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 ۸۰۲,۱۱–۱۹۹۷ را به عنوان اولین استانداردِ شبکه‌های محلی بی‌سیم منتشر ساخت. این استاندارد در سال ۱۹۹۹ مجدداً بازنگری شد و نگارش روز آمد شده آن تحت عنوان IEEE ۸۰۲,۱۱–۱۹۹۹ منتشر شد. استاندارد جاری شبکه‌های محلی بی‌سیم یا همان IEEE 802.11 تحت عنوان ISO/IEC 8802-11:1999، توسط سازمان استاندارد سازی بین‌المللی (ISO) و مؤسسه استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال ۱۹۹۷، شکل گیری و پیدایش شبکه سازی محلی بی‌سیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد ۱۹۹۷، پهنای باند ۲Mbps را تعریف می‌کند با این ویژگی که در شرایط نامساعد و محیطهای دارای اغتشاش (نویز) این پهنای باند می‌تواند به مقدار ۱Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند ۱ Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیطهای عاری از اغتشاش (نویز) پهنای باند ۲ Mbpsنیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی ۲,۴ GHz عمل می‌کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون‌های رادیویی DSSS و FHSS به عنوان رسانهانتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری ۸۰۲,۱۱ به زیر گروه‌های متعددی تقسیم می‌شود. شکل‌های ۱–۱ و ۱–۲ گروه‌های کاری فعال در فرآیند استاندارد سازی را نشان می‌دهد. برخی از مهم‌ترین زیر گروه‌ها 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 e۸۰۲,۱۱ کمیته‌ای است که سعی دارد قابلیت QoS اِترنت را در محیط شبکه‌های بی‌سیم ارائه کند. توجه داشته باشید که فعالیت‌های این گروه تمام گونه‌های 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 بیاورد. کمیته g۸۰۲,۱۱ 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 g۸۰۲,۱۱ تا کنون نهایی نشده است و مهم‌ترین علت آن رقابت شدید میان تکنیک‌های مدولاسیون است. اعضاء 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 h۸۰۲,۱۱ مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصرفی و نیز توان امواج ارسالی توسط فرستنده‌های مبتنی بر ۸۰۲,۱۱ است. فعالیت دو کمیته i۸۰۲,۱۱ و x۸۰۲,۱۱ در ابتدا برروی سیستم‌های مبتنی بر b۸۰۲,۱۱ 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 رمز نگاری 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 بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از

امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند : WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN یا Network Wireless Personal Area برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند. شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی‌ست که در کنار مزایایی که این پویایی برای استفاده کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عمل‌کرد Bluetooth بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل‌توجه‌یی محسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می‌گردد. به‌عبارت دیگر

این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب 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 به‌جای 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 نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان 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 پهنای‌باند 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 جنبه‌یی 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 ویژه‌یی را نیز موجب است.

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

– اطلاعات حیاتی‌یی 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، به‌راحتی 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 نیز بیابد.

– در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل‌کرد 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 ۲-۱

اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌یی 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 a۸۰۲,۱۱ و b۸۰۲,۱۱ توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه‌ی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل GHz۵، پهنای باندی تا Mbps۵۴ را فراهم می‌کند. در حالی‌که نوع b با استفاده از فرکانس حامل GHz۲,۴، تا Mbps۱۱ 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 b۸۰۲,۱۱ است.

استاندارد دیگری نیز به‌تازه‌گی توسط IEEE معرفی شده است که به g۸۰۲,۱۱ شناخته می‌شود. این استاندارد بر اساس فرکانس حامل GHz۲,۴ عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا Mbps۵۴ 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 b۸۰۲,۱۱، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.

- **توپولـــــــــــــــــــــوژی هـــــــــــــــــــــای ۸۰۲,۱۱**

در یک تقسیم بندی کلی می‌توان دو همبندی (توپولوژی) را بـرای شـبکه‌هـای محلـی بی‌سیم در نظر گرفت. سـاده‌ترین همبندی، فی‌البداهه (Ad Hoc) و براساس فرهنگ واژگان استاندارد ۸۰۲,۱۱، IBSS است. در این همبندی ایسـتگاه‌هـا از طریـق رسـانه بی‌سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و بـرای تبـادل داده (تبـادل پیام) از تجهیزات یا ایستگاه واسطی استفاده نمی‌کنند. واضح است که در این همبنـدی به سبب محدودیت‌های فاصله هر ایستگاهی ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در همبنـدی IBSS آن اسـت کـه ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان بُرد شبکه بی‌سـیم قـرار داشـته باشـند. شکل۲-۱همبندی IBSSرا نشان می‌دهد.

- **معمـاری شـبکه‌هـای محلـی بـی‌سـیم - INFRASTRUCTURE , ADHOC**

استاندارد b۸۰۲,۱۱ به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شـبکه برقـرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه ?همان‌گونـه در شبکه‌های Ad hoc به‌کار مـی‌رود- و اتصـال بـه شـبکه از طریـق نقـاط تمـاس یـا دسترسی (AP=Access Point).

تهیه کننده : امیر انصاری