

به نام خدا

شبکه های Wire Less

امیر انصاری

• استاندارد شبکه های محلی بی سیم

در ماه ژوئن سال ۱۹۹۷ انجمن مهندسان برق و الکترونیک (IEEE) استاندارد IEEE 802.11-۸۰۲،۱۱ را به عنوان اولین استاندارد شبکه های محلی بی سیم منتشر ساخت. این استاندارد در سال ۱۹۹۹ مجدداً بازنگری شد و نگارش روز آمد شده آن تحت عنوان IEEE 802.11-۸۰۲،۱۱ منتشر شد. استاندارد جاری شبکه های محلی بی سیم یا همان IEEE 802.11 تحت عنوان ISO/IEC 8802-11:1999، توسط سازمان استاندارد سازی بین المللی (ISO) و مؤسسه استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال ۱۹۹۷، شکل گیری و پیدایش شبکه سازی محلی بی سیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد ۱۹۹۷، پهنای باند 2 Mbps را تعریف می کند با این ویژگی که در شرایط نامساعد و محیط های دارای اغتشاش (نویز) این پهنای باند می تواند به مقدار 1 Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند 1 Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط های عاری از اغتشاش (نویز) پهنای باند 2 Mbps نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی 2.4 GHz عمل می کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون های رادیویی DSSS و FHSS به عنوان رسانه انتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری ۸۰۲،۱۱ به زیر گروه های متعددی تقسیم می شود. شکل های ۱-۱ و ۱-۲ گروه های کاری فعال در فرآیند استاندارد سازی را نشان می دهد. برخی از مهم ترین زیر گروه ها به قرار زیر است:

- 802.11D: Additional Regulatory Domains
- 802.11E: Quality of Service (QoS)
- 802.11F: Inter-Access Point Protocol (IAPP)
- 802.11G: Higher Data Rates at 2.4 GHz
- 802.11H: Dynamic Channel Selection and Transmission Power Control
- 802.11i: Authentication and Security

کمیته ۸۰۲،۱۱ e کمیته ای است که سعی دارد قابلیت QoS اینترنت را در محیط شبکه های بی سیم ارائه کند. توجه داشته باشید که فعالیت های این گروه تمام گونه های ۸۰۲،۱۱ شامل a، b، و g را در بر دارد. این کمیته در نظر دارد که ارتباط کیفیت سرویس سیمی یا Ethernet

QoS را به دنیای بی‌سیم بی‌آورد. کمیته ۸۰۲٫۱۱g کمیته‌ای است که با عنوان ۸۰۲٫۱۱ توسعه یافته نیز شناخته می‌شود. این کمیته در نظر دارد نرخ ارسال داده‌ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یا باند فرکانسی صنعتی، پژوهشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده ۲۴۰۰ مگاهرتز تا ۲۴۸۳٫۵ مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهای تشعشع رادیویی نیازی به مجوز ندارد. استاندارد ۸۰۲٫۱۱g تا کنون نهایی نشده است و مهم‌ترین علت آن رقابت شدید میان تکنیک‌های مدولاسیون است. اعضای این کمیته و سازندگان تراشه توافق کرده‌اند که از تکنیک تسهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می‌تواند به عنوان یک روش جایگزین و رقیب مطرح باشد.

کمیته ۸۰۲٫۱۱h مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصرفی و نیز توان امواج ارسالی توسط فرستنده‌های مبتنی بر ۸۰۲٫۱۱ است. فعالیت دو کمیته ۸۰۲٫۱۱i و ۸۰۲٫۱۱x در ابتدا بر روی سیستم‌های مبتنی بر ۸۰۲٫۱۱b تمرکز داشت. این دو کمیته مسئول تهیه پروتکل‌های جدید امنیت هستند. استاندارد اولیه از الگوریتمی موسوم به WEP استفاده می‌کند که در آن دو ساختار کلید رمزنگاری به طول ۴۰ و ۱۲۸ بیت وجود دارد. WEP مشخصاً یک روش رمزنگاری است که از الگوریتم RC4 برای رمزنگاری فریم‌ها استفاده می‌کند. فعالیت این کمیته در راستای بهبود مسائل امنیتی شبکه‌های محلی بی‌سیم است.

این استاندارد لایه‌های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بی‌سیم را دربردارد. شکل ۱-۱ جایگاه استاندارد ۸۰۲٫۱۱ را در مقایسه با مدل مرجع نشان می‌دهد

• شبکه‌های بی‌سیم و انواع WPAN , WWAN, WLAN

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط امواج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌ی چون شبکه‌های بی‌سیم سلولی - که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN - Wireless LAN) گرفته تا انواع ساده‌ی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از

امواج مادون قرمز نیز استفاده می کنند، مانند صفحه کلیدها، ماوس ها و برخی از گوشی های همراه، در این دسته بندی جای می گیرند. طبیعی ترین مزیت استفاده از این شبکه ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه ها و همچنین امکان ایجاد تغییر در ساختار مجازی آن ها است. از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم می گردند: **WLAN**، **WWAN** و **WPAN**.

مقصود از **WWAN**، که مخفف **Wireless WAN** است، شبکه هایی با پوشش بی سیم بالاست. نمونه ای از این شبکه ها، ساختار بی سیم سلولی مورد استفاده در شبکه های تلفن همراه است. **WLAN** پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می کند. کاربرد شبکه های **WPAN** یا **Network Wireless Personal Area** برای موارد خانه گی است. ارتباطاتی چون **Bluetooth** و مادون قرمز در این دسته قرار می گیرند. شبکه های **WPAN** از سوی دیگر در دسته ی شبکه های **Ad Hoc** نیز قرار می گیرند. در شبکه های **Ad hoc**، یک سخت افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه می شود. مثالی از این نوع شبکه ها، **Bluetooth** است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرار گرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده ها با دیگر تجهیزات متصل به شبکه را می یابند. تفاوت میان شبکه های **Ad hoc** با شبکه های محلی بی سیم (**WLAN**) در ساختار مجازی آن ها است. به عبارت دیگر، ساختار مجازی شبکه های محلی بی سیم بر پایه ی طرحی ایستاست درحالی که شبکه های **Ad hoc** از هر نظر پویا هستند. طبیعی ست که در کنار مزایایی که این پویایی برای استفاده کننده گان فراهم می کند، حفظ امنیت چنین شبکه هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل های موجود برای افزایش امنیت در این شبکه ها، خصوصاً در انواعی همچون **Bluetooth**، کاستن از شعاع پوشش سیگنال های شبکه است. در واقع مستقل از این حقیقت که عمل کرد **Bluetooth** بر اساس فرستنده و گیرنده های کم توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل توجهی محسوب می گردد، همین کمی توان سخت افزار مربوطه، موجب وجود منطقه ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می گردد. به عبارت دیگر

این مزیت به همراه استفاده از کدهای رمز نه چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به حساب می‌آیند.

• منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قدرت‌مند این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد. در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است:

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌ی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌ی را نیز موجب است.

- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.

- اطلاعات حیاتی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.

- حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.

- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در

شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.

- با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.

- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.

- یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دستیابی به منابع شبکه‌ی سیمی نیابند.

- در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل کرد شبکه نیز وجود دارد.

• مشخصات و خصوصیات WLAN

تکنولوژی و صنعت WLAN به اوایل دهه‌ی ۸۰ میلادی باز می‌گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه‌های محلی بی‌سیم به کندی صورت می‌پذیرفت. با ارایه‌ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای شبکه‌های محلی امکان‌پذیر می‌ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکل‌ها و استانداردهای خانواده‌ی IEEE 802.11 است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می‌دهد.

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

جدول ۱-۲

اولین شبکه‌ی محلی بی‌سیم تجاری توسط **Motorola** پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌ی بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد ۸۰۲٫۱۱ در **IEEE** شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای ۸۰۲٫۱۱a و ۸۰۲٫۱۱b توسط **IEEE** نهایی شده و تولید محصولات بسیاری بر پایه‌ی این استانداردها آغاز شد. نوع **a**، با استفاده از فرکانس حامل ۵GHz، پهنای باندی تا ۵۴Mbps را فراهم می‌کند. در حالی که نوع **b** با استفاده از فرکانس حامل ۲٫۴GHz، تا ۱۱Mbps پهنای باند را پشتیبانی می‌کند. با این وجود تعداد کانال‌های قابل استفاده در نوع **b** در مقایسه با نوع **a**، بیش‌تر است. تعداد این کانال‌ها، با توجه به کشور مورد نظر، تفاوت می‌کند. در حالت معمول، مقصود از **WLAN** استاندارد ۸۰۲٫۱۱b است.

استاندارد دیگری نیز به‌تازگی توسط **IEEE** معرفی شده است که به ۸۰۲٫۱۱g شناخته می‌شود. این استاندارد بر اساس فرکانس حامل ۲٫۴GHz عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا ۵۴Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی‌شدن و معرفی آن نمی‌گذرد، بیش از یک‌سال است که آغاز شده و با توجه سازگاری آن با استاندارد ۸۰۲٫۱۱b، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.

• توپولوژی هـ ای ۸۰۲,۱۱

در یک تقسیم بندی کلی می توان دو همبندی (توپولوژی) را برای شبکه های محلی بی سیم در نظر گرفت. ساده ترین همبندی، فی البداهه (Ad Hoc) و براساس فرهنگ واژگان استاندارد ۸۰۲,۱۱، IBSS است. در این همبندی ایستگاه ها از طریق رسانه بی سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده (تبادل پیام) از تجهیزات یا ایستگاه واسطی استفاده نمی کنند. واضح است که در این همبندی به سبب محدودیت های فاصله هر ایستگاهی ضرورتاً نمی تواند با تمام ایستگاه های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در همبندی IBSS آن است که ایستگاه ها در محدوده عملیاتی بی سیم یا همان بُرد شبکه بی سیم قرار داشته باشند. شکل ۱-۲ همبندی IBSS را نشان می دهد.

• معماری شبکه های محلی بی سیم - , INFRASTRUCTURE ADHOC

استاندارد ۸۰۲,۱۱ b به تجهیزات اجازه می دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت اند از برقراری ارتباط به صورت نقطه به نقطه ؟ همان گونه در شبکه های Ad hoc به کار می رود- و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).

تهیه کننده : امیر انصاری