Network Security
IEEE 802.11

اسماعیل طغرایی

Web Developer – Network – Programming

Toghraee_university@yahoo.com

Wi-Fi چیست؟

wifi مخفف کلمات Wireless Fidelity می باشد و در حقیقت یک شبکه بی سیم است که مانند امواج رادیو و تلویزیون و سیستم های تلفن همراه از امواج رادیویی استفاده می کند. برقراری ارتباط با شبکه بی سیم شباهت زیادی به یک ارتباط رادیویی دو طرفه (مانند بی سیم پلیس) دارد.

اسماعیل طغرایی
Toghraee_university@yahoo.com

Web Developer – Network – Programming

شبکه های بی سیم و تکنولوژی WI-FI

WiFiروش بیسیم برای ایجاد و اداره شبکه است که به آن شبکه سازی ۸۰۲.۱۱ و شبکه سازی بیسیم نیز گفته می شود . بزرگترین نقطه قوت WiFi، سادگی آسان است . شما می توانید کامپیوترهای منزل یا محل کار خود را بدون نیاز به سیم به یکدیگر متصل کنید . کامپیوترهایی که شبکه را تشکلیل می دهند می توانند تا بیش از ۱۰۰ فوت از هم فاصله داشته باشند

اسماعیل طغرایی
Toghraee_university@yahoo.com

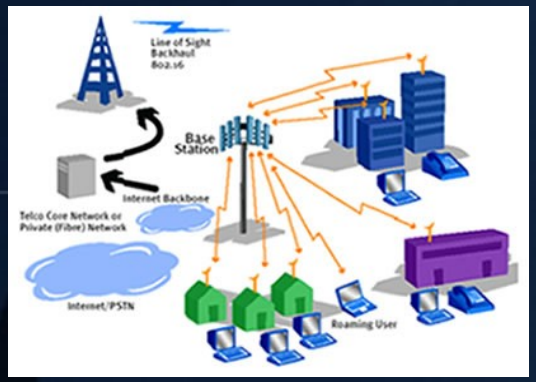
انواع شبکه های بیسیم

WLANS(Wireless Local Area Networks)

WPANS(Wireless Personal Area Networks)

WMANS(Wireless Metropolitan Area Networks)

WWANS(Wireless Wide Area Networks)



امنیت در شبکه های بی سیم

WEP(Wired Equivalent Privacy)

SSID (Service Set Identifier)

MAC (Media Access Control)

اسماعیل طغرایی
Toghraee_university@yahoo.com

انجمن استانداردهای IEEE

این استاندارد برای اولین بار در سال ۱۹۹۰ بوسیله انستیتیو IEEEمعرفی گردید.

- اکنون تکنولوژیهای متفاوتی از این استاندارد برای شبکه های بی سیم ارائه شده است:

- ۸۰۲.۱۱
- a۸۰۲.۱۱
- b۸۰۲.۱۱
- g۸۰۲.۱۱

802.11c : جهت بهبود ارتباط دستگاه ها با یکدیگر

- 802.11d : جهت بهبود عمل گردش در شبکه (roaming)
- 802.11e: جهت اصلاح و بهبود کیفیت سرویس (Quality of Service)
- 802.11f: جهت تنظیم بهتر دسترسی Access Point ها

IEEE انجمن استانداردهاي

TABLE I

THE EVOLUTION OF THE 802.11 STANDARDS

Protocol	Year Introduced	Maximum Data Transfer Speed	Frequency	Highest Order Modulation	Channel Bandwidth	Antenna Configurations
802.11a	1999	54 Mbps	5 GHz	64 QAM	20 MHz	1×1 SISO
802.11b	1999	11 Mbps	2.4 GHz	11 CCK	20 MHz	1×1 SISO
802.11g	2003	54 Mbps	2.4 GHz	64 QAM	20 MHz	1×1 SISO
802.11n	2009	65 to 600 Mbps	2.4 or 5 GHz	64 QAM	20 and 40 MHz	Up to 4×4 MIMO
802.11ac	2012	78 Mbps to 3.2 Gbps	5 GHz	256 QAM	20, 40, 80 and 160 MHz	Up to 8×8 MIMO; MU-MIMO

Toghraee_university@yahoo.com

:IEEE 802.11b

دستگاه هایی که این استاندارد را رعایت می کنند جهت کار در باند فرکانسی ۴/۲ گیگاهرتز و سرعت انتقال ۱۱ مگابیت ثانیه در فواصل حدود ۵۰ تا ۱۰۰ متر طراحی شده اند. در

بسیاری از سازندگان معتبر تجهیزات شبکه بی سیم از این استاندارد پیروی می کنند و در حالت حاضر اغلب سازمان ها از
آن سود می برند.

از آن جایی که مشخصه هایی که در این استاندارد تعریف شده اند بسیار کم اشکال و پایدار هستند ، توصیه می شود که در
سازمان های بزرگ از آن استفاده شود.

شیوه ارتباطی نیز طیف گسترده رشته ای مستقیم است.

اسماعیل طغرایی
Web Developer – Network – Programming Toghraee_university@yahoo.com

IEEE 802.11g:

این مشخصه نیز مربوط به باند فرکانس ۴/۲ گیگا هرتزاست ولی جهت کار با سرعت ۲۲ مگابیت بر ثانیه در مسافت های
۳۰ الی ۷۰ متری هر چند که سرعت این استاندارد در حد ۲۲ مگابیت تعریف شده است.

اما پیاده سازی آن بسیار گران قیمت بوده و به همین علت در کاربردهای محدودتر نظیر بازار ادوات مــورد استفاده قرار می گیرد.

اسماعیل طغرایی
Web Developer – Network – Programming
Toghraee_university@yahoo.com

:IEEE 802.11a

اين استاندارد جهت دستگاه هايي تعريف شده است كه در باند فركانسي صفر گيگا هرتز عمل مي كنند و ميزان گذردهي 54 مگابيت بر ثانيه را در محدوده 10 تا 30 متري پوشش مي دهند.

802.11a استفاده از 13 كانال را مجاز شمرده است.

سرعت بسيار بالاتر دستگاه هايي كه از اين استاندارد پشتيباني مي كنند، براي كاربراني كه به چنين سرعتي نياز دارند، مناسب است اما محدوديت فاصله آن نيز بايد در نظر گرفته شود، ضمن آن كه همچنان پياده سازي آن گران بوده و استفاده از آن در همه مكان ها مقرون به صرفه نيست.

البته سازمان هايي هستند كه تمامي اين هزينه ها را تقبل مي كنند تا چنين شبكه اي را راه اندازي كنند و از مزاياي سرعت بالا، امكان فعال سازي سرويس هايي نظير كيفيت سرويس و امنيت بالا بهره ببرند.

:IEEE 802.11h

اين مشخصه نوع اروپايي استاندارد 802.11a است كه بعضي ويژگي ها به آن اضافه گرديده است از جمله رعايت TPC يا Transmit Power Control كه كارت هاي شبكه بي سيم را از انتشار بيش از اندازه سيگنال هاي راديويي منع ميكند .

همچنين پشتيباني از DFS (Dynamci Frequency Selection) كه به كارت هاي شبكه اجازه مي دهد قبل از اشغال نمودن يك كانال، به رويدادهاي راديويي اطراف خود توجه كنند.

اسماعيل طغرايی
Web Developer – Network – Programming
Toghraee_university@yahoo.com

:IEEE 802.11I

اين استاندارد هنوز در حال بررسي واعمال تغييرات است و قرار است در آن ويژگي هاي امنيتي تقويت گردد و شيوه هاي رمزنگاري 802.11 بهبود يابد. در ضمن سازمان IEEE سرگرم كار بر روي استانداردهاي ديگري نيز هست كه هر يك داراي ويژگي و كاربرد خاصي هستند.

برخي از اين استانداردها عبارتند از:

802.11c : جهت بهبود ارتباط دستگاه ها با يكديگر

802.11d : جهت بهبود عمل گردش در شبكه (roaming)

802.11e: جهت اصلاح و بهبود كيفيت سرويس (Quality of Service)

802.11f: جهت تنظيم بهتر دسترسي Access Point ها

Table 1. Main features of WEP, WPA, and WPA-2

	WEP	*WPA*	*WPA-2*
Authentication	N/A	IEEE 802.1X/ EAP/PSK	IEEE 802.1X/ EAP/PSK
Cryptographic algorithm	RC4	RC4	AES
Key size	40 O 104 bits	128 bits	128 bits
Encryption method	WEP	TKIP	CCMP
Data integrity	CRC32	MIC	CCM
Keys for packets	No	Yes	Yes
IV length	24 bits	48 bits	48 bits

اسماعیل طغرایی
Toghraee_university@yahoo.com

IEEE 802.1X

برای بهینه کردن سیستم احراز هویت در شبکه های WLAN سازمان IEEE در حال تدوین استانداردهای 802.1x از پروتکل EAP به این منظور استفاده می‌کند.

Extensible Authentication Protocol یکی از پروتکل های عمومی برای احراز هویت است که از شیوه هایی نظیر : کارت های token ، روش Kerberos، روش کلید عمومی، روش گواهینامه (Certificate) و روش One-time Password پشتیبانی می کند.

اسماعیل طغرایی
Toghraee_university@yahoo.com

سه قابلیت و سرویس پایه توسط IEEE

Authentication

Confidentiality

Integrity

اسماعیل طغرایی

Web Developer – Network – Programming

Toghraee_university@yahoo.com

زیر ساخت WLAN:

به طور کلی ، شبکه های **WLAN** به عنوان ضمیمه یا بخشی از یک شبکه بزرگ تر **LAN** برپا می شوند و بدین طریق کاربران **mobile** این امکان را می یابند که با شبکه اصلی در تماس باشند.

اجزای کلی که در شبکه های **WLAN** به کار می رود عبارتند از : **Wireless Access Point** که به آن نقطه دسترسی یا **AP** هم گفته می شود.

این دستگاه عمل روتر را انجام می دهد (در حالت انفرادی عمل **Switch** یا **hub** را انجام می دهد) و فراهم کننده دسترسی دستگاه های بی سیم به شبکه بی سیم است.

AP ها عموماً در پشت یک فایروال قرار می گیرند تا حفاظت بهتری از شبکه به عمل آید و معمولاً از اغلب استانداردهای **802.11** پشتیبانی می کنند.

بعضی از آن ها در ۲ باند عمل می کنند.

اسماعیل طغرایی
Toghraee_university@yahoo.com

Mobile Device:

همان واحد متحرکی است که باید ارتباط آن با شبکه برقرار شود کامپیوترهای کیفی، دستیارهای دیجیتالی دستگاه هایی
نظیر این ها، مثال هایی که از واحدهای متحرک می باشند.

Wireless Network Interface Card:

یا کارت های شبکه بی سیم که دستگاه های سیار را قادر می سازند با **AP** ارتباط برقرار کنند هر کات که همانند کارت شبکه معمولی عمل می کند دارای یک آدرس **MAC** منحصر به فرد است، ضمن آن که لازم است این کارت با **AP** هماهنگی کامل داشته باشد یعنی به عنوان مثال هر دو گروه **802.11a** باشند.

مشابه **AP** ها، کارت های شبکه بی سیم نیز برخی **Dual band** هستند که مزیت خوبی برای آن ها محسوب می گردد.

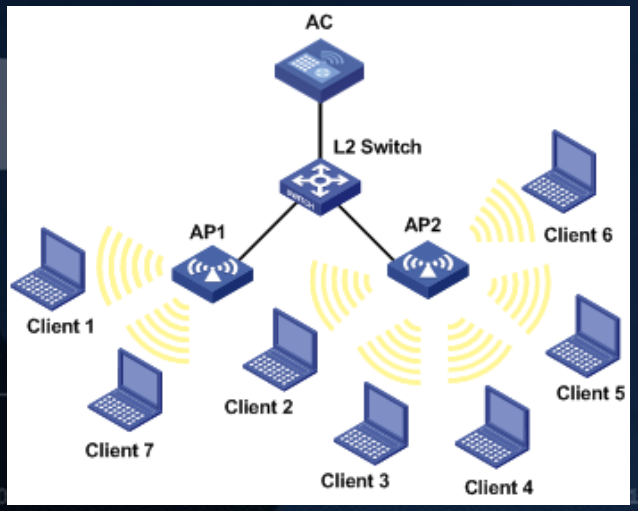
اسماعیل طغرایی
Toghraee_university@yahoo.com

سرور امنیتی :

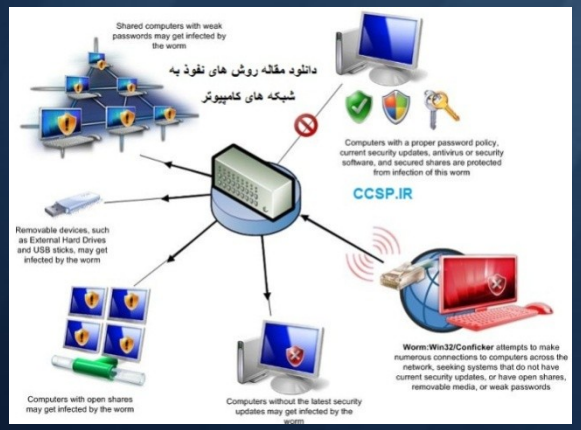
سروری وجود دارد که مسوول مدیریت کردن مسایل امنیتی است تا **WLAN**در اغلب شبکه های اطلاعات تبادلی روی شبکه آسیب نبینند. این اجزا در شکل های یک و دو نمایش داده شده اند.

امنیت در WLAN

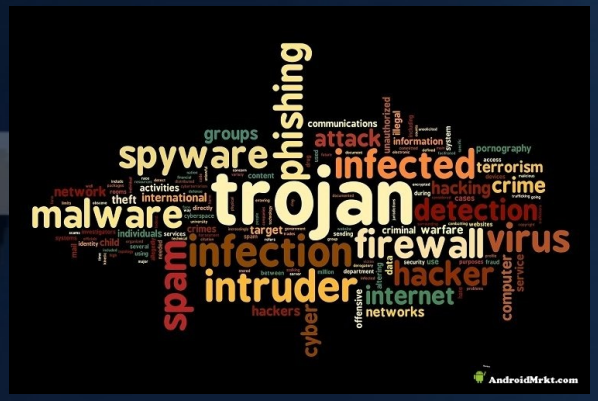
مشخصه های تعریف شده برای شبکه های محلی بی سیم به طور ذاتی نا امن هستند زیرا اساساً بنیاد آن ها بر این فرض استوار است که همگان باید بتوانند به شبکه دسترسی داشته باشند و از منابع آن استفاده کنند. در نتیجه ویژگیهای امنیتی باید به مجموعه تعاریف WLAN افزوده شود تا برای سازمان های بزرگ قابل استفاده باشد.



انواع حملات:



- Sniffing ❖
- Spoofing ❖
- Jamming ❖
- Session Hijacking ❖
- Denial Of Service ❖
- Man in the Middle ❖



اسماعیل طغرایی
Toghraee_university@yahoo.com

Sniffing :

این اصطلاح هنگامی به کار می رود که شخص مشغول نظارت بر ترافیک شبکه (به طور قانونی یا غیرقانونی) باشد.

اغلب اطلاعات ارسالی توسط Access Point ها به راحتی قابل Sniff کردن است زیرا فقط شامل متون معمولی و رمز نشده است.

پس خیلی آسان است که نفوذگر با جعل هویت دیجیتالی یکی از کاربران شبکه به داده های ارسالی یا دریافتی AP دسترسی پیدا کند.

اسماعیل طغرایی
Web Developer – Network – Programming
Toghraee_university@yahoo.com

Spoofing :

این اصطلاح هنگامی استفاده می شود که شخصی با جعل هویت یکی از کاربران مجاز اقدام به سرقت داده های شبکه بنماید.

به عنوان مثال ،فرد نفوذگر ابتدا با **Sniff** کردن شبکه، یکی از آدرس های **MAC** مجاز شبکه را به دست می آورد، سپس با استفاده از آن، خود را به عنوان یکی از کاربران معتبر به **AP** معرفی می نماید و اقدام به دریافت اطلاعات می کند.

اسماعیل طغرایی
Toghraee_university@yahoo.com

Jamming :

این اصطلاح به معنای ایجاد تداخل رادیویی به جهت جلوگیری از فعالیت سالم و مطمئن AP است و از این طریق فعالیت AP مختل شده و امکان انجام هیچ گونه عملی روی شبکه میسر نخواهد شد.

به عنوان نمونه، دستگاه های منطبق بر 802.11b (به جهت شلوغ بودن باند فرکانسی کاری آن ها) به سادگی مختل می شوند.

اسماعیل طغرایی
Toghraee_university@yahoo.com

Session Hijacking :

در این جا فرد نفوذگر خود را دستگاهی معرفی می کند که ارتباطش را با AP از دســت داده و مجــدداً تقاضــای ایجــاد ارتباط
دارد.

اما در همین حین، نفوذگر همچنان با شبکه مرتبط بوده و مشغول جمع آوری اطلاعات است.

اسماعیل طغرایی
Toghraee_university@yahoo.com

Denial Of Service :

این اصطلاح هنگامی به کار می رود که نفوذگر وارد شبکه شده است و ترافیک شبکه را با داده های بی ارزش بـالا مـی برد
تا حدی که شبکه به طور کلی از کار بیفتد یا اصطلاحاً **Down** شود.

یکی از راه های ساده این کار، ارسال درخواست اتصال به شبکه **(Log on)** به تعداد بی نهایت است.

اسماعیل طغرایی
Web Developer – Network – Programming
Toghraee_university@yahoo.com

Man in the Middle :

در این حالت، فرد نفوذگر اقدام به تغییر پیکربندی ادوات متحرک به همراه شبیه سازی وضعیت Access Point می نماید.

در نتیجه ترافیک شبکه به محل دیگری که در آن AP شبیه سازی شده انتقال می یابد. در چنین وضعیتی ، نفوذگر می تواند کلیه اطلاعات را بدون نگرانی و واسطه بخواند و جمع آوری کند، ضمن آن که کاربران همگی فکر می کنند که مشغول کار در شبکه خودشان هستند.

انجام این کار چندان مشکل نیست زیرا تمامی شبکه های WLAN از احراز هویت در سمت سرویس گیرنده استفاده می کنند و احراز هویتی در سمت AP صورت نمی گیرد.

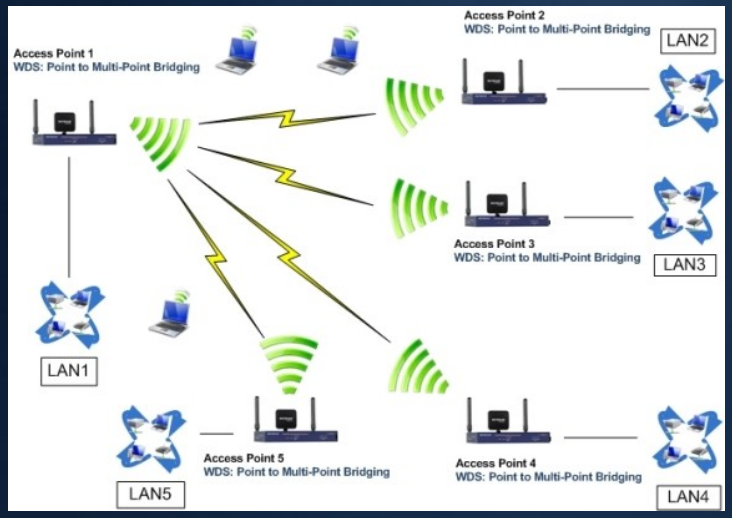
در نتیجه، کاربران از اتصال به AP مجازی یا غیرمجاز مطلع نمی شوند.

اسماعیل طغرایی
Toghraee_university@yahoo.com

Access Point های تقلبی

یکی دیگر از شیوه های نفوذ به درون شبکه های WLAN استفاده از AP های غیرمجاز یا تقلبی است.

شکل ۳- شبکه های WLAN را می توان به صورت Point – to-multipiont هم راه اندازی نمود. به این صورت می توان چندین شبکه LAN فرعی که ممکن است خودشان بی سیم باشند را به یک نقطه مرکزی متصل نموده و شبکه محلی بی سیم بزرگتری تشکیل داد.



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 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.