پردیس بین الملل

پایان نامه کارشناسی ارشد

پروتکل های مدیریت کلید در شبکه های حسگر بی سیم ناهمگن

از

طه یاسین رضاپور

اساتید راهنما:

دکتر رضا ابراهیمی آتانی

و

دکتر محمود سلماسی زاده

شهریور ۱۳۹۲


بسم الله الرحمن الرحیم

دانشکده پردیس بین الملل

گروه مهندسی فناوری اطلاعات

گرایش تجارت الکترونیکی

پروتکل های مدیریت کلید در شبکه های حسگر بی سیم ناهمگن

از

طه یاسین رضاپور

اساتید راهنما:

دکتر رضا ابراهیمی آتانی

و

دکتر محمود سلماسی زاده

شهریور ۱۳۹۲

تقدیم به:

پدر و مادر عزیز

همسر مهربان

و

دختر دلبندم

تشکر و قدردانی:

با شکر گذاری از درگاه حق تعالی بر خود لازم می دانم از استاد ارجمند و عزیزم جناب دکتر ابراهیمی که همانند چراغی روشن و پر نور مرا به کوتاه ترین مسیر برای رسیدن به موفقیت رهنمون شدند و همچنین استاد بزرگوارم جناب دکتر سلماسی زاده که جایگاه واقعی علم را به من نشان دادند نهایت قدردانی و تشکر را داشته باشم.

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

چکیده

پروتکل های مدیریت کلید در شبکه های حسگر بی سیم ناهمگن

طه یاسین رضاپور

شبکه های حسگر بی سیم مجموعه ای متشکل از تعداد زیادی گره حسگر با قابلیت ثبت اطلاعاتی مانند دما، رطوبت، فشار، نور و صوت از محیط می باشند؛ به صورتیکه گره های حسگر با تبادل اطلاعات گرد آوری شده با یکدیگر، دیدی کامل از محیط تحت نظارت شبکه فراهم می نمایند. شبکه های حسگر به دلایلی ازجمله کانال ارتباطی نا امن و ارتباطات بی سیم با چالش های امنیتی فراوانی روبرو هستند؛ چگونگی مدیریت کلیدهای رمزنگاری در بین گره های حسگر مستقر در شبکه به منظور ایجاد امنیت حداکثری با حداقل هزینه به عنوان یک رویکرد اساسی در ایجاد امنیت در این دسته از شبکه ها همواره مورد توجه محققان بوده است.

با توجه به محدودیت های موجود در شبکه های حسگر، بکارگیری روش های مدیریت کلید در آن با چالش هایی همراه می باشد. اکثر پژوهش های انجام شده در زمینه مدیریت کلید در شبکه های حسگر، شامل طرح هایی می گردد که برای شبکه هایی با ساختار همگن ارائه شده اند. ضعف های موجود در شبکه های حسگر همگن از نظر مقیاس پذیری و کارایی منجر به این شد که محققان ساختاری ناهمگن را برای این دسته از شبکه ها در نظر بگیرند. اخیراً نیز تعدادی طرح مدیریت کلید برای شبکه های حسگر ناهمگن ارائه شده است.

در این پایان نامه، پس از بررسی پروتکل ها و طرح های مدیریت کلید در شبکه های حسگر ناهمگن و دسته بندی آنها یک طرح نوین مدیریت کلید ارائه شده است. در طرح ارائه شده، رمزنگاری مبتنی بر موقعیت مکانی به منظور استفاده در احراز اصالت و تخصیص کلید به اجزاء شبکه بکار گرفته شده است. در این طرح با در نظر گرفتن یک سلسله مراتب برای اجزاء شبکه، روشی برای ارتباطات امن آنها ارائه گردیده است. مقیاس پذیری شبکه و کاهش فضای مورد نیاز برای ذخیره سازی خصوصیت بارز طرح ارائه شده می باشد.

واژه‌های کلیدی: شبکه های حسگر بی سیم، رمز نگاری مبتنی بر موقعیت مکانی، مدیریت کلید، گره حسگر، امنیت.

Abstract

Key Management Protocols in Heterogeneous Wireless Sensor Networks

Taha Yasin Rezapour

Wireless sensor networks are a collection of numerous sensor nodes with the ability to record information such as temperature, humidity, pressure, light, and sound from environment; so that sensor nodes provides full view of networks environmental monitoring by the gathered information exchange with other nodes. Sensor networks face a lot of security challenges for reasons such as insecure communication channel and wireless communications. Management of the cryptographic keys between sensor nodes for providing the maximum security with minimum cost is a research direction which has attracted scientist in the field of computer science.

Due to limitations in sensor nodes, using key management techniques have faced a lot of security and implementation challenges. Most research conducted in the area of key management in sensor networks include schemes which have been proposed for networks with homogeneous structure. Because of some limitations such as performance and scalability of homogeneous sensor networks, researchers started considering these networks with heterogeneous structure. Recently a number of key management schemes for heterogeneous sensor networks were presented.

In this thesis, a novel key management scheme for heterogeneous wireless sensor networks is presented. In proposed Scheme, position based cryptography is applied for key assignment and authentication for network components. In this scheme, taking into account a hierarchical network design, a method for secure communication is established. In the proposed scheme, the network scalability and reduced storage space requirements is a special feature.

Keywords: Wireless sensor networks, Position based cryptography, Key management, Sensor node, Security.

فصل ۱:

مقدمه

۱-۱- مقدمه

شبکه های حسگر بی سیم[1] یکی از شاخص ترین فناوری های روز ارائه شده در عرصه فناوری اطلاعات و ارتباطات می باشد که دریچه ای نوین را به روی زندگی بشر و ارتباط او با محیط پیرامون گشوده است. این شبکه ها که به اختصار با WSN نشان داده می شوند، زیر ساختی برای دریافت پارامترهای محیطی، انجام محاسبه و ارسال اطلاعات می باشند.

WSN ها از تعداد زیادی گره حسگر[2] با سخت افزار محدود جهت مشاهده و ثبت پدیده ها و حتی عکس العمل نسبت به آنها تشکیل شده اند. حسگرهایی که در محیط پخش شده اند با کمک یکدیگر می توانند شرایطی مانند دما، فشار، صوت، لرزش، حرکت و آلودگی را اندازه گیری نمایند. حسگرهای بکار گرفته شده در WSN ها اطلاعات دریافتی از محیط پیرامون را با یکدیگر تبادل می نمایند تا دیدی کلی از محیط تحت نظارت خود بسازند، این اطلاعات برای کاربران خارج از شبکه به وسیله دروازه های ارتباطی قابل دسترس می باشد. این حسگرها در واقع حاصل به هم آمیختن آخرین پیشرفت ها در حوزه های الکترومکانیک، ارتباطات بی سیم و الکترونیک دیجیتال می باشند که با داشتن مشخصه هایی از جمله توان مصرفی و هزینه کم، اندازه کوچک و برد رادیویی محدود امکان نظارت در محیط هایی که حضور دائمی در آنها سخت و یا غیر ممکن است را فراهم می نمایند[۲].

با استفاده از شبکه های حسگر بی سیم تمامی حوادث غیر مترقبه می توانند قابل پیش بینی گردند. WSN ها در موقعیت های متنوع جغرافیایی، سامانه های زیست سنجی و به ویژه میادین جنگ گسترده می شوند. از کاربردهای شبکه های حسگر می توان به کاربردهای تجاری، تشخیص بازماندگان بعد از حوادثی مانند زلزله و حتی اعلام وضعیت لحظه به لحظه میدان نبرد اشاره نمود. از آنجایی که استفاده از کامپیوترها و پروتکل های مخابراتی معمولی و استاندارد شده برای انجام چنین کاری بسیار پرهزینه است، از WSN ها با هزینه کم در این عرصه ها استفاده می شود. استفاده فراگیر از شبکه های بی سیم، پیشرفت فناوری در حوزه الکترونیک از جمله طراحی آنتن،

[1] Wireless Sensor Networks

[2] sensor node

مدارات بی سیم و توانایی ساخت پردازنده های پر سرعت همراه با میزان حافظه قابل توجه از جمله عواملی است که سبب رشد روز افزون استفاده از WSN ها شده است.

بدیهی است که در شبکه های حسگر بی سیم مانند دیگر شبکه ها باید از الگوریتم ها و روش هایی جهت رسیدن به محرمانگی[1]، تمامیت[2] و احراز اصالت[3] بهره جست. اما نیل به اهداف امنیتی با توجه به محدودیت های همه جانبه در WSN کار ساده ای نیست. این شبکه ها با توجه به خصوصیاتی که دارند مانند سایر انواع شبکه ها همواره در معرض حملات مختلف از سوی مهاجمان به منظور نفوذ و مختل سازی سامانه می باشند. مهاجمین داده های کاربردی را دستکاری(شنود، تغییر، جاسازی و حذف) می نمایند. طبیعت ارتباطات بی سیم، ضعف زیرساخت و محیط غیر قابل کنترل، قابلیت های مهاجم را در شبکه های حسگر افزایش می دهد. ارتباطات بی سیم به مهاجم کمک می کند تا انواع حملات را اجرا نماید. بنابراین، امنیت عاملی بسیار مهم در نائل شدن به قابلیت های واقعی یک شبکه حسگر می باشد. از اینرو باید در طراحی آن همواره سازوکارهای امنیتی در نظر گرفته شود. علاوه بر این بر خلاف انواع دیگر شبکه ها که دسترسی فیزیکی به گره های شبکه توسط مهاجم در آنها به سادگی امکان پذیر نیست، گره های حسگر در WSN ها در معرض دسترسی مهاجمین قرار دارند که این موضوع توانایی مهاجمین را برای انجام حملات مختلفی مانند حملات کانال جانبی[4] و تسخیر گره[5] افزایش می دهد. بنابراین سامانه های مخابراتی با محدودیت منابع مانند شبکه های حسگر ناگزیر به استفاده از اولیه های رمزنگاری سبک می باشند. اما در یک شبکه پیچیده تنها لحاظ نمودن این نکته کافی نیست. اولیه های رمزنگاری نیازمند کلیدهای امن منحصر بفرد در داخل هر گره می باشند که سامانه های مدیریت کلید وظیفه تولید، توزیع، نگهداری، بروز رسانی امن و انهدام این کلیدها را بر عهده دارند. علاوه بر این، طرح های مدیریت کلید در بسیاری از موارد وظیفه احراز اصالت دوطرفه را نیز بر دوش می کشند. لذا موضوع مدیریت کلید به عنوان پیش نیاز تحقق امنیت در شبکه های حسگر بی سیم مطرح می باشد.

[1] Confidentiality
[2] Integrity
[3] Authentication
[4] side channel attack
[5] node capture attack

۱-۲- طرح مسئله

از آنجاییکه طرح های سنتی رمزنگاری به شکلی مستقیم در شبکه های حسگر به کار گرفته نمی شود تدارک مدیریت کلید شامل تولید، توزیع و بروز رسانی و انهدام کلید به عنوان رویکردی پایه ای در ایجاد امنیت در کل شبکه موضوعی می باشد که اخیراً بسیار قابل توجه محققان بوده و طرح های متنوعی برای مدیریت کلیدهای رمز نگاری در این نوع از شبکه ها ارائه شده است. در صورتیکه به تمامی گره های شبکه تنها یک کلید مشترک اختصاص دهیم، به پایین ترین سطح امنیت نائل شده ایم زیرا با کشف رمز تنها یک گره امنیت کل شبکه حسگر از بین خواهد رفت. از سوی دیگر اگر به هر گره یک کلید منحصر بفرد اختصاص دهیم به بالاترین سطح امنیت نائل شده ایم، چرا که با کشف رمز هر گره تنها امنیت همان گره زیر سئوال می رود. اما سربار مخابراتی، و حافظه مورد نیاز این مکانیزم به هیچ وجه برای شبکه های حسگر قابل قبول نیست. لذا تا بحال زیر ساخت های متنوعی جهت نیل به امنیت حداکثری با سربار حداقلی طراحی شده است. این چارچوب های امنیتی به عنوان پیش نیاز نیل به محرمانگی، تمامیت و احراز اصالت مفروض است. از سوی دیگر شبکه های حسگر بی سیم به دو دسته اصلی همگن و ناهمگن تقسیم می شوند. اکثر طرح هایی که تا کنون برای مدیریت کلید در شبکه های حسگر ارائه شده اند برای WSN هایی با ساختار همگن می باشند. اما وجود محدودیت هایی مانند کارایی و مقیاس پذیری در شبکه های حسگر همگن محققان را بر آن داشت که این شبکه ها را با ساختاری ناهمگن در نظر بگیرند. باتوجه به تغییر نسبی رویکرد ساختار شبکه های حسگر از حالت توزیع شده به سلسله مراتبی و ناهمگن در عمل، ارتقاء عملکرد الگوریتم های موجود از نظر امنیت، کارآیی و مقایسه نظری طرح ها از مباحث مهم به نظر می رسد.

۱-۳- روش تحقیق

در سال های اخیر تعدادی طرح مدیریت کلید برای شبکه های حسگر ناهمگن علی الخصوص از نوع سلسله مراتبی ارائه شده است. تفاوت موجود میان اجزای شبکه بالاترین انگیزه برای طراحی این خانواده از مدل های ترکیبی است چرا که در مجموع بار محاسباتی و مصرف انرژی کل شبکه

را کاهش می دهند. تقسیم بندی گره ها، در تعدادی خوشه و کنترل هر خوشه توسط یک سر خوشه در شبکه های سلسله مراتبی ناهمگن نه تنها سربار مخابراتی و توان مصرفی را کاهش می دهد بلکه مقیاس پذیری، انعطاف پذیری و کارآیی در این شبکه ها را افزایش می دهد. لذا در این پایان نامه با در نظر گرفتن این مساله مهم طرحی نوین برای مدیریت کلید در شبکه های حسگر بی سیم با ساختاری ناهمگن ارائه شده است که اساس آن بر پایه موقعیت مکانی گره های حسگر می باشد. در واقع در این طرح با ارائه مدلی برای شبکه و با استفاده از موقعیت مکانی گره های حسگر به عنوان جزئی از هویت آنها در احراز اصالت گره های شبکه، طرحی جدید در مدیریت کلید ارائه شده است.

مراحل تحقیق در انجام این پایان نامه در قالب محورهای پژوهشی زیر قابل بحث و ارائه است:

۱. بررسی شبکه های حسگر بی سیم، کاربردها و ساختار آن.
۲. بررسی مسئله امنیت در این دسته از شبکه ها و نیازمندی های امنیتی موجود در آن.
۳. بررسی حملات مختلف روی این شبکه ها و راه کارهای جلوگیری از آنها.
۴. بررسی زیرساخت مدیریت کلید در شبکه های حسگر بی سیم.
۵. بررسی تکنیک رمز نگاری مبتنی بر موقعیت مکانی به منظور استفاده از آن برای ارائه یک راه کار نوین مدیریت کلید.
۶. بررسی طرح ها و پروتکل های مدیریت کلید در شبکه های حسگر ناهمگن.
۷. ارائه یک طرح نوین مدیریت با استفاده از تکنیک رمز نگاری مبتنی بر موقعیت مکانی.
۸. تحلیل و ارزیابی طرح پیشنهادی و مقایسه آن با طرح های پیشین.
۹. نتیجه گیری، شامل ارائه نتایج و همچنین طرح محورهای پژوهشی آینده در این راستا.

۱-٤- اهداف

اهدف اصلی این پایان نامه، بررسی طرح های مدیریت کلید ارائه شده در شبکه های حسگر ناهمگن، طبقه بندی و مقایسه آنها به منظور دستیابی به دیدی کامل از این روش ها، بررسی تکنیک رمزنگاری مبتنی بر موقعیت مکانی به عنوان رویکردی قابل توجه در ایجاد امنیت و ارائه

یک روش کاملاً نوین مدیریت کلید برای شبکه های حسگر ناهمگن می باشد.

۱-۵- ساختار کلی پایان نامه

این پایان نامه شامل پنج فصل می باشد که فصل های بعدی آن به شکل زیر سازماندهی شده است:

فصل ۲ : در این فصل، پیرامون معرفی شبکه های حسگر، کاربردها، ساختار، اجزاء سخت افزاری و نرم افزاری، مقوله امنیت در این شبکه ها، چالش ها و طرح های امنیتی، مدیریت کلید در شبکه های حسگر، تکنیک رمزنگاری مبتنی بر موقعیت مکانی، توابع درهم ساز، HMAC و به طور کلی مفاهیم پیش زمینه بحث شده است.

فصل ۳: در این فصل، بعد از بیان اولین روش مدیریت کلید در شبکه های حسگر در بخش مقدمه که مختص شبکه های همگن است طرح های مدیریت کلید ارائه شده برای شبکه های حسگر ناهمگن بررسی شده است.

فصل ۴: در این فصل، طرحی نوین برای مدیریت کلید در شبکه های حسگر ناهمگن ارائه شده است.

فصل ۵: در این فصل، جمع بندی پایان نامه و کارهای پیشنهادی برای پژوهش های آتی ارائه شده است.