

باسمه تعالی

عنوان:

امنیت در شبکه های وای فای (Wi-Fi Security)



گردآورنده:

جواد حاجیان نژاد



تقدیم به مادر بزرگوارم که هر چه دارم از اوست...

چکیده

امروزه امنیت یکی از ضروری ترین مواردی است که در راه اندازی هر شبکه ای باید اعمال گردد. با گسترش شبکه های بی سیم (وای فای) و استفاده زیاد و عمومی شدن این شبکه ها، برقراری امنیت در آن یک امر مهم و ضروری می باشد. همانطور که راه اندازی این شبکه بی سیم بسیار راحت و اتصال به آن نیز بسیار سریع می باشد، به همین سادگی و سرعت نیز امکان رخنه در آن وجود دارد. امنیت در شبکه های وای فای که در کاربردهای نظامی، تجاری و سازمانی هستند به یکی از بزرگترین چالش های این شبکه ها تبدیل شده است و نشت هرگونه اطلاعات یا آسیب رسیدن به شبکه می تواند فاجعه انگیز باشد و گاهها جبران آن غیر ممکن باشد.

با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آن ها که به مدد پیکربندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت.

در این مجموعه سعی کرده ام که معرفی اجمالی از طریقه کار این شبکه ها و استانداردها و پروتکل های به کار رفته در آن بپردازم، سپس به معرفی مفاهیم و چالش های امنیتی موجود و راه حل آنها و در نهایت ارائه پروتکل ها و استانداردهای امنیتی در این شبکه ها بپردازم.

جواد حاجیان نژاد - مشهد مقدس

فهرست مطالب

۹	فصل اول : معرفی شبکه های وای فای
۱۰	۱-۱ شبکه های WI-FI چیست؟
۱۱	۲-۱ کاربردهای WI-FI
۱۲	۳-۱ دلایل رشد WI-FI
۱۴	۴-۱ ترکیب سیستم WI-FI با رایانه
۱۴	۵-۱ شبکه WI-FI چگونه کار می کنند؟
۱۵	۱-۶ تحلیل ترافیک شبکه های WI-FI
۱۸	۷-۱ آینده شبکه های WI-FI
۱۸	۸-۱ نتیجه گیری
۱۹	فصل دوم : استاندارد های شبکه محلی بی سیم
۲۰	۱-۲ معرفی
۲۳	۲-۲ معماری شبکه های محلی بی سیم
۲۳	۱-۲-۲ همبندی های ۸۰۲.۱۱
۲۵	۳-۲ خدمات ایستگاهی
۲۶	۴-۲ خدمات توزیع
۲۷	۵-۲ دسترسی به رسانه
۲۸	۵-۲-۱ الایه فیزیکی
۳۵	۶-۲ استاندارد 802.11B
۳۶	۶-۲-۱ اثرات فاصله
۳۶	۶-۲-۲ پل بین شبکه ای
۳۷	۷-۲ استاندارد 802.11A
۳۹	۸-۲ استاندارد بعدی IEEE 802.11G
۴۰	فصل سوم : مفاهیم امنیتی در شبکه های بی سیم
۴۱	۱-۳ فاکتور های امنیتی در شبکه های بی سیم
۴۳	۲-۳ سیستم تشخیص نفوذ
۴۶	۳-۳ چالش های امنیتی در شبکه های WI-FI
۴۷	۴-۳ نقاط آسیب پذیر و قابل نفوذ در شبکه های WI-FI
۵۰	۵-۳ امن سازی شبکه های بی سیم
۵۰	۵-۳-۱ حرراز هویت
۵۳	۵-۳-۲ امنیت داده ها

۵۴.....	۶-۳ مدیریت کلید ها
۵۵.....	۷-۳ صحت داده
۵۵.....	۸-۳ نتیجه گیری
۵۶.....	فصل چهارم: چالش های امنیتی و راه کارها در شبکه های وای فای
۵۷.....	۱-۴ مقدمه
۵۷.....	۲-۴ مشکل اول: دسترسی آسان
۵۸.....	۱-۲-۴ راه حل مشکل اول: تقویت کنترل دسترسی قوی
۵۹.....	۳-۴ مسأله دوم: نقاط دسترسی نامطلوب
۶۰.....	۱-۳-۴ راه حل مشکل دوم: رسیدگی های منظم به سایت
۶۱.....	۴-۴ مشکل سوم استفاده غیرمجاز از سرویس
۶۲.....	۱-۴-۴ راه حل مشکل سوم: طراحی و نظارت برای تأیید هویت محکم
۶۲.....	۵-۴ مشکل چهارم: محدودیت های سرویس و کارایی
۶۳.....	۱-۵-۴ راه حل مشکل چهارم: دیدبانی شبکه
۶۴.....	۶-۴ مشکل پنجم جعل MAC و SESSION ربایی!
۶۵.....	۱-۶-۴ راه حل شماره ۵: پذیرش پروتکل های قوی و استفاده از آنها
۶۵.....	۷-۴ مشکل ششم: تحلیل ترافیک و استراق سمع
۶۶.....	۱-۷-۴ راه حل مشکل ششم: انجام تحلیل خطر
۶۷.....	۸-۴ مشکل هفتم: حملات سطح بالاتر
۶۷.....	۱-۸-۴ راه حل مشکل هفتم: هسته را از LAN بی سیم محافظت کنید
۶۷.....	۹-۴ چند نکته در مورد امن سازی شبکه های وای فای
۷۹.....	۱۱-۴ جمع بندی
۸۱.....	فصل پنجم: پروتکل های امنیتی در شبکه های وای فای
۸۲.....	۱-۵ مقدمه
۸۲.....	۲-۵ پروتکل اتصال/دسترسی در شبکه های وای فای
۸۳.....	۳-۵ قابلیت ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱
۸۴.....	احراز هویت (Authentication)
۸۴.....	محرمانگی (Confidentiality)
۸۵.....	صحت (Integrity)
۸۵.....	۴-۵ خدمات ایستگاهی
۸۶.....	۱-۴-۵ احراز هویت Authentication
۸۶.....	۲-۴-۵ سرویس امنیت (Privacy یا confidentiality)
۸۸.....	۳-۴-۵ صحت (Integrity)
۸۹.....	۵-۵ ضعف های اولیه ای امنیتی WEP

۹۰.....	۱-۵-۵ استفاده از کلیدهای ثابت WEP
۹۰.....	Initialization Vector – IV ۲-۵-۵
۹۰.....	۳-۵-۵ ضعف در الگوریتم
۹۱.....	۴-۵-۵ استفاده از CRC رمز نشده
۹۴.....	۶-۵ پروتکل WPA(WI-FI PROTECTED ACCESS)
۹۶.....	۷-۵ پروتکل WPA2
۹۸.....	۸-۵ پروتکل امنیتی WPS
۹۹.....	۹-۵ جمع بندی
۱۰۰.....	مشکلات فعلی و کارهای آتی

مقدمه

شبکه های بی سیم (Wireless) یکی از تکنولوژی های جذابی هستند که توانسته اند توجه بسیاری را بسوی خود جلب نمایند و عده ای را نیز مسحور خود نموده اند. هرچند این تکنولوژی جذابیت و موارد کاربرد بالایی دارد ولی مهمترین مرحله که تعیین کننده میزان رضایت از آن را بدنبال خواهد داشت ارزیابی نیازها و توقعات و مقایسه آن با امکانات و قابلیت های این تکنولوژی است.

شبکه های WLAN را نمی توان جایگزینی برای شبکه های Ethernet معرفی کرده، بلکه شبکه های WLAN یک راه حل هستند برای مواقعی که امکان کابل کشی و استفاده از شبکه Ethernet امکانپذیر نیست و یا اولویت با Mobility و یا حفظ زیبایی محیط است. سالن های کنفرانس، انبارها، محیط های کارخانه ای، کارگاه های عمرانی و محیط های نمایشگاهی بهترین نمونه ها برای استفاده موثر از شبکه های WLAN میباشند.

شبکه های LAN به صورت ذاتی از شبکه های بی سیم امن تر می باشند، چرا که از نظر ساختاری قسمت عمده و یا تمام ساختار آنها در درون یک ساختمان قرار دارد و بدین دلیل از دسترسی های غیر مجاز در امان هستند. اما شبکه های بی سیم که با استفاده از امواج رادیویی فعالیت می کنند از آنجا که همانند شبکه های LAN دارای ساختاری فیزیکی نیستند، بیشتر در معرض نفوذ قرار داشته و آسیب پذیرترند، بنابراین مسئله امنیت به طور جدی در این شبکه ها مطرح می شود و گاهی مسائل و مشکلاتی امنیتی که در این شبکه ها وجود دارد، در شبکه های محلی سیمی وجود نداشته و باید دنبال راه کارها و پروتکل های امنیتی باشیم که در صدد رفع و برآورده کردن نیازهای امنیتی خاص این شبکه ها باشد.

اتصال بی سیم، یک رسانه فیزیکی است و برای تأمین امنیت آن نمی توان تنها به وجود یک دیوار آتش تکیه کرد. کاملاً واضح است که نقاط دسترسی غیرمجاز، به واسطه ایجاد راه های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آنها، نوعی تهدید علیه شبکه به شمار می روند. علاوه بر این نقاط دسترسی، باید نگران لپ تاپ های بی سیم متصل به شبکه سیمی نیز باشیم. یافتن لپ تاپ های متصل به شبکه سیمی که یک کارت شبکه بی سیم فعال دارند، اقدامی متداول برای ورود به شبکه محسوب می شود. در اغلب موارد این لپ تاپ ها توسط SSID شبکه هایی را که قبلاً مورد دسترسی قرار داده اند، جست و جو می کنند و در صورت یافتن آنها صرف نظر از این که اتصال به شبکه قانونی یا مضر باشد یا شبکه بی سیم در همسایگی شبکه فعلی قرار داشته باشد، به طور خودکار به آن وصل می شوند. به محض این که لپ تاپ به یک شبکه مضر متصل شود، مهاجمان آن را مورد حمله قرار داده و پس از اسکن و یافتن نقاط ضعف ممکن است کنترل آن را به دست گرفته و به عنوان میزبانی برای اجرای حمله ها به کار گیرند. در این شرایط علاوه

بر افشای اطلاعات مهم لپ‌تاپ، مهاجم می‌تواند از آن به عنوان نقطه شروعی برای حمله به شبکه سیمی استفاده کند. مهاجم در صورت انجام چنین اقداماتی، به‌طور کامل از دیواره آتش شبکه عبور می‌کند.

چنین نقطه ضعفی شبکه را به یک اسباب سرگرمی برای مهاجم تبدیل می‌کند. در حقیقت، نفوذ به چنین شبکه‌ای حتی نیازمند یک اسکن فعال یا حمله واقعی نیست. به واسطه ردیابی جریان اطلاعاتی یک شبکه بی‌سیم علاوه بر شناسایی توپولوژی بخش سیمی آن می‌توان اطلاعات مربوط به تجهیزات حیاتی شبکه و حتی گاهی اطلاعات مربوط به حساب‌های کاربری را به‌دست آورد.

با توجه به مطالب گفته شده در بالا نیاز به پروتکل‌ها و تدابیر امنیتی ویژه‌ای داریم که خاص این شبکه‌ها باشد و بتوان امنیت در این شبکه‌ها را تامین کرد. در این ادامه تکنیک‌ها و روش‌های امن سازی این شبکه‌ها و پروتکل‌ها و استانداردهای امنیتی موجود را بررسی می‌کنیم.

فصل اول : معرفی شبکه های وای فای

Chapter One: Introduction Wi-Fi Networks

مراجع: [1],[2]

۱-۱ شبکه های Wi-Fi چیست؟

وای-فای (Wi-Fi)، مخفف عبارت Wireless Fidelity است و استاندارد از زیرمجموعه Bluetooth است و تحت آن ارتباطی با قدرتی بیشتر از خود Bluetooth ایجاد خواهد شد. ارتباط Wi-Fi بیشتر بر پایه ارتباط شبکه اینترنت به صورت بی سیم تاکید می کند و همین امر باعث محبوبیت بسیار زیاد آن شده است با استفاده از این تکنولوژی به راحتی در مسافرت، هواپیما و یا هتل می توان از طریق Laptop به اینترنت متصل شد. Wi-Fi، که همان استاندارد IEEE802.11 است در مدل های 802.11a و 802.11b مورد استفاده قرار می گیرد و استاندارد اصلی آن IEEE 802.11b است. در این مدل حداکثر سرعت انتقال اطلاعات ۱۱ مگابیت بر ثانیه است و از فرکانس رادیویی ۲/۴ گیگاهرتز استفاده می کند. برای سرعت بخشیدن به این استاندارد مدل دیگری نیز به نام 802.11b+ ایجاد شده که سرعت انتقال را تا ۲۲ مگابیت بر ثانیه افزایش می دهد. در مدل 802.11a سرعت اطلاعات حدود ۵۴ مگابیت بر ثانیه است و از فرکانس ۵۰ گیگاهرتز استفاده می شود. به طور حتم این مدل در آینده ای نه چندان دور جای 802.11b را خواهد گرفت.

شبکه های ارتباطی بدون سیم همواره از امواج رادیویی استفاده می کنند. در این شبکه ها یک قطعه رایانه ای، اطلاعات را تبدیل به امواج رادیویی می نماید و آنها را از طریق آنتن ارسال می کند. در طرف دیگر یک روتر بدون سیم، با دریافت سیگنال های فوق و تبدیل آنها به اطلاعات اولیه، داده ها را برای رایانه قابل فهم خواهد ساخت.

به زبانی ساده، سیستم Wi-Fi را می توان به یک جفت واکی - تاکی که شما از آن برای مکالمه با دوستان خود استفاده می کنید تشبیه نمود. این لوازم، رادیوهای کوچک و ساده ای هستند که قادرند تا سیگنال های رادیویی را ارسال و دریافت نمایند. هنگامی که شما بوسیله آنها صحبت می کنید، میکروفون دستگاه، صدای شما را دریافت نموده و با تلفیق آن با امواج رادیویی، از طریق آنتن آنها را ارسال می کند. در طرف دیگر، دستگاه مقصد، با دریافت سیگنال ارسال شده از طرف شما توسط آنتن، آنها را آشکار سازی نموده و از طریق بلندگوی دستگاه، صدای شما را پخش خواهد کرد. توان خروجی و یا قدرت فرستنده این گونه لوازم اغلب در حدود یک چهارم وات است و با این وصف، برد آنها چیزی در حدود ۵۰ تا ۱۰۰ متر می رسد.

حال فرض کنید بخواهید میان دو کامپیوتر به صورت یک شبکه و آن هم به شکل بدون سیم (همانند واکی - تاکی) ارتباط برقرار سازید. مشکل اساسی در این راه آن است که این لوازم از آن رو که جهت

انتقال صوت ساخته شده اند، از نرخ سرعت انتقال کمی برخوردار هستند و نمی توانند حجم بالایی از داده ها را در زمان کوتاه منتقل کنند.

رادیوهایی که در سیستم Wi-Fi مورد استفاده قرار می گیرند، همانند مثال پیشین قابلیت ارسال و دریافت را دارا می باشند اما تفاوت اصلی آنها در این است که این رادیو ها قادر هستند تا اطلاعات به شکل صفر و یک دیجیتالی را به حالت امواج رادیویی تبدیل نمایند و سپس منتقل کنند.

در کل سه تفاوت عمده میان رادیوهای سیستم Wi-Fi و رادیوهای وای - تاکی معمولی وجود دارد که به شرح زیر است:

(۱) رادیوهای سیستم Wi-Fi با استاندارد های 802.11b و 802.11g کار می کنند و عمل ارسال و دریافت را بر روی فرکانس های ۲.۴ گیگاهرتزی و یا ۵ گیگاهرتزی انجام می دهند. اما وای - تاکی های مذکور بر روی فرکانس ۴۹ مگاهرتزی کار می کنند.

(۲) رادیوهای سیستم Wi-Fi از انواع مختلفی از تکنیک های کدگذاری اطلاعات بهره می برند که نتیجه آن افزایش نرخ سرعت تبادل داده ها خواهد بود. این روشها برای استاندارد 802.11a و 802.11g شامل تکنیک OFDM و برای استاندارد 802.11b، شامل CCK می باشد.

(۳) رادیو هایی که در سیستم Wi-Fi مورد استفاده قرار می گیرند، قابلیت تغییر فرکانس را دارا هستند. مزیت این ویژگی در آن است که موجب جلوگیری از ایجاد تداخل کار سیستم های مختلف Wi-Fi در نزدیکی هم می شود.

۲-۱ کاربردهای Wi-Fi

تکنولوژی Wi-Fi علاوه بر استفاده در ارتباط رایانه های شخصی در اتصال به اینترنت، به صورت بی سیم امکان استفاده از هر شبکه دیگری را نیز دارد. به عنوان نمونه در تلفن های همراه نسل جدید امکان اتصال به اینترنت از طریق Wi-Fi فراهم شده است. همچنین به عنوان راه حلی مؤثر به منظور توسعه شبکه های داخلی، بدون صرف هزینه سیم کشی مطرح شده است. دو تکنولوژی Wi-Fi و Bluetooth به عنوان رقبای یکدیگر در شبکه های بی سیم مطرح شده اند و هم اکنون نیز رقابت آنها در حال افزایش است، اما هدف این دو فناوری یکسان نبوده و هر کدام هدف جداگانه ای را در پیش گرفته اند.

بلوتوث برای استفاده در شبکه های بی سیم کوچک در نظر گرفته شده است که دارای مصرف پائین برق و برد کوتاه تری است اما Wi-Fi برای استفاده در شبکه های بی سیم متوسط با برد و پهنای باند وسیع تری مطرح شده است. تکنولوژی Wi-Fi در باندهای رادیویی ۲.۴ و ۵ گیگاهرتز فعال است و می تواند

سرعتی در حدود ۱۱Mbps تا ۵۴Mbps داشته باشد، اما در مقابل Bluetooth تنها سرعتی در حدود ۷۲۰kbps را دارد. علاوه بر مواردی که در بالا به آن اشاره شد سرویس VOIP، انتقال صدا از طریق تکنولوژی اینترنت، که امکان برقراری تماس تلفنی روی شبکه های رایانه ای را مقدور می سازد نیز از Wi-Fi بهره می گیرد. با استفاده از Dual Mode Telephony دستگاه های تلفن همراه نیز قادر خواهند بود با استفاده از تکنولوژی Wi-Fi تماس هایی با کیفیت تکنولوژی سلولی را برقرار سازند و بدین ترتیب شما هم امکان اتصال به اینترنت را روی گوشی خود و هم امکان مکالمه تلفنی را خواهید داشت.

۳-۱ دلایل رشد Wi-Fi

شبکه های مبتنی بر Wi-Fi راه موفقیت و پیشرفت را در پیش گرفته است. تعداد کاربران تکنولوژی Wi-Fi که در سال ۲۰۰۰ در حدود ۲/۵ میلیون نفر بود اکنون به ۱۸ میلیون کاربر رسیده است و می رود تا مسیر رشد و پیشرفت خود را ادامه دهد، از مهم ترین دلایل رشد تکنولوژی Wi-Fi می توان به موارد زیر اشاره کرد:

۱- پشتیبانی شرکت های مختلف: شرکت های بزرگ و معتبری همچون مایکرو سافت، اینتل، سیسکو و آی بی ام بشدت مشغول کار روی تکنولوژی Wi-Fi هستند و سرمایه گذاری های هنگفتی نیز در این زمینه انجام داده اند به عنوان نمونه شرکت اینتل سیصد میلیون دلار برای توسعه صنعت Wi-Fi بر روی Centrino سرمایه گذاری کرده است.

۲- توسعه ارتباطات باند پهن: استفاده از فناوری Wi-Fi سبب توسعه شبکه های باندپهن شده است به گونه ای که در سال جاری حدود ۳۰ درصد رشد در زمینه باندپهن مشاهده شده است.

۳- شبکه های بزرگ ملی: هم اکنون در برخی از کشورهای دنیا شبکه های بزرگ و ملی Wi-Fi در حال فعالیت هستند به عنوان نمونه در کشور آمریکا چهار شبکه voice stream, cometa Networks, Toshiba و Boingo مشغول سرویس دهی به کاربران هستند.

۴- تجهیزات آماده: شرکت های تولیدکننده سخت افزار در سال های اخیر همراه با سخت افزارهای خود لوازم و متعلقات مورد نیاز سیستم های Wi-Fi را نیز به صورت آماده در اختیار مشتریان قرار می دهند و دیگر نیازی به تهیه این وسایل از بازارهای رایانه به صورت جداگانه وجود ندارد. هم اکنون شرکت های Dell, Toshiba, TIVO و ... در رایانه ها و قطعات تولیدی خود تکنولوژی Wi-Fi را گنجانده اند.

۵- گسترش شبکه: پیشگامان صنعت Wi-Fi در همه نقاط دنیا بشدت در حال توسعه شبکه ها هستند، به عنوان نمونه در پارک ها، رستوران ها، اماکن تفریحی و گردشگری این تکنولوژی به چشم می خورد.

۶ - کاهش قیمت ها: هم اکنون قیمت تجهیزات Wi-Fi در نقاط مختلف دنیا سیر نزولی را آغاز کرده است و به نصف کاهش یافته است و همین کاهش قیمت ها سبب گرایش بیشتر افراد به سوی تکنولوژی Wi-Fi خواهد شد.

۷- نوآوری های بیشتر: تکنولوژی Wi-Fi به دلیل تازه وارد بودن به سرعت در حال پیشرفت است. شرکت های اینتل و Mash Networks در حال ساخت آنتن هایی هستند که نسبت به آنتن های فعلی محدوده بیشتری را پوشش می دهد به علاوه شرکت های سازنده گوشی تلفن همراه نیز در حال ساخت گوشی هایی با امکانات Wi-Fi می باشند.

۸- هزینه: تجهیزات مورد استفاده در شبکه های کابلی نسبت به تجهیزات مورد استفاده در شبکه های بی سیم ارزان تر است اما با توجه به رشد روزافزون شبکه های بی سیم قیمت تجهیزات آن نیز در حال کاهش است.

۹- کارایی: شبکه های کابلی دارای بالاترین کارایی هستند، ابتدا پهنای باند ۱۰Mbps در این شبکه ها رواج داشت اما با گذشت زمان این سرعت به پهنای باند ۱۰۰Mbps و سپس ۱۰۰۰Mbps افزایش یافت. هم اکنون سوئیچ هایی با پهنای باند ۱Gbps در بازار وجود دارد. اما در مقابل شبکه های بی سیم با استاندارد 802.11b و حداکثر ۱۱Mbps و با استاندارد 802.11a پهنای باندی در حدود ۵۴Mbps دارد و در استانداردهای جدید این سرعت به ۱۰۸Mbps افزایش یافته است. علاوه بر فاکتور سرعت و پهنای باند، فاصله نیز از ملاک های مهم در سرعت ارسال داده ها در شبکه ها می باشد. با توجه به این که فناوری Wi-Fi به فاصله حساس می باشد و تنها در فواصل زیر یکصد متر قابل به سرویس دهی می باشد، نباید از این تکنولوژی در فواصل بالای یکصد متر و یا در مکان هایی که موانع فیزیکی دارد استفاده کرد.

۱۰- اطمینان پذیری: شبکه های کابلی در مقابل شبکه های بی سیم از اطمینان بیشتری برخوردار هستند اما در موقع راه اندازی باید تجهیزات را به درستی نصب کرد تا در آینده مشکلی در سرویس دهی شبکه به وجود نیاید، به علاوه تجهیزات بی سیم مشکلات خاص خود مانند قطع شدن های پیاپی، تداخل امواج الکترومغناطیسی - تداخل با شبکه های بی سیم مجاور و غیره را دارند که روند رو به رشد آن بیانگر بهبود ضعف ها و کمبودها در شبکه است.

۱۱- امنیت: در شبکه های کابلی به دلیل firewall امنیت بیشتری وجود دارد در حالی که در شبکه های بی سیم به دلیل استفاده از هوا به عنوان بستری برای انتقال اطلاعات، بدون داشتن تکنیک خاصی برای رمزنگاری و نیز رمزگشایی اطلاعات، امنیت اطلاعات به خطر می افتد و لزوم به کارگیری تکنیک های رمزنگاری (WEP (wired Equivalent privacy) سبب افزایش امنیت اطلاعات در این شبکه ها می شود.

۴-۱ ترکیب سیستم Wi-Fi با رایانه

امروزه اغلب رایانه های لپ تاپ مجهز به سیستم Wi-Fi داخلی هستند و در غیر این صورت نیازمند نصب یک کارت Wi-Fi بر روی لپ تاپ و یا رایانه رومیزی خود خواهیم بود. شما می توانید یک کارت Wi-Fi در سیستم 802.11a یا 802.11b و یا 802.11g تهیه کنید که البته نوع 802.11g نسبت به تجهیزات 802.11b از سرعت بالاتری برخوردار است. برای لپ تاپ ها این تجهیزات در قالب کارت های PCMCIA که در محل مخصوص خود نصب می شوند و یا به صورت اتصال خارجی از طریق یک درگاه USB عرضه می شوند.

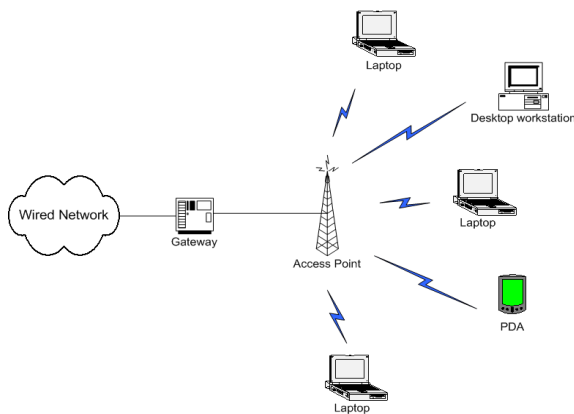
برای رایانه های رومیزی، می توانید از کارت های PCI و یا درگاه USB برای این منظور استفاده کنید. پس از نصب این تجهیزات کاربر قادر است تا در مکان هایی که اینترنت به شکل بدون سیم ارائه می شود با داشتن یک اشتراک، از خدمات بهره گرفته و به شبکه متصل شود.

۵-۱ شبکه Wi-Fi چگونه کار می کنند؟

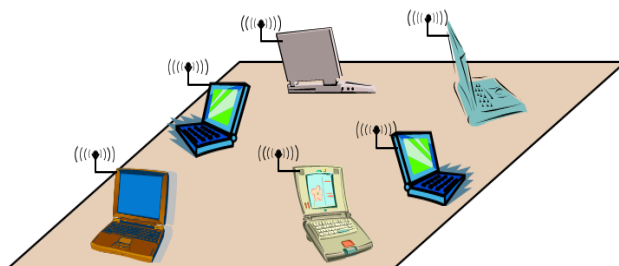
دو نوع مد عملیات برای برقراری ارتباطات، در این استاندارد وجود دارد، حالت دارای زیر ساخت^۱ و حالت بدون زیر ساخت یا موردی^۲. در حالت دارای زیر ساخت یک کدام از نود های شرکت کننده در شبکه به عنوان نقطه دسترسی عمل می کند و سایر نود ها برای ارتباط با یک دیگر، ابتدا باید با نقطه دسترسی ارتباط برقرار کنند، در حالت بدون زیر ساخت هیچ گونه نود مرکزی و نقطه دسترسی وجود ندارد و نود ها برای ارتباط با یک دیگر به طور مستقیم عمل می کنند و احتمالاً از نود های دیگر نیز می توانند برای کمک در مسیر یابی استفاده کنند. نمونه ای از این شبکه ها در تصاویر ۱.۱ و ۱.۲ نشان داده شده است.

^۱ Infrastructure-based

^۲ Ad hoc



شکل ۱.۱: ساختار شبکه های بی سیم در حالت دارای زیر ساخت



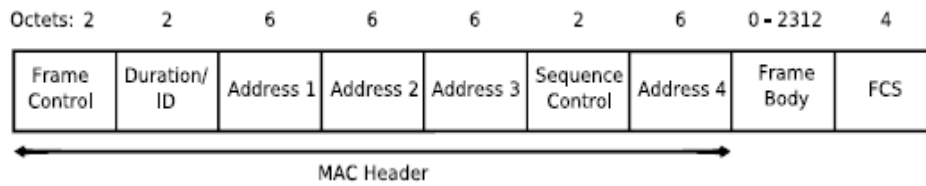
شکل ۱.۲: ساختار شبکه های بی سیم در حالت بدون زیر ساخت

برای پشتیبانی ارتباطات بی سیم کلاینت ها و نقطه دسترسی شامل یک رادیو و آنتن می باشند، ایده اصلی مورد استفاده در استاندارد IEEE802.11 برای شناسایی و ارتباطات ایستگاه ها با یک دیگر استفاده از فریم هایی به نام Beacon و Request/ Release می باشد، فریم های Beacon در هر ثانیه ده بار توسط نقطه دسترسی به تمام ایستگاه ها ارسال می شود و به این ترتیب نقطه دسترسی خود را به ایستگاه ها معرفی می کند و آنها قادر خواهند بود به راحتی نقطه دسترسی را شناسایی کنند، همچنین ایستگاه ها یا کلاینت ها با ارسال فریم های Broadcast به نام probe Broadcast خود را به نقطه دسترسی معرفی می کنند و نقطه دسترسی نیز در پاسخ به آن ایستگاه یک فریم پاسخ به ایستگاه ارسال می کند که به عنوان تصدیقی برای شناسایی آن ایستگاه از جانب نقطه دسترسی محسوب می شود.

۶-۱ تحلیل ترافیک شبکه های Wi-Fi

هر بسته انتقالی در شبکه های Wi-Fi شامل بیت های می شود که در لایه های مختلف برای ارتباطات استفاده می شود، هر چند که ممکن است بسته ها در این نوع شبکه ها رمز نگاری شوند، ولی همیشه دارای هدر های هستند که رمز نمی شوند، در نتیجه هدر بسته ها برای همه قابل دسترس خواهد بود و

مهاجمین قادرند که ترافیک شبکه را آنالیز کنند. تمام بسته ها در شبکه های Wi-Fi با ساختار بسته های MAC مطابقت می کنند، ساختار قاب های MAC در شکل ۱.۳ نمایش داده شده است.



شکل ۳.۱: ساختار قاب MAC

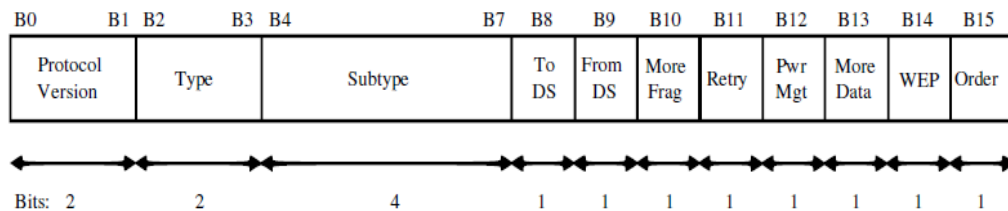
فیلد Frame Control برای مشخص کردن نوع داده بسته به کار می رود، به طور کلی سه نوع داده و تعداد بسیار زیادی زیر نوع وجود دارد که در زیر لیت شده است:

۱. مدیریتی: Association, Probe, Beacon, Authentication.

۲. کنترلی: RTS, CTS, PS-Poll, ACK, CF-Ack/Poll.

۳. داده: Data, Data + CF-Ack/Poll and Null-function.

در شکل زیر ساختار بیتی فیلد Frame Control نمایش داده شده است:



شکل ۴.۱: ساختار فیلد frame control

اگر شبکه قسمتی از شبکه های بی سیم توزیع شده باشد (WDS) ^۳ آنگاه:

$$\text{FromDS} = 1 \text{ و } \text{ToDS} = 1$$

اگر شبکه در مد موردی یا بدون زیر ساخت باشد آنگاه:

$$\text{ToDS} = 0, \text{ FromDS} = 0, \text{ Type} = \text{Data}$$

اگر شبکه در مد دارای زیر ساخت باشد آنگاه:

$$\text{ToDS} = 1, \text{ FromDS} = 0, \text{ Type} = \text{Data}$$

به طور کلی پنج نوع آدرس در این بسته ها ممکن است به کار روند که عبارتند از:

آدرس مقصد (DA): گیرنده نهایی بسته را مشخص می کند.

آدرس مبدا (SA): گیرنده ابتدایی بسته را مشخص می کند

آدرس دریافت کننده (RA): آدرس نقطه دسترسی گیرنده بعدی بسته را مشخص می کند.

آدرس انتقال دهنده (TA): آدرس نقطه دسترسی قبلی که بسته را فرستاده است، مشخص می کند.

شناسه BSS: نقطه دسترسی را در یک BSS مشخص می کند

نحوه قرار گیری این آدرس ها بسته مقادیر فیلد های ToDS و FromDS می باشد که در شکل زیر نمایش داده شده است.

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	n/a
0	1	DA	BSSID	SA	n/a
1	0	BSSID	SA	DA	n/a
1	1	RA	TA	DA	SA

شکل ۵.۱: فیلد های آدرس در فریم MAC

هر فریم دریافتی شامل قدرت سیگنال دریافتی می باشد که توسط رادیوی گیرنده محاسبه می شود که از ترکیب این اطلاعات با اطلاعات GPS می توان برای به دست آوردن محدوده شبکه، محل قرارگیری نقطه دسترسی و به دست آوردن محل کلاینت مورد استفاده قرار گیرد. اطلاعات تحلیلی به دست آمده از فریم های دریافت شده در شکل زیر دسته بندی شده است:

Fact	Frame	Requirements
WDS	Data	1 frame
Ad-hoc/Infrastructure	Beacon/Probe/Data	1 frame
Network range	Any	3 frames and GPS
Client/Access point location	Any	3 frames and GPS
WEP	Beacon/Probe/Data	1 frame
WPA	Beacon/Probe/Data	1 frame
SSID	Beacon/Probe	1 frame
Access point MAC address	Any	1 frame
Client MAC address	Probe Request/Data	1 frame
Wired client MAC address	Data	1 frame
Contents of data	Data	Intelligent guess

شکل ۶.۱: اطلاعات قابل دسترس از تحلیل بسته های WI-Fi

۷-۱ آینده شبکه های Wi-Fi

WiMAX استاندارد دیگری است که توسط IEEE 802.16 مطرح شده و ارتباطات بی سیم تا شعاعی در حدود ۵۰ کیلومتر و پهنای باندی حدود ۷۰Mbps را فراهم میکند. این یک تکنولوژی جدید، بسیار مؤثر و کارا بوده و قدم بزرگتری بر فراز WiFi است.

آنچه بنظر می رسد آنست که بزودی شاهد موبایل هایی مجهز به تکنولوژی WiFi در فروشگاه ها خواهیم بود. این تکنولوژی فرصتهای کاری جدید بسیاری را برای اپراتورهای موبایل و سازنده های گوشی موبایل ایجاد خواهد کرد.

سرویس هایی نظیر VoIP, Push Email و IMS و ... همه نسبت به آنچه احتمالاً اکنون ارائه می شوند ارزانتر خواهند شد و میزان بازده و کارایی این تکنولوژی می تواند ترافیک شبکه های موبایل را کاهش دهد.

۸-۱ نتیجه گیری

با توجه به تمامی ویژگی های مثبت شبکه های Wi-Fi و امکاناتی خوبی که به ارمغان می آورد باید توجه داشت که راه اندازی یک شبکه بی سیم بسیار راحت و سریع امکانپذیر است ولیکن به همین سادگی و سرعت نیز امکان رخنه در آن وجود دارد. روش های مختلفی جهت امن سازی این شبکه های توسعه داده شده که با صرف کمی وقت میتوان یکی از این روش ها را بکار برد تا از سوء استفاده و یا صدمه جلوگیری شود.

با توجه محدود بودن پهنای باند شبکه های بی سیم کد های مخرب مخصوصاً کرم های اینترنتی (Worm) بسادگی میتوانند در صورت ورود به شبکه Access Point را بدلیل بار مضاعف مختل کنند. حتماً در شبکه های بی سیم هر چند کوچک از وجود برنامه های آنتی ویروس و بروز بودن آنها باید مطمئن بود. بسیار اوقات حرکت Wormها باعث از کار افتادگی Access Point و اصطلاحاً Hang کردن آن میشود که ممکن است در برداشت اولیه خراب بودن Access Point منبع مشکل تشخیص داده شود.

شبکه های بی سیم حداقل با مشخصات فعلی یک راه حل هستند برای شرایطی که در آن امکان استفاده از Ethernet و کابل کشی وجود ندارد و نه یک جایگزین Ethernet، بکارگیری از شبکه های بی سیم در کنار شبکه Ethernet برای کاربران Mobile که ممکن است هر لحظه با Laptop و یا PDA خود از گرد راه برسند و یا سالن کنفرانس و اجتماعات همواره بسیار سودمند و رضایت بخش خواهد بود. همچنین امکانی که بصورت موقتی برپا شده اند نظیر پروژه های عمرانی و حتی برنامه های نظامی و نمایشگاه ها و دفاتر استیجاری نیز در فهرست موارد کاربرد شبکه های بی سیم قرار دارند.

۲ فصل دوم : استاندارد های شبکه محلی بی

سیم

Chapter Two: The 802.11 Standard Defined

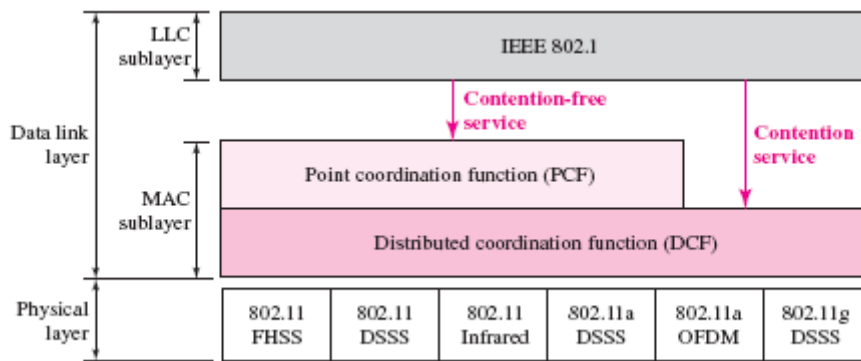
مراجع: [3],[4],[5],[6],[7],[8]

۱-۲ معرفی

امروزه با بهبود عملکرد، کارایی و عوامل امنیتی، شبکه های بیسیم به شکل قابل توجهی در حال رشد و گسترش هستند و استاندارد IEEE 802.11 استاندارد IEEE 802.11 استاندارد بنیادی است که شبکه های بیسیم بر مبنای آن طراحی و پیاده سازی می شوند. در ماه ژوئن سال ۱۹۹۷ انجمن مهندسان برق و الکترونیک (IEEE) استاندارد IEEE 802.11-1997 را به عنوان اولین استاندارد شبکه های محلی بیسیم منتشر ساخت. این استاندارد در سال ۱۹۹۹ مجدداً بازنگری شد و نگارش روز آمد شده آن تحت عنوان IEEE 802.11-1999 منتشر شد. استاندارد جاری شبکه های محلی بیسیم یا همان IEEE 802.11 تحت عنوان ISO/IEC 8802-11:1999 توسط سازمان استاندارد سازی بین المللی (ISO) و مؤسسه استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال ۱۹۹۷، شکل گیری و پیدایش شبکه سازی محلی بیسیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد ۱۹۹۷، پهنای باند ۲Mbps را تعریف می کند با این ویژگی که در شرایط نامساعد و محیط های دارای اغتشاش (نویز) این پهنای باند می تواند به مقدار ۱Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند ۱Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط های عاری از اغتشاش (نویز) پهنای باند ۲Mbps نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی ۲.۴ 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 ۸۰۲.۱۱ به زیر گروه های متعددی تقسیم می شود. 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

شکل زیر گروه های کاری در لایه فیزیکی در استاندارد ۸۰۲.۱۱ را نمایش می دهد.



شکل ۲.۱: جایگاه استاندارد ۸۰۲.۱۱

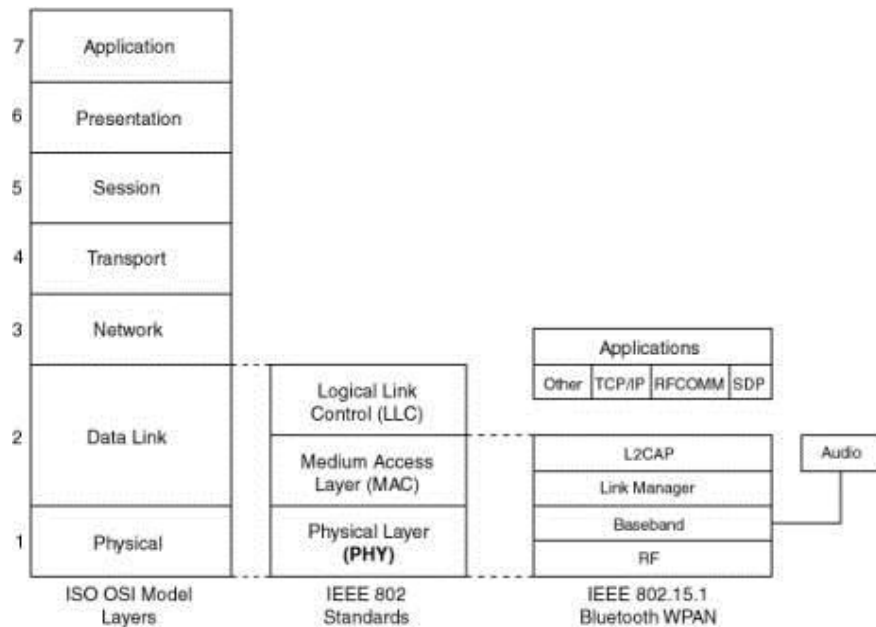
کمیته ۸۰۲.۱۱ e کمیته ای است که سعی دارد قابلیت QoS اترنت را در محیط شبکه های بیسیم ارائه کند. توجه داشته باشید که فعالیت های این گروه تمام گونه های ۸۰۲.۱۱ شامل a, b, و g را در بر دارد. این کمیته در نظر دارد که ارتباط کیفیت سرویس سیمی یا Ethernet QoS را به دنیای بی سیم بیاورد.

کمیته ۸۰۲.۱۱ g کمیته ای است که با عنوان ۸۰۲.۱۱ توسعه یافته نیز شناخته می شود. این کمیته در نظر دارد نرخ ارسال داده ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یا باند فرکانسی صنعتی، پژوهشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده ۲۴۰۰ مگاهرتز تا ۲۴۸۳.۵ مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهای تشعشع رادیویی نیازی به مجوز ندارد. استاندارد ۸۰۲.۱۱ g تا کنون نهایی نشده است و مهم ترین علت آن رقابت شدید میان تکنیک های مدولاسیون است. اعضای این کمیته و سازندگان تراشه توافق کرده اند که از تکنیک تسهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می تواند به عنوان یک روش جایگزین و رقیب مطرح باشد.

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

فعالیت دو کمیته ۸۰۲.۱۱ i و ۸۰۲.۱۱ x در ابتدا بر روی سیستم های مبتنی بر ۸۰۲.۱۱ b تمرکز داشت. این دو کمیته مسئول تهیه پروتکل های جدید امنیت هستند. استاندارد اولیه از الگوریتمی موسوم به WEP استفاده می کند که در آن دو ساختار کلید رمز نگاری به طول ۴۰ و ۱۲۸ بیت وجود دارد. WEP مشخصاً یک روش رمز نگاری است که از الگوریتم RC4 برای رمز نگاری فریم ها استفاده می کند. فعالیت این کمیته در راستای بهبود مسائل امنیتی شبکه های محلی بیسیم است.

این استاندارد لایه های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بیسیم را در بر دارد. شکل ۲.۲ جایگاه استاندارد ۸۰۲.۱۱ را در مقایسه با مدل مرجع نشان می دهد.



شکل ۲.۲: مقایسه استاندارد ۸۰۲.۱۱ با استاندارد مرجع OSI

محیط های بیسیم دارای خصوصیات و ویژگی های منحصر به فردی می باشند که در مقایسه با شبکه های محلی سیمی جایگاه خاصی را به این گونه شبکه ها می بخشد. به طور مشخص ویژگی های فیزیکی یک شبکه محلی بیسیم محدودیت های فاصله، افزایش نرخ خطا و کاهش قابلیت اطمینان رسانه، همبندی های پویا و متغیر، تداخل امواج، و عدم وجود یک ارتباط قابل اطمینان و پایدار در مقایسه با اتصال سیمی است. این محدودیت ها، استاندارد شبکه های محلی بیسیم را وا می دارد که فرضیات خود را بر پایه یک ارتباط محلی و با برد کوتاه بنا نهد. پوشش های جغرافیایی وسیعتر از طریق اتصال شبکه های محلی بیسیم کوچک برپا می شود که در حکم عناصر ساختمانی شبکه گسترده هستند. سیار بودن ایستگاه های کاری بیسیم نیز از دیگر ویژگی های مهم شبکه های محلی بیسیم است. در حقیقت اگر در یک شبکه محلی بیسیم ایستگاه های کاری قادر نباشند در یک محدوده عملیاتی قابل قبول و همچنین میان سایر شبکه های بیسیم تحرک داشته باشد، استفاده از شبکه های محلی بیسیم توجیه کاربردی مناسبی نخواهد داشت.

از سوی دیگر به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر استانداردها، لایه دسترسی به رسانه (MAC) در استاندارد ۸۰۲.۱۱ می بایست از دید لایه های بالاتر مشابه یک شبکه محلی مبتنی بر استاندارد ۸۰۲ عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیار بودن ایستگاه های کاری را به گونهای شفاف پوشش دهد که از دید لایه های بالاتر استاندارد این سیار بودن احساس نشود. این نکته سبب می شود که لایه MAC در این استاندارد وظایفی را بر عهده بگیرد که معمولاً توسط لایه های بالاتر شبکه انجام می شوند. در واقع این استاندارد لایه های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه می کند و به طور مشخص لایه فیزیکی جدید از فرکانس های رادیویی به عنوان رسانه انتقال بهره می برد.

۲-۲ معماری شبکه های محلی بی سیم

معماری ۸۰۲.۱۱ از عناصر ساختمانی متعددی تشکیل شده است که در کنار هم، سیار بودن ایستگاه های کاری را پنهان از دید لایه های فوقانی برآورده می سازد. ایستگاه بیسیم یا به اختصار ایستگاه (STA)، بنیادی ترین عنصر ساختمانی در یک شبکه محلی بیسیم است. یک ایستگاه، دستگاهی است که بر اساس تعاریف و پروتکل های ۸۰۲.۱۱ (لایه های MAC و PHY) عمل کرده و به رسانه بیسیم متصل است. توجه داشته باشید که براساس تعریف کلاسیک شبکه های کامپیوتری، یک شبکه کامپیوتری مجموعه ای از کامپیوترهای مستقل و متصل است که منظور از اتصال در این تعریف، توانایی جابجایی و مبادله پیام ها است. ایستگاه های کاری بیسیم امروزی عمدتاً به صورت مجموعه سخت افزاری/نرم افزاری کارت های شبکه بیسیم پیاده سازی می شوند. همچنین یک ایستگاه می تواند یک کامپیوتر قابل حمل، کامپیوتر جیبی و یا یک نقطه دسترسی باشد. نقطه دسترسی در واقع در حکم پلی است که ارتباط ایستگاه های بیسیم را با سیستم توزیع یا شبکه سیمی برقرار می سازد. کوچکترین عنصر ساختمانی شبکه های محلی بیسیم در استاندارد ۸۰۲.۱۱ مجموعه سرویس پایه یا BSS نامیده می شود. در واقع BSS مجموعه ای از ایستگاه های بیسیم است.

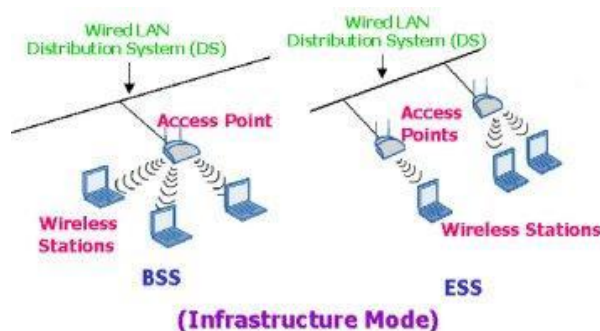
۱-۲-۲ همبندی های ۸۰۲.۱۱

در یک تقسیم بندی کلی می توان دو همبندی را برای شبکه های محلی بیسیم در نظر گرفت. ساده ترین همبندی، فی البداهه (Ad Hoc) و براساس فرهنگ واژگان استاندارد ۸۰۲.۱۱، IBSS است. در این همبندی ایستگاه ها 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 نمی کنند. واضح است که در این همبندی به سبب محدودیت های فاصله هر ایستگاهی ضرورتاً نمی تواند با تمام ایستگاه های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در همبندی IBSS آن است که ایستگاه ها در محدوده عملیاتی بیسیم یا همان برد شبکه بیسیم قرار داشته باشند. شکل ۲.۳ همبندی IBSS را نشان می دهد.



شکل ۲.۳: ساختار شبکه در حالت موردی

همبندی دیگر زیرساختار است. در این همبندی عنصر خاصی موسوم به نقطه دسترسی وجود دارد. نقطه دسترسی ایستگاه های موجود در یک مجموعه سرویس را به سیستم توزیع متصل می کند. در این همبندی تمام ایستگاه ها با نقطه دسترسی تماس می گیرند و اتصال مستقیم بین ایستگاه ها وجود ندارد در واقع نقطه دسترسی وظیفه دارد فریم ها (قاب های داده) را بین ایستگاه ها توزیع و پخش کند. شکل ۲-۲ همبندی زیرساختار را نشان می دهد.



شکل ۲.۴: همبندی زیرساختار در دو گونه BSS و ESS

در این همبندی سیستم توزیع، رسانه ای است که از طریق آن نقطه دسترسی (AP) با سایر نقاط دسترسی در تماس است و از طریق آن می تواند فریم ها را به سایر ایستگاه ها ارسال نماید. از سوی دیگر می تواند بسته ها را در اختیار ایستگاه های متصل به شبکه سیمی نیز قرار دهد. در استاندارد ۸۰۲.۱۱ توصیف ویژه ای برای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین می کند که سیستم توزیع می بایست ارائه نماید. بنابراین سیستم توزیع می تواند یک شبکه ۸۰۲.۳ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم می کند.

استاندارد ۸۰۲.۱۱ با استفاده از همبندی خاصی محدوده عملیاتی شبکه را گسترش می دهد. این همبندی به شکل مجموعه سرویس گسترش یافته (ESS) بر پا می شود. در این روش یک مجموعه گسترده و متشکل از چندین BSS یا مجموعه سرویس پایه از طریق نقاط دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیک داده بین مجموعه های سرویس پایه مبادله شده و انتقال پیام ها شکل می گیرد. در این همبندی ایستگاه ها می توانند در محدوده عملیاتی بزرگ تری گردش نمایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم می شود. در واقع سیستم توزیع ستون فقرات شبکه های محلی بیسیم است و می تواند با استفاده از فناوری بیسیم یا شبکه های سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان یک لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش می باشد. نکته

قابل توجه در این همبندی آن است که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه های سیار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت یک شبکه منفرد در سطح لایه MAC تلقی می کنند. به این ترتیب پروتکل های رایج شبکه های کامپیوتری کوچکترین تأثیری از سیار بودن ایستگاه ها و رسانه بیسیم نمی پذیرند. جدول ۲.۱ همبندی های رایج در شبکه های بیسیم مبتنی بر ۸۰۲.۱۱ را به اختصار جمع بندی می کند.

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

جدول ۲.۱: همبندی های رایج در استاندارد ۸۰۲.۱۱

۳-۲ خدمات ایستگاهی

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

Open System Authentication -

Shared Key Authentication -

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می کند. ایستگاه گیرنده نیز فریمی در پاسخ می فرستد که آیا فرستنده را می شناسد یا خیر. روش دوم کمی پیچیده تر است و فرض می کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سری دریافت کرده است. ایستگاه های کاری با استفاده از این کلید مشترک و با بهره گیری از

پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می نمایند. 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 می گردد.

در یک شبکه بی سیم، تمام ایستگاه های کاری و سایر تجهیزات قادر هستند ترافیک داده های را "بشنوند" - در واقع ترافیک در بستر امواج مبادله می شود که توسط تمام ایستگاه های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بیسیم را تحت تأثیر قرار می دهد. به همین دلیل در استاندارد ۸۰۲.۱۱ پروتکلی موسوم به WEP تعیبه شده است که بر روی تمام فریم های داده و برخی فریم های مدیریتی و هویت سنجی اعمال می شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء و پوشش را معادل با شبکه های سیمی نماید.

۴-۲ خدمات توزیع

خدمات توزیع عملکرد لازم در همبندی های مبتنی بر سیستم توزیع را مهیا می سازد. معمولاً خدمات توزیع توسط نقطه دسترسی فراهم می شوند. خدمات توزیع در این استاندارد عبارتند از:

- پیوستن به شبکه

- خروج از شبکه بی سیم

- پیوستن مجدد

- توزیع

- مجتمع سازی

سرویس اول یک ارتباط منطقی میان ایستگاه سیار و نقطه دسترسی فراهم می کند. هر ایستگاه کاری قبل از ارسال داده می بایست با یک نقطه دسترسی بر روی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می دهد که فریم های ارسال شده به سمت ایستگاه سیار را به درستی در اختیارش قرار دهد. خروج از شبکه بیسیم هنگامی بکار می رود که بخواهیم اجباراً ارتباط ایستگاه سیار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی سیم" است با این تفاوت که در این سرویس ایستگاه سیار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می کند که با نقطه دسترسی قبلی تماس گرفته و فریم

های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیار فرستاده شده اند. با استفاده از سرویس توزیع فریم های لایه MAC به مقصد مورد نظرشان می رسند. مجتمع سازی سرویسی است که شبکه محلی بیسیم را به سایر شبکه های محلی و یا یک یا چند شبکه محلی بیسیم دیگر متصل می کند. سرویس مجتمع سازی فریم های ۸۰۲.۱۱ را به فریم هایی ترجمه می کند که بتوانند در سایر شبکه ها (به عنوان مثال ۸۰۲.۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم های سایر شبکه ها نیز به فریم های ۸۰۲.۱۱ ترجمه شده و از طریق امواج در اختیار ایستگاه های کاری سیار قرار می گیرند.

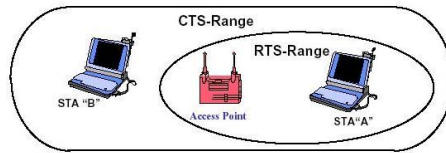
۲-۵ دسترسی به رسانه

روش دسترسی به رسانه در این استاندارد CSMA/CA است که تاحدودی به روش دسترسی CSMA/CD شباهت دارد. در این روش ایستگاه های کاری قبل از ارسال داده کانال رادیویی را کنترل می کنند و در صورتی که کانال آزاد باشد اقدام به ارسال می کنند. در صورتی که کانال رادیویی اشغال باشد با استفاده از الگوریتم خاصی به اندازه یک زمان تصادفی صبر کرده و مجددا اقدام به کنترل کانال رادیویی می کنند. 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 می کند. گیرنده فیلد کنترلی فریم یا همان CRC را چک می کند و سپس یک فریم تصدیق می فرستد. دریافت تصدیق به این معنی است که تصادمی بروز نکرده است. در صورتی که فرستنده این تصدیق را دریافت نکند، مجددا فریم را ارسال می کند. این عمل تا زمانی ادامه می یابد که فریم تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم ها به تعداد آستان های مشخصی برسد که پس از آن فرستنده فریم را دور می اندازد.

در شبکه های بیسیم بر خلاف اترنت امکان شناسایی و آشکار سازی تصادم به دو علت وجود ندارد:

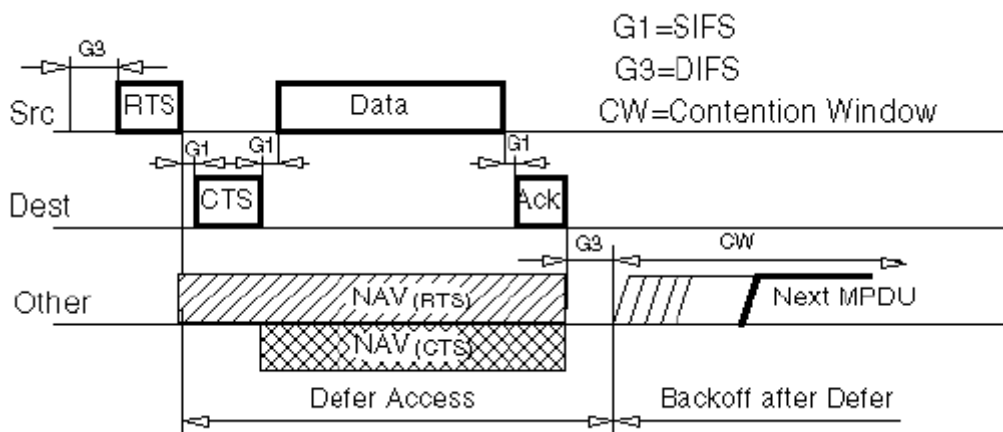
پیاده سازی مکانیزم آشکار سازی تصادم به روش ارسال رادیویی دوطرفه نیاز دارد که با استفاده از آن ایستگاه سیار بتواند در حین ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می شود.

در یک شبکه بی سیم، بر خلاف شبکه های سیمی، نمی توان فرض کرد که تمام ایستگاه های سیار امواج یکدیگر را دریافت می کنند. در واقع در محیط بیسیم حالتی قابل تصور است که به آنها نقاط پنهان می گوئیم. در شکل زیر ایستگاه های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.



شکل ۲.۵: روزه ها پنهان

برای غلبه بر این مشکل، استاندارد ۸۰۲.۱۱ از تکنیکی موسوم به اجتناب از تصادم و مکانیزم تصدیق استفاده می کند. همچنین با توجه به احتمال بروز روزه های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به شنود مجازی رسانه یا VCS استفاده می شود. در این روش ایستگاه فرستنده ابتدا یک بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می فرستد. هنگامی که گیرنده این فریم را دریافت می کند، رسانه را کنترل می کند و در صورتی که رسانه آزاد باشد فریم کنترلی CTS را به نشانی فرستنده ارسال می کند. تمام ایستگاه هایی که فریم های کنترلی RTS/CTS را دریافت می کنند وضعیت کنترل رسانه خود موسوم به شاخص NAV را تنظیم می کنند. در صورتی که سایر ایستگاه ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می کنند که مرتبا به صورت پویا تغییر می کند. به این ترتیب مشکل روزه های پنهان حل شده و تصادم ها نیز به حداقل مقدار می رسند. شکل ۲-۴ زمان بندی RTS/CTS و وضعیت سایر ایستگاه ها را نشان می دهد.



شکل ۲.۶: زمان بندی RTS/CTS

۲-۵-۱ لایه فیزیکی

در این استاندارد لایه فیزیکی سه عملکرد مشخص را انجام می دهد. اول آنکه رابطی برای تبادل فریم های لایه MAC جهت ارسال و دریافت داده ها فراهم می کند. دوم اینکه با استفاده از روش های تسهیم فریم های داده را ارسال می کند و در نهایت وضعیت رسانه (کانال رادیویی) را در اختیار لایه بالاتر (MAC) قرار می دهد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر می باشند:

۱. استفاده از تکنیک رادیویی DSSS

۲. استفاده از تکنیک رادیویی FHSS

۳. استفاده از امواج رادیویی مادون قرمز

در این استاندارد لایه فیزیکی می تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ ۱ یا ۲ مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون ۱۶-PPM و ۴-PPM مبادله می شوند.

۲-۵-۱-۱ ویژگی های سیگنال های طیف گسترده

عبارت طیف گسترده به هر تکنیکی اطلاق می شود که با استفاده از آن پهنای باند سیگنال ارسالی بسیار بزرگ تر از پهنای باند سیگنال اطلاعات باشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیک مطرح می شود 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 ویژگی های جالب توجه سیگنال های طیف گسترده نهفته است. این ویژگی های عبارتند از:

۱. مصونیت بالا در مقابل پارازیت و تداخل

۲. رسایی با تفکیک پذیری و دقت بالا

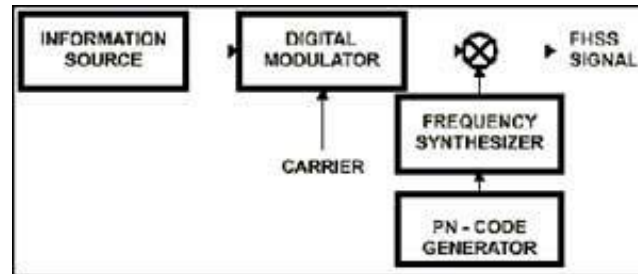
۳. امکان استفاده در CDMA

۴. 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 می رسد.

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

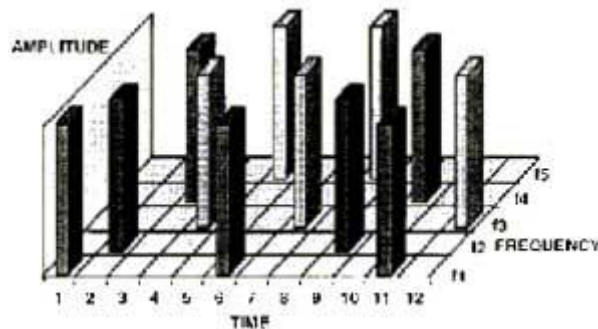
۲-۱-۵-۲ سیگنال های طیف گسترده با جهش فرکانسی

در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می کند. شکل ۲-۵ این تکنیک را در قالب یک نمودار نشان می دهد.



شکل ۲.۷: تکنیک PN-CODE= Pseudonoise code FHSS

در این شکل سیگنال اطلاعات با استفاده از یک تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگ تری در مقایسه با سیگنال اطلاعات انتخاب می شود. با توجه به اینکه فرکانس های pn-code با استفاده از یک ثبات انتقالی همراه با پس خور ساخته می شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملاً تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می گوئیم.



شکل ۲.۸: تغییر فرکانس سیگنال تسهیم شده به شکل شبه تصادفی

بر اساسی مقررات FCC و سازمان های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی ۴۰۰ میلی ثانیه است که برابر با حداقل ۲.۵ جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد ۸۰۲.۱۱ حداقل فرکانس جهش در آمریکای شمالی و اروپا ۶ مگاهرتز و در ژاپن ۵ مگاهرتز می باشد.

۳-۱-۵-۲ سیگنال های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال بر روی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کد به گونه ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یک کد تسهیم می شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می گردد. در این استاندارد ۸۰۲.۱۱ روش مدولاسیون مورد استفاده در سیستم های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تسهیم می شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.

از آنجا که در استاندارد ۸۰۲.۱۱ و سیستم DSSS از روش تسهیم DPSK استفاده می شود، داده های خام به صورت تفاضلی تسهیم شده و ارسال می شوند و در گیرنده نیز یک آشکار ساز تفاضلی سیگنال های داده را دریافت می کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال های داده تغییر می کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت های داده تغییر می کند. جدول زیر ایده مدولاسیون فاز را نشان می دهد.

Symbols	Bits	Phase Modulation
1	00	$A \sin(\omega t + \theta_1)$
2	01	$A \sin(\omega t + \theta_2)$
3	10	$A \sin(\omega t + \theta_3)$
4	11	$A \sin(\omega t + \theta_4)$

شکل ۲.۹: مدولاسیون فاز

در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می گیرند و چهار نماد را پدید می آورند. 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 می شوند. به عنوان مثال در روش $\pi/4$ -DQPSK، چهار مقدار تغییر فاز $\pi/4$ ، $3\pi/4$ ، $\pi/4$ ، $3\pi/4$ و $-\pi/4$ است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می تواند دو بیت را کدگذاری 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

شکل ۲.۱۰: مدولاسیون تفاضلی

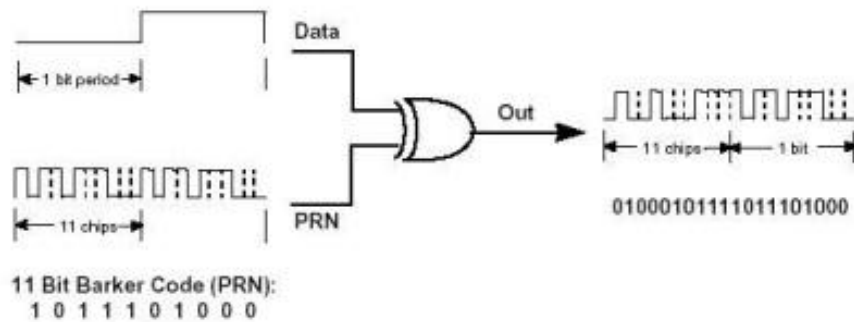
در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیماً توسط یک دنباله از کدهای شبه تصادفی تسهیم می شود. در این تکنیک نرخ بیتی شبه کد تصادفی، نرخ تراشه نامیده می شود. در استاندارد ۸۰۲.۱۱ از کدی موسوم به کد بارکر برای تولید کدها تراشه سیستم DSSS استفاده می شود. مهم ترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه آن یک فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند.

جدول زیر فهرست کامل کدهای بارکر را نشان می دهد. همانگونه که در این جدول مشاهده می شود کدهای بارکر از ۸ دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد ۸۰۲.۱۱ مورد استفاده قرار می گیرد، از کد بارکر با طول ۱۱ ($N=11$) استفاده می شود. این کد به ازاء یک نماد، شش مرتبه تغییر فاز می دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد ۶ مرتبه تغییر فاز خواهد داد.

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

شکل ۲.۱۱: کدهای بارکر

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



شکل ۲.۱۲: مدار مدولاسیون با استفاده از کدهای بارکر

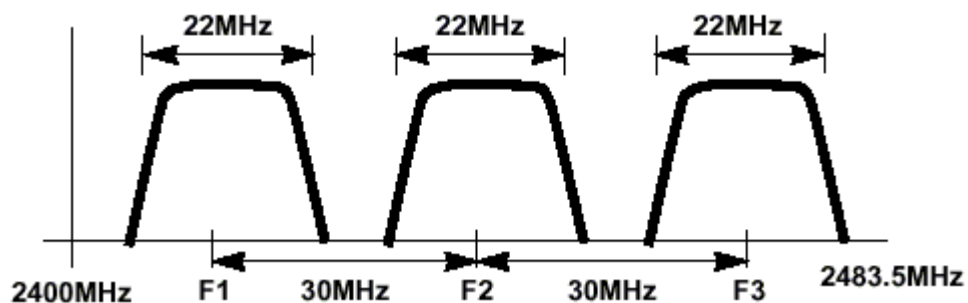
شکل ۲.۱۲ مدل منطقی مدولاسیون و پخش سیگنال اطلاعات با استفاده از کدهای بارکر را نشان می

دهد.

یکی از نکات مهم در طراحی شبکه های بی سیم، طراحی شبکه سلولی به گونه ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد. شکل ۲-۸ سه کانال DSSS در محدوده فرکانسی ISM را نشان می

دهد.

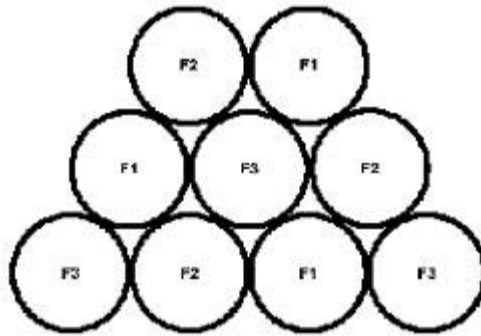
۲-۵-۱-۴ استفاده مجدد از فرکانس



شکل ۲.۱۲: سه کانال فرکانسی F3, F2, F1

شکل ۲.۱۳ مفهوم استفاده مجدد از فرکانس با استفاده از شبکه های مجاور فرکانسی را نشان می دهد. در

این شکل مشاهده می شود 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 ۲.۱۳: طراحی شبکه سلولی

در این طراحی به هر یک از سلول های همسایه یک کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول های همسایه به حداقل رسیده است. این تکنیک همان مفهومی است که در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می رود. نکته جالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است. خوانندگان علاقمند می توانند دایره های جدید را در چهار جهت شبکه سلولی شکل فوق با فرکانس های متمایز F1, F2, F3 ترسیم و گسترش دهند.

۲-۵-۱-۵-۲ آنتن ها

در یکی تقسیم بندی کلی آنتن های مورد استفاده در استاندارد IEEE 802.11 به دو دسته: تمام جهت و نقطه به نقطه تقسیم می شوند. واضح است که آنتن های تمام جهته با توجه به آنکه نیازی به تنظیم ندارند، راحت تر مورد استفاده قرار می گیرند. این آنتن ها در اغلب کارت های شبکه (کارت های دسترسی) و نیز نقاط دسترسی یا ایستگاه های پایه بکار می روند.

این آنتن ها در فواصل کوتاه قابل استفاده هستند و برای بهره گیری در فواصل طولانی تر به تقویت کننده های خارجی نیاز دارند که البته در بسیاری موارد استفاده از این تقویت کننده های خارجی میسر و یا قانونی نیست. از سوی دیگر آنتن های نقطه به نقطه یا خطی در کاربردهای خارجی استفاده می شوند و به تنظیم دقیق نیاز دارند. محدوده عملیاتی رایج در آنتن های تمام جهته ۴۵ متر و محدوده عملیاتی آنتن های نقطه به نقطه و توان بالا در حدود ۴۰ کیلومتر است. در کاربردهایی که استفاده از تقویت کننده بلا مانع است، این محدوده عملیاتی به شکل قابل توجهی افزایش یافته و تنها توسط خط دید (مسیر دید) محدود می شود. از جمله عوامل مهمی که محدوده عملیاتی تجهیزات مبتنی بر IEEE 802.11 را تحت تأثیر قرار می دهد محل نصب نقاط دسترسی یا ایستگاه پایه و نیز تداخل رادیویی است. همانگونه که پیشتر گفته شد، تجهیزات مبتنی بر این استاندارد سعی می کنند که با بالاترین نرخ ارسال داده کار کنند و در صورت نیاز به سرعت های پایین تر برگردند.

۶-۲ استاندارد 802.11b

همزمان با برپایی استاندارد IEEE 802.11b یا به اختصار b11 در سال ۱۹۹۹، انجمن مهندسين برق و الکترونیک تحول قابل توجهی در شبکه سازی های رایج و مبتنی بر اترنت ارائه کرد. این استاندارد در زیر لایه دسترسی به رسانه از پروتکل CSMA/CA سود می برد. سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر است:

۱. استفاده از تکنیک رادیویی DSSS در باند فرکانسی ۲.۴ GHz به همراه روش مدولاسیون CCK

۲. استفاده از تکنیک رادیویی FHSS در باند فرکانسی ۲.۴ GHz به همراه روش مدولاسیون CCK

۳. استفاده از امواج رادیویی مادون قرمز

در استاندارد ۸۰۲.۱۱ اولیه نرخ های ارسال داده ۱ و ۲ مگابیت در ثانیه است. در حالی که در استاندارد ۸۰۲.۱۱ با استفاده از تکنیک CCK و روش تسهیم QPSK نرخ ارسال داده به ۵.۵ مگابیت در ثانیه افزایش می یابد همچنین با به کارگیری تکنیک DSSS نرخ ارسال داده به ۱۱ مگابیت در ثانیه می رسد.

به طور سنتی این استاندارد از دو فناوری DSSS یا FHSS استفاده می کند. هر دو روش فوق برای ارسال داده با نرخ های ۱ و ۲ مگابیت در ثانیه مفید هستند. جدول ۲.۲ سرعت مختلف قابل دسترسی در این استاندارد را نشان می دهد.

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

جدول ۲.۲: نرخ های ارسال داده در استاندارد b 802.11

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC، مخبره و ارسال فرکانس های رادیویی را کنترل می کند. این کمیسیون باند فرکانس خاصی موسوم به ISM را در محدوده ۲.۴GHz تا ۲.۴۸۳۵ GHz برای فناوری های رادیویی استاندارد IEEE 802.11b اختصاص داده است.

۲-۶-۱ اثرات فاصله

فاصله از فرستنده بر روی کارایی و گذردهی شبکه های بیسیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد ۸۰۲.۱۱ با توجه به نرخ ارسال داده تغییر می کند و به طور مشخص در پهنای باند ۱۱ Mbps این فاصله ۳۰ تا ۴۵ متر و در پهنای باند ۵.۵ Mbps این فاصله ۴۰ تا ۴۵ متر و در پهنای باند ۲ Mbps این فاصله ۷۵ تا ۱۰۷ متر است. لازم به یادآوری است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل استقرار فرستنده و گیرند و شرایط فیزیکی و محیطی تغییر می کنند.

در استاندارد ۸۰۲.۱۱ پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می نماید توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزم های تصدیق رایج در سطح لایه انتقال (نظیر آنچه در پروتکل TCP اتفاق می افتد) عمل می کند. در صورتی که بسته تصدیق ظرف مدت زمان مشخصی از طرف گیرنده به فرستنده نرسد، فرستنده فرض می کند که بسته از دست رفته است و مجدداً آن بسته را ارسال می کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می یابد (Fall Back) تا در نهایت به مقدار ۱ Mbps برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته ای را برای آن گیرنده ارسال نمی کند. به این ترتیب فاصله نقش مهمی در کارایی (میزان بهره وری از شبکه) و گذردهی (تعداد بسته های غیرتکراری ارسال شده در واحد زمان) ایفا می کند.

۲-۶-۲ پل بین شبکه ای

بر خلاف انتظار بسیاری از کارشناسان شبکه های کامپیوتری، پل بین شبکه ای یا Bridging در استاندارد ۸۰۲.۱۱ پوشش داده نشده است. در پل بین شبکه ای امکان اتصال نقطه به نقطه (و یا یک نقطه به چند نقطه) به منظور برقراری ارتباط یک شبکه محلی با یک یا چند شبکه محلی دیگر فراهم می شود. 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 می باشد. با وجود اینکه استاندارد ۸۰۲.۱۱ این کاربرد را پوشش نمی دهد ولی بسیاری از شرکت ها پیاده سازی های انحصاری از پل بیسیم را به صورت گسترش و توسعه استاندارد ۸۰۲.۱۱ ارائه کرده اند. پل های بیسیم نیز توسط مقررات FCC کنترل می شوند و گذردهی مؤثر یا به عبارت دیگر توان مؤثر ساطع شده همگرا (EIRP) در این تجهیزات نباید از ۴ وات بیشتر باشد. بر اساس مقررات FCC توان سیگنال های ساطع شده در شبکه های محلی نیز نباید از ۱ وات تجاوز نماید.

۷-۲ استاندارد 802.11a

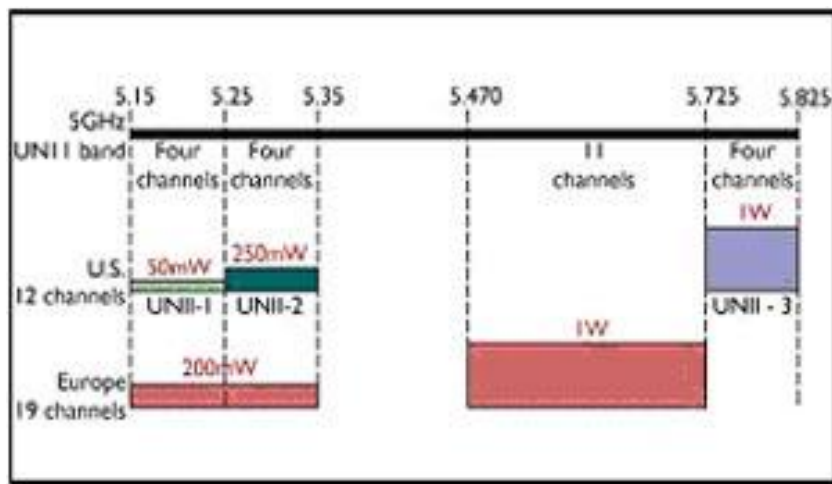
استاندارد 802.11a ، از باند رادیویی جدیدی برای شبکه های محلی بیسیم استفاده می کند و پهنای باند شبکه های بیسیم را تا ۵۴ Mbps افزایش می دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک مدولاسیونی موسوم به OFDM است. نرخ های ارسال داده در استاندارد IEEE 802.11a عبارتند از: ۶,۹,۱۲,۱۸,۲۴,۳۶,۴۸,۵۴ Mbps که بر اساس استاندارد، پشتیبانی از سرعت های ۶,۱۲,۲۴ مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه های محلی بیسیم، استاندارد IEEE 802.11a را نسل آینده IEEE 802.11 تلقی می کنند و حتی برخی از محصولات مانند تراشه های Atheros و کارت های شبکه PCMCIA/Cardbus محصول Card Access Inc. استاندارد IEEE 802.11a را پیاده سازی کرده اند. بدون شک این پهنای باند وسیع و نرخ داده سریع محدودیت هایی 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 می شود. 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 می کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می شود:

UNII-1 @ 5.2 GHz

UNII-2 @ 5.7 GHz

UNII-3 @ 5.8 GHz

یکی از تصورات غلط در زمینهاستانداردهای ۸۰۲.۱۱ این باور است که a ۸۰۲.۱۱ قبل از b ۸۰۲.۱۱ مورد بهره برداری واقع شده است. در حقیقت b ۸۰۲.۱۱ نسل دوم استانداردهای بیسیم (پس از ۸۰۲.۱۱) است و a ۸۰۲.۱۱ نسل سوم از این مجموعه استاندارد به شمار می رود. استاندارد a ۸۰۲.۱۱ برخلاف ادعای بسیاری از فروشندگان تجهیزات بیسیم نمی تواند جایگزین b ۸۰۲.۱۱ 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 ۲.۱۴: تخصیص باند فرکانسی در UNII

در شکل ۴-۱ این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می شود. این سه ناحیه کاری ۱۲ کانال فرکانسی را فراهم می کنند. 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 شبکه ای به کار برده می شوند. این نواحی فرکانسی در ژاپن نیز قابل استفاده هستند. این استاندارد در حال حاضر در قاره اروپا قابل استفاده نیست. در اروپا HyperLAN2 برای شبکه های بیسیم مورد استفاده قرار می گیرد که به طور مشابه از باند فرکانسی a۸۰۲.۱۱ استفاده می کند. یکی از نکات جالب توجه در استاندارد a۸۰۲.۱۱ تعریف کاربردهای پل سازی شبکه ای در کاربردهای داخلی و فضای باز است. در واقع این استاندارد مقررات لازم برای پل سازی و ارتباط بین شبکه های از طریق پل را در کاربردهای داخلی و فضای باز فراهم می نماید. در یکی تقسیم بندی کلی می توان ویژگی ها و مزایای a۸۰۲.۱۱ را در سه محور زیر خلاصه نمود.

افزایش در پهنای باند در مقایسه با استاندارد b۸۰۲.۱۱ (در استاندارد a۸۰۲.۱۱ حداکثر پهنای باند ۵۴ Mbps) می باشد.

استفاده از طیف فرکانسی خلوت (باند فرکانسی ۵ GHz)

استفاده از ۱۲ کانال فرکانسی غیرپوشا (سه محدوده فرکانسی که در هر یک ۴ کانال غیرپوشا وجود دارد)

۸-۲ استاندارد بعدی IEEE 802.11g

این استاندارد مشابه IEEE 802.11b از باند فرکانسی ۲.۴ 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 تا حدودی این محدوده عملیاتی را کاهش می دهد. پهنای باند ۵۴ Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می رود. یکی دیگر از مزایای جالب توجه IEEE 802.11g سازگاری با IEEE 802.11b است. در نتیجه ارتقاء از تجهیزات IEEE 802.11b به استاندارد جدید IEEE 802.11g امری سر راست خواهد بود. جدول ۲.۳ سه استاندارد شبکه های بیسیم را با یکدیگر مقایسه می کند.

IEEE802.11g	IEEE802.11a	IEEE802.11b	
<ul style="list-style-type: none"> -ارتقای شبکه های IEEE 802.11b -رقیبی برای IEEE 802.11a -کارایی مشابه با IEEE 802.11a در فواصل طولانی 	<ul style="list-style-type: none"> -جایگزین شبکه های بیسیم -فراهم کننده پهنای باند زیاد در کاربرد های صدا و تصویر و نظایر آن -شبکه سازی در محل هایی که استفاده ازسیم امکان پذیر نمی باشد 	<ul style="list-style-type: none"> -جایگزین شبکه های بیسیم -فراهم آوردن تحرک و سیار بودن کاربران -شبکه سازی در محل هایی که استفاده ازسیم امکان پذیر نمی باشد -پل سازی بین شبکه های محلی دور فواصل دور (۰.۴ کیلومتر) 	کاربرد های احتمالی
<ul style="list-style-type: none"> -سازگاری با IEEE 802.11b -محدوده عملیاتی زیاد (نظیر IEEE 802.11b) -گذر دهی (نرخ ارسال) بیشتر 	<ul style="list-style-type: none"> -گذر دهی بالا در فواصل کم -افزایش تعداد کانال های فرکانسی غیر پوشا -تداخل فرکانسی کمتر 	<ul style="list-style-type: none"> -استاندارد رایج و تکامل یافته -قیمت منطقی =گذر دهی قابل قبول در فواصل زیاد (نرخ ارسال) 	مزایا
<ul style="list-style-type: none"> -عدم وجود محصول فراگیر -محدودیت های کانال فرکانسی نظیر IEEE 802.11b (ه کانال غیر پوشا) 	<ul style="list-style-type: none"> -فناوری نسبتا گران -ناسازگاری با IEEE 802.11b -محدوده عملیاتی کوچک -محدودیت های FFC (حداکثر توان) بر روی آنتن ها در هر باند فرکانسی 	<ul style="list-style-type: none"> -دارا بودن کمترین گذر دهی (نرخ ارسال) در مقایسه با سایر فناوری های بیسیم -استفاده از تنها سه کانال فرکانسی غیرپوشا 	معایب

جدول ۲.۳ : مقایسه استانداردهای بیسیم IEEE 802.11

۳ فصل سوم: مفاهیم امنیتی در شبکه های بی سیم

Chapter three: Security Concepts in Wi-Fi

مراجع: [9]

۳-۱ فاکتور های امنیتی در شبکه های بی سیم

فاکتور هایی که امنیت در شبکه ها بی سیم را تعریف می کند به پنج مفهوم کلی دسته بندی می شود که عبارتست از :

۱. **سارقان (thefts):** سارقان کاربران غیر مجاری هستند که قصد نفوذ و ورود به شبکه را دارند تا داده ها و اطلاعات مهم را برای اهداف خاص سرقت کنند. اهداف این سارقان متفاوت است و از افراد مهاجم خارجی می تواند باشد تا کارمندان داخلی سازمان، بنابراین باید یک تدبیر امنیتی در نظر گرفت تا از ورود این افراد به سیستم جلوگیری شود.

۲. **کنترل دسترسی (Access control):** بسیاری از سازمان ها یک سری از مجوز های دسترسی بسیار ساده ای دارند و این می توان از هر چیزی خطرناک تر باشد به خصوص در یک شبکه محلی بی سیم که به راحتی می توان نفوذ کرد، در نتیجه روال های کنترل دسترسی سیستم هایی که در شبکه های بی سیم استفاده می شوند، باید حتما اعمال شود و به اندازه های قوی باشد که از ورود افراد مهاجم و خارجی و حتی ویروس ها، به شبکه جلوگیری کند.

۳. **احراز هویت (Authentication):** آیا شما مطمئن هستید کاربری که از قصد استفاده از سیستم را دارد واقعا همان شخصی است که ادعا می کند؟ متأسفانه یک امر رایج در شبکه ای بی سیم این است که افراد از اکانت های یک دیگر برای استفاده از شبکه استفاده می کنند و این بهترین فرصت برای مهاجمان برای ورود به شبکه می باشد، برای جلوگیری از ورود این افراد به شبکه، باید تنظیمات روتر را طوری انجام دهید که تنها اتصالات از طریق کارت شبکه های مجاز احراز هویت شده را قبول کند، همانطور که می دانیم هر کارت شبکه دارای یک آدرس مک منحصر به فرد می باشد، و برای افزایش امنیت می توانیم تنها اتصالات از کارت شبکه هایی را قبول کنیم که از قبل در روتر شناسایی شده باشند.

۴. **رمز نگاری (Encryption):** اگر مهاجم به طور مستقیم نتواند به شبکه دسترسی پیدا کند و نفوذ کند می تواند از طریق شنود ترافیک وبسته های شبکه، به شبکه حمله کند و این بدین معنی است که مهاجمی که نتوانسته به طور مستقیم به شبکه نفوذ کند قادر است از طریق دیگری به اطلاعات مهم دسترسی پیدا کند و آنها را سرقت کند و حتی می تواند از طریق شنود بسته های انتقالی اطلاعات حساس شما مثل نام کاربری و کلمه عبور را شنود کرده و بدین ترتیب دوباره به شکل مستقیم در سیستم نفوذ کند.

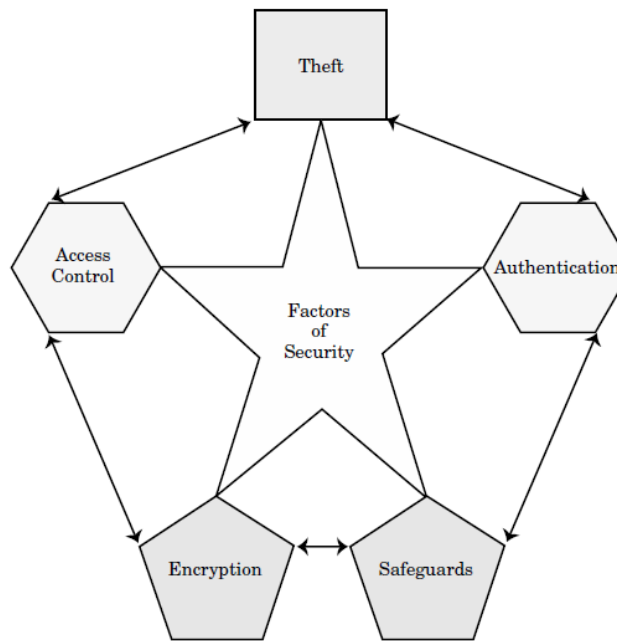
روتر های بی سیم سطوح مختلفی از رمزنگاری را پشتیبانی می کنند، متأسفانه اکثر مدیران شبکه این امکانات در روتر را فعال نمی کنند.

امنیت معادل سیمی (WEP) پروتکل امنیتی است که توسط استاندارد IEEE802.11 برای استفاده در شبکه های بی سیم، تعریف شده است. WEP سطوح مختلف امنیتی معادل با یک شبکه سیمی را ارائه می دهد، این پروتکل در هر دو لایه فیزیکی و پیوند داده مورد استفاده قرار می گیرد و امنیت نقطه به نقطه را فراهم نمی کند.

بیشتر روترها بی سیم رمزنگاری ۶۴ بیت و ۱۲۸ بیتی را پشتیبانی می کنند و از یک کلید رمزنگاری از پیش تعیین شده برای عملیات رمزنگاری استفاده می کنند که در طرف مقابل از این کلید برای رمزگشایی استفاده می شود.

۵. محافظت های امنیتی (Safeguards): برای اعمال روش های محافظتی در شبکه های بی سیم، در مرحله اول باید شبکه بی سیم مورد نظر را کاملاً شناخت، سپس باید تنظیمات امنیتی روتر را پیکر بندی نمود و از کلید های حداقل با طول ۶۴ بیت استفاده نمود، البته باید این نکته را توجه داشت که بعضی از کارت های شبکه بی سیم فقط سطوح خاصی امنیتی را پشتیبانی می کنند.

بعد از اعمال تنظیمات امنیتی روتر می توان روش های دیگر برای افزایش امنیت شبکه استفاده نمود، مثلاً از روش هایی استفاده نمود که بلافاصله بعد از هک شدن شبکه مطلع شویم تا از خرابکاری بیشتر جلوگیری کنیم، مثلاً روترها دارای امکانی هستند که جریان ترافک را در شبکه نشان می دهند و نرم افزار های مختلفی وجود دارند که می توانند که از این اطلاعات برای تحلیل ترافیک استفاده کنند، پس ما می توانیم از این نرم افزارها برای مدیریت و نظارت بهتر شبکه استفاده کنیم و مثلاً اگر حجم نامعقولی از ترافیک را متوجه شدیم سریعاً حجم تفکیکی به ازای هر اتصال را بررسی کنیم و با ردگیری ترافیکی به منشا آن برسیم و سریعتر برای جلوگیری از کار افتادن شبکه، اقدام کنیم.



شکل ۳.۱: فاکتور های امنیتی در شبکه های بی سیم

۲-۳ سیستم تشخیص نفوذ:

تعداد زیادی از نرم افزار های تجاری وجود دارد که از تکنیک نقش - مبنا (Role-Based)، به طور اتوماتیک برای تشخیص نفوذ به سیستم استفاده می کنند، سیستم تشخیص نفوذ تمام فعالیت های به -داخل وبه -خارج شبکه را بررسی می کند تا حمله از سوی مهاجمی را که قصد دارد به شکل غیر مجاز به سیستم وارد شود را، شناسایی کند.

انواع مختلف روش های تشخیص نفوذ عبارتست از:

۱. شناسایی الگو (Pattern detection): در این تکنیک که معمولاً با نام تشخیص مبتنی بر امضاء شناخته شده است، الگوهای نفوذ از پیش ساخته شده (امضاء) به صورت قانون نگهداری می شوند. به طوری که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته و در صورت بروز چنین الگویی در سیستم، وقوع نفوذ اعلام می شود. در این روش ها، معمولاً تشخیص دهنده دارای پایگاه داده ای از امضاء ها یا الگوهای حمله است و سعی می کند با بررسی ترافیک شبکه، الگوهای مشابه با آن چه را که در پایگاه داده خود نگهداری می کند، بیابد. این دسته از روش ها تنها قادر به تشخیص نفوذهای شناخته شده می باشند و در صورت بروز حملات جدید در سطح شبکه، نمی توانند آن ها را شناسایی کنند و مدیر شبکه باید همواره الگوی حملات جدید را به سامانه تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آن ها عیناً به سیستم داده شده است.

روش دیگری هم وجود دارد که می تواند زیر دسته این روش قرار بگیر و عبارتست از روش تشخیص رفتار غیرعادی، در این روش، یک نما از رفتار عادی ایجاد می شود. یک ناهنجاری ممکن است نشان دهنده یک نفوذ باشد. برای ایجاد نماهای رفتار عادی از رویکردهایی از قبیل شبکه های عصبی، تکنیک های یادگیری ماشین و حتی سیستم های ایمنی زیستی استفاده می شود. برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آن ها پیدا کرد. رفتارهایی که از این الگوها پیروی می کنند، عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند، به عنوان رفتار غیرعادی تشخیص داده می شود. نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می پیوندد، غیرعادی فرض می شود.

۲. سامانه تشخیص نفوذ مبتنی بر میزبان و شبکه (NIDS^۶, HIDS^۷): سیستم مبتنی بر میزبان، شناسایی و تشخیص فعالیت های غیرمجاز بر روی رایانه میزبان را بر عهده دارد. سامانه تشخیص نفوذ مبتنی بر میزبان می تواند حملات و تهدیداتی را روی سیستم های بحرانی تشخیص دهد (شامل دسترسی به فایل ها، اسب های تروا و ...). که توسط سامانه های تشخیص نفوذ مبتنی بر شبکه قابل تشخیص نیستند. HIDS فقط از میزبان هایی که روی آن ها مستقر است محافظت می کند و کارت واسط شبکه (NIC) آن ها به صورت پیش فرض در حالت باقاعده کار می کند. حالت باقاعده در بعضی از موارد می تواند مفید باشد چون همه کارت های واسط شبکه قابلیت حالت بی قاعده را ندارند. HIDS به واسطه مکان شان روی میزبانی که باید نظارت شود، از همه انواع اطلاعات محلی اضافی با پیاده سازی های امنیتی (شامل فراهوانی های سیستمی، تغییرات فایل های سیستمی و اتصالات سیستم) مطلع می باشند. این مساله هنگام ترکیب با ارتباطات شبکه ای، داده های خوبی را برای جستجوی رویدادهای ممکن فراهم می کند.

شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیستم های بحرانی، به عهده سامانه تشخیص نفوذ مبتنی بر شبکه است. NIDS، به عنوان دومین نوع IDS ها، در بسیاری از موارد عملاً یک Sniffer هستند که با بررسی بسته ها و پروتکل های ارتباطات فعال، به جستجوی تلاش هایی که برای حمله صورت می گیرد می پردازند. به عبارت دیگر معیار NIDS، تنها بسته هایی است که بر روی شبکه ها رد و بدل می گردد. از آن جایی که NIDS تشخیص را به یک سیستم منفرد محدود نمی کنند، عملاً گستردگی بیش تری داشته و فرایند تشخیص را به صورت توزیع شده انجام می دهند. با این وجود این سیستم ها در رویایی با بسته های رمز شده و یا شبکه هایی با سرعت و ترافیک بالا کارایی خود را از دست می دهند.

^۶ Network-based intrusion detection system

^۷ host-based intrusion detection system

۳. پاسخ فعال و غیر فعال در سیستم تشخیص نفوذ: در پاسخ فعال، IDSها، به مدیر امنیتی سیستم

اطلاعاتی درباره حمله توسط تلفن همراه، نامه الکترونیکی، پیام روی صفحه رایانه یا پیامی برای کنسول SNMP می دهند. این اطلاعات شامل: آدرس IP منبع حمله

، آدرس IP مقصد حمله، نتیجه حمله، ابزار یا مکانیزم های مورد استفاده برای مهار حملات گزارش ها و اتصال ها حمله های سیستم و رویدادهای مربوطه باشد.

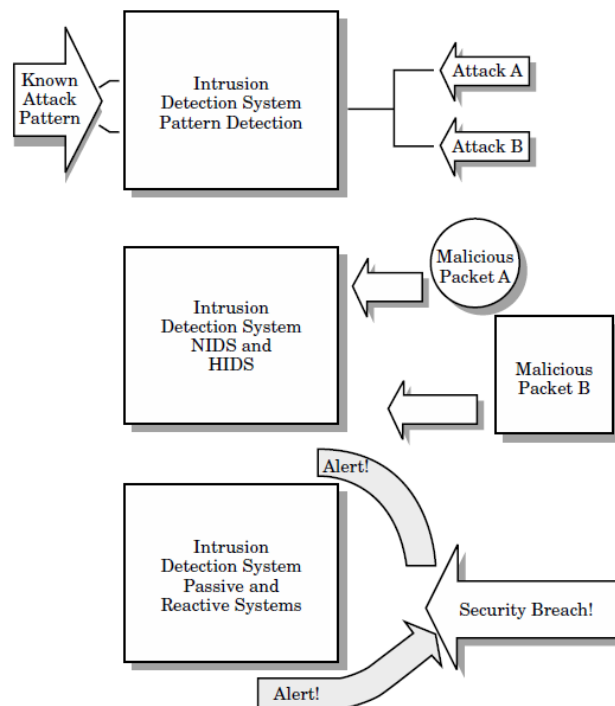
در پاسخ فعال سامانه های تشخیص نفوذ از لحظه ای که به کار می افتند، ضمن به دست آوردن اطلاعات مربوط به رخدادها و تجزیه و تحلیل آن ها، اگر نشان هایی دال بر وقوع یک حمله را تشخیص دهند، پاسخ لازم را در قبال آن به نحوه های مختلف تولید می کنند. گاهی این پاسخ به صورت یک هشدار به مدیر شبکه است و گاهی نوشتن یک اطلاع در فایل رخدادها و یا به صورت تنظیم مجدد دیوار آتش و یا دستگاه های دیگری در شبکه است. IDSهای فعال هر نفوذی را که تشخیص دهد به طور خودکار پاسخ می دهند و خود به سه دسته تقسیم می شوند:

الف: پاسخ فعال براساس جمع آوری اطلاعات اضافی

ب: پاسخ فعال از نوع تغییر محیط

ج: پاسخ فعال از نوع عکس العمل در مقابل حمله

نمایی کلی از روش های سیستم نفوذ در شکل ۳.۲ نمایش داده شده است



شکل ۳.۲: روش های تشخیص نفوذ

۳-۳ چالش های امنیتی در شبکه های WI-Fi

مطمئناً یکی از بزرگترین نگرانی ها، بعد از راه اندازی و پیکر بندی شبکه های بی سیم، برقراری امنیت می باشد، با توجه به این که محیط بی سیم محیطی نا امنی محسوب می شود و هر لحظه می تواند مورد حمله قرار گیرد و اطلاعات و داده های شبکه سرقت شود، برقراری امنیت یکی از بزرگترین چالش ها در این شبکه ها می باشد.

انواع تهدید هایی که ممکن است امنیت در شبکه ای بی سیم را به خطر اندازد عبارتند از:

۱. **افشای اطلاعات:** هرگونه دسترسی غیر مجاز به اطلاعات و داده های شبکه که گاهی می تواند اطلاعات حیاتی و مهم مثل اطلاعات نظامی یا اطاعات حساب بانکی افراد باشد.

۲. **دسترسی های غیر مجاز:** هرگونه دسترسی به اطلاعات و داده ها و نفوذ به شبکه توسط افراد غیر مجاز و احراز هویت نشده به سیستم، دسترسی غیر مجاز نام دارد.

۳. **منع سرویس (DOS):** هرگونه عملیات خرابکارانه که منجر به این شود که سرویس دهی سیستم مختل شود، حملات منع سرویس گفته می شود. در چند سال اخیر این حمله یکی از مهمترین حملات به شمار می رود که در آن حمله کننده با اعمال بار زیاد به شبکه باعث مختل شدن کار شبکه می شود.

خطر معمول در کلیه شبکه های بی سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قدرت مند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جازده و در صورت تحقق این امر، امکان دستیابی به اطلاعات حیاتی، حمله به سرویس دهنده گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیر واقعی و گمراه کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت های مخرب وجود دارد.

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

- تمامی ضعف های امنیتی موجود در شبکه های سیمی، در مورد شبکه های بی سیم نیز صدق می کند. در واقع نه تنها هیچ جنبه ایی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه های بی سیم وجود

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

- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به راحتی 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.

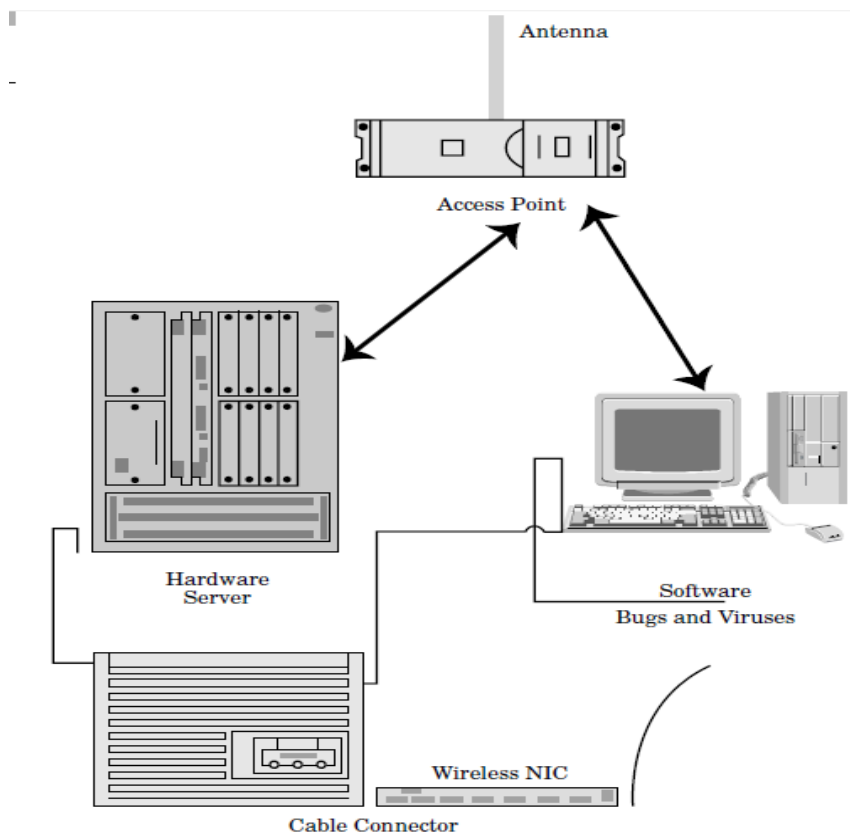
- کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.

- یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس تری 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 عمل کرد شبکه نیز وجود دارد.

۳-۴ نقاط آسیب پذیر و قابل نفوذ در شبکه های Wi-Fi

به طور کلی چندین نقطه آسیب پذیر در شبکه های بی سیم وجود دارد و در صورتی که مهاجمین از این نقاط اطلاعات به دست آورند به راحتی می توانند به شبکه نفوذ کرده و زیر ساخت شبکه را به هم بریزند، این نقاط در شکل ۳.۳ نمایش داده شده است.



شکل ۳.۳ نقاط حساس در شبکه های بی سیم

این نقاط عبارتست از :

۱. نقطه دسترسی

۲. آنتن

۳. کارت های شبکه بی سیم

۴. کابل های اتصال

۵. سرور سخت افزاری

۶. باگ های نرم افزاری و ویروس ها

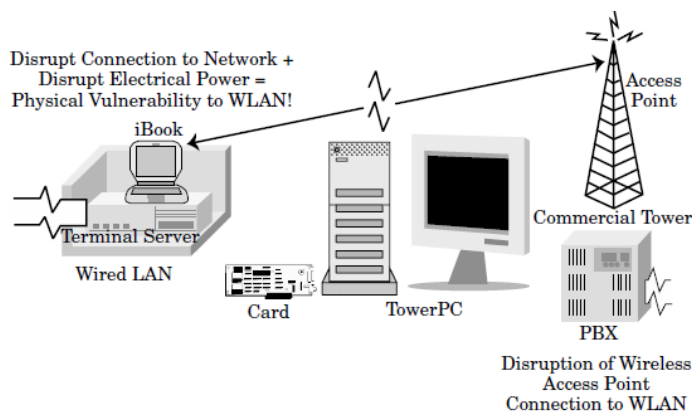
این امکان وجود دارد که از هر کجا به سیستم نرم افزاری نفوذ کرد، هر چند که firmware های کاملاً مناسب در نقاط دسترسی و روترها نصب شده باشد، در حقیقت firmware ها در این وسایل نرم افزارهایی هستند که ویژگی ها و قابلیت هایی را از جمله قابلیت های امنیتی را به ارمغان می آورند، اما باید توجه داشت که اگر هکرها بتوانند به تجهیزات و وسایل دسترسی پیدا کنند به راحتی می توانند firmware و نرم افزارهای جدید را بر روی این تجهیزات قرار دهند تا مطابق خواسته ی آنها عمل کنند یا حتی این نرم افزارها دستکاری کرده تا نتوانند وظایف امنیتی خود را به درستی انجام دهند.

سرور ها و نرم افزار ها می توانند توسط ویروس ها مورد حمله قرار بگیرند، اکثر ویروس های جدید اتصالات آداپتور شبکه را شناسایی می کنند و ارتباطات را در شبکه به هم می ریزند، اساسا این ویروس ها با اهداف خاموش کردن کامل تجهیزات شبکه های بی سیم و خراب کردن سیگنال و رساندن گذر دهی سیگنال در حد صفر می باشد. خاموش کردن تجهیزات شبکه مثل نقاط دسترسی یا روتر ها می توانند کل شبکه را مختل کند و از کار بیاندازد، نکته قابل توجه در این حملات سخت بودن شناسایی حمله و شناسایی این که دلیل خرابی سخت افزاری یا نرم افزاری بوده، می باشد.

- هر گونه دست کاری و مختل کردن و از کار انداختن، در شبکه های بی سیم می تواند به صورت زیر باشد:

- بر هم زدن ارتباطات بین نقاط دسترسی
- قطع کردن اتصال اساسی شبکه بی سیم به شبکه سیمی
- ایزوله کردن و جدا سازی چندین نقطه دسترسی برای این که نتوانند با سایر نقاط دسترسی ارتباط برقرار کنند، که می تواند منجر به کار افتادن شبکه های بی سیم شود.
- خاموش کردن و قطع برق یک یا چند نقطه دسترسی

این روش ها در شکل ۳.۴ نمایش داده شده است. در مجموع باید گفت که برای یک هکر خیلی ساده می باشد که از یک کارت شبکه بی سیم که قبلا در شبکه شناخته شده است و مجاز شماری شده استفاده کند و به شبکه حمله کند و در نتیجه بر هم زدن اتصالات در نقاط دسترسی، منابع شبکه، سرور، منبع برق و قطع کردن ارتباط با شبکه سیمی سبب از کار افتادن و کاهش کارایی و خراب شدن شبکه شود.



شکل ۳.۴: تهدیدات فیزیکی در شبکه بی سیم

۳-۵ امن سازی شبکه های بی سیم

در مجموع برای امن سازی شبکه های بی سیم باید از امکانات امنیتی ادغام شده در استاندارد ۸۰۲.۱۱ استفاده نمود، در حقیقت این استاندارد امکانات و ویژگی هایی را فراهم می آورد که باعث افزایش میزان امنیت در یک شبکه می شود. به طور کلی ابتدا برای این که بتوان به امنیت در این شبکه ها رسید باید ویژگی های زیر را اعمال کرد که در پروتکل WEP برای برقراری امنیت در شبکه های بی سیم استفاده شده است:

۱. احراز هویت: یکی از اهداف پروتکل WEP که در استاندارد ۸۰۲.۱۱ مورد استفاده قرار گرفته است، کنترل دسترسی و احراز هویت در شبکه های بی سیم می باشد.

۲. ایمنی (Privacy): WEP سطح کنترل زیادی در هنگام برقراری در ارتباطات بی سیم فراهم می آورد و جلوی هر گونه تغییر و استراق سمع در داده های ارتباطی را می گیرد و به عبارت دیگر برای این که کار می رود که به شما این اطمینان را بدهد که داده های دریافت شده از یک منبع مورد اعتماد است و هرگونه تغییر و دست کاری در آن رخ نداده است.

۳-۵-۱ احراز هویت

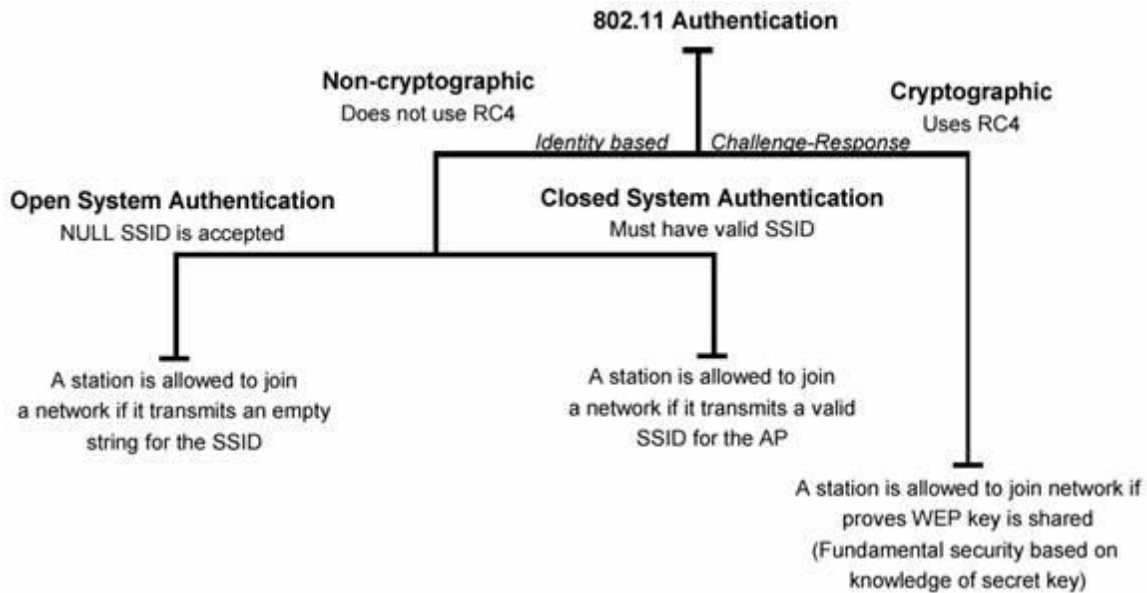
وقتی یک کاربر شبکه بی سیم سعی می کند که به زیر ساخت شبکه سیمی وصل شود، دو رویکرد را می توان درباره ی این در خواست اعمال کرد:

۱. سیستم های باز: هر کاربری که در محدوده رادیویی نقطه دسترسی باشد به راحتی می تواند به شبکه وصل شود و هیچ گونه محدودیتی در رابطه با وصل شدن کارت های شبکه اعمال نمی کند.

۲. سیستم رمز شده (بسته): در این سیستم داده ها با استفاده از الگوریتم RC4 رمز می شود و هکر ها نمی توانند به داده های در حال جریان در شبکه دسترسی پیدا کنند. در این سیستم برای این که کاربری به شبکه وصل شود باید به نقطه دسترسی SSID^۹ را ارسال کند، که در حقیقت یک عدد منحصر به فرد است که تنها کاربران ثبت شده در سیستم می دانند. در این سیستم برای مجاز شمار نیز از رمز نگاری استفاده می شود

شکل زیر شمایی از فرایند Authentication را در این شبکه ها نشان می دهد :

^۹ service set identifier



شکل ۳.۵ روش های Authentication در استاندارد 802.11

همان گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می کند و روش دیگر از هیچ تکنیک رمزنگاری بی استفاده نمی کند.

۳-۱-۵-۳ Authentication بدون رمزنگاری

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

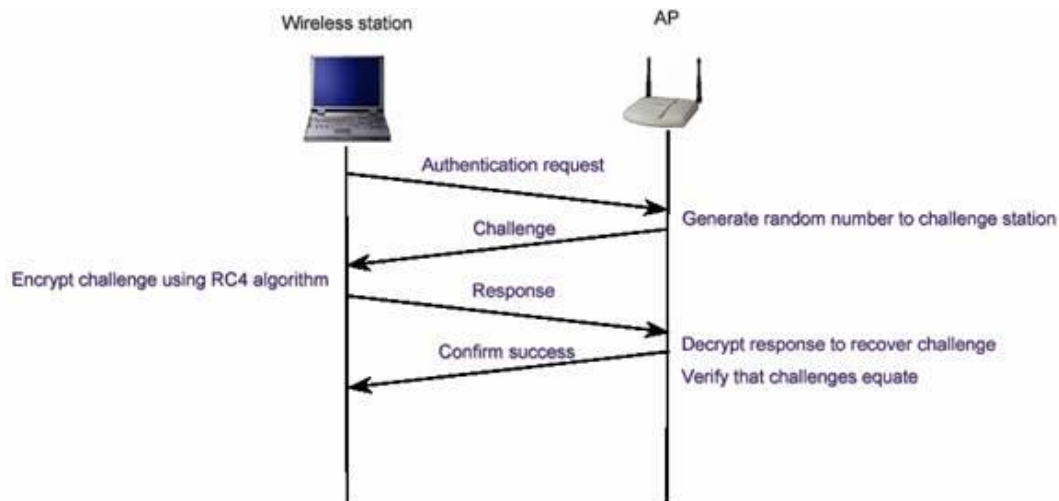
در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه اتصال به شبکه کفایت می کند. در واقع در این روش تمامی کلاینت هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می کنند با پاسخ مثبت روبه رو می شوند و تنها آدرس آنها توسط نقطه دسترسی نگاهداری می شود. به همین دلیل به این روش NULL Authentication نیز اطلاق می شود.

در روش دوم از این نوع، باز هم یک SSID به نقطه دسترسی ارسال می گردد با این تفاوت که اجازه اتصال به شبکه تنها در صورتی از سوی نقطه دسترسی صادر می گردد که SSID ارسال شده جزو SSID های 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 آن جایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم تجربه 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 رخ دادن حملات نیز خود تضمینی ندارد!

۲-۱-۵-۳ 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 کلاینت از کلیدی سری آگاه است، هویتش تأیید می‌شود. شکل زیر این روش را نشان می‌دهد:



شکل ۳.۶ فرایند Authentication با رمزنگاری RC4

در این روش، نقطه‌ی دسترسی (AP) یک رشته‌ی تصادفی تولید کرده و آن را به کلاینت می‌فرستد. کلاینت 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 کلاینت 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 کلاینت اطمینان حاصل می‌کند. به بیان دیگر کلاینت هیچ دلیلی در اختیار ندارد که بداند نقطه‌ی دسترسی‌یی که با آن در حال تبادل داده‌های رمز شده 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 به‌گونه‌یی هر یک از دو طرف را گمراه می‌کند.

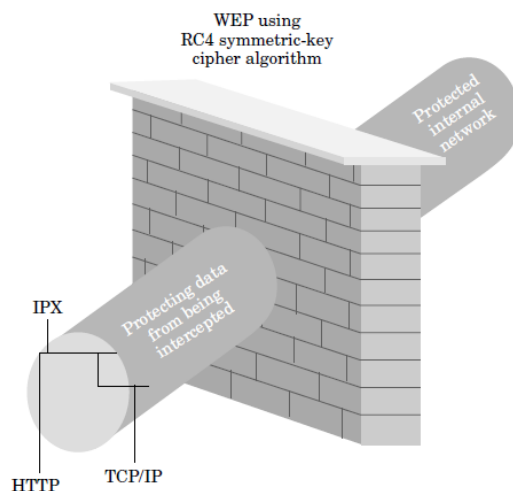
۳-۵-۲ امنیت داده‌ها

استاندارد ۸۰۲.۱۱ از طریق مکانیسم رمزنگاری امنیت در شبکه‌های بی‌سیم را تامین می‌کند. پروتکل WEP در استاندارد ۸۰۲.۱۱ از الگوریتم RC4 با کلید متقارن برای رمزنگاری استفاده می‌کند. WEP برای تمامی داده‌ها در شبکه‌های بی‌سیم مناسب می‌باشد و برای حفاظت و امن‌سازی کانال مورد استفاده قرار می‌گیرد. این پروتکل از داده‌ها محافظت می‌کند زمانی که در حال انتقال از کانال هستند و از پروتکل‌های زیر استفاده می‌کنند:

- پروتکل کنترل انتقال (TCP)/پروتکل اینترنت (IP)

- تبادل بسته‌های اینترنت (IPX)^{۱۰}

- پروتکل HTTP



شکل ۳.۷: محافظت از داده ها در کانال های ارتباطی

WEP برای رمزنگاری با طول کلید بین ۴۰ تا ۱۰۴ بیت طراحی شده است و هر چه طول کلید افزایش یابد میزان امنیت در کانال نیز افزایش خواهد یافت، در حقیقت اگر کلید با طول کم انتخاب شود به هکرها اجازه ی حمله "جست و جوی تمام حالات" داده می شود و می توانند کلید را به دست آورده و اطلاعات را رمز گشایی کنند. متأسفانه تجربه نشان داده است که بسیاری از سازمان ها تنظیمات امنیتی را فعال نمی کنند و اگر هم استفاده کنند از طول کلید کوچک استفاده می کنند که در نهایت منجر به هک شدن شبکه شده است.

۶-۳ مدیریت کلید ها

یکی از چالش های مهم در استاندارد ۸۰۲.۱۱ مدیریت کلید ها می باشد. مدیران در شبکه های بی سیم در مورد چند مورد در رابطه با کلید ها مسئول می باشند:

۱. ایجاد کلید ها
۲. اشتراک کلید بین کاربران شبکه
۳. نگه داری کلید ها به شکلی که دست مهاجمین و هکرها نیافتد
۴. نظارت بر این که هرکسی از چه کلیدی برای عملیات رمزنگاری استفاده می کند
۵. حذف کلید هایی که لو رفته و به صورت اشتراکی استفاده می شود

اما چه اتفاقی می افتد اگر کسی مسئولیتی در رابطه با مدیریت کلید ها که در بالا ذکر شده است بر عهده نگیرد؟ در واقع شبکه شما در برابر حملات هکر ها آسیب پذیر خواهد شد و منجر به موارد زیر خواهد شد:

- کلیدهای WEP یکتا نیستند و می توانند توسط چندین کاربر استفاده شوند!
- پسورد های پیش فرض که توسط کارخانه تنظیم شده اند تغییر پیدا نمی کند و باعث می شود که به راحتی هکر ها از این پسورد ها مطلع شوند.
- کلید های نا مناسب نه کلید هایی که همه اعداد آن یک یا همه اعداد آن صفر باشند، بلکه کلید هایی که به راحتی هکر ها می توانند حدس بزنند و در اولین جست و جو به آن خواهند رسید.

۷-۳ صحت داده

یکی دیگر از امکانات امنیتی که استاندارد ۸۰۲.۱۱ فراهم می آورد، حفظ صحت داده زمانی که در کانال و چندین نقطه دسترسی می گذرد، می باشد. تکنیکی که استفاده می شود استفاده از کد های CRC می باشد در حقیقت بعد از دریافت بسته و رمز گشایی آن کد CRC بر اساس محتوای بسته محاسبه می شود و با کد CRC که فرستنده در بسته گذاشته است مقایسه می شود، اگر مطابقت کرد یعنی بسته از تغییرات مصون بوده و گرنه متوجه می شویم که بسته در راه دچار تغییرات شده و فاقد اعتبار می باشد.

۸-۳ نتیجه گیری

با توجه به ماهیت محیط شبکه های بی سیم Wi-Fi و در دسترس بودن ابزار های پیشرفته حمله و نفوذ به شبکه توسط هکر ها، برقراری امنیت در شبکه های بی سیم یکی از بزرگترین چالش ها شناخته می شود. در قدم اول کاربران در این سیستم باید اقدامات امنیتی را همواره در نظر گرفته و از پسورد های مناسب استفاده کنند و از استفاده اشتراکی اکانت خود با همکاران یا دوستان خود بپرهیزند و امکانات امنیتی را که از جانب مدیریت شبکه برای آنها فراهم شده است، استفاده کنند، و در قدم بعدی مدیران باید جدیدترین مکانیسم ها و روش ها را برای امن سازی شبکه به کار ببرند و از تجهیزاتی استفاده کنند که حداکثر امنیت را به ارمغان آورد.

۴ فصل چهارم: چالش های امنیتی و راه کارها در شبکه های وای فای

Chapter Four: Security Challenges and solution in Wi-Fi Networks

مراجع: [10],[11]

۱-۴ مقدمه

موفقیت حیرت انگیز ۸۰۲.۱۱ به علت توسعه «اترنت بی سیم» است. همچنانکه ۸۰۲.۱۱ به ترقی خود ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایه ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفته می شوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد.

در این فصل هفت مشکل از مهم ترین آسیب پذیری های امنیتی موجود در LAN های بی سیم، راه حل آنها و در نهایت چگونگی ساخت یک شبکه بی سیم امن مورد بحث قرار می گیرد. بسیاری از پرسش ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می توانند استفاده کنند. یک آنالایزر از اولین خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سیم را کند می کنند، استفاده شوند. این سلسله مقاله هر یک از این «هفت مسأله امنیتی» را بررسی می کند و توضیح می دهد که چگونه و چرا آنالایزر بی سیم، یک ابزار حیاتی برای تضمین امنیت شبکه های بی سیم است.

۲-۴ مشکل اول: دسترسی آسان

LAN های بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها باید فریم های Beacon با پارامترهای شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن به یک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فریم های Beacon توسط هیچ فانکشن اختصاصی پردازش نمی شوند و این به این معنی است که شبکه ۸۰۲.۱۱ شما و پارامترهایش برای هر شخصی با یک کارت ۸۰۲.۱۱ قابل استفاده است. نفوذگران با آنتن های قوی می توانند شبکه ها را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجام حملاتی کنند حتی بدون اینکه به امکانات شما دسترسی فیزیکی داشته باشند.



شکل ۴.۱: نمونه ای از شبکه های بی سیم

۴-۲-۱ راه حل مشکل اول: تقویت کنترل دسترسی قوی

دسترسی آسان الزاماً با آسیب پذیری مترادف نیست. شبکه های بی سیم برای ایجاد امکان اتصال مناسب طراحی شده اند، اما می توانند با اتخاذ سیاستهای امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی سیم می تواند تا حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی دهد. به هر حال، برای بیشتر موسسات چنین برد هایی لازم نیستند. تضمین اینکه شبکه های بی سیم تحت تأثیر کنترل دسترسی قوی هستند، می تواند از خطر سوءاستفاده از شبکه بی سیم بکاهد.

تضمین امنیت روی یک شبکه بی سیم تا حدی به عنوان بخشی از طراحی مطرح است. شبکه ها باید نقاط دسترسی را در بیرون ابزار پیرامونی امنیت مانند فایروال ها قرار دهند و مدیران شبکه باید به استفاده از VPN ها برای میسر کردن دسترسی به شبکه توجه کنند. یک سیستم قوی تأیید هویت کاربر باید به کار گرفته شود و ترجیحاً با استفاده از محصولات جدید که برپایه استاندارد IEEE 802.1x هستند. x۸۰۲.۱ انواع فریم های جدید برای تأیید هویت کاربر را تعریف می کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می گیرد. آنالیزهای باسیم سنتی می توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت ۸۰۲.۱۱ شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم های آنالیز خبره که پیام های تأیید هویت 802.1x را دنبال می کنند، ثابت کرده اند که برای استفاده در LANهای استفاده کننده از 802.1x فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چینی فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم ها انجام می دهند و می توانند چندین مسأله معمول امنیت 802.1x را تشخیص دهند. تعدادی از حملات روی شبکه های باسیم در سال های گذشته شناخته شده اند و لذا وصله های فعلی به خوبی تمام ضعف های شناخته شده را در این گونه شبکه ها نشان می دهند. آنالیزهای خبره پیاده سازی های ضعیف را برای مدیران شبکه مشخص می کنند و به این ترتیب مدیران شبکه می توانند با به کارگیری سخت افزار و نرم افزار ارتقاء یافته، امنیت شبکه را حفظ کنند.

پیکربندی های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LAN های بی سیم بدون نظارت مهندسان امنیتی به کار گرفته شده باشند. موتورهای آنالیز خبره می توانند زمانی را که پیکربندی های پیش فرض کارخانه مورد استفاده قرار می گیرند، شناسایی کنند و به این ترتیب می توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی های امنیتی پیکربندی نشده اند، تعیین موقعیت کنند. این آنالیزها همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPN ها یا 802.1x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

۳-۴ مسأله دوم: نقاط دسترسی نامطلوب

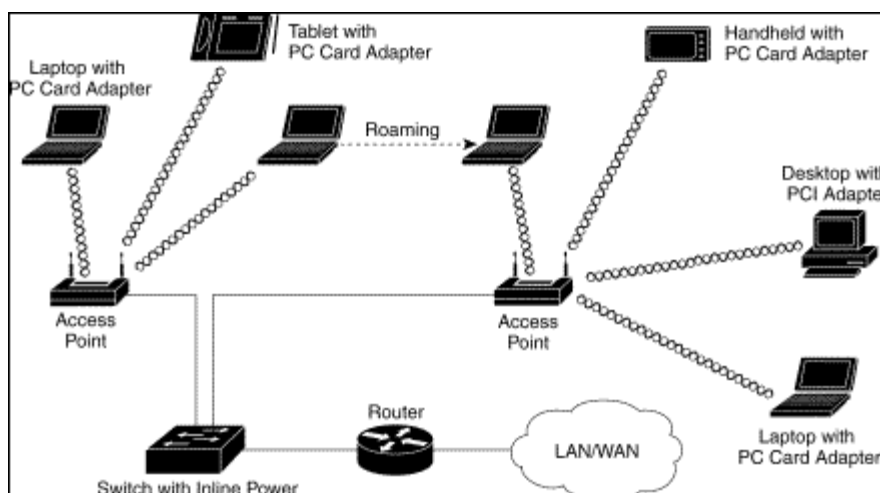
دسترسی آسان به شبکه های LAN بی سیم امری منفک از راه اندازی آسان آن نیست. این دو خصوصیت در هنگام ترکیب شدن با یکدیگر می توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می تواند به فروشگاه کامپیوتر نزدیک خود برود، یک نقطه دسترسی! بخرد و بدون کسب اجازه ای خاص به کل شبکه متصل شود. بسیاری از نقاط دسترسی با اختیارات مدیران میانی عرضه می شوند و لذا دپارتمان ها ممکن است بتوانند LAN بی سیمشان را بدون صدور اجازه از یک سازمان IT مرکزی در معرض عموم قرار دهند. این دسترسی به اصطلاح «نامطلوب» بکار گرفته شده توسط کاربران، خطرات امنیتی بزرگی را مطرح می کند. کاربران در زمینه امنیتی خبره نیستند و ممکن است از خطرات ایجاد شده توسط LAN های بی سیم آگاه نباشند. ثبت بسیاری از ورودها به شبکه نشان از آن دارد که ویژگی های امنیتی فعال نیستند و بخش بزرگی از آنها تغییراتی نسبت به پیکربندی پیش فرض نداشته اند و با همان پیکربندی راه اندازی شده اند.

۴-۳-۱ راه حل مشکل دوم: رسیدگی های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه های بی سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می گیرند، لذا آموختن نحوه یافتن شبکه های امن نشده از اهمیت بالایی برخوردار است.

روش بدیهی یافتن این شبکه ها انجام همان کاری است که نفوذگران انجام می دهند: استفاده از یک آنتن و جستجوی آنها به این منظور که بتوانید قبل از نفوذگران این شبکه ها را پیدا کنید. نظارت های فیزیکی سایت باید به صورت مرتب و در حد امکان انجام گیرد. اگرچه هرچه نظارت ها سریع تر انجام گیرد، امکان کشف استفاده های غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرف کنند، کشف تمامی استفاده های غیرمجاز را بجز برای محیط های بسیار حساس، غیرقابل توجیه می کند. یک راهکار برای عدم امکان حضور دائم می تواند انتخاب ابزاری در اندازه دستی باشد. این عمل می تواند استفاده تکنسین ها از اسکنرهای دستی در هنگام انجام امور پشتیبانی کاربران، برای کشف شبکه های غیرمجاز باشد.

یکی از بزرگترین تغییرات در بازار ۸۰۲.۱۱ در سال های اخیر ظهور a ۸۰۲.۱۱ به عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های ۸۰۲.۱۱ را بوجود آورد. خوشبختانه، a ۸۰۲.۱۱ از همان MAC پیشینان خود استفاده می کند، بنابراین بیشتر آنچه مدیران راجع به ۸۰۲.۱۱ و تحلیل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استاندارد a ۸۰۲.۱۱ و b ۸۰۲.۱۱ را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست های دوباندی a/b ۸۰۲.۱۱ و کارت های ساخته شده با آنها به آنالایزرها اجازه می دهد که روی هر دو باند بدون تغییرات سخت افزاری کار کنند، و این بدین معنی است که مدیران شبکه نیاز به خرید و آموزش فقط یک چارچوب پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا g ۸۰۲.۱۱ ادامه یابد، تا جایی که سازندگان آنالایزرها کارت های a/b/g ۸۰۲.۱۱ را مورد پذیرش قرار دهند.



بسیاری از ابزارها می توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می توانند در هر باند فرکانسی تعریف شده در ۸۰۲.۱۱ بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی های سایت بتوانند کل محدوده فرکانسی را پوشش دهند. حتی اگر شما استفاده از b ۸۰۲.۱۱ را انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی a ۸۰۲.۱۱ را نیز پوشش کند تا در طول یک بررسی کامل نیازی به جایگزین های سخت افزاری و نرم افزاری نباشد.

بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال های b ۸۰۲.۱۱ به کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال های ۱ تا ۱۱ از b ۸۰۲.۱۱ را می دهد. کانال های ۱۲ تا ۱۴ جزء مشخصات آن تعریف شده اند اما فقط برای استفاده در اروپا و ژاپن کاربرد دارند. به هر حال، بعضی کاربران ممکن است از نقطه دسترسی کانال های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال های مطابق با FCC از کانال های فرکانس بالاتر چشم پوشی کند. این قضیه مخصوصاً برای ردیابی ابزارهایی اهمیت دارد که بیرون باند فرکانسی مجاز بکارگرفته شده اند تا از اعمال اجرایی اتخاذ شده توسط نمایندگی های مجاز برحذر باشند. آنالایزرهای غیرفعال (Passive Analyzers) ابزار ارزشمندی هستند زیرا استفاده های غیرمجاز را تشخیص می دهند، اما چون توانی ارسال نمی کنند استفاده از آنها قانونی است.

مدیران شبکه همواره تحت فشار زمانی هستند، و به روش آسانی برای یافتن نقاط دسترسی نامطلوب و در عین حال چشم پوشی از نقاط دسترسی مجاز نیاز دارند. موتورهای جستجوی خبره به مدیران اجازه می دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند. هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده ای می شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس های قدرت سیگنال استفاده کنند. اگرچه این ابزارها ممکن است خیلی دقیق نباشند، ولی برای محدود کردن محوطه جستجوی نقطه دسترسی نامطلوب به اندازه کافی مناسب هستند.

۴-۴ مشکل سوم استفاده غیرمجاز از سرویس

چندین شرکت مرتبط با شبکه های بی سیم نتایجی منتشر کرده اند که نشان می دهد اکثر نقاط دسترسی با تنها تغییرات مختصری نسبت به پیکربندی اولیه برای سرویس ارائه می گردند. تقریباً تمام نقاط دسترسی که با پیکربندی پیش فرض مشغول به ارائه سرویس هستند، (WEP (Wired Equivalent Privacy را فعال

نکرده اند یا یک کلید پیش فرض دارند که توسط تمام تولیدکنندگان محصولات استفاده می شوند. بدون WEP دسترسی به شبکه به راحتی میسر است. دو مشکل به دلیل این دسترسی باز می تواند بروز کند: کاربران غیرمجاز لزوماً از مفاد ارائه سرویس تبعیت نمی کنند، و نیز ممکن است تنها توسط یک اسپم ساز اتصال شما به ISPتان لغو شود.

۴-۱-۴ راه حل مشکل سوم: طراحی و نظارت برای تأیید هویت محکم

راه مقابله مشخص با استفاده غیرمجاز، جلوگیری از دسترسی کاربران غیرمجاز به شبکه است. تأیید هویت محکم و محافظت شده توسط رمزنگاری یک پیش شرط برای صدور اجازه است، زیرا امتیازات دسترسی برپایه هویت کاربر قرار دارند. روش های VPN که برای حفاظت از انتقال در لینک رادیویی به کارگرفته می شوند، تأیید هویت محکم را ارائه می کنند. تخمین مخاطرات انجام شده توسط سازمان ها نشان می دهد که دسترسی به ۸۰۲.۱x باید توسط روش های تأیید هویت برپایه رمزنگاری تضمین شود. از جمله این روش ها می توان به TLS (Transport Layer Security)، TLS (Tunneled TLS) یا PEAP (Protected Extensible Authentication Protocol) اشاره کرد.

هنگامی که یک شبکه با موفقیت راه اندازی می شود، تضمین تبعیت از سیاست های تأیید هویت و اعطای امتیاز مبتنی بر آن حیاتی است. همانند مسأله نقاط دسترسی نامطلوب، در این راه حل نیز نظارت های منظمی بر تجهیزات شبکه بی سیم باید انجام شود تا استفاده از مکانیسم های تأیید هویت و پیکربندی مناسب ابزارهای شبکه تضمین شود. هر ابزار نظارت جامع باید نقاط دسترسی را در هر دو باند فرکانسی b ۸۰۲.۱۱ (باند GHz ISM 2.4) و a ۸۰۲.۱۱a (GHz U-NII 5) تشخیص دهد و پارامترهای عملیاتی مرتبط با امنیت را نیز مشخص کند. اگر یک ایستگاه غیرمجاز متصل به شبکه کشف شود، یک رسیور دستی می تواند برای ردیابی موقعیت فیزیکی آن استفاده شود. آنالایزرها نیز می توانند برای تأیید پیکربندی بسیاری از پارامترهای نقاط دسترسی استفاده گردند و هنگامی که نقاط دسترسی آسیب پذیری های امنیتی را نمایان می کنند، علائم هشدار دهنده صوتی تولید کنند.

۴-۵ مشکل چهارم: محدودیت های سرویس و کارایی

LAN های بی سیم ظرفیت های ارسال محدودی دارند. شبکه های b ۸۰۲.۱۱ سرعت انتقالی برابر با ۱۱ Mbps و شبکه های برپایه تکنولوژی جدید a ۸۰۲.۱۱ نرخ انتقال اطلاعاتی تا ۵۴ Mbps دارند. البته ماحصل مؤثر واقعی، به دلیل بالاسری لایه MAC، تقریباً تا نیمی از ظرفیت اسمی می رسد. نقاط دسترسی کنونی این ظرفیت محدود را بین تمام کاربران مربوط به یک نقطه دسترسی قسمت می کنند. تصور اینکه چگونه برنامه های محلی احتمالاً چنین ظرفیت محدودی را اشغال می کنند یا چگونه یک نفوذگر ممکن است یک حمله انکار سرویس (DoS) روی این منابع محدود طرح ریزی کند، سخت نیست.

ظرفیت رادیویی می تواند به چندین روش اشغال شود. ممکن است توسط ترافیکی که از سمت شبکه باسیم با نرخ بزرگتر از توانایی کانال رادیویی می آید، مواجه شود. اگر یک حمله کننده یک ping flood را از یک بخش اترنت سریع بفرستد، می تواند به راحتی ظرفیت یک نقطه دسترسی را اشغال کند. با استفاده از آدرس های broadcast امکان اشغال چندین نقطه دسترسی متصل به هم وجود دارد. حمله کننده همچنین می تواند ترافیک را به شبکه رادیویی بدون اتصال به یک نقطه دسترسی بی سیم تزریق کند. ۸۰۲.۱۱ طوری طراحی شده است که به چندین شبکه اجازه به اشتراک گذاری یک فضا و کانال رادیویی را می دهد. حمله کنندگانی که می خواهند شبکه بی سیم را از کار بیاندازند، می توانند ترافیک خود را روی یک کانال رادیویی ارسال کنند و شبکه مقصد ترافیک جدید را با استفاده از مکانیسم CSMA/CA تا آنجا که می تواند می پذیرد. مهاجمان بدانندیش که فریم های ناسالم می فرستند نیز ظرفیت محدود را پر می کنند. همچنین ممکن است مهاجمان تکنیک های تولید پارازیت رادیویی را انتخاب کنند و اقدام به ارسال اطلاعات با نویز بالا به شبکه های بی سیم مقصد کنند.

بارهای بزرگ ترافیک الزاماً با نیت بدخواهانه تولید نمی شوند. انتقال فایل های بزرگ یا سیستم client/server ترکیبی ممکن است مقادیر بالایی از دیتا روی شبکه ارسال کنند. اگر تعداد کافی کاربر شروع به گرفتن اندازه های بزرگی از دیتا از طریق یک نقطه دسترسی کنند، شبکه شبیه سازی دسترسی dial-up را آغاز می کند.

۴-۵-۱ راه حل مشکل چهارم: دیدبانی شبکه

نشان یابی مسائل کارایی با دیدبانی و کشف آنها آغاز می شود. مدیران شبکه بسیاری از کانال ها را برای کسب اطلاعات در مورد کارایی در اختیار دارند: از ابزارهای تکنیکی خاص مانند Simple (SNMP) Network Management Protocol گرفته تا ابزارهای بالقوه قوی غیرفنی مانند گزارش های کارایی کاربران. یکی از مسائل عمده بسیاری از ابزارهای تکنیکی، فقدان جزئیات مورد نیاز برای درک بسیاری از شکایت های کاربران در مورد کارایی است. آنالایزهای شبکه های بی سیم می توانند با گزارش دهی روی کیفیت سیگنال و سلامت شبکه در مکان کنونی خود، کمک باارزشی برای مدیر شبکه باشند. مقادیر بالای ارسال های سرعت پایین می تواند بیانگر تداخل خارجی یا دور بودن یک ایستگاه از نقطه دسترسی باشد. توانایی نشان دادن سرعت های لحظه ای روی هر کانال، یک تصویر بصری قوی از ظرفیت باقی مانده روی کانال می دهد که به سادگی اشغال کامل یک کانال را نشان می دهد. ترافیک مفرط روی نقطه دسترسی می تواند با تقسیم ناحیه پوشش نقطه دسترسی به نواحی پوشش کوچک تر یا با اعمال روش شکل دهی ترافیک در تلاقی شبکه بی سیم با شبکه اصلی تعیین شود.

در حالیکه هیچ راه حل فنی برای آسیب پذیری های ناشی از فقدان تأیید هویت فریم های کنترل و مدیریت وجود ندارد، مدیران می توانند برای مواجهه با آنها گام هایی بردارند. آنالیزها اغلب نزدیک محل های دردرساز استفاده می شوند تا به تشخیص عیب کمک کنند و به صورت ایده آل برای مشاهده بسیاری از حملات DoS کار گذاشته می شوند. مهاجمان می توانند با تغییر دادن فریم های ۸۰۲.۱۱ با استفاده از یکی از چندین روش معمول واسط های برنامه نویسی ۸۰۲.۱۱ موجود، از شبکه سوءاستفاده کنند. حتی یک محقق امنیتی ابزاری نوشته است که پیام های قطع اتصال فرستاده شده توسط نقاط دسترسی به کلاینت ها را جعل می کند. بدون تأیید هویت پیام های قطع اتصال بر اساس رمزنگاری، کلاینت ها به این پیام های جعلی عمل می کنند و اتصال خود را از شبکه قطع می کنند. تا زمانی که تأیید هویت به صورت یک فریم رمز شده استاندارد درنیاید، تنها مقابله علیه حملات جعل پیام، مکان یابی حمله کننده و اعمال عکس العمل مناسب است.

۴-۶ مشکل پنجم جعل MAC و session ربایی!

شبکه های ۸۰۲.۱۱ فریم ها را تأیید هویت نمی کنند. هر فریم یک آدرس مبدا دارد، اما تضمینی وجود ندارد که ایستگاه فرستنده واقعاً فریم را ارسال کرده باشد! در واقع همانند شبکه های اترنت سنتی، مراقبتی در مقابل جعل مبدا آدرس ها وجود ندارد. نفوذگران می توانند از فریم های ساختگی برای هدایت ترافیک و تخریب جداول (ARP (Address Resolution Protocol استفاده کنند. در سطحی بسیار ساده تر، نفوذگران می توانند آدرس های (MAC (Medium Access Control ایستگاه های در حال استفاده را مشاهده کنند و از آن آدرس ها برای ارسال فریم های بدخواهانه استفاده کنند. برای جلوگیری از این دسته از حملات، مکانیسم تصدیق هویت کاربر برای شبکه های ۸۰۲.۱۱ در حال ایجاد است. با درخواست هویت از کاربران، کاربران غیرمجاز از دسترسی به شبکه محروم می شوند. اساس تصدیق هویت کاربران استاندارد ۸۰۲.۱ x است که در ژوئن ۲۰۰۱ تصویب شده است. ۸۰۲.۱ x می تواند برای درخواست هویت از کاربران به منظور تأیید آنان قبل از دسترسی به شبکه مورد استفاده قرار گیرد، اما ویژگی های دیگری برای ارائه تمام امکانات مدیریتی توسط شبکه های بی سیم مورد نیاز است.

نفوذگران می توانند از فریم های جعل شده در حملات اکتیو نیز استفاده کنند. نفوذگران علاوه بر ربودن نشست ها (sessions) می توانند از فقدان تصدیق هویت نقاط دسترسی بهره برداری کنند. نقاط دسترسی توسط پخش فریم های Beacon (چراغ دریایی) مشخص می شوند. فریم های Beacon توسط نقاط دسترسی ارسال می شوند تا کلاینت ها قادر به تشخیص وجود شبکه بی سیم و بعضی موارد دیگر شوند. هر ایستگاهی که ادعا می کند که یک نقطه دسترسی است و (SSID (Service Set Identifier که معمولاً network name نیز نامیده می شود، منتشر می کند، به عنوان بخشی از شبکه مجاز به نظر خواهد رسید. به

هرحال، نفوذگران می توانند به راحتی تظاهر کنند که نقطه دسترسی هستند، زیرا هیچ چیز در ۸۰۲.۱۱ از نقطه دسترسی نمی خواهد که ثابت کند واقعاً یک نقطه دسترسی است. در این نقطه، یک نفوذگر می تواند با طرح ریزی یک حمله man-in-the-middle گواهی های لازم را سرقت کند و از آنها برای دسترسی به شبکه استفاده کند. خوشبختانه، امکان استفاده از پروتکل هایی که تأیید هویت دوطرفه را پشتیبانی می کنند در ۸۰۲.۱ وجود دارد. با استفاده از پروتکل (TLS (Transport Layer Security، قبل از اینکه کلاینت ها گواهی های هویت خود را ارائه کنند، نقاط دسترسی باید هویت خود را اثبات کنند. این گواهی ها توسط رمزنگاری قوی برای ارسال بی سیم محافظت می شوند. ربودن نشست حل نخواهد شد تا زمانی که ۸۰۲.۱۱ MAC تصدیق هویت در هر فریم را به عنوان بخشی از I ۸۰۲.۱۱ بپذیرد.

۴-۶-۱ راه حل شماره ۵: پذیرش پروتکل های قوی و استفاده از آنها

تا زمان تصویب ۸۰۲.۱۱ i جعل MAC یک تهدید خواهد بود. مهندسان شبکه باید روی خسارت های ناشی از جعل MAC تمرکز کنند و شبکه های بی سیم را تا آنجا که ممکن است از شبکه مرکزی آسیب پذیرتر جدا کنند. بعضی راه حل ها جعل AP (نقاط دسترسی) را کشف می کنند و به طور پیش فرض برای مدیران شبکه علائم هشدار دهنده تولید می کنند تا بررسی های بیشتری انجام دهند. در عین حال، می توان فقط با استفاده از پروتکل های رمزنگاری قوی مانند IPsec از نشست ربایی! جلوگیری کرد. آنالایزرها می توانند در بخشی از تحلیل فریم های گرفته شده، سطح امنیتی مورد استفاده را تعیین کنند. این تحلیل می تواند در یک نگاه به مدیران شبکه بگوید آیا پروتکل های امنیتی مطلوبی استفاده می شوند یا خیر.

علاوه بر استفاده از پروتکل های VPN قوی، ممکن است که تمایل به استفاده از تصدیق هویت قوی کاربر با استفاده از ۸۰۲.۱ داشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق x ۸۰۲.۱، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت x ۸۰۲.۱ ارائه می کند. هنگام انجام نظارت بر سایت، آنالایزر نوع تصدیق هویت را مشخص می کند و این بررسی به مدیران شبکه اجازه می دهد که محافظت از کلمات عبور توسط رمزنگاری قوی را تضمین کنند.

۴-۷ مشکل ششم: تحلیل ترافیک و استراق سمع

۸۰۲.۱۱ هیچ محافظتی علیه حملاتی که بصورت غیرفعال (passive) ترافیک را مشاهده می کنند، ارائه نمی کند. خطر اصلی این است که ۸۰۲.۱۱ روشی برای تامین امنیت دیتای در حال انتقال و جلوگیری از استراق سمع فراهم نمی کند. Header فریم ها همیشه «in the clear» هستند و برای هرکس با در اختیار داشتن یک آنالایزر شبکه بی سیم قابل مشاهده هستند. فرض بر این بوده است که جلوگیری از استراق سمع در مشخصات WEP (Wired Equivalent Privacy) ارائه گردد. بخش زیادی در مورد رخنه های WEP نوشته شده است که فقط از اتصال ابتدایی بین شبکه و فریم های دیتای کاربر محافظت می کند. فریم

های مدیریت و کنترل توسط WEP رمزنگاری و تصدیق هویت نمی شوند و به این ترتیب آزادی عمل زیادی به یک نفوذگر می دهد تا با ارسال فریم های جعلی اختلال به وجود آورد. پیاده سازی های اولیه WEP نسبت به ابزارهای crack مانند AirSnort و WEPCrack آسیب پذیر هستند، اما آخرین نسخه ها تمام حملات شناخته شده را حذف می کنند. به عنوان یک اقدام احتیاطی فوق العاده، آخرین محصولات WEP یک گام فراتر می روند و از پروتکل های مدیریت کلید برای تعویض کلید WEP در هر پانزده دقیقه استفاده می کنند. حتی مشغول ترین LAN بی سیم آنقدر دیتا تولید نمی کند که بتوان در پانزده دقیقه کلید را بازیافت کرد.

۴-۷-۱ راه مشکل ششم : انجام تحلیل خطر

هنگام بحث در مورد خطر استراق سمع، تصمیم کلیدی برقراری توازن بین خطر استفاده از WEP تنها و پیچیدگی بکارگیری راه حل اثبات شده دیگری است. در وضعیت فعلی برای امنیت لایه لینک، استفاده از WEP با کلیدهای طولانی و تولید کلید پویا توصیه می شود. WEP تا حد زیادی مورد کنکاش قرار گرفته است و پروتکل های امنیتی علیه تمام حملات شناخته شده تقویت شده اند. یک قسمت بسیار مهم در این تقویت، زمان کم تولید مجدد کلید است که باعث می شود نفوذگر نتواند در مورد خصوصیات کلید WEP، قبل از جایگزین شدن، اطلاعات عمده ای کسب کند.

اگر شما استفاده از WEP را انتخاب کنید، باید شبکه بی سیم خود را نظارت کنید تا مطمئن شوید که مستعد حمله AirSnort نیست. یک موتور آنالیز قوی به طور خودکار تمام ترافیک دریافت شده را تحلیل می کند و ضعف های شناخته شده را در فریم های محافظت شده توسط WEP بررسی می کند. همچنین ممکن است بتواند نقاط دسترسی و ایستگاه هایی را که WEP آنها فعال نیست نشان گذاری کند تا بعداً توسط مدیران شبکه بررسی شوند. زمان کوتاه تولید مجدد کلید ابزار بسیار مهمی است که در کاهش خطرات مربوط به شبکه های بی سیم استفاده می شود. بعنوان بخشی از نظارت سایت، مدیران شبکه می توانند از آنالیزهای قوی استفاده کنند تا مطمئن شوند که سیاست های تولید کلید مجدد WEP توسط تجهیزات مربوطه پیاده سازی شده اند.

اگر از LAN بی سیم شما برای انتقال دیتای حساس استفاده می شود، ممکن است WEP برای نیاز شما کافی نباشد. روش های رمزنگاری قوی مانند SSH، SSL و IPsec برای انتقال دیتا به صورت امن روی کانال های عمومی طراحی شده اند و برای سال ها مقاومت آنها در برابر حملات ثابت شده است، و یقیناً سطوح بالاتری از امنیت را ارائه می کنند. نمایشگرهای وضعیت نقاط دسترسی می توانند بین نقاط دسترسی که از WEP، 802.1x و VPN استفاده می کنند، تمایز قائل شوند تا مدیران شبکه بتوانند بررسی کنند که آیا در آنها از سیاست های رمزنگاری قوی تبعیت می شود یا خیر.

علاوه بر استفاده از پروتکل های VPN قوی، ممکن است که تمایل به استفاده از تصدیق هویت قوی کاربر با استفاده از X ۸۰۲.۱ داشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق X ۸۰۲.۱، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت X ۸۰۲.۱ ارائه می کند. آنالیزر هنگام انجام نظارت بر سایت، نوع تصدیق هویت را مشخص می کند و این بررسی به مدیران شبکه اجازه می دهد که محافظت از کلمات عبور توسط رمزنگاری قوی را تضمین کنند.

۸-۴ مشکل هفتم: حملات سطح بالاتر

هنگامی که یک نفوذگر به یک شبکه دسترسی پیدا می کند، می تواند از آنجا به عنوان نقطه ای برای انجام حملات به سایر سیستم ها استفاده کند. بسیاری از شبکه ها یک پوسته بیرونی سخت دارند که از ابزار امنیت پیرامونی تشکیل شده، به دقت پیکربندی شده و مرتب دیده بانی می شوند. اگرچه درون پوسته یک مرکز آسیب پذیر نرم قرار دارد. LAN های بی سیم می توانند به سرعت با اتصال به شبکه های اصلی آسیب پذیر مورد استفاده قرار گیرند، اما به این ترتیب شبکه در معرض حمله قرار می گیرد. بسته به امنیت پیرامون، ممکن است سایر شبکه ها را نیز در معرض حمله قرار دهد، و می توان شرط بست که اگر از شبکه شما به عنوان نقطه ای برای حمله به سایر شبکه ها استفاده شود، حسن شهرت خود را از دست خواهید داد.

۸-۴-۱ راه حل مشکل هفتم: هسته را از LAN بی سیم محافظت کنید

به دلیل استعداد شبکه های بی سیم برای حمله، باید به عنوان شبکه های غیرقابل اعتماد مورد استفاده قرار بگیرند. بسیاری از شرکت ها درگاه های دسترسی guest در اتاق های آموزش یا سالن ها ارائه می کنند. شبکه های بی سیم به دلیل احتمال دسترسی توسط کاربران غیرقابل اعتماد می توانند به عنوان درگاه های دسترسی guest تصور شوند. شبکه بی سیم را بیرون منطقه پیرامون امنیتی شرکت قرار دهید و از تکنولوژی کنترل دسترسی قوی و ثابت شده مانند یک فایروال بین LAN بی سیم و شبکه مرکزی استفاده کنید، و سپس دسترسی به شبکه مرکزی را از طریق روش های VPN تثبیت شده ارائه کنید.

۹-۴ چند نکته در مورد امن سازی شبکه های وای فای

۹-۴-۱ کلمه عبور پیش فرض مدیر سیستم (administrator) را روی نقاط دسترسی و مسیریاب های

بی سیم تغییر دهید.

اغلب نقاط دسترسی (Access Point) و مسیریاب های بی سیم امکان مدیریت شبکه WiFi را از طریق یک حساب کاربری مدیریتی فراهم می کنند. این حساب کاربری امکان دسترسی ابزار و پیکربندی آن را با نام کاربری و کلمه عبور فراهم می کند. اغلب تولیدکنندگان نام کاربری و کلمه عبور را در کارخانه تنظیم

می‌کند. نام کاربری معمول admin یا administrator و کلمه عبور یا خالی است یا کلماتی مثل admin ، public ، password و می‌باشد.

اولین گام برای افزایش امنیت شبکه بی‌سیم تغییر کلمه عبور پیش فرض نقاط دسترسی و مسیریاب‌های بی‌سیم بلافاصله پس از نصب است. اغلب ابزارها اجازه تغییر نام کاربری را نمی‌دهند اما اگر ابزارهای شما این امکان را می‌دهند، اکیدا توصیه می‌شود که نام کاربری را هم تغییر دهید. برای امن نگه داشتن شبکه در آینده، می‌بایست به طور منظم این کلمه عبور را تغییر دهید. اغلب کارشناسان توصیه می‌کنند کلمه عبور را بعد از ۳۰ تا ۹۰ روز تغییر دهید.

۴-۹-۲ فعال‌سازی قابلیت WPA/WEP

WPA (WiFi Protected Access) یک استاندارد امنیتی برای شبکه‌های بی‌سیم است (با Windows XP Product Activation اشتباه نشود). برای استفاده از WPA با Windows XP باید Client‌های دارای Windows XP را به صورت دستی patch کنید و همچنین مطمئن شوید کارت شبکه‌ها و نقاط دسترسی به درستی پیکربندی شده‌اند. برای پیکربندی WPA در شبکه با client‌های دارای ویندوز XP مراحل زیر را انجام دهید:

۱. نوشتار Overview of the WPA wireless security update in Windows XP را مطالعه کنید.
۲. بررسی کنید که تمام Client ها حداقل Service Pack 1 داشته باشند.
۳. روی هر Client بررسی کنید که کارت شبکه با سرویس WZC (Windows Zero Configuration) سازگار باشد.
۴. برای هر client وصله Windows XP Support Patch for Wi-Fi Protected Access را بارگزاری و نصب کنید.
۵. تغییرات لازم برای نقاط دسترسی بی‌سیم از گام ۱ را اعمال کنید.

۴-۹-۳ تغییر SSID پیش فرض

نقاط دسترسی و مسیریاب‌های بی‌سیم دارای یک نام شبکه (SSID) (Service Set Identifier) هستند که توسط تولیدکنندگان به طور پیش فرض انتخاب می‌شود. SSID از ابزارهای پیکربندی بر مبنای وب یا ویندوز این سازندگان قابل دسترسی است. اغلب SSIDهای پیش فرض کلمات ساده‌ای مثل netgear, wireless, default, linksys و ... هستند. هرچند نفوذگر صرفا با دانستن SSID قادر به نفوذ به شبکه شما نیست ولی این مساله به عنوان یک نقطه شروع خوب برای نفوذگر به حساب می‌آید. زمانی که کسی شبکه‌ای با

SSID پیش فرض بیابند، با دانستن این نکته که به احتمال فراوان این شبکه به درستی پیکربندی نشده است، ترغیب به نفوذ به شبکه می شود.

SSID می تواند هر زمانی تغییر کند به شرطی که این تغییر در تمام clientها نیز اعمال شود. برای افزایش امنیت شبکه های بی سیم، نام پیش فرض SSID را تغییر دهید. در انتخاب SSID توصیه های زیر را در نظر داشته باشید:

۱. از نام، آدرس، تاریخ تولد، شماره تلفن یا دیگر اطلاعات شخصی تان به عنوان بخشی از SSID استفاده نکنید.
۲. از کلمات عبور نام کاربری ویندوزتان یا emailتان یا ... استفاد نکنید.
۳. با استفاده از عباراتی مثل "FUNNY_BOX, TOP_SECRET" و ... نفوذگران را وسوسه نکنید!!!
۴. از ترکیب حروف و اعداد استفاده کنید.
۵. عباراتی با طول حداکثر یا نزدیک به حداکثر انتخاب کنید.
۶. هر چند ماه یک بار SSIDتان را تغییر دهید.

۴-۹-۴ قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیریاب های بی سیم فعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم دارای قابلیتی به نام پالایش آدرس MAC (Address Filtering) هستند. این مشخصه اغلب به طور پیش فرض فعال نیست. برای افزایش امنیت شبکه بی سیم تان این قابلیت را فعال کنید. در صورتی که این قابلیت فعال نباشد، هر clientی با دانستن SSID شبکه شما (در نظر داشته باشید که فهمیدن SSID کار بسیار ساده ای است) شاید چند پارامتر امنیتی دیگر مثل کلید رمزگذاری (در صورتی که قابلیت WEP فعال باشد) می تواند به شبکه شما وصل شود.

برای تنظیم قابلیت پالایش آدرس MAC شما به عنوان مدیر شبکه بی سیم باید لیست clientهایی که مجازند به شبکه وصل شوند را پیکربندی کنید. ابتدا آدرس MAC هر client را از طریق سیستم عامل یا ابزارهای پیکربندی به دست آورید و سپس آن ها را در صفحه پیکربندی نقاط دسترسی و مسیریاب های بی سیم وارد کنید و نهایتاً قابلیت پالایش را فعال کنید. از این پس هر درخواست اتصال به شبکه بی سیم که برسد آدرس MAC آن با لیست تنظیم شده بررسی شده و در صورتی که در لیست نباشد اجازه اتصال به

شبکه را نمی یابد. البته باید توجه داشت که نفوذگران با جعل آدرس (MAC Spoofing) (MAC) قادرند به شبکه بی سیم شما وصل شوند ولی این مساله نباید باعث شود که شما از خیر این قابلیت بگذرید.

۴-۹-۵ قابلیت همه پخشی SSID را روی نقاط دسترسی و مسیریاب های بی سیم غیرفعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم به طور خودکار SSID خوشان را در فواصل زمانی مشخص پخش می کنند. این مشخصه برای این است که clientها بتوانند به طور پویا شبکه های بی سیم را تشخیص دهند و بین آن ها جابه جا شوند (از شبکه ای به شبکه دیگر نقل مکان کنند). لازم به ذکر است که این مشخصه برای hotspotهای تجاری و سیار طراحی شده است که clientهای زیادی می آیند و می روند ولی برای شبکه های خانگی لازم نیست. از آن جایی که SSID به صورت واضح پخش می شود و هیچ رمزگذاری روی آن صورت نمی گیرد، به دست آوردن آن توسط نفوذگران کار راحتی است. همان طور که در گام ۳ اشاره شد نفوذگر با دانستن SSID یک مرحله به هدف نزدیک تر می شود.

در یک شبکه بی سیم بحث roaming (جابه جایی بین دو شبکه بی سیم) مطرح نیست و پخش کردن SSID هیچ ضرورتی ندارد. برای افزایش امنیت شبکه بی سیم باید این قابلیت را غیرفعال کنید. یک بار که client شما با SSID درست پیکربندی شد دیگر نیازی به پیغام های همه پخشی نیست.

دقت داشته باشید که غیرفعال کردن قابلیت همه پخشی SSID فقط یکی از تکنیک های محکم سازی و افزایش امنیت شبکه های بی سیم است. این روش ۱۰۰ درصد موثر نیست و نفوذگرها هنوز می توانند با sniff کردن پیغام های مختلف پخش شده در پروتکل WiFi، SSID را تشخیص دهند. در واقع تکنیک هایی مثل غیرفعال کردن همه پخشی SSID باعث می شند که شبکه بی سیم شما هدف راحتی برای نفوذگران نباشد.

۴-۹-۶ به شبکه های WiFi باز وصل نشوید

مطمئن شوید که تنظیمات سیستم به گونه ای است که مانع اتصال خودکار به نقاط دسترسی ناامن شود. اتصال به یک شبکه WiFi باز مثل یک hotspot یا مسیریاب بی سیم آزاد، کامپیوتر شما را در معرض خطرات فراوانی قرار می دهد. هرچند به طور معمول این امکان فعال نیست ولی اغلب کامپیوترها دارای تنظیماتی هستند که امکان اتصال خودکار بدون اطلاع کاربر را فراهم می کنند. این تنظیمات به جز در موارد ضروری و به طور موقت نباید فعال باشد.

برای بررسی این که آیا اتصال خودکار به شبکه های WiFi باز، مجاز است یا نه، تنظیمات بی سیم کامپیوتر را بررسی کنید. برای مثال در کامپیوترهایی که دارای Windows XP هستند، تنظیمات بی سیم

Automaticly connect to non-preferred networks نامیده می شود. برای بررسی مراحل زیر را انجام دهید:

۱. از منوی start به گزینه Windows Control Panel بروید.
۲. به گزینه Network Connections بروید
۳. بر روی Wireless Network Connection کلیک راست کنید و گزینه Properties را انتخاب کنید.
۴. روی گزینه Wireless Networks کلیک کنید.
۵. بر روی دکمه Advanced کلیک کنید.
۶. گزینه Automatically connect to non-preferred networks را پیدا کنید، اگر انتخاب شده بود این تنظیمات فعال است در غیر این صورت غیرفعال است.

اگرچه در Windows XP به طور پیش فرض Automatically connect to non-preferred networks فعال نیست، برخی کاربران برای سهولت اتصال به شبکه خودشان آن را فعال می کنند. کاربران باید شبکه خودشان را به عنوان Windows XP Preferred networks تنظیم کنند که اجازه اتصال خودکار را می دهد و اتصال خودکار به بقیه شبکه ها را غیرفعال کنند.

۴-۹-۷ به تجهیزات آدرس (IP) ایستا اختصاص دهید.

اختصاص آدرس ایستا جایگزینی برای پروتکل DHCP است. اختصاص آدرس پویا با استفاده از DHCP راحت تر است و هم چنین به کامپیوترهای سیار اجازه می دهد که بین شبکه های مختلف جابه جا شوند.

آدرس دهی ایستا نیز مزایایی دارد، از جمله:

- آدرس ثابت ترجمه آدرس را بهتر پشتیبانی می کند، بنابراین یک کامپیوتر روی شبکه با نام دامنه اش به طور مطمئن قابل دستیابی است. مخصوصا سرورهایی مثل سرور وب و سرور FTP بهتر است آدرس ایستا داشته باشند.
- استفاده از آدرس دهی ایستا در مقابل DHCP محافظت بیشتری در برابر حملات امنیتی فراهم می کند.
- برخی تجهیزات شبکه پروتکل DHCP را پشتیبانی نمی کنند.
- استفاده از آدرس دهی ایستا برای تمام اجزای شبکه تضمین می کند که ناسازگاری آدرس ها رخ نمی دهد.

آدرس های ایستا باید از محدوده آدرس های خصوصی استاندارد انتخاب شود از جمله:

۱. "۱۰.۰.۰.۰" تا "۱۰.۲۵۵.۲۵۵.۲۵۵"

۲. "۱۷۲.۱۶.۰.۰" تا "۱۷۲.۳۱.۲۵۵.۲۵۵"

۳. "۱۹۲.۱۶۸.۰.۰" تا "۱۹۲.۱۶۸.۲۵۵.۲۵۵"

این محدوده ها تعداد زیادی آدرس را پشتیبانی می کنند. برخلاف تصور اکثر افراد، تمام آدرس های این محدوده ها نمی توانند انتخاب شوند. برای انتخاب آدرس درست نکات زیر را مدنظر داشته باشد:

۱. آدرس هایی که با "۰" یا "۲۵۵" تمام می شوند را انتخاب نکنید. این آدرس ها برای استفاده پروتکل های شبکه رزرو شده اند.

۲. آدرس های ابتدای یک محدود آدرس خصوصی را انتخاب نکنید. آدرس هایی مثل "۱۰.۰.۰.۱" یا "۱۹۲.۱۶۸.۰.۱" معمولاً به مسیریاب های شبکه اختصاص می یابند. این آدرس ها اولین آدرس هایی هستند که معمولاً یک نفوذگر تلاش می کند به آن ها نفوذ کند، بنابراین بهتر است از آن ها استفاده نکنید.

۳. از آدرس هایی که خارج از محدوده mask شبکه شما می باشد استفاده نکنید. برای مثال، برای پشتیبانی تمام آدرس های محدوده "۱۰.x.x.x" mask شبکه برای تمام سیستم ها باید به "۲۵۵.۰.۰.۰" تنظیم شود، در غیراین صورت برخی آدرس های ایستای این محدوده کار نمی کنند.

۴-۹-۸ قابلیت فایروال را روی تمام کامپیوترها و مسیریاب ها فعال کنید

یکی از آسان ترین و ارزان ترین راه ها برای محافظت از شبکه در برابر حملات استفاده از فایروال شخصی است.

۴-۹-۹ مسیریاب ها و نقاط دسترسی را در مکان های امن قرار دهید

کارایی شبکه Wi-Fi به میزان زیادی بستگی به قدرت سیگنال مسیریاب یا نقطه دسترسی بی سیم دارد. اگر یک client بی سیم خارج از محدوده قدرت سیگنال قرار بگیرد ارتباط آن با شبکه قطع می شود یا ارتباط بسیار ضعیف می باشد. Client های بی سیم واقع شده در لبه شبکه ممکن است به دفعات زیاد ارتباطشان قطع شود، ولی حتی زمانی که یک Client بی سیم در محدوده قدرت سیگنال هم باشد، کارایی شبکه از مواردی همچون فاصله، انسداد، یا تداخل تاثیر می گیرد.

برای تعیین محل قرار گرفتن تجهیزات بی سیم نکات زیر را مدنظر داشته باشد:

- اولین و مهم ترین نکته این است که، از قبل جایی را برای مسیریاب یا نقطه دسترسی بی سیم در نظر نگیرید. سعی کنید تجهیزات را در چندین نقطه متفاوت امتحان کنید. با وجود این که روش آزمون و خطا راهکار علمی برای یافتن محل قرارگیری تجهیزات بی سیم نیست اما از دیدگاه عملی بهترین روش برای به دست آوردن حداکثر کارایی است.
- سعی کنید مسیریاب یا نقطه دسترسی بی سیم را نزدیک به مرکز قرار دهید. Client هایی که از ایستگاه مرکزی فاصله بیشتری دارند، در مقایسه با Client هایی که نزدیک ایستگاه مرکزی هستند، فقط از ۱۰ تا ۵۰ درصد پهنای باند بهره مند می شوند.
- تا حد امکان سعی کنید از موانع فیزیکی دوری کنید. هرگونه مانعی در فاصله خط دید بین Client و ایستگاه مرکزی باعث کاهش قدرت سیگنال می شود. دیوارهای آجری، خشتی، یا ساروج اندود بیش ترین تاثیر منفی را دارند ولی موانع دیگر نیز باعث کاهش قدرت سیگنال می شوند.
- تا حد امکان از سطوح بازتابی اجتناب کنید. برخی سطوح بازتابی مثل پنجره ها، آینه ها و ... باعث کاهش محدوده قدرت سیگنال های WiFi و در نتیجه کارایی شبکه می شود.
- مسیریاب یا نقطه دسترسی بی سیم را حداقل به فاصله یک متر از دیگر تجهیزاتی که در محدوده فرکانس مشابه سیگنال بی سیم می فرستند قرار دهید. این ابزارها می تواند شامل تلفن بی سیم، اجاق های مایکروویو و ... باشد.
- همچنین مسیریاب یا نقطه دسترسی بی سیم را دور از تجهیزات الکتریکی که باعث ایجاد تداخل می شوند قرار دهید.
- اگر مکان مناسبی که پیدا کردید فقط به طور مرزی قابل قبول شود، آنتن های ایستگاه مرکزی را برای بهبود کارایی تنظیم کنید. می توانید آنتن های مسیریاب و نقاط دسترسی بی سیم را بچرخانید و محل آن را تغییر دهید، دستورالعمل های کارخانه سازنده را اعمال کنید تا بهترین کارایی را به دست آورید.
- اگر با استفاده از این نکات و دستورالعمل ها باز هم مشکل دارید، می توانید به عنوان مثال آنتن های خود را تغییر دهید، یک تکرارکننده نصب کنید، یا در مواردی ایستگاه مرکزی دیگری پیکربندی و استفاده کنید.

۴-۹-۱۰ در فواصل زمانی طولانی که از شبکه استفاده نمی کنید تجهیزات را خاموش کنید.

اغلب ارتباطات اینترنت باندپهن همیشه برخط هستند. به همین خاطر دارندگان شبکه ترجیح می دهند اکثر تجهیزات شبکه مثل مسیریاب یا مودم روشن بماند حتی اگر برای مدت های طولانی بدون استفاده

باشند. ولی آیا شبکه های محلی هم لازم است همیشه روشن بمانند؟ خاموش کردن تجهیزات شبکه چه مزایا و معایبی دارد؟

در ادامه برخی از مزایا و معایب خاموش کردن تجهیزات شبکه را هنگامی که استفاده ای از آن ها نمی شود، بررسی می کنیم:

امنیت: خاموش کردن تجهیزات شبکه زمانی که در حال استفاده نیستند، باعث افزایش امنیت شبکه می شود. زمانی که تجهیزات شبکه خاموش باشند نفوذگران قادر به انجام کاری نیستند.

صرفه جویی در مصرف برق: خاموش کردن تجهیزات شبکه باعث صرفه جویی در هزینه ها می شود. در برخی کشورها این صرفه جویی چندان قابل توجه نیست اما در برخی کشورها نیز به علت بالا بودن هزینه انرژی میزان قابل توجهی است.

محافظت در برابر اعوجاج سیگنال: جدا کردن تجهیزات شبکه باعث جلوگیری از خرابی های احتمالی منتج از اعوجاج سیگنال می شود. ممکن است گفته شود که محافظ ها هم قادرند از ابزارها در برابر اعوجاج مراقبت کنند ولی این محافظ ها به خصوص انواع ارزان قیمت آن قادر به مراقبت در برابر نوسانات شدید نیستند.

قابلیت اطمینان سخت افزار: قطع و وصل مدام منبع انرژی تجهیزات شبکه باعث کاهش طول عمر آن ها می شود. دیسک درایوها اغلب آسیب پذیر هستند. به عبارت دیگر، دمای زیاد هم باعث کاهش طول همه ابزارهای شبکه می شود. همیشه روشن گذاشتن تجهیزات شبکه در مقایسه با زمانی که تجهیزات گهگاه خاموش می شوند، احتمالا باعث آسیب های بیش تری می شود.

قابلیت اطمینان ارتباطات: بعد از خاموش و روشن کردن تجهیزات ممکن است فرآیند برقراری ارتباط مجدد با خطا مواجه شود. باید فرآیند راه اندازی مجدد را با احتیاط دنبال کنید. به عنوان مثال باید ابتدا مودم های باندپهن روشن شوند و ابزارهای دیگر پس از این که مودم آماده شد، روشن شوند. همچنین اگر هنگام راه اندازی یا نصب با خطایی مواجه می شوید حتما راه حلی برای آن پیدا کنید در غیراین صورت ممکن است در آینده منجر به مشکلات بزرگ تری شود.

سهولت: تجهیزات شبکه مثل مسیریاب بی سیم یا مودم ممکن است در مکان هایی مثل سقف یا مکان هایی که دسترسی به آن ها سخت است قرار داشته باشد. هنگام خاموش کردن این تجهیزات احتیاط نموده و به جای استفاده از دکمه خاموش و روشن کردن تجهیزات، رویه های توصیه شده توسط کارخانه سازنده را حتما رعایت کنید.

۴-۱۰ پنج اشتباه متداول درباره امنیت شبکه های بی سیم

۴-۱۰-۱ دیواره آتش = تأمین امنیت کامل در برابر ورود غیرمجاز به شبکه

اغلب سازمان ها، شبکه های بی سیم را به عنوان بخش مکملی برای شبکه سیمی خود راه اندازی می کنند. اتصال بی سیم، یک رسانه فیزیکی است و برای تأمین امنیت آن نمی توان تنها به وجود یک دیوار آتش تکیه کرد. کاملاً واضح است که نقاط دسترسی غیرمجاز، به واسطه ایجاد راه های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آن ها، نوعی تهدید علیه شبکه به شمار می روند. علاوه بر این نقاط دسترسی، باید نگران لپ تاپ های بی سیم متصل به شبکه سیمی خود نیز باشید. یافتن لپ تاپ های متصل به شبکه سیمی که یک کارت شبکه بی سیم فعال دارند، اقدامی متداول برای ورود به شبکه محسوب می شود. در اغلب موارد این لپ تاپ ها توسط SSID شبکه هایی را که قبلاً مورد دسترسی قرار داده اند، جست و جو می کنند و در صورت یافتن آن ها صرف نظر از این که اتصال به شبکه قانونی یا مضر باشد یا شبکه بی سیم در همسایگی شبکه فعلی قرار داشته باشد، به طور خودکار به آن وصل می شوند. به محض این که لپ تاپ به یک شبکه مضر متصل شود، مهاجمان آن را مورد حمله قرار داده و پس از اسکن و یافتن نقاط ضعف ممکن است کنترل آن را به دست گرفته و به عنوان میزبانی برای اجرای حمله ها به کار گیرند. در این شرایط علاوه بر افشای اطلاعات مهم لپ تاپ، مهاجم می تواند از آن به عنوان نقطه شروعی برای حمله به شبکه سیمی استفاده کند. مهاجم در صورت انجام چنین اقداماتی، به طور کامل از دیواره آتش شبکه عبور می کند.

اغلب سازمان ها دیواره آتش شبکه را به گونه ای تنظیم می کنند که از آن ها در برابر حمله های مبتنی بر اینترنت محافظت می کند، اما امنیت شبکه در مقابل خروج از شبکه (Extrusion) و خروج غیرمجاز اطلاعات (leakage) تأمین نمی شود. اصولاً زمانی که درباره خروج غیرمجاز اطلاعات صحبت می کنیم، منظورمان خروج اطلاعات از شبکه است.

بسیاری از سازمان ها تنظیمات دیواره آتش را برای کنترل ترافیک اطلاعات خروجی به درستی انجام نمی دهند. در نتیجه این سهل انگاری معمولاً اطلاعات محرمانه سازمان به خارج منتقل می شود. به عنوان مثال، یکی از متداول ترین مواردی که هنگام انجام آزمون های امنیتی با آن مواجه شدیم، خروج اطلاعات شبکه سیمی از طریق نقاط دسترسی بی سیم بود. در این آزمون ها با استفاده از یک نرم افزار ردیاب (Sniffer) بی سیم توانستیم حجم زیادی از ترافیک اطلاعات خروجی ناخواسته را شناسایی کنیم. این اطلاعات شامل داده های مربوط به STP (سرنام Spanning Tree Protocol, IGRP) سایر سرویس های شبکه و حتی در مواردی اطلاعات مربوط به NetBIOS بودند.

چنین نقطه ضعفی شبکه را به یک اسباب سرگرمی برای مهاجم تبدیل می کند. در حقیقت، نفوذ به چنین شبکه ای حتی نیازمند یک اسکن فعال یا حمله واقعی نیست. به واسطه ردیابی جریان اطلاعاتی یک شبکه

بی سیم علاوه بر شناسایی توپولوژی بخش سیمی آن می توان اطلاعات مربوط به تجهیزات حیاتی شبکه و حتی گاهی اطلاعات مربوط به حساب های کاربری را به دست آورد.

۲-۱۰-۴ دیواره آتش = تأمین امنیت کامل در برابر ورود غیرمجاز به شبکه

این تصور اشتباه، بسیار گیج کننده است. چگونه می توان بدون اسکن شبکه از نبود تجهیزات بی سیم در آن مطمئن شد؟! در محل هایی که شبکه های LAN بی سیم راه اندازی نشده اند، علاوه بر نقاط دسترسی غیرمجاز، می توان از شبکه های Ad-Hoc، دسترسی تصادفی لپ تاپ ها و ایجاد پل های ارتباطی با شبکه، به عنوان تهدیدات بالقوه برای امنیت شبکه نام برد. دسترسی تصادفی لپ تاپ های بی سیم یک خطر امنیتی برای صاحبان این لپ تاپ ها محسوب می شود. اگر شرکت مجاور شما از یک نقطه دسترسی بی سیم یا یک شبکه Ad-Hoc استفاده می کند، احتمال اتصال تصادفی لپ تاپ های بی سیم عضو شبکه شما به این شبکه های بی سیم زیاد است. این اتصال نوعی خروج از شبکه است. مهاجمان نحوه بهره برداری از این شرایط را به خوبی می دانند و در نتیجه می توانند از یک نقطه دسترسی نرم افزاری یا Soft AP (نرم افزاری که از روی یک لپ تاپ اجرا می شود) برای ارسال شناسه های SSID موجود روی لپ تاپ به یک کامپیوتر خارج از شبکه و حتی ارسال آدرس IP لپ تاپ برای کامپیوتر خارجی استفاده کنند. چنان که گفته شد، این نقطه ضعف امکان کنترل لپ تاپ و حمله به شبکه سیمی را برای مهاجمان فراهم می کند. به علاوه، مهاجمان می توانند از طریق لپ تاپ، حمله های MITM (سرنام Man In The Middle) یا سرقت هویت را به اجرا در آورند.

۳-۱۰-۴ اسکن دستی = شناسایی تمام نقاط دسترسی غیرمجاز

در این مورد، تلاش مدیران شبکه برای اتخاذ یک رویکرد پیش گیرانه به منظور شناسایی نقاط دسترسی غیرمجاز در شبکه قابل تقدیر است. اما متأسفانه ابزارهایی که در اختیار این افراد قرار دارد، کارایی لازم را برای شناسایی نقاط دسترسی غیرمجاز ندارد. به عنوان مثال، بسیاری از مدیران شبکه از ابزارهای مدیریتی اسکن نقاط ضعف شبکه های سیمی به منظور شناسایی نقاط دسترسی غیرمجاز متصل به شبکه استفاده می کنند. تجربه کاری نگارنده با ابزارهای اسکن نقاط ضعف از هر دو نوع این سورس و تجاری، بیانگر این است که اغلب مدیران شبکه با تعداد انگشت شماری نقطه دسترسی مواجه می شوند که توسط سیستم عامل شناسایی شده است و هنگامی که شبکه را اسکن می کنند، این تجهیزات در قالب یک سیستم مبتنی بر لینوکس همراه یک وب سرور شناسایی می شوند. هنگام اسکن شبکه های Class C و بزرگ تر، دستگاه های غیرمجاز بین سایر تجهیزات شبکه پنهان شده و نتایج حاصل از اسکن شبکه برای شناسایی نقاط دسترسی غیرمجاز حقیقی نیست.

کارکرد ابزارهای اسکن بی سیم مانند NetStumbler و Kismet بسیار خوب است، اما زمانی که نوبت به شناسایی نقاط دسترسی غیرمجاز می رسد، این ابزارها از کارایی لازم برخوردار نیستند. به عنوان نمونه این ابزارها نمی توانند مشخص کنند که نقاط دسترسی شناسایی شده واقعاً به شبکه شما متصل هستند یا خیر. علاوه بر این، در تعیین موقعیت تقریبی دستگاه بی سیم مشکوک نیز دچار مشکل می شوند. اگر شرکت شما در یک ساختمان چندطبقه یا یک برج قرارداد، باید امواج دریافتی آنتن های بزرگ و دستگاه های منتشرکننده سیگنال را نیز به این مشکلات بیافزایید. در چنین شرایطی یک مدیر شبکه با مهارت متوسط در ردگیری و شناسایی تجهیزات بی سیم شبکه با مشکلات بزرگی روبه رو خواهد شد.

۴-۱۰-۴ به روزرسانی تمام نقاط دسترسی به منظور حذف پروتکل WEP = تأمین امنیت کامل شبکه

پروتکل WEP سالیان دراز مورد حمله مهاجمان قرار گرفته است. علاوه بر این، براساس اعلان PCI پروتکل WEP باید تا ماه ژوئن سال ۲۰۱۰ به طور کامل کنار گذاشته شود. بعضی از شرکت ها نیز به سراغ روش های توانمندتر کدگذاری و اعتبارسنجی رفته اند.

برای جایگزینی این پروتکل، چندگزینه مختلف وجود دارد. متأسفانه بعضی از این گزینه ها نیز دارای نقاط ضعف هستند. به عنوان مثال، نسخه PSK (سرنام Pre-Shared Key) از پروتکل WPA به دلیل نیاز به انتشار اطلاعات موردنیاز برای ساخت و تأیید کلید رمزگشایی اطلاعات، در مقابل نوعی حمله Offline که روی واژه نامه آن انجام می شود، آسیب پذیر است. برای اجرای این حمله ها چندین ابزار مختلف شامل coWPAtty و aircrack-ng وجود دارد. اغلب حمله ها شامل گردآوری تعداد زیادی از بسته های اطلاعاتی و استفاده از ابزار درمقابل سیستم دریافت بسته های اطلاعاتی است. بسته نرم افزاری Backtrack 3 تمام ابزارهای لازم را برای اجرای این نوع حمله ها فراهم می کند. در نوامبر سال ۲۰۰۸ به منظور اثبات این ضعف، پروتکل TKIP هک شد.

در این حمله صرف نظر از به کارگیری سیستم اعتبارسنجی PSK یا x۸۰۲.۱ مهاجمان توانستند به تمام نسخه های پروتکل TKIP شامل WPA و WPA2 نفوذ کنند. با وجود این، کلیدهای TKIP شناسایی نشدند و در نتیجه محتوای تمام قاب های کدشده افشا نشد. یک حمله می تواند در هر دقیقه یک بایت از داده های یک بسته اطلاعاتی رمزنگاری شده را افشا کرده و به ازای هر بسته کدگشایی شده تا پانزده قاب رمزنگاری شده را به سیستم تحمیل می کند. چنین سیستمی، یک گزینه مناسب برای آلودگی ARP محسوب می شود. درک این نکته ضروری است که آن دسته از شبکه های WPA و WPA2 که الگوریتم های کدگذاری AES-CCMP پیچیده تر را مورد استفاده قرار می دهند، در برابر حمله ها مقاوم تر هستند و استفاده از چنین الگوریتم هایی به عنوان بهترین رویکرد تدافعی پیشنهاد می شود.

اگر هیچ گزینه دیگری به غیر از راه اندازی یک سیستم WPA-PSK پیش رو ندارید، از یک کلمه عبور بسیار مطمئن که حداقل هشت کاراکتر دارد، استفاده کنید. کلمه عبور پیچیده‌ای که از شش کاراکتر تشکیل شده باشد، به طور متوسط ظرف سیزده روز کشف می‌شود.

۴-۱۰-۵ استفاده از نرم افزار کلاینت VPN = محافظت از کارمندان سیار

با وجود این که استفاده از برنامه کلاینت VPN همراه یک دیوار آتش نخستین گام برای حفاظت از کارمندان سیار به شمار می‌رود، تعداد بسیاری از نقاط ضعف چنین ارتباطی بدون محافظت باقی می‌ماند. کاربرانی که در حال مسافرت هستند، به ناچار در هتل‌ها، کافی شاپ‌ها و فرودگاه‌ها از شبکه‌های وای فای استفاده می‌کنند.

ابزارهایی مانند Hotspotter که در بسته نرم افزاری BackTrack در اختیار همگان قرار می‌گیرند، برای مهاجم امکان ایجاد یک ناحیه خطرناک را فراهم می‌کنند که اغلب توسط شبکه به عنوان یک ناحیه خطرناک مجاز شناخته می‌شود. این فرآیند شامل ایجاد یک نقطه دسترسی جعلی با استفاده از یک شناسه SSID متداول و همچنین صفحات وب شبیه به یک ناحیه خطرناک واقعی است. سپس مهاجم منتظر اتصال کاربران بی اطلاع، به نقطه دسترسی جعلی شده و با استفاده از پروتکل DHCP برای آن‌ها یک آدرس IP و یک صفحه وب ایجاد می‌کند. به این ترتیب، کاربر فریب خورده و به منظور ورود به ناحیه خطرناک اعتبارنامه خود را در اختیار مهاجم قرار می‌دهد. در بعضی موارد مهاجم حتی دسترسی کاربران به اینترنت را امکان پذیر کرده و به این ترتیب برای اجرای حمله‌های MITM و سرقت سایر اطلاعات مهم کاربران مانند شناسه و کلمه عبور و شماره حساب بانکی آن‌ها اقدام می‌کند.

حفاظت از کارمندان سیار به ویژه در برابر این نوع حمله‌ها، اقدامی چالش برانگیز بوده و علاوه بر استفاده از نرم افزار کلاینت VPN و دیوار آتش نیازمند تمهیدات امنیتی دیگری است. البته، هیچ یک از این اقدامات به طور کامل از کاربر محافظت نمی‌کند، اما خطرات امنیتی را کاهش می‌دهند. مدیران شبکه‌های مبتنی بر ویندوز با استفاده از گزینه *Access point (infrastructure) networks only* می‌توانند از اتصال کاربران به شبکه‌های Ad-Hoc جلوگیری می‌کنند.

بسیاری از ابزارهای مهاجمان که برای شبیه سازی عملکرد نقاط دسترسی به کار گرفته می‌شوند، در حقیقت، شبکه‌های Ad-Hock را شبیه سازی می‌کنند. غیرفعال کردن گزینه مذکور در سیستم عامل ویندوز می‌تواند از کاربران در برابر چنین حمله‌هایی محافظت کند. به علاوه، غیرفعال کردن گزینه (Any Available Network (Access Point Preferred نیز از بروز چنین حملاتی جلوگیری می‌کند. سرانجام، با

غیرفعال کردن گزینه Automatically Connect to Non-Preferred networks نیز می توان از اتصال تصادفی کاربران به شبکه های Ad-Hock جلوگیری کرد.

۴-۱۱ جمع بندی

در تأمین امنیت شبکه های بی سیم، به کارگیری یک رویکرد چندلایه، کلید اجتناب از بروز مشکلات امنیتی است. درک درست خطرات امنیتی قسمت بزرگی از فرآیند کاهش این خطرات محسوب می شود. اغلب حمله های بی سیم نسبت به لایه دوم شبکه اجرا می شوند. بنابراین، بازبینی تنظیمات دیوار آتش فعلی برای حصول اطمینان از فیلترسازی لایه دوم ضروری است. بسیاری از دیوارهای آتش تنها از لایه سوم و لایه های بالاتر حفاظت می کنند و بسیاری از آن ها نیز به جای نظارت دائمی بر ترافیک اطلاعات به صورت یک فیلتر بسته های اطلاعاتی عمل می کنند. پیکربندی فیلتر بسته های اطلاعاتی می تواند به کاری ملال آور تبدیل شود. بنابراین، نظارت دائمی بر لایه های دوم و سوم شبکه رویکرد مناسب تری برای تأمین امنیت شبکه های بی سیم است.

به روزرسانی و تغییر پیکربندی نقاط دسترسی نیز می تواند مکمل خوبی برای سیستم های کدگذاری و اعتبارسنجی ضعیف باشد. همچنین این اقدامات می توانند بسیاری از ملزومات فنی و تکنیکی فعلی و آتی شبکه را تأمین کنند.

بسیاری از حمله های امنیتی نیازمند برقراری شرایط خاص هستند و اجرای آن ها مستلزم بهره مندی از یک سیستم IDS/IPS بی سیم برای شبیه سازی محیط و تدابیر امنیتی مورد تأیید برای زیرساخت های بی سیم است. استفاده از یک سیستم IDS/IPS پیشرفته اقدام مؤثری برای شناسایی بسیاری از حمله های مذکور و همچنین محافظت در برابر آن دسته از ابزارهای مهاجمان است که برای انجام حمله های دنباله دار شناخته شده مورد استفاده قرار می گیرند. دیوارهای آتش به هیچ وجه قادر به تأمین این نوع امنیت نیستند.

یک سیستم IDS/IPS بی سیم ابزارهای بهتری را برای تشخیص نقاط دسترسی غیرمجاز در اختیار ما می گذارد. اسکنرهای دستی فقط برای بررسی لحظه ای وضعیت شبکه کاربرد دارند و هیچ ابزاری را برای تأمین خودکار امنیت شبکه در برابر نقاط دسترسی غیرمجاز ارائه نمی کنند. استفاده از یک سیستم IDS/IPS بی سیم به منظور نظارت شبانه روزی بر شبکه و نابودی خودکار نقاط دسترسی غیرمجاز رویکرد کارآمدتری برای کاهش خطرات امنیتی شبکه محسوب می شود. به علاوه، این رویکرد موجب صرفه جویی در زمان طولانی مورد نیاز برای نظارت و بررسی دستی شبکه می شود.

یک موضوع مشترک مسائل امنیت این است که مکانیسم های تکنولوژیکی برای بسیاری از رخنه های مشاهده شده وجود دارد و به خوبی درک می شوند، اما باید به منظور محافظت از شبکه فعال شوند. اقدامات پیشگیرانه معقول می توانند شبکه های بی سیم را برای هر سازمانی که می خواهد فواید سیار بودن و انعطاف پذیری را در کنار هم گرد آورد، امن کنند. همراه با به کارگیری بسیاری از تکنولوژی های شبکه، ایده اصلی و کلیدی، طراحی شبکه با در نظر داشتن امنیت در ذهن است. بعلاوه انجام نظارت های منظم را برای تضمین اینکه طراحی انجام شده اساس پیاده سازی است، باید در نظر داشت. یک آنالایزر شبکه بی سیم یک ابزار ضروری برای یک مهندس شبکه بی سیم است.

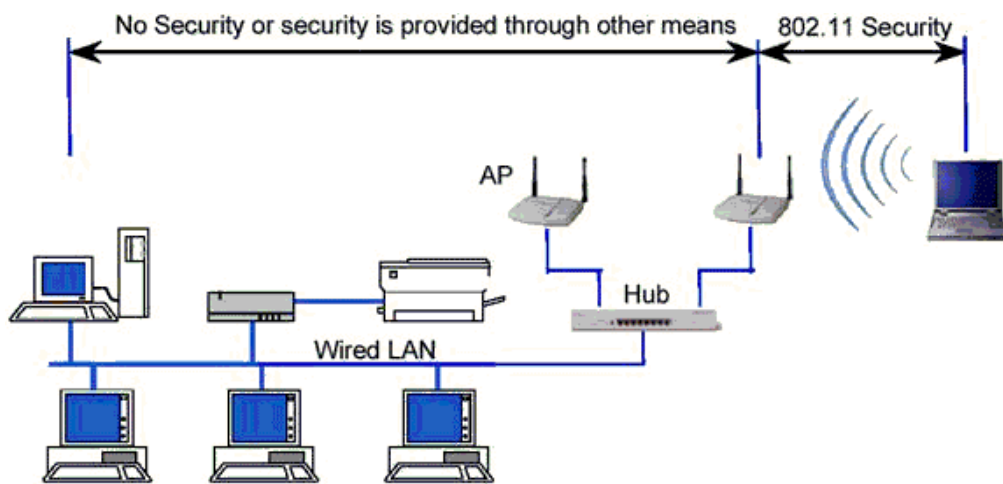
۵ فصل پنجم: پروتکل های امنیتی در شبکه های وای فای

Chapter Five: Security Protocols in Wi-Fi Networks

مراجع: [11],[12],[13],[14],[15],[16]

۱-۵ مقدمه

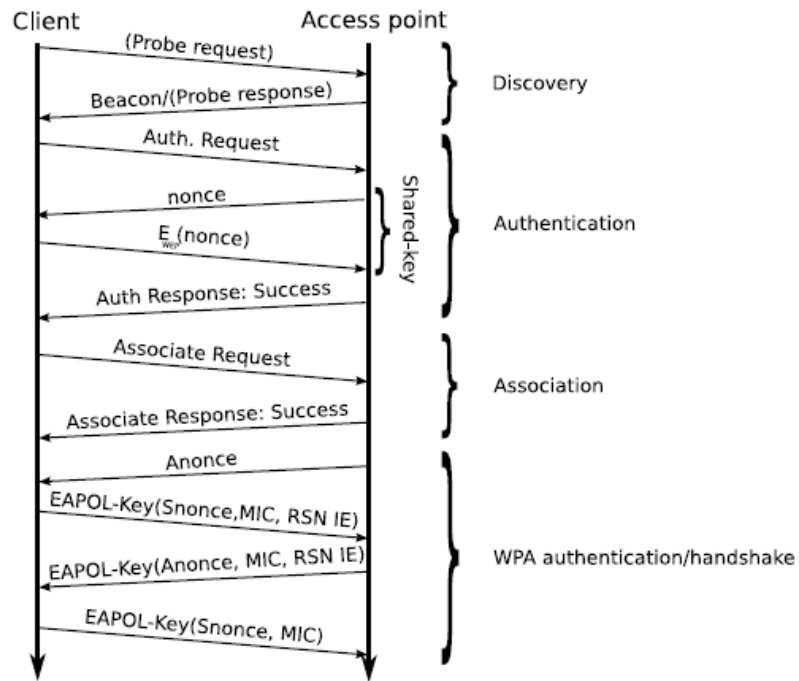
این فصل به بررسی روش ها و استانداردهای امن سازی شبکه های محلی بی سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می کنیم. با طرح قابلیت های امنیتی این استاندارد، می توان از محدودیت های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد. استاندارد ۸۰۲.۱۱ سرویس های مجزا و مشخصی را برای تأمین یک محیط امن بی سیم در اختیار قرار می دهد. این سرویس ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می گردند و وظیفه ی آن ها امن سازی ارتباط میان کلاینت ها و نقاط دسترسی بی سیم است. درک لایه یی که این پروتکل به امن سازی آن می پردازد اهمیت ویژه یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایه ی ارتباطی بی سیم که مبتنی بر استاندارد ۸۰۲.۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



شکل ۵.۱: محدودیت های استانداردهای امنیتی ۸۰۲.۱۱ خصوصاً WEP

۲-۵ پروتکل اتصال/دسترسی در شبکه های وای فای

شکل ۵.۱ روند جریان مبادله فریم ها برای اتصال یک کلاینت به نقطه دسترسی را نشان می دهد، که در تمامی پروتکل ها از روند استفاده می شود.



شکل ۵.۱: پروتکل اتصال به شبکه های وای فای

در این روند یک کلاینت برای اتصال به شبکه های وای فای ابتدا با ارسال یک فریم به نام Request Probe و دریافت فریم ProbeResponse از جانب نقطه دسترسی یا به وسیله فریم هایی به نام Beacon که مکرراً از نقطه دسترسی به تمام ایستگاهها ارسال می شود، نقطه دسترسی را شناسایی می کند. بعد از شناسایی نقطه دسترسی، کلاینت باید خودش را به نقطه دسترسی شناسایی کرده و عملیات احراز هویت را انجام دهد و اگر توانست خودش را به نقطه دسترسی شناسایی کند و با موفقیت احراز هویت را انجام دهد، آنگاه سعی می کند که به نقطه دسترسی وصل شود و با ارسال فریم هایی به نام association request به نقطه دسترسی درخواست وصل شدن می کند و در صورتی که نقطه دسترسی موافقت کند با ارسال فریمی به نام positive association response به کلاینت اجازه اتصال می دهد، اگر WPA فعال باشد روش احراز هویت کلید اشتراکی که در پروتکل WEP به کار می رود استفاده نمی شود و از احراز هویت واقعی به جای آن استفاده می شود.

بعد از انجام چهار مرحله بالا کلاینت می تواند به دریافت و ارسال و مبادله فریم با نقطه دسترسی بپردازد

۳-۵ قابلیت ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم بر اساس استاندارد ۸۰۲.۱۱ فراهم می کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن

همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته یی که باید به خاطر داشت این است که اغلب حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می گذارد، هرچند که فی نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه های ارتباطی دیگری که بر روی کلاینت ها و سخت افزارهای بی سیم، خصوصاً کلاینت های بی سیم، وجود دارد، به شبکه ی بی سیم نفوذ می کنند که این مقوله نشان دهنده ی اشتراکی هرچند جزئی میان امنیت در شبکه های سیمی و بی سیمی است که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی سیم تعریف می گردد :

Authentication •

Confidentiality •

Integrity •

احراز هویت (Authentication)

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

محرمانگی (Confidentiality)

محرمانه گی هدف دیگر WEP است. این بُعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی سیم است.

صحت (Integrity)

هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان کلاینت های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم و بیش وجود دارد.

۴-۵ خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه های کاری پیاده سازی می شوند. در حقیقت تمام ایستگاه های کاری موجود در یک شبکه محلی مبتنی بر ۸۰۲.۱۱ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه های سیمی، در شبکه های بی سیم قابل اعمال نیست استاندارد ۸۰۲.۱۱ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می نماید. سرویس هویت سنجی به ایستگاه کاری امکان می دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی ۸۰۲.۱۱ دو گونه خدمت هویت سنجی را تعریف می کند:

Open System Authentication –

Shared Key Authentication –

روش اول، متد پیش فرض است و یک فرآیند دو مرحله ای است. در ابتدا ایستگاهی که می خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می کند. ایستگاه گیرنده نیز فریمی در پاسخ می فرستد که آیا فرستنده را می شناسد یا خیر. روش دوم کمی پیچیده تر است و فرض می کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سری دریافت کرده است. ایستگاه های کاری با استفاده از این کلید مشترک و با بهره گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می نمایند. 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 می گردد.

در یک شبکه بی سیم، تمام ایستگاه های کاری و سایر تجهیزات قادر هستند ترافیک داده ای را "بشنوند" - در واقع ترافیک در بستر امواج مبادله می شود که توسط تمام ایستگاه های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی سیم را تحت تأثیر قرار می دهد. به همین دلیل در استاندارد ۸۰۲.۱۱ پروتکلی موسوم به WEP تعبیه شده است که بر روی تمام فریم های داده و برخی فریم های مدیریتی و هویت سنجی اعمال می شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء و پوشش را معادل با شبکه های سیمی نماید.

۱-۴-۵ احراز هویت Authentication

استاندارد ۸۰۲.۱۱ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه ی بی سیم را به نقاط دسترسی ارسال می کنند، دارد که یک روش بر مبنای رمزنگاری ست و دیگری از رمزنگاری استفاده نمی کند. جزئیات این روش در فصل ۵ و در قسمت به طور کامل بیان گردیده است و از تکرار مجدد آن خودداری می کنیم. (رجوع شود به [۱-۵-۳](#))

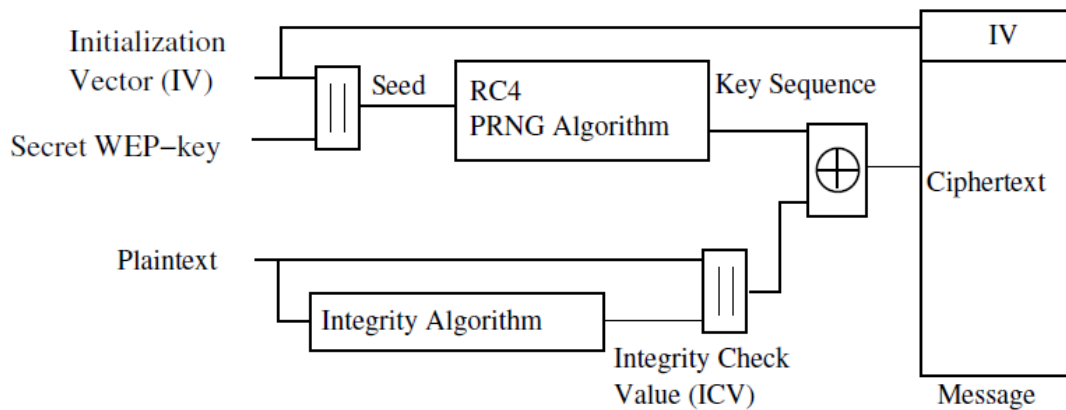
۲-۴-۵ سرویس امنیت (Privacy یا confidentiality)

این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می گردد به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه گی عموماً از تکنیک های رمزنگاری استفاده می گردد، به گونه یی 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 ۸۰۲.۱۱b، از تکنیک های رمزنگاری WEP استفاده می گردد که بر پایه ی RC4 است. RC4 یک الگوریتم رمزنگاری متقارن است که در آن یک رشته ی نیمه تصادفی تولید می گردد و توسط آن کل داده رمز می شود. این رمزنگاری بر روی تمام بسته ی اطلاعاتی پیاده می شود. به بیان دیگر داده های تمامی لایه های بالای اتصال بی سیم نیز توسط این روش رمز می گردند، از IP گرفته تا لایه های بالاتری مانند HTTP. از آنجایی که این روش عملاً اصلی ترین بخش از اعمال سیاست های امنیتی در شبکه های محلی بی سیم مبتنی بر استاندارد ۸۰۲.۱۱b است، معمولاً به کل پروسه ی امن سازی اطلاعات در این استاندارد به اختصار WEP گفته می شود.

در شکل زیر بلوک دیاگرام رمزنگاری پروتکل WEP را مشاهده می کنید، WEP از الگوریتم RC4 PRNG برای تولید یک عدد شبه تصادفی استفاده می کند، تمام ایستگاهها از یک کلید اشتراکی به نام Secret WEP-Key استفاده می کنند، در مجموع برای انجام عملیات رمز نگاری یک مقدار اولیه (IV) به کلید اصلی

الحاق می گردد و به عنوان ورودی برای الگوریتم RC4 PRNG به کار می رود، خروجی این الگوریتم دنباله ای از کلید ها می باشد، متن خام ورودی توسط الگوریتم Integrity به یک مقدار تست کننده صحت (ICV)، تبدیل می شود و به متن خام اصلی اضافه می شود و سپس با دنباله کلید تولید شده XOR می شود و خروجی به عنوان Payload در فریم داده قرار می گیرد، برای عملیات رمزگشایی بسته عکس عملیات رمزنگاری در فرستنده انجام می شود تا داده ای بسته به دست آیند.



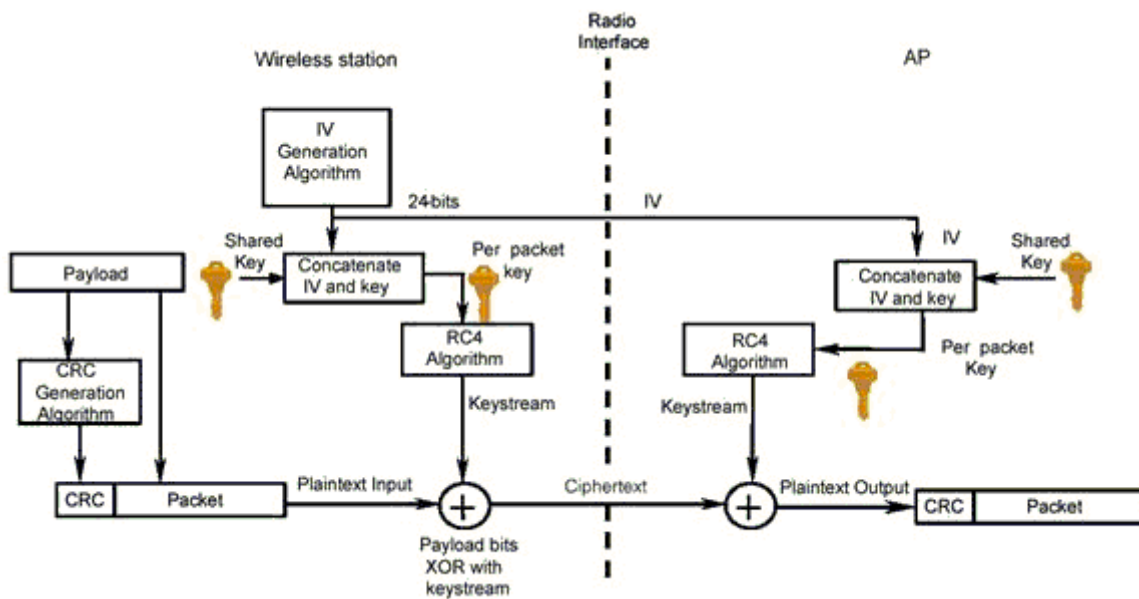
شکل ۵.۲: بلوک رمزنگاری پروتکل WEP

همان طور که گفته شد پروتکل WEP سرویس های امنیتی محرمانگی، احراز هویت و کنترل دسترسی را فراهم می کند، اما می توان روش های به کار برد که این سرویس ها را از میان برداشت و بتوان به شبکه های وای فای نفوذ کرد، در زیر روش هایی که می تواند این سرویس ها را بشکند و به پروتکل حمله کند.

کلیدهای WEP اندازه هایی از ۴۰ بیت تا ۱۰۴ بیت می توانند داشته باشند. این کلیدها با IV (مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می دهند. طبیعتاً هرچه اندازه ی کلید بزرگ تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می دهد که استفاده از کلیدهایی با اندازه ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه ی ۸۰ بیت (که تعداد آن ها از مرتبه ی ۲۴ است) به اندازه ی بالاست که قدرت پردازش سیستم های رایانه یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی کند.

هرچند که در حال حاضر اکثر شبکه های محلی بی سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته های اطلاعاتی استفاده می کنند ولی نکته یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این است که روش تأمین محرمانه گی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روش brute-force، نیز آسیب پذیر است و این آسیب پذیری ارتباطی به اندازه ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانگی در شکل ۵.۳ نمایش داده شده است :



شکل ۵.۳: عملیات الگوریتم WEP برای تضمین محرمانگی

۵-۴-۳ صحت (Integrity)

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست های امنیتی یی که Integrity را تضمین می کنند روش هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم ترین میزان تقلیل می دهند.

در استاندارد b ۸۰۲.۱۱ نیز سرویس و روشی استفاده می شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان کلاینت های بی سیم و نقاط دسترسی کم می شود. روش مورد نظر استفاده از یک کد CRC است. همان طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمز شدن بسته تولید می شود. در سمت گیرنده، پس از رمزگشایی، CRC داده های رمزگشایی شده مجدداً محاسبه شده و با CRC نوشته شده در بسته مقایسه می گردد 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 اندازه ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب پذیر است.

متأسفانه استاندارد b ۸۰۲.۱۱ هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می گیرد باید توسط کسانی که شبکه ی بی سیم را نصب می کنند به صورت دستی پیاده سازی گردد. از آنجایی که این بخش از امنیت یکی از معضله های اساسی در مبحث رمزنگاری

است، با این ضعف عملاً روش های متعددی برای حمله به شبکه های بی سیم قابل تصور است. این روش ها معمولاً بر سهل انگاری های انجام شده 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 توجهی ها نتیجه بی 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 کلاینت 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.

۵-۵ ضعف های اولیه ی امنیتی WEP

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 ۸۰۲.۱۱ 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.

نکته یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه ی کلیدهاست. با وجود آن که با بالارفتن اندازه ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می رود، ولی از آن جاکه این کلیدها توسط کاربران و بر اساس یک کلمه ی عبور تعیین می شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر همان طور که در قسمت های پیشین نیز ذکر شد، دستیابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه ی کلید اهمیت ی ندارد.

متخصصان امنیت بررسی های بسیاری را برای تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است.

حاصل بررسی های انجام شده فهرستی از ضعف های اولیه ی این پروتکل است :

۱. استفاده از کلیدهای ثابت WEP

۲. Initialization Vector -IV

۳. ضعف در الگوریتم

۳. استفاده از CRC رمز نشده

۱-۵-۵ استفاده از کلیدهای ثابت WEP

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبکه های محلی بی سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می کند به سرقت برود یا برای مدت زمانی در دست رس نفوذگر باشد، کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه های کاری عملاً استفاده از تمامی این ایستگاه ها ناامن است.

از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۲-۵-۵ 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.

۳-۵-۵ 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.

۵-۵-۴ استفاده از CRC رمز نشده

در پروتکل WEP، کد CRC رمز نمی شود. لذا بسته های تأییدی که از سوی نقاط دست رسی بی سیم به سوی گیرنده ارسال می شود بر اساس یک CRC رمز نشده ارسال می گردد و تنها در صورتی که نقطه ی دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می فرستد. این ضعف این امکان را فراهم می کند 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 عکس العمل نقطه ی دست رسی بماند که آیا بسته ی تأیید را صادر می کند یا خیر.

ضعف های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEP هستند. نکته یی که در مورد ضعف های فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آن ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می گردد و بقیه ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

جدول ۵.۱ ضعف های امنیتی پروتکل WEP را به اختصار جمع بندی 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.

جدول ۵.۱ : ضعف های امنیتی استاندارد WEP

لیستی از انواع حملات به شبکه های وای فای به همراه سرویسی را که به مخاطره می اندازد و نیازمندی

ها و زمان مورد نیاز را مشاهده می کنید:

Attack	Service	Requirements	Approximate Time
RC4	Confidentiality, Authentication	300,000 WEP encrypted frames	20 minutes
WEP dictionary	Confidentiality, Authentication	Pass-phrase seeded key, 1 data frame	Norwegian word list in 5 sec.
Chosen plaintext	Confidentiality	WEP enabled. Allow 10 byte data size	50 minutes for full frame
Redirect	Confidentiality	WEP enabled	Insignificant
Double encryption	Confidentiality	Internet connection	At least a few hours
One way auth	Authentication	Shared-key authentication	Insignificant
Spoofing	Authentication	1 active and authenticated client	Insignificant
Rogue access point	Authentication	1 client	Insignificant
Packet injection	Access control	Known IV/key sequence	Insignificant
Profiling	Access control	Known IV/key sequence	Insignificant
MAC filter	Access control	MAC filter enabled	Insignificant
Captive Portal	Access control	MAC filter access control	Insignificant
WPA-PSK dictionary	Confidentiality, Authentication	Pass-phrase seeded key, handshake	Norwegian word list in 1 hour

با وجود اینکه نفوذگران مصمم، می توانند در WEP نفوذ نمایند، استفاده از WEP می تواند مانع از جداکردن داده های بی سیم شناور اطراف شبکه تان توسط بسته های نظارت و ردگیری (اسنیفر پاکت ها) شود (یکی از قدیمی ترین روش های سرقت اطلاعات در یک شبکه، استفاده از فرآیندی موسوم به "ردگیری بسته ها در شبکه" است. در این روش مهاجمان از تکنیک هایی به منظور تکثیر بسته های اطلاعاتی که در طول شبکه حرکت می کنند، استفاده نموده و در ادامه با آنالیز آنها از وجود اطلاعات حساس در یک شبکه آگاهی می یابند.

امروزه پروتکل هائی نظیر IPsec به منظور پیشگیری از "ردگیری بسته ها در شبکه" طراحی شده است که با استفاده از آن بسته های اطلاعاتی رمزنگاری می گردند. در حال حاضر تعداد بسیار زیادی از شبکه ها از تکنولوژی IPsec استفاده نمی نمایند و یا صرفاً بخش اندکی از داده های مربوطه را رمزنگاری می نمایند و همین امر باعث شده است که "ردگیری بسته ها در شبکه" همچنان یکی از روش های متداول به منظور سرقت اطلاعات باشد. یک "ردگیر بسته ها در شبکه" که در برخی موارد از آن به عنوان دیده بان شبکه و یا تحلیلگر شبکه نیز یاد می شود، می تواند توسط مدیران شبکه به منظور مشاهده و اشکال زدائی ترافیک موجود بر روی شبکه استفاده گردد تا به کمک آن بسته های اطلاعاتی خطاگونه و گلوگاه های حساس شبکه شناسائی و زمینه لازم به منظور انتقال موثر داده ها فراهم گردد. به عبارت ساده تر، یک "ردگیر بسته ها در شبکه" تمامی بسته های اطلاعاتی که از طریق یک اینترفیس مشخص شده در شبکه ارسال می گردند را تا موقعی که امکان بررسی و آنالیز آنان فراهم گردد جمع آوری می نماید. عموماً از برنامه های "ردگیر بسته ها در شبکه" به منظور جمع آوری بسته های اطلاعاتی به مقصد یک دستگاه خاص استفاده می شود. برنامه های فوق قادر به جمع آوری تمامی بسته های اطلاعاتی قابل حرکت در شبکه، صرف نظر از مقصد مربوطه نیز هستند. یک مهاجم با استقرار یک "ردگیر بسته ها در شبکه" در شبکه، قادر به جمع آوری و آنالیز تمامی ترافیک شبکه خواهد بود. اطلاعات مربوط به نام و رمز عبور عموماً به صورت متن معمولی و رمز نشده ارسال می شود و این بدان معنی است که با آنالیز بسته های اطلاعاتی، امکان مشاهده اینگونه اطلاعات حساس وجود خواهد داشت. یک "ردگیر بسته ها در شبکه" صرفاً قادر به جمع آوری اطلاعات مربوط به بسته های اطلاعاتی درون یک subnet مشخص شده است. بنابراین، یک مهاجم نمی تواند یک "ردگیر بسته ها در شبکه" را در شبکه خود نصب نماید و از آن طریق به شبکه شما دستیابی و اقدام به جمع آوری نام و رمز عبور به منظور سوء استفاده از سایر ماشین های موجود در شبکه نماید. مهاجمان به منظور نیل به اهداف مخرب خود می بایست یک "ردگیر بسته ها در شبکه" را بر روی یک کامپیوتر موجود در شبکه اجراء نمایند. در بیشتر نقاط دسترسی، پیشنهاد می کنند حداقل اندازه کلید برای رمزگذاری ۶۴ بیت باشد و بعضی دیگر حتی پیشنهاد ۱۲۸ بیتی برای رمزگذاری را داده اند. مدل WEP بسته های داده های مورد استفاده را بصورت الگوریتم های مبهم و مبتنی بر یک کلید

الکترونیکی تبدیل نموده و آنرا بصورت یک سری از الفبای عددی یا کاراکترهای شانزده شانزدهمی (هگزا دسیمال) پنهان می نماید. سیستم دریافت باید یک کلید نظیر آن را به منظور کشف رمز بسته داده داشته باشد.

بر روی نقطه دسترسی، گزینه ای را که اتصال WEP را فعال نموده و یا نیاز دارد، جستجو کنید. کلیدی را روی نقطه دسترسی تعریف نموده و همان کلید را در پیکربندی بی سیم هر سرویس گیرنده وارد کنید.

۶-۵ پروتکل (WPA (Wi-Fi Protected Access

اتحادیه Wi-Fi در سال ۲۰۰۳ استاندارد جدیدی را برای شبکه های بی سیم معرفی کرد. این استاندارد برای به کار گیری در ابزارهای شبکه موجود که از استاندارد WEP استفاده می کردند، طراحی شد و از قابلیت سازگاری با ابزارهای قدیمی تر نیز برخوردار است. به کارگیری این استاندارد مستلزم پیکربندی آن روی ابزارهای موجود در شبکه بوده و در صورتی که تنظیمات مورد نظر روی دستگاهی اعمال نشود همچنان رمزگذاری اطلاعات بر اساس استاندارد WEP انجام می شود. مهم ترین ویژگی این استاندارد که آن را نسبت به WEP متمایز می کند، قابلیت تغییر کلید به صورت دینامیک با استفاده از پروتکل TKIP (Temporal Key Integrity) است. این استاندارد برای رمز گذاری اطلاعات از الگوریتم MIC (Message Integrity Check) استفاده می کند و با افزودن ویژگی بررسی کامل کلید، اطمینان می یابد که کلید تعریف شده مورد استفاده کاربران غیر مجاز قرار نخواهد گرفت.

پروتکل (TKIP (Temporal Key Integrity Protocol) به این منظور در پروتکل WPA به وجود آمد که بتواند ضعف های امنیتی ناشی از الگوریتم RC4 در پروتکل WEP را جبران کند. یکی از مهم ترین برتری های WPA بر WEP این است که در آن هر بسته با استفاده از یک کلید منحصر به فرد و متفاوت با بسته قبل رمزنگاری می شود و این کار توسط پروتکل TKIP انجام می گردد. پروتکل TKIP به جای استفاده مستقیم از کلید مشترک برای رمزنگاری از آن تنها برای تولید سایر کلیدها استفاده می کند. این پروتکل دو تابع ترکیب کلید دارد که این توابع از ترکیب کلید مشترک، آدرس MAC سرویس گیرنده و بردار اولیه، به ازای هر بسته یک کلید را تولید می کنند. با استفاده از TKIP، کلید رمزنگاری به جای یک کلید ۶۴ یا ۱۲۸ بیتی که تنها ۲۴ بیت آن پویا است (کلید مشترک مورد استفاده در WEP) به یک کلید پویای ۱۲۸ بیتی کاملاً مؤثر تعبیر می کند و در نتیجه امنیت شبکه ی بی سیم افزایش می یابد.

برای رمز گذاری شبکه بر اساس استاندارد WPA، یک ترکیب منحصر به فرد از کلید تعریف شده به همراه SSID شبکه ایجاد شده و به هر کاربر شبکه بی سیم به صورت مجزا اختصاص می یابد که به طور

ثابت و اتوماتیک تغییر می یابد در نتیجه امکان دسترسی افراد غیر مجاز به شبکه را به حداقل می رساند. قابلیت شناسایی کاربران که در استاندارد WEP نادیده گرفته شده بود، در این استاندارد و به کمک پروتکل EAP (Extensible Authentication Protocol) تامین شد. در حقیقت WEP دسترسی کاربران را بر اساس آدرس MAC کامپیوترهای شبکه تنظیم می کرد که به راحتی توسط هکرها قابل شناسایی بود. EAP بر پایه یک سیستم کلید عمومی ایمن تر ساخته شده است تا دسترسی به شبکه را تنها برای کاربران واجد شرایط و شناسایی شده فراهم کند.

در شبکه ای که از پروتکل WPA استفاده می شود، در ابتدا یک میزبان با نقطه دسترسی ارتباط برقرار می کند. تا هنگامی که هویت کاربر تصدیق نشده است، نقطه دسترسی از دسترسی کاربر به شبکه محلی جلوگیری می کند. اگر هویت کاربر توسط سرویس دهنده احراز هویت تصدیق شود، میزبان می تواند به شبکه محلی ملحق شود. در غیر این صورت از دسترسی میزبان به شبکه جلوگیری می شود. پس از ملحق شدن میزبان به شبکه محلی، سرویس دهنده تصدیق هویت، یک کلید رمزنگاری TKIP میان میزبان و نقطه دسترسی توزیع می کند. سپس میزبان می تواند ارتباط خود را روی شبکه محلی آغاز کرده و داده ها را به صورت رمزنگاری شده منتقل کند.

WPA مخفف دسترسی محافظت شده Wi-Fi یا Wi-Fi Protected Access می باشد و عبارتست از استانداردهایی که برای افزایش ویژگی های امنیتی WEP طراحی شده است. این تکنولوژی به گونه ای طراحی شده است که بتوان از آن در دستگاه های موجود که از Wi-Fi پشتیبانی کرده و دارای سیستم امنیتی WEP هستند، استفاده نمود. (به عنوان مثال از طریق بروزرسانی نرم افزار این دستگاه ها..)

این تکنولوژی نسبت به WEP دارای دو مزیت است :

- رمزنگاری داده پیشرفته تر با استفاده از پروتکل TKIP. این پروتکل کلیدهای رمزنگاری را با استفاده از الگوریتم Hashing به هم ریخته و با افزودن کد بررسی پیوستگی به آن از عدم جعل کلید توسط هکرها اطمینان حاصل می نماید.
- تایید هویت کاربران با استفاده از پروتکل EAP، این ویژگی در تکنولوژی WEP به عنوان یک نقیصه بشمار می آمد. WEP دسترسی به شبکه های بی سیم را بر اساس آدرس MAC کامپیوترها کنترل می نماید و از آنجا که آدرس MAC به راحتی قابل شناسایی و استفاده توسط هکرها می باشد، روش مناسبی به شمار نمی آید. پروتکل EAP بر اساس کلید رمزنگاری عمومی بسیار ایمن تر عمل نموده و بر این اساس تنها کاربران تایید شده قادر به دسترسی به شبکه خواهند بود.

اگر بخواهیم مقایسه بین پروتکل های WEP و WPA داشته باشیم می توان گفت که پروتکل WEP در کمتر از ده دقیقه درهم شکسته می شود، اما درهم شکستن WPA با یک کلید ۲۱ بیتی بیشتر از 4×10^{20}

سال طول می کشد WEP. تنها می تواند از کلیدهای ۶۴، ۱۲۸ و ۱۵۲ بیتی و یک IV (Initialization Vector) یکسان یا همان بردار تولید کلیدهای ابتدایی رمزنگاری استفاده کند، اما در WPA از دو الگوریتم رمزنگاری پیچیده به نام های TKIP سرنام (Temporal Key Integrity Protocol) و AES (Advanced Encryption Standard) استفاده می شود که در هر کدام کلیدها ده ها بار تولید شده و در رمزنگاری اطلاعات شرکت کرده و از بین می روند. طول بردار IV دو برابر WEP است. IV در WPA قابلیت تعریف پانصد تریلیون کلید مقایسه را فراهم می کند، اما این تعداد در WEP نزدیک به ۱۶/۷ میلیون کلید مقایسه است.

در پروتکل WEP برای تولید کد صحت پیام از روش CRC (جمع تطبیقی) استفاده می شود که یک تابع خطی ساده است، در حالی که پروتکل WPA از الگوریتم Michael برای محاسبه ی کد صحت پیام (MIC) استفاده می کند که یک تابع بسیار پیچیده است. تفاوت دیگر کد صحت پیام محاسبه شده در پروتکل های WEP و WPA این است که در پروتکل WEP کد CRC فقط از روی قسمت اصلی بسته-ی داده محاسبه می شود و کاری به سرآیند بسته ندارد، در حالی که پروتکل WPA از کل داده ها (داده های اصلی با اضافه ی سرآیند) برای محاسبه ی کد MIC استفاده می کند. بنابراین، در پروتکل WEP ممکن است اطلاعات سرآیند بسته (از قبیل آدرس فرستنده، آدرس گیرنده و غیره) در حین ارسال دچار تغییر شوند بدون این که گیرنده متوجه شود.

اما دلیلی که هنوز دیده می شود که از پروتکل WEP استفاده می شود این است که بسیاری از دستگاه های بی سیم امروزی هنوز از WPA و نسخه های جدیدتر آن پشتیبانی نمی کنند و تنها گزینه امنیتی آن ها WEP است. بسیاری از کارت های شبکه بی سیم قدیمی، بسیاری از دستگاه های بازی مانند Nintendo DS و نوت بوک های قدیمی فقط از WEP پشتیبانی می کنند. همچنین نمی توان گفت که تحت هیچ شرایطی از WEP استفاده نکنید، بلکه که WPA بهتر از WEP است و WEP بهتر از رمزنگاری نکردن اطلاعات روی شبکه های بی سیم است. اگر در شبکه دستگاه بی سیمی دارید که از WPA پشتیبانی نمی کند، ناچارید از WEP استفاده کنید. بالاخره هر فردی نمی تواند به سادگی رمزنگاری این پروتکل را دور بزند.

۷-۵ پروتکل WPA2

WPA2 مخفف دسترسی محافظت شده به Wi-Fi ویرایش دوم یا "Wi-Fi Protected Access 2" می باشد، که این پروتکل در جهت بهبود پروتکل WPA که در شبکه های بی سیم کاربرد دارد، ارائه شده است. این پروتکل در کنترل شبکه و حفاظت داده ها بسیار قوی تر عمل نموده و استفاده از این پروتکل

در شبکه های بی سیم شرکت های بزرگ و کاربران خانگی سطح بسیار بالایی از امنیت را فراهم کرده و کاربران این پروتکل می توانند از جلوگیری از دسترسی غیر مجاز به شبکه خود اطمینان داشته باشند.

بر اساس استاندارد IEEE 802.11i، WPA2 با بکار گیری استانداردها FIPS 140-2 متعلق به موسسه استاندارد سازی و تکنولوژی ایالات متحده (NIST) به همراه الگوریتم رمزنگاری AES و همچنین روش تایید هویت موجود در استاندارد های ۸۰۲.۱ می تواند امنیت داده را هم تراز با استانداردهای دولتی ایالات متحده فراهم نماید.

این استاندارد نسخه کامل تر استاندارد WPA است که در سال ۲۰۰۴ تعریف شد و مهم ترین تفاوت این دو استاندارد در نحوه رمزگذاری اطلاعات برای ارسال به مقصد می باشد. WPA2 یا استاندارد i ۸۰۲.۱۱ که قوی ترین استاندارد رمزگذاری شبکه های بی سیم است و پس از WPA ارائه شد، از یک سیستم با نام AES (Advanced Encryption Standard) بهره می گیرد که موجب می شود شکستن کلید رمز به راحتی امکان پذیر نباشد. WPA2 در دو نسخه پیاده سازی می شود: WPA2-Personal و WPA2-Enterprise. WPA2-Personal که با نام WPA-PSK شناخته می شود برای استفاده در شبکه هایی با کاربران محدود مانند دفاتر اداری کوچک و خانه ها طراحی شده است. این استاندارد دسترسی غیرمجاز به شبکه را با استفاده از تنظیم رمز عبور غیرفعال خواهد کرد و دسترسی هر دستگاه بی سیم با استفاده از یک کلید ۲۵۶ بیتی به منابع شبکه امکان پذیر خواهد بود. نسخه WAP2-Enterprise یا WPA-802.1X، برای استفاده در موسسات و سازمان ها مورد استفاده قرار می گیرد و کاربران از طریق سرور به شبکه دسترسی خواهند یافت. پیاده سازی این استاندارد به تنظیمات پیچیده تری نسبت به سایر استانداردها نیاز دارد اما امنیت بالاتری را برای شبکه ای با تعداد کاربران متعدد فراهم خواهد کرد.

کارشناسان شبکه توصیه می کنند در صورتی که ابزار بی سیم مورد استفاده در شبکه شما از استاندارد WEP پشتیبانی می کنند بدون اتلاف وقت به سراغ استانداردهای قوی تر و مطمئن تر رفته و امنیت شبکه بی سیم خود را به سرعت ارتقا دهید، زیرا عدم استفاده از استاندارد رمزگذاری و یا به کارگیری WEP هر دو تقریباً به یک معنا است و این شرایط تفاوت چشم گیری با یکدیگر نخواهند داشت. در حال حاضر بهترین و کارآمدترین استاندارد رمزگذاری، WPA2 است و تقریباً می توان گفت امروزه تمامی محصولات شرکت های فعال در حوزه ابزارهای شبکه سازی بی سیم قابلیت پشتیبانی از استاندارد رمزگذاری WPA2 را دارند بنابراین به شما توصیه می کنیم برای برقراری امنیت اطلاعات و همچنین جلوگیری از دسترسی افراد غیر مجاز به شبکه در صورتی که ابزار بی سیمی که مورد استفاده قرار می دهید، قابلیت پشتیبانی از این استاندارد را دارد از WPA2 استفاده کنید.

WPA یک پروتکل به روزتر و سازگارتر با استاندارد n 802.11 است و از متدهای رمزنگاری و امن کردن اطلاعات برای انتقال توسط امواج استفاده می کند که تا کنون هیچ کس نتوانسته آن را شکسته و رمزگشایی کند. نسخه های WPA2 و WPA2 Enterprise نسخه های جدیدتری نسبت به WPA هستند و به یقین از الگوریتم ها و روش های بهتر رمزنگاری استفاده می کنند. اگر روتر یا نقطه دسترسی شما از WPA2 یا WPA2 Personal پشتیبانی می کند، این گزینه را انتخاب کنید. در غیر این صورت WPA ساده نیز بهترین انتخاب برای رمزنگاری داده های بی سیم است.

پروتکل WPA2 از الگوریتم رمزنگاری AES استفاده می کند، در حالی که پروتکل WPA از پروتکل TKIP استفاده می کند ولی الگوریتم رمزنگاری آن همان الگوریتم RC4 استفاده شده در پروتکل WEP است. تفاوت دیگر پروتکل های WPA و WPA2 در روش محاسبه کد صحت پیام (MIC) می باشد. پروتکل WPA برای تولید کد صحت پیام از الگوریتم Michael استفاده می کند ولی پروتکل WPA2 از شیوهی زنجیره سازی بلوک های رمز (CBC)* برای تولید کد صحت پیام استفاده می کند. با وجود پیچیده بودن الگوریتم Michael، روش CBC به کار گرفته شده در پروتکل WPA2 برای محاسبه ی کد صحت پیام دارای پیچیدگی بیشتر بوده و در نتیجه امنیت بیشتری را تأمین می کند.

۸-۵ پروتکل امنیتی WPS

Wi-Fi Protected Setup یا راه اندازی حفاظت شده Wi-Fi (به اختصار WPS) استاندارد است برای پیاده سازی شبکه های بی سیم خانگی به شکلی امن و آسان است. این استاندارد در ۸ ژانویه ۲۰۰۷ توسط اتحادیه Wi-Fi به صورت رسمی تایید شد.

هدف این استاندارد تسهیل در روند پیکربندی امنیتی شبکه های بی سیم می باشد و به همین دلیل است که قبلاً با نام Wi-Fi Simple Config نامیده می شد. این پروتکل به منظور میسر کردن امنیت برای کاربرانی طراحی شده که اطلاعات کمی در مورد امنیت شبکه های بی سیم دارند و ممکن است در میان گزینه های موجود برای ایجاد امنیت در شبکه های بی سیم سردرگم بمانند.

این استاندارد با تمرکز بر امنیت و قابلیت استفاده آسان چهار روش برای شبکه های خانگی فراهم می کند، که عبارتند از:

روش PIN: در این روش باید یک PIN (کد شناسایی شخصی) از روی برچسب نصب شده روی دستگاه و یا صفحه نمایش (در صورت وجود) خوانده شده و در نقطه دسترسی (AP) ثبت گردد. این متد روش پایه در نظر گرفته می شود و بر این اساس می بایست در تمامی تجهیزاتی که دارای گواهینامه این استاندارد می باشند الزاماً وجود داشته باشد.

روش PBC: در این روش لازم است که کاربر به سادگی یک دکمه فیزیکی یا مجازی را بر روی هر یک از دو نقطه شامل نقطه دسترسی و دستگاهی که می خواهد بانقطه دسترسی ارتباط امن داشته باشد، بفشارد. پشتیبانی از این روش برای نقطه دسترسی ها اجباری ولی برای دستگاه های بی سیم دیگر اختیاری می باشد.

روش NFC: در این روش فقط کافیست که کاربر دستگاه مورد نظر را نزدیک نقطه دسترسی قرار دهد تا امکان یک ارتباط میدانی کوتاه برد بین این تجهیزات برقرار شود. بجای این کار، بهره بردن از برچسب های RFID سازگار نیز امکان پذیر می باشد. پشتیبانی از این روش اختیاری است.

روش USB: در این روش کاربر از یک حافظه USB (USB Stick) برای انتقال داده بین دستگاه و نقطه دسترسی استفاده می نماید. پشتیبانی از این روش اختیاری است.

از دو روش آخر غالباً به عنوان روش های خارج از باند "Out Of Band" یاد می شود، چراکه انتقال اطلاعات در این دو روش نیاز به راه حلی به غیر از استفاده از خود شبکه Wi-Fi دارد.

به خاطر داشته باشید که در حال حاضر برای اعطای گواهینامه این استاندارد فقط دو روش اول لحاظ می گردد و روش USB نیز از رده خارج شده محسوب گردیده و از روند اعطای گواهینامه خارج شده است.

مزایا

۱. پیکربندی خودکار نام شبکه (SSID) و کلید امنیتی (WPA) بر روی دستگاه و نقطه دسترسی
۲. عدم نیاز به دانستن نام شبکه (SSID)، کلیدهای امنیتی و گذرواژه ها در هنگام اتصال به شبکه های دارای WPS
۳. پایین بودن احتمال اینکه گذرواژه ها و کلیدهای امنیتی قابل حدس زدن باشند، زیرا که به صورت تصادفی تولید می شوند.

۹-۵ جمع بندی

امروزه روش های زیادی برای امن کردن شبکه های بی سیم وجود دارد که هر کدام ضعف ها و سختی های خاص خود را دارد ولی این باعث نشده است که شبکه های بی سیم پیش رفت روز افزون خود را به دست نیاورند. به همین دلیل فراهم کردن شبکه ای بی سیم و امن یکی از تخصص های پول ساز می باشد.

۶ مشکلات فعلی و کارهای آتی

روش ها و پروتکل های امن سازی در شبکه های وای فای بررسی شد و نقاط قوت و ضعف هریک از روش ها بررسی شد، همچنین چالش ها و نقاط ضعف امنیتی این شبکه ها و راه حل آنها نیز اشاره شد. اما همچنان برای امن سازی این شبکه ها نیاز به روش های بهتر و بهینه تر نیاز می شود در زیر لیستی از کارهایی که باید برای امنیت بیشتر در این شبکه ها کار شود و به عنوان مسائل باز مطرح می شود را بیان می کنیم:

۱. **حملات منع سرویس:** حملات منع سرویس (Denial Of Service) یکی از معروفترین حملاتی است که در چند سال اخیر امنیت تمام شبکه را تهدید کرده است، در این حملات هکر قصد دارد که با حمله کردن به سرور و شبکه آن را از کار انداخته و مانع انجام روال های عادی و سرویس دهی آن شود. این حملات در شبکه های وای فای نیز به طور جدی مطرح است و حتی به می توان گفت با توجه به ماهیت این شبکه ها، شدید تر نیز می باشد، پروتکل های که در این تحقیق معرفی شدند می توانند جلوی این حمله را بگیرند و در نتیجه نیاز به اصلاحاتی در این پروتکل ها یا ارائه پروتکل های جدیدتر برای مقابله با این حملات می باشم.
۲. پروتکل های WPA WEP: همانطور که بررسی شد این پروتکل ها به عنوان پروتکل های غالب برای تامین امنیت در شبکه های وای فای محسوب می شوند و از طرفی مشکلات این پروتکل ها نیز بررسی شد و همانطور که گفته شد این پروتکل ها امنیت را تا سطحی تامین می کنند و هیچ وقت قادر به تامین امنیت کامل نمی باشند و از طرفی برای بهینه شدن نیاز به تغییراتی دارند و ایده های نو می تواند کارایی و عملکرد این پروتکل ها را افزایش دهد.

مراجع

- [1] "Wi-Fi Security How to Break and Exploit", Thesis for the degree Master of Science Hallvar Hellesteth Department of Informatics University of Bergen June 2006
- [2] "An Introduction to Wi-Fi®", Part Number 019-0170 • 090409-B • Printed in U.S.A. Digi International Inc. © 2007-2008
- [3] IEEE 802.11 Working group website ,<http://www.ieee802.org/11>
- [4] Introduction to IEEE 802.11 "",intellgraphics",<http://www.intellgraphics.com> "
- [5] Steve Kapp, "802.11: Leaving the wire behind ",IEEE internet computing ,January-February 2002,pp.82-85
- [6] Steve Kapp "802.11a :More bandwidth without the wire ",IEEE internet computing ,July-August 2002,pp.75-79
- [7] Edgar Danielyan "IEEE 802.11 ",the internet Protocol Journal ,Vol.5,No.1,March 2002,pp.2-13
- [8] "A condensed review of Spread Spectrum Techniques for ISM band System ",Intersil Application Note,AN9820.1,May 2000
- [9] "Wi-Fi Security" Stewart S. Miller, McGraw-Hill-New York Chicago San Francisco Lisbon London Madrid Mexico City Milan New Delhi San Juan Seoul Singapore Sydney Toronto
- [10] بانک مقالات گروه امداد امنیت کامپیوتری ایران - (CERT)
- [11] "Overview of Wi-Fi Security What is left?",Philippe Teuwen,Security Engineer and Contributor to Wi-Fi Alliance Easy Setup Task Group,N.V. Philips,October 14 & 15, Hack.lu 2005
- [12] WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement By A.K.M. Nazmus Sakib, Shamim Ahmed, Samiur Rahman, Ishtiaque Mahmud & Md. Habibullah Belali Dhaka International University (DIU), Dhaka
- [13] "Vulnerabilities of Wireless Security protocols (WEP and WPA2)" Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 2, April 2012
- [14] "Security Improvement of WPA 2 (Wi-Fi Protected Access 2) A.K.M. Nazmus Sakib CSE Department, Chittagong University of Engineering & Technology, Chittagong, Bangladesh Fariha Tasmin Jaigirdar Lecturer, Dept of Computer Science Stamford University, Bangladesh Muntasim Munim Programmer Affiliation : Bangladesh Computer Society Armin Akter ,CSE Department, Chittagong University of Engineering & Technology, Chittagong, Bangladesh, A.K.M. Nazmus Sakib et al. / International Journal of Engineering Science and Technology (IJEST)
- [15] "Overview of Wi-Fi Security What is left?" Philippe Teuwen, Security Engineer and Contributor to Wi-Fi Alliance Easy Setup Task Group ,N.V. Philips October 14 & 15 Hack.lu 2005
- [16] Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) Paul Arana INFS 612 – Fall 200