

در دنیای تلفن، ۲۵ سال گذشته سال های طلایی تلفن همراه بوده است. تعداد مشترکان تلفن همراه در سراسر جهان از ۳۴ میلیون در سال ۱۹۹۳ به ۸.۳ میلیارد مشترک در سال ۲۰۱۹ افزایش یافته است. اکنون تعداد مشترکان تلفن همراه بیشتر از تعداد افراد در سیاره ما است. مزایای بسیاری از تلفن های همراه برای همه مشهود است - در هر مکان، در هر زمان، دسترسی بدون اتصال به شبکه تلفن جهانی از طریق یک دستگاه سبک وزن بسیار قابل حمل. اخیراً تلفن های هوشمند، تبلت ها و لپ تاپ ها به صورت بی سیم از طریق شبکه تلفن همراه یا WiFi به اینترنت متصل شده اند. و به طور فزاینده ای، دستگاه هایی مانند کنسول های بازی، ترموستات ها، سیستم های امنیتی خانگی، لوازم خانگی، ساعت ها، عینک های چشمی، خودروها، سیستم های کنترل ترافیک و غیره به صورت بی سیم به اینترنت متصل می شوند.

از نقطه نظر شبکه، چالش های ناشی از شبکه سازی این دستگاه های بی سیم و تلفن همراه، به ویژه در لایه پیوند و لایه شبکه، آنقدر با شبکه های کامپیوتری سیمی سنتی متفاوت است که یک فصل جداگانه به مطالعه شبکه های بی سیم و موبایل اختصاص داده شده است (یعنی این فصل) مناسب است.

ما این فصل را با بحثی در مورد کاربران تلفن همراه، پیوندهای بی سیم و شبکه ها و رابطه آنها با شبکه های بزرگتر (معمولاً سیمی) که به آنها متصل می شوند، آغاز می کنیم. ما بین چالش های ناشی از ماهیت بی سیم پیوندهای ارتباطی در چنین شبکه هایی و تحرکی که این پیوندهای بی سیم ایجاد می کنند، تمایز قائل می شویم. ایجاد این تمایز مهم - بین بی سیم و تحرک - به ما این امکان را می دهد که مفاهیم کلیدی را در هر زمینه بهتر جداسازی، شناسایی و تسلط دهیم.

ما با مروری بر زیرساخت های دسترسی بی سیم و اصطلاحات مرتبط شروع خواهیم کرد. سپس ویژگی های این پیوند بی سیم را در بخش ۷.۲ در نظر خواهیم گرفت. ما در بخش ۷.۲ مقدمه کوتاهی برای دسترسی چندگانه تقسیم کد (CDMA)، یک پروتکل دسترسی اشتراکی متوسط که اغلب در شبکه های بی سیم استفاده می شود، ارائه می کنیم. در بخش ۷.۳، جنبه های سطح پیوند استاندارد LAN بی سیم (WiFi) IEEE 802.11 را تا حدودی بررسی خواهیم کرد. ما همچنین چند کلمه در مورد شبکه های شخصی بی سیم بلوتوث خواهیم گفت. در بخش ۷.۴، مروری بر دسترسی به اینترنت سلولی، از جمله فناوری های سلولی G۴ و نوظهور G۵ که هم دسترسی صوتی و هم به اینترنت پرسرعت را فراهم می کنند، ارائه می کنیم. در بخش ۷.۵، ما توجه خود را به جابجایی معطوف خواهیم کرد، با تمرکز بر مشکلات مکان یابی کاربر تلفن همراه، مسیریابی به کاربر تلفن همراه، و "تحويل" کاربر تلفن همراه که به صورت پویا از یک نقطه اتصال به شبکه به نقطه دیگر منتقل می شود. نحوه پیاده سازی این سرویس های تحرک در شبکه های سلولی G/5G۴ و استاندارد IP موبایل در بخش ۷.۶ را بررسی خواهیم کرد. در نهایت، تأثیر

پیوندهای بی سیم و تحرک بر پروتکل های لایه انتقال و برنامه های کاربردی شبکه را در بخش ۷.۷ در نظر خواهیم گرفت.

۷.۱ مقدمه

شکل ۷.۱ تنظیماتی را نشان می دهد که در آن ما موضوعات ارتباط داده های بی سیم و تحرک را در نظر خواهیم گرفت. ما با کلی نگه داشتن بحث خود به اندازه کافی برای پوشش طیف گسترده ای از شبکه ها، از جمله شبکه های محلی بی سیم مانند WiFi و شبکه های سلولی G4 و G5، شروع می کنیم. در بخش های بعدی به بحث مفصل تری در مورد معماری های بی سیم خاص خواهیم پرداخت. ما می توانیم عناصر زیر را در یک شبکه بی سیم شناسایی کنیم:

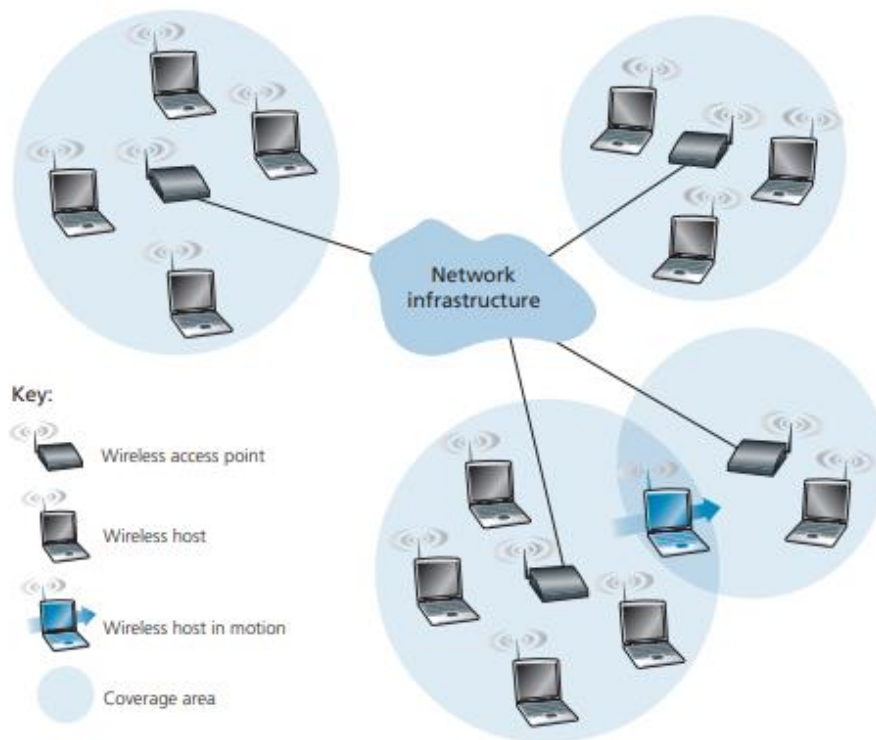


Figure 7.1 ♦ Elements of a wireless network

- هاست های بی سیم. همانطور که در مورد شبکه های سیمی، هاست ها دستگاه های سیستم نهایی هستند که برنامه ها را اجرا می کنند. یک میزبان بی سیم ممکن است یک گوشی هوشمند، تبلت یا لپ تاپ باشد، یا می تواند یک دستگاه اینترنت اشیا (IoT) باشد، مانند سنسور، دستگاه، خودرو یا هر دستگاه دیگری که به اینترنت متصل است. خود میزبان ها ممکن است متحرک باشند یا نباشند.

- پیوندهای بی سیم. یک میزبان از طریق یک پیوند ارتباطی بی سیم به یک ایستگاه پایه (تعریف شده در زیر) یا به یک میزبان بی سیم دیگر متصل می شود. فناوری های مختلف پیوند بی سیم دارای نرخ های انتقال متفاوتی

هستند و می‌توانند در فواصل مختلف ارسال کنند. شکل ۷.۲ دو ویژگی کلیدی، نرخ انتقال لینک و محدوده پوشش، از استانداردهای رایج شبکه بی سیم را نشان می‌دهد. (شکل فقط به منظور ارائه یک ایده تقریبی از این ویژگی‌ها است. به عنوان مثال، برخی از این نوع شبکه‌ها فقط در حال حاضر در حال گسترش هستند و برخی از نرخ‌های پیوند می‌توانند بیش از مقادیر نشان داده شده بسته به فاصله، شرایط کانال و همچنین افزایش یا کاهش پیدا کنند. تعداد کاربران در شبکه بی سیم.) ما این استانداردها را بعداً در نیمه اول این فصل پوشش خواهیم داد. ما همچنین سایر ویژگی‌های پیوند بی سیم (مانند نرخ خطای بیت و علل خطاهای بیت) را در بخش ۷.۲ در نظر خواهیم گرفت.

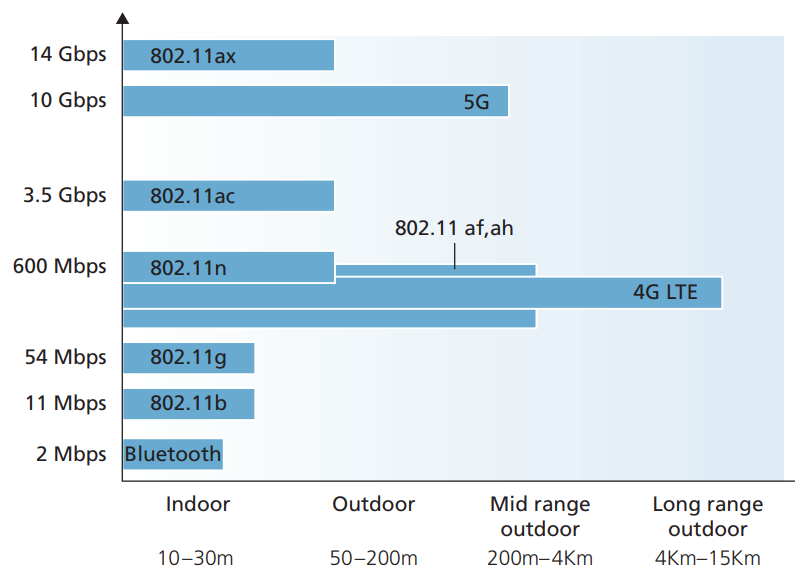


Figure 7.2 ♦ Wireless transmission rates and range for WiFi, cellular 4G/5G and Bluetooth standards (note: axes are not linear)

در شکل ۷.۱، پیوندهای بی سیم میزبان‌های بی سیم واقع در لبه شبکه را به زیرساخت شبکه بزرگتر متصل می‌کنند. ما عجله داریم اضافه کنیم که پیوندهای بی سیم نیز گاهی در داخل شبکه برای اتصال روترها، سوئیچ‌ها و سایر تجهیزات شبکه استفاده می‌شوند. با این حال، تمرکز ما در این فصل بر روی استفاده از ارتباطات بی سیم در لبه شبکه خواهد بود، زیرا اینجاست که بسیاری از هیجان‌انگیزترین چالش‌های فنی و بیشتر رشد در حال رخ دادن است.

• ایستگاه پایه. ایستگاه پایه بخش کلیدی زیرساخت شبکه بی سیم است. برخلاف میزبان بی سیم و پیوند بی سیم، یک ایستگاه پایه هیچ مشابه آشکاری در یک شبکه سیمی ندارد. یک ایستگاه پایه مسئول ارسال و دریافت داده‌ها (مثلاً بسته‌ها) به/از یک میزبان بی سیم است که با آن ایستگاه پایه مرتبط است. یک ایستگاه پایه اغلب مسئول هماهنگی انتقال چندین میزبان بی سیم است که با آن مرتبط است. وقتی می‌گوییم یک میزبان بی سیم با یک ایستگاه پایه "ارتباط" دارد، منظور ما این است که (۱) میزبان در فاصله ارتباطی بی سیم ایستگاه پایه قرار دارد،

و (۲) میزبان از آن ایستگاه پایه برای انتقال داده ها بین خود استفاده می کند. میزبان) و شبکه بزرگتر. برج های سلولی در شبکه های سلولی و نقاط دسترسی در شبکه های محلی بی سیم ۸۰۲.۱۱ نمونه هایی از ایستگاه های پایه هستند.

در شکل ۷.۱، ایستگاه پایه به شبکه بزرگتر (به عنوان مثال، اینترنت، شبکه شرکتی یا خانگی) متصل است، بنابراین به عنوان یک رله لایه پیوند بین میزبان بی سیم و بقیه جهان که میزبان با آن ارتباط برقرار می کند، عمل می کند.

میزبان های مرتبط با یک ایستگاه پایه اغلب به عنوان کار در حالت زیرساخت نامیده می شوند، زیرا تمام خدمات شبکه سنتی (به عنوان مثال، تخصیص آدرس و مسیریابی) توسط شبکه ای که میزبان از طریق ایستگاه پایه به آن متصل است، ارائه می شود. در شبکه های ad hoc، هاست های بی سیم چنین زیرساختی برای اتصال ندارند. در غیاب چنین زیرساختی، خود هاست ها باید خدماتی مانند مسیریابی، تخصیص آدرس، ترجمه نام شبیه به DNS و غیره را ارائه دهند.

هنگامی که یک میزبان سیار از محدوده یک ایستگاه پایه فراتر می رود و به محدوده دیگری می رود، نقطه اتصال خود را به شبکه بزرگتر تغییر می دهد (یعنی ایستگاه پایه ای که با آن مرتبط است را تغییر می دهد) - فرآیندی که به آن انتقال داده می شود. یا واگذاری چنین تحرکی سوالات چالش برانگیزی را ایجاد می کند. اگر میزبانی بتواند جابجا شود، چگونه می توان مکان فعلی میزبان تلفن همراه را در شبکه پیدا کرد تا بتوان داده ها را به آن میزبان تلفن همراه ارسال کرد؟ با توجه به اینکه یک میزبان می تواند در یکی از مکان های ممکن باشد، آدرس دهی چگونه انجام می شود؟ اگر هاست در حین اتصال TCP یا تماس تلفنی حرکت کند، داده ها چگونه مسیریابی می شوند تا اتصال بدون وقفه ادامه یابد؟ اینها و بسیاری (بسیاری!) سوالات دیگر، شبکه های بی سیم و تلفن همراه را به حوزه ای برای تحقیقات شبکه هیجان انگیز تبدیل می کند.

• زیرساخت شبکه. این شبکه بزرگ تری است که میزبان بی سیم ممکن است بخواهد با آن ارتباط برقرار کند. پس از بحث در مورد "قطعات" یک شبکه بی سیم، خاطرنشان می کنیم که این قطعات را می توان به روش های مختلف ترکیب کرد تا انواع مختلفی از شبکه های بی سیم را تشکیل دهد. ممکن است همانطور که در این فصل می خوانید، طبقه بندی این نوع شبکه های بی سیم مفید باشد، یا فراتر از این کتاب درباره شبکه های بی سیم بیشتر بخوانید/بیاموزید. در بالاترین سطح می توانیم شبکه های بی سیم را بر اساس دو معیار طبقه بندی کنیم: (i) اینکه آیا یک بسته در شبکه بی سیم دقیقاً از یک پرش بی سیم یا چند پرش بی سیم عبور می کند، و (۲) آیا زیرساختی مانند یک ایستگاه پایه در شبکه وجود دارد یا خیر. :

• تک هاپ، مبتنی بر زیرساخت. این شبکه ها دارای یک ایستگاه پایه هستند که به یک شبکه سیمی بزرگتر (مثلاً اینترنت) متصل است. علاوه بر این، تمام ارتباطات بین این ایستگاه پایه و یک میزبان بی سیم از طریق یک پرش بی سیم است. شبکه های ۸۰۲.۱۱ که در کلاس، کافه یا کتابخانه استفاده می کنید. و شبکه های داده G ۴ LTE که به زودی در مورد آنها خواهیم آموخت، همگی در این دسته قرار می گیرند. اکثریت قریب به اتفاق تعاملات روزانه ما با شبکه های بی سیم تک هاپ و مبتنی بر زیرساخت است.

• تک هاپ، بدون زیرساخت. در این شبکه ها هیچ ایستگاه پایه ای که به شبکه بی سیم متصل باشد وجود ندارد. با این حال، همانطور که خواهیم دید، یکی از گره ها در این شبکه تک هاپ ممکن است انتقال گره های دیگر را هماهنگ کند. شبکه های بلوتوث (که دستگاه های بی سیم کوچکی مانند صفحه کلید، بلندگوها و هدست ها را به هم متصل می کنند و در بخش ۷.۳.۶ بررسی خواهیم کرد) شبکه های تک هاپ و بدون زیرساخت هستند.

• چند هاپ، مبتنی بر زیرساخت. در این شبکه ها، یک ایستگاه پایه وجود دارد که به شبکه بزرگتر متصل است. با این حال، برخی از گره های بی سیم ممکن است مجبور شوند ارتباط خود را از طریق گره های بی سیم دیگر رله کنند تا از طریق ایستگاه پایه ارتباط برقرار کنند. برخی از شبکه های حسگر بی سیم و به اصطلاح شبکه های مش بی سیم مستقر در خانه ها در این دسته قرار می گیرند.

• چند پرش، بدون زیرساخت. هیچ ایستگاه پایه ای در این شبکه ها وجود ندارد و گره ها برای رسیدن به مقصد ممکن است مجبور شوند پیام ها را بین چندین گره دیگر ارسال کنند. گره ها همچنین ممکن است متحرک باشند، با تغییر اتصال بین گره ها - دسته ای از شبکه ها که به عنوان شبکه های ad hoc موبایل (MANET) شناخته می شوند. اگر گره های سیار وسایل نقلیه باشند، شبکه یک شبکه موردی خودرویی (VANET) است. همانطور که ممکن است تصور کنید، توسعه پروتکل ها برای چنین شبکه هایی چالش برانگیز است و موضوع تحقیقات مداوم بسیاری است. در این فصل، ما بیشتر خود را به شبکه های تک هاپ و سپس بیشتر به شبکه های مبتنی بر زیرساخت محدود می کنیم.

اکنون بیایید به چالش های فنی که در شبکه های بی سیم و تلفن همراه به وجود می آیند، عمیق تر بپردازیم. ابتدا پیوند بی سیم فردی را در نظر می گیریم و بحث خود را در مورد تحرک به بعد در این فصل ماکول می کنیم.

۷.۲ لینک های بی سیم و ویژگی های شبکه

لینک های بی سیم از چند جنبه مهم با همتایان سیمی خود متفاوت هستند:

- کاهش قدرت سیگنال. تشعشعات الکترومغناطیسی با عبور از ماده (به عنوان مثال، سیگنال رادیویی که از دیوار عبور می کند) کاهش می یابد. حتی در فضای آزاد، سیگنال پراکنده می شود و در نتیجه با افزایش فاصله بین فرستنده و گیرنده، قدرت سیگنال کاهش می یابد (که گاهی اوقات از دست دادن مسیر نامیده می شود).

- تداخل از منابع دیگر. منابع رادیویی که در همان باند فرکانسی ارسال می شوند با یکدیگر تداخل خواهند داشت. به عنوان مثال، تلفن های بی سیم ۲.۴ گیگاهرتز و شبکه های محلی بی سیم ۸۰۲.۱۱ b در یک باند فرکانسی ارسال می کنند. بنابراین، کاربر LAN بی سیم ۸۰۲.۱۱ b که با تلفن بی سیم ۲.۴ گیگاهرتز صحبت می کند، می تواند انتظار داشته باشد که نه شبکه و نه تلفن عملکرد خوبی نداشته باشند. علاوه بر تداخل منابع انتقال، نویز الکترومغناطیسی در محیط (مثلاً یک موتور نزدیک، یک مایکروویو) می تواند منجر به تداخل شود. به همین دلیل، تعدادی از استانداردهای جدیدتر ۸۰۲.۱۱ b در باند فرکانسی ۵ گیگاهرتز کار می کنند.

- انتشار چند مسیره. انتشار چند مسیره زمانی اتفاق می افتد که بخش هایی از موج الکترومغناطیسی از اجسام و زمین منعکس می شود و مسیرهایی با طول های مختلف بین فرستنده و گیرنده طی می کند. این باعث تار شدن سیگنال دریافتی در گیرنده می شود. جابجایی اشیاء بین فرستنده و گیرنده می تواند باعث شود که انتشار چند مسیری در طول زمان تغییر کند.

برای بحث مفصل در مورد ویژگی ها، مدل ها و اندازه گیری های کانال بی سیم، [Anderson 1995; آلمرز ۲۰۰۷]. بحث بالا نشان می دهد که خطاهای بیت در پیوندهای بی سیم بیشتر از پیوندهای سیمی رایج است. به همین دلیل، شاید تعجب آور نباشد که پروتکل های پیوند بی سیم (مانند پروتکل ۸۰۲.۱۱ b که در بخش بعدی بررسی خواهیم کرد) نه تنها از کدهای تشخیص خطای قدرتمند CRC، بلکه از پروتکل های انتقال داده قابل اعتماد سطح پیوند نیز استفاده می کنند که دوباره ارسال می کنند. فریم های خراب

با در نظر گرفتن آسیب هایی که ممکن است در یک کانال بی سیم رخ دهد، اجازه دهید توجه خود را به میزبانی که سیگنال بی سیم را دریافت می کند معطوف کنیم. این میزبان یک سیگنال الکترومغناطیسی دریافت می کند که ترکیبی از شکل تخریب شده سیگنال اصلی است که توسط فرستنده ارسال می شود (به دلیل اثرات تضعیف و انتشار چند مسیری که در بالا مورد بحث قرار گرفتیم) و نویز پس زمینه در محیط. نسبت سیگنال به نویز (SNR) اندازه گیری نسبی قدرت سیگنال دریافتی (یعنی اطلاعات در حال ارسال) و این نویز است. SNR معمولاً با واحد دسی بل (dB) اندازه گیری می شود، واحد اندازه گیری که برخی فکر می کنند مهندسان برق در درجه اول برای سردرگمی

دانشمندان کامپیوتر از آن استفاده می کنند. SNR که در دسی بل اندازه گیری می شود، ۲۰ برابر نسبت لگاریتم پایه ۱۰ دامنه سیگنال دریافتی به دامنه نویز است. برای اهداف ما در اینجا، فقط باید بدانیم که یک SNR بزرگتر، استخراج سیگنال ارسالی از نویز پس زمینه را برای گیرنده آسان تر می کند.

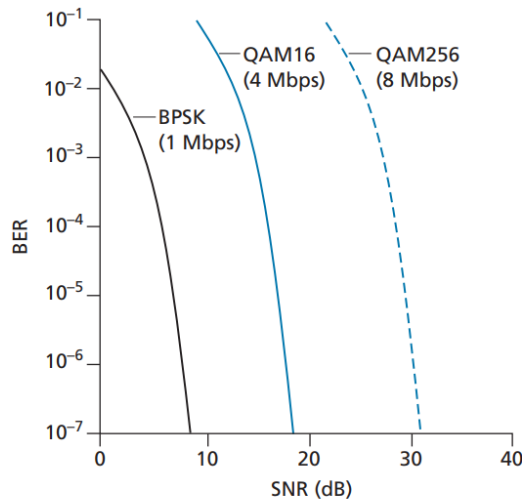


Figure 7.3 ♦ Bit error rate, transmission rate, and SNR

شکل ۷.۳ (اقتباس از [Holland 2001]) نرخ خطای بیت (BER) را نشان می دهد - به طور کلی، احتمال اینکه یک بیت ارسالی به اشتباه در گیرنده دریافت شود - در مقابل SNR برای سه تکنیک مدولاسیون مختلف برای رمزگذاری اطلاعات برای انتقال در یک کانال بی سیم ایده آل تئوری مدولاسیون و کدگذاری، و همچنین استخراج سیگنال و BER، بسیار فراتر از محدوده این متن است (برای بحث در مورد این موضوعات به [Schwartz 1980; Goldsmith 2005] مراجعه کنید). با این وجود، شکل ۷.۳ چندین ویژگی لایه فیزیکی را نشان می دهد که در درک پروتکل های ارتباطی بی سیم لایه بالاتر مهم هستند:

- برای یک طرح مدولاسیون معین، هر چه SNR بیشتر باشد، BER کمتر است. از آنجایی که یک فرستنده می تواند SNR را با افزایش توان انتقال خود افزایش دهد، یک فرستنده می تواند با افزایش قدرت انتقال فریم، احتمال دریافت اشتباه فریم را کاهش دهد. با این حال، توجه داشته باشید که احتمالاً سود عملی کمی در افزایش توان فراتر از یک آستانه خاص، مثلاً کاهش BER از ۱۰^{-۲} به ۱۰^{-۳} وجود دارد. همچنین معایبی در ارتباط با افزایش توان انتقال وجود دارد: انرژی بیشتری باید توسط فرستنده صرف شود (یک نگرانی مهم برای کاربران موبایلی که با باتری کار می کنند)، و انتقال فرستنده بیشتر در انتقال فرستنده دیگر تداخل ایجاد می کند (شکل ۷.۴ را ببینید). (ب).
- برای یک SNR معین، یک تکنیک مدولاسیون با نرخ انتقال بیت بالاتر (چه در اشتباه باشد چه نباشد) BER بالاتری خواهد داشت. به عنوان مثال، در شکل ۷.۳، با SNR 10 دسی بل، مدولاسیون BPSK با نرخ انتقال ۱ مگابیت در ثانیه دارای BER کمتر از ۱۰^{-۷} است، در حالی که با مدولاسیون QAM16 با سرعت انتقال ۴ مگابیت در ثانیه،

BER 10- است. ۱، بسیار بالا است که عملاً مفید باشد. با این حال، با SNR 20 دسی بل، مدولاسیون QAM16 دارای نرخ انتقال ۴ مگابیت بر ثانیه و BER 10-7 است، در حالی که مدولاسیون BPSK دارای نرخ انتقال تنها ۱ مگابیت در ثانیه و BER است که آنقدر پایین است که (به معنای واقعی کلمه) "خارج از نمودار." اگر کسی بتواند BER 10-7 را تحمل کند، نرخ انتقال بالاتر ارائه شده توسط QAM16 آن را به تکنیک مدولاسیون ترجیحی در این شرایط تبدیل می کند. این ملاحظات منجر به مشخصه نهایی می شود که در ادامه توضیح داده می شود.

• انتخاب دینامیکی تکنیک مدولاسیون لایه فیزیکی می تواند برای تطبیق تکنیک مدولاسیون با شرایط کانال استفاده شود. SNR (و در نتیجه BER) ممکن است در نتیجه تحرک یا به دلیل تغییرات در محیط تغییر کند. مدولاسیون و کدگذاری تطبیقی در وای فای ۸۰۲.۱۱ و در شبکه های داده سلولی G4 و G5 استفاده می شود که در بخش های ۷.۳ و ۷.۴ مطالعه خواهیم کرد. به عنوان مثال، این امکان انتخاب یک تکنیک مدولاسیون را فراهم می کند که بالاترین نرخ انتقال ممکن را با توجه به محدودیتی در BER برای ویژگی های کانال داده شده فراهم می کند. نرخ خطای بیت بالاتر و متغیر با زمان تنها تفاوت بین پیوند سیمی و بی سیم نیست. به یاد بیاورید که در مورد پیوندهای پخش سیمی، همه گره ها ارسال ها را از تمام گره های دیگر دریافت می کنند. در مورد پیوندهای بی سیم، وضعیت به همین سادگی نیست، همانطور که در شکل ۷.۴ نشان داده شده است. فرض کنید که ایستگاه A در حال انتقال به ایستگاه B است. همچنین فرض کنید که ایستگاه C در حال انتقال به ایستگاه B است. با به اصطلاح مشکل پایانه پنهان، موانع فیزیکی در محیط (به عنوان مثال، یک کوه یا یک ساختمان) ممکن است مانع A و C شوند. از شنیدن ارسال های یکدیگر، حتی اگر ارسال های A و C در واقع در مقصد تداخل داشته باشند، B. این در شکل ۷.۴ (a) نشان داده شده است. سناریوی دومی که منجر به برخوردهای غیرقابل تشخیص در گیرنده می شود، ناشی از کمرنگ شدن قدرت سیگنال در حین انتشار از طریق رسانه بی سیم است. شکل ۷.۴ (ب) حالتی را نشان می دهد که در آن A و C به گونه ای قرار می گیرند که سیگنال های آن ها به اندازه کافی قوی نیستند تا انتقال های یکدیگر را شناسایی کنند، اما سیگنال های آن ها به اندازه ای قوی هستند که در ایستگاه B با یکدیگر تداخل کنند. همانطور که در بخش خواهیم دید، ۷.۳، مشکل ترمینال پنهان و محو شدن، دسترسی چندگانه را در یک شبکه بی سیم به طور قابل توجهی پیچیده تر از یک شبکه سیمی می کند.

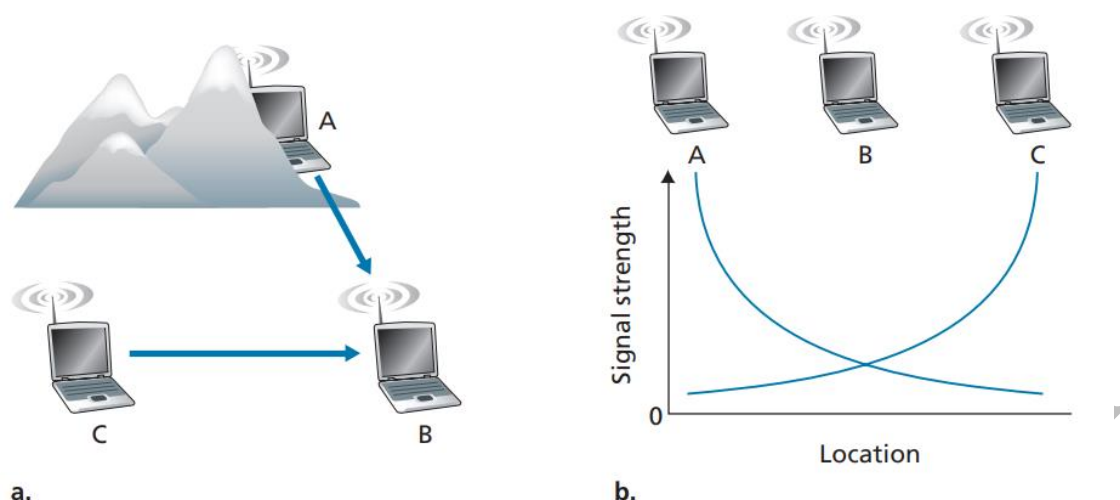


Figure 7.4 ♦ Hidden terminal problem caused by obstacle (a) and fading (b)

CDMA ۷.۲.۱

از فصل ۶ به یاد بیاورید که وقتی میزبان‌ها از طریق یک رسانه مشترک با هم ارتباط برقرار می‌کنند، یک پروتکل مورد نیاز است تا سیگنال‌های ارسال شده توسط چندین فرستنده در گیرنده‌ها تداخل نداشته باشند. در فصل ۶، سه دسته از پروتکل‌های دسترسی متوسط را شرح دادیم: پارتیشن بندی کانال، دسترسی تصادفی، و به نوبت. دسترسی چندگانه تقسیم کد (CDMA) به خانواده پروتکل‌های پارتیشن بندی کانال تعلق دارد. در LAN بی سیم و فناوری‌های سلولی رایج است. از آنجایی که CDMA در دنیای بی سیم بسیار مهم است، پیش از ورود به فناوری‌های دسترسی بی سیم خاص در بخش‌های بعدی، اکنون نگاهی گذرا به CDMA خواهیم داشت.

در یک پروتکل CDMA، هر بیت ارسالی با ضرب بیت در یک سیگنال (کد) که با سرعت بسیار بیشتری (معروف به نرخ تراشه) نسبت به دنباله اصلی بیت‌های داده تغییر می‌کند، کدگذاری می‌شود. شکل ۷.۵ یک سناریوی کدگذاری/رمزگشایی CDMA ساده و ایده آل را نشان می‌دهد. فرض کنید سرعتی که بیت‌های داده اصلی به رمزگذار CDMA می‌رسند، واحد زمان را مشخص می‌کند. یعنی هر بیت داده اصلی برای انتقال نیاز به زمان اسلات یک بیتی دارد. اجازه دهید مقدار بیت داده برای شکاف بیت آن باشد. برای راحتی ریاضی، یک بیت داده را با مقدار $0-1$ نشان می‌دهیم. هر شکاف بیت بیشتر به شکاف‌های کوچک M تقسیم می‌شود. در شکل ۷.۵، $M = 8$ ، اگرچه در عمل M بسیار بزرگتر است. کد CDMA که توسط فرستنده استفاده می‌شود متشکل از دنباله‌ای از مقادیر M ، c_m ، $m = 1, \dots, M$ ، هر کدام یک مقدار 1 یا -1 می‌گیرند. در مثال شکل ۷.۵، کد CDMA M -bit که توسط فرستنده استفاده می‌شود $(1, 1, 1, -1, -1, -1, -1, 1)$ است.

برای نشان دادن نحوه کار CDMA، اجازه دهید روی بیت i th داده تمرکز کنیم، d_i . برای مینی اسلات m th زمان انتقال بیت d_i ، خروجی رمزگذار CDMA، $Z_{i,m}$ ، مقدار d_i ضرب در بیت m th در کد اختصاص داده شده، c_m است:

$$Z_{i,m} = d_i * c_m \quad (7.1)$$

در یک دنیای ساده، بدون فرستنده مزاحم، گیرنده بیت های کدگذاری شده، $Z_{i,m}$ را دریافت می کند و بیت داده اصلی، d_i ، را با محاسبه:

$$d_i = \frac{1}{M} \sum_{m=1}^M Z_{i,m} * c_m \quad (7.2)$$

خواننده ممکن است بخواهد روی جزئیات مثال در شکل ۷.۵ کار کند تا ببیند که بیت های داده اصلی واقعاً به درستی در گیرنده با استفاده از معادله ۷.۲ بازیابی شده اند.

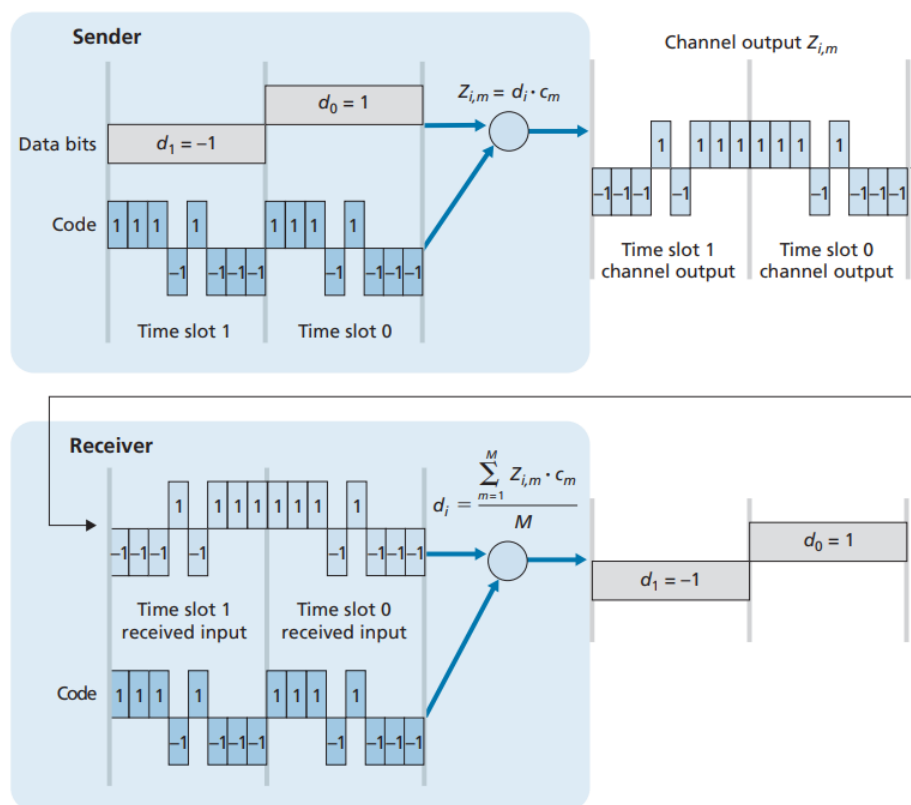


Figure 7.5 ♦ A simple CDMA example: Sender encoding, receiver decoding

با این حال، جهان از ایده آل فاصله زیادی دارد، و همانطور که در بالا ذکر شد، CDMA باید در حضور فرستنده های مزاحم که داده های خود را با استفاده از کد اختصاص داده شده دیگری رمزگذاری و انتقال می دهند، کار کند. اما چگونه یک گیرنده CDMA می تواند بیت های داده اصلی فرستنده را بازیابی کند، در حالی که این بیت های داده با بیت هایی که توسط فرستنده های دیگر منتقل می شوند درهم می آیند؟ CDMA با این فرض کار می کند که

سیگنال های بیت ارسالی تداخلی افزودنی هستند. این بدان معناست که برای مثال، اگر سه فرستنده مقدار ۱ را ارسال کنند و فرستنده چهارم مقدار ۱- را در همان اسلات کوچک ارسال کند، سیگنال دریافتی در تمام گیرنده‌ها در طول آن شکاف کوچک ۲ است (از $1 - 1 + 1 + 1 = 2$). در حضور چندین فرستنده، فرستنده s ارسال های رمزگذاری شده خود، $Z_{i,m}^s$ را دقیقاً به همان روشی که در معادله ۷.۱ محاسبه می کند. با این حال، مقدار دریافتی در یک گیرنده در طول مینی اسلات یکمین شکاف بیتی، اکنون مجموع بیت های ارسالی از همه N فرستنده در طول آن شکاف کوچک است:

$$Z_{i,m}^* = \sum_{s=1}^N Z_{i,m}^s$$

به طور شگفت انگیزی، اگر کدهای فرستنده با دقت انتخاب شوند، هر گیرنده می تواند داده های ارسال شده توسط فرستنده معین را از سیگنال کل به سادگی با استفاده از کد فرستنده دقیقاً به همان روشی که در معادله ۷.۲ درج شده است، بازیابی کند:

$$d_i = \frac{1}{M} \sum_{m=1}^M Z_{i,m}^* \cdot c_m \quad (7.3)$$

همانطور که در شکل ۷.۶ برای مثال CDMA دو فرستنده نشان داده شده است. کد CDMA M بیتی که توسط فرستنده بالایی استفاده می شود $(1, 1, 1, -1, -1, -1, 1, -1)$ است، در حالی که کد CDMA که توسط فرستنده پایین استفاده می شود $(1, -1, 1, 1, -1, 1, 1, -1)$ است. شکل ۷.۶ دریافت کننده ای را نشان می دهد که بیت های داده اصلی را از فرستنده بالایی بازیابی می کند. توجه داشته باشید که گیرنده قادر است داده ها را از فرستنده ۱ استخراج کند، علیرغم اینکه ارسال تداخلی از فرستنده ۲ وجود دارد.

تشبیه کوکتل ما را از فصل ۶ به یاد بیاورید. یک پروتکل CDMA شبیه به صحبت کردن مهمانداران به چندین زبان است. در چنین شرایطی، انسان‌ها در قفل کردن مکالمه به زبانی که می فهمند، در حالی که مکالمات باقی مانده را فیلتر می کنند، کاملاً خوب هستند. در اینجا می بینیم که CDMA یک پروتکل پارتیشن بندی است که فضای کد را پارتیشن بندی می کند (بر خلاف زمان یا فرکانس) و به هر گره یک قطعه اختصاصی از فضای کد اختصاص می دهد.

بحث ما در اینجا در مورد CDMA لزوماً مختصر است. در عمل باید به تعدادی از مسائل دشوار پرداخته شود. ابتدا، برای اینکه گیرنده های CDMA بتوانند سیگنال فرستنده خاصی را استخراج کنند، کدهای CDMA باید با دقت انتخاب شوند. دوم، بحث ما فرض کرده است که قدرت سیگنال دریافتی از فرستنده های مختلف یکسان است.

در واقعیت، دستیابی به این امر می تواند دشوار باشد. ادبیات قابل توجهی وجود دارد که به این مسائل و سایر مسائل مربوط به CDMA می پردازد. [Pickholtz 1982; Viterbi 1995] برای جزئیات.

۷.۳ 802.11 WiFi : شبکه های محلی بی سیم

شبکه های محلی بی سیم که در محیط کار، خانه، موسسات آموزشی، کافه ها، فرودگاه ها و گوشه و کنار خیابان ها فراگیر شده اند، اکنون یکی از مهم ترین فناوری های شبکه دسترسی در اینترنت هستند. اگرچه بسیاری از فناوری ها و استانداردها برای شبکه های محلی بی سیم در دهه ۱۹۹۰ توسعه یافتند، یک کلاس خاص از استانداردها به وضوح به عنوان برنده ظاهر شد: IEEE 802.11 LAN بی سیم، همچنین به عنوان WiFi شناخته می شود. در این بخش، نگاهی دقیق به شبکه های محلی بی سیم ۸۰۲.۱۱ خواهیم داشت، ساختار فریم، پروتکل دسترسی متوسط آن، و کار اینترنتی آن با شبکه های محلی ۸۰۲.۱۱ با شبکه های اترنت سیمی را بررسی می کنیم.

همانطور که در جدول ۷.۱ خلاصه شده است، چندین استاندارد ۸۰۲.۱۱ وجود دارد. [IEEE 802.11 2020] 802.11 b, g, n, ac, ax نسل های متوالی فناوری ۸۰۲.۱۱ هستند که برای شبکه های محلی بی سیم (WLAN) هدف قرار می گیرند که معمولاً برد کمتر از ۷۰ متر در دفتر خانه، محل کار یا محیط تجاری دارند. استانداردهای ۸۰۲.۱۱ ax و ac اخیراً به ترتیب به عنوان WiFi 4، ۵ و ۶ نامگذاری شده اند که بدون شک با نام تجاری شبکه سلولی 4G و 5G رقابت می کنند. استانداردهای ۸۰۲.۱۱ af, ah در فواصل طولانی تر عمل می کنند و هدفشان اینترنت اشیاء، شبکه های حسگر و برنامه های اندازه گیری است.

استانداردهای مختلف ۸۰۲.۱۱ ax, ac, n, g, b همگی دارای ویژگی های مشترک هستند، از جمله فرمت فریم ۸۰۲.۱۱ که به زودی مطالعه خواهیم کرد، و سازگار با عقب هستند، به این معنی که برای مثال، موبایلی که فقط قادر به ۸۰۲.۱۱ گرم است ممکن است همچنان با ایستگاه پایه ۸۰۲.۱۱ ac یا ۸۰۲.۱۱ ax جدیدتر تعامل داشته باشید. همچنین همه آنها از یک پروتکل دسترسی متوسط، CSMA/CA استفاده می کنند که به زودی در مورد آن صحبت خواهیم کرد، در حالی که ۸۰۲.۱۱ ax نیز از برنامه ریزی متمرکز توسط ایستگاه پایه انتقال از دستگاه های بی سیم مرتبط پشتیبانی می کند.

با این حال، همانطور که در جدول ۷.۱ نشان داده شده است، استانداردها تفاوت های عمده ای در لایه فیزیکی دارند. دستگاه های ۸۰۲.۱۱ در دو محدوده فرکانس مختلف کار می کنند: ۲.۴-۲.۴۸۵ گیگاهرتز (به عنوان محدوده ۲.۴ گیگاهرتز شناخته می شود) و ۵.۱-۵.۸ گیگاهرتز (به عنوان محدوده ۵ گیگاهرتز شناخته می شود). محدوده ۲.۴ گیگاهرتز یک باند فرکانسی بدون مجوز است که در آن ۸۰۲.۱۱ دستگاه ممکن است برای طیف فرکانس با تلفن های

۲.۴ گیگاهرتز و وسایلی مانند اجاق های مایکروویو رقابت کنند. در فرکانس ۵ گیگاهرتز، شبکه های محلی ۸۰۲.۱۱ فاصله انتقال کمتری برای یک سطح توان معین دارند و از انتشار چند مسیر به بیشتر رنج می برند. استانداردهای ۸۰۲.۱۱n، ۸۰۲.۱۱ac، و ۸۰۲.۱۱ax از آنتن های چند خروجی چند ورودی (MIMO) استفاده می کنند. یعنی دو یا چند آنتن در سمت فرستنده و دو یا چند آنتن در سمت گیرنده که سیگنال های متفاوتی را ارسال/دریافت می کنند [Diggavi 2004].

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11 b	1999	11 Mbps	30 m	2.4 Ghz
802.11 g	2003	54 Mbps	30 m	2.4 Ghz
802.11 n (WiFi 4)	2009	600	70 m	2.4, 5 Ghz
802.11 ac (WiFi 5)	2013	3.47 Gbps	70 m	5 Ghz
802.11 ax (WiFi 6)	2020 (expected)	14 Gbps	70 m	2.4, 5 Ghz
802.11 af	2014	35–560 Mbps	1 Km	unused TV bands (54–790 MHz)
802.11 ah	2017	347 Mbps	1 Km	900 Mhz

Table 7.1 ♦ Summary of IEEE 802.11 standards

ایستگاه های پایه محور ۸۰۲.۱۱ac و ۸۰۲.۱۱ ممکن است به چندین ایستگاه به طور همزمان ارسال کنند و از آنتن های "هوشمند" برای شکل دهی پرتوهای تطبیقی برای هدف قرار دادن انتقال در جهت گیرنده استفاده کنند. این امر تداخل را کاهش می دهد و مسافتی را که در یک نرخ داده معین به دست می آید افزایش می دهد. نرخ داده نشان داده شده در جدول ۷.۱ برای یک محیط ایده آل است، به عنوان مثال، یک گیرنده نزدیک به ایستگاه پایه، بدون تداخل - سناریویی که بعید است در عمل آن را تجربه کنیم! بنابراین همانطور که گفته می شود، YMMV: مسافت پیموده شده (یا در این مورد نرخ داده بی سیم شما) ممکن است متفاوت باشد.

۷.۳.۱ معماری LAN بی سیم ۸۰۲.۱۱

شکل ۷.۷ اجزای اصلی معماری LAN بی سیم ۸۰۲.۱۱ را نشان می دهد. بلوک اصلی ساختمان معماری ۸۰۲.۱۱ مجموعه خدمات پایه (BSS) است. یک BSS شامل یک یا چند ایستگاه بی سیم و یک ایستگاه پایه مرکزی است که در اصطلاح ۸۰۲.۱۱ به عنوان نقطه دسترسی (AP) شناخته می شود. شکل ۷.۷ AP را در هر یک از دو BSS که به یک دستگاه اتصال (مانند سوئیچ یا روتر) متصل می شوند، نشان می دهد که به نوبه خود به اینترنت منتهی می شود. در یک شبکه خانگی معمولی، یک AP و یک روتر (معمولاً به عنوان یک واحد با هم یکپارچه شده اند) وجود دارد که BSS را به اینترنت متصل می کند.

مانند دستگاه های اترنت، هر ایستگاه بی سیم ۸۰۲.۱۱ دارای یک آدرس MAC 6 بایتی است که در سیستم عامل آداپتور ایستگاه (یعنی کارت رابط شبکه ۸۰۲.۱۱) ذخیره می شود. هر AP همچنین یک آدرس MAC برای رابط بی سیم خود دارد. همانند اترنت، این آدرس های MAC توسط IEEE اداره می شوند و (در تئوری) در سطح جهانی منحصر به فرد هستند.

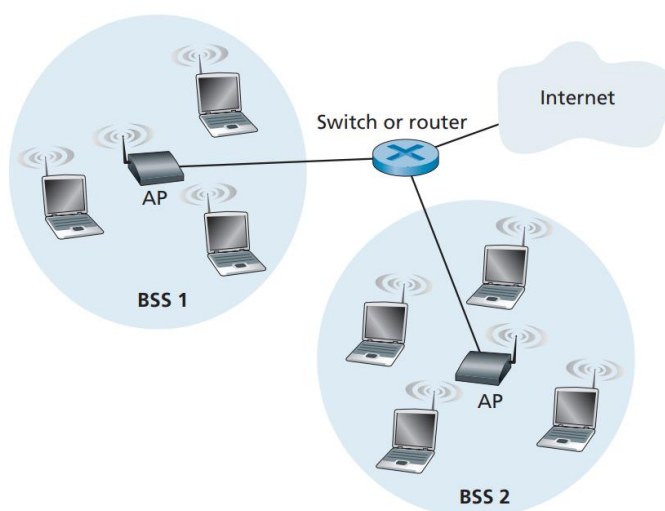


Figure 7.7 ♦ IEEE 802.11 LAN architecture

همانطور که در بخش ۷.۱ اشاره شد، شبکه های محلی بی سیمی که AP ها را مستقر می کنند، اغلب به عنوان شبکه های محلی بی سیم زیرساخت نامیده می شوند، با "زیرساخت" AP ها به همراه زیرساخت اترنت سیمی که AP ها و یک روتر را به هم متصل می کند.

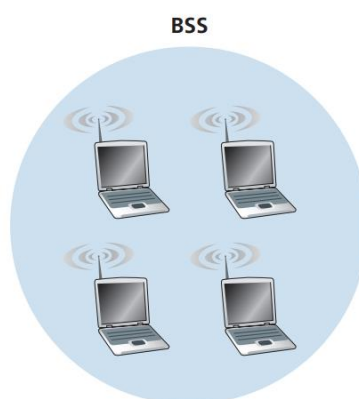


Figure 7.8 ♦ An IEEE 802.11 ad hoc network

شکل ۷.۸ نشان می دهد که ایستگاه های IEEE 802.11 می توانند خود را با هم گروه بندی کنند تا یک شبکه ad hoc را تشکیل دهند - شبکه ای بدون کنترل مرکزی و بدون اتصال به "جهان بیرون". در اینجا، شبکه «در حال پرواز» توسط دستگاه های تلفن همراهی شکل می گیرد که خود را در مجاورت یکدیگر یافته اند، نیاز به برقراری ارتباط دارند و هیچ زیرساخت شبکه از قبل موجود در محل خود پیدا نمی کنند. هنگامی که افراد دارای لپ تاپ دور هم جمع

می‌شوند (مثلاً در یک اتاق کنفرانس، قطار یا ماشین) و می‌خواهند در غیاب یک AP متمرکز، داده‌ها را مبادله کنند، ممکن است یک شبکه ad hoc تشکیل شود. از آنجایی که دستگاه‌های قابل حمل ارتباطی همچنان در حال گسترش هستند، علاقه زیادی به شبکه‌های ad hoc وجود دارد. در این بخش، با این حال، ما توجه خود را بر زیرساخت‌های شبکه‌های بی‌سیم متمرکز خواهیم کرد.

کانال‌ها و انجمن

در ۸۰۲.۱۱، هر ایستگاه بی‌سیم قبل از اینکه بتواند داده‌های لایه شبکه را ارسال یا دریافت کند، باید با یک AP مرتبط شود. اگرچه همه استانداردهای ۸۰۲.۱۱ از ارتباط استفاده می‌کنند، ما این موضوع را به طور خاص در زمینه IEEE 802.11b، g، n، ac، ax مورد بحث قرار خواهیم داد.

هنگامی که یک مدیر شبکه یک AP را نصب می‌کند، مدیر یک یا دو کلمه شناسه مجموعه خدمات (SSID) را به نقطه دسترسی اختصاص می‌دهد. (به عنوان مثال، وقتی Wi-Fi را در زیر تنظیمات در iPhone خود انتخاب می‌کنید، لیستی نمایش داده می‌شود که SSID هر AP در محدوده را نشان می‌دهد.) مدیر همچنین باید یک شماره کانال به AP اختصاص دهد. برای درک اعداد کانال، به یاد بیاورید که ۸۰۲.۱۱ در محدوده فرکانس ۲.۴ گیگاهرتز تا ۲.۴۸۳۵ گیگاهرتز کار می‌کند. در این باند ۸۵ مگاهرتز، ۸۰۲.۱۱ ۱۱ کانال تا حدی همپوشانی را تعریف می‌کند. هر دو کانال همپوشانی ندارند اگر و فقط در صورتی که با چهار یا چند کانال از هم جدا شوند. به طور خاص، مجموعه کانال‌های ۱، ۶ و ۱۱ تنها مجموعه‌ای از سه کانال غیر همپوشانی است. این بدان معناست که یک مدیر می‌تواند با نصب سه AP 802.11 در یک مکان فیزیکی، و اختصاص کانال‌های ۱، ۶ و ۱۱ به AP‌ها، یک شبکه محلی بی‌سیم با حداکثر نرخ انتقال سه برابر حداکثر نرخ انتقال نشان‌داده‌شده در جدول ۷.۱ ایجاد کند. و اتصال هر یک از AP‌ها با یک سوئیچ.

اکنون که درک اولیه‌ای از کانال‌های ۸۰۲.۱۱ داریم، بیا یک موقعیت جالب (و نه کاملاً غیر معمول) را شرح دهیم - وضعیت جنگل Wi-Fi. جنگل Wi-Fi هر مکان فیزیکی است که در آن یک ایستگاه بی‌سیم سیگنال به اندازه کافی قوی از دو یا چند AP دریافت می‌کند. برای مثال، در بسیاری از کافه‌ها در شهر نیویورک، یک ایستگاه بی‌سیم می‌تواند سیگنالی را از چندین AP‌های مجاور دریافت کند. یکی از AP‌ها ممکن است توسط کافه مدیریت شود، در حالی که سایر AP‌ها ممکن است در آپارتمان‌های مسکونی نزدیک کافه باشند. هر یک از این AP‌ها احتمالاً در یک زیرشبکه IP متفاوت قرار دارند و به طور مستقل یک کانال به آنها اختصاص داده شده است.

حالا فرض کنید با گوشی هوشمند، تبلت یا لپ تاپ خود وارد چنین جنگل وای فای شده اید و به دنبال دسترسی به اینترنت بی سیم و یک مافین بلوبری هستید. فرض کنید پنج AP در جنگل WiFi وجود دارد. برای دسترسی به اینترنت، دستگاه بی سیم شما باید دقیقاً به یکی از زیرشبکه ها بپیوندد و از این رو باید دقیقاً با یکی از AP ها مرتبط شود. Associating به این معنی است که دستگاه بی سیم یک سیم مجازی بین خود و AP ایجاد می کند. به طور خاص، فقط AP مرتبط فریم های داده (یعنی فریم های حاوی داده مانند دیتاگرام) را به دستگاه بی سیم شما ارسال می کند و دستگاه بی سیم شما فریم های داده را فقط از طریق AP مرتبط به اینترنت ارسال می کند. اما چگونه دستگاه بی سیم شما با یک AP خاص مرتبط می شود؟ و اساساً، چگونه دستگاه بی سیم شما می داند که کدام AP ها، در صورت وجود، در جنگل وجود دارند؟

استاندارد ۸۰۲.۱۱ مستلزم آن است که یک AP به صورت دوره ای فریم های beacon را ارسال کند که هر کدام شامل آدرس SSID و MAC AP است. دستگاه بی سیم شما، با علم به اینکه AP ها فریم های بیکن را ارسال می کنند، ۱۱ کانال را اسکن می کند و از هر AP هایی که ممکن است وجود داشته باشد، فریم های بیکن را جستجو می کند (برخی از آن ها ممکن است در همان کانال مخابره می کنند—در آنجا جنگلی است!). شما (یا دستگاه بی سیم خود) پس از آشنایی با AP های موجود از فریم های چراغ، یکی از AP ها را برای ارتباط انتخاب می کنید.

استاندارد ۸۰۲.۱۱ الگوریتمی را برای انتخاب کدام یک از AP های موجود برای مرتبط کردن مشخص نمی کند. این الگوریتم به طراحان سیستم عامل و نرم افزار ۸۰۲.۱۱ در دستگاه بی سیم شما واگذار شده است. به طور معمول، دستگاه نقطه ای را انتخاب می کند که فریم بیکن آن با بالاترین قدرت سیگنال دریافت می شود. در حالی که قدرت سیگنال بالا خوب است (به عنوان مثال، شکل ۷.۳ را ببینید)، قدرت سیگنال تنها مشخصه AP نیست که عملکرد دریافتی دستگاه را تعیین می کند. به طور خاص، ممکن است AP انتخاب شده سیگنال قوی داشته باشد، اما ممکن است با سایر دستگاه های وابسته بارگذاری شود (که باید پهنای باند بی سیم را در آن AP به اشتراک بگذارند)، در حالی که یک AP تخلیه نشده به دلیل سیگنال کمی ضعیف تر انتخاب نشده است. بنابراین اخیراً تعدادی روش جایگزین برای انتخاب AP ها پیشنهاد شده است [Vasudevan 2005; نیکلسون ۲۰۰۶; Sundaresan 2006]. برای یک بحث جالب و ساده در مورد چگونگی اندازه گیری قدرت سیگنال، به [Bardwell 2004] مراجعه کنید.

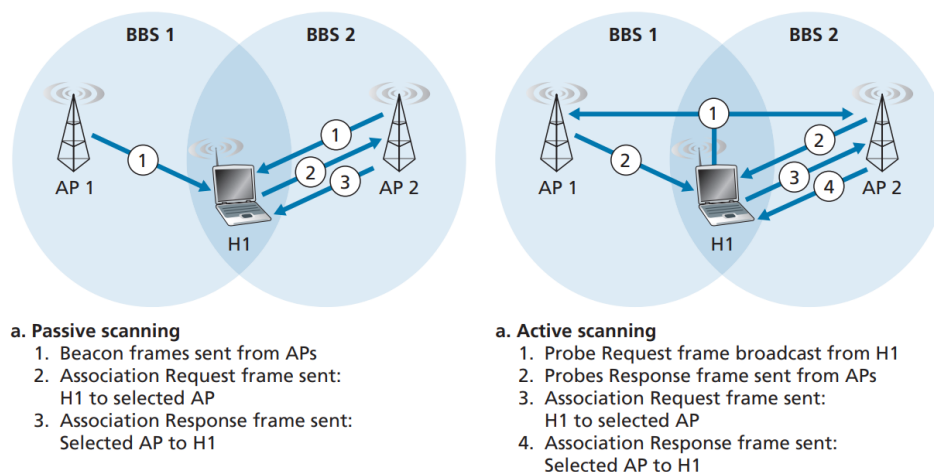


Figure 7.9 ♦ Active and passive scanning for access points

فرآیند اسکن کانال ها و گوش دادن به فریم های بیکن به عنوان اسکن غیرفعال شناخته می شود (شکل ۷.۹a را ببینید). همانطور که در شکل ۷.۹b نشان داده شده است، یک دستگاه بی سیم همچنین می تواند اسکن فعال را با پخش یک قاب پروب انجام دهد که توسط تمام AP ها در محدوده دستگاه بی سیم دریافت می شود. AP ها به چارچوب درخواست پروب با یک قاب پاسخ پروب پاسخ می دهند. سپس دستگاه بی سیم می تواند از میان AP های پاسخ دهنده، AP را انتخاب کند که با آن ارتباط برقرار کند.

پس از انتخاب AP که با آن ارتباط برقرار می شود، دستگاه بی سیم یک فریم درخواست ارتباط را به AP ارسال می کند و AP با یک قاب پاسخ انجمن پاسخ می دهد. توجه داشته باشید که این دومین درخواست/پاسخ دست دادن با اسکن فعال مورد نیاز است، زیرا یک AP که به فریم درخواست کاوش اولیه پاسخ می دهد نمی داند دستگاه با کدام یک از (احتمالاً تعداد زیادی) AP های پاسخ دهنده ارتباط برقرار می کند، تقریباً به روشی مشابه. که یک سرویس گیرنده DHCP می تواند از بین چندین سرور DHCP انتخاب کند (شکل ۴.۲۱ را ببینید). هنگامی که با یک AP مرتبط شد، دستگاه می خواهد به زیر شبکه (به مفهوم آدرس دهی IP در بخش ۴.۳.۳) که AP به آن تعلق دارد، بپیوندد. بنابراین، دستگاه معمولاً یک پیام کشف DHCP (نگاه کنید به شکل ۴.۲۱) از طریق AP به زیر شبکه ارسال می کند تا یک آدرس IP در زیر شبکه به دست آورد. هنگامی که آدرس به دست آمد، بقیه جهان آن دستگاه را به سادگی به عنوان میزبان دیگری با آدرس IP در آن زیر شبکه مشاهده می کنند.

به منظور ایجاد ارتباط با یک AP خاص، ممکن است دستگاه بی سیم مورد نیاز باشد تا خود را در AP تأیید کند. شبکه های محلی بی سیم ۸۰۲.۱۱ تعدادی جایگزین برای احراز هویت و دسترسی فراهم می کنند. یکی از رویکردها که توسط بسیاری از شرکت ها استفاده می شود، اجازه دسترسی به یک شبکه بی سیم بر اساس آدرس MAC دستگاه است. رویکرد دوم که توسط بسیاری از کافی نت ها استفاده می شود، از نام کاربری و رمز عبور استفاده

می کند. در هر دو مورد، AP معمولاً با یک سرور احراز هویت ارتباط برقرار می کند و اطلاعات را بین دستگاه بی سیم و سرور تأیید هویت با استفاده از پروتکلی مانند RADIUS [RFC 2865] یا DIAMETER [RFC 6733] منتقل می کند. جداسازی سرور احراز هویت از AP به یک سرور احراز هویت اجازه می دهد تا به بسیاری از APها سرویس دهد، تصمیمات (اغلب حساس) احراز هویت و دسترسی را در سرور واحد متمرکز می کند و هزینه ها و پیچیدگی AP را پایین نگه می دارد. در فصل ۸ خواهیم دید که پروتکل جدید IEEE 802.11i که جنبه های امنیتی خانواده پروتکل های ۸۰۲.۱۱ را تعریف می کند دقیقاً از این رویکرد استفاده می کند.

۷.۳.۲ پروتکل 802.11 MAC

هنگامی که یک دستگاه بی سیم با یک AP مرتبط می شود، می تواند شروع به ارسال و دریافت فریم های داده به/از نقطه دسترسی کند. اما از آنجایی که چندین دستگاه بی سیم یا خود AP ممکن است بخواهند فریم های داده را همزمان از طریق یک کانال ارسال کنند، یک پروتکل دسترسی چندگانه برای هماهنگ کردن انتقال ها مورد نیاز است. در ادامه، دستگاه ها یا AP را به عنوان «ایستگاه های» بی سیمی که کانال دسترسی چندگانه را به اشتراک می گذارند، معرفی می کنیم. همانطور که در فصل ۶ و بخش ۷.۲.۱ بحث شد، به طور کلی سه کلاس از پروتکل های دسترسی چندگانه وجود دارد: پارتیشن بندی کانال (از جمله CDMA)، دسترسی تصادفی، و به نوبت. با الهام از موفقیت عظیم اترنت و پروتکل دسترسی تصادفی آن، طراحان ۸۰۲.۱۱ یک پروتکل دسترسی تصادفی را برای شبکه های محلی بی سیم ۸۰۲.۱۱ انتخاب کردند. این پروتکل دسترسی تصادفی به عنوان CSMA با اجتناب از برخورد یا به طور خلاصه تر به عنوان CSMA/CA شناخته می شود. مانند CSMA/CD اترنت، "CSMA" در CSMA/CA مخفف "دسترسی چندگانه حس حامل" است، به این معنی که هر ایستگاه قبل از ارسال، کانال را حس می کند و زمانی که کانال مشغول احساس می شود، از ارسال خودداری می کند. اگرچه هم اترنت و هم ۸۰۲.۱۱ از دسترسی تصادفی حسگر حامل استفاده می کنند، دو پروتکل MAC تفاوت های مهمی با هم دارند. اول، به جای استفاده از تشخیص برخورد، ۸۰۲.۱۱ از تکنیک های جلوگیری از برخورد استفاده می کند. دوم، به دلیل نرخ خطای بیت نسبتاً بالای کانال های بی سیم، ۸۰۲.۱۱ (برخلاف اترنت) از طرح تایید/انتقال مجدد لایه پیوند (ARQ) استفاده می کند. در زیر طرح های جلوگیری از برخورد و تایید لایه پیوند ۸۰۲.۱۱ را شرح خواهیم داد.

از بخش های ۶.۳.۲ و ۶.۴.۲ به یاد بیاورید که با الگوریتم تشخیص برخورد اترنت، یک ایستگاه اترنت هنگام ارسال به کانال گوش می دهد. اگر در حین ارسال، تشخیص دهد که ایستگاه دیگری نیز در حال ارسال است، ارسال خود را

متوقف می کند و پس از مدت زمان کمی و تصادفی، دوباره سعی می کند ارسال کند. برخلاف پروتکل اترنت ۸۰۲.۳، پروتکل 802.11 MAC تشخیص برخورد را اجرا نمی کند. دو دلیل مهم برای این امر وجود دارد:

- توانایی تشخیص برخورد مستلزم توانایی ارسال (سیگنال خود ایستگاه) و دریافت (برای تعیین اینکه آیا ایستگاه دیگری نیز در حال ارسال است) به طور همزمان می باشد. از آنجایی که قدرت سیگنال دریافتی معمولاً در مقایسه با قدرت سیگنال ارسالی در آداپتور ۸۰۲.۱۱ بسیار کم است، ساخت سخت افزاری که بتواند برخورد را تشخیص دهد هزینه بر است.

- مهمتر از آن، حتی اگر آداپتور بتواند همزمان ارسال و گوش دهد (و احتمالاً زمانی که یک کانال شلوغ را احساس می کند، ارسال را متوقف می کند)، آداپتور باز هم نمی تواند تمام برخوردها را تشخیص دهد، به دلیل مشکل ترمینال پنهان و محو شدن، همانطور که در بخش ۷.۲ بحث شد. از آنجایی که شبکه های محلی بی سیم ۸۰۲.۱۱ از تشخیص برخورد استفاده نمی کنند، هنگامی که ایستگاه شروع به ارسال فریم می کند، فریم را به طور کامل ارسال می کند. یعنی زمانی که یک ایستگاه راه اندازی می شود، دیگر راه برگشتی وجود ندارد. همانطور که انتظار می رود، انتقال کل فریم ها (به ویژه فریم های طولانی) در هنگام برخورد رایج می تواند به طور قابل توجهی عملکرد یک پروتکل دسترسی چندگانه را کاهش دهد. به منظور کاهش احتمال برخورد، ۸۰۲.۱۱ از چندین تکنیک جلوگیری از برخورد استفاده می کند که به زودی در مورد آنها صحبت خواهیم کرد. با این حال، قبل از بررسی اجتناب از برخورد، ابتدا باید طرح تایید لایه پیوند ۸۰۲.۱۱ را بررسی کنیم.

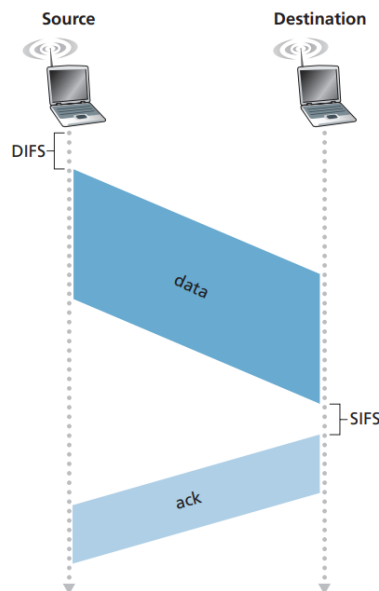


Figure 7.10 ♦ 802.11 uses link-layer acknowledgments

از بخش ۷.۲ به یاد بیاورید که وقتی یک ایستگاه در یک LAN بی سیم یک فریم می فرستد، ممکن است فریم به دلایل مختلف دست نخورده به ایستگاه مقصد نرسد. برای مقابله با این احتمال ناچیز شکست، پروتکل MAC

802.11 از تایید لایه پیوند استفاده می کند. همانطور که در شکل ۷.۱۰ نشان داده شده است، هنگامی که ایستگاه مقصد فریمی را دریافت می کند که از CRC عبور می کند، مدت زمان کوتاهی به نام فاصله کوتاه بین فریم (SIFS) منتظر می ماند و سپس یک فریم تایید را ارسال می کند. اگر ایستگاه فرستنده تاییدیه ای را در مدت زمان معین دریافت نکند، فرض می کند که یک خطا رخ داده است و با استفاده از پروتکل CSMA/CA برای دسترسی به کانال، فریم را دوباره ارسال می کند. اگر پس از تعداد معینی از ارسال مجدد، تاییدیه ای دریافت نشود، ایستگاه فرستنده منصرف شده و فریم را دور می اندازد.

پس از بحث در مورد نحوه استفاده 802.11 از تایید لایه پیوند، اکنون در موقعیتی هستیم که پروتکل 802.11 CSMA/CA را توضیح دهیم. فرض کنید یک ایستگاه (دستگاه بی سیم یا AP) یک فریم برای ارسال دارد.

۱. اگر در ابتدا ایستگاه بیکار بودن کانال را حس کند، فریم خود را پس از مدت کوتاهی که به عنوان فضای بین فریم توزیع شده (DIFS) شناخته می شود، ارسال می کند. شکل ۷.۱۰ را ببینید.

۲. در غیر این صورت، ایستگاه با استفاده از عقب نشینی نمایی باینری (همانطور که در بخش ۶.۳.۲ با آن مواجه شدیم) یک مقدار عقبگرد تصادفی انتخاب می کند و زمانی که کانال بیکار احساس می شود این مقدار را پس از DIFS شمارش معکوس می کند. در حالی که کانال مشغول احساس می شود، مقدار شمارنده ثابت می ماند.

۳. هنگامی که شمارنده به صفر می رسد (توجه داشته باشید که این فقط زمانی رخ می دهد که کانال بیکار است)، ایستگاه کل فریم را ارسال می کند و سپس منتظر تایید می ماند.

۴. در صورت دریافت تصدیق، ایستگاه فرستنده می داند که فریم آن به درستی در ایستگاه مقصد دریافت شده است. اگر ایستگاه فریم دیگری برای ارسال داشته باشد، پروتکل CSMA/CA را در مرحله ۲ آغاز می کند. اگر تایید دریافت نشد، ایستگاه فرستنده مجدداً وارد فاز backoff در مرحله ۲ می شود، با مقدار تصادفی انتخاب شده از یک بازه زمانی بزرگتر.

به یاد بیاورید که تحت پروتکل CSMA/CD اترنت، پروتکل دسترسی چندگانه (بخش ۶.۳.۲)، یک ایستگاه به محض اینکه کانال بیکار تشخیص داده شود شروع به ارسال می کند. با این حال، با CSMA/CA، ایستگاه هنگام شمارش معکوس از ارسال خودداری می کند، حتی زمانی که کانال را بی حرکت احساس می کند. چرا CSMA/CD و CDMA/CA در اینجا چنین رویکردهای متفاوتی را اتخاذ می کنند؟

برای پاسخ به این سوال، بیایید سناریویی را در نظر بگیریم که در آن دو ایستگاه هر کدام یک قاب داده برای ارسال دارند، اما هیچ یک از ایستگاهها فوراً ارسال نمی کنند، زیرا هر ایستگاه احساس می کند که ایستگاه سوم در حال ارسال است. با CSMA/CD اترنت، دو ایستگاه هر کدام به محض اینکه تشخیص دهند که ایستگاه سوم ارسال را

تمام کرده است، ارسال می کنند. این امر باعث برخورد می شود که در CSMA/CD مشکل جدی نیست، زیرا هر دو ایستگاه ارسال خود را قطع می کنند و بنابراین از ارسال بی فایده باقیمانده فریم های خود جلوگیری می کنند. اما در ۸۰۲.۱۱ وضعیت کاملاً متفاوت است. از آنجایی که ۸۰۲.۱۱ برخورد را تشخیص نمی دهد و ارسال را متوقف نمی کند، فریمی که دچار تصادم می شود به طور کامل منتقل می شود. بنابراین هدف در ۸۰۲.۱۱ جلوگیری از برخورد در صورت امکان است. در ۸۰۲.۱۱، اگر دو ایستگاه احساس کنند که کانال مشغول است، هر دو بلافاصله وارد backoff تصادفی می شوند، امیدواریم مقادیر مختلف backoff را انتخاب کنند. اگر این مقادیر واقعاً متفاوت باشند، هنگامی که کانال بیکار شود، یکی از دو ایستگاه قبل از دیگری شروع به ارسال می کند و (اگر دو ایستگاه از یکدیگر پنهان نباشند) "ایستگاه بازنده" "ایستگاه برنده" را می شنود. سیگنال دهید، شمارنده آن را منجمد کنید و تا زمانی که ایستگاه برنده ارسال خود را کامل نکند، از ارسال خودداری کنید. به این ترتیب از برخورد پرهیزنه جلوگیری می شود. البته، در این سناریو هنوز هم ممکن است برخورد با ۸۰۲.۱۱ اتفاق بیفتد: دو ایستگاه می توانند از یکدیگر پنهان شوند، یا دو ایستگاه می توانند مقادیر پس انداز تصادفی را انتخاب کنند که به اندازه کافی نزدیک باشند که انتقال از ایستگاه اول هنوز به ایستگاه دوم نرسد. ایستگاه. به یاد بیاورید که ما قبلاً در بحث خود در مورد الگوریتم های دسترسی تصادفی در زمینه شکل ۶.۱۲ با این مشکل مواجه شدیم.

برخورد با پایانه های پنهان: RTS و CTS

پروتکل MAC 802.11 همچنین شامل یک طرح رزرو زیبا (اما اختیاری) است که به جلوگیری از برخورد حتی در حضور پایانه های مخفی کمک می کند. بیاید این طرح را در زمینه شکل ۷.۱۱ بررسی کنیم که دو ایستگاه بی سیم و یک نقطه دسترسی را نشان می دهد. هر دو ایستگاه بی سیم در محدوده AP هستند (که پوشش آن به صورت دایره ای سایه دار نشان داده شده است) و هر دو با AP مرتبط هستند. با این حال، به دلیل محو شدن، محدوده سیگنال ایستگاه های بی سیم به فضای داخلی دایره های سایه دار نشان داده شده در شکل ۷.۱۱ محدود می شود. بنابراین، هر یک از ایستگاه های بی سیم از دیگری پنهان است، اگرچه هیچ یک از AP پنهان نیست.

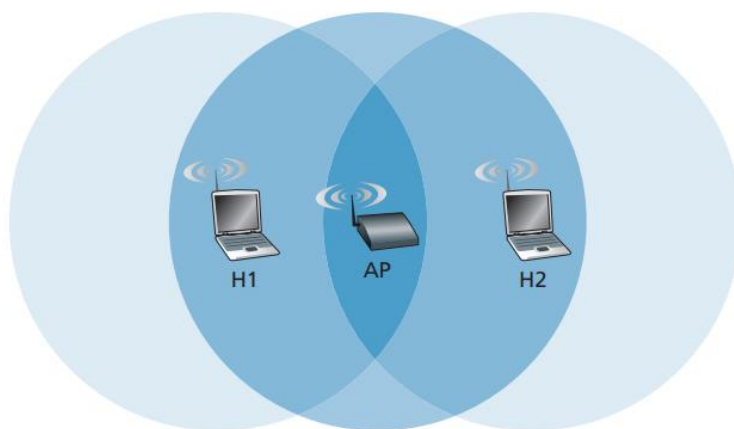


Figure 7.11 ♦ Hidden terminal example: H1 is hidden from H2, and vice versa

حال بیابید در نظر بگیریم که چرا پایانه های مخفی می توانند مشکل ساز باشند. فرض کنید ایستگاه H1 یک فریم را ارسال می کند و در نیمه راه انتقال H1، ایستگاه H2 می خواهد یک فریم را به AP ارسال کند. H2 که صدای ارسال را از H1 نمی شنود، ابتدا یک بازه DIFS منتظر می ماند و سپس فریم را ارسال می کند و در نتیجه برخورد می کند. بنابراین کانال در طول کل دوره انتقال H1 و همچنین در طول انتقال H2 هدر خواهد رفت.

برای جلوگیری از این مشکل، پروتکل IEEE 802.11 به ایستگاه اجازه می دهد تا از یک فریم کنترلی درخواست ارسال (RTS) و یک فریم کنترل کوتاه برای ارسال (CTS) برای رزرو دسترسی به کانال استفاده کند. هنگامی که یک فرستنده می خواهد یک فریم داده ارسال کند، ابتدا می تواند یک فریم RTS را به AP ارسال کند که کل زمان لازم برای ارسال فریم داده و قاب تأیید (ACK) را نشان می دهد. هنگامی که AP فریم RTS را دریافت می کند، با پخش یک فریم CTS پاسخ می دهد. این فریم CTS دو هدف را دنبال می کند: به فرستنده اجازه ارسال صریح می دهد و همچنین به ایستگاه های دیگر دستور می دهد برای مدت زمان رزرو شده ارسال نکنند. بنابراین، در شکل ۷.۱۲، قبل از ارسال یک فریم DATA، H1 ابتدا یک فریم RTS را پخش می کند که توسط تمام ایستگاه های دایره آن، از جمله AP شنیده می شود. سپس AP با یک فریم CTS پاسخ می دهد که توسط تمام ایستگاه های محدوده آن، از جمله H1 و H2 شنیده می شود. ایستگاه H2 با شنیدن صدای CTS، برای مدت زمان مشخص شده در فریم CTS از ارسال خودداری می کند. فریم های RTS، CTS، DATA و ACK در شکل ۷.۱۲ نشان داده شده است.

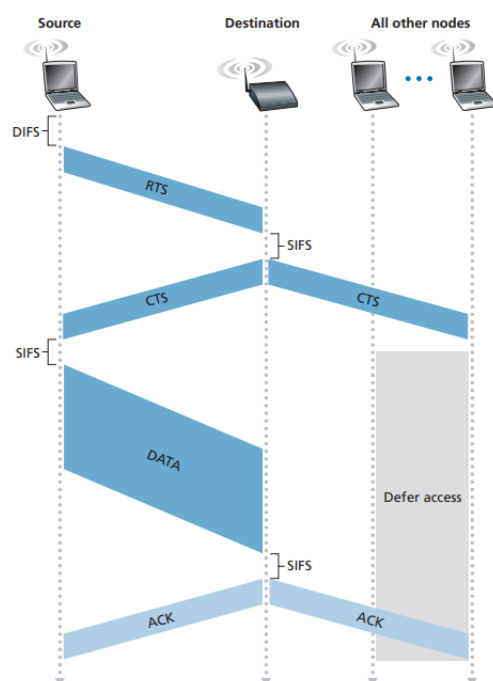


Figure 7.12 • Collision avoidance using the RTS and CTS frames

استفاده از فریم های RTS و CTS می تواند عملکرد را از دو طریق مهم بهبود بخشد:

- مشکل ایستگاه مخفی کاهش می یابد، زیرا یک فریم DATA طولانی تنها پس از رزرو کانال ارسال می شود.
- از آنجایی که فریم های RTS و CTS کوتاه هستند، تصادم شامل یک فریم RTS یا CTS فقط برای مدت زمان فریم کوتاه RTS یا CTS ادامه خواهد داشت. هنگامی که فریم های RTS و CTS به درستی ارسال می شوند، فریم های DATA و ACK زیر باید بدون برخورد ارسال شوند.

توصیه می شود انیمیشن ۸۰۲.۱۱ را در وب سایت کتاب درسی بررسی کنید. این انیمیشن تعاملی پروتکل CSMA/CA، از جمله دنباله تبادل RTS/CTS را نشان می دهد.

اگرچه تبادل RTS/CTS می تواند به کاهش برخوردها کمک کند، اما تاخیر را نیز معرفی می کند و منابع کانال را مصرف می کند. به همین دلیل، تبادل RTS/CTS فقط برای رزرو کانال برای ارسال یک فریم داده طولانی (در صورت وجود) استفاده می شود. در عمل، هر ایستگاه بی سیم می تواند یک آستانه RTS تنظیم کند به طوری که دنباله RTS/CTS تنها زمانی استفاده می شود که فریم از آستانه بلندتر باشد. برای بسیاری از ایستگاه های بی سیم، مقدار آستانه پیش فرض RTS از حداکثر طول فریم بزرگ تر است، بنابراین دنباله RTS/CTS برای همه فریم های داده ارسالی نادیده گرفته می شود.

استفاده از ۸۰۲.۱۱ به عنوان پیوند نقطه به نقطه

بحث ما تاکنون بر استفاده از ۸۰۲.۱۱ در تنظیمات دسترسی چندگانه متمرکز بوده است. لازم به ذکر است که اگر دو گره هر کدام یک آنتن جهت دار داشته باشند، می توانند آنتن های جهت دار خود را به سمت یکدیگر گرفته و پروتکل ۸۰۲.۱۱ را روی چیزی که اساساً یک پیوند نقطه به نقطه است اجرا کنند. با توجه به هزینه کم سخت افزار کالا ۸۰۲.۱۱، استفاده از آنتن های جهت دار و افزایش قدرت انتقال اجازه می دهد تا ۸۰۲.۱۱ به عنوان وسیله ای ارزان برای ارائه اتصالات نقطه به نقطه بی سیم در فاصله ده ها کیلومتر استفاده شود. [ارمان ۲۰۰۷] یکی از اولین شبکه های بی سیم چند هاپ را توصیف می کند که در دشت های روستایی گنگ در هند با استفاده از پیوندهای نقطه به نقطه ۸۰۲.۱۱ کار می کند.

۷.۳.۳ قاب IEEE 802.11

اگرچه فریم ۸۰۲.۱۱ شباهت های زیادی با فریم اترنت دارد، اما حاوی تعدادی فیلد است که مخصوص استفاده از آن برای پیوندهای بی سیم است. فریم ۸۰۲.۱۱ در شکل ۷.۱۳ نشان داده شده است. اعداد بالای هر یک از فیلدهای قاب نشان دهنده طول فیلدها در بایت هستند. اعداد بالای هر یک از زیر فیلدها در فیلد کنترل فریم، طول زیر فیلدها را به بیت نشان می دهند. حال بیایید فیلدهای فریم و همچنین برخی از زیر فیلدهای مهمتر در فیلد کنترل فریم را بررسی کنیم.

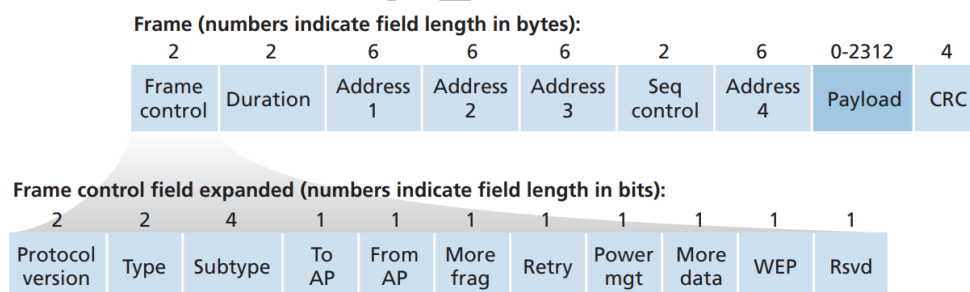


Figure 7.13 ♦ The 802.11 frame

بار و میدان های CRC

در قلب قاب، payload قرار دارد که معمولاً از یک دیتاگرام IP یا یک بسته ARP تشکیل شده است. اگرچه این فیلد مجاز است تا ۲۳۱۲ بایت باشد، اما معمولاً کمتر از ۱۵۰۰ بایت است و یک دیتاگرام IP یا یک بسته ARP را در خود جای داده است. همانند یک فریم اترنت، یک فریم ۸۰۲.۱۱ شامل یک بررسی افزونگی چرخه ای ۳۲ بیتی (CRC) است تا گیرنده بتواند خطاهای بیت را در فریم دریافتی تشخیص دهد. همانطور که دیدیم، خطاهای بیت در شبکه های محلی بی سیم بسیار رایج تر از شبکه های محلی سیمی هستند، بنابراین CRC در اینجا حتی مفیدتر است.

فیلدهای آدرس

شاید بارزترین تفاوت در فریم ۸۰۲.۱۱ این است که چهار فیلد آدرس دارد که هر کدام می توانند یک آدرس MAC ۶ بایتی را در خود جای دهند. اما چرا چهار فیلد آدرس؟ آیا یک فیلد MAC مبدا و فیلد MAC مقصد، همانطور که برای اترنت کافی است، کافی نیست؟ به نظر می رسد که سه فیلد آدرس برای اهداف کار اینترنتی مورد نیاز است - به ویژه برای انتقال داده های لایه شبکه از یک ایستگاه بی سیم از طریق یک AP به یک رابط روتر. فیلد آدرس چهارم زمانی استفاده می شود که AP ها فریم ها را در حالت موقت به یکدیگر ارسال می کنند. از آنجایی که ما در اینجا فقط شبکه های زیرساخت را در نظر می گیریم، بیاید توجه خود را بر روی سه فیلد آدرس اول متمرکز کنیم. استاندارد ۸۰۲.۱۱ این فیلدها را به صورت زیر تعریف می کند:

- آدرس ۲ آدرس MAC ایستگاهی است که فریم را ارسال می کند. بنابراین، اگر یک ایستگاه بی سیم فریم را ارسال کند، آدرس MAC آن ایستگاه در قسمت آدرس ۲ درج می شود. به طور مشابه، اگر یک AP فریم را ارسال کند، آدرس MAC AP در قسمت آدرس ۲ درج می شود.
- آدرس ۱ آدرس MAC ایستگاه بی سیمی است که قرار است فریم را دریافت کند. بنابراین اگر یک ایستگاه بی سیم سیار فریم را ارسال کند، آدرس ۱ حاوی آدرس MAC AP مقصد است. به طور مشابه، اگر یک AP فریم را ارسال کند، آدرس ۱ حاوی آدرس MAC ایستگاه بی سیم مقصد است.
- برای درک آدرس ۳، به یاد بیاورید که BSS (متشکل از AP و ایستگاه های بی سیم) بخشی از یک زیر شبکه است، و این زیر شبکه از طریق برخی از رابط های روتر به زیر شبکه های دیگر متصل می شود. آدرس ۳ حاوی آدرس MAC این رابط روتر است.

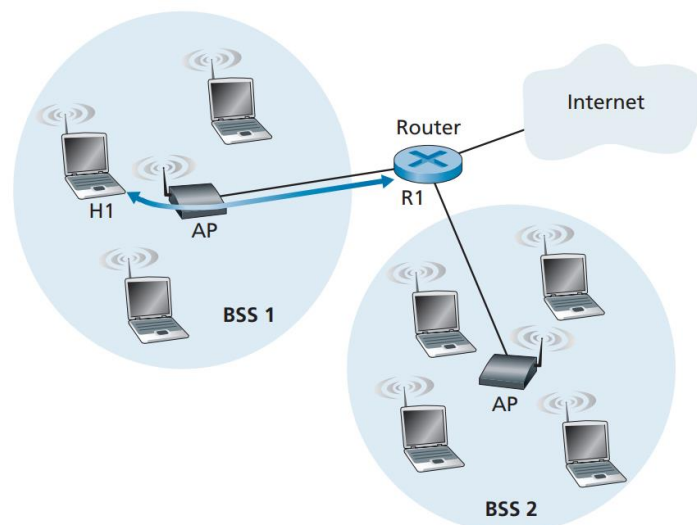


Figure 7.14 ♦ The use of address fields in 802.11 frames: Sending frames between H1 and R1

برای به دست آوردن بینش بیشتر در مورد هدف آدرس ۳، اجازه دهید از طریق یک مثال کار اینترنتی در زمینه شکل ۷.۱۴ بگذریم. در این شکل دو AP وجود دارد که هر کدام مسئولیت تعدادی ایستگاه بی سیم را بر عهده دارند. هر یک از AP ها یک اتصال مستقیم به یک روتر دارد که به نوبه خود به اینترنت جهانی متصل می شود. ما باید در نظر داشته باشیم که یک AP یک دستگاه لایه پیوند است و بنابراین نه IP را "صحبت می کند" و نه آدرس های IP را درک می کند. اکنون یک دیتاگرام را از رابط روتر R1 به ایستگاه بی سیم H1 منتقل کنید. روتر از وجود یک AP بین آن و H1 آگاه نیست. از دیدگاه روتر، H1 فقط یک میزبان در یکی از زیرشبکه هایی است که به آن (روتر) متصل است.

- روتر که آدرس IP H1 را می داند (از آدرس مقصد دیتاگرام)، از ARP برای تعیین آدرس MAC H1 استفاده می کند، درست مانند یک شبکه اترنت معمولی. پس از به دست آوردن آدرس MAC H1، رابط روتر R1 دیتاگرام را در یک فریم اترنت کپسوله می کند. فیلد آدرس منبع این فریم حاوی آدرس MAC R1 و فیلد آدرس مقصد حاوی آدرس MAC H1 است.

- هنگامی که فریم اترنت به AP می رسد، AP قاب اترنت ۸۰۲.۳ را قبل از انتقال فریم به کانال بی سیم به یک فریم ۸۰۲.۱۱ تبدیل می کند. AP آدرس ۱ و آدرس ۲ را به ترتیب با آدرس MAC H1 و آدرس MAC خودش پر می کند، همانطور که در بالا توضیح داده شد. برای آدرس ۳، AP آدرس MAC R1 را درج می کند. به این ترتیب، H1 می تواند (از آدرس ۳) آدرس MAC رابط روتر را که دیتاگرام را به زیر شبکه فرستاده است، تعیین کند. حال در نظر بگیرید که چه اتفاقی می افتد زمانی که ایستگاه بی سیم H1 با انتقال دیتاگرام از H1 به R1 پاسخ می دهد.

- H1 یک فریم ۸۰۲.۱۱ ایجاد می کند و فیلدهای آدرس ۱ و آدرس ۲ را به ترتیب با آدرس MAC AP و آدرس MAC H1 پر می کند، همانطور که در بالا توضیح داده شد. برای آدرس ۳، H1 آدرس MAC R1 را درج می کند.
- هنگامی که AP فریم ۸۰۲.۱۱ را دریافت می کند، فریم را به فریم اترنت تبدیل می کند. فیلد آدرس مبدا برای این فریم آدرس MAC H1 و فیلد آدرس مقصد آدرس MAC R1 است. بنابراین، آدرس ۳ به AP اجازه می دهد تا آدرس MAC مقصد مناسب را هنگام ساخت فریم اترنت تعیین کند.

به طور خلاصه، آدرس ۳ نقش مهمی برای کار اینترنتی BSS با یک شبکه LAN سیمی دارد.

تعداد دنباله، مدت زمان و فیلدهای کنترل فریم

به یاد بیاورید که در ۸۰۲.۱۱، هر زمان که یک ایستگاه به درستی فریمی را از ایستگاه دیگر دریافت کرد، یک تأییدیه را پس می فرستد. از آنجایی که اعترافات ممکن است گم شوند، ایستگاه فرستنده ممکن است چندین نسخه از یک فریم مشخص را ارسال کند. همانطور که در بحث خود در مورد پروتکل rdt2.1 (بخش ۳.۴.۱) دیدیم، استفاده از اعداد دنباله ای به گیرنده اجازه می دهد بین یک فریم تازه ارسال شده و ارسال مجدد فریم قبلی تمایز قائل شود. بنابراین، فیلد شماره ترتیبی در فریم ۸۰۲.۱۱ دقیقاً همان هدفی را در اینجا در لایه پیوند انجام می دهد که در لایه انتقال در فصل ۳ انجام شد.

به یاد بیاورید که پروتکل ۸۰۲.۱۱ به ایستگاه فرستنده اجازه می دهد تا کانال را برای یک دوره زمانی رزرو کند که شامل زمان ارسال فریم داده آن و زمان ارسال یک تایید است. این مقدار مدت زمان در قسمت مدت زمان قاب (هم برای فریم های داده و هم برای فریم های RTS و CTS) گنجانده شده است.

همانطور که در شکل ۷.۱۳ نشان داده شده است، فیلد کنترل فریم شامل بسیاری از زیر فیلدها است. ما فقط چند کلمه در مورد برخی از زیرشاخه های مهم تر می گوئیم. برای بحث کامل تر، توصیه می شود با مشخصات ۸۰۲.۱۱ [برگزاری ۲۰۰۱؛ کلاغ ۱۹۹۷؛ IEEE 802.11 1999]. از فیلدهای نوع و نوع فرعی برای تشخیص ارتباط، RTS، CTS، ACK و فریم های داده استفاده می شود. از فیلدهای to و from برای تعریف معانی فیلدهای آدرس مختلف استفاده می شود. (این معانی بسته به استفاده از حالت های موقت یا زیرساخت و در مورد حالت زیرساخت، اینکه آیا یک ایستگاه بی سیم یا یک AP فریم را ارسال می کند، تغییر می کند.) در نهایت فیلد WEP نشان می دهد که آیا از رمزگذاری استفاده می شود یا نه (WEP). در فصل ۸ مورد بحث قرار گرفته است.

۷.۳.۴ تحرک در زیر شبکه IP یکسان

به منظور افزایش برد فیزیکی یک شبکه محلی بی سیم، شرکت ها و دانشگاه ها اغلب چندین BSS را در یک زیر شبکه IP مستقر می کنند. این به طور طبیعی موضوع تحرک را در بین BSS ها مطرح می کند - چگونه ایستگاه های بی سیم به طور یکپارچه از یک BSS به BSS دیگر حرکت می کنند در حالی که جلسات TCP مداوم را حفظ می کنند؟ همانطور که در این بخش خواهیم دید، وقتی BSS ها بخشی از زیر شبکه هستند، تحرک را می توان به روشی نسبتاً ساده مدیریت کرد. هنگامی که ایستگاه ها بین زیر شبکه ها حرکت می کنند، پروتکل های پیچیده تری برای مدیریت تحرک مورد نیاز خواهند بود، مانند پروتکل هایی که در بخش های ۷.۵ و ۷.۶ مطالعه خواهیم کرد.

بیاید اکنون به یک مثال خاص از تحرک بین BSS ها در همان زیر شبکه نگاه کنیم. شکل ۷.۱۵ دو BSS به هم پیوسته را با میزبان H1 نشان می دهد که از BSS1 به BSS2 حرکت می کند. از آنجایی که در این مثال، دستگاه

اتصال که دو BSS را به هم متصل می‌کند، یک روتر نیست، همه ایستگاه‌های دو BSS، از جمله AP، متعلق به یک زیرشبکه IP هستند. بنابراین، هنگامی که H1 از BSS1 به BSS2 منتقل می‌شود، ممکن است آدرس IP و تمام اتصالات TCP در حال انجام خود را حفظ کند. اگر دستگاه اتصال یک روتر بود، H1 باید یک آدرس IP جدید در زیرشبکه‌ای که در آن حرکت می‌کرد به دست آورد. این تغییر آدرس باعث اختلال (و در نهایت خاتمه) هر گونه اتصال TCP در حال انجام در H1 می‌شود. در بخش ۷.۶، خواهیم دید که چگونه می‌توان از پروتکل تحرک لایه شبکه، مانند IP موبایل، برای جلوگیری از این مشکل استفاده کرد.

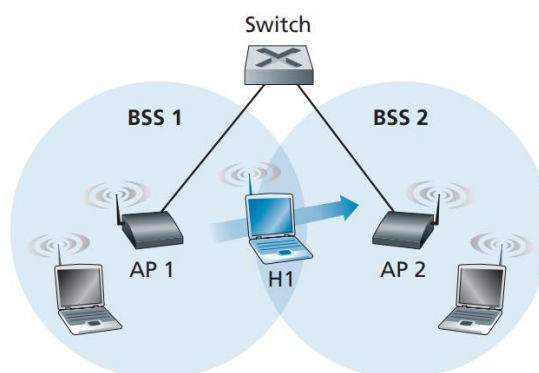


Figure 7.15 ♦ Mobility in the same subnet

اما وقتی H1 از BSS1 به BSS2 می‌رود، به طور خاص چه اتفاقی می‌افتد؟ همانطور که H1 از AP1 دور می‌شود، H1 یک سیگنال ضعیف از AP1 را تشخیص می‌دهد و شروع به اسکن برای سیگنال قوی‌تر می‌کند. H1 فریم‌های beacon را از AP2 دریافت می‌کند (که در بسیاری از تنظیمات شرکت‌ها و دانشگاه‌ها همان SSID AP1 را دارند). سپس H1 با AP1 ارتباط برقرار می‌کند و با AP2 ارتباط برقرار می‌کند، در حالی که آدرس IP خود را حفظ می‌کند و جلسات TCP مداوم خود را حفظ می‌کند.

این مشکل انتقال را از دیدگاه میزبان و AP برطرف می‌کند. اما سوئیچ در شکل ۷.۱۵ چگونه متوجه می‌شود که میزبان از یک AP به دیگری منتقل شده است؟ همانطور که ممکن است از فصل ۶ به یاد داشته باشید، سوئیچ‌ها "خودآموز" هستند و به طور خودکار جداول ارسال خود را می‌سازند. این ویژگی خودآموزی به خوبی حرکات گاه به گاه را کنترل می‌کند (به عنوان مثال، زمانی که یک کارمند از یک بخش به بخش دیگر منتقل می‌شود). با این حال، سوئیچ‌ها برای پشتیبانی از کاربران بسیار موبایلی که می‌خواهند اتصالات TCP را در حین حرکت بین BSS‌ها حفظ کنند، طراحی نشده‌اند. برای درک مشکل در اینجا، به یاد بیاورید که قبل از حرکت، سوئیچ یک ورودی در جدول ارسال دارد که آدرس MAC H1 را با رابط سوئیچ خروجی جفت می‌کند که از طریق آن می‌توان به H1 دسترسی داشت. اگر H1 ابتدا در BSS1 باشد، دیتاگرام مقصد H1 از طریق AP1 به H1 هدایت می‌شود. با

این حال، هنگامی که H1 با BSS2 مرتبط شد، فریم های آن باید به A P2 هدایت شوند. یک راه حل (واقعاً کمی هک) این است که AP2 یک فریم اترنت پخش شده با آدرس منبع H1 را درست بعد از ارتباط جدید به سویچ ارسال کند. هنگامی که سویچ فریم را دریافت می کند، جدول فوروارد خود را به روز می کند و امکان دسترسی به H1 را از طریق A P2 فراهم می کند. گروه استانداردهای ۸۰۲.۱۱ در حال توسعه یک پروتکل بین AP برای رسیدگی به این موارد و مسائل مرتبط است.

بحث ما در بالا بر تحرک با همان زیرشبکه LAN متمرکز شده است. به یاد بیاورید که VLAN ها، که در بخش ۶.۴.۴ مطالعه کردیم، می توانند برای اتصال جزایر شبکه های محلی به یک LAN مجازی بزرگ که می تواند یک منطقه جغرافیایی بزرگ را در بر گیرد، استفاده شود. تحرک بین ایستگاه های پایه در چنین VLAN را می توان دقیقاً به همان روشی که در بالا انجام داد [Yu 2011].

۷.۳.۵ ویژگی های پیشرفته در ۸۰۲.۱۱

ما پوشش خود را از ۸۰۲.۱۱ با یک بحث کوتاه در مورد دو قابلیت پیشرفته موجود در شبکه های ۸۰۲.۱۱ به پایان می رسانیم. همانطور که خواهیم دید، این قابلیت ها به طور کامل در استاندارد ۸۰۲.۱۱ مشخص نشده اند، بلکه با مکانیسم های مشخص شده در استاندارد امکان پذیر شده اند. این به فروشندگان مختلف اجازه می دهد تا با استفاده از رویکردهای (اختصاصی) خود، این قابلیت ها را پیاده سازی کنند و احتمالاً به آنها برتری نسبت به رقابت می دهد.

۸۰۲.۱۱ تطبیق نرخ

قبلاً در شکل ۷.۳ دیدیم که تکنیک های مدولاسیون مختلف (با نرخ های انتقال متفاوتی که ارائه می کنند) برای سناریوهای مختلف SNR مناسب هستند. به عنوان مثال، یک کاربر موبایل ۸۰۲.۱۱ را در نظر بگیرید که در ابتدا ۲۰ متر از ایستگاه پایه فاصله دارد و نسبت سیگنال به نویز بالایی دارد. با توجه به SNR بالا، کاربر می تواند با استفاده از تکنیک مدولاسیون لایه فیزیکی که نرخ انتقال بالایی را در حالی که BER پایین را حفظ می کند، با ایستگاه پایه ارتباط برقرار کند. این یک کاربر خوشحال است! اکنون فرض کنید کاربر متحرک شده و از ایستگاه پایه دور می شود و با افزایش فاصله از ایستگاه پایه، SNR سقوط می کند. در این حالت، اگر تکنیک مدولاسیون مورد استفاده در پروتکل ۸۰۲.۱۱ که بین ایستگاه پایه و کاربر کار می کند، تغییر نکند، با کاهش SNR، BER به طور غیرقابل قبولی بالا می رود و در نهایت هیچ فریم ارسالی به درستی دریافت نمی شود. به همین دلیل، برخی از پیاده سازی های ۸۰۲.۱۱ دارای قابلیت انطباق نرخ هستند که به طور تطبیقی تکنیک مدولاسیون لایه فیزیکی زیربنایی را برای استفاده بر اساس ویژگی های کانال فعلی یا اخیر انتخاب می کند. اگر یک گره دو فریم را پشت سر هم بدون دریافت

تایید ارسال کند (نشان ضمنی خطاهای بیت در کانال)، نرخ انتقال به نرخ پایین بعدی برمی گردد. اگر ۱۰ فریم پشت سر هم تأیید شود، یا اگر تایمیری که زمان را از آخرین بازگشت بازگشتی ردیابی می کند منقضی شود، نرخ ارسال به نرخ بالاتر بعدی افزایش می یابد. این مکانیسم انطباق نرخ، همان فلسفه «کاوشگری» را با مکانیسم کنترل تراکم TCP دارد - وقتی شرایط خوب باشد (که توسط دریافت‌های ACK منعکس می‌شود)، نرخ انتقال افزایش می‌یابد تا زمانی که اتفاقی «بد» بیفتد (فقدان دریافت‌های ACK). هنگامی که اتفاقی "بد" می افتد، سرعت انتقال کاهش می یابد. بنابراین، انطباق نرخ ۸۰۲.۱۱ و کنترل تراکم TCP شبیه به کودک خردسالی است که دائماً والدین خود را برای بیشتر و بیشتر تحت فشار قرار می دهد (مثلاً آب نبات برای یک کودک خردسال، ساعات بعدی منع رفت و آمد برای نوجوان) تا زمانی که والدین در نهایت بگویند "بس است!" و کودک عقب نشینی می کند (فقط برای اینکه بعداً پس از بهبود شرایط، دوباره تلاش کند!). تعدادی طرح دیگر نیز برای بهبود این طرح تعدیل نرخ خودکار پایه پیشنهاد شده است [Kamerman 1997; هلند ۲۰۰۱; Lacage 2004].

مدیریت قدرت

برق یک منبع گرانبها در دستگاه‌های تلفن همراه است و بنابراین استاندارد ۸۰۲.۱۱ قابلیت‌های مدیریت انرژی را فراهم می‌کند که به گره‌های ۸۰۲.۱۱ اجازه می‌دهد تا مدت زمانی را که عملکردهای حس، انتقال و دریافت و سایر مدارها باید «روشن» باشند، به حداقل برسانند. مدیریت توان ۸۰۲.۱۱ به شرح زیر عمل می‌کند. یک گره قادر است به صراحت بین حالت خواب و بیداری متناوب کند (بر خلاف یک دانش آموز خواب‌آلود در کلاس درس نیست!). یک گره به نقطه دسترسی نشان می‌دهد که با تنظیم بیت مدیریت انرژی در سربرگ یک فریم ۸۰۲.۱۱ روی ۱ به نقطه دسترسی می‌رود. سپس یک تایمر در گره تنظیم می‌شود تا درست قبل از برنامه‌ریزی AP، گره را بیدار کند. برای ارسال فریم بیکن خود (به یاد بیاورید که یک AP معمولاً هر ۱۰۰ میلی‌ثانیه یک فریم فانوس دریایی ارسال می‌کند). از آنجایی که AP از بیت انتقال توان تنظیم شده می‌داند که گره به خواب می‌رود، (AP) می‌داند که نباید هیچ فریمی را به آن گره ارسال کند و هر فریمی را که برای میزبان خواب ارسال شده است بافر می‌کند تا انتقال بعدی. یک گره درست قبل از اینکه AP یک قاب چراغ را بفرستد بیدار می‌شود و به سرعت وارد حالت کاملاً فعال می‌شود (برخلاف دانش آموز خواب‌آلود، این بیداری تنها به ۲۵۰ میکروثانیه نیاز دارد [Kamerman 1997]). فریم‌های beacon ارسال شده توسط AP حاوی لیستی از گره‌هایی هستند که فریم‌های آنها در AP بافر شده‌اند. اگر هیچ فریم بافری برای گره وجود نداشته باشد، می‌تواند به حالت خواب برگردد. در غیر این صورت، گره می‌تواند صریحاً با ارسال یک پیام نظرسنجی به AP درخواست کند که فریم‌های بافر شده ارسال شوند. با زمان بین بیکن ۱۰۰

میلی ثانیه، زمان بیداری ۲۵۰ میکروثانیه، و زمان مشابهی برای دریافت فریم بیکن و بررسی برای اطمینان از عدم وجود فریم بافر، گره‌ای که هیچ فریمی برای ارسال یا دریافت ندارد، می‌تواند در ۹۹ درصد مواقع خوابید که در نتیجه صرفه جویی قابل توجهی در مصرف انرژی می‌شود.

۷.۳.۶ شبکه‌های شخصی: بلوتوث*

*عبارات استفاده شده در زیر ممکن است با اصطلاحات موجود در مشخصات رسمی بلوتوث متفاوت باشد. اصطلاحات استفاده شده در مشخصات رسمی با تعهد پیرسون به ارتقای تنوع، برابری، و شمول، و محافظت در برابر تعصب و کلیشه در جمعیت جهانی فراگیرانی که به آنها خدمت می‌کنیم، همسو نیست.

به نظر می‌رسد شبکه‌های بلوتوث به سرعت بخشی از زندگی روزمره شده‌اند. شاید از یک شبکه بلوتوث به عنوان فناوری «تعویض کابل» برای اتصال رایانه خود با صفحه کلید بی‌سیم، ماوس یا سایر دستگاه‌های جانبی استفاده کرده باشید. یا شاید از یک شبکه بلوتوث برای اتصال هدفون‌های بی‌سیم، بلندگو، ساعت، یا باند نظارت بر سلامت خود به تلفن هوشمند خود یا برای اتصال گوشی هوشمند خود به سیستم صوتی خودرو استفاده کرده باشید. در تمام این موارد، بلوتوث در بردهای کوتاه (دهها متر یا کمتر)، با قدرت کم و با هزینه کم کار می‌کند. به همین دلیل، شبکه‌های بلوتوث گاهی اوقات به عنوان شبکه‌های شخصی بی‌سیم (WPAN) یا پیکونت شناخته می‌شوند.

اگرچه شبکه‌های بلوتوث از نظر طراحی کوچک و نسبتاً ساده هستند، اما مملو از بسیاری از تکنیک‌های شبکه‌سازی در سطح پیوند هستند که قبلاً مطالعه کرده‌ایم، از جمله تقسیم زمان مالتی پلکس (TDM) و تقسیم فرکانس (بخش ۶.۳.۱)، پس‌انداز تصادفی (بخش ۶.۳.۲)، نظرسنجی (بخش ۶.۳.۳)، تشخیص و تصحیح خطا (بخش ۶.۲)، انتقال داده قابل اعتماد از طریق ACKs و NAKs (بخش ۳.۴.۱). و این فقط با در نظر گرفتن لایه پیوند بلوتوث است!

شبکه‌های بلوتوث در باند رادیویی صنعتی، علمی و پزشکی بدون مجوز ۲.۴ گیگاهرتز (ISM) همراه با سایر لوازم خانگی مانند مایکروویو، درب بازکن گاراژ و تلفن‌های بی‌سیم کار می‌کنند. در نتیجه، شبکه‌های بلوتوث به صراحت با در نظر گرفتن نویز و تداخل طراحی می‌شوند. کانال بی‌سیم بلوتوث به روش TDM با اسلات‌های زمانی ۶۲۵ میکروثانیه کار می‌کند. در طول هر شکاف زمانی، یک فرستنده در یکی از ۷۹ کانال ارسال می‌کند، با کانال (فرکانس) به شیوه‌ای شناخته شده اما شبه تصادفی از شکافی به شکاف دیگر تغییر می‌کند. این شکل از جهش کانال، که به عنوان طیف گسترده پرش فرکانس (FHSS) شناخته می‌شود، به گونه‌ای استفاده می‌شود که تداخل

دستگاه یا وسیله دیگری که در باند ISM کار می کند، تنها در ارتباطات بلوتوث حداکثر در زیر مجموعه ای از شکاف ها تداخل ایجاد کند. نرخ داده بلوتوث می تواند تا ۳ مگابیت در ثانیه برسد.

شبکه های بلوتوث شبکه های موقتی هستند—به هیچ زیرساخت شبکه (به عنوان مثال، نقطه دسترسی) نیاز نیست. در عوض، دستگاه های بلوتوث باید خود را در یک پیکونت تا هشت دستگاه فعال سازماندهی کنند، همانطور که در شکل ۷.۱۶ نشان داده شده است. یکی از این دستگاه ها به عنوان کنترل کننده متمرکز تعیین می شود و بقیه دستگاه ها به عنوان مشتری عمل می کنند. گره کنترل کننده متمرکز واقعاً بر پیکونت حکومت می کند - ساعت آن زمان را در پیکنت تعیین می کند (مثلاً مرزهای اسلات TDM را تعیین می کند)، توالی پرش فرکانس شیار به اسلات را تعیین می کند، ورود دستگاه های مشتری به پیکنت را کنترل می کند، و توان (۱۰۰ مگاوات، ۲.۵ مگاوات، یا ۱ مگاوات) که در آن دستگاه های مشتری انتقال می دهند. و از نظرسنجی برای اعطای مجوز به مشتریان برای ارسال پس از ورود به شبکه استفاده می کند. علاوه بر دستگاه های فعال، می توان تا ۲۵۵ دستگاه «پارک شده» نیز در پیکونت وجود داشته باشد. این دستگاه های پارک شده اغلب در نوعی «حالت خواب» برای صرفه جویی در انرژی هستند (همانطور که در مدیریت توان ۸۰۲.۱۱ دیدیم) و به طور دوره ای، طبق برنامه کنترل کننده متمرکز، برای دریافت پیام های چراغ از کنترل کننده متمرکز بیدار می شوند. یک دستگاه پارک شده نمی تواند ارتباط برقرار کند مگر اینکه وضعیت آن توسط گره کنترل کننده متمرکز از پارک شده به فعال تغییر کند.

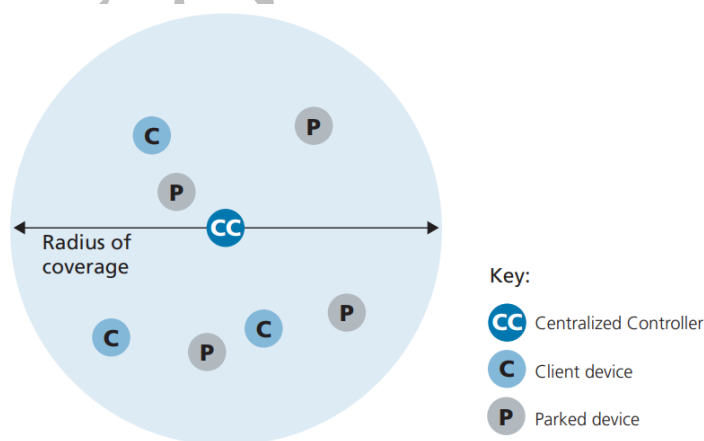


Figure 7.16 ♦ A Bluetooth piconet

از آنجایی که شبکه های تک تک بلوتوث باید خود سازماندهی شوند، ارزش آن را دارد که چگونه ساختار شبکه خود را راه اندازی کنند. هنگامی که یک گره کنترل کننده متمرکز می خواهد یک شبکه بلوتوث تشکیل دهد، ابتدا باید مشخص کند که کدام دستگاه های بلوتوث دیگر در محدوده قرار دارند. این مشکل کشف همسایه است. کنترل کننده متمرکز این کار را با پخش مجموعه ای از ۳۲ پیام درخواستی، هر کدام در یک کانال فرکانس متفاوت انجام

می دهد و دنباله ارسال را تا ۱۲۸ بار تکرار می کند. یک دستگاه سرویس گیرنده به فرکانس انتخابی خود گوش می دهد، به این امید که یکی از پیام های درخواست کنترل کننده متمرکز را در این فرکانس بشنود. هنگامی که پیام درخواستی را می شنود، مقدار زمانی تصادفی بین ۰ تا ۰.۳ ثانیه را پشت سر می گذارد (برای جلوگیری از برخورد با سایر گره های پاسخ دهنده، یادآور عقب نشینی باینری اترنت) و سپس با پیامی حاوی شناسه دستگاه خود به کنترل کننده متمرکز پاسخ می دهد.

هنگامی که کنترلر متمرکز بلوتوث تمام مشتریان بالقوه را در محدوده کشف کرد، سپس مشتریانی را که مایل است به پیکونت بپیوندند دعوت می کند. این مرحله دوم به عنوان صفحه بندی بلوتوث شناخته می شود و یادآور ۸۰۲.۱۱ مشتریانی است که با یک ایستگاه پایه ارتباط دارند. از طریق فرآیند صفحه بندی، کنترل کننده متمرکز مشتری را از الگوی پرسش فرکانس مورد استفاده و ساعت فرستنده مطلع می کند. کنترل کننده متمرکز فرآیند صفحه بندی را با ارسال مجدد ۳۲ پیام دعوت صفحه بندی یکسان آغاز می کند، که هر کدام اکنون به یک کلاینت خاص خطاب می شوند، اما دوباره از فرکانس های متفاوتی استفاده می کنند، زیرا آن مشتری هنوز الگوی پرسش فرکانس را یاد نگرفته است. هنگامی که مشتری با یک پیام ACK به پیام دعوت صفحه بندی پاسخ می دهد، کنترل کننده متمرکز اطلاعات مربوط به پرسش فرکانس، اطلاعات هماهنگ سازی ساعت و یک آدرس عضو فعال را برای مشتری ارسال می کند و سپس در نهایت از مشتری نظرسنجی می کند، اکنون از الگوی پرسش فرکانس استفاده می کند. برای اطمینان از اینکه مشتری به شبکه متصل است.

در بحث بالا، ما فقط به شبکه بی سیم بلوتوث پرداختیم. پروتکل های سطح بالاتر برای انتقال بسته داده قابل اعتماد، جریان مدار مانند صدا و تصویر، تغییر سطوح توان انتقال، تغییر حالت فعال/پارک (و سایر حالت ها) و موارد دیگر را فراهم می کنند. نسخه های جدیدتر بلوتوث به ملاحظات کم انرژی و امنیت پرداخته اند. برای اطلاعات بیشتر در مورد بلوتوث، خواننده علاقه مند باید به [Bisdikian 2001, Colbach 2017 و Bluetooth 2020] مراجعه کند.

۷.۴ شبکه های تلفن همراه: G4 و G5

در بخش قبل، ما بررسی کردیم که چگونه یک هاست می تواند به اینترنت دسترسی داشته باشد، در مجاورت یک نقطه دسترسی (AP) WiFi 802.11. اما همانطور که دیدیم، AP ها مناطق تحت پوشش کوچکی دارند و یک میزبان مطمئناً نمی تواند با هر AP که با آن روبرو می شود ارتباط برقرار کند. در نتیجه، دسترسی به WiFi برای کاربر در حال حرکت به سختی در همه جا وجود دارد.

در مقابل، دسترسی به شبکه سلولی G4 به سرعت فراگیر شده است. یک مطالعه اندازه گیری اخیر روی بیش از یک میلیون مشترک شبکه تلفن همراه ایالات متحده نشان داد که آنها می توانند سیگنال های G4 را در بیش از ۹۰ درصد مواقع با سرعت دانلود ۲۰ مگابیت بر ثانیه و بالاتر پیدا کنند. کاربران سه اپراتور تلفن همراه اصلی کره می توانند سیگنال G4 را بین ۹۵ تا ۹۹.۵ درصد مواقع پیدا کنند [سیگنال باز ۲۰۱۹]. در نتیجه، در حال حاضر پخش ویدئوهای HD یا شرکت در کنفرانس های ویدئویی در حین حرکت در ماشین، اتوبوس یا قطار پرسرعت رایج است. فراگیر بودن دسترسی به اینترنت G4 همچنین بی شمار برنامه های جدید IoT مانند سیستم های دوجرخه و روروک مخصوص بچه های مشترک متصل به اینترنت و برنامه های کاربردی گوشی های هوشمند مانند پرداخت های موبایلی (از سال ۲۰۱۸ در چین رایج) و پیام رسانی مبتنی بر اینترنت (WeChat, WhatsApp و غیره) را فعال کرده است. اصطلاح سلولی به این واقعیت اشاره دارد که منطقه تحت پوشش یک شبکه سلولی به تعدادی از مناطق تحت پوشش جغرافیایی تقسیم می شود که به سلول ها معروف هستند. هر سلول شامل یک ایستگاه پایه است که سیگنال ها را به دستگاه های موبایلی که در حال حاضر در سلول خود هستند ارسال می کند و سیگنال ها را از آن دریافت می کند. سطح پوشش یک سلول به عوامل زیادی بستگی دارد، از جمله قدرت انتقال ایستگاه پایه، قدرت انتقال دستگاه ها، ساختمان های مسدود کننده در سلول و ارتفاع و نوع آنتن های ایستگاه پایه.

در این بخش، مروری بر شبکه های سلولی G4 فعلی و نوظهور G5 ارائه می کنیم. ما اولین پرش بی سیم بین دستگاه تلفن همراه و ایستگاه پایه، و همچنین شبکه هسته تمام IP حامل تلفن همراه را در نظر خواهیم گرفت که اولین پرش بی سیم را به شبکه اپراتور، سایر شبکه های حامل و اینترنت بزرگتر متصل می کند. شاید تعجب آور باشد (با توجه به خاستگاه شبکه های تلفن همراه در دنیای تلفن، که معماری شبکه ای بسیار متفاوت از اینترنت داشت)، ما با بسیاری از اصول معماری در شبکه های G4 که در مطالعات متمرکز بر اینترنت در فصل ها با آنها مواجه شدیم، مواجه خواهیم شد. ۱-۶، شامل لایه بندی پروتکل، تمایز لبه/هسته، اتصال شبکه های ارائه دهنده متعدد برای تشکیل یک «شبکه شبکه ها» جهانی، و جداسازی واضح داده ها و سطوح کنترل با کنترل منطقی متمرکز. ما اکنون این اصول را از دریچه شبکه های تلفن همراه (و نه از طریق یک لنز اینترنتی) خواهیم دید و بنابراین این اصول را به روش های مختلف مشاهده خواهیم کرد. و البته، با داشتن یک هسته تمام IP شبکه یک اپراتور، با بسیاری از پروتکل های اینترنتی که اکنون به خوبی می دانیم نیز مواجه خواهیم شد. بعد از توسعه اصول اولیه مورد نیاز برای این موضوعات، موضوعات اضافی G4 - مدیریت تحرک در بخش ۷.۶ و امنیت G4 در بخش ۸.۸ - را پوشش خواهیم داد. بحث ما در اینجا در مورد شبکه های G4 و G5 نسبتاً مختصر خواهد بود. شبکه های سلولی تلفن همراه منطقه ای با وسعت و عمق زیاد است که بسیاری از دانشگاه ها دوره های متعددی را در این زمینه ارائه می دهند. خوانندگانی

که به دنبال درک عمیق تر هستند تشویق می شوند [گودمن ۱۹۹۷; کارانن ۲۰۰۱; Lin 2001; کورهونن ۲۰۰۳; شیلر ۲۰۰۳; Palat 2009; اسکوریاس ۲۰۱۲; ترنر ۲۰۱۲; Akyildiz 2010]، و همچنین کتابهای بسیار عالی و جامع [Mouly 1992; ساتر ۲۰۱۴].

همانطور که RFC های اینترنت معماری و پروتکل های استاندارد اینترنت را تعریف می کنند، شبکه های G4 و G5 نیز توسط اسناد استاندارد می شوند که به عنوان مشخصات فنی شناخته می شوند، تعریف می شوند. این اسناد به صورت رایگان به صورت آنلاین در [GPP 2020۳] در دسترس هستند. دقیقاً مانند RFC ها، مشخصات فنی می تواند خواندن نسبتاً متراکم و دقیق را ایجاد کند. اما وقتی سوالی دارید، آنها منبع قطعی پاسخ هستند!

۷.۴.۱ شبکه های سلولی 4G LTE: معماری و عناصر

شبکه های 4G که تا زمان نگارش این مقاله در سال ۲۰۲۰ فراگیر هستند، استاندارد تکامل بلندمدت 4G یا به طور خلاصه 4G LTE را اجرا می کنند. در این بخش، شبکه های 4G LTE را توضیح خواهیم داد. شکل ۷.۱۷ عناصر اصلی معماری شبکه 4G LTE را نشان می دهد. این شبکه به طور گسترده به شبکه رادیویی در لبه شبکه سلولی و شبکه اصلی تقسیم می شود. همه عناصر شبکه با استفاده از پروتکل IP که در فصل ۴ مطالعه کردیم با یکدیگر ارتباط برقرار می کنند. مانند شبکه های 2G و 3G قبلی، 4G LTE مملو از کلمات اختصاری و نام عناصر نسبتاً مبهم است. ما سعی خواهیم کرد با تمرکز بر عملکردهای عنصر و نحوه تعامل عناصر مختلف شبکه 4G LTE با یکدیگر در هر دو صفحه داده و کنترل، این درهم ریختگی را برطرف کنیم:

- دستگاه موبایل. این یک گوشی هوشمند، تبلت، لپ تاپ یا دستگاه اینترنت اشیا است که به شبکه اپراتور تلفن همراه متصل می شود. اینجاست که برنامه هایی مانند مرورگرهای وب، برنامه های نقشه، برنامه های کنفرانس صوتی و ویدئویی، برنامه های پرداخت موبایلی و موارد دیگر اجرا می شوند. دستگاه تلفن همراه معمولاً پشته کامل پروتکل اینترنت ۵ لایه، از جمله لایه های انتقال و برنامه را پیاده سازی می کند، همانطور که با میزبان ها در لبه شبکه اینترنت دیدیم. دستگاه تلفن همراه یک نقطه پایانی شبکه است، با یک آدرس IP (همانطور که خواهیم دید از طریق NAT به دست می آید). این دستگاه تلفن همراه همچنین دارای یک شناسه ۶۴ بیتی منحصر بفرد جهانی به نام شناسه بین المللی مشترک تلفن همراه (IMSI) است که روی سیم کارت (ماژول هویت مشترک) آن ذخیره می شود. IMSI مشترک را در سیستم شبکه سراسری حامل تلفن همراه، از جمله کشور و شبکه حامل سلولی خانگی که مشترک به آن تعلق دارد، شناسایی می کند. از برخی جهات، IMSI مشابه آدرس MAC است. سیم کارت همچنین اطلاعات خدماتی را که مشترک می تواند به آنها دسترسی داشته باشد ذخیره می کند و اطلاعات کلید آن مشترک

را رمزگذاری می کند. در اصطلاح رسمی 4G LTE، دستگاه تلفن همراه به عنوان تجهیزات کاربر (UE) نامیده می شود. با این حال، در این کتاب درسی، ما از اصطلاح خواننده پسندتر «دستگاه تلفن همراه» استفاده خواهیم کرد. ما همچنین در اینجا متذکر می شویم که یک دستگاه تلفن همراه همیشه متحرک نیست. به عنوان مثال، دستگاه ممکن است یک سنسور دمای ثابت یا یک دوربین نظارتی باشد.

• ایستگاه پایه. ایستگاه پایه در "لبه" شبکه حامل قرار دارد و مسئول مدیریت منابع رادیویی بی سیم و دستگاه های تلفن همراه با منطقه تحت پوشش آن است (به عنوان یک سلول شش ضلعی در شکل ۷.۱۷ نشان داده شده است). همانطور که خواهیم دید، یک دستگاه تلفن همراه با یک ایستگاه پایه تعامل خواهد کرد تا به شبکه حامل متصل شود. ایستگاه پایه احراز هویت دستگاه و تخصیص منابع (دسترسی به کانال) را در شبکه دسترسی رادیویی هماهنگ می کند. از این نظر، عملکردهای ایستگاه پایه سلولی قابل مقایسه (اما به هیچ وجه یکسان) با عملکردهای AP در شبکه های محلی بی سیم هستند. اما ایستگاه های پایه سلولی چندین نقش مهم دیگر در شبکه های محلی بی سیم دارند. به طور خاص، ایستگاه های پایه تونل های IP خاص دستگاه را از دستگاه تلفن همراه به دروازه ها ایجاد می کنند و با یکدیگر تعامل می کنند تا تحرک دستگاه را در میان سلول ها مدیریت کنند. ایستگاه های پایه نزدیک نیز برای مدیریت طیف رادیویی برای به حداقل رساندن تداخل بین سلول ها با یکدیگر هماهنگ می شوند. در اصطلاح رسمی 4G LTE، ایستگاه پایه به عنوان "eNode-B" نامیده می شود که نسبتاً غیر شفاف و غیر توصیفی است. در این کتاب درسی، ما به جای آن از اصطلاح خواننده دوستانه «ایستگاه پایه» در سرتاسر استفاده خواهیم کرد.

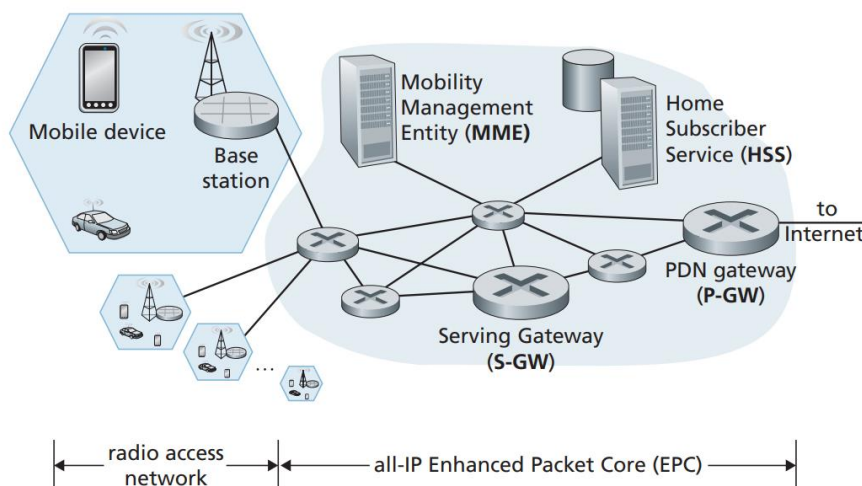


Figure 7.17 ♦ Elements of the 4G LTE architecture

به عنوان یک کنار، اگر اصطلاحات LTE را کمی مبهم می دانید، تنها نیستید! ریشه شناسی "eNode-B" ریشه در اصطلاحات قبلی 3G دارد، جایی که نقاط عملکرد شبکه به عنوان "گره" نامیده می شدند، با "B" به اصطلاحات قبلی "ایستگاه پایه 1G" (BS) یا "ایستگاه فرستنده و گیرنده پایه (BTS)" در اصطلاحات 2G. 4G LTE یک تحول

"e" بر روی 3G است، و از این رو، "e" اکنون مقدم بر "Node-B" در اصطلاحات 4G LTE است. این نامشخص بودن هیچ نشانه‌ای در توقف ندارد! در سیستم‌های 5G، عملکردهای eNode-B اکنون به عنوان "ng-eNB" شناخته می‌شوند. شاید بتوانید حدس بزنید که مخفف آن چیست!

• سرور مشترک خانگی (HSS). همانطور که در شکل ۷.۱۸ نشان داده شده است، HSS یک عنصر صفحه کنترل است. HSS یک پایگاه داده است که اطلاعات مربوط به دستگاه‌های تلفن همراه را که شبکه HSS شبکه خانگی آنهاست ذخیره می‌کند. برای احراز هویت دستگاه همراه با MME (در زیر بحث شده است) استفاده می‌شود.

• دروازه سرویس (S-GW)، دروازه شبکه داده بسته (P-GW)، و سایر روترهای شبکه. همانطور که در شکل ۷.۱۸ نشان داده شده است، دروازه سرویس و دروازه شبکه داده بسته دو روتر هستند (اغلب در عمل با هم قرار می‌گیرند) که در مسیر داده بین دستگاه تلفن همراه و اینترنت قرار دارند. دروازه PDN همچنین آدرس‌های IP NAT را برای دستگاه‌های تلفن همراه ارائه می‌دهد و عملکردهای NAT را انجام می‌دهد (به بخش ۴.۳.۴ مراجعه کنید). دروازه PDN آخرین عنصر LTE است که دیتاگرام منشأ گرفته از یک دستگاه تلفن همراه قبل از ورود به اینترنت بزرگتر با آن روبرو می‌شود. از نظر دنیای خارج، P-GW مانند هر مسیریاب دروازه دیگری به نظر می‌رسد. تحرک گره‌های تلفن همراه در شبکه LTE حامل سلولی از دنیای بیرون در پشت P-GW پنهان است. علاوه بر این مسیریاب‌های دروازه، هسته تمام IP یک حامل سلولی دارای روترهای اضافی خواهد بود که نقش آنها شبیه به روترهای IP سنتی است - برای ارسال داده‌های IP بین خود در طول مسیرهایی که معمولاً به عناصر شبکه اصلی LTE ختم می‌شوند.

• نهاد مدیریت تحرک (MME). همانطور که در شکل ۷.۱۸ نشان داده شده است، MME نیز یک عنصر صفحه کنترل است. همراه با HSS، نقش مهمی در احراز هویت دستگاهی ایفا می‌کند که می‌خواهد به شبکه خود متصل شود. همچنین تونل‌ها را در مسیر داده از/به دستگاه و مسیریاب دروازه اینترنت PDN تنظیم می‌کند و اطلاعات مربوط به مکان سلولی یک دستگاه تلفن همراه فعال را در شبکه تلفن همراه حامل حفظ می‌کند. اما همانطور که در شکل ۷.۱۸ نشان داده شده است، در مسیر ارسال دیتاگرام‌های دستگاه تلفن همراه به/از اینترنت نیست.

احراز هویت. برای شبکه و دستگاه تلفن همراه متصل به شبکه مهم است که به طور متقابل یکدیگر را احراز هویت کنند—برای اینکه شبکه بداند که دستگاه متصل در واقع دستگاه مرتبط با یک IMSI معین است و برای دستگاه تلفن همراه بداند که شبکه به آن را متصل می‌کند نیز یک شبکه حامل سلولی قانونی است. ما احراز هویت را در فصل ۸ و احراز هویت 4G را در بخش ۸.۸ پوشش خواهیم داد. در اینجا، ما به سادگی متذکر می‌شویم که MME نقش واسطه‌ای را بین سرویس تلفن همراه و مشترکین خانگی (HSS) در شبکه خانگی تلفن همراه ایفا

می کند. به طور خاص، پس از دریافت درخواست پیوست از دستگاه تلفن همراه، MME محلی با HSS در شبکه خانگی تلفن همراه تماس می گیرد. سپس HSS خانه تلفن همراه به اندازه کافی اطلاعات رمزگذاری شده را به MME محلی برمی گرداند تا به دستگاه تلفن همراه ثابت کند که HSS خانه از طریق این MME احراز هویت را انجام می دهد و دستگاه تلفن همراه به MME ثابت کند که واقعاً تلفن همراه مرتبط با آن IMSI است. هنگامی که یک دستگاه تلفن همراه به شبکه خانگی خود متصل می شود، HSS که در طول احراز هویت با آن تماس گرفته می شود در همان شبکه خانگی قرار دارد. با این حال، هنگامی که یک دستگاه تلفن همراه در یک شبکه بازدید شده رومینگ است که توسط یک حامل شبکه سلولی متفاوت اداره می شود، MME در آن شبکه رومینگ باید با HSS در شبکه خانگی دستگاه تلفن همراه تماس بگیرد.

راه اندازی مسیر همانطور که در نیمه پایینی شکل ۷.۱۸ نشان داده شده است، مسیر داده از دستگاه تلفن همراه به مسیریاب دروازه حامل شامل اولین پرش بی سیم بین دستگاه تلفن همراه و ایستگاه پایه، و تونل های IP به هم پیوسته بین ایستگاه پایه و دروازه سرویس است. Serving Gateway و PDN Gateway. تونل ها تحت کنترل MME راه اندازی می شوند و برای ارسال اطلاعات (به جای ارسال مستقیم بین مسیریاب های شبکه) برای تسهیل تحرک دستگاه استفاده می شوند—هنگامی که دستگاه حرکت می کند، تنها نقطه پایانی تونل که به ایستگاه پایه ختم می شود باید تغییر کند، در حالی که سایر تونل ها باید تغییر نکنند. نقاط پایانی، و کیفیت خدمات مرتبط با یک تونل، بدون تغییر باقی می ماند.

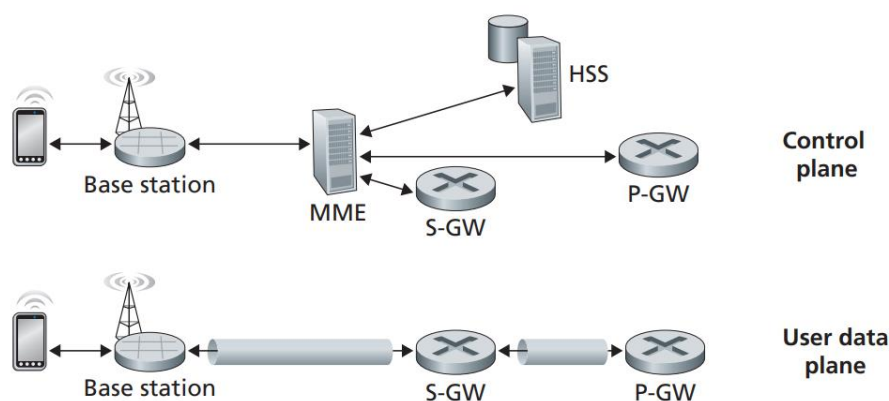


Figure 7.18 ♦ LTE data-plane and control-plane elements

ردیابی موقعیت سلولی همانطور که دستگاه بین سلول ها حرکت می کند، ایستگاه های پایه MME را در مکان دستگاه به روز می کنند. اگر دستگاه تلفن همراه در حالت خواب باشد اما با این وجود بین سلول ها حرکت کند، ایستگاه های پایه دیگر نمی توانند مکان دستگاه را ردیابی کنند. در این صورت، مسئولیت مکان یابی دستگاه برای بیدار شدن، از طریق فرآیندی به نام پیچینگ، بر عهده MME خواهد بود.

جدول ۷.۲ عناصر کلیدی معماری LTE را که در بالا مورد بحث قرار داده‌ایم خلاصه می‌کند و این عملکردها را با عملکردهایی که در مطالعه خود در مورد شبکه‌های محلی بی‌سیم (WiFi (WLAN) با آن‌ها مواجه بودیم، مقایسه می‌کند. شرح عنصر LTE عملکرد(های) مشابه WLAN

LTE Element	Description	Similar WLAN function(s)
Mobile device (UE: User equipment)	End user's IP-capable wireless/mobile device (e.g., smartphone, tablet, laptop)	Host, end-system
Base Station (eNode-B)	Network side of wireless access link into LTE network	Access point (AP), although the LTE base station performs many functions not found in WLANs
The Mobility Management Entity (MME)	Coordinator for mobile device services: authentication, mobility management	Access point (AP), although the MME performs many functions not found in WLANs
Home Subscriber Server (HSS)	Located in a mobile device's <i>home</i> network, providing authentication, access privileges in home and visited networks	No WLAN equivalent
Serving Gateway (S-GW), PDN-Gateway (P-GW)	Routers in a cellular carrier's network, coordinating forwarding to outside of the carrier's network	iBGP and eBGP routers in access ISP network
Radio Access Network	Wireless link between mobile device and a base station	802.11 wireless link between mobile and AP

Table 7.2 ♦ LTE Elements, and similar WLAN (WiFi) functions

۷.۴.۲ پشته پروتکل های LTE

از آنجایی که معماری 4G LTE یک معماری تمام IP است، ما در حال حاضر با پروتکل های لایه بالاتر در پشته پروتکل LTE، به ویژه پروتکل های IP، TCP، UDP و لایه های کاربردی مختلف، از مطالعات خود در فصل ۲ بسیار آشنا هستیم. از طریق ۵. در نتیجه، پروتکل های LTE جدید که در اینجا بر آنها تمرکز خواهیم کرد، در درجه اول در پیوند و لایه های فیزیکی و در مدیریت تحرک هستند.

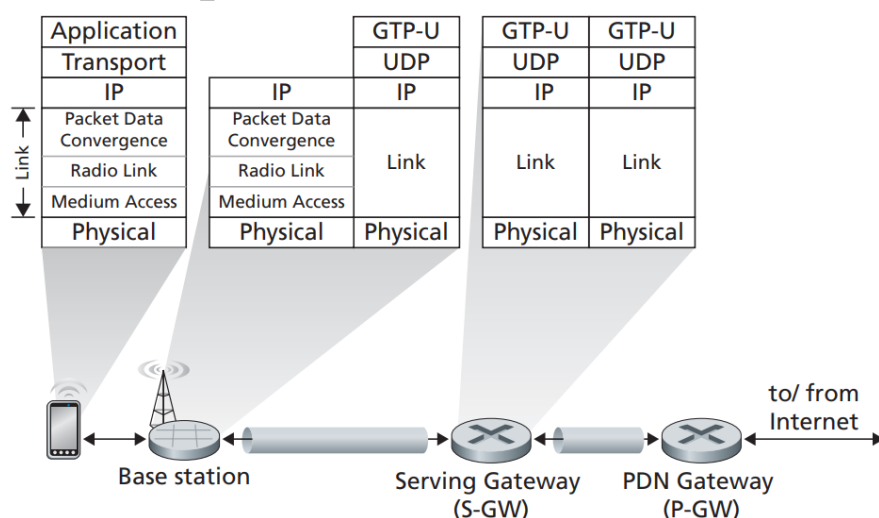


Figure 7.21 ♦ LTE data-plane protocol stacks

شکل ۷.۲۱ پشته های پروتکل صفحه کاربر را در گره موبایل LTE، ایستگاه پایه و دروازه سرویس دهی نشان می دهد. ما بعداً با مطالعه مدیریت تحرک LTE (بخش ۷.۶) و امنیت (بخش ۸.۸) به چندین پروتکل صفحه کنترل LTE خواهیم پرداخت. همانطور که از شکل ۷.۲۱ می بینیم، بیشتر فعالیت های جدید و جالب پروتکل صفحه کاربر در پیوند رادیویی بی سیم بین دستگاه تلفن همراه و ایستگاه پایه انجام می شود.

LTE لایه پیوند دستگاه تلفن همراه را به سه زیر لایه تقسیم می کند:

- همگرایی داده های بسته. Packet Data Convergence این بالاترین زیرلایه لایه پیوند درست زیر IP قرار دارد. پروتکل همگرایی داده های بسته [3GPP PDCP 2019] (PDCP) سرآیند/فشرده سازی IP را به منظور کاهش تعداد بیت های ارسال شده از طریق پیوند بی سیم و رمزگذاری/رمزگشایی دیتاگرام IP با استفاده از کلیدهایی که از طریق پیام های سیگنالینگ بین دستگاه تلفن همراه LTE و نهاد مدیریت تحرک (MME) هنگامی که دستگاه تلفن همراه برای اولین بار به شبکه متصل شد. ما جنبه های امنیت LTE را در بخش ۸.۸.۲ پوشش خواهیم داد.

- کنترل پیوند رادیویی. Radio Link Control. پروتکل کنترل پیوند رادیویی [3GPP RLCP 2018] (RLC) دو عملکرد مهم را انجام می دهد: (i) تکه تکه کردن (در سمت ارسال) و مونتاژ مجدد (در گیرنده) دیتاگرام های IP که خیلی بزرگ هستند و نمی توانند در لایه پیوند زیرین قرار بگیرند. فریم ها، و (ii) انتقال داده های قابل اعتماد در لایه پیوند با استفاده از یک پروتکل ARQ مبتنی بر ACK/NAK. به یاد بیاورید که ما عناصر اساسی پروتکل های ARQ را در بخش ۳.۴.۱ مطالعه کرده ایم.

- کنترل دسترسی متوسط (MAC). لایه MAC برنامه ریزی انتقال را انجام می دهد، یعنی درخواست و استفاده از اسلات های انتقال رادیویی شرح داده شده در بخش ۷.۴.۴. زیرلایه MAC همچنین توابع تشخیص/تصحیح خطای اضافی را انجام می دهد، از جمله استفاده از انتقال بیت اضافی به عنوان یک تکنیک تصحیح خطا به جلو. مقدار افزودنی را می توان با شرایط کانال تطبیق داد.

شکل ۷.۲۱ نیز استفاده از تونل ها را در مسیر داده های کاربر نشان می دهد. همانطور که در بالا توضیح داده شد، این تونل ها، تحت کنترل MME، زمانی ایجاد می شوند که دستگاه تلفن همراه برای اولین بار به شبکه متصل می شود. هر تونل بین دو نقطه پایانی دارای یک شناسه نقطه پایانی تونل (TEID) منحصر به فرد است. هنگامی که ایستگاه پایه دیتاگرام ها را از دستگاه تلفن همراه دریافت می کند، آنها را با استفاده از پروتکل تونل زنی GPRS [3GPP GTPv1-U 2019] شامل TEID کپسوله می کند و آنها را در بخش های UDP به دروازه سرویس در انتهای دیگر تونل می فرستد. در سمت دریافت، ایستگاه پایه دیتاگرام های UDP تونلی شده را کپسوله می کند، دیتاگرام

IP محصور شده را که برای دستگاه تلفن همراه ارسال می شود استخراج می کند و دیتاگرام IP را از طریق پرش بی سیم به دستگاه تلفن همراه ارسال می کند.

۷.۴.۳ شبکه دسترسی رادیویی LTE

LTE از ترکیبی از مالتی پلکسی تقسیم فرکانس و مالتی پلکس تقسیم زمانی در کانال پایین دستی استفاده می کند که به عنوان مالتی پلکسی تقسیم فرکانس متعامد (OFDM) شناخته می شود [Hwang 2009]. (اصطلاح "متعامد" از این واقعیت ناشی می شود که سیگنال هایی که در کانال های فرکانس مختلف ارسال می شوند به گونه ای ایجاد می شوند که تداخل بسیار کمی با یکدیگر دارند، حتی زمانی که فرکانس های کانال با یکدیگر فاصله دارند). در LTE، به هر دستگاه تلفن همراه فعال یک یا چند اسلات زمانی ۰.۵ میلی ثانیه در یک یا چند فرکانس کانال اختصاص داده می شود. شکل ۷.۲۲ تخصیص هشت شکاف زمانی را در چهار فرکانس نشان می دهد. با تخصیص روزافزون اسلات های زمانی بیشتر (چه در یک فرکانس یا در فرکانس های مختلف)، یک دستگاه تلفن همراه قادر به دستیابی به نرخ های انتقال فزاینده ای است. تخصیص (دوباره) اسلات بین دستگاه های تلفن همراه را می توان به اندازه یک بار در هر میلی ثانیه انجام داد. همچنین می توان از طرح های مدولاسیون مختلف برای تغییر نرخ انتقال استفاده کرد. بحث قبلی ما در مورد شکل ۷.۳ و انتخاب پویا از طرح های مدولاسیون در شبکه های WiFi را ببینید.

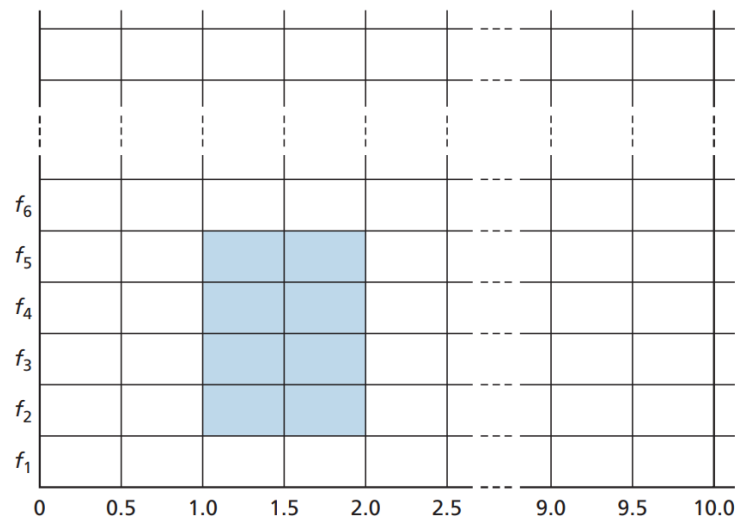


Figure 7.22 ♦ Twenty 0.5-ms slots organized into 10 ms frames at each frequency. An eight-slot allocation is shown shaded.

تخصیص خاص اسلات های زمانی به دستگاه های تلفن همراه توسط استاندارد LTE الزامی نیست. در عوض، تصمیم گیری در مورد اینکه کدام دستگاه های تلفن همراه مجاز به انتقال در یک شکاف زمانی معین در یک فرکانس

معین هستند، توسط الگوریتم های زمان بندی ارائه شده توسط فروشنده تجهیزات LTE و/یا اپراتور شبکه تعیین می شود. با برنامه ریزی فرصت طلبانه [Bender 2000; کلدینگ ۲۰۰۳; Kulkarni 2005]، تطبیق پروتکل لایه فیزیکی با شرایط کانال بین فرستنده و گیرنده و انتخاب گیرنده هایی که بسته ها بر اساس شرایط کانال به آنها ارسال می شود، به ایستگاه پایه اجازه می دهد تا بهترین استفاده را از رسانه بی سیم داشته باشد. علاوه بر این، اولویت های کاربر و سطوح قراردادی خدمات (به عنوان مثال، نقره، طلا یا پلاتین) می توانند در برنامه ریزی انتقال بسته های پایین دستی استفاده شوند. علاوه بر قابلیت های LTE که در بالا توضیح داده شد، LTE-Advanced با تخصیص کانال های انبوه به یک دستگاه تلفن همراه، پهنای باند پایین دستی صدها مگابیت در ثانیه را امکان پذیر می کند [Akyildiz 2010].

۷.۴.۴ توابع اضافی LTE: پیوست شبکه و مدیریت توان

اجازه دهید در اینجا G_{LTE4} را با در نظر گرفتن دو عملکرد مهم LTE نتیجه گیری یا مطالعه کنیم: (۱) فرآیندی که یک دستگاه تلفن همراه برای اولین بار به شبکه متصل می شود و (۲) تکنیک های مورد استفاده دستگاه تلفن همراه، در ارتباط با عناصر اصلی شبکه، برای مدیریت مصرف برق آن

پیوست شبکه

فرآیندی که توسط آن یک دستگاه تلفن همراه به شبکه حامل تلفن همراه متصل می شود به طور کلی به سه مرحله تقسیم می شود:

- پیوست به یک ایستگاه پایه. این مرحله اول اتصال دستگاه از نظر هدف مشابه است، اما در عمل کاملاً متفاوت از پروتکل ارتباطی ۸۰۲.۱۱ است که در بخش ۷.۳۱ مطالعه کردیم. دستگاه تلفن همراهی که بخواهد به یک شبکه حامل سلولی متصل شود، یک فرآیند بوت استرپ را برای یادگیری و سپس ارتباط با یک ایستگاه پایه نزدیک آغاز می کند. دستگاه تلفن همراه در ابتدا همه کانال ها را در همه باندهای فرکانسی برای یک سیگنال همگام سازی اولیه جستجو می کند که به صورت دوره ای هر ۵ میلی ثانیه توسط یک ایستگاه پایه پخش می شود. هنگامی که این سیگنال پیدا شد، دستگاه تلفن همراه در این فرکانس باقی می ماند و سیگنال همگام سازی ثانویه را تعیین می کند. با اطلاعاتی که در سیگنال دوم یافت می شود، دستگاه می تواند اطلاعات اضافی مانند پهنای باند کانال، پیکربندی کانال و اطلاعات حامل سلولی آن ایستگاه پایه را (پس از چند مرحله دیگر) پیدا کند. مجهز به این اطلاعات، دستگاه تلفن همراه می تواند یک ایستگاه پایه را برای ارتباط با آن انتخاب کند (در صورت وجود ترجیحاً به شبکه خانگی خود متصل شود) و یک اتصال سیگنالینگ صفحه کنترل را در سراسر پرش بی سیم با آن ایستگاه پایه برقرار کند. این کانال تلفن همراه به ایستگاه پایه از طریق بقیه فرآیند پیوست شبکه استفاده خواهد شد.

• احراز هویت متقابل. در توضیحات قبلی ما در مورد نهاد مدیریت تحرک (MME) در بخش ۷.۴.۱، اشاره کردیم که ایستگاه پایه با MME محلی تماس می گیرد تا احراز هویت متقابل را انجام دهد - فرآیندی که در بخش ۸.۸.۲ با جزئیات بیشتر بررسی خواهیم کرد. این مرحله دوم اتصال به شبکه است که به شبکه امکان می دهد بداند که دستگاه متصل در واقع دستگاه مرتبط با یک IMSI مشخص است، و دستگاه تلفن همراه بداند که شبکه ای که به آن متصل می شود نیز یک شبکه حامل سلولی قانونی است. هنگامی که این مرحله دوم از اتصال به شبکه کامل شد، MME و دستگاه تلفن همراه متقابلاً یکدیگر را احراز هویت کردند، و MME همچنین هویت ایستگاه پایه ای را که تلفن همراه به آن متصل است، می داند. مجهز به این اطلاعات، MME اکنون آماده پیکربندی مسیر داده Mobile-Device-to-PDN-gateway است.

• پیکربندی مسیر داده از دستگاه موبایل به دروازه MME. PDN با دروازه PDN (که همچنین یک آدرس NAT برای دستگاه تلفن همراه ارائه می دهد)، دروازه سرویس و ایستگاه پایه برای ایجاد دو تونل نشان داده شده در شکل ۷.۲۱ تماس می گیرد. پس از تکمیل این مرحله، دستگاه تلفن همراه قادر است دیتاگرام های IP را از طریق ایستگاه پایه از طریق این تونل ها به و از اینترنت ارسال و دریافت کند!

مدیریت انرژی: حالت های خواب

در بحث قبلی ما در مورد ویژگی های پیشرفته در ۸.۲.۱۱ (بخش ۷.۳.۵) و بلوتوث (بخش ۷.۳.۶) به یاد بیاورید که یک رادیو در یک دستگاه بی سیم ممکن است در حالت خواب برای صرفه جویی در مصرف برق در زمانی که ارسال یا دریافت نمی کند به منظور به حداقل رساندن آن وارد شود. مدت زمانی که مدار دستگاه تلفن همراه برای ارسال/دریافت داده و برای سنجش کانال باید "روشن" باشد. در 4G LTE، یک دستگاه تلفن همراه خواب می تواند در یکی از دو حالت خواب متفاوت باشد. در حالت دریافت ناپیوسته، که معمولاً پس از چند صد میلی ثانیه عدم فعالیت وارد می شود [Sauter 2014]، دستگاه تلفن همراه و ایستگاه پایه زمان های دوره ای را از قبل برنامه ریزی می کنند (معمولاً با فاصله چند صد میلی ثانیه) که در آن دستگاه تلفن همراه بیدار می شود و به طور فعال کانال را برای انتقال پایین دست (ایستگاه پایه به دستگاه تلفن همراه) نظارت کنید. با این حال، جدا از این زمان های برنامه ریزی شده، رادیو دستگاه تلفن همراه در حالت خواب خواهد بود.

اگر حالت دریافت ناپیوسته را بتوان یک "خواب سبک" در نظر گرفت، حالت خواب دوم - حالت بیکار - که پس از دوره های طولانی تری از ۵ تا ۱۰ ثانیه بی تحرکی دنبال می شود، ممکن است به عنوان "خواب عمیق" در نظر گرفته شود. در حالی که در این خواب عمیق، رادیو دستگاه تلفن همراه بیدار می شود و کانال را حتی کمتر نظارت می کند. در واقع، این خواب آنقدر عمیق است که اگر دستگاه تلفن همراه در حین خواب به سلول جدیدی در شبکه

حامل منتقل شود، نیازی به اطلاع ایستگاه پایه ای که قبلاً با آن مرتبط بوده است، نیست. بنابراین، هنگام بیدار شدن دوره‌ای از این خواب عمیق، دستگاه تلفن همراه باید مجدداً با یک ایستگاه پایه (احتمالاً جدید) ارتباط برقرار کند تا پیام‌های صفحه‌بندی پخش شده توسط MME به ایستگاه‌های پایه نزدیک ایستگاه پایه را بررسی کند. تلفن همراه آخرین بار مرتبط شد. این پیام‌های صفحه‌بندی صفحه‌کنترلی، که توسط این ایستگاه‌های پایه برای همه دستگاه‌های تلفن همراه در سلول‌هایشان پخش می‌شوند، نشان می‌دهند که کدام دستگاه‌های تلفن همراه باید به طور کامل بیدار شوند و یک اتصال صفحه داده جدید به ایستگاه پایه را دوباره برقرار کنند (شکل ۷.۱۸ را ببینید) جهت دریافت بسته های دریافتی

۷.۴.۵ شبکه سلولی جهانی: شبکه ای از شبکه ها

پس از مطالعه معماری شبکه سلولی G4، اجازه دهید یک گام به عقب برگردیم و نگاهی به نحوه سازماندهی شبکه سلولی جهانی – که خود یک «شبکه شبکه‌ها» مانند اینترنت است، بیاندازیم. شکل ۷.۲۳ تلفن هوشمند تلفن همراه کاربر را نشان می‌دهد که از طریق یک ایستگاه پایه G4 به شبکه خانگی خود متصل شده است. شبکه تلفن همراه خانگی کاربر توسط یک شرکت مخابراتی تلفن همراه مانند AT&T، Verizon، T-Mobile یا Sprint در ایالات متحده اداره می‌شود. نارنجی در فرانسه؛ یا SK Telecom در کره. شبکه خانگی کاربر، به نوبه خود، به شبکه های دیگر حامل های سلولی و به اینترنت جهانی متصل است، اگرچه یک یا چند مسیریاب دروازه در شبکه خانگی، همانطور که در شکل ۷.۲۳ نشان داده شده است. خود شبکه‌های تلفن همراه یا از طریق اینترنت عمومی یا از طریق یک شبکه تبادل بسته پروتکل اینترنت [GSMA 2018a] (IPX) به یکدیگر متصل می‌شوند. IPX یک شبکه مدیریت شده است که به طور خاص برای اتصال حامل های سلولی به هم متصل می‌شود، مشابه نقاط تبادل اینترنت (به شکل ۱.۱۵ مراجعه کنید) برای هم‌تاسازی بین ISP ها. از شکل ۷.۲۳، می‌توانیم ببینیم که شبکه سلولی جهانی در واقع "شبکه ای از شبکه ها" است – درست مانند اینترنت (شکل ۱.۱۵ و بخش ۵.۴ را به یاد بیاورید). شبکه‌های G4 همچنین می‌توانند با شبکه‌های صوتی/داده سلولی G3 و شبکه‌های فقط صوتی قبلی هم‌تا شوند.

ما به زودی به موضوعات اضافی G LTE4 – مدیریت تحرک در بخش ۷.۶، و امنیت G4 در بخش ۸.۸.۲ – بعد از توسعه اصول اولیه مورد نیاز برای این موضوعات، باز خواهیم گشت. بیایید اکنون نگاهی گذرا به شبکه های در حال ظهور G5 بیندازیم.

۷.۴.۶ شبکه های سلولی G5

سرویس دیتای وسیع منطقه نهایی، سرویسی با سرعت اتصال گیگابیتی همه جا، تأخیر بسیار کم و محدودیت های نامحدود در تعداد کاربران و دستگاه هایی است که می‌توانند در هر منطقه ای پشتیبانی شوند. چنین سرویسی

درها را به روی انواع برنامه های کاربردی جدید از جمله واقعیت افزوده فراگیر و واقعیت مجازی، کنترل وسایل نقلیه خودران از طریق اتصالات بی سیم، کنترل ربات ها در کارخانه ها از طریق اتصالات بی سیم، و جایگزینی فناوری های دسترسی مسکونی مانند DSL و کابل، با خدمات اینترنت بی سیم ثابت (یعنی اتصالات بی سیم مسکونی از ایستگاه های پایه به مودم ها در خانه ها).

انتظار می رود که 5G، که نسخه های بهبود یافته آن احتمالاً در دهه ۲۰۲۰ عرضه می شوند، گام بزرگی در جهت دستیابی به اهداف سرویس داده گسترده گسترده خواهد برد. پیش بینی می شود که 5G تقریباً ۱۰ برابر افزایش در اوج بیت ریت، کاهش ۱۰ برابری تأخیر و افزایش ۱۰۰ برابری ظرفیت ترافیک را نسبت به 4G ارائه می کند [Qualcomm 2019].

در اصل، 5G به "G NR (راديو جديد)" اشاره دارد که استاندارد است که توسط 3GPP اتخاذ شده است. با این حال، سایر فناوری های 5G به جز NR وجود دارند. به عنوان مثال، شبکه G TFA اختصاصی Verizon روی فرکانس های ۲۸ و ۳۹ گیگاهرتز کار می کند و فقط برای سرویس اینترنت بی سیم ثابت و نه در گوشی های هوشمند استفاده می شود.

استانداردهای 5G فرکانس ها را به دو گروه تقسیم می کنند: FR1 (۴۵۰ مگاهرتز-۶ گیگاهرتز) و FR2 (۲۴ گیگاهرتز-۵۲ گیگاهرتز). بیشتر استقرارهای اولیه در فضای FR1 خواهد بود، اگرچه از سال ۲۰۲۰ در فضای FR2 برای دسترسی به اینترنت ثابت مسکونی همانطور که در بالا ذکر شد، استقرارهای اولیه وجود دارد. نکته مهم، جنبه های لایه فیزیکی (یعنی بی سیم) 5G با سیستم های ارتباطات سیار 4G مانند LTE سازگار نیست: به ویژه، نمی توان آن را با به روزرسانی های ایستگاه پایه یا به روزرسانی های نرم افزاری به گوشی های هوشمند موجود تحویل داد. بنابراین، در انتقال به 5G، اپراتورهای بی سیم باید سرمایه گذاری قابل توجهی در زیرساخت های فیزیکی انجام دهند.

فرکانس های FR2 به فرکانس های موج میلی متری نیز معروف هستند. در حالی که فرکانس های موج میلی متری سرعت داده های بسیار سریع تری را امکان پذیر می کنند، اما دو اشکال عمده دارند:

- فرکانس های موج میلی متری از ایستگاه پایه تا گیرنده برد بسیار کوتاه تری دارند. این باعث می شود که فناوری امواج میلی متری در مناطق روستایی نامناسب باشد و مستلزم استقرار مکرر تر ایستگاه های پایه در مناطق شهری است.

- ارتباط موج میلی متری به شدت مستعد تداخل جوی است. شاخ و برگ های نزدیک و باران می توانند برای استفاده در فضای باز مشکلاتی ایجاد کنند.

۵G یک استاندارد منسجم نیست، اما در عوض از سه استاندارد مشترک تشکیل شده است [Dahlman 2018]:

- eMBB (پهن باند موبایل پیشرفته). استقرار اولیه 5G NR بر روی eMBB متمرکز شده است که پهنای باند بیشتری را برای سرعت دانلود و آپلود بالاتر و همچنین کاهش متوسط تاخیر در مقایسه با 4G LTE فراهم می کند. eMBB برنامه های رسانه ای غنی، مانند واقعیت افزوده موبایل و واقعیت مجازی، و همچنین وضوح 4K موبایل و پخش ویدئو ۳۶۰ درجه را فعال می کند.

- URLLC (ارتباطات با تأخیر کم بسیار قابل اعتماد). URLLC برای برنامه هایی که به تأخیر بسیار حساس هستند، مانند اتوماسیون کارخانه و رانندگی مستقل، هدف قرار می گیرد. URLLC تأخیرهای ۱ میلی ثانیه را هدف قرار می دهد. از زمان نگارش این مقاله، فناوری هایی که URLLC را فعال می کنند هنوز در حال استاندارد شدن هستند.

- mMTC (ارتباطات نوع ماشین عظیم). mMTC یک نوع دسترسی باریک برای کاربردهای سنجش، اندازه گیری و نظارت است. یکی از اولویتهای طراحی شبکه های 5G، کاهش موانع برای اتصال شبکه برای دستگاه های IoT است. علاوه بر کاهش تأخیر، فناوری های نوظهور برای شبکه های 5G بر کاهش نیازهای برق تمرکز می کنند و استفاده از دستگاه های IoT را فراگیرتر از 4G LTE می کنند.

فرکانس های امواج 5G و میلی متری

بسیاری از نوآوری های 5G نتیجه مستقیم کار در فرکانس های امواج میلی متری در باند ۲۴ گیگاهرتز تا ۵۲ گیگاهرتز خواهد بود. به عنوان مثال، این فرکانس ها پتانسیل دستیابی به ۱۰۰ برابر افزایش ظرفیت را در 4G ارائه می دهند. برای به دست آوردن بینش در این مورد، ظرفیت را می توان به عنوان حاصل ضرب سه عبارت تعریف کرد [Björnson 2017]:

ظرفیت = چگالی سلول * طیف موجود * بازده طیفی

که در آن چگالی سلول بر حسب واحد سلول/کیلومتر مربع است، طیف موجود بر حسب واحد هرتز است، و بازده طیفی معیاری است از میزان کارآمدی هر ایستگاه پایه می تواند با کاربران ارتباط برقرار کند و بر حسب واحد bps/Hz/cell است. با ضرب این واحدها، به راحتی می توان دریافت که ظرفیت بر حسب واحد bps/km² است. برای هر یک از این سه عبارت، مقادیر برای 5G بزرگتر از 4G خواهد بود:

- از آنجایی که فرکانس های میلی متری برد بسیار کمتری نسبت به فرکانس های 4G LTE دارند، به ایستگاه های پایه بیشتری نیاز است که به نوبه خود تراکم سلول را افزایش می دهد.

• از آنجایی که G FR25 در یک باند فرکانسی بسیار بزرگتر ($52 - 24 = 28$ گیگاهرتز) نسبت به G LTE4 (تا حدود 2 گیگاهرتز) کار می کند، طیف در دسترس بیشتری دارد.

• با توجه به بازده طیفی، نظریه اطلاعات می گوید که اگر می خواهید بازده طیفی را دو برابر کنید، افزایش 17 برابری در توان لازم است [Björnson 2017]. به جای افزایش قدرت، G5 از فناوری MIMO استفاده می کند (همان فناوری که در مطالعه خود درباره شبکه های 802.11 در بخش 7.3 با آن مواجه شدیم)، که از چندین آنتن در هر ایستگاه پایه استفاده می کند. هر آنتن MIMO به جای پخش سیگنال در همه جهات، از شکل دهی پرتو استفاده می کند و سیگنال را به سمت کاربر هدایت می کند. فناوری MIMO به یک ایستگاه پایه اجازه می دهد تا به 10 تا 20 کاربر به طور همزمان در یک باند فرکانسی یکسان ارسال کند.

انتظار می رود با افزایش هر سه عبارت معادله ظرفیت، G5 افزایش 100 برابری ظرفیت را در مناطق شهری ایجاد کند. به طور مشابه، با توجه به باند فرکانسی بسیار گسترده تر، انتظار می رود G5 حداکثر سرعت دانلود 1 گیگابیت بر ثانیه یا بالاتر را ارائه دهد.

با این حال، سیگنال های موج میلی متری به راحتی توسط ساختمان ها و درختان مسدود می شوند. ایستگاه های سلولی کوچک برای پر کردن شکاف های پوشش بین ایستگاه های پایه و کاربران مورد نیاز است. در یک منطقه بسیار پرجمعیت، فاصله بین دو سلول کوچک می تواند از 10 تا 100 متر متغیر باشد [Dahlman 2018].

شبکه اصلی G5

شبکه G Core5 شبکه داده ای است که تمام اتصالات صوتی، داده و اینترنت G5 تلفن همراه را مدیریت می کند. شبکه G Core5 برای ادغام بهتر با اینترنت و خدمات مبتنی بر ابر در حال طراحی مجدد است و همچنین شامل سرورهای توزیع شده و حافظه پنهان در سراسر شبکه می شود و در نتیجه تاخیر را کاهش می دهد. مجازی سازی عملکرد شبکه (همانطور که در فصل های 4 و 5 مورد بحث قرار گرفت)، و برش شبکه برای برنامه ها و سرویس های مختلف، در هسته مدیریت خواهد شد.

مشخصات جدید G Core5 تغییرات عمده ای را در نحوه پشتیبانی شبکه های تلفن همراه از طیف گسترده ای از خدمات با عملکرد متفاوت ایجاد می کند. همانطور که در مورد شبکه هسته G4 (شکل های 7.17 و 7.18 را به یاد آورید)، هسته G5 ترافیک داده را از دستگاه های پایانی رله می کند، دستگاه ها را احراز هویت می کند و تحرک دستگاه را مدیریت می کند. هسته G5 همچنین شامل تمام عناصر شبکه ای است که در بخش 7.4.2 با آنها مواجه شدیم - دستگاه های تلفن همراه، سلول ها، ایستگاه های پایه و نهاد مدیریت تحرک (اکنون به دو عنصر فرعی تقسیم می شوند، همانطور که در زیر بحث می شود). HSS و سرویس دهی و دروازه های PDN.

اگرچه شبکه‌های هسته‌ای G4 و G5 عملکردهای مشابهی را انجام می‌دهند، اما تفاوت‌های عمده‌ای در معماری هسته جدید G5 وجود دارد. هسته G5 برای کنترل کامل و جداسازی کاربر از صفحه طراحی شده است (به فصل ۵ مراجعه کنید). هسته G5 کاملاً از عملکردهای شبکه مبتنی بر نرم افزار مجازی سازی شده تشکیل شده است. این معماری جدید به اپراتورها این انعطاف‌پذیری را می‌دهد تا نیازهای متنوع برنامه‌های G5 مختلف را برآورده کنند. برخی از عملکردهای جدید شبکه اصلی G5 عبارتند از [Rommer 2019]:

- عملکرد هواپیمای کاربر (UPF). کنترل و جداسازی صفحه کاربر (به فصل ۵ مراجعه کنید) به پردازش بسته اجازه می‌دهد تا به لبه شبکه توزیع شود.
- عملکرد مدیریت دسترسی و تحرک (AMF). هسته G5 اساساً موجودیت مدیریت تحرک 4 (MME) G را به دو عنصر کاربردی تجزیه می‌کند: AMF و SMF. تمام اطلاعات اتصال و جلسه را از تجهیزات کاربر نهایی دریافت می‌کند اما فقط وظایف مدیریت اتصال و تحرک را انجام می‌دهد.
- عملکرد مدیریت جلسه (SMF). مدیریت جلسه توسط عملکرد مدیریت جلسه (SMF) انجام می‌شود. SMF مسئول تعامل با صفحه داده جدا شده است. SMF همچنین مدیریت آدرس IP را انجام می‌دهد و نقش DHCP را ایفا می‌کند.

از زمان نوشتن این مقاله (۲۰۲۰)، G5 در مراحل اولیه استقرار خود است و بسیاری از استانداردهای G5 هنوز نهایی نشده‌اند. فقط زمان نشان خواهد داد که آیا G5 به یک سرویس بی سیم پهن باند فراگیر تبدیل خواهد شد، آیا با موفقیت با WiFi برای خدمات بی سیم داخلی رقابت خواهد کرد، آیا تبدیل به یک جزء حیاتی در اتوماسیون کارخانه و زیرساخت خودروهای خودمختار خواهد شد یا خیر، و آیا این امر ما را به موفقیت بزرگی خواهد برد. گام به جلو به سمت خدمات بی سیم وسیع منطقه نهایی.

۷.۵ مدیریت تحرک: اصول

پس از پوشش ماهیت بی سیم پیوندهای ارتباطی در یک شبکه بی سیم، اکنون زمان آن رسیده است که توجه خود را به تحرکی که این پیوندهای بی سیم فعال می‌کنند معطوف کنیم. در گسترده‌ترین مفهوم، دستگاه تلفن همراه دستگاهی است که در طول زمان نقطه اتصال خود را به شبکه تغییر می‌دهد. از آنجایی که اصطلاح تحرک هم در دنیای کامپیوتر و هم در دنیای تلفن معانی زیادی به خود گرفته است، ابتدا به خوبی به بررسی دقیق اشکال تحرک کمک خواهد کرد.

۷.۵.۱ تحرک دستگاه: دیدگاه لایه شبکه

از نقطه نظر لایه شبکه، یک دستگاه فیزیکی متحرک، بسته به میزان فعال بودن دستگاه در حین حرکت بین نقاط اتصال به شبکه، مجموعه بسیار متفاوتی از چالش‌ها را برای لایه شبکه ارائه می‌کند. در یک انتهای طیف، سناریوی (الف) در شکل ۷.۲۴ کاربر موبایلی است که خودش به صورت فیزیکی بین شبکه‌ها حرکت می‌کند، اما هنگام حرکت، دستگاه تلفن همراه را خاموش می‌کند. به عنوان مثال، دانش آموزی ممکن است از شبکه کلاس درس بی سیم قطع شود و دستگاه خود را خاموش کند، به بخش مشترک غذاخوری رفته و در حین غذا خوردن به شبکه دسترسی بی سیم در آنجا متصل شود، و سپس از شبکه مشترک ناهار خوری جدا شده و خاموش شود. کتابخانه، و در حین مطالعه به شبکه بی سیم کتابخانه متصل شوید. از منظر شبکه، این دستگاه سیار نیست - به یک شبکه دسترسی متصل می‌شود و در حالی که روشن است در آن شبکه دسترسی باقی می‌ماند. در این مورد، دستگاه به صورت سریالی با هر شبکه دسترسی بی سیمی که با آن مواجه می‌شود ارتباط برقرار می‌کند و بعداً از آن جدا می‌شود. با استفاده از مکانیسم‌های شبکه‌ای که قبلاً در بخش‌های ۷.۳ و ۷.۴ مطالعه کرده‌ایم، می‌توان این مورد (غیر) تحرک دستگاه را به طور کامل مدیریت کرد.

در سناریوی (ب) در شکل ۷.۲۴، دستگاه از نظر فیزیکی متحرک است اما به همان شبکه دسترسی متصل باقی می‌ماند. این دستگاه همچنین از منظر لایه شبکه موبایل نیست. به علاوه، اگر دستگاه با همان ایستگاه پایه ۸۰۲.۱۱ AP یا LTE مرتبط باقی بماند، دستگاه حتی از منظر لایه پیوند متحرک نیست.

از نقطه نظر شبکه، علاقه ما به تحرک دستگاه واقعاً با مورد (c) شروع می‌شود، جایی که یک دستگاه شبکه دسترسی خود را تغییر می‌دهد (به عنوان مثال، سلول WLAN یا LTE 802.11) در حالی که به ارسال و دریافت دیتاگرام IP ادامه می‌دهد، و در عین حال سطح بالاتری را حفظ می‌کند. به عنوان مثال، TCP (اتصالات. در اینجا، شبکه باید تحویل داده شود - انتقال مسئولیت برای ارسال دیتاگرام به/از یک AP یا ایستگاه پایه به دستگاه تلفن همراه - همانطور که دستگاه در بین WLAN ها یا بین سلول های LTE حرکت می‌کند. ما در بخش ۷.۶ به تفصیل به واگذاری خواهیم پرداخت. اگر تحویل در شبکه‌های دسترسی متعلق به یک ارائه‌دهنده شبکه اتفاق بیفتد، آن ارائه‌دهنده می‌تواند به تنهایی واگذاری را هماهنگ کند. هنگامی که یک دستگاه تلفن همراه بین چندین شبکه ارائه دهنده پرسه می‌زند، مانند سناریوی (د)، ارائه دهندگان باید تحویل را با هم هماهنگ کنند، که به طور قابل توجهی فرآیند تحویل را پیچیده می‌کند.

۷.۵.۲ شبکه های خانگی و رومینگ در شبکه های بازدید شده

همانطور که در بحث های خود در مورد شبکه های 4G LTE سلولی در بخش ۷.۴.۱ آموختیم، هر مشترک یک "خانه" با برخی از ارائه دهندگان تلفن همراه دارد. ما متوجه شدیم که سرویس مشترک خانگی (HSS) اطلاعات مربوط به هر یک از مشترکین خود را ذخیره می کند، از جمله شناسه دستگاه منحصر به فرد جهانی (جاسازی شده در سیم کارت مشترک)، اطلاعات مربوط به خدماتی که مشترک ممکن است به آنها دسترسی داشته باشد، کلیدهای رمزنگاری که برای ارتباط استفاده می شود، و اطلاعات صورتحساب / شارژ. هنگامی که یک دستگاه به یک شبکه تلفن همراه، به غیر از شبکه خانگی خود متصل می شود، گفته می شود که آن دستگاه در یک شبکه بازدید شده در حال رومینگ است. هنگامی که یک دستگاه تلفن همراه به یک شبکه بازدید شده متصل می شود و در آن پرسه می زند، هماهنگی بین شبکه خانگی و شبکه بازدید شده لازم است.

اینترنت مفهوم قوی مشابهی از شبکه خانگی یا شبکه بازدید شده ندارد. در عمل، شبکه خانگی یک دانش آموز ممکن است شبکه ای باشد که توسط مدرسه او اداره می شود. برای متخصصان موبایل، شبکه خانگی آنها ممکن است شبکه شرکت آنها باشد. شبکه بازدید شده ممکن است شبکه یک مدرسه یا شرکتی باشد که آنها از آن بازدید می کنند. اما هیچ مفهومی از شبکه خانگی/بازدید شده عمیقاً در معماری اینترنت وجود ندارد. پروتکل IP موبایل [پرکینز ۱۹۹۸، RFC 5944]، که به طور خلاصه در بخش ۷.۶ به آن خواهیم پرداخت، پیشنهادی بود که به شدت مفهوم شبکه های خانگی/بازدید شده را در بر می گرفت. اما IP موبایل در عمل شاهد استقرار/استفاده محدود بوده است. همچنین فعالیت هایی در حال انجام است که بر روی زیرساخت IP موجود ساخته شده اند تا دسترسی به شبکه احراز هویت شده در سراسر شبکه های IP بازدید شده را فراهم کنند. [Eduroam 2020] Eduroam یکی از این فعالیت ها است.

مفهوم یک دستگاه تلفن همراه دارای یک شبکه خانگی دو مزیت مهم را به همراه دارد: شبکه خانگی یک مکان واحد را فراهم می کند که در آن اطلاعات مربوط به آن دستگاه را می توان یافت، و (همانطور که خواهیم دید) می تواند به عنوان یک نقطه هماهنگی برای ارتباط با/از عمل کند. یک دستگاه تلفن همراه رومینگ برای درک ارزش بالقوه نقطه مرکزی اطلاعات و هماهنگی، قیاس انسانی یک باب بالغ ۲۰ ساله را در نظر بگیرید که از خانه خانواده خارج می شود. باب متحرک می شود، در یک سری از خوابگاه ها و آپارتمان ها زندگی می کند و اغلب آدرس ها را تغییر می دهد. اگر یکی از دوستان قدیمی آلیس بخواهد با او تماس بگیرد، آلیس چگونه می تواند آدرس فعلی باب را پیدا کند؟ یکی از راه های متداول تماس با خانواده است، زیرا یک بزرگسال ۲۰ ساله تلفن همراه اغلب آدرس فعلی خود را در خانواده ثبت می کند (اگر دلیل دیگری نداشته باشد جز اینکه والدین بتوانند پولی برای کمک به پرداخت اجاره بفرستند!). خانه خانواده به مکان منحصر به فردی تبدیل می شود که دیگران می توانند به

عنوان اولین قدم در برقراری ارتباط با باب به آنجا بروند. علاوه بر این، ارتباط پستی بعدی از آلیس ممکن است یا غیرمستقیم باشد (مثلاً با ارسال نامه ابتدا به خانه خانواده باب و سپس ارسال به باب) یا مستقیم (مثلاً با استفاده از آلیس از آدرس دریافت شده از والدین باب برای ارسال مستقیم نامه به باب).

۷.۵.۳ مسیریابی مستقیم و غیرمستقیم به/از دستگاه موبایل

حال اجازه دهید معمایی را که میزبان متصل به اینترنت (که به عنوان خبرنگار از آن یاد خواهیم کرد) در شکل ۷.۲۵ در نظر بگیریم که مایل به برقراری ارتباط با یک دستگاه تلفن همراه است که ممکن است در شبکه خانه سلولی آن دستگاه تلفن همراه قرار داشته باشد یا ممکن است در رومینگ باشد. یک شبکه بازدید شده در توسعه خود در زیر، دیدگاه شبکه سلولی 4G/5G را اتخاذ خواهیم کرد، زیرا این شبکه ها سابقه طولانی در پشتیبانی از تحرک دستگاه دارند. اما همانطور که خواهیم دید، چالش های اساسی و رویکردهای راه حل اساسی برای پشتیبانی از تحرک دستگاه به همان اندازه در شبکه های سلولی و اینترنت قابل اجرا هستند.

همانطور که در شکل ۷.۲۵ نشان داده شده است، فرض می کنیم که دستگاه تلفن همراه دارای یک شناسه منحصر به فرد جهانی مرتبط با آن است. در شبکه های سلولی 4G، LTE (به بخش ۷.۴ مراجعه کنید)، این شناسه مشترک بین المللی تلفن همراه (IMSI) و یک شماره تلفن مرتبط است که در سیم کارت دستگاه تلفن همراه ذخیره می شود. برای کاربران اینترنت موبایل، این یک آدرس IP دائمی در محدوده آدرس IP شبکه خانگی آن خواهد بود، مانند مورد معماری IP Mobile.

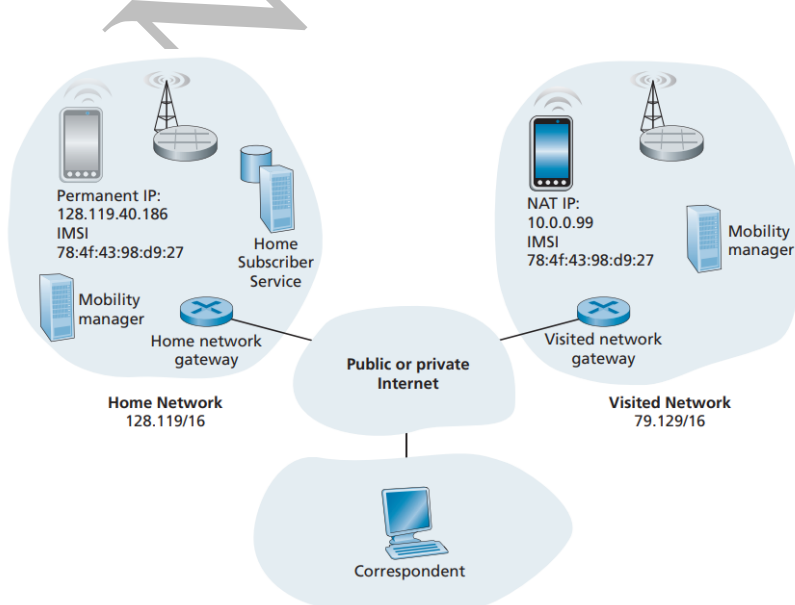


Figure 7.25 ♦ Elements of a mobile network architecture

چه رویکردهایی ممکن است در معماری شبکه تلفن همراه مورد استفاده قرار گیرد که به دیتاگرام ارسال شده توسط خبرنگار اجازه دسترسی به آن دستگاه تلفن همراه را بدهد؟ سه رویکرد اساسی را می توان شناسایی کرد و در زیر مورد بحث قرار می گیرد. همانطور که خواهیم دید، دو مورد اخیر در عمل پذیرفته شده اند.

استفاده از زیرساخت آدرس IP موجود

شاید ساده ترین رویکرد برای مسیریابی به یک دستگاه تلفن همراه در یک شبکه بازدید شده، استفاده ساده از زیرساخت آدرس دهی IP موجود باشد تا چیز جدیدی به معماری اضافه نشود. چه چیزی می تواند ساده تر باشد! از بحث ما در مورد شکل ۴.۲۱ به یاد بیاورید که یک ISP از BGP برای تبلیغ مسیرها به شبکه های مقصد با برشمردن محدوده آدرس CIDRized شبکه های قابل دسترسی استفاده می کند. بنابراین، یک شبکه بازدید شده می تواند به همه شبکه های دیگر تبلیغ کند که یک دستگاه تلفن همراه خاص در شبکه خود ساکن است، صرفاً با تبلیغ یک آدرس بسیار خاص - آدرس IP دائمی کامل ۳۲ بیتی دستگاه تلفن همراه - اساساً به شبکه های دیگر اطلاع می دهد که مسیری را دارد که باید انجام شود. برای ارسال دیتاگرام به آن دستگاه تلفن همراه استفاده می شود. این شبکه های همسایه سپس این اطلاعات مسیریابی را در سراسر شبکه به عنوان بخشی از روند عادی BGP برای به روز رسانی اطلاعات مسیریابی و جداول ارسال می کنند. از آنجایی که دیتاگرام ها همیشه به مسیریاب ارسال می شوند که مشخص ترین مقصد آن آدرس را تبلیغ می کند (به بخش ۴.۳ مراجعه کنید)، همه دیتاگرام های خطاب شده به آن دستگاه تلفن همراه به شبکه بازدید شده ارسال می شوند. اگر دستگاه تلفن همراه یک شبکه بازدید شده را ترک کند و به شبکه دیگری بپیوندد، شبکه بازدید شده جدید می تواند یک مسیر جدید و بسیار خاص به دستگاه تلفن همراه را تبلیغ کند و شبکه بازدید شده قدیمی می تواند اطلاعات مسیریابی خود را در مورد دستگاه تلفن همراه پس بگیرد. این کار دو مشکل را همزمان حل می کند و این کار را بدون ایجاد تغییرات در زیرساخت لایه شبکه انجام می دهد! سایر شبکه ها مکان دستگاه تلفن همراه را می دانند، و به راحتی می توان دیتاگرام ها را به دستگاه تلفن همراه هدایت کرد، زیرا جداول ارسال، دیتاگرام ها را به شبکه بازدید شده هدایت می کنند. با این حال، ایراد مهم، مقیاس پذیری است - روترهای شبکه باید ورودی های جدول ارسال را برای میلیاردها دستگاه تلفن همراه بالقوه حفظ کنند و هر بار که دستگاه به شبکه دیگری روم می کند، ورودی دستگاه را به روز کند. واضح است که این رویکرد در عمل کارساز نخواهد بود. برخی از اشکالات اضافی در مسائل در پایان این فصل بررسی شده است.

یک رویکرد جایگزین، کاربردی تر (و رویکردی که در عمل به کار گرفته شده است) این است که عملکرد تحرک را از هسته شبکه به لبه شبکه هدایت کنیم - موضوعی تکراری در مطالعه ما از معماری اینترنت. یک راه طبیعی برای

انجام این کار از طریق شبکه خانگی دستگاه تلفن همراه است. تقریباً به همان روشی که والدین بزرگسال ۲۰ ساله تلفن همراه مکان فرزندان را ردیابی می کنند، یک نهاد مدیریت تحرک (MME) در شبکه خانگی دستگاه تلفن همراه می تواند شبکه بازدید شده را که دستگاه تلفن همراه در آن قرار دارد ردیابی کند. این اطلاعات ممکن است در یک پایگاه داده وجود داشته باشد که به عنوان پایگاه داده HSS در شکل ۷.۲۵ نشان داده شده است. پروتکلی که بین شبکه بازدید شده و شبکه خانگی کار می کند برای به روز رسانی شبکه ای که دستگاه تلفن همراه در آن قرار دارد مورد نیاز است. شاید به خاطر داشته باشید که ما در مطالعه خود در مورد 4G LTE با عناصر MME و HSS مواجه شدیم. ما در اینجا از نام عناصر آنها استفاده مجدد خواهیم کرد، زیرا آنها بسیار توصیفی هستند و همچنین به این دلیل که به طور گسترده در شبکه های 4G مستقر هستند.

اجازه دهید عناصر شبکه بازدید شده در شکل ۷.۲۵ را با جزئیات بیشتر در نظر بگیریم. دستگاه تلفن همراه به وضوح به یک آدرس IP در شبکه بازدید شده نیاز دارد. امکانات در اینجا شامل استفاده از یک آدرس دائمی مرتبط با شبکه خانگی دستگاه تلفن همراه، تخصیص یک آدرس جدید در محدوده آدرس شبکه بازدید شده، یا ارائه یک آدرس IP از طریق NAT است (به بخش ۴.۳.۴ مراجعه کنید). در دو مورد اخیر، یک دستگاه تلفن همراه دارای یک شناسه گذرا (یک آدرس IP جدید تخصیص یافته) علاوه بر شناسه های دائمی آن است که در HSS در شبکه خانگی خود ذخیره شده است. این موارد مشابه با نویسنده ای است که نامه ای را به آدرس خانه ای که بالغ ۲۰ ساله سیار ما در آن زندگی می کند، خطاب می کند. در مورد آدرس NAT، دیتاگرام های مقصد به دستگاه تلفن همراه در نهایت به مسیر یاب دروازه NAT در شبکه بازدید شده می رسند، که سپس ترجمه آدرس NAT را انجام می دهد و دیتاگرام را به دستگاه تلفن همراه ارسال می کند.

اکنون تعدادی از عناصر راه حل برای معضل خبرنگار را در شکل ۷.۲۴ دیده ایم: شبکه های خانگی و بازدید شده، MME و HSS، و آدرس دهی دستگاه تلفن همراه. اما چگونه باید دیتاگرام ها آدرس دهی شوند و به دستگاه تلفن همراه ارسال شوند؟ از آنجایی که فقط HSS (و نه روترهای سراسر شبکه) مکان دستگاه تلفن همراه را می دانند، خبرنگار نمی تواند به سادگی یک دیتاگرام را به آدرس دائمی دستگاه تلفن همراه نشان دهد و آن را به شبکه ارسال کند. باید کار بیشتری کرد. دو رویکرد را می توان شناسایی کرد: مسیریابی غیر مستقیم و مستقیم.

مسیریابی غیر مستقیم به یک دستگاه تلفن همراه

بیا یاد دوباره خبرنگاری را در نظر بگیریم که می خواهد دیتاگرام را به یک دستگاه تلفن همراه ارسال کند. در رویکرد مسیریابی غیرمستقیم، خبرنگار به سادگی دیتاگرام را به آدرس دائمی دستگاه تلفن همراه نشانی می دهد و

دیتاگرام را به شبکه ارسال می‌کند، با خوشحالی از اینکه دستگاه تلفن همراه در شبکه خانگی خود ساکن است یا در یک شبکه بازدید شده. بنابراین تحرک برای خبرنگار کاملاً شفاف است. چنین دیتاگرام‌هایی ابتدا طبق معمول به شبکه خانگی دستگاه تلفن همراه هدایت می‌شوند. این در مرحله ۱ در شکل ۷.۲۶ نشان داده شده است.

بیاید اکنون توجه خود را به HSS معطوف کنیم، که مسئول تعامل با شبکه‌های بازدید شده برای ردیابی مکان دستگاه تلفن همراه و مسیر یاب دروازه شبکه خانگی است. یکی از وظایف این مسیر یاب دروازه این است که مراقب یک دیتاگرام در حال ورود به دستگاهی باشد که خانه آن در آن شبکه است، اما در حال حاضر در یک شبکه بازدید شده قرار دارد. دروازه شبکه خانگی این دیتاگرام را رهگیری می‌کند، با HSS مشورت می‌کند تا شبکه بازدید شده را تعیین کند که دستگاه تلفن همراه در آن ساکن است، و دیتاگرام را به سمت مسیر یاب دروازه شبکه بازدید شده هدایت می‌کند - مرحله ۲ در شکل ۷.۲۶. سپس روتر دروازه شبکه بازدید شده دیتاگرام را به سمت دستگاه تلفن همراه هدایت می‌کند - مرحله ۳ در شکل ۷.۲۶. اگر از ترجمه NAT استفاده شود، مانند شکل ۷.۲۶، روتر دروازه شبکه بازدید شده، ترجمه NAT را انجام می‌دهد.

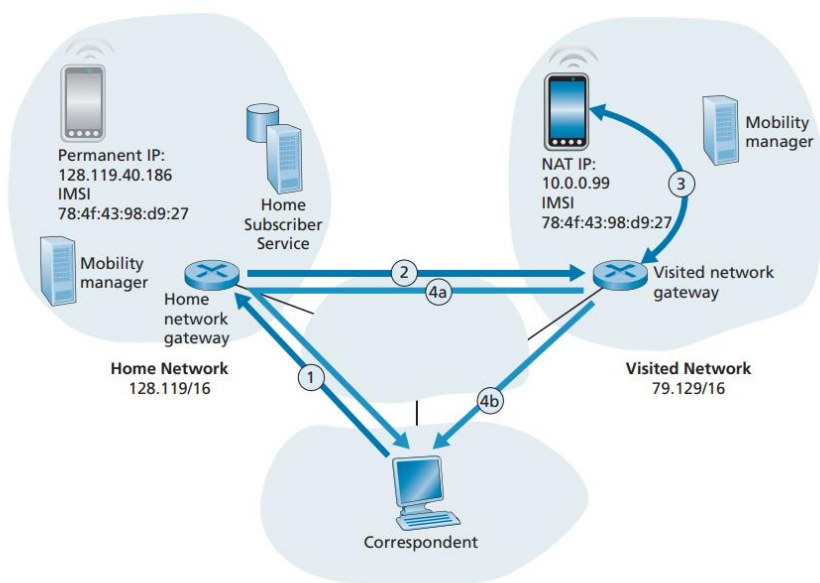


Figure 7.26 ♦ Indirect routing to a mobile device

آموزنده است که مسیریابی مجدد در شبکه خانگی را با جزئیات بیشتری در نظر بگیرید. واضح است که دروازه شبکه خانگی باید دیتاگرام ورودی را به مسیر یاب دروازه در شبکه بازدید شده ارسال کند. از طرف دیگر، بهتر است دیتاگرام خبرنگار را دست نخورده رها کنید، زیرا برنامه دریافت کننده دیتاگرام باید از ارسال دیتاگرام از طریق شبکه خانگی غافل باشد. هر دو هدف را می‌توان با محصور کردن دیتاگرام کامل اصلی خبرنگار در یک دیتاگرام جدید (بزرگتر) توسط دروازه اصلی برآورده کرد. سپس این دیتاگرام بزرگ‌تر آدرس‌دهی می‌شود و به مسیر یاب دروازه شبکه بازدید شده تحویل داده می‌شود، که دیتاگرام را کپسوله می‌کند - یعنی دیتاگرام اصلی خبرنگار را از داخل

دیتاگرام کپسوله‌شده بزرگ‌تر حذف می‌کند - و (مرحله ۳ در شکل ۷.۲۶) دیتاگرام اصلی را به سمت دیتاگرام ارسال می‌کند. دستگاه موبایل، خواننده تیزبین متوجه خواهد شد که کپسوله‌سازی/کپسوله‌زدایی شرح داده شده در اینجا دقیقاً مفهوم تونل‌زنی است که در بخش ۴.۳ در زمینه IPv6 مورد بحث قرار گرفته است. در واقع، زمانی که صفحه داده 4G LTE را معرفی کردیم، در مورد استفاده از تونل در شکل ۷.۱۸ نیز بحث کردیم.

در نهایت، بیاید در نظر بگیریم که دستگاه تلفن همراه چگونه دیتاگرام‌ها را به خبرنگار ارسال می‌کند. در زمینه شکل ۷.۲۶، دستگاه تلفن همراه به وضوح باید دیتاگرام را از طریق مسیر یاب دروازه بازديد شده ارسال کند تا بتواند ترجمه NAT را انجام دهد. اما چگونه باید مسیر یاب دروازه بازديد شده دیتاگرام را به خبرنگار ارسال کند؟ همانطور که در شکل ۷.۲۶ نشان داده شده است، دو گزینه در اینجا وجود دارد: (a۴) دیتاگرام را می‌توان به مسیر یاب دروازه خانگی تونل زد و از آنجا به خبرنگار ارسال کرد، یا (b۴) دیتاگرام را می‌توان از شبکه بازديد شده مستقیماً به خبرنگار - رویکردی که به عنوان شکست محلی [GSMA 2019a] در LTE شناخته می‌شود.

بیاید بحث خود را در مورد مسیریابی غیرمستقیم با بررسی عملکرد لایه شبکه جدید مورد نیاز برای پشتیبانی از تحرک خلاصه کنیم.

• پروتکل ارتباط تلفن همراه به شبکه بازديد شده. دستگاه تلفن همراه باید با شبکه بازديد شده مرتبط شود، و به طور مشابه هنگام خروج از شبکه بازديد شده، نیاز به قطع ارتباط دارد.

• یک پروتکل ثبت نام شبکه به شبکه خانه-خانه-HSS. شبکه بازديد شده باید مکان دستگاه تلفن همراه را با HSS در شبکه خانگی ثبت کند و شاید از اطلاعات به دست آمده از HSS در انجام احراز هویت دستگاه استفاده کند.

• یک پروتکل تونل زنی دیتاگرام بین دروازه شبکه خانگی و روتر دروازه شبکه بازديد شده. طرف فرستنده کپسوله سازی و ارسال دیتاگرام اصلی خبرنگار را انجام می‌دهد. در سمت دریافت کننده، مسیر یاب دروازه، کپسولاسیون، ترجمه NAT و ارسال دیتاگرام اصلی به دستگاه تلفن همراه را انجام می‌دهد.

بحث قبلی تمام عناصر مورد نیاز یک دستگاه تلفن همراه را فراهم می‌کند تا ارتباط مداوم با یک خبرنگار را در حین حرکت دستگاه در میان شبکه‌ها حفظ کند. هنگامی که دستگاهی از یک شبکه بازديد شده به شبکه دیگر روم می‌کند، اطلاعات شبکه بازديد شده جدید باید در HSS شبکه خانگی به روز شود و نقطه پایانی تونل مسیر یاب دروازه خانه به دروازه بازديد شده باید منتقل شود. اما آیا دستگاه تلفن همراه در حین حرکت بین شبکه‌ها، جریان قطعی دیتاگرام‌ها را مشاهده می‌کند؟ تا زمانی که فاصله زمانی بین قطع شدن دستگاه تلفن همراه از یک شبکه بازديد شده و اتصال آن به شبکه بازديد شده بعدی کم باشد، دیتاگرام‌های کمی از بین می‌روند. از فصل ۳ به یاد بیاورید که اتصالات سرتاسر ممکن است به دلیل ازدحام شبکه از دست دادن دیتاگرام را تجربه کنند. از این رو، از

دست دادن گاه به گاه دیتاگرام در یک اتصال زمانی که یک دستگاه بین شبکه ها حرکت می کند، به هیچ وجه یک مشکل فاجعه بار نیست. اگر ارتباط بدون تلفات مورد نیاز باشد، مکانیسم های لایه بالایی از دست دادن دیتاگرام بازیابی می شوند، خواه این فقدان ناشی از ازدحام شبکه باشد یا از تحرک دستگاه.

بحث ما در بالا به طور هدفمند تا حدودی کلی بوده است. یک رویکرد مسیریابی غیرمستقیم در استاندارد IP تلفن همراه [RFC 5944]، و همچنین در شبکه های 4G LTE [Sauter 2014] استفاده می شود. جزئیات آنها، به ویژه روش های تونل زنی به کار گرفته شده، فقط کمی با بحث عمومی ما در بالا متفاوت است.

مسیریابی مستقیم به یک دستگاه تلفن همراه

رویکرد مسیریابی غیرمستقیم نشان داده شده در شکل ۷.۲۶ از یک ناکارآمدی به نام مشکل مسیریابی مثلثی رنج می برد - دیتاگرام های خطاب به دستگاه تلفن همراه باید ابتدا به شبکه خانگی و سپس به شبکه بازدید شده ارسال شوند، حتی زمانی که مسیر بسیار کارآمدتری بین دستگاه ها وجود داشته باشد. خبرنگار و دستگاه تلفن همراه رومینگ. در بدترین حالت، یک کاربر تلفن همراه را تصور کنید که در همان شبکه ای که شبکه خانگی یک همکار خارجی است که کاربر تلفن همراه ما از آن بازدید می کند، در حال رومینگ است. این دو در کنار هم نشسته اند و داده ها را رد و بدل می کنند. دیتاگرام بین کاربر تلفن همراه و همکار خارج از کشور او به شبکه خانگی کاربر تلفن همراه ارسال می شود و سپس دوباره به شبکه بازدید شده باز می گردد!

مسیریابی مستقیم بر ناکارآمدی مسیریابی مثلثی غلبه می کند، اما این کار را به قیمت پیچیدگی بیشتر انجام می دهد. در رویکرد مسیریابی مستقیم، نشان داده شده در شکل ۷.۲۷، خبرنگار ابتدا شبکه بازدید شده ای را که موبایل در آن ساکن است، کشف می کند. این کار با پرس و جو از HSS در شبکه خانگی دستگاه تلفن همراه انجام می شود، با این فرض (مانند مورد مسیریابی غیرمستقیم) که شبکه بازدید شده دستگاه تلفن همراه در HSS ثبت شده است. این به صورت مراحل ۱ و ۲ در شکل ۷.۲۷ نشان داده شده است. سپس خبرنگار دیتاگرام ها را از شبکه خود مستقیماً به مسیر یاب دروازه در شبکه بازدید شده دستگاه تلفن همراه تونل می کند.

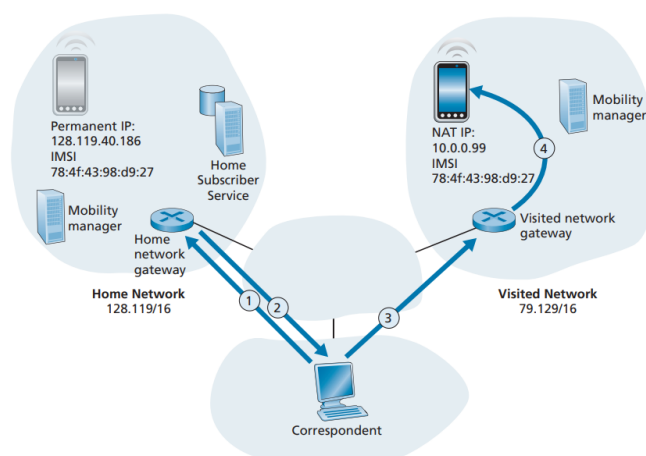


Figure 7.27 • Direct routing to a mobile device

در حالی که مسیریابی مستقیم بر مشکل مسیریابی مثلثی غلبه می کند، دو چالش مهم دیگر را معرفی می کند:

- یک پروتکل مکان کاربر تلفن همراه برای پاسخگویی به HSS برای بدست آوردن شبکه بازدید شده دستگاه تلفن همراه مورد نیاز است (مراحل ۱ و ۲ در شکل ۷.۲۷). این علاوه بر پروتکل مورد نیاز برای دستگاه تلفن همراه برای ثبت موقعیت مکانی خود با HSS است.
- هنگامی که دستگاه تلفن همراه از یک شبکه بازدید شده به شبکه دیگر منتقل می شود، خبرنگار چگونه می داند که اکنون دیتاگرام ها را به شبکه بازدید شده جدید ارسال می کند؟ در مورد مسیریابی غیرمستقیم، این مشکل با به روز رسانی HSS در شبکه خانگی و تغییر نقطه پایانی تونل برای پایان دادن به مسیریاب دروازه شبکه بازدید شده جدید به راحتی حل شد. با این حال، با مسیریابی مستقیم، این تغییر در شبکه های بازدید شده به راحتی قابل کنترل نیست، زیرا HSS تنها در ابتدای جلسه توسط خبرنگار درخواست می شود. بنابراین، مکانیسم های پروتکل اضافی برای به روز رسانی فعالانه خبرنگار هر بار که دستگاه تلفن همراه حرکت می کند، مورد نیاز است. دو مسئله در پایان این فصل راه حل های این مشکل را بررسی می کند.

۷.۶ مدیریت تحرک در عمل

در بخش قبل، چالش های اساسی کلیدی و راه حل های بالقوه در توسعه معماری شبکه برای پشتیبانی از تحرک دستگاه را شناسایی کردیم: مفاهیم شبکه های خانگی و بازدید شده. نقش شبکه خانگی به عنوان یک نقطه مرکزی اطلاعات و کنترل برای دستگاه های تلفن همراه مشترک در آن شبکه خانگی؛ عملکردهای صفحه کنترل مورد نیاز نهاد مدیریت تحرک شبکه خانگی برای ردیابی دستگاه تلفن همراه در حال رومینگ در بین شبکه های بازدید شده. و رویکردهای صفحه داده مسیریابی مستقیم و غیرمستقیم برای فعال کردن یک خبرنگار و یک دستگاه تلفن همراه برای تبادل دیتاگرام. حال بیایید ببینیم این اصول چگونه عملی می شوند! در بخش ۷.۲.۱، مدیریت تحرک را در

شبکه های 4G/5G مطالعه خواهیم کرد. در بخش ۷.۲.۱، به IP موبایل که برای اینترنت پیشنهاد شده است نگاه می کنیم.

۷.۶.۱ مدیریت تحرک در شبکه های 4G/5G

مطالعه قبلی ما در مورد 4G و معماری های نوظهور 5G در بخش ۷.۴ ما را با تمام عناصر شبکه که نقش اصلی در مدیریت تحرک 4G/5G دارند آشنا کرد. اکنون بیایید نشان دهیم که چگونه آن عناصر با یکدیگر برای ارائه خدمات تحرک در شبکه های 4G/5G امروزی کار می کنند [Sauter 2014; GSMA 2019b]، که ریشه در شبکه های صوتی و داده سلولی 3G قبلی [Sauter 2014]، و حتی شبکه های فقط صوتی 2G اولیه [Mouly 1992] دارند. این به ما کمک می کند تا آنچه را که تاکنون آموخته ایم ترکیب کنیم، به ما امکان می دهد چند موضوع پیشرفته تر را نیز معرفی کنیم، و لنزهایی را در مورد آنچه ممکن است برای مدیریت تحرک 5G وجود داشته باشد ارائه دهیم.

بیایید یک سناریوی ساده را در نظر بگیریم که در آن یک کاربر تلفن همراه (به عنوان مثال، یک مسافر در یک ماشین)، با یک گوشی هوشمند به یک شبکه 4G/5G بازدید شده متصل می شود، شروع به پخش یک ویدیو HD از یک سرور راه دور می کند و سپس از پوشش سلولی خارج می شود. یک ایستگاه پایه 4G/5G به دیگری. چهار مرحله اصلی در این سناریو در شکل ۷.۲۸ نشان داده شده است:

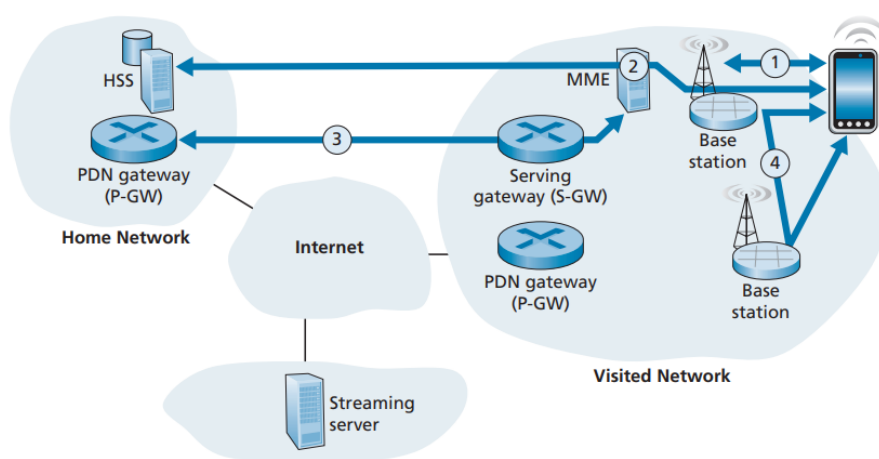


Figure 7.28 ♦ An example 4G/5G mobility scenario

۱. ارتباط دستگاه تلفن همراه و ایستگاه پایه. دستگاه تلفن همراه با یک ایستگاه پایه در شبکه بازدید شده مرتبط است.

۲. پیکربندی صفحه کنترل عناصر شبکه برای دستگاه تلفن همراه. شبکه های بازدید شده و شبکه های خانگی حالت صفحه کنترل را ایجاد می کنند که نشان می دهد دستگاه تلفن همراه در شبکه بازدید شده ساکن است.

۳. پیکربندی صفحه داده تونل های حمل و نقل برای دستگاه تلفن همراه. شبکه بازدید شده و شبکه خانگی تونل هایی ایجاد می کنند که از طریق آن دستگاه تلفن همراه و سرور جریان می توانند دیتاگرام های IP را با استفاده از مسیریابی غیرمستقیم از طریق دروازه شبکه داده های بسته شبکه خانگی (P-GW) ارسال/دریافت کنند.

۴. تحویل دستگاه تلفن همراه از یک ایستگاه پایه به ایستگاه دیگر. دستگاه تلفن همراه از طریق انتقال از یک ایستگاه پایه به ایستگاه دیگر، نقطه اتصال خود را به شبکه بازدید شده تغییر می دهد.

حال بیایید هر یک از این چهار مرحله را با جزئیات بیشتری در نظر بگیریم.

۱. انجمن ایستگاه پایه. به یاد بیاورید که در بخش ۷.۴.۲، رویه هایی را مطالعه کردیم که توسط آن یک دستگاه تلفن همراه با یک ایستگاه پایه مرتبط می شود. ما آموختیم که دستگاه تلفن همراه به سیگنال های اولیه که توسط ایستگاه های پایه در منطقه خود ارسال می شود، به تمام فرکانس ها گوش می دهد. دستگاه تلفن همراه به تدریج اطلاعات بیشتری در مورد این ایستگاه های پایه به دست می آورد، در نهایت ایستگاه پایه ای را انتخاب می کند که با آن ارتباط برقرار کند، و یک کانال سیگنالینگ کنترلی را با آن ایستگاه پایه راه اندازی می کند. به عنوان بخشی از این ارتباط، دستگاه تلفن همراه شناسه مشترک بین المللی تلفن همراه خود (IMSI) را به ایستگاه پایه ارائه می کند، که به طور منحصربه فرد دستگاه تلفن همراه و همچنین شبکه خانگی آن و سایر اطلاعات اضافی مشترک را شناسایی می کند.

۲. پیکربندی صفحه کنترل عناصر شبکه LTE برای دستگاه تلفن همراه. هنگامی که کانال سیگنالینگ دستگاه تلفن همراه به ایستگاه پایه ایجاد شد، ایستگاه پایه می تواند با MME در شبکه بازدید شده تماس بگیرد. MME تعدادی از عناصر 4G/5G را هم در شبکه های خانگی و هم در شبکه های بازدید شده برای ایجاد وضعیت از طرف گره تلفن همراه مشورت و پیکربندی می کند:

- MME از IMSI و سایر اطلاعات ارائه شده توسط دستگاه تلفن همراه برای بازیابی احراز هویت، رمزگذاری، و اطلاعات سرویس شبکه موجود برای آن مشترک استفاده خواهد کرد. این اطلاعات ممکن است در حافظه پنهان محلی MME، از MME دیگری که دستگاه تلفن همراه اخیراً با آن تماس گرفته است، یا از HSS در شبکه خانگی دستگاه تلفن همراه بازیابی شده باشد. فرآیند احراز هویت متقابل (که در بخش ۸.۸ با جزئیات بیشتر به آن خواهیم پرداخت) تضمین می کند که شبکه بازدید شده از هویت دستگاه تلفن همراه مطمئن است و دستگاه می تواند شبکه ای را که به آن متصل می شود احراز هویت کند.

- MME به HSS در شبکه خانگی دستگاه تلفن همراه اطلاع می دهد که دستگاه تلفن همراه اکنون در شبکه بازدید شده ساکن است و HSS پایگاه داده خود را به روز می کند.

• ایستگاه پایه و دستگاه تلفن همراه پارامترهایی را برای کانال صفحه داده انتخاب می کنند تا بین دستگاه تلفن همراه و ایستگاه پایه ایجاد شود (به یاد بیاورید که یک کانال سیگنالینگ صفحه کنترل از قبل در حال کار است).

۳. پیکربندی صفحه داده تونل های حمل و نقل برای دستگاه تلفن همراه. MME سپس صفحه داده را برای دستگاه تلفن همراه پیکربندی می کند، همانطور که در شکل ۷.۲۹ نشان داده شده است. دو تونل ایجاد می شود. یک تونل بین ایستگاه پایه و یک دروازه سرویس در شبکه بازدید شده است. تونل دوم بین آن سرویس دروازه و روتر PDN Gateway در شبکه خانگی دستگاه تلفن همراه است. 4G LTE این شکل از مسیریابی غیرمستقیم متقارن را پیاده سازی می کند—تمام ترافیک به/از دستگاه تلفن همراه از طریق شبکه خانگی دستگاه تونل می شود. تونل های 4G/5G از پروتکل تونل سازی (GTP) GPRS، مشخص شده در [GPP GTPv1-U 2019۳] استفاده می کنند. شناسه نقطه پایانی تونل (TEID) در هدر GTP نشان می دهد که یک دیتاگرام به کدام تونل تعلق دارد و به جریان های متعدد اجازه می دهد تا توسط GTP بین نقاط انتهایی تونل چندگانه شوند و چندگانه شوند.

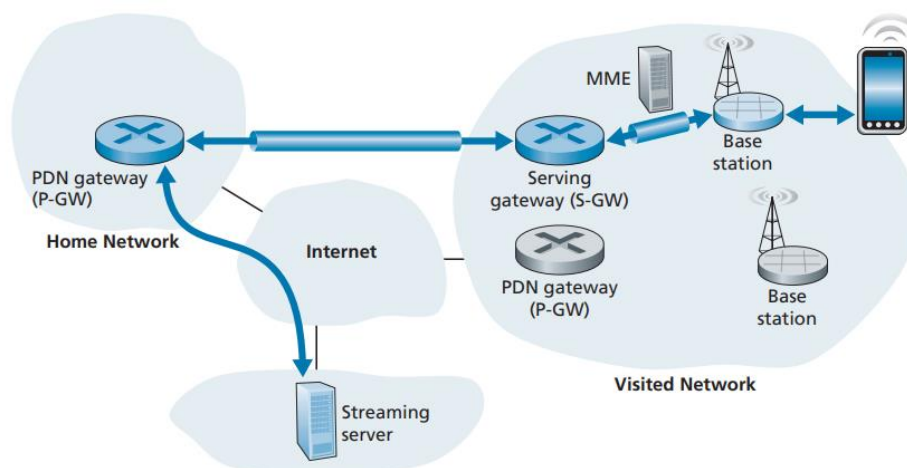


Figure 7.29 ♦ Tunneling in 4G/5G networks between the Serving Gateway in the visited network and the PDN gateway in the home network

آموزنده است که پیکربندی تونل ها را در شکل ۷.۲۹ (مورد رومینگ تلفن همراه در یک شبکه بازدید شده) با شکل ۷.۱۸ (مورد تحرک فقط در شبکه خانگی دستگاه تلفن همراه) مقایسه کنید. می بینیم که در هر دو مورد، سرویس دهی در همان شبکه با دستگاه تلفن همراه ساکن است، اما دروازه PDN (که همیشه دروازه PDN در شبکه خانگی دستگاه تلفن همراه است) ممکن است در شبکه ای متفاوت از دستگاه تلفن همراه باشد. این دقیقاً مسیریابی غیر مستقیم است. جایگزینی برای مسیریابی غیرمستقیم، معروف به شکست محلی [GSMA 2019a] مشخص شده است که در آن دروازه سرویس یک تونل به دروازه PDN در شبکه محلی و بازدید شده ایجاد می کند. با این حال، در عمل، شکست محلی به طور گسترده استفاده نمی شود [Sauter 2014].

هنگامی که تونل ها پیکربندی و فعال شدند، دستگاه تلفن همراه اکنون می تواند بسته ها را به/از اینترنت از طریق دروازه PDN در شبکه خانگی خود ارسال کند!

۴. مدیریت واگذاری. تحویل زمانی اتفاق می افتد که یک دستگاه تلفن همراه ارتباط خود را از یک ایستگاه پایه به ایستگاه دیگر تغییر دهد. بدون توجه به اینکه دستگاه تلفن همراه در شبکه خانگی خود ساکن است یا در یک شبکه بازدید شده در حال رومینگ است، فرآیند تحویل که در زیر توضیح داده شده است، یکسان است.

همانطور که در شکل ۷.۳۰ نشان داده شده است، دیتاگرام ها به/از دستگاه در ابتدا (قبل از تحویل) به موبایل از طریق یک ایستگاه پایه (که ما به عنوان ایستگاه مبدأ از آن یاد می کنیم) ارسال می شوند و پس از تحویل به دستگاه تلفن همراه از طریق آن هدایت می شوند. ایستگاه پایه دیگری (که ما به عنوان ایستگاه پایه هدف از آن یاد خواهیم کرد). همانطور که خواهیم دید، انتقال بین ایستگاه های پایه نه تنها منجر به انتقال/دریافت دستگاه موبایل به/از یک ایستگاه پایه جدید می شود، بلکه باعث تغییر سمت ایستگاه پایه تونل سرویس-دروازه-به-ایستگاه پایه نیز می شود. در شکل ۷.۲۹. در ساده ترین حالت تحویل، زمانی که دو ایستگاه پایه در نزدیکی یکدیگر و در یک شبکه قرار دارند، بنابراین تمام تغییراتی که در نتیجه تحویل رخ می دهند، نسبتاً محلی هستند. به طور خاص، دروازه PDN که توسط دروازه سرویس استفاده می شود، به طرز سعادتمندانه ای از تحرک دستگاه بی اطلاع است. البته، سناریوهای انتقال پیچیده تر نیاز به استفاده از مکانیسم های پیچیده تری دارند [Sauter 2014; GSMA 2019a].

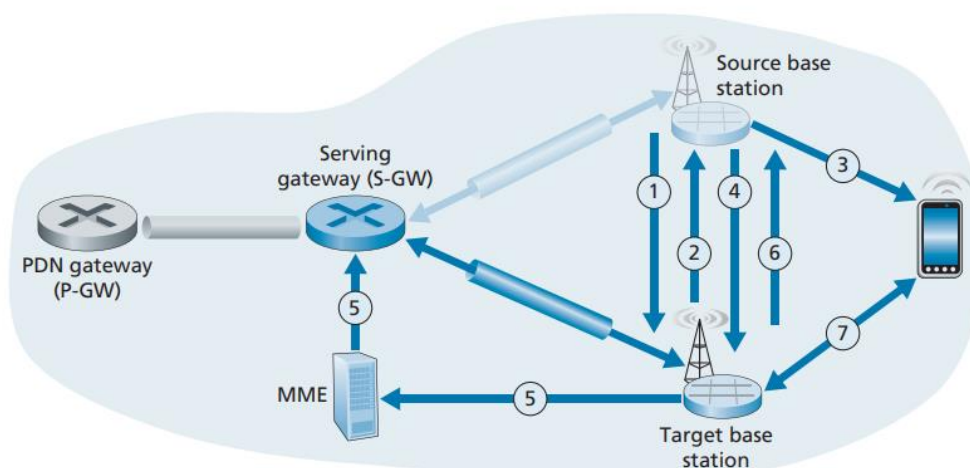


Figure 7.30 ♦ Steps in handing over a mobile device from the source base station to the target base station

ممکن است دلایل متعددی برای وقوع واگذاری وجود داشته باشد. برای مثال، سیگنال بین ایستگاه پایه فعلی و تلفن همراه ممکن است به حدی بدتر شده باشد که ارتباط به شدت مختل شده باشد. یا ممکن است یک سلول بیش از حد بارگذاری شده باشد و حجم زیادی از ترافیک را مدیریت کند. سپردن دستگاه های تلفن همراه به سلول های مجاور با تراکم کمتر ممکن است این ازدحام را کاهش دهد. یک دستگاه تلفن همراه به طور دوره ای ویژگی های

سیگنال بیکن را از ایستگاه پایه فعلی خود و همچنین سیگنال‌های ایستگاه‌های پایه مجاور را که می‌تواند «شنود» را اندازه‌گیری کند. این اندازه‌گیری‌ها یک یا دو بار در ثانیه به ایستگاه پایه فعلی (منبع) دستگاه تلفن همراه گزارش می‌شود. بر اساس این اندازه‌گیری‌ها، بارهای فعلی تلفن‌های همراه در سلول‌های مجاور، و سایر عوامل، ایستگاه پایه منبع ممکن است تصمیم بگیرد که انتقال را آغاز کند. استانداردهای 4G/5G الگوریتم خاصی را برای استفاده توسط ایستگاه پایه برای تعیین اینکه آیا باید تحویل داده شود یا نه، یا اینکه کدام ایستگاه پایه هدف را انتخاب کند، مشخص نمی‌کند. این یک حوزه فعال تحقیقاتی است [Zheng 2008; الکساندریس ۲۰۱۶].

شکل ۷.۳۰ مراحل مربوط به زمانی که یک ایستگاه پایه منبع تصمیم می‌گیرد یک دستگاه تلفن همراه را به ایستگاه پایه هدف تحویل دهد را نشان می‌دهد.

۱. ایستگاه پایه فعلی (منبع) ایستگاه پایه هدف را انتخاب می‌کند و یک پیام درخواست تحویل به ایستگاه پایه هدف ارسال می‌کند.

۲. ایستگاه پایه هدف بررسی می‌کند که آیا منابع لازم برای پشتیبانی از دستگاه تلفن همراه و کیفیت خدمات مورد نیاز آن را دارد یا خیر. اگر چنین است، منابع کانال (به عنوان مثال، شکاف‌های زمانی) را در شبکه دسترسی رادیویی خود و سایر منابع برای آن دستگاه از قبل تخصیص می‌دهد. این پیش تخصیص منابع، دستگاه تلفن همراه را از گذراندن پروتکل زمان‌بر ارتباط ایستگاه پایه که قبلاً مورد بحث قرار گرفت، رها می‌کند و اجازه می‌دهد تا تحویل در سریع‌ترین زمان ممکن انجام شود. ایستگاه پایه هدف با یک پیام تأیید درخواست تحویل، به ایستگاه پایه مبدأ پاسخ می‌دهد، که شامل تمام اطلاعات ایستگاه پایه هدف است که دستگاه تلفن همراه برای مرتبط کردن آن با ایستگاه پایه جدید نیاز دارد.

۳. ایستگاه پایه مبدأ پیام تأیید درخواست تحویل را دریافت می‌کند و دستگاه تلفن همراه را از هویت ایستگاه پایه هدف و اطلاعات دسترسی به کانال مطلع می‌کند. در این مرحله، دستگاه تلفن همراه می‌تواند شروع به ارسال/دریافت دیتاگرام به/از ایستگاه پایه هدف جدید کند. از نقطه نظر دستگاه تلفن همراه، تحویل در حال حاضر کامل است! با این حال، هنوز مقداری کار باید در داخل شبکه انجام شود.

۴. ایستگاه مبدأ نیز ارسال دیتاگرام‌ها به دستگاه تلفن همراه را متوقف می‌کند و در عوض هر دیتاگرام تونلی‌شده‌ای را که دریافت می‌کند به ایستگاه پایه هدف ارسال می‌کند، که بعداً این دیتاگرام‌ها را به دستگاه تلفن همراه ارسال می‌کند.

۵. ایستگاه پایه هدف به MME اطلاع می دهد که آن (ایستگاه پایه هدف) ایستگاه پایه جدیدی خواهد بود که دستگاه تلفن همراه را سرویس می کند. MME به نوبه خود به دروازه سرویس و ایستگاه پایه هدف سیگنال می دهد تا تونل سرویس-دروازه-به-ایستگاه را مجدداً پیکربندی کند تا به ایستگاه پایه هدف ختم شود تا در ایستگاه مبدأ.

۶. ایستگاه پایه هدف مجدداً به ایستگاه پایه منبع تأیید می کند که تونل مجدداً پیکربندی شده است و به ایستگاه پایه منبع اجازه می دهد منابع مرتبط با آن دستگاه تلفن همراه را آزاد کند.

۷. در این مرحله، ایستگاه پایه هدف همچنین می تواند دیتاگرام‌ها را به دستگاه تلفن همراه تحویل دهد، از جمله دیتاگرام‌هایی که توسط ایستگاه مبدأ در حین تحویل به ایستگاه پایه هدف ارسال می شوند، و همچنین دیتاگرام‌هایی که به تازگی به تونل پیکربندی شده مجدداً از دروازه سرویس می‌رسند. . همچنین می تواند دیتاگرام های خروجی دریافت شده از دستگاه تلفن همراه را به داخل تونل به دروازه سرویس ارسال کند.

پیکربندی‌های رومینگ در شبکه‌های 4G LTE امروزی، مانند آنچه در بالا مورد بحث قرار گرفت، در شبکه‌های 5G در حال ظهور آینده [GSMA 2019c] نیز استفاده خواهد شد. با این حال، از بحث ما در بخش ۷.۴.۶ به یاد بیاورید که شبکه‌های 5G متراکم‌تر خواهند بود و اندازه سلول‌های بسیار کوچک‌تری دارند. این کار انتقال را به یک عملکرد شبکه مهم تر تبدیل می کند. علاوه بر این، تاخیر تحویل کم برای بسیاری از برنامه‌های 5G بلادرنگ حیاتی خواهد بود. مهاجرت صفحه کنترل شبکه سلولی به چارچوب SDN که قبلاً در فصل ۵ مطالعه کردیم [GSMA 2018b. Condoluci 2018] وعده می دهد که اجرای یک صفحه کنترل شبکه سلولی 5G با ظرفیت بالاتر و تاخیر کمتر را امکان پذیر می کند. کاربرد SDN در زمینه 5G موضوع تحقیقات قابل توجهی است [Giust 2015; Ordonez-Lucena 2017; نگوین ۲۰۱۶].

۷.۶.۲ آی پی موبایل

اینترنت امروزی هیچ زیرساخت گسترده‌ای ندارد که خدماتی را برای کاربران تلفن همراه «در حال حرکت» که برای شبکه‌های سلولی 4G/5G با آن مواجه بودیم، ارائه دهد. اما این قطعاً به دلیل نبود راه حل های فنی برای ارائه چنین خدماتی در یک محیط اینترنتی نیست! در واقع، معماری IP موبایل و پروتکل‌ها [RFC 5944] که در زیر به طور خلاصه به آن‌ها خواهیم پرداخت، بیش از ۲۰ سال است که توسط RFC‌های اینترنتی استاندارد شده‌اند و تحقیقات بر روی راه‌حل‌های جدید، ایمن‌تر و تعمیم‌یافته‌تر تحرک ادامه یافته است [Venkataramani 2014].

در عوض، شاید فقدان موارد انگیزشی برای تجارت و استفاده [Arko 2012] و توسعه و استقرار به موقع راه حل های جایجایی جایگزین در شبکه های سلولی بوده است که استقرار IP موبایل را کمرنگ کرده است. به یاد بیاورید

که ۲۰ سال پیش، شبکه های سلولی 2G قبلاً راه حلی برای خدمات صوتی تلفن همراه ("برنامه قاتل" برای کاربران تلفن همراه ارائه کرده بودند. علاوه بر این، نسل بعدی شبکه های 3G که از صدا و داده پشتیبانی می کنند در افق بودند. شاید راه حل فناوری دوگانه- خدمات تلفن همراه از طریق شبکه های سلولی زمانی که واقعاً سیار هستیم و در حال حرکت هستیم (یعنی سمت راست طیف تحرک در شکل ۷.۲۴) و خدمات اینترنتی از طریق شبکه های ۸۰۲.۱۱ یا شبکه های سیمی هنگامی که ساکن هستیم یا حرکت به صورت محلی (یعنی سمت چپ ترین طیف تحرک در شکل ۷.۲۴) - که ۲۰ سال پیش داشتیم و هنوز هم داریم، در آینده نیز ادامه خواهد داشت.

با این وجود، مرور مختصر استاندارد IP موبایل در اینجا آموزنده خواهد بود، زیرا بسیاری از خدمات مشابه شبکه های سلولی را ارائه می دهد و بسیاری از اصول اولیه جابجایی را پیاده سازی می کند. نسخه های قبلی این کتاب درسی، مطالعه عمیق تری در مورد IP موبایل نسبت به آنچه در اینجا ارائه خواهیم کرد، ارائه کرده است. خواننده علاقه مند می تواند این مطالب بازنشسته را در وب سایت این کتاب درسی بیابد. معماری اینترنت و پروتکل های پشتیبانی از تحرک، که در مجموع به عنوان IP Mobile شناخته می شوند، در درجه اول در RFC 5944 برای IPv4 تعریف شده اند. IP تلفن همراه، مانند 4G/5G، یک استاندارد پیچیده است و برای شرح جزئیات به یک کتاب کامل نیاز دارد. در واقع یکی از این کتابها [پرکینز b۱۹۹۸] است. هدف ساده ما در اینجا ارائه نمای کلی از مهمترین جنبه های IP Mobile است.

معماری کلی و عناصر IP Mobile به طرز چشمگیری شبیه به شبکه های ارائه دهنده تلفن همراه است. یک مفهوم قوی از شبکه خانگی وجود دارد که در آن یک دستگاه تلفن همراه دارای یک آدرس IP دائمی است، و شبکه های بازدید شده (معروف به شبکه های "خارجی" در IP تلفن همراه)، که در آن به دستگاه تلفن همراه یک آدرس مراقبت اختصاص داده می شود. عامل خانگی در IP تلفن همراه عملکردی مشابه با LTE HSS دارد: با دریافت به روزرسانی ها از نمایندگان خارجی در شبکه های خارجی که توسط آن دستگاه تلفن همراه بازدید می شوند، موقعیت یک دستگاه تلفن همراه را ردیابی می کند، درست همانطور که HSS به روزرسانی ها را از نهادهای مدیریت تحرک (MMEs) دریافت می کند. (در شبکه های بازدید شده که یک دستگاه تلفن همراه 4G در آن قرار دارد. و هر دو 4G/5G و IP Mobile از مسیریابی غیرمستقیم به یک گره تلفن همراه استفاده می کنند و از تونل هایی برای اتصال روترهای دروازه در خانه و شبکه های بازدید شده/خارجی استفاده می کنند. جدول ۷.۳ عناصر معماری IP موبایل را به همراه مقایسه با عناصر مشابه در شبکه های 4G/5G خلاصه می کند.

4G/5G element	Mobile IP element	Discussion
Home network	Home network	
Visited network	Foreign network	
IMSI identifier	Permanent IP address	Globally unique routable address information
Home Subscriber Service (HSS)	Home agent	
Mobility Management Entity (MME)	Foreign agent	
Data plane: indirect forwarding via the home network, with tunneling between the home and visited network, and tunneling within the network in which the mobile device resides	Data plane: indirect forwarding via the home network, with tunneling between the home and visited network	
Base station (eNode-B)	Access Point (AP)	No specific AP technology is specified in Mobile IP
Radio Access Network	WLAN	No specific WLAN technology is specified in Mobile IP

Table 7.3 ♦ Commonalities between 4G/5G and Mobile IP architectures

استاندارد IP موبایل از سه بخش اصلی تشکیل شده است:

- کشف عامل. IP موبایل پروتکل‌هایی را تعریف می‌کند که توسط یک نماینده خارجی برای تبلیغ خدمات تحرک خود به دستگاه تلفن همراهی که می‌خواهد به شبکه خود متصل شود، استفاده می‌کند. این خدمات شامل ارائه مراقبت از آدرس به دستگاه تلفن همراه برای استفاده در شبکه خارجی، ثبت دستگاه تلفن همراه نزد نماینده خانگی در شبکه خانگی دستگاه تلفن همراه، و ارسال دیتاگرام‌ها به/از دستگاه تلفن همراه، از جمله می‌باشد. خدمات دیگر
- ثبت نام با نماینده خانه. IP تلفن همراه پروتکل‌هایی را که توسط دستگاه تلفن همراه و/یا نماینده خارجی برای ثبت و لغو ثبت آدرس مراقبت در نمایندگی خانگی دستگاه تلفن همراه استفاده می‌شود، تعریف می‌کند.
- مسیریابی غیر مستقیم دیتاگرام‌ها. IP موبایل همچنین روشی را که در آن دیتاگرام‌ها توسط یک عامل خانگی به دستگاه‌های تلفن همراه ارسال می‌شوند، از جمله قوانینی برای ارسال دیتاگرام‌ها و شرایط خطا در رسیدگی، و چندین شکل از تونل زدن تعریف می‌کند [RFC 2003, RFC 2004].
- باز هم، پوشش ما در اینجا از IP موبایل عمده‌اً مختصر بوده است. خواننده علاقه مند باید به منابع موجود در این بخش یا بحث‌های مفصل‌تر در مورد IP موبایل در نسخه‌های قبلی این کتاب درسی مراجعه کند.

۷.۷ بی سیم و تحرک: تأثیر بر پروتکل‌های لایه بالاتر

در این فصل، دیدیم که شبکه‌های بی‌سیم به‌طور قابل‌توجهی با همتایان سیمی خود در لایه پیوند (در نتیجه ویژگی‌های کانال بی‌سیم مانند محو شدن، چند مسیر و پایانه‌های مخفی) و در لایه شبکه (در نتیجه کاربران تلفن همراه که نقاط پیوست خود را به شبکه تغییر می‌دهند). اما آیا تفاوت‌های مهمی در لایه‌های حمل و نقل و کاربرد وجود دارد؟ وسوسه‌انگیز است که فکر کنیم این تفاوت‌ها جزئی خواهند بود، زیرا لایه شبکه همان مدل خدمات تحویل بهترین تلاش را به لایه‌های بالایی در شبکه‌های سیمی و بی‌سیم ارائه می‌دهد. به‌طور مشابه، اگر از پروتکل

هایی مانند TCP یا UDP برای ارائه خدمات لایه انتقال به برنامه ها در شبکه های سیمی و بی سیم استفاده شود، لایه برنامه نیز باید بدون تغییر باقی بماند. از یک نظر، شهود ما درست است—TCP و UDP می توانند (و انجام می دهند) در شبکه هایی با پیوندهای بی سیم کار کنند. از سوی دیگر، پروتکل های انتقال به طور کلی، و TCP به طور خاص، گاهی اوقات می توانند عملکرد بسیار متفاوتی در شبکه های سیمی و بی سیم داشته باشند و در اینجا، از نظر عملکرد، تفاوت ها آشکار می شود. بیایید ببینیم چرا.

به یاد بیاورید که TCP قطعه ای را که در مسیر بین فرستنده و گیرنده از بین رفته یا خراب شده را مجدداً ارسال می کند. در مورد کاربران تلفن همراه، از دست دادن می تواند ناشی از ازدحام شبکه (سرریز شدن بافر روتر) یا از انتقال (به عنوان مثال، از تأخیر در مسیریابی مجدد بخش ها به نقطه اتصال جدید تلفن همراه به شبکه) باشد. در تمام موارد، ACK گیرنده به فرستنده TCP فقط نشان می دهد که یک بخش دست نخورده دریافت نشده است. فرستنده از اینکه آیا بخش به دلیل ازدحام، در حین تحویل یا به دلیل خطاهای بی تی شناسایی شده گم شده است، بی اطلاع است. در همه موارد، پاسخ فرستنده یکسان است - برای ارسال مجدد بخش. پاسخ کنترل تراکم TCP نیز در همه موارد یکسان است - همانطور که در بخش ۳.۷ بحث شد TCP پنجره تراکم خود را کاهش می دهد. با کاهش بی قید و شرط پنجره تراکم، TCP به طور ضمنی فرض می کند که از دست دادن بخش ناشی از تراکم است نه فساد یا واگذاری. در بخش ۷.۲ دیدیم که خطاهای بیت در شبکه های بی سیم بسیار رایج تر از شبکه های سیمی است. هنگامی که چنین خطاهای بی تی رخ می دهد یا زمانی که از دست دادن انتقال رخ می دهد، واقعاً دلیلی وجود ندارد که فرستنده TCP پنجره تراکم خود را کاهش دهد (و در نتیجه نرخ ارسال خود را کاهش دهد). در واقع، ممکن است بافرهای روتر خالی باشند و بسته ها در امتداد مسیر انتها به انتها بدون ازدحام جریان داشته باشند.

محققان در اوایل تا اواسط دهه ۱۹۹۰ متوجه شدند که با توجه به نرخ خطای بیت بالا در پیوندهای بی سیم و احتمال از دست دادن انتقال، پاسخ کنترل تراکم TCP می تواند در تنظیمات بی سیم مشکل ساز باشد. سه دسته کلی از رویکردها برای مقابله با این مشکل امکان پذیر است:

- بازیابی محلی. پروتکل های بازیابی محلی خطاهای بیت را در زمان و مکان (مثلاً در پیوند بی سیم) بازیابی می کنند، برای مثال، پروتکل ARQ ۸۰۲.۱۱ که در بخش ۷.۳ مطالعه کردیم، یا رویکردهای پیچیده تری که از ARQ و FEC استفاده می کنند [Ayanoglu 1995]. اره مورد استفاده در شبکه های 4G/5G در بخش ۷.۴.۲.

- آگاهی فرستنده TCP از پیوندهای بی سیم. در رویکردهای بازیابی محلی، فرستنده TCP با خوشحالی از اینکه بخش هایش از یک پیوند بی سیم عبور می کنند بی اطلاع است. یک رویکرد جایگزین این است که فرستنده و گیرنده TCP از وجود یک پیوند بی سیم آگاه باشند، بین تلفات احتمالی رخ داده در شبکه سیمی و خرابی از دست دادن در

پیوند بی سیم تمایز قائل شوند و کنترل تراکم را فقط در پاسخ به تلفات احتمالی شبکه سیمی [لیو ۲۰۰۳] تکنیک هایی را برای تمایز بین تلفات در بخش های سیمی و بی سیم یک مسیر سرتاسر بررسی می کند. [Huang 2013]

بینش هایی را در مورد توسعه مکانیسم ها و برنامه های پروتکل حمل و نقل ارائه می کند که سازگارتر با LTE هستند.

• رویکردهای اتصال تقسیم. در یک رویکرد اتصال تقسیم شده [باکر ۱۹۹۵]، اتصال سرتاسر بین کاربر تلفن همراه و نقطه پایانی دیگر به دو اتصال لایه حمل و نقل شکسته می شود: یکی از میزبان موبایل به نقطه دسترسی بی سیم، و دیگری از نقطه دسترسی بی سیم به نقطه پایانی ارتباطی دیگر (که در اینجا فرض می کنیم میزبان سیمی است). بنابراین اتصال انتها به انتها با الحاق یک قطعه بی سیم و یک قطعه سیمی شکل می گیرد. لایه انتقال روی بخش بی سیم می تواند یک اتصال TCP استاندارد [Bakre 1995]، یا یک پروتکل بازیابی خطای خاص در بالای UDP باشد. [Yavatkar 1994] استفاده از پروتکل تکرار انتخابی لایه حمل و نقل را بر روی اتصال بی سیم بررسی می کند. اندازه گیری های گزارش شده در [Wei 2006] نشان می دهد که اتصالات TCP تقسیم شده به طور گسترده در شبکه های داده سلولی استفاده شده است و در واقع می توان از طریق استفاده از اتصالات TCP تقسیم شده، پیشرفت های قابل توجهی انجام داد.

برخورد ما با TCP از طریق پیوندهای بی سیم در اینجا لزوماً مختصر بوده است. بررسی های عمیق چالش ها و راه حل های TCP در شبکه های بی سیم را می توان در [Hanabali 2005; Leung 2006]، ما شما را تشویق می کنیم تا برای جزئیات بیشتر این حوزه تحقیقاتی در حال انجام، به منابع مراجعه کنید.

با در نظر گرفتن پروتکل های لایه حمل و نقل، اجازه دهید بعداً تأثیر بی سیم و تحرک را بر پروتکل های لایه کاربردی در نظر بگیریم. به دلیل ماهیت مشترک طیف بی سیم، برنامه هایی که از طریق پیوندهای بی سیم، به ویژه از طریق پیوندهای بی سیم سلولی کار می کنند، باید پهنای باند را به عنوان یک کالای کمیاب در نظر بگیرند. به عنوان مثال، سرور وب که محتوا را به مرورگر وب در حال اجرا در تلفن هوشمند 4G ارائه می کند، احتمالاً نمی تواند همان محتوای غنی از تصویر را که به مرورگری که از طریق اتصال سیمی کار می کند، ارائه دهد. اگرچه پیوندهای بی سیم چالش هایی را در لایه برنامه ایجاد می کنند، تحرکی که آنها را فعال می کنند همچنین مجموعه ای غنی از برنامه های کاربردی آگاه از موقعیت و متن را ممکن می سازد [Baldauf 2007]. به طور کلی تر، شبکه های بی سیم و موبایل همچنان نقش کلیدی در تحقق محیط های محاسباتی فراگیر آینده ایفا خواهند کرد [Weiser 1991]. منصفانه است که بگوییم که ما تنها زمانی که صحبت از تأثیر شبکه های بی سیم و موبایل بر برنامه های کاربردی شبکه و پروتکل های آنها می شود، نوک کوه یخ را دیده ایم!

شبکه‌های بی‌سیم و تلفن همراه ابتدا انقلابی در تلفن ایجاد کردند و اکنون تأثیر عمیق‌تری در دنیای شبکه‌های رایانه‌ای نیز دارند. آنها با دسترسی بدون اتصال خود به زیرساخت شبکه جهانی در هر زمان و هر مکان، نه تنها دسترسی به شبکه را فراگیرتر می‌کنند، بلکه مجموعه جدیدی از خدمات وابسته به مکان را فعال می‌کنند. با توجه به اهمیت روزافزون شبکه‌های بی‌سیم و تلفن همراه، این فصل بر روی اصول، فناوری‌های پیوند رایج و معماری‌های شبکه برای پشتیبانی از ارتباطات بی‌سیم و سیار متمرکز شده است.

ما این فصل را با مقدمه‌ای بر شبکه‌های بی‌سیم و تلفن همراه آغاز کردیم، و تمایز مهمی را بین چالش‌های ناشی از ماهیت بی‌سیم پیوندهای ارتباطی در چنین شبکه‌هایی و تحرکی که این پیوندهای بی‌سیم ایجاد می‌کنند، ترسیم کردیم. این به ما امکان داد تا مفاهیم کلیدی را در هر حوزه بهتر جداسازی، شناسایی و تسلط دهیم. ما ابتدا بر روی ارتباطات بی‌سیم تمرکز کردیم، با در نظر گرفتن ویژگی‌های یک پیوند بی‌سیم در بخش ۷.۲. در بخش‌های ۷.۳ و ۷.۴، جنبه‌های سطح پیوند استاندارد LAN بی‌سیم (WiFi) IEEE 802.11، بلوتوث و شبکه‌های سلولی 4G/5G را بررسی کردیم. سپس توجه خود را به موضوع تحرک معطوف کردیم. در بخش ۷.۵، ما انواع مختلفی از تحرک را شناسایی کردیم، با نقاطی در امتداد این طیف که چالش‌های متفاوتی را مطرح می‌کنند و راه‌حل‌های متفاوتی را پذیرفته‌اند. ما مشکلات مکان‌یابی و مسیریابی به یک کاربر تلفن همراه و همچنین رویکردهای تحویل کاربر تلفن همراه را که به صورت پویا از یک نقطه اتصال به شبکه به نقطه دیگر حرکت می‌کند در نظر گرفتیم. ما بررسی کردیم که چگونه این مسائل در شبکه‌های 4G/5G و در استاندارد IP موبایل مورد توجه قرار گرفته است. در نهایت، ما تأثیر پیوندهای بی‌سیم و تحرک را بر پروتکل‌های لایه انتقال و برنامه‌های کاربردی شبکه در بخش ۷.۷ در نظر گرفتیم. اگرچه ما یک فصل کامل را به مطالعه شبکه‌های بی‌سیم و تلفن همراه اختصاص داده‌ایم، یک کتاب کامل (یا بیشتر) برای کشف کامل این حوزه هیجان‌انگیز و به سرعت در حال گسترش مورد نیاز است. ما شما را تشویق می‌کنیم تا با مراجعه به منابع متعدد ارائه شده در این فصل، عمیق‌تر به این زمینه بپردازید.

مسائل و سوالات تکالیف

فصل ۷ سوالات مروری

بخش ۷.۱

R1. عملکرد یک شبکه بی‌سیم در "حالت زیرساخت" به چه معناست؟ اگر شبکه در حالت زیرساخت نیست،

در چه حالت عملیاتی قرار دارد و تفاوت آن حالت کار با حالت زیرساخت چیست؟

R2. MANET و VANET هر دو شبکه‌های بی‌سیم بدون زیرساخت چند هاپ هستند. چه تفاوتی بین آنها

وجود دارد؟

بخش ۷.۲

R3. تفاوت بین انواع زیر از اختلالات کانال بی سیم چیست: از دست دادن مسیر، انتشار چند مسیری، تداخل از

منابع دیگر؟

R4. همانطور که یک گره متحرک از یک ایستگاه پایه دورتر و دورتر می شود، دو اقدامی که یک ایستگاه پایه

می تواند انجام دهد تا اطمینان حاصل کند که احتمال از دست دادن یک فریم ارسالی افزایش نمی یابد چیست؟

بخش ۷.۳

R5. نقش قاب های چراغ را در ۸۰۲.۱۱ شرح دهید.

R6. یک نقطه دسترسی به صورت دوره ای فریم های چراغ را ارسال می کند. محتویات قاب های بیکن چیست؟

R7. چرا از اعترافات در ۸۰۲.۱۱ استفاده می شود اما در اترنت سیمی استفاده نمی شود؟

R8. تفاوت بین اسکن غیرفعال و اسکن فعال چیست؟

R9. دو هدف اصلی یک قاب CTS چیست؟

R10. فرض کنید فریم های IEEE 802.11 RTS و CTS به اندازه فریم های استاندارد DATA و ACK بودند.

آیا استفاده از فریم های CTS و RTS مزیتی دارد؟ چرا و چرا نه؟

R11. بخش ۷.۳.۴ تحرک ۸۰۲.۱۱ را مورد بحث قرار می دهد که در آن یک ایستگاه بی سیم از یک BSS به

دیگری در همان زیرشبکه حرکت می کند. هنگامی که AP ها با یک سوئیچ به هم متصل می شوند، ممکن است یک

AP نیاز به ارسال یک فریم با یک آدرس MAC جعلی داشته باشد تا سوئیچ بتواند فریم را به درستی ارسال کند.

چرا؟

R12. تفاوت بین بلوتوث و Zigbee از نظر سرعت داده چیست؟

R13. نقش ایستگاه پایه در معماری سلولی G/5G۴ چیست؟ با کدام عناصر شبکه G/5G۴ دیگر (دستگاه تلفن

همراه، HSS، MME، روتر دروازه سرویس، روتر دروازه PDN) مستقیماً در صفحه کنترل ارتباط برقرار می کند؟ در

صفحه داده؟

R14. شناسه مشترک بین المللی تلفن همراه (IMSI) چیست؟

R15. نقش سرویس مشترکین خانگی (HSS) در معماری سلولی G/5G۴ چیست؟ با کدام عناصر شبکه G/5G۴

دیگر (دستگاه تلفن همراه، ایستگاه پایه، MME، روتر دروازه سرویس، روتر دروازه PDN) مستقیماً در صفحه کنترل

ارتباط برقرار می کند؟ در صفحه داده؟

R16. نقش نهاد مدیریت تحرک (MME) در معماری سلولی G/5G⁴ چیست؟ با کدام عناصر شبکه G/5G⁴ دیگر (دستگاه تلفن همراه، ایستگاه پایه، HSS، روتر دروازه سرویس، روتر دروازه PDN) مستقیماً در صفحه کنترل ارتباط برقرار می کند؟ در صفحه داده؟

R17. هدف دو تونل در صفحه داده معماری سلولی G/5G⁴ را شرح دهید. هنگامی که یک دستگاه تلفن همراه به شبکه خانگی خود متصل است، در کدام عنصر شبکه G/5G⁴ (دستگاه تلفن همراه، ایستگاه پایه، HSS، MME، روتر دروازه سرویس، روتر دروازه PDN) هر انتهای هر یک از دو تونل به پایان می رسد؟

R18. سه زیرلایه در لایه پیوند در پشته پروتکل LTE چیست؟ عملکرد آنها را به طور خلاصه شرح دهید.

R19. آیا شبکه دسترسی بی سیم LTE از FDMA، TDMA یا هر دو استفاده می کند؟ پاسخ خود را توضیح دهید.

R20. دو حالت خواب احتمالی یک دستگاه تلفن همراه G/5G⁴ را توضیح دهید. در هر یک از این حالت‌های خواب، آیا دستگاه تلفن همراه بین زمانی که به خواب می‌رود و زمانی که بیدار می‌شود و برای اولین بار دیتاگرام جدیدی را ارسال/دریافت می‌کند، با همان ایستگاه پایه مرتبط باقی می‌ماند؟

R21. منظور از "شبکه بازدید شده" و "شبکه خانگی" در معماری سلولی G/5G⁴ چیست؟

R22. سه تفاوت مهم بین شبکه های سلولی G⁴ و G⁵ را فهرست کنید.

بخش ۷.۵

R23. این که گفته می شود یک دستگاه تلفن همراه "رومینگ" است، به چه معناست؟

R24. منظور از "تحويل" یک دستگاه شبکه چیست؟

R25. تفاوت بین مسیریابی مستقیم و غیرمستقیم دیتاگرام ها به/از میزبان موبایل رومینگ چیست؟

R26. "مسیریابی مثلثی" به چه معناست؟

*عبارات استفاده شده در بالا ممکن است با اصطلاحات موجود در مشخصات رسمی بلوتوث متفاوت باشد. اصطلاحات استفاده شده در مشخصات رسمی با تعهد پیرسون به ارتقای تنوع، برابری، و شمول، و محافظت در برابر تعصب و کلیشه در جمعیت جهانی فراگیرانی که به آنها خدمت می کنیم، همسو نیست.

بخش ۷.۶

R27. تشابه و تفاوت‌های پیکربندی تونل را هنگامی که یک دستگاه تلفن همراه در شبکه خانگی خود ساکن است، در مقابل زمانی که در یک شبکه بازدید شده رومینگ است، توضیح دهید.

R28. هنگامی که یک دستگاه تلفن همراه از یک ایستگاه پایه به ایستگاه دیگر در یک شبکه G/5G^۴ تحویل داده می شود، کدام عنصر شبکه تصمیم می گیرد که این انتقال را آغاز کند؟ کدام عنصر شبکه ایستگاه پایه هدفی را که دستگاه تلفن همراه به آن تحویل داده می شود انتخاب می کند؟

R29. توضیح دهید که چگونه و چه زمانی مسیر ارسال دیتاگرام هایی که وارد شبکه بازدید شده می شوند و به دستگاه تلفن همراه ارسال می شوند، قبل، حین و پس از تحویل تغییر می کند.

R30. عناصر زیر از معماری IP موبایل را در نظر بگیرید: شبکه خانگی، آدرس IP دائمی شبکه خارجی، عامل اصلی، عامل خارجی، ارسال هواپیمای داده، نقطه دسترسی (AP) و WLAN در لبه شبکه. نزدیکترین عناصر معادل در معماری شبکه سلولی G/5G^۴ کدامند؟

بخش ۷.۷

R31. سه رویکردی که می توان برای جلوگیری از داشتن یک پیوند بی سیم واحد که باعث کاهش عملکرد یک اتصال TCP لایه انتقال انتها به انتها می شود، مورد استفاده قرار گیرد؟

چالش ها و مسائل

P1. مثال CDMA تک فرستنده در شکل ۷.۵ را در نظر بگیرید. اگر کد CDMA فرستنده (۱، ۱، ۱، ۱، ۱، ۱، ۱، ۱) -

۱، ۱، ۱) باشد، خروجی فرستنده (برای ۲ بیت داده نشان داده شده) چه خواهد بود؟

P2. فرستنده ۲ را در شکل ۷.۶ در نظر بگیرید. خروجی فرستنده به کانال (قبل از اینکه به سیگنال فرستنده ۱

اضافه شود)، $Z_{2i,m}$ چیست ؟

P3. پس از انتخاب AP که با آن ارتباط برقرار می شود، یک میزبان بی سیم یک فریم درخواست ارتباط را به AP ارسال می کند و AP با یک قاب پاسخ انجمن پاسخ می دهد. هنگامی که با یک AP مرتبط شود، میزبان می خواهد به زیرشبکه (در مفهوم آدرس دهی IP در بخش ۴.۴.۲) که AP به آن تعلق دارد، بپیوندد. بعد میزبان چه کاری انجام می دهد؟

P4. اگر دو فرستنده CDMA دارای کدهای (۱، ۱، ۱، ۱، ۱، ۱، ۱، ۱) و (۱، ۱، ۱، ۱، ۱، ۱، ۱، ۱) باشند.

گیرنده ها می توانند داده ها را به درستی رمزگشایی کنند؟ توجیه.

P5. فرض کنید دو ISP وجود دارد که دسترسی WiFi را در یک کافه خاص فراهم می کند، با هر ISP که AP

خود را دارد و بلوک آدرس IP خود را دارد.

آ. علاوه بر این، فرض کنید که به طور تصادفی، هر AP ISP خود را برای عملکرد در کانال ۱۱ پیکربندی کرده

است. آیا پروتکل ۸۰۲.۱۱ در این شرایط به طور کامل خراب می شود؟ در مورد اینکه چه اتفاقی می افتد زمانی که

دو ایستگاه که هر کدام با یک ISP متفاوت مرتبط هستند، به طور همزمان اقدام به ارسال می کنند، چه اتفاقی می افتد.

ب حال فرض کنید که یک AP روی کانال ۱ و دیگری روی کانال ۱۱ کار می کند. پاسخ های شما چگونه تغییر می کنند؟

P6. در مرحله ۴ پروتکل CSMA/CA، ایستگاهی که با موفقیت یک فریم را ارسال می کند، پروتکل CSMA/CA را برای فریم دوم در مرحله ۲ و نه در مرحله ۱ آغاز می کند. طراحان CSMA/CA چه منطقی ممکن است در ذهن داشته باشند. با داشتن چنین ایستگاهی فریم دوم را فوراً ارسال نمی کند (اگر کانال بیکار احساس شود)؟

P7. فرض کنید یک ایستگاه $802.11b$ پیکربندی شده است تا همیشه کانال را با دنباله RTS/CTS رزرو کند. فرض کنید این ایستگاه به طور ناگهانی می خواهد ۱۰۰۰ بیت داده ارسال کند و تمام ایستگاه های دیگر در این زمان بیکار هستند. نرخ انتقال ۱۰ مگابیت بر ثانیه را در نظر بگیرید. زمان لازم برای ارسال فریم و دریافت تصدیق را به عنوان تابعی از SIFS و DIFS محاسبه کنید، با نادیده گرفتن تاخیر انتشار و با فرض عدم وجود خطای بیت.

P8. سناریوی نشان داده شده در شکل ۷.۳۱ را در نظر بگیرید که در آن چهار گره بی سیم A، B، C و D وجود دارد. پوشش رادیویی چهار گره از طریق بیضی های سایه دار نشان داده شده است. همه گره ها فرکانس یکسانی دارند. هنگامی که A ارسال می کند، فقط می تواند توسط B شنید/دریافت شود. وقتی B ارسال می کند، A و C می توانند از B بشنوند/دریافت کنند. وقتی C ارسال می کند، B و D می توانند از C بشنوند/دریافت کنند. وقتی D ارسال می کند، فقط C می تواند از D بشنود/دریافت کند.

اکنون فرض کنید هر گره دارای منبع بی نهایت پیام است که می خواهد به هر یک از گره های دیگر ارسال کند. اگر مقصد یک پیام، همسایه فوری نباشد، پیام باید ارسال شود. به عنوان مثال، اگر A بخواهد به D ارسال کند، ابتدا باید یک پیام از A برای B ارسال شود، سپس پیام را به C می فرستد، سپس پیام را به D می فرستد. زمان شکاف است، با زمان ارسال پیام دقیقاً یک زمان. شکاف زمانی، به عنوان مثال، مانند در شکاف Aloha. در طول یک شکاف، یک گره می تواند یکی از موارد زیر را انجام دهد: (i) پیامی ارسال کند، (ب) پیامی را دریافت کند (اگر دقیقاً یک پیام برای آن ارسال شود)، (iii) ساکت بماند. مانند همیشه، اگر یک گره دو یا چند ارسال همزمان را بشنود، یک برخورد رخ می دهد و هیچ یک از پیام های ارسالی با موفقیت دریافت نمی شود. در اینجا می توانید فرض کنید که هیچ خطایی در سطح بیت وجود ندارد و بنابراین اگر دقیقاً یک پیام ارسال شود، توسط کسانی که در شعاع ارسال فرستنده هستند به درستی دریافت می شود.

آ. حال فرض کنید یک کنترل کننده دانای کل (یعنی کنترل کننده ای که از وضعیت هر گره در شبکه اطلاع دارد) می تواند به هر گره دستور دهد هر کاری را که می خواهد (کنترل کننده دانای کل) انجام دهد، یعنی پیامی ارسال کند، پیامی را دریافت کند. یا ساکت ماندن با توجه به این کنترل کننده دانای کل، با توجه به اینکه هیچ پیام دیگری بین هیچ جفت منبع/مقصد دیگری وجود ندارد، حداکثر سرعتی که یک پیام داده را می توان از C به A منتقل کرد چقدر است؟

ب اکنون فرض کنید که A پیام ها را به B می فرستد و D پیام هایی را به C ارسال می کند. حداکثر سرعت ترکیبی که در آن پیام های داده می توانند از A به B و از D به C جریان پیدا کنند چقدر است؟

ج اکنون فرض کنید که A پیام ها را به B می فرستد و C پیام هایی را برای D ارسال می کند. حداکثر سرعت ترکیبی که در آن پیام های داده می توانند از A به B و از C به D منتقل شوند چقدر است ؟

د اکنون فرض کنید که لینک های بی سیم با لینک های سیمی جایگزین شده اند. سوالات (الف) تا (ج) را دوباره در این سناریوی سیمی تکرار کنید.

ه. اکنون فرض کنید که ما دوباره در سناریوی بی سیم هستیم و برای هر پیام داده ای که از منبع به مقصد ارسال می شود، مقصد یک پیام ACK را به منبع ارسال می کند (مثلاً مانند TCP). همچنین فرض کنید که هر پیام ACK یک اسلات را اشغال کند. سوالات (c)-(a) بالا را برای این سناریو تکرار کنید.

P9. برق یک منبع گرانبها در دستگاه های تلفن همراه است و بنابراین استاندارد ۸۰۲.۱۱ قابلیت های مدیریت انرژی را فراهم می کند که به گره های ۸۰۲.۱۱ اجازه می دهد تا مدت زمانی را که عملکردهای حس، انتقال و دریافت و سایر مدارها باید «روشن» باشند، به حداقل برسانند. در ۸۰۲.۱۱، یک گره قادر است به طور واضح بین حالت خواب و بیداری متناوب کند. به طور خلاصه توضیح دهید که چگونه یک گره با AP برای انجام مدیریت توان ارتباط برقرار می کند.

P10. سناریوی ایده آل LTE زیر را در نظر بگیرید. کانال پایین دست (شکل ۷.۲۲ را ببینید) در زمان، در فرکانس های F شکاف دارد. چهار گره A، B، C و D وجود دارد که از ایستگاه پایه به ترتیب با سرعت ۱۰ مگابیت در ثانیه، ۵ مگابیت در ثانیه، ۲.۵ مگابیت در ثانیه و ۱ مگابیت در ثانیه در کانال پایین دست قابل دسترسی هستند. این نرخ ها فرض می کنند که ایستگاه پایه از تمام اسلات های زمانی موجود در تمام فرکانس های F برای ارسال فقط به یک ایستگاه استفاده می کند. ایستگاه پایه دارای تعداد نامتناهی داده برای ارسال به هر یک از گره ها است و می تواند با استفاده از هر یک از فرکانس های F در هر شکاف زمانی در فریم پایین دست به هر یک از این چهار گره ارسال کند.

آ. حداکثر سرعتی که ایستگاه پایه می تواند به گره ها ارسال کند، با فرض اینکه می تواند در طول هر شکاف زمانی به هر گره ای که انتخاب می کند ارسال کند، چقدر است؟ آیا راه حل شما منصفانه است؟ منظورتان از «عادلانه» را توضیح دهید و تعریف کنید.

ب اگر یک شرط انصاف وجود داشته باشد که هر گره باید مقدار مساوی داده را در طول هر بازه یک ثانیه دریافت کند، میانگین نرخ انتقال توسط ایستگاه پایه (به همه گره ها) در طول فریم فرعی پایین دست چقدر است؟ توضیح دهید که چگونه به پاسخ خود رسیده اید.

ج فرض کنید که معیار انصاف این است که هر گره می تواند حداکثر دو برابر هر گره دیگری در طول فریم فرعی، داده دریافت کند. میانگین نرخ انتقال توسط ایستگاه پایه (به همه گره ها) در طول زیر فریم چقدر است؟ توضیح دهید که چگونه به پاسخ خود رسیده اید.

P11. در بخش ۷.۵، یک راه حل پیشنهادی که به کاربران تلفن همراه اجازه می داد آدرس های IP خود را در حین جابجایی در بین شبکه های خارجی حفظ کنند، این بود که یک شبکه خارجی مسیر بسیار خاصی را برای کاربر تلفن همراه تبلیغ کند و از زیرساخت مسیریابی موجود برای انتشار این اطلاعات در سراسر شبکه استفاده کند. ما مقیاس پذیری را به عنوان یکی از نگرانی ها شناسایی کردیم. فرض کنید وقتی یک کاربر تلفن همراه از یک شبکه به شبکه دیگر منتقل می شود، شبکه خارجی جدید یک مسیر مشخص را برای کاربر تلفن همراه تبلیغ می کند و شبکه خارجی قدیمی مسیر خود را پس می گیرد. در نظر بگیرید که چگونه اطلاعات مسیریابی در یک الگوریتم برداری فاصله منتشر می شود (به ویژه در مورد مسیریابی بین دامنه ای در بین شبکه هایی که در سراسر جهان هستند).

آ. آیا سایر روترها می توانند به محض اینکه شبکه خارجی تبلیغات مسیر خود را آغاز کرد، دیتاگرام ها را بلافاصله به شبکه خارجی جدید هدایت کنند؟

ب آیا روترهای مختلف می توانند باور کنند که شبکه های خارجی مختلف حاوی کاربر موبایل هستند؟
ج در مورد محدوده زمانی بحث کنید که مسیریاب های دیگر در شبکه در نهایت مسیر دسترسی به کاربران تلفن همراه را یاد می گیرند.

P12. در شبکه های 4G/5G، انتقال داده چه تأثیری بر تأخیرهای سرتاسر دیتاگرام ها بین مبدا و مقصد خواهد داشت؟

P13. دستگاه تلفن همراهی را در نظر بگیرید که روشن می شود و به یک شبکه A بازدید شده LTE متصل می شود، و فرض کنید که مسیریابی غیرمستقیم به دستگاه تلفن همراه از شبکه خانگی H در حال استفاده است. متعاقباً،

در حین رومینگ، دستگاه از محدوده شبکه بازدید شده A خارج می شود و به محدوده شبکه B بازدید شده LTE منتقل می شود. شما یک فرآیند تحویل را از یک ایستگاه پایه BS.A در شبکه بازدید شده A به یک ایستگاه پایه BS.B طراحی خواهید کرد. در شبکه بازدید شده B. مجموعه مراحل را که باید برداشته شوند، ترسیم کنید، و مراقب باشید که عناصر شبکه درگیر (و شبکه هایی که به آنها تعلق دارند) را شناسایی کنید تا این واگذاری انجام شود. فرض کنید که پس از تحویل، تونل از شبکه خانگی به شبکه بازدید شده به بازدید از شبکه B ختم می شود.

P14. دوباره سناریوی مشکل P13 را در نظر بگیرید. اما اکنون فرض کنید که تونل از شبکه خانگی H تا شبکه بازدید شده A همچنان استفاده خواهد شد. یعنی شبکه A بازدید شده به عنوان یک نقطه لنگر پس از انتقال عمل خواهد کرد. (به غیر از: این در واقع فرآیندی است که برای مسیریابی تماس های صوتی سوئیچ مدار به یک تلفن همراه رومینگ در شبکه های GSM 2G استفاده می شود.) در این مورد، تونل (های) اضافی باید برای دسترسی به دستگاه تلفن همراه ساکن آن ساخته شود. شبکه B. یک بار دیگر، مجموعه مراحل را که باید برداشته شوند، ترسیم کنید، و مراقب باشید که عناصر شبکه درگیر (و شبکه هایی که به آنها تعلق دارند) را شناسایی کنید تا این واگذاری انجام شود.

یک مزیت و یک معایب این رویکرد نسبت به رویکردی که در راه حل شما برای مشکل P13 اتخاذ شده است

چیست؟