فصلنامه علمی-ترویجی پدافند غیرعامل
سال هشتم، شماره ۲، تابستان ۱۳۹۶، (پیاپی ۳۰): صص ۳۴-۲۳

مروری بر امنیت، حریم خصوصی، حسابرسی و مدیریت کلید در شبکه‌های بی‌سیم

رحیم یزدانی[۱]، علی محمدی[۲*]، ناصر مدیری[۳]

تاریخ دریافت: ۱۳۹۴/۱۲/۰۲
تاریخ پذیرش: ۱۳۹۵/۰۶/۰۸

چکیده

طی سال‌های اخیر، شبکه‌های بی‌سیم به‌جهت سهولت استفاده، گستردگی کاربرد و تنوع خدمات، بسیار مورد توجه قرار گرفته است. ازجمله کاربردهای این شبکه‌ها می‌توان به حوزه‌های تجارت، سلامت، نظامی و خودکارسازی خانگی اشاره کرد. ازجمله موضوعات مهم در این شبکه‌ها امنیت، حسابرسی، حریم خصوصی و مدیریت کلید است. فعالیت‌های علمی زیادی درخصوص این موضوعات صورت پذیرفته است که به‌صورت پراکنده قابل دست‌یابی و بهره‌برداری است. دسته‌بندی و بررسی ویژگی‌های روش‌های ارائه‌شده در یک مطالعه می‌تواند کمک شایانی به پژوهشگران برای تکمیل و توسعه علوم مربوطه و همچنین برای بهره‌برداران از این شبکه‌ها باشد. در این مقاله طرح‌های ارائه‌شده برای ارتقاء امنیت، حسابرسی، حریم خصوصی و مدیریت کلید در شبکه‌های بی‌سیم دسته‌بندی و بررسی گردیده و ویژگی‌های منحصربه‌فرد هر طرح نیز ذکر شده است. این پژوهش ازنظر نوع پژوهش، کاربردی و ازنظر رویکرد، کیفی و ازنظر روش، توصیفی تحلیلی و ازنظر طرح پژوهش گذشته‌نگر و نتیجه‌گراست. یافته‌ها نشان می‌دهد که طرح‌های رمزنگاری فرصت‌طلبانه، IRL، Hybrid-Accountability و +LEAP به‌ترتیب در مقوله ارتقاء امنیت، حفظ حریم خصوصی، حسابرسی و مدیریت کلید از جامعیت نسبی برخوردارند.

کلیدواژه‌ها: شبکه‌های بی‌سیم، امنیت، حسابرسی، حریم خصوصی، مدیریت کلید.

۱- دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی
۲- عضو هیات علمی، گروه مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، Email:mohammadii@aut.ac.ir- نویسنده مسئول
۳- عضو هیات علمی، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، زنجان

۱- مقدمه

امروزه فناوری‌های بی‌سیم در زندگی روزانه بشر بیشتر ظهور و بروز پیدا کرده است. دستیارهای[1] رقمی اجازه دسترسی انفرادی را به وب و پست الکترونیکی و شبکه‌های اجتماعی و ... می‌دهد. برخی از فناوری‌ها مجهز به خدمات تعیین موقعیت جهانی[2] بوده و مکان وسیله را در سراسر جهان نشان می‌دهد. تعداد کثیری از مؤسسات در نواحی مختلف عمومی، بخش‌های خصوصی و کاربرهای خانگی از فناوری‌های ارتباطی بی‌سیم استفاده می‌کنند. از ویژگی‌های مفید این فناوری می‌توان به قابلیت سیار، انعطاف‌پذیری، پایین‌بودن هزینه نصب و سوددهی افزایشی آن اشاره کرد. این فناوری محدوده وسیعی را پوشش می‌دهد به‌طوری‌که می‌توان رایانه را از ناحیه‌ای به ناحیه دیگری بدون از دست‌دادن اتصال و بدون نیاز به سیم‌کشی جابجا کرد. سیم‌کشی کمتر و درنتیجه انعطاف‌پذیری بیشتر و به‌تبع آن هزینه کمتر، ازجمله مزایای دیگر این شبکه‌ها است. به‌عنوان مثال شبکه‌های ارتباطی بلوتوث اجازه ارسال داده و همگام‌سازی را از طریق دستگاه‌های شبکه و به اشتراک‌گذاری بین تجهیزات مختلف می‌دهد. همچنین با این فناوری کابل‌کشی برای چاپگر، اسکنر، پلاتر و دیگر وسایل محیطی حذف شده است. تجهیزات دستی همانند تلفن‌های همراه اجازه می‌دهند که کاربر به خدمات شبکه همانند اینترنت دسترسی داشته باشند؛ اما با وجود این‌که این فناوری‌ها قابلیت‌های متنوع جدیدی را به همراه دارند، آسیب‌پذیری‌های بیشتری نسبت به شبکه‌های سیمی دارند. برخی از آسیب‌پذیری‌ها مشابه آسیب‌پذیری‌های شبکه‌های سیمی و برخی دیگر مختص شبکه‌های بی‌سیم است. مخدوش ساختن محرمانگی، جامعیت و تهدید منع خدمات[3] همواره ارتباطات بی‌سیم را تهدید می‌کنند. ممکن است کاربران غیرمجاز به شبکه ارتباطی دسترسی داشته باشند و داده‌ها و پهنای باند را تسخیر کنند و کارکرد شبکه را کاهش داده و حمله‌ای را ترتیب دهند که مانع از دسترسی کاربران مجاز به شبکه شوند و یا از منابع برای راه‌اندازی حمله به دیگر شبکه‌های ارتباطی استفاده کنند. لذا ممانعت از دسترسی غیرمجاز، حفاظت از حریم خصوصی کاربر، استفاده از سازوکارهای عدم انکار و پاسخگوبودن سیستم و همچنین مدیریت کلید جزو دغدغه‌های پژوهشگران درخصوص شبکه‌های بی‌سیم است.

بنابراین، شناخت آسیب‌پذیری‌ها، تهدیدات و همچنین طرح‌های مقابله با مخاطرات این شبکه‌ها ضروری است تا درصورت راه‌اندازی و یا استفاده از این شبکه‌ها، از طرح‌های پیشنهادی برای کاهش مخاطرات استفاده شود.

در این پژوهش طرح‌های ارائه‌شده برای ارتقاء امنیت (تشخیص نفوذ و ممانعت از دسترسی غیرمجاز)، حسابرسی (ردیابی و غیرقابل انکارکردن اتفاقات)، حفظ حریم خصوصی (حفظ حریم مکانی و هویتی کاربر) و مدیریت کلید (توزیع کلیدهای محرمانه) در شبکه‌های بی‌سیم بررسی گردیده است. ضرورت تحقیق در آن است که درصورت ضعف‌داشتن شبکه بی‌سیم در هرکدام از مقوله‌های فوق، باعث مشکلاتی مانند عدم تشخیص ورود غیرمجاز به شبکه بی‌سیم، ردیابی گام‌به‌گام و شناسائی حریم مکانی کاربر و مسیر داده و هویت کاربر، شکل‌گیری انواع حملات علیه شبکه و ضعف امنیت ارتباطات می‌شود.

در ادامه، ابتدا مقدمه سپس مروری بر شبکه‌های بی‌سیم بیان گردیده است. در بخش بعد طرح‌های ارائه‌شده در حوزه‌های امنیت، حریم خصوصی، حسابرسی و مدیریت کلید در شبکه‌های بی‌سیم بررسی گردیده و در انتها جمع‌بندی و نتیجه‌گیری ارائه گردیده است.

۲- شبکه‌های بی‌سیم

شبکه‌های بی‌سیم به شبکه‌های رایانه‌ای اشاره می‌کند که از کابل برای اتصال استفاده نمی‌کنند. این روشی است که سازمان‌ها از کابل‌کشی پرهزینه برای شبکه‌کردن و متصل‌کردن تجهیزات مختلف اجتناب می‌کنند. ارتباطات بی‌سیم از امواج رادیوئی استفاده می‌کنند.

شکل ۱- نمایی از یک شبکه بی‌سیم

1- Assistants
2 -GPS
3 -DoS

در شبکه‌های بی‌سیم که شبکه‌هایی با رسانه ارتباطی هوا است، منظور از ارتقاء امنیت، استفاده از طرح‌هایی برای تشخیص نفوذ و ممانعت از دسترسی غیرمجاز است. درحالی‌که هدف از طرح‌های حفظ حریم، استفاده از طرح‌هایی برای حفظ حریم مکانی، هویتی و ترافیکی کاربر است. همچنین با استفاده از طرح‌های حسابرسی، دنبال عدم انکار اتفاقات و قابلیت ردیابی‌کردن اتفاقات در یک شبکه بی‌سیم است. و نهایتاً با استفاده از طرح‌های مدیریت کلید، نحوه توزیع کلیدهای محرمانگی برای ارسال داده بررسی می‌شود.

شبکه‌های حسگر بی‌سیم برای نظارت و کنترل یک محیط خاص استفاده می‌شود. این شبکه مرکب از تعداد زیادی گره و حسگر پراکنده است. اطلاعات جمع‌آوری شده به‌وسیله حسگر یا مستقیم و یا با چندگام به ایستگاه پایه ارسال می‌شود. طول عمر شبکه بستگی به مصرف انرژی دارد. برای افزایش طول عمر شبکه و مدیریت مصرف انرژی، خوشه‌بندی گره‌ها مناسب است. در خوشه‌بندی، شبکه به تعدادی خوشه مستقل قسمت‌بندی می‌شود که هرکدام یک سر خوشه دارند و همه اطلاعات گره‌های داخل خوشه را جمع می‌کنند سپس این سر خوشه‌ها اطلاعات را مستقیماً یا گام‌به‌گام و صرفاً با استفاده از گره‌های سرخوشه به مرکز اصلی (گره چاهک) می‌فرستند. لذا هزینه ارتباطی کاهش می‌یابد. نقش گره چاهک شامل جمع‌آوری داده، برنامه‌ریزی مجدد حسگرها و تشخیص و لغوکردن گره‌های مشکل‌دار است. در طرح‌های موجود از جفت کلید بین گره‌های حسگر و چاهک استفاده می‌شود و مهاجم امکان دارد با تعدادی کلید، بخشی از گره‌ها را در اختیار بگیرد و شروع به تکثیر چاهک نماید.

۳- مفاهیم پایه

طبیعت ارتباط بی‌سیم، اجازه دریافت سیگنال ارسالی را در محدوده مشخصی می‌دهد لذا مهاجم قادر به انواع حملات غیرفعال (مانند استراق، تحلیل ترافیک و...) و فعال (پارازیت، اصلاح، منع خدمات و...) خواهد بود. برای امن‌سازی داده از الگوهای رمزنگاری کلاسیک می‌توان استفاده کرد. این الگوها به‌حدی پیچیده هستند که زمان لازم برای رمزشکنی بسیار بیشتر از زمان اعتبار پیام است. این الگوها شامل دو نوع رمزنگاری کلاسیک (رمزنگاری متقارن[1] با کلیدهای همسان و رمزنگاری نامتقارن[2] با کلید عمومی و جفت کلیدهای اختصاصی متفاوت مورد استفاده برای توزیع کلید) و امن‌سازی لایه فیزیکی (امنیت بدون کلید[3] و پنهان‌سازی کلید پایه[4]) است [۱]. رمزنگاری کلاسیک که به لایه‌های بالاتر پروتکل‌های ارتباطی اعمال می‌شود، بستگی به پیچیدگی محاسباتی لگاریتم گسسته دارد. همچنین نیاز به زیرساخت مدیریت کلید دارند. لذا در شبکه‌های حسگر بی‌سیم وادهاک(شبکه های آنی و موقت با گره های متحرک و فاقد هسته مرکزی) که‌دلیل محدودیت ظرفیت محاسباتی‌شان و توزیع‌یافتگی‌شان کاربرد ندارند. الگوهای امنیت لایه فیزیکی[5] نیز از مشخصه تصادفی و غیرقابل پیش‌بینی‌بودن کانال ارتباطی برای افزایش امنیت اطلاعات استفاده می‌کنند. این الگوها متشکل از «امنیت بدون کلید» که از طراحی کد ویژگی کانال ارتباطی استفاده می‌کند و «پنهان‌سازی کلید پایه» هستند که در آن هر بیت پیام با بیت تصادفی کلید مخفی مستخرج از کانال، رمز می‌شود و از کاربردهای آن می‌توان به WLAN[6]، WSN[7] اشاره کرد.

ازجمله حملات متعددی که به شبکه حسگر بی‌سیم می‌شود و باعث نقص حریم می‌شود می‌توان به سایبل[8] (یک ابزار بدخواه نادرست با جعل هویت جهت حمله به پروتکل‌های مسیریابی)، سیاه چاله[9] (استراق سمع درخواست‌های مسیر و انحراف هدفمند مسیرها)، تحلیل ترافیک، کرمچاله[10] (ضبط بسته‌های ترافیکی و انتقال آن‌ها با تونل‌زنی در مرحله شناسایی حسگرهای همسایه)، حمله Helloflood (جا انداختن حسگر دشمن به‌عنوان دوست با استفاده از بسته‌های سلام) اشاره کرد.

۴- کارهای انجام‌شده

سریشا [۲]، چارچوب امنیتی سه‌وجهی برای تصدیق و برقراری کلید جفتی بین گره‌ها و چاهک از طریق مسیریاب و سرور پیشنهاد کرده است. همچنین در این چارچوب برای انتقال امن داده از الگوریتم رمزنگاری استفاده می‌شود. ژانگ [۱]، روش‌هایی مختلفی را مقایسه می‌کند که با استفاده از «اعمال کانال‌های مجازی» یا «شکل‌دهی تصادفی به تشعشعات آنتن» در کانال‌های بی‌سیم کلید تولید می‌کنند ولی استدلال کرده که این روش‌ها عام نبوده و چند آنتنه و یا مدولاسیون متعامد نیاز دارند. همچنین استدلال کرده که با

1 -Symmetric Encryption
2- Asymmetric Encryption

3 -Keyless Security
4 -Secret Key-Based Secrecy
5-Physical Layer Security(PLS)
6 -Wireless Local Area Networks(WLAN)
7-Wireless Sensor Networks(WSN)
8 -Sybil
9 -Blackhole
10 -Wormhole

استفاده از خواص لایه فیزیکی محیط بی‌سیم مثلاً طیف و عدم همبستگی کانال رادیوئی، می‌توان خدمات محرمانگی و احراز هویت را ارتقاء داد. سودیک [۳]، امنیت و حریم خصوصی را در برخی از شبکه‌های بی‌سیم نوظهور آزموده است. در این مطالعه چالش‌های حریم خصوصی و چالش‌های امنیتی و همچنین نارسایی رویکردهای جاری مشخص شده است. برخی از چالش‌ها از عدم مراقبت، اتصالات بین‌راهی و عملکرد شبکه موبایل ناشی می‌شود.

لی [۴]، به چالش‌های امنیتی و حریم خصوصی یکی از کاربری‌های شبکه بی‌سیم در حوزه سلامت پرداخته و نیازمندی‌های امنیتی و حریم خصوصی داده‌های شخص مریض که از طریق حسگرهای کاشته‌شده جمع‌آوری‌شده و از بستر ارتباطی بی‌سیم با برد کوتاه به دستگاه‌های پاسخ پزشکی اضطراری منتقل می‌شود احصاء شده است.

کین [۵]، به نیازمندی‌های امنیتی شبکه‌های بی‌سیم زمان واقعی مدرن برای تحویل‌دهی امن بسته‌های اطلاعاتی ذخیره‌شده به گیرنده پرداخته و سپس یک الگوی جدید پویا بر اساس امنیت ـ مراقبت و زمان‌بندی ـ بسته پیشنهاد کرده است. به‌طوری‌که قادر است امنیت با کیفیت بالا را برای بسته‌های زمان واقعی برقرار کند. این الگوی پیشنهادی هم کیفیت امنیت و هم‌زمان واقعی‌بودن بسته‌ها در محدوده وسیعی را تضمین می‌کند.

جیندال [۶]، چارچوبی را به نام رمزنگاری فرصت‌طلبانه پیشنهاد کرده که از فرصت‌های کانال (نسبت سیگنال به نویز قابل قبول) برای حداکثرکردن توان عملیاتی طبق مراحل زیر استفاده می‌کند.

الف) مدل‌های ریاضی جهت به‌دست‌آوردن نقطه توازن بین توان عملیاتی و امنیت

ب) مدل‌کردن دشمن و حملات آن‌ها

ج) پیونددادن بهینه مدولاسیون و رمزنگاری

د) استفاده از کدهای تصحیح خطا به‌صورت جلورونده برای حفاظت بسته‌ها از خطا

هـ) شبیه‌سازی نتایج برای رمز Rijndael

این الگوی رمزنگاری فرصت‌طلبانه، در اجرا پیشرفت معنی‌داری را نسبت به رویکردهای سنتی می‌دهد.

شین [۷]، بحث جامعی از مشکلات امنیتی و فناوری‌های جاری در دستگاه‌های شبکه‌های محلی بی‌سیم و نسل سوم ارائه کرده و پیشنهادهایی برای مشکلات مزبور ارائه کرده است. دنگ [۸]، بررسی امنیتی شبکه‌های سیار را ارائه کرده و به‌صورت ویژه یک نوع حمله با نام حفره سیاه را که به‌راحتی علیه شبکه‌های سیار استفاده می‌شود، مورد مطالعه قرار داده و راه‌حلی برای مشکل حفره سیاه ارائه کرده است. جیونگ [۹]، ضمن پرداختن به سازوکار امنیتی جامع که یکی از چالش‌های معماری شبکه‌های بی‌سیم بازاست، خواص یکتایی تمرکز–شبکه و سازوکارهای امنیتی شبکه‌های بی‌سیمی ناهمگن را که بخشی از شبکه‌های بی‌سیم باز هستند، نسبت به هم تحلیل کرده و نهایتاً یک طرح امنیتی جامع بر اساس مفهوم امنیت پیشنهاد داده است.

۵- حسابرسی در شبکه‌های بی‌سیم

حسابرسی یک مقوله مهم در دستگاه‌های رایانه‌ای و شبکه‌ای است. از اهداف حسابرسی، عدم امکان انکار دریافت یا ارسال توسط گیرنده و فرستنده و همچنین قابلیت ردیابی یک اتفاق است به‌طوری‌که بعد از وقوع اتفاق علت آن قابل شناسایی باشد. مثلاً با استفاده از حسابرسی می‌توان ردیابی کرد که چه اتفاقاتی در مبادلات بانکی یک شخص رخ داده است. این کار با مرور مبادلات و با علم به این‌که چه کسی از طریق یک شناسه مشخص کاربر وارد حساب بانکی شده است امکان‌پذیر است. تقریباً تمام پروتکل‌ها نیازهای جامعیت را پشتیبانی می‌کنند به‌طوری‌که محتویات ارتباطات نمی‌توانند تغییر یابند، اما بیشتر آن‌ها از عدم انکار پشتیبانی نمی‌کنند و به این ترتیب امکان ایجاد رکوردهای پایداری را که هویت منبع را به محتوای پیام پیوند دهند، ندارند. استانداردهای بی‌سیم در لایه‌های ۱ و ۲ مدل OSI هستند و لذا مبحث حسابرسی در لایه‌های بالاتر پروتکل بایستی پیاده‌سازی شود. طرح Hybrid که در جدول (۱) ارائه شده است و ترکیبی از Flow-net برای تشخیص حملات و P-Accountability و Q-Accountability برای افزایش حسابرسی است، طرح جامع و پرکاربرد است [۱۴].

در جدول (۱)، راه‌حل‌های پیشنهادشده توسط افراد مختلف مذکور در ردیف مؤلف برای افزایش جوابگویی و حسابرسی در شبکه های متنوع بی‌سیم و ملاحظات و مراحل مربوط به هر راه‌حل در ستون انتهایی ذکرشده است.

جدول ۱- حسابرسی در شبکه بی‌سیم

ردیف	مؤلف	نام طرح پیشنهادی	توضیحات
۱	یانگ [۱۰]	A-NET	یک معماری تضمینی برای شبکه با نام A-NET پیشنهاد می‌شود که مدیریت پاسخگو و قابل حسابرسی نام دارد. این طرح برای شبکه‌های محلی و شبکه‌های مش بی‌سیم ارائه شده است.
۲	یانگ [۱۱]	Flow-NET	۱- این روش به لایه‌های مسیریابی و کنترل محیط دسترسی در شبکه‌های بی‌سیم اعمال می‌شود. ۲- رویکرد این طرح بر مبنای تجمیع ترافیک داده و بررسی فایل‌های ثبت شده است و برای تشخیص ورود غیرمجاز نیز استفاده می‌شود. ۳- دقت این طرح به پارامترهای زیادی بستگی دارد و قابل تأمل است.
۳	لو [۱۲]	طرح امضای Boneh and Shacham	در این طرح، تجمیع امنیت، حفظ حریم و حسابرسی با محوریت حسابرسی در شبکه‌های بی‌سیم دیده‌شده است.
۴	ژیفنگ [۱۳]	P-Accountability	۱- برای حسابرسی شبکه‌های بی‌سیم چند گامی است. ۲- ارزیابی ورود به سیستم پاسخگو از طریق مشخصه کاربران پذیرفته شده است. ۳- قابل استفاده در محیط شبکه سلسله مراتبی است. ۴- می‌توان به درجات مختلفی از حسابرسی دست یافت.
۵	فو [۱۴]	Hybrid (Flow-net with P- and Q-Accountability)	۱- حسابرسی را به‌صورت قابل سنجش بیان کرده است. ۲- از طریق تعیین اثر انگشت، قادر به تشخیص حملات است ۳-ثبت وقایع را بهینه کرده است ۴- دارای کاربرد وسیعی است (درحوزه‌های اجتماعی، اقتصادی، شبکه‌های توزیعی)

۶- حریم خصوصی در شبکه‌های بی‌سیم

هدف، جلوگیری از ردیابی حرکات کاربر در محیط بی‌سیم است. در واقع از طریق مکان کاربر، مهاجم اطلاعاتی درباره کاربر کسب می‌کند. البته مکانیسم‌های حفظ حریم مکان در کنار بالابردن حفاظت حریم باعث اختلال وسیع در شبکه و کاهش کارایی می‌شود. افراد زیادی بر روی حریم داده، مکان منبع، حریم مکان گره‌های اصلی، حریم لول شبکه کار کرده‌اند که از سازوکارهای متنوع استفاده شده است که از آن جمله می‌توان به CPDA، SMART، IRL، LPR اشاره کرد که در جدول (۲) به‌طور مشروح آمده است. در جدول (۲)، راه‌حل‌های پیشنهادشده توسط افراد مذکور در ردیف مؤلف برای ارتقای حفظ حریم خصوصی و ملاحظات و مراحل مربوط به هر راه‌حل در ستون انتهایی ذکرشده است.

۷- امنیت در شبکه‌های بی‌سیم

امنیت شبکه‌های بی‌سیم عبارت است از ممانعت از دسترسی‌های غیرمجاز به رایانه‌های موجود در شبکه بی‌سیم مبتنی بر استاندارد، IEEE 802 11 .

سه پروتکل امنیتی WPA2،WPA،WEP معرفی‌شده‌اند.WEP بسیار ضعیف بوده و درعرض چند ثانیه قابل شکستن است. WPA که در سال ۲۰۰۳ یعنی یک سال قبل از از دور خارج شدن WEP معرفی شد کلید را به صورت دینامیک تغییر می داد و امنیت بیشتری نسبت به کلید ثابت استفاده شده در WEP داشت ولی آسیب پذیری WPA نیز همچون نسل پیشین آن به وسیله proof-of-concept و همچنین به وسیله آزمایش های مختلف اثبات شد. WPA2 که بالاترین امنیت را دارد برای رمزنگاری شبکه از ۲۵۶ بیت کلید استفاده می‌کند. طولانی‌بودن طول کلید امنیت را بهبود بخشیده است.

حملاتی مانند تحلیل ترافیک، استراق سمع فعال، استراق سمع غیرفعال، دسترسی غیرمجاز، حمله ملاقات در میانه، تکرار (گرفتن غیرفعال یک داده) و ارسال مجدد، پارازیت، انکار خدمات، وقفه، اصلاح، شنود، جعل، کلاه‌برداری و ... تهدیدات امنیتی هستند [۲۳].

در جدول (۳)، راه‌حل‌های پیشنهادشده توسط افراد مذکور در ردیف مؤلف برای ارتقای امنیت و ملاحظات و مراحل مربوط به هر راه‌حل در ستون انتهایی ذکر شده است.

جدول ۲- حفظ حریم خصوصی در شبکه‌های بی‌سیم

ردیف	مؤلف	راه‌حل پیشنهادی	توضیحات
۱	دفراوی [۱۵]	PEUC-WiN	طرح ارائه‌شده اهدافش را از طریق به‌کارگیری همکاری کاربران در ناحیه تحت پوشش نقطه دسترسی پیگیری می‌کند.
۲	ونبو [۱۶]	Cluster-based Private Data and Aggregation (CPDA) Slice-Mix-AggRegaTe (SMART)	در شبکه‌های حسگر بی‌سیم، تجمیع داده همراه با حفظ حریم چالش است. در طرح CPDA، از پروتکل‌های خوشه‌بندی و خواص جبری چندجمله‌ای‌ها برای گردهم‌آوری دو مقوله تجمیع داده و حفظ حریم خصوصی استفاده می‌کند درحالی‌که در SMART برپایه روش‌های برش‌دهی و خواص شرکت‌پذیری داده‌های جمع‌آوری‌شده هست. CPDA، دارای سرریز ارتباطی پایین (هزینه ارسال و دریافت و طول مسیر) ولی سرریز محاسباتی بالاست. درحالی‌که در SMART سرریز محاسباتی پایین است.
۳	شیخ [۱۷]	Identity, Route and Location (IRL)	۱- این طرح شامل حفظ حریم داده، مکان، مسیر و هویت کاربر است (طرح جامع حفظ حریم). ۲- حفظ جامع حریم به‌خاطر محدودیت‌های اعمالی از طرف گره‌های حسگر و مشکلات کیفیت خدمات، بحث مهم چالشی است. ۳- این طرح مؤثر در قبال حملات استراق سمع و ردیابی گام‌به‌گام است. ۴- این طرح قابلیت اعتماد را شدیداً افزایش داده است. ۵- متنوع‌کردن تعداد مسیرها و طولانی مسیرها از ویژگی این طرح است. لذا از نظر هزینه انرژی و حافظه قابل تأمل است.
۴	ینگ [۱۸]	Location privacy routing protocol (LPR)	۱- با توجه به ماهیت باز شبکه حسگر، استراق سمع و ردیابی بسته‌ها و درنهایت در اختیار گرفتن گیرنده کار مشکلی نیست. ۲- این طرح، به‌منظور حفظ حریم مسیر، از تزریق بسته‌های جعلی استفاده می‌کند تا مهاجم اطلاعات ترافیکی کمتری کسب نماید. ۳- در واقع توزیع یک‌نواختی به ورودی‌ها و خروجی‌های هر گره اعمال می‌شود لذا تحلیل و کشف محل تجمع اطلاعات و تشخیص سمت گیرنده برای مهاجم سخت می‌شود. ۴- سه پارامتر زمان تحویل بسته، قدرت حفاظت از حریم و هزینه انرژی محور این طرح است. ۵- این طرح دارای زمان امن طولانی‌تری نسبت به طرح‌های مسیریابی دیگر است.
۵	جیانبو [۱۹]	Data Aggregation Different Privacy-levels Protection (DADPP)	در DADPP، همه گره‌های داخل یک خوشه، به گروه‌هایی متناسب با سطوح مطلوب حریم جزءبندی شده‌اند. سطح حفظ حریم تناسب مستقیم با سرریز محاسباتی و ارتباطی دارد. لذا حفظ حریم بالا، سرریز بالایی خواهد داشت.
۶	یانفی [۲۰]	Coding Based Privacy-Preserving	۱- طرح پیشنهادشده دو ویژگی مهم حفظ حریم را پیشنهاد کرده تا حملات آنالیز ترافیک خنثی شوند. این دو ویژگی عبارتنداز: غیرقابل ردیابی بودن جریان بسته و محرمانگی محتوای پیام ۲- طرح پیشنهادی خاصیت کدگذاری تصادفی را دارد و هرکدام می‌توانند بسته‌های منبع را از طریق معکوس‌کردن بازیابی کنند.
۷	محمد [۲۱]	Cloud-Base	۱- این طرح برای حفظ حریم مکان-منبع در قبال حمله تشخیص مکان‌های حساس در شبکه‌های حسی است. ۲- با ایجاد یک ابر با شکل نامنظم ترافیکی و مخفی‌کردن گره‌های اصلی (منبع) در داخل ابر، الگوی ترافیک شبکه خنثی می‌شود. ۳- به‌منظور کاهش هزینه انرژی، ابرها فقط در حین ارسال داده فعال می‌شوند.
۸	ژیگو [۲۲]	Priv-Code	۱- این روش بر اساس کدگذاری شبکه در قبال حملات تحلیل شبکه است. ۲- بهینه‌سازی، یکسان‌بودن سرعت انتقال هر گره، حفاظت حریم قوی‌تری نسبت به سیستم ترکیبی، عملکرد بهتر شبکه پارامترهای مهم در این طرح هستند.

جدول ۳- امنیت در شبکه بی‌سیم

ردیف	مؤلف	پیشنهادها	توضیحات
۱	لازیم [۲۴]	Wireless Intrusion Detection System (WIDS)	یک سیستم تشخیص نفوذ بی‌سیم به‌منظور حفاظت شبکه بی‌سیم چندکاربره طراحی و اجرا شده است. این طرح جهت جا گرفتن در وسایل بی‌سیمی مختلف بسیار کوچک بوده و همچنین هزینه پایین و اجرای قابل قبول دارد تا بتواند سرعت ارسال داده را در شبکه‌های محلی بی‌سیمی حمایت کند.
۲	جی [۲۵]	DLMSA	۱- این طرح برای تشخیص و تعیین محل حملات کلاه‌برداری[1] در شبکه‌های بی‌سیم است. ۲- این روش، از داده‌های مکانی، خواص فیزیکی گره‌ها و بدون اتکا به رمزنگاری استفاده می‌کند. ۳- تعداد مهاجمان از طریق مکانیسم‌های خوشه پایه[2] تعیین می‌شود (وقتی‌که چندین مهاجم مبدل از یک گره استفاده می‌کنند).
۳	راشد [۲۶]	Three-Tier Security	وظیفه گره چاهک، تجمیع داده، برنامه‌ریزی مجدد، تشخیص و حذف حسگر معیوب است. این طرح برای جلوگیری از حملات تسخیر گره و تکرار گره از دوسری کلید استفاده می‌کند؛ که یک سری برای ارتباط حسگرها با هم و سری دیگر برای ارتباط بین سینک و نقطه خاصی از شبکه است.
۴	یان [۲۷]	تشخیص نفوذ پیوندی	سیستم تشخیص پیشنهادی یک سیستم تشخیص نفوذ پیوندی است که شامل برد تشخیص سوءاستفاده و نامتعارف است. هدف، ترفیع نرخ تشخیص صحیح و کاهش نرخ مثبت کذب از طریق مزایای تشخیص استفاده سوء و نامتعارف است.
۵	ویجیا [۲۸]	Secure and Distributed Reprogramming Protocol (SDRP)	در شبکه‌های حسگر بی‌سیم، موقع تغییرات در گره‌ها، نیاز به بازسازی مجدد مسیرهای مسیریابی و انتخاب سرخوشه جدید تزریق کدهای اجرایی به گره‌ها ... است. می‌توان این برنامه‌ریزی را در سطح گره‌ها توسط افراد مجاز و بدون ایستگاه مرکزی انجام داد که در این طرح پیشنهاد شده است. این طرح مقاوم در برابر حمله جعل هویت است. اضافه‌کردن داده جهت جبران‌سازی ضعف طراحی، از ویژگی طرح است.
۶	مائورو [۲۹]	Randomized, Efficient, and Distributed (RED) Protocol	یکی از حملات علیه شبکه‌های حسگر بی‌سیم، تکثیر گره‌های جعل‌شده و به‌دست‌آوردن کنترل شبکه است. این پروتکل توزیع‌یافته و مؤثر و تصادفی‌شده برای کشف تکثیر گره است که نیاز به حافظه کم و مصرف کم انرژی دارد. از محدودیت‌های این طرح، قابلیت اجرای کم در شبکه‌های متراکم است.
۷	جئورجو [۳۰]	رویکرد سیاست محور	در این طرح پیاده‌سازی مدیریت امنیت WLAN با معماری سلسله مراتبی، سیاست‌گذاری مرکزی، اعتبارسنجی سیاست‌ها و پیکربندی جدید در صورت نقض سیاست‌ها با نظارت بر نقاط دسترسی ارائه شده است. با نظارت محلی، نفوذ تشخیص داده می‌شود. این طرح در شبکه‌های با سیم نیز کاربرد دارد.
۸	دبائو [۳۱]	معماری امنیتی بر پایه تشخیص نفوذ	ارائه یک معماری امنیتی برای شبکه‌های بی‌سیمی متحرک خودسازمانی که قادر به جلوگیری از اکثر حملات بر پایه تشخیص نفوذ است. آنالیز لایه‌ای این معماری امنیتی مورد بحث قرار گرفته و اندازه‌گیری‌های امنیتی در لایه لینک و لایه شبکه با جزئیات کامل ارائه‌شده است

[1] Spoofing
[2] Cluster-based

۸- مدیریت کلید در شبکه‌های بی‌سیم

مدیریت کلید به‌عنوان بخش اساسی یک ارتباط امن محسوب می‌شود. پروتکل ارتباطی امن در شبکه، به سیستم مدیریت کلید موثر و مقاوم و امن بستگی دارد. پیاده‌سازی یک جفت کلید برای شبکه حسگر به‌دلیل مصرف انرژی و محاسبات بالا مقدور نیست. با توجه به تفاوت زیرساخت ارتباطی و محاسباتی متفاوت در این شبکه‌ها که از مقیاس بزرگ توسعه، ظرفیت محاسباتی کم و توان محدود ناشی می‌شود، نیازمندی‌های مدیریت کلید این شبکه متفاوت‌تر از دیگر شبکه‌هاست این نیازمندی‌ها عبارتنداز [۳۲]: اولاً ارتباطات حسگرها شامل فرایند توزیع کلید بین طرفین ارتباط است که ممکن است از طریق کانال ناامن تبادل شود. لازم است محرمانگی کلید و جامعیت در کل پروسه انجام شود. ثانیاً در طراحی پروتکل مدیریت کلید باید به محدودیت‌های توان توجه شود. ثالثاً طرح مدیریت کلید باید مقیاس‌پذیر باشد و شبکه‌های بزرگ را پوشش دهد. رابعاً در صورت تبانی گره حسگر، اعتبار امنیت که در گره حسگر ذخیره شده است و یا بر روی لینک رادیوئی تبادل می‌شود نباید آشکار شود. علی‌رغم چالش‌ها و نیازمندی‌های فوق‌الذکر، طرح‌هایی برای مدیریت کلید در شبکه‌های بی‌سیم ازجمله شبکه‌های حسگر خودسازمان‌ده سلسله مراتبی پیشنهاد شده‌اند؛ که در جدول (۴) نشان داده شده‌اند.

جدول ۴- مدیریت کلید در شبکه‌های بی‌سیم

ردیف	مؤلف	پیشنهادها	توضیحات
۱	کارمان [۳۳]	Survivable and Efficient Clustered Keying (SECK)	این روش برای مدیریت کلید در شبکه‌های حسگر سلسله مراتبی است که از گره‌های حسگر خوشه‌بندی‌شده حول گره‌های گیت وی تشکیل شده‌اند. ۵ سازوکار مدیریتی امنیتی ارائه می‌دهد: ۱- خوشه‌بندی و تنظیمات کلید ۲- اضافه‌شدن گره ۳- نوسازی کلید ۴- بازسازی گره‌های تسخیرشده ۵- خوشه‌بندی مجدد
۲	کارمان [۳۴]	Pairwise Asymmetric Keying	از رمز نامتقارن و تابع درهم‌ساز یک‌طرفه برای هدایت احراز هویت زیرساخت کلید عمومی و مدیریت کلید استفاده می‌کند. رمزنگاری نامتقارن ازنظر انرژی کارآمد نیست.
۳	اشنائر [۳۵]	Symmetric Keying Management	در این طرح هر گره همراه با زیرمجموعه تصادفی از کلیدها جانمایی می‌شوند. دو گره بر روی یک جفت کلید، زمانی موافقت می‌کنند که هر دو کلید رمز به اشتراک گذاشته شده را در زیرمجموعه‌شان پیدا کنند. عیب این طرح، نیازمندی به حافظه بالا است.
۴	پارک [۳۶]	LiSP(Lightweight Security Protocol)	پروتکل امنیتی سبک‌وزن، نقطه توافق بین امنیت و محدودیت منابع است که از طریق انجام کلیدکردن مجدد به دست می‌آید. قلب این پروتکل، سازوکار کلید مجدد است که ۴ مورد زیر را نتیجه می‌دهد: ۱- پخش مؤثر کلید بدون نیاز به ارسال مجدد ۲- احراز هویت برای هر کلید بدون سرآیند اضافی ۳- توانایی در کشف یا بازیابی کلیدهای گم‌شده ۴- تازه‌سازی کلید بدون توقف عملیات رمز
۵	ژو [۳۷]	LEAP+ (Localized Encryption and Authentication Protocol)	پروتکل احراز هویت رمزنگاری محلی، یک پروتکل مدیریت برای شبکه‌های حسگر است. مبنای طراحی این پروتکل این است که پیام‌های مختلف تبادل‌شده بین گره‌های حسگر نیازمندی‌های امنیتی متفاوتی دارند و یک سازوکار کلید تنها، مناسب برای همه این نیازمندی‌ها نیست. این پروتکل ۴ نوع کلید (منحصربه‌فرد که با ایستگاه پایه به اشتراک گذاشته می‌شود، جفت کلید بین گره‌ها، کلید خوشه که بین گره‌های همسایه به اشتراک گذاشته می‌شود، کلید عام بین تمام گره‌ها) برای هر گره حسگر در نظر می‌گیرد. گرچه این طرح ایده‌های خوبی دارد ولی شامل مقیاس‌پذیری نیست.
۶	اشنائر [۳۸]	Basic	در این طرح از پیش توزیع تصادفی کلید استفاده می‌شود شامل مراحل پیش توزیع کلید، کشف کلید اشتراکی، ایجاد مسیر-کلید است. پیام‌ها از گره کنترل‌کننده، به‌صورت امضاءشده با جفت کلید اشتراکی بین حسگرها ارسال می‌شود. عدم مقیاس‌پذیری و کم‌بهره‌وری حافظه از ایرادات این طرح است.
۷	چان [۳۹]	q-Composite	در این طرح، با افزایش تعداد هم‌پوشانی کلید در حلقه کلید، انعطاف‌پذیری در مقابل با دام‌افتادگی گره افزایش می‌یابد. در این طرح برای راه‌اندازی یک کلید جهت ارتباط امن بین حسگرها، حداقل به تعداد q کلید مشترک لازم است که به اشتراک گذاشته شوند.

ادامه جدول (۴)

۸	بولوندو [۴۰]	Polynomial-based key predistribution protocol	دارای رویکرد احتمالی است. چندجمله‌ای دومتغیره به‌صورت تصادفی به توزیع کلید می‌پردازد. از معایب این طرح هزینه ذخیره‌سازی برای اشتراک‌گذاری چندجمله‌ای است. امنیت نسبتاً بالایی را ارائه می‌دهد.
۹	دئو [۴۱]	Key management scheme using deployment knowledge	این طرح، بر اساس طرح پایه[1] است. از تابع چگالی احتمال غیریکنواخت بهره می‌برد. الگوی موقعیت استقرار حسگرها باید مشخص شود.
۱۰	پوزو [۴۲]	SPINS(Security Protocols for Sensor Networks)	شامل دو بلوک اصلی است که در آن بلوک پروتکل رمزنگاری شبکه امن[2]، محرمانگی داده و احراز هویت دوطرفه را با رمز متقارن ارائه می‌دهد درحالی‌که بلوک پروتکل میکروتسلا[3] احراز هویت همگانی را ارائه می‌دهد که برای شبکه حسگر بی‌سیم مهم است. از ایستگاه پایه برای تبادل کلید بین گره‌ها استفاده می‌کند.
۱۱	پرانوشا [۴۳]	Hybrid	۱- این طرح در شبکه‌های بی‌سیم موردی[4] که در آن گره‌ها نیازی به زیرساخت ثابت ندارند و همچنین پیکربندی خودکار دارند، کاربرد دارد. در این شبکه‌ها هر گره می‌تواند فرستنده و گیرنده و یا رله‌کننده باشد. ۲- این طرح به‌منظور داشتن امنیت پایدار و غلبه بر چالش مدیریت کلید، از ترکیب هویت و اعتماد بهره می‌برد تا گره‌های بدخواه را تشخیص دهد و آن‌ها را به گره‌های مورد اعتماد تبدیل کند. ۳- فاکتور اعتماد و امنیت هویت پایه مؤلفه‌های اصلی این طرح‌اند و روش مخلوط برای تضمین احراز هویت صحیح استفاده می‌شود. ۴- در این طرح امنیت در بخش‌های مختلف اعمال می‌شود و درصورت آسیب‌دیدن قسمتی از آن، دیگر بخش‌ها پشتیبانی و جبران می‌کنند. ۵- هر گره مولد جفت کلید معتبر است و به‌طور متوالی به‌روز می‌شوند.
۱۲	کیتور [۴۴]	SeAK (Secure Authentication and Key Generation)	۱- این طرح در شبکه‌های حسگر بدنی[5] کاربرد دارد که از مؤلفه‌های این شبکه، سیاربودن کاربر و نظارت بر سلامت کاربر، امنیت داده‌های شخصی و حفظ این داده‌ها از سرقت، خرابکاری و دست‌کاری است. ۲- دو مقوله مهم در شبکه‌های حسگر بدنی، احراز هویت و تولید کلید در این طرح دیده شده است. ۳- ابتدا تجهیزات، درخواست همکاری را می‌فرستند و منتظر دریافت پیام تأیید می مانند، پس از دریافت تائید، چندین بسته بین تجهیزات و واحد مرکزی از طریق آنتن‌های متعدد رد و بدل می‌شوند. گره‌های حسی مقدار پارامتر قدرت سیگنال دریافتی را محاسبه می‌کنند. شرط احراز هویت برابری این پارامتر با مقدار توافق شده اولیه است. ۴- مدیریت کلید برای ارتباط امن بین گره‌ها اعمال می‌شود به‌طوری‌که یک کلید جفتی متناسب با داده برای مدیریت و یک کلید برای ارتباط بین گره‌های حسگر استفاده می‌شود. گره‌ها داده را با این کلید جفتی رمزنگاری و رمزگشایی می‌کنند. قبل از دریافت، سرور شخصی، کلید گره‌ها را به‌وسیله تابع چکیده‌ساز کلیددار[6] چک می‌کند. در صورت برابری داده دریافت خواهد شد.
۱۳	الوهالی [۴۵]	V2G (Vehicle to Grid) Key Management	۱- این طرح در شبکه‌های بی‌سیم ارتباطی بین وسایل نقلیه سیار برقی با شبکه هوشمند برق جهت تبادل برق بکار می‌رود که مستلزم نظارت مداوم وسایل نقلیه است. ۲- این طرح امن، حفظ حریم خصوصی را نیز شامل می‌شود. ۳- از امضای پنهان محدودشده برای تشخیص مالکان وسایل نقلیه استفاده می‌کند. به‌منظور سادگی مدیریت تائید، از رمزنگاری کلید عمومی فاقد تائید بهره می‌برد. ۴- تمامیت، احراز هویت، محرمانگی، حفظ حریم، جامعیت ارتباط، امنیت از ویژگی‌های این طرح است.

1 Basic
2 Secure Network EncryptionProtocol(SNEP)
3 micro version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol(μTESLA)
4 Mobile Ad Hoc Network (MANET)
5 Wireless Body Area Networks(WBAN)
6 keyed-hash

۹- بحث و تحلیل

در این پژوهش چهار مقوله ارتقای امنیت، حفظ حریم، حسابرسی و مدیریت کلید در شبکه‌های بی‌سیم و به‌خصوص شبکه حسگر بی‌سیم مطرح شدند.

با افزایش حجم اطلاعات در محیط بی‌سیم، موضوع امنیت بعد با اهمیتی شده است. امنیت شبکه‌های بی‌سیم به‌وسیله رمزنگاری انجام می‌شود. ارزیابی مقدار امنیت ارائه‌شده به‌وسیله رمزنگاری، مسئله مشکلی است. یکی از روش‌های اندازه‌گیری میزان امنیت ارائه‌شده، عملکرد محاسباتی لازم توسط دشمن جهت رمزشکنی است. سطح امنیت نسبت به قدرت مزاحمت‌های محیطی نیز سنجیده می‌شود [۶]. این قدرت محیطی قابل مدل‌سازی با تابع توزیع احتمال است که با فرض کمتربودن توان رمزشکنی دشمن نسبت به پیچیدگی محاسباتی رمز به‌دست می‌آید. در رمزنگاری شبکه‌های بی‌سیم، اولاً برخی خواص مربوط به قدرت رمزنگاری به خطای کانال ارتباطی حساس هستند [۶]. ثانیاً امنیت انتقال داده بی‌سیم باعث افت توان عملیاتی می‌شود. لذا توازن بین امنیت و توان عملیاتی مفهوم مهمی در شبکه‌های بی‌سیم است. در رمزنگاری فرصت‌طلبانه [۶] که طرح رمزنگاری وفقی با کانال است و با بالا بودن نسبت قدرت سیگنال به نویز، طول بلوک‌ها نیز بالا بوده و سطح امنیت و همچنین توان عملیاتی بهتر خواهد بود همچنین در این طرح، مدل‌سازی اثرات مهاجم، ترکیب مدولاسیون با رمزنگاری و کد تصحیح خطای پیش‌رونده برای حداقل‌سازی لحاظ شده است.

حفظ حریم در سطح شبکه‌ای حسگر بی‌سیم در ۴ گروه دسته‌بندی می‌شود [۴۷]: حریم هویت گره فرستنده (به‌طوری‌که هیچ گره میانی نتواند اطلاعات درباره هویت فرستنده بسته به‌دست آورد)، حریم مکان گره فرستنده (به‌طوری‌که هیچ گره میانی نتواند اطلاعات درباره مکان فرستنده بسته به‌دست آورد)، حریم مسیر (از مبدأ تا مقصد قابل پیش‌بینی کامل برای گره‌های میانی نباشد)، حریم بسته داده (هیچ گره میانی نداند که داخل بسته چه اطلاعاتی نهفته است). اغلب طرح‌های مربوط به شبکه حسگر بی‌سیم، تنها بخشی از حفظ حریم را پوشش می‌دهند. ارائه حفظ حریم در سطح کل شبکه، به‌خاطر محدودیت‌های اعمال‌شده در گره‌های حسگر (انرژی، حافظه، توان محاسباتی)، شبکه حسگر (متحرک‌بودن و ساختار شبکه)، توان رسیدن بسته و میزان اعتماد دارای چالش است. طرح IRL که گمنامی هویت، گمنامی مکان گره فرستنده، مسیریابی از گره‌های میانی مورد اعتماد و همچنین بالا بردن احتمال رسیدن بسته به مقصد را از طریق امن‌سازی مسیر پوشش می‌دهد، دارای حفظ حریم جامع در قبال حملات استراق سمع و ردیابی است.

حسابرسی در شبکه جهت پاسخگوبودن افراد برای کنششان و شناسایی دلایل افشای اطلاعات حساس لازم است [۱۴]. به‌دلایل متعددی که باعث ضعف امنیتی شبکه است، بایستی از طرح‌هایی برای نظارت بر رفتار بدخواهانه در شبکه که قادر به تشخیص حملات باشند استفاده کرد. لاگ‌ها که اتفاقات را ثبت می‌کنند به طور گسترده جهت اطمینان از حسابرسی مورد استفاده قرار می گیرند. سامانه‌های تشخیص حملات متعددی نیز وجود دارند که می‌توان به ۵ نوع سامانه تشخیص حملات برپایه رفتارهای غیرعادی، سامانه تشخیص حملات برپایه پروتکل‌های کاربردی، سامانه تشخیص حملات برپایه تعریف نفوذ، سامانه تشخیص حملات برپایه بسته‌های شبکه، سامانه تشخیص حملات برپایه دسترسی به شبکه تقسیم‌بندی کرد [۱۴]. در طرح Hybrid Accountability که شامل قسمت‌های flow-net، P-Accountable و Q-Accountable است، قسمت flow-net برای ثبت اتفاقات، تحلیل روابط بین اتفاقات، تشخیص حملات در شبکه از طریق همکاری گره‌های شبکه استفاده می‌شود. درحالی‌که قسمت‌های لاگ‌گیری Q-Accountable و P-Accountable برای افزایش و ارزیابی حسابرسی شبکه و همچنین برای تعیین میزان احتمال وقوع حمله مورد استفاده قرار می‌گیرد [۱۴]. از flow-net می‌توان در کاربردهای شبکه اجتماعی، تجارت الکترونیک، برنامه‌نویسی‌ها، کنترل دسترسی، مدیریت حقوق رقمی و ... بهره برد.

در موضوع امنیت شبکه حسگر بی‌سیم، به‌منظورجلوگیری از شنود مهاجم و تزریق اطلاعات غلط به شبکه، احراز هویت و محرمانگی نیاز به مدیریت کلید وجود دارد. روش‌های ایجاد کلید برای کاربری امن، بایستی شرایط خاصی مانند اصالت، محرمانگی، یکپارچگی، مقیاس‌پذیری، انعطاف‌پذیری و بهره‌وری انرژی را پوشش دهد [۴۶]. کارایی یک طرح مدیریت کلید به‌عواملی مانند توانایی ارائه محرمانگی، ممانعت در برابر تکثیرسازی گره‌ها، داشتن قدرت حذف گره‌های به دام افتاده، عدم افشای اطلاعات گره‌ها بستگی دارد [۴۶]. طرح‌های رمزنگاری به دو دسته رمزنگاری متقارن و رمزنگاری نامتقارن (کلید عمومی) تقسیم می‌شوند. به‌دلیل محدودیت منابع شبکه حسگر بی‌سیم، کلیدهای عمومی که دارای پیچیدگی محاسباتی هستند مناسب نیستند لذا اغلب طرح‌های مدیریت کلید که هدف‌شان تولید کلید بین گره‌های حسگر است، برپایه رمزنگاری کلید متقارن هستند. این طرح‌ها شامل دو نوع مدیریت متمرکز کلید و مدیریت توزیع‌یافته کلید است. در مدیریت متمرکز، مرکز توزیع کلید[1]، یک نهاد واحدی برای تولید و توزیع و ابطال است؛ مثلاً در طرح LKHW برپایه سلسله مراتب کلیدی منطقی[2]، ایستگاه پایه در

1 Key Disribution Center (KDC)
2 Logical Key Hierrachy (LKH)

نقش مرکز توزیع کلید بوده و همه کلیدها به‌طور منطقی در ایستگاه پایه به‌صورت درختی توزیع می‌شوند. این طرح نیاز به حافظه کم داشته و کنترل‌کننده تکرار گره است. درصورت تهاجم به ایستگاه پایه، امنیت کل شبکه ممکن است مخدوش شود. در طرح‌های مدیریت توزیع‌یافته کلید، دو رویکرد احتمالی و با قطعیت وجود دارد [۴۶]. طرح LEAP [۳۷]، مثالی از رویکرد با قطعیت است. در این طرح ۴ نوع کلید برای هر حسگر با نام‌های کلیدهای فردی، کلیدهای جمعی، کلیدهای جفتی و کلیدهای خوشه وجود دارند. درحالی‌که در طرح‌های مختلف [۳۸] تا [۴۱] رویکرد احتمالی است. درصورتی‌که براساس نتایج گزارش‌شده، طرح‌های مدیریت کلید را از نظر مقیاس‌پذیری، سرریز محاسباتی، بار ذخیره‌سازی، انعطاف‌پذیری در قبال به دام افتادن حسگر بررسی کنیم جدول (۵) را خواهیم داشت. دیده می‌شود که طرح مدیریت کلیدی وجود ندارد که برای همه حالت‌ها ایده‌آل باشد و بایستی براساس نیازمندی‌های کاربری نهایی و منابع شبکه تصمیم گرفت. لکن طرح LEAP دارای وضعیت نسبتاً بهتری است.

جدول ۵- مقایسه طرح‌های مدیریت کلید

طرح	مقیاس پذیری	سرریز محاسباتی	سرریز ارتباطی	بار ذخیره سازی	انعطاف‌پذیری
LEAP	خوب	کم	کم	کم	ضعیف
Basic	محدود	متوسط	متوسط	بالا	متوسط
q-Composite	خوب	بالا	بالا	بالا	خوب
Polynomial-based	خوب	متوسط	متوسط	بالا	خوب
deployment knowledge	خوب	متوسط	کم	متوسط	خوب

۱۰- نتیجه‌گیری

برای سازمان‌ها لازم است که سنجش‌هایی برای دستگاه‌های فناوری اطلاعاتشان به‌خصوص درحوزه بی‌سیم داشته باشند. سیاست‌های مدیریتی و مراحل سازمانی بایستی اطمینان‌بخش برای داشتن دانش مدیریت فناوری اطلاعات جدید باشند. در استفاده از فناوری‌های جدید باید به مقولات تهدیدکننده امنیت، حفظ حریم خصوصی، حسابرسی و مدیریت کلید توجه شود. استفاده از طرح‌های پیشنهادی برای مباحث مذکور در کنار استانداردهای پایه، می‌تواند در رضایت کاربر و تداوم شغلی نقش مؤثری داشته باشد. یافته‌های این پژوهش نشان می‌دهد که طرح‌های رمزنگاری فرصت‌طلبانه، IRL، Hybrid Accountability، LEAP به ترتیب در مقوله ارتقاء امنیت، حفظ حریم خصوصی، حسابرسی، مدیریت کلید از جامعیت نسبی برخوردارند.

با توجه به این‌که شبکه‌های بی‌سیم کاربری‌های مختلف ازجمله وای فای، وایمکس، شبکه‌های حسگر بی‌سیم، اینترنت سیار، محاسبات فراگیر و ... را شامل می‌شوند ولی در این پژوهش، عمده طرح‌ها معطوف به شبکه‌های حسگر بی‌سیم بودند لذا پیشنهاد می‌شود پژوهش مشابهی با محوریت دیگر کاربری‌های فوق‌الذکر انجام گیرد.

۱۱- مراجع

1. J. Zhang, T. Duong, and A. Marshal, "Key Generation From Wireless Channels: A Review," IEEE Access 2016, vol. 4, pp. 614-626, 2016
2. A. Sirisha, P. P. Priyanka, and P. Ratnakumari, "Design and Analysis of a Novel Extended Three-Tier Security Scheme for Efficient Data Transfer in Mobile Networks," IJCA, vol. 6, no. 1, Feb. 2016.
3. D. Ma and G. Tsudik, "Security and privacy in emerging wireless networks," IEEE Wireless Communications, October 2010.
4. M. LI and W. LOU, "Data security and privacy in wireless body area networks," IEEE Wireless Communications, 2010.
5. X. Qin, M. Alghamdi, M. Nijim, and Z. Zong, "Improving Security of Real-Time Wireless Networks through Packet Scheduling," IEEE TWC, vol. 7, no. 9, 2008.
6. P. Jindal and B. Singh, "Study and Performance Evaluation of Security-Throughput Tradeoff with Link Adaptive Encryption Scheme," IJSPTM, vol. 1, no. 5, October 2012.
7. M. Shin and J. Ma, and A. Mishra, "Wireless Network Security and Interworking," Proceedings of the IEEE, vol. 94, no. 2, 2006.
8. H. Deng and W. Li, "Agrawal D. P., Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, October 2002.
9. J. Jeong and Z. J. Haas, "An integrated security framework for Open wireless networking architecture," IEEE Wireless Communications, 2007.
10. X. Yang, "Accountability for Wireless LANs, Ad Hoc Networks, and Wireless Mesh Networks," IEEE, 2008.
11. X. Yang, "Flow-Net Methodology for Accountability in Wireless Networks," IEEE, 2009.
12. W. LOU and K. REN, "Security, privacy, and accountability in wireless access networks," IEEE Wireless Communications, 2009.
13. X. Zhifeng and X. Yang, "A Quantitative Study of Accountability in Wireless Multi-hop Networks," 39th International Conference on Parallel Processing, IEEE, 2010.
14. B. Fu and Y. Xiao, "Accountability and Q-Accountable Logging in Wireless Netwoks," Wireless Personal Communication, vol. 75, no. 3, pp. 1715-1746, Apr. 2014.
15. K. Defrawy and C. Soriente, "PEUC-WiN: Privacy Enhancement by User Cooperation inWireless Networks," IEEE, 2006.

16. H. Wenbo, L. Xue, and N. Hoang, “PDA: Privacypreserving Data Aggregation in Wireless Sensor Networks,” IEEE INFOCOM 2007 proceedings, 2007.

17. R. A. Shaikh, S. Lee, and A. Albeshri, “Security Completeness Problem in Wireless Sensor Networks,” Autosoft, DOI: 10,108/10798587.2014.970345, 2014.

18. J. Ying, C. Shigang, and Z. Zhan, “A Novel Scheme for Protecting Receiver’s Location Privacy in Wireless Sensor Networks,” IEEE TWC, vol. 7, no. 10, 2008.

19. Y. Jianbo and W. Guangjun, “Protecting Classification Privacy Data Aggregation in Wireless Sensor Networks,” IEEE, 2008.

20. F. Yanfei, “Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks,” IEEE TWC, vol. 10, no. 3, 2011.

21. M. E. A. Mohamed Mahmoud and S. Xuemin (Sherman), “A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks,” IEEE *TPDS*, vol. 23, no. 10, 2012.

22. W. Zhiguo, X. Kai, and L. Yunhao, “Priv-Code: Preserving Privacy Against Traffic Analysis through Network Coding for Multihop Wireless Networks,” Proceedings IEEE INFOCOM, 2012.

23. A. Chandrashekhar and A. Sumit, “Security, Privacy and Accountability in Wireless Network,” IJERT, vol. 2, Issue 7, pp. 1-10, 2013.

24. S. lazim and Q. I. Ali, “Design and implementation of an embedded intrusion detection system for wireless applications,” IET Inf. Secur., vol. 6, Issue 3, pp. 171-182, 2012.

25. Y. Jie and C. Yingying, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks,” IEEE TPDS, vol. 24, 2013.

26. A. Rasheed and N. Rabi, “The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks”, IEEE TPDS, vol. 23, no. 5, 2012.

27. K.Q. Yan and S. C. Wang et al., “Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network,” IEEE, 2010.

28. W. Weijia, H. Lei, and L. Yong, “Security Analysis of a Dynamic Program Update Protocol for Wireless Sensor Networks,” IEEE Communications Letters, vol. 14, no. 8, 2010.

29. C. Mauro and D. Roberto, “Distributed Detection of Clone Attacks in Wireless Sensor Networks,” IEEE TDSC, vol. 8, no. 5, 2011.

30. L. George, K. Byungsuk, and F. Anjum, “A Policy-based Approach to Wireless LAN Security Management,” IEEE, 2007.

31. X. Debao, C. Chao, and C. Gaolin, “Intrusion Detection based Security Architecture for Wireless Sensor Networks,” Proceedings of ISCIT, 2005.

32. L. Shu Yun and L. Meng-Hui, “Energy-Efficient and Scalable Group Key Management for Hierarchical Sensor Network,” JUSPN, vol. 2, no. 1, pp. 39-47, 2011.

33. D. Carman, B. Matt, and G. Cirincione, “Energy-efficient and Low-latency Key Management for Sensor Networks,” Proceedings of 23rd Army Science Conference, 2002.

34. D. Carman, P. Kruus, and B. Matt, “Constraints and Approaches for Distributed Sensor Network Security,” NAI Labs: Technical Report #۰-010, 2000.

35. L. Eschenauer and D. Virgil, “A key-management scheme for distributed sensor networks,” Proceedings of the 9th ACM CCCS, Washington, DC, USA, 2002.

36. T. Park and K.G. Shin, “LiSP: A Lightweight Security Protocol for Wireless Sensor Networks,” ACM TECS, vol. 3, no. 3, 2004.

37. S. Zhu and S. Setia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed WSN Networks,” ACM TSON, vol. 2, Issue 4, pp. 500-528, Nov. 2006.

38. L. Eschenauer and V. D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” 9th ACM CCCS, New York: ACM Press, pp. 41-47, 2002.

39. H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” Proc. IEEE SSP, May 2003.

40. C. Blundo et al., “Perfectly-Secure Key Distribution for Dynamic Conferences,” CRYPTO Proc. 12th Annual Int’l.Cryptology Conf. Advances in Cryptology, London: Springer-Verlag, pp. 471-486, 1993.

41. W. Du et al., “A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge,” Proc. IEEE INFOCOM, Hong Kong, pp. 586–597, 2004.

42. R. R. Pozo, “Protecting Contextual Information in WSNs Source- and Receiver-Location Privacy Solutions,” submitted in fulfillment of the requirements for the Degree of Doctor in Computer Science, pp. 1-252, 2014.

43. A. Pranusha and G. Murali, “A Hybrid Key Management Scheme for Secure Manet Communications,” IJRET, vol. 4, Issue 2, 2015.

44. N. Kittur and M. Dharishini, “Review of Key Management Technique for Wireless Body Area Networks,” IRJET, vol. 2, Issue 4, pp. 82-86, July 2015.

45. B. Alohali and K. Kifayat, “A Survey on Cryptography Key Management Schemes for Smart Grid,” JCSA, vol. 3, no. 3, pp. 27-39, 2015.

46. P. Sivakumar, S. Saravanan, and M. Anandaraj, “A survey in Wireless Sensor Networks based on Key Management Schemes,” IJATCSE, vol. 4, no. 2, 2015.

47. A. Arul and M. Merlin, “Efficient Message Authentication and Source Privacy in Wireless Sensor Networks,” IJCSITR ISSN 2348-120X, vol. 3, Issue 1, pp. 222-227, 2015.

An Overview on Security, Privacy, Accountability and Key Management in Wireless Networks

R. Yazdani, A. Mohammadi*, N. Modiri

Abstract

In recent years, wireless network is highly regarded for the ease of use, the extent of usage and variety of services. Including the application of these networks can be pointed in trade, health, military and home automation areas. Among the most important issues in these networks are Security, Accountability, Privacy and Key Management. Scientific activities on these issues have been achieved and exploited discretely. The Classification and study of presented methods features can help researchers to complete the development of science as well as to take the advantage of these networks. In this article, provided schemes to enhance the Security, Accountability, Privacy and Key Management in wireless networks are investigated and unique features of each scheme are listed. This research in terms of type is practical and in terms of approach is qualitative and in terms of methods is descriptive-analytical and also in terms of study design is result-oriented. The results show that Opportunistic Encryption, IRL, Hybrid Accountability and LEAP+ schemes on Security, Privacy, Accountability and Key Management, are relatively comprehensive, respectively.

Key Words: *Wireless Networks, Security, Accountability, Privacy, Key Management.*

* Supreme National Defense University, (mohammadii@aut.ac.ir) - Writer-in-Charge