
بسم الله الرحمن الرحيم

پردیس بین‌الملل دانشگاه گیلان
گروه مهندسی فناوری اطلاعات
گرایش شبکه‌های کامپیوتری

عنوان

پیش‌توزیع کلید در شبکه‌های حسگر بی‌سیم مبتنی بر طرح‌های ترکیبیاتی

از:
امیر حسنی کرباسی

استادان راهنما:
دکتر رضا ابراهیمی آتانی
دکتر شهاب‌الدین ابراهیمی آتانی

اسفند ۱۳۹۱

جهان غرق رحمت او است

خدایا، شکرت برای دستان یاری رسان، برای همه آن عشق و محبت و چیزهای شگفت انگیزی که دریافت کردم.

پروردگارا، به من قلبی فرمانبردار، گوشی شنوا، ذهنی هوشیار و دستانی ساعی عنایت فرما تا بتوانم تسلیم رضایت گردم و آنچه را که به کمال برایم خواسته ای بدیده منت بپذیرم. خدایا، بر تمام عزیزانم برکت و بهروزی عطا کن، و صلح و دوستی و آرامش بر قلوب انسانها حاکم گردان.

آمین یارب العالمین

تشکر و قدردانی:

در آغاز بر خود لازم دانسته که،

از استاد گرانقدرم، جناب آقای دکتر رضا ابراهیمی آتانی که با حوصله فراوان به راهنمایی اینجانب اهتمام ورزیدند و نیز به خاطر حمایت های بی دریغ شان، نهایت تشکر و سپاسگزاری را دارم.

از استاد بزرگوارم، جناب آقای دکتر شهاب الدین ابراهیمی آتانی به خاطر مساعدت های با ارزش و راهنمایی های سودمند و الطاف بی پایانشان، کمال سپاس و امتنان را دارم.

همین طور از جناب آقای دکتر صابری نجفی و جناب آقای دکتر میر روشندل که داوری این پایان نامه را با نهایت دقت و صرف وقت زیاد انجام دادند، بسیار تشکر می نمایم.

و سپاس بیکران بر همدلی و همراهی و همگامی پدر و مادر مهربانم که با محبت ها و توجه شان مرا یاری کردند و هرچه که دارم از دعای خیر آنان است.

امیر حسن کرباسی

فهرست مطالب

فصل ۳: روش تحقیق

فصل ۴: نتایج و تفسیر آنها

فصل ۵: جمع‌بندی و پیشنهادات آتی

فهرست اشکال

فهرست جداول

چکیده:

پیش‌توزیع کلید در شبکه‌های حسگر بی‌سیم مبتنی‌بر طرح‌های ترکیبیاتی

امیر حسنی کرباسی

شبکه‌های حسگر بی‌سیم (*WSNs*) به طور گسترده برای نظارت و کنترل محیط و سیستم‌هایی که خارج از دسترس انسان هستند، بکار می‌روند. مانند سایر شبکه‌های کامپیوتری و مخابراتی، شبکه‌های حسگر بی‌سیم نیز از نظر تهدیدات و حملات مخرب بسیار آسیب‌پذیر هستند و طراحی ساده سخت‌افزار این ابزارهای الکترونیکی، مانع از بکارگیری مکانیسم‌های دفاعی مرسوم شبکه‌ها می‌شود. استقرار کلید از اساسی‌ترین عملکردهای رمزگذاری در تمامی انواع کاربردهایی است که در آن امنیت به عنوان یک نگرانی محسوب می‌شود.

طرح پیش‌توزیع جفت کلید به خاطر تاثیرپذیری از محدودیت منابع و تسخیر شدن فیزیکی گره‌های حسگر، عامل ضروری برای شبکه‌های حسگر بی‌سیم است. امنیت شبکه‌های حسگر بی‌سیم بدون زیرساخت و توزیع‌شده متراکم و در مقیاس بزرگ، نیازمند توزیع کلید مؤثر و مکانیسم‌های مدیریتی است. طراحی ترکیبیاتی به دلیل برتری‌های تعیین‌کننده نسبت به مدل‌های احتمالاتی پیش‌توزیع کلید و سایر مدل‌ها، مورد توجه قرار داده شده است. یک ساختار ریاضی ترکیبیاتی بنام طرح بلوک ناقص بالانس شده (*BIBD*) برای ساخت حلقه‌های کلید مورد استفاده قرار می‌گیرد. با طراحی مناسب *BIBD*، می‌توان از اتصال مناسب طرح توزیع کلید اطمینان حاصل نمود. این طرح از صفحه‌تصویری (*projective plane*) متناهی رتبه n (برای توان‌های عدد اول n) جهت تولید یک طراحی متقارن (یا *BIBD* متقارن) استفاده می‌کند. از معایب این طرح این است که پارامتر n باید عدد اول یا یکی از توان‌های عدد اول n باشد، از این رو سایز شبکه حسگر نمی‌تواند برای یک اندازه دلخواه حلقه کلید یا به تعداد دلخواهی حسگر پشتیبانی شود.

مجموعه احاطه‌گر همبند (*CDS*) برای استفاده مانند یک ستون فقرات مجازی، جهت کاهش سربار مسیریابی، صرفه‌جویی در مصرف انرژی و کنترل توپولوژی پیشنهاد شده است که مسیریابی را با محدود کردن وظایف اصلی مسیریابی فقط به گره‌های احاطه‌گر، سبب بهبود امنیت شبکه می‌شود. ما بر روی الگوریتم‌های مجموعه احاطه‌گر همبند، شامل موارد توزیع‌شده و متمرکز برای چگونگی ایجاد *CDS* تمرکز کرده و آنالیزهای تئوریکی را نیز ارائه خواهیم داد. در این پایان‌نامه، سیستم‌های مجموعه ترکیبیاتی را در طراحی قطعی پیش‌توزیع کلید برای شبکه‌های حسگر بی‌سیم توزیع‌شده (*DSNs*) مورد مطالعه قرار می‌دهیم و طرح‌های عملی را جهت دستیابی به پیوستگی، انعطاف‌پذیری و حالت ارتجاعی بالا شرح می‌دهیم و ضمن ارایه یک مدل جدید برای اصلاح صفحات‌تصویری با طرح کپی و تبادل کلید (*KCAE*) بر اساس مجموعه‌های احاطه‌گر همبند با کنترل توپولوژی مبتنی بر ستون فقرات مجازی، به ارزیابی کارایی طرح با تحلیل‌های امنیتی میزان مقاومت مدل برای انعطاف‌پذیری در مقابل حمله تسخیر گره، بازدهی منابع، اتصال یا همبندی مدل و قابلیت مقیاس‌پذیری در شبکه می‌پردازیم.

کلید واژه: امنیت شبکه حسگر بی‌سیم، پیش‌توزیع کلید، صفحات‌تصویری، مجموعه‌های احاطه‌گر، ستون فقرات مجازی، کپی و تبادل کلید.

Abstract:

Key Pre-distribution For Wireless Sensor Networks Based on Combinatorial Schemes

Amir Hassani Karbasi

Wireless Sensor Networks (*WSNs*) are now widely used for monitoring and controlling of systems where human intervention is not desirable or possible. Like other computer and telecommunication networks, wireless sensor networks are susceptible to regarding destructive threats and attacks and simple hardware of these electronic devices prevents applying defensive mechanisms called networks. Positioning key is of main performances of coding in all kinds of applications in which security is considered as an anxiety.

Pair-wise key pre-distribution design because of being under the influence of resource limitations and physical nodes of the sensor is essential for wireless sensor networks. Security of large scale densely deployed and infrastructure-less wireless sensor networks requires efficient key pre-distribution and management mechanisms. Combinatorial design is considered for distinct advantages than probabilistic model and other models of key pre-distribution. One mathematical structure called balanced incomplete block design (*BIBD*) is used to construct the key rings. With the proper design of BIBD, one can ensure the connectivity of key distribution scheme. The scheme uses *finite projective plane* of order *n* (for prime power n) to generate a *symmetric design* (or symmetric BIBD). Disadvantage of this solution is that, parameter *n* has to be a prime power; therefore, not all network sizes can be supported for a fixed key-chain size.

Connected Dominating Set (*CDS*) has been recommended to serve as a virtual backbone for a WSN to reduce routing overhead, energy efficiency and topology control that network security is improved by restricting the main routing tasks to the dominators only. We focus on connected dominating set algorithms, including both centralized and distributed, for how to construct CDS. Theoretical analysis are also presented. In this dissertation, we discuss the use of combinatorial set systems in the design of deterministic key pre-distribution schemes for distributed sensor networks (*DSNs*). We concentrate on analyzing combinatorial properties of the set systems that relate to the connectivity and resilience of the resulting distributed sensor networks and besides presenting a new model for reforming projective plane with key copying and exchanging (*KCAE*) based on dominating sets and virtual backbone-based topology control, we deal with the evaluation of design efficiency by analyzing security of the model resistance rate for resilience against sensor compromises, resource efficiency, connectivity of the model and scalability in sensor network.

Keywords: wsn security, key pre-distribution, projective plane, dominating sets, virtual backbone, key copying and exchanging.

فصل ۱:

مقدمه

۱-۱- مقدمه

شبکه‌های حسگر بی‌سیم[۱] (*WSNs*) را می‌توان به عنوان نوع ویژه‌ای از شبکه‌های اقتضایی درنظرگرفت که از تعداد زیادی حسگر کوچک، ارزان و با منبع انرژی محدود تشکیل شده است. همچنین شبکه‌های حسگر، بسیاری از جنبه‌های مشترک با شبکه‌های عمومی موردی[۲] را به اشتراک می‌گذارند. طبیعت خودکار و پراکنده این حسگرها، سازمان‌دهی شبکه را به عملکرد آن بسیار وابسته می‌کند و شبکه‌ای به وجود می‌آورد که بسیار پویاست. حسگرهای شبکه با همکاری یکدیگر، داده‌ها (اعم از مکانیکی، گرمایی، زیستی، شیمیایی و داده‌های بصری) را از محیط دریافت کرده و در کاربردهای متنوعی همچون نظارت محیط، تدارک یگان‌ها، واکنش به وضعیت اضطراری، مراقبت‌های پزشکی و نیز عملیات نظامی مورد استفاده قرار می‌گیرند[۱]. وقتی گره‌ها به طرز بی‌مراقبت[۳] در محیط دشمن گسترش بیابند، براحتی توسط دشمن مورد مداخله قرار می‌گیرند و یا کانال ارتباطی، شنود می‌شود. از آنجایی که انتقال اطلاعات در شبکه‌های حسگر از طریق کانال بی‌سیم انجام می‌گیرد، باید تدابیر امنیتی لازم اندیشیده شود تا جلوی استراق سمع یا دستکاری اطلاعات توسط دشمن گرفته شود. برای رسیدن به این هدف، باید با به‌کارگیری روش‌های رمزنگاری، خدمات پایه‌ای نظیر محرمانگی[۴]، جامعیت[۵] و اصالت پیام[۶] را فراهم کرد[۱۰۶-۲,۱۰۴]. طرح‌های توصیه شده برای شبکه‌های کامپیوتری، برای این شبکه‌ها موثر نیستند و توانایی‌های محدود گره‌های حسگر بعنوان مانع و سد جلوی راه بوده و به همین دلیل رمزنگاری کلید عمومی[۷] به سختی قابل پیاده‌سازی بوده و به جهت کارایی بالا تمرکز ما بیشتر بر روی رمزنگاری متقارن[۸] و بهینه کردن این طرح‌ها است[۱۰۶-۲,۱۰۴].

به طور کلی بنانهادن جفت‌کلید بین گره‌ها به سه دسته زیر تقسیم می‌شوند[۲]:

۱- بنانهادن کلیدهای رمز با زیرساخت کلید عمومی[۹] (*PKI*)، اگرچه رمزنگاری نامتقارن به دلیل نیاز به حجم زیاد محاسبات و حافظه، هزینه‌بر هستند.

---

[۱] Wireless Sensor Networks

[۲] Ad hoc Networks

[۳] Unattended

[۴] Confidentiality

[۵] Integrity

[۶] Message Authentication

[۷] Public Key

[۸] Symmetric Encryption

[۹] Public Key Infrastructure

۲- وجود یک پایگاه مرکزی مورد اطمینان[۱] (*TA*) برای تخصیص کلیدهای با طول عمر زیاد و توزیع کلید نشست بر حسب تقاضا که این روش هم دارای مشکلاتی در ارسال مجدد پیام‌های کنترلی و توافق بین گره‌ها بوده و هزینه‌بر می‌باشد.

۳- طرح‌های پیش‌توزیع کلید[۲] (*KPS*) که در آن مجموعه‌ای از کلیدهای مخفی قبل از توزیع گره‌ها در محیط در حافظه آنها نصب می‌شوند.

بسیاری از روش‌های رمزنگاری، نیاز به کلیدهای محرمانه[۳] دارند و باید روش‌هایی برای توزیع امن کلید یافت. در طرح‌های توزیع و پیش‌توزیع کلید، یک مرکز توزیع کلید[۴] (*KDC*) وظیفه بارگذاری کلید در حسگر - چه از طریق فیزیکی و چه از طریق رابط‌های امن بی‌سیم- را برعهده دارد. در *KPS*، مجموعه‌ای از کلیدهای مخفی قبل از توزیع گره‌ها در محیط در حافظه آنها نصب می‌شوند. بعد از برپایی شبکه، دیگر وابستگی به آن ساختار مرکزی وجود نخواهد داشت. این طرح‌ها برای اجتناب از تحمیل سربار ناشی از فرایندهای تولید کلید پیشنهاد شده‌اند. طرح‌های توزیع کلید بر مبنای شاخص‌های امنیت، کارایی و انعطاف‌پذیری با یکدیگر مقایسه می‌شوند. اگرچه عموماً در معیارهایی نظیر کم‌مصرف بودن، ارتباط بین تعداد بیشتری از حسگرهای شبکه و مقاوم بودن در برابر حملات با یکدیگر مصالحه دارند[۳,۱۰,۱۰۵,۱۰۶].

در ادامه این فصل به بررسی جامع آنچه تاکنون شرح دادیم، می‌پردازیم. این فصل به کلیات اختصاص دارد و شامل معرفی مفاهیم اصلی، بیان مسئله و رویکرد انتخابی و ساختار پایان‌نامه است. لازم به ذکر است که معادل فارسی تمامی اصطلاحات و واژه‌های انگلیسی که در متن پایان‌نامه آمده است از واژه‌نامه امنیت فضای تبادل اطلاعات (افتا) استخراج شده‌اند.

۱-۲- معرفی مفاهیم اصلی

طرح‌های توزیع کلید را از یک دیدگاه می توان به سه دسته ۱- احتمالی[۵] ۲- قطعی[۶] ۳- هیبرید[۷]، تقسیم کرد[۴,۱۰۵]:

در راه‌حل‌های احتمالی، حلقه‌های کلید[۸] به طور تصادفی از استخر کلید انتخاب شده و در گره‌های حسگر توزیع می‌شوند.

---

[۱] Trusted Authority

[۲] Key Pre-distribution Schemes

[۳] Secret Keys

[۴] Key Distribution Center

[۵] Probabilistic

[۶] Deterministic

[۷] Hybrid

[۸] Key Ring

در راه‌حل‌های قطعی، فرایندهای قطعی برای طراحی استخر کلید و حلقه‌های کلید برای ایجاد اتصال بهتر کلید، مورد استفاده قرار می‌گیرند. نهایتاً راه‌حل‌های هیبرید، از دیدگاه‌های احتمالی در راه‌حل‌های قطعی برای بهبود مقیاس‌پذیری[۱] و انعطاف‌پذیری استفاده می‌کند.

طرح‌های پیش‌توزیع کلید مبتنی بر ترکیبیات[۲]، سربار مخابراتی تحمیل شده در مرحله کشف کلید مشترک را کاهش می‌دهد و از این نظر بر طرح‌های احتمالاتی برتری دارد. از طرف دیگر از طرح‌های ترکیبیاتی می توان برای شبکه‌هایی با الگوی خاص مثل شبکه‌هایی با موقعیت معین حسگرها یا الگوهای گروهی بهره جست. در نتیجه هدف ما بکارگیری و بهینه‌سازی طرح‌های قطعی ترکیبیاتی در مکانیزم پیش‌توزیع کلید در شبکه‌های حسگر بی‌سیم است. در راه‌حل‌های قطعی پیش‌توزیع کلید مبتنی بر طراحی ترکیبیاتی، احتمال کشف کلید مشترک در طول گره‌های حسگر می‌تواند توسط طراحی مناسب حلقه‌های کلید، افزایش یابد[۲,۵,۶,۱۰۵].

در طرح ما از تئوری ترکیبیات برای افزایش اتصال بهره برده می‌شود. در حقیقت طرح پیش‌توزیع کلید مبتنی بر طراحی ترکیبیاتی یک نوع قطعی از انتساب کلید است که در آن حلقه کلید هر کدام از گره‌های حسگر بصورت قطعی طراحی می‌شود[۲,۵,۶,۱۰۵].

تعدادی از تحقیقات، چالش‌های طراحی پروتکل‌های مسیریابی[۷,۱۰۶] و به مراتب آن، پروتکل‌های امنیتی[۸,۱۰۶] را معرفی می‌کنند. اولاً، با توجه به تعداد نسبتاً زیاد گره‌های حسگر، امکان ساخت یک طرح آدرس‌دهی سراسری برای ایجاد تعداد زیادی از گره‌های حسگر که به عنوان پشتیبانی از *ID*های بسیار زیاد با سرباری بالا، وجود ندارد. از این جهت، پروتکل‌های مبتنی بر *IP* مرسوم ممکن است برای *WSN*ها به کار نروند. دوماً، گره‌های حسگر دارای محدودیت‌های انرژی، پردازش و ظرفیت ذخیره‌سازی می‌باشند. بنابراین، آنها نیازمند مدیریت منبع دقیق هستند. نهایتاً، آگاهی به موقعیت گره‌های حسگر نیز بسیار مهم است، استفاده از سخت‌افزار سیستم موقعیت جهانی[۳] (*GPS*) برای این منظور امکان‌پذیر نیست. *GPS* فقط می‌تواند در موقعیت‌های فضای بیرونی بکار رود و در حضور هیچ مانعی کاربرد ندارد. به علاوه، گیرنده‌های *GPS* گران‌قیمت بوده و برای ساخت گره‌های حسگر کوچک ارزان‌قیمت نامناسب هستند[۸,۹]. از این رو، با توجه به چنین تفاوت‌هایی، بسیاری از الگوریتم‌های جدید برای مسائل مسیریابی امن در *WSN*ها پیشنهاد شده‌اند.

[۱] Scalability

[۲] Combinatorial Key Pre-distribution

[۳] Global Positioning System

تقریباً تمامی پروتکل‌های مسیریابی امن می‌توانند با توجه به ساختار شبکه حسگر بی‌سیم به صورت ۱- توزیع‌شده[۱] (*DSNs*) و ۲- سلسله‌مراتبی[۲] (*HSNs*) دسته‌بندی شوند[۱۰].

در شبکه‌های توزیع‌شده، گره‌ها از یک جنس و ساختار بوده و هر گره به صورت نوعی نقش مشابهی را ایفا می‌کنند و گره‌های حسگر برای انجام کارهای نظارتی با هم همکاری می‌کنند. مجموعه‌ای از مشکلات مربوطه، تحت عنوان طوفان پخش همگانی[۳] [۱۱] باید در *DSNs* مورد توجه قرار گیرند، چرا که کشف یک مسیر چندگامی متصل از گره منبع به مقصد معمولاً نیازمند انتشار سیل‌آسای[۴] پیام‌های کنترلی در شبکه است که بسیار هزینه‌بر بوده و امنیت شبکه را به خطر می‌اندازد[۱۲,۱۳,۱۴]. علاوه بر این، *WSN*ها به دلیل پویایی و عدم اطمینان گره‌ها، بسیار فرّار هستند. از این جهت، تاریخ منقضی شدن اطلاعات کنترلی مسیریابی جمع‌آوری شده توسط یک ارسال پخش همگانی هزینه‌بر می‌تواند به سرعت، خارج از مُهر زمان پیام‌ها شود. روش‌هایی پیشنهاد شده‌اند که با این طبیعت طوفانی سر وکار دارند. برخی از این الگوریتم‌ها مانند *DSR* [۱۵] و *AODV* [۱۶] که به طور گسترده در شبکه *Ad hoc* مورد استفاده قرار می‌گیرند، در *WSN*ها هم به کار رفته‌اند. طبیعت بر حسب تقاضا بودن این دیدگاه‌های واکنشی می‌تواند آنها را نسبت به تشخیص و تطبیق با تغییرات توپولوژی، سریع‌تر سازد. به هرحال، عیب عمده این است که بافرینگ اطلاعات کنترلی، هنگامی که گره‌ها حرکت کنند و یا خراب شوند، کمتر مؤثر است. در این شرایط، الگوریتم‌های واکنشی، مسیرهای غیربهینه را آشکار می‌کنند و مسیریابی‌های دوباره، فوق العاده پر هزینه خواهد بود. پروتکل‌های دیگر مسیریابی برای تک‌پخشی، چندپخشی و یا پخش‌همگانی در *WSN*ها مانند *SPIN* [۱۷]، *COUGAR* [۱۸] و مبتنی بر *Quality of Service* (*QoS*) [۱۹-۲۳]، ... معرفی می‌شوند. هر چند، تقریباً تمام این الگوریتم‌ها در *DSN* دارای ۱- سربار پروتکل و تداخل بالا، ۲- تأخیرهای زیاد در انتشار داده‌ها، ۳- نیازمندی به سنکرون‌سازی در میان گره‌ها، ۴- عدم وجود کنترل توپولوژی عملی در شبکه، ۵- مناسب نبودن برای برخی از شبکه‌های حسگر بی‌سیم با توجه به پهنای باند محدود و ۶- نادیده گرفتن امنیت مسیریابی، می‌باشند.

پروتکل‌های مسیریابی برای *DSN*، پروتکل‌های مبتنی بر شایعات[۵] [۲۴-۲۶] و احتمالات [۲۷,۲۸] به عنوان روش‌های مؤثر پخش همگانی یا ارسال سیل‌آسای اطلاعات در *WSN*ها مورد توجه قرار می‌گیرند.

نوع دیگری از پروتکل مسیریابی توزیع‌شده، مسیریابی مبتنی بر مکان، مانند *GPSR* [۲۹]، *GOAFR* [۳۰] و ... است که گره‌های حسگر به وسیله مکان آنها آدرس‌دهی می‌شوند. همچنین ممکن است در بعضی از شرایط، نیاز به کنترل توپولوژی یا

---

[۱] Distributed Sensor Networks

[۲] Hierarchical Sensor Networks

[۳] Broadcast Storm

[۴] Flooding

[۵] Gossip-based

به معنای دیگر ایجاد یک سیستم مختصات مکان‌یابی حسگرها، احساس شود. بسیاری از تکنیک‌های مکان‌یابی پیشنهادی به تکنیک‌های بازگشتی سه بعدی یا چند بعدی [۳۱,۳۲] بستگی دارند، که دقت کافی را در *WSN*ها فراهم نمی‌کنند.

روش‌های مبتنی بر کلاستر یا سلسله‌مراتبی، که عموماً در شبکه‌های بی‌سیم مطرح می‌شوند، روش‌های شناخته شده‌ای با مزایای خاص مربوط به امنیت، مقیاس‌پذیری و ارتباط مؤثر است. همینطور، مفهوم مسیریابی سلسله‌مراتبی می‌تواند برای ایجاد مسیریابی امن و با صرفه‌جویی در مصرف انرژی مؤثر نیز مورد استفاده قرار گیرد. ایجاد کلاسترها و تخصیص کارهای خاص به سردسته کلاسترها می‌تواند به طور گسترده برای مقیاس‌پذیری، طول عمر و کارایی انرژی سراسری شبکه، مورد استفاده واقع شود[۳۳].

۱-۳- بیان مسئله و رویکرد انتخابی

معمولاً *WSN*ها با استفاده از مدل شبکه قطعی[۱] (*DNM*) مدل‌سازی می‌شوند[۳۳]. تحت این مدل‌سازی، یک شعاع انتقال برای هر گره وجود دارد. با توجه به این شعاع، اگر فاصله فیزیکی هر جفت مشخص از گره‌ها کمتر از این شعاع باشد، همیشه به همسایگان خود متصل خواهند بود، در حالی که بقیه جفت‌ها همیشه غیر متصلند. مدل گراف دیسک واحد[۲] (*UDG*) [۳۴] یک حالت خاص از مدل *DNM* است که در آن تمام گره‌ها دارای شعاع انتقال مشابهی می‌باشند. زمانی که تمام گره‌ها از طریق یک مسیر تک‌گامی به یکدیگر متصل هستند، گفته می‌شود که *WSN* دارای ارتباطات کامل[۳] است. اگرچه در کاربردهای واقعی، مدل *DNM* نمی‌تواند به طور کامل رفتار لینک‌های بی‌سیم را مشخص کند که دلیل آن، پدیده ناحیه انتقالی[۴] می‌باشد که توسط بسیاری از مطالعات ضمنی بیان شده است[۳۸-۳۵]. در واقع، علاوه بر ناحیه دارای ارتباطات کامل با تک‌گام (گراف کامل)، یک ناحیه انتقالی وجود دارد که یک جفت از گره‌ها به طور احتمالی به هم متصل هستند. چنین جفت‌هایی از گره‌ها کاملاً متصل نبوده اما از طریق لینک‌هایی که پراتلاف[۵] نامیده می‌شوند با چند گام قابل دسترسی هستند[۳۸]. همانگونه که در [۳۸] آمده است، معمولاً تعداد زیادی لینک پراتلاف نسبت به لینک‌های کاملاً مرتبط در *WSN*ها وجود دارد. به علاوه، در یک حالت خاص [۳۹] بیش از ۹۰٪ لینک‌های شبکه، لینک‌های پراتلاف هستند.

زمانی که لینک‌های پراتلاف در شبکه به کار گرفته می‌شوند، هیچ تضمینی برای اتصال کل شبکه وجود ندارد. هنگامی که

---

[۱] Deterministic Network Model

[۲] Unit Disk Graph

[۳] Full Connectivity

[۴] Transitional Region Phenomenon

[۵] Lossy Links

انتقال داده‌ها از طریق چنین توپولوژی‌هایی صورت گیرد، ممکن است نرخ تحویل گره به گره را کاهش دهد. شکل ۱-۱ مدل‌هایی از توسعه یک شبکه حسگر نوعی را با استفاده از گراف‌ها نشان می‌دهد.

معمولاً یک *WSN* دارای تراکم بسیار گره‌ها و افزونگی داده‌ای بالایی است، از این رو، کارایی مشخصی برای بسیاری از کاربردهای *WSN* مورد انتظار می‌باشد. بنابراین، تا زمانی که بتوان به درصد قابل قبولی از امنیت شبکه دست یافت و نرخ مناسب تحویل گره به گره را تأمین کرد، طرح کنترل توپولوژی[۱] با ایجاد ستون فقرات مجازی[۲] (*VB*) توسط مجموعه احاطه‌گر همبند[۳](*CDS*) در شبکه‌های حسگر بی‌سیم توزیع‌شده مورد نیاز می‌باشد. به عبارت دیگر، اتصال شبکه‌ای کامل، همیشه ضروری نیست و برخی از کاربردهای مجموعه احاطه‌گر مانند مجموعه احاطه‌گر همبند می‌تواند امنیت ارتباطات شبکه‌ای کامل و یا چندگامی را با کارایی انرژی[۴] بیشتر و ظرفیت شبکه بزرگتر مهیا کند.

یک ساختار ریاضی پیش‌توزیع کلید ترکیبیاتی بنام طرح بلوک ناقص بالانس شده[۵] (*BIBD*) برای ساخت حلقه‌های کلید مورد استفاده قرار می‌گیرد. *BIBD* متقارن یا صفحه‌تصویری[۶] یک سیستم مجموعه‌ای با پنج پارامتر $(n^2+n+1,n^2+n+1,n+1,n+1,\lambda)$ می‌باشد. با طراحی مناسب صفحات‌تصویری، می‌توان از اتصال طرح پیش‌توزیع کلید اطمینان حاصل نمود. با این وجود *BIBD* محدودیت‌هایی را نیز دارد، عیب اول این مدل این است که برای شبکه‌های کوچک مؤثر است ولی در شبکه‌های بزرگ با مشکل محدودیت حافظه مواجه می‌باشد. عیب دوم این مدل این است که پارامتر n باید یک عدد اول یا توان‌های یک عدد اول[۷] باشد، از این رو تمام اندازه‌های شبکه حسگر نمی‌توانند برای یک اندازه حلقه کلید دلخواه یا سایز شبکه دلخواه پشتیبانی شوند. دو طرح ترکیبیاتی مکمل برای اصلاح معایب فوق ارائه شده‌اند: ۱- مربعات تعمیم یافته[۸] (*GQ*)، ۲- طرح هیبرید.

این دو طرح نیز دارای معایبی می‌باشند: ۱- کشف کلید مشترک همیشه با احتمال 1 امکان‌پذیر نیست، ۲- پارامتر n همچنان باید یکی از توان‌های عدد اول باشد، ۳- سرریز ارتباطی[۹] و سرریز ذخیره‌سازی وجود دارد. تشریح کامل طرح‌های فوق را در فصل ۲ و ۳ ارائه داده‌ایم.

---

[۱] Topology Control

[۲] Virtual Backbone

[۳] Connected Dominating Set

[۴] Energy Efficiency

[۵] Balanced Incomplete Block Design

[۶] Projective Plane

[۷] Prime Power

[۸] Generalized Quadrangles

[۹] Communication Overhead