

WIRELESS

مباحثی پیرامون شبکه های بی سیم

ملاحظات:

لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسندگان این مقاله و مدیریت سایت شبرگرد و جهنم شیطنانی هیچ گونه مسوولیتی نسبت به استفاده نادرست از این مقاله را بر عهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسندگان و همچنین گروه های مربوط بلامانع است.

منابع:

Sun Microsystems , WH Emergency Response ,
Computer Magazine, IEEE 802.11 Working group
Steve Kapp "802.11a:More Bandwidth without the Wire",
Intelligraphics, IEEE 802.11 "Intrnet Protocol Journal"
Wi-foo:"the secret of wireless hacking"

به نام ایزد یکتا

مقدمه:

راه های زیادی برای وصل شدن به اینترنت و شبکه نتورک میباشد
مثله: دیال آپ , لن , دی اس ال , اچ دی اس ال و بی سیم
با گسترش اینترنت متخصصان تکنولوژی را اختراع کردن که بدون
هیچ سیمی میشود به اینترنت وصل شود و بیشتر در مکان های
کاربرد داشت که دسترسی به تلفن قادر نبود و یا شخص در حال
حرکت بود.

خوبی این نوع ارتباطات در این بود که دارای سرعت خوب ,
کاربرد بدون سیم و ... بود.
اولین سیستم برای ارسال سیگنال های الکتریکی از طریق هوا و
بدون سیم (از طریق امواج الکترو مغناطیس) در ابتدا «بی سیم»
نامیده شد.

فیزیکدان بریتانیایی، جیمز کلارک مکسول (۱۸۳۱-۷۹) مهندس
برق امریکایی ایتالیایی الاصل و گوگلیلمو مارکونی (-۱۹۳۷
۱۸۷۴) بودند که این اصول را برای اختراع اولین دستگاه رادیویی
بی سیم واقعی جهان در سال ۱۸۹۵ به کار بردند. سیستم رادیویی
می توانست سیگنالی را تا فاصله نزدیک به سه کیلومتر ارسال و
دریافت کند.

wireless چیست؟

Wireless به تکنولوژی ارتباطی اطلاق می شود که در آن از
امواج رادیویی، مادون قرمز و مایکروویو ، به جای سیم و کابل ،
برای انتقال سیگنال بین دو دستگاه استفاده می شود. تکنولوژی

Wireless به سرعت در حال پیشرفت است و نقش کلیدی را در زندگی ما در سرتاسر دنیا ایفا می کند. تکنولوژی Wireless به کاربر امکان استفاده از دستگاه های متفاوت ، بدون نیاز به سیم یا کابل ، در حال حرکت را می دهد.

شما می توانید صنوق پست الکترونیکی خود را بررسی کنید، بازار بورس را زیر نظر بگیرید، اجناس مورد نیاز را خریداری کنید و یا حتی برنامه تلویزیون مورد علاقه خود را تماشا کنید.

بسیاری از زمینه های کاری از جمله مراقبت های پزشکی، اجرا قوانین و سرویس های خدماتی احتیاج به تجهیزات Wireless دارند. تجهیزات Wireless به شما کمک می کند تا تمام اطلاعات را به راحتی برای مشتری خود به نمایش در بیاورید.

از طرفی می توانید تمامی کارهای خود را در حال حرکت به سادگی به روز رسانی کنید و آن را به اطلاع همکاران خود برسانید. تکنولوژی Wireless در حال گسترش است تا بتواند ضمن کاهش هزینه ها، به شما امکان کار در هنگام حرکت را نیز بدهد. در مقایسه با شبکه های سیمی ، هزینه نگهداری شبکه های Wireless کمتر می باشد. شما می توانید از شبکه های Wireless برای انتقال اطلاعات از روی دریاها، کوهها و ... استفاده کنید و این در حالی است که برای انجام کار مشابه توسط شبکه های سیمی، کاری مشکل در پیش خواهید داشت.

شبکه های بی سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه های بی سیم، با استفاده از انتقال داده ها توسط اموج رادیویی، در ساده ترین صورت، به تجهیزات سخت افزاری امکان می دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه های بی سیم بازه ی وسیعی از

کاربردها، از ساختارهای پیچیدمی چون شبکه‌های بی‌سیم سلولی - که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انواع ساده‌ی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده 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: WLAN، WWAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌ی 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 Wireless Personal Area Network برای موارد خانگی 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

قرار گرفتن 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. به عبارت 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 کنندگان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه‌حل‌های 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 قابل‌توجهی محسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می‌گردد. به عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می‌آیند.

دندان آبی یا همان Bluetooth

ارتباط شبکه اینترنت با بهره‌گیری از تکنولوژی به نام Bluetooth صنعت IT در جهان از سال 2000 به بعد تحولات بسیاری را به خود دیده است. هر روزه مردم با يك تکنولوژی جدید روبه‌رو می‌شوند و دنیای پیچیده و پیشرفته امروزی مردم را وادار به حرکت می‌کند.

اما سرعت این حرکت به قدری زیاد است که حتی متخصصین IT را هم به تعجب واداشته است. با ایجاد هر تکنولوژی مردم مشتاق

شده تا با آن آشنا شوند ولی بلافاصله تکنولوژی پیشرفته دیگری متولد می شود. یکی از این تکنولوژی ها، Bluetooth است که به ارتباط بی سیم با برد کوتاه مربوط می شود. این تکنولوژی در تمام قطعات، وسائل الکترونیکی و ارتباطی کاربرد دارد و استفاده از آن تنها به شبکه و اینترنت مربوط نمی شود، به طوری که امروزه حتی موس و کی بورد Bluetooth هم به بازار آمده است. اکثر کارشناسان و متخصصین کامپیوتر و شبکه اعتقاد دارند که امسال یعنی سال 2004 سال پیشرفت هر چه بیشتر این تکنولوژی خواهد بود.

فرض کنید در منزلتان از تکنولوژی Bluetooth استفاده می کنید و در حال چك کردن E-mail های خود از طریق تلفن همراه هستید، در همان حال نامه ای از دوست خود دریافت می کنید. شما هم نامه او را از طریق Bluetooth به پرینتر که به این سیستم مجهز است ارسال کرده و يك پرینت از آن تهیه می کنید. در همین زمان تلویزیون هم مشغول پخش برنامه ای است که بلافاصله تصویر را به مانیتور انتقال داده و توسط CD-Writer که به تکنولوژی Bluetooth مجهز است تصاویر را روی CD ذخیره می کند.

اینها تنها برخی از موارد استفاده تکنولوژی Bluetooth در زندگی امروز است. تجهیزات مجهز به این تکنولوژی در کنار هم شبکه ای خانگی به نام PAN (Personal Area Network) را ایجاد می کنند.

Bluetooth از کجا آمد؟

شاید جالب باشد تا از تاریخچه نام Bluetooth هم اطلاع داشته باشیم. این نام از نام يك پادشاه دانمارکی به نام Harald Blaaland گرفته شده است. کلمه Blaaland پس از انتقال به زبان انگلیسی به شکل Bluetooth تلفظ شد که به معنی دندان آبی است. این پادشاه که

بین سال های 940 تا 986 می زیست، توانست دانمارك و نروژ را که در جنگ های مذهبی با هم مشکل پیدا کرده بودند متحد کند و از آن پس شهرت زیادی کسب کرد. در واقع تکنولوژی Bluetooth هم بر پایه اتحاد یکپارچه سیستم های کامپیوتر در قالبی بدون سیستم تاکید دارد که نماد کار و تلاش پادشاه دانمارکی است. ایده اصلی ایجاد این سیستم در سال 1994 توسط شرکت موبایل Ericsson ارائه شد. این شرکت به همراه چند شرکت دیگر به دنبال يك سیستم ارتباطی بین وسایل الکترونیکی مختلف بودند تا قادر به هماهنگی و سازگاری با هم باشند.

امروزه بسیاری از وسایل ارتباطی مانند PC، PDA، موبایل، پرینتر و... از پروتکل های متفاوت و ناسازگار با یکدیگر استفاده می کنند و همین امر باعث عدم ارتباط مناسب بین آنها خواهد شد. بنابراین شرکت های مربوطه تصمیم به ایجاد يك استاندارد مشترك برای انواع وسایل ارتباطی گرفتند تا ارتباط میان آنها تحت يك پروتکل ثابت و مشخص برقرار شود. در حال حاضر Ericsson، Intel، Nokia، IBM و Toshiba از پدیدآورندگان و توسعه دهندگان این تکنولوژی هستند. این شرکت ها با تشکیل گروهی به نام SIG Bluetooth (Special Interest Group) موفق شدند استاندارد مورد نظر را ایجاد کنند.

هر وسیله ای که از سیم برای انتقال اطلاعات خود استفاده نمی کند از امواج رادیویی بهره می گیرد در واقع امواج رادیویی سیگنال هایی هستند که توسط فرستنده در هوا پخش می شود. امواج رادیویی قادر به انتقال صدا، تصویر و هر نوع Data هستند. تلفن های بی سیم، موبایل، ماهواره ها، اداره تلویزیون و غیره جزء وسایلی هستند که ارتباط خود را از طریق این امواج فراهم می کنند. حتی دزدگیر اتومبیل شما هم از طریق امواج رادیویی کنترل می شود. Bluetooth نوعی از ارتباطات امواج رادیویی ولی با برد کوتاه است و از پروتکل خاصی برای ارسال اطلاعات خود استفاده می کند

و به همین دلیل است که شرکت های معتبر سازنده دستگاه های ارتباطی و کامپیوتری علاقه زیادی دارند تا در این پروژه شرکت کنند. در واقع تمام دستگاه هایی که بر پایه Bluetooth ایجاد می شود باید با استاندارد مشخصی سازگاری داشته باشند. همان طور که می دانید فرکانس های امواج رادیویی با استفاده از واحد هرتز محاسبه می شوند. فرستنده این فرکانس ها که Transmitter نام دارد امواج مورد نظر را در يك فرکانس خاص ارسال می کند و دستگاه گیرنده در همان طول موج اقدام به دریافت اطلاعات می کند و دامنه آن GHZ2.40 تا GHZ2.48 است.

مزایای Bluetooth

عوامل بسیاری موجب شده تا شرکت ها و موسسات ارتباطی به دنبال استفاده از Bluetooth باشند. یکی از این عوامل محدودیت در انتقال Data از طریق سیم است. دستگاه هایی که با سیم کار می کنند از طریق رابط های سریال یا پارالل و یا USB به کامپیوتر متصل می شوند. اگر از ارتباط سریال استفاده شود در هر سیکل زمانی يك بیت ارسال می شود و ارتباط پارالل در هر سیکل 8 تا 16 بیت را ارسال می نماید. این مقادیر در دنیای ارتباطات پرسرعت امروزی بسیار کم است. تا چندی پیش در مقام کشور های پیشرفته برای ارتباط اینترنت به طور کامل از ارتباطات سیمی و تکنولوژی هایی چون DSL و ISON استفاده می شد. البته این سیستم ها هنوز هم جزء پرطرفدارترین و کاربردی ترین وسایل ارتباطی در جهان هستند. بگذریم که در کشور ما هنوز به طور کامل از این سیستم ها استفاده نمی شود و همچنان سیستم قدیمی و بسیار ضعیف Dial up مورد استفاده قرار می گیرد.

به لطف تکنولوژی جدید Bluetooth کشور هایی چون آمریکا و برخی کشورهای اروپایی که در زمینه تکنولوژی حرف اول را در

دنیا می زنند به سمت استفاده از ارتباطات بی سیم بین شبکه ها و اینترنت حرکت می کنند که علاوه بر سرعت زیاد، کیفیت بسیار خوبی را در اختیار کاربران قرار می دهد. از دیگر مشکلاتی که متخصصین بخش ارتباط با آن سروکار داشتند عدم وجود يك استاندارد مشخص و ثابت برای ارتباط دستگاه های مختلف با یکدیگر بود. تا پیش از این هر شرکت دستگاه های خود را براساس استانداردهای ارتباطی خود تولید می کرد و به همین خاطر اغلب آنها برای ارتباط با دستگاه هایی از همان نوع ولی متعلق به يك کمپانی دیگر دچار مشکل می شدند زیرا پروتکل ثابتی وجود نداشت. حال این مشکل توسط استاندارد Bluetooth به راحتی قابل حل است. قبل از مطرح شدن مسئله استفاده از Bluetooth متخصصان اعتقاد داشتند که در ارتباطات نزدیک از اشعه مادون قرمز استفاده شود.

مثلاً در کنترل از راه دور تلویزیون از این سیستم استفاده می شود. تکنولوژی مادون قرمز IrDA نام دارد و مخفف Infrared Data Association است. در عمل ثابت شده که استفاده از این استاندارد قابل اطمینان است و هزینه بسیار کمی به خود اختصاص می دهد. ولی با این وجود معایبی نیز دارد. اولین مشکل حرکت نور در خط راست است. فرستنده مادون قرمز و گیرنده آن می بایست در مقابل هم قرار بگیرند تا ارسال اطلاعات صورت گیرد، در غیر این صورت و وجود داشتن مانعی در بین راه، انتقال اطلاعات به درستی صورت نمی گیرد. یکی دیگر از مشکلات مادون قرمز اصطلاح «يك به يك» است. به این معنی که شما فقط می توانید اطلاعات را از يك دستگاه تنها به يك دستگاه دیگر ارسال کنید و در يك لحظه قادر به ارسال اطلاعات از يك دستگاه به چند دستگاه نخواهید بود اما هر دو مشکل IrDA از طریق Bluetooth قابل رفع است. یکی دیگر از دلایل استفاده از تراشه های Bluetooth قیمت بسیار مناسب آن است.

قیمت این تراشه ها عملاً 15 تا 30 دلار است که با توجه به کارایی بسیار خوب، این قیمت کاملاً مناسب به نظر می رسد .

همان طور که اشاره شد این تکنولوژی از محدوده فرکانس 40/2 تا 48/2 گیگا هرتز که محدوده ای رایگان است استفاده می کند که 79 کانال ارتباطی را شامل می شود. البته این محدوده در اروپا و آمریکا مورد استفاده قرار می گیرد ولی در ژاپن این محدوده بین 47/2 تا 49/2 گیگا هرتز است و 23 کانال ارتباطی را شامل می شود. هر کدام از این کانال های ارتباطی قابلیت ارسال يك مگابایت اطلاعات را دارد و برد موثر آن 10 متر ذکر شده که شرکت های ارائه کننده این سیستم ها تا برد 7 متر را ضمانت می کنند و بیشتر از آن به فضای اتاقی بستگی دارد که دستگاه ها در آن قرار دارند و همچنین به میزان وجود اگر امواج رادیویی هم وابسته است. سرعت انتقال اطلاعات در استاندارد Bluetooth بستگی به نوع سیستم ارتباطی دارد. مثلاً اگر از ارتباط همزمان یا Synchronous استفاده شود نرخ انتقال اطلاعات 423 کیلوبایت در ثانیه خواهد بود .

در این نوع ارتباط دستگاه فرستنده و گیرنده به طور همزمان قادر به دریافت و ارسال اطلاعات هستند. در نوع دیگر ارتباط که ارتباط غیرهمزمان یا Asynchronous نام دارد نرخ انتقال اطلاعات 721 کیلوبایت در ثانیه خواهد بود. البته با وجود سرعت بیشتر این ارتباط نسبت به ارتباط همزمان، قابلیت ارسال و دریافت در يك زمان را ندارد. البته تکنولوژی های مانند Wi-Fi که بر پایه Bluetooth است برد موثر و نرخ انتقال اطلاعات بیشتر می شود. Bluetooth از سیستم بسیار حساسی نیز برخوردار است و از این لحاظ با استفاده از آن احتمال تداخل بین دستگاه های مجهز به امواج رادیویی به حداقل خود می رسد و حتی در صورت بروز تداخل در ارتباط بلافاصله اطلاعات از بین رفته مجدداً به طور خودکار برای دستگاه گیرنده ارسال خواهد شد. حال این تصور به وجود می آید که با وجود چندین دستگاه مجهز به این تکنولوژی در يك اتاق چگونه آنها

روی يك فرکانس مشخص و بدون تداخل با یکدیگر به تبادل اطلاعات می پردازند .

برای جلوگیری از تداخل اطلاعات Bluetooth از تکنیکی به نام Frequency Spread Spectrum استفاده می کند و این تکنیک به دستگاه ها اجازه می دهد که در يك محدوده فرکانسی مشخص شده به صورت خودکار تغییر فرکانس داشته باشند. در واقع در این تکنولوژی یابنده کانال آزاد بیش از 1500 بار در ثانیه کانال های ارتباطی را چک می کند تا از کانال های اشغال شده با خبر باشد و در صورت ایجاد يك ارتباط جدید يك کانال آزاد را به آن ارتباط اختصاص دهد. مثلاً يك دستگاه کامپیوتر در حال ارتباط با پرینتر از طریق فرکانس GHZ2.47 باشد در همین زمان موبایل قصد ارتباط با اسکنر را دارد. با استفاده از تکنیکی که ذکر شد به طور خودکار فرکانس اشغال شده توسط کامپیوتر و پرینتر شناسایی شده و ارتباط موبایل و اسکنر به روی يك فرکانس جدید برقرار می شود.

سیستم های Wireless می توانند به سه دسته اصلی تقسیم شوند :

سیستم Wireless ثابت :

از امواج رادیویی استفاده می کند و خط دید مستقیم برای برقراری ارتباط لازم دارد. بر خلاف تلفن های همراه و یا دیگر دستگاه های Wireless، این سیستم ها از آنتن های ثابت استفاده می کنند و به طور کلی می توانند جانشین مناسبی برای شبکه های کابلی باشند و می توانند برای ارتباطات پرسرعت اینترنت و یا تلویزیون مورد استفاده قرار گیرند. امواج رادیویی وجود دارند که می توانند اطلاعات بیشتری را انتقال دهند و در نتیجه از هزینه ها می کاهند.

سیستم Wireless قابل حمل :

دستگاهی است که معمولاً خارج از خانه، دفتر کار و یا در وسایل نقلیه مورد استفاده قرار می گیرند. نمونه های این سیستم عبارتند از : تلفن های همراه، نوت بوکها، دستگاه های پیغام گیر و PDA ها. این سیستم از مایکروویو و امواج رادیویی جهت انتقال اطلاعات استفاده می کند.

سیستم Wireless مادون قرمز :

این سیستم از امواج مادون قرمز جهت انتقال سیگنالهایی محدود بهره می برد. این سیستم معمولاً در دستگاه های کنترل از راه دور، تشخیص دهنده های حرکت، و دستگاه های بی سیم کامپیوترهای شخصی استفاده می شود یا پیشرفت حاصل در سالهای اخیر، این سیستم ها امکان اتصال کامپیوتر های نوت بوک و کامپیوتر های معمول به هم را نیز می دهند و شما به راحتی می توانید توسط این نوع از سیستم های Wireless ، شبکه های داخلی راه اندازی کنید.

آینده Wireless

نسل سوم شبکه ها ،G3، نسل آینده شبکه های Wireless نامگذاری شده است. سیستم های G3 کمک می کنند تا صدا و تصویر و داده را با کیفیت مناسب و به سرعت انتقال دهیم. پیش بینی IDC برای کاربردی شدن G3 سال 2004 می باشد و تا آن موقع در حدود 29 میلیون کاربر (m-commerce) در آمریکا وجود خواهند داشت. از طرفی IBM معتقد است که بازار کلی تجهیزات Wireless در سال 2003 به رقمی بالغ بر 83 بلیون دلار خواهد رسید.

منشأ ضعف امنیتی در شبکه های بی سیم 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 حقایق 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 ویژه‌ی 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.

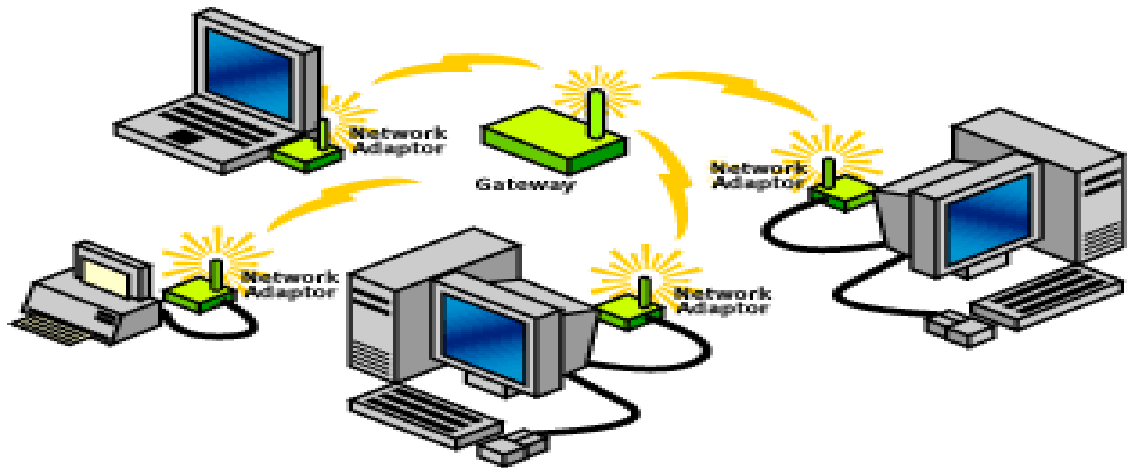
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.

- 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، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.

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

- در سطحی دیگر، با نفوذ به عناصر کنترل‌کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عملکرد شبکه نیز وجود دارد.



شبکه‌های محلی بی‌سیم

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. |

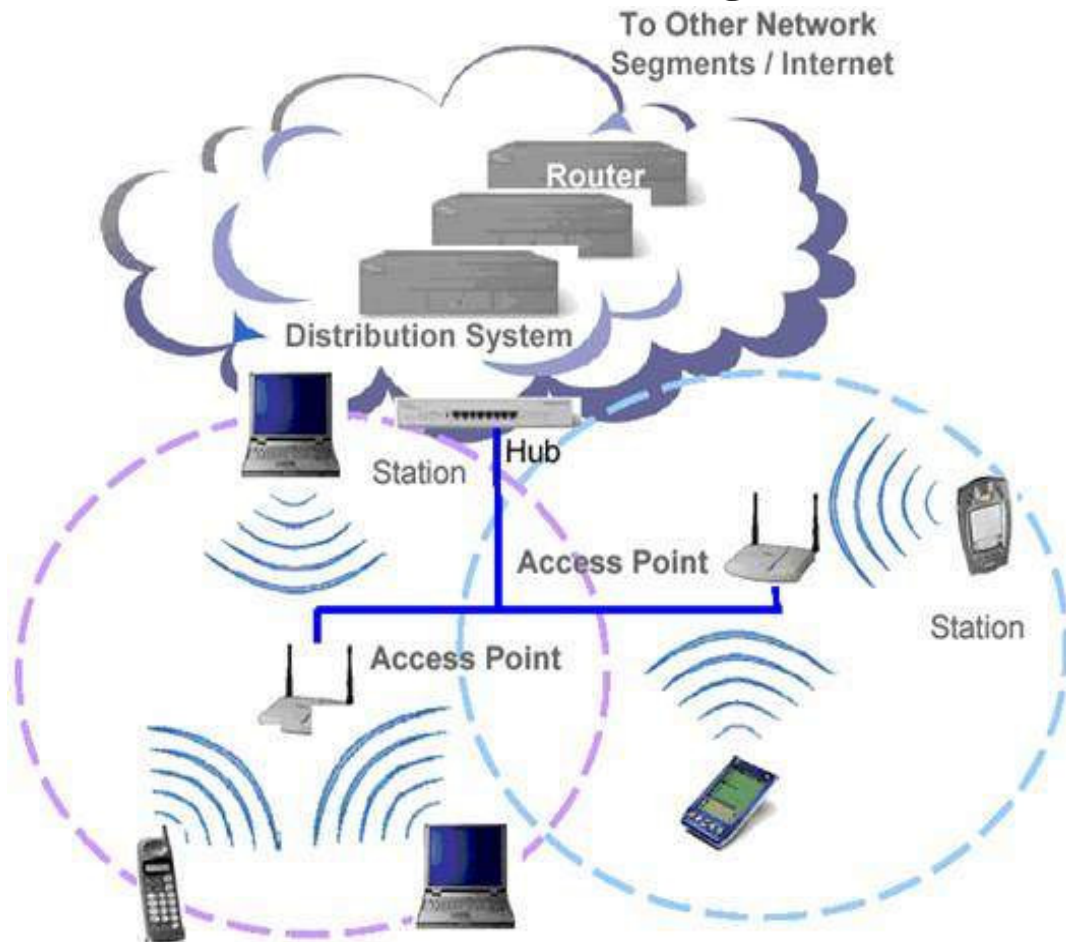
اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌ی بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ 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 5GHz، پهنای باندی تا 54Mbps را فراهم می‌کند. در حالی‌که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps 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 به‌تازگی توسط IEEE معرفی شده است

که به 802.11g شناخته می‌شود. این استاندارد بر اساس فرکانس حامل 2.4GHz عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا 54Mbps 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 802.11b، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.

معماری شبکه‌های محلی بی‌سیم

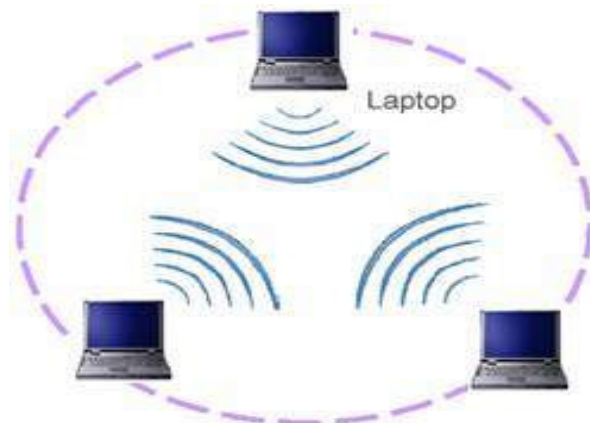
استاندارد 802.11b به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه – همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود- و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point). معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده 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 802.11b را میان سلول‌های مختلف حرکت داد. گستریمی 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 مخدوم 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 مخدوم‌های مجهز به کارت

شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود. شکل زیر نمایی از این ساختار را نشان می‌دهد :



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. شکل زیر شمایی ساده از یک شبکه‌ی Ad hoc را نشان می‌دهد :



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 خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می‌توانند پرونده‌های مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند.

IEEE 802.11

استاندارد شبکه‌های محلی بی‌سیم

در ماه ژوئن سال 1997 انجمن مهندسان برق و الکترونیک (IEEE) استاندارد IEEE 802.11-1997 را به عنوان اولین استاندارد شبکه‌های محلی بی‌سیم منتشر ساخت.

این استاندارد در سال 1999 مجدداً بازنگری شد و نگارش روز آمد شده آن تحت عنوان IEEE 802.11-1999 منتشر شد. استاندارد جاری شبکه‌های محلی بی‌سیم یا همان IEEE 802.11 تحت عنوان ISO/IEC 8802-11:1999، توسط سازمان سازی بین‌المللی (ISO) و مؤسسه

استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال 1997، شکل گیری و پیدایش شبکه سازی محلی بی سیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد 1997، پهنای باند 2Mbps را تعریف می کند با این ویژگی که در شرایط نامساعد و محیط های دارای اغتشاش (نویز) این پهنای باند می تواند به مقدار 1Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است.

بر اساس این استاندارد پهنای باند 1 Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط های عاری از اغتشاش (نویز) پهنای باند 2Mbps نیز قابل استفاده است.

هر دو روش مدولاسیون در محدوده باند رادیویی 2.4 GHz عمل می کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون های رادیویی DSSS و FHSS به عنوان رسانه انتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری 802.11 به زیر گروه های متعددی تقسیم می شود. شکل های 1-1 و 2-1 گروه های کاری فعال در فرآیند استاندارد سازی را نشان می دهد. برخی از مهم ترین زیر گروه ها به قرار زیر است:

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

کمیته 802.11e کمیته ای است که سعی دارد قابلیت QoS اینترنت را در محیط شبکه های بی سیم ارائه کند. توجه داشته باشید که فعالیت های این گروه تمام گونه های 802.11 شامل a، b، و g را در بر دارد. این کمیته در نظر

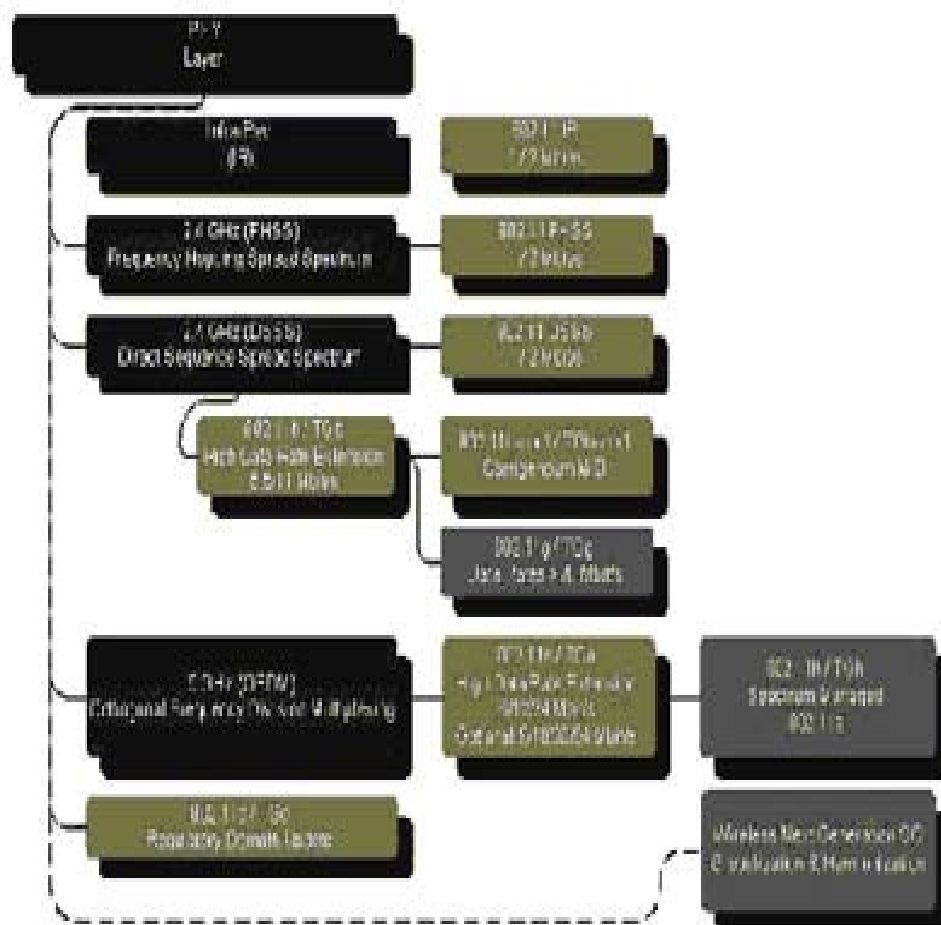
دارد که ارتباط کیفیت سرویس سیمی یا Ethernet QoS را به دنیای بی سیم بیاورد.

کمیته 802.11g کمیته‌ای است که با عنوان 802.11 توسعه یافته نیز شناخته می‌شود. این کمیته در نظر دارد نرخ ارسال داده‌ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یا باند فرکانسی صنعتی، پژوهشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده 2400 مگاهرتز تا 2483.5 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.

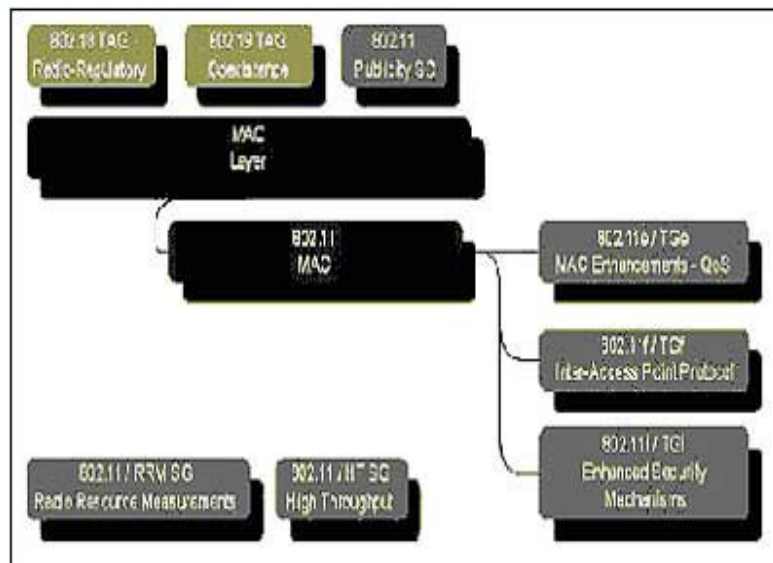
اعضاء این کمیته و سازندگان تراشه توافق کرده‌اند که از تکنیک تسهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می‌تواند به عنوان یک روش جایگزین و رقیب مطرح باشد.

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

فعالیت دو کمیته 802.11i و 802.11x در ابتدا بر روی 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 رمزنگاری به طول 40 و 128 بیت وجود دارد. WEP مشخصاً یک روش رمزنگاری است که از الگوریتم RC4 برای رمزنگاری فریم‌ها استفاده می‌کند. فعالیت این کمیته در راستای بهبود مسائل امنیتی شبکه‌های محلی بی سیم است.

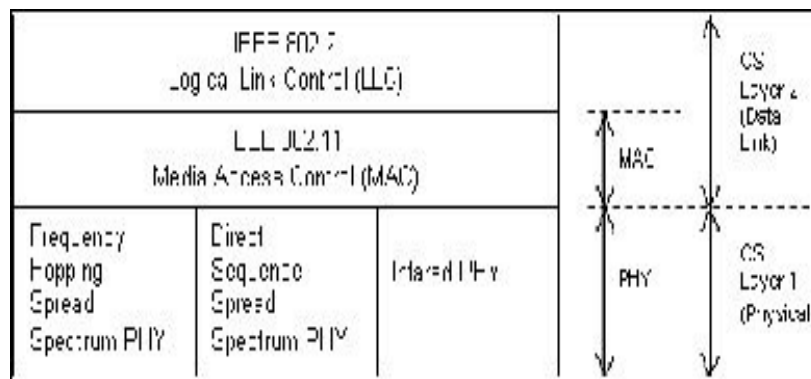


شکل 1-1- گروه‌های کاری لایه فیزیکی



شکل 1-2- گروه‌های کاری لایه دسترسی به رسانه

این استاندارد لایه‌های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بی‌سیم را دربردارد. شکل 1-3 جایگاه استاندارد 802.11 را در مقایسه با مدل مرجع نشان می‌دهد.



شکل 1-3- مقایسه مدل مرجع OSI و استاندارد 802.11

محیط‌های بی‌سیم دارای خصوصیات و ویژگی‌های منحصر به فردی می‌باشند که در مقایسه با شبکه‌های محلی سیمی جایگاه خاصی را به این گونه شبکه‌ها می‌بخشد. به طور مشخص ویژگی‌های فیزیکی یک شبکه محلی بی‌سیم محدودیت‌های فاصله، افزایش نرخ خطا و کاهش قابلیت اطمینان رسانه، همبندی‌های پویا و متغیر، تداخل امواج، و عدم وجود یک ارتباط قابل اطمینان و پایدار در مقایسه با اتصال سیمی است. این محدودیت‌ها، استاندارد

برای کسب اطلاعات بیشتر در خصوص گروه‌های کاری IEEE 802.11 می‌توانید به نشانی <http://www.ieee802.org/11> مراجعه کنید. علاوه بر استاندارد 1999-802.11 IEEE دو الحاقیه IEEE 802.11a و IEEE 802.11b تغییرات و بهبودهای قابل توجهی را به استاندارد اولیه اضافه کرده است که در ادامه این مقاله به بررسی آنها خواهیم پرداخت.

2. معماری شبکه‌های محلی بی‌سیم

معماری 802.11 از عناصر ساختمانی متعددی تشکیل شده است که در کنار هم، سیار بودن ایستگاه‌های کاری را پنهان از دید لایه‌های فوقانی برآورده می‌سازد. ایستگاه بی‌سیم یا به اختصار ایستگاه (STA)، بنیادی‌ترین عنصر ساختمانی در یک شبکه محلی بی‌سیم است. یک ایستگاه، دستگاهی است که بر اساس تعاریف و پروتکل‌های 802.11 (لایه‌های MAC و PHY) عمل کرده و به رسانه بی‌سیم متصل است. توجه داشته باشید که بر اساس تعریف کلاسیک شبکه‌های کامپیوتری، یک شبکه کامپیوتری مجموعه‌ای از کامپیوترهای مستقل و متصل است که منظور از اتصال در این تعریف، توانایی جابجایی و مبادله پیام‌ها است.

ایستگاه‌های کاری بی‌سیم امروزی عمدتاً به صورت مجموعه سخت‌افزاری/نرم‌افزاری کارت‌های شبکه بی‌سیم پیاده‌سازی می‌شوند. همچنین یک ایستگاه می‌تواند یک کامپیوتر قابل حمل، کامپیوتر کفدستی و یا یک نقطه دسترسی باشد. نقطه دسترسی در واقع در حکم پلی است که ارتباط ایستگاه‌های بی‌سیم را با سیستم توزیع یا شبکه سیمی برقرار می‌سازد. کوچکترین عنصر ساختمانی شبکه‌های محلی بی‌سیم در استاندارد 802.11 مجموعه سرویس پایه یا BSS نامیده می‌شود. در واقع BSS مجموعه‌ای از ایستگاه‌های بی‌سیم است.

2-1- همبندی‌های 802.11

در یک تقسیم‌بندی کلی می‌توان دو همبندی را برای شبکه‌های محلی بی‌سیم در نظر گرفت. ساده‌ترین همبندی، **فی‌البداهه** (Ad Hoc) و بر اساس فرهنگ واژگان استاندارد 802.11، IBSS است. در این همبندی 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 نمی‌کنند. واضح است که در این همبندی به سبب محدودیت‌های فاصله هر ایستگاهی ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد.

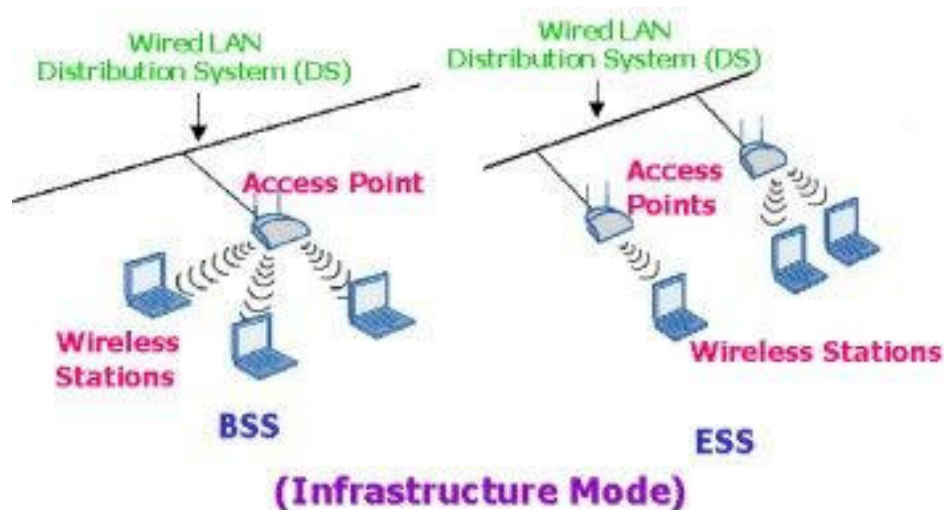
به این ترتیب شرط اتصال مستقیم در همبندی IBSS آن است که ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان بُرد شبکه بی‌سیم قرار داشته باشند. شکل 1-2 همبندی IBSS را نشان می‌دهد.



شکل 1-2- همبندی فی‌البداهه یا IBSS

همبندی دیگر زیرساختار است. در این همبندی عنصر خاصی موسوم به نقطه دسترسی وجود دارد.

نقطه دسترسی ایستگاه‌های موجود در يك مجموعه سرویس را به سیستم توزیع متصل می‌کند. در این همبندی تمام ایستگاه‌ها با نقطه دسترسی تماس می‌گیرند و اتصال مستقیم بین ایستگاه‌ها وجود ندارد در واقع نقطه دسترسی وظیفه دارد فریم‌ها (قاب‌های داده) را بین ایستگاه‌ها توزیع و پخش کند. شکل 2-2 همبندی زیرساختار را نشان می‌دهد.



شکل 2-2- همبندی زیرساختار در دو گونه 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 ایستگاه‌ها ارسال نماید. از سوی دیگر می‌تواند بسته‌ها را در اختیار ایستگاه‌های متصل به شبکه سیمی نیز قرار دهد. 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. بنابر این سیستم توزیع می‌تواند یک شبکه 802.3 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 مجموعه‌های سرویس پایه مبادله شده و انتقال پیام‌ها شکل می‌گیرد. در این همبندی 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 فناوری بی‌سیم یا شبکه‌های سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان يك 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 ایستگاه‌های سیار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت يك شبکه منفرد در سطح لایه MAC تلقی می‌کنند. به این ترتیب پروتکل‌های رایج شبکه‌های کامپیوتری کوچکترین تأثیری از سیار بودن ایستگاه‌ها و رسانه بی‌سیم نمی‌پذیرند. جدول 1-2 همبندی‌های رایج در شبکه‌های بی‌سیم 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) |

جدول 1-2- همبندیهای رایج در استاندارد 802.11

2-2- 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 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 شبکه‌های سیمی، در شبکه‌های 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 يك تقسیم بندی کلی 802.11 دو گونه خدمت هویت سنجی را تعریف می‌کند:

- Open System Authentication
- Shared Key Authentication

روش اول، متد پیش فرض است و يك فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود يك 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 يك کانال مستقل و امن، يك کلید مشترك سری دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترك و با بهرگیری 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 يك شبکه بی‌سیم، تمام ایستگاه‌های کاری و سایر تجهیزات قادر هستند ترافیک داده‌ای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه‌های کاری قابل دریافت است. این ویژگی سطح امنیتی يك ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد.

به همین دلیل در استاندارد 802.11 پروتکلی موسوم به WEP تعبیه شده است که بر روی 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 و پوشش را معادل با شبکه‌های سیمی نماید.

2-3 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 بی‌سیم
- پیوستن مجدد
- توزیع
- مجتمع سازی

سرویس اول يك ارتباط منطقی میان ایستگاه سیّار و نقطه دسترسی فراهم می‌کند. هر ایستگاه کاری قبل از ارسال داده می‌بایست با يك نقطه دسترسی بر روی 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 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 بی‌سیم را به سایر

شبکه‌های محلی و یا يك يا چند شبکه محلی بی‌سیم دیگر متصل می‌کند. سرویس مجتمع سازی فریم‌های 802.11 را به فریم‌هایی ترجمه می‌کند که بتوانند در سایر شبکه‌ها (به عنوان مثال 802.3) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم‌های سایر شبکه‌ها نیز به فریم‌های 802.11 ترجمه شده و از طریق امواج در اختیار ایستگاه‌های کاری سیار قرار می‌گیرند.

4-2- 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 چک 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.

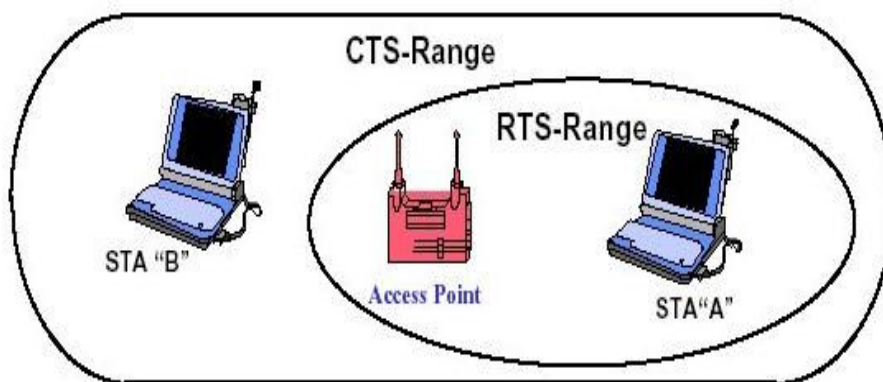
این عمل تا زمانی ادامه می‌یابد که فریم تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم‌ها به تعداد آستان‌های مشخصی برسد که پس از آن فرستنده فریم را دور می‌اندازد.

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

1. پیاده سازی مکانیزم آشکار سازی تصادم به روش ارسال رادیویی دوطرفه نیاز دارد که با استفاده از آن ایستگاه سیار بتواند در حین

ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می‌شود.

2. در يك شبکه بی‌سیم، بر خلاف شبکه‌های سیمی، نمی‌توان فرض کرد که تمام ایستگاه‌های سیار امواج یکدیگر را دریافت می‌کنند. در واقع در محیط بی‌سیم حالاتی قابل تصور است که به آنها نقاط پنهان می‌گوییم. در شکل زیر ایستگاه‌های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.

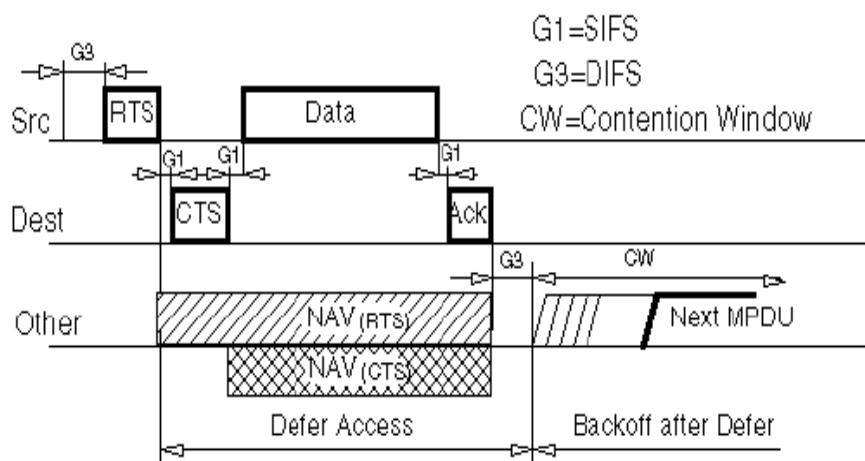


شکل 2-3- روزه‌های پنهان

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 روزه‌های 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 شاخص NAV 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. شکل 2-4 زمان‌بندی RTS/CTS و وضعیت سایر ایستگاه‌ها را نشان می‌دهد.



شکل 2-4- زمان‌بندی RTS/CTS

5-2- 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 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 استاندارد لایه فیزیکی می‌تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ 1 یا 2 مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون PPM-16 و 4-PPM مبادله می‌شوند.

2-5-1- 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 تکنیک مطرح می‌شود آن است که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یک 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:

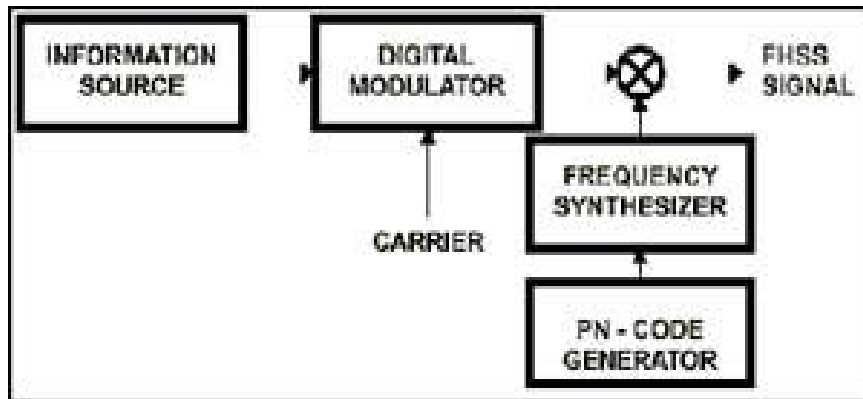
- پایین بودن توان چگالی طیف به طوری که سیگنال اطلاعات برای شنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می‌رسد.

- مصونیت بالا در مقابل پارازیت و تداخل
- رسانی با تفکیک پذیری و دقت بالا
- امکان استفاده در CDMA

مزایای فوق کمیسیون FCC را بر آن داشت که در سال 1985 مجوز استفاده از این سیگنال‌ها را با محدودیت حداکثر توان یک وات در محدوده ISM صادر نماید.

2-5-2- سیگنال‌های طیف گسترده با جهش فرکانسی

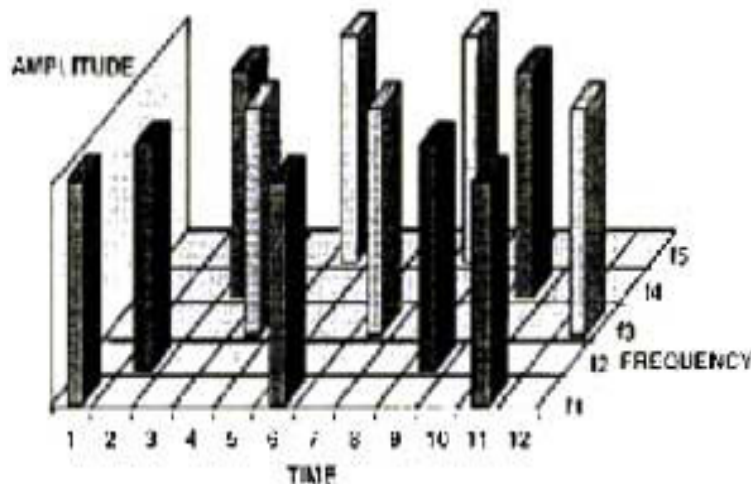
در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می‌کند. شکل 2-5 این تکنیک را در قالب یک نمودار نشان می‌دهد.



PN-CODE = Pseudonoise code

شکل 5-2 - تکنیک FHSS

در این شکل سیگنال اطلاعات با استفاده از یک 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 یک ثبات انتقالی همراه با پس‌خور ساخته می‌شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملاً تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می‌گوییم.







شکل 2-6- تغییر فرکانس سیگنال تسهیم شده به شکل شبه تصادفی

بر اساسی مقررات FCC و سازمان‌های قانون‌گذاری، حداکثر زمان توقف در هر کانال فرکانسی 400 میلی ثانیه است که برابر با حداقل 2.5 جهش

فرکانسی در هر ثانیه خواهد بود. در استاندارد 802.11 حداقل فرکانس جهش در آمریکای شمالی و اروپا 6 مگاهرتز و در ژاپن 5 مگاهرتز می‌باشد.

2-5-3 سیگنال‌های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش يك سيگنال بر روی يك باند فرکانسی بزرگتر از طریق تسهیم آن با يك امضاء یا گد به گونه‌ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با يك گد تسهیم می‌شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می‌گردد. در استاندارد 802.11 روش مدولاسیون مورد استفاده در سیستم‌های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تسهیم می‌شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. از آنجا که در استاندارد 802.11 و سیستم DSSS از روش تسهیم DPSK استفاده می‌شود، داده‌های خام به صورت تفاضلی تسهیم شده و ارسال می‌شوند و در گیرنده نیز يك 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 تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت‌های داده تغییر می‌کند. جدول زیر ایده مدولاسیون فاز را نشان می‌دهد.

| Symbols | Bits | Phase Modulation |
|---------|------|--|
| 1 | 00 |  |
| 2 | 01 |  |
| 3 | 10 |  |
| 4 | 11 |  |

جدول 2-2- 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 $\pi/4$ -3، $\pi/4$ ، $3\pi/4$ 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 گذگذاری نماید.

| اختلاف فاز | بیت‌های زوج | بیت‌های فرد |
|------------|-------------|-------------|
| $-3\pi/4$ | 1 | 1 |
| $3\pi/4$ | 1 | 0 |
| $\pi/4$ | 0 | 0 |
| $-\pi/4$ | 0 | 1 |

جدول 2-3- مدولاسیون تفاضلی

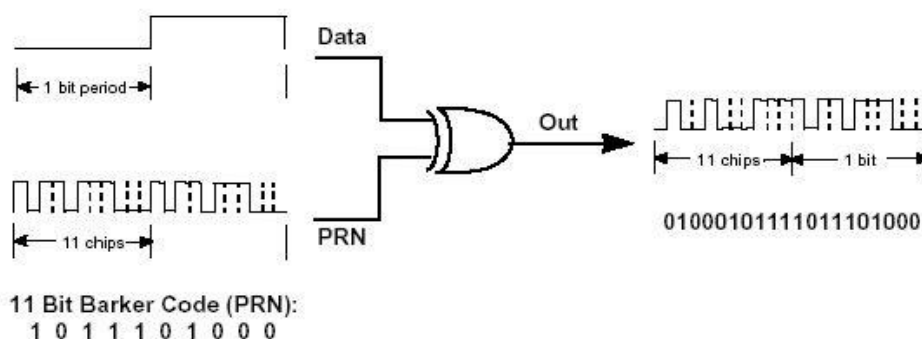
در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از يك كد شبه تصادفی برای پخش و گسترش سیگنال استفاده می‌شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیماً توسط يك دنباله از کدهای شبه تصادفی تسهیم می‌شود. در این تکنیک نرخ بیتی شبه كد تصادفی، نرخ تراشه نامیده می‌شود. در استاندارد 802.11 از كدی موسوم به كد 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 يك فیلتر تطبیقی دیجیتال قادر است به راحتی محل كد بارکر را در يك دنباله بیتی شناسایی کند.

جدول زیر فهرست کامل کدهای بارکر را نشان می‌دهد. همانگونه که در این جدول مشاهده می‌شود کدهای بارکر از 8 دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد 802.11 مورد استفاده قرار می‌گیرد، از کد بارکر با طول 11 ($N=11$) استفاده می‌شود. این کد به ازاء يك نماد، شش مرتبه تغییر فاز می‌دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد 6 مرتبه تغییر فاز خواهد داد.

| CODE LENGTH (N) | BARKER SEQUENCE |
|-----------------|-----------------|
| 1 | + |
| 2 | ++ or +- |
| 3 | ++- |
| 4 | +++ - or +-+ - |
| 5 | ++++ - |
| 7 | ++++--+- |
| 11 | ++++--+-+-- |
| 13 | +++++--++--++ |

جدول 2-4- کدهای بارکر

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

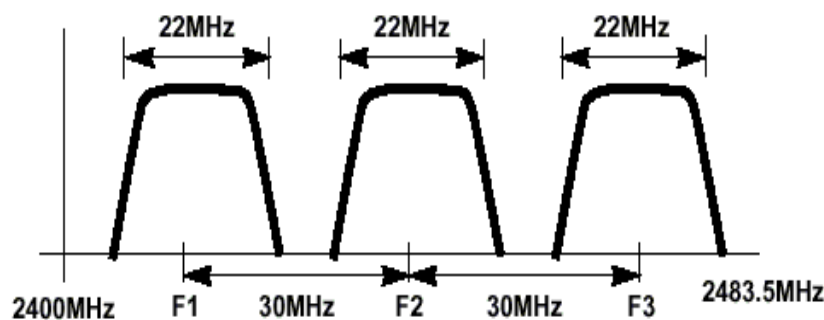


شکل 2-7- مدار مدولاسیون با استفاده از کدهای بارکر

شکل 2-7 مدل منطقی مدولاسیون و پخش سیگنال اطلاعات با استفاده از کدهای بارکر را نشان می‌دهد.

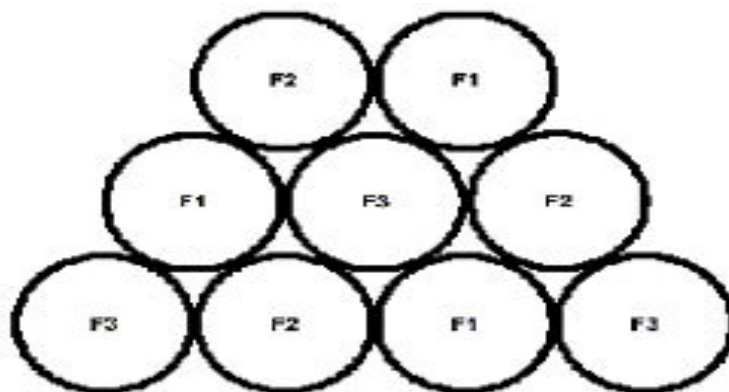
2-6- استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه‌های بی‌سیم، طراحی شبکه سلولی به گونه‌ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد. شکل 2-8 سه کانال DSSS در محدوده فرکانسی ISM را نشان می‌دهد.



شکل 2-8- سه کانال فرکانسی $F3, F2, F1$

شکل 2-9 مفهوم استفاده مجدد از فرکانس با استفاده از شبکه‌های مجاور فرکانسی را نشان می‌دهد. در این شکل مشاهده می‌شود که با استفاده از یک طراحی شبکه سلولی خاص، تنها با استفاده از سه فرکانس متمایز $F3, F2, F1$ امکان استفاده مجدد از فرکانس فراهم شده است.



شکل 2-9- طراحی شبکه سلولی

در این طراحی به هر يك از سلول‌های همسایه يك كانال 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. نکته‌جالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است. خوانندگان علاقمند می‌توانند دایره‌های جدید را در چهار جهت شبکه سلولی شکل فوق با فرکانس‌های متمایز F1, F2, F3 ترسیم و گسترش دهند.

2-7- آنتن‌ها

در یکی تقسیم بندی کلی آنتن‌های مورد استفاده در استاندارد IEEE 802.11 به دو دسته: تمام جهت و نقطه به نقطه تقسیم می‌شوند. واضح است که آنتن‌های تمام جهت با توجه به آنکه نیازی به تنظیم ندارند، راحت‌تر مورد استفاده قرار می‌گیرند. این آنتن‌ها در اغلب کارت‌های شبکه (کارت‌های دسترسی) و نیز نقاط دسترسی یا ایستگاه‌های پایه بکار می‌روند.

این آنتن‌ها در فواصل کوتاه قابل استفاده هستند و برای بهره‌گیری در فواصل طولانی‌تر به تقویت‌کننده‌های خارجی نیاز دارند که البته در بسیاری موارد استفاده از این تقویت‌کننده‌های خارجی میسر و یا قانونی نیست. از سوی دیگر آنتن‌های نقطه به نقطه یا خطی در کاربردهای خارجی استفاده می‌شوند و به تنظیم دقیق نیاز دارند.

محدوده عملیاتی رایج در آنتن‌های تمام جهت 45 متر و محدوده عملیاتی آنتن‌های نقطه به نقطه و توان بالا در حدود 40 کیلومتر است. در کاربردهایی که استفاده از تقویت‌کننده بلا مانع است، این محدوده عملیاتی به شکل قابل توجهی افزایش یافته و تنها توسط خط دید (مسیر دید) محدود می‌شود. از جمله عوامل مهمی که محدوده عملیاتی تجهیزات مبتنی بر IEEE 802.11 را تحت تأثیر قرار می‌دهد محل نصب نقاط دسترسی یا ایستگاه پایه و نیز تداخل رادیویی است. همانگونه که پیشتر گفته شد، تجهیزات مبتنی بر این

استاندارد سعی می‌کنند که با بالاترین نرخ ارسال داده کار کنند و در صورت نیاز به سرعت‌های پایین‌تر برگردند.

3- استاندارد b802.11

همزمان با برپایی استاندارد IEEE 802.11b یا به اختصار b11 در سال 1999، انجمن مهندسين برق و الكترونيك 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 2.4 GHz به همراه روش مدولاسیون CCK
- استفاده از تکنیک رادیویی FHSS در باند فرکانسی 2.4 GHz به همراه روش مدولاسیون CCK
- استفاده از امواج رادیویی مادون قرمز

در استاندارد 802.11 اولیه نرخ‌های ارسال داده 1 و 2 مگابیت در ثانیه است.

در حالی که در استاندارد b802.11 با استفاده از تکنیک CCK و روش تسهیم QPSK نرخ ارسال داده به 5.5 مگابیت در ثانیه افزایش می‌یابد همچنین با به کارگیری تکنیک DSSS نرخ ارسال داده به 11 مگابیت در ثانیه می‌رسد.

به طور سنتی این استاندارد از دو فناوری DSSS یا FHSS استفاده می‌کند. هر دو روش فوق برای ارسال داده با نرخ‌های 1 و 2 مگابیت در ثانیه مفید هستند. جدول 1-3 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 |

جدول 3-1- نرخ‌های ارسال داده در استاندارد 802.11b

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC، مخابره و ارسال فرکانس‌های رادیویی را کنترل می‌کند. این کمیسیون باند فرکانس خاصی موسوم به ISM را در محدوده GHz 2.4 تا GHz 2.4835 برای فناوری‌های رادیویی استاندارد IEEE 802.11b اختصاص داده است.

3-1- اثرات فاصله

فاصله از فرستنده بر روی کارایی و گذردهی شبکه‌های 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 11 Mbps این فاصله 30 تا 45 متر و در پهنای باند 5.5 Mbps، 40 تا 45 متر و در پهنای باند 2 Mbps، 75 تا 107 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 b802.11 پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می‌نماید (رجوع کنید به بخش 2-4 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 1 Mbps 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 بسته‌های غیرتکراری ارسال شده در واحد زمان) ایفا می‌کند.

3-2 پل بین شبکه‌ای

بر خلاف انتظار بسیاری از کارشناسان شبکه‌های کامپیوتری، پل بین شبکه‌ای یا Bridging در استاندارد b802.11 پوشش 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.

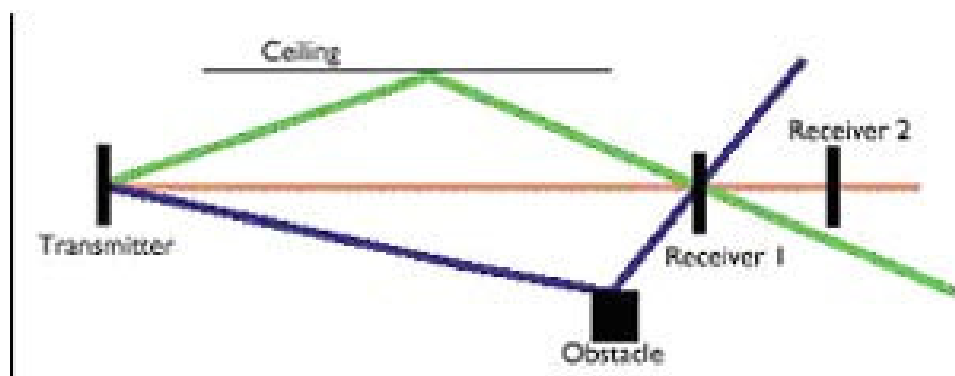
با وجود اینکه استاندارد b802.11 این کاربرد را پوشش نمی‌دهد ولی بسیاری از شرکت‌ها پیاده‌سازی‌های انحصاری از پل بی‌سیم را به صورت

گسترش و توسعه استاندارد b802.11 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 4 وات بیشتر باشد. بر اساس مقررات FCC توان سیگنال‌های ساطع شده در شبکه‌های محلی نیز نباید از 1 وات تجاوز نماید.

3-3- پدیده چند مسیری

شکل 3-1 پدیده چند مسیری را نشان می‌دهد. در این پدیده مسیر و زمان بندی سیگنال در اثر برخورد با موانع و انعکاس تغییر می‌کند. پیاده سازی‌های اولیه از استاندارد b802.11 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 کانال‌های متعددی (79 کانال) با پهنای باند نسبتاً کوچک استفاده شده و فرستنده و گیرنده به تناوب کانال فرکانسی خود را تغییر می‌دهند.

این تغییر کانال هر 400 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.



شکل 3-1- پدیده چند مسیری

4- استاندارد a802.11

استاندارد a802.11، از باند رادیویی جدیدی برای شبکه‌های محلی بی‌سیم استفاده می‌کند و پهنای باند شبکه‌های بی‌سیم را تا 54 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: 6, 9, 12, 18, 24, 36, 48, 54 Mbps که بر اساس استاندارد، پشتیبانی از سرعت‌های 6, 12, 24 مگابیت در ثانیه اجباری است.

برخی از کارشناسان شبکه‌های محلی بی‌سیم، استاندارد IEEE 802.11a را نسل آینده IEEE 802.11 تلقی می‌کنند و حتی برخی از محصولات مانند تراشه‌های Atheros و کارت‌های شبکه PCMCIA/Cardbus محصول Access Inc Card. استاندارد IEEE 802.11a را پیادسازی 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 قیمت 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.

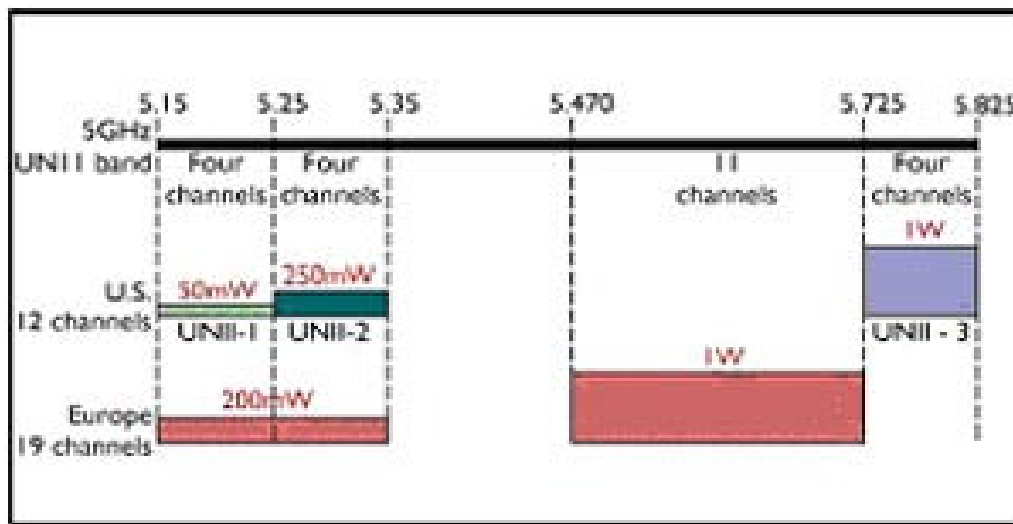
این استاندارد از باند فرکانسی خاصی موسوم به UNII استفاده می‌کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می‌شود:

UNII-1 @ 5.2 GHz

UNII-2 @ 5.7 GHz

UNII-3 @ 5.8 GHz

یکی از تصورات غلط در زمین‌هاستنداردهای 802.11 این باور است که a802.11 قبل از b802.11 مورد بهره برداری واقع شده است. در حقیقت b802.11 نسل دوم استاندارد‌های بی‌سیم (پس از 802.11) است و a802.11 نسل سوم از این مجموعه استاندارد به شمار می‌رود. استاندارد a802.11 برخلاف ادعای بسیاری از فروشندگان تجهیزات بی‌سیم نمی‌تواند جایگزین b802.11 شود زیرا لایه فیزیکی مورد استفاده در هر یک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هر یک متفاوت است.



شکل 4-1- تخصیص باند فرکانسی در UNII

در شکل 4-1 این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می‌شود. این سه ناحیه کاری 12 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 قاره اروپا قابل استفاده نیست. در اروپا HyperLAN2 برای شبکه‌های بی‌سیم مورد استفاده قرار می‌گیرد که به طور مشابه از باند فرکانسی a802.11 استفاده می‌کند. یکی از نکات جالب توجه در استاندارد a802.11 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 a802.11 را در سه محور زیر خلاصه نمود.

- افزایش در پهنای باند در مقایسه با استاندارد b802.11 (در استاندارد a802.11 حداکثر پهنای باند 54 Mbps) می‌باشد.
- استفاده از طیف فرکانسی خلوت (باند فرکانسی 5 GHz)
- استفاده از 12 کانال فرکانسی غیر پوشا (سه محدود فرکانسی که در هر يك 4 کانال غیر پوشا وجود دارد)

4-1- افزایش پهنای باند

استاندارد a802.11 در مقایسه با b802.11 و پهنای باند 11 Mbps حداکثر پهنای باند 54 Mbps را فراهم می‌کند. مهم‌ترین عامل افزایش قابل توجه پهنای باند در این استاندارد استفاده از تکنیک پیشرفته مدولاسیون، موسوم به OFDM است. تکنیک OFDM يك تکنولوژی (فناوری) 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 چندآهنکی گسسته نیز شناخته می‌شود. این تکنیک 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. آندرو مک کورمیک McCormik Andrew از دانشگاه ادینبورو نمایش محاوره‌ای جالبی از این فناوری گردآوری کرده که در نشانی

است. <http://www.ee.ed.ac.uk/~acmc/OFDMTut.html> قابل مشاهده

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 فرکانس‌های 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.

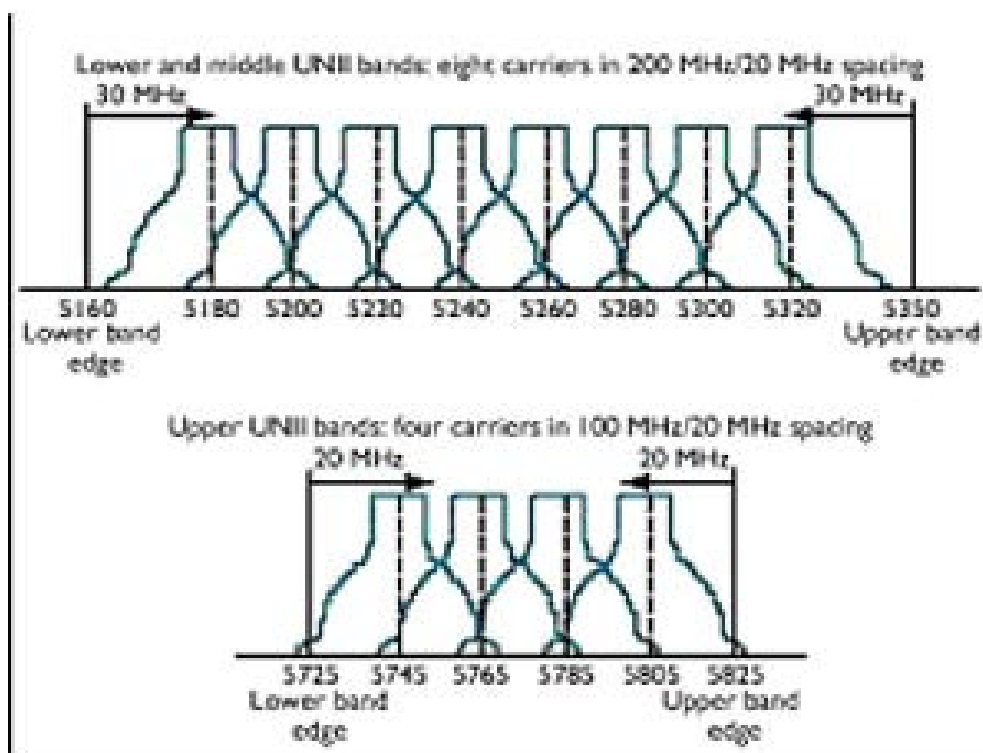
در واقع باند فرکانسی 5 GHz تقریباً دوبرابر باند فرکانسی 2.4 ISM (GHz) است که در استاندارد 802.11b مورد استفاده قرار می‌گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه‌های بی‌سیم متفاوت و متغیر است ولی به عنوان یک قاعده سرراست می‌توان فواصل در این استاندارد را یک سوم محدوده فرکانسی 2.4 (802.11b) GHz در نظر گرفت.

در حال حاضر محدوده عملیاتی (فاصله از فرستنده) در محصولات مبتنی بر 802.11a و پهنای باند 54 Mbps در حدود 10 تا 15 متر است. این محدوده در پهنای باند 6 Mbps در حدود 61 تا 84 متر افزایش می‌یابد.

2-4- 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، اجاق‌های مایکروویو، تلفن‌های بی‌سیم و نظایر آن

وجود دارند. این تجهیزات بی‌سیم در باند 2.4 GHz یا طیف ISM هیچگونه تداخلی با تجهیزات باند UNII (تجهیزات بی‌سیم a802.11) ندارند. شکل 2-4 فرکانس مرکزی و فاصله‌های فرکانسی در باند UNII را نشان می‌دهد.



شکل 2-4- فرکانس مرکزی و فواصل فرکانسی در باند UNII

3-4- کانال‌های غیرپوشا

باند فرکانسی UNII، دوازده کانال منفرد و غیر پوشای فرکانسی را برای شبکه‌سازی فراهم می‌کند. از این 12 کانال 8 کانال مشخص (UNII-1, 2) در شبکه‌های محلی بی‌سیم مورد استفاده قرار می‌گیرند. این ویژگی غیرپوشایی گسترش و پیاده‌سازی شبکه‌های بی‌سیم را ساده‌تر از باند ISM می‌کند که در آن تنها 3 کانال غیر پوشا از مجموع 11 کانال وجود دارد.

5- همکاری Wi-Fi

ائتلاف "همکاری اینترنت بی سیم" یا WECA (<http://www.wi-fi.org>) کنسرسیومی از شرکت های Enterasys, Lucent, Cisco, 3Com و سایر شرکت های شبکه سازی است. اعضاء WECA از طریق همکاری مشترک تلاش دارند تا قابلیت همکاری تجهیزات بی سیم 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 می کند.

در حال حاضر این ائتلاف برای بیش از 100 محصول گواهی سازگاری Wi-Fi صادر کرده است و تعداد این محصولات رو به افزایش است. با گسترش فزاینده محصولات IEEE 802.11a، WECA برنامه دیگری برای صدور گواهینامه برای این نوع محصولات نیز ارائه می کند.

6- استاندارد بعدی IEEE 802.11g

این استاندارد مشابه IEEE 802.11b از باند فرکانسی 2.4 GHz (یا طیف ISM) استفاده می کند و از تکنیک OFDM به عنوان روش مدولاسیون بهره می برد. البته PBCC نیز یکی از روش های جایگزین و تحت بررسی برای انتخاب تکنیک مدولاسیون در این استاندارد به شمار می رود. IEEE 802.11g از نظر فرکانسی، تعداد کانال های غیرپوشا، و توان مشابه IEEE 802.11b است. محدوده های عملیاتی نیز کم و بیش مشابه هستند با این تفاوت که حساسیت OFDM به نویز تاحدودی این محدوده عملیاتی را کاهش می دهد. پهنای باند 54 Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می رود.

یکی دیگر از مزایای جالب توجه IEEE 802.11 سازگاری با IEEE 802.11b است. در نتیجه ارتقاء از تجهیزات IEEE 802.11 به استاندارد جدید IEEE 802.11g امری सरراست خواهد بود.

جدول 6-1 سه استاندارد شبکه‌های بی‌سیم را با یکدیگر مقایسه می‌کند.

| IEEE 802.11g | IEEE 802.11a | IEEE 802.11b | |
|--|---|--|-------------------|
| <p>- ارتقاء شبکه‌های b802.11 و رقیبی برای a802.11</p> <p>- کارایی مشابه با a802.11 در فواصل طولانی</p> | <p>- جایگزین شبکه‌های سیمی</p> <p>- فراهم کننده پهنای باند زیاد در کاربردهای (صدا، تصویر، CAD و نظایر آن)</p> <p>- شبکه سازی در محل‌هایی که استفاده از سیم میسر نیست.</p> | <p>- جایگزین شبکه‌های سیمی</p> <p>- فراهم آوردن تحرک و سیار بودن کاربران</p> <p>- شبکه‌سازی در محل‌هایی که استفاده از سیم میسر نیست</p> <p>- پل‌سازی بین شبکه‌های محلی در فواصل دور (40 کیلومتر)</p> | کاربردهای احتمالی |
| <p>- سازگاری با b802.11</p> <p>- محدوده عملیاتی زیاد (نظیر b802.11)</p> <p>- گذردهی (نرخ ارسال داده) بیشتر</p> | <p>- گذردهی (نرخ ارسال داده) بالا در فواصل کم</p> <p>- افزایش تعداد کانال‌های فرکانسی غیرپوشا (4 برابر بیشتر از b802.11)</p> <p>- تداخل فرکانسی کمتر</p> | <p>- استاندارد رایج و تکامل یافته</p> <p>- قیمت منطقی</p> <p>- گذردهی قابل قبول در فاصله زیاد (نرخ ارسال داده)</p> | مزایا |

| | | | |
|-------|---|--|--|
| معایب | - دارا بودن کمترین گذردهی (نرخ ارسال داده) در مقایسه با سایر فناوری‌های بی‌سیم (11 Mbps) - استفاده از تنها 3 کانال فرکانسی غیر پوشا | - فناوری نسبتاً گران - ناسازگاری با b802.11 - محدوده عملیاتی کوچک - محدودیت‌های FCC بر روی آنتن‌ها (حداکثر توان مجاز) در هر باند فرکانسی | - عدم وجود محصول فراگیر (احتمالاً تا اواسط سال 2003 میلادی) - محدودیت‌ها کانال فرکانسی نظیر b (3802.11) کانال (غیرپوشا) |
|-------|---|--|--|

جدول 6-1 – مقایسه استانداردهای بی‌سیم IEEE 802.11

عناصر فعال شبکه‌های محلی بی‌سیم

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

1. ایستگاه بی‌سیم

ایستگاه یا مخدم 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 پوشش 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 به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه بی سیم نیست. کارت های شبکه بی سیم عموماً برای استفاده در چاک های PCMCIA است. در صورت نیاز به استفاده از این کارت ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت ها را بر روی چاک های گسترش PCI نصب می کنند.

2. نقطه ی دسترسی

نقاط دسترسی در شبکه های بی سیم، همان گونه که در قسمت های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه های بی سیم را بازی کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم ها و ایستگاه های بی سیم به شبکه ی سیمی اصلی متصل می گردد.

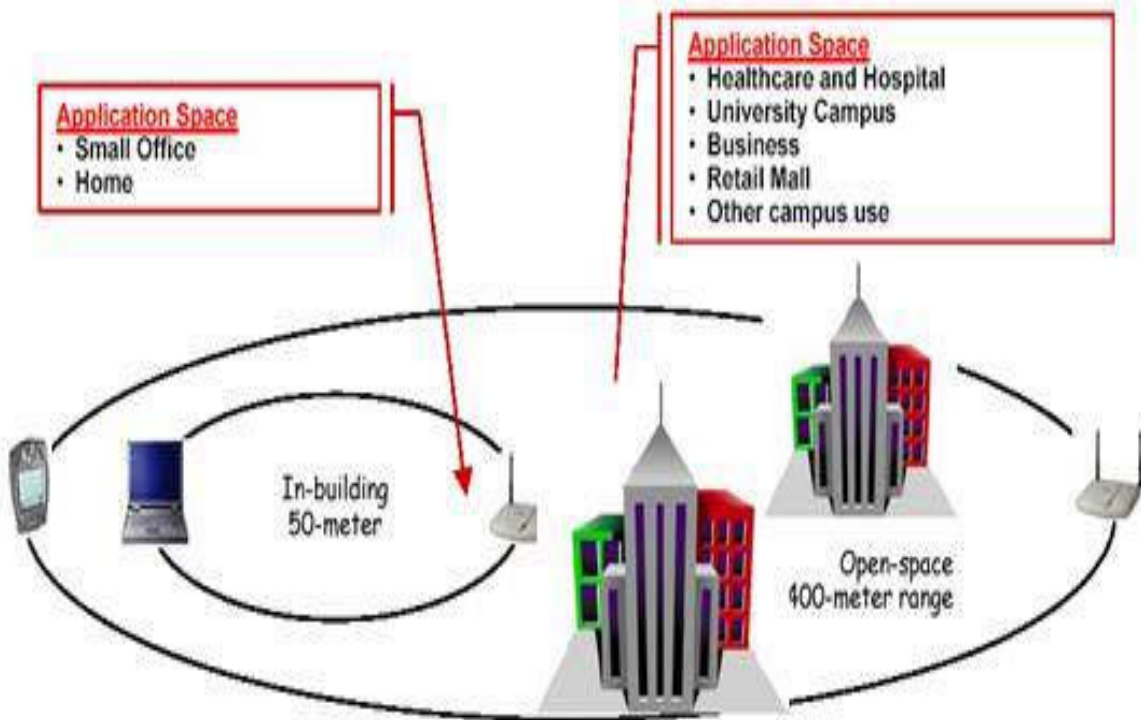
برد و سطح پوشش

شعاع پوشش شبکه ی بی سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بسته گی دارد که برخی از آن ها 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 ۲۹ متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵ متر (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 ۱۰۰ متر است. این شعاع عمل‌کرد مقداریست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد. شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد :

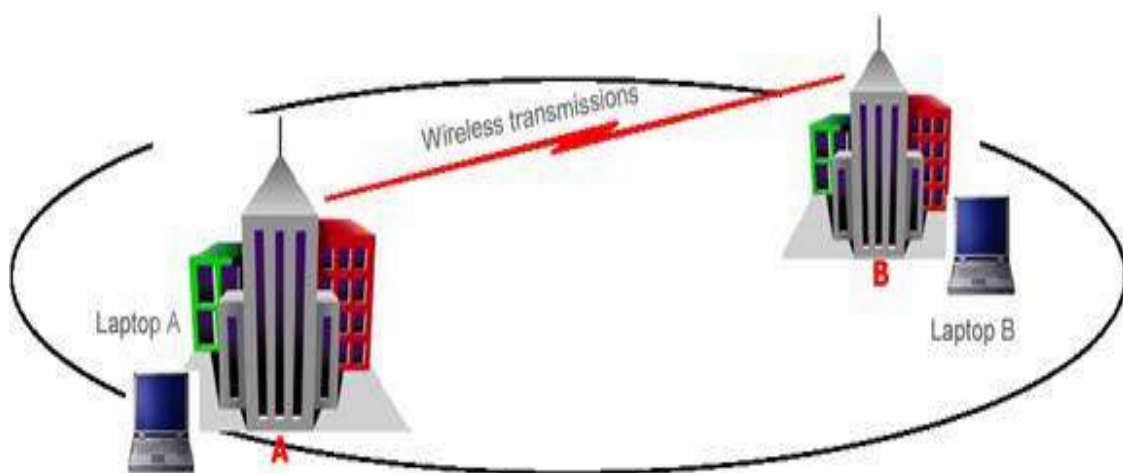


یکی از عملکردهای نقاط دسترسی به عنوان سویچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به عبارت دیگر با استفاده از چند سویچ بی‌سیم می‌توان عملکردی مشابه Bridge برای شبکه‌های بی‌سیم را به دست آورد.

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 به صورت 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 به معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به دست آورد.

شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان می‌دهد :

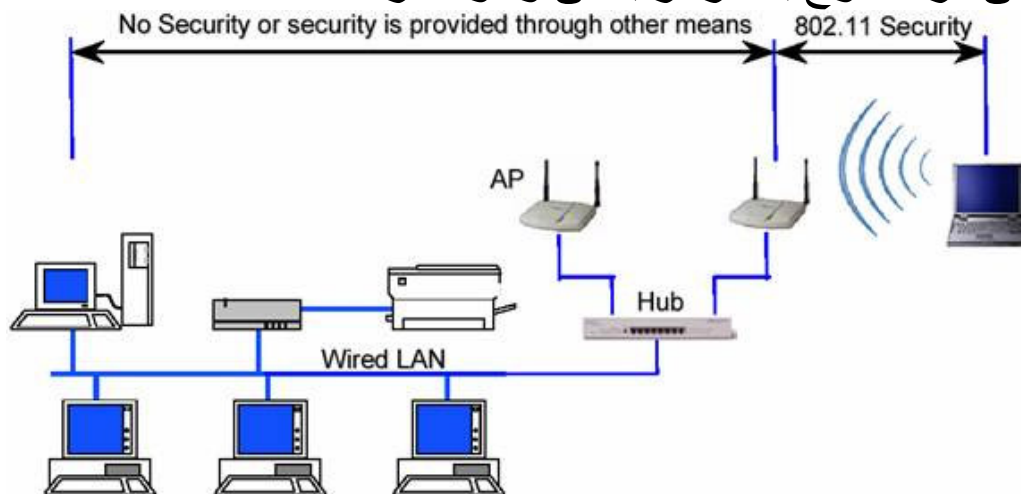


از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه‌های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دسترسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمان‌ها، سطح پوشش شبکه را تا ساختمان‌های دیگر گسترش داد.

امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

پس از آن‌که در سه قسمت قبل به مقدمه‌یی در مورد شبکه‌های بی‌سیم محلی و عناصر آن‌ها پرداختیم، 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 802.11 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 مخدم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌ی دارد، به عبارت دیگر این پروتکل کل

ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به معنی 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.



شکل بالا محدوده‌ی عمل کرد استانداردهای امنیتی 802.11 (خصوصاً WEP) را نشان می‌دهد.

قابلیت‌ها و ابعاد امنیتی استاندارد 802.11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد 802.11 فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌ی 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 مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزئی میان امنیت در شبکه‌های سیمی و بی‌سیمی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

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

Authentication.1

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

Confidentiality.2

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.3

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

نکته‌ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس‌های معمول Auditing و Authorization در میان سرویس‌های ارایه شده توسط این پروتکل است.

سرویس‌های امنیتی WEP - Authentication

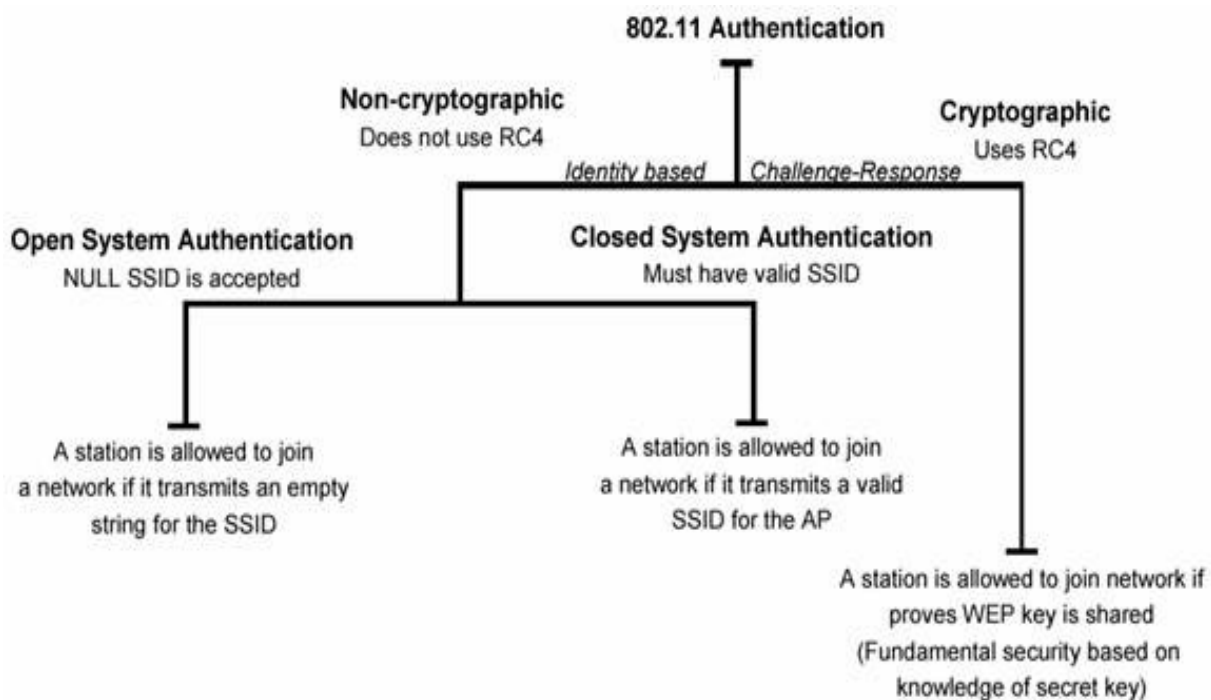
در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن‌سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد 802.11 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم.

در این قسمت به معرفی سرویس اول، یعنی Authentication، می‌پردازیم.

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 رمزنگاری است و دیگری از رمزنگاری استفاده نمی‌کند.
 شکل زیر شمایی 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 رمزنگاری استفاده نمی‌کند.

Authentication بدون رمزنگاری

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 نگامداری 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 SSID ارسال شده جزو SSIDهای مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته‌ی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد.

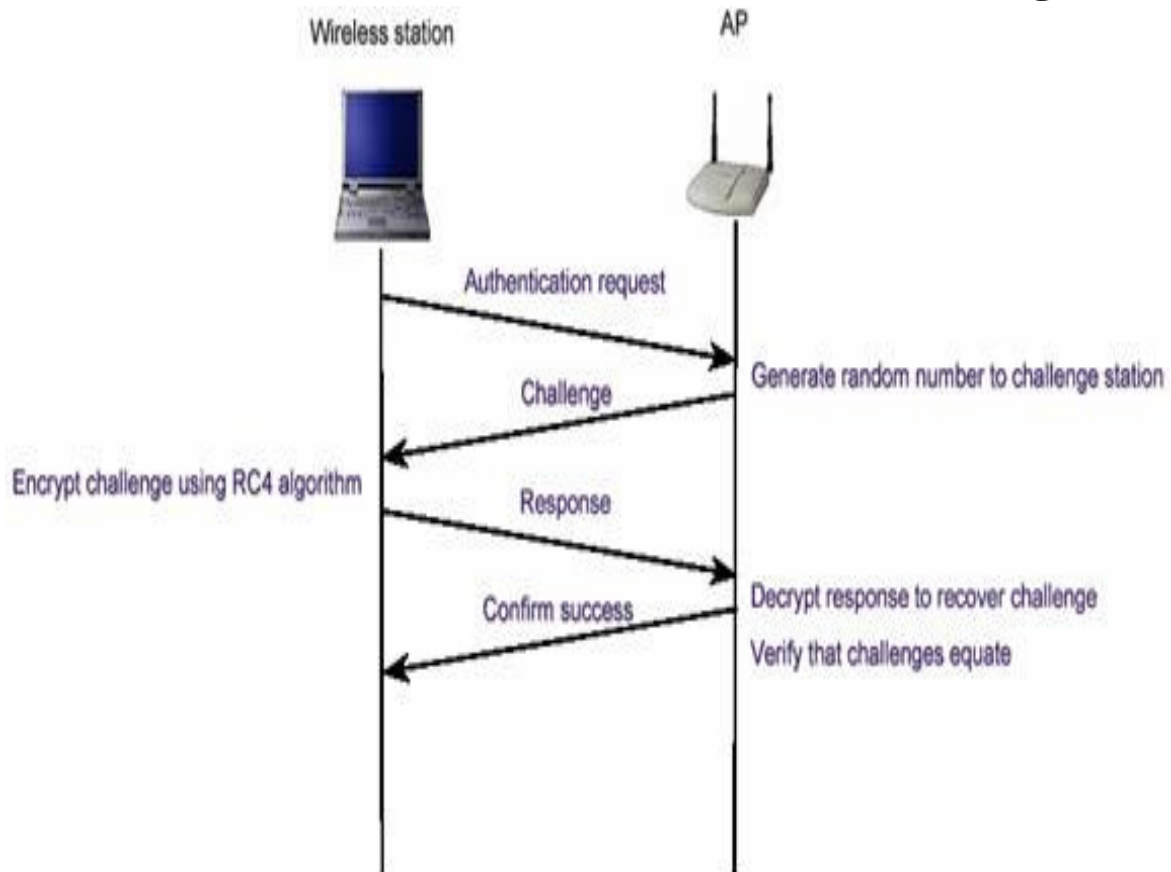
این دو روش عملاً روش امنی از احراز هویت را ارائه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آنجایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌ی 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!

Authentication با رمزنگاری RC4

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 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 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 دسترسی‌یی که با آن در حال تبادل داده‌های رمزی‌ست نقطه‌ی دسترسی اصلی‌ست.

(ب)

تمامی روش‌هایی که مانند این روش بر پایه‌ی سؤال 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.

سرویس‌های امنیتی 802.11b – Integrity و Privacy

در قسمت قبل به سرویس اول از سرویس‌های امنیتی 802.11b پرداختیم. این قسمت به بررسی دو سرویس دیگر اختصاص دارد. سرویس اول Privacy (محرمانه‌گی) و سرویس دوم Integrity است.

Privacy

این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به‌معنای حفظ امنیت و محرمانه نگه‌داشتن اطلاعات کاربر یا گروه‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از

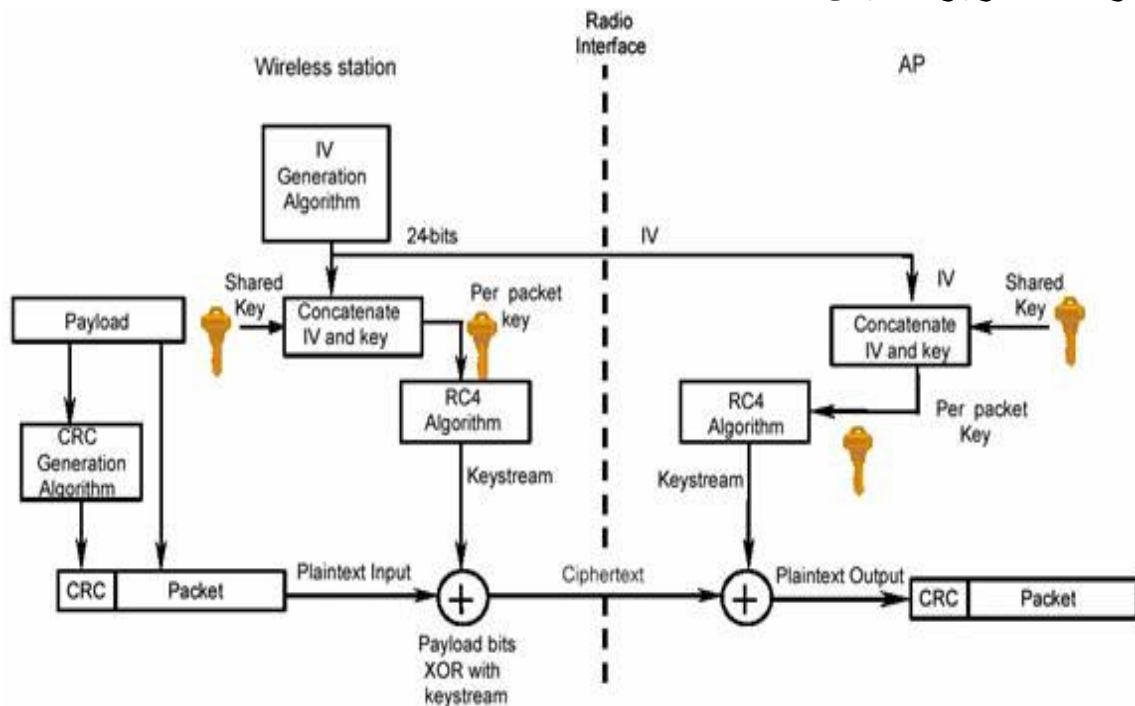
تکنیک‌های رمزنگاری استفاده می‌گردد، به‌گونه‌یی که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

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 تعداد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌ی 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 زیر 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 802.11b نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدم‌های 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 رمز شدن 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 به معنای 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 802.11b 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 به صورت دستی پیاده‌سازی گردد.

از آنجایی که این بخش از امنیت یکی از معضله‌های 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 تغییر ندادن کلید به صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی‌ها نتیجه‌ی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد.

این مشکل از شبکه‌های بزرگتر بیش‌تر خود را نشان می‌دهد. حتی با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گهگاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می‌دهد که همان باعث رخنه در کل شبکه می‌شود.

ضعف‌های اولیه‌ی امنیتی WEP

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802.11 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 تولیدکنندگان 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

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 به راحتی 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.

۲. Initialization Vector (IV)

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می‌شود. از آنجایی که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می‌شود، 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 به همراه 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.

۳. ضعف در الگوریتم

از آنجایی که 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 رمز شده 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.

۴. 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 رمز نشده 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، به راحتی عوض کند و منتظر عکس‌العمل نقطه‌ی دسترسی بماند که آیا بسته‌ی تأیید را صادر می‌کند یا خیر.

ضعف‌های بیان شده از مهم‌ترین ضعف‌های شبکه‌های بی‌سیم مبتنی بر پروتکل WEP هستند. نکته‌ی 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.

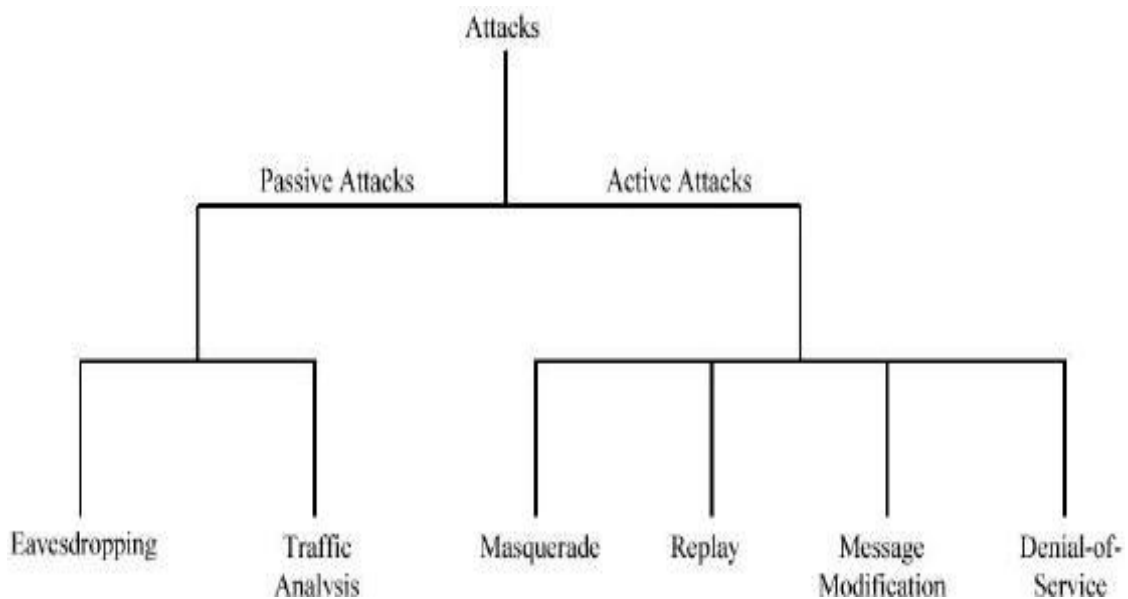
جدول زیر ضعف‌های امنیتی پروتکل WEP را به اختصار جمع‌بندی کرده است :

| 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. |

خطر ها، حملات و ملزومات امنیتی

همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده بی نه چندان دور باید منتظر گسترده گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم. این گسترده گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است، توسعه ی این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات، خطر ها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازیم.

شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد :



مطابق درخت فوق، حملات امنیتی به دو دسته ی فعال و غیرفعال تقسیم می گردند.

حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمی کند. این

نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

- شنود

در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.

- آنالیز ترافیک

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.

حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند :

- تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می کند. این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد.

- پاسخ های جعلی

نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند.

این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه به روشی- توسط نفوذگر قطع شده است، می تواند مورد سوء استفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

- تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه های متنوعی از ترافیک بر روی شبکه رفت و آمد می کنند و هریک از این ترافیک ها و پروتکل ها از شیوه یی برای مدیریت جنبه های امنیتی خود استفاده می کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام ها و در نتیجه حملات را اتخاذ کند.

با توجه به گسترده گی این نوع حمله، که کاملاً به نوع پروتکل بسته گی دارد، در این جا نمی توانیم به انواع مختلف آن بپردازیم، تنها به یادآوری این نکته بسنده می کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می تواند با اعمال تغییرات

خاصی، به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دست رسی – که می تواند یک کاربر عادی باشد – فراهم کند.

- حمله های (Denial-of-Service DoS)

این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی اقدام می کند. ساده ترین نمونه سعی در از کار انداختن خادم های نرم افزاری و سخت افزاری ست.

پیرو چنین حملاتی، نفوذگر پس از از کار انداختن یک سامانه، که معمولاً سامانه یی ست که مشکلاتی برای نفوذگر برای دست رسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می کند.

در برخی از حالات، در پی حمله ی انجام شده، سرویس مورد نظر به طور کامل قطع نمی گردد و تنها کارایی آن مختل می گردد. در این حالت نفوذگر می تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از طریق/به همان سرویس نیز اقدام کند.

تمامی ریسک هایی که در شبکه های محلی، خصوصاً انواع بی سیم، وجود دارد ناشی از یکی از خطرات فوق است.



هکینگ بیسیم (wireless hacking)



در این بخش به مشکلات امنیتی، راه‌های مقابله و فناوری پایه‌ای که عموماً برای 802.11 وجود دارند پرداخته و آن را از نقطه نظر متدولوژی حملات استاندارد مورد بررسی قرار می‌دهیم. مثل (footprint) یا همان ردیابی (scan) یا پویش (enumerate) یا برشماری (penetrate) یا نفوذپذیری و در آخر به عدم سرویس دهی می‌پردازیم.

از آنجا که فن آوری بیسیم در مقایسه با دستگاه‌های سیمی تا حدودی از لحاظ تکنیک‌های حمله استاندارد فرق دارد متدولوژی ما دو فن آوری برشماری و پویش را در یکجا جمع می‌کند. در ادامه آخرین ابزاری که توسط خرابکاران برای حمله به شبکه‌های بیسیم و نفوذ در آن‌ها مورد استفاده قرار می‌گیرد به اختصار شرح خواهیم داد.

ردیابی بیسیم

شبکه های بیسیم و نقاط دسترسی یا تماس (access points=AP) راحتترین و ارزانتترین نوع اهدافی هستند که برای ردیابی بکار میروند و جزوسخت ترین بستر ها جهت شناسایی و رسیدگی میباشند. جنگ در حال حرکت (war-driving) سابقا مترادف با پیکربندی ساده یک (laptop) یک کارت بیسیم و یک network stumbler خوانده میشد ولیکن در حال حاضر مفهوم حرفه ای تری را در بر دارد که میتواند چندین نوع از آنتن های بسیار قدرتمند، کارت های بیسیم و دستگاه های کامپیوتری به اندازه ی کف دست را شامل شود که میتوان از IPaq و palm نام برد.

ما از عبارت جنگ در حالت تحرک در قلمرو متدولوژی هکینگ و ردیابی کمتر استفاده میکنیم زیرا شما برای انجام این عمل مجبور به رانندگی کردن نیستید:) ممکن است در حال قدم زدن در پارک یا شهر باشید و در همان هنگام از لپ تاپ برای واریسی شبکه های بیسیم استفاده کنیم ردیابی دستگاه های بیسیم بخصوص AP ها با انجام وظیفه ساده یافتن آن ها از طریق روش غیر فعال (PASSIVE) گوش دادن به امواج رادیویی (BEACON) پخش خبر AP و یا روش تهاجمی تر ارسال امواج رادیویی کلاینت (CILENT BEACONS) برای پیدا کردن پاسخ ها ی AP صورت میگیرد .

توجه داشته باشید که تمام ردیابی های WLAN را میتوانید در زمانی که در محدوده ی دریافت و ارسال امواج و بسته ها به AP قرار دارید از راه دور انجام دهید . با این گفته ،فایده ی بیشتری خواهد داشت که آنتنی قویتر از آنتنی تهیه کنید که هنگام خرید کارت بیسیم شبکه همراه با آن عرضه میشود .انواع زیادی کارت شبکه بیسیم وجود دارند که تنها تفاوتشان در نوع چیپ ست هایشان

میباشد برخی از این نوع کارت ها به ما اجازه میدهند که آنها را در حالت بی قاعده قرار دهیم که این عمل برای SNIFF در این شبکه ها است. برخی کارت ها بهتر کار میکنند چون از OS های مختلفی پیروی میکنند. قدرت آنتن و جهت آن نیز جزو فاکتورهای مهم این تجهیزات میباشد.

اگر در خیابان های شلوغ در حال راندن هستید از آنتن های همه جهته یا OMNIDIRECTIONAL و هنگامی که در ساختمان و یک محل هستید از آنتن مستقیم یا DIRECTIONAL استفاده کنید. سیستم موقعیت جهانی یا همان GPS افزودنی جالبی است که میتوانید به لیست تجهیزات خود بیافزائید تا بتوانید براحتی AP ها را رد گیری کرده، محدوده ی انتقال آنها را زیر نظر بگیرید و بعد آنها را ریست کنید.

تجهیزات

انواع معینی از تجهیزات مورد نیاز هستند تا بتوان یک زیر مجموعه از حملات معرفی شده را انجام داد که البته به نرم افزار نیز نیاز میباشد.

کارت های بیسیم، آنتن ها و دستگاه های GPS نقش مهمی در اینکه چه نوع حملاتی و در چه محدوده ای موفق خواهند بود دارند.

کارت ها:

توجه کنید که تمام کارت های بیسیم یکسان نیستند. مهم است که محدودیت ها و نیازهای کارت های خود را بشناسیم. برخی از کارت ها به برق کمتری نیاز دارند حساس هستند و برای نصب آنتن های قوی تر، اتصال JACK نیازی ندارند.

نوع OS که بوسیله آن از کارت ها استفاده میکنید اهمیت فراوانی دارد اگر از لینوکس یا FreeBSD استفاده میکنید، میبایستی کرنل های آن ها را با درایورهای PCMCIA-CS کامپایل نمائید که اگر تجربه کمی در لینوکس داشته باشید این کار برای شما آسان نخواهد بود ویندوز فرایند نصب راحتی دارد و لیکن توجه داشته باشید که ابزار، اکسپلویت ها و تکنیک های کمی وجود دارند که بتوان آنها را از کنسول win32 استفاده نمود برای محیط ویندوز، AiroPeek NX تنها اسنیفر ارزشمندی است که توصیه میشود. Net Stumbler وسیله ایست که آن را به اشتباه اسنیفر شبکه های بیسیم میشناسند در حالیکه این برنامه فقط کار تجزیه (parse) سرآمد های (headers) یک بسته بیسیم را بعهده دارد و از یک رابط گرافیکی برای گزارش گیری و چند ویژگی خاص دیگر استفاده میکند.

این برنامه از طریق پروتکل های 802.11 بسته ها را بچنگ می آورد. این برنامه همچنین از حرکت در کانال های کشور های غیر امریکایی پشتیبانی میکند کشور آمریکا خود برای استفاده از کانال های 1 تا 11 برای نقل و انتقالاتش استفاده میکند و لیکن دیگر کشورهای جهان از کانال های 1 تا 24 استفاده میکنند این برنامه در خارج از کشور آمریکا توانایی پشتیبانی از 24 کانال را دارد.

در آدرس های زیر کارت هایی که توسط AiroPeek پشتیبانی میشوند قید شده اند

Windows Wlan Sniffer

<http://www.wildpackets.com/support/hardware/airopeek-nt>

DRIVER COMPATIBILITY

سیستم عاملی که از نقطه نظر ابزار حمله بیسیم، درایور ها و اسنایفر ها، آن ها را کاملاً پشتیبانی میکند. لینوکس می باشد. سازندگان لینوکس وقت زیادی صرف میکنند تا تمام درایور های PCMCIA را که با بیشتر نسخه های چیپ ست PRISM2 که با پروتکل 802.11 سازگار باشند گردآوری نمایند.

البته می بایستی این درایور ها را در کرنل کامپایل مجدد مائید. روال نصب درایور ها مثل نصب دیگر ادوات در لینوکس کار راحتی است. دستورات زیر برای درایور های PCMCIA-CS نسخه 3.2.3 آمده است:

احکام عمومی نصب درایور ها:

1. فایل فشرده pcmcia-cs-3.2.3 را از حالت فشرده در می آوریم (untar) و فایل های تولیدی را در مسیر `usr/src/` قرار می دهیم.

2. فرمان (Make Config) را از مسیر زیر اجرا میکنیم:

`usr/src/pcmcia-cs-3.2.3`

3. سپس فرمان (make all) را هم در مسیر گفته شده در بالا هم اجرا میکنیم

4. و در انتها فرمان (make install) را از مسیر گفته شده در بالا اجرا میکنیم

بسته به Wlan پیکربندی سیستم یا شبکه های مقصد مدنظرتان، ممکن است نیاز به آن داشته باشید که اسکریپت شروع (startup) و فایل های اختیاری در دایرکتوری `etc/pcmcia/` را دستکاری کنید

آنتن ها:

برای یافتن و نصب آنتن مناسب ممکن است وظیفه ی سنگین برپاسازی را به شما ثابت نماید. در ابتدا باید تصمیم بگیرید که چه نوع war-driving می خواهید انجام دهید

در این مقاله منظور از جنگ در حال حرکت یا راندن یعنی بصورت متحرک میتوان از هر نقطه ای حملات خود را آغاز نمائید.

ابتدا می بایستی درباره جهت آنتن ها و تکنولوژی بکار رفته در آنها بدانیم سه نوع آنتن جهت استفاده وجود دارد که با توجه به جهت مورد استفاده کاربرد دارند

1. مستقیم یا جهت دار (directional)

2. چندجهته (multi directional)

3. همه جهته (omni directional)

آنتن های مستقیم وقتی بکار میروند که قصد برقراری ارتباط یا پیدا کردن نواحی خاصی را داشته باشید و خیلی برای جنگ در حال حرکت اصراری نداشته باشید. این آنتن ها برای گرفتن یک بسته از محدوده های بزرگ بسیار مناسب هستند. زیرا قدرت و امواج کاملاً در یک جهت تمرکز دارد. آنتن های چندطرفه یا بصورت دوطرفه هستند یا بصورت چهارطرفه. همه جهت همانی است که وقتی درباره ی آنتن صحبت میشود به یاد آن می افتید این نوع آنتن میتواند در تمام جهات عمل ارسال و دریافت را انجام دهد و بدین وسیله محدوده ی وسیع تری را دربر گیرد.

نکته: منظور از driving رانندگی یعنی اینکه شما کار ارسال و دریافت را هنگام حرکت انجام می‌دهید. آنتن اتومبیل را میتوان یکی آنتن های همه جهته تصور کرد.

حال می بایستی ببینیم چطور میتوان آنتن های خوب و بد را از یکدیگر تمیز داد. کلمه ی (gain) برای توصیف انرژی یک آنتن متمرکز جهت دار بکار میرود.

تمام آنتن ها, gain را حداقل در 2 جهت در خود دارند- جهت ارسال اطلاعات و دریافت آن اگر می خواهید که با فواصل دور تماس بگیرید به یک آنتن با gain بالا و تمرکز محدود نیاز دارید

و بالعکس, اگر نیازی به ارتباط طولانی ندارید از آنتن با gain کم و تمرکز وسیع استفاده نمائید چندین نوع آنتن نیز وجود دارند که بصورت یکطرفه کار میکنند, زیرا ارتباط یک دستگاه ثابت را با دستگاه ثابت دیگر برقرار میکنند مرسوم ترین این نوع آنتن ها به عنوان پلی بیسیم میان این دو قرار میگیرد.

یک آنتن patch یا panel تمرکز زیادی دارد و تمرکز بستگی به اندازه ی پنل آن دارد. یک دیش نوع دیگری از آنتن است که ممکن است مورد استفاده قرار گیرد.

ولیکن تنها برای دستگاهایی بدرد میخورد که در یک مسیر معمولی انتقال را انجام میدهند, زیرا پشت دیش نمیتواند انتقالی انجام دهد برای تمامی مقاصد بهتر است از آنتن های چند جهته استفاده کنید زیرا تمرکز بالا و (gain) کوچکی دارد که به راحتی به کارت بیسیمتان وصل میشود بدون آنکه نیازی به منبع تغذیه ی اضافی داشته باشید در آدرس های زیر میتوانید تجهیزات صحیح برای war-driving را مشاهده نمائید:

hyperlinktech <http://www.hyperlinktech.com>

wireless central <http://www.wirelesscentral.net>

fleeman, anderson, and bird corporation

<http://www.fab-corp.com>

نرم افزار war-driving:

راه اندازی نرم افزار برای war-driving (w-d) قدری پیچیده است که این پیچیدگی بستگی به پیش نیاز های نصب نرم افزار و سخت افزار آن دارد .

از آنجا که نرم افزار w-d نیاز به یک یونیت Gps برای پیدا کردن موقعیت laptop دارد را اندازی آن میتواند به یک چالش تلقی شود . رانندگان متخصص مجاز هستند که یونیت یا واحد های GPS را که بسیار سودمند هستند برای انجام حملات پیاده سازی نمایند . این یک واقعیت است چرا که به شما اجازه میدهد تا Ap های آسیب پذیر را شناسائی نمائید و برای استفاده های آتی یا محکم سازی سیستم از آن ها استفاده کنید .

فن آوری بیسیم از چند کلمه ی مخفف استفاده میکند که عبارت است از:

1.SSID بعنوان شناسه ای (معرف) برای تشخیص یک AP از دیگری میباشد . مثلاً آن را مثل نام یک حوزه برای شبکه های بیسیم در نظر بگیرید

2. MAC آدرس عبارت از آدرسی یکتاست که برای شناسایی و معرفی هر گره در شبکه استفاده میشود. در محیط Wlan این آدرس می تواند بعنوان یک منبع برای کنترل دسترسی مشتریان بکار رود. 3. IV ای یا همان (initialization Vector) یک بسته Wep بعد از سرآمد یا همان عنوان لحاظ میشود و در ترکیب با کلید مخفی مشترک برای رمزگذاری بسته داده استفاده میشود.

Net Stumbler اولین برنامه war-driver می باشد که بعنوان ابزاری برای تجزیه و تحلیل سرآمد 802.11 و فیلدهای IV ای بسته ی بیسم استفاده میشود تا از آن طریق بتوان آدرس بسته ی MAC,SSID, نحوه ی استفاده از Wep, طول کلید Wep, محدوده ی سیگنال و فروشنده ی نقطه ی تماس را مشخص نمود. ابزار دیگری برای محیط لینوکس و یونیکس طراحی شده که اجازه شکستن قفل Wep و بسته ی اطلاعاتی واقعی را در اختیار تان قرار می دهد

Net Stumbler

وسیله ای برای انجام حمله در حرکت بوده و مبتنی بر ویندوز میباشد که شبکه های بیسیم را کشف کرده و موقعیت نسبی آنها را به کمک GPS معلوم میسازد این برنامه یک تقاضای واریسی 802.11 (Probe 802.11) برای آدرس مقصد پخش میکند

که باعث میشود تا تمام AP های واقع در آن ناحیه به این تقاضای واریسی پاسخ دهند که در خود اطلاعات پیکربندی شبکه را به همراه دارد و این اطلاعات شامل مواردی چون SSID و وضعیت WEP خواهد بود.

وقتی به یک GPS وصل شد, Net Stumbler برای بالاترین سیگنال قدرتمندی که به ازای هر AP پیدا کرده مختصات GPS را

ثبت میکند. با استفاده از شبکه و داده GPS, میتواند نقشه هایی از طریق stumb verter یا microsoft mappoint ایجاد نمائید. net stumbler از کارت هایی با چیپ hermes در ویندوز 2000 پشتیبانی می کند و معروف ترین آنها کارت هایی با مارک lucent, orinoco هستند .

در ویندوز xp کتابخانه ی شبکه سازی ndis5.1 قابلیت های 802.11 را در خود دارد که به برنامه ی Net Stumbler این اجازه را میدهد تا با بیشتر کارت هایی که از آن پشتیبانی می کنند از این کتابخانه استفاده کنند.

برای استفاده از NetStumbler کارت بیسیمتان را نصب کرده و برای SSID یا نام شبکه تان مقدار ANY را وارد کنید برای کارت های orinoco این مطلب را میتوان در یوتیلتی client manager پیدا کرد .

وارد کردن این کلمه در قسمت NETWROK Name به درایور میگوید که از یک ssid بطول صفر در درخواست های واریسی اش استفاده میکند بطور پیش فرض اکثر AP ها به درخواست های واریسی جواب میدهند که SSID ای بطول صفر را در خود داشته باشند به محض اینکه کارت را بدرستی پیکربندی نمودید برنامه NetStumbler را اجرا کنید و روی پیکان سبز رنگ در نوار ابزار (toolbar) کلیک کنید .

اگر AP هایی در آن ناحیه باشند که به تقاضای واریسی منتشره پاسخ دهند در پنجره برنامه ظا هر میشوند از فیلتر برنامه نیز میتوانید استفاده کنید .

Network Stumbler - [20050104190407.ns1]

File Edit View Device Window Help

Channels

SSIDs

0001E341FC6A

00022D08C995

00040E254017

0030F188D9BA

Crest

0001E30E608D

D-Link 614+

0080C803C01C

default

000D88A3700F

00904B1728DE

00904B668463

EDOTGROUP

0030AB2358CF

HOME

004005CB843A

Lederer

00032F22A704

Psalm119,114DubistmeinSchutzundm

000958C433F2

SW

000D88868155

WLAN

0030F19875A9

0030F1B042A5

0030F1E13A37

0030F1F10503

ZoRoNet

000272032257

Filters

| MAC | SSID | Chan | Speed | Vendor | Type | Encr... | SNR | Signal+ | Noise+ | SNR+ |
|--------------|----------------|------|---------|----------------|------|---------|-----|---------|--------|------|
| 000272032257 | ZoRoNet | 11 | 11 Mbps | CC&C | AP | | | -55 | -100 | 45 |
| 00904B1728DE | default | 6 | 11 Mbps | Gemtek | AP | | | -54 | -100 | 46 |
| 000D88868155 | SW | 6 | 22 Mbps | D-Link | AP | WEP | | -79 | -100 | 21 |
| 0030F1E13A37 | WLAN | 11 | 54 Mbps | Accton | AP | WEP | | -65 | -100 | 35 |
| 0030F19875A9 | WLAN | 13 | 11 Mbps | Accton | AP | | | -63 | -100 | 37 |
| 0030AB2358CF | EDOTGROUP | 12 | 11 Mbps | Delta (Netg... | AP | WEP | | -71 | -100 | 29 |
| 004005CB843A | HOME | 11 | 22 Mbps | D-Link | AP | WEP | | -79 | -100 | 21 |
| 0001E30E608D | Crest | 11 | 54 Mbps | | AP | WEP | | -71 | -100 | 29 |
| 00904B668463 | default | 6 | 11 Mbps | Gemtek | AP | | | -80 | -100 | 20 |
| 0080C803C01C | D-Link 614+ | 9 | 22 Mbps | D-Link | AP | WEP | | -52 | -100 | 48 |
| 00032F22A704 | Lederer | 6 | 54 Mbps | GST (Links... | AP | WEP | | -61 | -100 | 39 |
| 00022D08C995 | | 11 | 11 Mbps | Proxim (Age... | AP | WEP | | -76 | -100 | 24 |
| 0030F1B042A5 | WLAN | 11 | 54 Mbps | Accton | AP | WEP | | -77 | -100 | 23 |
| 0030F188D9BA | | 1 | 11 Mbps | Accton | AP | WEP | | -59 | -100 | 41 |
| 00040E254017 | | 8 | 11 Mbps | | AP | WEP | | -54 | -100 | 46 |
| 0030F1F10503 | WLAN | 11 | 54 Mbps | Accton | AP | | | -45 | -100 | 55 |
| 000D88A3700F | default | 11 | 22 Mbps | D-Link | AP | WEP | | -72 | -100 | 28 |
| 0001E341FC6A | | 11 | 54 Mbps | | AP | WEP | | -80 | -100 | 20 |
| 000958C433F2 | Psalm119,11... | 7 | 54 Mbps | Netgear | AP | | | -65 | -100 | 35 |

Ready 2 APs active GPS: Disabled 19

از آنجا که یک شبکه IBBS از گروهی از سیستم ها تشکیل شده که بدون یک AP کار میکنند و فرد خرابکار میتواند فقط به سیستم های درون آن شبکه دسن پیدا کند و ضرورتی ندارد که از شبکه بیسیم بعنوان پلی به lan داخلی استفاده نماید با انتخاب هر شبکه میتوانید شکا گرافیکی نسبت سیگنال به نویز (signal-to-noise) را مشاهده نمائید

اقدام مقابل در برابر NetStumbler:

ضعف اساسی در این برنامه این است که فقط به یک شکل از کشف شبکه بیسیم متکی است که آن هم درخواست و ارسی بخش است. فروشندگان تجهیزات بیسیم معمولاً گزینه ای برای غیرفعال ساختن ویژگی 802.11 ارائه میدهند که بطور موثری ایم برنامه را کور میکند. نرم افزار دیگری برای این نوع حملات نرم افزار kismet است که از این روش استفاده میکند اما مکانیزم های کشف دیگری دارد که در صورت مواجهه با شکست آن را سرپا نگه میدارد. این طور گفته شده که هیچ کمبودی در شبکه ها وجود ندارد که تا این برنامه آن ها را کشف کند و لیکن با این وجود ویژگی پاسخ برای تقاضای و ارسی پخشی هنوز هم توسط بسیاری از فروشندگان فعال گذاشته می شود.

kismet:

برای دریافت این برنامه به این سایت مراجعه کنید: (www.kismetwireless.net)

این برنامه یک پویشگر و اسنایفر بیسیم مبتنی بر BSD و لینوکس میباشد که قابلیت های حمله در حال حرکت را در خود دارد. این وسیله به شما این امکان را میدهد تا API های بیسیم و موقعیت GPS شان را پیگیری نمائید و قابلیت های بیشتری هم نسبت به NetStumbler دارد. kismet یک وسیله ی کشف شبکه ی غیرفعال است که کانال های بیسیم موجود را دور میزند و بدنبال بسته های 802.11 می گردد که حضور یک wlan را مشخص می سازد مثل درخواست های Beacons و Association.

این برنامه اطلاعات دیگری از جمله آدرس دهی ip و اسامی CID که به پروتکل کشف سیسکو مشهور است بدست می آورد. برنامه ی

دیگری که در این برنامه وجود دارد Gpsmap می باشد که یک نقشه از نتایج kismet را تولید می کند برای استفاده از kismet می بایستی درایور های سفارشی را خود ساخته را نصب کنید که برای نشان دادن حالت عملیات لازم می باشد این مورد می تواند بسته به نوع چیپ ست کارت بیسیم شبکه متفاوت باشد

| Name | T M Ch | Pkts | Flags | IP Range | Size |
|------------|--------|-------|-------|-------------|------|
| linksys | A N 06 | 224 F | | 192.168.1.1 | 0B |
| BRIDGE | A N 11 | 10 FM | | 10.1.1.95 | 371B |
| <no ssid> | H N — | 1 U | | 10.1.2.1 | 98B |
| linksys | A N 06 | 10 F | | 192.168.1.1 | 0B |
| linksys | A N 06 | 0 F | | 0.0.0.0 | 0B |
| linksys | A N 06 | 0 F | | 0.0.0.0 | 0B |
| GHOSTRIDER | A N 06 | 1 | | 0.0.0.0 | 0B |
| safewd | A Y 11 | 2 | | 0.0.0.0 | 0B |
| <no ssid> | A Y 06 | 1 | | 0.0.0.0 | 0B |
| 188ALT | A Y 06 | 141 | | 0.0.0.0 | 0B |
| 188ALT | A Y 06 | 19 | | 0.0.0.0 | 0B |
| 188ALT | A Y 11 | 24 | | 0.0.0.0 | 0B |
| 188ALT | A Y 06 | 48 | | 0.0.0.0 | 0B |
| orange | A Y 11 | 17 | | 0.0.0.0 | 0B |
| 188ALT | A Y 11 | 5 | | 0.0.0.0 | 0B |
| orange | A Y 06 | 19 | | 0.0.0.0 | 0B |
| 188ALT | A Y 11 | 14 | | 0.0.0.0 | 0B |
| 188ALT | A Y 06 | 92 | | 0.0.0.0 | 0B |
| 188ALT | A Y 11 | 38 | | 0.0.0.0 | 0B |
| 188ALT | A Y 06 | 3 | | 0.0.0.0 | 0B |
| 188ALT | A Y 01 | 2 | | 0.0.0.0 | 0B |
| 188ALT | A Y 06 | 2 | | 0.0.0.0 | 0B |
| linksys | A N 06 | 1 F | | 192.168.1.1 | 0B |
| tmbg | H N 10 | 0 | | 0.0.0.0 | 0B |
| tmbg | H N 10 | 0 | | 0.0.0.0 | 0B |
| tmbg | H N 10 | 5 | | 0.0.0.0 | 0B |
| tmbg | H N 10 | 6 | | 0.0.0.0 | 0B |
| tmbg | H N 10 | 8 | | 0.0.0.0 | 0B |
| ! tmbg | P N — | 3 | | 0.0.0.0 | 0B |
| tmbg | H N 10 | 3 | | 0.0.0.0 | 0B |
| tmbg | H N 10 | 6 | | 0.0.0.0 | 0B |
| . tmbg | H N 10 | 5 | | 0.0.0.0 | 0B |

| Info | |
|--------|----------|
| Ntwrks | 32 |
| Pckets | 786 |
| Cryptd | 0 |
| Weak | 0 |
| Noise | 22 |
| Discrd | 36 |
| Pkts/s | 1 |
| | |
| prism2 | |
| Ch: 10 | |
| | |
| Elapsd | 01:08:06 |

Status

```
Found new network "tmbg" bssid 02:06:7B:1B:42:94 WEP N Ch 10 @ 11.00 mbit
Found new network "tmbg" bssid 02:06:8F:1B:42:94 WEP N Ch 10 @ 11.00 mbit
Found new network "tmbg" bssid 02:06:78:1B:42:94 WEP N Ch 10 @ 11.00 mbit
Found new network "tmbg" bssid 02:06:72:1B:42:94 WEP N Ch 10 @ 11.00 mbit
Battery: 95% 2h24m0s
```


اما این نرم افزار یک روش منحصر بفرد در خود دارد که تمام آنها را برای مانیتور کردن عملیات فعال می سازد قبل از شروع برنامه kismet اسکریپت kismet_monitor اجرا کنید تا کارت خود را در حالت مانیتور قرار دهید مطمئن شوید که قبل از راه اندازی kismet مجوز دسترسی به دایرکتوری kismet را داشته باشید در مثال ما کارت بیسم را در

در این مثال کارت بیسیم را در فایل kismet.conf پیکربندی میکند و آن را در حالت مانیتورینگ قرار میدهد. به محض اینکه برنامه بار میشود، رابط هر شبکه ای که در محدوده ی مورد نظر واقع شده نشان می دهد بطور پیش فرض این برنامه شبکه ها را در حالت autofit مرتب مینماید که به شما اجازه نمی دهد از میان آن ها گام بردارید روی حرف s برای یافتن sort کلیک میکنیم و سپس یکی از گزینه هایش را انتخاب میکنیم پنجره ی اصلی نام شبکه یا SSID را نشان میدهد ستون T نوع شبکه را نشان میدهد W فعال و غیر فعال بودن WEP را نشان میدهد و CH بجای شمارهی کانال قرار میگیرد ستون محدوده ی IP هر آدرس IP که پیدا شده نشان میدهد.

اقدامات متقابل در برابر آن:

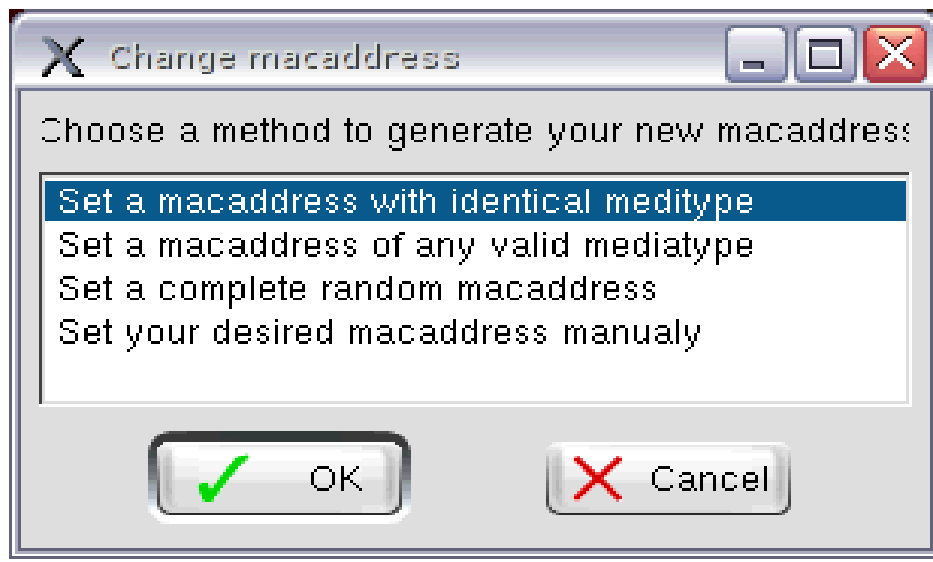
از آنجا که اقدامات متقابل زیادی در برابر آن وجود ندارد در حال حاضر بهترین وسیله برای این نوع حملات است در این برنامه علاوه بر قابلیت اکتشاف شبکه در آن این برنامه میتواند بطور اتوماتیک بسته های WEP را با نبود IV های جهت استفاده در AIRSNORT همراه با کشف IP ها برای استفاده در WLAN ثبت و گزارش می کند.

ChangeMac

یکی دیگر از نرم افزار های که برای هک کردن شبکه بی سیم دیگر موارد مورد استفاده هکرها قرار میگیرد نرم افزار مک چینج می باشد.

این نرم افزار را میتوانید از لینک زیر دانلود کنید:

<http://galeb.etf.bg.ac.yu/~azdaja/changemac.html>



شما میتوانید با 4 روش مک آدرس خود را تغییر دهید که به ترتیب:

1. ست کردن مک آدرس با یکسان نمودن نوع مد
2. ست کردن مک آدرس با نوع های معتبر مد
3. ست کردن مک آدرس برای عوض شدن تصادفی با مک آدرس های دیگر
4. مایل بودن برای ست کردن مک آدرس به صورت دستی