پیش‌توزیع کلید مبتنی‌بر صفحه‌تصویری با کپی و تبادل کلید جایگشتی بر اساس مجموعه‌های غالب در شبکه‌های حسگر بی‌سیم

امیر حسنی‌کرباسی[۱]، رضا ابراهیمی‌آتانی[۲]، شهاب الدین ابراهیمی‌آتانی[۳]، جواد مهری‌تکمه[۴]

چکیده

شبکه‌های حسگر بی‌سیم بطور گسترده برای نظارت و کنترل محیط و سیستم‌هایی که خارج از دسترس انسان هستند، بکار می‌روند. این شبکه‌ها در برابر حملات آسیب‌پذیر هستند و طراحی ساده سخت‌افزار این ابزارهای الکترونیکی، مانع از بکارگیری مکانیسم‌های دفاعی مرسوم می‌شود. طرح پیش‌توزیع جفت کلید به خاطر تاثیرپذیری از محدودیت منابع و تسخیر شدن فیزیکی گره‌های حسگر، عاملی ضروری برای شبکه‌های حسگر بی‌سیم است. امروزه طرحهای ترکیبیاتی مدیریت کلید به دلیل برتری‌های تعیین‌کننده نسبت به مدل‌های احتمالاتی پیش‌توزیع کلید و سایر مدل‌ها، مورد توجه قرار داده شده است. با طراحی مناسب BIBD، می‌توان از اتصال مناسب طرح توزیع کلید اطمینان حاصل نمود. این طرح از صفحه‌تصویری متناهی رتبه n جهت تولید یک طراحی متقارن استفاده می‌کند. از آنجایی که پارامتر n باید عدد اول یا یکی از توان‌های عدد اول n باشد، از این رو اندازه شبکه حسگر نمی‌تواند برای یک اندازه دلخواه حلقه کلید یا به تعداد دلخواهی حسگر پشتیبانی شود. مجموعه غالب همبند ضعیف (WCDS) برای استفاده مانند یک زیرساخت مجازی، جهت کاهش سربار مسیریابی و کنترل توپولوژی پیشنهاد شده است که مسیریابی را با محدود کردن وظایف اصلی مسیریابی فقط به گره‌های غالب، سبب بهبود امنیت شبکه می‌شود. در این مقاله، ضمن ارایه یک مدل جدید برای اصلاح معایب صفحات‌تصویری با طرح کپی و تبادل کلید جایگشتی (PKCAE) بر اساس مجموعه‌های غالب همبند ضعیف با کنترل توپولوژی مبتنی بر زیرساخت مجازی، به ارزیابی کارایی طرح با بررسی احتمال وجود کلید مشترک در شبکه‌ای با اندازه دلخواه و قابلیت مقیاس‌پذیری شبکه و برقراری مسیر کلید می‌پردازیم.

کلید واژه

امنیت شبکه حسگر بی سیم، پیش توزیع کلید، BIBD، صفحات تصویری، مجموعه غالب، کپی و تبادل کلید جایگشتی.

مقدمه

شبکه های حسگر بی سیم[۵](*WSNs*) در بسیاری از حوزه‌ها شامل ماشینی‌سازی یا اتوماسیون صنعتی، امنیت، تحلیل شرایط آب و هوا، دامنه وسیعی از سناریوهای نظامی و غیره کاربرد دارند. شبکه‌های حسگر بی‌سیم، گره‌هایی برای جمع‌آوری و انتشار داده‌های محیطی هستند. گره‌های حسگر ابزارهایی با محدودیت در محاسبات، محدودیت در ارتباطات و توانایی‌های ذخیره‌سازی می‌باشند و معمولاً به خاطر دلایل اقتصادی به این شکل تولید می‌شوند. آنها در اطراف یک دیگر بوده و با برد کوتاه کانال رادیویی به برقراری ارتباط می‌پردازند و به دفعات به جهت صرفه‌جویی در مصرف انرژی، به حالت خواب می‌روند. معماری‌های *WSN* در ساختارهای سلسله مراتبی[۶](*HSN*) و توزیع شده[۷](*DSN*) تشکیل شده است[۲,۱]. در *WSNs* سلسله مراتبی، یک سلسله مراتب بین گره‌ها بر اساس قابلیت‌هایشان وجود دارد:

۱) ایستگاه اصلی، ۲) سردسته‌های خوشه، ۳) گره‌های حسگر.

در *WSNs* توزیع شده، هیچ ساختار ثابتی وجود ندارد و توپولوژی شبکه قبل از گسترش شناخته شده نیست. گره‌های حسگر معمولاً به طور تصادفی در کل ناحیه هدف پراکنده شده‌اند. در این مقاله از ساختار *DSN* استفاده شده است و برای تحت پوشش قرار دادن یک ناحیه وسیع، از ارتباطات چندگامی بهره برده شده است. مهمترین موضوع در سیستم‌های حسگر مسئله مقابله با تهدیدات امنیتی بزرگ و کوچک می‌باشد. وقتی گره‌ها به طرز بی‌مراقبت در محیط توزیع شوند و یا در محیط دشمن گسترش یابند، براحتی توسط دشمن مورد مداخله قرار می‌گیرند و یا کانال ارتباطی، شنود می‌شود. بنابراین بنا نهادن جفت کلیدها با طرحی که بیشینه همبندی گره‌ها را تأمین کند و تهدیدات امنیتی را به

---

[۱] کارشناس ارشد فناوری اطلاعات، دانشگاه گیلان

[۲] استادیار گروه مهندسی کامپیوتر، دانشگاه گیلان، rebrahimi@guilan.ac.ir

[۳] استاد گروه ریاضی محض، دانشگاه گیلان

[۴] استادیار گروه ریاضی کاربردی، دانشگاه تبریز

[۵] Wireless Sensor Networks

[۶] Hierarchical Sensor Networks

[۷] Distributed Sensor Networks

کمینه برساند، مطلوب خواهد بود[۳،۴] یکی از دغدغه‌های اصلی در کاربردهای شبکه حسگر این است که چگونه محرمانه بودن اطلاعات تضمین شود و پیام کنترلی و داده مبادله شده در طول گره‌های حسگر می‌تواند از نظر امنیتی اثبات شود[۵-۸]. طرح‌های توصیه شده برای شبکه‌های کامپیوتری، برای شبکه‌های حسگر بی‌سیم مؤثر نیستند و توانایی‌های محدود گره‌های حسگر بعنوان مانع و سد جلوی راه بوده و به همین دلیل رمزنگاری کلید عمومی به سختی قابل پیاده‌سازی بوده و به جهت کارایی بالا تمرکز ما بیشتر بر روی رمزنگاری متقارن و بهینه سازی طرح های قطعی ترکیبیاتی می‌باشد[۹-۱۴]. چالش برای یافتن یک روش مؤثر از تولید کلیدها و انتساب آنها در گره‌های حسگر قبل از گسترش در محیط است. مکانیسم‌های پیش‌توزیع کلید در *DSNs* می‌توانند به سه دیدگاه زیر طبقه‌بندی شود[۱۴]: ۱) احتمالی ۲) قطعی ۳) هیبرید. در راه‌حل‌های قطعی، فرایندهای قطعی برای طراحی استخرکلید و حلقه‌های کلید، به منظور ایجاد اتصال بهتر کلید، مورد استفاده قرار می‌گیرند و با پیش‌توزیع کلید مبتنی بر طراحی ترکیبیاتی که یک نوع قطعی از انتساب کلید است، احتمال کشف کلید مشترک در طول گره‌های حسگر می‌تواند افزایش یابد. در طرح ما، از تئوری ترکیبیات برای افزایش اتصال بهره برده می‌شود [۱۵-۱۷]. یک ساختار ریاضی بنام طرح بلوک ناقص بالانس شده[۸](*BIBD*) برای ساخت حلقه‌های کلید مورد استفاده قرار می‌گیرد. *BIBD* یک سیستم مجموعه‌ای با پنج پارامتر (v,b,r,k,λ) می‌باشد. با طراحی مناسب *BIBD*، می‌توان از اتصال مناسب طرح توزیع کلید اطمینان حاصل نمود.این طرح از صفحه‌تصویری متناهی رتبه n (برای عدد اول n یا توان اول[۹]n) برای تولید یک طراحی متقارن (یا *BIBD*متقارن) با پارامترهای $(n^2+n+1,n^2+n+1,n+1,n+1,1)$ استفاده می‌کند[۱۵]. از معایب این طرح این است که پارامتر n باید عدد اول یا یک توان اول باشد، از این رو اندازه شبکه حسگر نمی‌تواند برای یک اندازه دلخواه حلقه کلید یا به تعداد دلخواهی حسگر پشتیبانی شوند. راه‌حل‌های مختلفی برای مقابله با این محدودیت ارائه شده‌اند که ضمن بررسی آنها، ما نیز مدلی را با ایجاد زیرساخت مجازی در شبکه بر اساس کپی و تبادل کلید جایگشتی[۱۰](*PKCAE*) با مجموعه غالب (احاطه‌گر) معرفی خواهیم کرد و به ارزیابی و مقایسه این مدل با طرح‌های قبلی خواهیم پرداخت و نشان خواهیم داد که مدل ما از نظر پارامترهای ارزیابی کارایی شبکه بهینه‌تر می‌باشد.

ادامه ساختار این مقاله به شرح زیر سازمان یافته است: در بخش دوم، پیش توزیع کلید با طراحی ترکیبیاتی و فرایندهای قطعی بحث خواهد شد. در بخش سوم، طرح پیشنهادی ما تحت عنوان کپی و تبادل کلید جایگشتی مبتنی‌بر مجموعه‌های غالب همبند ضعیف مطرح خواهد شد. در بخش چهارم، ارزیابی کارایی و مقایسه طرح ها با پارامترهای احتمال وجود کلید مشترک و میانگین طول مسیر کلید انجام خواهد شد. نهایتاً در بخش پنجم، نتیجه‌گیری را خواهیم داشت.

پیش‌توزیع کلید با طراحی ترکیبیاتی[۱۱]

تعریف ۱: یک سیستم مجموعه‌ای یا طراحی را با $(\chi,\mathcal{A})$ نشان می‌دهیم که در آن χ شامل مجموعه‌ای از نقاط یا اعضای $X\in\chi$ بوده و $\mathcal{A}$ یک مجموعه متناهی از زیر مجموعه‌های χ که بلوک نامیده می‌شود، می‌باشد. درجه یک عضو $X\in\chi$ با تعداد بلوک‌هایی که شامل X هستند مشخص می‌شود. $(\chi,\mathcal{A})$ را از درجه r و با قاعده گویند اگر همه اعضا درجه یکسان r داشته باشند. رتبه[۱۲] $(\chi,\mathcal{A})$ اندازه بزرگترین بلوک است و اگر همه بلوک‌ها هم اندازه باشند آنگاه $(\chi,\mathcal{A})$ را یک ریخت از رتبه k گویند.

مثال ۱: فرض کنید؛ $\chi=\{1,2,3,4,5,6,7,8,9\}$ و $\mathcal{A}=\{123,456,789,147,258,369,159,267,348,168,249,357\}$ باشند آنگاه $(\chi,\mathcal{A})$ یک سیستم مجموعه‌ای با ۹ عضو و ۱۲ بلوک است. این سیستم با قاعده از درجه ۴ و یک ریخت با رتبه ۳ می‌باشد. این سیستم‌های مجموعه‌ای می‌توانند در طرح پیش‌توزیع کلید مورد استفاده واقع شوند یعنی تعداد کلیدها را با $\chi=\{X_i : 1 \le i \le v\}$ و تعداد گره‌ها را با $\mathcal{A}=\{A_j : 1 \le j \le b\}$ نشان می‌دهیم. پس در حالت کلی، v عددکلید و b عدد حسگر داریم و گره‌های حسگر را با $N_1, N_2, \dots, N_b$ نشان می‌دهیم. برای هر گره N_j یک زیر مجموعه از کلیدهای $\mathcal{L}=\{L_i : X_i\in A_j\}$ که فضای حلقه کلید نامیده می‌شود، به تعداد ثابتی از گره‌ها انتساب می‌شوند. پس در مثال ۱ به تعداد $v = ۹$ عدد کلید و $b = ۱۲$ عدد گره داریم که به هر گره $k = ۳$عدد کلید اختصاص یافته است و هر کلید در $r = ۴$ عدد بلوک تکرار شده است.

تعریف ۲: به سیستم مجموعه‌ای فوق، (v,b,r,k)-*design*گویند که در آن $|\chi| = v$ و $|\mathcal{A}| = b$ ، r و k هم بترتیب درجه و رتبه را نشان می‌دهند. از این پس روی سیستم‌های مجموعه‌ای با قاعده و یک ریخت صحبت خواهیم کرد. شرط کافی برای اینکه یک (v,b,r,k)-*design* داشته باشیم $bk = vr$ می‌باشد[۱۷]. در نتیجه با برقراری شرط فوق، طراحی مثال ۱ را می توان بصورت $(9,12,4,3)$-*design* نمایش داد.

---

[۸] Balanced Incomplete Block Design

[۹] Prime Power

[۱۰] Permutation Key Copying And Exchanging

[۱۱] Combinatorial Designs

[۱۲] Rank

ارتباطات تک‌گامی[۱۳] در محدوده برد رادیویی

دو گره همسایه N_i و N_j در صورتی که دارای کلیدهای مشترک $\{A_i \cap A_j\} \neq \emptyset L \in$ باشند، می‌توانند هر کلید مشترک را جهت برقراری ارتباط محلی یا تک‌گامی انتخاب کنند. دو گره N_i و N_j اشتراک کلید دارند اگر و تنها اگر A_i و A_j در ماتریس مجاورت($G_{\mathcal{A}}$) وزن ۱ داشته باشند.

لم ۱: هر رأس A_j در $G_{\mathcal{A}}$ در یک سیستم مجموعه‌ای $(\chi,\mathcal{A})$ از (v,b,r,k)-*design* ، درجه $k(r-1)$ دارد. و یا همه بلوک ها در $G_{\mathcal{A}}$ درجه $k(r-1)$ دارند اگر و تنها اگر $|A_i \cap A_j| \leq 1$ باشد و $\mathcal{A}; i \neq j \in \forall A_i, A_j$ [۱۷].

تعریف ۳: یک (v,b,r,k)-*design* را (v,b,r,k,λ)-*BIBD* گوییم هرگاه هر جفت از اعضا دو به دو با هم در λ بلوک ظاهر شوند.

مثال ۲: در مثال ۱ برای هر جفت از اعضای (1,2)، (1,3)، ...، (9,8) دقیقاً یک بلوک داریم یعنی $\lambda=1$ خواهد بود، پس طراحی به صورت $(9,12,4,3,1)$-*BIBD* خواهد بود.

لم ۲: یک (v,b,r,k,λ)-*BIBD* وجود دارد اگر شرایط $\lambda(v-1) = r(k-1)$ و $bk = vr$، $b \geq v$ با هم برقرار باشند.

یک *BIBD* زمانی *BIBD* متقارن یا طراحی متقارن[۱۴] نامیده می شود که $b = v$ و در نتیجه $k = r$ باشد. در اینصورت (*SBIBD*) نامیده شده و با (v,k,λ)-*SB* نشان داده می شود[۱۷].

تعریف ۴: $(n^2+n+1,1)$-*BIBD* یا 2-$(n^2+n+1, n^2+n+1,n+1,n+1,1)$ را صفحه‌تصویری[۱۵] گویند و بیشترین و بهینه‌ترین ارتباطات محلی را تضمین می‌کند. این طرح از صفحه تصویری متناهی مرتبه n، برای عدد اول n یا توان اول n برای تولید یک طراحی متقارن (*SBIBD*)[۱۶] با پارامترهای فوق استفاده می‌کند یعنی n^2+n+1 گره را پشتیبانی می‌کند و از استخر کلید با اندازه n^2+n+1 استفاده می‌کند. این طرح n^2+n+1 حلقه کلید را با اندازه $n+1$ تولید می‌کند به طوری که هر جفت از حلقه‌های کلید، دقیقاً یک کلید مشترک دارند، و هر کلید دقیقاً در $n+1$ حلقه کلید ظاهر می‌شود. پس از گسترش، هر جفت از گره‌ها دقیقاً یک کلید مشترک را پیدا می‌کنند. از این رو، احتمال کلید مشترک در طول یک جفت گره حسگر برابر ۱ است. احتمال اینکه پس از تسخیر یک گره حسگر، یک لینک کشف رمز شود، $\approx 1/n$ است. در طرح صفحه تصویری، تعداد کلیدهای هر گره حداقل به بزرگی ریشه دوم (رادیکال) تعداد گره‌ها است.

قضیه ۱: فرض کنید که q یک عدد اول باشد. آنگاه یک طرح پیش‌توزیع کلید صفحه‌تصویری با $q^2 + q + 1$ گره و $q + 1$ کلید برای *DSN* وجود دارد و برای هر دو گره دقیقاً یک کلید مشترک خواهد بود[۱۷].

طرح قضیه ۱ برای شبکه‌های کوچک مؤثر است ولی در شبکه‌های بزرگ با مشکل محدودیت حافظه مواجه می‌باشد.

مثال ۳: قرار می‌دهیم $q = ۳۱$، در این صورت تعداد گره‌ها ۹۹۳ عدد خواهد بود که به هر گره ۳۲ کلید می‌رسد. حال اگر شبکه ۲۰۰۰۰ گره داشته باشد، عدد اول q با شرط $q^2 + q + 1 \geq ۲۰۰۰۰$ عدد $q = ۱۴۹$ بدست می آید و انتساب $q + 1 = ۱۵۰$ کلید توسط طرح *KPS* به هر گره از نظر عملی غیر ممکن است.

محدودیت‌های *BIBD*

عیب اول این مدل این است که برای شبکه‌های کوچک مؤثر است ولی در شبکه‌های بزرگ با مشکل محدودیت حافظه مواجه می‌باشد. مثال ۳ از بخش قبلی این محدودیت را نشان می‌دهد. عیب دوم این مدل این است که پارامتر n باید یک عدد اول یا توان اول باشد، از این رو تمام اندازه‌های شبکه حسگر نمی‌توانند برای یک اندازه حلقه کلید دلخواه یا اندازه شبکه دلخواه پشتیبانی شوند. دو راه حل برای اصلاح معایب فوق ارائه شده اند: ۱- مربعات تعمیم یافته[۱۷] (*GQ*) ۲- طرح هیبرید.

مربعات تعمیم یافته(*GQ*)[۱۸]: مربعات تعمیم یافته، یک ساختار انتشار S-(P,B,I) است که P و B گسسته و به ترتیب دسته‌هایی از خطوط و نقاط غیرتهی هستند و I نیز یک رابطه انتشار خط- نقطه متقارن است که از اصل زیر پیروی می‌کند:

(۱) هر نقطه به $t+1$ خط وابسته است $(t \geq 1)$ و دو نقطه مشخص با حداکثر یک خط روی می‌دهند. (۲) هر خط به $s+1$ نقطه $(s \geq 1)$ وابسته است و دو خط مشخص با حداکثر یک نقطه روی می دهند. (۳) اگر x یک نقطه و L یک خط باشد و I به x وابسته نباشد، یک جفت منحصر به فرد $(y,M) \in P \times B$ وجود دارد که x را به L وابسته می‌کند.

طراحی‌های GQ پیشنهادی، $GQ(n,n)$، $GQ(n,n^2)$ و $GQ(n^2,n^3)$ اندازه‌های شبکه از رتبه $O(n^5)$ و $O(n^4)$ در اندازه حلقه کلید را پشتیبانی می‌کنند و به ترتیب احتمال کلید مشترک $\approx 1/n$، $\approx 1/n^2$ و $\approx 1/n^{1.5}$ را فراهم می‌کند[۱۵]. پارامتر n همچنان باید یک توان اول باشد.

طرح هیبرید[۱۵]: بزرگترین عامل اول n به طوری که $k \leq K$ را یافته و N بلوک با اندازه k تولید می‌کند در واقع کلیدها از گروه کلید S با اندازه $|S| = v$ می‌آیند. تعداد b از بلوک N با استفاده از طراحی متقارن پایه یا GQ تولید می‌شود و $N - b$ بلوک به طور تصادفی از k زیر مجموعه از بلوک‌های طراحی متمم انتخاب

---

[۱۳] One-hop

[۱۴] Symmetric Design

[۱۵] Projective Plane

[۱۶] Symmetric BIBD

[۱۷] Generalized Quadrangles

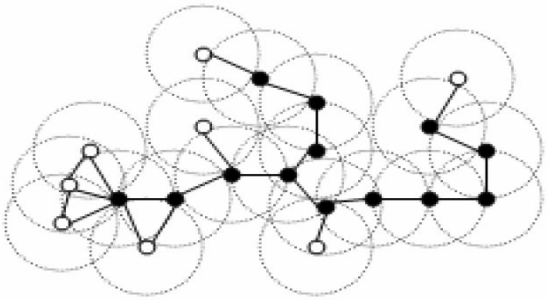
می‌شوند. احتمال دارد بین دو حسگر، کلید مشترک وجود نداشته باشد.

طرح پیشنهادی (*PKCAE*)

تعریف ۱: مجموعه‌ای چون S از رأس‌های گراف $G = (V,E)$ یک مجموعه غالب[۱۸] نامیده می‌شود هرگاه رأس $v \in V$ رأسی از S یا مجاور با یکی از اعضای S باشد. توجه کنید که اگر S مجموعه غالب گراف G باشد، هر زِبَر مجموعه[۱۹] $S' \supseteq S$ نیز مجموعه غالب G است در حالی که لزوماً هر زیر مجموعه $S'' \subseteq S$ مجموعه غالب نیست[۲۰,۱۹].

تعریف ۲: مجموعه غالب همبند[۲۰] (CDS)، S، از گراف G، مجموعه‌ای است که هم غالب باشد و هم زیرگراف القایی حاصل از آن همبند باشد[۲۰,۱۹].

مثال ۱: شکل ۱ استقرار زیرساخت مجازی با مجموعه غالب همبند (CDS) را در یک شبکه حسگر بی‌سیم توزیع شده نوعی (DSN) با استفاده از *Unit Disk Graph* [۲۱] نشان می‌دهد.



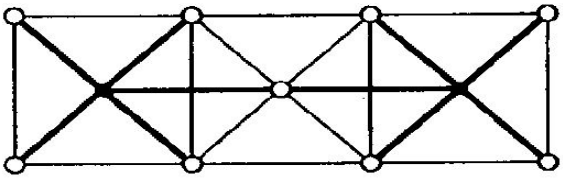
شکل ۱. ساختار زیرساخت مجازی با مجموعه غالب همبند در DSN[۱۹]

مجموعه‌های غالب کاربردهای بسیاری در مهندسی، نظریه شبکه‌ها، مسیریابی، پخش همگانی در شبکه و ... دارند.

تعریف ۳: برای یک زیر مجموعه S از رئوس گراف، زیرگراف به طور ضعیف القا شده از S، گراف $<S>_w = (N[S],E_w)$ است که در آن E_w شامل مجموعه تمام یال‌هایی است که حداقل یک رأسشان در S باشد. حال مجموعه غالب همبند ضعیف به صورت زیر تعریف می شود:

تعریف ۴: مجموعه S یک مجموعه غالب همبند ضعیف[۲۱] $(WCDS)$ از G است اگر S غالب باشد و $<S>_w$ همبند باشد.

رأس‌های تیره در شکل ۲ یک مجموعه غالب همبند ضعیف، و یال های پررنگ زیرگراف به طور ضعیف القا شده از آن را نشان می‌دهند.



شکل ۲. مجموعه غالب همبند ضعیف [۱۹]

یک روش برای ساختن مجموعه غالب همبند، استفاده از مجموعه های غالب همبند ضعیف است.

طرح ما یک روش کارا و امن کنترل توپولوژی[۲۲] و پیش‌توزیع کلید قطعی با کپی و تبادل کلید جایگشتی[۲۲] $(PKCAE)$ با ایجاد یک شاهراه ارتباطی یا زیرساخت مجازی با مفهوم مجموعه غالب همبند ضعیف برای شبکه‌های حسگر بی‌سیم توزیع شده را پیشنهاد می‌کند. هدف ما اطمینان یافتن از امنیت و بهبود معایب طرح $BIBD$ در شبکه است که منظور ما از ارتقاء امنیت این است که یک مجموعه کوچک از گره‌های غالب می‌توانند کل شبکه را بطور ایمن پوشش دهند و مسیریابی امن را فراهم کنند. برای شکل‌دهی یک شبکه ایمن ما یک عملیات دو مرحله‌ای را در شبکه بکار می‌گیریم:

۱- کپی کلید ۲- تبادل کلید جایگشتی.

کپی کلید

حسگرها در شبکه، حلقه کلید خود را از مدل پیش‌توزیع کلید صفحه تصویری دریافت می‌کنند. ما کل مجموعه حسگر های V را به سه زیرمجموعه (V_1,V_2,V_3) تقسیم می‌کنیم که V_1 شامل گروه حسگرهای غالب[۲۳] (DG) و V_2 شامل گروه حسگرهای مغلوب (احاطه شده)[۲۴] (DS) و V_3 شامل گروه حسگرهای واسطه می‌باشند.

فرض ۱: گره‌های خالی شامل یک کلید نشست تصادفی هستند که از طریق آن با DGهای در برد رادیویی خود (DG_{1hop}) ارتباط برقرار کرده و کلیدهایش را از آن می‌گیرد و یا DG_{1hop} به آن گره خالی، کلید کپی می‌کند.

فرض ۲: گره‌های غالب شامل $n+1$ کلید هستند و می‌توانند برای کپی کلید در گره‌های خالی داخل گروه خود از حسگرهای غالب همسایه خود نیز استفاده کنند.

[۱۸] Dominating Set

[۱۹] Super Set

[۲۰] Connected Dominating Set

[۲۱] Weakly Connected Dominating Set

[۲۲] Permutation Key Copying And Exchanging

[۲۳] Dominators Group

[۲۴] Dominated Sensors

فرض ۳: تعداد گره‌های یک گروه (η) بر حسب تعیین اولیه می‌باشد و η در واقع بیشینه درجه DGها در هر گروه است؛ در واقع $\eta = (\Delta(DG_i))$

فرض ۴: در $WCDS$، حسگرهای واسطه مابین حسگرهای غالب قرار دارند و ارتباط بین غالب‌ها را برقرار می‌سازند و نمی‌توانند برای خود گروهی از حسگرهای مغلوب را داشته باشند.

شکل‌گیری شبکه[۲۵]

بعد از تعیین تعداد حسگرهای غالب و مقدار η برای هر گروه، یک پیش‌توزیع کلید با طرح $BIBD$-$(n+1,\ n^2+n+1,n+1,n+1,1)$ انجام می‌گیرد و در صورتی که تعداد حسگرها را بطور دلخواه انتخاب کنیم و پارامتر آن را با n' نشان دهیم یعنی مقیاس شبکه را بالا ببریم آنگاه کوچک ترین n نزدیک به n' را بدست آورده $(n \le n')$ و صفحه تصویری فوق را تشکیل می دهیم. صفحه تصویری با پارامتر $n = 2$ را در شکل ۳ نشان داده‌ایم. گره‌های خالی را فقط با یک کلید نشست تصادفی یا دلخواه، در محیط توزیع می‌کنیم:

۱- هر گره خالی سعی می‌کند با ارسال یک بسته رمزگذاری شده درخواست اتصال به گروه، DG_{1hop} خود را بیابد. DG_{1hop} نیز با پاسخ دادن به این درخواست بصورت رمزگذاری شده، کلیدهای آن را ارسال کرده و آن گره را عضو گروه خود می‌کند. کلیدهای ارسال شده، تا حد امکان دارای کلید رمزنگاری مشترک متفاوتی نسبت به اعضای گروه هستند و DG_{1hop} حلقه کلید را از غالب‌های همسایه درخواست می‌کند.

۲- در برخی از مواقع ممکن است گره خالی با گره غالب خود (DG_{1hop})، کلید مشترک نداشته باشد، در این صورت گره غالب بسته دریافتی را به غالب همسایه خود (DG_n) به همراه شناسه یکی از کلیدهای خود که استفاده نشده است و یا کمتر استفاده می‌شود را ارسال می‌کند بدین ترتیب آن گره غالب در صورتی که کلید مشترک با گره خالی را داشته باشد، در پاسخ، حلقه کلید متناسب با درخواست (DG_{1hop}) را با کلید گره خالی رمزگذاری کرده و به (DG_{1hop}) ارسال می‌کند و آن هم به گره خالی می‌فرستد بدین ترتیب کلید مشترک گره خالی با غالب خود بدست می‌آید، ولی اگر غالب همسایه هم کلید مشترک با گره خالی نداشته باشد، آن غالب نیز بسته دریافتی را به غالب همسایه خود ارسال می‌کند و با تکرار مراحل فوق، کلید مشترک بدست می‌آید زیرا کلیدهای نشست تصادفی از جنس کلیدهای طرح صفحه‌تصویری انتخاب شده‌اند و احتمال وجود کلید مشترک در شبکه همیشه ۱ است.

تبادل کلید

حال فرض کنیم تعداد گره‌های شبکه بسیار زیاد باشند و فضای ذخیره‌سازی کلید بسیار محدود باشد، یعنی این بار تعداد کلیدها و حلقه کلید را بطور دلخواه و محدود انتخاب کرده باشیم در این صورت بر اساس تعداد کلیدهای موجود که آن را با پارامتر n'' نشان داده‌ایم، کوچک‌ترین n نزدیک به n'' را بدست آورده$(n \le n'')$ و صفحه‌تصویری $(n^2+n+1,\ n^2+n+1,n+1,n+1,1)$-$BIBD$ را تشکیل می‌دهیم.

شکل‌گیری شبکه

برای افزایش ضریب امنیتی شبکه با تعداد کلیدهای محدود و مقابله با حمله کشف رمز، پس از گسترش حسگرها در محیط و انجام مراحل کپی کلید، DGها در یک بازه زمانی مشخص[۲۶]، حلقه کلید خود را بین هم تعویض می‌کنند. چون از صفحات تصویری برای پیش‌توزیع کلید استفاده شده بود پس به طور قطعی، غالب‌ها با همه حسگرهای گروهشان کلید مشترک خواهند داشت با این تفاوت که این کلید مشترک دیگر همان کلید استفاده شده قبل از تبادل کلید نخواهد بود. جایگشت حلقه‌های کلید بصورت تصادفی انجام می‌گیرد یعنی گره‌های غالب یک جایگشت از $|DG|!$ تا جایگشت را اجرا می‌کنند. در شکل ۴ تبادل کلید را نشان داده‌ایم.شبه کد برای این الگوریتم در شکل ۵ نشان داده شده است. ممکن است به علت توزیع تصادفی حسگرها در محیط، برخی از DSها نتوانند در برد رادیویی DGها قرار بگیرند در این صورت به آنها مجوز غالب شدن را خواهیم داد یعنی اگر گره‌ای نتواند حداقل با یک DG ارتباط برقرار کند آنگاه با ارسال یک پیام خطا از DSهای اطرافش درخواست کمک می‌کند که بدین ترتیب یک DS بطور موقت به عنوان واسطه و با ارتباط چندگامی، پیام خطای دریافت کرده‌اش را به DG خود تکرار می‌کند و این DG است که تصمیم می‌گیرد که آیا آن گره صلاحیت اخذ مجوز غالب شدن را دارد یا نه، که در صورت پذیرفته شدن، تعداد مجموعه غالب افزایش خواهد یافت یعنی گره واسطه به همراه گرهی که پیام خطا ارسال کرده بود به ترتیب حسگر واسطه و حسگر غالب خواهند شد و مرحله کپی کلید انجام خواهد شد و به دنبال آن مرحله تبادل کلید را خواهیم داشت.

[۲۵] Network Formation

[۲۶] Threshold

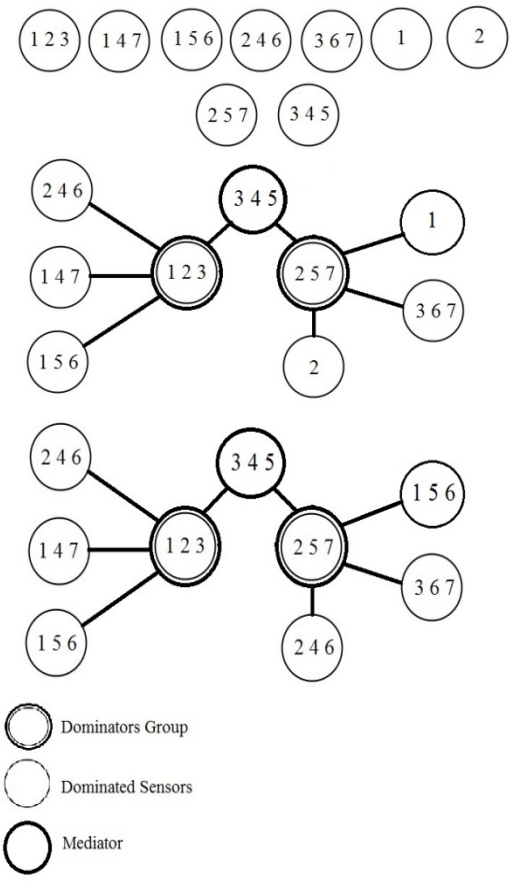
ارزیابی کارایی و مقایسه

در طرح ما با توجه به شبیه‌سازی‌هایی کـه انجـام داده‌ایـم، وجـود کلید مشترک را با توجه به مقدار حافظه دلخـواه و تعـداد دلخـواه حسگر، با احتمال ۱ فراهم کرده‌ایم و با مکانیسم تبادل کلید سعی کرده‌ایم از کشف الگوی پیام‌هـای مبادلـه شـده توسـط حملـه‌گـر جلوگیری به عمل آوریم.

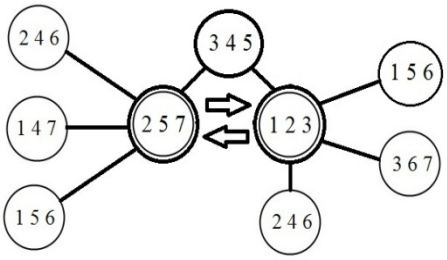
جدول ۱ نتایج محاسبات: ۱- احتمـال وجـود کلیـد مشـترک[۲۷] را بازای هر دو بلوک دلخواه و ۲- میانگین طول مسیر کلیـد[۲۸] بـرای کشـف کلیـد مشـترک، را بطـور خلاصـه بـرای طـرح *PKCAE* و طرح‌های *GQ* و هیبرید نشان می‌دهد. واضـح اسـت بعلـت اینکـه طرح *PKCAE* طراحی صفحات تصویری را بکار می‌گیرد، احتمـال وجود کلید مشترک در شبکه همیشه ۱ بوده و چون *DS*ها تنها در یک گام با *DG*های خود و زیرساخت شبکه در ارتباط هستند پس طول مسیر کلید و به مراتب آن طول مسیر ارسال پیام‌های *DS*هـا به زیرساخت شبکه فقط در یـک‌گـام مـی‌باشـد و ایـن زیرسـاخت مجازی شبکه است که مسئول تحویل بسته‌ها به تمـامی *DS*هـای شبکه است و ممکن است *DS*ها بـه هنگـام انتظـار بـرای دریافـت پاسخ از *DG*ها جهت صرفه‌جویی در مصرف انرژی به حالت خواب بروند.

در اندازه شبکه‌ای که با عدد اول یا توان اول n بدست آمده اسـت، طراحی متقارن، شبیه به طـرح مـا عمـل مـی‌کنـد ولـی در سـایر اندازه‌ها طرح *PKCAE* بهترین حالت را دارد. اندازه حافظه موجـود برای هر حسگر در ستون- اندازه حلقـه کلیـد[۲۹] - مشـخص شـده است. عدد موجود در ستون - میانگین مسیر کلید - متوسط تعداد گام‌هایی را نشان می‌دهد که دو حسگر نیاز دارند تا کلید مشـترک خود را بیابند. در جـدول ۱ طـرح *PKCAE* بـا سـایر طـرح‌هـا در شرایط یکسان مقایسه شده است که مقادیر آورده شده در جـدول ۱ از [۱۵] استخراج شده‌اند.

طرح ما اطمینان می‌دهد که یک زیرساخت مجازی توسط *WCDS* ساخته می‌شود که مسئول امنیت و مسیریابی شبکه است و تعـداد مناسب غالب‌ها استحکام شبکه را تأمین می‌کنند و نیـز از همـان اول شروع به کار شبکه پیام‌های رمزنگاری شده ارسـال و دریافـت می‌شوند. طـرح مـا بـه خـوبی در مقابـل انـواع حمـلات رایـج در شبکه‌های حسگر بی‌سیم مقاومت نشان می‌دهد زیرا بـا جایگشـت پی در پی کلیـدهای رمزنگـاری کشـف رمـز پیـام‌هـا بـه حـداقل می‌رسد. برای جلوگیری از ازدحام در زیرساخت شبکه می‌تـوان از تکنیک‌های موازنه بار بین *DG*ها استفاده کرد. در واقـع بایـد بـین اندازه مجموعه غالب و مقدار η یک موازنه یا تعادل برقرار شود.



شکل ۳. پیش‌توزیع کلید با صفحه‌تصویری و کپی کلید با ۹ حسگر با پارامتر n= ۲



شکل ۴. تبادل کلید بین دو *DG*

[۲۷] Common Key Probability

[۲۸] Average Path Key

[۲۹] Key Pool Size

```
Let,
enc_k(.) – message encrypted by secret key of k
enc_un(.) – message encrypted by an unknown secret key
dec_k(.) – message decrypted by secret key of k
dec_un(.) – message decrypted by an another DG_i with multi hop transmission
DS_j – set of dominated sensors
DG_1hop – dominators group with in one hop transmission range
DG_n – neighbor dominators group
brc(.) – broadcast message with in one hop transmission range
ℒ – key ring
t – number of successful communications between DG_1hop and DS_j
perm – permutation function for DGs key ring

#step 1: key copy
for each DS_j ∈ V_2
        brc(enc_k(Join_REQ))
                if dec_k(Join_REQ) from DG_1hop
    then DG_1hop send enc_k(ℒ)
         DG_1hop send enc_ℒi(Join_APRV)
         DS_j send enc_ℒi(ACK)
      else
    floodenc_un(Join_REQ) from DG_1hop
    end if
      for each DG_n
 ifdec_un(Join_REQ) from DG_n
 then M ←enc_un(ℒ) from DG_n
       DG_n send M to DG_1hop
        DG_1hop send M to DS_j
    end if
  end for
end for
#step 2: key exchange
if t ≥ threshold
thenbrc(key_EXCHANGE)
perm (ℒ_DGi)
end if
```

شکل۵. شبه کد کپی و تبادل کلید

جدول ۱. مقایسه *PKCAE* با طرح های متقارن، *GQ* و هیبرید

طراحی	سایز حلقه کلید	تعداد حسگرها	احتمال کلید مشترک	میانگین مسیر کلید
متقارن	۳	۱۳	۱	۱
	۶	۴۳	۱	۱
	۶	۵۰	قابل اجرا نیست	قابل اجرا نیست
	۱۲	۱۵۷	۱	۱
	۱۸	۳۴۳	۱	۱
	۱۸	۳۸۰	قابل اجرا نیست	قابل اجرا نیست
	۲۴	۵۵۳	۱	۱
	۳۸	۱۴۰۷	۱	۱
	۳۸	۱۵۰۰	قابل اجرا نیست	قابل اجرا نیست
PKCAE	۳	۱۳	۱	۱
	۶	۴۳	۱	۱
	۶	۵۰	۱	۱

PKCAE	۱۲	۱۵۷	۱	۱
	۱۸	۳۴۳	۱	۱
	۱۸	۳۸۰	۱	۱
	۲۴	۵۵۳	۱	۱
	۳۸	۱۴۰۷	۱	۱
	۳۸	۱۵۰۰	۱	۱

طراحی	سایز حلقه کلید	تعداد حسگرها	احتمال کلید مشترک	میانگین مسیر کلید
GQ(q,q)	۶	۱۵۶	۰.۱۹۲	۲.۵۳
	۸	۴۰۰	۰.۱۴۰	۳.۴۹
	۱۲	۱۴۶۴	۰.۰۹۰	۲.۷۱
	۱۴	۲۳۸۰	۰.۰۷۶	۳.۱۸
	۱۸	۵۲۲۰	۰.۰۵۸	۲.۸۸
	۲۰	۷۲۴۰	۰.۰۵۲	۲.۶۹
PKCAE	۶	۱۵۶	۱	۱
	۸	۴۰۰	۱	۱
	۱۲	۱۴۶۴	۱	۱
	۱۴	۲۳۸۰	۱	۱
	۱۸	۵۲۲۰	۱	۱
	۲۰	۷۲۴۰	۱	۱

طراحی	سایز حلقه کلید	تعداد حسگرها	احتمال کلید مشترک	میانگین مسیر کلید
$GQ(q, q^2)$	۳	۴۵	۰.۲۶۶	۲.۱۴
	۴	۲۸۰	۰.۱۲۸	۵.۴۹
	۶	۳۲۷۶	۰.۰۴۵	۳.۲۲
	۸	۱۷۲۰۰	۰.۰۲۲	۲.۹۶
PKCAE	۳	۴۵	۱	۱
	۴	۲۸۰	۱	۱
	۶	۳۲۷۶	۱	۱
	۸	۱۷۲۰۰	۱	۱

طراحی	سایز حلقه کلید	تعداد حسگرها	احتمال کلید مشترک	میانگین مسیر کلید
$GQ(q^2, q^3)$	۵	۲۹۷	۰.۱۳۴۷	۲.۶۹
	۱۰	۶۸۳۲	۰.۰۳۹۵	۲.۶۸
PKCAE	۵	۲۹۷	۱	۱
	۱۰	۶۸۳۲	۱	۱

طراحی	سایز حلقه کلید	تعداد حسگرها	احتمال کلید مشترک	میانگین مسیر کلید
هیبرید با هسته متقارن	۱۴	۲۵۰	۰.۸۹	۱.۱۴
	۲۴	۷۵۰	۰.۸۹	۱.۱۵
	۳۸	۱۵۰۰	۰.۹۷	۱.۰۴
	۵۴	۳۰۰۰	۰.۹۸	۱.۰۳
	۷۲	۵۲۵۰	۰.۹۹	۱.۰۱
	۱۰۲	۱۰۵۰۰	۰.۹۹	۱.۰۱
PKCAE	۱۴	۲۵۰	۱	۱
	۲۴	۷۵۰	۱	۱
	۳۸	۱۵۰۰	۱	۱
	۵۴	۳۰۰۰	۱	۱
	۷۲	۵۲۵۰	۱	۱
	۱۰۲	۱۰۵۰۰	۱	۱

نتیجه‌گیری

در این مقاله هدف ما آنالیز دیدگاه قطعی و سیستم مجموعه ترکیبیاتی *BIBD* در طراحی پیش‌توزیع کلید برای شبکه‌های حسگر بی‌سیم توزیع‌شده (*DSNs*) بود زیرا مدل‌های مبتنی بر طرح‌های ترکیبیاتی به دلیل برتری‌های تعیین کننده نسبت به مدل‌های احتمالاتی توزیع کلید مورد توجه قرار داده شده‌اند.

بر تعدادی از مشکلات شبکه حسگر بی‌سیم از قبیل مشکلات امنیتی، می‌توان با تکنیک‌های کنترل توپولوژی غلبه کرد یعنی ما به جای استفاده از حداکثر ارتباطات ممکن در یک شبکه، یک انتخاب عمدی برای محدود کردن توپولوژی شبکه با مجموعه‌های غالب را انجام دادیم. کنترل توپولوژی مبتنی بر مجموعه‌های غالب همبند ضعیف را که یکی از روش‌های سلسله مراتبی یا زیرساخت مجازی است برای کاهش افزونگی و سربار ارتباطی به وجود آوردیم که در نتیجه *WCDS* با محدود کردن وظایف اصلی مسیریابی به گره‌های غالب و واسطه‌ها سبب افزایش قابلیت اطمینان و امنیت در شبکه می‌شود.

در این مقاله، با طراحی و پیاده‌سازی یک زیرساخت مجازی توسط مجموعه غالب همبند ضعیف که مسئول توزیع کلید، امنیت، مسیریابی، مقیاس‌پذیری، کنترل توپولوژی و کنترل منابع حسگرهای شبکه است توانستیم نیازهای *DSN* را تأمین کرده و با تعداد مناسب غالب‌ها استحکام و انعطاف‌پذیری شبکه را تضمین کنیم و نیز با ارسال و دریافت پیام‌های رمزنگاری شده با استفاده از پیش‌توزیع قطعی کلیدهای رمزنگاری، در مقابل انواع حملات رایج در شبکه‌های حسگر بی‌سیم مقاومت نشان دهیم و ضمن ارائه یک مدل جدید برای اصلاح معایب صفحات‌تصویری از قبیل: ۱- مشکل محدودیت حافظه، ۲- عدم مقیاس‌پذیری شبکه،۳- محدودیت پارامتر n و ۴- مشکل اندازه حلقه کلید، یک روش کارا برای کنترل توپولوژی شبکه حسگر بی‌سیم بر اساس پیش‌توزیع کلید قطعی با طراحی ترکیبیاتی و کپی و تبادل کلید جایگشتی (*PKCAE*) را با استفاده از مجموعه غالب همبند ضعیف نشان داده و به ارزیابی کارایی طرح با تحلیل‌های اتصال یا احتمال وجود کلید مشترک و قابلیت مقیاس‌پذیری در شبکه نسبت به دو راه‌حل ۱- مربعات تعمیم یافته (*GQ*) و ۲- طرح هیبرید، پرداختیم.

مراجع

[1] G. Wang, G. Cao, T. Porta. *Movement-assisted sensor deployment.* IEEE TRANSACTIONS ON MOBILE COMPUTING, NY, USA, 2004. Vol. 6, No. 6, pp. 1-13.

[2] Y. Zou, K. Chakrabarty. *Sensor deployment and target localization based on virtual forces*. In IEEE INFOCOM, NY, USA, 2003. pp. 1293-1303.

[3] L. Zhou, Z. Haas. *Securing ad hoc networks*. IEEE Network Magazine, NY, USA, 1999. Vol. 13, No. 6, pp. 24-30.

[4] F. Stajano, R. Anderson. *The resurrecting duckling: security issues for ad-hoc wireless networks*. In AT&T software symposium, NJ, USA, 1999. pp. 172-194.

[5] TC. Aysal, KE. Barner. *Sensor data cryptography in wireless sensor networks*. IEEE Transactions on Information Forensics and Security, CA, USA, 2008. Vol. 3, No. 2, pp. 273-289.

[6] VC. Giruka, M. Singhal, J. Royalty, S. Varunasi. *Security in wireless sensor networks*. Wireless Communications and Mobile Computing, USA, 2008. Vol. 8, No. 1, pp. 1-24.

[7] D. Kundur, W. Luh, UN. Okorafor, T. Zourntos. *Security and privacy for distributed multimedia*

sensor networks. Proceedings of the IEEE, NC, USA, 2008. Vol. 96, No. 1, pp. 112-130.

[8] Y. Wang, G. Attebury, B. Ramamurthy. *A survey of security issues in wireless sensor networks*. IEEE commun. Surveys & Tutorials, Winnipeg, Canada, 2006. Vol.8, No. 2, pp. 2-23, second quarter.

[9] H. Lee, YH. Kim, DH. Lee, J. Lim. *Classification of key management schemes for wireless sensor networks*. In The International workshop on Application and Security service in web and Pervasive environments(ASWAN), Egypt, 2007. pp. 664-673.

[10] D-M. Sun, B. He. *Review of key management mechanisms in wireless sensor networks*. Acta Automatica sinica, China, 2006. Vol. 32, No. 6, pp. 6-900.

[11] D. Boyle, T. Newe. *Securing wireless sensor networks: security architectures*. Journal of Networks, USA, 2008. Vol. 3, No. 1, pp. 65-77.

[12] X. Ren, H. Yu. *Security mechanisms for wireless sensor networks*. IJCSNS International Journal of Computer Science and Network security, Seoul, Korea, 2006. Vol. 6, No. 3, pp. 62-155.

[13] Y. Xiao. *Security in distributed, grid, and pervasive computing*. CRC Press, Auerback Publication, USA, 2006.

[14] S.A. Camtepe, B. Yener. *Key Distribution Mechanisms for Wireless Sensor Networks: a Survey*. Technical Report TR-05-07, NY, USA, 2005.

[15] S.A. Camtepe, B. Yener. *Combinatorial design of key distribution mechanisms for wireless sensor networks*. IEEE/ACM Transaction on Networking, NJ, USA, 2007. Vol. 15, No. 2, pp. 346-358.

[16] J. Lee, D.R. Stinson. *On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs*. ACM Transactions on Information and System Security(TISSEC), NY, USA, 2008. Vol. 11, No. 2, pp. 5:1-5:35.

[17] J. Lee, D.R. Stinson. *A Combinatorial Approach to Key Predistribution for Distributed Sensor Networks*. IEEE Wireless Communications and Networking Conference, LA, USA, 2005. Vol. 2, pp. 1200-1205.

[18] JWP. Hirschfeld. *Projective geometries over finite fields*. clarendon press oxford, UK. 1979.

[19] T.W. Haynes, S.T. Hedetniemi, P.J. Slator. *Fundamentals of Domination in Graphs*. MARCEL DEKKER, INC. New York, USA, 1998.

[20] M.R. Garey, D.S. Johnson. *Computers and intractability: A guide to the theory of NP-completeness*. Freeman Publications, San Francisco, USA, 1978.

[21] M.V. Marathe, H. Breu, H.B.H. III, S.S. Ravi, D.J. Rosenkrantz. *Simple heuristics for unit disk graphs Networks*. Networks, USA, 1995. Vol. 25, No. 2, pp. 59-68.

[22] J. He. *Connected Dominating Set Based Topology Control In Wireless Sensor Networks*. Phd Thesis, in the college of Arts and Sciences, Georgia state University, USA, 2012.