شبکه های بیسیم


بسم الله الرحمن الرحيم

چکیده

برای انتقال اطلاعات، احتیاج به رسانه انتقال و سیستم انتقال می باشد . رسانه های انتقال اجزا فیزیکی می باشند که انتقال اطلاعات در آنها صورت می گیرند وعبار تند از : زوج سیم به هم تابید ه، کابل کواکس، فیبر نوری و مخابرات بی سیم.وجود منابع طبیعی از قبیل کوه ، جنگل، باتلاق، هزینه های بالای کابل کشی دربعضی مناطق، سختی کابل کشی و گاه ناممکن بودن کابل کشی در مناطق دورافتاده، زمان بری برپایی یک شبکه کابلی، نیاز به پهنای باند بالا و دسترسی آسان وهزینه های پایین نصب و بهره وری در شبکه بی سیم، امروزه کاربران را به سوی استفاده از این شبکه ها سوق داده است. همچنین یکی از پدیده های عصر ما معتادان اینترنتی می باشد .کسانی که می خواهند ۲۴ ساعته از اینترنت استفاده کنند . برای این قبیل افراد که دایما در حال جا به جا شدن هستند، دیگر زوج سیم به هم تابیده، کابل کواکس و فیبر نوری کاربرد ندارد . هر گاه کاربر، شرکت یا برنامه کاربردی خواهان آن باشد که داده ها واطلاعات مورد نیاز خود را به صورت متحرک و در هر لحظه در اختیار داشته باشند،شبکه های بی سیم، جواب مناسبی برای آنها است.

محیط های بی سیم دارای ویژگی های منحصر به فردی می باشند که در مقایسه باشبکه های محلی سیمی، جایگاه خاصی را به این گونه شبکه ها می بخشد . عموم به عنوان یک ایستگاه مرکزی کاری که می تواند ارتباط ر ا بین WiFi مردم به چندین کاربر به طور یکسان به اشتراک بگذارد

فهرست صفحه

فصل هشتم (جدول فرکانس ها)

آشنایی جامع و کامل با شبکه های بی سیم (Wireless) و تکنولوژیWi-Fi

2- مقدمه

نیاز روز افزون به پویایی کارها ، استفاده از تجهیزاتی مانند تلفن همراه، پیجرها و... بواسطه وجود شبکه های بی سیم امکان پذیر شده است.اگر کاربر یا شرکت یا برنامه کاربردی خواهان آن باشد که داده و اطلاعات مورد نیاز خود را به صورت متحرک در هر لحظه در اختیار داشته باشند شبکه های بی سیم جواب مناسبی برای آنها ست. انسان موجودی اجتماعی است. به عبارت دیگر ما برای زندگی بهتر ، به دیگران ،اطلاعات و تجربه آنها نیازمندیم . در گذشته محدودیت های زمانی و مکانیامکان استفاده از تجربه و اطلاعات دیگران را برای همه امکان پذیر نمی ساخت ، اما پدیده اینترنت این محدودیت ها را برداشته است . اگر در گذشته از نبود اطلاعات رنج می بردیم، امروزه با کثرت اطلاعات مواجه هستیم . اینترنت این امکان را به ما داده است که در هر مکان و هر زمانی به اقیانوسی از اطلاعات دسترسی داشته باشیم. اما آیا اینترنت این خاصیت را دارد که همه کس با هر سواد و تجربه ای بتوانددر آن اطلاعات خود را منتشر کند ؟ همچنین میلیونها سایت و منبع اطلاعاتی وجود دارد که اطلاعات بسیاری با موضوعات مختلف را منتشر می کنند . اما سوال همواره مطرح این است که در میان این اقیانوس پهناور، اطلاعات موردنیاز ما کجاست؟ راه دسترسی به اطلاعات مورد نیاز چیست؟ از میان حجم عظیم اطلاعات، کدامها موثق و قابل استناد هستند؟ آیا می توان به

هراطلاعاتی استناد کرد؟در دنیای امروز با افزایش جمعیت و رشد شهرها ضرورت برقراری ارتباط مفید وموثر بیش از پیش احساس می شود و همواره تغییر و تحول چشمگیری در این خصوص از سوی صاحبان صنعت ارتباطات در جهان صورت می گیرد . پیدایش ابزارهای ارتباطی اولیه نظیر مورس و تلگراف سبب شد تا انسان ها خود را به یکدیگر نزدیک تر کنند و اختراع تلفن

باعث گردید این نزدیکی بیشتر احساس شود . تلفن به عنوان یک پدیده خارق العاده در جهان ارتباطات از دیرباز مطرح بوده و تا ابد هم باقی خواهد ماند . سرانجام با به میان آمدن رایانه و آرپانت یاهمان اینترنت امروزی، افق جدیدی در عرصه ارتباطات گشوده شد و به همین بهانه شبکه های ارتباطی پایدار شدند . گسترش جوامع اداری باعث شد شبکه های رایانه ای نیز رشد چشمگیری پیدا کنند و امروزه شاهد یک نبرد واقعی دراین زمینه باشیم. مبحث شبکه بسیار گسترده و پیچیده است، اما ما در اینجا به بررسی شکل نوینی از شبکه های رایانه ای و ارتباطی تحت عنوان بی سیم یا Wireless خواهیم پرداخت . فن آوری بی سیم مدتهاست که مورد استفاده قرار می گیرد. برقراری ارتباط تلفن همراه ، بین شهری و یا بین المللی و نیز برقراری ارتباط بین یگان های نظامی فقط گوشه ای از این فن آوری است . اما تبادل اطلاعات ازیک محل به محل دیگر دسترسی جدیدی در دنیای بی سیم فراهم آورده و هر روزبر دامنه کاربران آن افزوده می شود.

3- مقایسه شبکه های بی سیم و کابلی:

در مقایسه شبکه های بی سیم و کابلی می تواند قابلیتهای زیر مورد بررسی قرار گیرد:

نصب و راه اندازی

هزینه

قابلیت اطمینان کارائی

امنیت

3-1- نصب و راه اندازی

در شبکه های کابلی بدلیل آنکه به هر یک از ایستگاههای کاری بایستی از محل سویئچ مربوطه کابل کشیده شود با مسائلی همچون سوارخکاری ، داکت کشی ، نصب پریز ومواجه هستیم در ضمن اگر محل فیزیکی ایستگاه مورد نظر تغییر یابد بایستی که کابل کشی مجدد .صورت پذیرد.

شبکه های بی سیم از امواج استفاده نموده و قابلیت تحرک بالائی را دارا هستند بنابراین تغییرات در محل فیزیکی ایستگاههای کاری به راحتی امکان پذیر می باشد برای راه اندازی آن کافیست که از روشهای زیر بهره برد:

Ad hoc: **که ارتباط مستقیم یا همتا به همتا (peer to peer) تجهیزات را با یکدیگر میسرمی سازد**

Infrastructure : که باعث ارتباط تمامی تجهیزات با دستگاه مرکزی می شود.

بنابراین میتوان دریافت که نصب و را ه اندازی شبکه های کابلی یا تغییرات در آن بسیار مشکلتر نسبت به مورد مشابه یعنی شبکه های بی سیم است.

3-2-هزینه تجهیزاتی همچون هاب ، سوئیچ یا کابل شبکه نسبت به مورد های مشابه در شبکه

های بی سیم ارزانتر می باشد اما درنظر گرفتن هزینه های نصب و تغییرات احتمالی محیطی نیز قابل توجه است. قابل به ذکر است که با رشد روز افزون شبکه های بی سیم ، قیمت آن نیز در حال کاهش است.

3-3- قابلیت اطمینانتجهیزات کابلی بسیار قابل اعتماد میباشند که دلیل سرمایه گذاری

تهیه کننده :سید حمید یاریان

سازندگان از حدود بیست سال گذشته نیز همین میباشد فقط بایستی در موقع نصب و یا جابجائی ، اتصالات با دقت کنترل شوند.

تجهیزات بی سیم همچون Broadband Router ها مشکلاتی مانند قطع شدن‌های پیاپی، تداخل امواج الکترومغناطیس، تداخل با شبکه‌های بی‌سیم مجاور و ... را داشته اند که روند رو به تکامل آن نسبت به گذشته مانند (802.11g) باعث بهبود در قابلیت اطمینان نیز داشته است.

3-4- کارائیشبکه های کابلی دارای بالاترین کارائی هستند در ابتدا پهنای باند 10 Mbps سپس به پهنای باندهای بالاتر100 Mbps و 1000 Mbps افزایش یافتند حتی در حال حاضر سوئیچهائی با پهنای باند 1 Gbps نیز ارائه شده است شبکه های بی سیم با استاندارد 802.11 b حداکثر پهنای باند 11 Mbpsو با 802.11 a و 802.11 g پهنای باند 54 Mbps را پشتیبانی می کنند حتی در تکنولوژیهای جدید این روند با قیمتی نسبتا بالاتر به 108 Mbpsنیز افزایش داده شده است علاوه بر این کارائی Wi-Fi نسبت به فاصله حساس می باشد یعنی حداکثر کارائی با افزایش فاصله نسبت به Access Point پایینخواهد آمد. این پهنای باند برای به اشتراک گذاشتن اینترنت یافایلها کافی بوده اما برای برنامه هائی که نیاز به رد و بدل اطلاعات زیاد بین سرور و ایستگاهای کاری(Client to Server) دارند کافی نیست .

3-5- امنیت بدلیل اینکه در شبکه های کابلی که به اینترنت هم متصل هستند، وجود دیواره آتش از الزامات است و تجهیزاتی مانند هاب یا سوئیچ به تنهایی قادر به انجام وظایف دیواره آتش نمی باشند بایست یدرچنین شبکه هایی دیواره آتش مجزایی نصب شود.

تهیه کننده :سید حمید یاریان

تجهیزات شبکه های بی سیم مانندBroadband Router ها دیواره آتش بصورت نرم افزاری وجود داشته و تنها بایستی تنظیمات لازم صورت پذیرد. از سوی دیگر به دلیل اینکه در شبکه‌های بی‌سیم از هوا بعنوان رسانه انتقال استفاده میشود، بدون پیاده سازی تکنیک‌های خاصی مانند رمزنگاری، امنیت اطلاعات بطور کامل تامین نمی گردد استفاده از رمزنگاری WEP (Wired Equivalent Privacy) باعث بالا رفتن امنیت در این تجهیزات گردیده است.

4-تشریح مقدماتی شبکه های بی سیم و کابلی

شبکه های محلی (LAN) برای خانه محیط کار می توانند به دو صورت کابلی (Wired) یا بی سیم(Wireless) طراحی گردند . درابتدا این شبکه ها به روش کابلی با استفاده از تکنولوژی Ethernet طراحی می شدند اما اکنون با روند رو به افزایش استفاده از شبکه های بی سیم با تکنولوژی Wi-Fi مواجه هستیم. در شبکه های کابلی (که در حال حاضر بیشتر با توپولوژی ستاره ای بکار می روند) بایستی از محل هر ایستگاه کاری تا دستگاه توزیع کننده (هاب یا سوئیچ) به صورت مستقل کابل کشی صورت پذیرد(طول کابل از نوع CAT5 نبایستی 100 متر بیشتر باشد در غیر اینصورت از فیبر نوری استفاده میگردد) که تجهیزات بکار رفته از دونوع غیر فعال (Passive) مانند کابل ، پریز، داکت پچ پنل و فعال(Active) مانند هاب ،سوئیچ ،روتر ، کارت شبکه هستند.

موسسه مهندسی IEEEاستانداردهای u 802.3 را برای Fast Ethernet وab 802.3 و z 802.3 را برای Gigabit Ethernet مربوط به کابلهای الکتریکی و نوری در نظر گرفته است

تهیه کننده :سید حمید یاریان

.شبکه های بی سیم نیز شامل دستگاه مرکزی (Access Point) می باشد که هر ایستگاه کاری می تواند حداکثرتا فاصله 30 متر ی آن (بدون مانع) قرار گیرد. شبکه های بی سیم(wln) یکی از سه استاندارد ارتباطیwi-fi زیر را بکار می برند .

استاندارد	مشخص
۸۰۲,۱۱ b	اولین استانداردی است که به صورت گسترده بکار ر فته است
۸۰۲,۱۱ a	سریعتر، اما گران تر از ۸۰۲ , ۱۱ b می باشد
۸ ۰۲,۱۱ G	جدیدترین استاندارد و شامل هر دو استاندارد قبلی است و از همه گران تر است

4- شبکه‌های بی‌سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط اموج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و

تهیه کننده :سید حمید یاریان

امکان نقل و انتقال تجهیزات متصل به این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند :

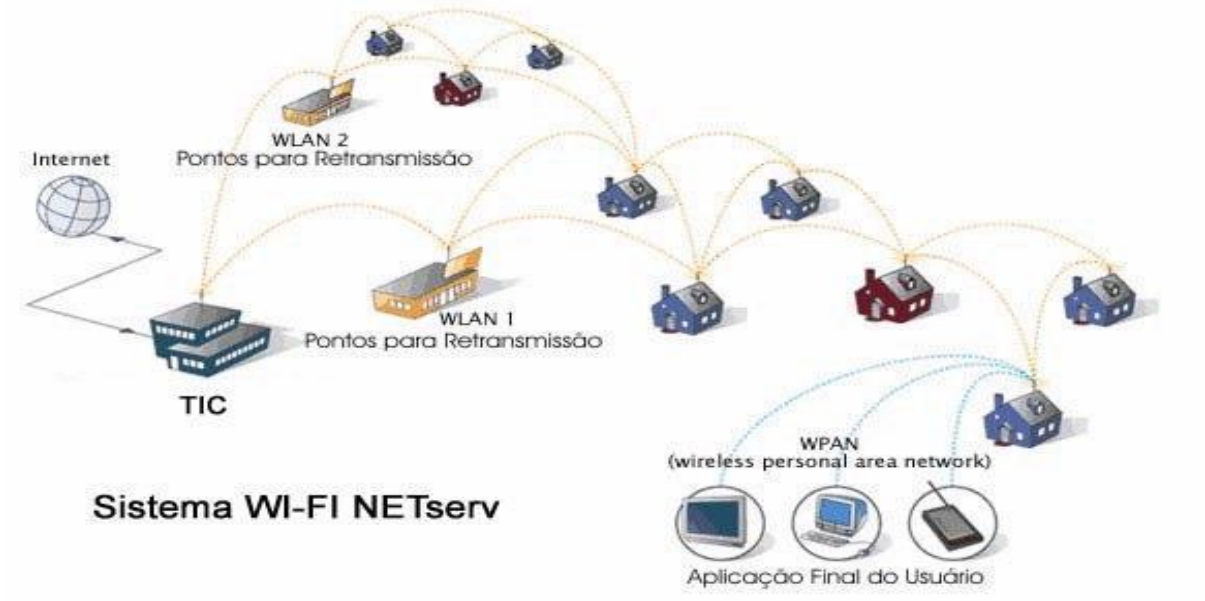
WWAN ، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند.کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانگی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند. شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad Hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی است که در کنار مزایایی که این پویایی برای استفاده کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این

حقیقت که عمل‌کرد Bluetooth بر اساس فرستنده و گیرنده‌های کم‌توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل‌توجه‌یی محسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می‌گردد. به‌عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می‌آیند .

تهیه کننده :سید حمید یاریان

5-انواع شبکه های **Wireless** از نظر ابعاد



با گسترش شهرها و بوجود آمدن فاصله های جغرافیایی بین مراکز سازمان ها و شرکت ها و عدم رشد امکانات مخابراتی با رشد نیاز ارتباطی داخل کشور ، یافتن راه حل و جایگزین مناسب جهت پیاده سازی این ارتباط شدیدا احساس می شود که در این زمینه سیستم های مبتنی بر تکنولوژی بی سیم انتخاب مناسبی می باشد.

5-1- (Personal Arean Network) PAN

سیستم های بی سیم که دارای برد و قدرت انتقال پایین هستند را شامل می شود که این ارتباط غالبا بین افراد برقرار می شود. نمونه این تکنولوژی در سیستم ها Infrared برای ارتباط نقطه به

تهیه کننده :سید حمید یاریان

نقطه دو شخص و یا **Bluethooth** برای ارتباط یک نقطه به چند نقطه جهت ارتباط یک شخص به چند شخص می باشد. استاندارد مورد استفاده در این محدوده کاربرد **IEEE ۸۰۲,۱۵** می باشد.

5-2- LAN (Local Area Netwok)

در این دسته بندی سیستم های بی سیم از استاندارد **IEEE ۸۰۲,۱۱** استفاده می کنند. این محدوده کاربری معادل محدوده شبکه های **LAN** باسیم بوده که برپایه تکنولوی بی سیم ایجاد شده است.

5-3- MAN (Metropolitan Area Netwok)

سیستم های بی سیم از استاندارد **IEEE ۸۰۲,۱۶** استفاده می کنند. محدوده پوشش فراتر از محدوده **LAN** بوده و قالبا چندین **LAN** را شامل می شود. سیستم های **WIMAX** اولیه مبتنی بر این استاندارد هستند.

5-4- WAN (Wide Area Netwok)

سیستم های بی سیم مبتنی بر استاندارد **IEEE ۸۰۲,۱۶ e** هستند که به **IEEE ۸۰۲,۲۰** نیز شهرت یافته اند. سیستم های **WIMAX** در ابعاد کلان و بدون محدودیت حرکتی در این محدوده کار می کنند.

5-5- WPAN (Wireless Personal Area Networks)

و محوطه کوچکی را پوشش می دهد و از استاندارد(IEEE 802.15) **Bluetooth** و **IR (Infra Red)** استفاده می کند . به قطعات (Device)اجازه برقراری ارتباط با یکدیگر در محدوده کوچک را می دهد . بهترین نمونه برای **W PAN، Bluetooth** می باشد . البته در **IR** نیاز به ارتباط مستقیم بوده و محد ودیت مسافت وجود دارد.

تهیه کننده :سید حمید یاریان

5-6- WLAN (Wireless Local Area Networks)

این نوع از شبکه های بی سیم، امکان به اشتراک گذاری اطلاعات را بین تجهیزات مختلف که در فاصله محدود از یکدیگر قرار دارند میسر می سازد . محدوده کوچکی را پوشش می دهد و از تکنولوژیWiFi استفاده می کند . این نمونه از شبکه هایWireless ی برای کاربران محلی از جمله محیطهای (Campus)دانشگاهی یا آزمایشگاه ها که نیاز به استفاده از اینترنت دارند مفید می باشد .در این حالت اگرتعداد کاربران محدود باشند می توان بدون استفاده ازAccess Point این ارتباط را برقرار نمود . در غیر این صورت استفاده ازAccess Point ضروری است .می توان با استفاده از آنتن های مناسب مسافت ارتباطی کاربران را به شرط عدم وجود مانع تا حدی طولانی تر نمود . استاندارد IEEE 802.11 در این زمینه مطرح است .

5-7- WWAN (Wireless Wide Area Networks)

برای شبکه هائی با فواصل زیاد همچون بین شهرها یا کشورها بکار می رود . این ارتباط از طریق آنتن های بی سیم یا ماهواره صورت می پذیرد.

5-8- WMAN (Wireless Metropolitan Area Networks)

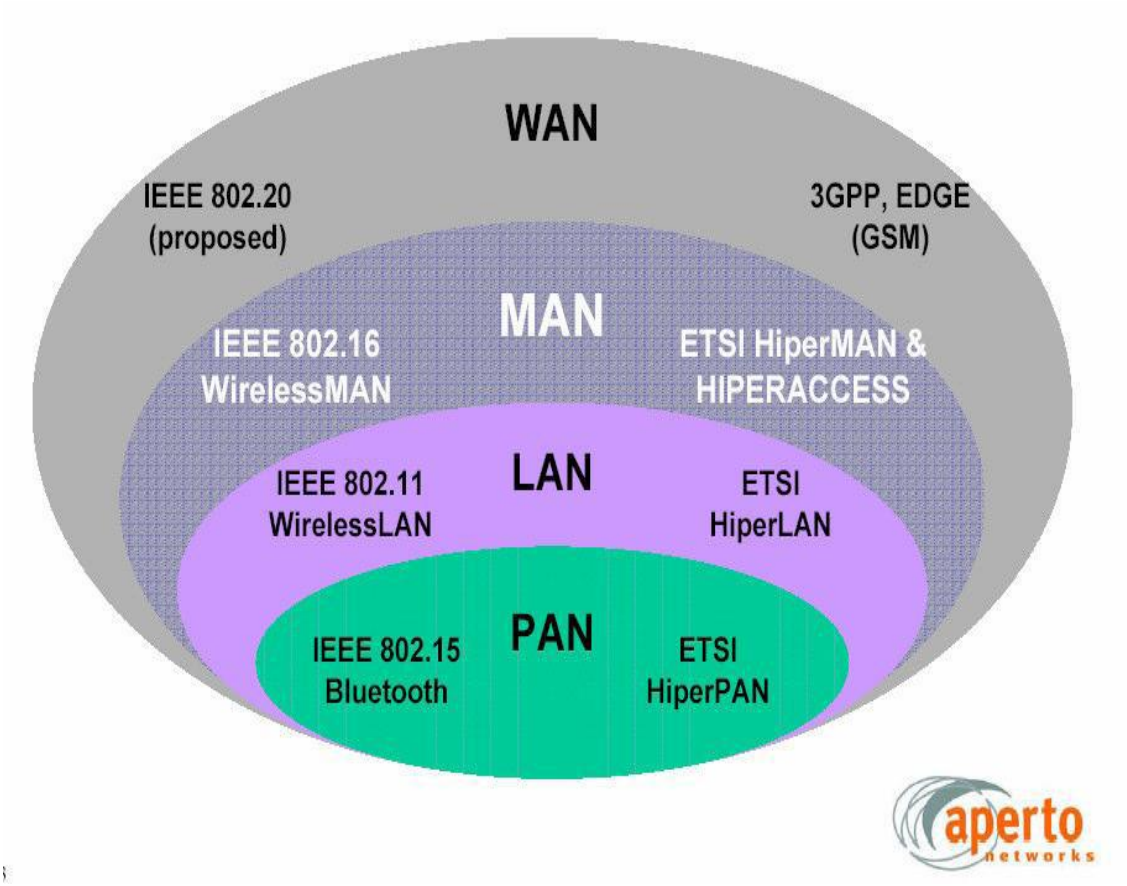
توسط این تکنولوژی ارتباط بین چندین شبکه یا ساختمان در یک شهر برقرار می شود. برای Backup آن می توان از خطوط اجاره ای، فیبر نوری یا کابل های مسی استفاده نمود . استاندارد IEEE 802.16در این زمینه مطرح شده است . در ضمن، از تکنولوژیها Wimax برای اتصال مناطق وسیع (به وسعت شهرها) در این شبکه استفاده می شود.

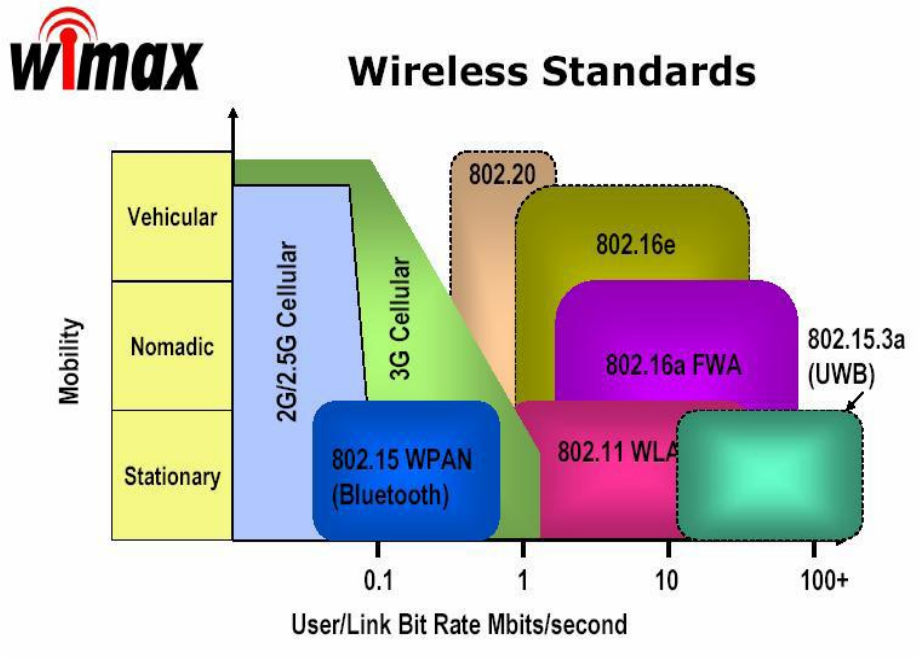
تهیه کننده :سید حمید یاریان

WAN (Wireless Global Area Networks)(WGAN_9-5

گام نهایی، شبکه جهانی (WGAN)است .طرح پیشنهادی برای آن IEEE 802.20 استیک شبکه WGAN می تواند مانند شبکهCell Phone کنونی عمل کند و کاربران می توانند در کشورها مسافرت کنند، در حالی که همه وقت به شبکه متصلند . چنین شبکه ای نظیر سرویس مودم کابلی، دارای پهنای باند کافی برای دستیابی به اینترنت است. در دو شکل زیر پوشش دهی، استانداردها و تکنولوژی های شبکه های بی سیم نشان داده شده است.

تهیه کننده :سید حمید یاریان





تهیه کننده :سید حمید یاریان

6- سیستم های Wireless

سیستم های Wireless می توانند به سه دسته اصل ی تقسیم شوند :

6-1- سیستم Wireless ثابت : این سیستم ها از امواج رادیوی ی استفاده می کنند و خط دید مستقیم بر ای برقرا ری ارتباط لازم را دار ند . بر خلاف تلفن های همراه و یا دیگر دستگاه های Wireless , این سیستم ها از آنتن های ثابت استفاده می کنند و به طور کلی می توانند جانشین مناسبی بر ای شبکه های کابلی باشند و می توانند بر ای‌ارتباطات پرسرعت اینترنت و یا تلویزیون مورد استفاده قرار گیرند . امواج رادیویی‌ای هم وجود دارند که می توانند اطلاعات بیشتری را انتقال دهند و در نتیجه از هزینه ها می‌کاهند.

6-2- سیستم Wireless قابل حمل : دستگاهی است که معمولا خارج از خانه، دفتر کار و یا در وسایل نقلیه مورد استفاده قرار می گیرند . نمونه های این سیستم عبارتند از : تلفن های همراه، نوت بوکها، دستگاه های پیغام گیر و PDA ها . این سیستم از مایکروویو و امواج رادیویی جهت انتقال اطلاعات استفاده می کند.

6-3- سیستم Wireless مادون قرمز : این سیستم از امواج مادون قرمز جهت انتقال سیگنالهای محدود بهره می برد . این سیستم معمولا در دستگاه‌های کنترل از راه دور، تشخیص دهنده‌های حرکت و دستگاه های بی سیم کامپیوترهای شخصی استفاده می شود . با پیشرفت حاصل در سال های اخیر، این سیستم ها امکان اتصال کامپیوتر های نوت بوک و کامپیوتر های معمول به هم

تهیه کننده :سید حمید یاریان

را نیز می دهند وشما به راحتی می توانید توسط این نوع از سیستم های Wireless شبکه های داخلی راه اندازی کنید.

7-انواع استاندارد 802.11

اولین بار در سال 1990 بوسیله انستیتیو IEEE معرفی گردید که اکنون تکنولوژیهای متفاوتی از این استاندارد برای شبکه های بی سیم ارائه گردیده است.

7-1-1- : 802.11

برای روشهای انتقال FHSS (frequency hopping spared spectrum) یا DSSS (direct sequence spread spectrum)با سرعت Mbps1 تا Mbps 2 در کانال GHz 2.4 قابل استفاده می باشد.

7-1-2- 802.11a

برای روشهای انتقال OFDM (orthogonal frequency division multi plexing) با سرعت Mbps 54در کانال GHz 5قابل استفاده است.

7-1-3- : 802.11b

این استاندارد با نام WI-Fi یا High Rate 802.11 قابل استفاده در روش DSSS بوده و در شبکه های محلی بی سیم نیز کاربرد فراوانی دارد همچنین دارای نرخ انتقال Mbps 11 می باشد .

7-1-4- : 802.11g

تهیه کننده :سید حمید یاریان

این استاندارد برای دستیابی به نرخ انتقال بالای 20 Mbps در شبکه های محلی بی سیم و در کانال 2.4 GHz کاربرد دارد.

7-2- استانداردهای ارتباطیWi-Fi :

شبکه های بی سیم (Wlan) یکی از سه استانداردارتباطی Wi-Fi زیر را بکار می برند:

802.11b : که اولین استانداردی است که به صورت گسترده بکار رفته است .

802.11a :سریعتر اما گرانتر از b 802.11 می باشد .

802.11g : جدیدترین استاندارد که شامل هر دو استاندارد قبلی بوده و از همه گرانتر میباشد.

هر دونوع شبکه های کابلی و بی سیم ادعای برتری بر دیگری را دارند اما انتخاب صحیح با در نظر گرفتن قابلیتهای آنها میسر می باشد.

8-استاندارد شبکه های محلی بی سیم

8-1- مقدمه

امروزه با بهبود عملکرد، کارایی و عوامل امنیتی، شبکه‌های بی‌سیم به شکل قابل توجهی در حال رشد وگسترش هستند و استاندارد IEEE 802.11 استاندارد بنیادی است که شبکه‌های بی‌سیم بر مبنای آن طراحی و پیاده سازی می‌شوند.

در ماه ژوئن سال 1997 انجمن مهندسان برق و الکترونیک (IEEE) استاندارد IEEE 802.11- 1997 را به عنوان اولین استانداردِ شبکه‌های محلی بی‌سیم منتشر ساخت. این استاندارد در سال 1999 مجدداً بازنگری شد و نگارش روز آمد شده آن تحت عنوان IEEE802.11- 1999 منتشر شد. استاندارد جاری شبکه‌های محلی بی‌سیم یا همان IEEE 802.11 تحت عنوان ISO/IEC تهیه کننده :سید حمید یاریان

8802.11_1999، توسط سازمان استاندارد سازی بین‌المللی (ISO) و مؤسسه استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال 1997، شکل گیری و پیدایش شبکه سازی محلی بی‌سیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد 1997، پهنای باند 2Mbps را تعریف می‌کند با این ویژگی که در شرایط نامساعد و محیط‌های دارای اغتشاش (نویز) این پهنای باند می‌تواند به مقدار 1Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند 1 Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط‌های عاری از اغتشاش (نویز) پهنای باند 2 Mbpsنیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی 2.4 GHz عمل می‌کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون‌های رادیویی DSSS و FHSS به عنوان رسانه انتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری 802.11 به زیر گروه‌های متعددی تقسیم می‌شود. شکل‌های 8-1 و 8-2 گروه‌های کاری فعال در فرآیند استاندارد سازی را نشان می‌دهد.

برخی از مهم‌ترین زیر گروه‌ها به قرار زیر است :

- 802.11D: Additional Regulatory Domains

- 802.11E: Quality of Service (QoS)

- 802.11F: Inter-Access Point Protocol (IAPP)

- 802.11G: Higher Data Rates at 2.4 GHz

- 802.11H: Dynamic Channel Selection and Transmission Power Control

تهیه کننده :سید حمید یاریان

- 802.11i: Authentication and Security

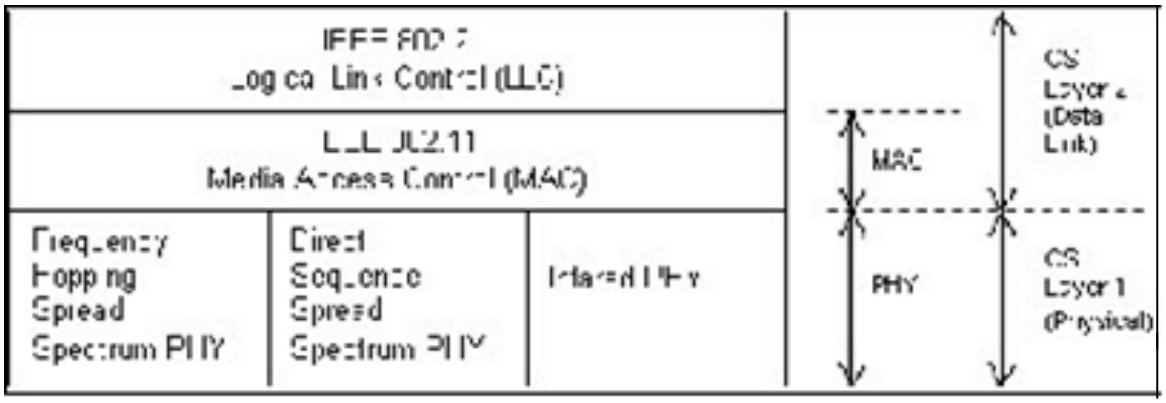
کمیته 802.11 e کمیته‌ای است که سعی دارد قابلیت QoS اِتـرنت را در محیط شبکه‌های بی‌سیم ارائه کند. توجه داشته باشید که فعالیت‌های این گروه تمام گونه‌های 802.11 شامل a، b، و g را در بر دارد. این کمیته در نظر دارد که ارتباط کیفیت سرویس سیمی یا Ethernet QoS را به دنیای بی‌سیم بیاورد.

کمیته 802.11 g کمیته‌ای است که با عنوان 802.11 توسعه یافته نیز شناخته می‌شود. این کمیته در نظر دارد نرخ ارسال داده‌ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یا باند فرکانسی صنعتی، پژوهشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده 2400 مگاهرتز تا 2483.5 مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهای تشعشع رادیویی نیازی به مجوز ندارد. استاندارد 802.11 g تا کنون نهایی نشده است و مهم‌ترین علت آن رقابت شدید میان تکنیک‌های مدولاسیون است. اعضاء این کمیته و سازندگان تراشه توافق کرده‌اند که از تکنیک تسهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می‌تواند به عنوان یک روش جایگزین و رقیب مطرح باشد.

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

فعالیت دو کمیته 802.11 i و 802.11 x در ابتدا برروی سیستم‌های مبتنی بر 802.11 b تمرکز داشت. این دو کمیته مسئول تهیه پروتکل‌های جدید امنیت هستند. استاندارد اولیه از

الگوریتمی موسوم به WEP استفاده می‌کند که در آن دو ساختار کلید رمز نگاری به طول 40 و 128 بیت وجود دارد. WEP مشخصاً یک روش رمزنگاری است که از الگوریتم RC4 برای رمزنگاری فریم‌ها استفاده می‌کند. فعالیت این کمیته در راستای بهبود مسائل امنیتی شبکه‌های محلی بی‌سیم است.این استاندارد لایه‌های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بی‌سیم را دربردارد.



شکل 3-8- مقایسه مدل مرجع OSI و استاندارد 802.11

محیط‌های بی‌سیم دارای خصوصیات و ویژگی‌های منحصر به فردی می‌باشند که در مقایسه با شبکه‌های محلی سیمی جایگاه خاصی را به این گونه شبکه‌ها می‌بخشد. به طور مشخص ویژگی‌های فیزیکی یک شبکه محلی بی‌سیم محدودیت‌های فاصله، افزایش نرخ خطا و کاهش قابلیت اطمینان رسانه، همبندی‌های پویا و متغیر، تداخل امواج، و عدم وجود یک ارتباط قابل اطمینان و پایدار در مقایسه با اتصال سیمی است. این محدودیت‌ها، استاندارد شبکه‌های محلی بی‌سیم را وا می‌دارد که فرضیات خود را بر پایه یک ارتباط محلی و با بُرد کوتاه بنا نهد. پوشش‌های جغرافیایی وسیع‌تر از

طریق اتصال شبکه‌های محلی بی‌سیم کوچک برپا می‌شود که در حکم عناصر ساختمانی شبکه گسترده هستند. سیـّار بودن ایستگاه‌های کاری بی‌سیم نیز از دیگر ویژگی‌های مهم شبکه‌های محلی بی‌سیم است. در حقیقت اگر در یک شبکه محلی بی‌سیم ایستگاه‌های کاری قادر نباشند در یک محدوده عملیاتی قابل قبول و همچنین میان سایر شبکه‌های بی‌سیم تحرک داشته باشد، استفاده از شبکه‌های 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 **802.11** می‌بایست از دید لایه‌های بالاتر مشابه یک شبکه محلی مبتنی بر استاندارد **802** عمل کند. بدین خاطر لایه **MAC** در این استاندارد مجبور است که سیـّاربودن ایستگاه‌های کاری را به گونه‌ای شفاف پوشش دهد که از دید لایه‌های بالاتر استاندارد این سیـّاربودن احساس نشود. این نکته سبب می‌شود که لایه**MAC** در این استاندارد وظایفی را بر عهده بگیرد که معمولاً توسط لایه‌های بالاتر شبکه انجام می‌شوند. در واقع این استاندارد لایه‌های فیزیکی و پیوند داده جدیدی به مدل مرجع **OSI** اضافه می‌کند و به طور مشخص لایه فیزیکی جدید از فرکانس‌های رادیویی به عنوان رسانه انتقال بهره می‌برد.

شکل **8-4**، جایگاه این دو لایه در مدل مرجع **OSI** را در کنار سایر پروتکل‌های شبکه سازی نشان می‌دهد. همانگونه که در این شکل مشاهده می‌شود وجود این دولایه از دید لایه‌های فوقانی شفاف است .

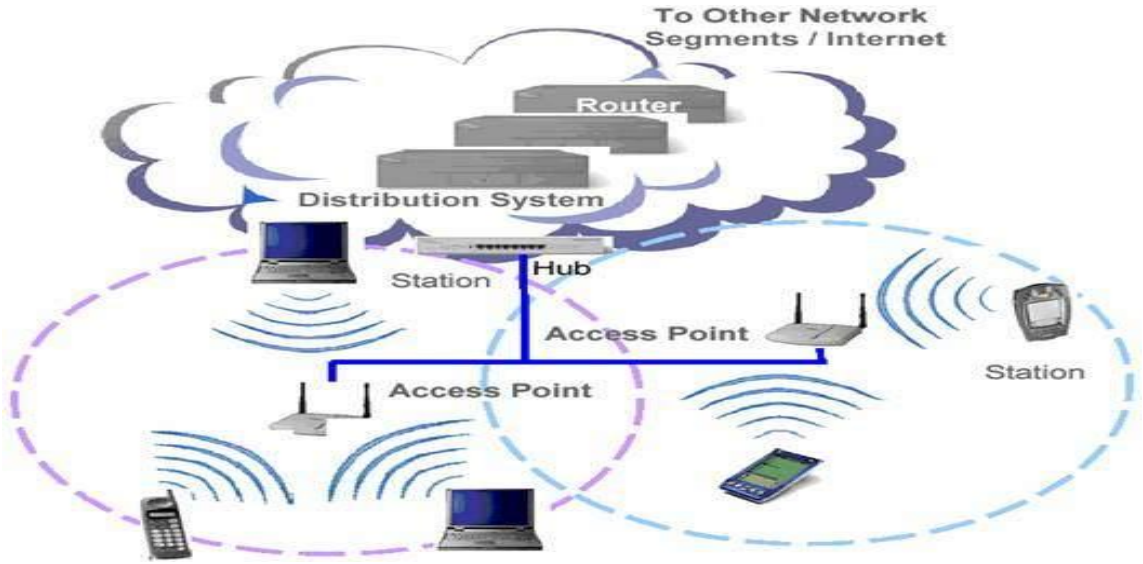
تهیه کننده :سید حمید یاریان

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

9- معماری شبکه‌های محلی بی‌سیم

معماری 802.11 از عناصر ساختمانی متعددی تشکیل شده است که در کنار هم، سـّیار بودن ایستگاه‌های کاری را پنهان از دید لایه‌های فوقانی برآورده می‌سازد. ایستگاه بی‌سیم یا به اختصار ایستگاه (STA)، بنیادی‌ترین عنصر ساختمانی در یک شبکه محلی بی‌سیم است. یک ایستگاه، دستگاهی است که بر اساس تعاریف و پروتکل‌های 802.11 (لایه‌های MAC و PHY) عمل کرده و به رسانه بی‌سیم متصل است. توجه داشته باشید که براساس تعریف کلاسیکِ شبکه‌های کامپیوتری، یک شبکه کامپیوتری مجموعه‌ای از کامپیوترهای مستقل و متصل است که منظور از اتصال در این تعریف، توانایی جابجایی و مبادله پیام‌ها است. ایستگاه‌های کاری بی‌سیم امروزی عمدتاً به صورت مجموعه سخت‌افزاری/نرم‌افزاری کارت‌های شبکه بی‌سیم پیاده‌سازی می‌شوند. همچنین یک ایستگاه می‌تواند یک کامپیوتر قابل حمل، کامپیوتر کفدستی و یا یک نقطه دسترسی باشد. نقطه دسترسی در واقع در حکم پلی است که ارتباط ایستگاه‌های بی‌سیم را با سیستم توزیع یا شبکه سیمی برقرار می‌سازد.کوچکترین عنصر ساختمانی شبکه‌های محلی بی‌سیم در استاندارد 802.11 *مجموعه سرویس پایه*یا(BSS(Basic Service Set نامیده می‌شود. در واقع BSS مجموعه‌ای از ایستگاه‌های بی‌سیم است.

تهیه کننده :سید حمید یاریان



9-1- همبندی‌های 802.11

در یک تقسیم بندی کلی می‌توان دو همبندی را برای شبکه‌های محلی بی‌سیم در نظر گرفت. ساده‌ترین همبندی، *فی‌البداهه* (**Ad Hoc**) و براساس فرهنگ واژگان استاندارد **802.11**، **IBSS (Independent Basic Service Set)** است. در این همبندی ایستگاه‌ها از طریق رسانه بی‌سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده (تبادل پیام) از تجهیزات یا ایستگاه واسطی استفاده نمی‌کنند. واضح است که در این همبندی به سبب محدودیت‌های فاصله هر ایستگاهی ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در همبندی **IBSS** آن است که ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان بُرد شبکه بی‌سیم قرار داشته باشند. شکل **9-1** همبندی **IBSS**را نشان می‌دهد.

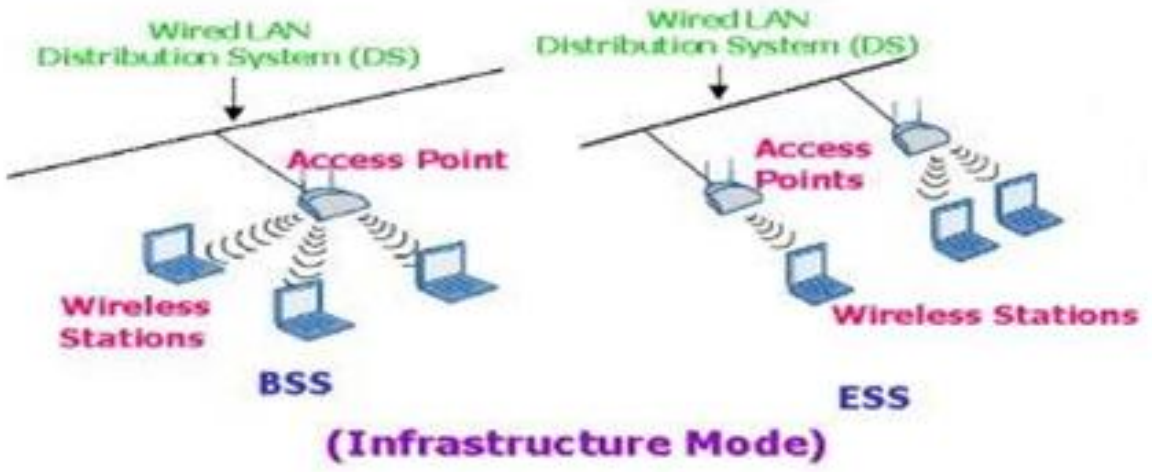
تهیه کننده :سید حمید یاریان

شکل 9-1- همبندی فی‌البداهه یا IBSS

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

تهیه کننده :سید حمید یاریان

شکل 9-2 همبندی زیرساختار را نشان می‌دهد.



شکل 9-2-همبندی زیرساختار در دوگونه BSS و ESS

در این هم بندی سیستم توزیع، رسانه‌ای است که از طریق آن نقطه دسترسی (AP) با سایر نقاط دسترسی در تماس است و از طریق آن می‌تواند فریم‌ها را به سایر ایستگاه‌ها ارسال نماید. از سوی دیگر می‌تواند بسته‌ها را در اختیار ایستگاه‌های متصل به شبکه سیمی نیز قراردهد. در استاندارد 802.11 توصیف ویژه‌ای برای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین می‌کند که سیستم توزیع می‌بایست ارائه نماید. بنابراین سیستم توزیع می‌تواند یک شبکه 802.3 معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم می‌کند.

استاندارد 802.11 با استفاده از همبندی خاصی محدوده عملیاتی شبکه را گسترش می‌دهد. این همبندی به شکل *مجموعه سرویس گسترش یافته* ESS(Extended Service Set) بر پا می‌شود. در این

روش یک مجموعه گسترده و متشکل از چندین **BSS** یا *مجموعه سرویس پایه* از طریق نقاط دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیک داده بین مجموعه‌های سرویس پایه مبادله شده و انتقال پیام‌ها شکل می‌گیرد. در این همبندی ایستگاه‌ها می‌توانند در محدوده عملیاتی بزرگ‌تری گردش نمایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم می‌شود. در واقع سیستم توزیع ستون فقرات شبکه‌های محلی بی‌سیم است و می‌تواند با استفاده از فنّاوری بی‌سیم یا شبکه‌های سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان یک لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش می‌باشد. نکته قابل توجه در این همبندی آن است که تجهیزات شبکه خارج از حوزه **ESS** تمام ایستگاه‌های سیـّار داخل **ESS** را صرفنظر از پویایی و تحرکشان به صورت یک شبکه منفرد در سطح لایه **MAC** تلقی می‌کنند. به این ترتیب پروتکل‌های رایج شبکه‌های کامپیوتری کوچکترین تأثیری از سیـّار بودن ایستگاه‌ها و رسانه بی‌سیم نمی‌پذیرند. جدول **9-1** همبندی‌های رایج در شبکه‌های بی‌سیم مبتنی بر **802.11** را به اختصار جمع بندی می‌کند.

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

*جدول **9-1**- همبندیهای رایج در استاندارد **802.11***

9-2- خدمات ایستگاهی

تهیه کننده :سید حمید یاریان

بر اساس این استاندارد خدمات خاصی در ایستگاه‌های کاری پیاده‌سازی می‌شوند. در حقیقت تمام ایستگاه‌های کاری موجود در یک شبکه محلی مبتنی بر **802.11** و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه‌های سیمی، در شبکه‌های بی‌سیم قابل اعمال نیست استاندارد **802.11** خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می‌نماید. سرویس هویت سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی‌سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی **802.11** دو گونه خدمت هویت سنجی را تعریف می‌کند:

- **Authentication Open System**

- **Shared Key Authentication**

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می‌کند. ایستگاه گیرنده نیز فریمی در پاسخ می‌فرستد که آیا فرستنده را می‌شناسد یا خیر. روش دوم کمی پیچیده‌تر است و فرض می‌کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سّری دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترک و با بهره‌گیری از پروتکلی موسوم به **WEP** اقدام به هویت سنجی یکدیگر

می‌نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این خدمت، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌گردد.

در یک شبکه بی‌سیم، تمام ایستگاه‌های کاری و سایر تجهیزات قادر هستند ترافیک داده‌ای را "بشنوند" در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه‌های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد. به همین دلیل در استاندارد 802.11 پروتکلی موسوم به WEP تعبیه شده است که برروی تمام فریم‌های داده و برخی فریم‌های مدیریتی و هویت سنجی اعمال می‌شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء وپوشش را معادل با شبکه‌های سیمی نماید.

9-3- خدمات توزیع

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

- پیوستن به شبکه

- خروج از شبکه بی‌سیم

- پیوستن مجدد

- توزیع

- مجتمع سازی

سرویس اول یک ارتباط منطقی میان ایستگاه سیّار و نقطه دسترسی فراهم می‌کند. هر ایستگاه کاری قبل از ارسال داده می‌بایست با یک نقطه دسترسی برروی سیستم میزبان مرتبط گردد.

تهیه کننده :سید حمید یاریان

این عضویت، به سیستم توزیع امکان می‌دهد که فریم‌های ارسال شده به سمت ایستگاه سیّار را به درستی در اختیارش قرار دهد. خروج از شبکه بی‌سیم هنگامی بکار می‌رود که بخواهیم اجباراً ارتباط ایستگاه سیّار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیّار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیّار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی‌سیم" است با این تفاوت که در این سرویس ایستگاه سیّار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می‌کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیّار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می‌کند که با نقطه دسترسی قبلی تماس گرفته و فریم‌های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیّار فرستاده شده‌اند. با استفاده از سرویس توزیع فریم‌های لایه **MAC** به مقصد مورد نظرشان می‌رسند. مجتمع سازی سرویسی است که شبکه محلی بی‌سیم را به سایر شبکه‌های محلی و یا یک یا چند شبکه محلی بی‌سیم دیگر متصل می‌کند. سرویس مجتمع سازی فریم‌های **802.11** را به فریم‌هایی ترجمه می‌کند که بتوانند در سایر شبکه‌ها (به عنوان مثال **802.3**) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم‌های سایر شبکه‌ها نیز به فریم‌های **802.11** ترجمه شده و از طریق امواج در اختیار ایستگاه‌های کاری سیّار قرار می‌گیرند.

9-4- دسترسی به رسانه

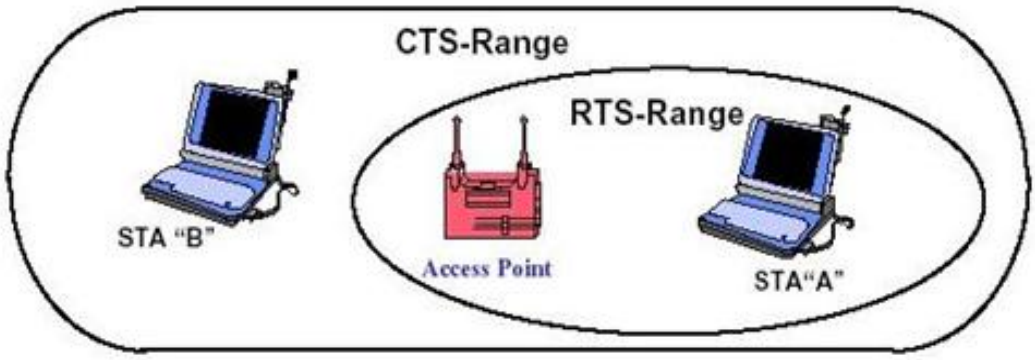
روش دسترسی به رسانه در این استاندارد **CSMA/CA** است که تاحدودی به روش دسترسی **CSMA/CD** شباهت دارد. در این روش ایستگاه‌های کاری قبل از ارسال داده کانال رادیویی را کنترل

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

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

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

تهیه کننده :سید حمید یاریان

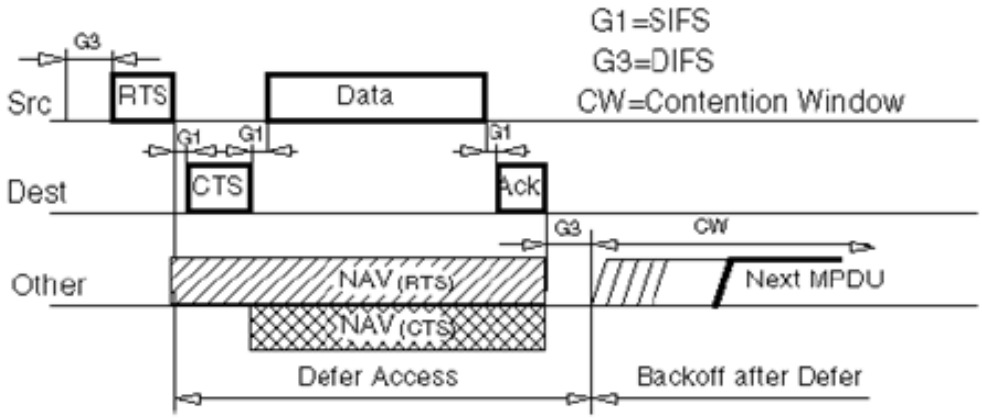


شکل 9-3- روزنه‌های پنهان

برای غلبه بر این مشکل، استاندارد 802.11 از تکنیکی موسوم به *اجتناب از تصادم* و مکانیزم تصدیق استفاده می‌کند. همچنین با توجه به احتمال بروز روزنه‌های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به *شنود مجازی رسانه* یا VCS استفاده می‌شود. در این روش ایستگاه فرستنده ابتدا یک بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می‌فرستد. هنگامی که گیرنده این فریم را دریافت می‌کند، رسانه را کنترل می‌کند و در صورتی که رسانه آزاد باشد فریم کنترلی CTS را به نشانی فرستنده ارسال می‌کند. تمام ایستگاه‌هایی که فریم‌های کنترلی RTS/CTS را دریافت می‌کنند وضعیت کنترل رسانه خود موسوم به شاخصNAV را تنظیم می‌کنند. در صورتی که سایر ایستگاه‌ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می‌کنند که مرتباً به صورت پویا تغییر می‌کند. به این ترتیب مشکل روزنه‌های پنهان حل شده و تصادم‌ها نیز به حداقل مقدار می‌رسند.

تهیه کننده :سید حمید یاریان

شکل 9-4 زمان‌بندی RTS/CTS و وضعیت سایر ایستگاه‌ها را نشان می‌دهد.



شکل 9-4- زمان‌بندی RTS/CTS

9-5- لایه فیزیکی

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

- **استفاده از تکنیک رادیویی DSSS**
- **استفاده از تکنیک رادیویی FHSS**
- **استفاده از امواج رادیویی مادون قرمز**

تهیه کننده :سید حمید یاریان

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

PPM-4مبادله می‌شوند.

9-5-1-ویژگی‌های سیگنال‌های طیف گسترده

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

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

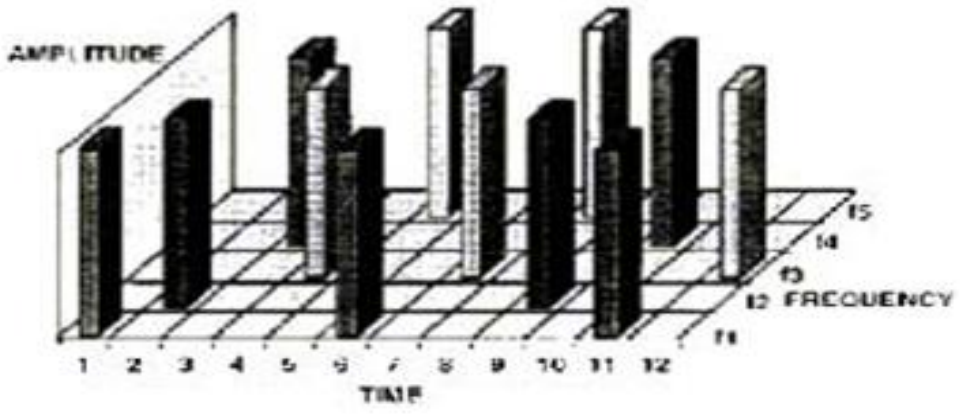
- مصونیت بالا در مقابل پارازیت و تداخل
- رسایی با تفکیک پذیری و دقت بالا
- امکان استفاده در CDMA

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

تهیه کننده :سید حمید یاریان

9-5-2-سیگنال‌های طیف گسترده با جهش فرکانسی

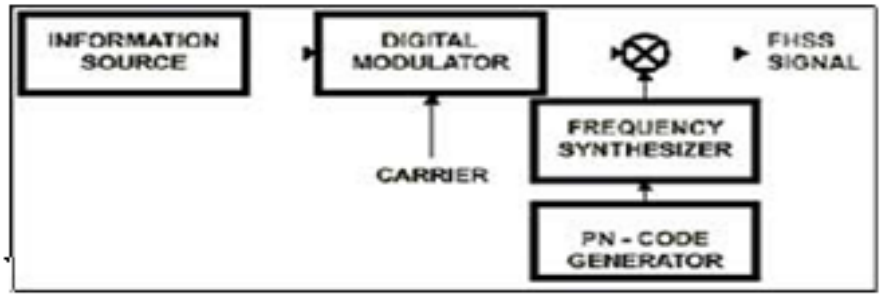
در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می‌کند. شکل 9-5 این تکنیک را در قالب یک نمودار نشان می‌دهد .



شکل 9-5 -تغییر فرکانس سیگنال تسهیم شده به شکل شبه تصادفی

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

تهیه کننده :سید حمید یاریان



code PN-CODE= Pseudonoise

شکل 9-6 - تکنیک FHSS

بر اساسی مقررات FCC و سازمان‌های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی 400 میلی ثانیه است که برابر با حداقل 2.5 جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد 802.11 حداقل فرکانس جهش در آمریکای شمالی و اروپا 6 مگاهرتز و در ژاپن 5 مگاهرتز می‌باشد.

9-5-3-سیگنال‌های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال برروی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کُد به گونه‌ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یک کُد تسهیم می‌شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می‌گردد. در استاندارد 802.11 روش مدولاسیون مورد استفاده در سیستم‌های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تهسیم می‌شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.

از آنجا که در استاندارد 802.11 و سیستم DSSS از روش تسهیم DPSK استفاده می‌شود، داده‌های خام به صورت تفاضلی تسهیم شده و ارسال می‌شوند و در گیرنده نیز یک آشکار ساز

تفاضلی سیگنال‌های داده را دریافت می‌کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی سیگنال‌های داده تغییر می‌کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت‌های داده تغییر می‌کند. جدول زیر ایده مدولاسیون فاز را نشان می‌دهد.

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

جدول 9-2- مدولاسیون فاز

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

تهیه کننده :سید حمید یاریان

بیتهای فرد	بیتهای زوج	اختلاف فاز
1	1	-3pi/4
0	1	3 pi/4
0	0	Pi/4
1	0	-pi/4

جدول 9-3- مدولاسیون تفاضلی

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می‌شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیماً توسط یک دنباله از کدهای شبه تصادفی تسهیم می‌شود. در این تکنیک نرخ بیتی شبه کُد تصادفی، نرخ تراشه نامیده می‌شود. در استاندارد 802.11 از کُدی موسوم به کُد *بارکر* برای تولید کدها تراشه سیستم DSSS استفاده می‌شود. مهم‌ترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه آن یک فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند.

جدول زیر فهرست کامل کدهای بارکر را نشان می‌دهد. همانگونه که در این جدول مشاهده می‌شود کدهای بارکر از 8 دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد 802.11 مورد استفاده قرار می‌گیرد، از کد بارکر با طول 11 (N=11) استفاده می‌شود. این کد به ازاء یک

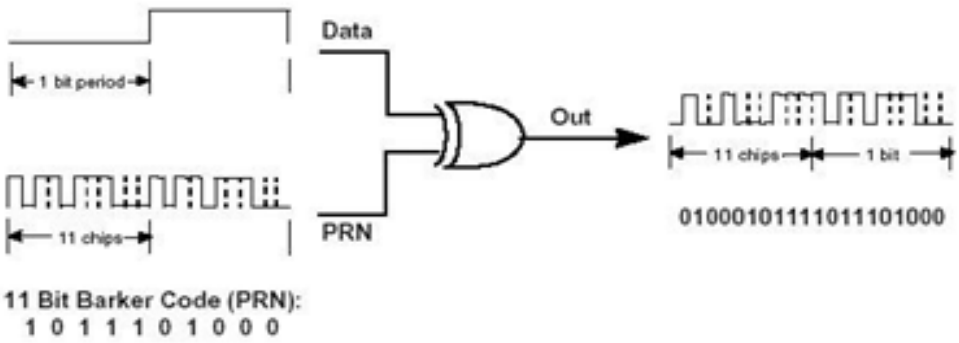
تهیه کننده :سید حمید یاریان

نماد، شش مرتبه تغییر فاز می‌دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد 6 مرتبه تغییر فاز خواهد داد .

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

جدول 9-4- کدهای بارکر

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



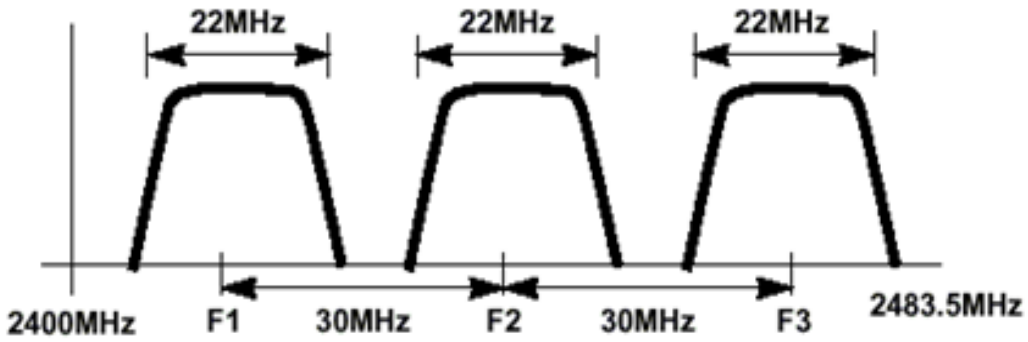
شکل 9-7- مدار مدولاسیون با استفاده از کدهای بارکر

شکل 9-7 مدل منطقی مدولاسیون و پخش سیگنال اطلاعات با استفاده از کدهای بارکر را نشان می‌دهد.

تهیه کننده :سید حمید یاریان

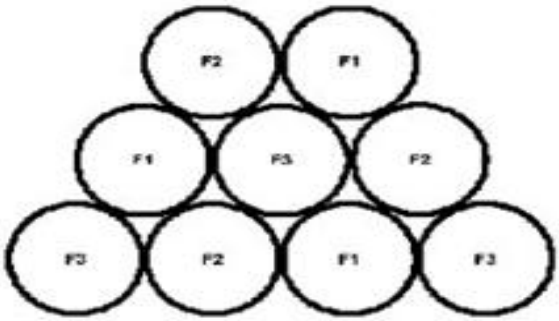
9-6-استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه‌های بی‌سیم، طراحی شبکه سلولی به گونه‌ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد. شکل 9-8 سه کانال DSSS در محدوده فرکانسی ISM را نشان می‌دهد.



شکل 9-8- سه کانال فرکانسی F3,F2,F1

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



شکل 9.9- طراحی شبکه سلولی

در این طراحی به هریک از سلول‌های همسایه یک کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول‌های همسایه به حداقل رسیده است. این تکنیک همان مفهومی است که در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می‌رود. نکته جالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است. خوانندگان علاقمند می‌توانند دایره‌های جدید را در چهار جهت شبکه سلولی شکل فوق با فرکانس‌های متمایز F1,F2,F3 ترسیم و گسترش دهند.

9-7- آنتن‌ها

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

این آنتن‌ها در فواصل کوتاه قابل استفاده هستند و برای بهره گیری در فواصل طولانی‌تر به تقویت کننده‌های خارجی نیاز دارند که البته در بسیاری موارد استفاده از این تقویت کننده‌های

خارجی میسر و یا قانونی نیست. از سوی دیگر آنتن‌های نقطه به نقطه یا خطی در کاربردهای خارجی استفاده می‌شوند و به تنظیم دقیق نیاز دارند. محدوده عملیاتی رایج در آنتن‌های تمام جهته **45** متر و محدوده عملیاتی آنتن های نقطه به نقطه و توان بالا در حدود **40** 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 می‌شود. از جمله عوامل مهمی که محدوده عملیاتی تجهیزات مبتنی بر **IEEE 802.11** را تحت تأثیر قرار می‌دهد محل نصب نقاط دسترسی یا ایستگاه پایه و نیز تداخل رادیویی است. همانگونه که پیشتر گفته شد، تجهیزات مبتنی بر این استاندارد سعی می‌کنند که با بالاترین نرخ ارسال داده کار کنند و در صورت نیاز به سرعت‌های پایین‌تر برگردند .

10-روش های ارتباطی بی سیم

تجهیزات و شبکه های کامپیوتری بی سیم بر دو قسم **Indoor** یا درون سازمانی و **Outdoor** یا برون سازمانی تولید شده و مورد استفاده قرار می گیرند.

10-1- شبکه های بی سیم Indoor :

نیاز سازمان ها و شرکت ها برای داشتن شبکه ای مطمئن و وجود محدودیت در کابل کشی ، متخصصین را تشویق به پیدا کردن جایگزین برای شبکه کامپیوتری کرده است. شبکه های **Indoor** به شبکه هایی اتلاق می شود که در داخل ساختمان ایجاد شده باشد. این شبکه ها بر دو گونه طراحی می شوند. شبکه های **Ad hoc** و شبکه های **Infra Structure**. در شبکه های **Ad hoc** دستگاه متمرکز کننده مرکزی وجود ندارد و کامپیوترهای دارای کارت شبکه بی سیم هستند. استراتژی **Ad hoc** برای شبکه های کوچک با تعداد ایستگاه کاری محدود قابل استفاده است. روش و استراتژی دوم

جهت پیاده سازی استاندارد شبکه بی سیم ، شبکه **Infra Structure** می باشد. در این روش یک یا چند دستگاه متمرکز کننده به نام **Access Point** مسؤولیت برقراری ارتباط را برعهده دارد.

10-2- شبکه های بی سیم **Outdoor** :

برقراری ارتباط بی سیم در خارج ساختمان به شبکه بی سیم **Outdoor** شهرت دارد. در این روش داشتن دید مستقیم یا **Line Of Sight** ، ارتفاء دو نقطه و فاصله، معیارهایی برای انتخاب نوع **Access Point** و آنتن هستند.

10-3- انواع ارتباط :

شبکه بی سیم **Outdoor** با سه توپولوژی **Point To Point** ، **Point To Multipoint** و **Mesh** قابل پیاده سازی می باشد.

10-4- **Point To point** :

در این روش ارتباط دو نقطه مدنظر می باشد. در هر یک از قسمت ها آنتن و **AccessPoint** نصب شده و ارتباط این دو قسمت برقرار می شود.

10-5- **Point Point To Multi** :

در این روش یک نقطه به عنوان مرکز شبکه درنظر گرفته می شود و سایر نقاط به این نقطه در ارتباط هستند.

10-6- **Mesh** :

تهیه کننده :سید حمید یاریان

ارتباط بی سیم چندین نقطه بصورت های مختلف را توپولوژی Mesh می گویند. در این روش ممکن است چندین نقطه مرکزی وجود داشته باشد که با یکدیگر در ارتباط هستند. ارتباط بی سیم بین دو نقطه به عوامل زیر بستگی دارد :

۱) توان خروجی Access Point (ارسال اطلاعات)

2)میزان حساسیت Access Point(دریافت اطلاعات)

3) توان آنتن

10-6-1- توان خروجی Access Point :

یکی از مشخصه های طراحی سیستم های ارتباطی بی سیم توان خروجی Access Point می باشد. هرچقدر این توان بیشتر باشد قدرت سیگنال های توایدی و برد آن افزایش می یابد.

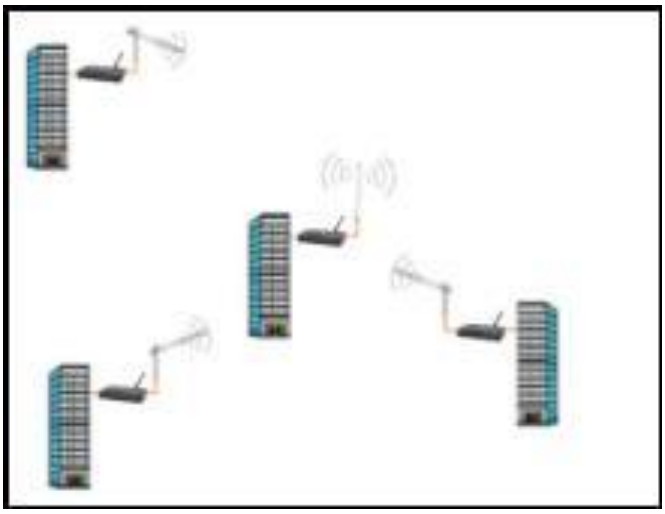
10-6-2- میزان حساسیت Access Point :

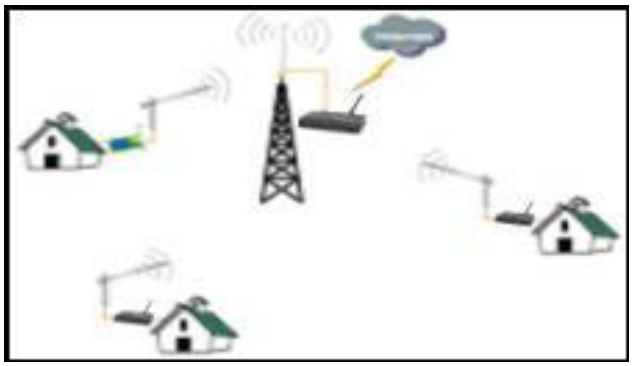
از مشخصه های تعیین کننده در کیفیت دریافت امواج تولید شده توسط Access Point نقطه مقابل میزان حساسیت Access Point می باشد. هرچقدر این حساسیت افزایش یابد احتمال عدم دریافت سیگنال کمتر می باشد و آن تضمین کننده ارتباط مطمئن و مؤثر خواهد بود.

10-6-3- توان آنتن :

در مورد هر آنتن توان خروجی آنتن و زاویه پوشش یا انتشار مشخصه های حائز اهمیت می باشند در این راستا آنتن های مختلفی با مشخصه های مختلف توان و زاویه انتشار بوجود آمده است که آنتن های Omni، Sectoral، Parabolic، Panel، Solied و . . . . مثال هایی از آن هستند.

تهیه کننده :سید حمید یاریان





11-ابزارهای جانبی در شبکه هایWireless

هر شبکه رایانه ای، به نسبت گستردگی خود از ابزار های مختلفی برای حفظ کیفیت داده ها در مسیر انتقال استفاده می کند . در شبکه های بدون سیم نیز، ابزارهای گوناگونی این فعالیت را بر عهده گرفته اند.

تهیه کننده :سید حمید یاریان

11-1- Repeater : یا تکرار کننده که یک نوع تقویت کننده سیگنال ضعیف شده است . از این وسیله برای تقویت سیگنال ارسال، جهت ارسال به فواصل دور مورداستفاده قرار می گیرد . تکرار کننده ها معمولا در لایه فیزیکی OSI قرار می گیرند و سیگنال ضعیف شده را از یک قسمت شبکه دریافت و پس از تقویت، آن را ازقسمت دیگر ارسال می کنند.

11-2- Hub : مسئولیت ارسال سیگنال ها را به قسمت های دیگر شبکه بر عه ده دارد هاب ها در دو نوع فعال و غیر فعال مورد استفاده قرار می گیرند. هاب غیر فعال فقط به عنوان اتصال دهنده مورد استفاده قرار می گیرد و هیچ گونه عملیات تولید مجدد سیگنال را بر عهده ندارد . در این صورت، هنگامی که سیگنالی ارسال می شود، تمام کامپیوترهای دیگر آن را دریافت خواهند کرد. نوع فعال، همانند هاب غیر فعال عمل می کند، با این تفاوت که در هاب های فعال، سیگنال تولید شده تقویت می شود و سپس ارسال می گردد . اما یک اشکال در هاب های فعال وجود دارد که به مجرد تقویت سیگنال، ارسال سیگنال نویز نیز تقویت شده و به شبکه انتقال می یابد.

11-3- Switch ها : که وظیفه اتصال قسمت های مختلف شبکه را به یکدیگر بر عهده دارند.

11-5- پل ها : که تمام خواص یک تکرار کننده را در خود دارد و می تواند بخش های خاصی از شبکه را که از روش های دسترسی متفاوتی استفاده می کنند را به هم وصل کند.

11-6- مسیریاب ها : که وظیفه انتخاب بهترین مسیر را برای ارسال بسته های داده ای در شبکه بر عهده دارد.

تهیه کننده :سید حمید یاریان

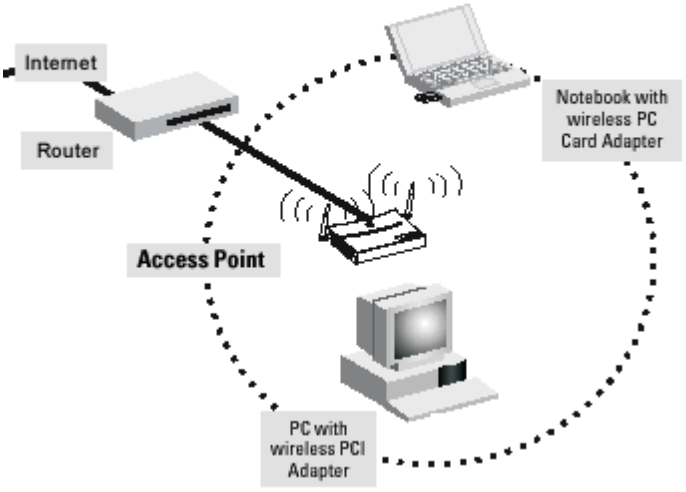
11-7- دروازه : که عهده دار اتصال شبکه هایی است که از نظر معماری کاملا متفاوت هستند .

معمولا دروازه ها روی کامپیوترهای سرور اختصاصی نصب می شوند.

12- راه اندازی شبکه های بی سیم Wireless Network

شما می توانید برای به اشتراک گذاشتن اتصال اینترنت، فایل ها، چاپگرها و امثال هم از یک شبکه ی بی سیم استفاده کنید .

اگر بخواهیدتمام اعضای خانواده تان از یک اتصال اینترنت، و یا از تنها چاپگری که در منزل دارید، و یا از فایل هایی که روی کامپیوتر شخصی خود دارید، مشترکاً استفاده کنند، می توانید یک شبکه ی بی سیم احداث کنید. به این ترتیب می توانید حتا هنگامی که پای حوض منزل تان نشسته اید، به سیر و سیاحت در اینترنت مشغول شوید. به علاوه نصب چنین شبکه ای از آن چه که فکر می کنید، خیلی ساده تر است .



تهیه کننده :سید حمید یاریان

برای عُلَم کردن هر شبکه ی بی سیم، چهار مرحله وجود دارد:

0) تجهیزات بی سیم خود را انتخاب کنید.

1) ۲) مسیریابِ بی سیم خود را متصل کنید.

2) ۳) مسیریاب بی سیم خود را پیکربندی کنید.

3) ۴) کامپیوترهای تان را به هم متصل کنید.

هر چند سرویس پک۲ی ویندوز ایکس پی برای احداث این شبکه ی بی سیم ضرورت ندارد، اما باعثِ سهولت کار می شود. در عین حال، سرویس پک۲ ازشما در برابر هکرها، کرم ها، و سایر تهدیدات اینترنتی نیز محافظت می کند. پس چه بهتر که قبل از بالازدنِ آستین تان، سرویس پک۲ را نصب کنید.(در مورد نصب سرویس پک۲ی ویندوز ایکس پی می توانید به شماره ی ۹۱ مجله ی کامپیوتر مراجعه کنید. و یا سی دی ویندوز ایکس پی را که سرویس پک۲ نیز با آن عجین شده است، تهیه کنید!)

0) اولین قدم آن است که مطمئن شوید تجهیزات مورد لزوم را در اختیار دارید. در حینِ دیدزدن مغازه ها، ممکن است متوجه شوید که تجهیزات بی سیم از سه استاندارد مختلف تبعیت می کنند: یعنی استانداردهای 802.11a ، 802.11b ، و 802.11g توصیه ی ما به شما این است که طرفِ استاندارد 802.11g را بگیرید، چرا که اولاً یک سرو گردن از دوتای دیگر بالاتر است و ثانیاً با هر دستگاه دیگری تقریباً سازگار است.

1) به این ترتیب، فهرست خریدتان باید شامل این سه قلم باشد:

2) الف) اتصال اینترنت پهن باند

3) ب) مسیریاب بی سیم

تهیه کننده :سید حمید یاریان

4) ج) یک کارت شبکه ی بی سیم (یا کامپیوتری که شبکه ی بی سیمِ سَرخود داشته باشد)

5) ▪ مسیریاب بی سیم

6) وظیفه ی مسیریاب بی سیم آن است که سیگنال های وارده از اتصال اینترنت تان را به یک سیگنال پهن باندِ بی سیم تبدیل کند، درست شبیه ایستگاه اصلی یک تلفن بی سیم .

7) حتماً باید حواس خود را جمع کنید که یک مسیریابِ بی سیم بخرید، نه یک نقطه گاه بی سیم.

8) ▪ کارت شبکه ی بی سیم

9) کارت های شبکه ی بی سیم، کامپیوتر شما را به مسیریابِ بی سیم تان متصل می کنند. اگر یکی از این کامپیوترهای کتابی جدید داشته باشید، به احتمال زیاد امکانات بی سیم از قبل روی آن سوار کرده اند. بنابراین دیگر لزومی ندارد که کارت شبکه ی بی سیم تهیه کنید. اما اگر لازم دارید که برای یک کامپیوتر رومیزی، یک کارت شبکه ی بی سیم خریداری کنید، یک کارت شبکه ی بی سیم مبتنی بر یو اس بی بخرید. اگر کامپیونر کتابی دارید، یک کارت شبکه ی مبتنی بر کارت های معمول کامپیوتری خریداری نمایید.

10)در هرحال، به ازای هر کامپیوتر موجود در شبکه تان، باید یک کارت شبکه نیز داشته باشید.

11) توجه! توجه! برای آن که جفت وجور کردنِ شبکه تان به سادگی انجام شود، کارت شبکه ای بخرید که سازنده اش همان سازنده ی مسیریابِ بی سیم تان باشد. برای مثال، اگر دیدید قیمت مسیریاب فلان شرکت، مناسب است، کارت شبکه را نیز از همان شرکت بخریدتا مطمئن باشید که زبان هم را می فهمند!

تهیه کننده :سید حمید یاریان

برای آن که خرید کردن تان از این هم راحت تر شود، می توانید یک کیتِ کامل- که شامل کلیه ی اقلام مورد نیاز برای نصب یک شبکه ی بی سیم خانگی هستند- بخرید. اگر یک کامپیوتر رومیزی دارید، مطمئن شوید که یکی از درگاه های یو اس بی آن خالی است تا بتوانید کارت شبکه ی بی سیم را در آن فرو کنید. اما اگر درگاه های آزاد یو اس بی در کامپیوترتان پیدا نمی شود، باید یک هاب بخرید تا درگاه های اضافی در اختیارتان بگذارد.

مسیریابِ بی سیم خود را متصل کنید.

اول از همه، مودم کابلی یا دیجیتالی خود را پیدا کرده و آن را بیرون بکشید تا خاموش شود. سپس، مسیریابِ بی سیم خودرا به مودم تان متصل نمایید. مودم شما باید مستقیماً به اینترنت وصل باشد. بعداً، وقتی همه را به هم وصل کردید، کامپیوترتان بدون سیم به مسیریاب تان متصل خواهد شد، و مسیریاب نیز به نوبه ی خود، سیگنال ها را از طریق مودم تان به اینترنت ارسال خواهد کرد.

و اکنون، مسیریاب تان را به مودم وصل کنید.

ـ اگر در حال حاضر کامپیوترتان مستقیماً به مودم وصل است، کابل شبکه را از پشتِ کامپیوتر بیرون آورده و آن را به درگاهی در پشت مسیریاب که برچسب Internet، WAN، و یا LAN خورده است، فروکنید.

ـ اگر در حال حاضر کامپیوتری ندارید که به اینترنت متصل باشد، یکی از دو سر کابل شبکه را (که جزو ضمایمِ مسیریاب تان بوده است)

به مودم خود وصل کرده، و سر دیگر ان را به درگاهی در پشت مسیریاب بی سیم تان که برچسبِ Internet، WAN ، و یا LAN، خورده است، فروکنید.

تهیه کننده :سید حمید یاریان

ـ اگر در حال حاضر، کامپیوترتان را به یک مسیریاب وصل کرده اید، کابل شبکه ای را که در یکی از درگاه های واقع در پشت مسیریابِ فعلی تان فرورفته است، بیرون کشیده، و این سرِ کابل را به درگاهی در پشت مسیریاب بی سیم تان که برچسب LAN،WAN،Internet خورده است، فروکنید. سپس، هر کابل شبکه ی دیگری که می بینید، بیرون آورده و آن ها را به درگاه های موجود در پشت مسیریابِ بی سیم تان فرو نمایید. شما دیگر به مسیریاب فعلی تان احتیاج ندارید، زیرا مسیریاب بی سیم جدیدتان، جای آن را گرفته است. نگرانِ دل آزار شدنِ کهنه ها هم نباشید!

سپس، مودم کابلی یا دیجیتالی خود را وصل کرده و آن را روشن کنید. چند لحظه به آن فرصت بدهید تا به اینترنت متصل شود، و پس از آن، مسیریابِ بی سیم تان را وصل نموده وروشن کنید. بعد از یک دقیقه، چراغ Internet، WAN، LAN روی مسیریاب بی سیم تان باید روشن شود، به این معنی که با موفقیت به مودم تان وصل شده است.

▪ مسیریاب بی سیم تان را پیکربندی کنید

با استفاده از کابل شبکه ای که جزو ضمایم مسیریابِ بی سیم تان بوده است، می بایست گاه به گاه کامپیوترتان را به یکی از درگاه های آزاد شبکه در پشتِ مسیریاب بی سیم تان متصل کنید (هر درگاهی که برچسب WAN،Internet ،و یا LAN نداشته باشد). اگر لازم است، کامپیوترتان را روشن کنید. در این حالت، کامپیوتر شما باید به طور خودکار به مسیریاب تان وصل شود.

سپس، مرورگر اینترنت تان را بازکرده و آدرس مربوط به پیکربندی مسیریاب را وارد کنید.

در این جا ممکن است از شما یک اسم رمز خواسته شود. آدرس و اسم رمزی که به کار خواهید برد، بسته به نوع مسیریاب شما فرق خواهد کرد، بنابراین باید به دستورالعمل های داده شده در دفتر چه ی مسیریاب تان رجوع کنید.

تهیه کننده :سید حمید یاریان

برای آن که بهتر متوجه منظورمان شوید، آدرس ها، شناسه ی کاربری و اسم رمز چند مسیریابِ موجود در بازار را در زیر می بینید:

ـ اسم رمز

ـ شناسه ی کاربری

ـ آدرس

ـ مسیریاب

admin ـ

Admin ـ

http:// ۱۹۲,۱۶۸,۱,۱ـ

Com۳ ـ

Admin ـ

Admin ـ

ttp:// ۱۹۲,۱۶۸,۰,۱ـ

D-Link ـ

admin ـ

Admin ـ

ttp:// ۱۹۲,۱۶۸,۱,۱ـ

Linksys ـ

تهیه کننده :سید حمید یاریان

password ـ

admin ـ

http://۱۹۲,۱۶۸,۱,0ـ

NetGear ـ

به این ترتیب، مرورگر اینترنت، صفحه ی پیکربندی مسیریاب تان را به نمایش در خواهدآورد. بیشتر تنظیمات کارخانه ای به راحتی جواب می دهند، منتها سه چیز را خودتان باید تنظیم کنید:

۱) اسم شبکه ی بی سیم تان، موسوم به SSTD. این اسم، معرّف شبکه ی شماست. شما می بایست یک اسم خاص منحصربه فرد که کسی از همسایگان تان به کارنبرده باشد، انتخابکنید.

۲) تعیین کردن یک گذرنامه برای محافظت از شبکه ی بی سیم تان. در مورد بیشتر مسیریاب ها، می بایست یک جمله ی قصار تعیین کنید تا مسیریاب تان برای تولید کلیدهای متعدد از آن استفاده کند. یادتان نرود که جمله ی قصارتان باید حتماً منحصر به فرد و دراز باشد. (احتیاجی نیست آن را از بَر کنید).

۳) تعیین یک اسم رمز سرپرستی، تا کل شبکه ی بی سیم تان را زیر نظر بگیرید. درست مثل هر اسم رمزی، این اسم رمز نیز نباید کلمه ای باشد که هرکس بتواند در فرهنگ لغات پیدایش کند. یک اسم رمزِ مطمئن، ترکیبی از حروف، اعداد و علایم است. باید مطمئن شوید که می توانید این اسم رمز را به خاطر بیاورید، زیرا درصورتی که مجبور باشید یکی از تنظیمات مسیریاب تان را تغییر دهید، به آن احتیاج پیدا می کنید.

تهیه کننده :سید حمید یاریان

مراحل دقیقی که باید برای پیکر بندی این تنظیمات طی کنید، بسته به نوع مسیریاب تان فرق می کنند. بعد از تنظیم هر پیکر بندی، باید حتماً Save Settings، Apply،و OK را برای ضبط کردن تنظیمات تان کلیک کنید. اکنون، می بایست کابل شبکه را از کامپیوترتان قطع کنید.

- **کامپیوتر های خود را وصل کنید**

اگر کامپیوتر تان، شبکه ی بی سیمِ سَرخود ندارد، کارت شبکه تان را در درگاه یو اس بی فرو کنید، و آنتن را در بالای سر کامپیوترتان قرار دهید (درصورتی که کامپیوتر رومیزی داشته باشید)، و یا کارت شبکه را در یکی از چاک های خالی پی سی کارت فرو کنید (درصورتی که کامپیوتر کتابی داشته باشید). خودِ ویندوز ایکس پی، کارتِ جدید را تشخیص داده، و ممکن است از شما بخواهد که سی دی مربوط به کارت شبکه را در اختیارش بگذارید.

دستورالعمل های داده شده از طریق نمایشگر، شما را درطولِ مرحله ی پیکربندی راهنمایی خواهند کرد.

توجه! توجه! مراتبِ زیر درصورتی صدق می کنند که سرویس پک۲ی ویندوز ایکس پی داشته باشید. اگر ویندوز ایکس پی شما هنوز سرویس پک۲ را زیارت نکرده است، باید در اسرع وقت آن را تهیه نموده و نصب کنید.

اینک، ویندوز ایکس پی باید شکلکی را در سینی سیستم به نمایش بگذارد مبنی بر این که یک شبکه ی بی سیم پیدا کرده است.

این مراحل را دنبال کنید تا کامپیوترتان به شبکه ی بی سیم مذکور وصل شود.

۱) در سینی سیستم- منطقه ی واقع در گوشه ی سمت راست پایین نمایشگر- روی شکلکِ شبکه ی بی سیم کلیک راست بزنید، وسپس از منوی متعاقبِ آن، گزینه ی

View Available Wireless Networks را انتخاب کنید. درصورت برخورد با هر مشکلی، به دفتر چه ی راهنمای کارت شبکه ی خود رجوع کنید. از این که به فروشنده تان زنگ بزنید و از آن ها سؤال کنید، هیچ وقت تردید به خود راه ندهید.

۲) به این ترتیب، پنجره ی «اتصال شبکه ی بی سیم» باید باز شود و شبکه ی بی سیم خود را با همان اسمی که قبلاً انتخاب کرده بودید- در بین شبکه های موجود ببینید. اما اگر به هر دلیلی موفق به دیدنِ شبکه ی خود نشدید، در صدر ستون سمت چپ، روی List Refresh Network کلیک کنید. اکنون روی شبکه تان کلیک کرده، و سپس در سینی سیستم (گوشه ی تحتانی راست)، روی Connect کلیک کنید.

۳) در این وقت ویندوز ایکس پی از شما می خواهد که کلید زیر را وارد کنید. کلید رمزگذار همان کلیدی ست که پیش از این در هردو حوزه ی Network Key و Confirm Network Key وارد کرده بودید. پس از آن روی Connect کلیک کنید.

۴) ویندوز ایکس پی مراحل پیشرفت کارش را در حین اتصال به شبکه ی شما نشان می دهد. بعد از متصل شدن تان، می توانید پنجره ی اتصال شبکه ی بی سیم را ببینید. کارتان در این لحظه به اتمام رسید! مبارک است!

توجه! توجه! اگر پنجره ی اتصال شبکه ی بی سیم هم چنان در حال زورزدن برای پیدا کردنِ آدرس شبکه باشد، ممکن است در واردکردنِ شاه کلیدِ رمزگذاری اشتباه کرده باشید .

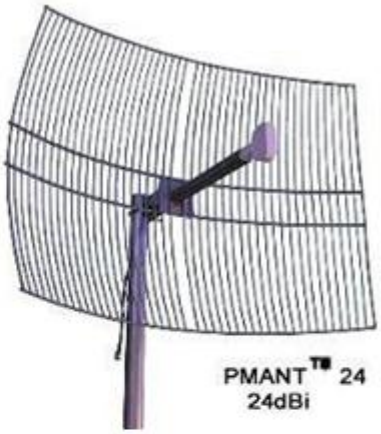
- **قوانین ومحدودیت ها :**

به منظور در دسترس قرار گرفتن امکانات شبکه های بی سیم برای عموم مردم و همچنین عدم تداخل امواج شرایط محدود کننده ای برای افراد توسط کمیته FCC تعیین شد که مهمترین آن ها این تهیه کننده :سید حمید یاریان

است که تجهیزات شبکه های بی سیم در باند فرکانسی ۲,۴ Ghz مجاز به داشتن حداکثر ۱۰mw توان خروجی با زاویه پوشش آنتن ۹ درجه هستند که توان خروجی برای باند فرکانسی ۵,۸ Ghz تا ۲۰۰ mw مجاز اعلام شده است

13- طریقه ارتباط Wireless جهت ارتباط بین Isp و User

در این طریقه می بایست تجهیزاتی در سمت Isp و User نصب گردد این تجهیزات معمولا به شرح زیر است:



آنتن

رادیو وایرلس

کابل های ارتباطی

تهیه کننده :سید حمید یاریان

13-1- رادیو : داده های خام(صفر و یک) را به سیگنال های رادیویی تبدیل می کند و از طریق کابلی که معمولا از نوع Coaxial (کابل هم محور) می باشد، داده ها را به سمت آنتن هدایت می کند.

آنتن: ها بایستی حتما در دو طرف کاملا رو به یکدیگر باشند و به هیچ وجه نباید مانعی در جلوی این دو قرار داشته باشد . رادیو دارای یک پورت خروجی به آنتن و یک پورت دیگر برای ارتباط با کامپیوتر یا تجهیزات شبکه می باشد.

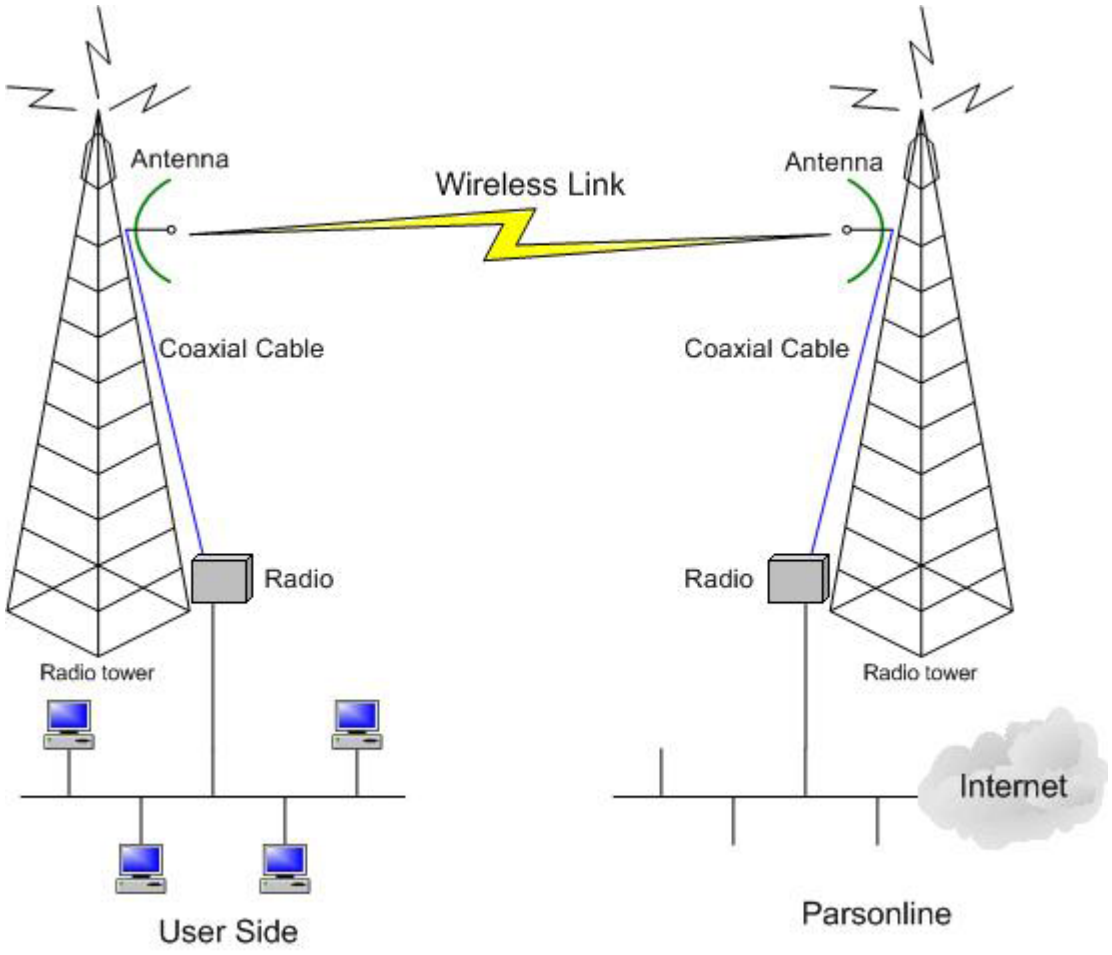
در ارتباط Wireless عواملی در کیفیت و پهنای باند تاثیر می گذارند که عبارتند از:

۱) دید دو منطقه نسبت به هم و نبودن مانع بین دو آنتن در طول مسیر.

۲) امواج مزاحم که از خطوط Wireless نزدیک یا ایستگاه ها ایجاد می شود.

۳) توانایی رادیوها و آنتن ها و قدرت ارسال و دریافت امواج

تهیه کننده :سید حمید یاریان



14- فواید تکنولوژی Wireless

تکنولو ژی Wireless به کابر امکان استفاده از دستگاه های متفا وت ، بدون نیاز به سیم یا کابل در حال حرکت را می دهد . شما می توانید صندوق پست الکترونیکی خود را بررس ی کنید، بازار بورس را زیر نظر بگیرید، اجناس مورد نیاز را خریدا ری کنید و یا حتی برنامه تلویزیون مورد علاقه خود را تماشا کنید . تجهیزات Wireless به شما کمک می کند تا تمام اطلاعات را به راحتی برای مشتری

تهیه کننده :سید حمید یاریان

خود به نمایش در بیاورید . از طرفی می تو انید تمامی کارهای خود را در حال حرکت به سادگی به روز رسانی کنید و آن را به اطلاع همکاران خود برسانید.

تکنولو ژی Wireless در حال گسترش است تا بتواند ضمن کاهش هزینه ها، به شما امکان کار در هنگام حرکت را نیز بدهد . در مقایسه با شبکه ه ای سیمی،هزینه نگهدا ری شبکه های Wireless کمتر می باشد .شما می توانید از شبکه هایWireless

برای انتقال اطلاعات از ر وی دریاها، کوهها و ... استفاده کنید و این در حال ی است که بر ای انجام کار مشابه توسط شبکه ه ای سیمی، کاری مشکل در پیش خواهید داشت.

در شبکه سازی بدون سیم، هزینه ای صرف کابل کشی هم محور یا بهم تابیده شده و نیز فیبر نوری نمی شود؛ بلکه تنها از فرکانس رادیویی یا RF استفاده می شود . نکته دیگر این که شبکه های بی سیم، انعطاف پذیری بیشتری نسبت به شبکه های کابلی دارند و نیز وقت کمتری صرف احداث آن شده و نگهداری آن بسیارآسان و با صرفه است . اما مزیت اصلی شبکه های بی سیم قابلیت تحرک کاربران است.

15- مشکلات استفاده از Wireless

اگر شبکه های Wireless بدون مشکل بود ند، حتما تا به حال جانشین شبکه های کابلی شده و آنها را از دور رقابت خارج می کردند؛ ولی مانند هر پدیده دیگری در برابر مزایایی که دارند، مشکلاتی نیز دارند.

۱) مهم ترین مشکل استفاده از سیستم هایWireless ی، سرعت انتقال داده ها درشبکه است . در متداول ترین شبکه های کابلی، نرخ ارسال اطلاعات Mbps ۱۰۰ است و البته شبکه هایی با سرعت نیز

در بازار وجود دارند، ولی به علت قیمت زیاد تجهیزات این شبکه ها، از آنها فقط در موارد خاصی استفاده می شود.

اما جدیدترین شبکه های Wireless دارای سرعتMbps ۱۰۸ است .اندازه این سرعت تابع شرایط مختلفی از جمله : امواج رادیویی مزاحم، وجود نقاط کور در شبکه محیط، توان فرستنده های Wireless، تعداد کاربران شبکه و عدم استفاده از Protocol های امنیتی در شبکه است .

۲) مساله دیگر، امنیت در شبکه های Wireless است . این شبکه ها خیلی آسان تر از شبکه های کابلی می توانند مورد دستبرد قرار بگیرند . استاندارد های جدید، روش های کد گذاری جدیدی معرفی می کنند تا امنیت این شبکه ها را بالا ببرند، اما روش های کدگذاری سرعت انتقال اطلاعات را کاهش می دهد.

۳) در شبکه های Wireless برای انتقال اطلاعات از امواج رادیویی استفاده می شود. بنابراین، این شبکه ها تمام مشکلات مربوط به استفاده از امواج رادیویی را نیزخواهند داشت.

چند نمونه از این مشکلات را در زیر مشاهده می کنید:

16-1- تاثیر وضعیت جغرافیایی و آب و هوا بر شبکه های Wireless

شبکه های Wireless به شدت تحت تاثیر متغیرهای خارجی و داخلی قرار می گیرندکه از آن جمله می توان به پدیده های آب و هوایی مانند : باد، باران، برف، مه،دما و فشار که همگی ناشی از موقعیت جغرافیایی منطقه موردنظر می باشداشاره کرد.

لازم به ذکر است که امواج حامل در شبکه های Wireless از نوع الکترومغناطیس(EM) می باشند .

تهیه کننده :سید حمید یاریان

16-2- شکست امواج الکترومغناطیسی در اتمسفر

امواج Wireless در لایه تروپوسفر که از سطح زمین شروع شده و بسته به موقعیت زمین و شرایط جوی به ارتفاع ۱۰ تا ۱۷ کیلومتر هم می رسد، انتشار می یابند.

***لایه تروپوسفر شامل مجموعه ای از گازها و همچنین بخار آب می باشد**

***با افزایش ارتفاع به ازای هر ۳۰۰ متر دما ۲ درجه کاهش می یابد.**

***سرعت فاز جبهه موج در ارتفاعات بالاتر کمی بیشتر خواهد بود که باعث ایجاد انحنا در اموج EM می شو د .**

***مسیر انتشار جبهه موج با عبور از اتمسفر انحنا پیدا می کند که به این خم شدگی ((پدیده شکست)) می گویند.**

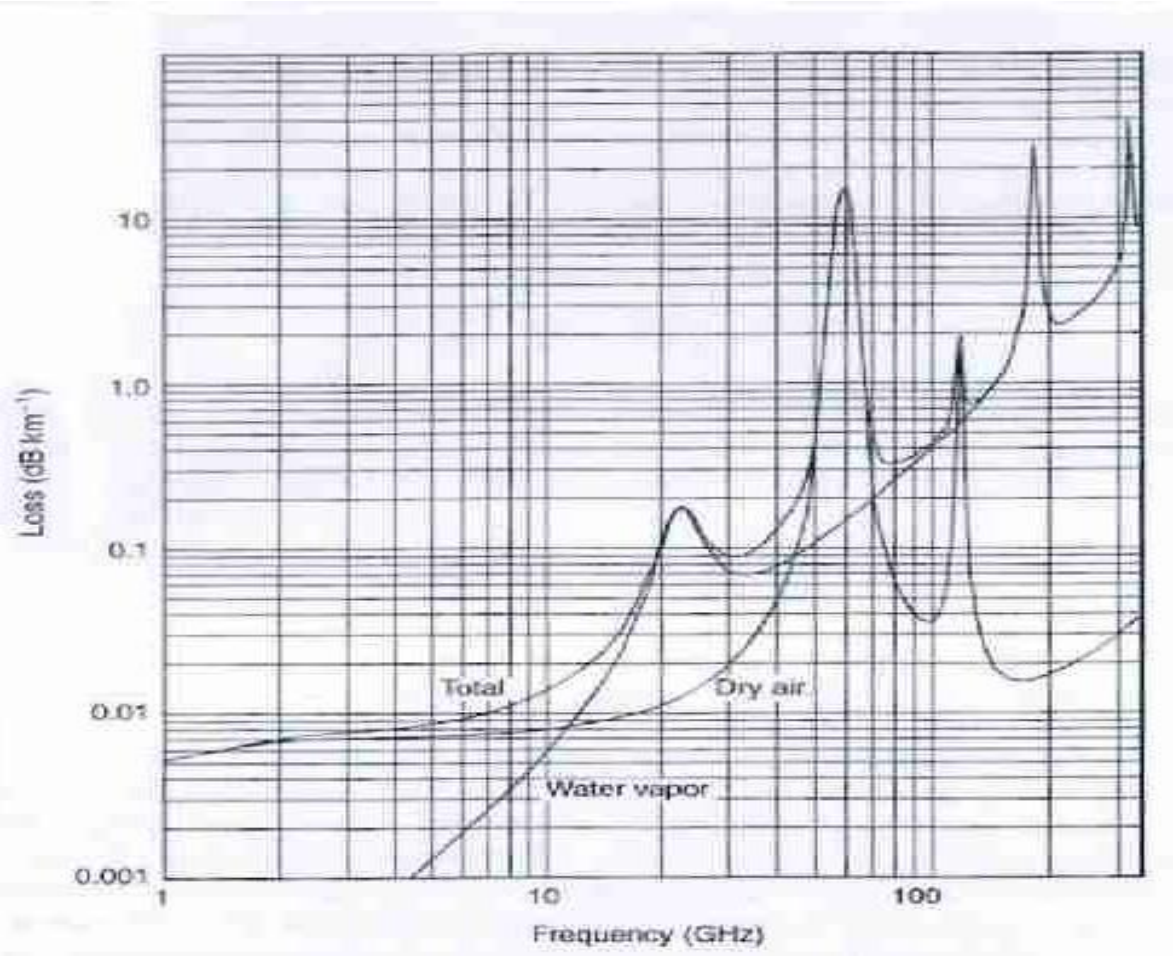
این ضریب شکست به عوامل زیر بستگی دار د:

۱) فشار کلی اتمسفر

۲) فشار بخار آب

۳) دمای هوا

تهیه کننده :سید حمید یاریان



16-3- تاثیر باران بر انتشار امواج EM در شبکه های Wireless

باران از ۳ طریق بر امواج EM تاثیر می گذار د:

۱) قطرات باران با شعاعی کمتر از طول موج تابشی، انرژی موج را با استفاده از تاثیر گرمازایی جذب می کنند و باعث کاهش انرژی موج می شوند که به شدت وابسته به فرکانس موج تابشی می باشد.

۲) قطرات بزرگ تر باران که تقریبا اندازه طول موج تابشی هستند، باعث پراکندگی طول موج می شوند و این امر باعث کاهش دامنه موج می شو د. میزان پراکندگی به عوامل زیر بستگی دار د:

الف) میزان توزیع قطرات باران

ب) جهت گیری قطرات باران

ج) شدت قطرات باران

تهیه کننده :سید حمید یاریان

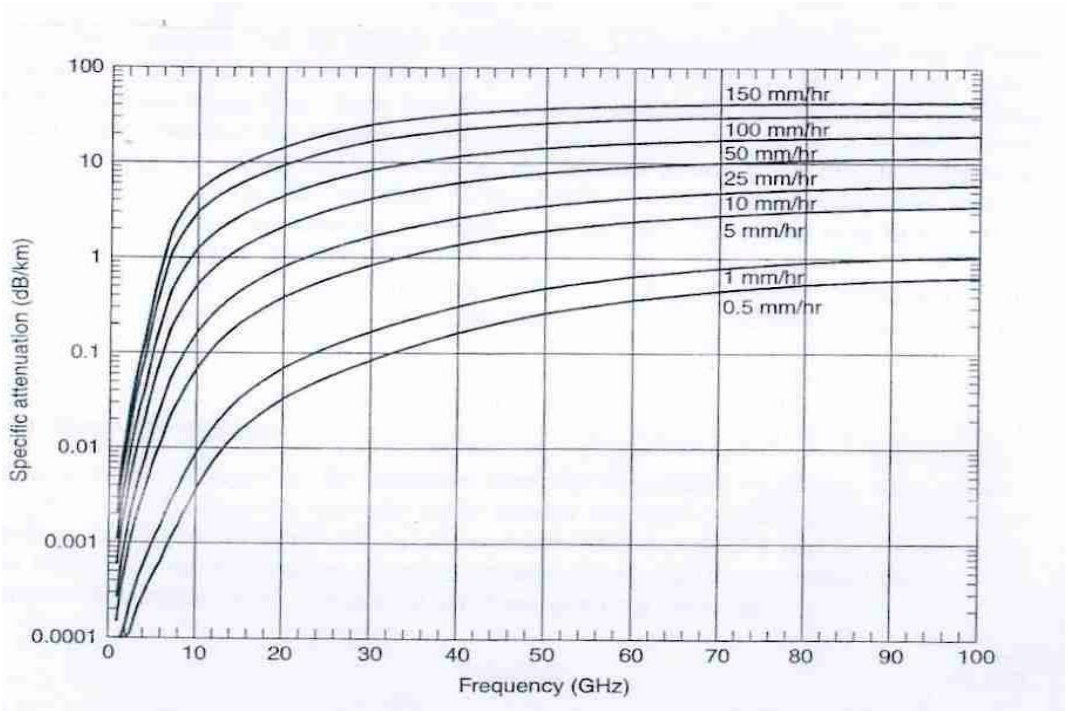
۳ (قطرات باران باعث می شوند قطبیت موج تابشی به دلیل پراکندگی از بین برود و موج تابشی تضعیف گردد که به عوامل زیر بستگی دارد:

الف) میزان توزیع قطرات باران

ب) جهت گیری قطرات باران

ج) شدت قطرات باران

د) میزان مسیری که موج در معرض باران قرار دارد



16-4- تاثیر باد بر شبکه های Wireless

وزش باد با فشار وارد بر روی آنتن ها و ایجاد لرزش و انحراف در آنها از کارایی شبکه های Wirelessمی کاهد.دو عامل زیر باعث کاهش میزان پوشش آنتن و در نتیجه افت شدید سیگنال دریافت میشو د:

۱) تغییر جهت آنتن

تهیه کننده :سید حمید یاریان

۲) لرزش آنتن

اتلاف در فضای آزاد

در حالت کلی می توان گفت میران اتلاف انرژی موج در اثر انتشار در فضای آزاد به عوامل زیر بستگی دار د:

۱) فاصله

۲) فرکانس موج

که از طریق رابطه زیر قابل محاسبه می باشد :

$$L = C+20 * Log (D) +20 * Log (F)$$

L = Loss	**F = Frequency**
C = Constant = 36.6	**D = Distance**

17–ارتباطات رادیویی

خانواده ارتباطات رادیویی بسیار گسترده است . شیوه های مختلفی نیز در در شبکه سازی بی سیم مورد استفاده قرار می گیرد که در ذیل به آنها اشاره می کنیم:

1) RF (Radio Frequency): که به فرکانس امواج رادیویی مشهور است . در این روش، شبکه بین محدود ۱۰ کیلوهرتز تا چند گیگا بایت قرار می گیرد . آنتن هایی که این امواج را انتقال می دهند ممکن است به

صورت تمام جهتی و یا با جهتی خاص استفاده شود . شعاع انتشار این امواج بسیار زیاد است که البته برای نقاط دورتر، امواج تقویت می شود . دیتا در این روش با سرعت ۱ تا ۱۱ مگابایت در ثانیه انتقال می یابد، ارتباطات در این محدوده نیازی به مجوز ندارد و تجهیزات ارتباطی نیز به صورت گسترده فراهم می باشد.

2) **Microwave** : مایکروویو شیوه دیگری از شبکه های بی سیم می باشد . امواج مایکروویو تنها از یک جهت منتشر می شوند، سرعت انتقال متغیر بوده و از یک تا دو مگابایت بر ثانیه می باشد . مایکروویو شدیدا تحت تاثیر اتمسفر و نوسانات جوی نظیر رعد و برق قرار دارد . این سیستم ها در دو نوع ماهواره ای و زمینی موجود بوده و از آنتن های بشقابی دو طرفه برای رله (تقویت) امواج در نوع زمینی استفاده می شود . برای استفاده از تجهیزات مایکروویو نیاز به اخذ مجوز است.

3) **IR** : یا مادون قرمز نوع دیگری از امواج رادیویی است . این امواج از طریق دیودهای نور گسیل **LED** یا لیزری **ILD** تولید می شوند . فرکانس امواج مادون قرمز بالاست، لذا سرعت انتقال دیتا از ۱ تا ۱۶ مگابایت در ثانیه می باشد.

17-1-مشکلات مربوط به استفاده از امواج رادیویی

۱) وجود نویز (Noise)در محیط : منظور از نویز در محیط، هر موج راد یویی می باشد که با امواج رادیویی موردنظر ما همراه است و پیدا کردن موج موردنظر ما را دشوار می سازد.

۲) تداخل امواج رادیویی : از آنجایی که برخی از تجهیزات الکترونیکی از امواج رادیویی استفاده می کنند، تداخل این امواج می تواند عملکرد این تجهیزات را مختل کند . متاسفانه فرکانس تلفن های بی سیم و اجاق های مایکروویو با فرکانس مورد استفاده بعضی از تجهیزات شبکه های **Wireless** یکسان است و این تلفن ها و اجاق ها می توانند تداخل امواج رادیویی ایجاد کنند که اولین نتیجه آن،کاهش سرعت انتقال اطلاعات است. ۳) تضعیف امواج رادیویی : اشکال دیگر امواج رادیویی، تضعیف آن

هاست که به هنگام انتقال آن ها در فضا رخ می دهد . تضعیف امواج رادیویی با شرایط جوی بیشتر می شود.

۴) انعکاس امواج رادیویی : مساله دیگر در انتشار امواج رادیویی، انعکاس این امواج در برخورد با اشیا است . وقتی موج رادیویی به یک شی برخورد می کند، گیرنده رادیویی موج اصلی را به همراه موج منعکس شده با هم دریافت می کند. اگر موج به اشیای زیادی برخورد کند، انرژی خود را از دست می دهد و به شدت تضعیف می شود.

18- انواع روش های امنیتی در شبکه های بی سیم

سه روش امنیتی در شبکه های بی سیم عبارتند از:

18-1- WEP(Wired Equivalent Privacy)-

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می آید که مناسب برای شبکه های کوچک بوده زیرا نیاز به تنظیمات دستی (KEY)مربوطه در هر **Client** می باشد.اساس رمز نگاری **WEP** بر مبنای الگوریتم **RC4** بوسیله **RSA** می باشد.

18-2- SSID (Service Set Identifier) -

شبکه های **WLAN** دارای چندین شبکه محلی می باشند که هر کدام آنها دارای یک شناسه (Identifier)یکتا می باشند این شناسه ها در چندین **Access Point** قرار داده می شوند . هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه **SSID** مربوطه را انجام دهد.

18-3- MAC (Media Access Control) -

تهیه کننده :سید حمید یاریان

لیستی از MAC آدرس های مورد استفاده در یک شبکه به AP (Access Point) مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرسها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می کند MAC آدرس آن با لیست MAC آدرس مربوطه در AP مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می گیرد .این روش امنیتی مناسب برای شبکه های کوچک بوده زیرا در شبکه های بزرگ امکان ورود این آدرسها به AP بسیار مشکل می باشد.

19- امنیت در شبکه‌های بی‌سیم

19-1- بخش اول : مقدمه

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

19-1-1-منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان

عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد.

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

تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.

نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.

- **اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.**

حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.

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

با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.

تهیه کننده :سید حمید یاریان

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

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

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

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

19-1-2- ضعف‌های اولیه‌ی امنیتی WEP

در قسمت‌های قبل به سرویس‌های امنیتی استاندارد 802.11 پرداختیم. در ضمنِ ذکر هریک از سرویس‌ها، سعی کردیم به ضعف‌های هریک اشاره‌یی داشته باشیم. در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد 802.11 بر اساس پروتکل WEP استوار است.

WEP در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از WEP را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند.

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

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

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

19-1-2-1- استفاده از کلیدهای ثابت WEP

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

تهیه کننده :سید حمید یاریان

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

19-1-2-2- 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 آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

19-1-2-3- ضعف در الگوریتم

از آن‌جایی‌که IV در تمامی بسته‌های تکرار می‌شود و بر اساس آن کلید تولید می‌شود، نفوذگر می‌تواند با تحلیل و آنالیز تعداد نسبتاً زیادی از IVها و بسته‌های رمزشده بر اساس کلید تولید شده

بر مبنای آن IV، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن‌جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می‌گردد.

19-1-2-4- استفاده از CRC رمز نشده

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

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

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

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

19-2- بخش دوم : شبکه‌های محلی بی‌سیم

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

19-2-1- پیشینه

تکنولوژی و صنعت **WLAN** به اوایل دهه‌ی ۸۰ میلادی باز می‌گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه‌های محلی بی‌سیم به کندی صورت می‌پذیرفت. با ارایه‌ی استاندارد **IEEE 802.11b**، که پهنای باند نسبتاً بالایی را برای شبکه‌های محلی امکان‌پذیر می‌ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از **WLAN** تمامی پروتکل‌ها و استانداردهای خانواده‌ی **IEEE 802.11** است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می‌دهد

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

اولین شبکه‌ی محلی بی‌سیم تجاری توسط Motorola پیاده‌سازی شد. این شبکه، به عنوان یک نمونه از این شبکه‌ها، هزینه‌یی بالا و پهنای باندی پایین را تحمیل می‌کرد که ابداً مقرون به‌صرفه نبود. از همان زمان به بعد، در اوایل دهه‌ی ۹۰ میلادی، پروژه‌ی استاندارد 802.11 در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای 802.11a و 802.11b توسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه‌ی این استانداردها آغاز شد. نوع a، با استفاده از فرکانس حامل 5GHz، پهنای باندی تا 54Mbps را فراهم می‌کند. در حالی‌که نوع b با استفاده از فرکانس حامل 2.4GHz، تا 11Mbps پهنای باند را پشتیبانی می‌کند. با این وجود تعداد کانال‌های

تهیه کننده :سید حمید یاریان

قابل استفاده در نوع b در مقایسه با نوع a، بیش‌تر است. تعداد این کانال‌ها، با توجه به کشور مورد نظر، تفاوت می‌کند. در حالت معمول، مقصود از WLAN استاندارد 802.11b است.

استاندارد دیگری نیز به‌تازه‌گی توسط IEEE معرفی شده است که به 802.11g شناخته می‌شود. این استاندارد بر اساس فرکانس حامل 2.4GHz عمل می‌کند ولی با استفاده از روش‌های نوینی می‌تواند پهنای باند قابل استفاده را تا 54Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی‌شدن و معرفی آن نمی‌گذرد، با توجه سازگاری آن با استاندارد 802.11b، استفاده از آن در شبکه‌های بی‌سیم آرام آرام در حال گسترش است.

19-3- بخش سوم : عناصر فعال و سطح پوشش WLAN

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

19-3-1- ایستگاه بی سیم

ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.

تهیه کننده :سید حمید یاریان

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

19-3-2- نقطه ی دسترسی

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

19-3-3- برد و سطح پوشش

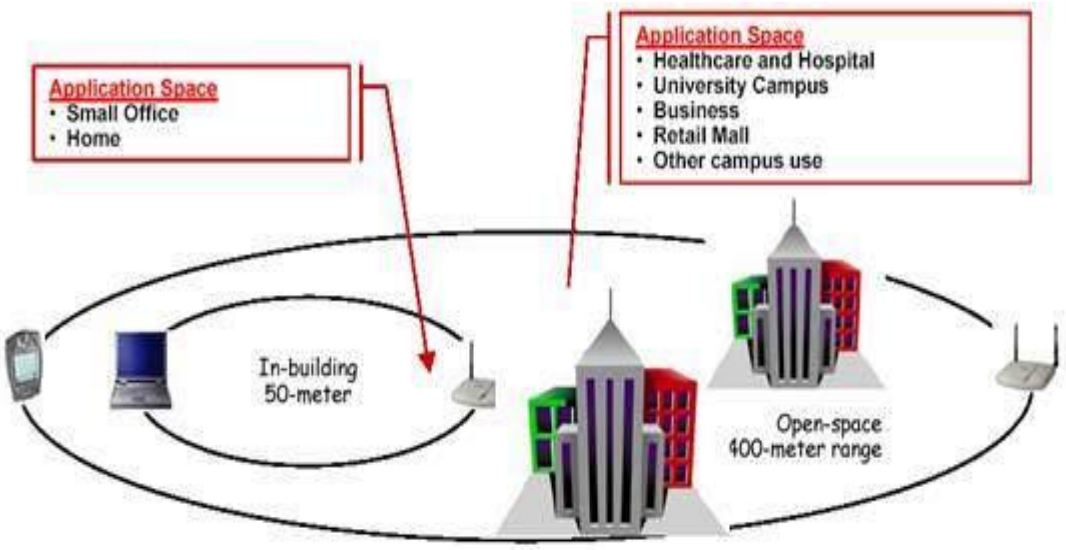
شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بستگی دارد که برخی از آن‌ها به شرح زیر هستند :

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

تهیه کننده :سید حمید یاریان

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

شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد :



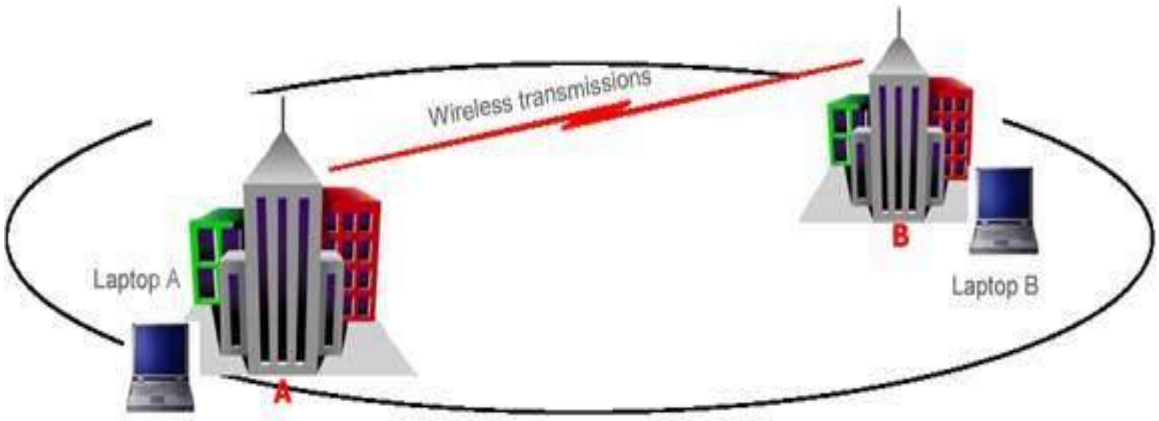
تهیه کننده :سید حمید یاریان

یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه **Bridge** برای شبکه‌های بی‌سیم را به‌دست آورد.

اتصال میان نقاط دست‌رسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.

نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل **802.11b** است. برای پروتکل‌های دیگری چون **802.11a** می‌توان فواصل بیشتری را نیز به‌دست آورد.

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



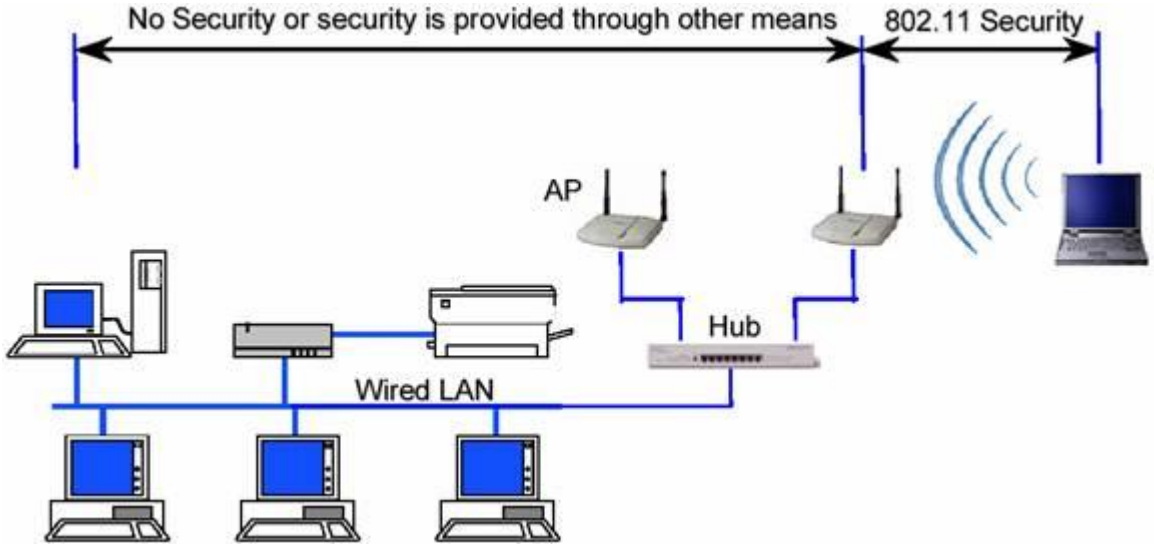
از دیگر استفاده‌های نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دست‌رسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک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

19-4- بخش چهارم : امنیت در شبکه‌های محلی بر اساس استاندارد 802.11

پس از آن‌که در سه قسمت قبل به مقدمه‌یی در مورد شبکه‌های بی‌سیم محلی و عناصر آن‌ها پرداختیم، از این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE 802.11 را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد، می‌توان از محدودیت‌های آن آگاه شد و این استاندارد و کاربرد را برای موارد خاص و مناسب مورد استفاده قرار داد.

تهیه کننده :سید حمید یاریان

استاندارد 802.11 سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.



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

تهیه کننده :سید حمید یاریان

19-4-1- قابلیت‌ها و ابعاد امنیتی استاندارد 802.11

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد **802.11** فراهم می‌کند **WEP** است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشت این‌ست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح **WEP** در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های سیمی و بی‌سیم‌یی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

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

19-4-1-1- Authenticatio

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

19-4-1-2- Confidentiality

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

19-4-1-3- Integrity

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم‌وبیش وجود دارد. نکته‌ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس‌های معمول Auditing وAuthorization در میان سرویس‌های ارایه شده توسط این پروتکل است.

19-5- بخش پنجم : سرویس‌های امنیتی WEP – Authentication

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

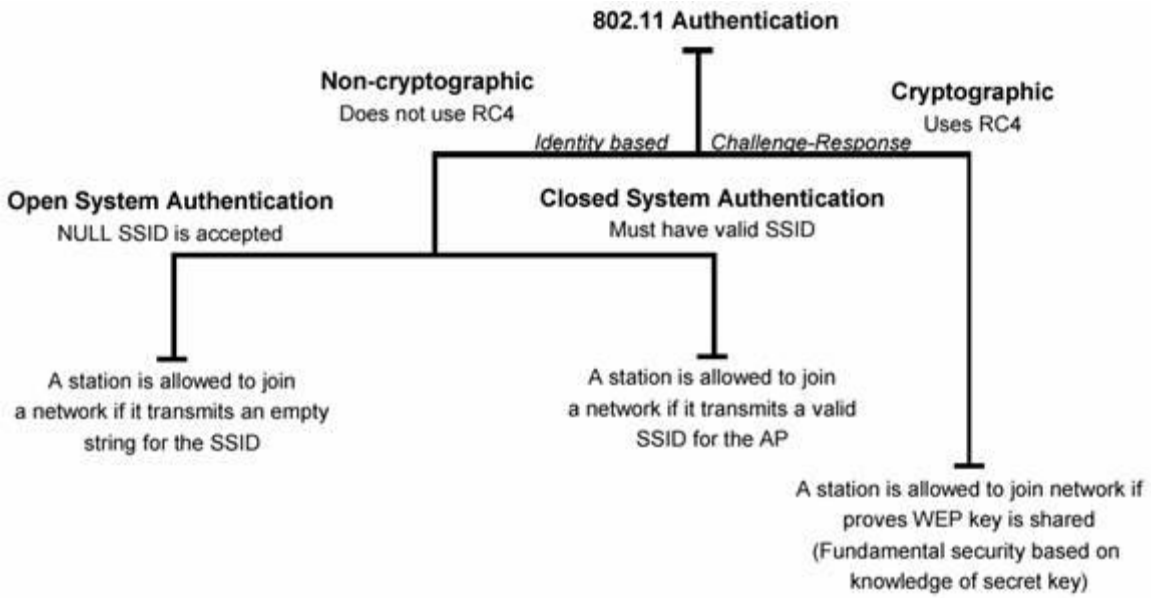
در این قسمت به معرفی سرویس اول، یعنی Authentication، می‌پردازیم.

Authentication

تهیه کننده :سید حمید یاریان

استاندارد 802.11 دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه‌ی بی‌سیم را به نقاط دسترسی ارسال می‌کنند، دارد که یک روش بر مبنای رمزنگاری‌ست و دیگری از رمزنگاری استفاده نمی‌کند.

شکل زیر شَمایی از فرایند Authentication را در این شبکه‌ها نشان می‌دهد :



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

19-5-1- Authentication بدون رمزنگاری

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

تهیه کننده :سید حمید یاریان

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

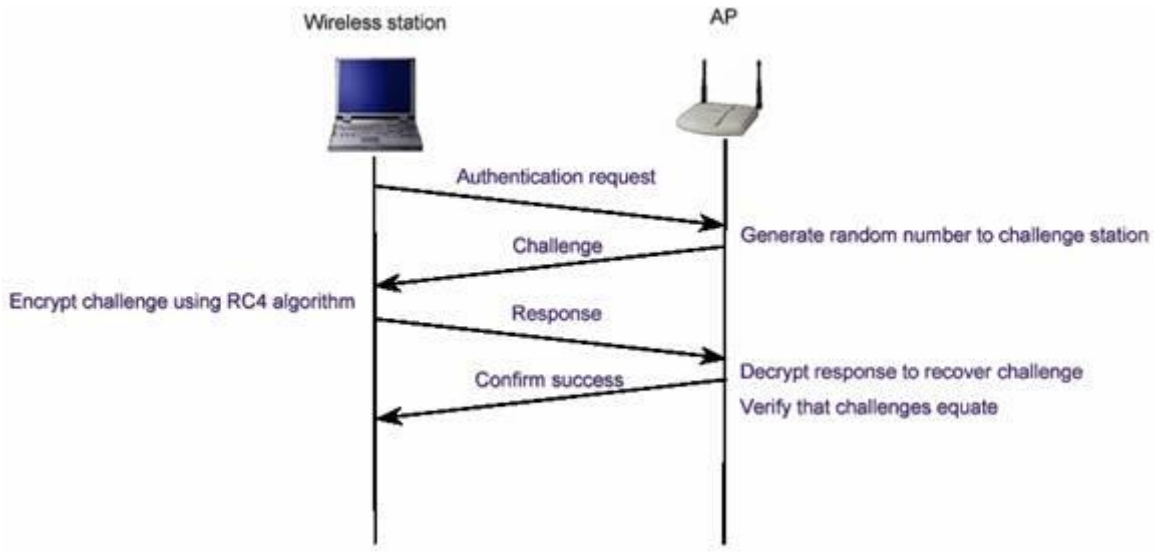
در روش دوم از این نوع، بازهم یک **SSID** به نقطه‌ی دسترسی ارسال می‌گردد با این تفاوت که اجازه‌ی اتصال به شبکه تنها در صورتی از سوی نقطه‌ی دسترسی صادر می‌گردد که **SSID**ی ارسال شده جزو **SSID**های مجاز برای دسترسی به شبکه باشند. این روش به **Closed System Authentication** موسوم است.

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 ارایه نمی‌دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست‌کننده هستند. با این وصف از آن‌جایی‌که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم‌تجربه و مبتدی، به شبکه‌هایی که بر اساس این روش‌ها عمل می‌کنند، رخ می‌دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه‌یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده‌ی یک شبکه‌ی بی‌سیم – که مانند شبکه‌های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ‌دادن حملات نیز خود تضمینی ندارد!

تهیه کننده :سید حمید یاریان

19-5-2- Authentication با رمزنگاری RC4

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



در این روش، نقطه‌ی دسترسی **(AP)** یک رشته‌ی تصادفی تولید کرده و آن‌را به مخدوم می‌فرستد. مخدوم این رشته‌ی تصادفی را با کلیدی از پیش تعیین شده (که کلید **WEP** نیز نامیده می‌شود) رمز می‌کند و حاصل را برای نقطه‌ی دسترسی ارسال می‌کند. نقطه‌ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و بارشته‌ی ارسال شده مقایسه می‌کند. در صورت هم‌سانی این دو پیام، نقطه‌ی دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل

تهیه کننده :سید حمید یاریان

می‌کند. روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است.در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است

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

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

19-6-بخش ششم : سرویس‌های امنیتی Privacy – 802.11b و Integrity

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

Privacy -1-6-19

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

تهیه کننده :سید حمید یاریان

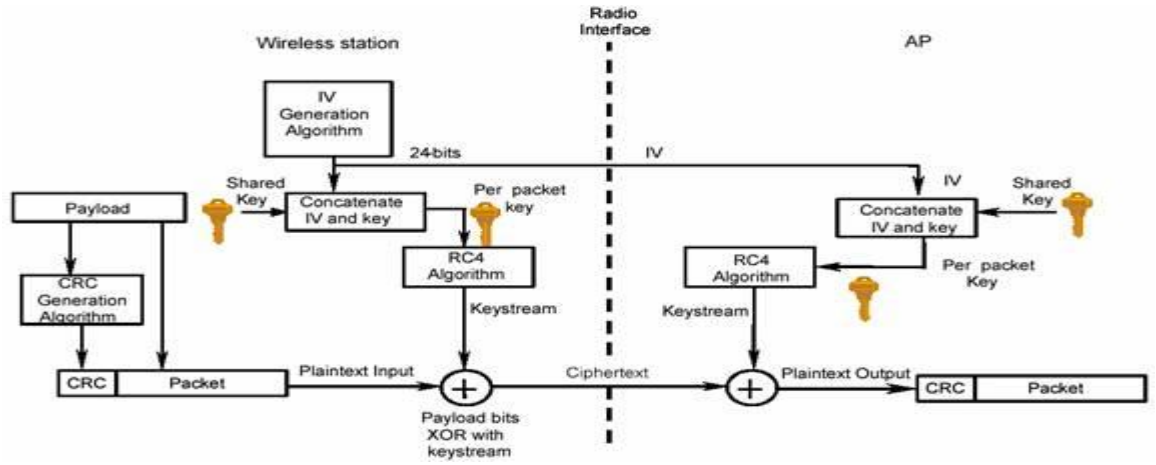
به‌گونه‌یی‌که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

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

کلیدهای **WEP** اندازه‌هایی از ۴۰ بیت تا ۱۰۴ بیت می‌توانند داشته باشند. این کلیدها با **IV** (مخفف **Initialization Vector** یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی **RC4** را تشکیل می‌دهند. طبیعتاً هرچه اندازه‌ی کلید بزرگ‌تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می‌دهد که استفاده از کلیدهایی با اندازه‌ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک **brute-force** را برای شکستن رمز غیرممکن می‌کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه‌ی ۸۰ بیت (که تعدد آن‌ها از مرتبه‌ی ۲۴ است) به اندازه‌یی بالاست که قدرت پردازش سیستم‌های رایانه‌یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی‌کند.

هرچند که در حال حاضر اکثر شبکه‌های محلی بی‌سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته‌های اطلاعاتی استفاده می‌کنند ولی نکته‌یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این‌ست که روش تأمین محرمانه‌گی توسط **WEP** در مقابل حملات دیگری، غیر از استفاده

از روش **brute-force**، نیز آسیب‌پذیر است و این آسیب‌پذیری ارتباطی به اندازه‌ی کلید استفاده شده ندارد. نمایی از روش استفاده شده توسط **WEP** برای تضمین محرمانه‌گی در شکل زیر نمایش داده شده است :



Integrity -2-6-19

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

در استاندارد **802.11b** نیز سرویس و روشی استفاده می‌شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم‌های بی‌سیم و نقاط دست‌رسی کم می‌شود. روش مورد نظر استفاده از یک کد **CRC** است. همان‌طور که در شکل قبل نیز نشان داده شده است، یک **CRC-32** قبل از رمزشدن بسته تولید می‌شود. در سمت گیرنده، پس از رمزگشایی، **CRC** داده‌های رمزگشایی شده مجدداً محاسبه شده و با **CRC** نوشته شده در بسته مقایسه می‌گردد که هرگونه اختلاف میان دو

CRC به‌معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسط RC4، مستقل از اندازه‌ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب‌پذیر است.

متأسفانه استاندارد 802.11b هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می‌گیرد باید توسط کسانی که شبکه‌ی بی‌سیم را نصب می‌کنند به‌صورت دستی پیاده‌سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل‌های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش‌های متعددی برای حمله به شبکه‌های بی‌سیم قابل تصور است. این روش‌ها معمولاً بر سهل انگاری‌های انجام‌شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به‌صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه‌های بی‌سیم ندارد. این مشکل از شبکه‌های بزرگ‌تر بیش‌تر خود را نشان می‌دهد. حتی با فرض تلاش برای جلوگیری از رخداد چنین سهل‌انگاری‌هایی، زمانی که تعداد مخدوم‌های شبکه از حدی می‌گذرد عملاً کنترل‌کردن این تعداد بالا بسیار دشوار شده و گه‌گاه خطاهایی در گوشه و کنار این شبکه‌ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می‌شود.

19-7-بخش هفتم : ضعف‌های اولیه‌ی امنیتی WEP

در قسمت‌های قبل به سرویس‌های امنیتی استاندارد 802.11 پرداختیم. در ضمنِ ذکر هریک از سرویس‌ها، سعی کردیم به ضعف‌های هریک اشاره‌یی داشته باشیم. در این قسمت به بررسی ضعف‌های تکنیک‌های امنیتی پایه‌ی استفاده شده در این استاندارد می‌پردازیم.

تهیه کننده :سید حمید یاریان

همان‌گونه که گفته شد، عملاً پایه‌ی امنیت در استاندارد **802.11** بر اساس پروتکل **WEP** استوار است. **WEP** در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم **RC4** استفاده می‌شود، هرچند که برخی از تولیدکننده‌گان نگارش‌های خاصی از **WEP** را با کلیدهایی با تعداد بیت‌های بیش‌تر پیاده‌سازی کرده‌اند.

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

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

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

19-7-1- استفاده از کلیدهای ثابت WEP

یکی از ابتدایی‌ترین ضعف‌ها که عموماً در بسیاری از شبکه‌های محلی بی‌سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می‌دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می‌کند به سرقت برود یا برای مدت زمانی در دست‌رس نفوذگر باشد، کلید آن به‌راحتی

لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه‌های کاری عملاً استفاده از تمامی این ایستگاه‌ها ناامن است.

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

19-7-2- 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 آن‌جایی‌که کلیدی که برای رمزنگاری مورد استفاده قرار می‌گیرد بر اساس IV تولید می شود، محدوده‌ی IV عملاً نشان‌دهنده‌ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است. به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می‌توان به کلیدهای مشابه دست یافت.

این ضعف در شبکه‌های شلوغ به مشکلی حاد مبدل می‌شود. خصوصاً اگر از کارت شبکه‌ی استفاده شده مطمئن نباشیم. بسیاری از کارت‌های شبکه از IVهای ثابت استفاده می‌کنند و بسیاری از کارت‌های شبکه‌ی یک تولید کننده‌ی واحد IVهای مشابه دارند. این خطر به‌همراه ترافیک بالا در یک شبکه‌ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می‌برد و در نتیجه کافی‌ست نفوذگر در مدت زمانی معین به ثبت داده‌های رمز شده‌ی شبکه بپردازد و IVهای بسته‌های اطلاعاتی را ذخیره کند. با ایجاد بانکی از IVهای استفاده شده در یک شبکه‌ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

تهیه کننده :سید حمید یاریان

19-7-3- ضعف در الگوریتم

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

19-7-4- استفاده از **CRC** رمز نشده

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

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

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

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

19-8- قسمت هشتم : خطرها، حملات و ملزومات امنیتی

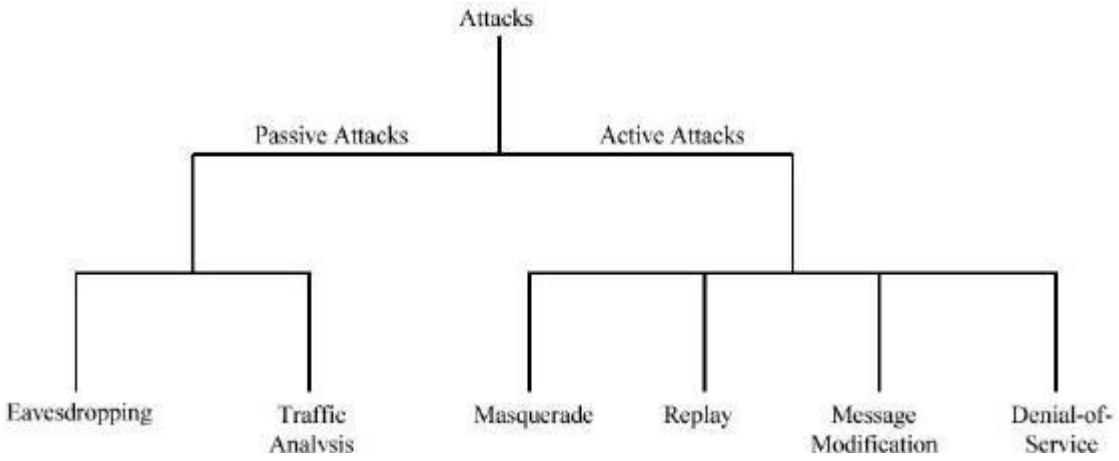
همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده یی نه چندان دور باید منتظر گسترده گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم. این گسترده گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این

تهیه کننده :سید حمید یاریان

نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است،

توسعه ای این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات، خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازیم.

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



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

19-8-1- حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوال اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

تهیه کننده :سید حمید یاریان

19-8-2- شنود

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

19-8-3- آنالیز ترافیک

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

19-8-4- حملات فعال

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

19-8-4-1- تغییر هویت

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

19-8-4-2- پاسخ های جعلی

تهیه کننده :سید حمید یاریان

نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه –به روشی- توسط نفوذگر قطع شده است، می تواند مورد سوء استفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

19-8-4-3- تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است. از آن جایی که گونه های متنوعی از ترافیک بر روی شبکه رفت وآمد می کنند و هریک از این ترافیک ها و پروتکل ها از شیوه یی برای مدیریت جنبه های امنیتی خود استفاده می کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام ها و در نتیجه حملات را اتخاذ کند. با توجه به گسترده گی این نوع حمله، که کاملاً به نوع پروتکل بسته گی دارد، در این جا نمی توانیم به انواع مختلف آن بپردازیم، تنها به یادآوری این نکته بسنده می کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می تواند با اعمال تغییرات خاصی،

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

19-8-4-4- حمله های (DoS (Denial-of-Service

این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی اقدام می کند. ساده ترین نمونه سعی در از کارانداختن خادم های نرم افزاری و سخت افزاری ست. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن یک سامانه، که معمولاً سامانه یی ست که مشکلاتی برای نفوذگر برای دست رسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می کند. در برخی از حالات، در پی حمله ی انجام شده، سرویس مورد نظر به طور کامل قطع نمی گردد و تنها کارایی آن مختل می گردد. در این حالت نفوذگر می تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از همان طریق به سرویس نیز اقدام کند.

20- رویکردی عملی به امنیت شبکه لایه بندی شده

20-1- مقدمه

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است. {گروه امداد امنیت کامپیوتری ایران}

تهیه کننده :سید حمید یاریان

در این قسمت رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی می گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیرساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد.

رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد.

۱- پیرامون

۲- شبکه

۳- میزبان

۴- برنامه کاربردی

۵- دیتا

در این قسمت هریک از این سطوح تعریف می شوند و یک دید کلی از ابزارها و سیستمهای امنیتی گوناگون که روی هریک عمل می کنند، ارائه می شود. هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. مخاطبان این قسمت متخصصان فناوری اطلاعات، مدیران تجاری و تصمیم گیران سطح بالا هستند.

محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله،خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. بعلاوه، با رویکرد

عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید.

20-1-1- افزودن به ضریب عملکرد هکرها

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد (work factor) استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است. ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از سیستمها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه

بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که شما می خواهید .

تکنولوژی های بحث شده در این سری مقالات مجموعاً رویکرد عملی خوبی برای امن سازی دارایی های دیجیتالی شما را به نمایش می گذارند. در یک دنیای ایده آل، شما بودجه و منابع را برای پیاده سازی تمام ابزار و سیستم هایی که بحث می کنیم خواهید داشت. اما متأسفانه در چنین دنیایی زندگی نمی کنیم. بدین ترتیب، باید شبکه تان را ارزیابی کنید – چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و غیره ...و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی کنید.

20-1-2-مدل امنیت لایه بندی شده

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند. این تکنولوژی ها با جزئیات بیشتر در بخش های بعدی مورد بحث قرار خواهند گرفت.

تهیه کننده :سید حمید یاریان

ردیف	سطح امنیتی	ابزار و سیستم های امنیتی قابل استفاده
۱	پیرامون	فایروال آنتی ویروس در سطح شبکه رمزنگاری شبکه خصوصی مجازی
۲	شبکه	سیستم تشخیص/جلوگیری از نفوذ (**IDS/IPS**) سیستم مدیریت آسیب پذیری تبعیت امنیتی کاربر انتهایی کنترل دسترسی/ تایید هویت کاربر
۳	میزبان	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان تبعیت امنیتی کاربر انتهایی آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
۴	برنامه کاربردی	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
۵	داده	رمزنگاری کنترل دسترسی/ تایید هویت کاربر

تهیه کننده :سید حمید یاریان

20-2- سطح ۱: امنیت پیرامون سطح پیرامون

منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان **DMZ** (**zone demilitarized**) شناخته می شود. **DMZ** معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای **DNS** را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرورها در **DMZ** می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد.پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست. تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:

20-2-1- -1- د فایروال معمولاً یک فایروال روی سروری نصب می گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می دهد .

1-کنترل ترافیک

۲- تبدیل آدرس و ۳- نقطه پایانی **VPN**. فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های **IP** داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش

تهیه کننده :سید حمید یاریان

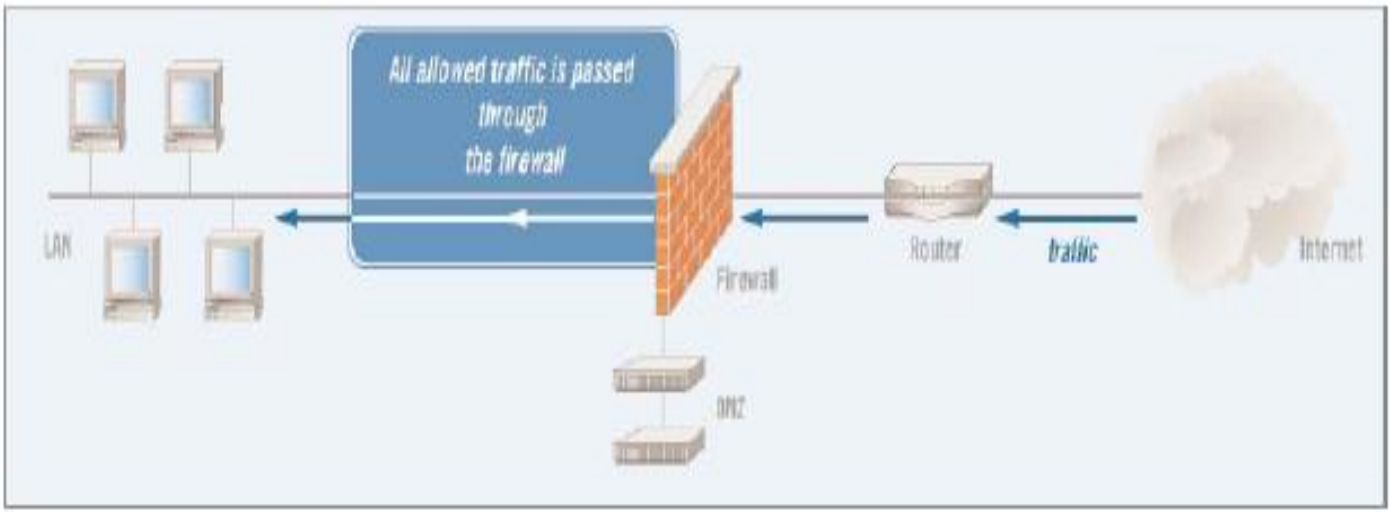
فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.

20-2-1-2- آنتی ویروس شبکه ـ این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.

20-2-1-3- VPNـ یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند.

VPN اساساً یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود.

تهیه کننده :سید حمید یاریان



20-2-2- مزایا

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند. بعض از فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

20-2-3- معایب

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری

مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان **IT** تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

20-2-4- ملاحظات

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

انواع ابزاری که در **DMZ** شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

20-3- سطح 2 : امنیت پیرامون سطح شبکه

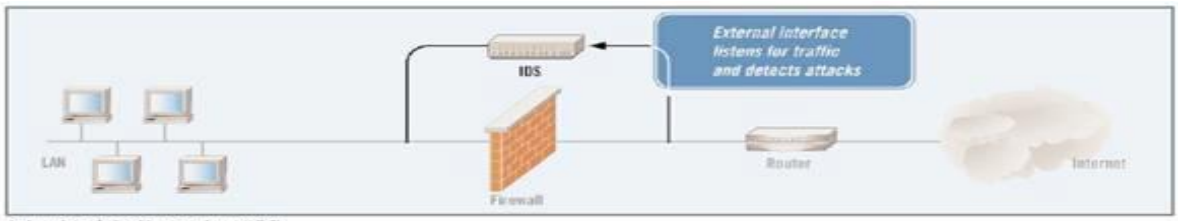
سطح شبکه در مدل امنیت لایه بندی شده به **WAN** و **LAN** داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند. تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند:

تهیه کننده :سید حمید یاریان

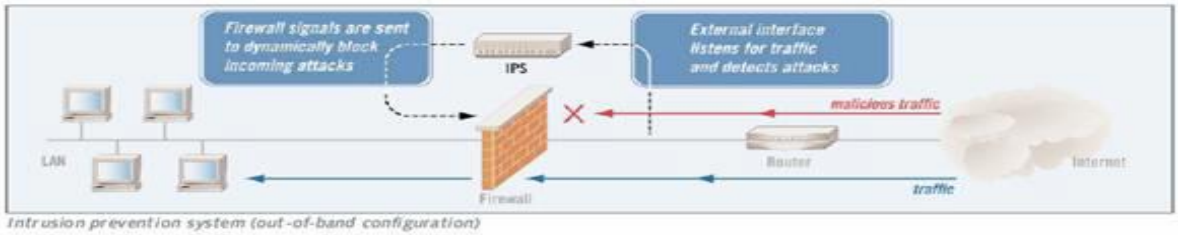
20-3-1-1- IDSها (سیستم های تشخیص نفوذ) و IPSها (سیستم های جلوگیری از نفوذ) ـ

تکنولوژیهای IDS و IPS ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسؤولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و بصورت خودکار ترافیک آسیب رسان را مسدود می کنند. IDSها و IPSها مشخصات مشترک زیادی دارند. در حقیقت، بیشتر IPSها در هسته خود یک IDS دارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می شود. محصولات IDS تنها ترافیک آسیب رسان را تشخیص می دهند، در حالیکه محصولات IPS از ورود چنین ترافیکی به شبکه شما جلوگیری می کنند. پیکربندی های IDS و IPS استاندارد در شکل نشان داده شده اند:

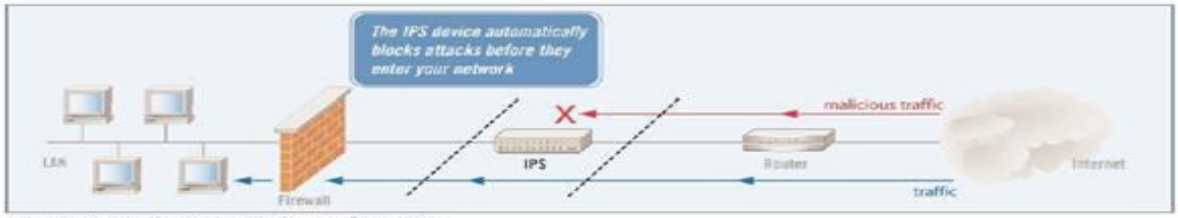
تهیه کننده :سید حمید یاریان



Intrusion detection system (IDS)



Intrusion prevention system (out-of-band configuration)



Intrusion prevention system (in-line configuration)

20 -3-1-2- مدیریت آسیب پذیری : سیستم های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می کنند و (۲)روند مرمت آسیب پذیری یافته شده را مدیریت می کنند. در گذشته، این تکنولوژی **VA (تخمین آسیب پذیری)** نامیده می شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می دهند.

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری هایی که می توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می کنند. آنها معمولاً پایگاه داده ای از قوانینی را نگهداری می کنند که آسیب پذیری های شناخته شده برای گستره ای از ابزارها و برنامه های شبکه را مشخص می کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می آزماید.

تهیه کننده :سید حمید یاریان

همچنانکه از نامش برمی آید، سیستم مدیریت آسیب پذیری شامل ویژگیهایی است که روند بازسازی را مدیریت می کند. لازم به ذکر است که میزان و توانایی این ویژگی ها در میان محصولات مختلف، فرق می کند.

20-3-1-3- تابعیت امنیتی کاربر انتهایی : روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می کنند که تضمین می کنند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند، رعایت کرده اند. این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم های ناامن کارمندان و ابزارهای **VPN** و **RAS** می گیرد.

روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می دهند، اجازه دسترسی می دهند. هدف آنها از این تست ها معمولاً برای بررسی (۱) نرم افزار مورد نیاز، مانند سرویس پک ها، آنتی ویروس های به روز شده و غیره و (۲) کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است.

20-3-1-4- کنترل دسترسی\تأیید هویت : کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند. هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

نکته: در این سلسله مباحث، به کنترل دسترسی و تأییدهویت در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در

مقابل دید کاربر اتفاق می افتد. اما به خاطر داشته باشید که کنترل دسترسی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند.

20-3-2- مزایا

تکنولوژی های **IDS**، **IPS** و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد، ابزار **IPS** و **IDS** تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد.

سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند. انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیرعملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید، ارتقاءدادن نرم افزارها و وصله ها، و افزودن و کاستن از کاربران، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری های جدید پیمایش کنید.

روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است. هکرها بصورت روز افزون به

دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، همچانکه پدیده های اخیر چون Mydoom، Sobig، و Sasser گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند .

20-3-3- معایب

IDS ها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان false positives نیز شناخته می شوند. در حالیکه IDS ممکن است که یک حمله را کشف و به اطلاع شما برساند، این اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری بالا، یک IDS باید بصورت پیوسته بررسی شود و برای الگوهای مورد استفاده و آسیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند .

سطح خودکار بودن در IPSها می تواند به میزان زیادی در میان محصولات، متفاوت باشد. بسیاری از آنها باید با دقت پیکربندی و مدیریت شوند تا مشخصات الگوهای ترافیک شبکه ای را که در آن نصب شده اند منعکس کنند. تأثیرات جانبی احتمالی در سیستمهایی که بهینه نشده اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می شود.

بسیاری، اما نه همه روش های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر نقطه انتهایی دارد. این عمل می تواند مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه کند.

تهیه کننده :سید حمید یاریان

تکنولوژی های کنترل دسترسی ممکن است محدودیت های فنی داشته باشند. برای مثال، بعضی ممکن است با تمام ابزار موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای ایجاد پوشش نیاز داشته باشید. همچنین، چندین فروشنده سیستم های کنترل دسترسی را به بازار عرضه می کنند، و عملکرد می تواند بین محصولات مختلف متفاوت باشد. پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد. چنین عمل وصله-پینه ای یعنی رویکرد چند محصولی ممکن است در واقع آسیب پذیری های بیشتری را در شبکه شما به وجود آورد.

20-3-4- ملاحظات

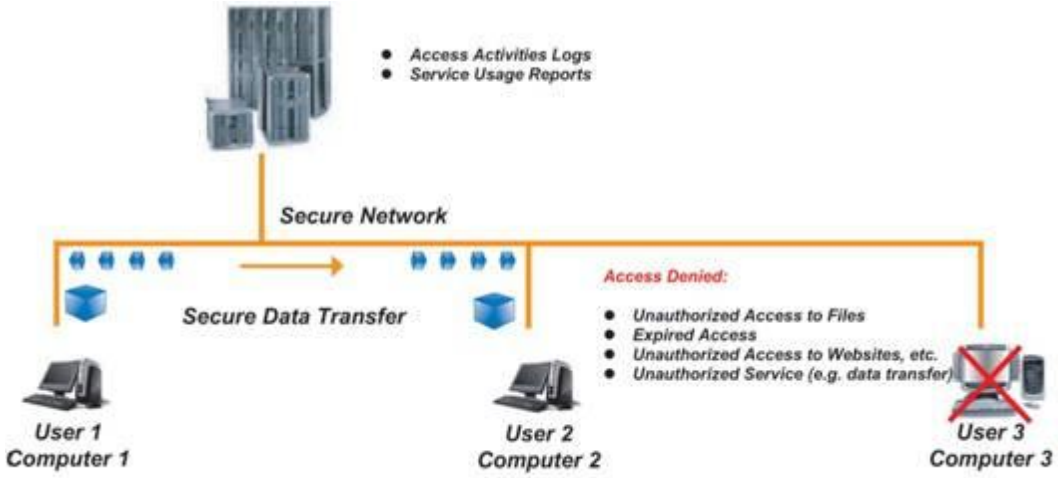
موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS/IPS ، مدیریت آسیب پذیری و امنیت کاربر انتهایی ممکن است منابعی از شبکه ای را که از آن محافظت می کنند، مصرف کنند. سرعت های اتصالی بالاتر تأثیری را که این ابزارها بر کارایی شبکه دارند به حداقل خواهد رساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت بهبودیافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد.

وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد

20-4- سطح 3: امنیت پیرامون سطح میزبان سطح میزبان

تهیه کننده :سید حمید یاریان

سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها و غیره در شبکه است. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادرستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات رجیستری، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.



تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

20-4-1-1- IDS در سطح میزبان ـ IDSهای سطح میزبان عملیاتی مشابه IDSهای شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است.

IDS های سطح میزبان برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.

20-4-1-2- VA (تخمین آسیب پذیری) سطح میزبان - ابزارهای VA سطح میزبان یک ابزار شبکه مجزا را برای آسیب پذیری های امنیتی پویش می کنند. دقت آنها نسبتا بالاست

تهیه کننده :سید حمید یاریان

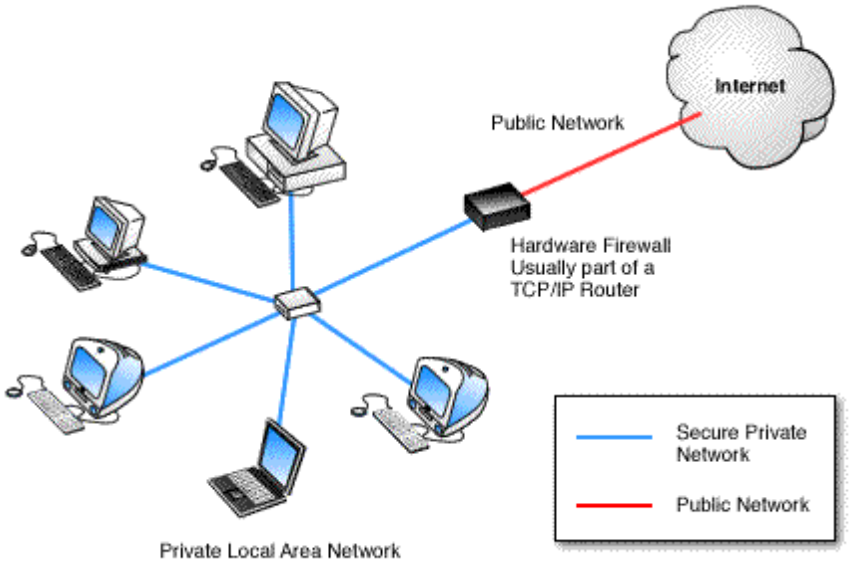
و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، درصورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.

20-4-1-3- تابعیت امنیتی کاربر انتهایی – روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیوسته میزبان را برای عملیات زیان رسان و آلودگی ها بررسی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.

20 -4-1-3- آنتی ویروس - هنگامی که آنتی ویروس های مشخص شده برای ابزار در کنار آنتی ویروس های شبکه استفاده می شوند ، لایه اضافه ای برای محافظت فراهم می کنند.

20 -4 -1-4- کنترل دسترسی\تصدیق هویت- ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.

تهیه کننده :سید حمید یاریان



20-4-2- مزایا

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن مشخصات عملیاتی مخصوص یک ابزار پیکربندی می گردند. دقت و پاسخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت مشخص کنند کدام تنظیمات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.

20-4-2- معایب

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز رسانی مداوم دارند، اغلب ساعات زیادی برای مدیریت مناسب می طلبند. اغلب نصبشان مشکل است و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است. همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر

خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد.

20-4-3- ملاحظات

بدلیل هزینه ها و باراضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند. بعنوان یک اصل راهنما، بیشتر سازمان ها این ابزار را فقط روی سیستم های بسیار حساس شبکه نصب می کنند. استثناء این اصل یک راه حل تابعیت امنیتی کاربر انتهایی است، که اغلب برای پوشش دادن به هر ایستگاه کاری که تلاش می کند به شبکه دسترسی پیدا کند، بکار گرفته می شود .

20-5- سطح 4: امنیت پیرامون سطح برنامه کاربردی

در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند. این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند. این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیات بد دارند، باشند. بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تهیه کننده :سید حمید یاریان

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

20-5-1-1- پوشش محافظ برنامه :

از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شفاف است و با درجه بالایی با سیستم یکپارچه می شود.

یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور پیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.

20-5-1-2- کنترل دسترسی/تصدیق هویت:

مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.

20-5-1-3- تعیین صحت ورودی :

ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد.

اگر ابزارهای امنیتی مناسب در جای خود مورد استفاده قرار نگیرند، هر تراکنش بین افراد و واسط تهیه کننده :سید حمید یاریان

کاربر می تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود!

به عنوان مثال، یک فرم وبی با یک بخش **zip code** را در نظر بگیرید. تنها ورودی قابل پذیرش در این قسمت فقط پنج کاراکتر عددی است. تمام ورودی های دیگر باید مردود شوند و یک پیام خطا تولید شود. تعیین صحت ورودی باید در چندین سطح صورت گیرد. در این مثال، یک اسکریپت جاوا می تواند تعیین صحت را در سطح مرورگر در سیستم سرویس گیرنده انجام دهد، در حالیکه کنترل های بیشتر می تواند در سرور وب قرار گیرد. اصول بیشتر شامل موارد زیر می شوند:

-کلید واژه ها را فیلتر کنید. بیشتر عبارات مربوط به فرمانها مانند «**insert**»، باید بررسی و در صورت نیاز مسدود شوند.

- فقط دیتایی را بپذیرید که برای فلید معین انتظار می رود. برای مثال، یک اسم کوچک ۷۵ حرفی یک ورودی استاندارد نیست.

20-5-2- مزایا

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

20-5-3- معایب

پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با امنیت سطح

برنامه می تواند عملی ترسناک! و غیرعملی باشد. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

20-5-4- ملاحظات

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی بلندمدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند .

20-6- سطح 5: امنیت پیرامون سطح دیتا

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان روشی بسیار مناسب توصیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند. امنیت دیتا تا حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد که سیاست های دسترسی و ابزار امنیتی مناسبی را که باید بکار گرفته شوند، مشخص کنید.تکنولوژی های زیر امنیت در سطح دیتا را فراهم می کنند:

تهیه کننده :سید حمید یاریان

20-6-1-1- رمزنگاری – طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/رمزگشایی هستند که تمام افرادی که به دیتا دسترسی دارند، باید داشته باشند. استراتژی های رمزنگاری معمول شامل PKI، PGP و RSA هستند.

19-6-1-2- کنترل دسترسی / تصدیق هویت – مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.

20-6-2- مزایا

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می کند.

20-6-3- معایب

تهیه کننده :سید حمید یاریان

بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

20-6-4- ملاحظات:رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری باید برای تمام ابزارها و برنامه های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است .

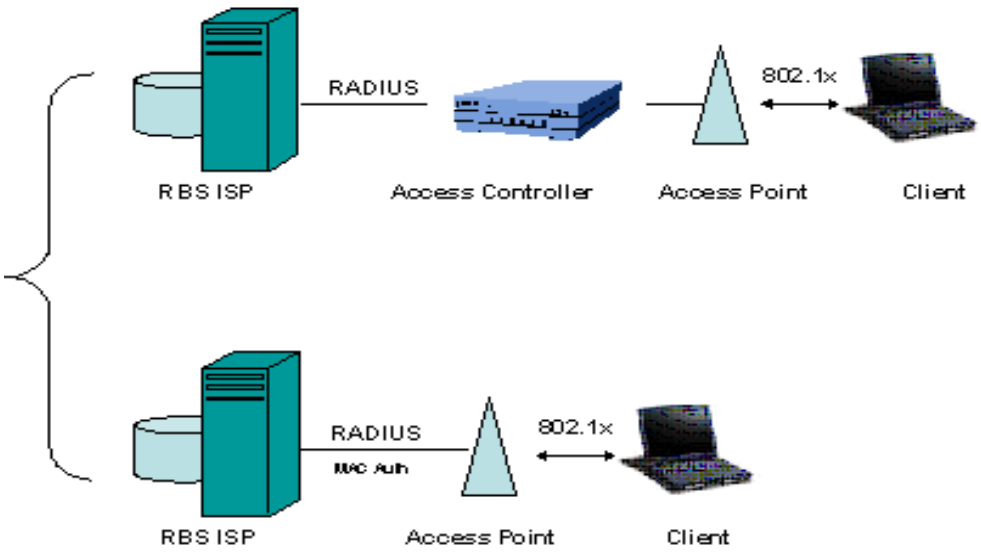
21- چهارمشکل امنیتی مهم شبکه های بی سیم 802.11 :

21-1- مقدمه

موفقیت حیرت انگیز 802.11 به علت توسعه «اترنت بی سیم» است. همچنانکه 802.11 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 قسمت هفت مشکل از مهم ترین آسیب پذیری های امنیتی موجود در LANهای 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 قسمت هریک از این «چهارمسأله 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. قسمت



21-2- مسأله شماره ۱: دسترسی آسان

LANهای بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها باید فریم های **Beacon** با پارامتر های 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

802.11 شما و پارامترهایش برای هر شخصی با یک کارت 802.11 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.

21-2-1- راه حل شماره ۱: 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 هرحال، 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.

تهیه کننده :سید حمید یاریان

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 VPNها 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. 802.1x انواع فریم های جدید برای تأیید هویت کاربر را تعریف می کند و از دیتابیس های کاربری جامعی مانند RADIUS بهره می گیرد. آنالایزرهای 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 802.11 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 چینش 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. آنالایزرهای 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.

تهیه کننده :سید حمید یاریان

پیکربندی های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LANهای بی سیم بدون نظارت مهندسان امنیتی به کارگرفته 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 آنالایزرها همچنین می توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا 802.1x استفاده نمی کنند، علائم هشدار دهنده را ثبت کنند.

21-3- مسئله شماره 2: 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» بکارگرفته 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.

تهیه کننده :سید حمید یاریان

کارت شبکه های بی سیم یاهامان نقطه دسترسی

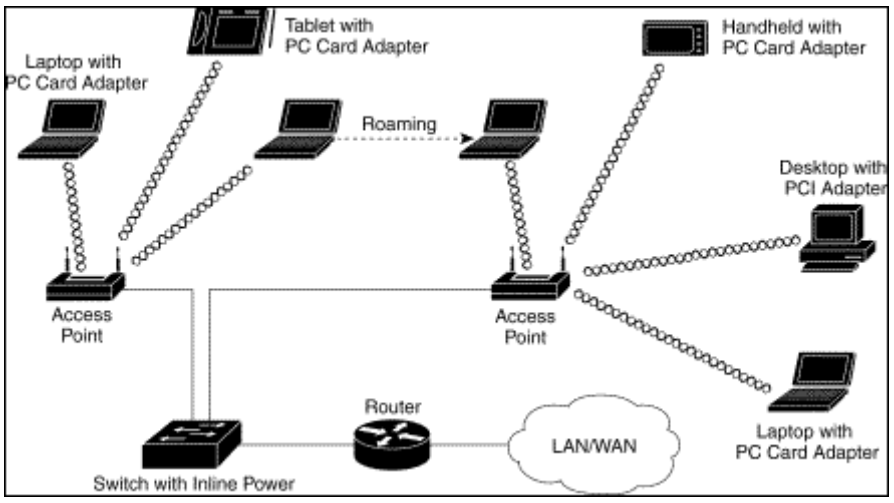
21-3-1- راه حل مئسله شماره2 : رسیدگی های منظم به سایت

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

تهیه کننده :سید حمید یاریان

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 802.11 در سال های اخیر ظهور 802.11a به عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های 802.11a را بوجود آورد. خوشبختانه، 802.11a از همان MAC پیشینیان خود استفاده می کند، بنابراین بیشتر آنچه مدیران راجع به 802.11 و تحلیل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استاندارد 802.11a و 802.11b را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست های دوباندی 802.11a/b 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 چارچوپ پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا 802.11g ادامه یابد، تا جایی که سازندگان آنالایزرها کارت های 802.11a/b/g را مورد پذیرش قرار دهند .



تهیه کننده :سید حمید یاریان

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 802.11 بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی های سایت بتوانند کل محدوده فرکانسی را پویش کنند. حتی اگر شما استفاده از 802.11b را انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی 802.11a را نیز پویش 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 802.11b به کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال های ۱ تا ۱۱ از 802.11b 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 هرحال، 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.

تهیه کننده :سید حمید یاریان

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.

21-4- مسأله شماره 3: تحلیل ترافیک و استراق سمع

802.11 هیچ محافظتی علیه حملاتی که بصورت غیرفعال **(passive)** ترافیک را مشاهده می کنند، ارائه نمی کند. خطر اصلی این است که **802.11** روشی برای تامین امنیت دیتای در حال انتقال و جلوگیری از استراق سمع فراهم نمی کند .

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 .

21-4-1- راه حل شماره3 : 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 وتولیدکلیدپویاتوصیه می شود.

WEP تاحدزیادی 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. بعنوانبخشی از نظارت

سایت، مدیران شبکه می توانند از آنالایزرهای 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 مانندSSH ، SSLو 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 ازWEP ، 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 802.1 xداشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق 802.1x، نتایج باارزشی روی قسمت بی سیم تبادل تصدیق هویت 802.1 xارائه می کند. آنالایزر 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 .

21-5- مسأله شماره 4: 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 اینترتیب 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 .

21-5-1- راه حل شماره4 : 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 درگا ه 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 LANبی سیم و شبکه مرکزی استفاده کنید، و سپس دسترسی به شبکه مرکزی را از طریق روش های VPN تثبیت شده ارائه کنید .

21-6 نتیجه گیری

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

تهیه کننده :سید حمید یاریان

فوائد 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.

22-پنج نکته در مورد امنیت شبکه های بی سیم

با به کارگیری نکات زیر می توان یک امنیت شبکه بی سیم را تا حد قابل قبولی بهبود بخشید.لازم به ذکر است که این نکات لازم است ولی کافی نیست.

22-1- کلمه عبور پیش‌فرض مدیر سیستم (administrator)را روی نقاط دسترسی ومسیریاب‌های بی‌سیم تغییر دهید.

اغلب نقاط دسترسی(Access Point) و مسیریاب‌های بی‌سیم امکان مدیریت شبکه WiFi را از طریق یک حساب کاربری مدیریتی فراهم می‌کنند. این حساب کاربری امکان دسترسی ابزار و پیکربندی آن را با نام کاربری و کلمه عبور فراهم می‌کند. اغلب تولیدکنندگان نام کاربری و کلمه عبور را در کارخانه تنظیم می‌کنند . 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 پیش‌فرض 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 نگه‌داشتن شبکه در آینده، می‌بایست به‌طور منظم این کلمه عبور را تغییر دهید. اغلب کارشناسان توصیه می‌کنند کلمه عبور را بعد از 30 تا 90 روز تغییر دهید.

تهیه کننده :سید حمید یاریان

22-2- فعال‌سازی قابلیتWPA/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** بایدClient های 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 باclient های دارای ویندوز **XP** مراحل زیر را انجام دهید :

- نوشتار **Overview of the WPA wireless security update in Windows XP** را مطالعه کنید .
- بررسی کنید که تمام **Client** ها حداقل **Service Pack1** داشته باشند .
- روی هر **Client** بررسی کنید که کارت شبکه با سرویس **WZC(Windows Zero Configuration)**سازگار باشد .
- برای هر **client** وصله **Windows XP Support Patch for Wi-Fi Protected Access** را بارگزاری و نصب کنید .
- تغییرات لازم برای نقاط دسترسی بی‌سیم از گام **1** را اعمال کنید .
- تغییرات لازم برای کارت شبکه‌های بی‌سیم از گام **1** را اعمال کنید .

22-3- تغییر **SSID** پیش فرض

نقاط دسترسی و مسیریاب‌های بی‌سیم دارای یک نام شبکه **SSID(Service Set Identifier)** هستند که توسط تولیدکنندگان به‌طور پیش‌فرض انتخاب می‌شود **SSID** . از ایزارهای پیکربندی بر مبنای وب یا ویندوز این سازندگان قابل دسترسی است. اغلب**SSID** های پیش فرض کلمات ساده‌ای

مثل**wireless**، **netgear**، **linksys** ، **default** 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 می آید. زمانی که کسی شبکه ای با **SSID** پیش فرض بیابد، با دانستن این نکته که به احتمال فراوان این شبکه به درستی پیکربندی نشده است،

ترغیب به نفوذ به شبکه می‌شود. **SSID** می تواند هر زمانی تغییر کند به شرطی که این تغییر در تمام**client** ها 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 :

- از نام، آدرس، تاریخ تولد، شماره تلفن یا دیگر اطلاعات شخصی تان به عنوان بخشی از **SSID**استفاده نکنید .
- از کلمات عبور نام کاربری ویندوزتان یا**email** تان یا ... استفاد نکنید .
- با استفاده از عباراتی مثل**"TOP_SECRET"** ، **"FUNNY_BOX"**و ... نفوذگران را وسوسه نکنید **!!!.**
- از ترکیب حروف و اعداد استفاده کنید .
- عباراتی با طول حداکثر یا نزدیک به حداکثر انتخاب کنید .
- هرچند ماه یک بار**SSID** تان را تغییر دهید .

22-4- قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیریاب‌های بی‌سیم فعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم دارای قابلیتی به نام پالایش آدرس **MAC (MAC Address Filtering)**هستند. این مشخصه اغلب به‌طور پیش فرض فعال نیست. برای افزایش امنیت شبکه بی سیم تان این قابلیت را فعال کنید. در صورتی که این قابلیت فعال نباشد، هر **client**ای با دانستن **SSID** شبکه شما (در نظر داشته باشید که فهمیدن **SSID** کار بسیار ساده ای تهیه کننده :سید حمید یاریان

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 لیستclient هایی 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 نهایتا 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 نوجه داشت که نفوذگران با جعل آدرس MAC (MAC Spoofing)قادرند به شبکه بی سیم شما

وصل شوند ولی این مساله نباید باعث شود که شما از خیر این قابلیت بگذرید.

22-5- قابلیت همه‌پخشی SSID را روی نقاط دسترسی و مسیریاب‌های بی‌سیم غیرفعال کنید.

اغلب نقاط دسترسی و مسیریاب های بی سیم به‌طور خودکار SSID خوشان را در فواصل زمانی مشخص پخش می کنند. این مشخصه برای این است کهclient ها بتوانند به‌طور پویا شبکه های بی سیم را تشخیص دهند و بین آن ها جابه‌جا شوند (از شبکه ای به شبکه دیگر نقل مکان کنند). لازم به ذکر است که این مشخصه برایhotspot های تجاری و سیار طراحی شده است کهclient های 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. همان‌طور که در گام 3 اشاره شد نفوذگر با دانستن SSID یک مرحله به هدف نزدیک تر می شود.

تهیه کننده :سید حمید یاریان

در یک شبکه بی سیم بحث) roaming جابه‌جایی 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 همه‌پخشی نیست.

دقت داشته باشید که غیرفعال کردن قابلیت همه‌پخشی SSID فقط یکی از تکنیک‌های محکم‌سازی و افزایش امنیت شبکه‌های بی سیم است .این روش 100 درصد موثر نیست و نفوذگرها هنوز می توانند با sniff کردن پیغام های مختلف پخش شده در پروتکلWiFi ، SSID را تشخیص دهند. در واقع تکنیک هایی مثل غیرفعال کردن همه‌پخشی SSID باعث می شئد که شبکه بی سیم شما هدف راحتی برای نفوذگران نباشد.

Wifi –23 :

دسترسی به اینترنت روی شبکه های بی سیم مبحث جدیدی به نام Wifi را مطرح کرده است که توسط آن مراکر فرهنگی ، پارک ها ، کتابخانه ها و ... تحت پوشش wifi و درنتیجه اینترنت قرارگرفته اند. مثال بارز

این امکان در محل دائمی نمایشگاه های تهران می باشد و بازدید کنندگان قادر به دسترسی به اینترنت توسط کامپیوترهای قابل حمل خود هستند. در راستای تسهیل ارتباط و پوشش و سرعت بیشتر دسترسی تکنولوژی جدیدی در حال شکل گیری است که به نام Wimax شناخته می شود. این تکنولوژی از استاندارد IEEE e۸۰۲,۱۶ بهره می برد.

Wimax –24

تهیه کننده :سید حمید یاریان

این امکان در محل دائمی نمایشگاه های تهران می باشد و بازدید کنندگان قادر به دسترسی به اینترنت توسط کامپیوترهای قابل حمل خود هستند. در راستای تسهیل ارتباط و پوشش و سرعت بیشتر دسترسی تکنولوژی جدیدی در حال شکل گیری است که به نام **Wimax** شناخته می شود. این تکنولوژی از استاندارد **IEEE e۸۰۲,۱۶** بهره می برد.

24-1- DomainKeys: اثبات هویت فرستنده ایمیل و حفاظت از آن

آیا تا کنون جمله زیر توجه شما را جلب کرده است؟

Yahoo! DomainKeys has confirmed that this message was sent by yahoo.com

اخیراً هنگامی که ایمیل های خود را در یاهو چک می کنید، چنانچه فرستنده هم از اکانت یاهو استفاده کرده باشد، در قسمت **From:** و بعد از نام فرستنده، جمله فوق را می بینید.

جعل ایمیل که عبارتست از جعل آدرس ایمیل شخص یا شرکت دیگر به منظور جلب اعتماد کاربران برای بازکردن پیام ها، یکی از بزرگترین چالش هایی است که امروزه جامعه اینترنت و تکنولوژی های ضداسپم با آن مواجه هستند. ارائه کنندگان سرویس های ایمیل بدون تأیید هویت فرستنده و امکان ردگیری آن، هرگز نمی توانند مطمئن باشند که آیا یک پیام اصلی است یا جعلی و بنابراین مجبورند برای آنکه مشخص شود کدام ایمیل ها را تحویل گیرنده بدهند یا کدام را مسدود کنند و کدام را قرنطینه کنند، از بعضی روش های مبتنی بر حدس استفاده کنند.

DomainKeys یک طرح پیشنهادی فنی از طرف یاهو است که می تواند پاسخی واضح به پروسه تصمیم گیری در مورد صحت ایمیل بدهد. این تکنولوژی امکان این عمل را با ارائه مکانیسمی برای تأیید دامنه هر فرستنده ایمیل و جامعیت پیام های ارسالی میسر می کند (جامعیت یعنی ایمیل ها در

طول ارسال تغییر نکرده اند). هنگامی که وجود دامنه مورد تأیید قرار بگیرد، می توان آن را با دامنه استفاده شده توسط فرستنده در فیلد **From:** پیام مقایسه کرد تا در صورت جعل، مشخص گردد. اگر جعلی باشد، یا هرزنامه (اسپم) است یا پیام تقلبی و می توان بدون دخالت کاربر پیام را حذف کرد. اگر جعلی نباشد، دامنه شناخته شده است و یک پروفایل ماندگار می تواند برای دامنه ارسال کننده برقرار گردد و به ارائه کنندگان سرویس ارائه و حتی برای کاربران نمایش داده شود.

برای شرکت های شناخته شده که معمولاً ایمیل تجاری به مشتریان می فرستند، مانند بانک ها و سرویس های تجارت الکترونیک، فایده تأیید هویت بسیار بیشتر است، چرا که می توانند به کاربرانشان در حفاظت از «حملات **phishing** یا هویت ربایی» کمک کند.

برای مشتریان، مانند کاربران ایمیل یاهو یا سایرین، حمایت از تکنولوژی های تأیید هویت به این معنی است که می توانند اعتماد به ایمیل را از سر بگیرند و ایمیل می تواند به نقش خود به عنوان یکی از قویترین ابزارهای ارتباطی در زمان ما ادامه دهد .

24-2- استانداردسازی

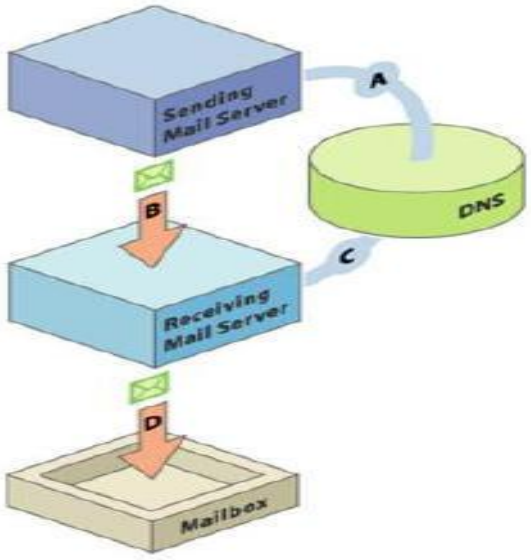
شرکت یاهو سعی دارد **DomainKeys** را به یک استاندارد اینترنتی تبدیل کند. یاهو امیدوار است که **DomainKeys** پروسه استانداردهای اینترنتی **IETF** (**Internet Engineering Task Force**) را طی کند و نهایتاً به عنوان یک استاندارد اینترنتی **IETF** تصویب شود.

24-3- سرورهای ایمیل فرستنده

برای امضاء کردن یک ایمیل با **DomainKeys** دو مرحله وجود دارد:

24-3-1- Set up (راه اندازی): صاحب دامنه (معمولاً تیمی که سیستم های ایمیل را در یک شرکت یا ارائه کننده سرویس اداره می کند) یک جفت کلید عمومی/اختصاصی را برای استفاده در امضای تمام پیامهای خروجی تولید می کند. کلید عمومی در **DNS** (**Domain Name System**) منتشر می شود و کلید اختصاصی در اختیار سرویس دهنده ارسال ایمیل قرار داده می شود. مرحله «**A**» در شکل نشانگر این بخش است.

24-3-2- Siging (امضاءکردن): هنگامی که هر ایمیل توسط یک کاربر مجاز آن دامنه، ارسال می شود، سیستم ایمیل مجهز به **DomainKeys**، به صورت خودکار از کلید اختصاصی ذخیره شده برای تولید امضای دیجیتالی پیام استفاده می کند. این امضاء سپس به **header** ایمیل الصاق می شود و ایمیل به سرور ایمیل گیرنده ارسال می شود. این مرحله «**B**» است که در شکل نشان داده شده است.



24-4- سرورهای ایمیل گیرنده

تهیه کننده :سید حمید یاریان

24-4-1- Preparing (آماده سازی): سیستم دریافت کننده ایمیل مجهز به **DomainKeys** امضاء و «دامنه ارسال کننده ادعاشده» (**Claimed From: Domain**) را از داخل **header** ایمیل استخراج می کند و کلید عمومی مربوط به دامنه ارسال کننده ادعاشده را از **DNS** می گیرد. این مرحله «**C**» در شکل نشان داده شده است.

24-4-2- Verifyin (تأیید هویت): سپس با استفاده از کلید عمومی گرفته شده از **DNS**، سیستم دریافت کننده ایمیل کنترل

می کند که امضاء توسط کلید اختصاصی متناظر تولید شده باشد. این امر ثابت می کند که ایمیل واقعاً توسط فرستنده ادعا شده در ابتدای ایمیل و با اجازه وی ارسال شده است و اینکه **header** و محتوا درطول ارسال تغییر نکرده است.

24-4-3-Delivering (تحویل): سیستم دریافت کننده ایمیل سیاست های محلی را براساس نتیجه بررسی امضاء اعمال می کند. اگر دامنه مورد تأیید قرار بگیرد و سایر بررسی های ضداسپم نیز تشخیص اسپم ندهند، ایمیل می تواند به **inbox** کاربر تحویل داده شود. اگر امضاء تأیید نگردد یا وجود نداشته باشد، ایمیل می تواند حذف شود، علامت زده شود یا قرنطینه شود. مرحله «**D**» در شکل، این بخش را نشان داده است.

عموماً یاهو انتظار دارد که **DomainKeys** توسط سرورهای دریافت کننده ایمیل تأیید گردد. به هرحال، سرویس گیرنده های ایمیل می توانند برای داشتن قابلیت تأیید امضاء، تغییر داده شوند و براساس نتایج بررسی و سیاست هایشان، در مورد ایمیل های دریافتی تصمیم گیری کنند.

25- Bluetooth

تهیه کننده :سید حمید یاریان

نوع ساده ای از ارتباط شبکه های بی سیم است که حداکثر ارتباط **8** دستگاه را با تکنولوژی **Bluetooth**پشتیبانی می کند دستگاههایی از قبیل **PDA** ، نوت بوک ، تلفن های همراه و کامپیوترهای شخصی از جمله این موارد هستند اگرچه این تکنولوژی ممکن است در صفحه کلیدها ،موس ها و **Headset** و **Hands-free** تلفن های همراه نیز دیده شود این تکنولوژی در سال **1994** توسط شرکت اریکسون ایجاد شد در سال **1998** تعداد کوچکی از کمپانیهای مشهور مانند اریکسون ،نوکیا ، اینتل و توشیبا استفاده شد . بلوتوس در فواصل کوتاهی بین **9** تا **90** متر کار می کنند این فاصله پشتیبانی به امنیت این تکنولوژی می افزاید .چرا که اگر کسی بخواهد ارتباط شما را شنود کند گر چه به ابزار خاصی نیاز ندارد اما بایستی در فاصله نزدیکی از شما قرار بگیرد مهمتری ویژگی بلوتوس این است که بر خلاف **Infrared** موانعی مانند دیوار تاثیری بر روی سیگنال آن ندارند از تکنولوژی رادیوئی استفاده کرده که خیلی گران نبوده و مصرف برق خیلی کمی دارد .

26- آینده Wireless

نسل سوم شبکه ها(۳ G) نسل آینده شبکه های **Wireless** نام گذا ری شده است. سیستم های۳ G کمک می کنند تا صدا و تصویر و داده را با کیفیت مناسب و با سرعت هر چه بیشتر انتقال دهیم . پیش بینی IDC بر ای کاربردی شدن G 3 سال ۲۰۰۴ می باشد و تا آن موقع در حدود ۲۹ میلیون کاربر mobile commerce (m commerce) در آمریکا وجود خواه د داشت . از طرفی IBM (بزرگترین شرکت سخت افزاری جها ن) معتقد است که بازار کلی تجهیزات در سال ۲۰۰۳ به رقم ی بالغ بر ۸۳ بیلیون دلار خواهد رسید.

تهیه کننده :سید حمید یاریان

نمونه ای از پیشرفت تکنولوژی به روایت طنز

27- رمزنگاری

۱-27 - معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست .یک هنر قدیمی است و برای قرنها بمنظورمحافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می شده، استفاده شده است تا پیغامهای آنها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و درضمن باید از عدم تغییر محتوای پیغام مطمئن شویم .این سه موضوع یعنی

تهیه کننده :سید حمید یاریان

محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند ومی توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند .روشی که تامین کننده این مساله باشد" رمزنگاری "نام دارد .رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند . رمزنگاری مخفف ها و اصطلاحات مخصوص به خود را دارد .برای درک عمیق تر به مقداری ازدانش ریاضیات نیاز است.برای محافظت ازدیتای اصلی که بعنوان**plaintext** شناخته می شود آنرا با استفاده از یک کلید) رشته ای محدود از بیتها بصورت رمز در می آوریم تا کسی که دیتای حاصله را می خواند قادر به درک آن نباشد.

(که بعنوان**ciphertext** شناخته می شود)بصورت یک سری بی معنی از دیتای رمزشده بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می رسد .برای حصول متن اولیه دریافت کننده آنرا رمزگشایی می کند .یک شخص ثالث) مثلا یک هکر (می تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمز نوشته**(cryptanalysis)** کند.بخاطرداشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید .الگوریتم یک مبدل یا فرمول ریاضی است .تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده اند .کلید، یک رشته از ارقام دودویی) صفر و یک (است که بخودی خود بی معنی است .رمزنگاری مدرن فرض می کند که الگوریتم شناخته شده

است یا می تواند کشف شود .کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده سازی تغییر می کند .رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچینی می شود؛ این عمل عموما بعنوان **scrambling** شناخته می شود، .بصورت مشخص تر **hash function** ها بلوکی از دیتا را)که می تواند هر اندازه ای داشته باشد (به طول از پیش مشخص شده کاهش می دهد.البته دیتای اولیه نمی تواند از **hashed value** بازسازی شود **Hash function** ها اغلب بعنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه ای از پیام) شامل مهم ترین قسمتها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا (قبل از رمزنگاری خود پیام، ساخته و **hash** می شود .

یک چک تایید پیام **(Message Authentication Check)** یا **MAC** یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است .هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است .هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می شود، منجر به ایجاد امضای دیجیتال **(digital signature)**می شود .

27- ۲ -الگوریتم ها

طراحی الگوریتمهای رمزنگاری مقوله ای برای متخصصان ریاضی است .طراحان سیستمهایی که در آنها از رمزنگاری استفاده می شود، باید از نقاط قوت و ضعف

الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم گیری داشته باشند .اگرچه رمزنگاری از اولین کارهای شانون(Shannon) در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده اند . بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری عملی و در سیستمهای برپایه کارت هوشمند بسیار کم است.

27-2-1- سیستمهای کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می کند .بیشترین شکل استفاده از رمزنگاری که در کارتهای هوشمند و البته در بیشتر سیستمهای امنیت اطلاعات وجود داردdata encryption algorithm یاDEA است که بیشتر بعنوان . DES شناخته می شودDES یک محصول دولت ایالات متحده است که امروزه بطور وسیعی بعنوان یک استاندارد بین المللی شناخته می شود .بلوکهای ۶۴ بیتی دیتا توسط یک کلید تنها که معمولا ۵۶ بیت طول دارد، رمزنگاری و رمزگشایی می شوند.DES از نظر محاسباتی ساده است و براحتی می تواند توسط پردازند ههای کند) بخصوص آنهایی که در کارتهای هوشمند وجود دارند (انجام گیرد.

این روش بستگی به مخفی بودن کلید دارد .بنابراین برای استفاده در دو موقعیت مناسب است :هنگامی که کلیدها می توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می شوند که قبلا هویت یکدیگر

را تایید کرده اند عمر کلیدها بیشتر از مدت تراکنش طول نمی کشد .رمزنگاریDES عموما برای حفاظت دیتا از شنود در طول انتقال استفاده می شود .کلیدهایDES ۴۰ بیتی امروزه در عرض چندین ساعت توسط کامپیوترهای معمولی شکسته می شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود .کلید ۵۶ بیتی عموما توسط سخت افزار یا شبکه های بخصوصی شکسته می شوند رمزنگاری DES سه تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می گیرد) .دو مرتبه با استفاده از یک کلید به سمت جلو(رمزنگاری)و یک مرتبه به سمت عقب (رمزگشایی)با یک کلید دیگر. این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعدا خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است. الگوریتمهای استاندارد جدیدتر مختلفی پیشنهاد شده اند .الگوریتمهایی مانند BlowfishوIDEA برای زمانی مورد استفاده قرار گرفته اند اما هیچکدام پیاده سازی سخت افزاری نشدند بنابراین بعنوان رقیبی برایDES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده اند .پروژه استاندارد رمزنگاری پیشرفته دولتی ایالات متحده(AES) الگوریتمRindael را برای جایگزیتی DES بعنوان الگوریتم رمزنگاری اولیه انتخاب کرده است .الگوریتمTwofish مشخصا برای پیاده سازی در پردازنده های توان پایین مثلا در کارتهای هوشمند طراحی شد.

در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتمهاSkipjack و مبادله کلید را که در کارتهایFortezza استفاده شده بود، از محرمانگی خارج سازد .یکی از دلایل این امر تشویق برای پیاده سازی بیشتر کارتهای هوشمند برپایه این الگوریتمها بود .برای تهیه کننده :سید حمید یاریان

رمزنگاری جریانی **(streaming encryption)** (که رمزنگاری دیتا در حین ارسال صورت می گیرد بجای اینکه دیتای کدشده در یک فایل مجزا قرار گیرد (الگوریتم **RC4** سرعت بالا و دامنه ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می کند. **RC4** که متعلق به امنیت دیتای **RSA** است، بصورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می شود.

27-2-2- سیستمهای کلید نامتقارن

سیستمهای کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می کنند .بسیاری از سیستمها اجازه می دهند که یک جزء(کلید عمومی یا**public key**) منتشر شود در حالیکه دیگری(کلید اختصاصی یا**private key**) توسط صاحبش حفظ شود .فرستنده پیام، متن را با کلید عمومی گیرنده کد می کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری میکند .بعبارتی تنها با کلید اختصاصی گیرنده می توان متن کد شده را به متن اولیه صحیح تبدیل کرد .یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده ای بجز گیرنده مورد نظر فرستنده بی معنی خواهد بود .معمولترین سیستم نامتقارن بعنوان **RSA** شناخته می شود(حروف اول پدیدآورندگان آن یعنی**Rivest, Shamir** و**Adlemen** است .)اگرچه چندین طرح دیگر وجود دارند . می توان از یک سیستم نامتقارن برای نشاندادن اینکه فرستنده پیام همان شخصی است

که ادعا می کند استفاده کرد که این عمل اصطلاحا امضاء نام داردRSA شامل دو تبدیل است که هرکدام احتیاج به بتوان رسانی ماجولار با توانهای خیلی طولانی دارد:

امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می کند؛

رمزگشایی عملیات مشابه ای روی متن رمزشده اما با استفاده از کلید عمومی است .برای تایید امضاء بررسی می کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر اینگونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده تر چنانچه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است .حال اگر متن رمزشده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشاندهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می شود .افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمز شده نیستند بطوریکه با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستمRSA این فرمول است: $X = Yk \pmod r$

که Xمتن کد شده Y متن اصلی k کلید اختصاصی و r حاصلضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده اند .برای اطلاع از جزئیات بیشتر می توان به مراجعی که در این زمینه وجود دارد رجوع کرد .این شکل محاسبات روی پردازنده های بایتی بخصوص روی ۸ بیتی ها که در کارتهای هوشمند استفاده می شود بسیار کند است .

تهیه کننده :سید حمید یاریان

بنابراین، اگرچه **RSA** هم تصدیق هویت و هم رمزنگاری را ممکن می سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارتهای هوشمند استفاده می شود و برای نشاندادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می شود. سایر سیستمهای کلید نامتقارن شامل سیستمهای لگاریتم گسسته می شوند مانند **Diffie-Hellman** , **ElGamal** و سایر طرحهای چندجمله ای و منحنی های بیضوی .بسیاری از این طرحها عملکردهای یک طرفه ای دارند که اجازه تاییدهویت را می دهند اما رمزنگاری ندارند .یک رقیب جدیدتر الگوریتم **RPK** است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می کند **RPK** یک پروسه دو مرحله ای .است :بعد از فاز آماده سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی)رشته هایی از دیتا بطور استثنایی کاراست و می تواند براحتی در سخت افزارهای رایج پیاده سازی شود .بنابراین بخوبی با رمزنگاری و تصدیق هویت در ارتباطات سازگار است .طولهای کلیدها برای این طرحهای جایگزین بسیار کوتاهتر از کلیدهای مورد استفاده در **RSA** است که آنها برای استفاده در چیپ کارتها مناسب تر است .اما **RSA** محکی برای ارزیابی سایر الگوریتمها باقی مانده است؛ حضور و بقای نزدیک به سه دهه از این الگوریتم، تضمینی در برابر ضعفهای عمده بشمار می رود.

27-3-کلیدها در رمزنگاری

با روشن شدن اهمیت وجود کلیدها در امنیت داده ها، اکنون باید به انواع کلیدهای موجود و مکان مناسب برای استفاده هر نوع کلید توجه کنیم.

3-1- کلیدهای محرمانه(Secret keys)

الگوریتمهای متقارن مانندDES از کلیدهای محرمانه استفاده می کنند؛ کلید باید توسط دو طرف تراکنش منتقل و ذخیره شود .چون فرض بر این است که الگوریتم شناخته شده و معلوم است، این قضیه اهمیت امن بودن انتقال و ذخیره کلید را مشخص می سازد . کارتهای هوشمند معمولا برای ذخیره کلیدهای محرمانه استفاده می شوند .در این حالت تضمین اینکه قلمرو کلید محدود است، مهم است :باید همیشه فرض کنیم که یک کارت ممکن است با موفقیت توسط افراد غیرمجاز تحلیل گردد، و به این ترتیب کل سیستم نباید در مخاطره قرار گیرد.

27-3-2- کلیدهای عمومی و اختصاصی (Public and private keys)

امتیاز اصلی و مهم سیستمهای کلید نامتقارن این است که آنها اجازه می دهند که یک کلید) کلید اختصاصی (با امنیت بسیار بالا توسط تولید کننده آن نگهداری شود در حالیکه کلید دیگر) کلید عمومی (می تواند منتشر شود .کلیدهای عمومی می توانند همراه پیامها فرستاده شوند یا در فهرستها لیست شوند(شروط و قوانینی برای کلیدهای عمومی در طرح فهرست پیام رسانی الکترونیکی ITU X. ۵۰۰ وجود دارد)، و از یک شخص به شخص بعدی داده شوند .مکانیسم توزیع کلیدهای عمومی می تواند رسمی

)یک مرکزتوزیع کلید (یا غیررسمی باشد .محرمانگی کلید اختصاصی در چنین سیستمی مهمترین مساله است؛ باید توسط ابزار منطقی و فیزیکی در کامپیوتری که ذخیره شده، محافظت گردد .کلیدهای اختصاصی نباید هرگز بصورت رمزنشده در یک سیستم کامپیوتر معمولی یا بشکلی که توسط انسان قابل خواندن باشد، ذخیره شوند .در اینجا نیز کارت هوشمند برای ذخیره کلیدهای اختصاصی یک فرد قابل استفاده است، اما کلیدهای اختصاصی سازمانهای بزرگ معمولا نباید در یک کارت ذخیره شود.

27-3-3- کلیدهای اصلی و کلیدهای مشتق شده (Master keys and derivedkeys)

یک روش کاستن از تعداد کلیدهایی که باید منتقل و ذخیره شوند، مشتق گرفتن از آنهاست هر زمانی که استفاده می شوند .در یک برنامه اشتقاق کلید، یک کلید اصلی همراه با چند پارامتر مجزا برای محاسبه کلید مشتق شده استفاده می شود که بعدا برای رمزنگاری استفاده می گردد .برای مثال، اگر یک صادرکننده با تعداد زیادی کارت سروکار دارد، می تواند برای هر کارت، با استفاده از کلید اصلی، شماره کارت را رمز کند و به این ترتیب کلید مشتق شده حاصل می شود و به آن کارت اختصاص داده می شود.

شکل دیگری از کلیدهای مشتق شده با استفاده ازtoken ها که محاسبه گرهای الکترونیکی با عملکردهای بخصوص هستند، محاسبه می شوند .آنها ممکن است بعنوان ورودی از یک مقدار گرفته شده از سیستم مرکزی، یکPIN وارد شده توسط کاربر و تاریخ و زمان استفاده کنند .خودtoken شامل الگوریتم و یک کلید اصلی است .چنینی token هایی اغلب برای دسترسی به سیستمهای کامپیوتری امن استفاده می شوند .

تهیه کننده :سید حمید یاریان

3-4-27 -کلیدهای رمزکننده کلید (keys Key-encrypting)

از آنجا که ارسال کلید یک نقطه ضعف از نظر امنیتی در یک سیستم بشمار می رود، رمزکردن کلیدها هنگام ارسال و ذخیره آنها بشکل رمزشده منطقی بنظر می رسد . کلیدهای رمزکننده کلید هرگز به خارج از یک سیستم کامپیوتری) یا کارت هوشمند (ارسال نمی شوند و بنابراین می توانند آسانتر محافظت شوند تا آنهایی که ارسال می شوند .اغلب الگوریتم متفاوتی برای تبادل کلیدها از آنچه که برای رمزکردن پیامها استفاده می شود، مورد استفاده قرار می گیرد. از مفهوم دامنه کلید (domain key) برای محدود کردن میدان کلیدها و محافظت کردن کلیدها در دامنه شان استفاده می کنیم .معمولا یک دامنه، یک سیستم کامپیوتری خواهد بود که می تواند بصورت فیزیکی و منطقی محافظت گردد .کلیدهای استفاده شده در یک دامنه توسط یک کلید رمزکننده کلید محلی ذخیره می شوند.هنگامی که کلیدها می خواهند به یک سیستم کامپیوتری دیگر فرستاده شوند، رمزگشایی و تحت یک کلید جدید رمز می شوند که اغلب بعنوان کلید کنترل ناحیه (key zone control) شناخته می شوند .با دریافت این کلیدها در طرف دیگر، تحت کلید محلی سیستم جدید رمز می شوند .بنابراین کلیدهایی که در دامنه های یک ناحیه قرار دارند از دامنه ای به دامنه دیگر بصورتی که بیان گردید منتقل می شوند.

3-5-27 -کلیدهای نشست (keys Session)

برای محدودکردن مدت زمانی که کلیدها معتبر هستند، اغلب یک کلید جدید برای هر نشست یا هر تراکنش تولید می شود .این کلید ممکن است یک عدد تصادفی تولید

شده توسط ترمینالی باشد که در مرحله تصدیق کارت قرار دارد باشد .اگر کارت قادر به رمزگشایی روش کلید عمومی باشد، یعنی کلید نشست می تواند با استفاده از کلید عمومی کارت رمز شود. بخشی از تراکنش که در آن کلید منتقل می شود اغلب در مقایسه با بقیه تراکنش کوتاهتر است؛ بنابراین بار اضافی این بخش نسبت به کل تراکنش قابل صرفنظر است .چنانچه بقیه تراکنش بسبب استفاده از کلید متقارن با بالاسری کمتری رمز شود، زمان پردازش برای فاز تایید هویت و انتقال کلید قابل پذیرش است .)توضیح اینکه روشهای رمز متقارن از نامتقارن بمراتب سریعتر هستند بنابراین می توان ابتدا یک کلید متقارن را با استفاده از روش نامتقارن انتقال داد و سپس از آن کلید متقارن برای انجام بقیه تراکنش استفاده کرد (.شکل خاصی از کلید نشست، سیستم انتقال کلید است که در برخی سیستمهای پرداخت الکترونیک و مبادله دیتای الکترونیک استفاده می شود .بدین صورت که در پایان هر تراکنش، یک کلید جدید منتقل می شود و این کلید برای تراکنش بعدی مورد استفاده قرار می گیرد.

27-4- رمزنگاری اطلاعات، حفاظت از اطلاعات حساس

گسترش و رشد بی سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است .امنیت اطلاعات یکی از مسائل مشترک شخصیت های حقوقی و حقیقی است .کاربران اینترنت در زمان استفاده از شبکه، اطلاعات حساس و مهمی را بدفعات ارسال و یا دریافت می دارند .اطمینان از عدم

دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات در اینترنت است .اطلاعات حساس که ما تمایلی به مشاهده آنان توسط دیگران نداریم، موارد متعددی را شامل می شود .برخی از اینگونه اطلاعات بشرح زیر می باشند:

- اطلاعات کارت اعتباری
- شماره های عضویت در انحمن ها
- اطلاعات خصوصی
- جزئیات اطلاعات شخصی
- اطلاعات حساس در یک سازمان
- اطلاعات مربوط به حساب های بانکی

تاکنون برای امنیت اطلاعات بر روی کامپیوتر و یا اینترنت از روش های متعددی استفاده شده است .ساده ترین روش حفاظت از اطلاعات نگهداری اطلاعات حساس بر روی محیط های ذخیره سازی قابل انتقال نظیر فلاپی دیسک ها است .متداولترین روش حفاظت اطلاعات، رمز نمودن آنها است .دستیابی به اطلاعات رمز شده برای افراد غیر مجاز امکان پذیر نبوده و صرفا "افرادیکه دارای کلید رمز می باشند، قادر به باز نمودن رمز و استفاده از اطلاعات می باشند .رمز نمودن اطلاعات کامپیوتر مبتنی بر علوم رمز نگاری است .استفاده از علم رمز نگاری دارای یک سابقه طولانی و تاریخی است .قبل از عصر اطلاعات، بیشترین کاربران رمزنگاری اطلاعات، دولت ها و مخصوصا "در موارد نظامی بوده است .سابقه رمز نمودن اطلاعات به دوران امپراطوری روم بر می گردد .امروزه اغلب

روش ها و مدل های رمزنگاری اطلاعات در رابطه با کامپیوتر بخدمت گرفته می شود . کشف و تشخیص اطلاعاتی که بصورت معمولی در کامپیوتر ذخیره و فاقد هر گونه روش علمی رمزنگاری باشند، براحتی و بدون نیاز به تخصصی خاص انجام خواهد یافت .اکثر سیستم های رمزنگاری اطلاعات در کامپیوتر به دو گروه عمده زیرتقسیم می گردند:

- رمزنگاری کلید - متقارن
- رمزنگاری کلید - عمومی

27-5- رمز نگاری کلید - متقارن

در روش فوق، هر کامپیوتر دارای یک کلید رمز) کد (بوده که از آن برای رمزنگاری یک بسته اطلاعاتی قبل از ارسال اطلاعات برروی شبکه و یا کامپیوتر دیگر،استفاده می نماید .دراین روش لازم است در ابتدا مشخص گردد که کدامیک از کامپیوترها قصد مبادله اطلاعاتی با یکدیگر را دارند، پس از مشخص شدن هر یک از کامپیوترها، در ادامه کلید رمز بر روی هر یک از سیستم ها می بایست نصب گردد .اطلاعات ارسالی توسط کامپیوترهای فرستنده با استفاده از کلید رمز، رمز نگاری شده وسپس اطلاعات رمز شده ارسال خواهند شد .پس از دریافت اطلاعات رمز شده توسط کامپیوترهای گیرنده،با استفاده از کلید رمز اقدام به بازگشائی رمز و برگرداندن اطلاعات بصورت اولیه و قابل استفاده خواهد شد .مثلا "فرض کنید پیامی را برای یکی از دوستان خود رمز و سپس ارسال می نمائید .شما برای رمز نگاری اطلاعات از روشی استفاده نموده اید که بر اساس آن هر یک از حروف موجود در متن پیام را به دو حرف بعد از خود تبدیل کرده

ايد .مثلا "حروفA موجود در متن پيام به حروفC و حروفB به حروف D تبديل می گردند .

پس از ارسال پيام رمز شده برای دوست خود، می بايست با استفاده از يک روش ايمن و مطمئن کليد رمز را نيز برای وی مشخص کرد .در صورتيکه گيرنده پيام دارای کليد رمز مناسب نباشد، قادر به رمز گشائی و استفاده از اطلاعات نخواهد بود .در چنين حالتی می بايست به دوست خود متذکر گرديد که کليد رمز،شيفت دادن هر حرف بسمت جلو و به اندازه دو واحد است ."گيرنده پيام با انجام عمليات معکوس قادر به شکستن رمز و استفاده از اطلاعات خواهد بود.

6-27- رمزنگاری کليد - عمومی

در روش فوق از ترکيب يک کليد خصوصی و يک کليد عمومی استفاده می شود .کليد خصوصی صرفا "متعلق به کامپيوتر فرستنده بوده و کليد عمومی توسط کامپيوتر فرستنده در اختيار هر يک از کامپيوترهائی که قصد برقراری ارتباط با يکديگر را دارند، گذاشته می شود .برای رمزگشائی يک پيام رمز شده، کامپيوتر می بايست از کليد عمومی که توسط فرستنده ارائه شده، بهمراه کليد خصوصی خود استفاده نمايد .يکی ازمتداولترين برنامه های رمزنگاری در اين رابطه (**Pretty Good Privacy** (**PGP**)است .با استفاده از **PGP** می توان هر چيز دلخواه را رمز نمود.

بمنظور پياده سازی رمزنگاری کليد، عمومی در مقياس بالا نظير يک سرويس دهنده وب، لازم است از رويکردهای ديگری در اين خصوص استفاده گردد ".امضای ديجيتال "يکی

از رویکردهای موجود در این زمینه است، یک امضای دیجیتالی صرفا "شامل اطلاعات محدودی بوده که اعلام می نماید، سرویس دهنده وب با استفاده و بکارگیری یک سرویس مستقل با نام" امضای مجاز"، امین اطلاعات است" .امضای مجاز "بعنوان یک میانجی بین دو کامپیوتر ایفای وظیف می نماید.

هویت و مجاز بودن هر یک از کامپیوترها برای برقراری ارتباط توسط سرویس دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد.یکی از متداولترین نمونه های پیاده سازی شده از رمزنگاری کلید -عمومی، روشSSL (Secure Sokets Layer) است .روش فوق در ابتدا توسط" نت اسکیپ"پیاده سازی گردید SSL یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس دهندگان وب بمنظور ارسال اطلاعات حساس، استفاده می گرددSSL اخیرا "بعنوان .بخشی از پروتکل Transport Layer(TLS) Securityدر نظر گرفته شده است.

در مرورگر می توان زمان استفاده از یک پروتکل ایمن نظیزTLS را با استفاده از روش های متعدد اعلام کرد .استفاده از پروتکل "http"درعوض پروتکل "https" یکی از روش های موجود است .در چنین مواردی در بخش وضعیت پنجره مرورگر یک"Padlock" نشان داده خواهد شد.

.

رمزنگاری کلید - عمومی، مدت زمان زیادی را صرف انجام محاسبات می نماید .بنابراین در اکثر سیستمها از ترکیب کلید عمومی و متقارن استفاده می گردد .زمانیکه دو کامپیوتر یک ارتباط ایمن را بایکدیگر برقرار می نمایند، یکی از کامپیوترها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید – عمومی، ارسال خواهد کرد .در ادامه دو کامپیوتر قادر به برقرار ارتباط بکمک رمزنگاری کلید متقارن می باشند .پس از اتمام ارتباط، هر یک از کامپیوترها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد، می بایست مجددا "فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن) . .

27-7- مقدارHash

رمزنگاری مبتنی بر کلید عمومی بر پایه یک مقدارhash استوار است .مقدار فوق، بر اساس یک مقدار ورودی که دراختیار الگوریتمhashing گذاشته می گردد، ایجاد می گردد .در حقیقت مقدارhash فرم خلاصه شده ای از مقدار اولیه ای خود ، است . بدون آگاهی از الگوریتم استفاده شده تشخیص عدد ورودی اولیه بعید بنظر می رسد . مثال زیر نمونه ای در این زمینه را نشان می دهد:

عدد ورودی	الگوریتم	مقدارHASH
10,667	Input # x 143	1,525,381

27-8- Hash عدد ورودی الگوریتم مقدار

تسخیص اینکه عدد 1,525,381 (مقدار **hash**)از ضرب دو عدد ۶۶۷,۱۰ و ۱۴۳ بدست آمده است، کار بسیار مشکلی است .در صورتیکه بدانیم که یکی از اعداد ۱۴۳ است، تشخیص عدد دوم کار بسیار ساده ای خواهد بود (.عدد ۶۶۷,۱۰) رمز نگاری مبتنی بر کلید عمومی بمراتب پیچیده تر از مثال فوق می باشند .مثال فوق صرفا "ایدهاولیه در این خصوص را نشان می دهد .کلیدهای عمومی عموما "از الگوریتم های پیچیده و مقادیر**Hash** بسیار بزرگ برای رمزنگاری استفاده می نمایند .در چنین مواردی اغلب از اعداد ۴۰ و یا حتی ۱۲۸ بیتی استفاده می شود .یک عدد ۱۲۸ بیتی دارای ۲۱۲۸ حالت متفاوت است .

آیا شما معتبر هستید ؟

همانگونه که در ابتدای بخش فوق اشاره گردید، رمزنگاری فرآیندی است که بر اساس آن اطلاعات ارسالی از یک کامپیوتر برای کامپیوتر دیگر، در ابتدا رمز و سپس ارسال خواهند شد .کامپیوتر دوم(گیرنده) ، پس از دریافت اطلاعات می بایست، اقدام به رمزگشائی آنان نماید .یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات توسط یک منبع ایمن و مطمئن، استفاده از روش معروف "اعتبارسنجی"است .در صورتیکه اطلاعات" معتبر "باشند، شما نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهید آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییر پیدا نکرده اند .با ترکیب فرآیندهای رمزنگاری و اعتبار سنجی می

توان یک محیط ایمن را ایجاد کرد .بمنظور بررسی اعتبار یک شخص و یا اطلاعات موجود بر روی یک کامپیوتر از روش های متعددی استفاده می شود:

- رمز عبور . استفاده از نام و رمز عبور برای کاربران، متداولترین روش" اعتبار سنجی "است . کاربران نام و رمز عبور خود را در زمان مورد نظر وارد و در ادامه اطلاعات وارد شده فوق، بررسی می گردند .در صورتیکه نام و یا رمز عبور نادرست باشند، امکان دستیابی به منابع تعریف شده بر روی سیستم به کاربر داده نخواهد شد.
- کارت های عبور . این نوع کارت ها دارای مدل های متفاوتی می باشند .کارت های دارای لایه مغناطیسی) مشابه کارت های اعتباری (و کارت های هوشمند)دارای یک تراشه کامپیوتر است (نمونه هائی از کارت های عبور می باشند.
- امضای دیجتالی .امضای دیجیتالی، روشی بمنظور اطمینان از معتبر بودن یک سند الکترونیکی) نظیر :نامه الکترونیکی، فایل های متنی و (...است .استاندارد امضای دیجیتالیبر اساس نوع خاصی از رمزنگاری کلید عمومی و استفاده از الگوریتم امضای ،(**DSS**)ایجاد می گردد .الگوریتم فوق شامل یک کلید عمومی)شناخته شده (**DSA**) دیجیتالیتوسط صاحب اولیه سند الکترونیکی - امضاء کننده (و یک کلید عمومی است .کلیدعمومی دارای چهار بخش است .در صورتیکه هر چیزی پس از درج امضای دیجیتالی بهیک سند الکترونیکی، تغییر یابد، مقادیر مورد نظری که بر اساس آنها امضای دیجیتالی باآن مقایسه خواهد شد، نیز تغییر خواهند کرد.

سیستم های متعددی برای" اعتبار سنجی "تاکنون طراحی و عرضه شده است .اکثر سیستم های فوق از زیست سنجی برای تعیین اعتبار استفاده می نمایند .در علم زیست سنجی از اطلاعات زیست شناسی برای تشخیص هویت افراد استفاده می گردد .برخی از روش های اعتبار سنجی مبتنی بر زیست شناسی کاربران، بشرح زیر می باشند:

- پیمایش اثر انگشت (انگشت نگاری)
- پیمایش شبکیه چشم
- پیمایش صورت
- مشخصه صدا

یکی دیگر از مسائل مرتبط با انتقال اطلاعات، صحت ارسال اطلاعات از زمان ارسال و یا رمزنگاری است .می بایست این اطمینان بوجود آید که اطلاعات دریافت شده، همان اطلاعات ارسالی اولیه بوده و در زمان انتقال با مشکل و خرابی مواجه نشده اند .در این راستا از روش های متعددی استفاده می گردد:

- **Checksum**

یکی از قدیمی ترین روش های استفاده شده برای اطمینان از صحت ارسال اطلاعات است **Checksum**به دو صورت متفاوت محاسبه می گردد .. . فرض کنید **Checksum** یک بسته اطلاعاتی دارای طولی به اندازه یک بایت باشد، یک بایت شامل هشت بیت و هر بیت یکی از دو حالت ممکن) صفر و یا یک (را می تواند داشته باشد .در چنین حالتی ۲۵۶ وضعیت متفاوت می تواند وجود داشته باشد .با توجه به اینکه در اولین وضعیت، تمام هشت بیت مقدار صفر را دارا خواهند بود، می تواند حداکثر ۲۵۵ حالت متفاوت را ارائه نمود.

- **درصورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی، ۲۵۵ و یا کمتر باشد،**

مقدار Checksum شامل اطلاعات واقعی و مورد نظر خواهد بود .

- **در صورتیکه مجموع سایر بایت های موجود در بسته اطلاعاتی، بیش از ۲۵۵ باشد، Checksum معادل باقیمانده مجموع اعداد بوده مشروط بر اینکه آن را بر ۲۵۶ تقسیم نمائیم. مثال زیر، عملکرد CheckSum را نشان می دهد.**

cheCheckSum	Total	Byte 8	Byte 7	Byte 6	Byte 5	Byte 4	Byte 3	Byte 2	Byte 1T
12127	1,151	80	17179	15	244	135	54	2322232	2122122

- **1,151 / 256 = 4.496 (round to 4)**
- **4 x 256 = 1,0241,**
- **1,151 - 1,024 = 127**

- **CRC (Cyclic Redundancy Check) .روش CRC مفهوم مشابه روش Checksum است .روش فوق از تقسیم چند جمله ای برای مشخص کردن مقدار CRC استفاده می کند طول CRC عمولا "۱۶ و یا ۳۲ بیت است .صحت عملکرد روش فوق بسیار بالا است .در صورتیکه صرفا "یک بیت نادرست باشد CRC با مقدار مورد نظر مطابقت نخواهد کرد روش های Checksum و CRC امکانات مناسبی برای .پیشگیری از بروز خطای تصادفی درارسال اطلاعات می باشند، روش های فوق در رابطه با حفاظت اطلاعات و ایمن سازی اطلاعات در مقابل عملیات غیر مجاز بمنظور دستیابی و استفاده از اطلاعات، امکانات**

محدودتری را ارائه می نمایند .رمزنگاری متقارن و کلید عمومی، امکانات بمراتب مناسب تری در این زمینه می باشند .بمنظور ارسال و دریافت اطلاعات بر روی اینترنت و سایر شبکه های اختصاصی، از روش های متعدد ایمنی استفاده می گردد .ارسال اطلاعات از طریق شبکه نسبت به سایر امکانات موجود نظیر :تلفن، پست ایمن تر می باشد .برای تحقق امرفوق می بایست از روش های متعدد رمزنگاری و پروتکل های ایمنی بمنظور ارسال و دریافت اطلاعات در شبکه های کامپیوتری خصوصا "اینترنت استفاده می شود.

27-9- شکستن کلیدهای رمزنگاری

چه طول کلیدی در رمزنگاری مناسب است؟

امنیت هر الگوریتم مستقیماً به پیچیده بودن اصولی مربوط است که الگوریتم براساس آن بنا شده است .امنیت رمزنگاری بر اساس پنهان ماندن کلید است نه الگوریتم مورد استفاده .در حقیقت، با فرض اینکه که الگوریتم از قدرت کافی برخوردار است)یعنی که ضعف شناخت هشده ای که بتوان برای نفوذ به الگوریتم استفاده کرد، وجود نداشته باشد (تنها روش درک متن اصلی برای یک استراق سمع کننده، کشف کلید است. در بیشتر انواع حمله، حمله کننده تمام کلیدهای ممکن را تولید و روی متن رمزشده اعمال می کند تا در نهایت یکی از آنها نتیجه درستی دهد .تمام الگوریتمهای رمزنگاری در برابر این نوع حمله آسیب پذیر هستند، اما با استفاده از کلیدهای طولانی تر، می توان کار را برای حمله کننده مشکل تر کرد .هزینه امتحان کردن تمام کلیدهای ممکن با

تعداد بیتهای استفاده شده در کلید بصورت نمایی اضافه می شود، و این در حالیست که انجام عملیات رمزنگاری و رمزگشایی بسیار کمتر افزایش می یابد.

27-9-1- الگوریتمهای متقارن

DES که یک الگوریتم کلید متقارن است معمولا از کلیدهای ۶۴ بیتی برای رمزنگاری و رمزگشایی استفاده می کند .الگوریتم متن اولیه را به بلوکهای ۶۴ بیتی می شکند و آنها رایکی یکی رمز می کند.

DES ۳ الگوریتم پیشرفته تر است و در آن الگوریتم**DES** سه بار اعمال می شود (در مقاله رمزنگاری به آن اشاره شده است) .نسخه دیگری از این الگوریتم (پایدار تر از قبلیها) از کلیدهای ۵۶ بیتی و با فضای کلید موثر ۱۶۸ بیت استفاده می کند و سه بار عملیات رمزنگاری را انجام می دهد.

جدول زیر زمان لازم برای یافتن کلید در الگوریتم**DES** را نشان میدهد.

طول کلید	تعداد کلیدهای ممکن	زمان مورد نیاز برای ۱رمزگشایی در هر میلی ثانیه	زمان مورد نیاز برای 1,000,000رمزگشایی در هر میلی ثانیه
۳۲ بیت	۱۰۹ × ۴/۳ =۲۳۲	۸ /۳۵ دقیقه = ۲۳۱ میلی ثانیه	2/15میلی ثانیه
۵۶ بیت	۱۰۱۶ × ۷/۲ =۲۵۶	۱۴۲ سال = ۲۵۵ میلی ثانیه	۱۰ ساعت
۱۲۸ بیت	۱۰۳۸ × ۳/۴ =۲۱۲۸	۱۰۲۴×۴/۵ سال = ۲۱۲۷ میلی ثانیه	18 10*5/4 سال
۱۶۸ بیت	۱۰۵۰ × ۳/۷ =۲۱۶۸	36 10*5/9 سال = ۲۱۶۷ میلی ثانیه	30 10*5/9 سال

ستون سوم مربوط به کامپیوترهایی است که می توانند در هر میلی ثانیه یک رمزگشایی را انجام دهند که برای کامپیوترهای امروزی توان محاسباتی معقولی محسوب می شود . ستون آخر برای سیستمهای بسیار بزرگ محاسباتی است بطوریکه قدرت پردازش یک میلیون برابر زیاد شده باشد .بدون در نظر گرفتن طول کلید، الگوریتمهای متقارن قوی نیز نمی توانند امنیت الگوریتمهای نامتقارن را داشته باشند، زیرا کلید باید بین دو طرف ارتباط مبادله شود.

27-9-2-الگوریتمهای نامتقارن

عموماً سیستمی امن محسوب می شود که هزینه شکستن آن بیشتر از ارزش دیتایی باشد که نگهداری می کند .اما در ذهن داشته باشید که با افزایش قدرت محاسباتی، سیستمهای رمزنگاری، آسانتر توسط روشهای سعی و خطا مورد حمله قرار خواهند گرفت. برای مثال، طبق گزارشی از سایت **RSA**، تخمین زده می شود که یک کلید ۲۱۵ بیتی می تواند با هزینه ای کمتر از ۱ میلیون دلار و یک تلاش ۸ ماهه شکسته شود **RSA**توصیه میکند که کلیدهای ۲۱۵ بیتی در حال حاضر امنیت کافی ایجاد نمی کنند و باید بنفع کلیدهای ۸۶۷ بیتی برای استفاده های شخصی کنار بروند !به همین ترتیب برای استفاده شرکتها کلیدهای ۱۰۲۴ بیتی و از ۲۰۴۸ بیت برای کلیدهای فوق العاده ارزشمند استفاده شود .البته پیش بینی شده است که این مقادیر تا حداقل سال ۲۰۰۴ معتبر خواهد بود .با پیشرفتهای موجود احتمالا در این زمان نیاز به افزودن بر طول کلید ها خواهد بود .جدول زیر نشاندهنده افراد یا گروههایی است که توانایی شکستن کلیدها با طولهای متفاوت را دارند.

تهیه کننده :سید حمید یاریان

طول کلید	نفوذگران بالقوه
۲۵۶ بیتی	افراد عادی
۳۸۴ بیتی	گروههای تحقیق دانشگاهی و شرکتها
۵۱۲ بیتی	گروههای دولتی با تمام امکانات
۷۶۸ بیتی	امن برای کوتاه مدت
۱۰۲۴ بیتی	امن تا آینده نزدیک
۲۰۴۸	امن احتمالا تا چند ده سال !

27-10- پروتکل های انتقال فایل امن

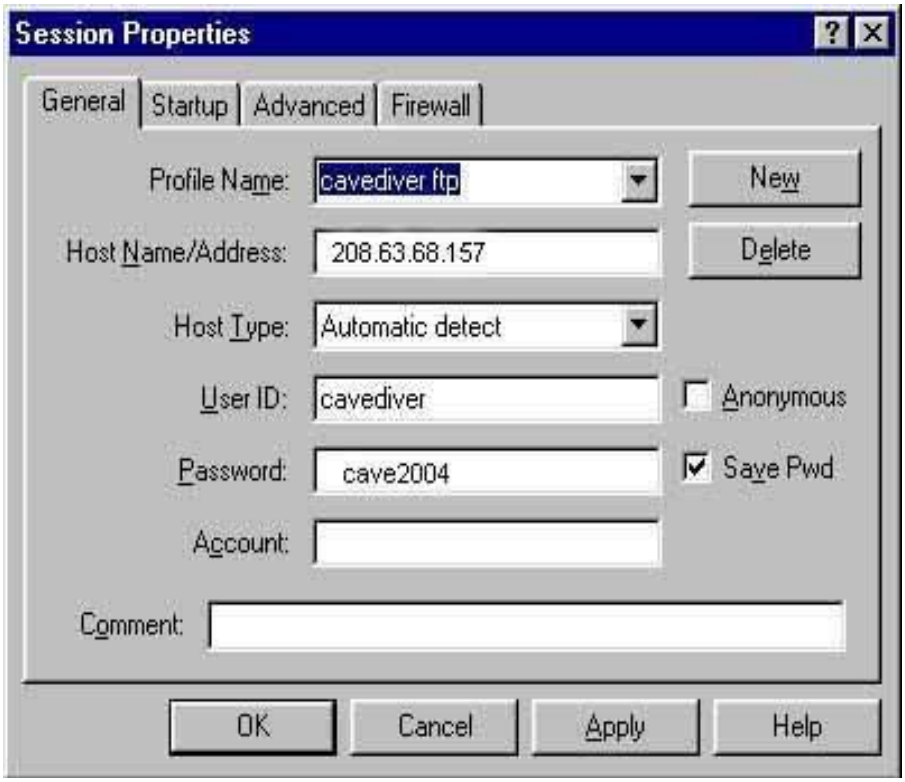
در این قسمت برای شما بطور مختصر از پروتکل هایی خواهیم گفت که امکان**FT** یا (**File Transfer**یا انتقال فایل را فراهم می آورند یا از بلوکهای سازنده پروتکل های ذکر شده در مقاله رمزنگاری در پروتکل های انتقال استفاده می کنند تا امکان**FT** امن را ایجاد کنند .درحالیکه پروتکلهای ذکر شده در مقاله مذکور سیستمهای امنیتی عمومی هستند که قابل کاربرد برای**FT** نیز هستند، آنچه در اینجا اشاره می شود، مشخصاً برای **FT**ایجاد شده اند :

27-10-1- AS2

AS۲ (Applicability Statement 2) گونه ای (Electronic Date EDI Exchange) یا تبادل دیتای الکترونیکی (اگرچه به قالبهای EDI محدود نشده) برای استفاده های تجاری با استفاده از HTTP است AS 2 در حقیقت بسط یافته نسخه قبلی یعنی AS1 است AS2 چگونگی تبادل دیتای تجاری را بصورت امن و مطمئن با استفاده از HTTP بعنوان پروتکل انتقال توصیف می کند .دیتا با استفاده از انواع محتوایی MIME استاندارد که , EDI EDI XML دیتای باینری و هر گونه دیتایی را که قابل توصیف در MIME باشد، پشتیبانی می کند، بسته بندی می شود .امنیت پیام (تایید هویت و محرمانگی (با استفاده از S/MIME پیاده سازی می شود .AS1 در عوض از SMTP استفاده می کند . با AS2 و استفاده از HTTP یا HTTP/S با(SSL برای انتقال، ارتباط بصورت زمان حقیقی ممکن می شود تا اینکه از طریق ایمیل انجام گیرد .امنیت، تایید هویت، جامعیت پیام، و خصوصی بودن با استفاده از رمزنگاری و امضاهای دیجیتال تضمین می شود، که برپایه S/MIME هستند و نه SSL.استفاده از HTTP/S بجای HTTP استاندارد بدلیل امنیت ایجادشده توسط S/MIME کاملاً انتخابی است .استفاده از S/MIME اساس ویژگی دیگری یعنی انکارناپذیری را شکل می دهد، که امکان انکار پیام های ایجادشده یا فرستاده شده توسط کاربران را مشکل می سازد، یعنی یک شخص نمی تواند منکر پیامی شود که خود فرستاده است .

2-10-27- برای FT: (File Transfer)

AS۲ مشخصاً برای درکنارهم قراردادن ویژگیهای امنیتی با انتقال فایل یعنی تایید هویت، رمزنگاری، انکارناپذیری توسطS/MIME وSSL انتخابی، طراحی شده است .از آنجا که AS2یک پروتکل در حال ظهور است، سازمانها باید تولید کنندگان را به پشتیبانی سریع از آن تشویق کنند .قابلیت وجود انکارناپذیری در تراکنش های برپایهAS2از اهمیت خاصی برای سازمانهایی برخوردار است که می خواهند پروسه های تجاری بسیار مهم را به سمت اینترنت سوق دهند .وجود قابلیت برای ثبت تراکنش پایدار و قابل اجراء برای پشتبانی از عملکردهای بسیار مهم مورد نیاز است .AS۲ از MDN(Message Disposition Notification)بر پایهRFC 2298استفاده می کند. MDN (که می تواند در اتصال به سایر پروتکل ها نیز استفاده شود) بر اساس محتوای MIME است که قابل خواندن توسط ماشین است و قابلیت آگاه سازی و اعلام وصول پیام را بوجود می آورد، که به این ترتیب اساس یک ردگیری نظارتی پایدار را فراهم می سازد.

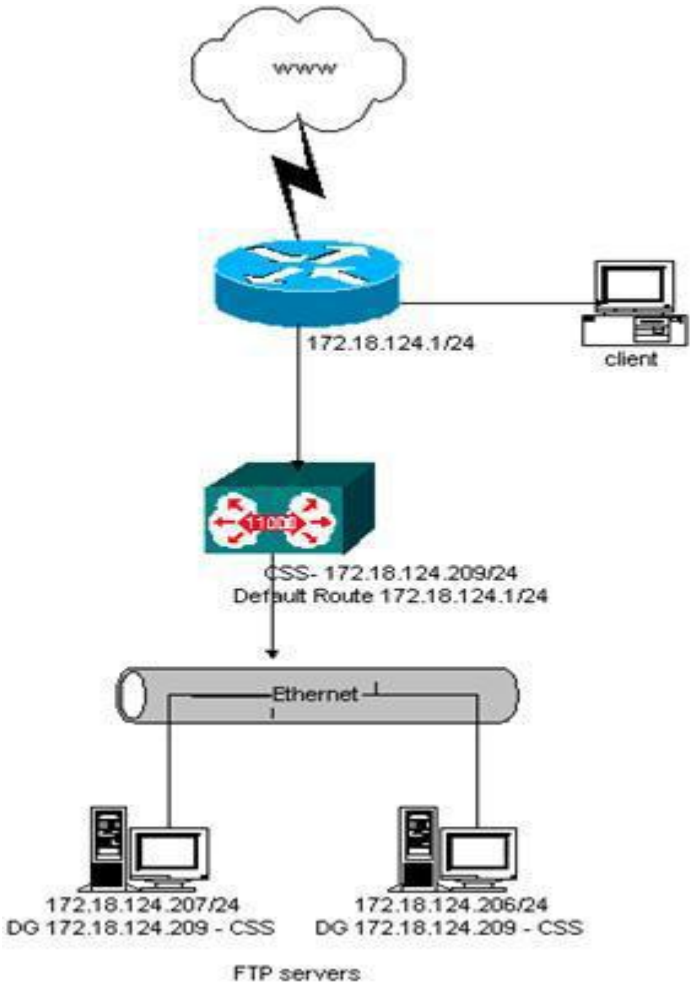


27-10-3- FTP (File Transfer Protocol)

FTP یا پروتکل انتقال فایل به منظور انتقال فایل از طریق شبکه ایجاد گشته است، اما هیچ نوع رمزنگاری را پشتیبانی نمی کند . FTPحتی کلمات عبور را نیز بصورت رمزنشده انتقال می دهد، و به این ترتیب اجازه سوءاستفاده آسان از سیستم را می دهد. بسیاری سرویس هاFTP بی نام را اجراء می کنند که حتی نیاز به کلمه عبور را نیز مرتفع می سازد (اگرچه در این صورت کلمات عبور نمی توانند شنیده یا دزدیده شوند)

27-10-4- برای FT :

FTPعنوان یک روش امن مورد توجه نیست، مگر اینکه درون یک کانال امن مانند **SSL** یا**IPSec** قرار گیرد .گرایش زیادی به**FTP** امن یا**FTP** بر اساس**SSL** وجود دارد (.می توانید به **SFTP**و**SSL** مراجعه کنید)



27-10-5- FTPS و SFTP

SFTP به استفاده از**FT** برروی یک کانال که با **SSH** امن شده، اشاره دارد، در حالیکه منظور از **FTPS** استفاده از**FT** بر روی **SSL** است .اگرچه**SFTP** دارای استفاده محدودی است،

FTPS (که هر دو شکلFTP روویSSL وFTP روی TLS را بخود می گیرد)نوید کارایی بیشتری را میدهد RFC 2228 ((FTPS رمزنگاری کانالهای دیتا را که برای ارسال تمام دیتا و کلمات عبور استفاده شده اند، ممکن می سازد اما کانالهای فرمان را بدون رمزنگاری باقی می گذارد) بعنوان کانال فرمان شفاف شناخته می شود . (مزیتی که دارد این است که به فایروالهای شبکه های مداخله کننده اجازه آگاهی یافتن از برقراری نشست ها و مذاکره پورتها را می دهد .این امر به فایروال امکان تخصیص پورت پویا را می دهد، بنابراین امکان ارتباطات رمزشده فراهم می شود بدون اینکه نیاز به این باشد که تعداد زیادی از شکاف های دائمی در فایروال پیکربندی شوند.

اگرچه معمول ترین کاربردهایFTP (مخصوصاً بسته های نرم افزاری کلاینت)هنوز کاملاً FTPS (FTP روی ، (SSLرا پشتیبانی نمی کنند و پشتیبانی مرورگر برای SSL برای استفاده کامل از مجموعه کامل فانکشن های RFC 2228 FTPSکافی نیست، اما این امر در حال پیشرفت است .بسیاری از تولیدکنندگان برنامه های کاربردی در حال استفاده از SSL استاندارد در کنارFTP استاندارد هستند .بنابراین، گرچه در بعضی موارد مسائل تعامل همچنان وجود دارند، اما امیدواری برای پشتیبانی گسترده ازFT امن در ترکیب با SSL وجود دارد(.و حتی امیدواری برای پذیرش گسترده مجموعه کامل فانکشنهای

RFC 2228 FTPS)

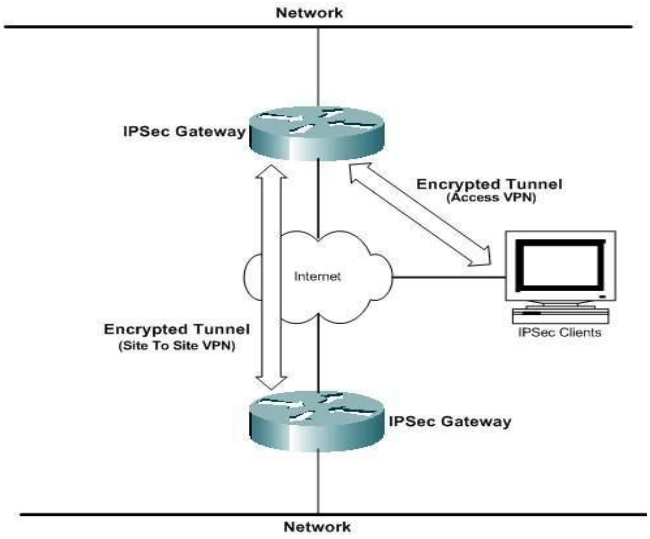
27-11- رمزنگاری در پروتکل های انتقال

تمرکز بیشتر روش های امنیت انتقال فایل بر اساس رمزنگاری دیتا در طول انتقال از طریق شبکه های عمومی مانند اینترنت است .دیتایی که در حال انتقال بین سازمانهاست بوضوح در معرض خطر ربوده شدن در هر کدام از محلها قرار دارد مثلا در شبکه های محلی برای هر یک از طرفین یا مرزهای **Internet-LAN**که سرویس دهندگان اینترنت از طریق آنها مسیر دیتا را تا مقصد نهایی مشخص می کنند .حساسیت دیتا ممکن است بسیار متغییر باشد، زیرا دیتای انتقالی ممکن است بهر شکلی از رکوردهای مالی بسته بندی شده تا تراکنش های مستقیم باشند .در بعضی موارد، ممکن است علاوه بر محافظت دیتا روی اینترنت، نیاز به محافظت دیتا روی **LAN**نیز باشد .مشخصاً، محافظت از دیتا در مقابل حملات**LAN** مستلزم رمزنگاری دیتای انتقالی روی خود**LAN** است .به این ترتیب، بهرحال، نیاز به بسط امنیت تا برنامه هایی است که خود دیتا را تولید و مدیریت می کنند، و تنها اطمینان به راه حلهای محیطی کفایت نمی کند و به این ترتیب بر پیچیدگی مسأله امنیت افزوده می شود.

27-11-1- پروتکل ها

اگرچه ثاب تشده است که رمزنگاری راه حل بدیهی مسائل محرمانگی است، اما سردرگمی در مورد دو نوع رمزنگاری) برنامه در مقابل شبکه (همچنان وجود دارد و بدلیل وجود پروتکلهای ارتباطی گوناگون است که نیازهای تعامل بیشتر آشکار می شود. (مانند**IPSec** ، **S/MIME**،**TLS** و**SSL**) ، اگرچه این پروتکلها قول تعامل را می دهند اما تعامل کامل بدلیل مستقل بودن محصولات پروتکلها در حال حاضر وجود ندارد.

آزمایشهایی در حال حاضر در حال انجام هستند که به حل شدن این مسائل کمک می کنند، اما کاربران باید مطمئن شوند که تعامل بین محصول انتخابیشان و محصولات سایر شرکای تجاری امری تثبیت شده است .پروتکل های ساده تر (**SSL/TLS** ، **IPSec** تا حدی پایین تر **S/MIME**) عموماً مسائل کمتری از نظر تعامل دارند.



27-11-2- پروتکل های رمزنگاری انتقال

با ترکیب توانایی ها برای تایید هویت توسط رمزنگاری متقارن و نامتقارن برای ممکن ساختن ارتباطات تاییدشده و رمزشده، این پروتکلها پایه های امنیت را فراهم می کنند. تقریباً تمام پروتکلها نیاز های جامعیت را پشتیبانی می کنند به طوری که محتویات ارتباطات نمی توانند تغییر یابند، اما بیشتر آنها از **Non-Repudiation**پشتیبانی نمی کنند و به این ترتیب امکان ایجاد رکوردهای پایداری را که هویت منبع را به محتوای پیام پیوند می دهند، ندارند. به این چند پروتکل به طور مختصر اشاره می شود:

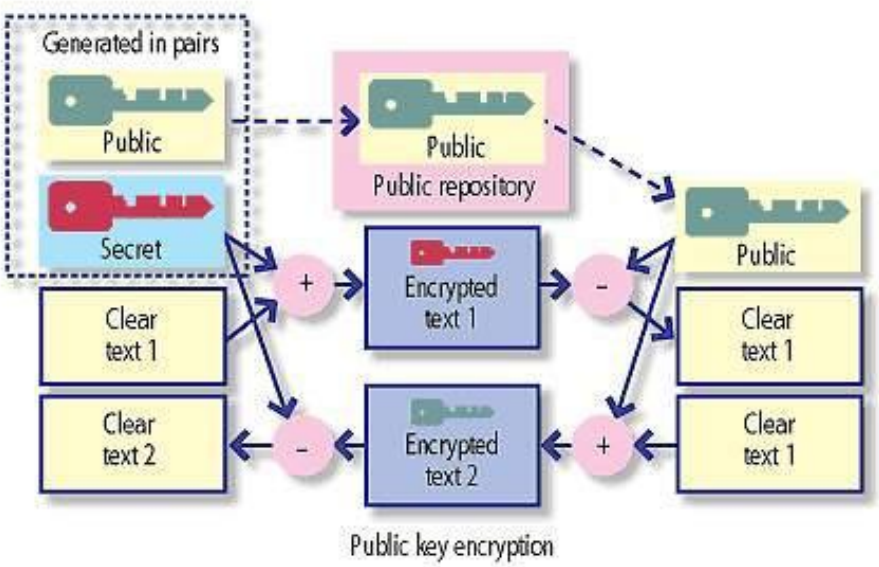
27-11-3- SSL

تکنولوژیSSL (Secure Socket Layer) اساس World Wide Web امن را تشکیل می دهدSSL که در مرورگرهای وب کاملاً جاافتاده است، توسط بسیاری از . سازمانها برای رمزنگاری تراکنش های وبی خود و انتقال فایل استفاده می شود .بعلاوه SSL بصورت روزافزون بعنوان یک مکانیسم امنیت در تلاقی با پروتکلهای پرشمار دیگر استفاده می شود و بهمین ترتیب ابزاری برای ارتباط سرورب هسرور امن است SSL ارتباطات رمزشده و بشکل آغازین خود تایید هویت سرور از طریق استفاده از گواهی را (در حالت کلاینت به سرور) پشتیبانی می کند .کاربران اغلب برای استفاده از برنامه ها از طریق کلمه عبور تایید هویت می شوند، و با پیشرفتSSL استاندارد(مثلا SSL V. 3.0) تایید هویت کلاینت از طریق گواهی به این پروتکل اضافه شده است.

27-11-4- برایFT (انتقال فایل):

ابزارFT اغلب ازSSL برای انتقال فایل در یکی از دو حالت استفاده می کنند .اولی، مد کلاینت به سرور است که کاربر را قادر می سازد، در حالیکه در حال استفاده از یک مرورگر وب استاندارد است مستندات را از یک سرور دریافت یا آنها را به سرور منتقل کند .که این قابلیت نیاز به نرم افزار مختص انتقال در کلاینت را برطرف می سازد و بسیار راحت است، اما اغلب فاقد بعضی ویژگیهای پیشرفته مانند نقاط آغاز مجدد و انتقالهای زمانبندی شده است که سازمانها نیاز دارند .SSL همچنین می تواند برای

اتصالات سروربه سرور امن – برای مثال، در اتصال باFTP و سایر پروتکلها – مورد استفاده قرار گیرد.



TLS -5-11-27

TLS (Transport Layer Security)، جانشینSSL، برپایه SSL 3. بنا شده است، اما به کاربران یک انتخاب کلید عمومی و الگوریتمهایHashing می دهد (الگوریتمهایHashing فانکشن های یک طرفه ای برای حفظ جامعیت پیامها هستند و توسط بیشتر پروتکلها استفاده می شوند.) اگرچه TLSو SSL تعامل ندارند، اما چنانچه یکی از طرفین ارتباط TLS را پشتیبانی نکند، ارتباط با پروتکل SSL 3.0 برقرار خواهد شد .بیشتر مزایا و معایبSSL به TLS هم منتقل می شود، و معمولا وجه تمایز خاصی وجود ندارد، و از همه نسخه ها به عنوانSSL یاد می شود .

S/MIME -6-11-27

S/MIME (Secure Multipurpose Internet Mail Extention) که اختصاصاً برای پیام رسانی ذخیره -و -ارسال طراحی شده است، بعنوان استاندارد امنیت ایمیل برتر شناخته شده است .مانند بیشتر پروتکل های رمزنگاری) مثلاSSL ، TLSوIPSec), S/MIME با رمزنگاری تنها سروکار ندارد .بهرحال، علاوه بر تصدیق هویت کاربران و ایمن سازی جامعیت پیامها (برای مثال مانند آنچهSSL انجام می دهدS/MIME) , توسط امضای دیجیتال، رکوردهای پایداری از صحت پیامها ایجاد می کند (ضمانت هویت فرستنده چنانچه به محتوای پیام مشخصی مرتبط شده .)این عمل باعث می شود فرستنده پیام نتواند ارسال آن را انکار کند.

27-11-7- برای FT :

سیستم های ایمیل رمزشده (با استفاده ازS/MIME) می توانند برای ارسال فایل های کوچک استفاده شوند) محدودیت حجم فایل بخاطر داشتن محدودیت حجم فایل در بیشتر سرورهای ایمیل است)، ولیS/MIME کلاً می تواند برای انتقال فایل های بزرگتر توسط پروتکلهای انتقال فایل استفاده شود.

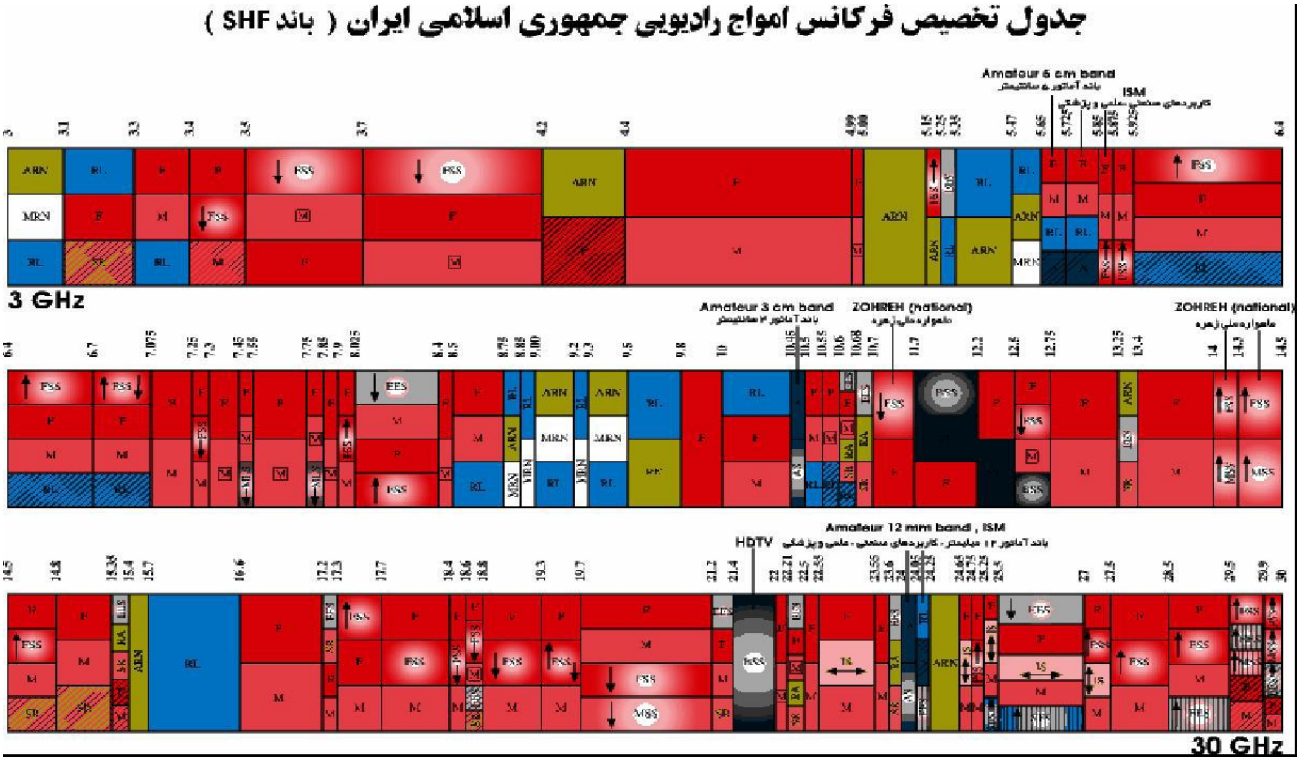
SSH-8-11-27

SSH (Secure Shell) هم یک برنامه و یک پروتکل شبکه بمنظور وارد شدن و اجرای فرمانهایی در یک کامپیوتر دیگر است .به این منظور ایجاد شد تا یک جایگزین رمز شده امن برای دسترسی های ناامن به کامپیوترهای دیگر مثلاrlogin یاtelnet باشد .

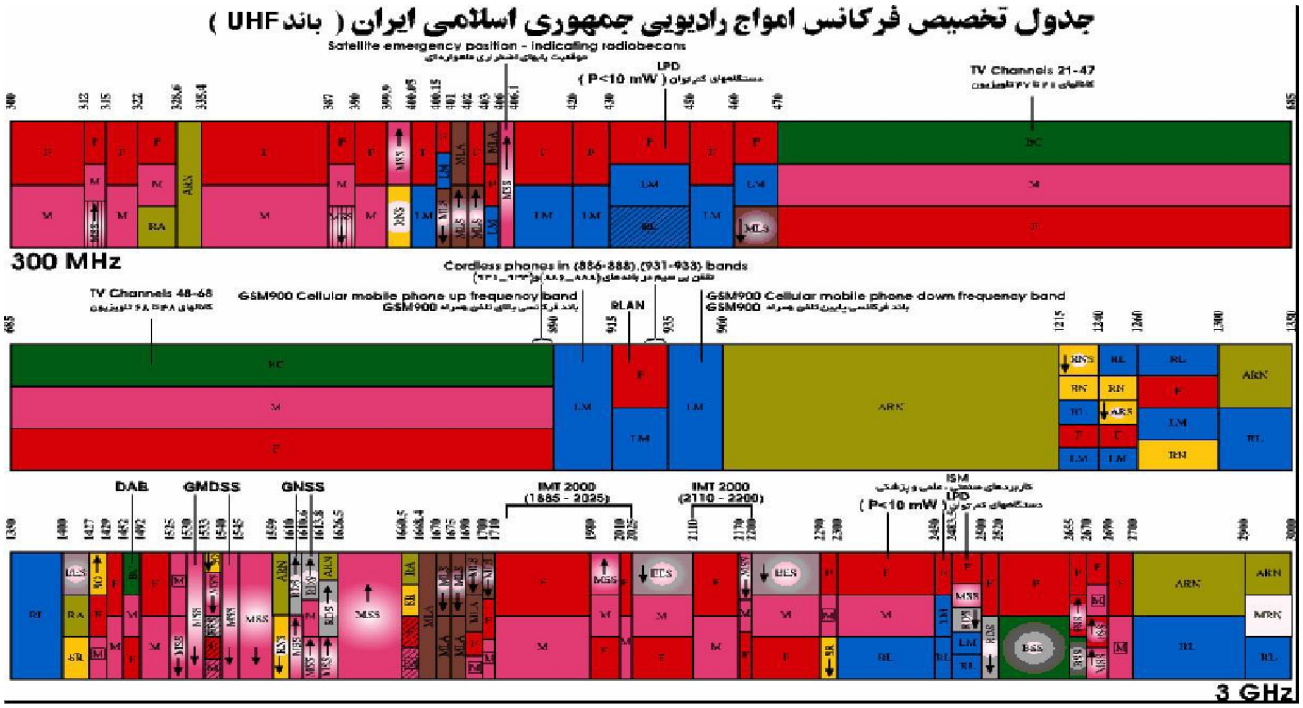
نسخه بعدی این پروتکل تحت نام**SSH 2**با قابلیتهایی برای انتقال فایل رمزشده از طریق لینک های**SSH** منتشر شد .

SSH می تواند برای پشتیبانی انتقال فایل رمزشده (به شکل **SFTP**) استفاده شود اما طبیعت خط فرمان بودن آن به این معنی است که بیشتر توسط مدیران سیستمها برای ارسال درون سازمان استفاده می شود تا برای انتقال فایل تجاری .بعلاوه استفاده از **SSH** نیاز به نرم افزار یا سیستم عاملهای سازگار با**SSH** در دو طرف اتصال دارد، که به این ترتیب **SSH**برای سرور به سرور انجام می گیرد .

28-جدول فرکانس ایران



02.11a



30-باندهای فرکانسی Wireless

درجمهوری اسلامی ایران

802.11a
UP TO 45Mb/s

Main Band
5.8 GHz
3.5 GHz
2.5 GHz

802.11 WLAN
UP TO 2Mb/s
2.4 GHz

802.11a
UP TO 45Mb/s
5.725 & 5.850 GHz
UNLL (Unlicensed National Information Infrastructure)

802.11b
UP TO 11Mb/s
2.4 TO 2.4835 GHz (ISM)
ISM = Industrial Scientific & Medical

802.11g
UP TO 54 Mb/s
2.4 TO 2.4835 GHz (ISM)

802.16e WMAN
UP TO 30Mb/s
5GHz

802.16Rev2004
UP TO 75Mb/s
211GHz