

به نام خدا

سازنده: سهراب نیازی

وب سایت: WwW.NiaziSoft.blogfa.CoM

ایمیل: NiaziSoft_Help@Yahoo.CoM

موضوع: امنیت در شبکه‌های بی‌سیم

امنیت در شبکه‌های بی‌سیم

اللَّهُمَّ احْمِزْ

از آن‌جا که شبکه‌های بی‌سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن‌ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به‌مدد پیکربندی صحیح می‌توان به‌سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این سری از مقالات با عنوان «امنیت در شبکه‌های بی‌سیم» ضمن معرفی این شبکه‌ها با تأکید بر ابعاد امنیتی آن‌ها، به روش‌های پیکربندی صحیح که احتمال رخداد حملات را کاهش می‌دهند بپردازیم.

شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط اموج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌ی چون شبکه‌های بی‌سیم سلولی - که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انواع ساده‌ی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده 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 این گونه شبکه‌ها و همچنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند: **WWAN**، **WLAN** و **WPAN**.

مقصود از **WWAN**، که مخفف **Wireless WAN** است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. **WLAN** پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های **WPAN** یا **Wireless Personal Area Network** برای موارد خانه‌گی است. ارتباطاتی چون **Bluetooth** و مادون قرمز در این دسته قرار می‌گیرند.

شبکه‌های **WPAN** از سوی دیگر در دسته‌ی شبکه‌های **Ad Hoc** نیز قرار می‌گیرند. در شبکه‌های **Ad hoc**، یک سخت‌افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، **Bluetooth** است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های **Ad hoc** با شبکه‌های محلی بی‌سیم (**WLAN**) در ساختار مجازی آن‌هاست. 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 کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون **Bluetooth**، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عمل کرد **Bluetooth** بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در

کامپیوترهای جیبی برتری قابل توجهی 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 به همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به حساب می‌آیند.

منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

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

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

- تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌ی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص

شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌ی را نیز موجب است.

- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌ی 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 کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل کرد شبکه نیز وجود دارد.

با مقدمه‌ی ذکر شده، در قسمت‌های آتی می‌توانیم به ویژه‌گی‌های این شبکه‌های، با تفکیک تکنولوژی‌های مرسوم، از بعد امنیتی پردازیم و چگونه‌گی پیکربندی صحیح یک شبکه‌ی بی‌سیم را، برای بالابردن امنیت آن، بررسی کنیم.

بخش دوم : شبکه‌های محلی بی‌سیم

در این قسمت، به‌عنوان بخش دوم از بررسی امنیت در شبکه‌های بی‌سیم، به مرور کلی شبکه‌های محلی بی‌سیم می‌پردازیم. اطلاع از ساختار و روش عمل‌کرد این شبکه‌ها، حتی به صورت جزئی، برای بررسی امنیتی لازم به‌نظر می‌رسد.

پیشینه

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 حالی که 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 نهایی شدن و معرفی آن نمی‌گذرد، بیش از یک سال 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.

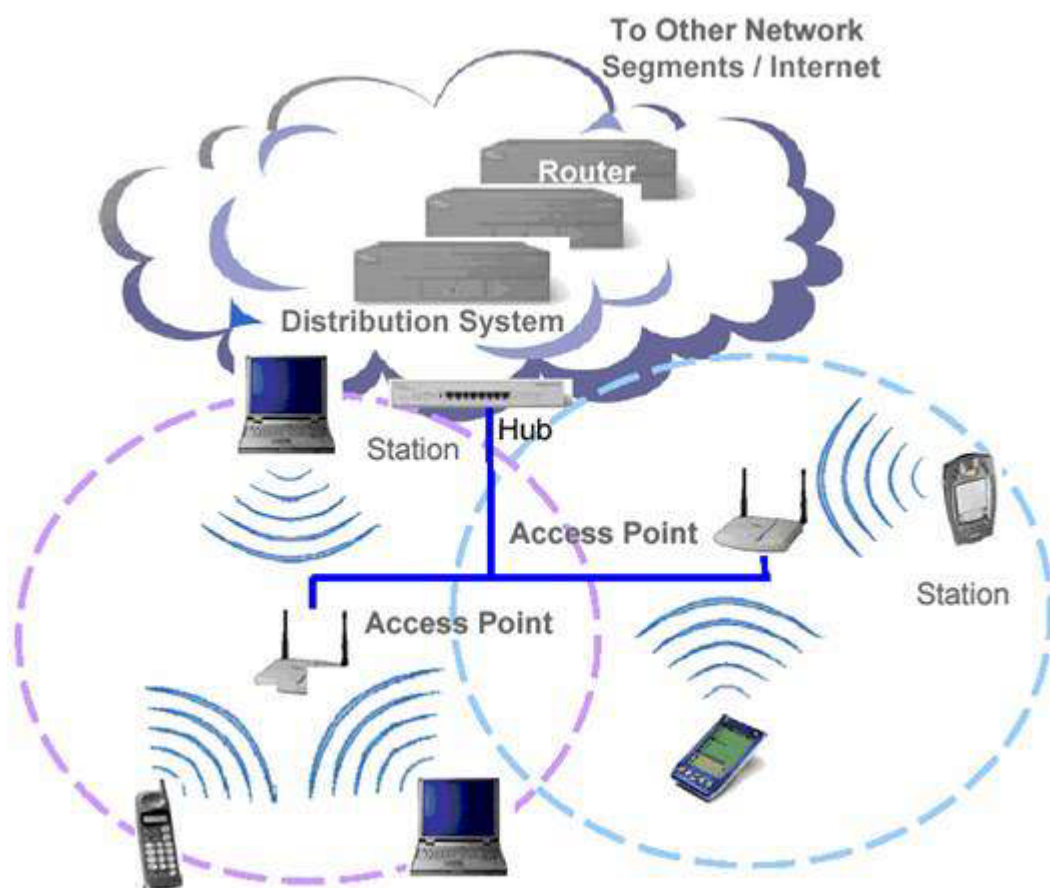
معماری شبکه‌های محلی بی‌سیم

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 به کار 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. گستره‌ی 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 شبکه‌ی 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

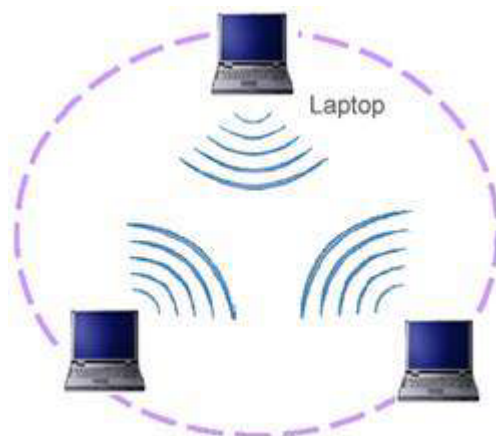
مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود. شکل زیر نمایی از این ساختار را نشان می‌دهد :



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.

در قسمت بعد، به دسته‌بندی اجزای فعال یک شبکه‌ی محلی بی‌سیم پرداخته و شعاع پوشش این دسته از شبکه‌ها را مورد بررسی قرار خواهیم داد.

بخش سوم : عناصر فعال و سطح پوشش WLAN

عناصر فعال شبکه‌های محلی بی‌سیم

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

- ایستگاه بی‌سیم

ایستگاه یا مخدوم بی سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه بی سیم به شبکه ی محلی متصل می شود. این ایستگاه می تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پوشش گر بارکد نیز باشد. در برخی از کاربردها برای این که استفاده از سیم در پایانه های رایانه یی برای طراح و مجری دردسرساز است، برای این پایانه ها که معمولاً در داخل کیوسک هایی به همین منظور تعبیه می شود، از امکان اتصال بی سیم به شبکه ی محلی استفاده می کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه ی بی سیم نیست.

کارت های شبکه ی 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.

- 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 سویچ 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 :

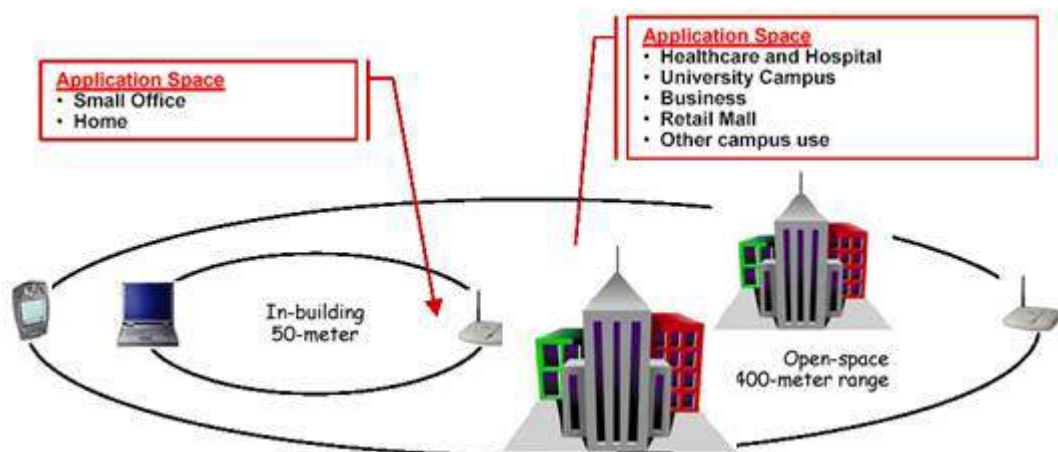
- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

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 این‌وجود 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 :



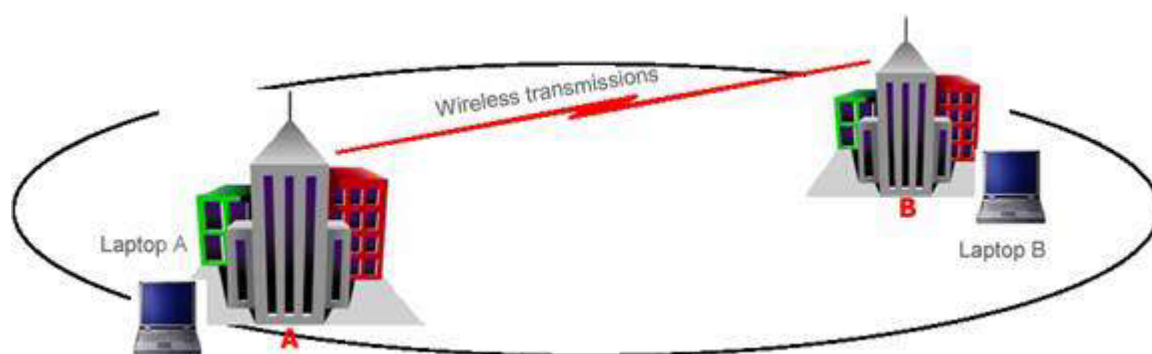
یکی از عملکردهای نقاط دسترسی به عنوان سویچهای بیسیم، عمل اتصال میان حوزههای بیسیم است. به عبارت دیگر با استفاده از چند سویچ بیسیم میتوان عملکردی مشابه Bridge برای شبکههای بیسیم را به دست آورد.

اتصال میان نقاط دسترسی میتواند به صورت نقطه به نقطه، 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 به‌دست آورد.

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



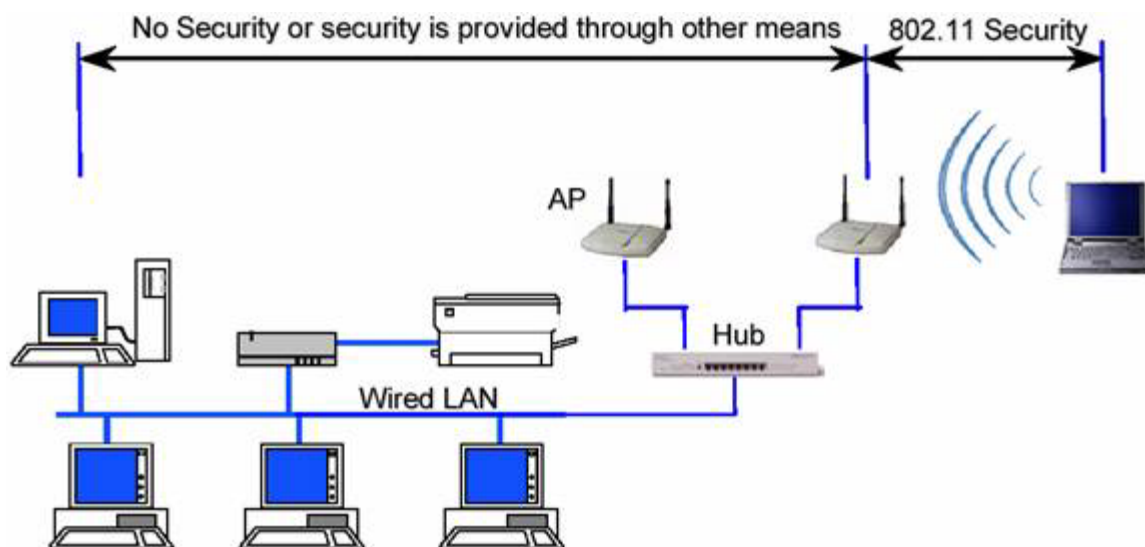
از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه‌های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دسترسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک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

در قسمت بعد به مزایای معمول استفاده از شبکه‌های محلی بی‌سیم و ذکر مقدماتی در مورد روش‌های امن سازی این شبکه‌ها می‌پردازیم.

بخش چهارم : امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

پس از آن که 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 مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 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

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

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

Integrity

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان 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 ارائه شده توسط این پروتکل است.

در قسمت‌های بعدی از بررسی امنیت در شبکه‌های محلی بی‌سیم به بررسی هریک از این سه سرویس می‌پردازیم.

بخش پنجم : سرویس‌های امنیتی WEP - Authentication

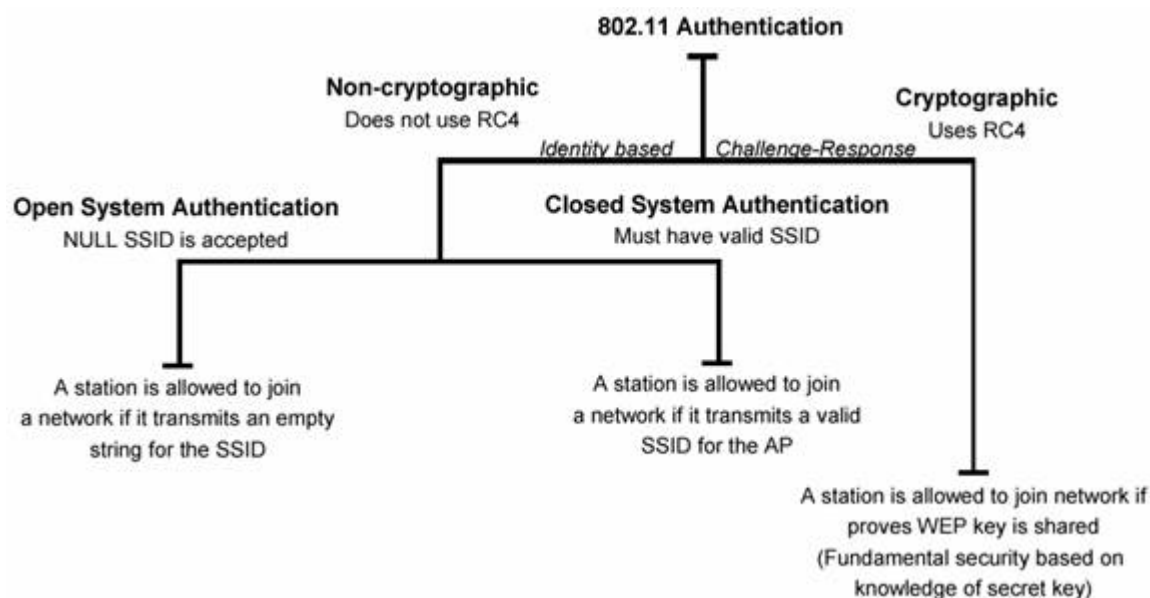
در قسمت قبل به معرفی پروتکل WEP که عملاً تنها روش امن‌سازی ارتباطات در شبکه‌های بی‌سیم بر مبنای استاندارد 802.11 است پرداختیم و در ادامه سه سرویس اصلی این پروتکل را معرفی کردیم.

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 رمزنگاری‌ست 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 رمزنگاری‌یی 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.

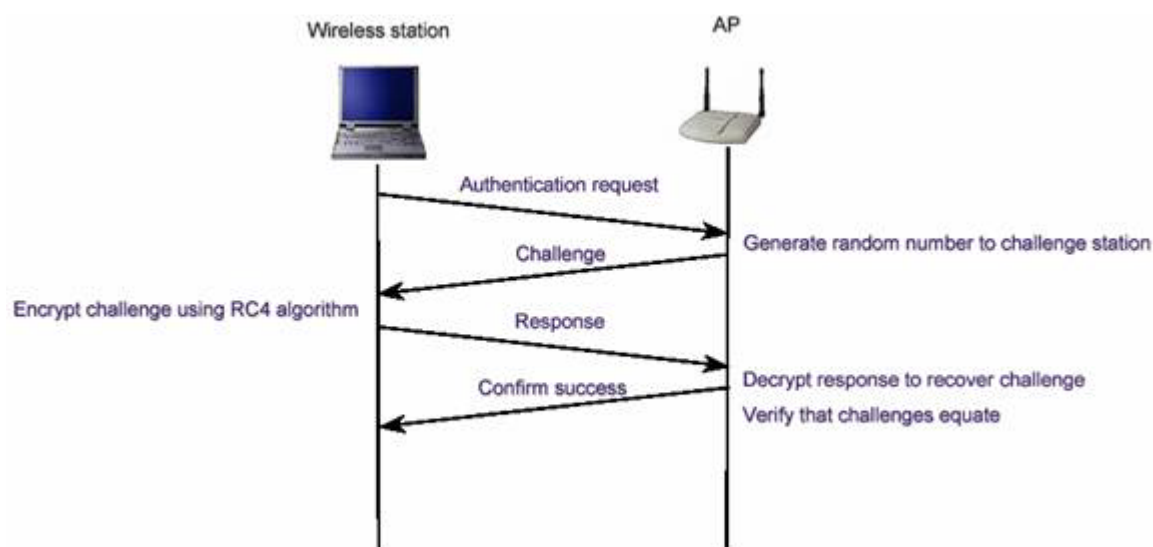
در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه‌ی اتصال به شبکه کفایت می‌کند. در واقع در این روش تمامی مخدوم‌هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می‌کنند با پاسخ مثبت روبه‌رو می‌شوند و تنها آدرس آن‌ها توسط نقطه‌ی دسترسی نگاه‌داری می‌شود. به‌همین دلیل به این روش NULL Authentication نیز اطلاق می‌شود.

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

نکته‌یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی‌ست که این روش در اختیار ما می‌گذارد. این دو روش عملاً روش امنی از احراز هویت را 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 شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم – که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخدادن حملات نیز خود تضمینی ندارد!

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 دسترسی است 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 رمزی است نقطه‌ی دسترسی اصلی است.

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 به‌گونه‌ی هریک از دو طرف را گمراه می‌کند.

در قسمت بعد به سرویس‌های دیگر پروتکل WEP می‌پردازیم.

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

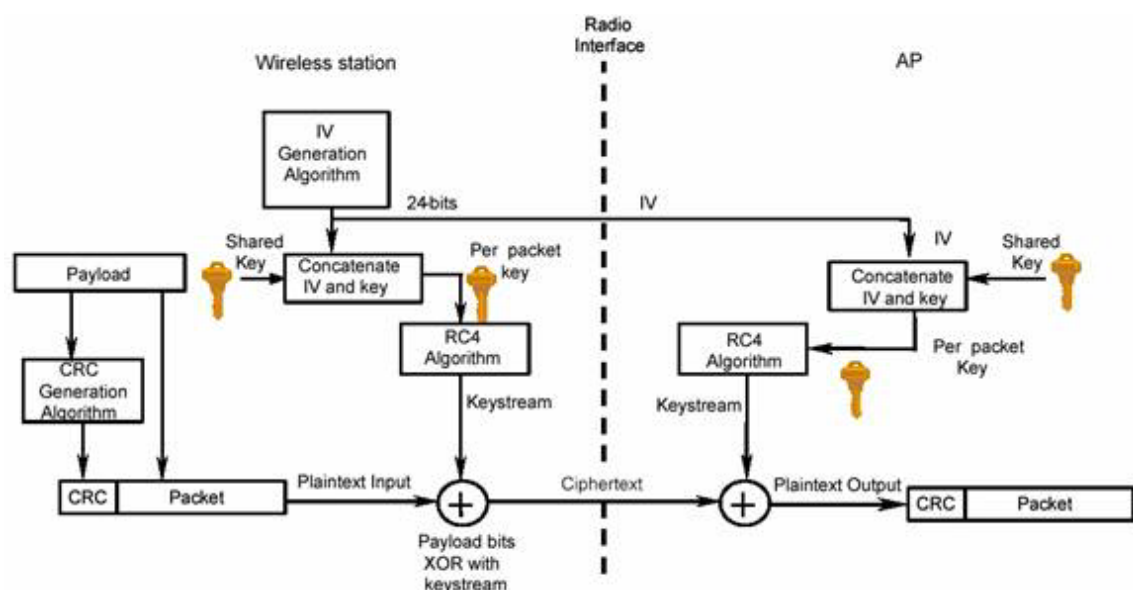
این سرویس که در حوزه‌های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می‌گردد به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره‌های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه‌گی عموماً از تکنیک‌های رمزنگاری استفاده می‌گردد، به گونه‌یی که در صورت شنود اطلاعات در حال تبادل، 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. به بیان 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 به اختصار WEP گفته می‌شود.

کلیدهای WEP اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌ی بالاست که قدرت پردازش سیستم‌های رایانه‌ی 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 نکته‌ی 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 مخدوم‌های بی‌سیم و نقاط دسترسی کم می‌شود. روش مورد نظر استفاده از یک کد CRC است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از 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 سهیل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرن دادن کلید به صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض

کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه های بی سیم ندارد. این مشکل از شبکه های بزرگ تر بیش تر خود را نشان می دهد. حتا با فرض تلاش برای جلوگیری از رخ داد چنین سهل انگاری هایی، زمانی که تعداد مخدوم های شبکه از حدی می گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گه گاه خطاهایی در گوشه و کنار این شبکه ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می شود.

در قسمت بعد به مشکلات و ضعف هایی که سرویس های امنیتی در استاندارد 802.11b دارند می پردازیم.

بخش هفتم : ضعف های اولیه ی امنیتی WEP

در قسمت های قبل به سرویس های امنیتی استاندارد 802.11 پرداختیم. در ضمن ذکر هریک از سرویس ها، سعی کردیم به ضعف های هریک اشاره یی داشته باشیم. در این قسمت به بررسی ضعف های تکنیک های امنیتی پایه ی استفاده شده در این استاندارد می پردازیم.

همان گونه که گفته شد، عملاً پایه ی 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 می شود، هرچند که برخی از تولیدکننده گان نگارش های خاصی از WEP را با کلیدهایی با تعداد بیت های بیش تر پیاده سازی کرده اند.

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 می شود. از آن جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گیرد بر اساس IV تولید می شود، محدوده IV عملاً نشان دهنده احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه های شلوغ به مشکلی حاد مبدل می شود. خصوصاً اگر از کارت شبکه ای استفاده شده مطمئن نباشیم. بسیاری از کارت های شبکه از IV های ثابت استفاده می کنند و بسیاری از کارت های شبکه ای یک تولید کننده واحد IV های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه ای شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی ست نفوذگر در مدت زمانی معین به ثبت داده های رمز شده شبکه بپردازد و IV های بسته های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IV های استفاده شده در یک شبکه ای شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم

از آن جایی که IV در تمامی بسته های تکرار می شود و بر اساس آن کلید تولید می شود، نفوذگر می تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IV ها و بسته های 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 آن جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می گردد.

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، به‌راحتی 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.

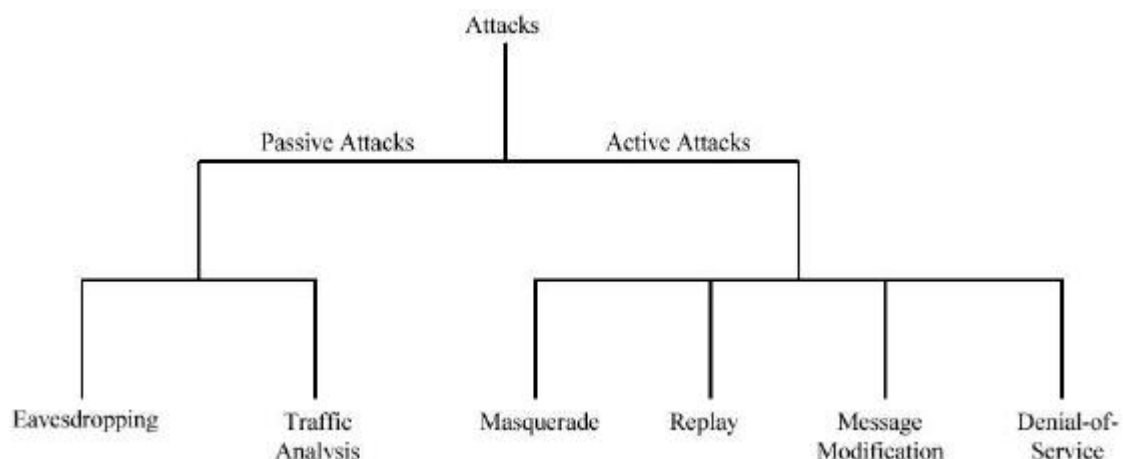
جدول زیر ضعف‌های امنیتی پروتکل WEP را به اختصار جمع‌بندی کرده است :

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 compromise 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.

قسمت هشتم : خطرهای، حملات و ملزومات امنیتی (بخش اول)

همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده یی 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، خطرهای 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 پردازیم، 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 کارانداختن خادم های نرم افزاری و سخت افزاری ست. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن 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. در قسمت بعدی به دسته بندی و شرح این ریسک ها و پیامدهای آن ها می پردازیم.