دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش : مخابرات

عنوان :

امنیت شبکه های بی سیم

استاد راهنما : دکتر مهدی قمری ادیان

نگارش : سید محمد علی قاسمی ۹۲٤٤۳۱۱٥

محمد خیام ۹۲٤٤۳۱۰۷

تابستان ۹٦

امنیت شبکه های بی سیم

سید محمد علی قاسمی-محمد خیام

فهرست

مقدمه

شبکه های بی سیم (Wireless) یکی از تکنولوژی های جذابی است که توانسته در ۳ دهه اخیر توجه بسیاری را به خود جلب کند و به دنبال آن پژوهش ها و تحقیقات زیادی صورت گرفته و هم اکنون نیز شاهد پیشرفت های زیادی در این زمینه هستیم . ارزیابی نیاز ها و توقعات و مقایسه آن با امکانات و قابلیت هایی که این تکنولوژی در اختیار میگذارد ، مهم ترین مرحله ی تعیین کننده میزان کارآمدی و رضایت از این دسته شبکه ها می باشد .

شبکه های WLAN را نمی توان جایگزینی برای شبکه های کابلی Ethernet کرد ، بلکه این شبکه ها راه حلی است برای مواردی که امکان کابل کشی و استفاده از شبکه Ethernet امکان پذیر نیست و یا اولویت با امکان جابجایی (Mobility) و یا زیبا سازی محیط میباشد.سالن های کنفرانس ، انبار ها ، کارخانجات ، کارگاه های عمرانی و محیط های نمایشگاهی بهترین نمونه ها برای استفاده موثر از شبکه های WLAN می باشند.

شبکه های سیمی به صورت ذاتی از شبکه های بی سیم امن تر می باشند ، چرا که تمام و یا بخش عمده ی آن دارای ساختاری یکپارچه می باشد و به همین دلیل است که امکان دسترسی غیر مجاز به این شبکه ها بسیار کم تر از شبکه های بی سیم است . این در حالی است که شبکه های بی سیم با استفاده از امواج رادیویی فعالیت میکنند و به علت فیزیکی نبودن آن ها مانند شبکه های سیمی ، بیشتر در معرض نفوذ قرار داشته و آسیب پذیرتر میباشند .

بنابراین مساله امنیت به طور جدی در این شبکه ها مطرح می شود و گاها مسائل و مشکلاتی امنیتی که در این شبکه ها وجود دارد ، در شبکه های محلی سیمی وجود نداشته و باید به دنبال راه کارها و پرتکل های امنیتی باشیم که در صدد رفع و برآورده کردن نیازهای امنیتی مختص این شبکه ها باشد. اتصال بی سیم ، یک رسانه غیر فیزیکی است و برای تامین امنیت آن نمی توان تنها به وجود یک دیوار آتش بسنده کرد . به وضوح می توان نقاط دسترسی غیر مجاز را به واسطه ی ایجاد راه های ورود مخفی به شبکه و مشکل بودن تعیین موقعیت فیزیکی آن ها ، نوعی تهدید برای شبکه به شمار آورد .

با توجه به نکات گفته شده برای تامین امنیت شبکه های مبتنی بر تکنولوژی بی سیم ، نیاز به پرتکل ها و تدابیر امنیتی ویژه ای که خاص این دسته از شبکه ها باشد احساس می شود . در این پروژه ضمن معرفی این دسته شبکه ها با تاکید بر ابعاد امنیتی آن ها ، به بررسی چالش ها و نیازمندی های امنیتی در شبکه های بی سیم پرداخته و در ادامه به بیان راهکار هایی مناسب برای مقابله با تهدیدات موجود و ایمن سازی در مواجهه با آن ها خواهیم پرداخت.

فصل اول

معرفی شبکه های Wi-Fi

مراجع : [۱] و [۲]

۱-۱ شبکه های Wi-Fi چیست ؟

وای فای (Wi-Fi) مخفف عبارت Wireless Fidelity است و استانداردی از زیر مجموعه Bluetooth است و تحت آن ارتباطی با قدرت بیشتر از خود Bluetooth ایجاد می شود . ارتباط Wi-Fi بیشتر بر پایه ارتباط شبکه اینترنت به صورت بی سیم تاکید می کند و همین امر باعث محبوبیت بسیار زیاد آن شده است . با استفاده از این تکنولوژی میتوان به راحتی در مسافرت ، هتل ،هواپیما ، دانشگاه و ... از طریق لپتاب ، موبایل و یا تبلت خود به اینترنت متصل شد . Wi-Fi که همان استاندارد IEEE ۸۰۲,۱۱ است در مدل های ۸۰۲,۱۱g و ۸۰۲.۱۱b مورد استفاده قرار می گیرد و استاندارد اصلی آن IEEE ۸۰۲,۱۱b است. در این مدل حد اکثر سرعت انتقال اطلاعات ۱۱ مگابیت بر ثانیه است و از فرکانس رادیویی ۲/۴ گیگاهرتز استفاده میکند . برای سرعت بخشیدن به این استاندارد مدل دیگری نیز به نام ۸۰۲,۱۱n ایجاد شده که سرعت انتقال را تا ۲۰۰ مگابیت بر ثانیه افزلیش می دهد . افزایش سرعت در ۸۰۲,۱۱n به دلیل استفاده از سیستم های چند آنتنه (MIMO) ، استفاده همزمان از دو محدوده ی فرکانسی ۲/۴ و ۵ گیگاهرتز ، و برخی تکنیک های خاص در دسترس محیط (Medium Access-MAC) است . برد Wi-Fi در حدود ۲۰ متر است . امروزه افراد برای استفاده از این نوع ارتباط بیشتر با موبایل وتبلت های خود که دارای این نوع خدمات هستند استفاده میکنند البته اغلب لپتاب های امروزی نیز دارای آن می باشند . کسانی که خواهان استفاده ازآن بر روی PC یا همان رایانه شخصی خود می باشند نیز می توانند از یک کارت خارجی گیرنده امواج Wi-Fi و یا مودمی که درون دستگاه قرار میگیرد استفاده کنند .

۱-۲ کاربرد های Wi-Fi

همانطور که گفته شد تکنولوژی Wi-Fi علاوه بر ارتباط رایانه های شخصی به اینترنت ، این امکان را برای تلفن های همراه نسل جدید و تبلت ها نیز فراهم می کند . همچنین به عنوان راه حلی موثر به منظور توسعه شبکه های داخلی ، بدون صرف هزینه سیم کشی مطرح شده است .

دو تکنولوژی Wi-Fi و Bluetooth به عنوان رقبای یکدیگر در شبکه های بی سیم مطرح شده اند و هم اکنون نیز رقابت آن ها در حال افزایش است ، اما هدف این دو فناوری یکسان نیست و هرکدام هدف جداگانه ای را در پیش گرفته اند .

Bluetooth برای استفاده در شبکه های بی سیم کوچک در نظر گرفته شده است که دارای مصرف پایین برق و برد کوتاه تری است اما Wi-Fi برای استفاده در شبکه های بی سیم متوسط با برد و پهنای باند وسیع تری مطرح شده است .

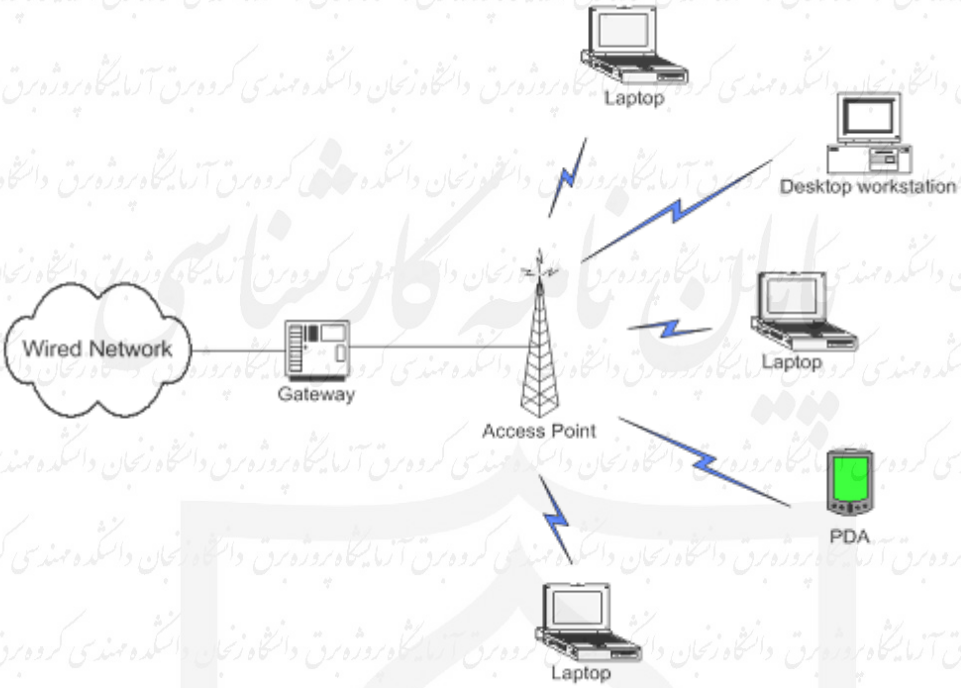
۱-۳ ترکیب سیستم Wi-Fi در رایانه

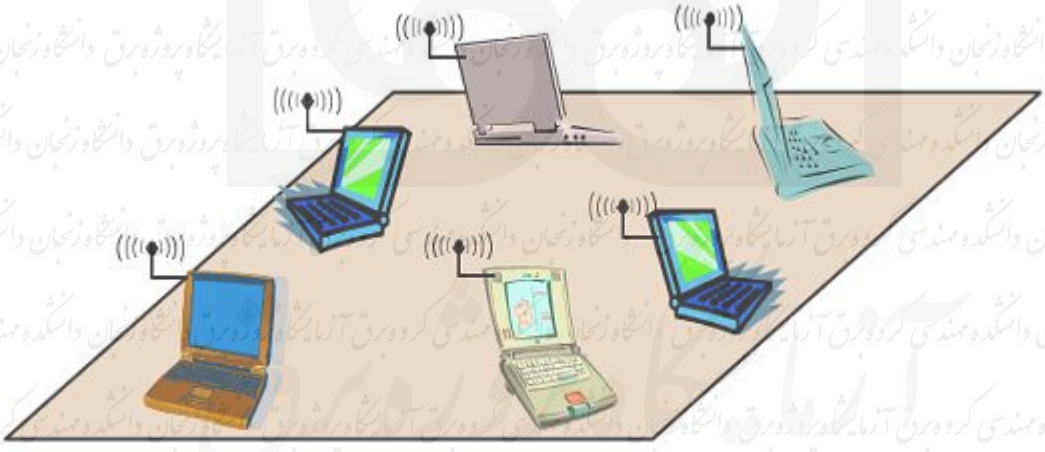
امروزه اغلب رایانه های لپتاب مجهز به سیستم Wi-Fi داخلی هستند و در غیر این صورت نیازمند نصب یک کارت Wi-Fi بر روی لپتاب و رایانه رومیزی خود خواهیم بود . شما می توانید یک کارت Wi-Fi در سیستم ۸۰۲,۱۱a یا ۸۰۲,۱۱b و یا ۸۰۲,۱۱n تهیه کنید که البته نوع ۸۰۲,۱۱n نسبت به تجهیزات دارای استاندارد های دیگر از سرعت بالاتری برخوردار است. برای لپتاب ها این تجهیزات در قالب کارت های PCMCIA که در محل مخصوص خود نصب می شوند و یا به صورت اتصال خارجی از طریق درگاه USB عرضه می شوند . برای رایانه های رومیزی ، می توانید از کارت های PCI و یا درگاه USB برای این منظور استفاده کنید . پس نصب و با به کار گیری این تجهیزات کاربر قادر است تا در مکان هایی که سرویس Wi-Fi ارائه می شود با داشتن یک اشتراک ، از خدمات بهره گرفته و به شبکه متصل شود .

۱-۴ شبکه Wi-Fi چگونه کار می کند ؟

دو نوع مود عملیات برای برقراری ارتباطات در استاندارد تعریف شده وجود دارد ، حالت دارای زیر ساخت (Infrastructure - based) و حالت بدون زیر ساخت یا موردی (Ad hoc) . در حالت دارای زیر ساخت ، هیچکدام از نود های شرکت کننده در شبکه به عنوان نقطه دسترسی عمل نمی کند و سایر نود ها برای ارتباط با یکدیگر ، ابتدا باید با نقطه دسترسی ارتباط برقرار کنند . اما در حالت بدون زیر ساخت هیچگونه مرکز و نقطه دسترسی وجود ندارد و نود ها برای ارتباط با یکدیگر به طور مستقیم عمل می کنند و احتمالا از نود های یکدیگر می توانند برای کمک در مسیریابی استفاده کنند .

نمونه ای از این شبکه ها :





برای پشتیبانی ارتباطات بی سیم کلاینت ها و نقطه دسترسی شامل یک رادیو و آنتن می باشند .

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

موارد همواره وجود دارد، استفاده از اینترنت شخصی که ممکن است برای کاربران هزینه داشته باشد، ایمن تر خواهد بود.

- در مواقعی که به اینترنت بی سیم نیاز ندارید، واسط شبکه ی بی سیم را غیرفعال نمایید. مادامی که واسط بی سیم دستگاه هایی مانند تلفن های همراه هوشمند و تبلت ها که قابل حمل هستند فعال باشد، این دستگاه ها در جستجوی شبکه های بی سیم ذخیره شده ی قبل، به طور مرتب فریم های probe را در محیط اطراف ارسال می کنند. این امر دستگاه بی سیم را در معرض اتصال خودکار به نقطه ی دسترسی مخرب با نام جستجو شده ی مشابه قرار می دهد .
- از ابزارهای اتصال امن جهت اتصال به نقاط دسترسی عمومی استفاده نمایید. به عنوان مثال، برنامه ای مانند IPASS مشتریان را از طریق یک صفحه ی ورود رمزنگاری شده به شبکه متصل می نماید که به این ترتیب تهدید حملات Phishing وب در بستر بی سیم را از بین خواهد برد.

۸-۱۲ نتیجه گیری

دستگاه های بی سیم مخرب و در رأس آن ها نقاط دسترسی ممکن است توسط عاملی داخلی (کارمندان سازمان) و یا خارجی (مهاجم) به طور غیرمجاز به کار گرفته شوند. در مورد اول، تهدیدی شکل می گیرد که خود شبکه ی سازمان را هدف قرار می دهد. به کارگیری نقطه ی دسترسی غیرمجاز توسط یک مهاجم با اهداف بدخواهانه، حمله ی مردی در میانه بی سیم را شکل می دهد که دستگاه های مشتریان را مورد هدف قرار می دهد. هر دو مورد از تهدیدات جدی و فعال در حوزه ی شبکه های محلی بی سیم تلقی می گردند.

مؤثرترین روش برای مقابله با تهدید نقاط دسترسی داخلی مخرب، استفاده از مکانیزم احراز هویت و کنترل دسترسی ۸۰۲,۱x/EAP در سمت کابلي شبکه است .همچنین، اگر ۸۰۲,۱x/EAP ۸۰۲,۱ در سمت بی سیم شبکه به کار گرفته شود، حملات مردی در میانه و دزدیدن اتصال بی سیم را متوقف خواهد نمود. روش دیگر برای مقابله با این تهدیدات به کارگیری سیستم های تشخیص و جلوگیری از نفوذ بی سیم است. شناسایی نقاط دسترسی مخرب در حال حاضر از زمینه های پژوهشی فعال در حوز هی شبکه های بی سیم ۸۰۲,۱۱ است.

منابع

[۱] “Wi-Fi Security How to Break and Exploit”, Thesis for the degree Master of Science Hallvar Helleseth Department of InformaticsUniversity of Bergen June ۲۰۰۶

[۲]" An Introductionto Wi-Fi®”, Part Number ۰۱۹-۰۱۷۰ • ۰۹۰۴۰۹–B • Printed in U.S.A.Digi International Inc. © ۲۰۰۷-۲۰۰۸

[۳] IEEE ۸۰۲,۱۱ Working group website ,http://www.ieee۸۰۲.org/۱۱

[۴] Introduction to IEEE ۸۰۲,۱۱ " ",intellgraphics" , http://www.intellgraphics.com "

[۵] steve Kapp,"۸۰۲,۱۱:Leaving the wire behind ",IEEE internet computing ,January-February ۲۰۰۲,pp.۸۲-۸۵

[۶] steve Kapp "۸۰۲,۱۱a :More bandwidth without the wire ",IEEE internet computing ,Julay Aguest ۲۰۰۲,pp.۷۵-۷۹

[۷] Edgar Danielyan "IEEE ۸۰۲,۱۱ ",the internet Protocol Journal ,Vol.۵,No.۱,March۲۰۰۲,pp.۲-۱۳

[۸] "A condensed review of Spread Spectrum Techniques for ISM band System ",Intersil Application Note,AN۹۸۲۰,۱,May ۲۰۰۰

[۹]" Wi-Fi Security"Stewart S. Miller,McGraw-Hill-New York Chicago San Francisco Lisbon London Madrid Mexico City Milan New Delhi San Juan Seoul Singapore Sydney Toronto

[۱۱] “Overview of Wi-Fi Security What is left?”,Philippe Teuwen,Security Engineer and Contributor to Wi-Fi Alliance Easy Setup Task Group,N.V. Philips,October ۱۴ & ۱۵, Hack.lu ۲۰۰۵

[۱۲] Andrew A. Vladimirov, Konstantin V. Gavrilenko, and Andrei A. Mikhailovsky. Wi- Foo: Addison Wesley, ۲۰۰۴

[۱۳] Rob Flickenger. Wireless Hacks: O'Reilly, ۲۰۰۳

[۱۴] Chris Hurley, Michael Puchol, et al. WarDriving: Drive, Detect, Defend: A Guide to Wireless Security: Syngress Publishing, ۲۰۰۴

[۱۵] Wright, Joshua.“Layer ۲ Analysis of WLAN Discovery Applications for Intrusion Detection”.۱۳ Apr.۲۰۰۵.< http://home.jwu.edu/jwright/papers/l۲-wlan-ids.pdf >

[۱۶] Brenner, Pablo.”A Technical Tutorial on IEEE ۸۰۲,۱۱ Protocol”.۱۳ Apr ۲۰۰۵.< http://www.sss-mag.com/pdf/۸۰۲_۱۱tut.pdf >

[۱۷] Loud Fat Blokes. ۸۰۲,۱۱ Home Page. ۱۳ Apr. ۲۰۰۵ < http://www.loud-fatbloke. co.uk/w۸۰۲۱۱.html >.

[۱۸] Ossmann ,Michael. ” WEP: Dead Again, Part ۲” Securityfocus.۸ Mar.۲۰۰۵,۱۳ Apr.۲۰۰۵ < http://www.securityfocus.com/infocus/۱۸۲۴ >.

[۱۹] Frankel Sh. And Eydt B. and Owens L. and Kent K.," Guide to IEEE ۸۰۲,۱۱i:Establishing Robust Security Networks,"Computer Security Division Information technology Laboratory National Institute of Standards and Technology ,Gaithersburg, MD ۲۰۸۹۹-۸۹۳۰ June ۲۰۰۶

[۲۰] Miller Stewart S. ," WiFi Security",Copyright ۲۰۰۳ by The McGraw-Hill Companies.

[۲۱] C. He and J. C. Mitchell. "Security analysis and improvements for IEEE ۸۰۲,۱۱i." In Proceedings of the ۱۲th Annual Network and Distributed System Security Symposium (NDSS'۰۵), ۲۰۰۵.

[۲۲]The Bell Labs Security Framework: "Making the Case for End-to-End Wi-Fi Security" , Wi-Fi Security v۱,۰۹۰۶ , http://www.lucent.com.,۲۰۰۶,whitepaper.

[۲۳]Buttyán L. and Dóra L."WiFi Security – WEP and ۸۰۲,۱۱i," Technical Report, CrySyS Lab, Budapest University of Technology and Economics, May ۲۰۰۶.

[۲٤] Wireless LAN Security (۸۰۲,۱۱) Wardriving & Warchalking. ۱۳ Apr. ۲۰۰۵ < http://۸۰۲,۱۱-security.com/security/tools >

[۲۵] AbsoluteValue Systems, Inc. “WLAN Adapter Chipset Directory“.۲ Feb.۲۰۰٤,۱۳Apr۲۰۰۵.<http://www.linuxwlan.org/docs/wlan_adapters.html.gz >

[۲٦]Kismet.HomePage.۲Apr.۲۰۰۵,۱۳Apr.۲۰۰۵.<http://www.kismetwireless.net >

[۲۷]Ethereal.HomePage.۱۱Mar.۲۰۰۵,۱۳Apr.۲۰۰۵.<http://www.ethereal.com >

[۲۸] David Coleman, CWSP (Certified Wireless Security Professional) Official Guide, Sybex Publishing , ۲۰۱۰.

[۲۹] http://www.watchguard.com/infocenter/editorial/۲۷۰۶۱.asp

[۳۰] Vivek Ramachandran, "BackTrack ۵ Wireless Penetration Testing Beginner's Guide: Chatper ۶ Attacking the Client", ۲۰۱۱

[۳۱] Vivek Ramachandran, Advanced WLAN attacks , ۲۰۱۱.