



معرفی یک الگوی جدید پیش توزیع کلید مبتنی بر طرح ترکیبیاتی μ - PBIBD در شبکه IoT با منابع محدود

اکبر مرشد اسکی^{۱*}، سید حمید حاج سید جواد^۲

*نویسنده مسئول، دریافت: ۱۳۹۹/۰۹/۲۳، بازنگری: ۱۳۹۹/۰۹/۲۶، پذیرش: ۱۳۹۹/۱۰/۱۰

^۱ استادیار، گروه کامپیوتر، دانشکده فنی و مهندسی، دانشگاه ورامین - پیشوا، دانشگاه آزاد اسلامی، ورامین، تهران، ایران

^۲ استاد، دانشکده ریاضی و علوم کامپیوتر، دانشگاه شاهد، تهران، ایران

چکیده

در شبکه IoT با منابع محدود از گره‌های انتهایی همچون حسگر بی‌سیم، RFID و سیستم‌های نهان استفاده می‌شود که دارای محدودیت حافظه، پردازش و انرژی می‌باشند. یکی از راه‌حل‌های توزیع کلید در این نوع شبکه‌ها، استفاده از روش پیش توزیع کلید است که عمل توزیع کلید را به‌صورت آفلاین قبل از استقرار دستگاه‌های منبع محدود در محیط انجام می‌دهد. همچنین به‌منظور کاهش سربار محاسباتی و ارتباطی کشف کلید مشترک، استفاده از طرح‌های ترکیبیاتی در پیش توزیع کلید به‌عنوان یک راهکار در سال‌های اخیر پیشنهاد شده است. در این مطالعه، به معرفی و ساخت یک طرح ترکیبیاتی از نوع μ - PBIBD پرداخته می‌شود و چگونگی نگاشت این طرح را به‌عنوان الگوی پیش توزیع کلید در شبکه IoT با منابع محدود بیان می‌گردد. با استفاده از این الگوی پیش توزیع کلید، کلیدهای بیشتری برای ارتباط بین دو دستگاه در شبکه IoT حاصل می‌شود. بدین معنی که بین هر دو دستگاه در شبکه حداکثر $q+2$ کلید موجود خواهد بود که در آن q توانی از یک عدد اول است. دو دستگاهی می‌توانند ارتباط امن مستقیم داشته باشند که به‌جای یک کلید مشترک، $q+2$ کلید مشترک در زنجیره کلیدشان داشته باشند که به‌این‌ترتیب باعث افزایش مقاومت الگوی پیش توزیع کلید در آن‌ها نسبت به روش‌های TD، Trade-KP، RD^* ، UKP* و μ - PBIBD 2-D خواهد شد.

کلمات کلیدی: شبکه IoT با منابع محدود، طرح‌های ترکیبیاتی، μ - PBIBD، مقاومت

۱- مقدمه

مفهوم IoT نخستین بار توسط کوین اشتن در سال ۱۹۹۹ بیان گردید که در آن به اشیاء هویت دیجیتال به‌منظور پردازش و تبادل اطلاعات داده شد. شبکه IoT در کاربردهای زیادی از جمله شهر و خانه هوشمند، سلامت و صنعت بکار گرفته شده است [۱].

همچنین در شبکه IoT با منابع محدود از گره‌های بسیار زیادی همچون حسگر بی‌سیم، RFID و سیستم‌های نهان استفاده شده است که این گره‌های دارای محدودیت‌هایی از قبیل حافظه، توان محاسباتی و ارتباطی و انرژی می‌باشند. از ویژگی‌های دیگر این نوع شبکه، وجود تعداد زیادی از گره‌ها در بسیاری از کاربردها است.

توزیع کلید به‌عنوان بخشی مهمی از مدیریت کلید در شبکه IoT است. به عمل توزیع کلید بین دستگاه‌ها قبل از استقرار آنها، پیش توزیع کلید گفته می‌شود و از آنجایی که این عمل به شکل آفلاین صورت می‌گیرد، لذا در مصرف انرژی گره‌ها صرفه‌جویی می‌گردد.

روش‌های پیش توزیع کلید به سه دسته اصلی تصادفی، قطعی و ترکیبی تقسیم می‌شوند [۲]. روش‌های تصادفی پیش توزیع کلید ابتدا توسط اسپنور و گلیگور در [۳] مطرح گردیده است. در روش‌های تصادفی، حلقه‌های کلید دستگاه‌ها، به‌صورت تصادفی از یک مخزن کلید گرفته می‌شود. این عمل توسط یک مرکز توزیع کلید موسوم به KDC انجام می‌شود (فاز پیش توزیع کلید)، پس از این مرحله، دستگاه‌ها با پخش همگانی مشخصه حلقه کلیدهای خود به دستگاه‌های همسایه و بازگشت نتیجه جستجو می‌توانند کلید مشترک بین هر دو دستگاه همسایه را در صورت

هستند. در [۱۹] و [۲۰] الگوی ترکیبیاتی مبتنی بر طرح‌های ماتریسی و چندجمله‌ای با طرح تصادفی EG ارائه شد. همچنین در [۲۱-۲۳] و [۲۰] از الگوهای پیش توزیع کلید ترکیبیاتی مبتنی بر طرح‌های ترکیبیاتی به منظور دستیابی به اتصال پذیری و مقاومت بهتر استفاده کردند.

در این کار یک طرح ترکیبیاتی جدیدی از نوع μ -PBIBD روی طرح متقارن تعریف کرده و با نگاشت آن به پیش توزیع کلید در شبکه IoT با منابع محدود به الگوی پیش توزیع کلیدی دست می‌یابیم که بین هر دو گره آن بیش از یک کلید برای ارتباط وجود دارد. دو دستگاه همسایه در آن می‌توانند دارای ارتباط امن مستقیمی باشند که $q+2$ کلید مشترک بین حلقه کلید خود داشته باشند. بدین ترتیب به الگوی پیش توزیع کلیدی با مقاومت و مقیاس پذیری بالایی دست می‌یابیم.

۲-۱- طرح‌های ترکیبیاتی

اگر X مجموعه از v عنصر متمایز و A یک مجموعه متناهی d عضو موسوم به بلوک، از زیرمجموعه‌های X باشد. به زوج (X, A) یک طرح ترکیبیاتی یا طرح بلوکی گویند. به تعداد بلوک‌های شامل عضو $x \in X$ ، درجه عضو x هستند. اگر تمام اعضای X از درجه r باشند، طرح (X, A) ، منظم نامیده می‌شود. به اندازه بزرگترین بلوک در طرح بلوکی مرتبه گفته می‌شود و در صورتی که تمام بلوک‌ها دارای تعداد اعضای برابر، k ، باشند، آنگاه، این طرح را یکنواخت از مرتبه k نامیده می‌شود. طرحی که در آن $r = k$ و $v = d$ باشد یک طرح متقارن نامیده می‌شود [۲۴].

مثال ۱: زوج (X, A) که در آن

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$A = \{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{1,4,7\}, \{2,5,8\}, \{3,6,9\}, \{1,5,9\}, \{2,6,7\}, \{3,4,8\}, \{1,6,8\}, \{2,4,9\}, \{3,5,7\}\}$$

طرحی است که از ۹ نقطه و ۱۲ بلوک تشکیل شده است. این طرح، منظم از درجه ۴ و یکنواخت از مرتبه ۳ است.

تعریف ۱: به طرح بلوکی (X, A) که در آن هر زوج از عناصر X دقیقاً در λ بلوک از مجموعه A موجود باشند (شرط بالانس بودن)، به آن یک BIBD می‌نامند و با نماد $B(v, d, r, k, \lambda)$ نشان می‌دهند. v و d و r و k و λ پارامترهای BIBD هستند که در رابطه $dk = vr$ و $\lambda(v-1) = r(k-1)$ صدق می‌کنند. به‌ویژه اگر $d=v$ باشد، آنگاه $r=k$ خواهد بود. در این صورت به BIBD حاصل، BIBD متقارن (SBIBD) گفته می‌شود و با نماد $SBIBD(v, r, \lambda)$ نشان داده می‌شود.

قضیه ۱: برای هر توانی از یک عدد اول مانند q که در آن $q \geq 2$ باشد یک SBIBD با پارامترهای $SBIBD(q^2 + q + 1, q, 1)$ وجود دارد. طبقه ساخت این SBIBD در [۲۱] و [۲۵] آورده شده است.

مثال ۲: اگر $V = \{1, 2, 3, 4, 5, 6, 7\}$ و $B = \{B_1, B_2, \dots, B_7\}$ که در آن $B_1 = \{1, 2, 3\}$ ، $B_2 = \{1, 4, 5\}$ ، $B_3 = \{1, 6, 7\}$ ، $B_4 = \{2, 4, 6\}$ ، $B_5 = \{2, 5, 7\}$ ، $B_6 = \{3, 4, 7\}$ و $B_7 = \{3, 5, 6\}$ ، در این صورت یک SBIBD به شکل $SBIBD(7, 3, 1)$ با مقدار $q=2$ خواهیم داشت.

تعریف ۲: در طرح BIBD اگر هر زوج از عناصر X در تعداد متفاوتی از بلوک‌های مجموعه A موجود باشند (شرط بالانس جزئی بودن) به آن یک BIBD جزئی (PBIBD) می‌گویند. به عبارت دیگر مجموعه‌ای مانند $F = \{\lambda_1, \lambda_2, \dots, \lambda_\mu\}$ از اعداد صحیح مثبت باشد که هر زوج از نقاط V در λ_i بلوک برای هر $1 \leq i \leq \mu$ ظاهر شود. در این صورت μ -PBIBD با پارامترهای μ -PBIBD($v, d, r, k, \lambda_1, \lambda_2, \dots, \lambda_\mu$) ظاهر شود. نشان داده می‌شود.

قضیه ۲: اگر $\lambda_1 = \lambda_2 = \dots = \lambda_\mu$ باشد μ -PBIBD به یک BIBD تبدیل می‌شود. مثال ۳: روی مجموعه $X = \{1, 2, 3, 4, 5, 6\}$ با در نظر گرفتن مجموعه بلوک‌های $A = \{\{1, 4, 2, 5\}, \{2, 5, 3, 6\}, \{3, 6, 1, 4\}\}$ یک μ -PBIBD ($6, 3, 2, 4, 1, 2$) به دست می‌آید که در آن $\mu = 2$ است. بدین صورت که این طرح بلوکی ۳ بلوک

وجود پیدا کنند (فاز کشف کلید مشترک) که در صورت وجود این کلید مشترک، دو دستگاه همسایه با استفاده از آن کلید مشترک، ارتباط امن و مستقیم برقرار می‌کنند. همچنین در صورت عدم وجود کلید مشترک بین حلقه کلیدهای دو دستگاه همسایه، این دو دستگاه بایستی از یک مسیر چند پرشی و با استفاده از دستگاه‌های میانی که با گره‌های همسایه کلید مشترک دارند، ارتباط امن غیرمستقیم داشته باشند (فاز کشف مسیر کلید). این روش پس از آن به الگوی EG معروف شد.

روش تصادفی دیگری برای پیش توزیع کلید در [۴]، توسط چان و دیگران موسوم به q - ترکیبی ارائه شد که مقاومت آن نسبت به روش EG بهبود بهتری پیدا کرد. بدین صورت که از یک مخزن کلید کوچک‌تر نسبت به الگوی EG در آن استفاده شد که باعث شد دستگاه‌ها، بیش از یک کلید مشترک مابین خود داشته باشند. دو دستگاهی که q کلید مشترک در حلقه کلیدهای خود داشتند قادر به ارتباط امن و مستقیم بودند. به علاوه آنها نشان دادند که اگر تعداد گره‌های تسخیر شده توسط مهاجم کم باشد مقاومت الگوی q - ترکیبی، بیشتر از طرح EG است. همچنین در [۵]، کیون با استفاده از تابع هش یک الگوی برای KPS ارائه دادند که با استفاده از آن مقاومت بهبود یافت اما در آن تضمینی ارائه نشد که دو دستگاه کلید مشترکی داشته باشند، و لذا بایستی از مسیر چند پرشی برای ارتباط استفاده می‌کردند. در [۶]، لی و دیگران یک آستانه‌ای برای پیش توزیع کلید تصادفی ارائه نمودند که هر دستگاه در آن شبکه، با یک مسیر کلید امن به طول l می‌توانست با دستگاه همسایه دیگر ارتباط برقرار کند. همچنین در [۷]، با استفاده از چند مخزن کلید مجزا، میزان مقاومت در شبکه افزایش دادند.

الگوهای قطعی پیش توزیع کلید به سه دسته ماتریسی و چندجمله‌ای و ترکیبیاتی تقسیم می‌شود. الگوهای ماتریسی و چندجمله‌ای در مقالات [۸-۱۱] مورد بررسی قرار گرفته‌اند اما مشکل عمده در آنها این است که دارای امنیت آستانه‌ای بودند. بدین معنی که با تسخیر t دستگاه تمام ارتباطات در شبکه ناامن می‌شود.

در پیش‌توزیع کلید با استفاده از طرح‌های ترکیبیاتی، به علت استفاده از یک الگوریتم کاملاً مشخص در تولید حلقه‌های کلید، سربار محاسباتی و ارتباطی کشف کلید مشترک کاهش می‌یابد. همچنین میزان اتصال پذیری را می‌توان با انتخاب طرح مناسب، تغییر داده و در عین حال مقاومت مناسبی را برای شبکه IoT فراهم نمود. اولین الگوی پیشنهادی مبتنی بر طرح‌های ترکیبیاتی در [۱۲] مطرح شد که در آن از طرحی ترکیبیاتی موسوم به طرح متقارن استفاده شد. الگوی پیش توزیع کلید پیشنهادی دارای اتصال پذیری کامل بوده، اما از لحاظ مقاومت و مقیاس‌پذیری چندان مطلوب نبوده است. در [۱۳]، لی و دیگران با استفاده از طرح ترکیبیاتی TD الگویی پیش توزیع کلیدی معرفی کردند که مقاومت بهتری را نسبت به طرح متقارن ایجاد می‌کرد. در [۱۴] و [۱۵] طرح‌های ترکیبیاتی دیگری به منظور افزایش مقاومت به کار گرفته شده است. در [۱۶]، بچکیت و دیگران از طرح ترکیبیاتی دیگری موسوم به طرح Unital، به منظور افزایش مقیاس‌پذیری و اتصال پذیری بهتر استفاده کردند. همچنین در [۱۷]، مدیری و دیگران با استفاده از طرح Residual (RD) یک الگوی پیش توزیع کلیدی را ارائه نمودند که در آن میزان مقیاس‌پذیری و اتصال پذیری نسبت به طرح‌های Trade و Unital بهبود داده شد. همچنین در [۱۸]، یان و دیگران، طرحی مبتنی بر طرح ترکیبیاتی μ -PBIBD روی فضای دو بعدی و سه بعدی ارائه داده‌اند و نشان دادند در حالت سه بعدی، این طرح نسبت به طرح ارائه شده در [۱۷] امنیت، بیشتر و اتصال‌پذیری بالاتری دارد علاوه بر آنکه از مقیاس‌پذیری بالایی نیز برخوردار است.

الگوهای پیش توزیع کلید ترکیبی از ترکیب الگوهای قطعی و تصادفی حاصل شده است. این الگوها علاوه بر سودمندی الگوهای تصادفی از لحاظ مقاومت و مقیاس‌پذیری، دارای سودمندی الگوهای قطعی که بیشتر به منظور بهبود اتصال‌پذیری و سربار کمتر کشف کلید مشترک بین دو دستگاه IoT می‌باشد، را دارا

در [۲۳] با توجه به وجود یک SST از نوع $(q^2 + q + 1, q + 1)$ در صورتی که q توانی از یک عدد اول باشد، بلوک‌های $T_1 \cup T_2$ را به‌عنوان زنجیر کلید به دستگاه‌ها اختصاص می‌دهند. و تعداد دستگاه‌های قابل پوشش در این طرح $2(q^2 + q + 1)$ است و هر دستگاه دارای طول زنجیره کلید $q+1$ است. همچنین آنها نشان دادند که، مقاومت طرح ارائه شده از مقاومت الگوهای قطعی قبل مانند SBIBD و طرح TD در [۲۶] و PBIBD در [۱۴] بیشتر است. اما فاقد خاصیت اتصال‌پذیری کامل است.

بچکیت و دیگران در [۱۶]، یک الگوی پیش‌توزیع کلید مبتنی بر طرح Unital ارائه دادند و آن را به‌اختصار NU-KP نامیدند. طرح Unital یک BIBD، با پارامترهای $(q^3 + 1, q^2(q^2 - q + 1), q^2, q + 1, 1)$ است. همچنین به‌منظور افزایش احتمال کلید مشترک و مقاومت طرح آنها یک الگوی پیش‌توزیع کلید موسوم به t-UKP معرفی کردند، که در آن به هر دستگاه، t بلوک متمایز از طرح NU-KP را به‌عنوان زنجیره کلید نسبت دادند و با انتخاب $t = \sqrt{q}$ ، طرح را UKP* نامیدند. با توجه به نتایج ارائه در آن مقاله، هرچند طرح‌های ارائه شده مقیاس‌پذیری بهتری نسبت به SBIBD داشتند، اما از مقاومت کمتری نسبت به آن برخوردار بودند.

مدیری و دیگران در [۱۷]، برای ساخت طرح Residual، از یک SBIBD با پارامترهای $(q^2 + q + 1, q + 1, 1)$ استفاده کردند. بدین صورت که با فرض اینکه بلوک‌های طرح SBIBD ساخته شده $B = \{B_1, B_2, B_3, \dots, B_b\}$ باشد که در آن تعداد بلوکها $b = q^2 + q + 1$ است. در طرح Residual تعداد $b = (q^2 + q + 1)(q^2 + q)$ بلوک به‌صورت $B_{ij} = B_i - B_j$ که در آن $i, j = 1, 2, 3, \dots, b$ است، را می‌سازند. که به‌اختصار آنرا RD نامگذاری کردند و سپس آنها در این مقاله به‌منظور افزایش مقاومت، بلوک‌های تکراری ایجاد شده در این طرح را حذف نمودند و آنرا به‌اختصار RD* نامیدند. و نشان دادند این طرح مقاومت و مقیاس‌پذیری بهتری نسبت به طرح‌های SBIBD و Trade-KP و UKP* دارد. با این حال این طرح نیز فاقد ویژگی اتصال‌پذیری کامل است.

Yuan و دیگران در [۱۸]، با ساخت یک PBIBD $\mu -$ با پارامترهای:

$$\mu - PBIBD(q^2, q^2, 2q - 2, 2q - 2, \lambda_1 = 2, \lambda_2 = q - 2)$$

که از روی یک صفحه دو بعدی ساخته می‌شود طرحی موسوم به $2D \mu -$ SPBIBD معرفی می‌کنند. که دارای خاصیت اتصال‌پذیری کامل بوده اما فاقد مقاومت مناسب نسبت به طرح‌های قبل بودند که با تعریف این طرح روی یک فضای سه بعدی و ساخت یک PBIBD $\mu -$ با پارامترهای:

$$\mu - PBIBD(q^3, q^3, 3q - 3, 3q - 3, \lambda_1 = 0, \lambda_2 = 2, \lambda_3 = q - 2)$$

طرحی موسوم به $3D \mu -$ SPBIBD معرفی می‌کنند که مقاومت آن نسبت به طرح‌های SBIBD، طرح TD در [۲۶]، و طرح RD* در [۱۷] بیشتر بوده اما فاقد خاصیت اتصال‌پذیری کامل بوده است.

۳- مدل پیشنهادی

به‌منظور ساخت طرح ترکیباتی مبتنی بر μ -PBIBD و نگاشت آن به شبکه IoT با اندازه حافظه K کلید، ابتدا توانی از عدد اول q را طوری در نظر می‌گیریم که $2 \leq (q+1) \leq K$. سپس با این q دو SBIBD1 و SBIBD2 با پارامترهای یکسان $(q_1^2 + q_1 + 1, q_1 + 1, 1)$ روی دو مجموعه مجزا X_1 و X_2 می‌سازیم که هر یک از دو مجموعه به‌عنوان مخزن کلید مجزا محسوب می‌شود. حال یک مش دو بعدی با $(q_1^2 + q_1 + 1)^2$ سلول در نظر می‌گیریم که تعداد سطر و ستون آن برابر $q_1^2 + q_1 + 1$ در نظر گرفته شده است. بلوک‌های SBIBD1 را به‌عنوان بخش اول زنجیره کلید به سطرهای مش دو بعدی و بلوک‌های SBIBD2 را به‌عنوان بخش دوم زنجیره کلید به ستون‌های مش دو بعدی نسبت می‌دهیم و در هر سلول اجتماع زنجیره کلید موجود در هر سر و ستون را قرار می‌دهیم. مشابه آنچه که در [۲۷] نشان داده شده است می‌توان به سادگی دید که طرح ترکیباتی حاصل یک $\mu -$

روی مجموعه ۶ عضوی X دارد و هر عضو از X در دو بلوک و هر بلوک ۴ عضو و همچنین هر دو عضو X در ۱ یا ۲ بلوک قرار دارد.

یک طرح Transversal با نماد $TD(k, q)$ نشان داده می‌شود. برای این‌که $TD(k, q)$ قابل ساختن باشد، q باید توانی از یک عدد اول و $2 \leq k \leq q$ در نظر گرفته شود. ابتدا یک مجموعه kq عضوی بنام V ، در نظر گرفته می‌شود. سپس دو مجموعه بنام‌های، مجموعه گروه‌ها و مجموعه بلوک‌ها بدین صورت ساخته می‌شود که مجموعه گروه‌ها یک مجموعه k عضوی از $q -$ زیرمجموعه‌های مجزای V ، است که V را افزای می‌کند و مجموعه بلوک‌ها، یک مجموعه از $k -$ زیرمجموعه‌های مجموعه V در نظر گرفته می‌شود به طوری که

۱- هر بلوک دقیقاً شامل یک عضو از هر گروه باشد.

۲- هر زوج عنصر از دو گروه مختلف دقیقاً در یک بلوک قرار داشته باشند.

$TD(k, q)$ دارای خواص زیر است.

۱- در این طرح تعداد kq نقطه داریم که در q^2 بلوک قرار گرفته‌اند.

۲- هر بلوک دقیقاً k نقطه دارد.

۳- هر نقطه دقیقاً در q بلوک قرار دارد.

مثال ۴: اگر $X = \{1, 2, 3, \dots, 12\}$ باشد یک $TD(4, 3)$ دارای گروه‌هایی مانند زیر

است:

$$G_1 = \{1, 2, 3\}, G_2 = \{4, 5, 6\}, G_3 = \{7, 8, 9\}, G_4 = \{10, 11, 12\}$$

و بلوک‌های آن به‌صورت زیر می‌باشند.

$$\{1, 4, 7, 10\}, \{1, 5, 8, 11\}, \{1, 6, 9, 12\}, \{2, 4, 8, 12\}, \{2, 5, 9, 10\}, \{2, 6, 7, 11\}, \{3, 4, 9, 11\}, \{3, 5, 7, 12\}, \{3, 6, 8, 10\}$$

در [۲۶]، ساخت طرح TD بیان شده است.

۳-۱- ساختار مقاله

سازماندهی مقاله در ادامه بدین صورت است که، ابتدا در بخش ۲ به کارهای مرتبط پرداخته و بعد از آن، در بخش ۳ مدل پیشنهادی مورد نظرمان را معرفی می‌نماییم. سپس در بخش‌های ۴ و ۵ به ترتیب به تحلیل و مقایسه کارایی مدل پیشنهادی پرداخته و در نهایت در بخش ۶ نتیجه‌گیری آورده می‌شود.

۲- کارهای مرتبط

چندین الگوی پیش‌توزیع کلید مبتنی بر طرح‌های ترکیباتی وجود دارد. اولین آنها از این نوع، توسط کامتپ و ینر در [۲۱]، ارائه گردیده است که برای پیش‌توزیع کلید از یک SBIBD با پارامترهای $(q^2 + q + 1, q + 1, 1)$ که در آن q توانی از یک عدد اول است، استفاده کردند و $q^2 + q + 1$ بلوک این طرح را به‌عنوان زنجیره کلید به دستگاه‌ها نسبت دادند. در این الگوی پیش‌توزیع کلید با طول زنجیره کلید $k = q + 1$ ، تعداد $N = q^2 + q + 1$ دستگاه IoT قابل پوشش است. همچنین این الگو دارای خاصیت اتصال‌پذیری کامل بود. بدین معنی که هر دو دستگاه در شبکه، دارای یک کلید مشترک برای ارتباط بودند، اما مقیاس‌پذیری و مقاومت پایینی را داشت. در [۱۵]، Ruj و دیگران یک الگوی پیش‌توزیع کلید موسوم به Trade-KP ارائه نمودند. یک Trade $t(v, k)$ موسوم به bitrade از دو گردایه m عضوی T_1 و T_2 از زیرمجموعه‌های k عضوی از X با v عنصر تشکیل شده‌اند، به طوری که $T_1 \cap T_2 = \emptyset$ و هر زیرمجموعه t عضوی از X دقیقاً در تعداد یکسانی از بلوک‌های T_1 و T_2 قرار دارد. m به‌عنوان اندازه Trade نامیده می‌شود.

یک Trade $t(v, k)$ را از نوع Steiner t گویند، هرگاه هیچ زیرمجموعه t عضوی بیش از یکبار در T_1 یا T_2 ظاهر نشود. و Trade $t(v, k)$ از نوع Strong Steiner Trade یا به‌اختصار SST گویند هرگاه هر بلوک از T_1 یا هر بلوک از T_2 حداکثر در ۲ عضو مشترک باشند. به‌عنوان مثال با فرض اینکه $X = \{1, 2, 3, 4, 5, 6\}$ باشد. $T = \{T_1, T_2\}$ یک Trade $2 - (6, 3)$ از نوع SST است. که در آن

$$T_1 = \{\{1, 2, 3\}, \{1, 5, 6\}, \{2, 4, 6\}, \{3, 4, 5\}\}$$

$$T_2 = \{\{1, 2, 6\}, \{1, 3, 5\}, \{2, 3, 4\}, \{4, 5, 6\}\}$$

$$\frac{\binom{N-(q^2+q+1)}{x}}{\binom{N-2}{x}} \quad (۲)$$

که در آن $N = (q^2 + q + 1)^2$.

بنابراین احتمال لو رفتن یک ارتباط در شبکه، در صورت تسخیر X دستگاه برابر

$$Res(x) = 1 - \frac{\binom{N-(q^2+q+1)}{x}}{\binom{N-2}{x}} \quad (۳)$$

که در آن $N = (q^2 + q + 1)^2$.

۳-۴- مقیاس پذیری

با توجه به مشخصات مدل پیشنهادی بیان شده در بخش ۳، لذا تعداد دستگاه قابل پوشش توسط آن برابر $N = (q^2 + q + 1)^2$ که طول حلقه کلید هر دستگاه در آن برابر $2(q^2 + q + 1)$ است.

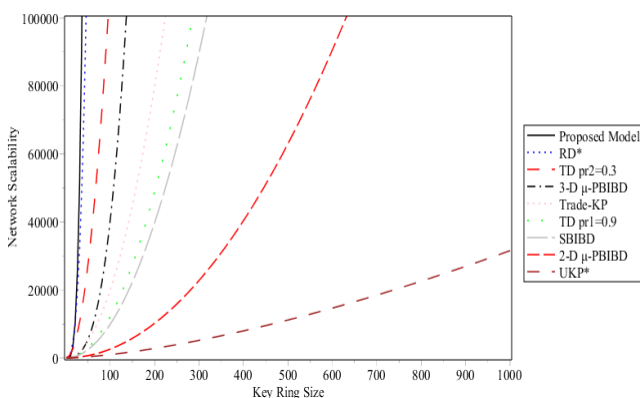
۵- مقایسه کارایی

۵-۱- مقیاس پذیری

جدول ۱ مقیاس پذیری الگوهای پیش توزیع کلید مختلف را با توجه به اندازه حلقه کلید هر طرح بیان می کند.

جدول ۱: پارامترهای طرح های مختلف پیش توزیع کلید			
طرح ترکیباتی	اندازه مخزن	تعداد حلقه های کلید	اندازه حلقه کلید
[۲۱] SBIBD	$q^2 + q + 1$	$q^2 + q + 1$	$q+1$
[۲۶] TD	kq	q^2	k
[۱۶] Trade-KP	$q^2 + q + 1$	$2q^2$	q
[۱۶] t-UKP	$q^3 + 1$	$q^2(q^2 + q + 1) - (t-1)(q^2-1)(q+1)$	$q+1$
[۱۷] RD*	$q^2 + q + 1$	$(q^2 + q + 1)(q + 1)$	q
2-D μ -PBIBD [۱۸]	q^2	q^2	$2q-2$
3-D μ -PBIBD [۱۸]	q^3	q^3	$3q-3$
مدل پیشنهادی	$2(q^2 + q + 1)$	$(q^2 + q + 1)^2$	$2(q+1)$

نمودار زیر که بر اساس مقادیر جدول فوق به ازای طول حلقه کلید، رسم گردیده و نشان دهنده مقیاس پذیری بیشتر مدل پیشنهادی نسبت به تمام طرح های مورد مقایسه است.



شکل ۱: مقایسه مقیاس پذیری الگوهای مختلف پیش توزیع کلید

PBIBD با پارامترهای $(v = 2(q^2 + q + 1), d = (q^2 + q + 1)^2, r = (q + 1)(q^2 + q + 1), k = 2(q + 1), \lambda_1 = (q^2 + q + 1)^2, \lambda_2 = (q + 1)^2)$ است. که بین هر دو بلوک در آن 2 یا $q+2$ کلید مشترک وجود دارد.

در این طرح ترکیباتی $\mu = 2$ است. همچنین این طرح بلوکی، $d = (q^2 + q + 1)^2$ بلوک روی مجموعه $v = 2(q^2 + q + 1)$ عضو X دارد و هر عضو X در $r = (q + 1)(q^2 + q + 1)$ بلوک و هر بلوک $k = 2(q + 1)$ عضو و هر دو عضو X در $\lambda_1 = (q^2 + q + 1)$ یا $\lambda_2 = (q + 1)^2$ بلوک قرار دارد.

۳-۱- نگاشت طرح ترکیباتی مبتنی بر μ -PBIBD به دستگاه های شبکه IoT با منابع محدود

با فرض آنکه هر دستگاه IoT دارای حافظه ای با طول K کلید است، مش دو بعدی در مدل پیشنهادی را مطابق بخش قبل ساخته و در KDC قرار می دهیم. در فاز پیش توزیع کلید در مدل پیشنهادی برای هر دستگاه شبکه، زنجیره کلید موجود در یک سلول از مش دو بعدی توسط KDC به عنوان زنجیره کلید به هر دستگاه نسبت داده می شود که در این انتساب علاوه بر زنجیره کلید، KDC موظف است شناسه ای را برای هر کلید در نظر گرفته و به همراه هر کلید در زنجیره کلید دستگاه ها ذخیره و به هر دستگاه IoT نسبت دهد. در این صورت شبکه ای با اندازه $N = (q^2 + q + 1)^2$ پوشش داده خواهد شد. که بین هر دو دستگاه در آن ۲ یا $q+2$ کلید مشترک وجود دارد. که این مرحله به شکل آفلاین انجام می شود. در فاز کشف کلید مشترک هر دستگاه شناسه های کلید موجود در حلقه کلید خود را به منظور کشف کلید مشترک، بین دستگاه های همسایه پخش همگانی می کند و دو دستگاهی که دارای $q+2$ کلید مشترک باشند، می توانند ارتباط مستقیم و امن برقرار کنند. در غیر این صورت فاز کشف کلید مسیر را اجرا می نمایند. در حقیقت اگر حلقه کلیدهای توزیع شده بین دو دستگاه از یک سطر یا یک ستون یکسان از مش دو بعدی باشد دو دستگاه $q+2$ کلید مشترک خواهند داشت. در فاز کشف مسیر کلید در صورتی که نتوان بین دو گره همسایه برای ارتباط $q+2$ کلید مشترک پیدا نمود. دو دستگاه همسایه از طریق دستگاه های میانی که با آنها $q+2$ کلید مشترک دارند و از طریق یک مسیر چند پرشی ارتباط امن برقرار می کنند. در حقیقت اگر حلقه کلیدهای توزیع شده بین دو دستگاه از سطر و ستون متفاوتی از مش دو بعدی باشند، دو دستگاه تنها ۲ کلید مشترک خواهند داشت. اما دو دستگاه یافت می شود که دارای سطر یکسان با یکی و ستون یکسان با دستگاه دیگر می باشد و لذا با هر یک از دو دستگاه همسایه $q+2$ کلید مشترک دارند. همچنین برای امنیت بیشتر به جای استفاده از $q+2$ کلید برای ارتباط، از hash آنها برای ارتباط استفاده می شود.

۴- تحلیل کارایی

۴-۱- احتمال داشتن $q+2$ کلید مشترک

$$pro = \frac{2 \binom{q^2+q+1}{1} \binom{q^2+q+1}{2}}{\binom{(q^2+q+1)^2}{2}} = \frac{2}{q^2 + q + 1} \quad (۱)$$

۴-۲- مقاومت

از آنجایی که هر کلید در $(q + 1)(q^2 + q + 1)$ قرار دارد. $q+2$ کلیدی که برای یک ارتباط استفاده می شود حداکثر در تعداد عناصر یک سطر یا یک ستون از مش دو بعدی، یعنی در $(q^2 + q + 1)$ دستگاه دیگر موجود است، لذا احتمال لو رفتن این ارتباط در صورت تسخیر X دستگاه از شبکه برابر

۵-۲- اتصال پذیری

در $SBIBD(q^2 + q + 1, q + 1, 1)$ احتمال کلید مشترک بین هر دو دستگاه برابر ۱ است، یعنی اتصال پذیری کامل را داریم [۲۱، ۱۸]. در طرح TD احتمال کلید مشترک برابر است با

$$\frac{k}{q+1} \quad (۴)$$

که برحسب دو پارامتر q و k است [۲۶]؛ لذا به منظور مقایسه، اندازه شبکه را در این طرح با طرح پیشنهادی یکسان در نظر می گیریم. در طرح Trade-KP، احتمال کلید مشترک برابر $\frac{q(q-1)}{2(2q^2-1)}$ است، و در طرح t-UKP، احتمال کلید مشترک برابر

$$1 - \left(1 - \frac{(q+1)}{(q^3 + q + 1)}\right)^{t^2} \quad (۵)$$

که در UKP* مقدار t برابر $\sqrt{q}$ است [۱۶].

و در

$$RD^*(q^2 + q + 1, (q^2 + q + 1)(q + 1), q(q + 1), q, 1)$$

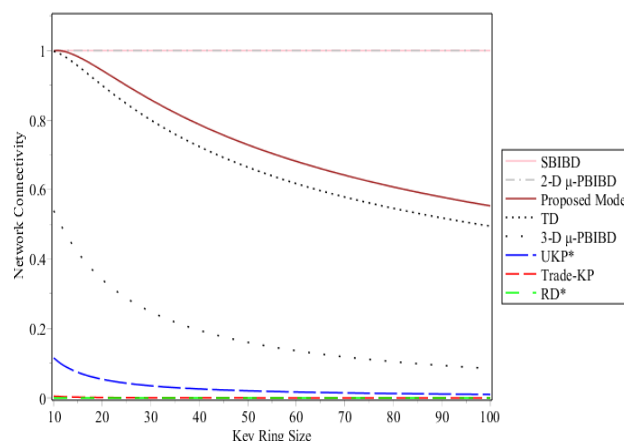
احتمال کلید مشترک طبق [۱۷]، از رابطه زیر به دست می آید.

$$PRD^* = \frac{\binom{q^2+q}{2}}{\binom{(q^2+q)(q^2+q+1)}{2}} \times \left(\frac{q^2}{q^2+q}\right) + \left(\frac{(q^2+q)^2}{\binom{(q^2+q)(q^2+q+1)}{2}}\right) \times \left(\frac{q^4+q-1}{(q^2+q)^2}\right) \quad (۶)$$

همچنین در 3-D μ PBIBD مطابق [۱۸]، احتمال کلید مشترک برابر است با

$$\frac{3q}{q^2 + q + 1} \quad (۷)$$

مقایسه نمودارهای احتمال کلید مشترک با زنجیره کلید یکسان، در شکل ۲ داده شده است؛ که بیانگر این است که مدل پیشنهادی اتصال پذیری بهتری نسبت به همه طرح های مقایسه شده به جز SBIBD و 2-D μ -PBIBD را دارد.



شکل ۲: مقایسه اتصال پذیری الگوهای مختلف پیش توزیع کلید

۵-۳- مقاومت

طبق [۲۱]، [۲۶]، [۱۶]، [۱۷] و [۱۸]، مقاومت در طرح های TD، SBIBD، Trade-KP، t-UKP، RD*، 2-D μ -PBIBD و 3-D μ -PBIBD طبق فرمول های زیر محاسبه می شود.

$$Res_{SBIBD}(x) = 1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}} \quad (۸)$$

$$Res_{TD}(x) = 1 - \left(1 - \frac{q-2}{q^2-2}\right)^x \quad (۹)$$

$$Res_{Trade-KP}(x) = 1 - \frac{\binom{2q^2-4q+2}{x} + 4(q-1)\binom{2q^2-4q+2}{x-1}}{\binom{2q^2}{x}} \quad (۱۰)$$

$$Res_{t-UKP}(x) = 1 - \sum_{i=1}^{t^2} \left(1 - \frac{\binom{q^3(q-1)}{xt}}{\binom{q^2(q^2-q+1)}{xt}}\right)^i \frac{\binom{t^2}{i} \left(\frac{(q+1)^2}{q^3+q+1}\right)^i \left(1 - \frac{(q+1)^2}{q^3+q+1}\right)^{t^2-i}}{1 - \left(1 - \frac{(q+1)^2}{q^3+q+1}\right)^{t^2}} \quad (۱۱)$$

که در UKP* که $t = \sqrt{q}$ است.

$$Res_{RD^*}(x) = \sum_{j=1}^{q^2+q+1} \frac{\binom{q(q+1)}{2}}{\binom{(q^2+q+1)(q+1)}{2}} \left(1 - \frac{\binom{(q+1)(q^2+q+1)}{x}}{\binom{(q^2+q+1)(q+1)}{x}}\right) \quad (۱۲)$$

$$Res_{2-D \mu PBIBD}(x) = \frac{q-1}{q+1} \left(1 - 2\left(1 - \frac{2q-4}{q^2-2}\right)^x + \left(1 - \frac{4q-8}{q^2-2}\right)^x\right) + \frac{2}{q+1} \left(1 - \frac{\binom{q^2-q}{x} + \binom{q-2}{1} \binom{q^2-q}{x-1}}{\binom{q^2-2}{x}} + \frac{Ch(x)}{\binom{q(q-1)}{x}}\right) \quad (۱۳)$$

که در آن

$$Ch(x) = \binom{q(q-1)}{x} - \binom{q-2}{1} \binom{(q-1)(q-1)}{x} + \binom{q-2}{2} \binom{(q-1)(q-2)}{x} + \dots + (-1)^\theta \binom{q-2}{\theta} \binom{(q-1)(q-\theta)}{x} \quad (۱۴)$$

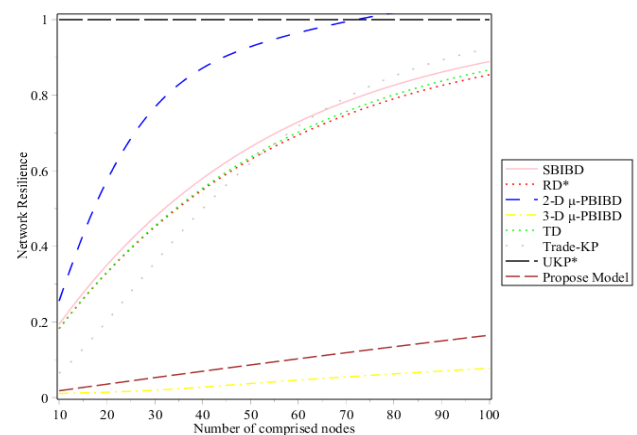
که در آن $0 \leq \theta \leq q-2$ و $q-2 \leq x \leq (q-1)(q-2)$

همچنین

- [6] W. S. Li, C. W. Tsai, M. Chen, W. S. Hsieh, and C. S. Yang, "Threshold behavior of multi-path random key pre-distribution for sparse wireless sensor networks," *Mathematical and Computer Modeling*, vol. 57, no. 11, pp. 2776–2787, 2013.
- [7] O. Catakoglu, and A. Levi, "Uneven key pre-distribution scheme for multi-phase wireless sensor networks," *Information Sciences and Systems, Springer, Baltimore, USA*, pp. 359–368, 2013.
- [8] R. Blom, "An optimal class of symmetric key generation systems," *Advances in Cryptology: Proceedings of Eurocrypt 84, Lecture Notes in Computer Science, Springer-Verlag, Berlin*, vol. 209, pp. 335–338, 1984.
- [9] Chien HY, Chen R-C, Shen A. Efficient key predistribution for sensor nodes with strong connectivity and low storage space, Proceedings of the 2nd International Conference on Advanced Information Networking and Applications (AINA08), IEEE, GinoWan, Okinawa, Japan, 2008; 327–333.
- [10] Blundo, C., Santis, A.D., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M., (1993), Perfectly-secure key distribution for dynamic conferences, In *Advances in Cryptology: CRYPTO 92, LNCS, 740*, 471–486.
- [11] N. C. Wang, H. L. Chen, "Improving pairwise key predistribution in wireless sensor networks", *Advances in Intelligent Systems and Applications, Springer, Hualien, Taiwan*, pp. 521–530, 2013.
- [12] S. A. Camtepe, and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," In *P. Samarati, P. Y. A. Ryan, D. Gollmann, and R. Molva (Eds.), ESORICS, volume 3193 of lecture notes in computer science, Springer*, pp. 293–308, 2004.
- [13] J. Lee, D. Stinson, "A combinatorial approach to key pre-distribution for distributed sensor networks," In *IEEE wireless communications and networking conference (WCN' 05), IEEE communication society*, pp. 1200–1205, 2005.
- [14] S. Ruj, and B. Roy, "Key predistribution using partially balanced designs in wireless sensor networks," *Proceedings of the 5th international conference on Parallel and Distributed Processing and Applications, August, Niagara Falls, Canada*, pp. 431–445, 2007.
- [15] S. Ruj, A. Nayak, and I. Stojmenovic, "Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2224–2237, 2013.
- [16] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 948–959, 2013.
- [17] V. Modiri, H. H. S. Javadi, and M. Anzani, "A Novel Scalable Key Pre-distribution Scheme for Wireless Sensor Networks Based on Residual Design," *Wireless Pers. Communications*, vol. 96, pp. 2821–2841, 2017.
- [18] Q. Yuan, C. Ma, H. Yu, and X. Bian, "A Key Pre-Distribution Scheme Based on μ -PBIBD for Enhancing Resilience in Wireless Sensor Networks," *Sensors*, vol. 18, pp. 1539, 2018.
- [19] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key pre-distribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.
- [20] J. Lee, and D. R. Stinson, "Deterministic key predistribution schemes for distributed sensor networks", *Selected Areas in Cryptography*, Springer, Kingston, Ontario, Canada, pp. 294–307, 2005.
- [21] S. A. Camtepe, and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *Journal of ACM/IEEE Transactions on Networking, Springer*, Vol. 15, no. 2, 2007.
- [22] D. Chakrabarti, S. Maitra, and B. Roy, "A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design," *International Journal of Information Security*, vol. 5 no. 2, pp. 105–114, 2006.
- [23] T. Kavitha, and D. Sridharan, "Hybrid design of scalable key distribution for wireless sensor networks," *IACSIT International Journal of Engineering and Technology*, vol. 2, no. 2, pp. 136–141, 2012.
- [24] M. B. Paterson, and D. R. Stinson, "A unified approach to combinatorial key predistribution schemes for sensor networks," *Designs Codes Cryptography*, vol. 71, pp. 433–457, 2014.
- [25] G. Xia, Z. Huang, and Z. Wang, "Key pre-distribution scheme for wireless sensor networks based on the symmetric balanced incomplete block design," *J. Comput. Res. Dev.*, vol. 45, pp. 154–164, 2008.
- [26] J. Lee, and D. R. Stinson, "On the construction of practical key predistribution schemes for distributed sensor networks," *Journal of ACM Trans. Inf. Syst. Secur.*, ACM, Vol. 11, no. 2, pp. 1–35, 2008.

$$Res_{3-D \mu PBIBD}(x) = \frac{3q-3}{q^2+q+1} \left(1 - 2 \left(1 - \frac{3q-5}{q^3-2} \right)^x \right) + \left(1 - \frac{6q-10}{q^3-2} \right)^x + \frac{3}{q^2+q+1} \left(1 - \frac{(q^2-q) + \binom{q-2}{1} \binom{q-2}{x-1}}{\binom{q^3-2}{x}} + \frac{Ch(x)}{\binom{q(q-1)}{x}} \right) \quad (15)$$

در شکل ۳ نمودار مقایسه مقاومت طرح‌های فوق با طرح پیشنهادی آورده شده است؛ که نشان‌دهنده این است که مقاومت طرح پیشنهادی نسبت به تمام طرح‌های مقایسه شده به جز 3-D μ -PBIBD بیشتر است.



شکل ۳: مقایسه مقاومت الگوهای مختلف پیش توزیع کلید

۶- نتیجه‌گیری

در این کار یک طرح ترکیبیاتی جدید از نوع μ -PBIBD معرفی شده و به‌عنوان الگوی پیش‌توزیع کلید به شبکه IoT با منابع محدود، نگاشت شده است. و به آنالیز طرح پیشنهادی به‌منظور بدست آوردن کارایی طرح پرداخته و نشان داده شد که با کمک این طرح ترکیبیاتی، به الگوی پیش‌توزیع کلیدی با مقیاس‌پذیری بالاتر و مقاومت بهتر در مقایسه با طرح‌های مطرح در سال‌های اخیر همچون SBIBD، TD، Trade-KP، UKP*، RD* و 2-D μ -PBIBD رسیده، همچنین هرچند که مدل پیشنهادی دارای اتصال‌پذیری کامل نیست، اما از اتصال‌پذیری بالایی نیز برخوردار می‌باشد.

۷- مراجع

- [1] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.
- [2] T. Dargahi, H.H.S. Javadi, and M. Hosseinzadeh, "Application-specific hybrid symmetric design of key pre-distribution for wireless sensor networks," *Security and Communication Networks*, Vol. 8, no. 8, pp. 1561–1574, 2015.
- [3] L. Eschenauer, and V. D. Gligor, "A key Management Scheme for distributed sensor networks," *Proceedings of the 9th ACM conference on computer and communications security, ACM*, pp. 41–47, 2002.
- [4] H. Chan, and A. Perrig, "Random key predistribution schemes for sensor networks," *Proceedings of the 2003 IEEE symposium on security and privacy (SP 03), IEEE*, pp. 197–213, 2003.
- [5] S. Qian, "A novel key pre-distribution for wireless sensor networks," *Physics Procedia*, vol. 25, pp. 2183–2189, 2012.

- [27] A. Morshed Aski, H.H.S. Javadi, and G.H. Shirdel, "A Full Connectable and High Scalable Key Pre-distribution Scheme Based on Combinatorial Designs for Resource-Constrained Devices in IoT Network," *Wireless Personal Communications*, vol. 114, no. 3, pp. 2079-2103, 2020.

اکبر مرشد اسکی، تحصیلات خود را در دکتری مهندسی کامپیوتر گرایش نرم افزار به انجام رسانده است و هم اکنون استادیار در دانشگاه آزاد ورامین – پیشوا می باشد. تحقیقات مورد علاقه ایشان در زمینه های امنیت شبکه IoT و داده کاوی است. آدرس پست الکترونیکی ایشان عبارت است: morshed486@gmail.com



سید حمید حاج سید جوادی، تحصیلات خود را در دکتری ریاضی و علوم کامپیوتر به انجام رسانده است و هم اکنون استاد تمام در دانشگاه شاهد می باشد. تحقیقات مورد علاقه ایشان در زمینه های امنیت شبکه، الگوریتم و جبر کامپیوتری است. آدرس پست الکترونیکی ایشان عبارت است: h.s.javadi@shahed.ac.ir



A novel key pre-distribution scheme based on μ -PBIBD combinatorial design in the resource-constrained IoT network

Akbar Morshed Aski¹, Hamid Haj Seyyed Javadi²

¹ Department of Computer Engineering, Varamin – Pishva Branch, Islamic Azad University, Varamin, Tehran, Iran

² Department of Mathematics and Computer Science, Shahed University, Tehran, Iran

Abstract

In a resource-constrained IoT network, end nodes like WSN, RFID, and embedded systems are used which have memory, processing, and energy limitations. One of the key distribution solutions in these types of networks is to use the key pre-distribution scheme, which accomplishes the key distribution operation offline before the resource-constrained devices deployment in the environment. Also, in order to reduce the shared key discovery computing and communication overhead, the use of combinatorial design in key pre-distribution has been proposed as a solution in recent years. In this study, a μ -PBIBD combinatorial design is introduced and constructed and the mapping of such design as a key pre-distribution scheme in the resource-constrained IoT network is explained. Through using such key pre-distribution scheme, more keys are obtained for communication between two devices in the IoT network. This means that there will be a maximum of $q + 2$ keys between the two devices in the network, where q is the prime power, that is, instead of having a common key for a direct secure connection, the two devices can have $q + 2$ common keys in their key chain. Accordingly, we would increase the resilience of the key pre-distribution scheme compared to the SBIBD, TD, Trade-KP, UKP *, RD * and 2-D μ -PBIBD designs.

Keywords: resource-constrained IoT network; combinatorial design; μ -PBIBD; resilience.