbee tidak mendukung mobilitas secara efisien [34].

Solusi lain yang agak populer adalah dengan menggunakan protokol mobilitas berbasis IP. Mereka biasanya dibedakan menjadi pendekatan mobilitas berbasis lebih dan yang berbasis jaringan.

Keluarga pertama mengandalkan motes hanya untuk menangani mobilitasnya sendiri, seperti solusi standar MIPv6 [35]. Di sisi lain, pendekatan berbasis jaringan adalah PMIPv6 [36].

Pada saat yang sama, ada juga masalah lain yang muncul dari WSN seluler. Salah satu yang paling menantang adalah kemampuan aksesibilitas dan debugging, saat node bersifat seluler.

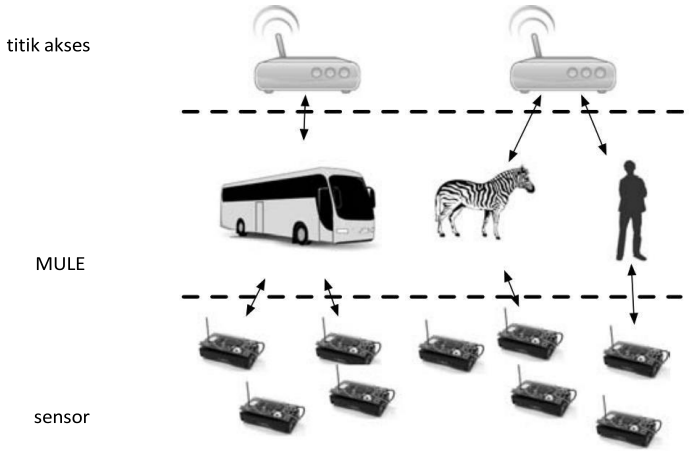
Dalam WSN statis, aksesibilitas dengan mudah disediakan oleh koneksi kabel ke masing-masing node, dan dengan demikian debugging dan visibilitas penuh dimungkinkan. Namun, dengan node seluler, pendekatan seperti itu menjadi tidak praktis. Untuk mengatasi masalah ini, beberapa teknik de bug dan visibilitas over-the-air telah diusulkan—misalnya, Marionette [37] untuk TinyOS.

Pada bagian selanjutnya kami akan menyajikan beberapa solusi yang dibahas di sini secara lebih rinci, lebih tepatnya MULE [38], yang merupakan arsitektur mobilitas berbasis sink dan

FLEXOR, yang merupakan arsitektur perangkat lunak pengelolaan mobilitas untuk mengaktifkan debugging dan kendali jarak jauh dari node seluler.

5.3.1 Mobilitas Berbasis Sink

Salah satu arsitektur yang mendukung mobilitas pertama, yang diusulkan terutama untuk domain WSN, adalah konsep MULE (Mobile Ubiquitous LAN Extensions) [38] atau sederhananya bagal data. Gagasan umumnya adalah mengumpulkan data sensorik dari bagian jaringan sensor yang terputus dengan menggunakan entitas bergerak, yang "membawa" data ke data sink. Arsitektur umum digambarkan pada Gambar 5.9. Ini terdiri dari tiga tingkatan: sensor, bagal, dan titik akses. Sensor mengumpulkan data, bagal membawa data dari sensor ke titik akses, dan titik akses menyimpan data sensorik. Tujuan utama arsitektur ini adalah untuk menghindari perutean multihop data sensorik dari sensor ke akses



Gambar 5.9 Arsitektur umum bagal data dengan tiga tingkatannya.

poin dan untuk menjembatani partisi jaringan yang terputus. Bagal data dapat berupa entitas seluler apa pun yang tersedia: bus, manusia, hewan, dan sebagainya.

Salah satu tantangan utama arsitektur adalah menemukan data bagal di sekitar sensor. Untuk ini, bagal mengirimkan pesan penemuan secara teratur. Mendengarkan pada sensor perlu diminimalkan dan didaur ulang. Properti utama dari arsitektur MULEs dapat diringkas sebagai:

• Efisiensi Energi. Energi disimpan karena sensor berkomunikasi hanya melalui jarak pendek dan tidak meneruskan data dari sensor lain.

• Kekokohan. Kegagalan MULE individu dalam jaringan meningkatkan end-to mengakhiri latensi, tetapi tidak menggagalkan pengiriman data.

• Skalabilitas. Menambahkan sensor dan bagal baru itu sepele dan tidak memerlukan apa pun konfigurasi ulang.

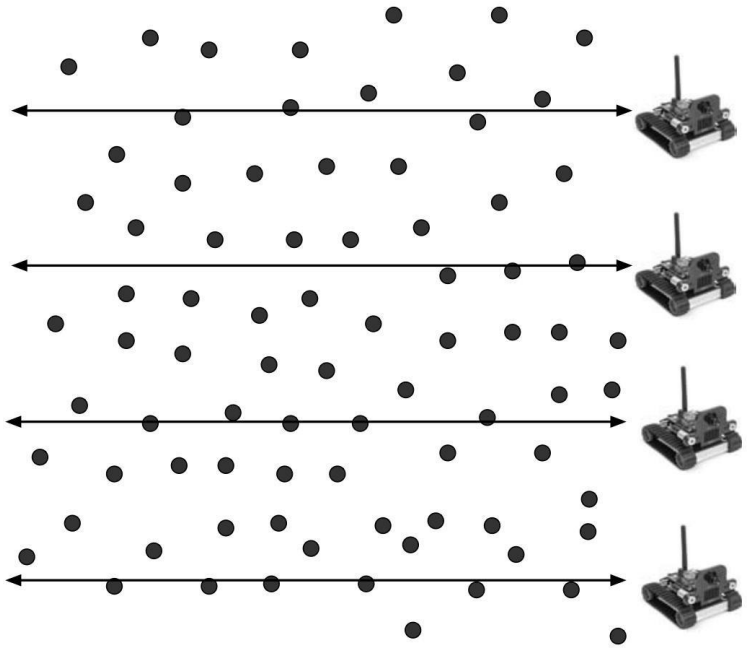
• Kesederhanaan. Proses penyebaran data sangat sederhana dan ringan. • Latensi. Di sisi lain, latensi dalam sistem bergantung pada pergerakan bagal, yang tidak dapat diprediksi dan dapat menjadi signifikan.

• Penyampaian Upaya Terbaik. Pengiriman data tidak dijamin.

Arsitektur MULE sangat umum, karena tidak membuat asumsi tentang pola pergerakan, ketersediaan atau jumlah bagal dalam jaringan.

Ini telah mengilhami banyak karya lain, yang memperluas ide orisinal melalui jumlah dan/atau pergerakan bagal yang terkontrol, atau mengimplementasikan arsitektur dalam aplikasi nyata. Dalam referensi 39, sebuah studi dengan satu entitas bergerak yang dikendalikan (robot) disajikan. Robot bergerak di sepanjang topologi sensor seperti rantai dan menyesuaikan

kecepatannya tergantung pada sensor yang ditemuinya dan jumlah paket yang perlu mereka transfer. Karena sensor dan garis pergerakan bagal adalah tetap, protokol multihop diperlukan untuk menghubungkan sensor lebih jauh dari jalur bagal ke bagal. Ini adalah



Gambar 5.10 Beberapa bagal data terkontrol, menurut referensi 40, bergerak sepanjang jalur tetap.

dicapai dengan menjalankan protokol pengumpulan bangunan pohon (seperti Directed Diffusion) ke node

yang paling dekat dengan jalur bagal. Saat bagal data bergerak di sepanjang jalurnya, ia bertemu dengan sensor dan mengunduh data mereka dan anak-anak mereka.

Penulis yang sama memperluas studi mereka ke beberapa robot seluler di referensi 40.

Di sini, penulis kembali berasumsi bahwa bagal data bergerak sepanjang garis dan kecepatannya dapat disesuaikan. Tantangan utama yang mereka hadapi dengan banyak bagal data adalah untuk memilih jumlah mereka secara optimal, mengingat nomor dan posisinya, dan untuk menangani node sensor,

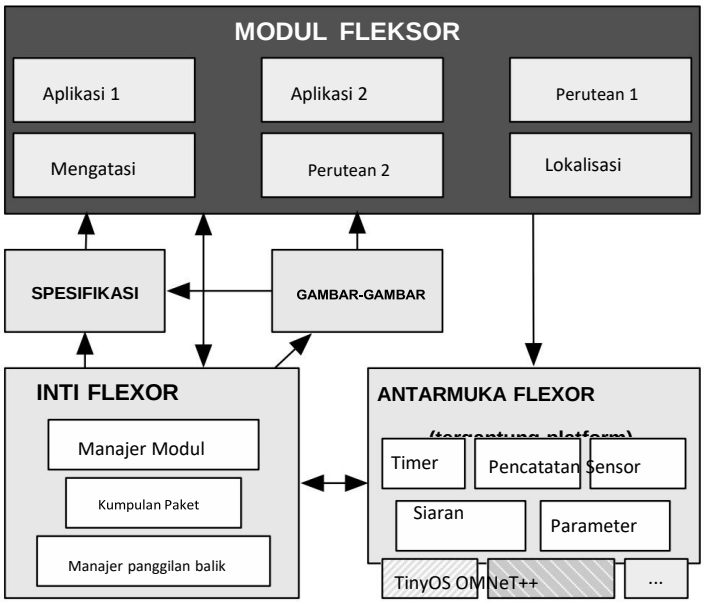
yang ditutupi oleh dua bagal data. Skenarionya digambarkan pada Gambar 5.10. Kerugian utama dari arsitektur ini adalah kebutuhan akan banyak perutean dan kebutuhan untuk mengidentifikasi node mana yang berada di sepanjang jalur bagal.

5.3.2 FLEXOR: Arsitektur Perangkat Lunak yang Mengaktifkan Mobilitas

Upaya kami sendiri untuk mengembangkan FLEXOR [41], arsitektur perangkat lunak baru untuk WSN, mengatasi masalah mobilitas di WSN dari perspektif yang berbeda. Alih-alih menggabungkan mobilitas dalam protokol atau algoritme apa pun dan mencoba menanganinya, kami mengidentifikasi dan mengaktifkan beberapa fungsi dasar dalam WSN tujuan umum dengan tujuan memungkinkan solusi berbasis mobilitas lebih lanjut. Gambaran FLEXOR diberikan pada Gambar 5.11.

FLEXOR terdiri dari antarmuka yang bergantung pada platform, inti yang tidak bergantung pada

platform, dan sekumpulan modul yang tidak bergantung pada platform yang disusun dalam spesifikasi, yang pada



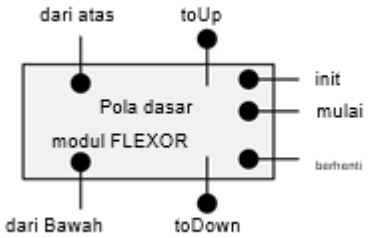
Gambar 5.11 Arsitektur umum FLEXOR.

giliran disusun menjadi gambar. Antarmuka yang bergantung pada platform mengimplementasikan fungsionalitas dasar WSN, seperti mengirim/menerima pesan, menjadwalkan pengatur waktu, membaca sensor, menulis data ke flash on-board, dan seterusnya. Ini juga menyediakan titik masuk bagi pengguna untuk menghidupkan dan mematikan fungsi. Misalnya, pengguna mungkin ingin secara aktif mengontrol status komponen tertentu (seperti radio, Flash, atau sensor individual) dengan mengaktifkan atau menonaktifkannya.

Fungsi Antarmuka. Fungsi antarmuka FLEXOR mencakup fungsi dasar seperti menjadwalkan/ menghapus timer, mengirim/menerima pesan melalui antarmuka radio dan serial, mendapatkan waktu lokal saat ini, ID node, atau parameter lainnya, menulis ke log, dan sebagainya.

Antarmuka adalah komponen utama yang memungkinkan implementasi platform-independen dari berbagai modul dan menyelaraskan berbagai sistem operasi, platform, dan bahkan simulator jaringan ke antarmuka khusus WSN yang sama. Perhatikan bahwa FLEXOR tidak menyediakan primitif pemrograman tingkat tinggi atau struktur data seperti tabel tetangga atau komunikasi multihop. Satu-satunya primitif yang disediakan FLEXOR adalah siaran satu-hop upaya terbaik, bersama dengan serangkaian protokol akses media yang memungkinkan untuk diaktifkan oleh pengguna. Ada lagi yang perlu diimplementasikan oleh pengguna dalam modul.

Modul. Modul FLEXOR adalah blok bangunan dasar untuk semua aplikasi yang dikembangkan di FLEXOR. Gambar 5.12 menyajikan struktur minimal dasar mereka. Pola dasar dasar modul FLEXOR terdiri dari tujuh fungsi antarmuka: init, start, stop, fromUp, fromDown, toUp, toDown. Tiga fungsi antarmuka pertama dipanggil di



Gambar 5.12 Pola dasar modul dasar FLEXOR.

node startup (init) serta setiap kali modul dinyalakan (start) atau dimatikan (stop) saat runtime. Ini memungkinkan pelestarian keadaan internal modul setiap saat.

Empat fungsi antarmuka lainnya memungkinkan sebuah modul untuk berinteraksi dengan modul lainnya. Modul menerima paket melalui fungsi fromUp, fromDown dan mengirimkan paket ke modul lain melalui toUp, toDown. Koneksi antar modul tidak statis, tetapi dikelola saat runtime oleh manajer modul (lihat di bawah). Dalam hal fungsionalitas internalnya, modul benar- benar bebas untuk mengimplementasikan protokol, layanan, algoritme, atau aplikasi apa pun. Praktik implementasi yang baik adalah menjaga agar modul tetap kecil dan fokus pada satu layanan atau fungsionalitas dan untuk mencapai fungsionalitas penuh yang diperlukan dengan menghubungkan beberapa modul. Perhatikan juga bahwa hanya modul yang diizinkan untuk menghasilkan atau menerima paket/pesan, meskipun tidak diharuskan melakukannya.

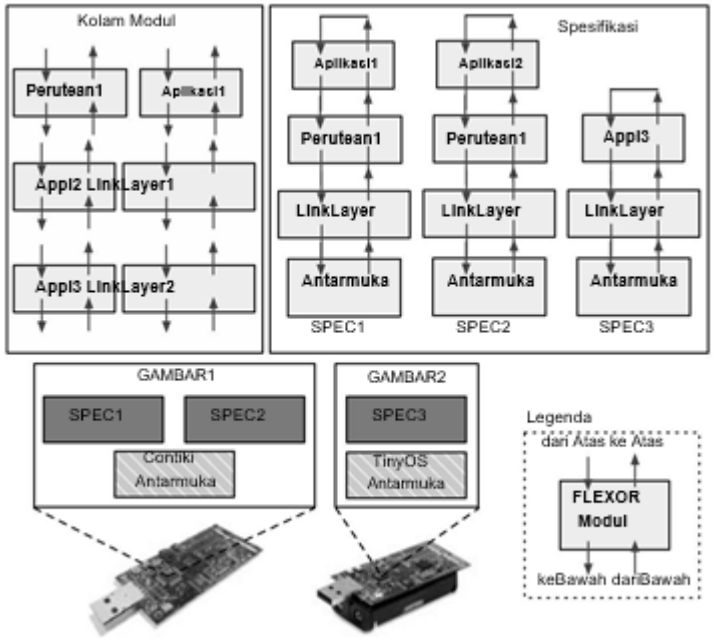
Selanjutnya, pengguna dapat memperluas arketipe yang disediakan dengan masuk baru/

gerbang keluar dan dengan demikian memungkinkan tumpukan dua dimensi.

Spesifikasi, Gambar, dan Pengelola Modul. Spesifikasi terdiri dari satu set modul dan interkoneksinya ke dalam tumpukan. Tumpukan bisa tradisional dan linier, tetapi juga dua dimensi, tergantung pada kebutuhan pengguna dan arketipe modul yang digunakan. Beberapa spesifikasi dapat hidup berdampingan pada node yang sama saat runtime, tetapi hanya satu spesifikasi yang dapat aktif pada waktu tertentu. Modul dapat dibagi di antara spesifikasi yang berbeda atau tidak, tergantung pada kebutuhan aplikasi. Satu set spesifikasi hidup berdampingan yang berada bersama dalam memori dari satu node disebut gambar. Contoh dua gambar disajikan pada Gambar 5.13. Satu-satunya tugas manajer modul adalah bertukar spesifikasi sebagai konsekuensi dari perintah internal atau eksternal (panggilan balik). Itu juga dapat menerima deskripsi spesifikasi (dengan modul yang dimuat

sebelumnya) dan dapat dengan mudah diperpanjang untuk menerima gambar modul baru dan menginstalnya.

Manajer Panggilan Balik dan Modul Panggilan Balik. Manajer panggilan balik adalah komponen yang menangani panggilan balik jarak jauh secara lokal di node. Semua komponen lain (modul, pengelola modul, dan antarmuka) dapat mendaftarkan dan membatalkan pendaftaran callback, yang diidentifikasi oleh pengidentifikasi callback dan pointer ke fungsi callback. Manajer panggilan balik menerima perintah pemanggilan panggilan balik dengan node tujuan dan sumber



Gambar 5.13 Spesifikasi FLEXOR dan contoh gambar

id, nomor urut, dan id panggilan balik. Setelah menerima perintah callback seperti itu, ia memeriksa apakah perintah ini sudah diketahui (dengan memeriksa id node sumber dan nomor urut), apakah id tujuan cocok dengan id node lokal, dan apakah callback dengan id ini terdaftar di node ini . Jika berhasil, ini akan memanggil fungsi callback terdaftar. Ada juga kemungkinan untuk mengirim beberapa parameter ke fungsi callback. Manajer callback dibantu oleh modul callback, yang diimplementasikan sebagai modul FLEXOR tipikal dan perlu menjadi bagian dari tumpukan modul spesifikasi, jika kemampuan untuk

menerima callback dari luar diperlukan. Ingatlah bahwa hanya modul FLEXOR yang dapat menghasilkan dan menerima paket. Jika tidak, hanya panggilan balik lokal yang

dimungkinkan, yang dapat digunakan untuk pemberitahuan peristiwa lokal dan komunikasi lintas lapisan.

Dukungan mobilitas FLEXOR berasal dari arsitektur itu sendiri, serta dari modul yang diimplementasikan secara spesifik. Manajer panggilan balik dan modul panggilan balik yang sesuai adalah contoh untuk ini. Prinsip utama FLEXOR adalah untuk mendukung kemudahan manajemen dan konfigurasi jaringan sensor tanpa infrastruktur, demikian juga jaringan sensor seluler. Keuntungan dari pendekatan ini adalah FLEXOR tidak mengajukan persyaratan apa pun tentang node mana yang

bergerak, jenis mobilitas apa yang digunakan, dan sebagainya. Alih-alih, ini memungkinkan fungsi manajemen

sederhana, yang memudahkan pengembangan protokol dan algoritme kompleks, baik untuk node sensor statis maupun seluler.

5.4 KESIMPULAN

Dalam bab ini kami menyajikan protokol dan arsitektur untuk mendukung mobilitas dalam jaringan wireless mesh dan jaringan sensor.

Merujuk pada WMN, dukungan mobilitas memerlukan penyediaan handoff ketika perangkat seluler bergerak dalam domain yang sama (mobilitas mikro) atau di antara sumber daya yang berbeda (mobilitas makro). Selain itu, dalam WMN, handoff dapat terjadi di antara tipe jaringan yang berbeda atau di antara jaringan dengan tipe yang sama. Terakhir, dalam aWMN, handoff dapat sepenuhnya di bawah kendali jaringan (jaringan dieksekusi) atau dimulai oleh terminal seluler (dieksekusi seluler). Kami melakukan survei terhadap pendekatan utama dalam literatur untuk mengoptimalkan proses handoff dan menyajikan beberapa arsitektur jaringan yang menyediakan dukungan mikromobilitas dan/atau makromobilitas. Kami mengklasifikasikan metode berdasarkan kriteria sebelumnya dan menjelaskan kelebihan dan kekurangannya.

Keadaan seni untuk arsitektur pendukung mobilitas untuk sensornets sangat langka. Yang pertama kami sajikan di sini, MULE, mengeksploitasi mobilitas yang sudah ada di jaringan untuk mengirimkan data secara lebih efisien di sink. Dari sudut pandang ini, ini lebih merupakan konsep penyebaran data daripada arsitektur mobilitas penggunaan umum.

Di sisi lain, FLEXOR tidak menyediakan protokol atau algoritme pendukung mobilitas siap pakai, tetapi berkonsentrasi pada fungsi dan primitif manajemen penggunaan umum. Banyak pekerjaan yang perlu diinvestasikan lebih lanjut ke dalam topik ini untuk mendefinisikan dan

mengimplementasikan kerangka kerja atau arsitektur penggunaan umum untuk mendukung jaringan sensor selule

CHAPTER 6 KERJA EKSPERIMENTAL DIBANDINGKAN SIMULASI DALAM STUDI PADA JARINGAN AD HOC SELULER

6.1 PENDAHULUAN

Simulator dan testbed fisik telah digunakan secara luas oleh komunitas riset jaringan ad hoc seluler dalam pengembangan sistem dan protokol yang baru dan lebih baik. Sementara model analitik memberikan banyak wawasan tentang kinerja desain yang diusulkan, mereka tidak memiliki detail yang cukup untuk menangani kompleksitas protokol dan implementasi perangkat terbaru dalam jaringan ad hoc seluler. Setiap pendekatan evaluasi memiliki kelebihan dan kekurangan. Manfaat menggunakan simulasi termasuk penerapan yang mudah dan cepat, lingkungan yang dapat dikontrol dan fleksibel, skalabilitas yang lebih baik, dan hasil yang dapat diulang. Namun, cukup mudah untuk menghasilkan simulasi yang tidak memiliki kredibilitas; pada kenyataannya, pendapat menyebar bahwa beberapa hasil yang diterbitkan menderita masalah ini [1]. Keandalan hasil simulasi dapat terancam terutama dalam dua cara: praktik simulasi yang buruk (kesalahan dalam pengaturan atau desain simulasi) atau asumsi model yang buruk [2]. Di sisi lain, testbed sebagian besar menghindari masalah yang terkait dengan pemodelan yang tidak sempurna dan dapat memberikan sesuatu yang mendekati lingkungan operasi target. Meski begitu, mereka jauh lebih sulit untuk membuat prototipe, mengkonfigurasi, dan menyebarkan, terutama jika kondisi operasi yang berbeda perlu dipertimbangkan. Dengan demikian, penting untuk memahami apa yang ditawarkan setiap opsi untuk membuat pilihan yang tepat selama validasi ide.

Dalam bab ini kita akan meninjau testbed dan alat simulasi yang ada dan kemudian membahas masalah yang menyebabkan kesenjangan antara hasilnya. Kami juga akan berpendapat tentang kemungkinan jalan untuk peningkatan alat simulasi dan lingkungan testbed. Kami berharap, sebagai hasilnya, pembaca dapat membuat keputusan berdasarkan informasi tentang strategi evaluasi yang sesuai untuk solusi mereka.

6.2 TINJAUAN SIMULASI JARINGAN AD HOC SELULER ALAT DAN PLATFORM EKSPERIMENTAL

Pada bagian ini kami akan memberikan ikhtisar simulator dan testbed yang ada, dengan fokus pada fitur dan karakteristik utamanya untuk memberikan gambaran yang baik kepada pembaca tentang solusi yang ada untuk penilaian MANET. Simulator dan testbed adalah dua alat yang dapat dimanfaatkan peneliti untuk menilai kinerja solusi MANET. Sejauh ini, penggunaan simulator telah dominan seperti yang ditunjukkan dalam statistik yang disajikan dalam referensi 3. Memang, modul dan ekstensi untuk jaringan ad hoc seluler telah disertakan di hampir semua simulator yang tersedia, baik open source maupun komersial.

Baru-baru ini, proliferasi perangkat keras WLAN yang murah telah mendorong penggunaan testbed yang direkomendasikan untuk evaluasi kinerja karena keakuratan dan keandalannya. Meskipun demikian, simulator masih lebih disukai, terutama jika diperlukan penerapan yang cepat.

6.2.1 Alat Simulasi

Dengan memberikan ikhtisar tentang simulator jaringan yang ada yang mendukung jaringan ad hoc seluler, kami bertujuan untuk mengilustrasikan keuntungan dan kerugian yang biasanya dikaitkan dengan struktur umum setiap simulator sebelum masuk ke rincian implementasi modul nirkabel masing-masing di Bagian 6.3.5.

Survei ini terutama berfokus pada simulator berikut yang paling banyak digunakan oleh para peneliti, menurut statistik penggunaan antara tahun 2000 dan 2005 yang disajikan dalam referensi 3: ns2 [4], GloMoSim [5], QualNet [6] dan Opnet [7] . Untuk mempertimbangkan simulator akun yang baru-baru ini mendapatkan popularitas, kami juga pertimbangkan hal berikut: ns3 [8], OMNeT++ [9] dan Jist [10]. Beberapa survei mendalam tentang simulator jaringan dapat ditemukan di referensi 11–13.

ns-2 [4] adalah simulator jaringan peristiwa diskrit paling populer yang digunakan oleh para peneliti.

Ini telah dikembangkan sebagai proyek sumber terbuka sejak 1989 dan ditulis dalam C++ dan OTcl. Sementara yang pertama digunakan untuk memprogram inti simulasi, yang terakhir diadopsi untuk menyusun skenario simulasi secara dinamis tanpa harus mengkompilasi ulang seluruh kode sumber setiap saat. Sebagai simulator jaringan open source yang paling banyak digunakan, keunggulan utamanya adalah banyaknya proyek eksternal yang digunakan untuk menambah fungsionalitas baru dan mendukung jaringan baru. Perilakunya sangat dipercaya dalam komunitas jaringan, karena merupakan proyek tertua dan paling banyak digunakan. Meskipun awalnya dirancang untuk jaringan kabel, modul nirkabel telah digunakan sebagai kontribusi eksternal dan kemudian dimasukkan ke

dalam versi resmi. Kelemahan utamanya adalah kompleksitas inheren yang disebabkan oleh kurangnya

modularitas, yang membuat penerapan fitur-fitur baru dalam inti asli menjadi tidak penting [13]. Kelemahan lainnya adalah kurangnya alat resmi untuk pengumpulan dan analisis statistik; bahkan jika solusi eksternal dapat ditemukan, versi resmi hanya menawarkan kemungkinan untuk menyimpan jejak yang harus diproses untuk mengumpulkan statistik.

ns3 [8] adalah revisi besar baru dari ns2. Seperti pendahulunya, ns3 bergantung pada C++ untuk implementasi model simulasi. Karena sering mengkompilasi ulang kode sumber tidak menjadi masalah saat ini, skenario didefinisikan dalam C++ murni atau secara opsional dalam Python. Inti telah dirancang dengan skalabilitas dalam pikiran untuk mendukung pengembangan di masa depan.

Meskipun ns3 tidak kompatibel dengan sebagian besar basis kode ns2 , beberapa proyek telah di-porting. Selain itu, beberapa fitur baru telah dikembangkan.

Salah satu yang paling menarik adalah dukungan integrasi dengan perangkat nyata. Meskipun perhatian dan upaya pengembangan pada ns3 semakin meningkat, proyek ini masih tergolong muda dan beberapa fungsi penting seperti modul pengumpulan statistik masih harus diimplementasikan.

GloMoSim [5] adalah simulator jaringan nirkabel terpopuler kedua. Ditulis dalam Parsec, ini mendapat manfaat dari kemampuan bahasa ini untuk berjalan di lingkungan paralel. Berbeda dengan ns2, paralelisasi memungkinkan GloMoSim menjalankan skenario yang lebih kompleks; jaringan yang disimulasikan dipartisi menjadi subnetwork yang berbeda, masing-masing dijalankan oleh prosesor yang berbeda. Fitur ini adalah alasan utama mengapa GloMoSim digunakan sebagai dasar simulator QualNet komersial. Kurangnya dokumentasi dan diskontinuitas proyek adalah kerugian utama.

QualNet [6] adalah simulator komersial berdasarkan inti dari GloMoSim. Inti dasar sebagian besar telah diperluas dan satu set protokol dan model baru didukung.

Proyek saat ini dipertahankan, dan dokumentasi yang diperbarui tersedia. Seperangkat alat grafis disediakan untuk membantu pengguna menentukan skenario simulasi, dan mengumpulkan serta menganalisis pengukuran.

Opnet [7] adalah simulator peristiwa diskrit komersial yang mapan yang terutama digunakan oleh perusahaan untuk mensimulasikan organisasi jaringan mereka. Ini menawarkan sejumlah besar model untuk jaringan kabel dan nirkabel melalui Wireless Suite-nya. Antarmuka pengguna grafis membantu pengguna dalam menentukan skenario simulasi dan menganalisis hasil. Semua model secara resmi dikembangkan oleh perusahaan itu sendiri yang bertanggung jawab atas validasinya. Pengguna memiliki opsi untuk menentukan modul baru melalui grafik antarmuka tetapi prosedurnya bisa rumit. Kelemahan utamanya adalah bahwa setiap modul baru harus didefinisikan sebagai mesin keadaan terbatas yang sulit untuk di-debug, diperluas, dan divalidasi. Selain itu, tindakan di balik setiap negara dijelaskan melalui bahasa yang tidak standar, Proto-C.

OMNeT++ [9] adalah platform simulator yang ditulis dalam C++ untuk simulasi kejadian diskrit tujuan umum. Namun, ini terutama diterapkan pada simulasi jaringan karena paket INET -nya yang menyediakan kumpulan protokol Internet. Selain itu, paket model lain seperti Paket Mobilitas dan Castalia memungkinkan simulasi jaringan ad-hoc seluler. OMNeT++ memiliki struktur modular; setiap modul atom (modul sederhana) dapat digunakan untuk menghasilkan entitas yang lebih kompleks (modul majemuk). Selain strukturnya yang luas dan fleksibel, keunggulan lainnya adalah dokumentasi yang besar dan ditulis dengan baik tersedia untuk disertakan dengan serangkaian tutorial di situs web proyek. Skenario simulasi ios dijelaskan melalui bahasa tingkat tinggi yang disebut Network Description (NED).

Skenario yang lebih kompleks dapat disusun dengan bantuan antarmuka pengguna grafis yang disediakan dalam paket standar. Satu-satunya kelemahan kecil adalah kurangnya dukungan untuk pengumpulan statistik dan analisis data.

Jist [10] adalah simulator tujuan umum yang ditulis dalam Java. Penulis menyediakan sebuah paket, Swans [14], yang mengimplementasikan kemampuan simulasi jaringan ad hoc seluler nirkabel. Seperti OMNeT++, Jist memiliki struktur modular yang terdiri dari entitas: setiap entitas mewakili elemen jaringan yang perilakunya dijelaskan oleh kelas Java. Tersedia mekanisme paralelisasi yang sangat sederhana: beban simulasi dapat didistribusikan tidak hanya pada banyak CPU di dalam mesin yang sama tetapi juga ke server yang berbeda. Tidak ada antarmuka default untuk mengonfigurasi skenario simulasi yang disediakan; baik kode Java atau file konfigurasi yang diuraikan pada waktu proses dapat diadopsi. Meskipun Swans adalah proyek yang relatif baru, pengembangan inti Jist tidak lagi dikejar oleh penulis aslinya.

6.2.2 Platform Eksperimental

Platform eksperimental dapat dikategorikan secara luas ke dalam penyebaran dan emulasi dunia nyata. Seperti yang disarankan oleh istilah tersebut, yang pertama mengacu pada testbed yang telah

disiapkan untuk mereplikasi karakteristik penerapan target seperti ukuran jaringan dan saluran nirkabel yang tidak dimodifikasi untuk menghasilkan pengamatan yang sangat mirip dengan apa yang diharapkan dalam penerapan "langsung". Namun, menyiapkan lingkungan ini melibatkan tingkat kerumitan yang tinggi, dan pembangun dihadapkan pada masalah yang terkait dengan biaya, skalabilitas, pengelolaan, kontrol eksperimental, pengulangan, dan penerapan pada banyak skenario.

Selain itu, mereka mungkin memiliki batasan dalam jumlah kemungkinan topologi yang dapat dieksplorasi. Dengan demikian, sebagian besar testbed dunia nyata tidak memberikan dukungan untuk pengujian mobilitas. Nyatanya, banyak eksperimen dunia nyata dilakukan dalam jangka pendek, bukti jaringan konsep yang dirancang sesuai kebutuhan oleh para peneliti. Perlakuan komprehensif dari eksperimen ini serta testbed statis ad hoc, sensor dan jaringan mesh dapat ditemukan di referensi 15-18. Sebagai gantinya, kami fokus pada beberapa testbed dunia nyata yang mendukung jaringan ad hoc seluler.

• APE (Ad Hoc Protocol Evaluation Testbed) [19] dirancang untuk mencapai keterulangan pengujian dan reproduktifitas hasil. Itu didistribusikan sebagai paket perangkat lunak terdiri dari skrip build dan kode sumber. Perangkat lunak tersebut dipasang di lap top yang dibawa berkeliling oleh peserta tes yang bisa berjalan kaki atau di kendaraan. Eksperimen dikoreografikan melalui file skenario gerakan, yang menginformasikan peserta kapan dan di mana mereka akan bergerak selama eksperimen. Selain itu, file skenario berisi perintah dan instruksi yang akan dijalankan selama durasi percobaan. • DOME (Diverse Outdoor Mobile Environment) [20] adalah skala besar, sistem seluler yang sangat beragam testbed yang menyediakan keragaman teknologi dan spasial yang cukup besar selain keragaman temporal berdasarkan itu beroperasi selama minimal 5 tahun. Ini terdiri dari tiga komponen perangkat keras utama: node kendaraan DieselNet, setengah lusin kotak lempar yang dapat berfungsi sebagai relai, dan jaringan mesh WiFi kota dengan 26 titik akses stasioner. Konstituen utama, DieselNet, mencakup 150 mil persegi dan terdiri dari 40 bus transit yang dilengkapi dengan node berkemampuan 802.11abg. Setiap node memiliki AP 802.11g, modem USB 3G nirkabel, dan modem RF USB 900 MHz. Dengan demikian, pengendara bus dapat terhubung ke Internet melalui modem 3G, setelah terhubung dengan AP. Antarmuka WiFi juga dapat terhubung ke AP di bus lain. Kotak lempar menggunakan baterai bertenaga surya yang memungkinkan mereka menjadi nomaden. Mereka dapat dipasang di depan sepeda dan juga dapat dibiarkan diam selama beberapa jam atau hari. AP WiFi dipasang di berbagai bangunan dan tiang lampu di dalam area perkotaan, tetapi hanya AP yang dipasang di gedung yang memiliki tautan ke jaringan serat lokal.

Sistem ini juga memiliki modul perangkat lunak untuk manajemen tautan, pembaruan perangkat lunak jarak jauh, logging, dan pemantauan pemeliharaan. Saat ini, DOME tidak tersedia untuk umum, tetapi sedang direncanakan untuk memungkinkan akses jarak jauh melalui proyek GENI [21]. Selain itu, jejak eksperimen yang dijalankan di DOME dapat ditemukan di http://traces.cs.umass.edu.

• Mobile Emulab [22] disusun untuk menyediakan sensor yang dapat diakses dari jarak jauh dan platform percobaan jaringan seluler di lingkungan dalam ruangan. Eksperimen mudah diterapkan melalui front-end berbasis web Emulab [23] dengan menyediakan skrip ns-2 . Testbed berbentuk L seluas 60 m2 dengan tinggi 2,5 m.

Ada 6 robot Acroname Garcia [24] untuk memberikan mobilitas. Setiap robot memiliki komputer yang dilengkapi WiFi dan sensor mote. Pemosisian robot dilakukan melalui peralatan kamera video berbiaya menengah. Sayangnya, mulai tahun 2011, Emulab seluler tidak didukung dan tidak lagi dapat diakses publik.

• QuRiNet(Jaringan Jaring Nirkabel Quail Ridge) [25] diatur dalam cagar alam seluas 2000 acre dan menyediakan pengaturan eksperimental yang bebas dari interferensi elektromagnetik yang tidak diinginkan karena pengaturan cadangan yang jauh. Ini memiliki 38 node statis yang menjalankan protokol perutean ad hoc OLSR, dengan upaya berkelanjutan untuk menginstal node seluler secara permanen pada enam kendaraan segala medan. Mobilitas juga didukung dengan meminta peserta tes berjalan atau mengendarai kendaraan segala medan sambil membawa laptop untuk membuat skenario mobilitas. Peneliti eksternal dapat menggunakan QuRiNet dengan meminta akses ke pengelola testbed.

Gambar 6.1 menunjukkan penempatan simpul statis QuRiNet, beserta akses jalan yang digunakan peserta tes dan kendaraan segala medan.

Gambar 6.1 Tata Letak QuRiNet.

Emulator menjembatani kesenjangan antara testbed dunia nyata dan simulator lengkap.

Seperti jaringan nirkabel nyata, mereka menggunakan tumpukan jaringan dan perangkat keras nyata, tetapi mereka juga memperkenalkan beberapa tingkat kontrol pada jaringan — misalnya, dengan melemahkan sinyal frekuensi radio untuk memungkinkan miniaturisasi jaringan, atau memfasilitasi pola mobilitas yang dapat diprediksi untuk node seluler. Karena pengaruh tambahan pada jaringan,

secara komparatif lebih mudah untuk menyebarkan, menskalakan, dan memberikan hasil yang berula Selain itu, pemantauan dan manajemen jaringan tidak terlalu menjadi masalah, karena platform ini

biasanya dihosting di lingkungan laboratorium. Hal ini memungkinkan pengawasan yang lebih dekat dan penggunaan saluran out-of band untuk mengelolanya. Sayangnya, mengecilkan sistem dan mengubah sinyal RF membuatnya sulit untuk menangkap fisik dan MAC dengan tepat karakteristik lapisan diamati dalam jaringan yang lebih besar. Di bawah ini, kami memberikan ikhtisar tentang platform ini, dengan fokus pada kemampuan dan fasilitasnya untuk eksperimen seluler.

Kami membagi testbed menjadi emulator lapisan fisik dan MAC, sebuah taksonomi yang kami pinjam dari Kiess dan Mauve [15].

Emulator lapisan fisik mengimplementasikan semua lapisan kecuali lapisan fisik menggunakan sistem nyata. Dalam hal ini, sinyal RF dimanipulasi—misalnya, dengan melemahkannya—untuk meniru apa yang akan dialami dalam pengaturan dunia nyata.

• MiNT [26] meredam sinyal radio pada pemancar dan penerima menggunakan pelemah sinyal radio tetap untuk memperkecil testbed. Ini terdiri dari node inti tetap yang dikelola dari jarak jauh oleh node pengontrol melalui tautan kabel. Setiap node inti berkomunikasi dengan rekan-rekannya menggunakan NIC nirkabel IEEE 802.11b yang dipasang ke antena eksternal oleh peredam sinyal dan kabel RF.

Mobilitas dicapai dengan memasang antena pada robot LEGO Mindstorms [27]. Namun, gerakan dibatasi oleh panjang kabel RF. Terlihat bahwa jalur sinyal di MiNT memiliki pola propagasi yang mirip dengan yang dipancarkan oleh jaringan serupa yang tidak melemahkan sinyalnya. Testbed saat ini tidak dipertahankan.

• Dalam EWANT (Emulated Wireless Ad Hoc Network Testbed) [28], output yang dilemahkan dari kartu nirkabel dimasukkan ke input konektor RF 1 hingga 4. Pada output, empat antena terhubung ke node lain. Perubahan posisi disimulasikan oleh perubahan mendadak pada kekuatan sinyal yang diterima. EWANT tidak lagi aktif dipertahankan.

• Terowongan Angin Nirkabel Illinois [29] diimplementasikan dalam ruang anechoic elektromagnetik untuk menghindari kebisingan elektromagnetik yang tidak diinginkan. Ini memiliki host statis dan seluler; host seluler diimplementasikan menggunakan mobil yang dikendalikan dari jarak jauh yang membawa perangkat nirkabel. Ukuran jaringan diperkecil hanya dengan menurunkan daya pancar. Testbed tidak tersedia untuk umum. • ORBIT

(Open Access Research Testbed for Next-Generation Wireless Networks) [30,31] mengukur rentang radio dengan mentransmisikan pada level daya rendah. Untuk membuat interferensi RF buatan, ia menggunakan RF Vector Signal Generator sebagai generator interferensi.

Testbed dapat diakses dari jarak jauh, dan kode pengguna dijalankan pada node statis konstituen, yang terikat secara dinamis ke radio. Dengan mengubah pengikatan node ke radio yang berbeda, mobilitas disimulasikan melalui perubahan daya sinyal yang terpisah ini. • MeshTest [32] mengemulasi lapisan fisik dengan mengganti antena dengan kabel yang

menghubungkan perangkat nirkabel ke saklar matriks RF. Sakelar bertindak sebagai media bersama yang realistis dan memungkinkan perangkat mengalami gangguan fisik yang

sebenarnya satu sama lain. Dengan menggunakan sakelar, perangkat dapat saling berhubungan dengan pelemahan sewenang-wenang. Penundaan propagasi disimulasikan dengan menunda

pengiriman paket dan waktu pemrosesan dalam perangkat lunak pada pengirim dan penerima. Pemetaan topologi perangkat direpresentasikan sebagai matriks pelemahan ruas yang meniru kehilangan kualitas sinyal karena kehilangan jalur dan penghalang. Mobilitas dicapai dengan membiarkan nilai atenuasi bervariasi sebagai fungsi waktu. Diberikan sebuah matriks kehilangan jalur yang diinginkan, aljabar linier, dan teknik optimisasi digunakan untuk menghitung pengaturan atenuasi yang sesuai untuk sakelar matriks RF. Fading disimulasikan dengan secara acak mengganggu pelemahan yang dialami antara node sesuai dengan proses acak log-normal. Terlihat bahwa topologi acak dapat didekati dengan kira-kira 1,2 dB dari kehilangan jalur sinyal aktual.

MeshTest tidak tersedia untuk umum.

Ada kelas emulator khusus yang melakukan kebalikan dari emulasi lapisan fisik. Mereka mengimplementasikan segala sesuatu di atas lapisan PHY dalam perangkat lunak dan kemudian menggunakan perangkat keras nyata untuk mengirimkan sinyal. MiNT memiliki mode simulasi hybrid yang memanfaatkan teknik ini. Pendekatan ini juga terlihat di lingkungan jaringan sensor TOSSIM [33], EmStar/EmSim [34], dan EmTos [35].

Seperti yang ditunjukkan dalam referensi 26 dan 32, pelemahan dan miniaturisasi memiliki kelemahan. Yang terpenting, sulit untuk mengatur level daya pancar yang tepat untuk mendapatkan topologi multihop secara andal. Selain itu, sinyal dengan intensitas rendah lebih rentan terhadap interferensi dari sumber kebisingan eksternal. Juga, variasi spasial sinyal, yang

lebih menonjol pada sambungan jarak jauh, tidak sepenuhnya ditangkap oleh jaringan yang lebih kecil. Selain itu, karena kedekatan node, efek near-field dapat terjadi.

Akhirnya, kecuali testbed diatur dalam ruang anechoic terlindung, sulit untuk sepenuhnya mengontrol faktor lingkungan. Dengan demikian, hasil yang persis dapat direproduksi sulit, jika bukan tidak mungkin, untuk dicapai.

Emulator lapisan MAC mengimplementasikan semua lapisan kecuali lapisan fisik dan MAC menggunakan sistem nyata. Mereka biasanya memiliki model IEEE 802.11 yang dikembangkan dengan baik dengan dukungan untuk simulasi lapisan PHY dan MAC. Ada banyak emulator

dalam lit erature yang mengambil pendekatan ini karena biaya yang lebih rendah dan implementasi yang relatif mudah. Pengiriman dan penyaringan paket dilakukan berdasarkan kedekatan radio logis dari tujuan. Topologi dan mobilitas jaringan dibuat dengan memodifikasi aturan filter secara dinamis. Beberapa emulator memiliki komputer khusus sebagai pengontrol pusat untuk memproses pengiriman paket, topologi, dan informasi mobilitas.

Pendekatan ini diambil oleh JEmu [36], MobiNet [37], NEMAN [38] dan EMANE [39,40]. Lainnya, seperti MASSIVE [41], MobiEMu [42], NE [43], MNE [44], dan EMWIN/EMPOWER [45,46],

memiliki mekanisme kontrol terdistribusi dan menggunakan filter seperti aturan firewall di setiap node untuk merepresentasikan mobilitas dan topologi. Emulator dapat dirancang untuk terdiri dari node virtual yang direpresentasikan sebagai mesin virtual pada satu host. Ketika beberapa host digunakan, komunikasi nodal dicapai dengan Remote Procedure Calls (RPC). NEMAN MobiNet, MobiEmu, EMWIN/EMPOWER dan ManTS [47] dapat memiliki beberapa host virtual pada satu dukungan perangkat fisik sementara JEmu, NE, MASSIVE, MNE dan APE [19] memerlukan pemetaan satu-ke-satu dari mesin ke host.

Sementara testbed dunia nyata dan ditiru dapat memberikan hasil yang cukup mewakili dari apa yang akan terlihat dalam penerapan aktual, kehati-hatian harus dilakukan untuk memastikan bahwa penyiapan dan pengujian eksperimental dan metodologi pengumpulan data menjaga akurasi yang diharapkan dengan ini. sistem. Seperti yang ditunjukkan dalam referensi 48, para peneliti pertama-tama harus mengembangkan pemahaman yang baik tentang komponen jaringan nirkabel yang dimaksud. Kemudian, diperlukan karakterisasi perangkat keras jaringan yang dimaksud untuk mengidentifikasi sumber masalah potensial dan keterbatasan. Ini akan memungkinkan kalibrasi perangkat keras dan perangkat lunak yang tepat. Portoles-Comeras dkk. memberikan informasi yang sangat berharga untuk membantu mencapai tujuan tersebut [48].

Ringkasan testbed dan emulator dunia nyata dapat ditemukan di Tabel 6.1.

6.3 KESENJANGAN ANTARA SIMULASI DAN EKSPERIMEN: ISU DAN FAKTOR

Pada bagian ini kami akan memberikan ikhtisar di mana jarak antara simulator dan testbed berada. Tidak ada simulator jaringan yang akurat dan peneliti yang membutuhkan tingkat akurasi tinggi dalam hasil mereka akan ingin melakukan eksperimen mereka di testbed nyata.

Namun, jika tingkat ketidaktepatan tertentu dapat diterima, mereka dapat mengandalkan simulator jika penyimpangan kinerja dari sistem nyata tidak cukup untuk mempengaruhi hasil secara signifikan.

Karena simulasi yang sepenuhnya realistis tidak mungkin dilakukan, detail model terbatas.

Memilih tingkat detail yang sesuai bukanlah hal yang sepele. Secara khusus, untuk sistem kompleks seperti MANET, tantangannya adalah mengidentifikasi tingkat detail yang tepat yang tidak memengaruhi jawaban yang dicari peneliti. Di satu sisi, kurangnya detail dapat membawa kesimpulan yang menyesatkan yang tidak dapat diterapkan pada sistem nyata. Di sisi lain, tingkat abstraksi rendah yang tidak tepat dapat menyebabkan pemborosan sumber daya dalam hal implementasi dan waktu simulasi [49].

Terutama ketika area penelitian yang belum dijelajahi dipertimbangkan, praktik yang baik adalah mengevaluasi ketidakakuratan model melalui fase validasi yang membantu memperkirakan tingkat abstraksi yang diperlukan untuk mewakili sistem target secara memadai [50]. Dalam referensi 51, penulis menyimpulkan bahwa perbandingan langsung keluaran simulasi dengan pengukuran yang diperoleh

dari implementasi nyata adalah solusi terbaik. Namun, praktik yang baik ini tidak selalu memungkinkan: Validasi memerlukan biaya tinggi dan melibatkan penerapan sistem nyata yang tidak selalu tersedia.

Karena penggunaan simulator yang ada mendominasi solusi berbasis perangkat lunak khusus ad hoc, beberapa studi, misalnya dalam referensi 3, telah dilakukan untuk memvalidasi hasilnya. Jika validasi hasil tidak memungkinkan, literatur yang ada dapat digunakan untuk memperkirakan secara kasar keakuratan model atau simulator tertentu untuk menyimpulkan apakah tingkat detail yang diberikan sesuai untuk aplikasi tertentu. Dengan menggunakan pendekatan dari bawah ke atas, pada bagian ini kami terutama memanfaatkan studi validasi yang ada dalam literatur untuk mensurvei semua masalah utama yang memengaruhi kesenjangan antara simulasi dan eksperimen. Ringkasan disajikan pada Gambar 6.2.

6.3.1 Masalah Lapisan Fisik

Sebagian besar studi MANET berfokus pada lapisan MAC. Akibatnya, akurasi simulasi lapisan fisik sering diremehkan. Namun demikian, telah dibuktikan secara luas bahwa pemodelan lapisan PHY memiliki dampak yang signifikan terhadap hasil, dan penggunaan model radio yang tidak tepat atau serangkaian asumsi yang tidak realistis dapat mendistorsi hasil baik secara kuantitatif maupun kualitatif [52].

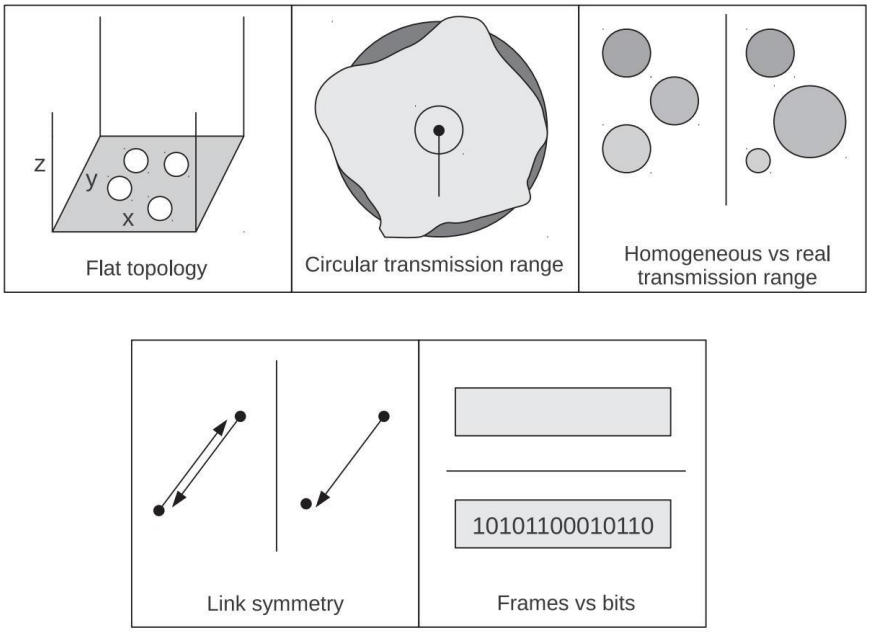
Table 6.1 Summary of Real-World Testbeds and Emulators for MANETs

Testbed	Architecture	Mobility Modeling	Wireless Medium Modeling	Physical Device to Virtual Device Mapping	Reported Size
APE [19]	Real-world testbed	Real (person)	IEEE 802.11b	1:1	37 physical
DOME [20]	Real-world testbed	Real (person, vehicular and bicycle)	IEEE 802.11, 3G, 900MHz RF Modem	1:1	72 physical
EMANE [39]	MAC layer emulator	Logical connectivity	On wired network; wireless PHY and wireless MAC emulation	1:n	Varies
EMWIN/EMPOWER [45,46]	MAC layer emulator	Logical connectivity	On wired network; 802.11 emulation	1:n	48 virtual
EWANT [28]	PHY layer emulator	Antenna switching	IEEE 802.11	1:1	4 physical
Illinois Wireless Wind Tunnel [29]	PHY layer emulator	Real (remote controlled cars)	IEEE 802.11	1:1	Varies
JEmu [36]	MAC layer emulator	Packet filtering	On wired network; centralized collision detection at frame level	1:1	12 physical
ManTS [47]	MAC layer emulator	Packet filtering	On wired network; MAC emulation	m:n	Varies
MASSIVE [41]	MAC layer emulator	Packet filtering	on wired network; no PHY or MAC emulation	1:1	13 physical
MeshTest [32]	PHY layer emulator	RF attenuation	IEEE 802.11	1:1	12 physical
MiNT [26]	PHY layer emulator	Real (robots), logical connectivity	IEEE 802.11	1:1	11 physical
MNE [44]	MAC layer emulator	Packet filtering	On wired network; no PHY or MAC emulation	1:1	Varies
MobiEmu [42]	MAC layer emulator	Packet filtering	On wired network	1:1	50 physical
Mobile Emulab [22]	Real-world testbed	Real (robots)	IEEE 802.11	1:1	31 physical
MobiNet [37]	MAC layer emulator	Logical connectivity	On wired network; wireless PHY and IEEE 802.11 emulation	m:n	200 virtual
NE [43]	MAC layer emulator	Logical connectivity	On wired network; wireless PHY and IEEE 802.11 emulation	1:1	Varies
NEMAN [38]	MAC layer emulator	Intra node pointer passing	On virtual Ethernet network	1:n	1 physical
ORBIT [30]	PHY layer emulation	Radio switching	IEEE 802.11	1:1	400 physical
QuRiNet [25]	Real-world testbed	Real (person, all-terrain vehicle)	IEEE 802.11	1:1	45 physical

Pada bagian ini kita akan membahas masalah yang terkait dengan pemodelan lapisan fisik. Kami pertama-tama memperkenalkan faktor-faktor yang dapat memperoleh hasil simulasi dari percobaan nyata dan kemudian memeriksanya secara lebih rinci.

Tujuan model lapisan fisik dalam simulator adalah untuk memprediksi apa yang terjadi pada sinyal nirkabel di dunia nyata. Dalam penyebaran nyata, setiap sinyal nirkabel dipancarkan ke luar angkasa untuk diterima oleh node mana pun. Penerima mendapatkan sinyal yang telah terdistorsi oleh pelemahan jarak transmisi dan ditumpangkan dengan sinyal nirkabel lain dari node lain dalam jaringan. Berhasil mendekode komunikasi asli adalah proses acak yang terutama bergantung pada tingkat kekuatan sinyal, kebisingan termal, dan sinyal yang mengganggu.

Dalam implementasi pertama simulator jaringan nirkabel, semua fenomena ini disimulasikan menggunakan model yang sangat sederhana berdasarkan asumsi komunikasi tetap dan jangkauan interferensi. Untuk mengatasi ketidakakuratan dramatis dari model awal, model fisik yang lebih kompleks telah digunakan.



Gambar 6.3 Asumsi yang biasa digunakan dalam model simulasi.

Keakuratan lapisan fisik bergantung pada seberapa baik faktor dari dunia nyata telah dipertimbangkan dalam model. Karena tidak mungkin memasukkan semua faktor yang ada di dunia nyata ke dalam sebuah model, seperangkat asumsi biasanya dibuat untuk hanya mempertimbangkan subset yang memiliki pengaruh paling besar. Asumsi yang dibuat mungkin hanya sedikit mempengaruhi hasil tetapi dalam kasus lain dapat berdampak serius terhadap kredibilitas mereka.

Sementara yang pertama dapat diterima, yang terakhir pada dasarnya mengkompromikan model yang menjadi tidak dapat diterapkan di dunia nyata.

Terlepas dari pengaruh mereka pada hasil, seperangkat asumsi dasar dibuat dalam model sebagian besar simulator. Adopsi mereka biasanya dianggap dapat diterima untuk mencapai tingkat abstraksi tertentu dan akibatnya menyederhanakan definisi model fisik (Gambar 6.3):

• Topologi Datar. Node terletak pada bidang dua dimensi. Masing-masing dapat ditempatkan secara unik hanya dengan menggunakan koordinat x, y. Baik dalam implementasi nyata di dalam maupun di luar ruangan, asumsi ini tidak realistis; topologi indoor multifloor dan medan berbukit di outdoor menyiratkan bahwa node dapat hadir di ketinggian yang berbeda.

• Jangkauan Transmisi Melingkar. Setiap radio diasumsikan memiliki area melingkar.

Antena directional, yang sebagian besar digunakan dalam topologi nyata untuk meningkatkan konektivitas, tidak sesuai dengan asumsi ini. Bahkan ketika hanya antena omni-directional yang dipertimbangkan, pola radiasi sebenarnya jauh dari sirkular. • Jangkauan Transmisi Homogen. Diasumsikan bahwa setiap radio dalam jaringan memiliki jangkauan transmisi yang sama. Kekuatan transmisi yang berbeda menentukan rentang

transmisi yang berbeda. Selain itu, dalam implementasi nyata, kartu nirkabel heterogen dengan sensitivitas berbeda dan dari pabrikan berbeda sering diadopsi, menghasilkan rentang yang berbeda.

• Tautan Simetri. Tautan yang dibuat antara sepasang node memiliki kualitas yang sama terlepas dari arah transmisinya. Dalam tautan nyata, asimetri berasal dari kekuatan transmisi yang berbeda, disengaja atau tidak.

• Bingkai sebagai Entitas Atom. Bingkai dianggap sebagai entitas yang tidak terpisahkan. Bingkai, bukan sedikit, adalah tingkat perincian terbaik di dalam simulator.

Ini menunjukkan bahwa korupsi satu bit tidak dipertimbangkan dan setiap frame berhasil diterima atau tidak secara keseluruhan. Asumsi ini tidak memperhitungkan efek redundansi yang diadopsi dalam kode transmisi dan mekanisme pemulihan kesalahan.

Meskipun berdampak pada hasil simulasi, asumsi yang disebutkan di atas biasanya diterima begitu saja dalam simulator MANET karena masing-masing dianggap sebagai pengorbanan yang dapat diterima untuk membantu mengurangi kompleksitas tanpa mengurangi akurasi model secara keseluruhan [53].

Terlepas dari ini, serangkaian faktor utama lainnya secara luas dianggap relevan [52,54,55], dan mengevaluasi dampaknya telah menjadi fokus dari beberapa studi validasi dalam literatur [56-58]. Beberapa di antaranya adalah sebagai berikut:

• Pembukaan Transmisi. Preamble (sinyal preamble plus header, selanjutnya preamble disingkat), yang mendahului transmisi setiap frame, sering dianggap diabaikan. Dalam komunikasi nirkabel, pembukaannya biasanya panjang dan overhead-nya tidak dapat diabaikan; evaluasi akurat dari durasi transmisi setiap badan pesawat juga harus memperhitungkan pembukaan. Contohnya adalah lapisan fisik standar IEEE 802.11b (DSSS PHY), yang memungkinkan dua jenis pembukaan: panjang dan pendek. Keduanya harus dikodekan menggunakan modulasi terendah. Pembukaan panjang menghasilkan durasi 192 mikrodetik, dengan 96 mikrodetik untuk pembukaan pendek. Bagaimanapun, dampak pada metrik seperti throughput tidak dapat diabaikan. Terutama ketika paket-paket pendek dipertimbangkan, overhead yang disebabkan oleh pembukaan dapat berada dalam urutan yang sama dengan data yang ditransmisikan.

Di sisi lain, jika kita mempertimbangkan standar IEEE 802.11g/n yang mengadopsi OFDMA, overhead berkurang secara signifikan (hingga 20 mikrodetik) dan dapat dianggap dapat diabaikan dalam beberapa kasus di mana tingkat akurasi yang tinggi tidak diperlukan. • Model Perbanyakan. Model propagasi radio mencirikan hilangnya jalur yang dialami oleh gelombang radio. Dengan kata lain, ini mengevaluasi level sinyal yang ditransmisikan pada penerima. Dalam literatur, banyak sekali model yang telah dikembangkan, dari model sederhana yang hanya merupakan fungsi frekuensi dan jarak hingga model yang lebih kompleks yang mengambil faktor lain seperti rintangan dan memperhitungkan efek interferensi. Karena path loss adalah faktor yang mendominasi dalam pemodelan saluran, kami mengeksplorasi aspek ini secara lebih rinci.

6.3.1.1 Interferensi dan Perhitungan SINR.

Interferensi adalah aspek penting lainnya, khususnya ketika jaringan multihop dipertimbangkan. Interferensi menyebabkan komunikasi yang tidak diinginkan di antara dua atau lebih pasang node karena sinyal nirkabel saling mengganggu. Model yang diadopsi untuk mengevaluasi interferensi dari komunikasi simultan lainnya dalam jaringan merupakan faktor penting lainnya dan dibahas secara luas

di Bagian 6.3.1.2. • Model Penerimaan. Setelah mengevaluasi kekuatan sinyal dan tingkat interferensi pada penerima, langkah terakhir adalah memodelkan apakah sebuah frame telah didekodekan dengan benar atau tidak. Seperti disebutkan sebelumnya, praktik umum adalah menganggap bingkai sebagai entitas atom. Model penerimaan berbasis SINR dan BER berbasis adalah dua model yang biasanya diadopsi oleh simulator. Dengan model berbasis SINR , rasio signal-to-interference-noise minimum yang dialami dari frame yang ditransmisikan dibandingkan dengan ambang: Jika SINR berada di atas ambang, seluruh frame diterima dengan benar. Kalau tidak, itu ditandai sebagai rusak. Ambang diukur secara eksperimental menggunakan perangkat keras nyata, dan ambang berbeda diadopsi untuk setiap kode modulasi. Sebaliknya, dengan model berbasis BER , bit error rate yang sesuai diturunkan secara analitik dari SINR dan akhirnya frame-error rate (FER) dihitung dengan meningkatkan BER ke seluruh panjang frame. Terutama ketika ukuran paket yang berbeda dipertimbangkan dalam skenario yang sama, model berbasis BER lebih akurat karena model berbasis SINR mengabaikan panjang frame, menetapkan FER yang sama terlepas dari durasi frame. Rincian lebih lanjut tentang model penerimaan dan bagaimana penerapannya dalam simulator dapat ditemukan di referensi 59.

Penelitian terbaru juga telah mengidentifikasi isu-isu berikut yang memerlukan definisi model baru:

• Rasa Pembawa. Pemodelan pengertian pembawa dan masalah terkait sering diabaikan. Dalam perangkat nyata, mengubah keadaan radio dan merasakan saluran menimbulkan penundaan variabel yang terutama bergantung pada energi sinyal yang dirasakan dan pada desain perangkat keras. Dalam simulasi, yang terakhir tidak termasuk dalam model atau dianggap sebagai penundaan konstan. Dalam referensi 60 penulis menunjukkan bahwa mengabaikan aspek-aspek ini secara signifikan mempengaruhi hasil. Dalam testbed, keterlambatan variabel dalam penginderaan saluran menurunkan kinerja CSMA/CA, meningkatkan jumlah tabrakan terutama dalam skenario dengan jumlah node yang tinggi. Model yang menggunakan penundaan konstan mungkin gagal menangkap degradasi ini secara memadai, terutama sehubungan dengan throughput jaringan, yang bisa 75% lebih rendah jika terjadi beban jaringan yang tinggi.

• Model Kebisingan Lingkungan. Mensimulasikan noise berbasis perangkat keras sebagai tambahan white Gaussian noise adalah cara de facto untuk mensimulasikan saluran nirkabel. Sebaliknya, kebisingan lingkungan biasanya tidak diperhitungkan dalam model karena dinamika temporal yang kompleks. Untuk meningkatkan akurasi, model baru mensimulasikan kebisingan lingkungan dalam pengiriman paket nirkabel baru-baru ini disajikan. Secara khusus, pendekatan baru yang berasal dari pengukuran nyata diusulkan untuk meningkatkan akurasi simulasi sehubungan dengan menciptakan kembali perilaku jaringan nyata [61].

• Interferensi Co-channel Berdekatan. Interferensi yang disebabkan oleh saluran yang berdekatan (ACI) sering tidak dipertimbangkan dalam model fisik bahkan jika diakui bahwa skema channelisasi yang buruk (misalnya, dalam IEEE 802.11b/g) menghasilkan interferensi co-channel yang berat [62]. Penggunaan saluran nonoverlapping ortogonal yang seharusnya bebas ACI sering diadopsi untuk mengatasi masalah ini. Namun, referensi 63 menunjukkan bahwa interferensi saluran bersama masih ada dalam skema penyaluran yang lebih efisien seperti IEEE 802.11a dan dapat disebabkan oleh saluran yang tidak berdekatan. Untuk mempertimbangkan fenomena ini dalam simulasi, model untuk menghitung pengaruh ACI dalam SINR telah ditetapkan [63,64].

• Tangkap Efek. Berlawanan dengan perilaku model simulasi, dalam testbed nyata dua frame yang ditransmisikan secara bersamaan tidak harus hilang. Bergantung pada kekuatan sinyal dan waktu bingkai, seseorang dapat selamat dari tabrakan. Fenomena ini disebut efek tangkapan dan bergantung pada bagaimana vendor chip yang berbeda mengimplementasikan penerimaan bingkai dan algoritme penangkapan. Dalam literatur, efek penangkapan telah dipelajari secara ekstensif melalui percobaan

testbed [65-67]. Hasilnya telah digunakan untuk menyebarkan model simulasi baru atau memodifikasi yang sudah ada untuk mempertimbangkannya [54,65,68].

• Model Antena. Simulator yang umum digunakan tidak mempertimbangkan arah antena dalam model propagasinya. Di sisi lain, di dunia nyata, antena omnidireksional sering kali menghindari antena terarah untuk meningkatkan kualitas sambungan dan mengurangi interferensi secara keseluruhan. Hampir semua model yang diadopsi secara umum tidak mempertimbangkan direktivitas sinyal. Asumsi penyederhanaan ini tidak realistis dan dapat menyebabkan hasil yang jauh dari kenyataan [69]. Untuk mengatasi masalah ini, dalam referensi 70 penulis mengusulkan metodologi baru untuk memodelkan antena directional dalam simulator untuk menghasilkan simulasi yang lebih konsisten dengan kenyataan. Sepengetahuan kami, studi validasi model

antena yang membandingkan hasil simulasi dengan pengukuran testbed belum pernah dilakukan.

• Emulasi Lapisan Fisik. Seperti disebutkan sebelumnya, granularity simulasi yang biasanya dipertimbangkan dalam model simulasi adalah frame; semua detail tentang

pemrosesan sinyal tingkat rendah dihilangkan. Model yang dihasilkan memperdagangkan akurasi simulasi untuk persyaratan sumber daya komputasi yang lebih rendah. Tingkat abstraksi ini cocok untuk sebagian besar skenario simulasi, tetapi beberapa kasus tertentu memerlukan tingkat akurasi simulasi yang tinggi di mana tingkat abstraksi yang diadopsi dalam model yang umum digunakan tidak dapat diterima. Untuk alasan ini, beberapa upaya baru-baru ini telah dilakukan untuk mengembangkan model fisik dengan tingkat perincian yang lebih baik. Tujuannya adalah untuk menentukan arsitektur baru untuk emulasi lapisan fisik di mana bit atau bahkan sinyal adalah entitas terkecil. Dalam referensi 71 penulis mengusulkan emulator lapisan fisik untuk jaringan IEEE 802.11 berbasis OFDM menggunakan perpustakaan pemrosesan sinyal untuk meniru perambatan sinyal melalui media nirkabel.

6.3.1.1 Model Propagasi Radio.

Model propagasi dimaksudkan untuk mensimulasikan propagasi sinyal radio melalui sarana nirkabel. Output dari model adalah sekumpulan karakteristik sinyal pada sisi penerima setelah terdistorsi selama transmisi. Dalam simulasi MANET, model propagasi radio yang diadopsi dianggap sebagai faktor terpenting dalam keakuratan model fisik secara keseluruhan. Karena cara sinyal merambat melalui udara dipengaruhi oleh sejumlah besar faktor, model komprehensif sulit untuk ditentukan dan tidak ada model tunggal yang mampu memprediksi path loss secara konsisten dengan baik [72]. Topologi dan mobilitas node memiliki banyak pengaruh terhadap distorsi sinyal. Gelombang radio mengalami difraksi, refraksi, dan hamburan yang disebabkan oleh elemen lingkungan.

Beberapa model propagasi statistik telah didefinisikan dalam literatur; masing-masing memiliki tingkat kompleksitas dan akurasi yang meningkat. Terlepas dari keakuratannya, setiap model propagasi sangat cocok untuk memodelkan skenario tertentu: lingkungan dalam ruangan daripada lingkungan luar, seluler daripada node tetap.

Model paling sederhana yang dapat didefinisikan hanya memperhitungkan faktor utama: kehilangan daya sinyal di sepanjang jalur, singkatnya kehilangan jalur . Model ini disebut Free Space Propagation dan mengasumsikan kondisi propagasi radio yang ideal dengan garis

pandang. Menurut model ini, kekuatan sinyal yang diterima sebanding dengan Ptr dimana d adalah jarak pengirim-penerima dan Ptr adalah daya transmisi. d2 ini

model, bagaimanapun, mengabaikan efek interferensi multipath yang disebabkan oleh lingkungan terestrial. Gelombang biasanya mengenai objek dan rintangan dan akhirnya bertemu di penerima setelah melewati jalur yang berbeda. Model yang sedikit lebih detail adalah model Two-Ray Ground . Berbeda dengan Ruang Bebas, ini tidak hanya memperhitungkan sinyal jalur langsung tetapi juga sinyal pantulan tanah, memberikan prediksi yang lebih akurat untuk jarak jauh. Daya terima yang dihasilkan sama dengan Ruang Kosong kecuali untuk kasus ketika jarak lebih besar dari titik persilangan di mana daya penerima dimodelkan secara proporsional dengan Ptr didÿm,anharÿusadÿa>la2h. eksponen kehilangan jalur yang

Baik model Free Space maupun Two-Ray Ground mengasumsikan propagasi ideal pada area melingkar—yakni, garis pandang sempurna dan tanpa hambatan. Dalam lingkungan nyata, daya yang diterima juga dipengaruhi oleh halangan seperti bukit atau bangunan besar yang menghasilkan area jangkauan yang tidak teratur. Model propagasi Shadowing memiliki dua komponen: satu untuk path loss yang mirip dengan model Free Space dan komponen acak lainnya untuk membuat variabel jangkauan komunikasi. Model ini memiliki dua parameter yang dapat digunakan untuk mewakili skenario yang berbeda, seperti lingkungan luar ruangan versus dalam ruangan atau daerah perkotaan versus pedesaan: ÿ adalah eksponen kerugian jalur, sama dengan model Two Ray Ground , dan ÿ adalah standar deviasi dari variabel acak (sering log-normal), yang digunakan untuk memodelkan perubahan amplitudo yang disebabkan oleh bayangan.

Untuk mempertimbangkan mobilitas simpul, model yang lebih kompleks telah ditentukan.

Pemudaran skala kecil disertakan untuk memodelkan fluktuasi cepat fase dan amplitudo sinyal yang disebabkan oleh berbagai kondisi jalur dari pemancar. Beberapa model fading telah didefinisikan, tetapi dua yang paling umum digunakan adalah distribusi Rayleigh dan Ricean . Model Rayleigh sangat cocok untuk memodelkan skenario dengan mobilitas tinggi di lingkungan yang tidak memiliki garis pandang, seperti perkotaan area di mana bangunan dan objek di antara pemancar dan penerima melemahkan sinyal dan menghasilkan banyak bentuk gelombang. Model Ricean , sebagai gantinya, mempertimbangkan fakta bahwa sinyal dapat tiba di penerima melalui beberapa jalur tetapi setidaknya satu kontribusi jauh lebih kuat daripada yang lain, mungkin karena adanya garis pandang. Model propagasi yang lebih kompleks dan akurat ditentukan. Untuk deskripsi yang lebih rinci tentang model propagasi radio stokastik, pembaca dapat merujuk ke buku teks komunikasi nirkabel (misalnya, referensi 73).

Tentu saja, setiap model menghasilkan trade off; semakin tinggi efisiensi komputasi, semakin rendah akurasinya. Model Free Space yang banyak digunakan secara komputasi efisien tetapi mengabaikan beberapa komponen propagasi sinyal nirkabel.

Di sisi lain, model yang lebih kompleks menghasilkan waktu eksekusi yang tidak dapat diterima ketika jaringan berskala besar disimulasikan. Beberapa pendekatan telah diusulkan untuk mengurangi waktu simulasi. Misalnya, Eksekusi Paralel [74] dan Partisi Jaringan dapat secara efektif mengurangi waktu simulasi, tetapi tidak selalu dapat diterapkan. Ketika tidak ada opsi untuk mengurangi waktu simulasi, penggunaan model propagasi sederhana adalah satu-satunya solusi.

Bahkan jika tidak ada model yang memiliki detail yang cukup untuk benar-benar cocok dengan hasil pengujian, setiap model memperkenalkan tingkat perkiraan yang harus diestimasi terlebih dahulu. Oleh karena itu, cara terbaik untuk melanjutkan adalah memverifikasi bahwa model propagasi yang diadopsi menghasilkan hasil yang mendekati percobaan nyata. Setelah memilih model propagasi dan pengaturannya, hasilnya harus selalu divalidasi melalui perbandingan dengan pengukuran yang

diperoleh melalui testbed nyata. Dalam referensi 56 evaluasi kinerja algoritma perutean ad-hoc dilakukan terlebih dahulu melalui simulasi dan kemudian menggunakan testbed sebenarnya. Perbandingan hasil menunjukkan bahwa semua model propagasi mengarah ke jaringan yang terhubung lebih padat daripada yang dialami penyebaran nyata.

Yang pertama menghasilkan rasio pengiriman yang lebih tinggi untuk intensitas lalu lintas tertentu karena ada lebih sedikit lompatan antar node. Perbedaan ini dapat dijelaskan dengan mempertimbangkan bahwa model mengasumsikan kehilangan jalur segala arah yang sebagian besar bergantung pada jarak. Di sisi lain, jika tujuan utamanya adalah untuk mendapatkan kesimpulan kualitatif dari simulasi, model stokastik sederhana dapat memberikan hasil yang dapat diterima, tetapi sangat penting untuk memilih model yang mewakili skenario dengan benar.

Akhirnya, penulis menunjukkan bagaimana hasilnya peka terhadap parameter model, sehingga menggarisbawahi pentingnya penyetelan yang benar. Tan dkk. memperoleh hasil yang serupa, menyimpulkan bahwa simulasi dapat cocok dengan eksperimen di lingkungan sederhana seperti di luar ruangan dengan transmisi line-of-sight [75].

Dalam referensi 76 penulis memvalidasi hasil simulasi jaringan multihop dalam ruangan

menggunakan testbed yang ditempatkan di koridor untuk mewakili lingkungan kantor yang khas. Hasil menunjukkan bahwa model stokastik yang diadopsi dapat secara kasar cocok dengan hasil pengujian ketika skenario aliran tunggal dipertimbangkan tetapi ketika aliran bersamaan disimulasikan, hasil dan pengukuran dapat berbeda secara signifikan. Koridor dan lingkungan dalam ruangan pada umumnya lebih kompleks daripada skenario luar ruangan. Model propagasi

tidak dapat dengan benar merepresentasikan tingginya tingkat interferensi yang disebabkan oleh transmisi bersamaan dari node tersembunyi.

Referensi 58 menyajikan validasi model Free Space, Two-Ray Ground, dan Shadowing ,

dengan mempertimbangkan lingkungan dalam dan luar ruangan. Ketidaktepatan dari Model Free Space dan Two-Ray Ground ditandai ketika jaringan padat dalam skenario dalam ruangan dipertimbangkan. Sebaliknya, ketidakakuratan terbukti dapat diterima di lingkungan luar ruangan di mana kompleksitas dinamika propagasi menurun. Sejauh menyangkut model Shadowing , hasil validasi menunjukkan bahwa hasil di dalam dan di luar ruangan mendekati pengukuran testbed, yang menegaskan bahwa model ini memiliki pertukaran yang baik antara kompleksitas dan akurasi. Oleh karena itu, penulis kembali menggarisbawahi pentingnya penyetelan parameter model yang benar melalui tahap validasi.

Studi validasi lain pada skenario yang lebih spesifik dapat ditemukan di referensi 57 dan 58.

6.3.1.2 Model Interferensi

Ketika sinyal radio dipancarkan ke luar angkasa, versi terdistorsinya di penerima ditumpangkan dengan sinyal yang ditransmisikan lainnya. Berhasil mendekode transmisi adalah peristiwa acak yang tidak hanya bergantung pada kekuatan sinyal pada penerima tetapi juga pada kekuatan interferensi. Untuk alasan ini, beberapa model interferensi telah didefinisikan dalam literatur dengan tingkat kompleksitas dan kelengkapan yang berbeda. Meskipun demikian, bahkan jika beberapa pekerjaan memvalidasi model path loss telah disajikan, hanya sedikit yang mengevaluasi validitas model interferensi. Kurangnya validasi ini telah memungkinkan penggunaan berkelanjutan dari model interferensi yang terlalu sederhana yang diimplementasikan dalam simulator jaringan, yang secara serius

membahayakan hasil temuan penelitian yang dievaluasi hanya dengan menggunakan simulator.

Pada awal implementasi simulator jaringan, dua model interferensi biner didefinisikan,

model Protocol dan Interference Range . Area interferensi tetap ditentukan dan transmisi dianggap tidak berhasil jika transmisi bersamaan lainnya terjadi di dalam area terlepas dari

kekuatannya. Ketidakakuratan model sederhana ini menyebabkan definisi model estimasi interferensi yang saat ini digunakan untuk mengevaluasi daya interferensi. Untuk setiap paket yang ditransmisikan, interferensi keseluruhan diperkirakan yang diadopsi untuk mengevaluasi SINR (dan kemudian BER, jika diperlukan). SINR atau BER kemudian digunakan dalam model penerimaan untuk memutuskan apakah suatu paket diterima dengan benar atau tidak. Menurut tingkat akurasi, model berikut didefinisikan:

• Model Interferensi Kumulatif Penuh. Tingkat gangguan diperoleh dengan menjumlahkan daya yang diterima di tujuan dari transmisi sinyal yang sedang berlangsung. Model ini, juga dikenal sebagai model Interferensi Fisik [77], dianggap paling akurat dalam memprediksi tabrakan.

• Model Interferensi Kumulatif Terbatas. Dalam model ini kompleksitas dikurangi dengan hanya mempertimbangkan kontribusi komunikasi yang terjadi dalam radius tertentu dari penerima.

• Model Interferensi Terkuat. Alih-alih mengevaluasi interferensi kumulatif, kekuatan komunikasi terkuat yang sedang berlangsung dianggap sebagai nilai interferensi.

Model interferensi kumulatif Terbatas dan model interferensi Terkuat biasanya diadopsi dalam simulator; mengevaluasi interferensi kumulatif penuh itu rumit dan dalam jaringan besar tidak selalu dapat dilakukan. Model interferensi kumulatif Terbatas dianggap memiliki tradeoff terbaik

karena hanya memperhitungkan sumber gangguan utama. Mengabaikan komunikasi yang terjadi di luar rentang tertentu menyebabkan sinyal yang mengganggu di bawah ambang batas tertentu diabaikan. Tingkat perkiraan yang diperkenalkan umumnya dianggap dapat diterima tetapi dalam praktiknya tidak selalu benar. Referensi 78 menunjukkan bahwa perkiraan ini menimbulkan sejumlah besar kesalahan ketika jaringan besar dipertimbangkan. Throughput yang diperoleh dengan model interferensi kumulatif terbatas dapat berbeda sekitar 210% dibandingkan dengan hasil yang diperoleh dengan model interferensi kumulatif penuh . Sebagai konsekuensinya, beberapa upaya dalam mengoptimalkan algoritma untuk menghitung keseluruhan interferensi telah diusulkan agar layak menggunakan model kumulatif Penuh dalam jaringan besar [79].

Dalam referensi 55 penulis menunjukkan bahwa penggunaan model interferensi yang berbeda secara signifikan mempengaruhi hasil simulasi. Secara khusus, mereka menggarisbawahi pentingnya mengadopsi model interferensi kumulatif untuk mendapatkan hasil yang akurat. Model Rentang Interferensi dapat menghasilkan hasil yang menyesatkan karena kontribusi komunikasi jarak jauh tidak selalu dapat diabaikan. Penulis menyarankan bahwa jika model aditif tidak dapat diadopsi karena kerumitannya, hasil yang diperoleh harus divalidasi sebelum dipertimbangkan.

Sejauh pengetahuan kami, tidak ada studi validasi yang menggunakan pengukuran

testbed untuk mengevaluasi kesenjangan antara model interferensi dan pengamatan dunia nyata.

6.3.2 Pemodelan Mobilitas

Karena keterbatasan medan, biaya penerapan, dan cakupan terbatas area penelitian yang ditargetkan, sebagian besar testbed dunia nyata seperti yang dibahas dalam referensi 20 dan 25 memiliki batasan variasi skenario mobilitas yang dapat direalisasikan.

Dengan kasus DOME [20], misalnya, komponen kemampuan mobilitas yang signifikan dicapai oleh sistem transportasi bus, yang biasanya dibatasi oleh rute yang ditentukan oleh otoritas transit. Masalah ini kurang lazim di testbed dalam ruangan seperti, misalnya, yang dibahas dalam referensi 22 dan 29, terutama jika testbed terletak di ruang khusus. Namun, seperti di testbed dalam ruangan, menyiapkan banyak koleksi skenario seluler memberikan beban yang signifikan dalam hal waktu, biaya, dan tenaga yang dibutuhkan. Jadi, daripada mengembangkan sistem berumur panjang, peneliti biasanya menggunakan eksperimen jangka pendek menggunakan perangkat rak komersial untuk mengevaluasi proposal mereka [15-18].

Untuk alasan ini, serangkaian model mobilitas yang komprehensif untuk simulator telah dikembangkan untuk memungkinkan pembuatan prototipe dan evaluasi ide penelitian secara cepat. Ada dua jenis model dalam simulasi jaringan seluler nirkabel: jejak mobilitas dan model sintetik. Jejak adalah pola mobilitas yang telah ditentukan sebelumnya yang diperoleh dari penggunaan dan eksperimen di dunia nyata. Mereka memberikan informasi yang realistis tentang pola mobilitas, terutama jika dikumpulkan dari pengguna sebenarnya dalam pengaturan terbatas seperti jalan dan jalan raya [80-82]. Namun, rekreasi yang tepat dari skenario mobilitas memerlukan pencatatan data jejak yang halus, yang berarti bahwa banyak informasi perlu dikumpulkan. Beberapa poin data dapat disimpulkan melalui

interpolasi atau perhitungan mati, tetapi ini dapat menyebabkan kasus di mana host seluler (MH) tampaknya berjalan melalui rintangan yang kokoh. Juga, meskipun jejak MANET sekarang lebih mudah ditemukan dari upaya seperti CRAWDAD [83], rangkaian jejak yang tersedia untuk umum tidak cukup beragam untuk memenuhi kebutuhan eksperimen tertentu.

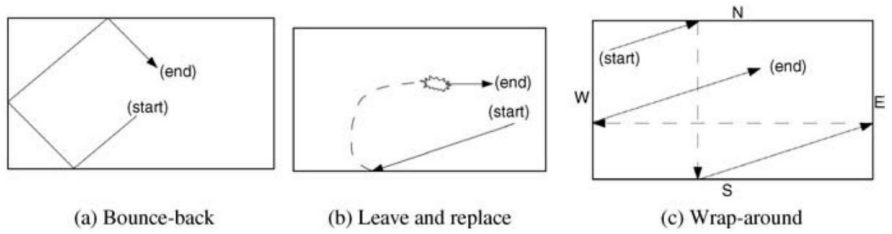
Model sintetik adalah model matematis yang didefinisikan untuk mewakili mobilitas pengguna dengan cara yang realistis. Selain mengatasi beberapa keterbatasan di atas, mereka memungkinkan untuk analisis sensitivitas, misalnya dengan memvariasikan distribusi kecepatan atau kepadatan node. Selain itu, dasar matematika mereka memungkinkan peneliti untuk menganalisis secara formal dampaknya terhadap desain dan perilaku sistem. Dengan demikian, banyak model mobilitas yang menghasilkan jejak sintetik telah dikembangkan [81]. Model sintetik dapat diklasifikasikan menjadi model entitas dan grup. MH dalam model entitas bertindak secara independen dari node lain dalam skenario simulasi, sedangkan pergerakan MH dalam skenario grup bergantung pada MH lain dalam grup atau pada faktor yang sama dengannya. Contoh model berbasis entitas termasuk, namun tidak terbatas pada, model Random Waypoint yang populer [84], Model Mobilitas Acak [80], model Jalan Acak [85,86], dan model Arah Acak [87]. Model Grup Referensi [88], model Grup Kecepatan Referensi [89], model Grup Terstruktur [90], dan Jalan Acak Heterogen [91] adalah beberapa model berbasis grup yang ditemukan dalam literatur.

Taksonomi kedua berpusat pada tingkat keacakan dalam pergerakan simpul. Kategori tersebut adalah: (1) model yang menggunakan proses pseudorandom statistik untuk memilih kecepatan dan arah (misalnya, model Random Direction, Random Waypoint, dan Random Direction); (2) model yang membatasi pergerakan pengguna dengan memfaktorkan jalan kota, tembok, dan jalan raya misalnya, tetapi masih memungkinkan pemilihan arah dan kecepatan pseudorandom di persimpangan (misalnya, Pemilihan Kota [81] dan model Manhattan [81]); dan (3) model sintetik berdasarkan jejak nyata. Model berbasis jejak memperoleh sifat statistik utama mengenai mobilitas manusia seperti

waktu interkoneksi dan durasi koneksi dari jaringan nyata dan mencoba menggeneralisasikannya [92-97].

Namun pengelompokan lain didasarkan pada kebijakan batas yang diadopsi. Kebijakan batas dapat berupa bangkit kembali, meninggalkan dan mengganti, atau membungkus. Kebijakan bangkit kembali menunjukkan praktek "mencerminkan" MH setelah menyentuh simulasi batas [80,81,98]. Dalam kebijakan cuti dan ganti, MH yang bergerak di luar batas wilayah digantikan oleh MH baru yang ditempatkan secara acak di dalam wilayah tersebut [80,81,98]. Perilaku lilitan atau torus membuat MH masuk kembali ke area batas setelah efek lilitan. Misalnya, node yang meninggalkan area di utara, timur, selatan, atau barat akan masuk kembali dengan kecepatan dan arah yang sama dari batas selatan, barat, utara, dan timur, masing-masing [80,81,98].

Gambar 6.4 mengilustrasikan masing-masing kebijakan batas ini. Perlakuan mendalam dari ketiga taksonomi ini berada di luar cakupan bab ini, tetapi dapat ditemukan di referensi 81 dan 98-100. Meskipun popularitas mereka di antara para peneliti, model sintetik dipertanyakan sehubungan dengan realisme mereka. Pertama, perilaku pseudorandom mereka tidak mencerminkan pengamatan dunia nyata. Misalnya, dalam referensi 95, terlihat bahwa dibandingkan dengan jejak nyata yang tersedia [83], properti model sintetik seperti waktu interkoneksi (waktu antara koneksi berikutnya) dan durasi koneksi berbeda dari apa yang diamati di dunia nyata. Selain itu, Gonzalez et al. [101] temukan itu



Gambar 6.4 Kebijakan batas.

bukannya acak, lintasan manusia memiliki tingkat keteraturan temporal dan spasial yang tinggi; pengguna biasanya berpindah di antara beberapa lokasi yang sering dikunjungi. Penting untuk dicatat bahwa salah satu model mobilitas yang paling populer, Random Waypoint, menunjukkan pengelompokan node di sekitar pusat area simulasi [87], dan kurangnya distribusi kondisi- mapan dari kecepatan node rata-rata berarti bahwa kecepatan node rata-rata turun. dari waktu ke waktu [102]. Dengan model mobilitas kelompok, meskipun ada korelasi dalam pergerakan antara anggota kelompok, sifat korelasinya mungkin tidak mencerminkan hubungan dunia nyata antara anggota kelompok [81].

Kebijakan batas model juga dapat memengaruhi hasil eksperimen.

Misalnya, dalam referensi 57, penulis mengevaluasi model dengan kebijakan batas yang berbeda, sehubungan dengan kinerja protokol perutean AODV. Jika dua node berada pada batas berlawanan dari model Boundless Simulation Area (BSA) (yang memiliki perilaku wrap- around atau torus yang dijelaskan di atas), mereka mungkin masih dapat berkomunikasi, berbeda dengan model Random Direction, Walk, dan Waypoint. , yang menggunakan kebijakan bangkit kembali. Ini menyiratkan bahwa node dalam model BSA memiliki garis pandang yang lebih besar ke node lain. Akibatnya, model BSA dapat menyebabkan topologi yang tidak

realistis dan analisis kinerja protokol routing yang salah karena node yang tidak dapat berkomunikasi dalam skenario dunia nyata diizinkan untuk melakukannya.

Masalah lain yang terkait erat dengan model propagasi adalah pemodelan hambatan.

Sebagian besar model mobilitas tidak memasukkan rintangan dan pengaruh artefak semacam itu pada pergerakan, perambatan sinyal, dan topologi, dan ini masih menjadi masalah penelitian terbuka. Akibatnya, sulit untuk menggunakannya untuk menilai kinerja protokol dan sistem di lingkungan dalam ruangan, di mana dinding dan perlengkapan lainnya memiliki efek mendalam pada perambatan sinyal. Beberapa pekerjaan yang menjanjikan dilakukan dalam hal ini oleh Jardosh et al. [103], di mana mereka memodelkan rintangan menggunakan grafik Voronoi

[104]. Hambatan dapat membatasi gerakan dan perambatan sinyal medan simulasi yang dihasilkan. Pendekatan mereka cukup umum untuk diterapkan pada model mobilitas lainnya.

Untuk mengatasi beberapa masalah yang disoroti di atas, dua jenis model mobilitas baru- baru ini telah diselidiki. Yang pertama bertujuan untuk memanfaatkan teori jaringan sosial dan pengamatan dalam desain model mobilitas [105]. Host dikelompokkan bersama berdasarkan hubungan sosial antar individu. Setelah pengelompokan selesai, informasi ditransfer ke area geografis yang disimulasikan. Durasi koneksi dan waktu interkoneksi dipengaruhi oleh kekuatan social hubungan antar node. Jenis lainnya kurang berfokus pada mobilitas dan lebih pada konektivitas antar node. Daripada hanya mendefinisikan pola mobilitas, mereka bertujuan untuk menggunakan karakteristik pola mobilitas seperti waktu interkoneksi dan durasi koneksi untuk mencapai informasi topologi yang lebih akurat dari waktu ke waktu. Perbedaan penting dari model mobilitas oversintetik ini adalah konektivitas, dan karenanya topologi yang bervariasi waktu, menentukan distribusi geografis node, sedangkan kebalikannya berlaku untuk model sintetik. Studi yang mengadopsi pendekatan ini dapat ditemukan dalam referensi 106 dan 107. Model konektivitas dapat melengkapi model mobilitas dan, seperti model berbasis jaringan sosial, akan menjadi penting dalam evaluasi protokol oportunistik dan aplikasi kolaboratif yang kinerjanya bergantung pada sifat interaksi antar node.

Secara keseluruhan, koleksi model mobilitas yang luas dalam simulasi dan kemudahan penggunaan serta konfigurasinya yang relatif telah menjadikannya favorit yang kuat dibandingkan model yang tersedia di testbed. Namun, seperti yang ditunjukkan di atas, keakuratan dan realismenya, serta penerapannya pada beberapa skenario, telah menerima kritik dari berbagai pihak. Oleh karena itu, penting untuk memahami batasan model mobilitas tertentu dan kesesuaiannya untuk skenario yang diuji.

6.3.3 Pertimbangan Lapisan MAC

Pada bagian ini kami akan memberikan ikhtisar dari semua faktor yang mempengaruhi keandalan simulasi dan eksperimen testbed yang terkait dengan lapisan MAC. Menurut definisi, lapisan MAC menyediakan mekanisme pengalamatan dan kontrol akses saluran yang memungkinkan terminal rendah dari vendor yang berbeda untuk berkomunikasi pada media nirkabel bersama, sehingga menjamin interoperabilitas. Semua tindakan, pesan dan protokol didefinisikan ke dalam standar (misalnya, IEEE 802.11 [108]) yang seharusnya diterapkan secara ketat pada driver kartu nirkabel. Sebelum memasuki pasar, kartu nirkabel diuji agar

sesuai dengan standar, dan sertifikasi dirilis ke perangkat yang perilakunya memenuhi spesifikasi.

Dalam simulator, penerapan lapisan MAC penuh biasanya lebih disukai daripada menentukan model untuk mengabstraksikan karakteristiknya. Meskipun penerapannya tidak disertifikasi seperti pada perangkat sebenarnya, perilaku tersebut dianggap memenuhi standar. Dalam proyek open source khususnya, kehadiran komunitas pengguna dan pengembang yang besar memperkuat kepercayaan pada asumsi ini yang sering kali dibuat tanpa verifikasi.

Beberapa pekerjaan pada penilaian eksperimental kartu nirkabel dari pabrikan yang berbeda dapat ditemukan di referensi 109 dan 110. Makalah ini menampilkan beberapa masalah kinerja yang berasal dari perilaku buruk kartu: Dalam skenario terkontrol yang bebas dari interaksi tak terduga dengan lingkungan, kartu bersertifikasi diproduksi oleh berbagai industri berbeda dalam hasil kinerja [111]. Penyebab perbedaan ini ditemukan dalam penerapan lapisan MAC tertentu dari vendor: Beberapa modifikasi diterapkan, dan akibatnya perilaku kartu tidak sepenuhnya sesuai dengan standar. Praktek ini biasanya diadopsi oleh vendor dengan tujuan berusaha mendapatkan kinerja yang lebih baik dibandingkan dengan produk lain. Peningkatan performa yang dijamin oleh modifikasi standar mengorbankan interoperabilitas.

Ketika skenario dengan kartu heterogen dipertimbangkan, masalah interoperabilitas dapat terjadi menyebabkan, misalnya, kehilangan paket yang tinggi antara kartu dari merek yang berbeda seperti yang ditunjukkan pada referensi 112.

Keuntungan untuk simulator adalah tidak ada insentif untuk melakukan modifikasi pada lapisan MAC untuk meningkatkan kinerjanya. Namun, studi validasi seperti yang dibahas dalam referensi 113 dan 114 menunjukkan bahwa beberapa perbedaan juga ada pada simulator. Mereka mengaitkan perbedaan dengan asumsi penyederhanaan yang diperkenalkan untuk mengurangi kompleksitas MAC—yang tidak selalu disarankan, terutama dalam skenario yang padat.

Berdasarkan literatur yang ada tentang validasi baik pada simulator maupun driver, modifikasi yang diterapkan pada definisi standar dapat dikategorikan sebagai berikut:

• Keistimewaan Pabrikan untuk Peningkatan Performa. Di tempat pengujian, vendor menerapkan beberapa modifikasi pada standar untuk mendapatkan peningkatan kinerja secara keseluruhan dibandingkan dengan perangkat lain. Bahkan jika interoperabilitas di antara perangkat heterogen berkurang, pabrikan mengadopsi solusi nonstandar untuk mendapatkan keuntungan dari pesaing—misalnya, memodifikasi prosedur mundur untuk meningkatkan kemungkinan keberhasilan. Karena kartu nirkabel dan drivernya sering disediakan sebagai kotak hitam, keistimewaan pabrikan ini sulit untuk dimodelkan dalam simulator.

• Penyederhanaan. Dalam simulator, penyederhanaan biasanya diperkenalkan. Tujuannya adalah untuk mengurangi kompleksitas, mengabaikan semua aspek yang tampaknya tidak relevan. Contoh umum adalah Address Resolution Protocol. Keterlambatan dan overhead sering dianggap diabaikan dan akibatnya penerapannya diabaikan.

Asumsi yang diperkenalkan sering dibuat tanpa memverifikasi dampak pada akurasi.

• Interpretasi Standar. Beberapa aspek implementasi dibiarkan tidak ditentukan oleh standar. Dalam kasus ini, kebebasan diberikan kepada produsen. Baik di simulator maupun perangkat nyata, area abu-abu ini memiliki lebih dari satu kemungkinan interpretasi.

Contohnya adalah mekanisme pemilihan laju transmisi yang tidak ditentukan oleh spesifikasi IEEE 802.11. • Bug dan Kesalahan. Ketidakakuratan dalam implementasi simulator dan

penggunaan driver yang sedang dikembangkan di perangkat nyata dapat menyebabkan perilaku buruk yang memengaruhi kinerja sistem. Misalnya, standar menyatakan bahwa data kontrol harus dikirim menggunakan laju transmisi paling lambat, tetapi dapat terjadi bahwa bug menyebabkan laju normal digunakan untuk transmisi pesan ACK [113]. Dalam referensi 114, ditunjukkan bagaimana bug dalam implementasi driver dapat membatasi kecepatan paket maksimum yang dapat dicapai.

Perbedaan lapisan MAC secara signifikan dapat mempengaruhi kinerja lapisan atas [115]. Untuk alasan ini, keakraban dengan implementasi lapisan MAC dalam simulator driver sangat penting untuk menilai akurasi simulasi dan percobaan.

Dalam referensi 114 penulis menunjukkan bagaimana membandingkan hasil simulasi dengan pengukuran testbed dapat membantu tidak hanya memvalidasi hasil simulator tetapi juga menemukan masalah pada driver testbed. Mereka memvalidasi model MAC ns3 [8] melalui testbed di mana efek propagasi saluran diminimalkan dengan menggunakan kabel koaksial untuk menghubungkan antarmuka nirkabel. Hasilnya menunjukkan kecocokan yang baik antara hasil simulasi dan pengukuran testbed, tetapi perbedaan ditampilkan dalam beberapa skenario. Dengan demikian, pendekatan kritis sangat disarankan; setiap perbedaan yang diamati harus ditangani dengan hati- hati, kasus per kasus, untuk memahami penyebab ketidaksesuaian. Aspek penting lain yang juga harus diperhatikan adalah pengaturan parameter lapisan MAC.

Cukup sering, efeknya diremehkan dan nilainya ditetapkan secara tidak tepat. Konfigurasi yang tepat dan akurat selalu diperlukan sebelum mensimulasikan atau menjalankan eksperimen.

Berikut ini kami memberikan ikhtisar penyebab paling sering dari ketidaksesuaian. Karena sebagian besar penerapan sebenarnya dilakukan menggunakan perangkat IEEE 802.11 [108], kami memfokuskan perhatian kami pada masalah yang terkait dengan standar WiFi.

• Prosedur Mundur. Mekanisme akses media nirkabel sangat penting untuk interoperabilitas perangkat karena secara nyata mempengaruhi kinerja. Untuk alasan ini operasi back-off sepenuhnya ditentukan oleh standar.

Namun demikian, beberapa implementasi menunjukkan back-off misbehavior atau bergantung pada parameter yang berbeda dari pedoman standar. Bianchi et al. [110] mempelajari implementasi back-off pada sekelompok perangkat nyata yang tersedia di pasar dan menunjukkan bahwa tidak satupun dari mereka bekerja persis seperti yang diharapkan.

Beberapa fitur diabaikan atau tindakan tidak standar diterapkan untuk mendapatkan keuntungan yang tidak adil atas pesaing. Implementasi back-off juga merupakan masalah dalam simulator.

Meski begitu, perilaku buruk mereka lebih merupakan hasil dari ketidakakuratan daripada upaya untuk mendapatkan keuntungan dari pesaing [113].

• Waktu Protokol. Standar biasanya membutuhkan operasi pengaturan waktu yang ketat. Namun, ditunjukkan dalam referensi 109 bahwa perangkat sebenarnya menunjukkan perilaku yang

berbeda sehubungan dengan beberapa nilai waktu standar. Juga, kesalahan pengaturan waktu di antara berbagai simulator ditunjukkan dalam referensi 113. Sebagai contoh, beberapa simulator menambahkan penundaan acak setelah timer DIFS dan SIFS kedaluwarsa, mungkin untuk mensimulasikan derau di jam perangkat keras.

• Pilihan Tingkat Transmisi. Prosedur pemilihan tingkat transmisi dibiarkan tidak ditentukan dan bergantung pada implementasi. Beberapa algoritme Auto Rate Fallback dapat ditemukan untuk menyesuaikan laju transmisi dengan kondisi saluran.

Meskipun demikian, implementasinya sangat mempengaruhi kinerja jaringan secara keseluruhan seperti yang ditunjukkan pada referensi 116. Dalam banyak kasus, pemilihan algoritma tidak dipertimbangkan baik dalam simulasi maupun percobaan testbed. Hal ini disebabkan oleh fakta bahwa peneliti biasanya memiliki sedikit kendali atas hal ini; simulator dan driver tidak menyediakan opsi algoritme default apa pun.

Demi kenyamanan, Tabel 6.2 merangkum semua masalah kinerja yang dapat membahayakan hasil simulasi dan pengujian. Diakui secara luas bahwa anomali ini dapat diperbaiki hanya melalui perencanaan eksperimen yang cermat dan analisis kritis terhadap hasilnya. Mengkalibrasi peralatan jaringan dan mengonfigurasi simulator secara akurat sangat penting dalam menemukan dan memperbaiki perilaku buruk.

Tabel 6.2 Rangkuman Perilaku Mac Layer

Kategori	Sumber	Konsekuensi
Keistimewaan pabrikan	Ketidakcocokan	Perangkat dari berbeda produsen menjadi tidak kompatibel. Kehilangan paket yang tidak dapat dijelaskan terjadi
	Perbedaan implementasi back-off	Kecepatan paket lebih tinggi dari maksimum yang diizinkan. Ketidakadilan di antara lalu lintas dari kartu yang berbeda
	Distribusi waktu	Distribusi waktu yang tidak terduga. Masalah ketidakadilan dan ketidakstabilan
Penyederhanaanb	Aspek implementasi diabaikan	Hasil simulasi yang tidak realistis. Tarif dan keterlambatan di atas/di bawah perkiraan.
	Batalkan parameter	Hasil yang tidak realistis, terlepas dari keakuratan model
Interpretasi standar	Tingkat transmisi yang berbeda strategi seleksi	Throughput dan loss berbeda tarif
	Keakuratan dan implementasi indera pembawa	Tingkat throughput dan kerugian yang berbeda, terutama dalam skenario multihop
Driver dan ketidakstabilan implementasi	Bug dan error	Throughput dan kerugian yang terdistorsi

Oleh karena itu disarankan untuk (a) mengkarakterisasi perangkat yang diuji untuk menetapkan kinerja dasarnya dan (b) mengidentifikasi dan mendiagnosis sumber perilaku yang tidak diharapkan. Ini termasuk masalah yang terkait dengan kurangnya kepatuhan terhadap standar (misalnya, prosedur

pencatat waktu mundur yang salah), atau masalah perangkat keras atau perangkat lunak seperti memori yang tidak mencukupi dan implementasi driver yang rusak. Selain menandai

perilaku tidak standar sebelum memengaruhi hasil eksperimen, karakterisasi perangkat memberikan informasi berguna untuk membantu konfigurasinya.

Misalnya, Portoles-Comeras et al. menyediakan prosedur untuk mengkarakterisasi perilaku sebuah node dalam hal pengukuran Carrier Sensing (CS) dan kemampuan untuk menangani lalu lintas masuk dan keluar secara bersamaan [117]. Pengukuran CS dapat berbeda karena penyetelan pengukuran energi pada tingkat perangkat keras, sementara penanganan lalu lintas masuk dan keluar secara bersamaan dipengaruhi oleh beragam faktor seperti penanganan interupsi pada node, memori perangkat, atau kinerja driver. Mereka mengadopsi dua parameter independen, ÿ dan ÿ, untuk mengkarakterisasi (a) akurasi CS perangkat dan (b) kapasitasnya masing-masing untuk menangani lalu lintas masuk dan keluar. ÿ memiliki nilai antara 0 dan 1, mewakili akurasi pendeteksian bahwa media sedang sibuk ketika node lain mentransmisikan. Dengan demikian,

ÿ = 1 ÿ Pr{node mendeteksi medium idle saat sedang digunakan}(6.1)

Parameter ÿ adalah ukuran beban kerja yang dapat didukung oleh node nirkabel sesuai dengan kondisi lingkungan multihop kolaboratif, di mana node dapat mengirim dan menerima frame secara bersamaan. Ini diukur dengan meningkatkan jumlah beban kerja secara berkala hingga node mulai menjatuhkan paket secara tidak terduga. Penulis membagi proses pengiriman paket menjadi tiga keadaan: keadaan diam , keadaan aktif dan keadaan kios . Keadaan siaga mengacu pada saat media nirkabel tidak ditempati oleh node, seperti DIFS dan slot waktu yang dihabiskan selama penghitung back-off eksponensial. Nilai-nilai ini dapat diperoleh dari spesifikasi standar. Keadaan aktif, di sisi lain, mencakup saat-saat ketika node benar-benar "mendorong" bit ke udara. Terakhir, kondisi kios menjelaskan saat node merasakan saluran, atau saat menerima data yang ditujukan untuk dirinya sendiri. Dengan demikian, total kecepatan data yang dapat dikirim oleh sebuah node dalam lingkungan jenuh adalah

$$\text{dataSentSTA} = L \cdot \frac{1}{\text{Tidle} + \text{Taktif} + \ddot{y} \cdot \text{Tstall}}, \quad 0 < \ddot{y} < 1 \qquad (6.2)$$

$$\ddot{y} = \frac{\frac{L}{\text{dataSentSTA}} \ddot{y}\ \text{Taktif}\ \ddot{y}\ \text{Tidle}}{\text{Mengirim}} \qquad (6.3)$$

di mana L adalah panjang tetap (dalam bit) dari paket yang dikirim, dan Tidle, Tactive, dan Tstall adalah waktu yang dihabiskan oleh node nirkabel yang akurat dalam status siaga, aktif, dan macet. Waktu idle dan aktif ditentukan oleh standar dan dapat dengan mudah diperoleh berdasarkan konfigurasi node. Tstall dapat diperoleh dengan alasan berikut: Dalam skenario dua node yang ideal, ketika satu node dalam keadaan aktif, yang lain mendeteksi medium sebagai sibuk dan jatuh dalam keadaan mati dan sebaliknya. Jadi, karena protokol 802.11 adil, Tstall untuk satu node harus persis sama dengan Tactive untuk node lainnya. Pengukuran terakhir dapat dihitung dari spesifikasi standar IEEE 802.11 [118]. Dengan demikian, persamaan (6.3) dapat digunakan untuk memperoleh ÿ setelah percobaan. Nilai ÿ yang secara signifikan kurang dari 1 merupakan indikasi bahwa CS tidak akurat dan perlu

dipertanggungjawabkan. Setelah masalah diidentifikasi, langkah diagnosis dapat dilakukan untuk mengidentifikasi sumber masalah yang tepat. Misalnya, penganalisa spektrum atau pengukur daya dapat digunakan untuk mengukur daya transmisi pada pengirim dan penerima jika diduga bahwa mekanisme CS yang tidak akurat adalah hasil dari pengaturan daya yang salah.

Secara umum, karakterisasi perangkat dapat digunakan untuk menganalisis banyak aspek

perangkat perangkat keras, dan Portoles-Comeras et al. [48] memberikan ringkasan yang bagus tentang atribut perangkat lain yang dapat diperiksa.

Sejauh menyangkut simulasi, kami berasumsi bahwa penerapan lapisan MAC penuh diadopsi; model yang mengimplementasikan semua fitur dan aspek didefinisikan dan digunakan untuk keseluruhan waktu simulasi. Ketika jaringan skala besar dipertimbangkan, lapisan MAC menjadi penghambat simulasi. Sekitar 90% dari waktu dihabiskan untuk mensimulasikan peristiwa lapisan MAC. Dia dkk. [119] mengusulkan model simulasi yang fleksibel untuk meningkatkan skalabilitas simulasi. Proposal adalah hibrida

solusi di mana tingkat abstraksi bervariasi secara dinamis sesuai dengan tingkat akurasi saat ini. Statistik yang dikumpulkan selama simulasi digunakan untuk beralih menjadi tween model lengkap yang mencakup semua aspek dan disederhanakan. Pendekatan ini didemonstrasikan untuk mendapatkan simulasi yang lebih cepat dengan hilangnya akurasi yang dapat disesuaikan.

6.3.4 Pengaruh pada Lapisan Atas dan Isu Lainnya

Perbedaan kinerja antara simulasi dan testbed sehubungan dengan protokol dan aplikasi lapisan atas sebagian besar disumbangkan oleh pemodelan saluran nirkabel yang tidak sempurna.

Sejumlah penelitian telah mendukung pernyataan ini. Nordstrom et al. [120] menarik kesimpulan ini setelah mengevaluasi protokol AODV, DSR, dan OLSR dalam skenario yang berbeda dan dengan jenis lalu lintas yang berbeda menggunakan kombinasi simulasi, emulasi, dan eksperimen dunia nyata. Mereka mengalami konektivitas yang berfluktuasi saat terpapar ke lingkungan radio nyata, menyebabkan masalah bagi protokol perutean dalam menyiapkan dan memelihara rute. Ini menyoroti dinamika dunia nyata dari saluran radio yang sangat memengaruhi kinerja protokol perutean. Perbedaan dapat disebabkan oleh model propagasi yang digunakan, yang dapat melebih-lebihkan atau kurang mewakili jangkauan transmisi, seperti yang ditemukan dalam referensi 56. Tan et al. [75] menemukan bahwa perilaku lapisan MAC yang berbeda dalam simulator dan testbed menyebabkan respons yang berbeda terhadap lalu lintas padat. Mereka melakukan pengukuran throughput di testbed nyata dan pada ns-2 dan QualNet, dan menemukan ketidaksetaraan tingkat aliran yang ekstrim dalam skenario di mana ada banyak aliran antara node yang berbeda di testbed sebenarnya. Mereka mengaitkan fenomena ini dengan perbedaan kemampuan transceiver nodal seperti daya transmisi dan sensitivitas penerima. Node yang memiliki kemampuan lebih lemah pada dasarnya tenggelam karena gangguan dari aliran yang lebih kuat. Simulator menganggap aliran identik jika daya transmisi, jarak, dan kualitas saluran di antara node serupa, yang biasanya tidak demikian di dunia nyata.

Perbedaan level node dalam simulator dan testbed juga dapat menyebabkan kesenjangan performa. Misalnya, node di dunia nyata dibatasi oleh daya komputasi dan antrian prosesor serta buffer paket dari sistem operasi. Jadi, mereka biasanya menjatuhkan paket jika mereka tidak dapat melanjutkan dengan kecepatan jalur nirkabel, bahkan jika paket diterima dengan benar [121]. Selain itu, masalah latensi dan waktu memainkan peran penting dalam lingkungan yang sangat dinamis. Protokol reaktif

seperti AODV dan DSR mengandalkan buffering paket selama masa pemutusan. Hal ini menyebabkan penumpukan antrian yang memengaruhi urutan pengaturan waktu dan pesan kontrol, sangat mengurangi efisiensi protokol [120]. Sebaliknya, simulasi memiliki model berbasis peristiwa dan buffer yang disederhanakan, dan oleh karena itu masalah pemrosesan, buffering, dan pengaturan waktu tidak terlihat.

Menggemakan aspek ini, Ivanov et al. [122] menemukan bahwa dibandingkan dengan testbed nyata, akurasi latensi paket lebih rendah di ns-2, bahkan setelah rasio pengiriman paket dan topologi jaringan direpresentasikan secara akurat dan parameter simulator disesuaikan dengan benar. Selain itu, keistimewaan perangkat keras dapat menyebabkan hasil pengujian yang bias. Ini adalah masalah penting untuk diperhatikan karena dengan pengaturan eksperimental yang sama, pengamatan yang berbeda dapat diperoleh dari simulator dan implementasi dunia nyata dan juga dari testbed yang berbeda. Kepercayaan terhadap kemungkinan ini diberikan oleh Angrisani et al. [123], yang mengukur kapasitas tautan nirkabel di lingkungan testbed dan menemukan bahwa kinerja beberapa alat pemantauan kapasitas sangat dipengaruhi oleh karakteristik kartu antarmuka jaringan.

Meskipun contoh yang diberikan di atas menyiratkan bahwa hasil testbed lebih pesimis daripada yang dikumpulkan dari simulasi, hal ini tidak selalu terjadi. Misalnya, di beberapa

simulator, efek tangkapan tidak dimodelkan. Pada kenyataannya, itu mungkin terjadi, artinya satu frame dapat bertahan dari tabrakan yang dihasilkan dari transmisi simultan dari terminal

yang berbeda. Dalam hal ini, akan ada dampak positif pada hasil testbed, karena lebih sedikit bingkai yang hilang. Hal utama yang dapat diambil adalah bahwa masalahnya bukanlah masalah kinerja melainkan masalah keandalan; penting untuk mengenali perbedaan antara dua paradigma eksperimen yang berpotensi mempengaruhi keandalan hasil yang diperoleh.

Meskipun tidak mungkin untuk mencerminkan dunia nyata melalui simulator, pendekatan yang sangat baik dapat dicapai. Ivanov dkk. [122], tunjukkan bahwa rasio pengiriman paket dan topologi jaringan secara akurat direpresentasikan dalam ns-2, setelah parameter simulator seperti model mobilitas dan propagasi dipilih dengan benar. Peneliti lain menyoroti pentingnya memilih simulator yang tepat dan parameterisasi sesuai dengan konteks [56,58,76]. Dengan melakukan itu, mereka dapat mencapai hasil yang sangat cocok dengan rekan eksperimental mereka. Untuk meningkatkan kesamaan latensi paket dan waktu pemrosesan dalam simulator, implementasi tumpukan TCP/IP dari Sistem Operasi dapat digunakan sebagai pengganti versi yang disediakan oleh simulator. Ns-3 menawarkan fasilitas ini melalui Network Simulator Cradle (NSC) [124]. Di sisi lain, ns-3, melalui komponen Emu NetDevice - nya , memungkinkan simulator mengirim dan menerima paket melalui jaringan nyata, secara efektif memungkinkannya menggunakan lapisan MAC dan PHY dari perangkat host [125]. Kerangka kerja simulasi INET dari OMNeT++ juga memiliki kemampuan ini [126]. Kami membahas fitur ini di Bagian 6.5.

6.3.5 Perbandingan Kemampuan Simulator

Pada bagian ini kami memberikan perbandingan simulator jaringan yang disajikan pada Bagian 6.2.1. Fokusnya adalah pada model dan fitur yang diberikan kepada pengguna untuk simulasi jaringan ad hoc seluler. Tujuan dari survei ini adalah untuk memberikan gambaran tentang informasi yang diperlukan untuk memutuskan simulator mana yang harus diadopsi untuk studi tertentu.

Memang, pemilihan simulator harus didorong oleh kebutuhan skenario simulasi. Selain aspek ini, faktor lain mungkin memainkan peran penting juga.

Misalnya, ketika skenario kompleks dengan jumlah node yang tinggi dipertimbangkan, simulator paralel akan menjadi pilihan yang bijak.

Kami mulai meringkas perbedaan model fisik pada Tabel 6.3. Seperti dapat dilihat, semua simulator mengimplementasikan hampir semua model umum dalam simulasi lapisan fisik.

Perbedaan utama di antara proyek-proyek tersebut adalah pada bagaimana interferensi disimulasikan. Setiap simulator mengimplementasikan hanya satu model untuk komputasi interferensi: Tiga simulator menggunakan model yang paling akurat, model interferensi penuh , sedangkan tiga simulator lainnya mengadopsi model terbatas , yang mendekati interferensi keseluruhan sebagai jumlah dari daya komunikasi yang diterima yang terjadi pada waktu tertentu. jarak dari penerima. Hanya ns2 yang mengadopsi model interferensi Terkuat .

Table 6.3 PHY Model Comparison

Parameter	ns2	ns3	QualNet	Jist/Swans	GloMoSim	OMNeT++	Opnet
Path loss	Free Space, Two-Ray	Free Space, Two-Ray	Free Space, Two-Ray	Free Space, Two-Ray	Free Space, Two-Ray	Free Space, Two-Ray	Free Space, Two-Ray
Shadowing	log-normal	log-normal	log-normal	NONE	log-normal	log-normal	None
Fading	Ricean, Rayleigh	Ricean, Rayleigh[a]	Ricean, Rayleigh	Ricean, Rayleigh	Ricean, Rayleigh	Rayleigh	Ricean
Interference	Limited, strongest	Full	Full	Limited, distance	Limited, distance	Limited, distance	Full
Reception	SINR[b]	SINR and BER	SINR and BER	SINR and BER	SINR and BER	SINR and BER	SINR and BER

[a] More complex fading model available.
[b] BER available through YANS extension.

Kami sengaja menghilangkan model mobilitas dalam perbandingan kami karena penerapan model mobilitas baru dalam simulator adalah tugas yang relatif sederhana dan berbagai model tersedia untuk simulator apa pun sebagai kontribusi eksternal. Di antara implementasi eksternal ini kami menyoroti alat Bonnmotion [127], yang dianggap sebagai model de facto dalam simulasi

mobilitas seperti yang ditunjukkan oleh sejumlah besar pekerjaan yang menggunakannya. Bonnmotion

adalah perangkat lunak berbasis Java yang dikembangkan untuk membuat dan menganalisis skenario mobilitas. Beberapa model mobilitas diimplementasikan: Random Waypoint, Random Walk, Gauss–Markov, Manhattan Grid, Reference Point Group Mobility, Disaster Area, Random Street, dan banyak lagi. Skenario yang dihasilkan dapat diekspor ke hampir semua simulator jaringan yang tersedia.

Pada Tabel 6.4 kami membandingkan kerangka simulator yang tersedia dari sudut pandang implementasi MAC mereka. Seperti perbandingan sebelumnya, kami fokus pada standar MAC IEEE

802.11 yang merupakan standar paling populer untuk penerapan MANET nyata.

Pada Tabel 6.5 kami membandingkan kerangka kerja simulator yang tersedia dari sudut pandang lapisan atas. Secara khusus, kami memberikan ikhtisar tentang perutean, protokol transport, dan implementasi aplikasi yang tersedia.

Terlepas dari pilihan simulator, kami harus menunjukkan bahwa keandalan dan keakuratan simulasi juga bergantung pada penggunaan alat yang benar. Terlepas dari asumsi model yang buruk, praktik simulasi yang buruk seperti kesalahan konfigurasi atau desain simulasi yang buruk juga dapat membahayakan keandalan hasil simulasi. Untuk menghindari kesalahan umum ini, seperangkat praktik terbaik dalam teknik simulasi dapat diadopsi.

Perrone et al. [136] memberikan pedoman tersebut. Kami membahasnya di bagian berikut.

6.4 SIMULASI YANG BAIK: VALIDASI, VERIFIKASI, DAN KALIBRASI

Seperti yang ditunjukkan dalam referensi 1 dan 2, beberapa studi simulasi kurang memiliki kredibilitas karena peneliti tidak mengikuti rekomendasi dasar dan praktik yang baik untuk memastikan keandalannya. Sumber bias hasil dalam simulasi dapat dikategorikan menjadi dua kelompok: praktik simulasi yang tidak tepat dan inkonsistensi model simulasi. Praktik simulasi yang baik secara langsung disebabkan oleh kesalahan yang dilakukan oleh peneliti pada saat simulasi; mereka dapat dengan mudah diperbaiki dengan mengikuti prosedur ilmiah yang ketat yang menyediakan pengulangan dan validitas statistik. Faktanya, menjalankan simulasi memerlukan perhatian khusus pada serangkaian praktik baik standar yang bertujuan untuk memastikan validitas statistik dan ketepatan hasil [2]. Di sisi lain, ketidakkonsistenan model yang tidak tepat lebih sulit ditemukan dan biasanya memerlukan modifikasi pada model simulasi untuk memperbaikinya.

Alur kerja yang ditunjukkan pada Gambar 6.5 adalah alur kerja umum yang dapat digunakan untuk menilai keandalan model simulasi dan memperbaiki ketidakakuratan dan bias: Verifikasi implementasi, validasi asumsi model, lalu kalibrasi parameter masukan. Sepanjang bab ini, kami terkadang menyebutkan verifikasi, validasi, dan kalibrasi.

Meskipun maknanya seharusnya diketahui dengan baik, istilah-istilah tersebut sering disalahgunakan

Table 6.4 IEEE 802.11 MAC Implementations Comparison

Parameter	ns2	ns3	QualNet	Jist/Swans	GloMoSim	OMNeT++	Opnet
Protocol operation[a]	DCF, EDCA	DCF, EDCA	DCF, EDCA	DCF	DCF	DCF, EDCA	DCF, EDCA
RTS/CTS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transmission rate	Single rate[b]	Multirate[c]	Multirate	Single rate	Single rate	Single rate	Multirate
Multichannel/ interface	Single channel/interface[d]	Multichannel/ interface	Multichannel/ interface	Single channel/interface[d]	Multichannel/ interface	Multichannel/ interface	Multichannel/ interface
Power saving mode	External patch [128]	None	Yes	None	None	Yes	Yes

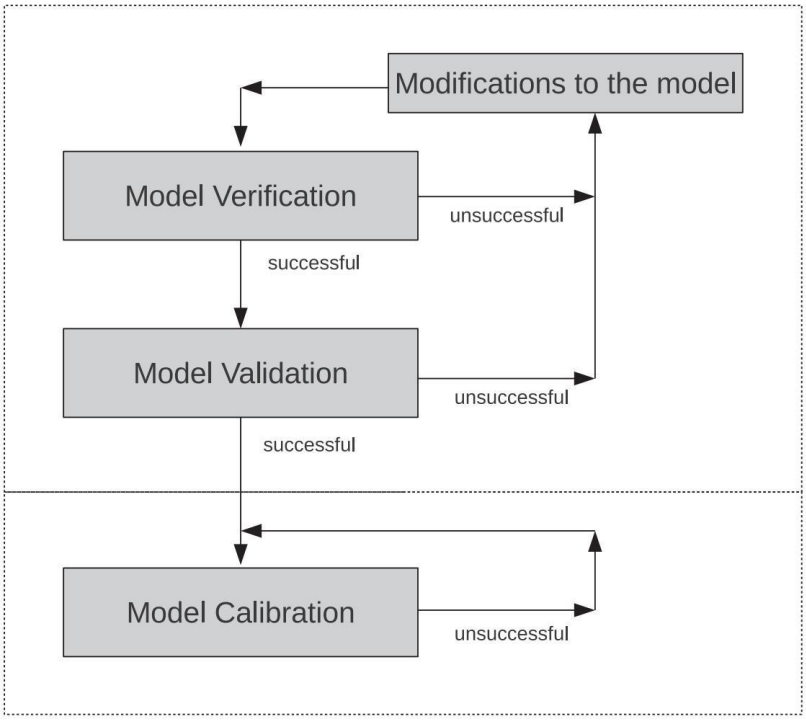
[a] We include only the operations allowed in ad hoc mode.
[b] Multirate with AARF algorithm provided by an external patch [129].
[c] ARF AARF and RRAA available as auto fallback algorithms.
[d] Multichannel/interfaces provided by an extension [130].
[e] Multichannel/interfaces provided by a MIRACLE extension [131].

Table 6.5 Upper Layers Implementations Comparison

	ns2	ns3	QualNet	Jist/Swans	GloMoSim	OMNeT++	Opnet
Routing protocols	AODV, DSR, OLSR, DYMO[a]	AODV, DSDV, DSR, OLSR	ZRP, DSR, AODV, DYMO	ZRP, DSR, AODV	AODV, DSR	AODV, DYMO, DSR, OLSR, BATMAN	AODV, DSR, OLSR
Transport Protocols	UDP, TCP, SCTP	UDP, TCP	UDP, TCP, RSVP-TE	UDP, TCP	UDP, TCP	UDP, TCP, RSVP-TE, SCTP, RTP	UDP, TCP, SCPS, RSVP-TE, RTP
Aplications	HTTP, FTP, VoIP[b]	OnOff, bulk sender, ping, UDP client-server	VoIP, CBR, FTP, HTTP, TRAFFIC	Real Java application	CBR, FTP, HTTP, Telnet	CBR, HTTP, FTP, Voice, Video, Peer To Peer	CBR, Custom, Database, Email, FTP, HTTP, TELNET, VBR, Voice, Video

[a] All provided by extensions, [132–134].
[b] VoIP traffic provided by ns2voip++ extension [135].

.



Gambar 6.5 Alur kerja praktik yang baik

atau lebih tepatnya kurang dipahami. Untuk alasan ini kami akan mulai memberikan ikhtisar tentang definisi mereka:

• Verifikasi adalah suatu proses yang dimaksudkan untuk mengevaluasi seberapa tepat implementasi tertentu cocok dengan model aslinya; yaitu, model mengimplementasikan asumsi dengan benar. Saat bug ditemukan, implementasi model diubah dan verifikasi dijalankan lagi untuk memeriksa kebenaran perbaikan. • Validasi mengestimasi seberapa

benar model merepresentasikan dunia nyata–yaitu, jika perkiraan dan asumsi yang diperkenalkan oleh model masuk akal sehubungan dengan sistem nyata. Ketika ketidakkonsistenan ditemukan dalam model, spesifikasinya harus dimodifikasi. Setelah memodifikasi model awal untuk menghapus atau mengurangi ketidakakuratan, verifikasi dapat dijalankan kembali untuk menemukan ketidakakuratan implementasi baru sebelum mengulangi prosedur validasi. • Kalibrasi adalah proses yang menentukan modifikasi yang

diperlukan oleh parameter input default untuk membuat pendekatan yang lebih baik dari sistem nyata.

Kebalikan dari validasi dan verifikasi, kalibrasi seharusnya dilakukan bukan oleh pengembang model tetapi oleh pengguna tepat sebelum menjalankan skenario simulasi tertentu. Sejauh menyangkut simulasi jaringan, prinsip dan praktik baik yang sama berlaku. Jaringan yang akan disimulasikan adalah sistem kompleks yang perlu dimodelkan dan akibatnya divalidasi dan diverifikasi. Dari sudut pandang ini, seluruh skenario simulasi dapat didekomposisi secara hierarkis menjadi skenario skala kecil: model sistem skala kecil (misalnya, transmisi saluran fisik) atau protokol komunikasi tunggal (misalnya, TCP, UDP). Strategi penguraian sistem secara hierarkis ini biasanya diadopsi untuk memvalidasi dan memverifikasi keseluruhan skenario. Sebagai praktik yang baik, alur kerja harus dimulai dari model

skala kecil dan diakhiri dengan keseluruhan sistem karena potensi ketidakakuratan dalam skenario skala kecil mungkin tidak diperbesar pada skala yang lebih besar.

Karena validasi dimulai dari asumsi bahwa implementasi model tanpa kesalahan, verifikasi harus dilakukan terlebih dahulu. Praktik verifikasi umum dipinjam dari peranan mobile ad hoc dalam komunikasi data: Model simulasi jaringan dapat dianggap sebagai program komputer besar yang penerapannya harus diverifikasi agar sesuai dengan spesifikasi model. Di antara praktik-praktik verifikasi yang paling banyak digunakan adalah sebagai berikut: code walk-through/one step analysis (analisis kode statis), tracing/ animation (untuk menyoroti perilaku buruk melalui bantuan alat), pengujian degenerasi (untuk memeriksa implementasi dalam kasus degenerasi yang dipilih), dan pengujian konsistensi (untuk memverifikasi bahwa beberapa perilaku yang diharapkan ditampilkan).

Setelah memverifikasi bahwa implementasi sesuai dengan spesifikasinya, validasi harus dijalankan untuk menunjukkan bahwa model merupakan representasi yang masuk akal dari sistem yang sebenarnya; yaitu, ini mewakili perilaku sistem dengan presisi dan ketepatan yang cukup sesuai dengan tujuan analisis. Bertentangan dengan verifikasi, tidak ada praktik dan teknik yang diakui secara luas untuk memvalidasi simulator jaringan dan mengevaluasi keterpercayaan hasil mereka. Pendekatan yang paling umum adalah membandingkan hasil yang diperoleh dari model dengan sesuatu yang dianggap sebagai kebenaran dasar untuk memperkirakan kesenjangan. Berikut ini sering diadopsi sebagai perbandingan:

• Pengukuran Sistem Nyata. Ini adalah cara validasi yang paling dapat diandalkan dan disukai karena merupakan cara paling langsung untuk mengukur kesenjangan antara model dan sistem nyata. Dalam praktiknya, perbandingan ini seringkali tidak layak karena penyebaran nyata belum ada atau harganya mahal.

• Hasil Teoritis. Perbandingan dengan hasil teoritis atau hasil dari analisis operasional dilakukan ketika model analisis dapat diturunkan. Teknik ini harus digunakan dengan hati-hati karena kriteria untuk perbandingan juga bisa tidak valid atau tidak akurat.

• Perbandingan Langsung Antara Model Independen. Kelompok independen mengembangkan model yang berbeda dan kemudian membandingkan hasil yang diperoleh dari mereka. Praktik ini sangat intensif sumber daya tetapi tingkat kepercayaannya biasanya sangat tinggi.

Kasus khusus yang terakhir adalah ketika perbandingan dilakukan di antara model yang berbeda yang diimplementasikan ke dalam simulator yang berbeda. Praktik ini berbiaya rendah, terutama jika model tertentu populer dan diterapkan di berbagai simulator open source.

Kelemahan utamanya adalah kenyataan bahwa tidak seorang pun di antara implementasi yang

berbeda dapat dianggap sebagai referensi yang baik secara apriori , atau setidaknya sebaik sistem nyata, dan akibatnya beberapa ketidakakuratan masih dapat tetap ada setelah proses. Baru-baru ini, peningkatan jumlah simulator open source yang tersedia telah memungkinkan praktik ini sering digunakan dalam skala besar. Untuk alasan ini, upaya dalam mengotomatisasi proses validasi telah dilakukan: Dalam referensi 137 sebuah kerangka kerja untuk mengotomatisasi perbandingan perilaku dan hasil dari simulator yang berbeda untuk validasi diusulkan.

Model biasanya diverifikasi dan divalidasi pada kasus penggunaan tertentu. Jika pengguna akhir atau pemodel berencana untuk mensimulasikan skenario yang sedikit berbeda dari default, kalibrasi harus dilakukan untuk memastikan hasil yang baik. Kalibrasi adalah proses iteratif yang melibatkan validasi

model setelah setiap langkah modifikasi sehingga keluaran model lebih mirip dengan sistem nyata. Ini menyiratkan bahwa output model harus dibandingkan dengan hasil sistem nyata atau pengganti yang sesuai melalui metode statistik atau "Uji Turing" di mana para ahli mencoba untuk mengetahui apakah ada perbedaan yang signifikan antara kedua output. Namun, kalibrasi adalah proses yang menakutkan karena kerumitan sistem yang dimodelkan. Sulit untuk membuat sistem atau pengganti yang tepat mewakili MANET yang ditargetkan karena biaya penyebaran, kurangnya pengulangan dan kerugian lain yang terkait dengan sistem nyata. Untuk mengatasinya, Green dan Reddy [138] menyarankan meniru lingkungan RF seluler untuk memberikan perkiraan lingkungan dunia nyata. Mereka menghubungkan delapan node dalam topologi bintang yang terhubung sepenuhnya dan menggunakan splitter yang terpasang pada atenuasi RF untuk mengizinkan koneksi sewenang-wenang antara node. Mereka kemudian mengadopsi tes termasuk pembentukan jaringan, entri simpul terlambat, simpul keluar, dan penggabungan dan partisi pulau, antara lain, dan mengumpulkan metrik seperti throughput, delay, jitter, byte yang ditransmisikan, dan kehilangan paket.

Metrik dikumpulkan berdasarkan per tautan dan dibandingkan dengan data simulasi menggunakan

alat analisis statistik (StatFit [139]) untuk menentukan apakah diperlukan langkah kalibrasi lebih lanjut. Perubahan dapat berupa, antara lain, penyesuaian untuk memperbaiki asumsi RF atau komponen komputer yang tidak benar, atau representasi model lingkungan RF yang buruk.

Sayangnya, tidak selalu praktis untuk memiliki sistem nyata yang mendekati skenario MANET. Oleh karena itu, jika tidak dapat diakses, kalibrasi mungkin harus melibatkan analisis subyektif dari data yang dikumpulkan. Ini adalah metode yang digunakan oleh Hong et al. untuk memilih model mobilitas yang tepat dalam skenario di mana node memiliki mobilitas tinggi tetapi tidak harus menempuh jarak yang jauh selama pergerakannya [140].

Diberikan dua model mobilitas, Jalan Acak dan Vektor Mobilitas, mereka mengukur jarak tempuh aktual dan perpindahan geografis selama beberapa interval dalam simulasi dan menormalkan rata-rata jarak tempuh sebenarnya dengan perpindahan geografis masing-masing. Hasilnya adalah jarak ekstra yang ditempuh untuk mencapai perpindahan geografis tertentu. Mereka kemudian menunjukkan bahwa Model Jalan Acak menghasilkan lebih banyak jarak perjalanan ekstra daripada Model Vektor Mobilitas untuk mencapai perpindahan yang sama, yang berarti bahwa pada kecepatan sesaat yang sama, former menghasilkan perpindahan geografis yang lebih sedikit. Dengan demikian, ini akan lebih cocok untuk skenario di mana node memiliki mobilitas tinggi tetapi menunjukkan perpindahan geografis aktual yang rendah.

Seperti dapat dilihat, kalibrasi merupakan proses yang sulit; tetapi, jika dilakukan dengan benar, ini dapat meredakan sakit kepala para peneliti yang timbul dari pemecahan masalah hasil simulasi yang tidak terduga dan meningkatkan ketepatan hasil.

6.5 SIMULATOR DAN TESTBED: PROSPEK MASA DEPAN

Prospek masa depan terkait dengan simulator dan testbed difokuskan pada tiga bidang utama: interoperabilitas, peningkatan akurasi , dan definisi model baru.

Simulator dan testbed telah dianggap dalam literatur sebagai dua alat berbeda yang jarang

diadopsi bersamaan pada waktu yang bersamaan. Baru belakangan ini kebutuhan untuk mengintegrasikan kedua pendekatan ini diakui sebagai fitur yang diinginkan untuk simulator generasi

berikutnya. pengembangan ns3 menunjukkan bagaimana mengintegrasikan simulator dan testbeds diakui sebagai fitur penting.

Meskipun validasi telah dibedakan sebagai praktik terbaik untuk mengevaluasi keakuratan hasil, belum banyak yang dilakukan untuk mengoptimalkan dan mengotomatiskan prosedur ini.

Di satu sisi, testbed dan simulator dikembangkan secara terpisah; di sisi lain, validasi memerlukan interaksi di antara keduanya: Protokol yang sama harus diterapkan pada simulator dan perangkat nyata. Alur kerja yang umum adalah mengimplementasikannya terlebih dahulu di satu platform lalu mem-porting atau mengimplementasikannya kembali di platform lain. Hasilnya adalah dua basis kode yang benar-benar terpisah untuk digunakan dan dipelihara, yang sangat tidak efisien dan rawan kesalahan.

Untuk mengatasi masalah ini, pendekatan baru telah diusulkan dalam literatur: eksekusi langsung kode dari perangkat nyata dalam simulator. Tujuannya adalah untuk memodifikasi struktur simulator untuk memungkinkan eksekusi kode secara langsung tanpa perlu migrasi kode antar platform. Referensi 56 menggarisbawahi pentingnya eksekusi langsung kode testbed di simulator untuk memfasilitasi validasi. Penulis memodifikasi simulator untuk memungkinkan eksekusi langsung dari algoritma routing secara langsung menggunakan kode sistem nyata. Pendekatan ini didemonstrasikan untuk menghasilkan implementasi ide-ide baru yang akurat, andal, dan cepat baik dalam simulasi maupun testbed dengan sedikit usaha.

Arah yang sama telah diadopsi oleh proyek click [141] dan Nsclick [142].

Click adalah kerangka kerja untuk membangun dan menerapkan router paket yang cepat, fleksibel, dan dapat dikonfigurasi. Perilaku router ditentukan dengan menghubungkan elemen perutean klik standar atau yang dipersonalisasi. Hasilnya adalah paket mengalir melalui router sebagai serangkaian manipulasi paket yang dijalankan oleh setiap elemen. Setiap modul diprogram sebagai objek C++ yang menerima dan mengirim paket dari/ke modul lain melalui port. Klik memungkinkan definisi perilaku router pada layer 2 dan layer 3; yaitu, penerapan standar lapisan MAC dan IP dapat ditimpa melalui elemen Klik. Kode klik dapat dijalankan baik di kernel maupun ruang pengguna. Namun, opsi yang pertama hampir selalu lebih disukai karena opsi yang terakhir menyiratkan tambahan di atas kepala yang menghasilkan jauh lebih lambat [143]. Nsclick bertujuan untuk mengintegrasikan klik dan ns-2 untuk mengaktifkan eksekusi langsung kode klik di dalam simpul ns-2. Proyek ini memungkinkan eksekusi langsung dari kode Layer-3 tanpa banyak modifikasi–misalnya, memungkinkan eksekusi algoritma routing pada simulator serta sistem nyata [144]. Di sisi lain, Layer 2 tidak dapat langsung dieksekusi di Nsclick dan membutuhkan lebih banyak modifikasi. Namun demikian, beberapa contoh porting dapat ditemukan dalam literatur; misalnya, Nsmadwifi yang memperluas Nsclick untuk mendukung fitur nirkabel [145]. Eksperimen yang menjanjikan namun masih baru lahir telah diusulkan lagi di ns-3 [146]. Solusi alternatif memungkinkan simpul simulasi untuk mengirim dan menerima paket melalui jaringan nyata, sehingga memberikannya akses ke lapisan MAC dan PHY dunia nyata. Emu NetDevice memberikan kemampuan ini ke ns-3. Ini membuka soket mentah dan mengikat antarmuka fisik yang dalam mode promiscuous [125]. Soket mentah memungkinkan penggunaan alamat MAC khusus, sehingga menghindari potensi tabrakan dengan perangkat lain. Paket dari lapisan atas dikirim melalui raw socket. Alamat IP yang digunakan oleh perangkat net yang diemulasi sesuai dengan yang dihasilkan selama penyiapan simulasi. Emu NetDevice memberikan kesempatan untuk menggunakan implementasi lapisan MAC dan PHY yang nyata, tetapi kelemahan utamanya adalah bahwa antarmuka nirkabel yang ditentukan harus dalam mode promiscuous, yang tidak didukung secara universal oleh driver kartu nirkabel. Selain itu, karena alamat IP dari perangkat yang disimulasikan dikonfigurasi sebagai alamat antarmuka, hanya satu node yang disimulasikan yang dapat dijalankan per host.

Sebuah solusi untuk ini adalah menjalankan simulator pada perangkat virtual seperti VMware [147]. Kerangka kerja INET untuk OMNeT++ memberikan utilitas serupa [126]. Salah satu perbedaan utama adalah bahwa simpul yang disimulasikan tidak dapat memiliki alamat IP yang dikonfigurasi sebagai alamat IP dari antarmuka sebenarnya. Oleh karena itu, alih-alih soket mentah, pustaka penangkap paket libpcap digunakan untuk menangkap paket yang diterima yang diuraikan dan diterjemahkan ke dalam objek OMNeT++. Karena alamat IP dari node yang disimulasikan berbeda dari host, antarmuka jaringan harus dalam mode promiscuous sehingga libpcap dapat menangkap paket yang secara teknis tidak ditujukan untuk host.

Mengirim paket dapat dilakukan menggunakan soket mentah IP dan libpcap. Keuntungan ekstra dari

implementasi ini adalah bahwa satu host fisik atau virtual dapat mendukung banyak node yang disimulasikan. Sama seperti Emu NetDevice, antarmuka yang digunakan harus diatur dalam mode promiscuous.

Pengembangan model mobilitas yang lebih realistis namun mudah diatur masih menjadi area penelitian yang aktif. Salah satu jalan untuk mengeksplorasi adalah ekstraksi dan generalisasi data jejak mobilitas untuk dimasukkan dalam desain model [148.149]. Selain itu, meningkatkan model berbasis kelompok menggunakan karakteristik jaringan sosial akan memungkinkan evaluasi proposal yang realistis seperti protokol routing oportunistik. Skenario dalam ruangan yang dibangun berdasarkan pemodelan hambatan kurang terwakili dalam model mobilitas saat ini, dan oleh karena itu aspek seperti pemodelan hambatan perlu ditingkatkan untuk memungkinkan penilaian skenario dalam ruangan yang lebih akurat. Saat ini, cara pengujian mobilitas dalam ruangan yang paling umum adalah melalui penerapan tempat pengujian dalam ruangan. Ketersediaan luas perangkat seluler yang memiliki beragam antarmuka jaringan seperti WiFi, Bluetooth, dan seluler, di samping kemampuan GPS, juga dapat dimanfaatkan untuk mengumpulkan jejak yang terkait dengan aplikasi tertentu, atau bahkan memungkinkan evaluasi aplikasi dan protokol. Ini dapat dilakukan dengan mengembangkan kerangka kerja atau perangkat lunak yang dapat diunduh yang memungkinkan protokol atau aplikasi yang menjalani pengujian berjalan di perangkat pengguna akhir.

Kerangka seperti itu juga dapat digunakan untuk memperluas kumpulan jejak yang tersedia untuk umum.

Standar komunikasi baru telah menunjukkan tingkat kompleksitas yang lebih tinggi karena penerapan teknik baru seperti MIMO [150] dan H-ARQ [151]. Model untuk teknik baru ini telah ditetapkan; namun, tidak satupun dari mereka telah diakui sebagai akurat dan dapat diandalkan. Untuk alasan ini, hanya sedikit yang bekerja untuk mengevaluasi standar terbaru seperti IEEE 802.11n [152] yang ada dalam literatur, dan hampir semuanya menggunakan testbed daripada simulasi. Mengembangkan model yang dengan tepat menggambarkan teknologi baru ini akan menjadi usaha yang menantang namun sangat bermanfaat.

6.6 KESIMPULAN

Dalam bab ini kami memberikan ikhtisar tentang bagaimana simulator dan testbed dapat digunakan untuk menilai kinerja jaringan ad hoc seluler. Secara khusus, kami fokus pada semua masalah yang memengaruhi kesenjangan antara hasil simulasi dan eksperimen.

Harapan penulis adalah bahwa bab ini akan membantu pembaca memahami kapan aman menggunakan simulator alih-alih penerapan nyata dan juga mengidentifikasi masalah yang dapat

membahayakan keandalan dan keakuratan hasil. Serangkaian pelajaran yang dapat diambil di rumah yang diperoleh dari literatur yang ada dapat diringkas:

1.Jika diperlukan hasil yang sangat akurat, implementasi testbed harus lebih disukai daripada simulasi.

2.Ketika simulasi diadopsi, simulator terbaik harus dipilih sesuai kebutuhan.

3.Validasi adalah praktik yang baik yang diperlukan untuk memperkirakan keandalan hasil dan untuk menemukan masalah kesalahan konfigurasi. Selain itu, dapat digunakan untuk memverifikasi kesesuaian model dan pengaturan yang tepat dari parameternya.

4.Perbandingan hasil simulasi dengan pengukuran testbed harus dilakukan keluar, dan perbedaan harus hati-hati dianalisis.

5.Serangkaian praktik yang baik harus diikuti untuk menyiapkan simulasi dan eksperimen untuk mengurangi bias yang disebabkan oleh kesalahan konfigurasi atau desain perangkat lunak dan perangkat keras yang buruk. Selain itu, karakterisasi, kalibrasi, dan konfigurasi yang tepat dan akurat harus mendahului simulasi dan eksperimen dunia nyata.

CHAPTER 7
OPTIMASI SUMBERDAYA PADA PT MULTISALURAN MULTI RADIO JARINGAN NIRKABEL MESH

7.1 PENDAHULUAN

Jaringan mesh nirkabel adalah salah satu solusi yang paling menjanjikan untuk penyediaan konektivitas nirkabel dengan cara yang fleksibel dan hemat biaya [1]. Jaringan mesh nirkabel (WMN) terdiri dari campuran node tetap dan seluler yang saling terhubung melalui tautan nirkabel untuk membentuk jaringan ad hoc multihop.

Perbedaan utama antara WMN dan jaringan ad hoc seluler (MANET) terletak pada arsitektur jaringan secara umum. Paradigma MANET klasik mendukung arsitektur datar dengan semua node seluler bekerja sama dengan fungsi yang sama untuk membangun jaringan nirkabel mandiri dan terdistribusi penuh. Di sisi lain, perangkat jaringan yang berpartisipasi dalam WMN diatur secara hierarkis dalam hal fungsionalitas internetworking dan kemampuan perangkat keras [2].

Secara kasar, perangkat jaringan yang menyusun WMN terdiri dari tiga jenis: router mesh (MR), titik akses mesh (MAP), dan klien mesh (MC). Fungsionalitas MR dan MAP ada dua: Mereka bertindak sebagai titik akses klasik ke MC, sedangkan mereka memiliki kemampuan untuk mengatur sistem distribusi nirkabel (WDS) dengan menghubungkan satu sama lain melalui tautan nirkabel titik ke titik. Baik MR dan MAP seringkali merupakan perangkat tetap dan bertenaga listrik. Selain itu, MAP dilengkapi dengan semacam konektivitas kabel broadband (seperti ADSL atau fiber) dan bertindak sebagai gateway menuju backbone kabel. MC mungkin merupakan node ad hoc MANET klasik yang dapat memperluas konektivitas yang disediakan oleh WDS melalui tautan ad hoc.

Keberhasilan arsitektur WMN baru-baru ini terutama disebabkan oleh fleksibilitas dan kelayakan biayanya. Bahkan, berbeda dari paradigma jaringan akses nirkabel di mana semua titik akses nirkabel terhubung langsung ke backbone kabel, di WMN MAP bertindak seperti gateway dengan ranah kabel; akibatnya jumlah MAP yang berpotensi rendah dapat memberikan konektivitas ke jumlah MC yang berpotensi tinggi [3].

Fleksibilitas yang disebutkan di atas dalam arsitektur jaringan membuat WMN sangat cocok untuk mendukung spektrum aplikasi yang luas mulai dari layanan Sistem Transportasi Cerdas untuk manajemen lalu lintas kendaraan hingga jaringan kota untuk tujuan pengawasan keamanan dan wilayah (koordinasi pemadam kebakaran dan patroli polisi).

Akhirnya, teknologi jaringan nirkabel dapat mewakili alternatif yang kompetitif untuk solusi kabel untuk penyediaan akses pita lebar yang murah dan andal ke lingkungan kota (referensi 2 dan 4 memberikan ikhtisar aplikasi WMN yang agak lengkap).

WMN sedang dipertimbangkan dalam beberapa teknologi nirkabel. Ini termasuk IEEE

802.11 WLAN, yang mungkin merupakan teknologi paling populer untuk WMN yang telah diadopsi secara luas untuk jaringan nirkabel kota, jaringan akses nirkabel bekerja di daerah pedesaan, dan bahkan jaringan komunitas nirkabel [4]. Arsitektur mesh berdasarkan base station relai juga telah dipertimbangkan untuk IEEE 802.16 Wireless Metropolitan Area Networks (WMAN) di mana tulang punggung nirkabel sangat penting untuk merancang jaringan hemat biaya [5]. WMNs juga dianggap

sebagai solusi yang cocok untuk backhaul sistem seluler generasi berikutnya berdasarkan LTE (long-term evolution) [6]. Selain teknologi standar, beberapa perusahaan mengusulkan solusi berpemilik yang menyediakan teknologi mesh nirkabel siap pakai untuk dibangun jaringan komoditas umum [7-9]. Perlu disebutkan bahwa juga teknologi radio jarak pendek

seperti IEEE 802.15.4 menggunakan topologi mesh; namun, mereka memiliki arsitektur datar dan tidak sesuai dengan definisi WMN yang kami gunakan di sini.

Dalam semua kasus yang disebutkan, WMN menggantikan sebagian jaringan backbone kabel dan harus dapat menyediakan layanan serupa dan jaminan kualitas. Jaringan tulang punggung biasanya dirancang untuk menyediakan penugasan sumber daya yang hampir statis untuk arus lalu lintas antara stasiun basis dan gateway jaringan. Pendekatan ini memungkinkan untuk menyederhanakan manajemen sumber daya radio pada antarmuka antara jaringan dan pengguna seluler dan untuk memberikan jaminan kualitas layanan.

Oleh karena itu, metodologi rekayasa lalu lintas untuk memberikan jaminan bandwidth pada arus lalu lintas dan untuk mengoptimalkan pemanfaatan sumber daya transmisi tampaknya menjadi elemen kunci dalam skenario ini. Skema akses berganda tingkat lanjut berdasarkan pembagian waktu, mekanisme kontrol daya, dan modulasi adaptif dan teknik pengkodean adalah alat yang paling tepat untuk menentukan algoritme manajemen sumber daya radio yang mampu mencadangkan laju yang diperlukan untuk arus lalu lintas dan untuk mencapai efisiensi jaringan yang tinggi. Alat ini sudah tersedia untuk jaringan IEEE 802.16 dan LTE. Juga untuk WMN berdasarkan standar IEEE 802.11, beberapa produsen menyediakan solusi yang dapat meniru kerangka pembagian waktu di atas mekanisme akses media dasar yang disediakan oleh platform perangkat keras [10].

Selain itu, karena aturan manajemen spektrum dan pembatasan teknologi nirkabel, penggunaan banyak antarmuka radio di setiap node dianggap sebagai solusi umum di WMN. Standar teknologi nirkabel menyediakan satu set saluran yang tidak tumpang tindih yang dapat disesuaikan dengan antarmuka nirkabel. Beberapa saluran ortogonal memungkinkan pemanfaatan penuh media nirkabel melalui komunikasi simultan yang tidak mengganggu pada saluran yang berbeda. Jelas, dua antarmuka dapat berkomunikasi hanya jika disetel pada saluran yang sama; ini membutuhkan penetapan saluran yang hati-hati untuk meningkatkan kapasitas global tanpa memutus jaringan. Node mesh nirkabel dengan beberapa antarmuka radio cenderung digunakan dengan antena direktif yang dapat statis atau berdasarkan susunan adaptif, untuk meningkatkan transmisi dan membatasi efek interferensi.

Untuk alasan ini, teknik pengoptimalan sumber daya radio dari skenario mesh berdasarkan algoritma terpusat dan terdistribusi adalah elemen penting. Ini termasuk penjadwalan transmisi paralel, kontrol daya, adaptasi laju, penetapan saluran, dan perutean.

Dalam bab ini kami menyajikan model optimisasi utama yang telah dipertimbangkan untuk pengelolaan WMN berbasis TDMA yang efisien. Model-model ini telah menarik cukup banyak perhatian dari komunitas riset tidak hanya karena dampak praktisnya pada WMN tetapi juga karena mereka telah merenovasi minat dalam analisis masalah dasar jaringan nirkabel yang dapat memberikan hasil kapasitas dalam topologi jaringan arbitrer.

Pada Bagian 7.2 kami meninjau model jaringan dan interferensi yang biasa diadopsi.

Pada bab ini kita fokus pada model interferensi fisik berdasarkan rasio signal-to-interference- and-noise. Pada Bagian 7.3 kita membahas masalah link activation, yang bertujuan untuk memaksimalkan jumlah transmisi paralel di bawah batasan interferensi. Masalah penjadwalan link yang optimal

dibahas dalam Bagian 7.4, di mana juga ditunjukkan bagaimana kontrol daya dan adaptasi laju dapat diperhitungkan.

Bagian 7.5 memperkenalkan perutean dan membahas bagaimana hal itu dapat dioptimalkan bersama dengan penjadwalan. Kami menunjukkan cara menangani penetapan saluran dan antena pengarah di Bagian 7.6. Akhirnya, dalam Bagian 7.7 kita membahas relaying kooperatif dan menunjukkan bagaimana model optimasi sumber daya dapat digeneralisasikan untuk memasukkan teknik transmisi ini. Beberapa kata penutup diberikan di Bagian 7.8.

7.2 JARINGAN DAN MODEL GANGGUAN

Dalam bab ini kami mewakili jaringan nirkabel dengan grafik terarah G = (N, A), di mana kumpulan node mewakili perangkat jaringan, dan setiap elemen dalam A mewakili tautan transmisi dua arah. Daya transmisi setiap node i ÿ N dilambangkan dengan Pi, dan daya

noise dengan ÿ. Gain saluran antara pasangan node i dan j dari G adalah gij = dimana dij adalah jarak Euclidean antara p1 as,angan node, dan ÿ adalah koefisien path loss.

Pada link (i, j) ÿ A, i adalah pemancar dan j adalah penerima. Kami berasumsi bahwa node beroperasi dalam mode half-duplex, sehingga mereka dapat terlibat dalam paling banyak satu komunikasi pada satu waktu, baik sebagai pemancar atau penerima. Kami menggunakan model ini

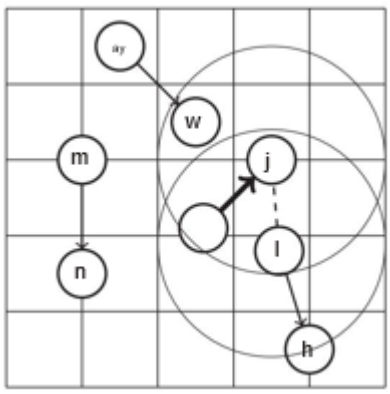
juga untuk kasus perangkat multiradio yang beroperasi pada beberapa saluran ortogonal, hanya

dengan asumsi bahwa antarmuka radio dapat beroperasi secara independen pada saluran berbeda yang berfungsi sebagai penerima atau pemancar.

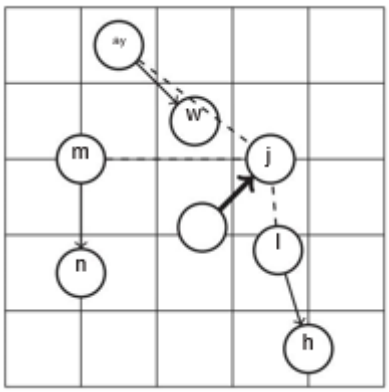
Setiap saat, pemancar dapat mengirimkan informasi, asalkan batasan interferensi pada penerima dipenuhi. Pada dasarnya ada dua model interferensi yang telah dipertimbangkan dalam literatur: model protokol dan model fisik, masing-masing dicontohkan pada Gambar

7.1 dan 7.2.

Model interferensi yang paling sederhana, model protokol, menganggap beberapa transmisi melalui tautan (i, j) dan (l, h) saling mengganggu jika dan hanya jika jarak Euclidian dari i ke h atau dari l ke j adalah kurang dari nilai yang diberikan, didefinisikan sebagai rentang interferensi. Efek dari interferensi dianggap boolean: Node mengganggu hanya jika mereka berada dalam kisaran interferensi timbal balik, yaitu penerima



Gambar 7.1 Model interferensi protokol.



Gambar 7.2 Model interferensi fisik.

dapat mendekodekan transmisi dengan benar jika tidak ada pemancar aktif yang berada dalam jangkauan gangguannya. Namun, model ini tidak memperhitungkan jumlah dari beberapa sinyal "jauh" yang, setelah diringkas, menyebabkan noise yang signifikan.

Dalam model fisik, sebagai gantinya, diberikan (i, j) ÿ A, node i mentransmisikan dengan benar ke node j jika dan hanya jika interferensi pada penerima j di bawah ambang batas yang diberikan. Dengan menggunakan model fisik interferensi, kita memiliki rasio signal-to-interference- noise (SINR) pada penerima j adalah di mana I adalah himpunan pengirim aktif dan ÿ adalah ambang terkecil agar transmisi berhasil. Jumlah pada penyebut memungkinkan untuk menghitung semua interferensi yang

diuji oleh penerima.

Perhatikan bahwa untuk memiliki link antara pasangan node i dan j, batasan SINR harus dipenuhi ketika node i adalah satu-satunya pengirim dalam jaringan, yaitu I \ {i}=ÿ. Memang, setiap busur (i, j) ÿ A harus memenuhi setidaknya rasio signal-to-noise:

7.3 AKTIVASI LINK MAKSIMUM DI BAWAH MODEL SINR

Masalah mendasar adalah menentukan jumlah maksimum transmisi paralel bebas interferensi, yang berkorelasi dengan throughput maksimum yang dapat didukung jaringan.

Dengan menggunakan model protokol, dimungkinkan untuk mendefinisikan grafik konflik H di mana ada simpul untuk setiap tautan dalam topologi jaringan asli G, dan ada tepi antara setiap pasangan tautan yang mengganggu. Dalam hal ini, masalah aktivasi tautan maksimum setara dengan menemukan Set Verteks Independen Maksimum, yang merupakan masalah NP-hard yang sangat sulit [11].

Masalah Aktivasi Tautan Maksimum telah terbukti menjadi NP-hard dengan node terdistribusi dalam ruang Euclidean bahkan di bawah kekuatan node yang seragam [12], bahkan jika back ground noise diabaikan [13]. Algoritma pendekatan dengan rasio bergantung pada jumlah koneksi [14], atau pada karakteristik geometris [12,13] tersedia.

Algoritma dengan jaminan pendekatan konstan telah diusulkan [15] di bawah asumsi daya seragam. Algoritma pendekatan faktor konstan untuk kasus umum daya variabel juga telah dikembangkan [16].

Sebuah metode yang efisien untuk menemukan optimum global, berdasarkan representasi kendala SINR alternatif dan lebih efektif, telah diusulkan di [17].

Masalah Aktivasi Tautan Maksimum adalah komponen dasar dari masalah manajemen sumber daya yang disajikan di bagian berikut.

7.4 PENJADWALAN LINK YANG OPTIMAL

Dalam sebagian besar skenario aplikasi jaringan mesh nirkabel, hanya sebagian kecil dari tautan dalam jaringan yang dapat diaktifkan secara bersamaan. Untuk memfasilitasi pengaktifan semua tautan, menjadi perlu untuk mengortogonalkan transmisi sepanjang beberapa dimensi kebebasan, seperti frekuensi dan waktu. Pada bagian ini, kami mempertimbangkan tugas

pengorganisasian aktivasi tautan secara optimal menggunakan skema time division multiple access (TDMA). Unit sumber daya dalam waktu disebut slot waktu. Slot waktu dapat digunakan untuk aktivasi beberapa tautan, asalkan mereka membentuk solusi yang layak untuk masalah aktivasi tautan. Dalam pengaturan dasar masalah penjadwalan, masing-masing tautan aktif dari slot waktu dapat mengirimkan satu paket. Secara intuitif, untuk masalah aktivasi tautan, solusinya cenderung terdiri dari tautan yang dipisahkan secara spasial, karena mereka menghasilkan sedikit interferensi satu sama lain. Dengan demikian skema akses yang kami pertimbangkan dapat dilihat sebagai penggunaan kembali sumber daya waktu secara spasial. Untuk alasan ini, skema ini juga disebut sebagai TDMA spasial, atau STDMA [18]. Meskipun kami akan fokus pada optimasi komputasi STDMA, perlu dicatat bahwa wilayah kapasitas STDMA telah dipelajari secara ekstensif juga dari perspektif teoretis informasi (lihat, misalnya, referensi 19).

Untuk mengkarakterisasi optimalitas dalam penjadwalan, metrik kinerja perlu didefinisikan. Target kinerja intuitif adalah minimalisasi jumlah slot waktu jadwal, tunduk pada batasan bahwa jadwal memenuhi jumlah lalu lintas yang akan dikirimkan pada setiap tautan. Jika tidak ada informasi lalu lintas pada tautan yang diberikan (yaitu, keputusan lapisan MAC selesai dipisahkan dari lapisan atas), batasannya adalah bahwa setiap tautan muncul setidaknya sekali dalam jadwal. Dalam hal ini, panjang jadwal secara efektif merepresentasikan tingkat efisiensi dalam penggunaan kembali sumber daya. Semakin pendek panjang jadwal, semakin tinggi efisiensinya. Selain itu, perlu diperhatikan bahwa, ketika penjadwalan digabungkan dengan perutean paket (lihat bagian selanjutnya), yang menentukan jumlah lalu lintas pada tautan, panjang jadwal sebenarnya menunjukkan penundaan ujung ke ujung secara keseluruhan.

Untuk alasan ini, kami akan fokus pada penjadwalan durasi minimum.

Perhatikan bahwa, dengan menggunakan panjang sebagai target performa, penjadwalan berkaitan dengan pengelompokan link ke dalam subset, satu per slot waktu. Urutan munculnya slot waktu dalam jadwal tidak penting.

Studi kinerja penjadwalan tautan dimulai sejak pengenalan jaringan radio paket multi-hop.

Kami mengacu pada referensi 20-23 untuk pengembangan awal heuristik, komputasi terdistribusi, dan algoritma aproksimasi. Pengaturan masalah terkait adalah mengalokasikan slot waktu ke node untuk komunikasi siaran [24-26].

Dalam beberapa referensi, pertimbangan SINR telah disederhanakan menjadi model protokol;

yaitu, node yang memiliki pemisahan spasial tertentu (seperti dua hop dan lebih) dapat mengirimkan dalam slot waktu yang sama.

Pembahasan yang akan datang tentang penjadwalan tautan mengambil perspektif pemrograman matematis. Tujuannya adalah untuk memperoleh kinerja maksimum yang dapat dicapai dari STDMA dalam hal panjang jadwal [27-30]. Untuk tujuan ini, kami berasumsi bahwa tidak ada batasan eksplisit pada waktu komputasi, dan informasi matriks gain saluran tersedia. Bahkan dengan dua asumsi ini, memecahkan masalah penjadwalan tautan sulit — ini agak diharapkan, karena penjadwalan adalah generalisasi dari aktivasi tautan, karena ini mencakup aktivasi tautan sebagai submasalah.

7.4.1 Formulasi Optimasi

Biarkan Rij menunjukkan jumlah lalu lintas, dalam jumlah paket, yang akan dikirim melalui tautan (i, j) ÿ A. Pertama-tama, kita memeriksa perpanjangan langsung dari aktivasi tautan Fungsi tujuan (7.7a) meminimalkan penggunaan slot waktu. Pada (7.7b), tautan (i, j) harus

muncul setidaknya kali Rij dalam jadwal. Kendala (7.7c) menghubungkan dua set variabel: Variabel yt harus satu (yakni slot t digunakan), jika ada link (i,j) yang aktif di slot. Kendala yang tersisa mirip dengan yang ada di (7.3) dan memperluas yang terakhir ke banyak slot waktu menggunakan indeks t. Kendala SINR (7.7e) dapat dilinearisasi dengan cara yang ditunjukkan pada (7.4).

Formulasi (7.7) padat: Baik jumlah variabel maupun kendala bersifat polinomial dalam ukuran jaringan. Kelemahan utama dari (7.7), selain penggunaan big-M untuk linierisasi (7.7e), adalah adanya apa yang disebut sebagai simetri dalam pemrograman bilangan bulat [31]. Pertimbangkan solusi penjadwalan apa pun yang menggunakan slot waktu t1.

Biarkan t2 menjadi slot waktu lainnya, baik ada atau tidak ada dalam solusi. Menukar nilai variabel t1 dan t2 memberikan solusi yang setara dengan yang asli dalam hal panjang jadwal. Oleh karena itu, formulasi (7.7) mengandung sejumlah besar solusi yang tampaknya berbeda tetapi pada kenyataannya kinerjanya setara. Dampak simetri pada perhitungan sangat besar; dalam praktiknya, penyelesaian (7.7) hingga optimal hanya dapat dilakukan untuk jaringan dengan sejumlah kecil tautan.

Pembahasan simetri di atas juga memberikan petunjuk untuk mengatasinya. Karena menukar isi slot waktu tidak berpengaruh pada kualitas jadwal, kami tidak tertarik pada indeks slot waktu yang digunakan, tetapi isinya. Setiap slot waktu dalam jadwal berisi subkumpulan tautan yang akan diaktifkan secara bersamaan.

Untuk selanjutnya, kami mengacu pada subkumpulan tautan seperti itu — yaitu, solusi untuk masalah aktivasi tautan (7.3) —sebagai kumpulan yang kompatibel, atau konfigurasi. Sedangkan yang pertama intuitif untuk masalah penjadwalan yang sedang dipertimbangkan, yang terakhir lebih akurat ketika kita memperluas penjadwalan untuk menilai adaptasi.

Misalkan, untuk sesaat, kita memiliki akses ke seluruh himpunan S yang berisi semua himpunan yang kompatibel. Subset dari link membentuk elemen s ÿ S jika dan hanya jika memenuhi batasan (7.3b)–(7.3d). Kemudian, jadwalkan jumlah untuk memilih elemen dari S, dan tentukan berapa banyak setiap elemen yang dipilih harus digunakan. Menjelang akhir ini, kami mengaitkan variabel integer ÿs, s ÿ S, yang menunjukkan berapa kali himpunan kompatibel s digunakan dalam jadwal, atau, ekuivalen, jumlah slot waktu yang dialokasikan ke himpunan kompatibel s. Untuk menyatakan

isi dari s, kita mendefinisikan parameter aijs, yaitu satu jika link (i, j) aktif pada set s yang kompatibel, dan nol jika sebaliknya. Masalah penjadwalan dapat diformulasikan sebagai program integer berikut.

Fungsi tujuan (7.8a) mewakili jumlah slot waktu yang ditetapkan untuk keseluruhan penggunaan set yang kompatibel. Kendala (7.8b) memastikan bahwa, untuk setiap link (i,j), set kompatibel yang berisi link bersama-sama harus memiliki setidaknya slot waktu Rij dalam jadwal.

Alih-alih menggunakan parameter aijs, seseorang dapat mendefinisikan himpunan Sij ÿ S untuk menunjukkan subhimpunan himpunan yang kompatibel yang berisi tautan (i, j). Dengan notasi

dalamhifmorpmuunlasiinsÿi,Skiej nddi atlas(7a.d8abl)amh ebnajhawdiaÿpsaÿraRmije, tÿe(ri,tje)rÿseAb.uAt ldaasapnatpdeiinngtegrupnraeatansipkaarnamseebteargaiijs jumlah paket (nol atau satu dalam masalah penjadwalan dasar) yang ditransmisikan oleh tautan (i,

j) jika satu slot waktu ditetapkan ke set s; interpretasi ini berguna nanti dalam diskusi tentang penyesuaian tarif.

7.4.2 Pembangkitan Kolom

Formulasi (7.8) memiliki kendala yang jauh lebih sedikit daripada (7.7). Juga, perumusan tidak memodelkan persyaratan SINR (yang “tersembunyi” dalam konstruksi perangkat yang kompatibel). Sebaliknya, set S berisi semua set yang kompatibel; dengan demikian jumlah variabel, atau kolom jika (7.8b) ditulis dalam bentuk matriks, umumnya eksponensial dalam ukuran jaringan. Untuk alasan ini, pendekatan solusi praktis harus membuat batasan pada set yang kompatibel untuk dipertimbangkan. Lebih disukai, perangkat yang kompatibel yang dimasukkan ke dalam formulasi terbatas kemungkinan adalah perangkat yang digunakan dalam jadwal yang optimal.

Untuk tujuan ini, cara yang sistematis adalah dengan menerapkan metode pembangkitan kolom ke relaksasi pemrograman linier (LP) dari (7.8). Dalam LP, pembangkitan kolom berlaku jika jumlah variabel banyak secara eksponensial; karenanya sebagian besar kolom dalam matriks kendala tidak tersedia secara eksplisit, tetapi struktur masalahnya memungkinkan konstruksi kolom baru dan menjanjikan untuk dimasukkan dalam matriks kendala [32].

Masalah terbatas, di mana sebagian kecil dari semua kolom yang mungkin disimpan, adalah disebut sebagai masalah utama. Dengan konstruksi, masalah utama yang optimal mewakili solusi yang layak tetapi belum tentu optimal untuk masalah asli dengan set variabel lengkap. Pembuatan kolom menggunakan kondisi optimalitas klasik dari metode simpleks, yaitu pengurangan biaya

semua variabel harus nonnegatif untuk minimalisasi (dan nonpositif untuk maksimalisasi). Menghitung pengurangan biaya sangat mudah dalam metode simpleks klasik. Sebaliknya, dalam pembangkitan kolom, perhitungan variabel yang memiliki pengurangan biaya terkecil (dengan asumsi minimisasi) dilakukan melalui pemecahan masalah optimisasi bantu lainnya, yang dikenal sebagai subproblem.

Submasalah diformulasikan sedemikian rupa sehingga ruang solusinya sesuai dengan kumpulan kolom lengkap (dalam kasus kita, kumpulan yang kompatibel) dalam masalah asli yang tidak dibatasi.

Dari solusi submasalah, seseorang dapat memperoleh kolom baru dengan pengurangan biaya

yang menguntungkan untuk menambah masalah utama, atau menyimpulkan tidak ada kolom seperti itu.

Metode pembangkitan kolom berganti-ganti antara masalah master dan sub masalah, sampai kondisi optimal terpenuhi. Biasanya, dibandingkan dengan kumpulan kolom lengkap, hanya sebagian kecil yang akan dihasilkan sebelum optimalitas tercapai.

Menerapkan pembuatan kolom untuk penjadwalan link, masalah utama didefinisikan oleh (7.8) dengan dua modifikasi. Pertama, variabelnya kontinu, yaitu, ÿs ÿ R+, s ÿ S. Kedua, alih-alih seluruh himpunan S, subset kecil S ÿ S digunakan dan ditambah secara berurutan. Setiap S ÿ S yang mengakui kelayakan masalah utama dapat berfungsi sebagai titik awal. Pilihan paling sederhana adalah memulai dengan S = A; yaitu, set yang kompatibel dengan tautan tunggal yang sesuai dengan penjadwalan TDMA murni. Untuk submasalah, jelas dari pembahasan di atas bahwa kendalanya persis seperti yang ada di masalah aktivasi tautan (7.3). Fungsi tujuan dari model subproblem mengurangi biaya set yang kompatibel. Dengan teori LP, untuk s ÿ S, pengurangan biaya ÿs dalam (7.8) memiliki bentuk sebagai berikut, di mana ÿij ÿ 0 menunjukkan variabel ganda yang terkait dengan (7.8b).

Nilai variabel ganda berasal dari masalah master yang optimal atas himpunan terbatas S . Jadi, dalam submasalah, kita mencari himpunan s yang cocok, yang diwakili oleh variabel x pada (7.7), yang meminimalkan pengurangan biaya atau setara, memaksimalkan penjumlahan pada (7.9).

Dalam penjumlahan ini, link (i, j) diasosiasikan dengan nilai ÿij atau nol, tergantung aktif atau tidaknya link tersebut. Dengan demikian kita sampai pada formulasi subproblem berikut. Formulasi (7.10) adalah aktivasi tautan dengan fungsi tujuan berbobot. Dengan desainnya, pembangkitan kolom memecahkan serangkaian masalah aktivasi tautan; ini jauh lebih efisien daripada membuat konten dari banyak set yang kompatibel sekaligus; lihat formulasi (7.7). Dengan bergantian antara memecahkan masalah utama dan subproblem, metode menguraikan tugas penjadwalan menjadi membangun set yang kompatibel dan mengoptimalkan penggunaannya.

Setelah terminasi, LP optimal dari (7.8) mungkin fraksional. Dalam hal ini, nilai fungsi tujuan membatasi bilangan bulat optimal dari bawah. Untuk mencapai solusi bilangan bulat dalam variabel ÿ, seseorang dapat menerapkan pemecah bilangan bulat linier ke (7.8) di atas himpunan himpunan kompatibel yang tersedia dalam iterasi terakhir dari pembuatan kolom, atau, jika ini membutuhkan waktu komputasi yang berlebihan, algoritma heuristik. Dalam kedua kasus tersebut, tidak ada jaminan optimalitas global, karena beberapa himpunan kompatibel dalam bilangan bulat optimum mungkin tidak ada dalam LP optimum.

Memastikan optimalitas global akan memerlukan teknik cabang-dan-harga pemrograman bilangan bulat [31]. Akan tetapi, secara empiris, untuk masalah penjadwalan, pembulatan LP optimum mengarah ke solusi optimum global, atau hampir optimal, yang bersama-sama dengan nilai LP membentuk interval yang sangat rapat membatasi optimum [27-29].

7.4.3 Perluasan untuk Kontrol Daya dan Adaptasi Laju

Setelah memeriksa model dasar penjadwalan tautan, mari kita pertimbangkan untuk memperluas pengaturan masalah ke kontrol daya dan adaptasi laju. Karena kontrol daya memperbesar ruang set yang kompatibel, ini berpotensi mengurangi jumlah slot waktu dalam jadwal yang optimal. Ketika pemilihan tingkat diaktifkan, pemilihan dapat dikombinasikan dengan tingkat daya, menggunakan pendekatan desain lintas lapisan, untuk mencapai peningkatan kinerja tambahan [33-35]. Perpanjangan lebih lanjut adalah untuk memasukkan end-to-end routing, yang akan diperiksa pada bagian berikutnya. Pertimbangkan formulasi (7.8). Kontrol daya tidak berdampak pada definisi variabel atau kendala, hanya karena konstruksi himpunan yang kompatibel bukan bagian dari formulasi. Metode pembuatan kolom tetap berlaku. Sub masalah, bagaimanapun, harus dimodifikasi untuk memasukkan kontrol daya, yaitu, untuk menggunakan batasan dari masalah aktivasi tautan daya variabel (7.5b)–(7.5f) di Bagian 7.3.

Selanjutnya, kami mengambil langkah lebih lanjut dari perluasan masalah dengan memasukkan penyesuaian tarif. Aspek tersebut berasal dari penggunaan beberapa modulasi dan skema pengkodean (MCS). Setiap MCS sesuai dengan tarif dan ambang SINR untuk tarif tersebut. Biarkan W menunjukkan himpunan MCS. Untuk setiap w ÿ W, kami menggunakan Tw untuk menunjukkan jumlah paket yang didukung oleh

tarif dalam slot waktu, dan kami menggunakan ÿw untuk menunjukkan ambang SINR. Perhatikan bahwa, dengan adaptasi laju, informasi yang menentukan slot waktu tidak hanya terdiri dari tautan yang aktif, tetapi juga tarifnya dalam hal jumlah paket. Karena alasan ini, akan lebih mudah menyebut konten slot waktu sebagai konfigurasi daripada set yang kompatibel.

Untuk formulasi (7.7), memasukkan jumlah adaptasi laju untuk memperluas definisi variable x.

7.5 ROUTING DAN PENJADWALAN BERSAMA

Dalam masalah penjadwalan link yang disajikan pada bagian sebelumnya, lalu lintas pada setiap link diasumsikan diberikan. Namun, dalam praktiknya, beban tautan ditentukan oleh jalur perutean. Perutean permintaan lalu lintas dalam jaringan adalah parameter lain yang dapat kita sesuaikan untuk mengoptimalkan kinerja: perutean menentukan pengiriman node dan jumlah paket yang dikirim oleh masing-masing node ini. Mentransmisikan node dan jumlah transmisinya, pada gilirannya, memengaruhi interferensi global. Oleh karena itu, penjadwalan yang optimal dipengaruhi oleh keputusan routing, dan ketergantungan ini membuat routing bersama dan optimalisasi penjadwalan langkah lebih lanjut menuju peningkatan kinerja jaringan.

Pada bagian ini, kami mempertimbangkan, selain penjadwalan tautan, masalah pengoptimalan perutean sekumpulan permintaan lalu lintas, masing-masing memiliki simpul sumber dan simpul tujuan. Sebagian besar protokol routing umum didasarkan pada jalur terpendek. Jalur terpendek adalah asumsi perutean yang dibuat demi kesederhanaan, bagaimanapun, itu mungkin tidak menghasilkan kinerja terbaik karena kendala yang dikenakan, tetapi tidak selalu diperlukan, untuk memilih hanya jalur terpendek. Dalam banyak kasus, itu bahkan dapat menghasilkan tautan kemacetan yang berat. Untuk mendapatkan pencapaian optimal yang nyata, penyederhanaan jalur terpendek harus dihilangkan dan pendekatan optimisasi harus mengasumsikan perspektif global.

Memanfaatkan perutean dan aktivasi tautan, tujuannya adalah untuk menyediakan bingkai terpendek yang memungkinkan pengiriman jumlah paket yang diperlukan dari node sumber ke tujuan. Perhatikan bahwa urutan slot tidak penting karena kami tidak peduli dengan batas buffering. Memang, tidak diperlukan bahwa paket tertentu ditransfer dari sumber ke tujuan dalam bingkai yang sama, melainkan, paket d dari aliran tertentu dikirim oleh pemancar dan diterima oleh tujuan dalam bingkai. Ini berarti bahwa paket yang diterima dapat ditransmisikan pada frame sebelumnya dan dikirimkan sepanjang jalur seperti pipa. Contoh sederhana ditunjukkan pada Gambar 7.3, di mana permintaan adalah satu paket dari node A ke node B dalam sebuah frame. Bahkan jika aktivasi tautan rusak, setelah keadaan transien yang dapat diabaikan, penjadwalan memenuhi permintaan satu paket yang dikirimkan per frame.

Karena setiap slot dari frame masih harus merupakan konfigurasi yang layak, pendekatan dari bagian sebelumnya dapat dengan mudah diadaptasi ke routing bersama dan optimasi penjadwalan, berkat pemisahan yang disediakan oleh algoritma pembangkitan kolom.

Kendala teknologi yang menentukan kumpulan tautan aktif secara bersamaan tidak berubah, oleh karena itu submasalah yang menghasilkan kumpulan yang kompatibel tetap sama. Masalah utama

yang mengoptimalkan penggunaan set yang kompatibel tersebut, sebagai gantinya, harus dimodifikasi untuk memperhitungkan masalah perutean tambahan. Sebuah pendekatan yang berhubungan dengan routing dan penjadwalan bersama mengadopsi strategi ini disajikan dalam referensi 36. Berbagai pendekatan lain untuk masalah ini disajikan dalam referensi 37-41. Gambar 7.3 Contoh penjadwalan out-of-order.

7.5.1 Perutean melalui Konservasi Aliran

Biarkan permintaan lalu lintas diwakili oleh satu set triplet D = {o, t, d | o, t ÿ N, d ÿ Z+}, dimana setiap triplet o, t, d menunjukkan jumlah paket d yang akan dirutekan dari node o ke node t. Untuk merumuskan masalah perutean, kita perlu memasukkan k variabel aliran tambahan ke masalah utama (7.8a)–(7.8c). Misalkan f adalah variabel aliran ij yang dirutekan melalui link (i,j) untuk permintaan lalu lintas ke-k Fungsi tujuan (7.14a) meminimalkan jumlah slot waktu. Kendala (7.14b) adalah kendala routing yang memaksakan keseimbangan aliran pada setiap simpul i, untuk setiap permintaan k.

Kendala (7.14c) menetapkan bahwa setiap tautan (i, j) ditugaskan ke sejumlah slot waktu setidaknya sama dengan berapa kali tautan digunakan untuk merutekan permintaan apa pun, sementara (7.14d) dan (7.14e) adalah integral kendala.

Perhatikan bahwa himpunan konfigurasi S sama seperti yang didefinisikan dalam Bagian 7.4.1.

Oleh karena itu, selama kita menangani masalah ini melalui pendekatan pembangkitan kolom seperti yang digunakan untuk masalah penjadwalan tautan, kita dapat dengan mudah menangani masalah perutean dan penjadwalan bersama dengan daya tetap, daya variabel, dan adaptasi laju. Perbedaan utama ada pada solusi masalah utama.

7.5.2 Perutean melalui Pembuatan Jalur

Karena dalam masalah (7.14) jumlah variabel aliran dan kendala keseimbangan aliran mungkin menjadi signifikan, masalah routing dan penjadwalan bersama dapat diformulasikan dengan formulasi yang sedikit berbeda yang menggunakan variabel jalur daripada variabel aliran penghubung. Formulasi ini awalnya diusulkan dan dievaluasi dalam referensi 42.

Misalkan H adalah himpunan semua jalur yang mungkin antara setiap pasangan node di G. Idenya adalah untuk memperkenalkan variabel integer jalur ÿp untuk setiap jalur p ÿ H yang menunjukkan jumlah paket yang dirutekan pada jalur p. Misalkan Hij adalah himpunan bagian dari jalur yang melalui

link (i,j) dan misalkan Ho,t adalah himpunan bagian dari jalur yang dimulai dari simpul o dan berakhir ke simpul t.

Maka masalah utama dapat dirumuskan kembali sebagai Kendala (7.15b) memastikan bahwa untuk setiap permintaan setidaknya d jalur dari sumber o ke tujuan t dipilih. Batasan (7.15c) memastikan bahwa ada cukup konfigurasi sesuai dengan jumlah jalur yang digunakan untuk merutekan permintaan lalu lintas.

Perhatikan bahwa jumlah jalur di H adalah eksponensial, tapi kita bisa mulai dengan rangkaian awal jalur dan kemudian kita bisa menggunakan submasalah penetapan harga tambahan untuk menghasilkan hanya jalur yang menarik—yaitu, jalur pengurangan biaya negatif. Masalah menghasilkan jalur biaya tereduksi negatif dapat dirumuskan sebagai masalah jalur terpendek, di mana biaya busur diberikan oleh pengali ganda yang terkait dengan (7.15c). Masalah jalur terpendek harus

diselesaikan untuk setiap permintaan, dengan biaya tetap tambahan yang diberikan oleh pengali kendala ganda (7.15b). Selama satu jalur pengurangan biaya negatif ada, algoritme pembuatan kolom akan berulang. Detail teknis tambahan tentang cara mengatasi masalah perutean dengan penetapan harga jalur dan konfigurasi subproblem dapat ditemukan pada referensi 42, dimana penulis telah mengaplikasikan ide ini pada masalah joint routing dan penjadwalan pada jaringan wireless mesh dengan model interferensi protokol.

7.6 MENGHADAPI TUGAS SALURAN DAN ANTENA DIRECTIONAL

Seperti yang jelas muncul dari bagian sebelumnya, penggunaan kembali sumber daya waktu secara spasial merupakan aspek penting untuk kinerja WMN. Secara kasar, semakin banyak konfigurasi tautan aktif , semakin baik throughput yang dapat dicapai sistem.

Hambatan utama yang mencegah aktivasi simultan banyak link dalam model SINR adalah interferensi pada penerima yang disebabkan oleh transmisi konkuren lainnya. Lapisan fisik lanjutan dapat membantu mengurangi efek interferensi.

Selain menggunakan modulasi dan pengkodean yang kuat atau komponen berkualitas tinggi yang memungkinkan decoding transmisi pada SINR rendah, bantuan besar datang dari penggunaan sistem antena canggih.

Pengurangan lebih lanjut dari efek interferensi, menghasilkan peningkatan kinerja, dapat diperoleh dalam skenario multichannel multiradio. Dengan pengembangan peralatan nirkabel yang baru dan siap pakai, penggunaan beberapa antarmuka radio di setiap node sekarang dianggap sebagai solusi umum di WMN. Selain itu, standar teknologi nirkabel menyediakan spektrum RF dengan seperangkat saluran antarmuka nirkabel yang tidak tumpang tindih yang dapat disetel.

Beberapa saluran ortogonal memungkinkan pemanfaatan penuh media nirkabel melalui komunikasi simultan yang tidak mengganggu pada saluran yang berbeda.

Jelas, dua antarmuka dapat berkomunikasi hanya jika disetel pada saluran yang sama, ini memerlukan penetapan saluran yang hati-hati untuk meningkatkan kapasitas global tanpa memutus jaringan. Pengaruh beberapa antarmuka pada kapasitas jaringan di hadapan banyak saluran telah dianalisis secara teoritis [35], dan beberapa solusi dari masalah penetapan saluran telah diusulkan [43-48].

Berikut ini kami menyajikan pendekatan penugasan saluran yang dibangun di atas solusi yang diberikan oleh model baik di Bagian 7.4 atau di Bagian 7.5. Ini terintegrasi erat dengan pendekatan yang diadopsi sejauh ini dan dapat dilihat sebagai blok kerangka kerja modular yang disajikan.

7.6.1 Penetapan Saluran

Untuk memodelkan dan menyelesaikan masalah penetapan saluran, kami memanfaatkan fitur dari formulasi masalah yang diusulkan di bagian sebelumnya, yang didasarkan pada rangkaian transmisi simultan yang kompatibel, yang disebut konfigurasi. Pendekatan umum adalah menetapkan konfigurasi ke saluran yang tersedia, dengan mempertimbangkan batasan karena karakteristik perangkat [49].

Setiap node jaringan dilengkapi dengan sejumlah antarmuka nirkabel, dan masing-masing dapat disetel pada satu saluran yang dipilih dari sekumpulan saluran ortogonal.

Menurut karakteristik perangkat keras dan perangkat lunak dari node dan kartu nirkabel, dua strategi penetapan saluran dapat dipertimbangkan:

• Tugas Dinamis. Penetapan saluran ke antarmuka dapat diubah berdasarkan slot demi slot. Kami berasumsi di sini bahwa antarmuka nirkabel dapat beralih dengan sangat cepat dari satu saluran ke saluran lainnya dengan penundaan peralihan yang dapat

diabaikan. • Tugas Statis. Antarmuka nirkabel disetel secara statis pada saluran dan penetapan tidak dapat diubah untuk seluruh durasi bingkai.

Algoritma pengoptimalan perutean dan penjadwalan yang disajikan di bagian sebelumnya menghasilkan bingkai saluran tunggal di mana setiap konfigurasi yang diaktifkan ditugaskan ke slot untuk memenuhi permintaan lalu lintas. Mulai dari solusi ini, solusi bingkai multichannel dapat diperoleh dengan menetapkan saluran ke setiap konfigurasi yang diaktifkan.

Bahkan, konfigurasi sudah berisi kumpulan tautan aktif simultan yang layak di mana transmisi dapat dilakukan secara paralel pada saluran yang sama. Dengan menetapkan saluran yang berbeda dengan benar ke konfigurasi aktif dan kemudian konfigurasi ke slot dalam bingkai multichannel, jumlah total slot yang diperlukan dapat diminimalkan dan, pada saat yang sama, batasan SINR dipenuhi secara implisit.

Jelas, penugasan saluran tunduk pada beberapa kendala. Dalam slot waktu multisaluran, kami tidak dapat mengaktifkan sejumlah konfigurasi yang lebih besar dari jumlah saluran ortogonal yang tersedia. Selain itu, sebuah node tidak dapat aktif selama slot waktu di sejumlah saluran yang lebih besar dari jumlah antarmuka yang tersedia karena kartu nirkabel setengah dupleks. Akhirnya, dalam kasus penugasan statis kita perlu menambahkan kendala untuk memastikan bahwa saluran yang digunakan oleh setiap node tetap sama untuk seluruh durasi frame.

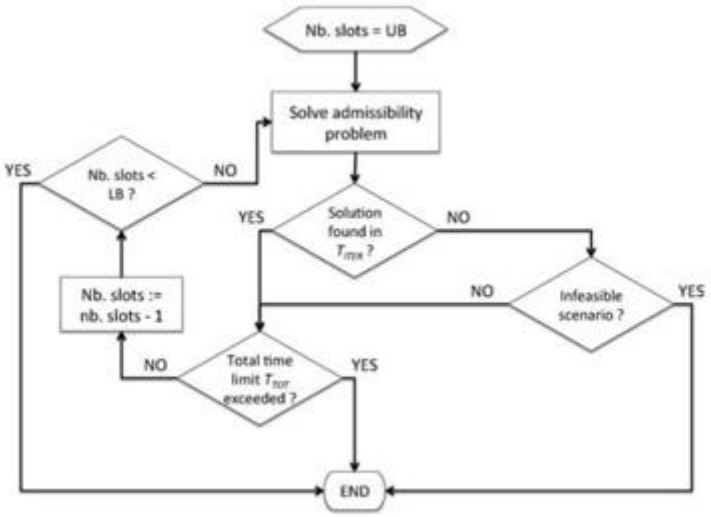
Untuk masalah penugasan saluran kami mengusulkan formulasi untuk kasus dinamis dan statis. Misalkan T adalah himpunan slot waktu multichannel, dan C adalah himpunan konfigurasi (solusi dari formulasi sebelumnya) yang akan dialokasikan ke dalam bingkai multichannel. Parameter masalah adalah sebagai berikut: I adalah jumlah maksimum antarmuka per-simpul, O adalah himpunan saluran ortogonal, dan aci sama dengan 1 jika simpul i muncul dalam konfigurasi c dan sama dengan 0 sebaliknya. Perhatikan bahwa node dapat muncul paling banyak sekali dalam konfigurasi karena kendala setengah dupleks. Perhatikan bahwa dalam formulasi di atas, saluran tidak secara eksplisit diidentifikasi. Kami hanya perlu memastikan bahwa jumlah saluran yang digunakan kompatibel dengan parameter masalah berkat kemampuan antarmuka nirkabel untuk berpindah dari satu saluran ke saluran lainnya. Kendala (7.16b) menjamin bahwa setiap konfigurasi ditetapkan ke slot.

Kendala (7.16c) dan (7.16d) masing-masing memaksa jumlah maksimum saluran ortogonal yang tersedia dan jumlah maksimum antarmuka per-node. Kendala (7.16e) mengatur aktivasi slot waktu multisaluran. Penugasan saluran yang layak selalu dapat diperoleh dengan menetapkan salah satu saluran yang tersedia untuk setiap konfigurasi dalam slot waktu multisaluran, karena kendala (7.16c) menjamin kebenaran proses.

Masalah penugasan statis adalah masalah yang lebih terbatas dan kompleks, dan saluran yang ditugaskan ke konfigurasi harus diidentifikasi secara eksplisit untuk memastikan bahwa penugasan saluran ke node tidak berubah dari slot ke slot. Untuk tujuan ini , set variabel biner baru harus

diperkenalkan, selain ts. Variabel b sama dengan 1 jika konfigurasi c ditugaskan ke slot s dengancs saluran f , rif dapat mengambil nilai 1 jika node i menggunakan saluran f . Masalah penugdasnavnari

statis dirumuskan sebagai di mana O adalah himpunan saluran ortogonal. Kendala (7.17b), (7.17d), (7.17f), dan (7.17g) memiliki ekuivalen masing-masing dalam masalah penugasan dinamis. Kami menambahkan kendala (7.17c), yang menyatakan bahwa di setiap slot waktu multichannel kami dapat menetapkan paling banyak satu konfigurasi per saluran dan kendala (7.17e) yang memungkinkan untuk menghitung jumlah saluran yang ditetapkan ke node dalam bingkai. Jumlah saluran yang ditetapkan sama dengan jumlah antarmuka yang akan dipasang.



Gambar 7.4 Algoritma heuristik penugasan saluran.

Algoritme heuristik dapat diimplementasikan menggunakan versi penerimaan dari masalah penugasan saluran. Kami fokus, tanpa kehilangan keumuman, pada statis sebagai formulasi penandaan di (7.17). Versi yang dapat diterima ini adalah masalah di mana fungsi tujuan (7.17a) dihapus bersama dengan kendala (7.17g) dan variabel ts , dan sejumlah slot waktu multichannel diperkenalkan. Tujuannya adalah untuk menemukan solusi layak yang secara tepat menggunakan jumlah slot waktu multisaluran yang diberikan dan memenuhi semua kendala. Jelas, kompleksitas versi ini tidak lebih besar dari versi pengoptimalan, dan biasanya berjalan dalam waktu singkat.

Bagan alir algoritme heuristik kami dilaporkan dalam Gambar 7.4, di mana batas atas jumlah slot waktu multichannel dari frame terakhir didefinisikan antarmuka, paling banyak |O| konfigurasi dapat ditugaskan ke slot.

Algoritme mulai menyelesaikan masalah penerimaan dengan sejumlah slot waktu multi saluran yang sama dengan UB dan, jika solusi yang layak ditemukan, angka ini dikurangi satu secara iteratif. Jika tidak, jika masalah dengan jumlah slot waktu tersebut tidak memungkinkan, eksekusi akan dihentikan. Artinya, selama iterasi sebelumnya diakhiri dengan solusi yang layak, jumlah slot waktunya juga optimal. Waktu eksekusi dari iterasi tunggal dan algoritma total masing-masing memiliki dua batas waktu, TITER dan TTOT untuk mendapatkan setidaknya satu solusi suboptimal dalam TTOT.

7.6.2 Antena Pengarah

Solusi teknologi berdasarkan antena directional untuk WMN telah dipelajari secara luas karena potensi peningkatan kinerja tinggi [50]. Keuntungan utama menggunakan antena directional dengan jaringan multihop nirkabel adalah berkurangnya gangguan dan kemungkinan memiliki transmisi paralel di antara tetangga dengan konsekuensi peningkatan penggunaan kembali sumber daya radio secara spasial.

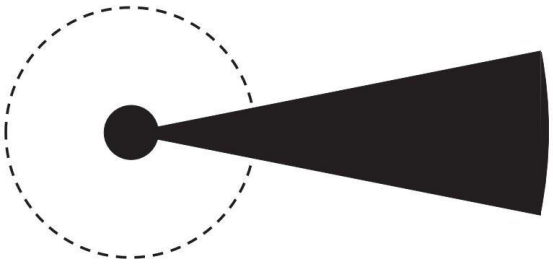
Antena directional memungkinkan konsentrasi energi yang ditransmisikan ke wilayah terbatas dan penerimaan yang lebih tinggi dari arah kedatangan tertentu. Akibatnya, pemancar dapat membatasi interferensi yang dihasilkan pada penerima yang tidak diharapkan dan, sama halnya, penerima dapat melemahkan daya interferensi yang berasal dari pemancar yang tidak diinginkan. Pengurangan interferensi memungkinkan penggunaan kembali saluran yang lebih tinggi sehubungan dengan antena omnidirectional, yang mengarah pada eksploitasi sumber daya yang lebih baik dan potensi kinerja yang lebih baik.

Pola radiasi antena mengungkapkan perolehan intensitas, sehubungan dengan antena om nidirectional, dari sinyal yang ditransmisikan atau diterima dari arah tertentu.

Dalam hal antena directional, biasanya dibentuk oleh lobus utama dengan gain maksimum dan beberapa lobus samping dengan gain lebih rendah. Pemodelan antena yang umum adalah dengan mempertimbangkan lobus radiasi utama sebagai sektor sudut yang memiliki lebar sama dengan derajat ÿ, sedangkan jangkauan omnidirectional di sekitar stasiun karena lobus samping direpresentasikan dengan lingkaran yang memiliki penguatan radiasi lebih rendah. Jika HH adalah penguatan radiasi lobus utama, penguatan lobus samping, HL, dapat diasumsikan paling tidak 10 dB lebih rendah [51]. Hal ini ditunjukkan pada Gambar 7.5. Lingkaran putus-putus mewakili cakupan segala arah di sekitar stasiun. Sektor melingkar mewakili lobus radiasi utama dengan perolehan transmisi/penerimaan maksimum. Lingkaran hitam menyumbang lobus samping dengan gain rendah; keuntungan side lobe pertama dapat diambil sebagai pilihan konservatif.

Karena topologi WMN adalah tetap, kami berasumsi bahwa setiap node mengetahui posisinya, serta tetangganya. Secara khusus, setiap perangkat dapat mengarahkan cuping utama antenanya ke arah tetangga penerima. Konsekuensinya, untuk menghitung gain saluran, kita hanya dapat mempertimbangkan set diskrit kemungkinan penunjukan antena di antara pasangan node [30].

Karena pola radiasi tidak seragam, maka perlu dibedakan antara tiga kasus berikut, tergantung pada penunjukan antena kedua simpul:



Gambar 7.5 Model radiasi antena directional.

7.7 JARINGAN KOPERASI

Garis penelitian baru-baru ini berkaitan dengan jaringan nirkabel multihop di mana perangkat bekerja sama untuk mengirimkan informasi yang sama [52]. Ini berbeda dari semua masalah yang disajikan sampai di sini, karena sebelumnya kami memiliki asumsi implisit bahwa transmisi melibatkan tepat satu pengirim dan satu penerima. Dengan kerja jaringan kooperatif, kita dapat memiliki dua atau lebih perangkat yang mengirimkan paket yang sama. Dalam hal ini, penerima dapat menggabungkan semua sinyal yang diterima dan meningkatkan rasio sinyal terhadap noise. Oleh karena itu, jaringan kerja sama dapat menghasilkan transmisi yang lebih andal. Selain itu, jika penerima terlalu jauh dari perangkat lain untuk menerima sinyal pemancar tunggal dengan benar, mungkin dengan menggabungkan sinyal dari dua atau lebih pemancar, keseluruhan sinyal menjadi cukup kuat (atau lebih kuat dari kebisingan), dan komunikasi dapat dibangun.

Berikut ini, kami menyajikan formalisme yang memungkinkan untuk mengadaptasi dengan upaya minimal semua model yang disajikan dalam bab ini untuk kasus jaringan kerja sama. Rincian mendalam bersama dengan hasil komputasi yang membandingkan jaringan ad hoc standar dengan jaringan ad hoc kooperatif disajikan dalam referensi 53.

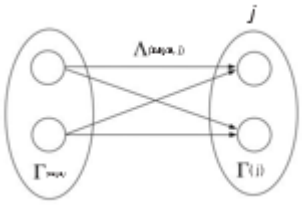
7.7.1 Grafik ÿ-Kerjasama

Model jaringan didasarkan pada konsep tingkat kerjasama.

Definisi 1. Sebuah jaringan nirkabel G memiliki tingkat kerjasama ÿ jika, selama slot waktu yang sama, paling banyak ÿ node diizinkan untuk mengirimkan paket yang sama ke satu atau lebih node penerima, dan setiap penerima dapat menggabungkan paket dari pemancar ÿ .

Untuk ÿ > 1, graf G tidak cukup untuk memodelkan transmisi kooperatif. Kami mengembangkan konsep grafik, yang kami sebut sebagai grafik ÿ-Cooperation, untuk menggeneralisasi topologi asli G.

Definisi 2. Untuk graf G = (N, A), ÿ -Cooperation Graph Gÿ = (Nÿ, Aÿ), adalah graf tambahan yang mewakili semua kemungkinan transmisi dalam G yang diizinkan oleh level ÿ



Gambar 7.6 Ilustrasi supernode dan superlink.

Sebuah node i ÿ Nÿ merepresentasikan subset kosong dari N yang memiliki kardinalitas hingga ÿ, dan sebuah link (i, j) ÿ Aÿ merepresentasikan transmisi simultan dari satu paket dari semua node di node i yang diset di N ke node j yang diset di N.

Demi kejelasan, kami menggunakan v dan w untuk menunjukkan node dalam grafik asli G, dan node i dan j dalam grafik kerjasama Gÿ. Node dan tautan di Gÿ juga disebut sebagai supernode dan superlink. Misalkan (i) menyatakan himpunan simpul di N yang membentuk supernode i di Nÿ, dan (i, j) himpunan tautan yang membentuk superlink (i, j) ÿ Aÿ: (i, j) = {(v, w) | v ÿ (i), w ÿ (j)}. Perhatikan bahwa ukuran Gÿ tumbuh secara eksponensial di ÿ. Ketika ÿ = 1, graf ÿ-cooperation Gÿ direduksi menjadi topologi asli G. Konsep supernode dan superlink diilustrasikan pada Gambar 7.6. Dalam contoh ini, masing-masing dari dua supernode i dan j berisi dua node di N, dan superlink (i, j) merepresentasikan transmisi dari semua node di (i) ke semua node di (j).

Pada Gambar 7.6, keempat transmisi tidak harus sesuai dengan tautan di grafik asli G. Ini karena kondisi SNR mengambil bentuk baru di grafik kerjasama Gÿ. Agar superlink (i, j) ÿ A ada, kondisi SNR berikut berlaku untuk semua penerima superlink; yaitu, untuk semua w ÿ (j) yang kita peroleh

$$SNRiw = \frac{vÿ(i)\ Pvgvw}{ÿ}\ ÿ\ ÿ. \qquad (7.21)$$

Pembilang pada (7.21) memodelkan fakta bahwa node (i) mentransmisikan paket yang sama dan karenanya semuanya berkontribusi untuk meningkatkan SNR. Untuk alasan ini, superlink dapat dibentuk, sebagai hasil kerja sama, bahkan jika beberapa atau mungkin tidak ada transmisi dari superlink ini merupakan bagian dari link yang diatur dalam topologi asli.

Ketika beberapa supernode mentransmisikan dalam slot waktu yang sama, interferensi harus diperhitungkan. Misalkan, selain i, satu set supernode melakukan transmisi pada slot waktu yang sama. Kondisi SINR untuk superlink (i, j) adalah bahwa untuk semua w ÿ (j), pertidaksamaan berikut berlaku:

$$SINRiw = \frac{vÿ(i)\ Pvgvw}{ÿ \quad uÿ(l)\ Puguw + ÿ}\ ÿ\ ÿ \qquad (7.22)$$

Pada (7.22), semua node yang membentuk supernode menghasilkan interferensi ke superlink (i, j). Perhatikan bahwa simpul u ÿ N dapat muncul paling banyak satu kali dalam penyebut, karena supernode yang mentransmisikan dalam slot waktu apa pun semuanya harus memiliki kumpulan node yang saling terpisah dalam grafik aslinya.

7.7.2 Kelas Superlink

Supernode di Gÿ bervariasi dalam kardinalitas himpunan bagian terkait dari node di grafik asli. Berdasarkan kardinalitas ini, kami mendefinisikan empat kelas superlink.

1. Satu-ke-Satu. Ini adalah tautan dalam topologi fisik asli — yaitu, tautan di A. Superlink (i, j) adalah kelas ini jika memenuhi kondisi (i) = {v}, (j) = {w}, dan (v, w) ÿ A.

2.Satu-ke-Banyak. Superlink dari kelas ini sesuai dengan sekelompok link di A yang berasal dari node yang sama di N. Jadi (i, j) ÿ Aÿ adalah superlink satu-ke-banyak jika

(i) = {v}, |(j)| > 1, dan (v, w) ÿ A untuk semua w ÿ (j). Tautan satu-ke-banyak juga disebut sebagai tautan siaran. Subkelas khusus dari tautan satu-ke-banyak disebut

tautan buffering, di mana sebuah simpul berperilaku seolah-olah ia juga mentransmisikan ke dirinya sendiri.

3. Banyak-ke-Satu. Sebuah superlink (i, j) ÿ Aÿ adalah kelas many-to-one, jika |(i)| > 1 dan (j) = {w}, w ÿ N \ (i). Superlink ini mewakili misi transmisi simultan dari paket yang sama dari semua node di (i) ke penerima tunggal w di (j). Tautan banyak-ke-satu tidak

harus terdiri dari sekelompok tautan di grafik asli; yaitu, (i) dapat memuat simpul v untuk mana (v, w) ÿ/ A, asalkan SNR di w memenuhi (7.21) dengan kerja sama.

Tautan dalam kelas banyak-ke-satu juga disebut sebagai tautan kerja sama.

4. Banyak-ke-Banyak. Kelas tautan ini mewakili transmisi dari paket yang sama antara banyak pemancar dan penerima dalam grafik aslinya. Superlink (i, j) adalah link banyak-ke-banyak jika dan hanya jika |(i)| > 1 dan |(j)| > 1. Superlink yang ditunjukkan pada Gambar 7.6 adalah dari kelas ini. Mirip dengan superlink banyak-ke-satu, superlink banyak-ke-banyak (i, j) dapat dibuat dengan kerja sama; karenanya mungkin memiliki transmisi antara satu atau beberapa pasang node v ÿ (i) dan w ÿ (j) yang (v,

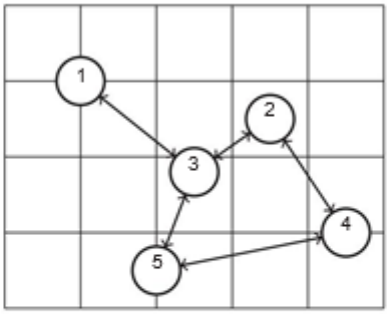
w) ÿ/ A. Banyak-ke-banyak superlink juga disebut tautan kerja sama luas atau tautan multicasting.

Contoh 7.1. Gambar 7.7 menunjukkan topologi fisik jaringan nirkabel dengan 5 node. Gambar 7.8 menunjukkan supernode dari jaringan 2-kerja sama yang sesuai.

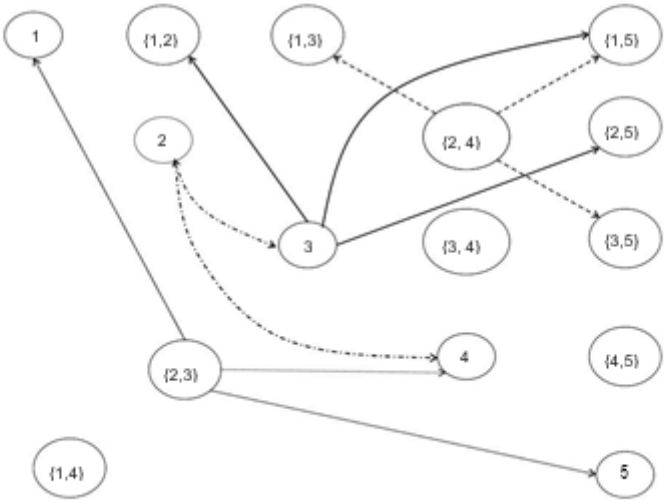
Untuk kejelasan, hanya beberapa superlink yang digambar. Tautan titik-putus adalah kelas satu-ke-satu; ini adalah insiden tautan ke simpul 2 dalam topologi asli.

Solid superlink menyiarkan link dari node 3 ke supernode {1, 2}, {1, 5}, dan {2, 5}, masing- masing. Masing-masing dari tiga superlink bertitik adalah link yang bekerja sama, mewakili transmisi paket secara simultan dari supernode {2, 3} ke satu penerima. Perhatikan bahwa transmisi pada (2, 1), (2, 5), dan (3, 4) tidak sesuai dengan link fisik pada Gambar 7.7.

Terakhir, superlink putus-putus adalah link multicasting, yang masing-masing membawa transmisi yang melibatkan dua pemancar dan dua penerima; beberapa transmisi ini terjadi antara node yang tidak memiliki link pada Gambar 7.7.



Gambar 7.7 Topologi jaringan nirkabel yang sangat sederhana.

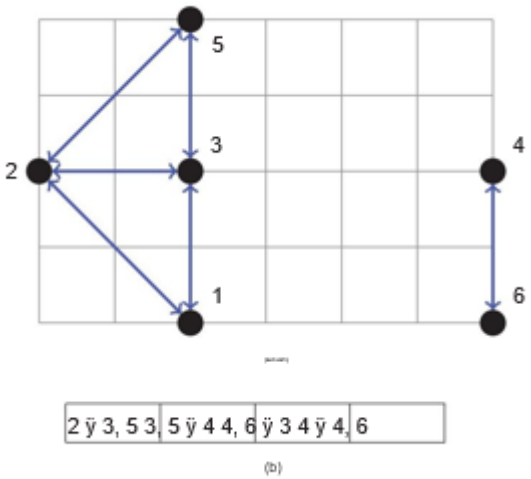


Gambar 7.8 Pemilihan supernode dan beberapa superlink dari grafik 2-kerja sama yang dihasilkan dari jaringan Gambar 7.7.

Jarak dalam hop antara pasangan sumber-tujuan mungkin mendapat manfaat dari tautan kerja sama dan multicasting. Misalnya, jalur terpendek dari simpul 4 ke simpul 1 memiliki tiga lompatan jika tidak ada kerjasama yang diperbolehkan. Jarak lintasan terpendek pada graf kerjasama menjadi dua lompatan, dan salah satu lintasan tersebut dibentuk oleh 4, {2, 5}, dan 1.

Contoh 7.2. Keuntungan yang jelas dari relay kooperatif terdiri dari memungkinkan komunikasi antar node yang, karena kendala SNR, tidak terhubung di jaringan asli. Gambar 7.9 menunjukkan contoh kecil jaringan dengan 6 node dan dua permintaan 2, 4 dan 4, 3. Dalam contoh, permintaan mewakili satu paket yang terkait dengan sumber dan tujuan. Daya transmisi P adalah 0,2 mW, kebisingan termal pada penerima ÿ adalah 10ÿ10 mW, dan ambang batas SNR ÿ adalah 10.

Karena simpul 4 terputus dari simpul 2 dan simpul 3, kedua permintaan tidak dapat



Gambar 7.9 Jaringan kooperatif untuk menyediakan konektivitas tambahan. (a) Topologi dengan P = 0,2 mW, ÿ = 10ÿ10 mW, ÿ = 10. (b) Perutean dan penjadwalan dua tuntutan 2, 4 dan 4, 3.

puas tanpa kerja sama. Jika kita mengizinkan kerjasama 2 tingkat, permintaan 2, 4 dipenuhi dengan konfigurasi 2 ÿ {3, 5} dan {3, 5} ÿ 4, dan permintaan 4, 3 dipenuhi dengan

konfigurasi 4 ÿ { 4, 6} dan {4, 6} ÿ 3. Perhatikan bahwa permintaan kedua menggunakan

link penyangga 4 ÿ {4, 6}.

Contoh 7.3. Keuntungan kerjasama cenderung menurun seiring dengan meningkatnya konektivitas jaringan. Untuk mengukur konektivitas, kami menggunakan dua properti

jaringan: |A| (i) densitas jaringan ÿ = yaitu, persentase link yang memenuhi.

7.11 menunjukkan dua jaringan yang berbeda hanya pada tingkat konektivitasnya. Dalam

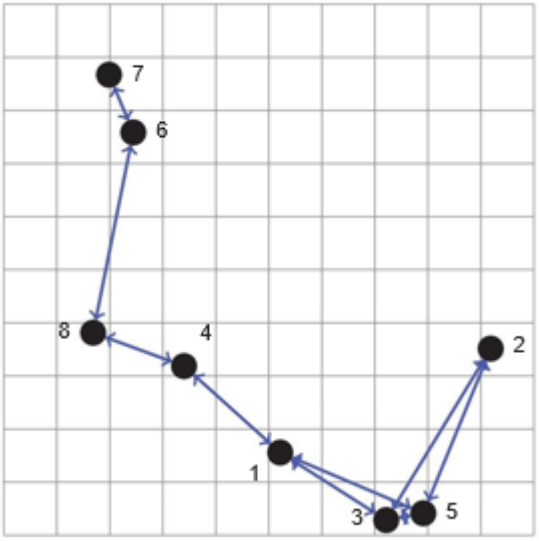
terkasus pertama, node mengirimkan dengan P = 0,1 mW. Dalam kasus kedua, daya P

adalah 0,4 mW. Dalam contoh ini, setiap pasang node dan j memiliki permintaan paket tunggal di kedua arah, yaitu i, j dan j, i. Untuk jaringan Gambar 7.10, solusi optimal membutuhkan 130 kali lot tanpa kerja sama, dan hanya 110 slot waktu dengan kerja sama, menunjukkan keuntungan kerja sama yang jelas. Sebaliknya, untuk jaringan pada Gambar

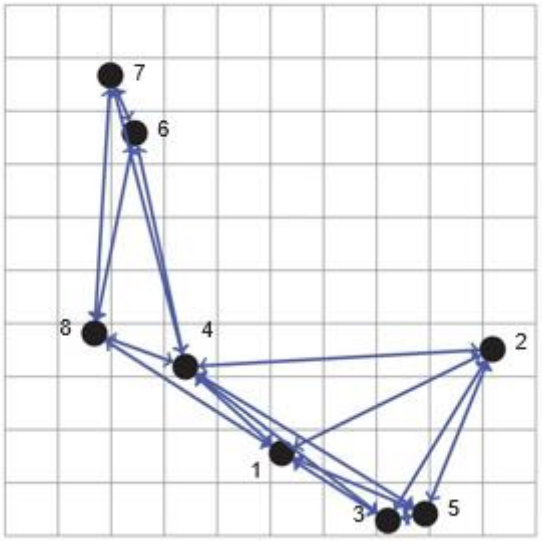
7.11 dimana konektivitas jauh lebih tinggi, panjang jadwal yang optimal adalah 74, dengan atau tanpa kerjasama.

7.7.3 Pembangkitan Kolom Diterapkan pada ÿ-Cooperation

Demi singkatnya, kita bahas di sini hanya masalah master dan sub masalah harga dari masalah routing dan penjadwalan bersama dalam jaringan kooperatif. Semua konsep dan definisi umum tentang pembuatan kolom sudah disajikan di halaman sebelumnya. Rincian tambahan diberikan dalam referensi 53.



Gambar 7.10 Topologi dengan kerapatan ÿ = 0,14 dan diameter = 6, diinduksi oleh parameter P = 0,1 mW dan ÿ = 10ÿ10 mW, ÿ = 15.



Gambar 7.11 Topologi dengan densitas ÿ = 0.30 dan diameter = 2, diinduksi oleh parameter P = 0.4 mW, ÿ = 10ÿ10 mW, dan ÿ = 15.

Misalkan S menunjukkan kumpulan dari semua konfigurasi yang layak, dan misalkan Sij ÿ S adalah himpunan konfigurasi yang berisi superlink (i, j) ÿ Aÿ.

7.8 PENUTUP DAN ISU MASA MENDATANG

Dalam bab ini kami menganalisis masalah manajemen sumber daya yang muncul dalam jaringan mesh nirkabel di mana node jaringan juga dapat dilengkapi dengan beberapa antarmuka radio yang dapat beroperasi pada saluran ortogonal yang berbeda.

Untuk menyajikan masalah, kami telah mengadopsi pendekatan analitik yang ketat berdasarkan formulasi pemrograman matematis dan telah menunjukkan bagaimana pendekatan pemodelan yang berbeda dapat memberikan wawasan tentang batasan dasar yang membatasi penggunaan sumber daya.

Kami mulai mempertimbangkan masalah aktivasi tautan yang bertujuan memaksimalkan jumlah transmisi paralel di bawah batasan interferensi. Ini adalah komponen dasar dari semua masalah pengoptimalan sumber daya di jaringan nirkabel. Kami kemudian menyajikan masalah penjadwalan tautan optimal di mana set transmisi paralel yang berbeda ditugaskan ke slot waktu. Perutean adalah elemen penting lainnya dari manajemen sumber daya yang telah kami tunjukkan dapat dioptimalkan bersama dengan transmisi penjadwalan. Isu-isu lain seperti kontrol daya, penyesuaian laju, penetapan saluran, dan antena pengarah juga telah didiskusikan dan disertakan dalam model.

Sebagai pernyataan terakhir, perlu dicatat bahwa upaya penelitian baru-baru ini yang telah dikhususkan untuk masalah manajemen sumber daya mendasar dalam jaringan wireless meshtelah memungkinkan kita untuk mempertimbangkan kembali beberapa masalah utama jaringan nirkabel umum. Sebagian besar hasil yang tersedia untuk jaringan nirkabel mengacu pada topologi acak dan sering memberikan informasi tentang perilaku jaringan asimptotik. Masalah yang dibahas dalam bab ini memungkinkan kita untuk mempertimbangkan topologi jaringan arbitrer dan menyediakan alat untuk menganalisis kapasitasnya.

Isi bab ini membahas isu-isu kunci utama yang harus dihadapi dalam optimalisasi sumber daya dalam jaringan mesh nirkabel multisaluran multiradio: perutean, penjadwalan, penetapan saluran, dan jaringan kooperatif. Kami menganggap teknik transmisi sebagai plugin dari formulasi umum dan menganalisis efek dari beberapa teknik lanjutan, seperti kontrol daya, adaptasi laju, dan antena terarah, dalam model interferensi yang sepenuhnya realistis berdasarkan SINR. Namun, ada teknik transmisi lain yang semakin umum dalam penerapan WMN saat ini, yang dampaknya pada manajemen sumber daya nirkabel berbasis SINR yang optimal masih harus diselidiki secara menyeluruh.

Dua perwakilan utama adalah teknik MIMO dan OFDM. Meskipun beberapa pekerjaan di mana teknik OFDM [54-57] dan MIMO [58-62] telah diperhitungkan untuk mempelajari beberapa masalah pengoptimalan sumber daya nirkabel, ada kebutuhan untuk mengembangkan formulasi baru yang lengkap dan dapat ditelusuri di mana teknik tersebut disertakan. dalam masalah optimisasi di bawah batasan SINR. Formulasi ini harus memberikan fitur utama dari solusi optimal dan dengan demikian mengarah pada pengembangan dan penilaian kualitas pendekatan heuristik.

Topik selanjutnya di mana pengoptimalan sumber daya di WMN dapat dan akan mendapatkan momentum adalah Jaringan Hijau. Mengikuti gagasan bahwa efisiensi energi terbaik dicapai ketika

konsumsi energi jaringan dapat disesuaikan secara dinamis dengan tingkat lalu lintas nyata dalam jaringan, masalah pengoptimalan WMN baru yang menarik dan menantang muncul. Secara khusus, masalah utama berasal dari persyaratan cakupan, konektivitas, dan kapasitas yang harus dipertimbangkan secara bersamaan dalam WMN. Daya pancar, jenis perangkat, biayanya, dan profil konsumsi energinya berdampak pada semua persyaratan dan, pada saat yang sama, pada konsumsi energi.

Semua parameter harus dioptimalkan dengan hati-hati agar sesuai dengan variasi lalu lintas selama cakrawala pengoptimalan.

REFERENCE

1. I. Chlamtac, M. Conti, dan J. Liu. Jaringan ad hoc seluler: Keharusan dan tantangan.

Jurnal Jaringan Ad Hoc 1(1):13–64, 2003.

2. S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic (Eds.). Jaringan Ad Hoc Seluler.

IEEE Press dan John Wiley & Sons, New York, 2004.

3. Marco Conti dan Silvia Giordano. Jaringan ad hoc multi-hop: Teori. Masalah tentang "Jaringan Ad hoc dan Sensor". Majalah Komunikasi IEEE 45(4):78–86, 2007.

4. Emilio Ancillotti, Raffaele Bruno, Marco Conti, and Antonio Pinizzotto. Konfigurasi otomatis alamat dinamis dalam jaringan ad hoc hybrid. Pervasif dan Komputasi Seluler 5(4): 300–317, 2009.

5. Emilio Ancillotti, Raffaele Bruno, Marco Conti, Enrico Gregori, and Antonio Pinizzotto.

Kerangka kerja Layer-2 untuk menghubungkan jaringan ad hoc ke Internet tetap: Implementasi test-bed dan evaluasi eksperimental. Jurnal Komputer 50(4):478–499, 2007.

6. J. Macker dan S. Corson. Jaringan ad hoc seluler (MANETs): Teknologi perutean untuk jaringan

nirkabel yang dinamis. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 9.

7. G.Zaruba dan S.Das. Pengaktif jaringan ad hoc siap pakai. Di Seluler Ad Hoc

Jaringan. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 2.

8. G. Anastasi, M. Conti, dan E. Gregori. IEEE 802.11 dalam jaringan ad hoc: Protokol, kinerja, dan masalah terbuka. Bab 3. Dalam Jaringan Ad Hoc Seluler, IEEE Press dan John Wiley & Sons, New York, 2004.

9. Giuseppe Anastasi, Eleonora Borgia, Marco Conti, dan Enrico Gregori, jaringan ad hoc IEEE 802.11b: Pengukuran kinerja. Komputasi Klaster 8(2–3):135–145, 2005.

10. Giuseppe Anastasi, Eleonora Borgia, Marco Conti, Enrico Gregori, and Andrea Passarella. Memahami perilaku sebenarnya dari jaringan ad hoc Mote dan 802.11: Pendekatan eksperimental. Pervasif dan Komputasi Seluler 1(2), 237–256, 2005.

11. S. Basagni, R. Bruno, dan C. Petrioli. Pembentukan scatternet di jaringan Bluetooth. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 4.

12. R. Bruno, M. Conti, E. Gregori. Bluetooth: Arsitektur, protokol, dan penjadwalan algoritma. Komputasi Klaster 5(2):117–131, 2002.

13. Giuseppe Anastasi, Marco Conti, dan Mario Di Francesco. Analisis komprehensif masalah MAC yang tidak dapat diandalkan di jaringan sensor nirkabel IEEE 802.15.4. Transaksi IEEE pada Informatika Industri 7(1):52-65, 2011.

14. Paolo Baronti, Prashant Pillai, Vince WC Chook, Stefano Chessa, Alberto Gotta, dan Yim-Fun Hu. Jaringan sensor nirkabel: Survei tentang kecanggihan dan standar 802.15.4 dan ZigBee. Komunikasi Komputer 30(7):1655–1695, 2007.

15 .R.Ramanathan. Antena beamforming dan kontrol daya untuk jaringan ad hoc. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 5. 16. http:// en.wikipedia.org/wiki/Daftar protokol perutean ad hoc.

17. Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, dan Jang-Ping Sheu. Masalah badai siaran di jaringan ad hoc seluler. Prosiding ACM/ IEEE Tahunan Kelima International Conference on Mobile Computing and Networking (MOBICOM '99), 15-19 Agustus 1999, Seattle, Washington, USA, hlm. 151-162.

18. I. Stojmenovic dan J.Wu. Penyiaran dan penjadwalan aktivitas di jaringan ad hoc. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 7.

19. S. Giordano dan I. Stojmenovic. Rute ad hoc berbasis posisi di jaringan ad hoc. Dalam Buku Pegangan Jaringan Nirkabel Ad Hoc, M. Ilyas (Ed.). CRC Press, Boca Raton, FL, 2003.

20. L. Blazevic, JY Le Boudec, and S. Giordano. Metode perutean berbasis lokasi untuk jaringan ad hoc seluler. Transaksi IEEE pada Komputasi Seluler 4(2):97–110, 2005.

21. E. Belding-Royer. Pendekatan perutean dalam jaringan ad hoc seluler. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 10.

22. Giuseppe Anastasi, Emilio Ancillotti, Marco Conti, and Andrea Passarella. Desain dan evaluasi kinerja protokol transport untuk jaringan ad hoc . Jurnal Komputer 52(2):186–209, 2009.

23. M. Conti, F. Delmastro, dan G. Turi. Komputasi peer-to-peer dalam jaringan ad hoc seluler. Dalam The Handbook of Mobile Middleware, Antonio Corradi dan Paolo Bellavista (Eds.). Publikasi Auerbach, Boca Raton, FL, 2007, hlm. 569–598.

24. Eleonora Borgia, Marco Conti, dan Franca Delmastro. MobileMAN: Integrasi dan eksperimen jaringan ad hoc multihop seluler lama. Majalah Komunikasi IEEE 44(7):74–79, 2006.

25. Eleonora Borgia, Marco Conti, dan Franca Delmastro. MobileMAN: Desain, integrasi, dan eksperimentasi jaringan ad hoc multihop seluler lintas lapisan. Majalah Komunikasi IEEE 44(7):80–85, 2006.

26. L. Feeney. Komunikasi hemat energi dalam jaringan nirkabel ad hoc. Dalam Mobile Ad Hoc Networking, IEEE Press dan John Wiley & Sons, New York, 2004, Bab 11.

27. P. Michiardi dan R. Molva. Keamanan jaringan ad hoc. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 12.

28. A. Urpi, M. Bonuccelli, dan S. Giordano. Memodelkan kerja sama dalam jaringan ad hoc seluler: deskripsi formal tentang keegoisan. Prosiding WiOpt'03: Pemodelan dan Optimasi di Jaringan Seluler, Ad Hoc, dan Nirkabel, 3–5 Maret 2003, Sophia-Antipolis, Prancis.

29. S. Giordano dan A. Urpi. Jaringan ad hoc yang terorganisir sendiri dan kooperatif. Dalam Mobile Ad Hoc Networking, IEEE Press dan John Wiley & Sons, New York, 2004, Bab 13.

30. G. Anastasi, M. Conti, A. Passarella. Manajemen daya dalam sistem komputasi seluler dan pervasif. Dalam Algoritma dan Protokol untuk Jaringan Nirkabel dan Seluler, Azzedine Boukerche (Ed.), Chapman dan Hall/CRC Computer and Information Science Publishers, Boca Raton, FL, November 2005, Bab 24.

31. G. Anastasi, M. Conti, E. Gregori, dan A. Passarella. Perbandingan kinerja strategi penghematan daya untuk akses Web seluler. Jurnal Evaluasi Kinerja 53(3–4): 273–294, 2003.

32. R. Bruno, M. Conti, dan E. Gregori. Optimalisasi efisiensi dan konsumsi energi pada LAN nirkabel berbasis CSMA yang persisten. Transaksi IEEE pada Mobile Computing 1(1):10– 31, 2002. 33.X.Li. Kontrol topologi dalam jaringan ad hoc nirkabel. Dalam Jaringan Ad Hoc Seluler. IEEE Press dan John Wiley & Sons, New York, 2004, Bab 6.

34. M. Conti, E. Gregori, dan G. Maselli. Masalah kerjasama dalam jaringan ad hoc seluler. Prosiding Konferensi Internasional IEEE ke-24 tentang Lokakarya Sistem Komputasi Terdistribusi, Masyarakat Komputer IEEE, Washington, DC, AS, 2004, hlm. 803–808.

35. AJ Goldsmith dan SB Wicker. Tantangan desain untuk ad hoc dengan energi terbatas jaringan nirkabel. Komunikasi Nirkabel IEEE 9(4):8–27, 2002.

36. M. Conti, G. Maselli, G. Turi, and S. Giordano. Lapisan silang dalam jaringan ad hoc seluler rancangan. Komputer IEEE 37(2):48–51, 2004.

37. V. Kawadia dan PR Kumar. Perspektif peringatan pada desain lintas lapisan. Majalah Komunikasi Nirkabel IEEE 12(1):3–11, 2005.

38. Vineet Srivastava dan Mehul Motani. Desain lintas lapisan: Sebuah survei dan jalan di depan.

Majalah Komunikasi IEEE, Desember 2005, hlm. 112–119.

39. M. Conti, S. Giordano, Martin May, dan A. Passarella. Dari jaringan oportunistik ke komputasi oportunistik. Majalah Komunikasi IEEE 48(9):126–139, 2010.

40. M. Conti, J. Crowcroft, G. Maselli, dan T. Turi. Sebuah arsitektur cross-layer modular untuk jaringan ad hoc. Dalam Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks, Jie Wu (Ed.). Auerbach Publications (Taylor & Francis Group), Boca Raton, FL, 2005, hlm. 5–16.

41. R. Knopp dkk. Sekilas tentang arsitektur WIDENS, jaringan ad hoc nirkabel untuk keamanan publik. Proses dari IEEE SECON'04, Sesi Poster, 2004.

42. Daniel Grobe Sachs, Wanghong Yuan, Christopher J. Hughes, Albert Harris, Sarita V. Adve, Douglas L. Jones, Robin H. Kravets, dan Klara Nahrstedt. GRACE: Kerangka Adaptasi Hirarki untuk Penghematan Energi. Ilmu Komputer, Laporan Teknis Universitas Illinois UIUCDCS- R-2004-2409, Februari 2004.

43. R. Winter, J. Schiller, N. Nikaein, dan C. Bonnet. CrossTalk: Dukungan keputusan lintas lapisan berdasarkan pengetahuan global. Majalah Komunikasi IEEE 44(1):93–99, 2006.

44. V. Raisinghani dan S. Iyer. Arsitektur umpan balik lintas lapisan untuk protokol perangkat seluler tumpukan. Majalah Komunikasi IEEE 44(1):85–92, 2006.

45. Herve Aiache, Vania Conan, Jeremie Leguay, dan Mikael Levy. XIAN: Antarmuka lintas lapisan untuk Jaringan ad hoc nirkabel. Prosiding MedHocNet 2006, Lipari, Juni 2006.

¨46. Christian F. Tschudin, Per Gunningberg, Henrik Lundgren, dan Erik Nordstrom. Pelajaran dari penelitian eksperimental MANET. Jaringan Ad Hoc 3(2):221–233, 2005.

47. L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, JP Hubaux, and JY Le Boudec. Organisasi mandiri dalam jaringan ad hoc seluler: pendekatan Terminode. Majalah Komunikasi IEEE 39(6), 166–174, Juni 2001.

48. Marco Conti dan Silvia Giordano. Jaringan Ad Hoc Multi-hop: Realitas. Masalah tentang “Jaringan Ad hoc dan Sensor”. Majalah Komunikasi IEEE 45(4):88–95, 2007.

49. R. Bruno, M. Conti, dan E. Gregori. Jaringan mesh: Jaringan ad hoc multihop komoditas. Majalah Komunikasi IEEE hal.123–131, 2005. 50. http://www.muniwireless.com/ 51. Emilio Ancillotti, Raffaele Bruno, dan Marco Conti. Desain dan evaluasi kinerja protokol adaptasi laju sadar throughput untuk jaringan nirkabel IEEE 802.11. Evaluasi Kinerja 66(12):811–825, 2009.

52. H. Skalli, S. Ghosh, SK Das, L. Lenzini, and M. Conti. Strategi penugasan saluran untuk jaringan mesh nirkabel multi-radio: Masalah dan solusi. Majalah Komunikasi IEEE 45(11):86–95, 2007.

53. Raffaele Bruno dan Maddalena Nurchis. Survei perutean berbasis keragaman dalam jaringan mesh nirkabel: Tantangan dan solusi. Komunikasi Komputer 33(16):1894–1906, 2010

54. Vinicius CM Borges, Marilia Curado, dan Edmundo Monteiro. Metrik perutean lintas lapisan untuk jaringan mesh: Status saat ini dan arah penelitian. Komunikasi Komputer 34(6):681– 703, 2011.

55. Emilio Ancillotti, Raffaele Bruno, Marco Conti, and Antonio Pinizzotto. “Muat perutean sadar di jaringan mesh: Model, algoritme, dan eksperimen. Komunikasi Komputer 34(8):948-961, 2011.

56. Bahador Bakhshi, Siavash Khorsandi, dan Antonio Capone. Routing QoS bersama online dan penugasan saluran dalam jaringan mesh nirkabel multi-channel multi-radio. Komunikasi Komputer, 34(11):1342–1360, 2011.

57. Raffaele Bruno, Marco Conti, dan Antonio Pinizzotto. Merutekan lalu lintas Internet dalam jaringan mesh heterogen: Analisis dan algoritme. Evaluasi Kinerja 68(9):841–858, 2011.

58. D. Gallucci dan S. Giordano. QoS mengaktifkan dukungan mobilitas untuk jaringan mesh. Lokakarya PerCom, Galveston, TX, AS, Maret 2009. doi.ieeecomputersociety.org/10.1109/ PERCOM.2009.4912846.

59. Jing Dong, Reza Curtmola, dan Cristina Nita-Rotaru. Pengkodean jaringan aman untuk jaringan mesh nirkabel: Ancaman, tantangan, dan arah. Komunikasi Komputer 32(17):1790– 1801, 2009.

60. Kefeng Tan, Daniel Wu, An (Jack) Chan, and Prasant Mohapatra. Membandingkan alat simulasi dan testbed eksperimental untuk jaringan mesh nirkabel. Pervasif dan Mobile Computing, 2011, doi:10.1016/j.pmcj.2011.04.004.

61. L. Pelusi, A. Passarella, dan M. Conti. Jaringan oportunistik: Penerusan data dalam jaringan ad hoc seluler yang terputus. Majalah Komunikasi IEEE (bagian khusus Topik dalam Jaringan Ad Hoc) November 2006, hlm. 134–141.

62. Marco Conti, Jon Crowcroft, Silvia Giordano, Pan Hui, Hoang Anh Nguyen, and Andrea Passarella. Masalah perutean dalam jaringan oportunistik. Dalam Middleware untuk Jaringan Eksentrik dan Aplikasi Seluler, B. Garbinato, H. Miranda, dan L. Rodrigues (Eds.). Springer, New York, 2009, hlm. 121–147.

63. Pan Hui, Jon Crowcroft, dan Eiko Yoneki. Bubble rap: Penerusan berbasis sosial dalam jaringan yang tahan tunda. Prosiding ACM MobiHoc 2008, hlm. 241–250.

64. C. Boldrini, M. Conti, and A. Passarella. Memanfaatkan hubungan sosial pengguna untuk meneruskan data dalam jaringan oportunistik: Solusi HiBOp. Pervasif dan Komputasi Seluler 4(5):633-657, 2008.

65. AH Nguyen, S. Giordano, and A. Puiatti. Protokol perutean probabilistik untuk jaringan ad hoc seluler intermit tently connected (PROPICMAN). Prosiding IEEE WoWMoM/ AOC 2007, Helsinki, 2007.

66. E. Daly dan M. Haahr. Analisis jaringan sosial untuk perutean dalam toleran tunda terputus manet. Dalam Prosiding ACM MobiHoc, 2007.

67. C. Boldrini, M. Conti, and A. Passarella. Desain dan evaluasi kinerja ContentPlace, sistem penyebaran data sadar sosial untuk jaringan oportunistik. Jaringan Komputer 54:589–604, 2010.

68. Proyek PodNET http://podnet.ee.ethz.ch/

69. M. Conti, M. Mordacchini, dan A. Passarella. Penyebaran data dalam jaringan oportunistik menggunakan heuristik kognitif. In Proceedings of IEEE WoWMoM AOC Workshop, Juni 2011, Lucca (Italia).

70. A. Shikfa, M. Onen, dan R. Molva. Privasi dan kerahasiaan dalam penerusan berbasis konteks dan epidemi. Komunikasi Komputer 33(13):1493–1504, 2010.

71. John Solis, N. Asokan, Kari Kostiainen, Philip Ginzboorg, dan Jorg Ott. Mengontrol babi sumber daya di jaringan toleran tunda seluler. Komunikasi Komputer 33(1): 2–10, 2010.

72. V. Cerf dkk. Arsitektur jaringan yang tahan tunda. RFC4838, 2007.

73. Vinny Cahill, Stephen Farrell, dan Jorg Ott. Masalah khusus komunikasi komputer pada jaringan yang toleran terhadap penundaan dan gangguan. Komunikasi Komputer 32(16): 1685–1780, 2009.

74. T. Karagiannis, JY Le Boudec, dan M. Vojnovic. Hukum kekuatan dan peluruhan eksponensial dari waktu interkontak antara perangkat seluler. Transaksi IEEE pada Komputasi Seluler 9:1377–1390, 2010.

75. Augustin Chaintreau, Pan Hui, Jon Crowcroft, Christophe Diot, Richard Gass, dan James Scott. Dampak mobilitas manusia pada algoritma penerusan oportunistik. Transaksi IEEE pada Komputasi Seluler 6(6):606–620, 2007.

76. W. Gao, Q. Li, B. Zhao, and G. Cao. Multicasting dalam jaringan toleran penundaan: Sosial perspektif jaringan. Prosiding ACM MobiHoc, 2009.

77. A. Passarella dan M. Conti. Mencirikan waktu antar-kontak agregat dalam jaringan oportunistik yang heterogen. Prosiding IFIP TC6 Networking 2011, Valencia, Mei 2011, hlm. 301–313.

78. C. Boldrini, M. Conti, dan A. Passarella. Lebih sedikit lebih banyak: Jalan panjang tidak membantu konvergensi penerusan yang tidak menyadari sosial dalam jaringan oportunistik. Dalam ACM MobiOpp 2012, Zurich, Maret 2012.

79. A. Forster, K. Garg, HA Nguyen, dan S. Giordano. Tentang kesadaran konteks dan jarak social dalam jejak mobilitas manusia. Prosiding lokakarya ACM ketiga tentang Jaringan Oportunistik Seluler (MobiOpp 2012), ACM New York, NY, USA 2012, Halaman 5–12.

80. Mirco Musolesi dan Cecilia Mascolo. Merancang model mobilitas berdasarkan teori jaringan sosial. Tinjauan Komputasi dan Komunikasi Seluler 11(3):59–70, 2007.

81. Chiara Boldrini dan Andrea Passarella. HCMM: Memodelkan hubungan spasial dan temporal yang tepat dari mobilitas manusia yang didorong oleh hubungan sosial pengguna. Komunikasi Komputer 33(9):1056–1074, 2010.

82. D. Karamshuk, C. Boldrini, M. Conti, dan A. Passarella. Model mobilitas manusia untuk jaringan oportunistik. Majalah Komunikasi IEEE 49(12):157–165, 2011.

83. C. Boldrini, M. Conti, dan A. Passarella. Memodelkan penerusan kesadaran sosial dalam jaringan oportunistik. Dalam Prosiding PERFORM 2010 dan LNCS 6821.

84. Thrasyvoulos Spyropoulos, Thierry Turletti, dan Katia Obraczka. Perutean dalam jaringan toleran tunda yang terdiri dari populasi node yang heterogen. IEEE Transaction Mobile Computing 8(8):1132–1147, 2009.

85. AH Nguyen dan S. Giordano. Prediksi informasi konteks untuk perutean berbasis sosial di jaringan oportunistik. Jurnal Jaringan Ad Hoc 10(8):1557–1569, 2012.

86. Utku Günay Acer, Petros Drineas, dan Alhussein A. Abouzeid. Konektivitas di grafik waktu. Pervasif dan Komputasi Seluler 7(2):160–171, 2011.

87. Fan Li dan Yu Wang. Routing di jaringan ad hoc kendaraan: Sebuah survei. Majalah Teknologi Kendaraan IEEE 2(2):12–22, 2007.

88. Hannes Hartenstein dan Kenneth P. Laberteaux. Survei tutorial tentang jaringan ad hoc kendaraan. Majalah Komunikasi IEEE 46(4):164–171, 2008.

89. N. Wisitpongphan, O. K Tonguz, JS Parikh, P. Mudalige, F. Bai, V. Sadekar. Teknik mitigasi badai siaran di jaringan ad hoc kendaraan. Komunikasi Nirkabel IEEE 14(6):84–94, 2007.

90. Hongseok Yoo dan Dongkyun Kim. Penyiaran kooperatif berbasis pengulangan untuk jaringan ad hoc kendaraan. Komunikasi Komputer 2011, doi:10.1016/j.com. 2011.05.007.

91. J. Burgess, B. Gallagher, D. Jensen, dan BN Levine. MaxProp: Perutean untuk jaringan yang toleran terhadap gangguan berbasis kendaraan. Dalam Prosiding IEEE Infocom, 2006.

92. Ramon S. Schwartz, Rafael R. Barbosa, Nirvana Meratnia, Geert Heijenk, dan Hans Scholten. Protokol penyebaran data terarah untuk lingkungan kendaraan. Komunikasi Komputer 34(17):2057–2071, 2011.

93. Zhendong Ma, Frank Kargl, dan Michael Weber. Mengukur privasi lokasi jangka panjang dalam sistem komunikasi kendaraan. Komunikasi Komputer 33(12):1414–1427, 2010.

94. J. Harri, F. Filali dan C. Bonnet, Model mobilitas untuk jaringan ad hoc kendaraan: Sebuah survei dan taksonomi. Survei & Tutorial Komunikasi IEEE 11(4):19–41, 2009.

95. R. Bruno dan M. Conti. Analisis Throughput dan Kewajaran Transfer Data Kendaraan ke Infrastruktur berbasis 802.11. Dalam Prosiding IEEE MASS 2011, Valencia (Spanyol), Oktober 2011.

96. Ekram Hossain, Garland Chow, Victor CM Leung, Robert D. McLeod, Jelena Misiÿc,´ Vincent WS Wong, dan Oliver Yang. Telematika kendaraan melalui jaringan nirkabel heterogen: Sebuah survei. Komunikasi Komputer 33(7):775–793, 2010.

97. M. Conti dkk. Melihat ke depan dalam komputasi pervasif: Tantangan dan peluang di era konvergensi siber-fisik. Pervasif dan Komputasi Seluler 8(1):2–21, 2012.

98. JIKA, Akyildiz dan IH Kasimoglu. Jaringan sensor dan aktor nirkabel: Penelitian tantangan. Jurnal Jaringan Ad Hoc (Elsevier) 2:351–367, 2004.

99. IF Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Jaringan sensor nirkabel: Survei. Jaringan Komputer 38(4):393–422, 2002.

100. M. Di Francesco, S. Das, dan G. Anastasi. Pengumpulan data dalam jaringan sensor nirkabel dengan elemen seluler: Survei. Transaksi ACM pada Jaringan Sensor 8(1), 2011, doi:10.1145/1993042.1993049.

101. Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Konservasi energi dalam jaringan sensor nirkabel: Sebuah survei. Jurnal Jaringan Ad Hoc 7(3):537– 568, 2009.

102. I. Demirkol, C. Ersoy, dan F. Alagoz, protokol MAC untuk jaringan sensor nirkabel: Survei. Majalah Komunikasi IEEE 44(4):115–121, 2006.

103. Kemal Akkaya dan Mohamed Younis. Survei tentang protokol perutean untuk sensor nirkabel jaringan. Jaringan Ad Hoc 3(3):325–349, 2005.

104. Ameer Ahmed Abbasi dan Mohamed Younis. Survei tentang algoritma pengelompokan untuk jaringan sensor nirkabel. Komunikasi Komputer 30(14–15):2826–2841, 2007.

105. F. Sivrikaya dan B. Yener. Sinkronisasi waktu dalam jaringan sensor: Survei. IEEE Jaringan 18(4):45–50, 2004.

ISBN 978-623-8120-09-3 (PDF)

YAYASAN PRIMA AGUS TEKNIK