(مروری بر امنیت در شبکه های حسگر بی سیم)

استاد راهنما : جناب آقای دکتر مهرداد احمد زاده

درس امنیت

دانشگاه علوم تحقیقات کرمانشاه

محمد حسین پوراسد

Pourasad.mh@gmail.com

چکیده : شبکه های حسگر بی سیم در اصل برای جمع آوری اطلاعات از محیطی غیرقابل اعتماد بوجود آمد. تقریباً همهٔ پروتکل های امنیتی برای WSN معتقدند که دشمن یا نفوذگر میتواند از طریق ارتباط مستقیم ، کنترل کامل یک نود حسگر را دردست گیرد. ظهور شبکه های حسگر بعنوان یکی از تکنولوژی های اصلی آینده، چالش های متعددی را پیش روی محققان قرار می دهد. شبکه های حسگربی سیم از تعداد زیادی از نودهای کوچک تشکیل شده است که بصورت جداگانه درحال کارکردن هستند و در موارد متعدد، بدون دسترسی به منابع انرژی تجدیدشدنی به کارشان ادامه می دهند . در نهایت، امنیت اهمیت بسزایی در پذیرش و استفاده از شبکه های حسگر، در کاربردهای متعدد دارد، همچنین چالش های گوناگون دیگری نیز وجود دارند. در این مقاله ما بر روی امنیت شبکه های حسگر بی سیم متمرکز می شویم و همچنین بر روی برخی از راه های کاربردی برای امنیت بیشتر مباحثی را مطرح می کنیم .

کلمات کلیدی : حمله به شبکه های حسگر بی سیم، مسیریابی امن، معماری، بازدهی، پروتکل های مسیریابی و مطالب راندمان .

پیشگفتار:

امنیت شبکه های حسگر بی سیم زمینه ای است که در سالیان گذشته بطور چشمگیری مورد تحقیق قرار گرفته است. کاربردهای این شبکه ها متنوع هستند و شامل سطوحی از نظارت، ردیابی، کنترل یا یک ترکیبی از آنهاست . شبکه های حسگربی سیم خصوصیات منحصربفردی دارند، مانند توانایی کارکردن در شرایط محیطی نامطلوب، توپولوژی شبکه پویا، خطاهای ارتباطی، توسعه در مقیاس بزرگ، افزایش ظرفیت نودها، تحرک نودها، عملیات بدون مراقبت همچون انرژی محدود و برخی دیگر. آنها همچنین ایستگاه های پایه هم دارند که منابع بیشتری دارند که مانند یک درگاه مابین نودها و کاربر نهایی عمل می کند.

در این مقاله ما حملات رایج را در شبکه های حسگربی سیم بطور خلاصه بیان میکنیم و فرضیات رایج و اهداف امنیتی در شبکه های حسگر بی سیم و معماری و پروتکل های مسیریابی را ارائه می کنیم. سپس بر روی مدیریت کلید و رمزنگاری، همزمان سازی امن، مکان یابی امن ،

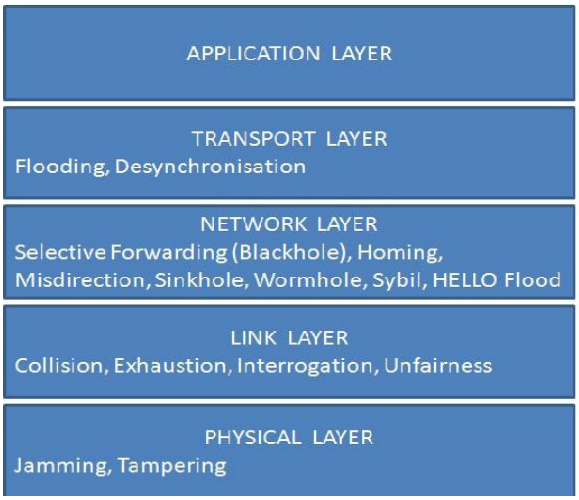
مطالب مربوط به راندمان ، پردازش درون شبکه ای و برخی از نکات امنیتی بحث خواهیم کرد. سپس یک چهارچوب کاری برای یک سیاست موثر در امنیت شبکه های حسگر بیسیم و همچنین یک معماری مدیریت امنیت مبتنی بر سیاست برای شبکه های حسگر بیسیم ارائه می کنیم . در ادامه پیرامون اجرای الگوریتم رمزنگاری RSA برای شبکه های حسگر بیسیم و همچنین رمزنگاری چندلایه ای برای کنترل دسترسی چندسطحی در شبکه های حسگر بیسیم مباحثی را مطرح می کنیم . به عنوان حسن ختام ، با خلاصه ای از امنیت شبکه متحرک بیسیم WiMAX به استقبال نتیجه گیری مقاله خواهیم رفت .

حملات در شبکه های حسگر بی سیم :

یک شبکه حسگر بی سیم در مقیاس بزرگ از هزاران نود از حسگرها تشکیل شده است و ممکن است در یک محیط پهناور پراکنده شده باشد. نودهای حسگر نوعاً کوچک هستند با توانایی محدود در محاسبات و ارتباطات که توسط باطری تغذیه می شوند. این نودهای حسگر کوچک مستعد انواع مختلفی از حملات هستند. برای یک شبکه حسگر با مقیاس بزرگ، نظارت و محافظت از هر حسگر منفرد از حملات فیزیکی یا منطقی عملی نیست. حملات در شبکه های حسگر بی سیم می توانند طبقه بندی شوند به حملات بر روی لایه های فیزیکی، ارتباطات (کنترل دسترسی به رسانه یا واسط)، شبکه، انتقال و لایهٔ کاربرد. حملات می توانند همچنین بر پایهٔ توانایی های مهاجمان طبقه بندی شوند، همچون سطح حسگر و سطح لپ تاپ. یک مهاجم سطح لپ تاپ قوی به مراتب می تواند خسارت بیشتری به شبکه وارد کند تا یک مهاجم سطح حسگر، چرا که تامین انرژی بهتری دارد. همچنین توانایی بیشتر در محاسبات و ارتباطات از یک نود حسگر. همچنین حملات می توانند به دو دستهٔ داخلی و خارجی نیز تقسیم شوند. یک مهاجم خارجی به بیشتر اجزای رمزنگاری در شبکهٔ حسگر دسترسی ندارد، درحالی که یک مهاجم داخلی ممکن است بخشی از اجزای کلید را در اختیار داشته باشد و مورد اعتماد برخی از نودهای دیگر باشد. شناسایی و مقابله با حملات داخلی بسیار مشکل است. Wood وStankovic حملات گوناگون انکار سرویس بر روی شبکه های حسگر بی سیم را بر طبق لایه های شبکه، طبقه بندی کرده اند. حملات شامل حملات انکار سرویس مورد ذکر و حملات شناسایی شدهٔ دیگر در نوشته های دیگر می باشد. برای هر نمونه از حمله ، ۳ آیتم به ترتیب زیر ارائه شده است : نام حمله، لایهٔ شبکه متناظر و تکنیک های تدافعی ممکن. ما حملات شبکه های حسگر بی سیم و تکنیک های تدافعی ممکن را بصورت زیر خلاصه کرده ایم :

۱- Jamming (لایهٔ فیزیکی):طیف گسترده، چرخهٔ کاری پایین تر.
۲- مداخله کردن (لایهٔ فیزیکی) : آزمون مداخله، طرح مدیریت موثر کلید.
۳- تصادم (لایهٔ اتصال) : کد تصحیح خطا.
۴- خستگی (لایهٔ اتصال) : محدودیت نرخ.
۵- دستکاری اطلاعات مسیریابی (لایهٔ شبکه) : اعتبارسنجی و رمزگذاری.
۶- حملهٔ ارسال انتخابی (لایهٔ شبکه) : فراوانیف کاوش.
۷- حملهٔ Sybil (لایهٔ شبکه) : اعتبارسنجی.
۸- حملهٔ حفره (حفرهٔ سیاه) (لایهٔ شبکه) : اعتبارسنجیف نظارت، افزونگی.
۹- حمله حفرهٔ کرم (لایهٔ شبکه) : نظارت، انتخاب انعطاف پذیر مسیر.
۱۰- حملهٔ سلام سیل آسا (لایهٔ شبکه) : اعتبار سنجی ۲ راهه، دست دادن ۳ راهه.
۱۱- سیل (لایهٔ انتقال) : محدودیت تعداد ارتباطات، جدول کلاینت ها.
۱۲- حملهٔ کپی (لایهٔ کاربرد) : کلید دوگانهٔ واحد.

۱۳- به علت محدودیت صفحات از توضیح بیشتر خودداری می کنیم.



شکل شماره ۰_ رده بندی حملات

تحلیل حمله :

هر مهاجمی که به هر روشی حمله به یک شبکه را طراحی کرده است یک نیت سوء دارد که طبق یک برنامهٔ از پیش مشخص شده پیش می رود. با استفاده از تحلیل حمله قادر خواهیم بود مکانیزمی را ایجاد کنیم که بتوانیم حملات را پیش بینی، جلوگیری، محافظت و پوشش دهیم. یک مهاجم می تواند در ۴ بعد تقسیم بندی شود : " انگیزه، اراده، دانش و منابع" . چهار بعد فوق بطور موثری می توانند مورد استفاده قرار گیرند برای پاسخ به سوالات اساسی پیرامون یک حملهٔ مورد انتظار در یک شبکه. اگر سوالات فوق قبل از توسعهٔ شبکه پاسخ داده شوند آنگاه شبکه می تواند گسترش یابد درحالی که تهدیدات احتمالی دیده می شوند. سوالات بالقوه ای که نیاز است پاسخ داده شوند برای تحلیل یک مهاجم و قصدو نیت آن عبارتند از :

- مهاجم کیست ؟
- یک مهاجم قادر به چه کارهایی است ؟
- هدف چیست ؟
- چگونه حمله صورت گرفته است ؟
- نتیجه یا پیامد حمله چه چیزهایی هستند ؟

معماری ها و پروتکل های مسیریابی :

یکی از جنبه های مهم مربوط به شبکه های حسگر بی سیم معماری ها و پروتکل های مسیریابی هستند. معماری ها ستون فقرات هر شبکه ای هستند و پروتکل های مسیریابی ابزاری هستند که شبکه ها برای ارتباطات از آنها استفاده می کنند. یک معماری و یک پروتکل مسیریابی به عنوان مثال ارائه شده اند.

الف - معماری : یک معماری استفاده شده برای شبکه های حسگر بی سیم ، یک شبکهٔ حسگر بی سیم خودسازنده(SOWSN) است که یک توپولوژی ستاره-مش را بکار برده است که شامل ۲ نوع از نود های بی سیم است : یک ایستگاه پایه و یک نود حسگر. نود حس گر مسئول جمع آوری رویدادهایی است که بخاطر اهداف خرابکارانه ایجاد شده اند که شامل موارد زیر است :

۱- جمع آوری اطلاعات در مورد کارهای خرابکارانه شامل ماهیت اهداف و موقعیت مرتبط.
۲- تولید رویداد بلادرنگ با توجه به اهداف محافظت شده با انتقال رویدادها به یک مرکز تحلیل گر رویداد از طریق یک ایستگاه پایه.
۳- ربط دادن رویدادهای تولید شده به یک ایستگاه پایه.

ایستگاه های پایه فعالیت های انجام شده را کنترل می کنند برای پشتیبانی از راندمان حسگرها. یک ایستگاه پایه موقعیت مرتبط را برای منابع رویداد محاسبه می کند. یک ایستگاه پایه می بایست هشداری را مرتبط با یک هدف مشخص دریافت کند، یک هویت برای این هدف باید مشخص شود، که تمام هشدارهای مرتبط با اهداف را مجاز می سازد که تهدیدات درخور را دریافت کنند. همهٔ اهداف می توانند شناسایی شوند اما تحرکات آنها قابل پیش بینی نیست. هر حسگر در شبکه یک مقدار اولیه از انرژی را دارد با ایستگاه های پایه که دروازه ای هستند مرتبط با حسگرهای تحلیلگر مرکزی.شکل شماره ۱ مثالی از معماری SOWSN است.

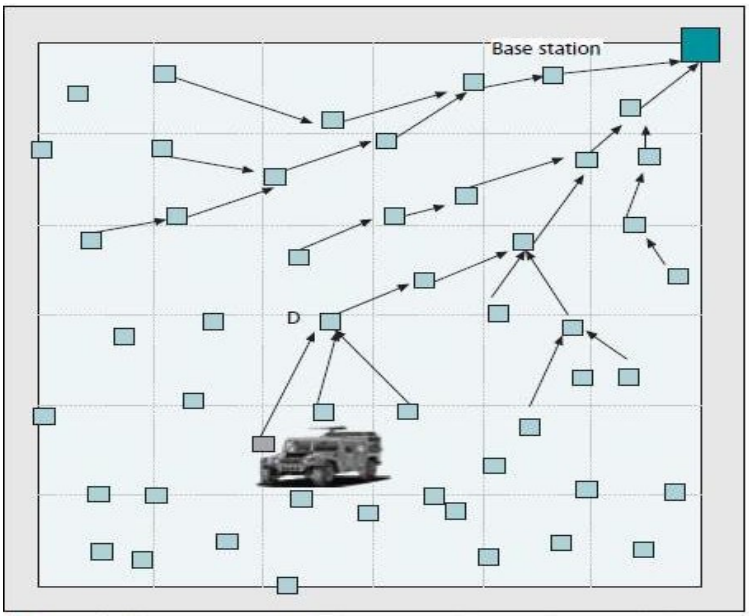
ب _ مسیریابی امن : عاملیت ابتدایی شبکه های حسگر بی سیم حس کردن اتفاقات محیط و انتقال اطلاعات کسب شده به ایستگاه پایه است برای پردازش بیشتر. بنابرین، میسریابی یک عملیات ضروری است در شبکه های حسگر. یک تعدادی از پروتکل های مسیریابی برای شبکه های حسگر پیشنهاد شده است. اگرچه، تحقیقات پیشین در زمینهٔ مسیریابی شبکه های حسگر تاکید زیادی بر روی اثر گذاری و کارائی انتشار داده ها داشت، مطالعات بسیار کمی موارد امنیتی را در نظر گرفتند در طراحی یک پروتکل مسیریابی. مطالعات و تحقیقات نشان دادند که امنیت درنظر گرفته شده در مرحله طراحی بهترین راه تامین امنیت است برای مسیریابی شبکه بی سیم. چندین پروتکل مسیریابی امن پیشنهاد شده است برای شبکه های موبایل Ad hoc (MANENs). اگرچه این پروتکل ها برای شبکه های حسگر بی سیم مناسب نیستند زیرا :

- آنها نیاز به عملیات محاسبات زیادی برای مسیریابی و امنیت دارند.
- آنها طراحی شدند برای یافتن و انتشار مسیرها بین هر جفت از نودها، که با الگوی ترافیکی چند به یک حاکم بر شبکه های حسگر متفاوت هستند. Wood وStankovic یک تعدادی از حملات انکار سرویس را در شبکه های حسگر بی سیم را شناسایی کردند. بسیاری از این حملات انکار سرویس برای مسیریابی شبکهٔ حسگر هستند. Karlof وWagner چندین حملهٔ امنیتی بر روی پروتکل های مسیریابی را در شبکه های حسگر تشریح کردند. آنها همچنین حملات احتمالی را بر روی چندین پروتکل مسیریابی تحلیل کردند، شامل نفوذ مستقیم و LEACH . اگرچه، Karlof و Wagner هیچ پروتکل مسیریابی امنی برای شبکه های حسگر ارائه ندادند.
- Karlof یک پروتکل مسیریابی امن و موثر ارائه داد برای شبکه های حسگر همگن. پروتکل باعث افزایش کارائی شده و می تواند در مقابل بسیاری از حملات رایج دفاع کند در مسیریابی حسگر. او درنظر گرفت چگونگی محافظت کارامد از تزریق داده های نادرست توسط نودهای به خطر افتاده.

اهداف امنیت :

هدف نهایی امنیت تامین محرمانگی، جامعیت، اعتبار سنجی و در دسترس بودن همهٔ پیام ها با وجود مهاجمان کاردان و ماهر است. هر دریافت کنندهٔ به سزا می بایست همهٔ پیام ها را با در نظر داشتن موارد فوق دریافت کند و بتواند تمامیت هر پیام را همچون هویتی

که از سمت فرستنده داشته است را تشخیص دهد. مهاجمان نباید بتوانند به محتویات پیام ها پی ببرند. در شبکه های کامپیوتری رایج هدف اصلی امنیت، تحویل مطمئن پیام است (مثلاً محافظت علیه حملهٔ انکار سرویس). اعتبار پیام، تمامیت و محرمانگی معمولاً توسط یک مکانیزم End-To-End حاصل می شوند مانند لایهٔ سوکت امن (SSL) . این به این دلیل است که الگوی ترافیکی حاکم ارتباط End-To-End است، در جایی که نه نیاز است و نه مطلوب که محتویات پیام ها برای مسیریاب های واسط قابل دسترس باشد. اگرچه، الگوی ترافیکی حاکم در شبکه های حسگر Many- To-End است، همانگونه که در شکل ۱ نشان داده شده است، وقتی که تعداد زیادی از نودهای حسگر داده ها را به یک نود می فرستند (یا چندتا) ایستگاه های پایه در سمت راست بالا می باشند. پردازش درون شبکه های همچون تراکم داده، حذف کپی ها، یا فشرده سازی داده ها برای شبکه های حسگر بسیارمهم است که این عملیات در یک حالت با بازدهی انرژی مناسب صورت پذیرد. مثلاً نود حسگر D در شکل ۱ از ۳ نود حسگر داده دریافت می کند که یک رویداد را پوشش می دهند. تراکم داده ها در نود Dبطور قابل ملاحظه ای می تواند هزینهٔ ارتباطات را کاهش دهد. تا زمانی که پردازش درون شبکه ای نیازمند نودهای واسط است، برای دسترسی، اصلاح، و در صورت امکان توقیف محتویات پیام ها، بسیار بعید است که امنیت مکانیزم End-To-End بین یک نود حسگر و یک ایستگاه پایه بتواند برای تضمین جامعیت، اعتبار و محرمانگی این چنین پیام هایی استفاده شود. با وجود مهاجمان داخلی، امنیت لایهٔ ارتباط برای پوشش دادن کل شبکه کافی نیست، تا زمانی که یک مهاجم داخلی به هر پیامی که درون شبکه مسیریابی شده است دسترسی کامل داشته باشد و می تواند اصلاح کند یا توقیف کند و یا حتی پیام ها را دور اندازد. در چنین مواردی کسی ممکن نیست بتواند محرمانگی، تمامیت، اعتبارسنجی و در دسترس بودن هر پیامی را تامین کند. بنابراین در صورت وجود حملات داخلی، اقدامات امنیتی می بایست تضمین کنند که شبکه حسگر می تواند عملیات اصلی را تامین کند با حداقل تراکم. در بخش بعدی ما بر روی تعدادی از مطالب امنیتی مهم در شبکه حسگر بحث می کنیم شامل مدیریت کلید، همزمان سازی امن، کشف مکان امن ، مسیریابی امن و ... .



شکل ۱: *The many-to-one traffic pattern and in-network processing in network*

مدیریت کلید:

برای دستیابی به امنیت در شبکه های حسگر بی سیم مهم است که بتوان عملیات روز نگاری متفاوتی را انجام داد، شاملرمزگذاری، اعتبارسنجی و موارد مشابه. کلیدهای این عملیات رمزنگاری باید توسط نودهای ارتباطی ست شوند قبل از اینکه انها بتوانند اطلاعات امنیتی را تغییر دهند. مدل های مدیریت کلید مکانیزم هایی هستند که نمونه های متنوعی از کلیدها را منتشر و در شبکه توزیع می کنند، همچون کلیدهای منفرد ، کلیدهای دوگانه، کلیدهای گروهی. مدیریت کلید یک عملیات اصلی و ضروری است در رمز نگاری که عملیات امنیتی دیگر بر مبنای آن شکل می گیرند. اکثر ملزومات امنیتی ، مانند حریم خصوصی، اعتبار سنجی و حفظ تمامیت می توانند توسط مدیریت مستحکم یک کلید قوی بنا شوند. در حقیقت، مدل مدیریت کلید امن برای امنیت پایه ضروری است، بنابراین لازم است برای ایجاد یک زیربنای امن در شبکه های حسگر. بخاطر محدودیت منابع دستیابی به یک چنین کلیدی در شبکه های حسگر بی سیم بسیار اهمیت دارد. چالش طراحی پروتکل های مدیریت کلید برای شبکه های حسگر بی سیم در انتشار یک زیر بنای ارتباطی امن نهفته است، قبل از اینکه هرگونه طراحی مسیریابی منتشر شود، یا بدون وجود هر هویت مورد تائید یا فیکس کردن سرور، از یک مجموعه ای از نودهای حسگر که هیچ ارتباطی از قبل با هم نداشتند. بعضی از اطلاعات رمز نگاری(مانند کلید) بصورت نرمال در نودهای حسگر قبل از توسعه بار می شوند و به نودهای حسگر اجازۀ ارتباط امن را می دهند با دیگر نودها. اکثر مدل های جمع آوری اطلاعات را از یک توپولوژی شبکه قبل از توسعه انجام نمی دهند و به نودها اجازه می دهند که به یک شبکه ملحق شوند بعد از توسعه. مدل ها می بایست نیازهای محاسباتی و ذخیرۀ کمی داشته باشند. ۴ نوع مدل مدیریت کلید وجود دارد : سرور مود اعتماد، جود اجرا کننده، کلید پیش توزیع، کلید رمزنگاری عمومی.

هم زمان سازی امن :

بخاطر ذات همکاری در نودهای حسگر، همزمان سازی برای بسیاری از عملیات شبکه های حسگر مهم می باشد، مانند کارهای حسی مرتبط، زمانبندی حسگرها(بیدار و خواب)، پیگیری اجسام متحرک، دسترسی تقسیم زمانی(TDMA) کنترل دسترسی به رسانه، تراکم داده ها و پروتکل تشخیص هویت منابع Multicast . به عنوان مثال، در کاربرد پیگیری هدف که در شکل ۲ نشان داده شده است، نودهای حسگر هم نیاز دارند موقعیت را بدانند و هم اینکه چه زمانی هدف حس می شود تا بتوانند بطور صحیح مسیر تحرکات هدف و سرعت آنرا تعیین کنند. پروتکل زمانی شبکه (NTP) برای همزمان سازی در اینترنت مورد استفاده قرار می گیرند. یک شبکه حسگر یک سیستم توزیع شدۀ محدود است و NTP نمی تواند بطور مستقیم توسط شبکه های حسگر مورد استفاده قرار گیرد. چندین الگوریتم همزمان سازی برای شبکه های حسگر پیشنهاد شده است. همۀ شبکه های همزمان سازی متکی است به برخی از انواع مبادلۀ پیام بین نودها. بصورت غیرجبری در شبکه های پویا، مانند زمان دسترسی به به کانال فیزیکی و سربار عملیات سیستم (مانند فراخوانی سیستم) چالش هایی را در همزمان سازی در شبکه های حسگر بی سیم ایجاد می کند. طرح پیشنهادی همزمان سازی برای شبکه های حسگر شامل همزمان سازی پخش منبع (RBS)، پروتکل همزمان سازی برای شبکه های حسگر (TPSN)،و موارد مشابه دیگر. ای الگوریتم های همزمان سازی سعی در بدست آوردن زمان همزمان سازی یا ساعت همزمان سازی پالس سراسری دارد. هدف همزمان سازی کلیدهای دوگانه ایجاد همزمانی بین زمان حسگر همسایه است، درحالی که زمان همزمان سازی سراسری تامین کنندۀ پالس ها هستند در تمامی شبکۀ حسگر. با وجود زمانهای دوگانه ، پروتکل های همزمان سازی از همزمان سازی گیرنده استفاده می کنند، که یک نوع منبع یک پیام را پخش همگانی می کند برای گیرنده ها جهت شناسایی اختلاف زمان ها. اکثر پروتکل های سراسری همزمان سازی، زمان مسیرهای چندگانه را در یک شبکۀ حسگر منتشر می کنند.

بنابراین همهٔ نودها قادر خواهند بود زمانهایشان را همزمان کنند به یک منبع داده شده مبتنی بر این مسیرها و اختلاف ساعت دوگانه بین نودهای مجاور در این مسیرها. اگرچه، هیچ کدام از الگوهای همزمان سازی فوق الذکر بصورت امن طراحی نشده اند. بنابراین، آنها برای محیط های ناسازگار مناسب نیستند (مثلاً میدان نبرد) و جاهایی که امنیت مهم و حیاتی است. اکثر تکنیک های همزمان سازی نسبت به یک سری از حملات آسیب پذیرند. ۴ حملهٔ ممکن در همزمان سازی حسگرها شناسایی شده اند :

- **حملهٔ فریبکارانه :** فرض کنید نود A برای دو تا از همسایگانش یک منبع را راهنمایی می کند و B و C .یک مهاجم و E می تواند وانمود کند که B است و اطلاعات همزمان سازی نا درست را با C تبادل کند، که فرایند همزمان سازی را بین B و C مختل می کند.
- **حملهٔ دوباره :** استفاده از همان سناریویی که در حملهٔ قبلی گفته شد، مهاجم E می تواند به بسته های زمانی قدیمی B پاسخ دهد، که C را بصورت نادرست همزمان می کند .
- **حملهٔ دستکاری پیام :** در این حمله، یک مهاجم ممکن است کم کند، تغییر دهد یا حتی جعل کند پیام های زمانی تبادل شده را که فرایند همزمانی را مختل می کند.
- **حملهٔ تاخیر :** مهاجم مدبرانه برخی از پیام ها را دچار تاخیر می کندکه در فرایند همزمانی به عنوان خطا مطرح می گردد.

قابل ذکر است که این نوع از حمله نمی تواند توسط تکنیک های رمزنگاری پوشش داده شود. در نهایت در ۴ حملهٔ فوق ، حملهٔ انکار سرویس همچنین می تواند اکثر همزمان سازی ها را مختل کند. مثلاً یک مهاجم می تواند باعث ایجاد Jamming یا تصادم بسته ها شود با زمان پیام ها. بنابراین موجب اختلال در همزمان سازی می شود. ۳ حملهٔ نخست می توانند توسط تکنیک های رمزنگاری مورد مورد خطاب قرار گیرند. اعتبار سنجی هم می تواند برای دفاع علیه حملات فریبکارانه مورد استفاده قرار گیرد. به عنوان مثال یک شبکهٔ حسگر ابتدا می تواند از یک مدل مدیریت کلید برای انتشار کلیدهای مشترک برای هرجفت از حسگرهای همسایه استفاده کند. سپس یک فرستنده یک کد اعتبارسنجی پیام را محاسبه کند(MAC). با استفاده از کلید مشترک MAC را به یک پیام خروجی ضمیمه می کند. MAC می تواند مانع جعل هویت نودهای دیگر شود توسط یک مهاجم یا اینکه محتویات یک پیام را بدون اینکه محافظت شود تغییر دهد.برای جلوگیری از حملهٔ مجدد ، یک رشته ای از اعداد می توانند اضافه شوند به هر پیام مبادله شده.افت پیام ممکن است توسط برخی از مدل های تشخیص رفتارهای سوء مورد توجه قرار گیرد. اگرچه، حملات تاخیر و انکار سرویس نمی توانند توسط تکنیک های رمزنگاری دفاع شوند. Song حملهٔ تاخیر را شناسائی کرد و راه حل های پیشنهادی را برای مقابله ارائه کرد. ایدهٔ اصلی جمع آوری یک ست از زمانهای ابتدایی است از نودهای درگیر چندگانه و برخی از روشهای آماری برای شناسایی زمان های ابتدایی مخرب بکار می رود. سپس پیامدهای زمانی خرابکارانهٔ شناسایی شده طرد می شوند و زمانهای دقیق تخمین زده می شوند. دو مدل پیشنهاد شدند برای دفاع در مقابل حملهٔ تاخیر. مدل اول از روش آماری استفاده می کند یا الگوریتم های منحرف کننده (GESD) و برای مقابله با نودهای منحرف شده و مدل دوم از یک تکنیک زمان انتقال استفاده می کند که خروجی ها را فیلتر کند. Wood وStankovic بحث می کنند در حملات انکار سرویس در شبکه های حسگر و طرح هایی را برای مقابله با این حملات لیست کرده اند. مثلاً، تکنیک طیف گسترده ممکن است برای مقابله با حملهٔ jamming استفاده شود و کد اصلاح خطا ممکن است برای مقابله یا تصادم استفاده شود. در اصل، محافظت و دفاع در مقابل حملات انکار سرویس در شبکه های حسگر کار ساده ای نیست. مدل های همزمان سازی فوق برای شبکه های حسگر همگن طراحی شده اند، تمام نودهای حسگر هم مدل باشنداز نظر توانایی. در این طرح ها محاسبات و ارتباطات قابل چشم پوشی نیستند پس به این ترتیب باعث ایجاد بار اضافی می شوند. علاوه بر این، خیلی از الگوریتم های همزمان سازی نیاز به انتشار یک پیام برای همزمانی دارند به برخی از نقاط منبع. (مثلاً ایستگاه های پایه) به تمام نودهای حسگر از طریق مسیرهای چندگانه و خطاهای همزمان سازی می توانند در طی انتقالات چند مسیری به این فرایند اضافه شوند. یکی از دانشمندان یک طرح همزمان سازی امن،

کارامد و موثر برای شبکه های حسگر ناهمگن ارائه نمود که شامل چندین نوع از نودهای فیزیکی مختلف است. حاصل این مدل امنیت قوی تر وبازدهی بهتر است با استفاده ازردهٔ انتقال وسیع تر و دیگر ویژگی حسگرها. شکل ۳ یک شبکه حسگر ناهمگن را نشان می دهد.

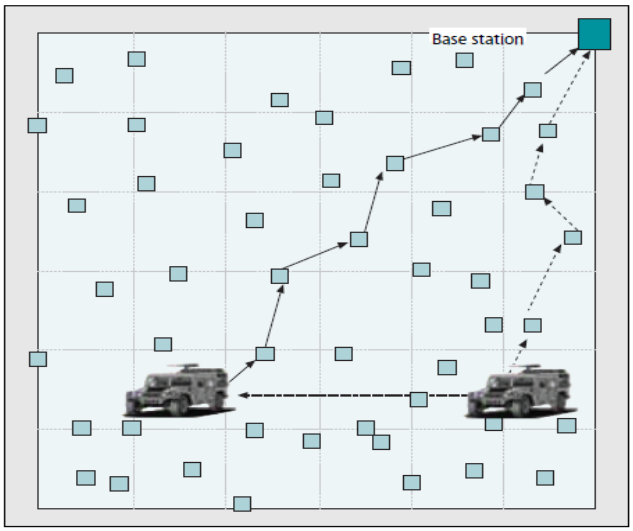


Figure 2. *Target tracking in a sensor network.*

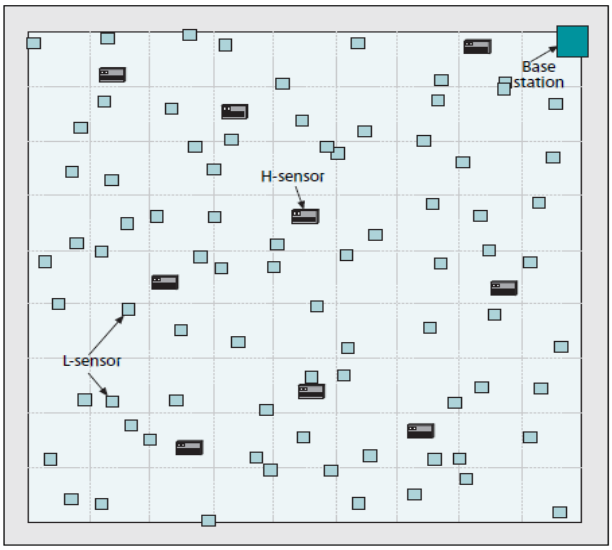


Figure 3. *An heterogeneous sensor network.*

کشف محل امن :

همانطور که قبلاً ذکر شد، موقعیت حسگرها نقش مهمی را در همهٔ کاربردها از شبکه های حسگر ایفا می کند. مانند کنترل محیط و ردیابی و پیگیری اهداف. بنابر این چندین تکنیک بنیادی توسعه یافته برای شبکه های حسگر بی سیم نیاز به اطلاعات موقعیت حسگرها دارند، مانند پروتکل های مسیریابی جغرافیایی که تصمیماتشان را بر مبنای موقعیت نودها اتخاذ می کنند. علاوه بر این، کاربردهای زیادی از شبکه های حسگر بدون اطلاع از موقعیت نودها کار نمی کنند. پروتکل های کشف/تخمین موقعیت زیادی برای شبکه های حسگر پیشنهاد شده اند، این پروتکل ها یک ویژگی عمومی مشترک دارند : همهٔ آنها می بایست از یکسری نودهای خاص استفاده کنند، که نودهای راهنما نامیده می شوند، که فرض بر این است موقعیت خودشان را می دانند (مثلاً از طریق گیرنده های GPS یا پیکربندی دستی). این پروتکل ها در ۲ مرحله کار

می کنند. در مرحلهٔ اول نودهای غیر راهنما سیگنال های رادیوئی را که منابع پیام نامیده می شوند از نودهای راهنما دریافت می کنند. یک پیام مبدا شامل محل نودهای راهنماست. در مرحلهٔ دوم نودهای غیر راهنما مقیاس های مورد اطمینانی را ایجاد می کنند (مثلاً فاصلهٔ بین نودهای راهنما و نودهای غیر راهنما) مبتنی بر ویژگی های پیام های منابع بدون حفاظت. یک مهاجم ممکن است به آسانی محل تخمینی یک نود حسگر را گمراه کندو موجب اختلال شود در عملکرد نرمال یک شبکهٔ حسگر. به عنوان مثال، یک مهاجم ممکن است با ایجاد موقعیت نادرست منابع باعث اختلال در مسیر یابی شود. علاوه بر این، یک مهاجم ممکن است باعث سردرگمی یک نود راهنما شود و موقعیت های نادرست را منتشر کند با دروغگوئی در مورد موقعیت ها یا دستکاری سیگنال های راهنما. در موارد مشابه، نودهای غیر راهنما موقعیتشان را بصورت نادرست تعیین می کنند. اخیراً چندین مدل مکان یابی امن و قوی ارائه شده اند. دو دستاورد مرتبط با حملات خرابکارانه در زمینهٔ شبکه های حسگر بی سیم ارائه شده است. اولین دستاورد مبتنی است بر حداقل میانگین تخمین میدان(MMSE). خطای میانگین میدان به عنوان یک نشان دهنده استفاده می شود برای شناسائی و حذف موقعیت منابع خرابکارانه. دستاورد دوم از یک تکنیک تخمین موقعیت مبتنی بر رای استفاده می کند و بطور دائم رای گیری را اصلاح می کند برای تحمل موقعیت منابع خرابکارانه که توسط مهاجمان ارسال شده است. یک دانشمند، یک مسئلهٔ مکان یابی امن را فرموله کرد به عنوان یک مطلب در مورد حفاظت در مقابل ناهنجاری دخالت و پیشنهاد کرد یک تعدادی طرح برای حفاظت در مقابل ناهنجاری های بوجود آمده توسط مهاجمان.

مطالبی دربارهٔ بازدهی :

اکنون نگاهی داریم به مطالب بازدهی برای شبکه های حسگر بی سیم فوق الذکر. این دستاوردها شامل SOWSN و PADS و مکانیزهای ارائه شده هستند برای پردازش درون شبکه ای برای SOWSN ، پارامترهایی برای ورودی و خروجی انتخاب شده اند. پارامترهای ورودی برای نشان دادن سناریوی واقعی که می توانند اتفاق بیوفتند، استفاده می شوند. آنها شامل : ایستگاه های پایه، ظرفیت هر ایستگاه پایه، تعداد حسگرهای بکار گرفته شده در محیط انتقال، سرعت حسگر، تعداد اهداف و دورهٔ شبیه سازی. پارامترهای خروجی برای نشان دادن تاثیراتی بکار می روند که ممکن است مورد مطالعه قرار گیرند. آنها شامل محدودهٔ تعداد رویدادها باشند، تعداد ارتباطات برای هر رویداد، مسیرهایی برای هر رویداد. از آزمایشات صورت گرفته توسط Boudriga ، برای یک تعداد قابل افزایش حسگرها، متوسط تعداد مسیرها و ارتباطات در حال افزایش هستند. نرخ انتقال هم افزایش می یابد. همانگونه که سرعت حسگرها در حال افزایش است، میانگین تعداد دست به دست کردن هم در حال افزایش است. احتمال افت به تعدادی از پارامترها وابسته است، که شامل نرخ انتقال ، ظرفیت ایستگاه پایه و تعداد حسگرها. با افزایش تعداد حسگرها ، احتمال افت هم کاهش می یابد و این مانند افزایش ظرفیت ایستگاه پایه و افزایش نرخ انتقال صحیح می باشد. Boudrigaبیان کرد زمانی که تعداد حسگرها ۶۰۰ یا بیشتر است احتمال افت ثابت می شود با وجود ظرفیت ایستگاه پایه و محدودهٔ انتقال.

:PADS

PADS در تمام شبه سازی ها در ۲ پروتکل دیگر قرار داشت، Tinysec و AODV و یک پروتکل مسیریابی نا امن. ۲ نوع شبیه سازی انجام شد بر روی هرکدام از این پروتکل ها. یک مجموعه از آن مستلزم یک سایز کلی پیام بود از ۲۳ بایت در حالی که دیگری نیاز به ۲ بایت داشت. در نتیجه در یک پیام به اندازهٔ ۱۸ بایت برای AODS و ۲۲ برای PADS و ۲۳ برای Tinysec. ۳ محدوده مورد ارزیابی قرار گرفت : پنهانی (زمان میانگینی که یک بسته نیاز دارد برای رسیدن به ایستگاه پایه)، خروجی بصورت بیت بر ثانیه است و میانگین انرژی برای هر نود استفاده می شود. زمانی که مجموعهٔ اول از شبیه سازی اجرا شد، رکود برای AODV و PADS یکسان بود، اما از میانگین بدتر بوددر افزایش تعداد نودها برای Tinysec. بازده افزایش تعداد نودها برای PADS و AODV قابل مقایسه هستند اما PADS یک سطح از امنیت هم دارد.

Tinysec از نظر بازدهی بدترین بود. مصرف انرژی برای PADS و AODV همچنین قابل مقایسه است به جز زمانی که تعداد نودها ۴۵ باشد. Tinysec بدترین استفاده از انرژی را دارد که به عنوان یک نتیجه از نرخ بالای خطا در دریافت پیام ها بیان می شود.برای ست دوم از شبیه سازی ها ، پنهان سازی برای PADS و AODV افزایش می یابد، اما Tinysec از هر دوی آنها بدتر است. بازدهی Tinysecربطی به پنهان سازی ندارد از زمانی که نرخ موفقیت آن پایین است. بازدهی برایAODV و PADS بطورقابل ملاحظه ای بهتر است از Tinysec و این بخاطر بازدهی Tinysec است که تعداد پیام کمتری دریافت می کند. همانند ست اول از شبیه سازی ها، مصرف انرژی Tinysec خیلی بالاتر از AODV و PADS است.

پردازش درون شبکه ای :

یک نمونهٔ اصلی شبیه سازی شده است در میان اجرای اصول رمزنگاری شامل تولیدکنندگان زنجیرهٔ درهم سازی یکطرفه و MAC بر روی ذراتBarkeley . مقیاس بندی در این نمونه اصلی شامل سربار نصب شبکه، بازدهی تراکم داده ها و تجهیزات ذخیرهٔ کم. مقیاس بندی توسط اجرای ذرات انجام می شود شامل محاسبه و تجهیزات حافظه. سنجش سربار نصب شبکه شامل ساختن یک شبکه حسگر بی سیم سلسله مراتبی چندسطحی است با ایستگاه پایه در مرکز شبکه. شبکه تقسیم میشود به چند گروه از حسگرها که هر سطح از یک گروه حسگر، تقسیم می شود به چندین سطح پایین تر از گروه حسگرها. برپایی شبکه شامل چندین سطح از پیام ها است برای مبادله با اندازه هایی برای تعدادی از بسته های مبادله شده برای برپایی یک شبکهٔ سلسله مراتبی چندسطحی. وقتی که تعداد سطوح افزایش می یابد، سطوح شبکه دچار سربار شده و تعداد گروه حسگرها نیز افزایش می یابند. سنجش بازدهی پردازش درون شبکه ای در طی یک آزمون برای تمام نودهای حسگر صورت گرفت که داده های جمع آوری شده توسط حسگرها را گزارش می کند هرکدام از مجموعه های مرتبط برای محاسبهٔ ارزش یک سیگنال حسگر. این اطلاعات از اعضای گروهش دریافت شده است که فرستاده شده است به سمت مجموعهٔ آن. برپایی شبکه برای این آزمایش همچون روش قبلی است. با افزایش تعداد پیام ها، تعداد بسته ها نیز افزایش می یابند در یک سرعت آرام برای جمع آوری کنندگان در ۳ سطح، اما افزایش چشمگیری خواهد داشت زمانی که هیچ جمع آوری نداشته باشد. در کل، وقتی که سطح جمع آوری افزایش می یابد، تعداد بسته های کمتری مبادله می شوند وقتی که تعداد پیام ها افزایش می یابد. جمع آوری کنندگان نیاز به حافظه دارند برای ذخیرهٔ کلیدهای رمزنگاری، زنجیرهٔ درهم ریختگی، اطلاعات توپولوژی از گروه حسگرهای آنها. حافظه ای که برای ذخیرهٔ این اطلاعات نیاز است کوچک است اما از نظر توپولوژی شبکه گسترش می یابد، همچنین نیازمندی به شبکه هم افزایش می یابد. نیاز به حافظه برای خود توپولوژی ممکن است فراتر باشد از آنها برای کلیدها و زیرکلیدها. دستگاه Berkeley ، KB۴ رم و KBEEPROM۵۱۲ دارد، بدین معنا که اطلاعات توپولوژی می تواند بر روی EEPROM ذخیره شود و اگر شبکه یک جمع کنندهٔ سطح بالا باشد، بیشتر زیر کلیدهای مشترک می توانند در EEPROM ذخیره شوند. جمع آوری کنندگان می توانند از ۲ مکانیزم برای ارسال فرمان به تمام نودهایشان در گروه حسگرها استفاده کنند : µTESLA و کلیدهای نا هموار. بسته ها نیاز دارند که یک دستور را منتشر کنند که توسط اندازه های مختلفی از حسگرهای گروه ها اندازه گیری شده باشد با همان تراکم. در مقایسه با استفاده از یک پیام واحد، هم µTESLA و هم کلیدهای ناهموار از سربار کمتری برخوردارند. باید توجه کرد که کلیدهای ناهموار نیاز به همزمان سازی ندارند و توسط کلیدهای تأخیری قابل جلوگیری نیستند، افزایش زمان نهایی نیاز به انتشار دستورات دارد.

نکات امنیتی بی سیم :

همزمان با توسعهٔ شبکه های بی سیم (حسگر) مبحث امنیت نیز مهمتر می نماید. از آنجایی که بیش از ۴۰% اطلاعات انتقالی از طریق نقاط دسترسی بدون رمزنگاری انتقال می یابد ، لذا نگرانی ها در مورد افزایش ا منیت بیشتر می شود که همین امر یک سیاست امنیتی قابل اجرا و کارامد را می طلبد.

به دلیل پخش همگانی در این شبکه ها، موجودیتی که مهارت و تجهیزاتی را داشته باشد می تواند این انتقال ها را رصد کند و به شبکه نفوذ کند. برای داشتن یک امنیت موفق می بایست کلیه خطرات درک شوند.

الف – آسیب پذیری WEP (Wireless Equivalent Privacy)

بسیاری از مطالب امنیتی ریشه در آسیب پذیری پروتکل WEP (Wireless Equivalent Privacy) دارد. این پروتکل در زمان اعمال محدودیت های حکومتی در مورد رمزنگاری های قدرتمند طراحی گردید. کلید محرمانهٔ WEP به تنها ۴۰ بیت محدود بود درحالی که اکنون می توان از کلیدهایی تا ۱۰۴ بیت نیز بهره جست. کلیدهای کوتاه برای شکستن به اندازه کافی سخت و مقاوم نبودند. یکی از آسیب های عمدهٔ WEP این است که یک مهاجم می تواند کلید محرمانه را با نظارت بر انتقالات بین WAP (Wireless Access Point)و یک کلاینت ، بدست آورد. (که از پروتکل RC4 استفاده می شود) . WEP از ۲ ضعف عمدهٔ دیگر هم رنج می برد. نخست، یک سیستم مدیریت کلید ضعیفی را ارائه می کند. دوم ، ضعف در سیستم حفظ تمامیت داده هاست زیرا Check sum ها رمزنگاری نمی شوند !!!

ب_ حفظ اعتبار و اطمینان

یکی دیگر از مطالب خطرناک و بدیهی دیگر این است که بسیاری از مدیران شبکه هیچ نگرانی از پیکربندی مناسب WAP های شبکه خود ندارند !! دسترسی فیزیکی به WAP ها یکی دیگر از نگرانی هاست .

ج _ کنترل انتقال

WLANs از لحاظ تحلیل بسته ها و نظارت پخش همگانی آسیب پذیر است. تحلیل بسته ها بدین معناست که یک مهاجم می تواند بسته ها را تفسیر کرده و بخواند. نگرانی دیگر از این است که داده ها بیشتر از محدودهٔ تحت پوشش انتقال یابند و به اصطلاح " چک کردن سیگنال " به وقوع بپیوندد .

د _ نگرانی های دیگر

یکی دیگر از نگرانی ها حملهٔ انکار سرویس یا DoS است که باعث خارج از سرویس شدن تجهیزات می گردد. نگرانی دیگر فریبکاری MAC Address است. از زمانی که پروتکل 802.11 از آدرس MAC برای اعتبارسنجی استفاده می کند، مهاجمان می توانند با تغییر MAC آدرس های خود به شبکه نفوذ کنند.

یک چهارچوب کاری برای یک سیاست موثر در امنیت شبکه های حسگر بی سیم :

با روند افزایش وابستگی به تکنولوژی ، سازمان ها هم دچار نگرانی بیشتری در مورد حفظ دارایی های اطلاعاتی خود گردیدند. از این رو می بایست یک چهارچوب کاری برای یک سیاست موثر در امنیت حسگر بی سیم را پیش بینی نمود.

الف _ چرا سیاست ؟

سیاست های امنیتی سازمانها را قادر به تعریف سرمایه های مهم می کند و امنیت گام به گامی را برای محافظت از این سرمایه ها ارائه می کند. یک سیاست امنیتی با نگارش مطلوب یک منبع مستند را ارائه می کند که به سوالات کاربران در مورد امنیت بی سیم حسگر پاسخ می دهد.

ب_ اجزای کلیدی

وجود یک سیاست امنیتی بجا و شایسته تضمین می کند که آسیب پذیری ها ، خطرات و مقیاس ها برای یک سازمان مستند سازی شده اند. سیاست های امنیتی به ۳ سطح طبقه بندی شده اند : طبقه بندی سطح بالا ، طبقه بندی شده بر اساس موارد امنیتی و طبقه بندی شده بر اساس سیستم. بطور خلاصه می توان نمونه های زیر را جزء اجزای کلیدی به حساب آورد : تخمین و ارزیابی مخاطرات، استانداردها، تکنولوژی ها ، Logging کردن و حسابرسی، امنیت WAP ، مجوزهای کاربران، آموزش کاربران و البته اجرای سیاست ها .

ج _ الگوهای سیاست ها

از بین الگوهای سیاست های امنیتی که مورد آزمایش واقع گردیدند ، الگوی سیاستی امنیتی محافظ از همه کاملتر بود. که البته این سیاست مشخصاً برای شبکه های بی سیم نوشته نشده است.

د _ کمبودهای نسبی

این امر که سیاست های امنیت اطلاعات در عصر اطلاعاتی امروزه یک نیاز هستند، بطور گسترده مورد پذیرش واقع گردیده است. اکثر منابع همچنین خط مشی هایی را برای توسعه دهندگان سیاست ها فراهم می کنند که به یاد داشته باشند چه زمانی نیاز به ارتقا و توسعهٔ سیاست ها می باشد.

یک معماری مدیریت امنیت مبتنی بر سیاست برای شبکه های حسگر بیسیم

کارهای متعددی در آثار و مطالعات علمی برای ممانعت از تاثیرات مهاجمان در شبکه، برای امنیت شبکه های حسگر بیسیم ارائه شده است. اگرچه، هر راه حل امنیتی عملیاتی را به شبکه می افزاید . عملیات یا فعالیت ها مانند پردازش و ارتباطات از انرژی و زمان استفاده می کنند و شبکه های حسگر بی سیم می بایست انرژی خود را برای افزایش طول عمر ذخیره کند زیرا امکان شارژ باطری وجود ندارد .

یکی از الزامات عمومی اکثر راه حل ها برای شبکه های حسگر، افزایش و ارتقای دسترسی به شبکه و منابع آن است. ذخیره انرژی یکی از اهداف اصلی است برای توسعه و ارتقای در دسترس بودن به وسیلهٔ ارتقای طول عمر شبکه. اگرچه مشکلات ایمنی ممکن است دیده شوند ، مخصوصاً حملهٔ خارج از سرویس کردن، که سرویس های شبکه را محدود می کنند قبل از اتمام باطری نودهای حسگر در شبکه های بیسیم.

تکنیک های مدیریت شبکه، که با هدف کارائی ممکن و بهینه سازی عملیات شبکه طراحی شده اند، می توانند مورد استفاده قرار گیرند برای شبکه های حسگربی سیم جهت گسترش و ارتقای استفاده از منابع .

یک سیستم مدیریت امنیت می تواند در یک شبکه جهت کاهش مصرف انرژی کار کند . به عنوان مثال ، خاموش و روشن شدن سرویس های امنیتی و توابع بر حسب تقاضا و نیاز شبکه . بنابراین شبکه می تواند انرژیش را ذخیره کند زمانی که هیچ نشانه یا احتمالی از حضور مهاجمان وجود ندارد. سیستم های شناسایی مهاجمان (IDS) می توانند در زمان حضور مهاجمان ، به شبکه هشدار بدهند توسط تولید و گزارش رویدادها . در روش مدیریت خودکار ، مدیریت سیستم می تواند بصورت خودکار سیستم های امنیتی شبکه را فعال یا غیرفعال کند.

کار صورت گرفته اخیر ، یک مدل مدیریت امنیت برای شبکه های حسگر بیسیم ارائه می دهد، شامل انتخاب اجزای امنیتی، توصیف مدیریت اطلاعات، تعریف پیام ها و تعریف رویدادهای امنیتی . در مدل خودکار ، عناصر امنیتی در چند سطح گروه بندی شده اند، که می توانند جهت پاسخگوئی به رویدادهای دفاع در مقابل مهاجمان استفاده شوند.

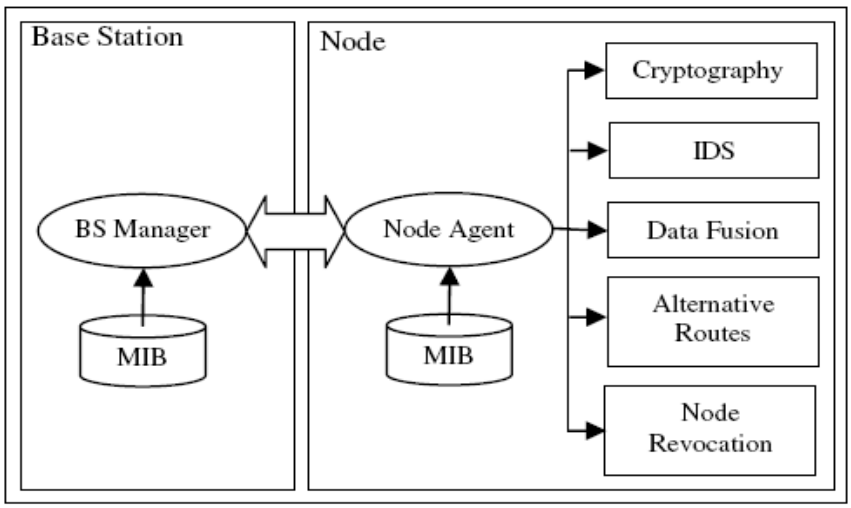
هدف افزایش طول عمر شبکه است به وسیله جلوگیری از تاثیرات حملات و ذخیره انرژی توسط فعالسازی سرویس های امنیتی فقط در زمان نیاز و ضرورت . مزیت اصلی این کار پیشنهاد یک معماری مدیریت امنیت است که در حملات امنیتی فعالسازی و غیرفعالسازی پویای عناصر امنیتی را فراهم می کند.

هدف این معماری ۲ گانه است : از یک جهت، برای حفاظت شبکه حسگر از حملات گوناگون و از جهت دیگر، صرف حداقل منابع ممکن برای یک موقعیت مطمئن از حملات .

تنها برای فعال کردن یک پیکربندی خاص برای هر کاربرد، معماری بصورت مبتنی بر سیاست ایجاد گردیده است. بنابراین شرایط بر پایه رویدادها بنا شده است و فعالیت ها مانند تغییر سطوح امنیت می تواند طبقه بندی شود.

الف ـ مدل مدیریت شبکه

در این مدل شبکه مرجع، یک شبکه مسطح همگن است ، بدین معنا که همهٔ نودها مشخصه های سخت افزاری مشابه دارند و توابع یکسانی را پردازش می کنند، به ویژه توابع مسیریابی و ارسال . مدل مدیریت ، که در ادامه نشان داده شده است، تشکیل شده است از یک مدل مبتنی بر اطلاعات، تبادل پیغام ها و رویدادها. شکل ۱ عناصر و اجزای شبکه را نشان می دهد. ایستگاه پایه نقش اداره کننده را دارد که با نمایندهٔ نودها در ارتباط است. هم مدیر و هم نماینده می بایست MIB (Management Information Base) را بشناسد . این مدل طوری در نظر گرفته شده است که اجزای امنیتی نوصیف شده می توانند جزئی از نمونه های مدیریت باشند . در این روش ، پیکربندی اجزاء امنیتی پویاست، بدین معنا که در زمان عملیات می توانند اضافه یا کم شوند، و همچنین فعال یا غیر فعال گردند.



مدل معماری امنیت

ب ـ مولفه های امنیت

برای رویارویی با مسائل امنیتی در شبکه های حسگر بی سیم تکنیک ها ، الگوریتم ها و استراتژی های زیادی مطرح شده اند. برای پشتیبانی از طرح پیشنهادی و تصدیق معماری مدیریت، یک مجموعه ای از راه حل های مدیریتی امنیتی انتخاب شده اند. البته این مجموعه کامل نیست اما راه حلهای خوبی را مطرح می کند. برای امنیت داده ها و جامعیت سرویس های رمزنگاری در نظر گرفته شده اند، برای توسعهٔ و ارتقای در دسترس بودن شبکه، مکانیزم مقابله با مهاجم انتخاب شده است برای یافتن مشکلات امنیتی ، مکانیزم مسیریابی امن و پیوستگی امن داده ها برای تضمین تحویل داده ها به ایستگاه پایه .

ج ـ سطوح امنیت

در شبکه های ملزم به استفاده کم از انرژی ، استراتژی بدینگونه است که استفاده از اجزاء امنیتی فقط بر حسب نیاز باشد . معیار تشخیص لزوم استفاده از آن عناصر هم مبتنی بر وجود مهاجمان است . بدین معنا که با تشخیص حضور مهاجمان، به نسبت مخاطرات امنیتی ، عناصر امنیتی فعال یا غیرفعال شوند.

در این طرح ، اجزای امنیتی به ۲ دستهٔ فعال و غیرفعال تقسیم می شوند پس از رخداد یک اتفاق خاص . این منجر به ایجاد حالت های عملیاتی متفاوتی در شبکه ها می شود که سطح امنیتی نامیده می شود که تصمیم گیری خودکار را برای مدیر آسانتر می کند بر پایهٔ اطلاعات رسیده از نودها . در هر سطح امنیتی، یک زیر مجموعه ای از عناصر امنیتی برای محافظت در برابر مهاجمان فعال می شوند .

شبکه می تواند بنا به نیاز به سطوح امنیتی بالاتر تغییر حالت دهد و یا با ناپدید شدن مهاجمان یا کمبود انرژی به سطوح امنیتی پائین تر تغییر حالت دهد . برای ذخیرهٔ انرژی اجزای امنیتی مانند سیستم های IDS می توانند غیرفعال شوند. در جدول شماره ۱ عناصر امنیتی به ترتیب مصرف انرژی دسته بندی شده اند . در پائین ترین سطح ،هیچ عنصر امنیتی فعال نیست و فقط پیوستگی داده ها برای کاهش مصرف انرژی شبکه فعال است . در سطح بحرانی کلیهٔ عناصر امنیتی فعال هستند .

SECURITY LEVELS

Level	Security components used
Low	- No intruder detection in nodes - No cryptography - Data fusion enabled
Medium	- 17% of nodes execute intruders detection - Routing update authenticated end-to-end - Hop-by-hop cryptography enabled - Data fusion enabled - Alternative routes
High	- 33% of nodes execute intruders detection - End-to-end cryptography enabled - Routing update authenticated hop-by-hop - Alternative routes - No data fusion
Critical	- 50% of nodes execute intruders detection - No data fusion - End-to-end and hop-by-hop cryptography enabled - Routing update authenticated hop-by-hop - Alternative routes

جدول شماره ۱

د ـ تشریح سیاست ها

چندین کاربرد متفاوت برای امنیت شبکه های حسگر ارائه شده است که هر کاربرد ملزومات امنیتی و محدودیت های انرژی خاص خود را دارد. فقط برای فعالسازی یک پیکربندی مشخص از شرایط و فعالیت ها در مدیریت امنیت، یک معماری مدیریت سیاست محور را ارائه داده ایم . یک سیستم مدیریت مبتنی بر سیاست مقررات را در قالب " شرایط – فعالیت " شرح می دهد .

چندین شرایط می توانند سطوح تراکنش را شروع کنند , مبتنی بر نقشهٔ محصول ، رویداد محافظت در برابر مهاجم، در نقشهٔ انرژی یا دیگر علائم حضور مهاجمان در شبکه . هر کاربرد می بایست قادر به تشخیص موقعیت های مهم باشد . ما استفاده از سیاست ها را برای تشخیص این شرایط برای هر کاربر پیشنهاد داده ایم .

قوانین سیاست های مدیریت امنیت می توانند تعریف کنند : شرایط سطوح تراکنش ، گروه های شبکه ، فعالسازی سطوح امنیتی متفاوت برای گروه های نودها ، کدام نودها می بایست IDS را اجرا کنند ، فعالیت های اجرائی در هر رویداد . قوانین باید در ایستگاه پایه تعریف شوند ، در جایی که مدیر حضور دارد و در حال اجرا است . مدیر قوانین را می خواند با توجه به رویدادهای رسیده از نودها ، فعالیت ها را صورت می دهد.

مهمترین قوانین می بایست شرایط خاص را برای سطوح تراکنش مشخص کند . آنها شامل : گم شدگان مهم در نقشهٔ محصول ، حفاظت در برابر نفوذگران در یک نود ، تقویت حفاظت در مقابل نفوذگران به کمک نودهای دیگر ، حفاظت در برابر نفوذ مهاجمان توسط ایستگاه پایه ، کاهش انرژی در برخی از نودها یا برخی از نواحی ، نودهای بدون محصول . هر کاربرد باید سیاست های خود را با توجه به ملزوماتش مشخص کند .

چندین مثال از سیاست ها : سطح امنیت می بایست افزایش یابد زمانی که تعداد رویدادهای X مهاجم دریافت شده است و سطح امنیت می بایست کاهش یابد پس از X ثانیه بدون حضور نشانه ای از مهاجمان . سطح امنیت می بایست کاهش یابد زمانی که میزان باطری کمتر از

X% باشد . زبانهای سیاست متعددی وجود دارند ، مانند Ponder ، SPL – CIM ، Rei . یک زیر مجموعه از Ponder می تواند برای مشخص کردن سیاست های ما استفاده گردد .

ذ _ اعمال مدیریتی

در این طرح از پیام های GET ، SET و TRAP استفاده می شود . در طی فرایند نصب ، نودها می بایست یک بستهٔ مسیریابی ارسال کنند ، با اطلاعاتی راجع به درخت مسیریابی . این اطلاعات برای حفاظت در مقابل نفوذگران در ایستگاه پایه مهم است . ایستگاه پایه یک پیام SET را برای تغییر سطح امنیت ارسال می کند ، زمانی که این عمل نیاز باشد . این پیام برای گروه هایی از نودها جهت تغییر سطح امنیت می تواند بصورت Broadcast یا Multicast ارسال شود . نودها از پیام های IDS برای مطلع کردن ایستگاه پایه از محافظت در برابر مهاجمان استفاده می کند . همچنین از محموله های اطلاعاتی می توان برای اطلاع رسانی از شرایط غیرعادی دیگر نظیر کاهش باطری بهره جست .

ارزیابی

در شبکه های WSN سه استراتژی در مورد راه حل های امنیتی وجود دارد : ۱- بدون راه حل امنیتی ، ۲ – وجود برخی راه حلهای امنیتی در تمام زمان ها ، حتی اگر هیچ نفوذگری در شبکه وجود نداشته باشد ، ۳ – استفاده از یک چهارچوب امنیتی برای ایجاد تعادل بین راه حل های امنیتی و استفاده از انرژی ، همانگونه که در این طرح مطرح گردید . استراتژی اول ، بدون راه حل امنیتی ، می تواند برای شبکه های بسته مفید باشد که در هر صورت از حضور دشمن جلوگیری می شود . اما در اکثر کاربردهای رایج ، حضور یک دشمن می بایست مد نظر قرار گیرد . بنابراین باید تفاوت های ما بین استفاده از انرژی را در استراتژی های دیگر مورد ارزیابی قرار دهیم ، با راهکارهای امنیتی تمام وقت یا با مدیریت امنیت .

شبیه سازی مدل

ما مجموعه ای از شبیه سازی ها را برای تصدیق مدل ارائه شده بیان کردیم . در این شبیه سازی ها ، ما علاقه مندیم تا در مورد مصرف انرژی هر عنصر امنیتی تحقیق کنیم . ما از یک شبیه ساز مبتنی بر رویدادهای گسسته استفاده کرده ایم ، که توسعه یافته است توسط DCC – UFMG .

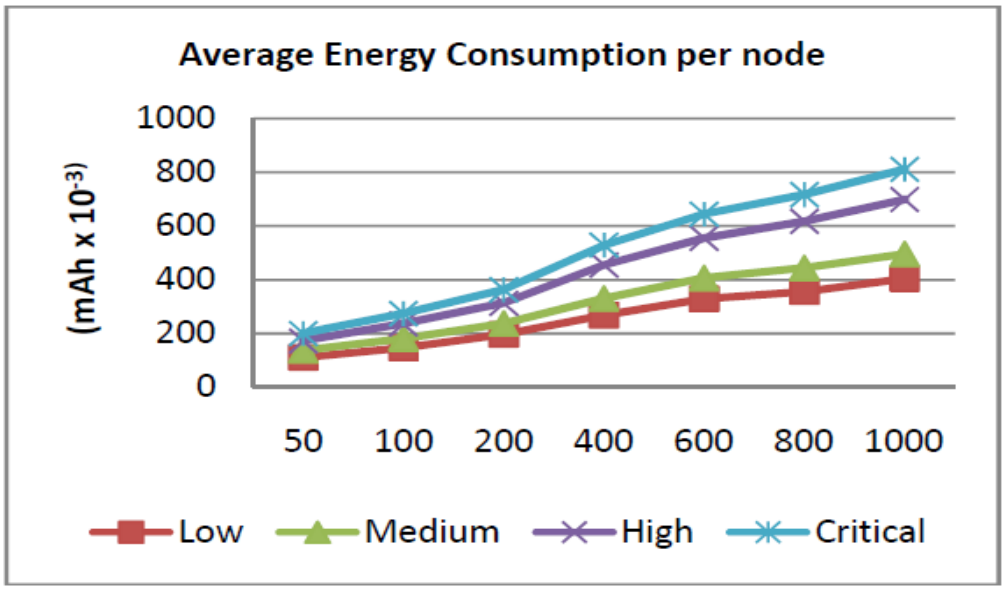
هر شبیه ساز در ۱۹۸۰ ثانیه عمل می کند ، حدوداً ۳۰ دقیقه . در این زمان ، ۱۳۵ عملیات توسط هر نود حس می شود . ۳ فاز به روز رسانی مسیریابی اجرا گردید ، یکی در زمان شروع و دیگری پس از هر ۴۵ عمل حسی . در گام اول پیوستگی داده ها جهت کاهش مصرف انرژی فعال شده است . جدول ۲ میانگین انرژی مصرفی را در حالت مرجع شبکه بدون تجهیزات امنیتی نشان می دهد .

ENERGY CONSUMPTION IN NETWORK WITHOUT SECURITY COMPONENTS

Number of nodes	Total transmitted packets	Total received packets	Average spent energy per node ($mAh \times 10^{-3}$)
50	16229	112170	110.27
100	42379	298276	146.33
200	112592	798710	195.75
400	308612	2186616	267.99
600	568560	4022888	328.74
800	817687	5802845	355.53
1000	1162417	8238595	403.87

مصرف انرژی در یک شبکه بدون اجزای امنیتی

ما افزایش مصرف انرژی توسط تجهیزات امنیتی را مورد ارزیابی قرار داده ایم ، که در مدل مدیریت امنیت استفاده شده است که بصورت گرافیکی در شکل ۲ نشان داده شده است . میانگین مصرف انرژی در سطح بحرانی می تواند تا ۰۰% افزایش یابد . سطوح حاوی اجزای مطابق جدول ۱ هستند . ما در این طرح موارد و مباحث رمزنگاری ، پیوستگی داده ، مسیریابی متناوب و محافظت در برابر نفوذگران را در نظر گرفته ایم .



مصرف انرژی در سطوح امنیتی برای هر نود

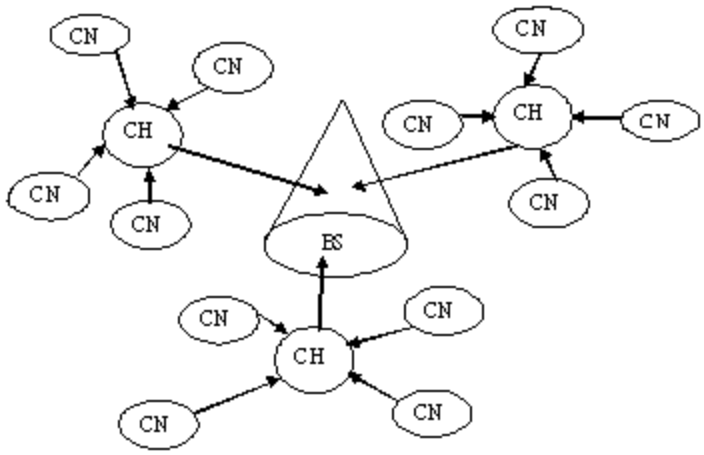
هزینهٔ مدیریت در مقایسه با انرژی ذخیره شده بسیار پایین تر است . مگر در حملات عظیم که پیام های مدیریتی ۱%کل پیامهاست . بر طبق مدل شبیه سازی شده ، انرژی ذخیره شده توسط این روش میتواند تا ۱۰۰%افزایش یابد .

اجرای الگوریتم رمزنگاری RSA برای شبکه های حسگر بیسیم

در شبکه های حسگر بیسیم ، به علت محدودیت منابع و کمبود انرژی ، معمولاً از پروتکل ها و الگوریتم های رمزنگاری متقارن استفاده شده است . اما پروتکل رمزنگاری RSA بخاطر محدودیت انرژی منابع و کمبود حافظه تا بحال بطور جدی مورد استفاده قرار نگرفته است . در زیر نشان داده خواهد شد که پروتکل RSA چگونه بصورت کارامد و با استفاده از محاسبات بهینه برای امنیت شبکه های حسگر بیسیم استفاده می گردد . برخی از محدودیت ها در امنیت شبکه های حسگر بیسیم عبارتند از منابع محدود ، محدودیت حافظه و فضای ذخیره سازی ، محدودیت انرژی و ...

اجرا

در اینجا به منظور کاهش هزینهٔ اجرای الگوریتم RSA و کاهش مصرف انرژی این الگوریتم ، ۳ مرحله تعریف شده است : نخست ، یک مدل طراحی شده است برای ارتباط امن از نودهای خوشه به سمت مرکز خوشه . دوم ، الگوریتم RSA را جهت کاهش هزینهٔ محاسبات اصلاح کرده ایم . سوم مبادرت به تغییر فرمت بسته ها کردیم . در این سناریو ، یک مقدار اولیهٔ انرژی را در نظر گرفتیم . این مقدار برای دامنه انتقال و دریافت و برای نودهای خوشه و مرکز خوشه همانند هم است . وقتی که نودهای حسگر مستقر می شوند ، در دامنهٔ خودشان یک خوشه را ایجاد می کنند . هر خوشه خوشهٔ مرکزی دارد و تعدادی گرهٔ معمولی . ارتباط با ایستگاه پایهٔ شبکه وظیفهٔ نودهای مرکزی است .

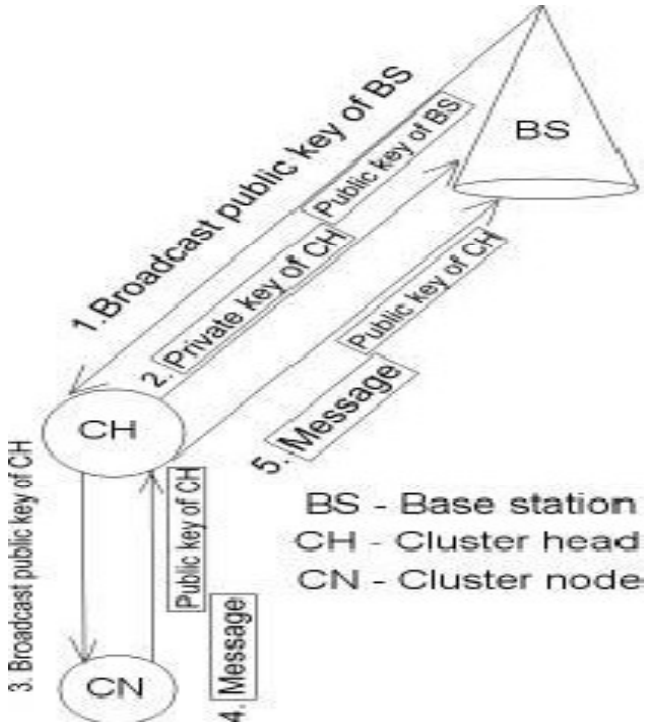


ارتباط نودهای مرکزی خوشه ها با ایستگاه پایه

توزیع کلید

در این سناریو ، ایستگاه پایه کلید عمومی خود را در شبکهٔ خود پخش همگانی می کند . نود مرکزی خوشه کلید عمومی را در حافظهٔ خود ذخیره می کند . هر نود مرکزی خوشه ۲ عدد اول طولانی متمایز p و q را تولید می کند . سپس با استفاده از این p و q ، نود اصلی خوشه یک مجموعه کلید عمومی (e , n) و یک مجموعه کلید خصوصی (d , n) تولید می کند . سپس نود اصلی خوشه ، کلیدهای خصوصی متناظر که توسط کلید عمومی ایستگاه پایه که رمزنگاری شده اند را ارسال می کند . ایستگاه پایه پیام های ارسالی از نود مرکزی خوشه را با استفاده

از کلید خصوصی خود رمزگشایی کرده و کلید خصوصی تمامی نودهای اصلی خوشه را که می خواهند با آن در ارتباط باشند را می گیرد . هر نود اصلی در خوشه کلید عمومی خود را پخش همگانی می کند . بعد از گرفتن کلید عمومی نود اصلی خوشه ، نود آن را در حافظه خود ذخیره می کند . آن نود از کلید عمومی زمانی که می خواهد پیامی را به سمت نود اصلی ارسال کند ، استفاده می کند . نود اصلی متناظر پس از دریافت پیام آن را رمز گشائی نکرده ولی آن را به ایستگاه پایه تحویل می دهد . ایستگاه پایه با استفاده از کلید خصوصی خود که متناظر با آن نود اصلی خوشه می باشد ، پیام را رمزگشایی کرده و پیام اصلی و اولیه را بدست می آورد . بدین ترتیب یک ارتباط ایمن بین نودهای خوشه و ایستگاه پایه ارائه شده است . نود مرکزی خوشه پیام های دریافتی از نودها را رمزگذاری یا رمزگشایی نمی کند بنا بر این انرژی این کارها را ذخیره می کند . از آنجا که نودهای اصلی تمامی پیام های دربافتی را به ایستگاه پایه تحویل می دهد ، بطورکلی انرژی بیشتری نسبت به نودهای خوشه از دست می دهد . به همین علت ، مدل شبکه را به گونه ای طراحی کرده ایم که نود اصلی خوشه در فرایند رمزگشایی پیام درگیر نباشد . هرگاه نود خوشه یک مجموعه جدید از کلید خصوصی و کلید عمومی تولید کند ، کلید خصوصی را به سمت ایستگاه پایه پخش همگانی می کند . در همان زمان ، کلید عمومی را به سمت نودهای حسگر پخش همگانی می کند که همگی در شکل زیر نشان داده شده اند.



مدل ارتباطی بین نودها و ایستگاه پایه

مجدداً بخاطر امنیت ، ایستگاه پایه کلید عمومی و خصوصی را تولید کرده و کلید عمومی خود را که توسط هر کلید عمومی نود اصلی خوشه رمز گذاری شده است را پخش همگانی می کند . بنابراین فقط نودهای اصلی خوشه در شبکه به کلید عمومی ایستگاه پایه دسترسی دارند و یک ارتباط امن بین ایستگاه پایه و نود اصلی محافظت می گردد . تکرار عمل پخش همگانی کلید عمومی برای ایستگاه پایه با نود اصلی خوشه متفاوت است . همانگونه که ایستگاه پایه محدودیت انرژی و حافظه ندارد ، پخش همگانی کلید عمومی را بیشتر از نود اصلی خوشه انجام می دهد . مدل ارتباط بین نود اصلی خوشه و ایستگاه پایه در شکل فوق به تصویر کشیده شده است .

رمزنگاری

در این سناریو خوشه ای که می خواهد پیامی را ارسال کند ، آن را رمزنگاری کرده و با استفاده از الگوریتم RSA و از طریق نود اصلی خوشه به ایستگاه پایه ارسال می کند . محدودیت انرژی و حافظه بخش های حیاتی نودهای خوشه هستند . ما فرمت بسته ها را با اضافه کردن یک فیلد بنام فیلد هویت تغییر می دهیم . فرمت بسته های اصلی ، تغییر داده شده و رمز نگاری شده به ترتیب در شکل زیر نشان داده شده اند :

SRC	Original msg	.....	DEST

Figure 2: Original Message Packet Format

SRC	ID Field	Modified msg	.....	DEST

Figure 3: Modified Message Packet Format

SRC	Encrypted ID Field	Encrypted Modified msg	.....	DEST

فرمت بسته (Packet) پیام های رمزنگاری شده

الگوریتم اصلی RSA برای اینکه برای نودهای حسگر قابل استفاده باشد تغییر داده شده است . زمانی که نودهای حسگر می خواهند تعدادی پیام را ارسال کنند ، مقدار اصلی کد ASCII به ۳ دامنه ۱ الی ۳ تغییر می کند و به همین علت است که فیلد هویت را به فرمت افزوده ایم .

الگوریتم RSA

الگوریتم اجرایی برای این طرح در زیر ارائه شده است :

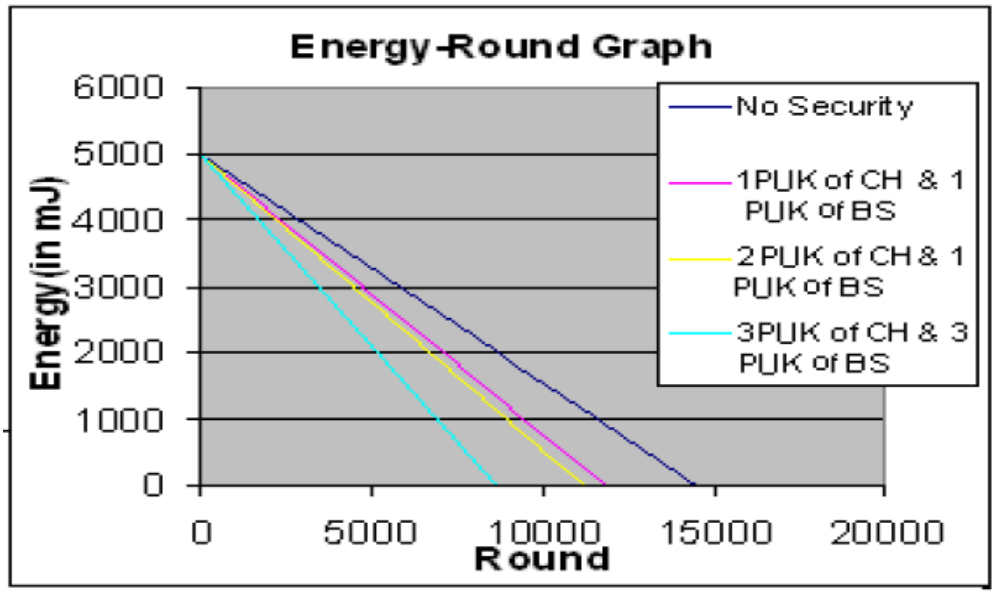
Step1. i=0 and p=5 and k= $(P_t)^5$ mod n // P_t is the modified value of the msg letters
Step2. A[i] =k, B[i] =p and k= (k*k) mod n
Step3. p=p*2 and i=i+1
Step4. **Repeat** Steps 2 to 3 For key>p
Step6. l=1, p=p/2 and i=i-1
Step6. l= {l*A[i]} mod n and key=key-p
Step7. **IF** (key>B[i]) **THEN** key=key - B[i] and
l= (l*A[i]) mod n
Step8. **Else** i--
Step9. **Repeat** Steps 7 to 8 **IF** Key >5
Step10. **IF** (key<=5) **THEN** compute b ←$(P_t)^k$ mod n
Step11. **Else** b=1
Step12. C_t←(l*b) mod n; // C_t is the Cipher text

نتیجه شبیه سازی

در این سناریو ، ما ۱۲ بسته از پیام ها را در نظر می گیریم که به عنوان یک دور فرستاده شده اند ، ارسال از ۴ نود خوشه به نود اصلی خوشه بدین معنا که در هر دور ۳ پیام توسط هر نود خوشه (CN) فرستاده می شود به نود اصلی خوشه (CH) . در شکل ۵ و شکل ۶ ، چهار مورد متفاوت را نشان داده ایم برای نودهای معمولی و نود اصلی خوشه تا زمان از بین رفتن . برای ۴ مورد متفاوت در CH و CN گراف دور انرژی در نظر گرفته شده است : ۱- بدون امنیت ۲- امنیت با یک کلید عمومی (PUK) برای CH و BS برای ۳ پیام از هر CN . ۳- امنیت با ۲ کلید عمومی برای CH و یک کلید عمومی برای BS برای ۳ پیام از هر CN . ۴- امنیت با ۳ کلید عمومی برای CH و ۳ کلید عمومی برای BS برای ۳ پیام از هر CN . نتایج تطبیقی گراف دور انرژی برای CH و CN در شکلهای ۵ و ۶ به ترتیب نشان داده شده اند . شاخص های شبیه سازی طبق جدول ۱ ارائه شده اند :

Total packet size	36 bytes
Processing power of sensor nodes	5nJ / bit
Transmission power	50nJ / bit
Receiving power	50nJ /bit
Initial Energy	5J
Encryption and Decryption energy consumed	5.22nJ /bit

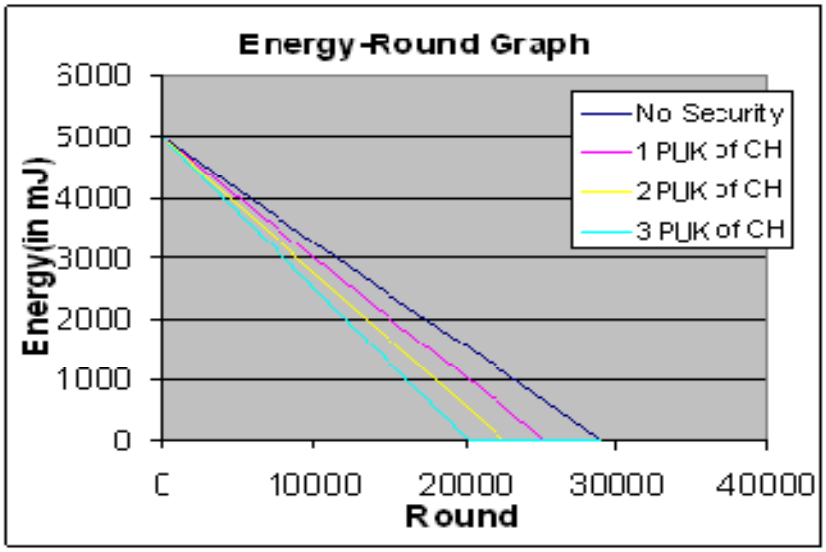
پارامترهای شبیه سازی



Energy-Round graph of Cluster Head (CH)

زمانی که هیچ امنیتی وجود ندارد ، CH میتواند به دور ۱۴۴۹۲ برود . زمانی که یک کلید عمومی رایج از CH استفاده می شود برای رمزنگاری ۳ پیام از CN و یک کلید عمومی رایج استفاده می شود برای رمزنگاری بستهٔ خصوصی CH ، CH می رود به دور ۱۱۸۲۰ . زمانی که ۲ کلید عمومی استفاده می شود ، به دور ۱۱۱۸۵ می رود .

در ۲ مورد پیشین ، BS از یک کلید عمومی برای رمزنگاریکلید خصوصیCH استفاده می شود . گراف فوق نشان می دهد که استفاده از ۳ کلید عمومی CH و ۳ کلید عمومی BS بالاترین ضریب امنیتی را برای هر نوع از شبکه ارائه می دهد زیرا CN هر پیام را رمزنگاری می کند توسط کلیدهای عمومی گوناگون CH و CH هر کدام از کلیدهای خصوصی خود را که توسط کلیدهای عمومی متفاوت BS رمزنگاری شده اند را ارسال می کند . 1PUKاز CH و 1PUK از BS امنیت کافی را به هر نوع از شبکه ارائه می کند . اگر چه ، اگر سیستم خواهان امنیت پائین تری باشد ، می توان با افزایش تعداد پیام ها در دور این کار را کرد . این کار همچنین بر طول عمر CH و CN می افزاید . همچنین استفاده کمتر از کلید عمومی برای پخش همگانی BS هم طول عمر CH را می افزاید . بنابراین سربار امنیت RSA برای نود اصلی خوشه به ترتیب ۱۸.۴ ٪ ،۲۲.۸٪ ، ۴۱.۳٪ است .

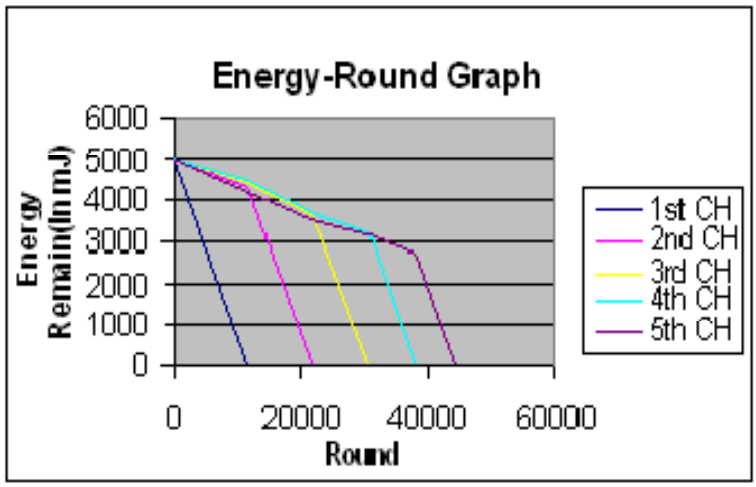


گراف دور- انرژی نود خوشه

بطور مشابه ، در شکل فوق موارد متعددی را برای نودهای خوشه نشان داده ایم . بنابراین سربار امنیتی نود خوشه برای RSA به ترتیب ۱۸.۴٪ ، ۲۲.۸٪ ، ۳۱٪ است . تا الان طول عمر یک نود اصلی خوشه منفرد و نود خوشه معمولی را برای محدودیت های امنیتی متعدد تحلیل کردیم . حال کل خوشه را تحلیل می کنیم . ما این سناریو را به ۲ دسته تقسیم می کنیم : (۱) نود اصلی خوشهٔ پویا با مقدار کل انرژی آستانه (۲) نود اصلی خوشهٔ پویا با نصف مقدار باقیمانده انرژی آستانه . نتیجه را با گرفتن 1PUK از CH و 1PUK از BS تحلیل می کنیم .

(۱) نود اصلی خوشهٔ پویا با مقدار کل انرژی آستانه

در اینجا ، نود اصلی خوشه تغییر می کند تا زمانی که نود اصلی خوشه از کار بیوفتد و اصطلاحاً بمیرد . زمانی که یک نود اصلی خوشه بمیرد یک نود خوشه معمولی جایگزین نود اصلی خوشه می گردد .



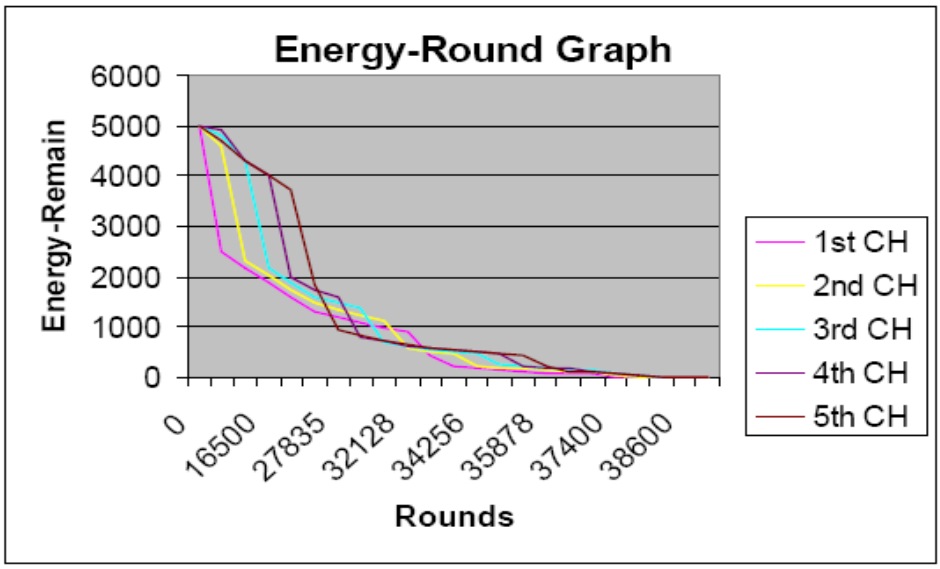
Energy-Round Graph of Dynamic Cluster Head

with its Total Energy Threshold

در شکل فوق ، گراف انرژی – دور یک کلاستر نشان داده شده است که شامل نود اصلی خوشه با مقدار کل انرژیش است . به بیان دیگر ، می توان گفت نود اصلی خوشه تا زمان مرگ تغییر نمی کند . می توان دید که اولین نود اصلی خوشه (CH) پس از ۱۱۸۲۰ دور می میرد . سپس یک نود خوشه ، به عنوان CH آن خوشه جایگزین می شود . سپس نود اصلی خوشه یعنی دومین نود اصلی خوشه پس از ۲۱۹۶۱ دور می میرد . بطور مشابه ، نودهای اصلی سوم و چهارم و پنجم به ترتیب پس از ۳۰۶۶۲ و ۳۸۱۲۷ و ۴۴۵۳۱ دور می میرند . بنابراین ، کل سیستم خوشه پس از ۴۴۵۳۱ دور می میرد . اما مرگ نودهای اصلی خوشه به ترتیب و یکی پس از دیگری اتفاق می افتد . در نتیجه پوشش سیستم شبکه ، با مرگ نودهای اصلی خوشه ، کاهش می یابد . بنابراین کارائی نودهای اصلی ثابت شبکه کاهش می یابد با تسلسل دورها .

(۲) نود اصلی خوشهٔ پویا با نصف مقدار باقیمانده انرژی آستانه

در اینجا ، نود اصلی خوشه تغییر می کند وقتی که مقدار باقیماندهٔ انرژی نود اصلی خوشه به نصف مقدار انرژی در زمانی که تبدیل به نود اصلی خوشه شد ، تقلیل می یابد . زمانی که انرژی باقیمانده کمتر از مقدار آستانه می شود ، نود اصلی خوشه تبدیل به یک نود معمولی شده و یک نود معمولی در خوشه مبدل به نود اصلی خوشه می گردد .



Energy-Round Graph for Dynamic Cluster Head
with its Half Remaining Energy Threshold

در شکل فوق ، گراف انرژی – دور یک خوشه نشان داده شده است که مقدار آستانهٔ نود اصلی خوشه مقداری معادل نصف انرژی باقیمانده است . به بیان دیگر ، می توان گفت نود اصلی خوشه تغییر نمی کند تا زمانی که انرژی باقیمانده اش به نصف انرژی اولیه اش تقلیل یابد . مشاهده می شود که نودهای خوشه پس از یک مقدار مساوی دور ، همگی می میرند . نودهای اصلی خوشه CH اول و دوم و سوم و چهارم و پنجم به ترتیب پس از ۳۷۴۰۰ ، ۳۸۰۰۰ ، ۳۸۵۰۰ ، ۳۸۶۰۰ و ۳۸۷۰۰ دور می میرند . در نتیجه ، پوشش شبکه سیستم نود اصلی خوشه پویا و کارائی راندمان آن خیلی بهتر از سیستم مبتنی بر نود اصلی خوشه ثابت است .

رمز نگاری چند لایه ای برای کنترل دسترسی چند سطحی در شبکه های حسگر بی سیم

هدف از رمز نگاری چند سطحی (MLE) یا Multi-layer Encryption این است که تنها یک متن رمز شده داشته باشیم . اما کاربرانی با کلیدهای مختلف بتوانند پس از اینکه با کلیدهای خودشان متن را رمز گشایی کردند ، به سطوح مختلفی از داده ها دسترسی داشته باشند . این برای کاربردهای نظارتی مفید است که نیاز به یک مکانیزم کارامد دارد برای دسترسی چند سطحی یا چند لایه ای به داده ها . در این طرح ،کاربران تنها نیاز به ذخیرهٔ یک تعداد ثابت از کلیدها دارند ، صرف نظر از لایه های محرمانهٔ تعریف شده ، کاربران سطح بالا نسبت به کاربران سطح پایین می توانند داده های بیشتری را رمزگشایی نمایند . (مثلاً در کاربردهای نظارت کلان شهرها ، پلیس می تواند کلیه داده ها را ببیند اما شهروندان معمولی فقط می توانند بخشی از داده ها را ببینند) . در این معماری ، یک سرور برای ذخیرهٔ داده های رمزنگاری شده از نودهای حسگر پیش بینی شده است و این سرور داده ، کاربران را در زمان درخواست برای خواندن داده های خاص ، تصدیق می کند .

به دلیل وجود برخی محدودیت ها در نودهای حسگر ، یک راه حل محبوب داشتن یک سرور است به عنوان یک کنترلر مکمل . در این معماری ، سرور داده ، داده های حس شده از نودهای حسگر را ذخیره می کند ، بصورت متناوب سیگنالهای راهنما را برای حفظ توپولوژی مسیریابی ، پخش همگانی می کند و وظایف چرخشی هر نود را زمان بندی می کند . این سیگنال های راهنمای پخش همگانی شدهٔ متناوب برای این طرح MLE مورد استفاده قرار می گیرد .

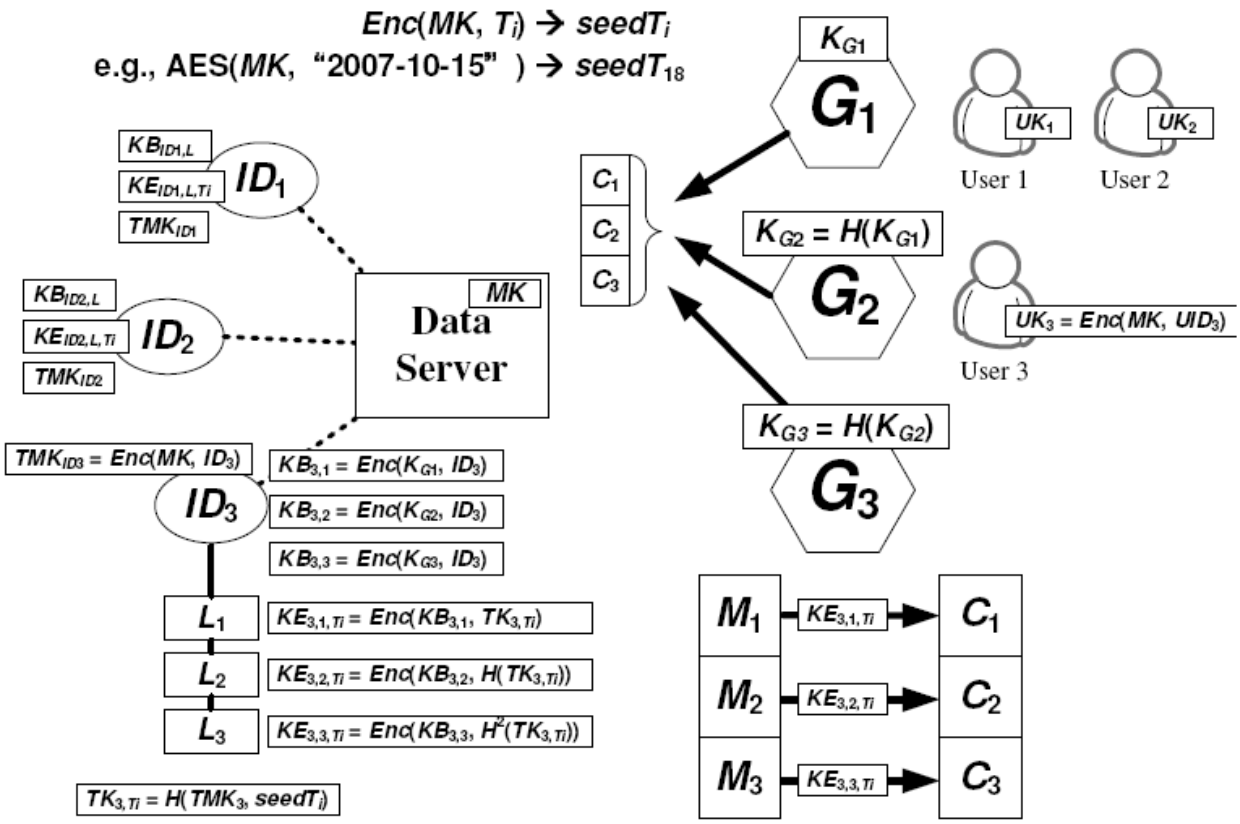
MK	Master Key
M_i	Plaintext of layered message i
C_i	Cipher text of corresponding M_i
ID_i	The identity of sensor node i
UID_i	The identity of user i
UK_i	User key for user i
K_{G_i}	Group Key (ex. K_{G_1} for Group G_1)
$Enc(K,M)$	Encrypt message M using key K
$\{M\}_K$	Encrypted message M by K

$H^n(M)$	Hash n times of message M
$H(M_1,M_2)$	Hash of M_1 concatenates M_2
KB_{ID_i,L_n}	Base key for layer n of node ID_i
KE_{ID_i,L_n,T_j}	Encryption key for layer n of node ID_i, during time period T_j
T_i	The ith Time period
TMK_{ID_i}	Time Master Key for node ID_i
TK_{ID_i,T_j}	Time Key for node ID_i, during time period T_j

جدول تعریف علائم

طرح رمز نگاری چند سطحی

بطور غیر رسمی ، اختفا و پنهان کاری پیشرو تضمین می کند که پیام های ارسالی محافظت می شوند حتی اگر کلید محرمانه فعلی در معرض حمله و تهاجم قرار گیرد و همچنین اختفای پسرو بدین معناست که کلید محرمانه مورد تهاجم واقع شده در آینده قابل استفاده نمی باشد .



MLE scheme

همانگونه که در شکل فوق نشان داده شده است ،این طرح نیاز به یک سرور دارد برای نگه داری کلید اصلی (MK) سرور دارد . بصورت تصادفی کلید KG_1،KG_1 تولید می کند و KG_2و KG_3،KG_3 با استفاده از توابع Hash یک طرفه محاسبه می کند و سپس این کلید ها را به ترتیب به کاربران G_1 و G_2و G_3 میدهد .

سرور داده بصورت متناوب $SeedT_i$ را به نودهای حسگر بیسیم پخش همگانی می کند ، مقدار $SeedT_i$می تواند یک مقدار محاسباتی باشد از زمان تناوب T_i. به عنوان مثال در شکل فوق ، "2007-10-15" می تواند دوره۱۸ ام سیستم باشد . بنا براین :

$$SeedT_{18} = AES(MK, \text{“2007-10-15”})$$

بطور اساسی ، $Seed\ T_i$ برای بروز رسانی کلیدهای رمزنگاری مورد استفاده قرار می گیرند ، از زمانی که این مقادیر $Seed\ T_i$ها در متن ساده پخش همگانی می شوند . یک مهاجم می تواند همه مقادیر را ثبت کرده و سیستم را به مخاطره اندازد .

برای اجتناب از این مشکل ، سرور به هر نود حسگر یک زمان واحد کلید اصلی ($TMK_{ID\ i}$) اختصاص می دهد از تابع

$$TMK_{ID\,I} = Enc\,(MK\ ,\ ID_i)$$

$TMK_{ID\,i}$برای تولید کلیدهای زمان استفاده می شوند ($TK_{ID\,I}$,T_j) و کلیدهای زمان به منظور به روز رسانی کلیدهای رمزنگاری برای هر کدام از لایه های محرمانه از طریق تابع Hash بکار می رود :

$$KE_{ID\,I\,,Ln,\ T\,j} = H\,(\,KB_{ID\,I\,,\,Ln}\ ,H^{Ln-1}\,(TK_{ID\,i\,,\,T\,j}))$$

دلیل انجام Hashیکطرفه بر روی کلیدهای زمان این است که هر لایهٔ محرمانه در اینجا از حملات توطئه گونه در امان بماند .

سرور به هر نود حسگر یک کلید مختلف ارائه می کند ، که در اینجا ما به عنوان کلید پایه ($KB_{ID\,I\,,\,Ln}$) از آن نام می بریم . که در اینجا ID $_i$یعنی این کلید مربوط به نود ID است و Ln مربوط به سطح محرمانهٔ کلید می باشد . ترکیب کردن مقادیر کلید پایه و کلید$TK_{ID\,i\,,\,Tj}$ می تواند کلید رمزنگاری ($KE_{\ ID\,I\,,Ln\,,\ \ T\,j}$) را تولید کند . که این روش تخت عنوان روش های عایق بندی کلید مطرح می شوند که برای تامین محرمانگی پیشرو / پسرو استفاده می گردد .

در این طرح ما به هر کاربر یک کلید کاربر (UK_i) با تابع مولد $UK_i = Enc\ (MK\ ,\ UID_i)$ اختصاص می دهیم . این کلیدهای کاربر می توانند مورد استفاده قرار بگیرند برای احراز هویت و رمزنگاری کلید زمان ($TK_{ID\,,\,Ti}$) قبل از ارسال به کاربران .

یک مثال ارائه می دهیم که در آن User 1 دادهٔ "200-10-15" را از نود ID $_3$ درخواست می کند ، روند جریان بصورت زیر است :

۱- User 1 از ID $_3$ در یک بازهٔ زمانی درخواست دادهٔ "2007-10-15"را دارد .

۲- سرور User 1 را توسط UK_1 احراز هویت می کند .

۳- سرور مقدار$Seed\ T_{18}\ =Enc\ (MK\ ,\ "2007\text{-}10\text{-}15")$را محاسبه می کند .

۴- سرور مقدار $TMK_3=(Enc\ (MK\ ,\ ID_3)$ را محاسبه می کند .

۵- سرور مقدار $TK_{3,18} = (TMK_3\ ,\ Seed\ T_{18})H$را محاسبه می کند .

۶- سرور مقدار $Enc\ (UK_1\ ,\ TK_{3,18}) = \{TK_{3,18}\}UK_1$ را برای User 1 می فرستد .

۷- User 1 مقدار $\{TK_{3,18}\}UK_1$ را رمز گشایی کرده و مقدار $TK_{3\ ,\ 18}$ را به دست می آورد .

۸- User 1 ،K_{G1}را دارد و حالا او $TK_{3,18}$ را دارد .

(a) User 1 ، K_{G1}را دارد و ID_3 را می شناسد (اطلاعات عمومی) بنابراین می تواند با محاسبهٔ مقدار $Enc\ (K_{G1}\ ,\ ID_3) = KB_{3,1}$ کلید پایهٔ $KB_{3,1}$را بدست آورد .

(b) User 1 مقدار$TK_{3,18}$ را می داند ، بنابراین می تواند با محاسبهٔ $KE_{3,1,18}=Enc\ (KB_{3\ ,\ 1}\ ,\ TK_{3,18})$ مقدار کلید رمز نگاری $KE_{3,1,18}$ را بدست آورد .

(c) سپس User 1 کلید رمزنگاری $KE_{3,1,18}$ را دارد و می تواند با رمزگشایی C_1به M_1 برسد .

(d) چون User 1 ، K_{G1}را دارد ، می تواند مقادیر K_{G2}و K_{G3} را توسط توابع یک طرفه Hash بدست آورد ، سپس می تواند مقادیر پایه کلید $KB_{3,2}$ و $KB_{3,3}$ را با محاسبهٔ $KB_{3,2}=Enc\ (K_2\ ,\ ID_3\ )$, $Enc\ (K_{G2}\ ,\ ID_3) = KB_{3,3}$بدست آورد .

(e) User 1 می تواند کلید رمزنگاری $KE_{3,2,18}$ و $KE_{3,3,18}$را برای رمزگشایی C_2 و C_3بکار ببرد ، بطوریکه :

$$KB_{3,2,18} = Enc(KB_{3,2}\ ,\ H(TK_{3,18}))$$

,

$$KB_{3,3,18} = Enc(KB_{3,3},\ H^2(TK_{3,18}))$$

۹- User 3 در گروه G_2فقط K_{G2}را دارد و می تواند KG_3را بدست آورد . اگر User 1 کلید زمانی را از سرور درخواست کند ، بعد از احراز هویت با استفاده از UK_3، سرور در می یابد که در گروه G_2قرار دارد و به جای مقدار $TK_{3,18}$ به آن مقدار $H(TK_{3,18})$ را می دهد . این می تواند از حملهٔ توطئه و تبانی جلوگیری کند حتی اگر User 3 بتواند KG_1را از کاربر G_1بدست آورد، او همچنان نمی تواند مقدار $TK_{3,18}$را بدست آورد ، پس User 3 می تواند حداکثر M_2 و M_3 را بدست آورد .

۴ - بحث

حملات زیادی در زمینهٔ شبکه های حسگر شناسایی شده اند ، شامل حملهٔ از سرویس خارج کردن (Denial Of Service) سیاه چال ، سوراخ کرم ، سیبل ، تحلیل ترافیک ، همتا سازی گره و حملات مشابه دیگر به عنوان یک راه حل تکمیلی ، تمرکز خود را بر روی امنیت طرح MLE قرار داده ایم . برخی از حملات وجود دارند که طرح را تحدید می کند و ما در این زمینه ها امنیت را ارزیابی می کنیم .

- **اسراق سمع :** در طرح پیشنهادی ما ، تنها دادهٔ متن ساده ای که یک مهاجم می تواند بدست آورد مقدار Seed T_i است ، اما بدون کلید اصلی زمان $TKM_{ID\ i}$ ، مقدار Seed T_iغیر قابل استفاده است زیرا این تنها یک مقدار است برای تولید کلید زمان$TK_{ID\ ,\ Tj}$

- **حملهٔ تبانی :**اگر یک کاربر در یک سطح پائین تر از بهره برداری با یک کاربر در سطوح بالاتر بهره وری تبانی می کند ، (مثلاً User 1 به User 3 تبانی کند) او می تواند به کلید گروهی سطح بالاتر دسترسی داشته باشد ، بعد از اینکه احراز هویت شد، سرور داده فقط کلید زمانی مرتبط با سطح بهره وری را به او می دهد . بدون کلید زمانی سطح بالاتر ، کاربر نمی تواند کلید رمزنگاری مشخصی را برای دست یافتن به داده ها بدست آورد .
- **نودها حسگر سازگار :** در این طرح ، به هر نود حسگر یک سری از کلید های مشخص و متمایز داده شده است و این کلیدها تنها نتایج محاسباتی هستند . حتی اگر یک نود حسگر مشخص مصالحه کند ، مهاجم فقط می تواند به این مقادیر محاسباتی پی ببرد و نمی تواند با نودهای دیگر مصالحه کند . بنابراین ، صدمه فقط محدود به نودهای سازشکار می شود .

امنیت شبکه متحرک بیسیم WiMAX

استاندارد 802.16 استانداردی است که بر روی شبکه های حمل کننده قرار می گیرد تا سطوح مناسبی از امنیت را با هزینهٔ معقول و مناسب برای شبکه فراهم آورد . برای یک شبکه پیشرفته استاندار بیسیم مانند WiMAX توجه کردن به مباحث امنیتی و مشخص نبودن راه حل های قابل اعتماد و موثق ، به عنوان یکی از اهداف مهم مدنظر قرار می گیرد . آموزه های فرا گرفته شده از ضعف ها و عیوب در امنیت Wi – Fi همگی در استاندارد IEEE 802.16 گردآوری شده اند .

این قسمت ، با معرفی ملزومات و مباحث اصلی امنیت شبکه های بیسیم آغاز می شود . سپس توابع و مباحث معرفی شده در استاندارد IEEE 802.16 e – 2005 برای واسط هوایی WiMAX ارائه می گردد .

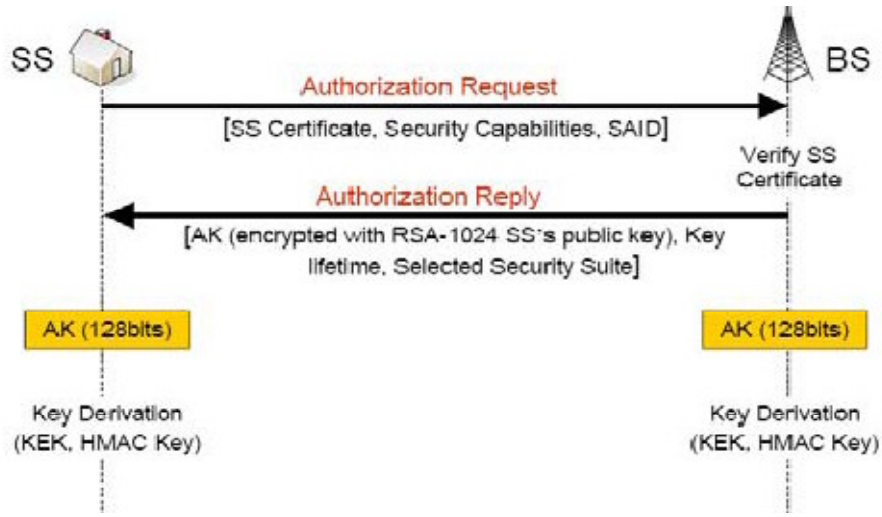
WiMAXشبکه های مبتنی بر IP است و چه بصورت بیسیم باشد یا نه ، موضوع آسیب پذیری هر شبکهٔ IPاست . حملهٔ از سرویس خارج کردن (Denial Of Service) به وسیلهٔ یک حکر بد نیت می تواند هر شبکه های را فلج کند و احتیاط هایی همچون حفاظت از عدم ورود نفوذگران می بایست صورت پذیرد . در اینجا فرض بر این است که همهٔ نیازها توسط ISP کنترل می شود . فرایند امنیت IEEE 802.16 در ۳ مرحله صورت می گیرد :

۱- اعتبار سنجی (شکل ۱)

۲- مبادلهٔ کلید (شکل ۲) ترابری کلید رمزنگاری (TEK) برای مبادلهٔ کلید مورد استفاده قرار می گیرد . TEKبصورت تصادفی توسط BS انجام می شود و رمزنگاری آن با 3DES با کلید ۱۲۸ بیتی ، RSA با استفاده از کلید عمومی SS و AES با استفاده از ۱۲۸

بیتی انجام می شود .پیام تصدیق کلید توسط HMAC – SHA1 مبادله می گردد . این تامین کنندۀ جامعیت پیام و تائید کلید احراز است .

۳- رمزنگاری داده (شکل ۲) فقط پیام های داده رمز نگاری شده از DES در حالت CBC استفاده می کنند . هیچ پیامی از شناسائی جامعیت و محافظت وجود ندارد . با استفاده از AES ، حفاظت از پخش تامین می شود با استفاده از شمارۀ بسته ها .



(۱)احراز هویت

امنیت WiMAX به عنوان یک زیر لایۀ محرمانه در پائین لایه پروتکل MAC اجرا شده است . (شکل ۳)

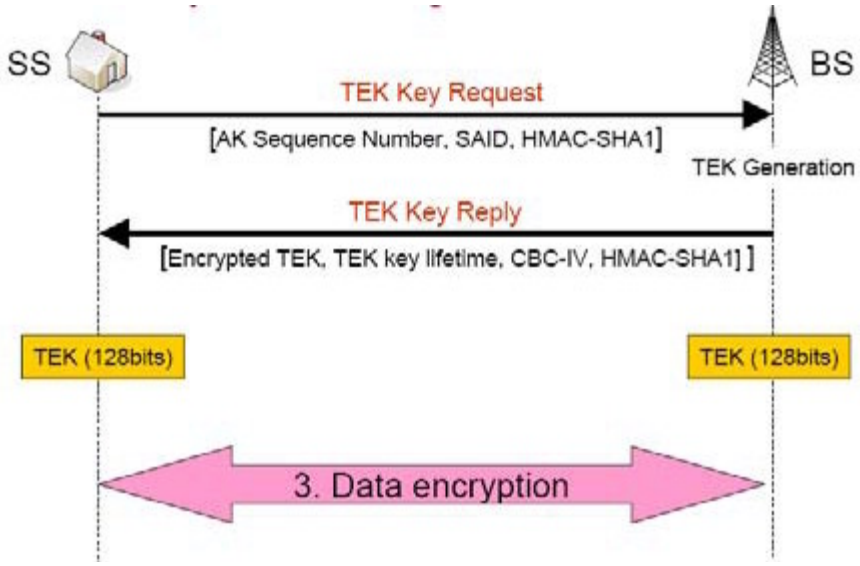
هدف تامین کنترل دسترسی و محرمانگی است :

- پروتکل کپسوله سازی برای رمزنگاری بسته های داده پیرامون شبکه های بی سیم .

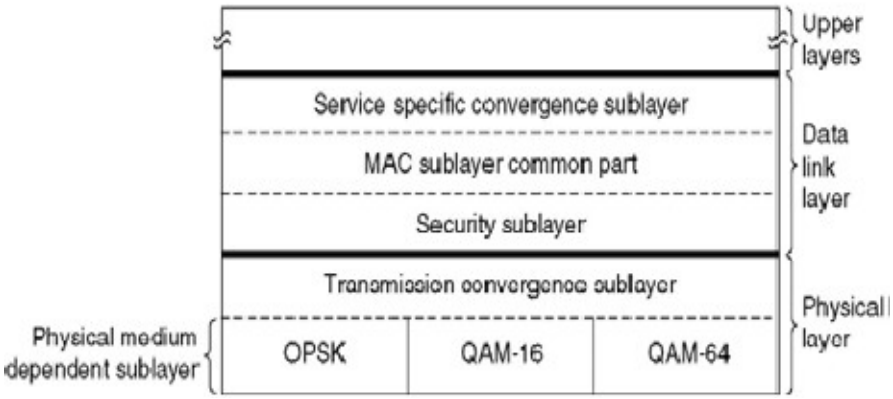
•تعریف به کار گماردن مجموعه های نهفته و پنهانی ، داده های رمزنگاری و الگوریتم های احراز هویت و قواعد درخواست آن الگوربتم ها برای محموله های MAC PDU .

▪ به مشترکان در شبکه های بی سیم یک محرمانگی می دهد .

- کپسوله سازی همیشه در محموله های MAC PDU درخواست شده است .



تبادل کلید و رمزنگاری



معماری امنیت 802.16

نتیجه گیری :

امنیت برای بسیاری از شبکه های حسگر یک مسئلهٔ حیاتی است . بخاطر محدودیت امکانات نودهای حسگر، تأمین امنیت و حفظ حریم خصوصی برای یک شبکهٔ حسگر یک کار چالش بر انگیز است. در این مقاله، ما حملات کاربردی را بر روی شبکه های حسگر بطور خلاصه بیان کردیم و مطالب متعدد مهمی را در مورد امنیت مورد بازبینی قرار دادیم برای شبکه های حسگر، شامل مدیریت کلید، همزمان سازی امن، کشف مکان امن، مسیریابی امن و سپس یک چهارچوب کاری برای یک سیاست موثر در امنیت شبکه های حسگر بیسیم و همچنین یک معماری مدیریت امنیت مبتنی بر سیاست برای شبکه های حسگر بیسیم ارائه شد . در ادامه پیرامون اجرای الگوریتم رمزنگاری RSA برای شبکه های حسگر بیسیم و همچنین رمزنگاری چندلایه ای برای کنترل دسترسی چندسطحی در شبکه های حسگر بیسیم مباحثی را مطرح کردیم و خلاصه ای از امنیت شبکه متحرک بیسیم WiMAX را مورد بازبینی قرار دادیم . بسیاری از مطالب امنیتی در شبکه های حسگر بی سیم بصورت باز باقی مانده اند که امید است فعالیت های تحقیقاتی بیشتری را از این مطالب در آینده شاهد باشیم و به امنیت نسبی مستحکم تری دست یابیم .

منابع :

[1] AXiaojiang Du , North Dakota State University , B Haiao – HWA Chen , National C heng Kung University , "SECURITY IN WIRELESS SENSOR NETWORKS "1536-1284/08/$25.00 © 2008 IEEE IEEE Wireless Communications • August 2008

[2] A Hasan Tahir , B Syed Asim Ali Shah "Wireless Sensor Networks – A Security Perspective " 978-1-4244-2824-3/08/$25.00 ©2008 IEEE

[3] A Daniel E. Burgner , B Luay A. Wahsheh , "Security of Wireless Sensor Networks "978-0-7695-4367-3/11 $26.00 © 2011 IEEE DOI 10.1109/ITNG.2011.62

[4] A Venkatesh Kannan , B Sahena Ahmed , "A Resource Perspective To Wireless Sensor Network Security "978-0-7695-4372-7/11 $26.00 © 2011 IEEE DOI 10.1109/IMIS.2011.96

[5] A Hero Modares B Rosli Salleh C Amirhossein Moravejosharieh , "Overview of Security Issues in Wireless Sensor Networks "978-0-7695-4562-2/11 $26.00 © 2011 IEEE

[6] Po-Yuan Teng, Shih-I Huang, and Adrian Perrig , "Multi-Layer Encryption for Multi-Level Access Control in Wireless Sensor Networks" - 2008, in IFIP International Federation for Information Processing

[7] Sérgio de Oliveira1,2, Thiago Rodrigues de Oliveira2, José Marcos Nogueira2 – "A Policy based Security Management Architecture for Sensor Networks" - 978-1-4244-3487-9/09/$25.00 c_ 2009 IEEE

[8]Michael E. Manley, Cheri **A.** McEntee, Anthony M. Molet, and Joon **S. Park,** ***Member, "***Wireless Security Policy Developmentfor Sensitive Organizations "- *0-7803-9290-61051$20.00 02005* IEEE

[9]Neeli Rashmi Prasad – "State of the Art of the wireless security in OFDM(A)-based Systems" - 978-0-7695-3719-1/09 $25.00 © 2009 IEEE

DOI 10.1109/MWS.2009.48

[10]Avijit Sahanaa ,Iti Saha Misra – "Implementation of RSA Security Protocol for Sensor Network Security: Design and Network Lifetime Analysis" _978-1-4577-0787-2/11/$26.00 ©2011 IEEE