
بسم الله الرحمن الرحيم

دانشکده پردیس بین الملل

گروه مهندسی فناوری اطلاعات

گرایش شبکه‌های کامپیوتری

ارزیابی و بهبود مقیاس‌پذیری پیش‌توزیع کلید در شبکه‌های حسگر بی‌سیم

از

ندا سولاری‌اصفهانی

استاد راهنما:

دکتر رضا ابراهیمی آتانی

دکتر سیدحمید حاج‌سیدجوادی

استاد مشاور:

مهندس اکبر مرشد اسکی

شهریور ماه ۱۳۹۲

تقدیم به:

پدر، مادر و همسر عزیزم

تشکر و قدردانی:

از استادان گرانقدر، جناب آقای دکتر ابراهیمی آتانی و جناب آقای دکترحاج سیدجوادی که در تمام مراحل انجام این پایان‌نامه راهنمای اینجانب بودند، و از جناب آقای مهندس اکبر مرشد اسکی مشاور محترم کمال قدردانی را دارم. چرا که آنان به تمام و کمال رسم استادی را هم در زمینه علمی و هم در کمالات انسانی به جای آوردند.

فهرست مطالب

فصل اول: مقدمه

فصل دوم: امنیت در شبکه‌های حسگر بی‌سیم

فصل سوم: طرح‌های ترکیبیاتی پیش‌توزیع کلید برای شبکه‌های حسگر بی‌سیم

فصل چهارم: طرح‌های ترکیبیاتی ترکیبی پیش‌توزیع کلید برای شبکه‌های حسگر بی‌سیم

فهرست جداول

فهرست اشکال

فهرست علائم اختصاری

BIBD	Balanced Incomplete Block Design
EG	Eschenauer, Gligor
PIKE	Peer Intermediaries for Key Establishment
TD	Transversal Design
μ-CID	μ-Common Intersection Design
RSA	Rivest, Shamir and Adleman
ECC	Elliptic Curve Cryptography

چکیده

ارزیابی و بهبود مقیاس‌پذیری پیش‌توزیع کلید در شبکه‌های حسگر بی‌سیم

ندا سولاری اصفهانی

شبکه حسگر بی‌سیم از تعدادی گره حسگر تشکیل شده است که از طریق امواج رادیویی با یکدیگر ارتباط برقرار می‌کنند. گره‌های حسگر توان محاسباتی، ارتباطی، ظرفیت حافظه و توان باتری محدودی دارند. این محدودیت‌ها پیاده‌سازی هر ایده‌ای را در شبکه حسگر بی‌سیم با چالش جدی مواجه می‌کنند. در بین نیازمندی‌های گوناگون شبکه حسگر بی‌سیم، برقراری امنیت یک نیاز اساسی است. یکی از راه‌کارهای برقراری امنیت، استفاده از رمزنگاری کلید عمومی است که نیازمند کلید عمومی و کلید خصوصی برای ارتباط امن است، که امنیت مناسبی را برای شبکه فراهم می‌کند اما این روش توان محاسباتی زیادی را با توجه به محدودیت حسگرها مصرف می‌کند.

پیش‌توزیع کلید یک راه‌کار مناسب است که در آن تعداد محدودی از کلیدها (حلقه کلید)، از یک مجموعه‌ی کلید (مخزن کلید) انتخاب می‌شوند و قبل از استقرار شبکه، به گره‌های حسگر نسبت داده می‌شود. اگر دو گره همسایه دارای کلید مشترک در حلقه کلیدهای خود باشند، ارتباط امن بین آنها برقرار می‌گردد، در غیر این صورت از یک کلید مسیر استفاده می‌کنند که در آن مسیر، هر دو گره همسایه کلید مشترک داشته و ارتباط امن برقرار می‌شود.

در این پایان‌نامه روش‌های متفاوت پیش‌توزیع کلید مورد مطالعه قرار می‌گیرد و استفاده از طرح‌های ترکیبیاتی در پیش‌توزیع کلید، به عنوان یک روش کارامد مورد توجه قرار گرفته و به منظور مقیاس‌پذیری از طرح‌های ترکیبیاتی ترکیبی استفاده می‌شود. در ادامه، طرح‌های ترکیبیاتی ترکیبی جدیدی معرفی شده، که در مقایسه با انواع مشابه، در برآورده ساختن شاخص‌های ارزیابی توزیع کلید، مانند اتصال‌پذیری، مقیاس‌پذیری و امنیت عملکرد قابل قبولی را ارائه می‌دهند.

واژه های کلیدی: شبکه‌های حسگر بی‌سیم، امنیت، پیش‌توزیع کلید، مقیاس‌پذیری، طرح‌های ترکیبیاتی ترکیبی

Abstract

Evaluation and improvement of scalable key pre-distribution for wireless sensor networks

Neda Solari Esfehani

Wireless sensor network is composed of a number of sensor nodes which can communicate with each other through radio wave. The sensor nodes are limited with computation ability, communication ability, and memory capacity and battery power. This makes the implementation of any task in Wireless Sensor Network is very challenging. Amid various requirements, secure communication in Wireless sensor Network is a major requirement. One of schemes security is public key cryptography, which requires public key and private key for secure communication. It provides good resiliency to the network. However, it consumes much computation which is a limitation for its application in wireless sensor network.

Key pre-distribution is an optimum scheme which loads a finite number of keys (key ring) to each node taking from a set of predefined keys (key pool) before deployment of the network. for secure communication either two nodes have a key in common in their key ring and they have a wireless link between them, or there is a path, called key-path, among these two nodes where each pair of neighboring nodes on this path have a key in common.

In this thesis, the variety of key pre-distributions are studied and using of the combinatorial design in the key pre-distribution is considered as one of the efficient methods, which is used to compare the hybrid combinatorial designs. Moreover, new hybrid combinatorial designs are introduced in this thesis, where they have suitable performance to construct the key pre-distribution assessment indicators such as connectivity, scalability and security with respect to other similar techniques.

Keywords: Wireless sensor networks (WSNs), Security, Key pre-distribution, Scalability, Hybrid combinatorial designs.

فصل اول

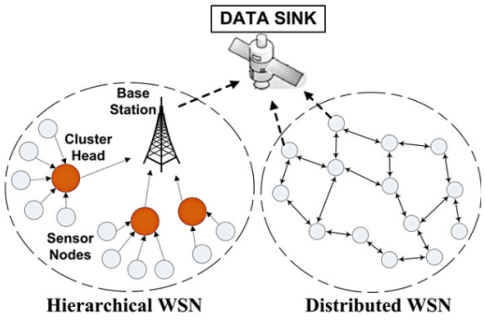
مقدمه

۱-۱ مقدمه

یک شبکه حسگر بی‌سیم[1]، از تعداد زیادی حسگر تشکیل شده است که به منظور گردآوری اطلاعات و انتقال آن‌ها، با یکدیگر ارتباط برقرار می‌کنند. پس به همین سبب از شبکه‌های حسگر بی‌سیم می‌توان برای نظارت بر محیط و ردیابی استفاده کرد. این شبکه‌ها در موارد گوناگون از جمله نظامی، پزشکی، محیطی، خانگی و حتی تولید کاربرد دارند.

برقراری ارتباط بین حسگرها در شبکه حسگر بی‌سیم، در اکثر کاربردها بویژه نظامی بایستی امن باشد. اما باید این را مد نظر قرار داد که حسگرها توان پردازشی، حافظه و توان مصرفی و همچنین پهنای باند محدودی دارند. به همین سبب در این شبکه‌ها از پروتکل‌های مسیریابی و امنیتی خاصی استفاده می‌گردد.

شبکه‌های حسگر بی‌سیم دارای دو معماری اصلی هستند: ۱- توزیع شده[2] یا همگن[3] ۲- سلسله مراتبی[4] یا ناهمگن[5]. در معماری توزیع شده، تمام حسگرها دارای سخت افزار مشابهی هستند و تمامی آن‌ها در اجرای پروتکل‌های داخلی، مانند مسیریابی همکاری دارند. اما در معماری سلسله مراتبی، شبکه به تعدادی خوشه[6] یا گروه تقسیم می‌شود که هر خوشه از تعدادی گره حسگر معمولی و یک سر خوشه[7] یا سر گروه تشکیل شده است. حسگرهای سر گروه در این نوع شبکه‌ها دارای سخت افزار کارآمدتری نسبت به حسگرهای معمولی هستند و قسمتی از مسئولیت‌های اضافی در شبکه، مانند جمع‌آوری اطلاعات از سایر گره‌ها و انتقال اطلاعات به چاهک[8] یا ایستگاه پایه[9] را بر عهده دارند. شکل ۱-۱ نحوه ارتباط در این دو معماری را نشان می‌دهد.



شکل ۱-۱ نحوه ارتباط حسگرها در دو معماری توزیع شده و سلسله مراتبی [۱]

[1] Wireless sensor network
[2] Distributed
[3] Homogeneous
[4] Hierarchical
[5] Heterogeneous
[6] Cluster
[7] Cluster head
[8] Sink
[9] Base station

طریقه قرار گرفتن گره‌ها با توجه به کاربرد آنها متفاوت است. در یک روش گره‌های حسگر به طور تصادفی در یک محدوده پخش می‌شوند و در روش دیگر، جایگاه همه گره های حسگر از قبل تعیین شده است.

۱-۲ تعریف مسئله

در این پایان‌نامه، تمرکز اصلی روی برقراری امنیت در شبکه حسگر بی‌سیم توزیع شده است که گره‌های حسگر در آن به طور تصادفی در یک محدوده گسترده شده و حسگرها غیر متحرک و خارج از دسترس هستند. این نوع شبکه‌ها در کاربردهایی مختلفی همچون نظامی مورد استفاده قرار می‌گیرند.

بسیاری از راهکارهی رمزنگاری، نیاز به کلیدهای محرمانه دارند. از آنجائیکه امکان دسترسی به حسگرها پس از پخش آن‌ها نیست بنابراین عمل توزیع کلید قبل از پخش آن‌ها انجام می‌گیرد، لذا به این روش پیش‌توزیع کلید گفته می‌شود. بسیاری از محققان، به دلیل سربار محاسباتی و ارتباطی زیاد رمزنگاری نامتقارن مانند RSA و ECC و... از رمزنگاری متقارن استفاده نموده‌اند [۲]. روش‌های رمزنگاری متقارن مورد استفاده در شبکه‌های حسگر بی‌سیم به سه دسته تقسیم می‌شوند. ۱- طرح‌های احتمالاتی ۲- طرح‌های قطعی ۳- طرح‌های ترکیبی. بسیاری از طرح‌های قطعی ارائه شده در پیش‌توزیع کلید در شبکه‌های حسگر بی‌سیم، از نوع طرح‌های ترکیبیاتی هستند. طرح‌های ترکیبیاتی به دلیل ایجاد یک الگوریتم مشخص، به منظور برقراری ارتباط امن بین حسگرها با استفاده از کلید مشترک و سر بار محاسباتی کم در کشف کلید مشترک نسبت به طرح‌های احتمالاتی برتری دارند. اما به دلیل محدودیت حسگرها اغلب این طرح‌ها مقیاس‌پذیر نیستند. به همین سبب مقیاس‌پذیر نمودن طرح‌های ترکیبیاتی یکی از چاش‌های اساسی است.

۱-۳ هدف

هدف از ارائه این پایان‌نامه، در ابتدا بررسی طرح‌های مهم احتمالاتی و ترکیبیاتی موجود در پیش‌توزیع کلید است. سپس طرح ترکیبیاتی صفحه تصویری را به علت اتصال‌پذیری کامل مورد توجه قرار داده و به منظور مقیاس‌پذیر نمودن آن، به معرفی طرح ترکیبیاتی ترکیبی (احتمالاتی-قطعی) موجود روی صفحه تصویری می‌پردازیم. در نهایت چند طرح ترکیبیاتی ترکیبی جدیدی را روی صفحه تصویری به منظور مقیاس‌پذیر کردن طرح پیش‌توزیع کلید با طرح‌های ترکیبیاتی صفحه تصویری ارائه می‌دهیم و آنها را از لحاظ میزان اتصال‌پذیری، امنیت و مقیاس‌پذیری با طرح مشابه موجود مقایسه می‌کنیم.

٤-١ ساختار کلی پایان‌نامه

پایان‌نامه پیش رو ۵ فصل دارد. در فصل دوم، ابتدا به مبانی مدیریت کلید در شبکه حسگر بی‌سیم می‌پردازیم. این مبانی شامل شاخص‌های ارزیابی مدیریت کلید و انواع طرح‌های مدیریت کلید است. سپس طرح‌های متقارن پیش‌توزیع کلید مورد توجه قرار گرفته و به معرفی انواع آن پرداخته می‌شود و در راستای هدف این پایان‌نامه به معرفی مبانی طرح‌های ترکیبیاتی می‌پردازیم و در انتها علت استفاده از طرح‌های ترکیبیاتی را بیان کرده و مزیت آن را نسبت به طرح‌های احتمالاتی بیان می‌کنیم.

در فصل سوم، به معرفی برخی از انواع طرح‌های ترکیبیاتی می‌پردازیم و ویژگی‌های هر یک از این طرح‌هارا بیان می‌کنیم.

طرح‌های ترکیبیاتی پرداخته شده در این فصل عبارتند از: ۱- طرح صفحه تصویری ۲- طرح مربع تعمیم یافته ۳- طرح عرضی ٤- طرح μ-متقاطع ۵- t-طرح. در این فصل طرح صفحه تصویری به علت اتصال‌پذیری کامل مورد توجه قرار می‌گیرد و مشکلات این طرح، بویژه مقیاس‌پذیری مورد بررسی قرار می‌گیرد تا در فصل بعد به حل این مشکل پرداخته شود.

در فصل چهارم، ابتدا به مشکل مقیاس‌پذیری طرح ترکیبیاتی صفحه تصویری پرداخته و به توسعه انجام گرفته در این طرح ترکیبیاتی، به منظور رفع این مشکل پرداخته می‌شود. سپس چند طرح ترکیبیاتی ترکیبی جدید، مبتنی بر طرح صفحه تصویری به منظور افزایش مقیاس‌پذیری ارائه داده و به کمک شبیه‌سازی نشان داده می‌شود که برخی از آنها نسبت به طرح متقارن ترکیبی که در [۳] و [٤] بیان شده، بهینه‌تر است. در حقیقت نشان داده می‌شود که، طرح نهایی پیشنهادی در این فصل، اتصال‌پذیری بیشتری نسبت به طرح ارائه شده در [۳] و [٤] را دارد بدون آنکه از امنیت شبکه کاسته شود.

در فصل پنجم، نتیجه‌گیری از پژوهش انجام گرفته در این پایان‌نامه بیان شده و پیشنهادهایی برای پژوهش‌های آینده ارائه داده می‌شود.

فصل دوم

امنیت در شبکه‌های حسگر بی‌سیم

۲-۱ مقدمه

یک شبکه حسگر بی‌سیم، از تعداد زیادی گره تشکیل شده است که به منظور گردآوری اطلاعات و انتقال آن‌ها، با یکدیگر همکاری می‌کنند. شبکه‌های حسگر بی‌سیم در موقعیت‌های گوناگونی مانند جنگل، دریا، آتشفشان، محیط‌های شهری، نظامی، فضایی، سیستم‌های بیولوژیکی و بدن انسان قرار می‌گیرند. با استفاده از شبکه حسگر بی‌سیم تمامی رویدادها را می‌توان مشاهده نمود.

بعضی از کاربردهای شبکه‌های حسگر بی‌سیم شامل کنترل عوامل محیطی، ردیابی بازماندگان بعد از بلایای طبیعی، تشخیص آتش‌سوزی در جنگل‌ها، نظارت میدان‌های جنگی، بررسی جابجایی حیوانات و بررسی وضعیت بیماران می‌باشد.

تامین سطحی از امنیت در شبکه‌های حسگر بی‌سیم در بسیاری از کاربردها ضروری به‌نظر می‌رسد. از جهتی دیگر به کارگیری هر نوع روش امنیتی، با توجه به محدودیت‌های حسگرها امکان پذیر نیست. به همین سبب، برقراری امنیت این سیستم‌ها با چالشی اساسی مواجه است. این چالش باعث شده تا حجم قابل قبولی از تحقیقات در سال‌های اخیر به روش‌های طراحی و به کارگیری الگوریتم‌ها و پروتکل‌های امنیتی در چنین شبکه‌های اختصاص داده شود. در این فصل ابتدا به معرفی شبکه‌های حسگر بی‌سیم پرداخته می‌شود. در ادامه به معرفی اجمالی روش‌های گوناگون مدیریت کلید، به منظور برقراری امنیت در شبکه‌های حسگر بی‌سیم پرداخته وسپس جایگاه الگوریتم‌های پیش‌توزیع کلید را در کارآیی طرح[10] مدیریت کلید، بیان می‌شود .

در پایان، به مبانی ترکیبیات پرداخته که مبنای بخشی از طرح‌های کارآی پیش توزیع کلید- که در فصل بعدی معرفی می شوند- است. در نهایت به مزایای طرح‌های مبتنی بر طرح ترکیبیاتی بر طرح‌های احتمالاتی پرداخته می‌شود.

۲-۲ شبکه‌های حسگر بی‌سیم

یک شبکه حسگر بی‌سیم از تعداد زیادی حسگر کوچک، ارزان و با منبع انرژی محدود تشکیل می‌شود. طبیعت خودکار و پراکنده این حسگرها، سازمان دهی شبکه را به عملکرد آن بسیار وابسته می‌کند و شبکه‌ای به وجود می‌آورد که بسیار پویاست.

[10] Schema or Design

حسگرهای شبکه با همکاری یکدیگر داده‌ها (اعم از مکانیکی، گرمایی، زیستی، شیمیایی و داده‌های بصری) را از محیط می‌گیرند و در کاربردهای متنوعی همچون نظارت محیط، تدارک یگان‌ها، عکس‌العمل به وضعیت اضطراری، مراقبت‌های پزشکی و نیز عملیات نظامی مورد استفاده قرار می‌دهند.

شبکه‌های حسگر، خودکار هستند و توسط انسان کنترل نمی‌شوند. این شبکه‌ها با محدودیت شدید انرژی مصرفی، توان پردازشی، حافظه در دسترس و قیمت تمام شده مواجه هستند. تعداد حسگرها در این شبکه زیاد و از مرتبه چند ده هزار است.

همان گونه که در فصل قبل ذکر شد دو معماری اصلی برای شبکه حسگر وجود دارد: ۱- توزیع شده[11] یا همگن[12] ۲-سلسله مراتبی[13] یا ناهمگن[14]. تصویر این شبکه‌ها در شکل ۱-۱ آورده شده است.

۲-۳ مبانی مدیریت کلید در شبکه حسگر بی سیم

به سبب اینکه تبادل اطلاعات در شبکه‌های حسگر از طریق کانال بی سیم صورت می گیرد، باید تدابیر امنیتی لازم مد نظر قرارداده شود تا از استراق سمع یا دست کاری اطلاعات توسط افراد ناشناس جلوگیری گردد. برای رسیدن به این هدف، باید به محدودیت های ذاتی حسگرها توجه نمود .

مدیریت کلید، مجموعه‌ای از روش‌ها و فرایندهای است که به برپایی و نگهداری کلید بین اعضا معتبر یک شبکه می‌پردازد و با شاخص‌های امنیت، کارایی، انعطاف‌پذیری و مقیاس‌پذیری مورد ارزیابی قرار می‌گیرد.

۲-۳-۱ شاخص‌های ارزیابی مدیریت کلید

۲-۳-۱-۱ امنیت

طرح مدیریت کلید مطلوب، باید تضمین کند که حسگرهای که در ارتباط با یکدیگر هستند، قادر به تایید هویت یکدیگر باشند. به این دلیل مقاومت شبکه در برابر حمله به حسگرهای معتبر و جعل هویت تضمین می‌شود. طرح‌های

[11] Distributed
[12] Homogeneous
[13] Hierarchical
[14] Heterogeneous

مدیریت کلید باید مقاومت قابل قبولی ایجاد کنند. میزان مقاومت نشان می‌دهد که با تسخیر[15] تعداد S حسگر، چه میزان از ارتباطات شبکه، به خطر می‌افتد. به عبارت دیگر مقاومت، احتمال لو رفتن یک ارتباط است، در صورتی که S گره تسخیر شده باشد. که آن را با نماد fail(S) نشان می‌دهند. رسم نمودار مقاومت[16] fail(S) یکی از پارامترهای مهم در شبکه حسگر است. تسخیر یک حسگر توسط مهاجم، به این معنا است که مهاجم به بخشی از سخت افزار حسگر نفوذ پیدا کرده است. در این حالت، کلیدهای اختصاص داده شده به آن حسگر را باید لو رفته تلقی نمود.

یک پروتکل مناسب مدیریت کلید، قادر است پس از کشف حسگرهای دستکاری شده آنها را حذف کند. این فرایند موجب می‌شود تا مهاجم قادر به وارد کردن حسگرهای بدرفتار به شبکه نباشد، حتی اگر بتواند از طریق بعضی حسگرها، به بعضی پارامترهای امنیتی شبکه دسترسی پیدا کند.

۲-۳-۱-۲ کارایی

طرح مدیریت کلید باید ضمن تامین کلیدهای مورد نیاز برای عملکرد صحیح ودقیق شبکه با محدودیت‌های ذاتی شبکه‌های حسگر بی سیم سازگار باشد. از این رو توزیع کلید باید از لحاظ پارامترهای حافظه، پردازش، پهنای باند و انرژی، سبک[17] باشد، در عین حال باید اتصال‌پذیری[18] کافی را برای شبکه برآورده سازد.

۲-۳-۱-۳ انعطاف‌پذیری و مقیاس‌پذیری

از آنجائیکه در بسیاری از کاربردها، حسگرها به صورت پویا و تصادفی در شبکه قرار می‌گیرند، اطلاع از موقعیت نهایی حسگرها کاردشواری است. بنابراین، طرح‌های مدیریت کلید باید انعطاف‌پذیری لازم را داشته باشند تا برای برقراری ارتباط در شبکه، نیازمند موقعیت‌یابی حسگرها نباشند. همچنین طرح‌های مدیریت کلید بایستی مقیاس‌پذیر[19] نیز باشند، بدین معنا که توانایی گسترش‌پذیری را داشته باشند، یعنی این که شبکه‌های بزرگتر را هم پشتیبانی کند و بدون کاستن از امنیت، قادر به معرفی حسگرهای جدید باشند و در این راه بایستی به محدودیت های حسگرها (بویژه حافظه) توجه شود.

[15] Compromise
[16] Resilience
[17] Lightweight
[18] Connectivity
[19] Scalable