عنوان پروژه

Wireless LANs

ارائه دهنده

هومن سلیمانی

به نام خدا

فصل اول

مقدمه
استاندارد شبکه های محلی بی سیم
شبکه‌های بی‌سیم و انواع WPAN , WWAN , WLAN
منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول
مشخصات و خصوصیات WLAN
معماری شبکه‌های محلی بی‌سیم - INFRASTRUCTURE , AD HOC
توپولوژی های ۸۰۲.۱۱
لایه فیزیکی
عناصر فعال شبکه‌های محلی بی‌سیم
دسترسی به رسانه
برد و سطح پوشش
خدمات توزیع

فصل دوم

امنیت و پروتکل WEP
قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱
خدمات ایستگاهی
Authentication
Authentication بدون رمزنگاری
Authentication با رمزنگاری RC4
سرویس Privacy یا confidentiality
Integrity
ضعف‌های اولیه‌ی امنیتی WEP
استفاده از کلیدهای ثابت WEP
IV - Initialization Vector
استفاده از CRC رمز نشده

فصل سوم

ویژگی‌های سیگنال‌های طیف گسترده
سیگنال‌های طیف گسترده با جهش فرکانسی
سیگنال‌های طیف گسترده با توالی مستقیم
استفاده مجدد از فرکانس

فصل چهارم

مقایسه مدلهای ۸۰۲.۱۱
اثرات فاصله
پدیده چند مسیری
استاندارد ۸۰۲.۱۱a
افزایش پهنای باند
طیف فرکانسی تمیزتر
کانال‌های غیرپوشا
استاندارد IEEE 802.11g

فصل پنجم

وضعیت های کاربردی wireless
mode access point
mode wireless ap client
wireless bridge mode
multiple bridge mode
repeater mode

فصل اول

مقدمه

از آن‌جا که شبکه‌های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت.

در این چکیده ، با توجه به گستردگی زیاد مباحث مطرح در زمینه شبکه های بیسیم ، به بررسی بعضی از اصول میپردازیم.

استاندارد شبکه های محلی بی سیم

در ماه ژوئن سال ۱۹۹۷ انجمن مهندسان برق و الکترونیك (IEEE) استاندارد IEEE 802.11-1997 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 802.11-1999 منتشر شد. استاندارد جاری شبکه‌های محلی بی‌سیم یا همانIEEE 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 2 Mbps را تعریف می‌کند با این ویژگی که در شرایط نامساعد و محیطهای دارای اغتشاش (نویز) این پهنای باند می‌تواند به مقدار 1 Mbps کاهش یابد. روش 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 محیطهای عاری از اغتشاش (نویز) پهنای باند2 Mbps نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی ۲.٤ GHz عمل می‌کنند. گروه کاری ۸۰۲.۱۱ به زیر گروه‌های متعددی تقسیم می‌شود. 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 802.11e کمیته‌ای است که سعی دارد قابلیت QoS اِتِرنت را در محیط شبکه‌های بی‌سیم ارائه کند. 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 802.11g 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، یك باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده ۲٤۰۰ مگاهرتز تا ۲٤۸۳.٥ مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهای تشعشع رادیویی نیازی به مجوز ندارد. استاندارد 802.11g تا کنون نهایی نشده است و مهم‌ترین علت آن رقابت شدید میان تکنیك‌های مدولاسیون است. اعضاء این کمیته و سازندگان تراشه توافق کرده‌اند که از تکنیك تسهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می‌تواند به عنوان یك روش جایگزین و رقیب مطرح باشد.

کمیته 802.11h مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصرفی و نیز توان امواج ارسالی توسط فرستنده‌های مبتنی بر ۸۰۲.۱۱ است.

فعالیت دو کمیته 802.11i و 802.11x در ابتدا برروی سیستم‌های مبتنی بر ۸۰۲.۱۱bتمرکز 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 ٤٠ و ١٢٨ بیت وجود دارد. WEP مشخصاً يك 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 يك شبکه محلی با اتصال بی‌سیم را دربردارد .

انواع شبکه های بی سیم

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط اموج 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 خصوصیاتWLAN

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.

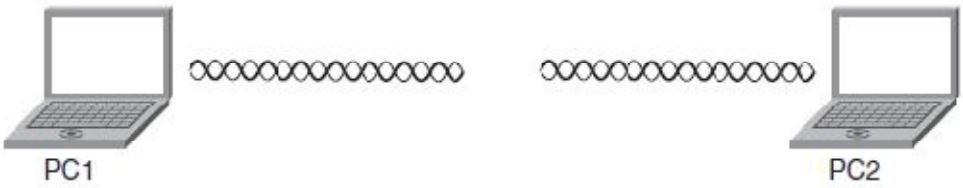
اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌یی بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد ۸۰۲.۱۱ در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و۸۰۲.۱۱b 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 Mbps٥٤ را فراهم می‌کند. در حالی‌که نوع b با استفاده از فرکانس حامل GHz۲.٤، 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 ۸۰۲.۱۱bاست.

استاندارد دیگری نیز به‌تازه‌گی توسط IEEE معرفی شده است که به 802.11gشناخته می‌شود. این استاندارد بر اساس فرکانس حامل GHz۲.٤ عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا Mbps٥٤ 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.

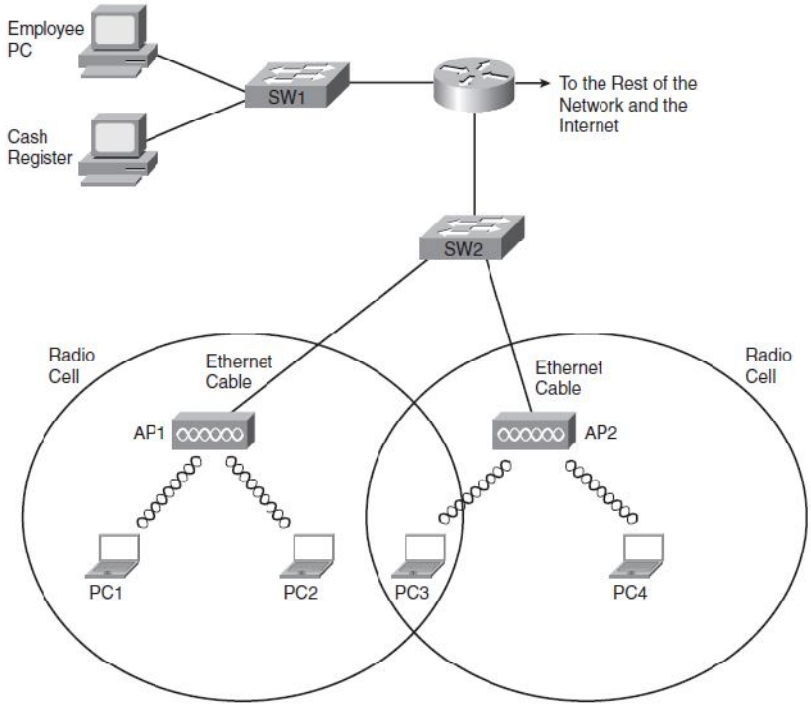
معماری شبکه‌های محلی بی‌سیم

INFRASTRUCTURE , AD HOC

استاندارد ۸۰۲.۱۱bبه تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه ?همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود- و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point). شکل زیر روش Ad hoc را نشان میدهد.



شکل زیر نیز نمایشی از مدل Infrastructure است



توپولوژی های ۸۰۲.۱۱

در یك تقسیم بندی كلی می‌توان دو توپولوژی را برای شبكه‌های محلی بی‌سیم در نظر گرفت. ساده‌ترین توپولوژی ، Ad Hoc و براساس فرهنگ واژگان استاندارد ۸۰۲.۱۱، IBSS است. در این توپولوژی ایستگاه‌ها از طریق رسانه بی‌سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده (تبادل پیام) از تجهیزات یا ایستگاه واسطی استفاده نمی‌كنند. واضح است كه در این توپولوژی به سبب محدودیت‌های فاصله هر ایستگاهی ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در توپولوژی IBSS آن است كه ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان بُرد شبكه بی‌سیم قرار داشته باشند.

توپولوژی دیگر زیرساختار است. در این توپولوژی عنصر خاصی موسوم به نقطه دسترسی وجود دارد. نقطه دسترسی ایستگاه‌های موجود در یك مجموعه سرویس را به سیستم توزیع متصل می‌کند. در این هم بندی تمام ایستگاه‌ها با نقطه دسترسی تماس می‌گیرند و اتصال مستقیم بین ایستگاه‌ها وجود ندارد در واقع نقطه دسترسی وظیفه دارد فریم‌ها را بین ایستگاه‌ها توزیع و پخش کند.

در این توپولوژی سیستم توزیع، رسانه‌ای است که از طریق آن نقطه دسترسی (AP) با سایر نقاط دسترسی در تماس است و از طریق آن می‌تواند فریم‌ها را به سایر ایستگاه‌ها ارسال نماید. از سوی دیگر می‌تواند بسته‌ها را در اختیار ایستگاه‌های متصل به شبکه سیمی نیز قراردهد. در استاندارد ۸۰۲.۱۱ توصیف ویژه‌ای برای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین می‌کند که سیستم توزیع می‌بایست ارائه نماید. بنابراین سیستم توزیع می‌تواند یك شبکه ۸۰۲.۳ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم می‌کند.

استاندارد ۸۰۲.۱۱ با استفاده از توپولوژی خاصی محدوده عملیاتی شبکه را گسترش می‌دهد. این توپولوژی به شکل مجموعه سرویس گسترش یافته (ESS) بر پا می‌شود. در این روش یك مجموعه گسترده و متشکل از چندین BSS یا مجموعه سرویس پایه از طریق نقاط دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیك داده بین مجموعه‌های سرویس پایه مبادله شده و انتقال پیام‌ها شکل می‌گیرد. در این توپولوژی ایستگاه‌ها می‌توانند در محدوده عملیاتی بزرگ‌تری گردش نمایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم می‌شود. در واقع سیستم توزیع ستون فقرات شبکه‌های محلی بی‌سیم است و می‌تواند با استفاده از فنّاوری بی‌سیم یا شبکه‌های سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان یك لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش می‌باشد. نکته قابل توجه در این توپولوژی آن است که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه‌های سیّار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت یك شبکه منفرد در سطح لایه MAC تلقی می‌کنند. به این ترتیب پروتکل‌های رایج شبکه‌های کامپیوتری کوچکترین تأثیری از سیّار بودن ایستگاه‌ها و رسانه بی‌سیم نمی‌پذیرند. جدول زیر توپولوژی‌های رایج در شبکه‌های بی‌سیم مبتنی بر ۸۰۲.۱۱ را به اختصار جمع بندی می‌کند.

802.11 Topologies		
Independent Basic Service Set (IBSS) ("Ad Hoc" or "Peer to Peer")	**Infrastructure**	
	Basic Service Set (BSS)	Extended Service Set (ESS)

معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شود و با روش‌هایی می‌توان یک سخت‌افزار مجهز به امکان ارتباط بر اساس استاندارد ۸۰۲.۱۱bرا میان سلول‌های مختلف حرکت داد. گستره‌یی که یک AP پوشش می‌دهد را BSS-Basic Service Set می‌نامند. مجموعه‌ی تمامی سلول‌های یک ساختار کلی شبکه، که ترکیبی از BSSهای شبکه است، را ESS-Extended Service Set می‌نامند. با استفاده از ESS می‌توان گستره‌ی وسیع‌تری را تحت پوشش شبکه‌ی محلی بی‌سیم درآورد.

در سمت هریک از سخت‌افزارها که معمولاً client هستند، کارت شبکه‌یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند. AP علاوه بر ارتباط با چند کارت شبکه‌ی بی‌سیم، به بستر پرسرعت‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان Clientهای مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود .

همان‌گونه که گفته شد، اغلب شبکه‌های محلی بی‌سیم بر اساس ساختار فوق، که به نوع

Infrastructure نیز موسوم است، پیاده‌سازی می‌شوند. با این وجود نوع دیگری از شبکه‌های محلی بی‌سیم نیز وجود دارند که از همان منطق نقطه‌به‌نقطه استفاده می‌کنند. در این شبکه‌ها که عموماً Ad hoc نامیده می‌شوند یک نقطه‌ی مرکزی برای دسترسی وجود ندارد و سخت‌افزارهای همراه (مانند کامپیوترهای کیفی و جیبی یا گوشی‌های موبایل) با ورود به محدوده‌ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می‌گردند. این شبکه‌ها به بستر شبکه‌ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set) نیز خواند می‌شوند

شبکه‌های Ad hoc از سویی مشابه شبکه‌های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه‌یی به عنوان Server وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می‌توانند پرونده‌های مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند.

به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر استانداردها، لایهدسترسی به رسانه (MAC) در استاندارد ۸۰۲.۱۱ می‌بایست از دید لایه‌های بالاتر مشابه يك شبكه محلی مبتنی بر استاندارد ۸۰۲ عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیّاربودن ایستگاه‌های کاری را به گونه‌ای شفاف پوشش دهد که از دید لایه‌های بالاتر استاندارد این سیّاربودن احساس نشود. این نکته سبب می‌شود که لایهMAC در این استاندارد وظایفی را بر عهده بگیرد که معمولاً توسط لایه‌های بالاتر شبکه انجام می‌شوند. در واقع این استاندارد لایه‌های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه می‌کند و به طور مشخص لایه فیزیکی جدید از فرکانس‌های رادیویی به عنوان رسانهانتقال بهره می‌برد.

لایه فیزیکی

در این استاندارد لایه فیزیکی سه عملکرد مشخص را انجام می‌دهد. اول آنکه رابطی برای تبادل فریم‌های لایه MAC جهت ارسال و دریافت داده‌ها فراهم می‌کند. دوم اینکه با استفاده از روش‌های تسهیم فریم‌های داده را ارسال می‌کند و در نهایت وضعیت رسانه (کانال راديويي) را در اختیار لایه بالاتر (MAC) قرار می‌دهد. سه تکنيك راديويی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر می‌باشند:

- استفاده از تکنيك راديويی DSSS
- استفاده از تکنيك راديويی FHSS
- استفاده از امواج راديويی مادون قرمز

در این استاندار لایه فیزیکی می‌تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ ۱ یا ۲ مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون ١٦-PPM و ٤-PPMمبادله می‌شوند.

عناصر فعال شبکه‌های محلی بی‌سیم

در شبکه‌های محلی بی‌سیم معمولاً دو نوع عنصر فعال وجود دارد :

-ایستگاه بی سیم

ایستگاه یا client بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود.

- نقطه ی دسترسی (access point)

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی‌کرده اند.

ايستگاه بي سيم

ایستگاه یا client بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک

کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.
کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در PCMCIA Slot است. در صورت نیاز به استفاده از این کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی PCI express slot نصب می‌کنند.

نقطه ی دسترسی - access point

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی‌کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، clientها و ایستگاه‌های بی‌سیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

دسترسی به رسانه

روش دسترسی به رسانه در این استاندارد CSMA/CA است که تاحدودی به روش دسترسی CSMA/CD شباهت دارد. در این روش ایستگاه‌های کاری قبل از ارسال داده کانال رادیویی را کنترل می‌کنند و در صورتی که کانال آزاد باشد اقدام به ارسال می‌کنند. در صورتی که کانال رادیویی اشغال باشد با استفاده از الگوریتم خاصی به اندازه يك زمان تصادفی صبر کرده و مجدداً اقدام به کنترل کانال رادیویی می‌کنند. در روش CSMA/CA ایستگاه فرستنده ابتدا کانال فرکانسی را کنترل کرده و در صورتی که رسانه به مدت خاصی موسوم به DIFS آزاد باشد اقدام به ارسال می‌کند. گیرنده فیلد کنترلی فریم یا همان CRC را چك می‌کند و سپس يك فریم تصدیق می‌فرستد. دریافت تصدیق به این معنی است که تصادمی بروز نکرده است. در صورتی که فرستنده این تصدیق را دریافت نکند، مجدداً فریم را ارسال می‌کند. این عمل تا زمانی ادامه می‌یابد که فریم تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم‌ها به تعداد آستان‌های مشخصی برسد که پس از آن فرستنده فریم را دور می‌اندازد.

در شبکه‌های بی‌سیم بر خلاف اِترنت امکان شناسایی و آشکار سازی تصادم به دو علت وجود ندارد:

پیاده سازی مکانیزم آشکار سازی تصادم به روش ارسال رادیویی دوطرفه نیاز دارد که با استفاده از آن ایستگاه سیّار بتواند در حین ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می‌شود.
در يك شبکه بی‌سیم، بر خلاف شبکه‌های سیمی، نمی‌توان فرض کرد که تمام ایستگاه‌های سیّار امواج یکدیگر را دریافت می‌کنند. در واقع در محیط بی‌سیم حالاتی قابل تصور است که به آنها نقاط پنهان می‌گوییم. در این حالت ایستگاه‌های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.

برای غلبه بر این مشکل، استاندارد ۸۰۲.۱۱ از تکنیکی موسوم به اجتناب از تصادم و مکانیزم تصدیق استفاده می‌کند. همچنین با توجه به احتمال بروز روزنه‌های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به شنود مجازی رسانه یا VCS استفاده می‌شود. در این روش ایستگاه فرستنده ابتدا يك بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می‌فرستد. هنگامی که گیرنده این فریم را دریافت می‌کند، رسانه را کنترل می‌کند و در صورتی که رسانه آزاد باشد فریم کنترلی CTS را به نشانی فرستنده ارسال می‌کند. تمام ایستگاه‌هایی که فریم‌های کنترلی RTS/CTS را دریافت می‌کنند وضعیت کنترل رسانه خود موسوم به

شاخصNAV را تنظیم می‌کنند. در صورتی که سایر ایستگاه‌ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می‌کنند که مرتباً به صورت پویا تغییر می‌کند. به این ترتیب مشکل روزنه‌های پنهان حل شده و تصادم‌ها نیز به حداقل مقدار می‌رسند

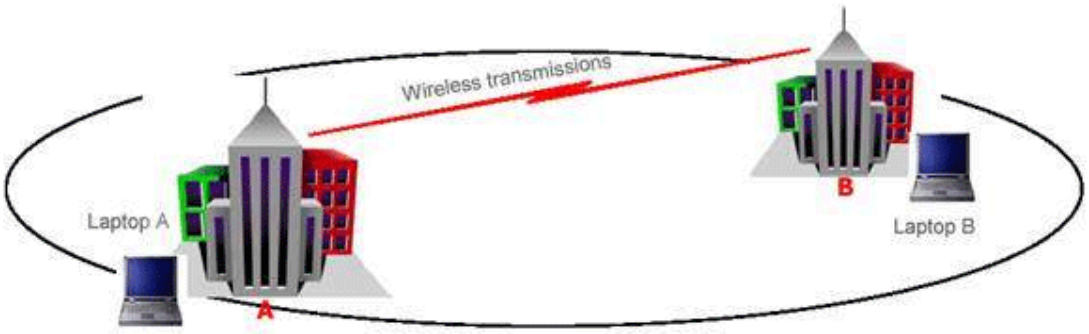
برد و سطح پوشش

شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد ۸۰۲.۱۱ به فاکتورهای بسیاری بسته‌گی دارد که برخی از آن‌ها به شرح زیر هستند :

- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این‌وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرت‌مندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.
با این وجود شعاع کلی‌یی که برای استفاده از این پروتکل 802.11b ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عمل‌کرد ، مقداری‌ست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌های بی‌سیم را به‌دست آورد.
اتصال میان نقاط دست‌رسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.
نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل ۸۰۲.۱۱bاست.
برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به‌دست آورد.
شکل ۳-٤ زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دست‌رسی مناسب را نشان می‌دهد :



از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند

نقطه‌ی دست‌رسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

خدمات توزیع

خدمات توزیع عملکرد لازم در توپولوژی‌های مبتنی بر سیستم توزیع را مهیا می‌سازد. معمولاً خدمات توزیع توسط نقطه دسترسی فراهم می‌شوند. خدمات توزیع در این استاندارد عبارتند از:

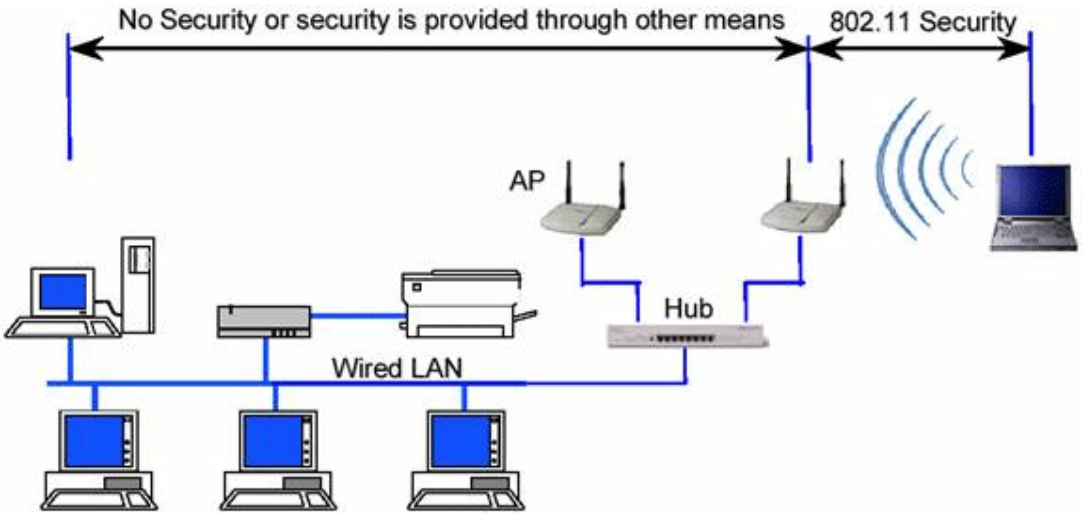
- پیوستن به شبکه
- خروج از شبکه بی‌سیم
- پیوستن مجدد
- توزیع
- مجتمع سازی

سرویس اول یك ارتباط منطقی میان ایستگاه سیّار و نقطه دسترسی فراهم می‌کند. هر ایستگاه کاری قبل از ارسال داده می‌بایست با یك نقطه دسترسی برروی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می‌دهد که فریم‌های ارسال شده به سمت ایستگاه سیّار را به درستی در اختیارش قرار دهد. خروج از شبکه بی‌سیم هنگامی بکار می‌رود که بخواهیم اجباراً ارتباط ایستگاه سیّار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیّار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیّار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی‌سیم" است با این تفاوت که در این سرویس ایستگاه سیّار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می‌کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرك و سیّار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمك می‌کند که با نقطه دسترسی قبلی تماس گرفته و فریم‌های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیّار فرستاده شده‌اند. با استفاده از سرویس توزیع فریم‌های لایه MAC به مقصد مورد نظرشان می‌رسند. مجتمع سازی سرویسی است که شبکه محلی بی‌سیم را به سایر شبکه‌های محلی و یا یك یا چند شبکه محلی بی‌سیم دیگر متصل می‌کند. سرویس مجتمع سازی فریم‌های ۸۰۲.۱۱ را به فریم‌هایی ترجمه می‌کند که بتوانند در سایر شبکه‌ها (به عنوان مثال ۸۰۲.۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم‌های سایر شبکه‌ها نیز به فریم‌های ۸۰۲.۱۱ ترجمه شده و از طریق امواج در اختیار ایستگاه‌های کاری سیّار قرار می‌گیرند.

فصل دوم

امنیت و پروتکلWEP

از این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت‌های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد. استاندارد ۸۰۲.۱۱ سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP =Wired Equivalent Privacy تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان clientها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد ۸۰۲.۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد ۸۰۲.۱۱ فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، هرچند سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشت این‌ست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.
بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی clientها و سخت‌افزارهای بی‌سیم، خصوصاً clientهای بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های سیمی و بی‌سیم‌یی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد :

- Authentication
- Confidentiality
- Integrity

Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت client بی‌سیم است. این عمل که در واقع کنترل دست‌رسی به شبکه‌ی بی‌سیم است، سعی دارد که امکان اتصال clientهایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality

محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

Integrity

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان clientهای بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد.

خدمات ایستگاهی

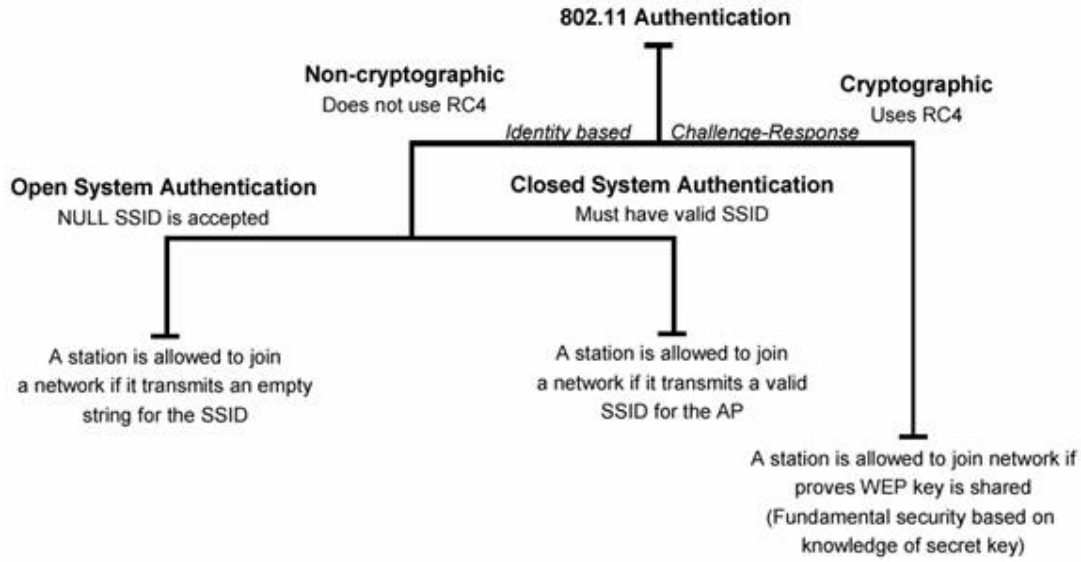
بر اساس این استاندارد خدمات خاصی در ایستگاه‌های کاری پیاده‌سازی می‌شوند. در حقیقت تمام ایستگاه‌های کاری موجود در يك شبکه محلی مبتنی بر ۸۰۲.۱۱ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه‌های سیمی، در شبکه‌های بی‌سیم قابل اعمال نیست استاندارد ۸۰۲.۱۱ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می‌نماید. سرویس هویت سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی‌سیم برای تبادل داده استفاده نماید. در يك تقسیم بندی کلی ۸۰۲.۱۱ دو گونه خدمت هویت سنجی را تعریف می‌کند:

- Authentication Open System
- Shared Key Authentication

روش اول، متد پیش فرض است و یك فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یك فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می‌کند. ایستگاه گیرنده نیز فریمی در پاسخ می‌فرستد که آیا فرستنده را می‌شناسد یا خیر.
روش دوم کمی پیچیده‌تر است و فرض می‌کند که هر ایستگاه از طریق یك کانال مستقل و امن، یك کلید مشترك سرّی دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترك و با بهره‌گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می‌نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این سرویس، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌گردد.
در یك شبکه بی‌سیم، تمام ایستگاه‌های کاری و سایر تجهیزات قادر هستند ترافیك داده‌ای را "بشنوند". در واقع ترافیك در بستر امواج مبادله می‌شود که توسط تمام ایستگاه‌های کاری قابل دریافت است. این ویژگی سطح امنیتی یك ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد. به همین دلیل در استاندارد ۸۰۲.۱۱ پروتکلی موسوم به WEP تعبیه شده است که برروی تمام فریم‌های داده و برخی فریم‌های مدیریتی و هویت سنجی اعمال می‌شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء وپوشش را معادل با شبکه‌های سیمی نماید.

Authentication

استاندارد ۸۰۲.۱۱ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.
شکل زیر شَمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد :



همان‌گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می‌کند و روش دیگر از هیچ تکنیک رمزنگاری‌یی استفاده نمی‌کند.

Authentication بدون رمزنگاری

Authentication بدون رمزنگاری (Open System Authentication)

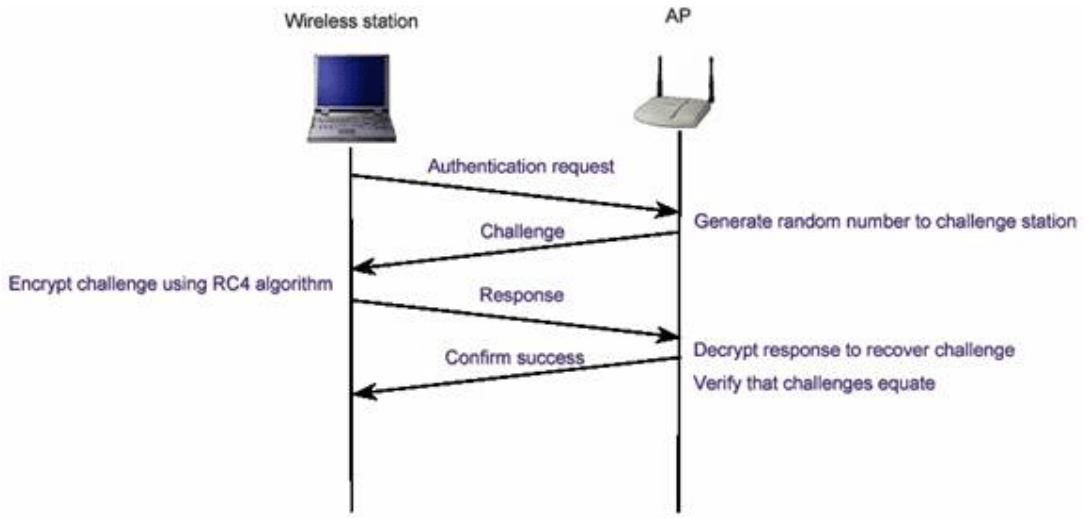
در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت client وجود دارد. در هر دو روش client متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک Service Set Identifier=SSID پاسخ می‌دهد.
در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی clientهایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به‌همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.
نکته‌یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را ارایه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن‌جایی‌که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم – که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخدادن حملات نیز خود تضمینی ندارد!

Authenticationبا رمزنگاری RC4

(shared key authentication)

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه client از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد :



در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن‌را به client می‌فرستد. Client این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته‌ی ارسال شده مقایسه می‌کند. در صورت هم‌سانی این دو پیام، نقطه‌ی دسترسی از اینکه client کلید صحیحی را در اختیار دارد اطمینان حاصل می‌کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.
در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است :

الف) در این روش تنها نقطه‌ی دسترسی‌ست که از هویت client اطمینان حاصل می‌کند. به بیان دیگر client هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمزی‌ست نقطه‌ی دسترسی اصلی‌ست.

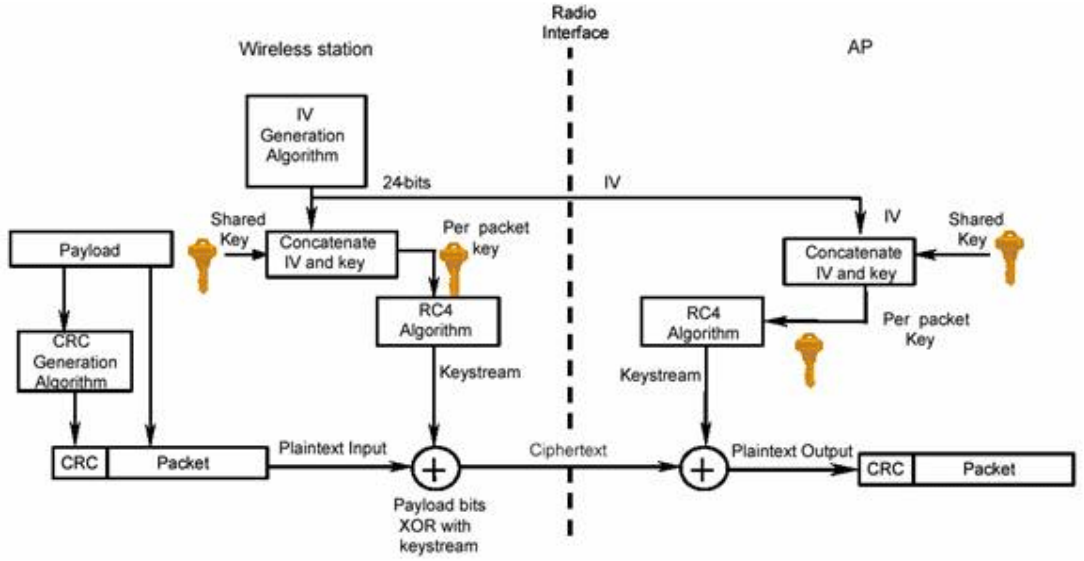
ب) تمامی روش‌هایی که مانند این روش بر پایه‌ی سئوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می‌گیرد و به‌گونه‌یی هریک از دو طرف را گمراه می‌کند.

سرویس Confidentiality

این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگاه‌داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی‌که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

در استاندارد 802.11b، از تکنیک‌های رمزنگاری WEP استفاده می‌گردد که برپایه‌ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته‌ی نیمه تصادفی تولید می‌گردد و توسط آن کل داده رمز می‌شود. این رمزنگاری بر روی تمام بسته‌ی اطلاعاتی پیاده می‌شود. به‌بیان دیگر داده‌های تمامی لایه‌های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه‌های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه‌های محلی بی‌سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به‌اختصار WEP گفته می‌شود.

کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌یی بالاست که قدرت پردازش سیستم‌های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.
هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این‌ست که روش تأمین محرمانه‌گی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute-force، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.
نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل نمایش داده شده است :



Integrity

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست‌های امنیتی‌یی که Integrity را تضمین می‌کنند روش‌هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم‌ترین میزان تقلیل می‌دهند.

در استاندارد ۸۰۲.۱۱ نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان clientهای بی‌سیم و نقاط دست‌رسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. یک CRC-32 قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده‌های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو CRC به‌معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد b.۸۰۲ ۱۱ هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به‌صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به‌صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد clientهای شبکه از حدی می‌گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

ضعف‌های اولیه‌ی امنیتیWEP

در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد ۸۰۲.۱۱ بر اساس پروتکل WEP استوار است. WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند.

نکته‌یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه‌ی کلیدهاست. با وجود آن که با بالارفتن اندازه‌ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می‌رود، ولی از آن‌جاکه این کلیدها توسط کاربران و بر اساس یک کلمه‌ی عبور تعیین می‌شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان‌طور که در قسمت‌های پیشین نیز ذکر شد، دست‌یابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه‌ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی‌های بسیاری را برای تعیین حفره‌های امنیتی این استاندارد انجام داده‌اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی‌های انجام شده فهرستی از ضعف‌های اولیه‌ی این پروتکل است :

۱. استفاده از کلیدهای ثابت WEP
۲. Initialization Vector -IV

استفاده از کلیدهای ثابتWEP

یکی از ابتدایی‌ترین ضعف‌ها که عموماً در بسیاری از شبکه‌های محلی بی‌سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می‌دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می‌کند به سرقت برود یا برای مدت زمانی در دست‌رس نفوذگر باشد، کلید آن به‌راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه‌های کاری عملاً استفاده از تمامی این ایستگاه‌ها ناامن است.
از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال‌های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

Initialization Vector - IV

این بردار یک فیلد ۲۴ بیتی است. این بردار به صورت متنی ساده فرستاده می شود. از آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.
این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

ضعف در الگوریتم

از آن‌جایی‌که IV در تمامی بسته‌های تکرار می‌شود و بر اساس آن کلید تولید می‌شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IVها و بسته‌های رمزشده بر اساس کلید تولید شده بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن‌جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی‌شود. لذا بسته‌های تأییدی که از سوی نقاط دسترسی بی‌سیم به‌سوی گیرنده ارسال می‌شود بر اساس یک CRC رمزنشده ارسال می‌گردد و تنها در صورتی که نقطه‌ی دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می‌فرستد. این ضعف این امکان را فراهم می‌کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به‌راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دسترسی بماند که آیا بسته‌ی تأیید را صادر می کند یا خیر.

ضعف‌های بیان شده از مهمترین ضعف‌های شبکه‌های بی‌سیم مبتنی بر پروتکل WEP هستند. نکته‌یی که در مورد ضعف‌های فوق باید به آن اشاره کرد این است که در میان این ضعف‌ها تنها یکی از آن‌ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می‌گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می‌گردد و بقیه‌ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

جدول زیر ضعف‌های امنیتی پروتکل WEP را به‌اختصار جمع‌بندی کرده است :

	Security Issue / Vulnerability	Remarks
1.	**Security features in vendor products are frequently not enabled.**	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2.	**IVs are short (or static).**	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3.	**Cryptographic keys are short.**	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4.	**Cryptographic keys are shared.**	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5.	**Cryptographic keys cannot be updated automatically and frequently.**	Cryptographic keys should be changed often to prevent brute-force attacks.
6.	**RC4 has a weak key schedule and is inappropriately used in WEP.**	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7.	**Packet integrity is poor.**	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8.	**No user authentication occurs.**	Only the device is authenticated. A device that is stolen can access the network.
9.	**Authentication is not enabled; only simple SSID identification occurs.**	Identity-based systems are highly vulnerable particularly in a wireless system.
10.	**Device authentication is simple shared-key challenge-response.**	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

فصل سوم

ویژگی‌های سیگنال‌های طیف گسترده

عبارت طیف گسترده به هر تکنیکی اطلاق می‌شود که با استفاده از آن پهنای باند سیگنال ارسالی بسیار بزرگ‌تر از پهنای باند سیگنال اطلاعات باشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیك مطرح می‌شود آن است که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یك منبع با ارزش، چه دلیلی برای گسترش طیف سیگنال و مصرف پهنای باند بیشتر وجود دارد. پاسخ به این سوال در ویژگی‌های جالب توجه سیگنال‌های طیف گسترده نهفته است. این ویژگی‌های عبارتند از:

- پایین بودن توان چگالی طیف به طوری که سیگنال اطلاعات برای شنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می‌رسد.
- مصونیت بالا در مقابل پارازیت و تداخل
- رسایی با تفکیك پذیری و دقت بالا
- امکان استفاده در CDMA

مزایای فوق کمیسیون FCC را بر آن داشت که در سال ۱۹۸۵ مجوز استفاده از این سیگنال‌ها را با محدودیت حداکثر توان یك وات در محدوده ISM صادر نماید.

سیگنال‌های طیف گسترده با جهش فرکانسی

در یك سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یك ترکیب کننده تغییر می‌کند.

Pseudonoise code =PN-CODE

در این شکل سیگنال اطلاعات با استفاده از یك تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می‌شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگ‌تری در مقایسه با سیگنال اطلاعات انتخاب می‌شود. با توجه به اینکه فرکانس‌های pn-code با استفاده از یك ثبات انتقالی همراه با پس خور ساخته می‌شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملا تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می‌گوییم.

بر اساسی مقررات FCC و سازمان‌های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی ٤۰۰ میلی ثانیه است که برابر با حداقل ۲.۵ جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد ۸۰۲.۱۱ حداقل فرکانس جهش در آمریکای شمالی و اروپا ٦ مگاهرتز و در ژاپن ۵ مگاهرتز می‌باشد.

سیگنال‌های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یك سیگنال برروی یك باند فرکانسی بزرگتر از طریق تسهیم آن با یك امضاء یا کُد به گونه‌ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یك کُد تسهیم می‌شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می‌گردد. در استاندارد ۸۰۲.۱۱ روش مدولاسیون مورد استفاده در سیستم‌های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تهسیم می‌شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.
از آنجا که در استاندارد ۸۰۲.۱۱ و سیستم DSSS از روش تسهیم DPSK استفاده می‌شود، داده‌های خام به صورت تفاضلی تسهیم شده و ارسال می‌شوند و در گیرنده نیز یك آشکار ساز تفاضلی سیگنال‌های داده را دریافت می‌کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم

PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال‌های داده تغییر می‌کند. به عنوان مثال در تکنیك QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت‌های داده تغییر می‌کند.

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیك FH از یك کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می‌شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیماً توسط یك دنباله از کدهای شبه تصادفی تسهیم می‌شود. در این تکنیك نرخ بیتی شبه کُد تصادفی، نرخ تراشه نامیده می‌شود. در استاندارد ۸۰۲.۱۱ از کُدی موسوم به کُد بارکر برای تولید کدها تراشه سیستم DSSS استفاده می‌شود. مهم‌ترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه آن یك فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یك دنباله بیتی شناسایی کند.
کدهای بارکر از ۸ دنباله تشکیل شده است. در تکنیك DSSS که در استاندارد ۸۰۲.۱۱ مورد استفاده قرار می‌گیرد، از کد بارکر با طول ۱۱ (N=11) استفاده می‌شود. این کد به ازاء یك نماد، شش مرتبه تغییر فاز می‌دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد ٦ مرتبه تغییر فاز خواهد داد.

لازم به یادآوری است که کاهش پیچیدگی سیستم ناشی از تکنیك تسهیم تفاضلی DPSK به قیمت افزایش نرخ خطای بیتی به ازاء یك نرخ سیگنال به نویز ثابت و مشخص است.

استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه‌های بی‌سیم، طراحی شبکه سلولی به گونه‌ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد.

در این طراحی به هریك از سلول‌های همسایه یك کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول‌های همسایه به حداقل رسیده است. این تکنیك همان مفهومی است که در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می‌رود. نکته جالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است.

فصل چهارم

مقایسه مدلهای ۸۰۲.۱۱

ستاندارد b۸۰۲.۱۱

همزمان با برپایی استاندارد IEEE 802.11bیا به اختصار b۱۱. در سال ۱۹۹۹، انجمن مهندسین برق و الکترونیك تحول قابل توجهی در شبکه سازی‌های رایج و مبتنی بر اترنت ارائه کرد. این استاندارد در زیر لایه دسترسی به رسانه از پروتکل CSMA/CA سود می‌برد. سه تکنیك رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر است:

- استفاده از تکنیك رادیویی DSSS در باند فرکانسی GHz۲.٤ به همراه روش مدولاسیون CCK
- استفاده از تکنیك رادیویی FHSS در باندفرکانسی ۲.٤ GHz به همراه روش مدولاسیون CCK
- استفاده از امواج رادیویی مادون قرمز

در استاندار ۸۰۲.۱۱ اولیه نرخ‌های ارسال داده ۱ و ۲ مگابیت در ثانیه است. در حالی که در استاندارد ۸۰۲.۱۱bبا استفاده از تکنیك CCK و روش تسهیم QPSK نرخ ارسال داده به ۵.۵ مگابیت در ثانیه افزایش می‌یابد همچنین با به کارگیری تکنیك DSSS نرخ ارسال داده به ۱۱ مگابیت در ثانیه می‌رسد.
به طور سنتی این استانداردر از دو فنّاوری DSSS یا FHSS استفاده می‌کند. هر دو روش فوق برای ارسال داده با نرخ های ۱ و ۲ مگابیت در ثانیه مفید هستند. جدول ۳-۱ سرعت مختلف قابل دسترسی در این استاندارد را نشان می‌دهد.

Bits/Symbol	Symbol Rate	Modulation	Code Length	Data Rate
1	1 MSps	BPSK	11 (Barker Sequence)	1 Mbps
2	1 MSps	QPSK	11 (Barker Seq.)	2 Mbps
4	1.375 MSps	QPSK	8 CCK	5.5 Mbps
8	1.375 MSps	QPSK	8 CCK	11 Mbps

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC، مخابره و ارسال فرکانس های رادیویی را کنترل می‌کند. این کمیسیون باند فرکانس خاصی موسوم به ISM را در محدوده ۲.٤ GHz تا ۲.٤۸۳٥ GHz برای فنّاوری‌های رادیویی استاندارد IEEE 802.11bاختصاص داده است.

اثرات فاصله

فاصله از فرستنده برروی کارایی و گذردهی شبکه‌های بی‌سیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد ۸۰۲.۱۱ با توجه به نرخ ارسال داده تغییر می‌کند و به طور مشخص در پهنای باند ۱۱ Mbps این فاصله ۳۰ تا ٤٥ متر و در پهنای باند ٥.٥ Mbps، 40 تا ٤٥ متر و در پهنای باند ۲ Mbps، 75 تا ۱۰۷ متر

است. لازم به یادآوری است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل استقرار فرستنده و گیرند و شرایط فیزیکی و محیطی تغییر می‌کنند.
در استاندارد ۸۰۲.۱۱bپروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می‌نماید . توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزم‌های تصدیق رایج در سطح لایه انتقال (نظیر آنچه در پروتکل TCP اتفاق می‌افتد) عمل می‌کند. در صورتی که بسته تصدیق ظرف مدت زمان مشخصی از طرف گیرنده به فرستنده نرسد، فرستنده فرض می‌کند که بسته از دست رفته است و مجدداً آن بسته را ارسال می‌کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می‌یابد (Fall Back) تا در نهایت به مقدار ۱ Mpbs برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته‌های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته‌ای را برای آن گیرنده ارسال نمی‌کند. به این ترتیب فاصله نقش مهمی در کارایی (میزان بهره‌وری از شبکه) و گذردهی (تعداد بسته های غیرتکراری ارسال شده در واحد زمان) ایفا می‌کند.

پل بین شبکه‌ای

بر خلاف انتظار بسیاری از کارشناسان شبکه‌های کامپیوتری، پل بین شبکه‌ای یا Bridging در استاندارد ۸۰۲.۱۱bپوشش داده نشده است . در پل بین شبکه‌ای امکان اتصال نقطه به نقطه (و یا يك نقطه به چند نقطه) به منظور برقراری ارتباط يك شبکه محلی با يك یا چند شبکه محلی دیگر فراهم می‌شود. این کاربرد به خصوص در مواردی که بخواهیم بدون صرف هزینه کابل کشی (فیبر نوری یا سیم مسی) شبکه محلی دو ساختمان را به یکدیگر متصل کنیم بسیار جذاب و مورد نیاز می‌باشد. با وجود اینکه استاندارد ۸۰۲.۱۱bاین کاربرد را پوشش نمی‌دهد ولی بسیاری از شرکت‌ها پیاده‌سازی‌های انحصاری از پل بی‌سیم را به صورت گسترش و توسعه استاندارد ۸۰۲.۱۱bارائه کرده‌اند. پل‌های بی‌سیم نیز توسط مقررات FCC کنترل می‌شوند و گذردهی مؤثر یا به عبارت دیگر توان مؤثر ساطع شده همگرا (EIRP) در این تجهیزات نباید از ٤ وات بیشتر باشد. بر اساس مقررات FCC توان سیگنال‌های ساطع شده در شبکه‌های محلی نیز نباید از ۱ وات تجاوز نماید.

پدیده چند مسیری

در این پدیده مسیر و زمان بندی سیگنال در اثر برخورد با موانع و انعکاس تغییر می‌کند. پیاده سازی‌های اولیه از استاندارد ۸۰۲.۱۱bاز تکنیك FHSS در لایه فیزیکی استفاده می‌کردند. از ویژگی‌های قابل توجه این تکنیك مقاومت قابل توجه آن در برابر پدیده چند مسیری است. در این تکنیك از کانال های متعددی (۷۹ کانال) با پهنای باند نسبتاً کوچك استفاده شده و فرستنده و گیرنده به تناوب کانال فرکانسی خود را تغییر می‌دهند. این تغییر کانال هر ٤۰۰ میلی ثانیه بروز می‌کند لذا مشکل چند مسیری به شکل قابل ملاحظه‌ای منتفی می‌شود. زیرا گیرنده، سیگنال اصلی (که سریع‌تر از سایرین رسیده و عاری از تداخل است) را دریافت کرده و کانال فرکانسی خود را عوض می‌کند و سیگنال‌های انعکاسی زمانی به گیرنده می‌رسد که گیرنده کانال فرکانسی قبلی خود را عوض کرده و در نتیجه توسط گیرنده احساس و دریافت نمی‌شوند.

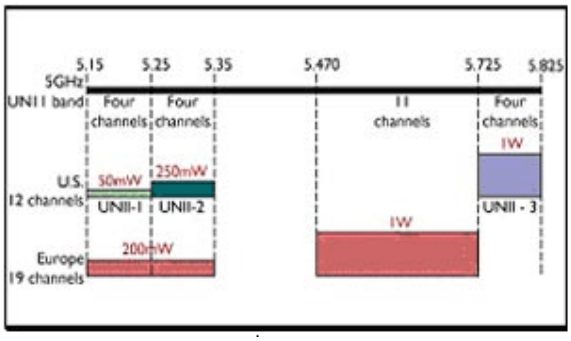
استاندارد 802.11 a

استاندارد ۸۰۲.۱۱a، از باند رادیویی جدیدی برای شبکه‌های محلی بی‌سیم استفاده می‌کند و پهنای باند شبکه‌های بی‌سیم را تا ٥٤ Mbps افزایش می‌دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیك مدولاسیونی موسوم به OFDM است. نرخ‌های ارسال داده در استاندارد IEEE 802.11a عبارتند از:٥٤,٤٨,٣٦,٢٤,١٨,١٢,٩,٦ Mbps که بر اساس استاندارد، پشتیبانی از سرعت های ٦,١٢,٢٤ مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه‌های محلی بی‌سیم، استاندارد IEEE 802.11aرا نسل آینده IEEE 802.11تلقی می‌کنند و حتی برخی از محصولات مانند تراشه‌های Atheros وکارت‌های شبکه PCMCIA/Cardbus محصول Card Access Inc. استاندارد IEEE 802.11a را پیاده‌سازی کرده‌اند. بدون شك این پهنای باند وسیع و نرخ داده سریع محدودیت‌هایی را نیز به همراه دارد. در واقع افزایش پهنای باند در استاندارد IEEE 802.11a باعث شده است که محدوده عملیاتی آن در مقایسه با IEEE 802.11/b کاهش یابد. علاوه بر آن به سبب افزایش سربارهای پردازشی در پروتکل، تداخل، و تصحیح خطاها، پهنای باند واقعی به مراتب کمتر از پهنای باند اسمی این استاندارد است. همچنین در بسیاری از کاربردها امکان سنجی و حتی نصب تجهیزات اضافی نیز مورد نیاز است که به تبع آن موجب افزایش قیمتِ زیرساختار شبکه بی‌سیم می‌شود. زیرا محدوده عملیاتی در این استاندارد کمتر از محدوده عملیاتی در استاندارد

IEEE 802.11bبوده و به همین خاطر به نقاط دسترسی یا ایستگاه پایه بیشتری نیاز خواهیم داشت که افزایش هزینه زیرساختار را به دنبال دارد. این استاندارد از باند فرکانسی خاصی موسوم به UNII استفاده می‌کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می‌شود:

UNII-1 @ 5.2 GHz
UNII-2 @ 5.7 GHz
UNII-3 @ 5.8 GHz

یکی از تصورات غلط در زمینه استانداردهای ۸۰۲.۱۱ این باور است که a۸۰۲.۱۱ قبل از b۸۰۲.۱۱مورد بهره برداری واقع شده است. در حقیقت b۸۰۲.۱۱نسل دوم استانداردهای بی‌سیم (پس از ۸۰۲.۱۱)است و a۸۰۲.۱۱ نسل سوم از این مجموعه استاندارد به شمار می‌رود. استاندارد a۸۰۲.۱۱ برخلاف ادعای بسیاری از فروشندگان تجهیزات بی‌سیم نمی‌تواند جایگزین b۸۰۲.۱۱شود زیرا لایه فیزیکی مورد استفاده در هریك تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هریك متفاوت است.



در شکل بالا این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می‌شود. این سه ناحیه کاری ۱۲ کانال فرکانسی را فراهم می‌کنند. باند UNII-1 برای کاربردهای فضای بسته، باند UNII-2 برای کاربردهای فضای بسته و باز، و باند UNII-3 برای کاربردهای فضای باز و پل بین شبکه‌ای به کار برده می‌شوند. این نواحی فرکانسی در ژاپن نیز قابل استفاده هستند. این استاندارد در حال حاضر در قارهاروپا قابل استفاده نیست. در اروپا HyperLAN2برای شبکه‌های بی‌سیم مورد استفاده قرار می‌گیرد که به طور مشابه از باند فرکانسی a۸۰۲.۱۱استفاده می‌کند. یکی از نکات جالب توجه در استاندارد a۸۰۲.۱۱ تعریف کاربردهای پل سازی شبکه‌ای در کاربردهای داخلی و فضای باز است. در واقع این استاندارد مقررات لازم برای پل سازی و ارتباط بین شبکه‌ای از طریق پل را در کاربردهای داخلی و فضای باز فراهم می‌نماید. در یکی تقسیم بندی کلی می‌توان ویژگی ها و مزایای a۸۰۲.۱۱ را در سه محور زیر خلاصه نمود.

- افزایش در پهنای باند در مقایسه با استاندارد 802.11 b(در استاندارد 802.11 a حداکثر پهنای باند ٥٤ Mbps) می‌باشد.
- استفاده از طیف فرکانسی خلوت (باند فرکانسی ٥ GHz)
استفاده از ۱۲ کانال فرکانسی غیرپوشا (سه محدودهفرکانسی که در هریك ٤ کانال غیرپوشا وجود دارد)

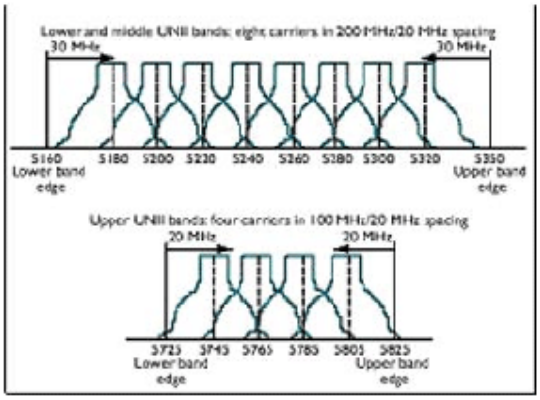
افزایش پهنای باند

استاندارد a۸۰۲.۱۱ در مقایسه با b۸۰۲.۱۱و پهنای باند ۱۱ Mbps حداکر پهنای باند ٥٤ Mbps را فراهم می‌کند. مهمترین عامل افزایش قابل توجه پهنای باند در این استاندارد استفاده از تکنیك پیشرفته مدولاسیون، موسوم به OFDM است. تکنیكOFDM یك تکنولوژی (فنّاوری) تکامل یافته و بالغ در کاربردهای بی‌سیم به شمار می‌رود. این تکنولوژی مقاومت قابل توجهی در برابر تداخل رادیویی داشته و تأثیر کمتری

از پدیده چند مسیری می‌پذیرد. OFDM تحت عناوین مدولاسیون چند حاملی و یا مدولاسیون چندآهنگی گسسته نیز شناخته می‌شود. این تکنیك مدولاسیون علاوه بر شبکه‌های بی‌سیم در تلویزیون‌های دیجیتال (در اروپا، ژاپن، و استرالیا) و نیز به عنوان تکنولوژی پایه در خطوط مخابراتی ADSL مورد استفاده قرار می‌گیرد
تکنیك OFDM از روش QAM و پردازش سیگنال‌های دیجیتال استفاده کرده و سیگنال داده را با فرکانس‌های دقیق و مشخصی تسهیم می‌کند. این فرکانس‌ها به گونه ای انتخاب می‌شوند که خاصیت تعامد را فراهم کنند و به این ترتیب علیرغم همپوشانی فرکانسی هر یك از فرکانس های حامل به تنهایی آشکار می‌شوند و نیازی به باند محافظت برای فاصله گذاری بین فرکانس‌ها نیست. در کنار افزایش پهنای باند در این استاندارد فواصل مورد استفاده نیز کاهش می‌یابند. در واقع باند فرکانسی ٥ GHz تقریباً دوبرابر باند فرکانسی 2.4 GHz) ISM) است که در استاندارد۸۰۲.۱۱bمورد استفاده قرار می‌گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه‌های بی‌سیم متفاوت و متغیر است ولی به عنوان یك قاعده سرراست می‌توان فواصل در این استاندارد را یك سوم محدوده فرکانسی ۲.٤ GHz (۸۰۲.۱۱b) در نظر گرفت. در حال حاضر محدوده عملیاتی (فاصله از فرستنده) در محصولات مبتنی بر ۸۰۲.۱۱a و پهنای باند ٥٤ Mbps در حدود ۱۰ تا ۱٥ متر است. این محدوده در پهنای باند٦ Mbps در حدود ٦۱ تا ۸٤ متر افزایش می‌یابد.

طیف فرکانسی تمیزتر

طیف فرکانسی UNII در مقایسه با طیف ISM خلوت‌تر است و کاربرد دیگری برای طیف UNII به جز شبکه‌های بی‌سیم تعریف و تخصیص داده نشده است. در حالی که در طیف فرکانسی ISM تجهیزات بی‌سیم متعددی نظیر تجهیزات پزشکی، اجاق های مایکروویو، تلفن‌های بی‌سیم و نظایر آن وجود دارند. این تجهیزات بی‌سیم در باند ۲.٤ GHz یا طیف ISM هیچگونه تداخلی با تجهیزات باند UNII (تجهیزات بی‌سیم ۸۰۲.۱۱a) ندارند. شکل٤-۲ فرکانس مرکزی و فاصله‌های فرکانسی در باند UNII را نشان می‌دهد.



کانال‌های غیرپوشا

باند فرکانسی UNII ، دوازده کانال منفرد و غیر پوشای فرکانسی را برای شبکه سازی فراهم می‌کند. از این ۱۲ کانال ۸ کانال مشخص (UNII-1 , 2) در شبکه‌های محلی بی‌سیم مورد استفاده قرار می‌گیرند. این ویژگی غیرپوشایی گسترش و پیاده سازی شبکه‌های بی‌سیم را ساده‌تر از باند ISM می‌کند که در آن تنها ۳ کانال غیر پوشا از مجموع ۱۱ کانال وجود دارد.

همکاری Wi-Fi

ائتلاف "همکاری اِترنت بی‌سیم" یا http://www.wi-fi.org(WECA) کنسرسیومی از شرکت‌های Cisco, 3Com, Enterasys, Lucent و سایر شرکت‌های شبکه‌سازی است. اعضاء WECA از طریق همکاری مشترك تلاش دارند تا قابلیت همکاری تجهیزات بی‌سیم با یکدیگر را تضمین نمایند. برنامه گواهینامه Wi-Fi که توسط این گروه مطرح شده است نقش کلیدی در گسترش و پذیرش استاندارد IEEE 802.11 ایفا می‌کند. در حال حاضر این ائتلاف برای بیش از ۱۰۰ محصول گواهی سازگاری Wi-Fi صادر کرده است و تعداد این محصولات رو به افزایش است. با گسترش فزآینده محصولات IEEE 802.11a، WECAبرنامه دیگری برای صدور گواهینامه برای این نوع محصولات نیز ارائه می‌کند.

استاندارد IEEE 802.11g

این استاندارد مشابه IEEE 802.11bاز باند فرکانسی ٢.٤ GHz (یا طیف ISM) استفاده می‌کند و از تکنیك OFDM به عنوان روش مدولاسیون بهره می‌برد. البته PBCC نیز یکی از روش‌های جایگزین و تحت بررسی برای انتخاب تکنیك مدولاسیون در این استاندارد به شمار می‌رود. g٨٠٢.١١ از نظر فرکانسی، تعداد کانال های غیرپوشا، و توان مشابه b٨٠٢.١١است. محدوده‌های عملیاتی نیز کم و بیش مشابه هستند با این تفاوت که حساسیت OFDM به نویز تاحدودی این محدوده عملیاتی را کاهش می‌دهد. پهنای باند ٥٤ Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می‌رود. یکی دیگر از مزایای جالب توجه g٨٠٢.١١ سازگاری با b٨٠٢.١١است. در نتیجه ارتقاء از تجهیزات b٨٠٢.١١به استاندارد جدید g٨٠٢.١١ امری سرراست خواهد بود. جدول زیر سه استاندارد شبکه‌های بی‌سیم را با یکدیگر مقایسه می کند.

	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
کاربردهای احتمالی	- جایگزین شبکه‌های سیمی - فراهم آوردن تحرک و سیار بودن کاربران - شبکه‌سازی در محل هایی که استفاده از سیم میسر نیست - پل‌سازی بین شبکه های محلی در فواصل دور (۴۰ کیلومتر)	- جایگزین شبکه‌های سیمی - فراهم کننده پهنای باند زیاد در کاربردهای (صدا، تصویر، CAD و نظایر آن) - شبکه سازی در محل هایی که استفاده از سیم میسر نیست.	- ارتقاء شبکه‌های ۸۰۲,۱۱b و رقیبی برای ۸۰۲,۱۱a - کارایی مشابه با ۸۰۲,۱۱a در فواصل طولانی
مزایا	- استاندارد رایج و تکامل یافته - قیمت منطقی -گذردهی قابل قبول در فاصله زیاد (نرخ ارسال داده)	- گذردهی (نرخ ارسال داده) بالا در فواصل کم - افزایش تعداد کانال‌های فرکانسی غیرپوشا (٤ برابر بیشتر از ۸۰۲,۱۱b) - تداخل فرکانسی کمتر	- سازگاری با ۸۰۲,۱۱b - محدوده عملیاتی زیاد (نظیر ۸۰۲,۱۱b) - گذردهی (نرخ ارسال داده) بیشتر
معایب	- دارابودن کمترین گذردهی (نرخ ارسال داده) در مقایسه با سایر فناوری‌های بی‌سیم (۱۱ Mbps) - استفاده از تنها ۳ کانال فرکانسی غیر پوشا	- فنّاوری نسبتاً گران - ناسازگاری با ۸۰۲,۱۱b - محدوده عملیاتی کوچك - محدودیت‌های FCC برروی آنتن‌ها (حداکثر توان مجاز) در هر باند فرکانسی	- عدم وجود محصول فراگیر (احتمالاً تا اواسط سال۲۰۰۲ میلادی) - محدودیت‌ها کانال فرکانسی نظیر 3) ۸۰۲,۱۱b کانال غیرپوشا)

فصل پنجم

وضعیت های کاربردی wireless

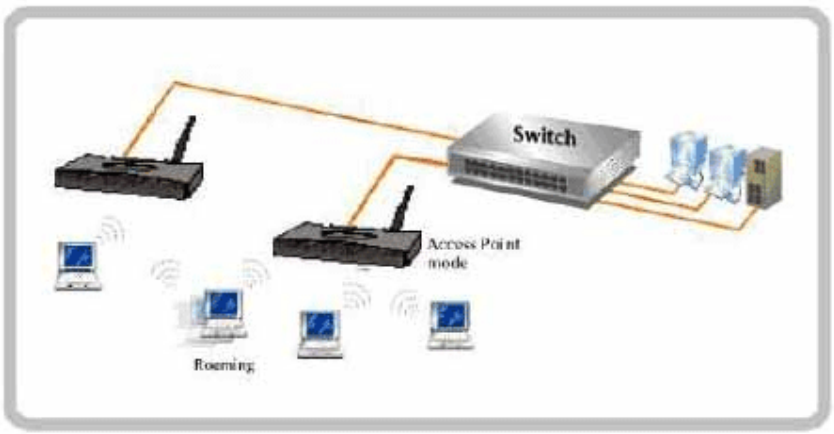
در این بخش وضعیت های کاربردی مختلف را برای شبکه های بی سیم بررسی میکنیم .این وضعیت هارامیتوان بطور کلی به ٥ دسته تقسیم نمود .

١- access point mode
٢- wireless ap client
٣- mode wireless bridge
٤- wireless multiple bridge mode
٥- repeater mode

access point mode

در این حالت همه نود های انتهایی (end nodes) به یک نقطه دسترسی (access point) توسط یک ارتباط بی سیم سالم متصل میگردند.مطابق شکل تمامی نودها متصله به access point باید دارای دو خصوصیت یکسان باشند:

- پروتکل wep یکسان
- ssid یکسان

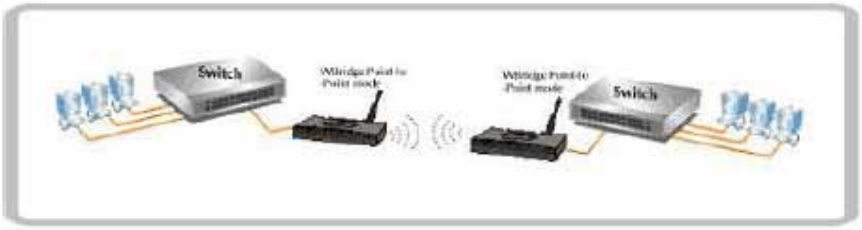


wireless ap client mode

در این حالت wireless ما به عنوان یک نود انتهایی نقش client را در شبکه بی سیم ما ایفا مینماید.در این حالت مهمترین مسئله سازگاری client با access point است .

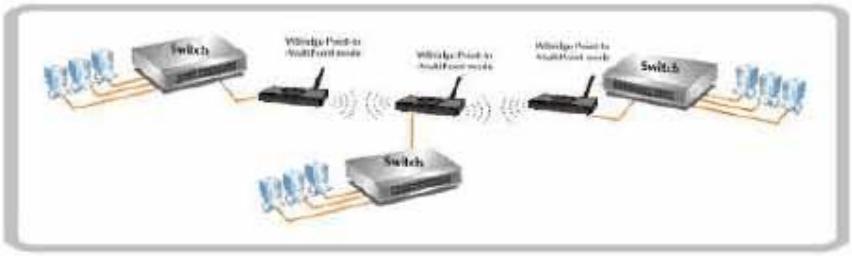
wireless bridge mode

عمده ترین کاربرد وضعیت bridge اتصال دو شبکه lan توسط یک ارتباط بی سیم میباشد.با رعایت بعد مسافت تا حد زیادی از مشکلات کابل کشی کاسته خواهد شد و البته توسط mac address ها میتوان یک ارتباط مطمئن تر را ایجاد نمود.



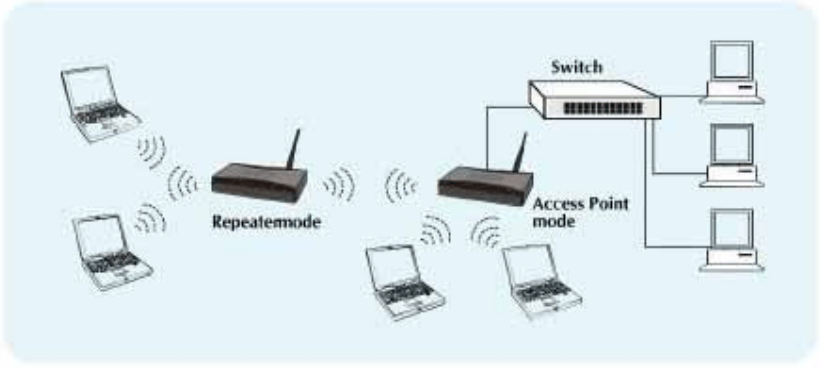
multiple bridge mode

بهترین وضعیت برای اتصال چند شبکه lan استفاده از حالت bridge multiple مطابق شکل میباشد.در این حالت از access pint های متوالی جهت پیکربندی و طراحی شبکه استفاده میشود.



Repeater mode

با کمک وضعیت repeater میتوان فاصله بین دو گیرنده - فرستنده را تا حدود دو برابر افزایش د اد و البته سرعت ارتباط حدودا نصف خواهد شد زیرا دو ارتباط مختلف در دو سوی repeater خواهیم داشت .



مراجع

WEB:

http://www.ieee802.org/11

http://www.intelligraphics.com

http://www.wifi.org

BOOKS:

Cisco press CCNA ICND1