# شبکه های بی سیم

## فهرست مطالب

Authentication با رمزنگاری RC4

---

سرویس Privacy یا confidentiality

Integrity

---

ویژگیهای سیگنالهای طیف گسترده

سیگنالهای طیف گسترده با جهش فرکانسی

سیگنالهای طیف گسترده با توالی مستقیم

استفاده مجدد از فرکانس

---

مقایسه مدلهای 802.11

اثرات فاصله

پدیده چند مسیری

استاندارد 802.11a

افزایش پهنای باند

طیف فرکانسی تمیزتر

کانالهای غیرپوشا

استاندارد بعدی IEEE 802.11g

---

معرفی شبکه بلوتوس

مؤلفه های امنیتی در بلوتوس

خطرات امنیتی

مقابله با خطرات

## استاندارد شبکه های محلی بی سیم

در ماه ژوئن سال ۱۹۹۷ انجمن مهندسان برق و الکترونیک (IEEE) استاندارد IEEE 802.11-1997 را به عنوان اولین استانداردِ ی محلی بی سیم 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 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 ۲ Mbps 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 Mbps نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی ۲،٤ 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 802.11 به زیر گروه های متعددی تقسیم میشود. برخی از مهمترین زیر گروه ها به قرار زیر است:

کمیته 802.11e کمیتهای است که سعی دارد قابلیت QoS اِترنت را در محیط شبکه های بی سیم ارائه کند. توجه داشته باشید که فعالیتهای این گروه تمام گونه های 802.11 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 بی سیم بیاورد. کمیته 802.11g کمیتهای است که با عنوان 802.11 توسعه یافته نیز شناخته میشود. این کمیته در نظر دارد نرخ ارسال داده ها 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 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 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 802.11h مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصرفی و نیز توان امواج ارسالی توسط فرستنده های مبتنی بر 802.11 است.

فعالیت دو کمیته 802.11i و 802.11x در ابتدا برروی سیستمهای مبتنی بر 802.11b 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 ٤۰ 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 شبکه های محلی بی سیم است. این استاندارد لایه های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بی سیم را دربردارد.

## شبکه های بی سیم و انواعWWAN , WLAN , WPAN

تکنولوژی شبکه های بی سیم، با استفاده از انتقال داده ها توسط اموج رادیویی، در سادهترین صورت، به تجهیزات سخت افزاری امکان میدهد تا بدوناستفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه های بی سیم بازهی وسیعی از کاربردها، از ساختارهای پیچیدهیی چون شبکه های بی سیم سلولی -که اغلب برای تلفنهای همراه استفاده میشود- و شبکه های محلی بی سیم (WLAN – Wireless LAN) گرفته تا انوع سادهیی چون هدفونهای بی سیم، 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 شبکه ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به اینگونه و همچنین امکان ایجاد تغییر در ساختار مجازی آنهاست. از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم میگردند : WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه هایی با پوشش بی سیم بالاست. نمونهیی 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 میکند. کاربرد شبکه های WPAN یا Wireless Personal Area Network برای موارد خانگی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار میگیرند.شبکه های WPAN از سوی دیگر در دسته ی شبکه های Ad Hoc نیز قرار میگیرند. در شبکه های Ad hoc، یک سخت افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه میشود. 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 قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده ها با دیگر تجهیزات متصل به شبکه را مییابند. تفاوت میان شبکه های Ad hoc با شبکه های محلی بی سیم (WLAN) در ساختار مجازی آنهاست. به عبارت دیگر، ساختار مجازی شبکه های محلی بی سیم بر پایهی طرحی ایستاست درحالیکه شبکه های Ad hoc از هر نظر پویا هستند. طبیعی ست که در کنار مزایایی که این پویایی برای استفاده کنندهگان فراهم میکند، حفظ امنیت چنین شبکه هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حلهای موجود برای افزایش امنیت در این ، 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 گیرنده های کمتوان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل توجه ای محسوب میگردد، همین کمی توان سخت افزار مربوطه، موجب وجود منطقه ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب میگردد. به عبارت دیگر این مزیت به همراه استفاده از کدهای رمز نه چندان پیچیده، تنها حربه های امنیتی این دسته از شبکه ها به حساب میآیند.

## منشأ ضعف امنیتی در شبکه های بی سیم و خطرات معمول

خطر معمول در کلیه ی شبکه های بی سیم 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 شبکه ها، خود را

به عنوان عضوی از این شبکه ها جا زده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهندهگان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیرواقعی و گمراه کننده، سوءاستفاده از پهنایباند مؤثر شبکه و دیگر فعالیتهای مخرب وجود دارد.

در مجموع، در تمامی دسته های شبکه های بی سیم، از دید امنیتی حقایقی مشترک صادق است :

- تمامی ضعفهای امنیتی موجود در شبکه های سیمی، در مورد شبکه های بی سیم نیز صدق میکند. در واقع نه تنها هیچ جنبه ای چه از لحاظ طراحی و چه از لحاظ ساختاری، خاصی بی سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه ای را نیز موجب است.

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

- اطلاعات حیاتی ای که یا رمز نشده اند و یا با روشی با امنیت پایین رمز شده اند، و میان دو گره در ی بی سیم در حال انتقال میباشند، میتوانند توسط نفوذگران سرقت شده یا تغییر یابند.

- حمله های DoS به تجهیزات و سیستمهای بی سیم بسیار متداول است.

- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در ی بی سیم، میتوانند به شبکه ی 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 اجازه ی استفاده از شبکه ی بی سیم 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 شبکه ی بی سیم در یک سازمان و شبکه ی سیمی آن (که در اغلب موارد شبکه ی اصلی و حساستری محسوب میگردد) استفاده کرده و با نفوذ به شبکه ی بی سیم عملاً راهی برای دستیابی به منابع شبکه ی سیمی نیز بیابد.

- در سطحی دیگر، با نفوذ به عناصر کنترل کنندهی یک شبکه ی بی سیم، امکان ایجاد اختلال در عملکرد شبکه نیز وجود دارد.

## مشخصات و خصوصیاتWLAN

تکنولوژی و صنعت WLAN به اوایل دهه ی 80 میلادی باز میگردد. مانند هر تکنولوژی دیگری، پیشرفت ی محلی بی سیم به کندی صورت میپذیرفت. با ارایه ی استاندارد IEEE 802.11b، که پهنای باند نسبتاً بالایی را برای ی محلی امکانپذیر می ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکلها و استانداردهای خانواده ی 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 شبکه ی محلی بی سیم تجاری توسط Motorola پیاده سازی شد. این شبکه، به عنوان یک نمونه از این ، هزینه ی بالا و پهنای باندی پایین را تحمیل میکرد که ابداً مقرون به صرفه نبود. از همان زمان به بعد، در اوایل دههی 90 میلادی، پروژهی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به 9 سال کار، در سال 1999 استانداردهای 802.11a و 802.11b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایهی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل GHz٥، پهنای باندی تا Mbps٥٤ را فراهم میکند. در حالیکه نوع b با استفاده از فرکانس حامل GHz٢,٤، تا Mbps١١ 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 802.11b است.

استاندارد دیگری نیز بهتازهگی توسط IEEE معرفی شده است که به 802.11g شناخته میشود. این استاندارد بر اساس فرکانس حامل GHz٢,٤ 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 سازگاریآن با استاندارد 802.11b ، استفاده از آن در ی بی سیم آرام آرام در حال گسترش است.

**- معماری شبکه های محلی بی سیم INFRASTRUCTURE , AD HOC**

استاندارد 802.11b به 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 ی Ad hoc به کار میرود- و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).

## توپولوژی های 802.11

در یک تقسیم بندی کلی میتوان دو همبندی (توپولوژی) را برای ی محلی بی سیم در نظر گرفت. سادهترین همبندی، فیالبداهه (Ad Hoc) و براساس فرهنگ واژگان استاندارد 802.11 ، 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 نمیکنند. واضح است که در این همبندی به سبب محدودیتهای فاصله هر ایستگاهی ضرورتاً نمیتواند 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.

## همبندی فی البداهه یا IBSS

همبندی دیگر زیرساختار است. در این همبندی عنصر خاصی موسوم به نقطه دسترسی وجود دارد. نقطه دسترسی ایستگاه های موجود در یک مجموعه سرویس را به سیستم توزیع متصل میکند. در این هم بندی تمام ایستگاه ها با نقطه دسترسی تماس میگیرند و اتصال مستقیم بین ایستگاه ها وجود ندارد در واقع نقطه دسترسی وظیفه دارد فریمها (قابهای داده) را بین ایستگاه ها توزیع و پخش کند.

## همبندی زیرساختار در دوگونه BSS و ESS

در این هم بندی 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 ایستگاه ها ارسال نماید. از سوی دیگر میتواند بسته ها را در اختیار ایستگاه های متصل به شبکه سیمی نیز قراردهد. در استاندارد

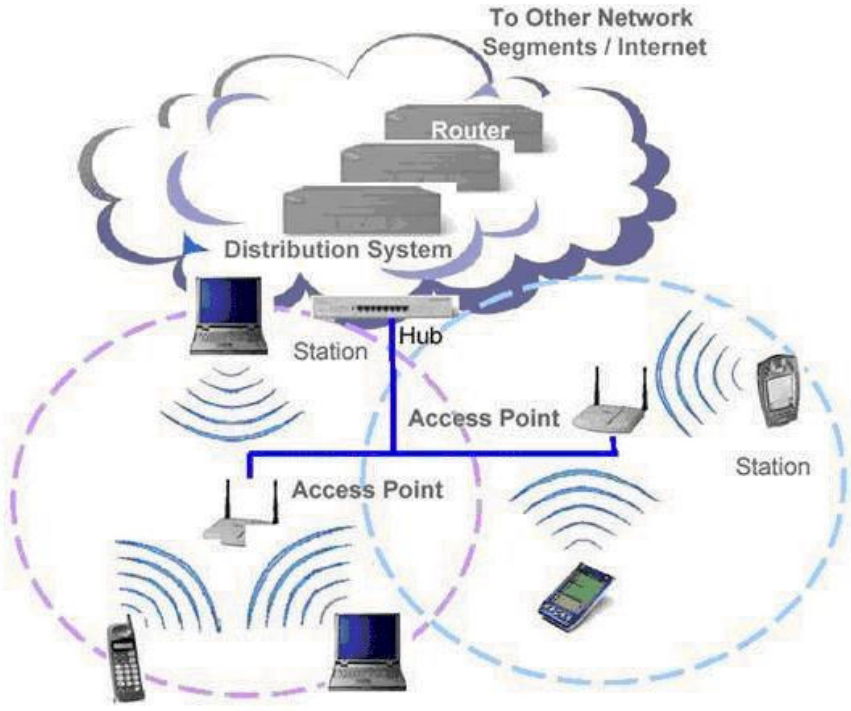
802.11 توصیف ویژهای برای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین میکند که سیستم توزیع میبایست ارائه نماید. بنابراین سیستم توزیع میتواند یک شبکه ۸۰۲,۳ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم میکند.

استاندارد 802.11 با استفاده از همبندی خاصی محدوده عملیاتی شبکه را گسترش میدهد. این همبندی به شکل مجموعه سرویس گسترش یافته (ESS) بر پا میشود. در این روش یک مجموعه گسترده و متشکل از چندین BSS یا مجموعه سرویس پایه از طریق نقاط دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیک داده بین مجموعه های سرویس پایه مبادله شده و انتقال پیامها شکل میگیرد. در این همبندی ایستگاه ها میتوانند در محدوده عملیاتی بزرگتری گردش نمایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم میشود. در واقع سیستم توزیع ستون فقرات ی محلی بی سیم است و میتواند با استفاده از فنّاوری بی سیم یا ی سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان یک لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش میباشد. نکته قابل توجه در این همبندی آن است که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه های سیّار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت یک شبکه منفرد در سطح لایه MAC تلقی میکنند. به این ترتیب پروتکلهای رایج ی کامپیوتری کوچکترین تأثیری از سیّار بودن ایستگاه ها و رسانه بی سیم نمیپذیرند. جدول زیر همبندیهای رایج در ی بی سیم مبتنی بر 802.11 را به اختصار جمع بندی میکند.

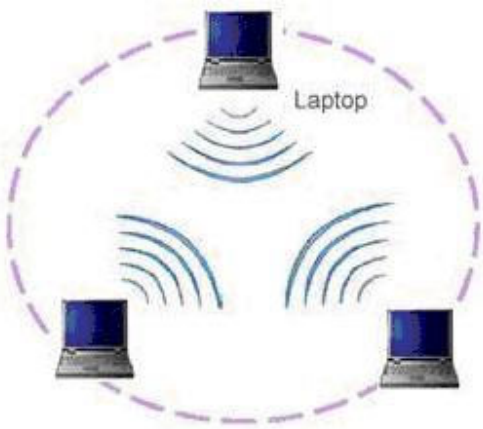
| 802.11 Topologies | | |
|---|---|---|
| Independent Basic Service Set (IBSS) ("Ad Hoc" or "Peer to Peer") | **Infrastructure** | |
| | Basic Service Set (BSS) | Extended Service Set (ESS) |

معماری معمول در شبکه های محلی بی سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص میشود و با روشهایی میتوان یک سخت افزار مجهز به امکان ارتباط بر اساس استاندارد 802.11b را میان سلولهای مختلف حرکت داد. گسترهیی که یک AP پوشش میدهد را BSS-Basic Service Set مینامند. مجموعهی تمامی سلولهای یک ساختار کلیشبکه، که ترکیبی از BSSهای شبکه است، را ESS-Extended Service Set مینامند. با استفاده از ESS میتوان گسترهی وسیعتری را تحت پوشش شبکه ی محلی بی سیم درآورد.

در سمت هریک از سخت افزارها که معمولاً مخدوم هستند، کارت شبکه یی مجهز به یک مودم بی سیم قرار دارد که با AP ارتباط را برقرار میکند. AP علاوه بر ارتباط با چند کارت شبکه ی بی سیم، به بستر پرسرعتتر شبکه ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدومهای مجهز به کارت شبکه ی بی سیم و شبکه ی اصلی برقرار میشود. شکل زیر نمایی از این ساختار را نشان میدهد :



همانگونه که گفته شد، اغلب ی محلی بی سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز موسوم است، پیادهسازی میشوند. با این وجود نوع دیگری از ی محلی بی سیم نیز وجود دارند که از همان منطق نقطهبهنقطه استفاده میکنند. در این که عموماً Ad hoc نامیده میشوند یک نقطهی مرکزیبرای دسترسی وجود ندارد و سخت افزارهای همراه مانند کامپیوترهای کیفی و جیبی یا گوشیهای موبایل با ورود به محدودهی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل میگردند. این به بستر شبکه ی سیمی متصل نیستند و به همین منظور ( IBSS Independent Basic Service Set) نیز خواند میشوند. شکل زیر شمایی ساده از یک شبکه Ad hoc را نشان میدهد :




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

به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر استانداردها، لایه دسترسی به رسانه (MAC) در استاندارد 802.11 میبایست از دید لایه های بالاتر مشابه یک شبکه محلی مبتنی بر

استاندارد 802 عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیّاربودن ایستگاه های کاری را به گونهای شفاف پوشش دهد که از دید لایه های بالاتر استاندارد این سیّاربودن احساس نشود. این نکته سبب میشود که لایهMAC در این استاندارد وظایفی را بر عهده بگیرد که معمولاً توسط لایه های بالاتر شبکه انجام میشوند. در واقع این استاندارد لایه های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه میکند و به طور مشخص لایه فیزیکی جدید از فرکانسهای رادیویی به عنوان رسانه انتقال بهره میبرد.

## جایگاه 802.11 در مقایسه با سایر پروتکلها

### 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 داده ها فراهم میکند. دوم اینکه با استفاده از روشهای تسهیم فریمهای داده را ارسال میکند و در نهایت وضعیت رسانه (کانال رادیویی) را در اختیار لایه بالاتر (MAC) قرار میدهد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر میباشند:

- استفاده از تکنیک رادیویی DSSS
- استفاده از تکنیک رادیویی FHSS
- استفاده از امواج رادیویی 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 PPM-١٦ و PPM-٤مبادله میشوند.

برای کسب اطلاعات بیشتر در خصوص گروه های کاری IEEE 802.11 میتوانید به نشانی http://www.ieee802.org/11 مراجعه کنید. علاوه بر استاندارد IEEE 802.11-1999 دو الحاقیه IEEE 802.11a و IEEE 802.11b تغییرات و بهبودهای قابل توجهی را به استاندارد اولیه اضافه کرده است.

## عناصر فعال ی محلی بی سیم

در شبکه ی محلی بی سیم معمولاً دو نوع عنصر فعال وجود دارد :

## ایستگاه

ایستگاه یا مخدوم بی سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه ی بی سیم به شبکه ی 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 پایانه های رایانه ای برای طراح و مجری دردسرساز است، برای این پایانه ها که معمولاً در داخل کیوسکهایی به همین منظور تعبیه میشود، از امکان اتصال بی سیم به شبکه ی محلی استفاده میکنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه ی بی سیم نیست.

کارتهای شبکه ی بی سیم عموماً برای استفاده در چاکهای PCMCIA است. در صورت نیاز به استفاده از این کارتها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارتها را بر روی چاکهای گسترش PCI نصب میکنند.

## نقطه ی دسترسی - access point

نقاط دسترسی در ی بی سیم، همانگونه که در قسمتهای پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در ی بی سیم 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، مخدومها و ایستگاه های بی سیم به شبکه ی 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 ایستگاه های 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 یک 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 چک میکند و سپس یک 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 شبکه ی بی سیم 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 یک شبکه بی سیم، بر خلاف ی سیمی، نمیتوان فرض کرد که تمام ایستگاه های سیّار امواج یکدیگر را دریافت میکنند. در واقع در محیط بی سیم حالاتی قابل تصور است که به آنها نقاط پنهان میگوییم. در شکل زیر ایستگاه های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.

## روزنه های پنهان

برای غلبه بر این مشکل، استاندارد 802.11 از تکنیکی موسوم به اجتناب از تصادم و مکانیزم تصدیق استفاده میکند. همچنین با توجه به احتمال بروز روزنه های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به شنود مجازیرسانه یا VCS استفاده میشود. در این روش ایستگاه فرستنده ابتدا یک 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 ایستگاه هایی که فریمهای کنترلی RTS/CTS را دریافت میکنند وضعیت کنترل رسانه خود موسوم به شاخصNAV را تنظیم میکنند. در صورتی که سایر ایستگاه ها 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 روزنه های پنهان حل شده و تصادمها نیز به حداقل مقدار میرسند.

## زمانبندی RTS/CTS

## برد و سطح پوشش

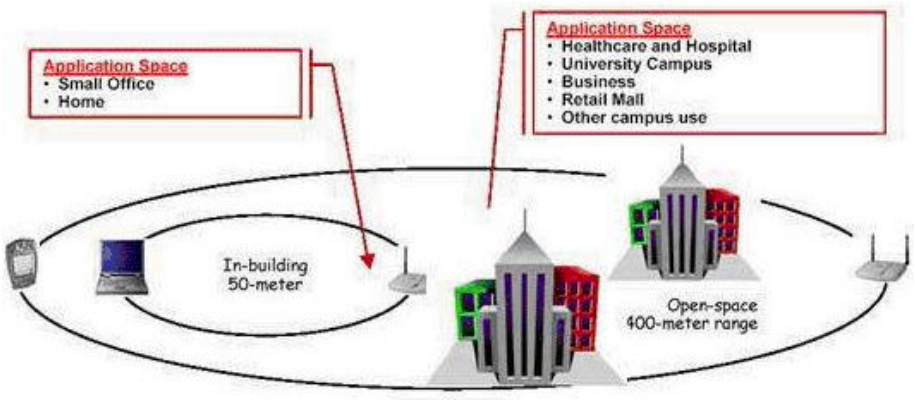
شعاع پوشش شبکه ی بی سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بستگی دارد که برخی از آنها به شرح زیر هستند :

- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه ی بی سیم
- قدرت امواج
- نوع و مدل آنتن

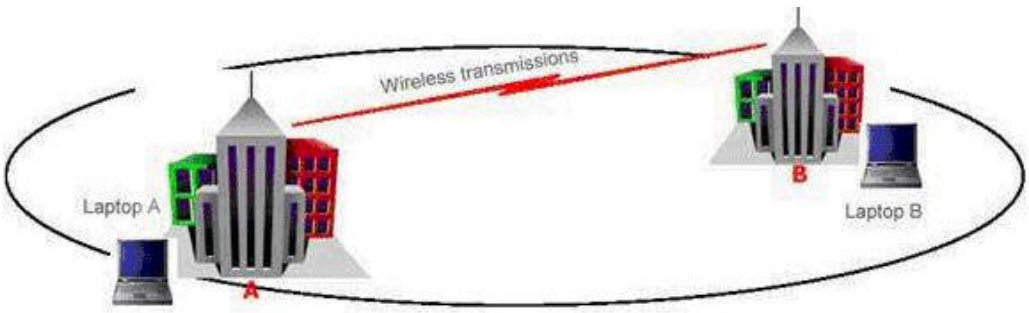
شعاع پوشش از نظر تئوری بین 29متر (برای فضاهای بستهی داخلی) و 485متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با اینوجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده ها و فرستنده های نسبتاً قدرتمندی که مورد استفاده قرار میگیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجود دارد که نمونه های عملی آن فراوانند.

با این وجود شعاع کلییی که برای استفاده از این پروتکل (802.11b) ذکر میشود چیزی میان 50 تا 100متر است. این شعاع عملکرد مقداریست که برای محلهای بسته و ساختمانهای چند طبقه نیز معتبر بوده و میتواند مورد استناد قرار گیرد.

شکل زیر مقایسهای میان بردهای نمونه در کاربردهای مختلف شبکه های بی سیم مبتنی بر پروتکل 802.11b را نشان میدهد :




یکی از عملکردهای نقاط دسترسی به عنوان سوییچهای بی سیم، عمل اتصال میان حوزه های بی سیم است. به عبارت دیگر با استفاده از چند سوییچ بی سیم میتوان عملکردی مشابه Bridge برای ی بی سیم را به دست آورد.اتصال میان نقاط دسترسی میتواند به صورت نقطه به نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه ای به چند نقطه یا بالعکس برای ایجاد اتصال میان زیری مختلف به یکدیگر به صورت همزمان صورت گیرد.نقاط دسترسیی که به عنوان پل ارتباطی میان ی محلی با یکدیگر استفاده میشوند از قدرت بالاتری برای ارسال داده استفاده میکنند و این به معنای شعاع پوشش بالاتر است. این سخت افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمانهایی بهکار میروند که فاصله ی آنها از یکدیگر بین 1 تا 5 کیلومتر است. البته باید توجه داشت که این فاصله، فاصله ی متوسط بر اساس پروتکل 802.11bاست. برای پروتکلهای دیگری چون 802.11a میتوان فواصل بیشتری را نیز به دست آورد. از دیگر



استفاده های نقاط دسترسی با برد بالا میتوان به امکان توسعه ی شعاع پوشش شبکه های بی سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه ی بی سیم، میتوان از چند نقطهی دسترسی بی سیم به صورت 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 همبندیهای 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 بی سیم
- پیوستن مجدد
- توزیع
- مجتمع سازی

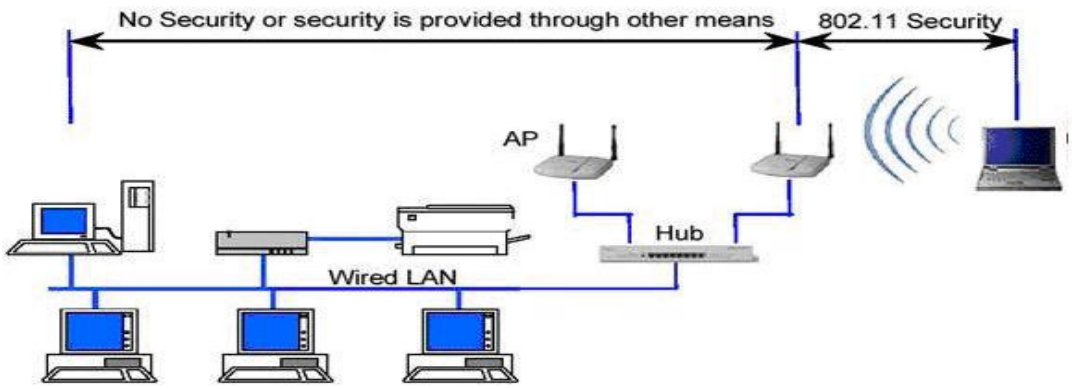
سرویس اول یک ارتباط منطقی میان ایستگاه سیّار و نقطه دسترسی فراهم میکند. هر ایستگاه کاری قبل از ارسال داده میبایست با یک نقطه دسترسی برروی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان میدهد که فریمهای ارسال شده به سمت ایستگاه سیّار را به درستی در اختیارش قرار دهد. خروج از شبکه بی سیم هنگامی 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 بی سیم" 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 تحرک و سیّار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک 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 بی سیم را به سایر ی محلی و یا یک یا چند شبکه محلی بی سیم دیگر متصل میکند. سرویس مجتمع سازی فریمهای 802.11 را به فریمهایی ترجمه میکند که بتوانند در سایر (به عنوان مثال ۸۰۲,۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریمهای سایر نیز به فریمهای 802.11 ترجمه شده و از طریق امواج در اختیار ایستگاه های کاری سیّار قرار میگیرند.

### امنیت و پروتکلWEP

از این قسمت بررسی روشها و استانداردهای امنسازی ی محلی بی سیم 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 802.11 سرویسهای مجزا و مشخصی را برای تأمین یک محیط امن بی سیم در اختیار قرار میدهد. این سرویسها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین میگردند و وظیفه ی آنها امنسازی ارتباط میان مخدومها و نقاط دسترسی بی سیم است. درک لایه

ای که این پروتکل به امنسازی آن میپردازد اهمیت ویژه ای دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایهی ارتباطی بی سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد ی محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.




محدوده‌ی عملکرد استانداردهای امنیتی ۸۰۲,۱۱ (خصوصاً WEP)

## قابلیتها و ابعاد امنیتی استاندارد 802.11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در ی بی سیم بر اساس استاندارد 802.11 فراهم میکند WEP است. این پروتکل با وجود قابلیتهایی که دارد، نوع استفاده از آن همواره امکان نفوذ به ی بی سیم را به نحوی، ولو سخت و پیچیده، فراهم میکند. نکته یی که باید به خاطر داشت اینست که اغلب حملات موفق صورت گرفته در مورد ی محلی بی سیم، 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 فی نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی ی بی سیم انجام میگیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه های ارتباطی دیگری که بر روی مخدومها و سخت افزارهای بی سیم، خصوصاً مخدومهای بی سیم، وجود دارد، به شبکه ی بی سیم نفوذ میکنند که این مقوله نشان دهندهی اشتراکی هرچند جزءیی میان امنیت در ی سیمی و بی سیم ایست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای ی محلی بی سیم تعریف میگردد :

- Authentication
- Confidentiality
- Integrity

## Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی سیم است. این عمل که در واقع کنترل دسترسی به شبکهی بی سیم است. این مکانیزم سعی دارد که امکان اتصال مخدومهایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

## Confidentiality

محرمانگی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکهی محلی بی سیم 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 مخدوم‌های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم وبیش وجود دارد.

## خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه های کاری پیادهسازی می‌شوند. در حقیقت تمام ایستگاه های کاری موجود در یک شبکه محلی مبتنی بر 802.11 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 شبکه ی سیمی، در شبکه ی بی‌سیم قابل اعمال نیست استاندارد 802.11 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 یک تقسیم بندی کلی 802.11 دو گونه خدمت هویت سنجی را تعریف می‌کند:

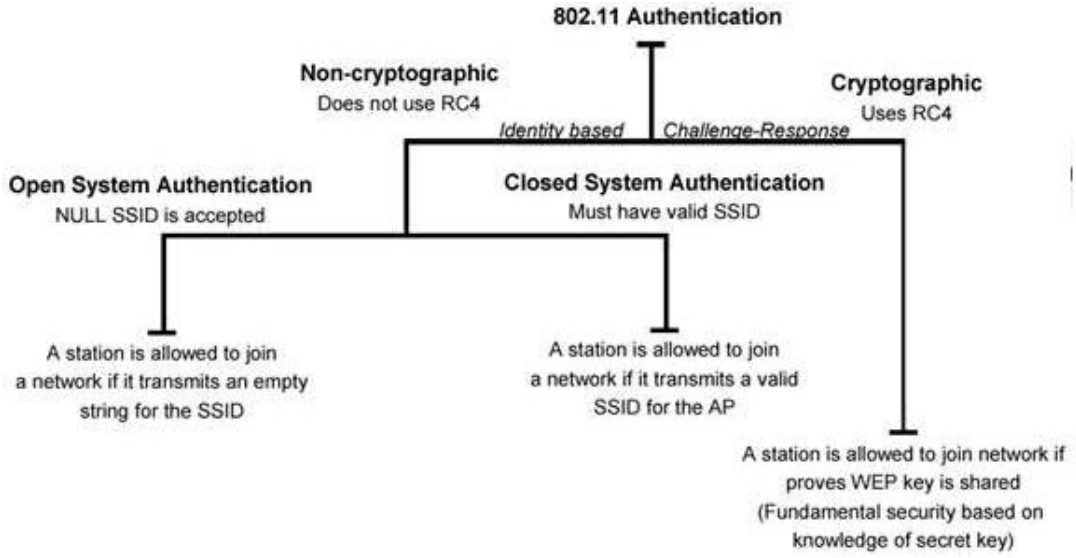
- Authentication Open System
- Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک 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 یک کانال مستقل و امن، یک کلید مشترک سرّی دریافت کرده است. ایستگاه های کاری با استفاده از این کلید مشترک و با بهرمگیری 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 خدمت، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌گردد.در یک شبکه بی‌سیم، تمام ایستگاه های کاری و سایر تجهیزات قادر هستند ترافیک داده‌ای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد. به همین دلیل در استاندارد 802.11 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 ی سیمی نماید.

## Authentication

استاندارد 802.11 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 شبکه ها نشان می‌دهد :




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

## Authentication بدون رمزنگاری

### Authentication بدون رمزنگاری(Open System Authentication)

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدوم متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه‌ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) 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 مخدوم‌هایی 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.

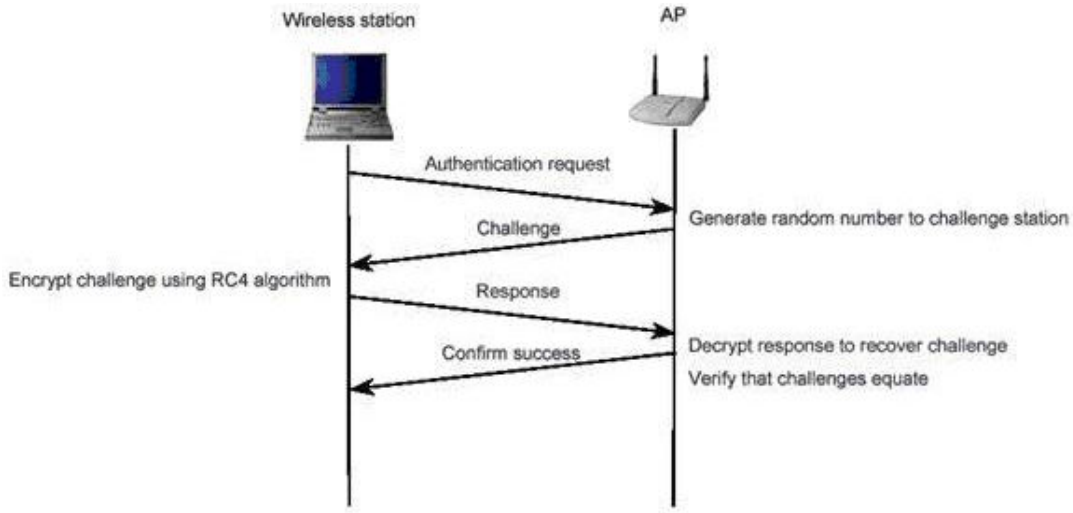
در روش دوم از این نوع، بازهم یک SSID به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که SSIDی ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌ای 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 آن جایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه هایی که بر اساس این روش‌ها عمل میکنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه ی 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 شبکه های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد!

## Authentication با 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 مخدوم 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 آن را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلید ی 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 مخدوم 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 مخدوم اطمینان حاصل میکند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی که با آن در حال تبادل داده های 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 می گیرد و به‌گونه‌ای هریک از دو طرف را گمراه میکند.

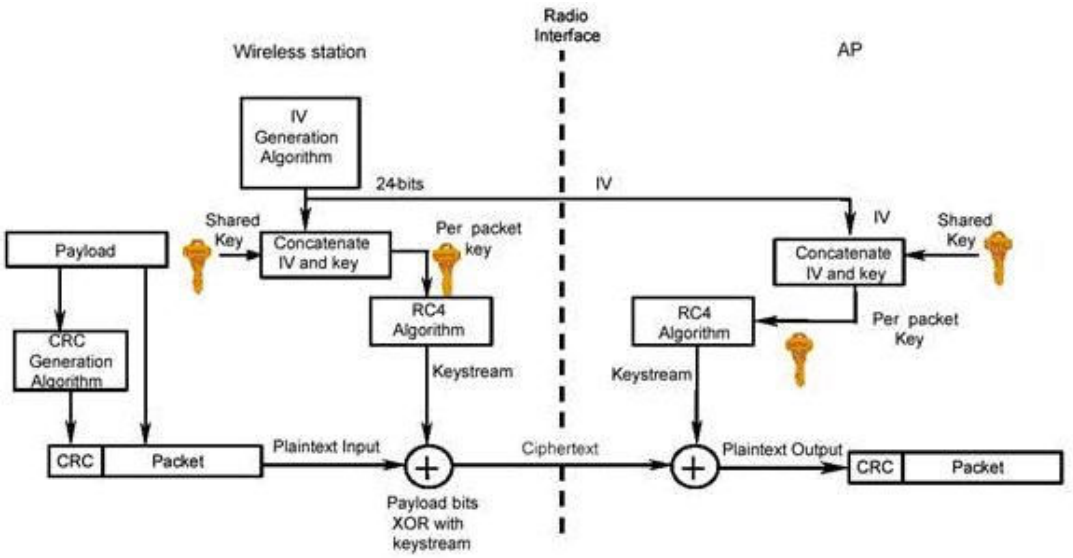
## سرویس Privacy یا confidentiality

این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌ای که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلید های 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 داده های تمامی لایه های بالای اتصال بی‌سیم نیز توسط این روش رمز می‌گردند، از IP گرفته تا لایه های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی‌ترین بخش از اعمال سیاست‌های امنیتی در شبکه های محلی بی‌سیم مبتنی بر استاندارد

802.11b است، معمولاً به کل پروسه‌ی امن‌سازی اطلاعات در این استاندارد به‌اختصار WEP گفته می‌شود. کلید های WEP اندازه هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلید ها 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 بزرگ تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلید هایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن میکند. به عبارت دیگر تعداد کلید های ممکن برای اندازه‌ی ۸۰ بیت (که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌ای بالاست که قدرت پردازش سیستم‌های رایانه‌ای کنونی برای شکستن کلید ی مفروض در زمانی معقول کفایت نمیکند.

هرچند که در حال حاضر اکثر شبکه های محلی بی‌سیم از کلید های ۴۰ بیتی برای رمزکردن بسته های اطلاعاتی استفاده میکنند ولی نکته‌ای 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 آسیب پذیر است و این آسیب پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه‌گی در شکل زیر نمایش داده شده است :




## Integrity

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

در استاندارد 802.11 نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دسترسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، CRC داده های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف مین دو CRC به‌معنای تغییر محتویت بسته در حی 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 802.11b هیچ مکانیزمی برای مدیریت کلید های امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلید ها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب میکنند به صورت 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 شبکه های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به صورت مداوم، لودادن کلید ، استفاده از کلید های تکراری یا کلید های پیش فرض کارخانه و دیگر بی توجهی ها نتیجه ای جز درصد نسبتاً بالایی از حملات موفق به شبکه های بی‌سیم ندارد. این مشکل از شبکه های بزرگ‌تر بیشتر خود را نشان می‌دهد. حتا با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های 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.

## مدولاسیون فاز

در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می‌گیرند و چهار نماد را پدید می‌آورند. واضح است که در این روش تسهیم، دامنه سیگنال ثابت است. در روش تسهیم تفاضلی سیگنال اطلاعات با توجه به میزان اختلاف فاز و نه مقدار مطلق فاز تسهیم و مخابره می‌شوند. به عنوان مثال در روش pi/4-DQPSK، چهار مقدار تغییر فاز ۳ -pi/4، 3pi/4، pi/4، و-pi/4 است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می‌تواند دو بیت را کُدگذاری نماید.

| بیتهای فرد | بیتهای زوج | اختلاف فاز |
|---|---|---|
| ۱ | ۱ | ۳pi/4- |
| ۰ | ۱ | ۳ pi/4 |
| ۰ | ۰ | Pi/4 |
| ۱ | ۰ | pi/4- |

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک 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 یک دنباله از کدهای شبه تصادفی تسهیم می‌شود. در این تکنیک نرخ بیتی شبه کُد تصادفی، نرخ تراشه نامیده می‌شود. در استاندارد 802.11 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 یک فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند. جدول زیر فهرست کامل کدهای بارکر را نشان می‌دهد. همانگونه که در این جدول مشاهده می‌شود کدهای بارکر از ۸ دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد 802.11 مورد استفاده قرار می‌گیرد، از کد بارکر با طول ۱۱ (N=11) استفاده می‌شود. این کد به ازاء یک 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.

### کدهای بارکر

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

### استفاده مجدد از فرکانس

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

### طراحی شبکه سلولی

در این طراحی به هریک از سلول‌های همسایه یک کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول‌های همسایه به حداقل رسیده است. این تکنیک 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. خوانندگان علاقمند می‌توانند دایره های جدید را در چهار جهت شبکه سلولی شکل فوق با فرکانس‌های متمایز F1,F2,F3 ترسیم و گسترش دهند.

### مقایسه مدلهای 802.11

### استاندارد 802.11b

همزمان با برپایی استاندارد IEEE 802.11b یا به اختصار b۱۱. در سال ۱۹۹۹، انجمن مهندسین برق و الکترونیک 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 تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر است:

- استفاده از تکنیک رادیویی DSSS در باند فرکانسی GHz۲,٤ به همراه روش مدولاسیون CCK
- استفاده از تکنیک رادیویی FHSS در باندفرکانسی GHz ۲,٤ به همراه روش مدولاسیون CCK
- استفاده از امواج رادیویی مادون قرمز

در استاندار 802.11 اولیه نرخ‌های ارسال داده ۱ و ۲ مگابیت در ثانیه است. در حالی که در استاندارد 802.11b با استفاده از تکنیک CCK و روش تسهیم QPSK نرخ ارسال داده به ٥,٥ مگابیت در ثانیه افزایش می‌یابد همچنین با به کارگیری تکنیک 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 زیر سرعت های 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 802.11b اختصاص داده است.

## اثرات فاصله

فاصله از فرستنده برروی کارایی و گذردهی ی بی‌سیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد 802.11 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 802.11b پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می‌نماید (رجوع کنید به بخش دسترسی به رسانه). 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 بسته های 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 کامپیوتری، پل بین شبکه‌ای یا Bridging در استاندارد 802.11b پوشش داده نشده است . در پل بین شبکه‌ای امکان اتصال نقطه به نقطه (و یا یک نقطه به چند نقطه) به منظور برقراری ارتباط یک شبکه محلی با یک 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 802.11b این کاربرد را پوشش نمی‌دهد ولی بسیاری از شرکت‌ها پیاده‌سازی‌های انحصاری از پل بی‌سیم را به صورت گسترش و توسعه استاندارد 802.11b ارائه 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 ی محلی نیز نباید از ١ 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 802.11b از تکنیک FHSS در لایه فیزیکی استفاده می‌کردند. از ویژگی‌های قابل توجه این تکنیک مقاومت قابل توجه آن در برابر پدیده چند مسیری است. در این تکنیک از کانال های متعددی (۷۹ کانال) با پهنای باند نسبتاً کوچک 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.

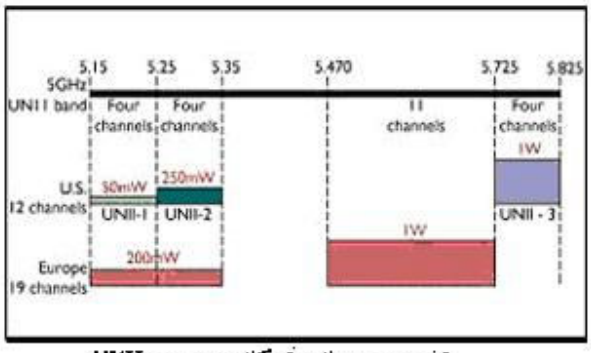
## استاندارد 802.11a

استاندارد 802.11a ، از باند رادیویی جدیدی برای شبکه ی محلی بی‌سیم استفاده می‌کند و پهنای باند شبکه ی بی‌سیم را تا ٥٤ Mbps افزایش می‌دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک 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 ٢٤،١٢،٦ مگابیت در ثانیه اجباری است. برخی از کارشناسان ی محلی بی‌سیم، استاندارد IEEE 802.11aرا نسل آینده IEEE 802.11تلقی می‌کنند و حتی برخی از محصولات مانند تراشه های Atheros وکارت‌های شبکه PCMCIA/Cardbus محصول Card Access

Inc. استاندارد IEEE 802.11a را پیادهسازی کردهاند. بدون شک 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 802.11b بوده 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 802.11 این باور است که 802.11a قبل از 802.11b مورد بهره برداری واقع شده است. در حقیقت 802.11b نسل دوم استانداردهای بیسیم (پس از 802.11)است و 802.11a نسل سوم از این مجموعه استاندارد به شمار میرود. استاندارد 802.11a برخلاف ادعای بسیاری از فروشندگان تجهیزات بیسیم نمیتواند جایگزین 802.11b شود زیرا لایه فیزیکی مورد استفاده در هریک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هریک متفاوت است.




تخصیص باند فرکانسی در UNII

در شکل فوق 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 ی بی‌سیم مورد استفاده قرار می‌گیرد که به طور مشابه از باند فرکانسی 802.11a استفاده می‌کند. یکی از نکات جالب توجه در استاندارد 802.11a 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 802.11a را در سه محور زیر خلاصه نمود.

- افزایش در پهنای باند در مقایسه با استاندارد 802.11b (در استاندارد 802.11a حداکثر پهنای باند ٥٤ Mbps) می‌باشد.

- استفاده از طیف فرکانسی خلوت (باند فرکانسی ٥ GHz)

- استفاده از ۱۲ کانال فرکانسی غیرپوشا (سه محدوده فرکانسی که در هریک ٤ کانال غیرپوشا وجود دارد)

## افزایش پهنای باند

استاندارد 802.11a در مقایسه با 802.11b و پهنای باند ۱۱ Mbps حداکر پهنای باند ٥٤ Mbps را فراهم می‌کند. مهمترین عامل افزایش قابل توجه پهنای باند در این استاندارد استفاده از تکنیک پیشرفته مدولاسیون، موسوم به OFDM است. تکنیکOFDM یک 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 تکنیک مدولاسیون علاوه بر ی بی‌سیم در تلویزیون‌های دیجیتال (در اروپا، ژاپن، و استرالیا) و نیز به عنوان تکنولوژی پایه در خطوط مخابراتی ADSL مورد استفاده قرار می‌گیرد. آندرو مک کورمیک Andrew McCormik از دانشگاه ادینبورو نمایش محاوره‌ای جالبی از این فناوری گردآوری کرده که در نشانی http://www.ee.ed.ac.uk/~acmc/OFDMTut.html قابل مشاهده است.

تکنیک 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 یک از فرکانس های حامل به تنهایی آشکار می‌شوند و نیازی به باند محافظت برای فاصله گذاری بین فرکانس‌ها نیست.

برای کسب اطلاعات بیشتر در خصوص این تکنیک می‌توانید به نشانی زیر مراجعه نمایید:

http://wireless.per.nl/telelearn/ofdm

در کنار افزایش پهنای باند در این استاندارد فواصل مورد استفاده نیز کاهش می‌یابند. در واقع باند فرکانسی ۵ GHz تقریباً دوبرابر باند فرکانسی 2.4 GHz (ISM) است که در استاندارد 802.11b مورد استفاده قرار می‌گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه های بی‌سیم متفاوت و متغیر است ولی به عنوان یک قاعده سرراست می‌توان فواصل در این استاندارد را یک سوم محدوده فرکانسی ۲,٤ GHz (802.11b) در نظر گرفت. در حال حاضر محدوده عملیاتی (فاصله از فرستنده) در محصولات مبتنی بر 802.11a و پهنای باند ٥٤ Mbps در حدود ۱۰ تا ۱۵ متر است. این محدوده در پهنای باند٦ Mbps در حدود ٦١ تا ٨٤ متر افزایش می‌یابد.

Tahiye Va Tanzim : Sohrab Niazi

WwW.NiaziSoft.blogfa.CoM