مجله پژوهش های معاصر در علوم و تحقیقات
سال اول، شماره ۸، اسفند ۱۳۹۸
ISSN: ۷۶۷۶-۵۷۶٤
www.jocrisar.ir

نقاط ضعف امنیتی در شبکه های حسگر بیسیم

ناهید ابراهیمی

ارشد مخابرات- دانشگاه صنعتی شیراز

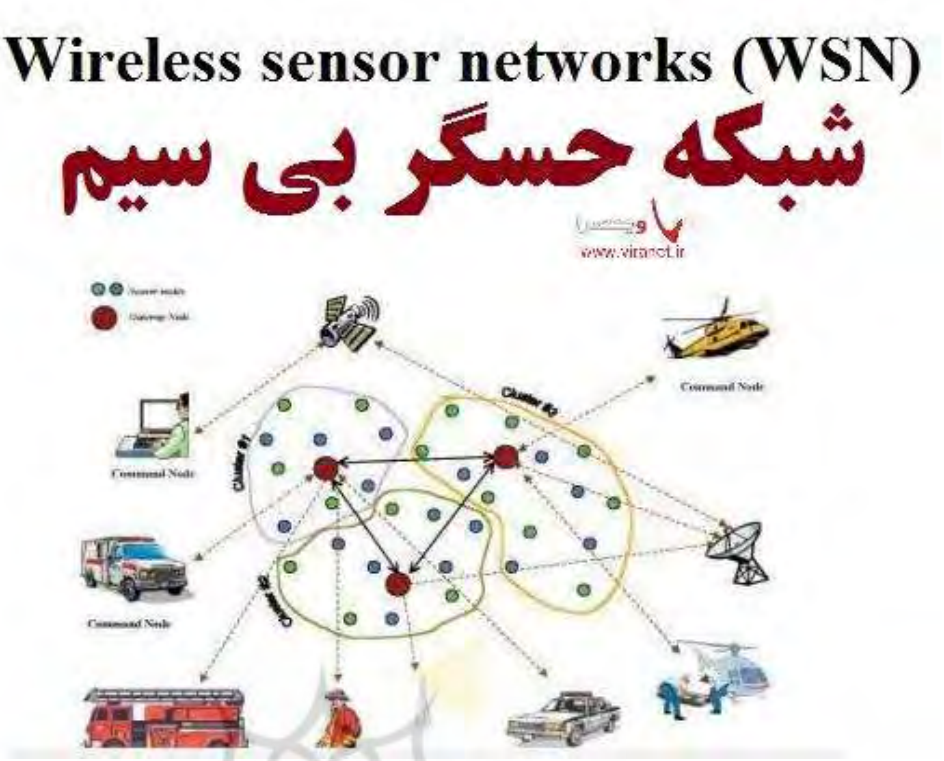
چکیده

شبکه های بیسیم یکی از شاخه های علم مخابرات در عصر حاضر هستند که اثرات آن در زندگی روزمره به وضوح دیده می شود. در نوع خاص از این شبکه ها، مجموعه ای از حسگرها برای جمع آوری اطلاعات در یک محیط بیسیم با یکدیگر مرتبط هستند و به نام شبکه های حسگر بیسیم شناخته می شوند. از آنجایی که امنیت و حفاظت حریم شخصی در بسیاری از کاربردهای پیشنهادی مربوط به شبکه های حسگر بیسیم بسیار با اهمیت هستند شبکه های حسگر بیسیم معمولاً برای جمع آوری رکوردها از محیط غیر ایمن تنظیم می شوند. تقریباً تمامی پروتکل های امنیتی WSN بر این تاکید دارند که یک مهاجم میتواند به طور کلی یک گره حسگر را با روش دسترسی فیزیکی مستقیم کنترل نماید. ظهور شبکه های حسگر به عنوان یکی از تکنولوژیهای عمده در آینده، چالشهای مختلفی را برای محققان در پی داشته است. شبکه های حسگر بیسیم از تعداد زیادی گره حسگر کوچک که جداگانه اجرا می شوند و در موارد مختلف بدون دسترسی به منابع تجدیدپذیر انرژی تشکیل شده است. علاوه بر این امنیت بحث اساسی در پذیرش و بکارگیری شبکه های حسگر برای کاربردهای مختلف است؛ همچنین چالش های مختلفی در شبکه های حسگر نیز وجود دارد. در این مقاله امنیت شبکه های حسگر بیسیم مورد بررسی قرار خواهد گرفت.

واژه‌های کلیدی: شبکه های حسگر بیسم، امنیت شبکه حسگر، ضعف شبکه.

۱. مقدمه

این یک شبکه حسگر شامل تعداد زیادی گره‌های حسگر است که در یک محیط بطور گسترده پخش شده و به جمع آوری اطلاعات از محیط می‌پردازند. لزوما مکان قرار گرفتن گره‌های حسگر، از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم. یک حمله استاندارد در شبکه‌های حسگر بی‌سیم، ایجاد پارازیت در یک گره یا گروهی از گره‌ها می باشد. حمله بر روی اطلاعات در حال عبور در یک شبکه حسگر از دیگر موارد تهدید کننده امنیت در این شبکه ها است، حسگرها تغییرات پارامترهای خاص و مقادیر را کنترل می‌کنند و طبق تقاضا به چاهک گزارش می‌دهند. در زمان ارسال گزارش ممکن است که اطلاعات در راه عبور تغییر کنند، مجدداً پخش شوند و یا ناپدید گردند. از آنجایی که ارتباطات بی‌سیم در مقابل استراق سمع آسیب پذیر هستند، هر حمله کننده می‌تواند جریان ترافیک را کنترل کند، در عملیات وقفه ایجاد کند و یا بسته‌ها را جعل کند. بنابراین، اطلاعات اشتباه به ایستگاه ارسال می‌شود شکل۱. از آنجایی که ارتباطات بی‌سیم در مقابل استراق سمع آسیب پذیر هستند، هر حمله کننده می‌تواند جریان ترافیک را کنترل کند، در عملیات وقفه ایجاد کند و یا بسته‌ها را جعل کند. بنابراین، اطلاعات اشتباه به ایستگاه ارسال می‌شود. به دلیل اینکه گره‌های حسگر معمولا دارای برد کوتاهی برای انتقال می باشند و منابع محدود دارند، حمله کننده‌ای با قدرت پردازش بالا و برد ارتباطی بیشتر می‌تواند بطور همزمان برای تغییر اطلاعات واقعی در طول انتقال، به چندین حسگر حمله کند. با توجه به اینکه محیط ارسال داده‌ها بدون سیم می‌باشد امنیت این نوع شبکه‌ها بسیار اهمیت پیدا می‌کند. همچنین به‌علت محدودیت‌های ذاتی این نوع شبکه‌ها نمی‌توان از رهیافت‌های موجود در شبکه‌های سنتی استفاده نمود. از این رو، با توجه به اهمیت امنیت در این شبکه ها، در این تحقیق به بررسی امنیت در شبکه های حسگر بی سیم می پردازیم. این شبکه‌ها به شدت در مقابل حملات آسیب پذیرند و امروزه مقاومت کردن در برابر این حملات از چالش‌های توسعه این شبکه هاست. دلایل اصلی این مشکلات عبارتند از : کانال رادیویی اشتراکی انتقال داده، محیط عملیاتی ناامن، قدرت مرکزی ناکافی، منابع محدود، آسیب پذیر بودن از لحاظ فیزیکی، کافی نبودن ارتباط نودهای میانی[۱].



شکل ۱ – ساختار کلی شبکه حسگر بیسیم

۲. ضعف امنیتی در شبکه های حسگر بیسیم و خطرات معمول

ساختار این شبکه‌ها مبتنی بر استفاده از سیگنال‌های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرتمند این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد. در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

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

حمله‌های DOS به تجهیزات و سیستم‌های بی سیم بسیار متداول است. کامپیوترهای قابل حمل و جیبی، که امکان استفاده از شبکهٔ بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت. یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکهٔ بی‌سیم در یک سازمان و شبکهٔ سیمی آن (که در اغلب موارد شبکهٔ اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکهٔ بی‌سیم عملاً راهی برای دست یابی به منابع شبکه سیمی نیز بیابد[۲].

۳. سه روش امنیتی در شبکه های حسگر بیسیم

WEP

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می‌آید که مناسب برای شبکه‌های کوچک بوده زیرا نیاز به تنظیمات دستی مربوطه در هر سرویس گیرنده می‌باشد. اساس رمز نگاری WEP بر مبنای الگوریتم ۴RC بوسیله RSA می‌باشد.

SSID

شبکه‌های WLAN دارای چندین شبکه محلی می‌باشند که هر کدام آنها دارای یک شناسه یکتا می‌باشند این شناسه‌ها در چندین نقطه دسترسی قرار داده می‌شوند. هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه SSID مربوطه را انجام دهد .

MAC

لیستی از MAC آدرس‌های مورد استفاده در یک شبکه به نقطه دسترسی مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرس‌ها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می‌کند MAC آدرس آن با لیست MAC آدرس مربوطه در نقطه دسترسی مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می‌گیرد. این روش امنیتی مناسب برای شبکه‌های کوچک بوده زیرا در شبکه‌های بزرگ امکان ورود این آدرس‌ها به نقطه دسترسی بسیار مشکل می‌باشد. در کل می‌توان به کاستن از شعاع تحت پوشش سیگنال‌های شبکه کم کرد و اطلاعات را رمزنگاری کرد.

۴. ابزار های Sniff و Scanشبکه های محلی بی سیم

این قسمت به معرفی چند ابزار می پردازیم که نمایانگر نا امنی و راه های سوء استفاده از شبکه های محلی بی سیم است ، با دانستن این موارد مدیران شبکه بهتر می توانند در مورد امنیت شبکه خود تصمیم گیری کنند.[۳]

ابزارهای مبتنی بر ویندوز و ساده و رایگان همانند NetStumbler امواج هوا را scan کرده و با جستجوی access point هایی که Access ID خود را broadcast می کنند ، راه بسیار ساده ای برای کشف شبکه های باز فراهم می کنند. ابزار های پیشرفته تری همانند Kismet نیز بر بستر لینوکس معرفی شده اند .Kismet بصورتی نامحسوس (Passive) ترافیک شبکه را ذخیره و مانیتور می کند. هر دوی این نرم افزار ها Netstumbler و Kismet از اطلاعات) GPS سیستم موقعیت یابی جهانی (برای نگاشت مکان دقیق شبکه های محلی بی سیم استفاده می کنند.

Driverها و مهاجمان از این ابزار استفاده می کنند تا وجود فیزیکی شبکه بی سیم را تشخیص دهند ، فارغ از اینکه این شبکه ها امن هستند یا خیر.

War Driverها کسانی هستند که با یک laptop یا وسیله ای مشابه داخل و اطراف شهرها می گردند تا سیگنالهایی از شبکه ای بی سیم بیابند. هکرها از این اطلاعات و لیست ها استفاده می کنند تا access point هایی را با SSID ، Mac آدرس یا شماره فیزیکی مشترک در یک آدرس و موقعیت بیایند.

آنتن ها : برای اتصال با شبکه های محلی بی سیم از راه دور ، هکر ها یا از انواع بسیار متنوع آنتن های تجاری استفاده می کنند ، یا اینکه به راحتی آنتن های خود را با قوطی خالی چیپس Pringle و یا هر وسیله مشابه فلزی دیگری می سازند .این آنتن ها هکرها را قادر می سازند تا امواج ۸۰۲,۱۱ را از فاصله چند هزارمتری دریافت کنند . آنها می توانند به شبکه دسترسی داشته باشند در حالی که کاملا دور از چشم همه قرار دارند [۴].

۵. ابزار هایی که رمزنگاری WEP را می شکنند

هکرها از ابزاری همانند WEPwedgie WEPCrack WEPAttack BSD-Airtools و AirSnort برای شکستن رمزنگاری استاندارد (Wired Equivalent Privacy) WEP استفاده می کنند . این ابزار از آسیب پذیری های (vulnerability)موجود درالگوریتم رمزنگاری WEP استفاده می کنند بدین شکل که بصورت نامحسوس (Passive) ترافیک شبکه محلی بی سیم را زیر نظر می گیرند تا زمانیکه اطلاعات کافی برای تشخیص الگو (pattern) بدست آورند.

سپس از این اطلاعات برای شکستن کلید (KEY) رمزنگاری استفاده می کنند WEPwedgie .و BSD-Airtools زمان طولانی مورد نیاز برای شکستن کلید های بلند WEP را به حد اقل می رسانند و این زمان را با استفاده از تکنیک تزریق ترافیک (traffic insertion) از چند روز به چند ساعت تقلیل می دهند . در این روش حجم وسیعی ترافیک کاذب برای بازیابی کلید ایجاد می شود . معمولا" برای برپایی یک WEP دستی اغلب تنها از یک کلید منفرد از چهار کلید برای گسترش شبکه استفاده می کنند که در مدت زمان بسیار کوتاه تری می توان شبکه را کاملا" تسخیر کرد. با وجود آسیب پذیری ها WEP همچنان مورد استفاده قرار می گیرد. نسل جدید رمزنگاری ها از پروتکل TKIP استفاده می کند که امتیازاتی همچون Integrity Check Per Packet Key Mixing و یک مکانیسم Re-Keying را فراهم می نماید . کلید ها به اندازه ای زود تغییر می کنند که مانع تسخیر و سوء استفاده شوند.اما چون اطلاعات روی هوا فرستاده می شود امکان دسترسی به آن وجود دارد و اگر رمزنگاری نشده باشد . به راحتی قابل استفاده خواهد بود.

۶. ابزارشکستن احراز هویت(Authentication)

هکر ها از ابزارهایی مانند THC-LEAPCracker برای شکستن یا تسخیر انواع مختلف و متداول پروتکلهای احراز هویت مبتنی بر پورت برای ۸۰۲,۱۱ Xبی سیم مانند پروتکل LEAP (Lightweight Extensible Authentication Protocol)و یا PEAP (Protected Extensible Authentication Protocol) استفاده می کنند. [۵]

این پروتکل ها برای استفاده شبکه های محلی با بستر سیمی که از نظر فیزیکی در محیطی امن قرار دارند طراحی شده اند. زمانی که اطلاعات در محیط اشتراکی و غیر قابل کنترل بی سیم پراکنده می گردد هکر ها به راحتی می توانند گواهینامه های احراز هویت را spoof jump in the middle و یا بوکشی کنند

۷. حملات متداول شبکه های محلی بی سیم

دراین قسمت چند حمله متداول بر روی شبکه های محلی بی سیم را بیان می کند که نمایانگر خطرات و ریسکهای مشخص آن می باشد. با گوناگونی و تنوع فعلی ابزار های هک که بصورت گسترده ای در اینترنت موجود می باشند حتی یک هکر نو آموز و تازه کار می تواند بسیاری از حملات منتشر شده را اجرا نماید.

تماس های تصادفی یا مغرضانه

یک هکر می تواند یک کاربر ساده را وادار نماید تا بصورت کاملا نا خودآگاه به یک شبکه spoof شده ۸۰۲,۱۱ متصل شود و یا اینکه تنظیمات این دستگاه را به گونه ای تغییر دهد که که در یک شبکه ad-hoc قرار گیرد. برای شروع یک هکر از یک laptopبعنوان یک access point نرم افزاری استفاده می کند که برای این کار از ابزارهای رایگانی همچون HostAP AirSnarf Hotspotterو یا ابزارهای موجود تجاری می توان استفاده کرد. (بعنوان مثال شرکت هایی همچون PCTel نرم افزار های تجاری تولید می کنند که تجهیزات ۸۰۲,۱۱ را به access point تبدیل می کنند/

همینطور که کامپیوتر قربانی یک درخواست برای اتصال به یک access point را broadcast می کند access point نرم افزاری هکر به این درخواست پاسخ می دهد و یک اتصال بین این دو برقرار می گردد. سپس این access point نرم افزاری یک آدرس IP به این کامپیوتر اختصاص می دهد . پس از اینکه این کار انجام شد هکر می تواند کامپیوتر قربانی را scan کرده و در آن به گشت و گذار بپردازد اطلاعاتی را برباید Trojan Horse و یا Spyware نصب کند و یا اگر کامپیو تر قربانی به یک شبکه مبتنی بر سیم متصل باشد از این کامپیوتر می تواند بعنوان راه ارتباط برای نفوذ به سرور های دیگر این شبکه استفاده کند.

شبکه های محلی بی سیم دستخوش دگرگونی فراوان هستند و اغلب ایستگاه های کاری نمی دانند به کدام access point متصل هستند. و از آنجایی که اغلب هیچگونه احراز هویتی برای اتصال به access point ها صورت نمی گیرد ایستگاه های کاری می توانند فریب خورده و یا مجبور به اتصال با یک access point نا امن شوند. این یک آسیب پذیری در لایه ۲ (Data Linkاز مدل ۷ لایه شبکه (OSI:Open System Interconnection) می باشد. نه احراز هویت لایه ۳ (شبکه) هیچگونه محافظتی در مقابل آن ارائه نمی دهد و نه استفاده از شبکه های مجازی شخصی . (VPN) احراز هویت لایه ۲ شبکه های محلی بی سیم مبتنی بر ۸۰۲,۱ xبرای محافظت در مقابل ارتباطات مشکوک می تواند مفید باشد ولی دارای آسیب پذیری های زیادی است[۶].

یک ارتباط مغرضانه و مشکوک سعی در شکستن VPN و یا موازین امنیتی ندارد ولی در عوض از لایه ۲ برای تسلط بر client ها استفاده می کند. برای جلوگیری از اتصال کاربرها به access point ها و شبکه های غیر مجاز شرکت ها باید مرتبا" امواج حوالی شبکه ی بی سیم خود را بررسی کنند تا از هرگونه خطراحتمالی مطلع شوند.

عملا هیچ شبکه ای به طور کامل امن نیست!!!

یک متخصص علوم کامپیوتر گفته : اگه دوست دارید که کسی به سیستم شما (یا شبکه) نفوذ نکنه ، هیچ وقت اون رو روشن نکنید

۸. مراجع

۱. Kifayat, K., et al., Security in wireless senso r networks, in Handbook of Information and Communication Security. ۲۰۱۰, Springer. p. ۵۱۳-۵۵۲.

۲. Ko, J., et al., Wireless sensor networks for healthcare. Proceedings of the IEEE, ۲۰۱۰. ۹۸(۱۱): p. ۱۹۴۷-۱۹۶۰.

۳. Panda, M. Data security in wireless sensor networks via AES algorithm. in Intelligent Systems and Control (ISCO), ۲۰۱۵ IEEE ۹th International Conference on. ۲۰۱۵. IEEE

٤. Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key echniques. in Computer Communication and Informatics (ICCCI), ۲۰۱۲ International Conference n. ۲۰۱۲. IEEE.

٥. Jain, A., K. Kant, and M. Tripathy. Security solutions for wireless sensor networks. in ۲۰۱۲ Second International Conference on Advanced Computing & Communication Technologies. ۲۰۱۲. IEEE.

٦. Jain, A., K. Kant, and M. Tripathy. Security solutions for wireless sensor networks. in ۲۰۱۲ Second International Conference on Advanced Computing & Communication Technologies. ۲۰۱۲. IEEE.