فصلنامه پدافند غیرعامل

سال دوم، شماره ۳، تابستان و پاییز ۱۳۹۰، (پیاپی ۷): صص ۱۹-۲۸

انتخاب پروتکل توزیع کلید مناسب در کاربردهای پدافندی شبکه‌های حسگر بی‌سیم

یوسف کاکاوندی[۱]، بهروز خادم[۲]

تاریخ دریافت: ۹۰/۰۷/۱۲
تاریخ پذیرش: ۹۰/۱۰/۲۶

چکیده

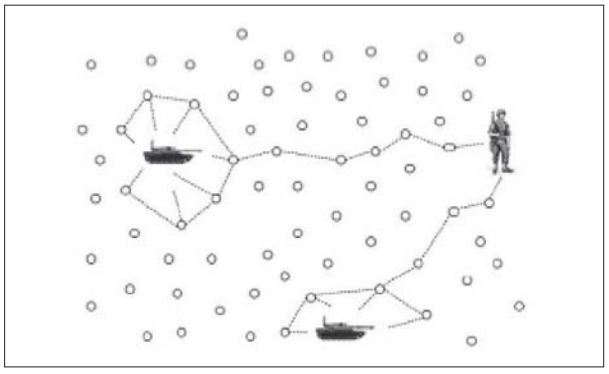
نیاز به سیستم‌های ارتباطی پیشرفته و قابل اطمینان، همزمان با افزایش احتمال بحران‌های اجتماعی، تهدیدات تروریستی و بلایای طبیعی به‌صورت روزافزونی احساس می‌شود. این سیستم‌های ارتباطی باید بتوانند در کمترین زمان، پیام‌های حیاتی و اضطراری را از مناطق بحران‌زده به مراکز کنترل و مدیریت بحران و از آنجا به افراد در معرض خطر و نیازمند امدادرسانی نمایند تا از جان و مال آسیب‌دیدگان، در برابر حوادث و بلایا محافظت نموده و یا میزان آسیب را به حداقل برسانند. یکی از مهم‌ترین ویژگی‌های چنین سیستم‌های ارتباطی این است که بتوانند در بدترین شرایط بحرانی به بهترین وجه عمل کرده و تحت هیچ شرایطی عمل‌کرد آن به‌طور عمدی یا سهوی آسیب‌پذیر نباشد. یکی از جدیدترین فناوری‌های ارتباطی برای استفاده در شرایط بحران و حوزه پدافند غیرعامل، شبکه‌های حسگر بی‌سیم می‌باشند. جهت تامین امنیت شبکه‌های حسگر بی‌سیم، انتخاب پروتکل‌های مدیریت کلید مناسب به‌خاطر محدودیت منابع حسگر، هنوز یک موضوع چالش برانگیز است. از آنجا که استانداردهای ارائه شده جهت شبکه‌های حسگر بی‌سیم فقط ویژگی‌های یک پروتکل مناسب را برشمرده‌اند و از یک پروتکل خاص نامی برده نشده است، لذا استفاده‌کنندگان از این تکنولوژی در انتخاب پروتکل توزیع کلید مناسب هنوز هم سردرگم می‌باشند. در سال‌های اخیر، طرح‌های مدیریت کلید متفاوتی برای برقراری تعادل بین کارآیی امنیتی و کارآیی عملیاتی ارائه شده است. در این مقاله ما ابتدا نیازمندی‌های امنیتی و عملیاتی شبکه‌های حسگر بی‌سیم را بررسی می‌کنیم و سپس ۸ پروتکل توافق کلید اشنور، q- مرکب، ینر، دوو، لیپ، شل، پانجا و یانگ را از جهت پاسخگویی به این نیازمندی‌ها مورد بررسی و مقایسه قرار می‌دهیم. در انتها پیشنهادهایی برای انتخاب یک پروتکل مناسب در کاربردهای پدافندی، به کاربران ارائه می‌کنیم.

کلیدواژه‌ها: شبکه حسگر بی‌سیم، پروتکل‌های مدیریت کلید، نیازمندی‌های عملیاتی، نیازمندی‌های امنیتی

۱- دانش‌آموخته کارشناسی ارشد مخابرات - رمز دانشگاه جامع امام حسین(ع)، Email: y.kakavand@gmail.com
۲- مدرس و عضو هیات علمی دانشگاه جامع امام حسین (ع)- گروه رمز، Email: Khadem@tmu.ac.ir

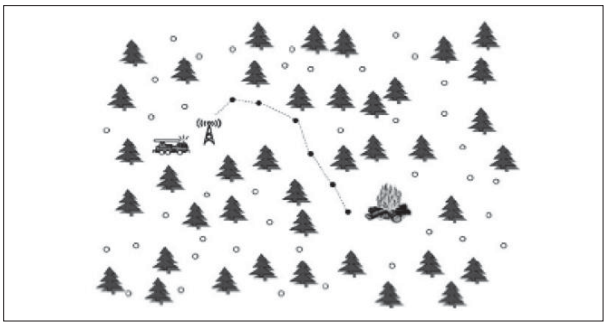
۱- مقدمه

امروزه حوزه‌های امنیت شبکه، مخابرات امن و مدیریت بحران ناشی از تهاجم، از محورهای اساسی پدافند غیرعامل محسوب می‌شوند. کاربرد چشمگیر یک تکنولوژی تقریباً نوپا به نام شبکه‌های حسگر بی‌سیم در این زمینه‌ها باعث شد خیلی سریع برای به‌کارگیری آنها استانداردهایی تعریف شود. یک شبکه حسگر بی‌سیم[1] (WSN) از تعداد زیادی گره حسگر تشکیل شده است که هر کدام از آنها با حسگر(هایی) برای شناسایی پدیده‌های فیزیکی مانند گرما، نور، حرکت یا صوت تجهیز شده‌اند. به‌طور مثال در دو شکل زیر دو نوع از کاربردهای شبکه‌های حسگر بی‌سیم در حوزه پدافند غیرعامل نشان داده شده است. در شکل (۱) تشخیص سریع دشمن با استفاده از حسگرهای تشخیص حرکت بسیار کوچک و ارزان که تحت یک پروتکل مشخص، یک شبکه هماهنگ را تشکیل می‌دهند، صورت می‌گیرد. یکی دیگر از کاربردهای این شبکه‌ها در حوزه پدافند غیرعامل، تشخیص آتش‌سوزی در مقیاس بسیار کوچک در جنگل‌ها و هر مکان دیگر می‌باشد. این کاربرد که در شکل (۲) نمای کلی آن آورده شده است می‌تواند در کشور عزیزمان ایران، که دارای جنگل‌های فراوان بوده و همواره از آتش‌سوزی‌های مکرر رنج می‌برد یک کاربرد حیاتی داشته باشد. کاربرد شبکه‌های حسگر بی‌سیم نه تنها در حوزه پدافند غیرعامل هر روز بیش از پیش گسترش می‌یابد، بلکه با استفاده از حسگرهای متفاوت، WSNها می‌توانند طوری پیاده‌سازی شوند که بسیاری از کاربردهای دیگر مانند تفریحات، اتوماسیون، مانیتورینگ صنعتی، صنایع عمومی و غیره را پشتیبانی کنند.



شکل ۱- کاربرد شبکه‌های حسگر بی‌سیم برای تشخیص دشمن

از یک طرف چون تجهیزات WSN دارای محدودیت‌های زیادی از لحاظ توان مصرفی، تعداد محاسبات، و حجم حافظه هستند و از طرف دیگر به‌دلیل ضرورت صرفه‌جویی در هزینه‌ها و نیاز به تعداد بسیار زیاد تجهیزات و نحوه پیکربندی شبکه در کاربردهای مختلف، دسترسی آسان به این تجهیزات به راحتی امکان‌پذیر نمی‌باشد. این محدودیت منابع، منجر به ایجاد مسائل بسیار زیادی مانند امنیت WSN شده که توسط محققان مورد مطالعه قرار گرفته است. بسیاری از کاربردها برای تبادل اطلاعات یا انجام فرآیندهای بازگشتی که قابلیت اطمینان بالایی را می‌طلبند، نیازمند WSNها می‌باشند و آنها به سطح بالایی از امنیت برای موفقیت نیاز دارند. هنوز هم، دستیابی به امنیت کافی با وجود محدودیت منابع گره‌های حسگر، سخت و دشوار است و بسیاری از روش‌های معروف غیر عملی است. در این مقاله، ما مسئله امنیت را برای مدیریت کلید در WSNها تشریح می‌کنیم. به این منظور ابتدا ملزومات و نیازمندی‌ها را برای مدیریت کلید بررسی می‌کنیم. سپس چند پروتکل توافق کلید پیشنهاد شده را توضیح داده و نهایتاً با بحث در مورد مسیر حرکت آینده که ممکن است منجر به توسعه آن طرح‌ها در حوزه پدافند غیرعامل شود، مقاله را خاتمه می‌دهیم.



شکل ۲- کاربرد محیطی شبکه حسگر برای تشخیص آتش‌سوزی

۱-۱- مدیریت کلید

پیش از آنکه یک WSN بتواند اطلاعات را به‌طور امن مبادله کند، کلیدهای رمزنگاری می‌بایست بین حسگرها ثبت شود. توزیع کلید به معنای توزیع چندین کلید بین حسگرها است. توافق کلید، یک اصطلاح کلی تر برای توزیع کلید است که علاوه بر آن، شامل فرآیندهای ثبت کلید، توزیع اولیه کلیدها، ابطال کلید و حذف کلید کشف شده می‌باشد.

۱-۲- پیش‌نیازهای مدیریت کلید

اولین لایه مدیریت کلید، لایه پیوندِ داده است. یک استاندارد عملی و قابل اجرا برای لایه پیوند داده در یک WSN، استاندارد IEEE 802.15.4 می‌باشد. همچنین این استاندارد، استفاده از کلید را برای انتقال امن اطلاعات درنظر می‌گیرد، اما تعیین نمی‌کند که چطور کلیدها به‌طور امن تبادل شوند. در کنار لایه پیوند، لایه‌های بالاتر مانند لایه کاربرد[2] یا لایه شبکه[3] نیز می‌بایست کلیدها را به‌طور امن مبادله کنند.

1- Wireless sensor network

2- Application layer
3- Network layer

۱-۳- نیازمندی‌های امنیتی و عملیاتی برای مدیریت کلید

نیازمندی‌های مدیریت کلید می‌توانند به دو بخش تقسیم شوند: ۱) نیازمندی‌های امنیتی که زیرمجموعه‌ای از کلیه نیازمندی‌های امنیتی WSN است و ۲) نیازمندی‌های عملیاتی که در طراحی و تحقق مدیریت کلید، محدودیت ایجاد می‌کنند.

جدول (۱) [۱] نیازمندی‌های کلی در WSNها را نشان می‌دهد. برای مدیریت کلید، مهم‌ترین نیازمندی، نیرومندی[۱] و خودسازماندهی[۲] است. با اینکه «محرمانگی[۳] و صحت[۴]» معیارهای مهمی هستند، توزیع کلیدهای مخفی بین حسگرها هر دوی این نیازمندی‌ها را برطرف می‌کند که تمام طرح‌های توزیع کلید این قابلیت را دارا هستند. به‌روزکردن اطلاعات[۵] نیز به همین صورت با یک برچسب زمانی[۶] رمزنگاری در هر بسته برای تشخیص جدید بودن اطلاعات میسر خواهد شد. این روش به صحت هر بسته از اطلاعات وابسته است تا اطمینان حاصل کند که برچسب زمانی تغییر پیدا نکرده است که این امر به‌سادگی بعد از ثبت یک کلید مخفی تسهیم شده مقدور می‌شود. از سوی دیگر، خودسازماندهی، توانایی خودسازمان دادن و خود ترمیم کردن در صورت بروز تغییرات دینامیکی در یک WSN، نیازمندی‌ای است که دستیابی به آن مشکل است. به‌طور معمول و بدون ملاحظات امنیتی، WSNها برای داشتن این ویژگی طوری طراحی می‌شوند که گره‌ها بتوانند به‌طور مستقل، ارتباطات حول یک گره خراب شده را تشکیل دهند یا بعد از تخریب شبکه بتوانند دوباره آن را بازسازی کنند. وقتی که یک طرح توافق کلید، کلیدهای ارتباطی معین را بین تعداد محدودی از گره‌ها توزیع کند، خودسازماندهی ممکن است توسط گره‌های دیگری که به‌دلیل نداشتن کلید مناسب نمی‌توانند ارتباطات را به‌طور فعال با این گره‌های معین برقرار کنند، به خطر بیفتد.

مسئله نیرومندی، زمانی خود را نشان می‌دهد که یک یا تعداد بیشتری از گره‌ها در خطر کشف باشند. به‌دلیل اینکه گره‌های WSN به‌طور متناوب در مکان‌های پرت و بدون کنترل مستقر می‌شوند، دست‌کاری فیزیکی آن‌ها یک تهدید واقعی است و WSN می‌بایست حتی با از دست رفتن چند گره خود را سرپا نگه دارد. اگر شبکه از چند کلید استفاده کند، این امید هست که تعیین کنیم از دست رفتن چه تعداد از گره‌ها باعث از بین رفتن کل امنیت شبکه می‌شود. ما بعداً طرح‌های توزیع کلید را بررسی و در مورد نیرومندی آنها با ذکر جزئیات بیشتر بحث می‌کنیم.

1- Robustness
2- Self-organization
3- Confidentiality
4- Integrity
5- Data freshness
6- Nonce

جدول ۱- نیازمندی‌های امنیتی برای شبکه‌های حسگر بیسیم [۱]

نیازمندی	شرح
محرمانگی	گره‌ها نباید هیچ اطلاعاتی را برای گیرنده‌های غیرمجاز فاش کنند.
صحت	اطلاعات نباید در مسیر ارسال به‌دلیل شرایط محیطی یا فعالیت‌های خرابه‌کارانه تغییر کند.
تجدید اطلاعات	اطلاعات نباید به‌عنوان اطلاعات جدید استفاده شوند(از حملات مجدد[۷] جلوگیری کند).
احراز هویت	اطلاعات استفاده شده در فرآیند تصمیم سازی[۸] باید از منبع مورد تایید تولید شده باشد.
نیرومندی[۹]	وقتی برخی از گره‌ها لو بروند، کل شبکه نباید لو برود. کمیت این گره‌ها و اینکه کدام نیازمندی باید برطرف گردد به نوع کاربرد بستگی دارد.
خودسازماندهی	گره‌ها باید به اندازه کافی مستقل و انعطاف‌پذیر باشند تا خودسازمانده و خودترمیم کننده باشند.
درجه فراهمی[۱۰]	شبکه نباید به‌طور متناوب به مشکل برخورد کند.
همزمان‌سازی[۱۱]	کاربردهایی که در آن گره‌ها با هم همکاری می‌کنند، نیاز به همزمان‌سازی دارند. پروتکل‌های همزمان‌ساز نباید زمان نادرست را اعمال کنند.
موضع‌یابی امن[۱۲]	گره‌ها باید بتوانند به‌طور دقیق و امن به اطلاعات موقعیت دسترسی پیدا کنند.

از طرف دیگر، نیازمندی‌های عملیاتی متعددی مانند دسترس‌پذیری[۱۳]، انعطاف‌پذیری[۱۴] و مقیاس‌پذیری[۱۵] برای WSNها وجود دارند. این نیازمندی‌ها به‌عنوان یک قید و محدودیت در طراحی امنیتی عمل می‌کنند؛ به این دلیل که می‌بایست مطمئن شد که آنها در طراحی و پیاده‌سازی یک طرح امنیتی خللی وارد نمی‌کنند. دسترس‌پذیری، در دسترس بودن اطلاعات برای تعداد زیادی از گره‌ها می‌باشد که این امر می‌بایست به درستی از منابع انرژی، محاسبات و حافظه محدود استفاده کند. این طرح برای دستیابی به بهره‌وری منبع، اجتماع اطلاعات[۱۶] یا ترکیب اطلاعات[۱۷] ارائه شده است، به نوعی که قبل از مسیریابی اطلاعات به سمت گره مقصد، اطلاعات گره‌های دیگر را با اطلاعات محلی ترکیب می‌کند. این روند، نیازمند گره‌های میانی می‌باشد که اطلاعات ارسالی توسط گره‌های دیگر را تفسیر و ترجمه کنند. بعداً در مورد این که چگونه طرح‌های مختلف، دسترس‌پذیری را مجتمع می‌کنند بحث خواهیم کرد. نیازمندی عملیاتی مهم دیگر، انعطاف‌پذیری است. برای مثال،

7- Replay attacks
8- Decision making
9- robustness
10- Availability
11- Time synchronization
12- Secure localization
13- accessibility
14- flexibility
15- scalibility
16- Data aggregation
17- Data fusion

در WSNهای بزرگ، گره‌ها بسته به ظرفیت شبکه یا تخلیه باطری می‌توانند به‌طور متناوب به شبکه بپیوندند یا آن را ترک کنند. یک طرح مدیریت کلید می‌بایست با کاهش یا افزایش کلید، این امر را پشتیبانی کند. در اینجا یک امر چالش‌برانگیز این است که عدم وجود یک مدیریت کلید مرکزی، اضافه کردن و یا حذف کلیدها را یک کار ناامن، ناکارآمد و ملال‌آور می‌کند. در نهایت، مقیاس‌پذیری طرح مدیریت کلید، یک عامل اجرایی مهم است. WSNهایی که از استاندارد IEEE 802.15.4 تبعیت می‌کنند در تئوری می‌توانند بیش از ۶۵۵۳۶ گره را پشتیبانی کنند. بنابراین یک طرح توافق کلید می‌بایست بیش از این اندازه، مقیاس‌پذیر باشد. اگرچه WSNها به‌ندرت چندهزار گره را پشتیبانی می‌کنند اما همین مقدار هم برای طرح‌های مدیریت کلید که کمتر مقیاس‌پذیر هستند، یک عدد چالش‌برانگیز است. بحث‌های قبلی به‌طور خلاصه در جدول (۲) آمده است.

جدول ۲- نیازمندی‌های عملیاتی برای شبکه‌های حسگر بی‌سیم [۱۳]

نیازمندی	شرح
دسترس‌پذیری[1]	گره‌های میانی باید با ترکیب اطلاعات دریافتی از گره‌های دیگر، بتوانند اطلاعات را تجمیع کنند. گره‌های همسایه نیز باید در حالت غیرفعال رخدادهای شبکه را مشاهده و از ثبت اطلاعات تکراری که در این شبکه‌ها بسیار زیاد است، خودداری کنند.
انعطاف‌پذیری[2]	گره‌ها باید زمانی که لو می‌روند، قابل تعویض باشند. اضافه کردن گره‌ها در زمان فعال بودن باید پشتیبانی شود.
مقیاس‌پذیری[3]	یک WSN باید بتواند به‌طور همزمان حداقل ۳۰۰۰ گره (بر اساس استاندارد IEEE 802.15.4) را مطابق با طرح مدیریت کلید در نظر گرفته شده برای آن پشتیبانی کند.

۲- طرح‌های توزیع کلید

در سال‌های اخیر، طرح‌های مدیریت کلید مختلفی برای ایجاد یک توازن بین عمل‌کرد و امنیت پیشنهاد شده است. برای برقراری این توازن، سه مدل از توزیع کلید به نام‌های **«مدل توزیع کلید شبکه‌ای، مدل توزیع کلید زوجی** و **مدل توزیع کلید گروهی»** وجود دارند. مقایسه‌ای بین مزایا و معایب این طرح‌ها در جدول (۳) آمده است.

مدل توزیع کلید شبکه‌ای دارای مزایایی چون مدیریت ساده، استفاده از منابع کم، همکاری ساده حسگرها، مقیاس‌پذیری، خودسازماندهی، انعطاف‌پذیری و دسترسی است. اما مهم‌ترین اشکال این مدل آن است که با از دست رفتن یک گره، تمام شبکه به خطر خواهد افتاد. از لحاظ مقیاس‌پذیری و انعطاف‌پذیری نیز بسیار عالی است؛ چون تنها یک کلید برای کل شبکه وجود دارد و با اضافه شدن گره‌ها کلید تغییر نمی‌کند. با این حال از لحاظ نیرومندی غیر قابل قبول می‌باشد. فرض کنید یک گره توسط مهاجم ضبط شود، در این صورت کلید کل شبکه فاش خواهد شد. با این کلید، یک مهاجم می‌تواند به همه پیام‌ها در شبکه اشراف داشته باشد و حتی پیام‌های جعلی را وارد شبکه کند و احتمالاً عمل‌کرد مناسب شبکه از بین می‌رود.

جدول ۳- طرح‌های توزیع کلید رایج برای شبکه‌های حسگر بی‌سیم [۱۳]

مدل	شرح	مزایا	مشکلات
شبکه‌ای[4]	کل شبکه از یک کلید مخفی تسهیم شده استفاده می‌کند.	• ساده • قابلیت ترکیب و اجتماع اطلاعات • مقیاس‌پذیر • قابلیت خودسازماندهی • انعطاف‌پذیر/ دسترس‌پذیر	• فاش شدن کلید یک گره باعث فاش شدن کلید کل شبکه می‌شود (نبود نیرومندی).
زوجی[5]	هر زوج از گره‌ها یک کلید مشترک متفاوت از زوج‌های دیگر دارند.	• بهترین نیرومندی • هویت هر گره احراز می‌شود.	• تعداد زیادی گره را پشتیبانی نمی‌کند. • خودسازمانده نیست. • برای اضافه یا حذف کردن گره‌ها انعطاف‌پذیر نیست.
گروهی[6]	هر گره از یک کلید تقسیم شده مشترک استفاده می‌کند.	• قابلیت انتشار در جهت‌های مشخص دارد • قابلیت همکاری گروهی دارد • نیرومندی بهتر از مدل شبکه‌ای • بر اساس تعداد گره، طرح قابل تغییر است • امکان اضافه یا حذف گره‌ها وجود دارد • قابلیت خودسازماندهی در خوشه را دارد	• نبود یک روش ذخیره‌سازی مؤثر برای توزیع کلید مطابق با استاندارد IEEE 802.15.4 • برپایی آن به‌طور امن سخت است. • نوع تشکیل خوشه وابسته به کاربرد آن است.

در مدل توزیع کلید زوجی، هر گره، $N-1$ کلید را به خدمت می‌گیرد که N اندازه شبکه است. این مدل بهترین نیرومندی و احراز هویت را فراهم می‌آورد؛ چون فاش شدن کلید یک گره باعث فاش

1- Accessibility
2- Flexibility
3- Scalability

4- Network
5- Pairwise
6- Group-based

شدن کلید هیچ‌کدام از گره‌های دیگر نمی‌شود، اما نیازمندی مقیاس‌پذیری را هم میسر نمی‌سازد؛ چون هزینه حافظه، به سرعت به نسبت اندازه شبکه بالا می‌رود. در حالتی که چندین هزار گره داشته باشیم، مدیریت این حجم از کلید برای هر گره مقدور نمی‌باشد. تعداد کل کلیدهای متمایز در شبکه $N(N-1)/2$ است که با نرخ N^2 افزایش می‌یابد. در این صورت وقتی که N عدد بزرگی باشد غیر قابل نگهداری خواهد بود. مسئله دیگر در مدل توزیع کلید زوجی آن است که اضافه کردن گره‌های جدید به شبکه مشکل بوده و این امر به نوبه خود، انعطاف‌پذیری را تحت‌الشعاع قرار می‌دهد. وقتی که یک گره جدید به شبکه اضافه می‌شود گره‌های دیگر برای برقراری ارتباط با وی نیازمند داشتن یک کلید جدید می‌باشند. این فرآیند، حجم بالایی از پردازش را به منبع تحمیل می‌کند که در مقایسه با مدل شبکه‌ای، توان بسیار بیشتری را مصرف می‌کند. به‌طور مشابه، ابطال و بازسازی کلید، بنا به مشکل مقیاس‌پذیری، مشکل و سخت است. در نهایت، در برخی طرح‌های توزیع کلید، خودسازماندهی مورد تردید قرار می‌گیرد زیرا مقیاس‌پذیری کلیدهای تسهیم شده را کاهش می‌دهد و در نتیجه، برخی گره‌ها نمی‌توانند با دیگران ارتباط برقرار کنند و خودسازماندهی و خودترمیمی شبکه به خطر می‌افتد.

در مدل توزیع کلید گروهی، ویژگی‌های طرح‌های توزیع کلید شبکه‌ای و زوجی ترکیب می‌شوند. در یک گروه از گره‌ها که یک خوشه را تشکیل می‌دهند، ارتباط بین اعضای یک گروه توسط یک کلید مشترک شبیه کلید شبکه‌ای برقرار می‌شود. برای برقراری ارتباط بین گروه‌ها از یک کلید متفاوت بین هر زوج از گروه‌ها، مشابه طرح توزیع کلید زوجی استفاده می‌شود. بنابراین برای یک گروه از گره‌ها دسترس‌پذیری به‌راحتی مقدور می‌شود؛ زیرا اجتماع و فشرده‌سازی اطلاعات بدون هیچ هزینه اضافی میسر می‌شود، در حالی که درجه نیرومندی بر سر جای خود باقی می‌ماند. وقتی کلید یکی از گره‌ها فاش شود، در بدترین حالت، کلید گره‌های هم‌گروه او فاش خواهد شد و نسبت به شبکه تقریباً منفرد می‌باشد. از لحاظ مقیاس‌پذیری به این دلیل که تعداد کلیدها با افزایش گروه‌ها - و نه با افزایش اندازه کل شبکه - افزایش می‌یابد، ایجاد یک توازن مناسب امکان‌پذیر است. با این حال مشکل این طرح این است که استقرار و همچنین تشکیل گروه‌ها سخت بوده و به نوع کاربرد آن بسیار وابسته است. برای توزیع مناسب کلیدها، یک طرح توزیع کلید، نیازمند اطلاعات گروه خواهد بود. علاوه براین ویژگی، استاندارد موجود IEEE 802.15.4 هیچ پشتیبانی از توزیع کلید گروهی در کاربردهای کنونی از لیست کنترل دسترسی نمی‌کند [۲].

برای تحقق یک مدل توزیع کلید نیرومند و عملی، محققان پروتکل‌های مدیریت کلید گوناگونی را پیشنهاد داده‌اند که هدف هر کدام، رفع مشکلات موجود در سه طرح پایه مورد بحث در بالا است. در این بخش، هشت پروتکل مدیریت کلید مختلف به ترتیب زمان معرفی آنها بررسی می‌شود.

۲-۱- طرح اشنور[1] و همکاران

اشنور و گلیگور [۳] یکی از طرح‌های توزیع کلید در حوزه WSNها را ارائه کردند که ظریف (طراحی یک برنامه کارا که با کم کردن تعداد دستورالعمل‌های به‌کار برده شده برای انجام کارهای گوناگون قابل استفاده باشد) و ساده است و یک تعادل مناسب و مؤثر بین نیرومندی و مقیاس‌پذیری برقرار می‌کند. این طرح به‌صورت زیر عمل می‌کند:

- یک مخزن بزرگ از کاندیدهای کلید انتخاب می‌شود (برای مثال ۱۰۰۰۰ کلید).
- k کلید از مخزن بیرون کشیده می‌شود که این کلیدها یک حلقه کلید[2] را تشکیل می‌دهند به‌طوری‌که $k \ll N$ باشد و N تعداد کل گره‌ها می‌باشد. هر گره، حلقه کلید منحصر به خود را دریافت می‌کند که شامل یک زیرمجموعه از کلیدها می‌باشد.
- زمانی که می‌بایست دو گره با هم ارتباط برقرار کنند، آنها با انتشار شناسه کلیدهایی که دارند، دنبال یک کلید مشترک در حلقه کلیدشان می‌گردند. اگر چنین کلیدی موجود نباشد آنها سعی می‌کنند ارتباط را از طریق یک کاربر سوم برقرار کنند که قادر است با هر دو کلید ارتباط داشته باشد. این فاز را فاز کشف مسیر کلید[3] می‌نامند.

در یک نگاه دیده می‌شود که اندازه کل کلیدهای ذخیره شده در یک گره، کمتر از $N-1$ است؛ بنابراین، این طرح از حافظه کمتری نسبت به طرح زوجی کامل، استفاده می‌کند. این طرح، مقیاس‌پذیر نیز می‌باشد؛ زیرا تعداد کلیدهای مخزن و اندازه حلقه کلید، هردو قابل تنظیم هستند. بنابراین، در کاربردهای بسیار امنیتی می‌توان از مخزن بزرگی از کلیدها استفاده کرد و اندازه حلقه کلید را به‌گونه‌ای تنظیم کرد که امنیت بیشتری داشته باشد. با این حال، این طرح برخی اشکالات نیز دارد. در مقایسه با طرح‌های جدیدتر، توزیع کلید تصادفی اشنور تنها یک طرح توزیع کلید است. فرآیند احراز هویت در آن وجود ندارد و به‌طور واضح روندی برای ابطال یا تجدید کلید تعریف نشده است. اگر یک رخداد به‌وسیله دو گره همسایه تشخیص داده شود این امر به ارسال دو سیگنال مجزا منجر خواهد شد. هیچ پشتیبانی از عمل‌کرد گروهی و یا همکاری وجود ندارد. اگر در یک ساختمان، از طرح اشنور برای اتوماسیون نوری آن استفاده شود، خاموش کردن همه لامپ‌ها در یک طبقه، مستلزم ارسال یک پیغام به هر لامپ است که خیلی ناکارآمد است. در نهایت، به این دلیل که هر گره لزوماً با همه گره‌های همسایه خود کلید مشترک ندارد، لذا

1- Eschenauer
2- Key pool
3- Path key discovery

این امکان وجود دارد که برخی گره‌ها غیر قابل دستیابی باشند. نتیجه اینکه طرح اشنور از لحاظ نیازمندی‌های امنیتی، احراز هویت را میسر نمی‌سازد و از لحاظ نیازمندی‌های عملیاتی نیز دارای دسترس‌پذیری نیست.

۲-۲- طرح دوو[1] و همکاران

در سال ۲۰۰۳، دوو و گروهش یک طرح مدیریت بر اساس مدل توزیع کلید زوجی ارائه کردند [۴]. این مدل، ترکیب کار اشنور و بلوم [۵] بود که از الگویی شبیه اشنور و گلیگور [۳] استفاده می‌کرد؛ با این تفاوت که به‌جای استفاده از کلیدهای منحصر به‌فرد از مفهوم ماتریس کلید بلوم استفاده می‌کرد که یک آرایه از کلیدها می‌باشد. در طرح دوو، k ماتریس کلید در هر گره وجود دارد و ماتریس‌های کلید به‌طور تصادفی توزیع می‌شوند. مدل بلوم بر پایه ایده ضرب ماتریس متقارن است، به‌طوری که ردیف i و ستون j متناسب با ردیف j و ستون i است. بنابراین وقتی که گره i کلید ij را، و گره j کلید ji را محاسبه می‌کند، این کلیدها معادل یکدیگرند. طرح بلوم، اطلاعات مورد نیاز برای این محاسبه را در قالب یک ماتریس عمومی و یک ماتریس خصوصی توزیع می‌کند. در طرح مدیریت کلید زوجی دوو، به جای استفاده از تنها یک ماتریس خصوصی، گره مقصد i ماتریس خصوصی را تولید می‌کند، و هر گره یک زیرمجموعه از این ماتریس‌ها را همانند حلقه کلید اشنور در خود ذخیره می‌کند. زمانی که گره‌ها می‌بایست ارتباط برقرار کنند، آنها با انتشار شناسه گره، شناسه ماتریس‌هایی را که در اختیار دارند و ستون ماتریس عمومی‌شان شروع می‌کنند. اگر آنها یک ماتریس کلید مشابه داشته باشند، می‌توانند کلید خصوصی زوج مشترکشان را با استفاده از طرح بلوم محاسبه کنند. اگر آنها ماتریس دارای کلید مشترک را تسهیم نکنند، به فاز کشف مسیر کلید می‌روند تا با استفاده از یک کاربر سوم، اطلاعات را مسیردهی کنند.

مزیت طرح دوو این است که نیرومندی بیشتری را در مقابل لو رفتن گره همراه با مقیاس‌پذیری مناسب به دنبال دارد (در مقایسه با طرح اشنور نیرومندی بیشتری دارد). تحلیل مقیاس‌پذیری نشان می‌دهد که هزینه انرژی در سطح مناسبی باقی می‌ماند و با هزینه انرژی یک WSN که از طرح متقارن AES استفاده می‌کند و قاعدتاً می‌تواند 2^{64} گره داشته باشد، برابر است که این عدد ۴۸ برابر ماکزیمم گره‌های تعریف شده در استاندارد IEEE 802.15.4 است.

عیب اصلی این طرح، پیچیدگی آن است که پیاده‌سازی آن را مشکل می‌سازد و هزینه پردازش مورد نیاز را بالا می‌برد. همچنین عمل‌کرد گروهی را به این دلیل که یک طرح توزیع کلید زوجی است، پشتیبانی نمی‌کند. در این طرح نه ابطال کلید و نه تجدید کلید در نظرگرفته نشده است. از لحاظ نیازمندی‌های عملیاتی دسترس‌پذیری نیز ندارد، به این دلیل که یک گره در حالت غیرفعال نمی‌تواند به ارتباطات گوش فرا دهد. نتیجه اینکه در مقایسه با طرح‌های ساده‌تر دیگر، طرح دوو به‌دلیل پیچیدگی محاسباتی بیشتر از توان بیشتری استفاده می‌کند. به‌طور خلاصه طرح دوو بیشتر نیازمندی‌ها را برطرف می‌سازد؛ اما در بخش نیازمندی‌های عملیاتی، نمی‌تواند دسترس‌پذیری را میسر سازد و نیز نمی‌تواند از لحاظ مقیاس‌پذیری با طرح‌های ساده‌تر از خود، به‌دلیل هزینه پردازش بالاتر رقابت کند.

۲-۳- طرح لیپ[2]

ژوو، ستیا و جاجوردیا یک پروتکل احراز هویت و رمزنگاری متمرکز لیپ را معرفی کردند که از یک روش ترکیبی[3] استفاده می‌کند. لیپ از چهار نوع کلید استفاده می‌کند: تکی، گروهی، خوشه‌ای[4] و زوجی. کلید تکی برای هر گره منحصر به فرد است تا بتواند با گره منبع[5] ارتباط برقرار کند. برای تشخیص پیام منتشر شده از سوی گره منبع، یک پروتکل احراز هویت به نام μTESLA[6] [۷] استفاده می‌شود که مطمئن می‌شود بسته‌های ارسالی همراه با کلید گروه از طرف گره منبع است. کلید خوشه برای برقراری ارتباط در داخل خوشه استفاده می‌شود. برای اینکه منبع ارسال اطلاعات، بدون ایجاد مانع برای فشرده‌سازی اطلاعات، احراز هویت شود، از یک مکانیسم احراز هویت شناخته شده به نام زنجیره کلید چکیده ساز یک طرفه[7] که یک عملگر ریاضی برگشت‌ناپذیر را به کار می‌گیرد، استفاده می‌شود. در نهایت، از یک کلید مشترک زوجی برای ارتباط امن بین گره‌های همسایه استفاده می‌شود.

لیپ از یک کلید پیش‌توزیع‌شده برای کمک به ثبت چهار نوع از کلیدها استفاده می‌کند. کلید منفرد ابتدا با استفاده از تابع مرجع توزیع کلید و شناسه گره ثبت می‌شود. سپس در فاز کلید زوجی، یک فرآیند کشف همسایه راه‌اندازی می‌شود و گره‌ها شناسه‌شان را منتشر می‌کنند. گره‌ها از یک تابع مرجع به همراه یک کلید اولیه استفاده می‌کنند تا کلید مشترک بین خود و همسایه‌هایشان را محاسبه کنند. بعد از آن کلید اولیه و هر کلید میانی که تولید شده است پاک می‌شود. در مرحله سوم، کلید خوشه توسط سرخوشه با استفاده از ارتباط امن دو به دو با کلید مشترک زوجی توزیع می‌شود. در نهایت برای توزیع کلید گروهی کل شبکه، گره منبع آن را در مسیرهای چندگانه، خوشه به خوشه[8] با شروع از نزدیک‌ترین خوشه منتشر می‌کند.

1- Du

2- LEAP(Localized encryption and authentication protocol)
3- Hybrid
4- Cluster
5- Sink node
6- μTimed Efficient Streaming Loss-tolerant Authentication
7- One-way hash-key chain
8- Cluster-by-cluster

لیپ مزیت‌های بسیاری دارد که نیازمندی‌هـای WSNهـا را برطـرف می‌سازد. اول اینکه، دارای µTESLA و احراز هویت زنجیره کلید یک طرفه بوده و ابطال و تجدیـد کلیـد را نیـز دارا مـی‌باشـد. نیازمنـدی دسترس‌پذیری به آسانی با رمزنگاری دیتا با استفاده از کلیـد خوشـه برای ایجاد تراکم میسر می‌شود. مقیاس‌پـذیری لیـپ را مـی‌تـوان بـا مقدار محاسـبات و حافظـه ارزیـابی کـرد. هزینـه محاسـبات، رابطـه معکوسی با تعداد گره‌هـای شـبکه و رابطـه مـستقیمی بـا گـره‌هـای همسایه دارد (چگالی گره) [۶]؛ زیرا با بیـشتر شـدن چگـالی شـبکه، تعداد ارتباطات بیشتری در هر خوشه برقرار می‌شود. میـزان حافظـه نیـز کـاملاً مناسـب اسـت و کـاملاً مـشهود اسـت کـه طـرح لیـپ نیازمندی‌های عملیاتی و امنیتی را به خوبی برآورده مـی‌سـازد. تنهـا عیب آن این است که فرض می‌شود که گره منبع هیچ‌وقت به دسـت مهاجم نخواهد افتاد.

۲-۴- طرح q – مرکب[1]

برای غلبه بر محدودیت‌های طرح اشنور، چان و همکارانش یک طرح پیش‌توزیع کلیـد متفـاوت q – مرکـب را در [۱۲] ارائـه کردنـد کـه اصلاحی از طرح اشنور بود، به این صورت که هـر زوج از گـره‌هـا بـه جای یک کلید، به q کلید مشترک نیاز داشتند. عدد صـحیح q یـک آستانه تلاقی[2] از پیش تعیین شده است.

به‌خوبی دیده می‌شود که در این طرح، تنها عـاملی کـه بهبـود یافتـه است، نیرومندی شبکه می‌باشد که از نیازمندی‌های امنیتی است. این امر به‌دلیل آن است که با اعمال این تغییر، احتمـال از دسـت رفـتن گره‌های دیگر - هنگامی که یک گره لو می‌رود - کم می‌شود. امـا در مقابل افزایش نیرومندی، پیچیدگی محاسبات و به تبـع آن، مـصرف انرژی و حافظه بالا می‌رود و پیـاده‌سـازی مـشکل‌تـر مـی‌شـود. ایـن درحـالی اسـت کـه تمـام ضـعف‌هـای دیگـر طـرح اشـنور ماننـد دسترس‌ناپذیری و نبود احراز هویت به قوت خود باقی است.

۲-۵- طرح ینر[3] و همکاران

آنها استفاده از روش‌های پیوندی و قطعی را برای حل مـسئله توزیـع کلید پیشنهاد دادند که در آن از یـک سـاختار جدیـد از طـرح‌هـای ترکیباتی استفاده می‌شد[11]. ادعای آنها این بود که روش‌های قطعی دارای برتری‌هایی نسبت به روش‌های تصادفی مـی‌باشـند. بـه‌عنـوان نمونه، در روش‌های قطعی احتمال این‌که دو گره یک کلید را تسهیم کنند افزایش می‌یابد یا طول مسیر کشف کلید کاهش پیدا می‌کنـد. در این طرح، از طرح بلوکی ناکامل متعادل[4] (BIBD) استفاده شده و سپس توسط یک نگاشت آنرا به مسئله توزیع کلیـد متنـاظر سـاخته است. BIBD چیدمان v شئ متمایز در b بلوک به‌گونه‌ای است کـه هر بلوک دقیقاً شـامل k شـئ متمـایز اسـت، و هـر شـئ دقیقـاً در r بلوک متفاوت تکرار می‌شود، و هر زوج از اشیاء متمـایز دقیقـاً در λ بلوک اتفاق می‌افتد. طرح بلوکی ناکامل متعـادل، یـک پـنج‌تـایی (v,b,r,k,λ) است، به‌گونـه‌ای کـه $bk = vr, \lambda(v-1) = r(k-1)$.

در این طرح با استفاده از نگاشت این طرح ترکیباتی به توزیع کلیـد، به هر گره یک زنجیره کلید از k کلید اختصاص می‌یابد کـه قبـل از استقرار در شبکه، درون حافظه ROM آنها قرار می‌گیرد. برای داشتن ارتباط امن بین آنها، یـک زوج از گـره‌هـا مـی‌بایـست دارای x کلیـد مشترک در زنجیره کلیدش باشد.

این طرح دارای مقیاس‌پـذیری و انعطـاف‌پـذیری مناسـب اسـت. در مقایسه با دیگر طرح‌های زوجی، ویژگی‌های امنیتی آن نیـز مناسـب است. اما پیچیدگی این طـرح بـه نـسبت نیـز بیـشتر اسـت. ارتبـاط گروهی را پشتیبانی نمی‌کند و عدم دسترس‌پذیری، بزرگتـرین عیـب این طرح می‌باشد زیـرا گـره‌هـای غیـر فعـال، از رخـدادهای شـبکه به‌خوبی مطلع نیستند.

۲-۶- طرح شل[5]

پروتکـل مقیـاس‌پـذیر، سلـسله مراتبـی، کارآمـد، موقعیـت‌سـنج[6]، و کم‌حجم شل [۸] یک طرح مدیریت کلید پیچیـده بـر پایـه خوشـه[7] است که اخیراً ارائه شده است. این طرح، تحت نفوذ طرح لیـپ قـرار دارد - از این بابت که از انواع مختلفی از کلید استفاده می‌کنـد - امـا یک توزیع کلید جدید را معرفی می‌کند که هر خوشه، مدیریت توزیع کلید مربوط به خود را دارد. بنابراین جهت داشتن مقاومـت بهتـر در مقابل لو رفتن گره، مسئولیت عملیاتی و مسئولیت مـدیریت کلیـد از هم مجزا شده است. به‌دلیل اینکه در این طرح بـیش از ۷ نـوع کلیـد وجود دارد، توزیع کلید و روند برقراری ارتباط بسیار پیچیده است.

مزیت اصلی شل آن است کـه دارای یـک نیرومنـدی بـسیار بـالا در مقابل فاش شدن کلید مـی‌باشـد. بـا فـاش شـدن کلیـد یـک گـره، کلیدهای کافی برای در اختیار گرفتن کل شبکه یا اخلال در کار آن، در اختیار دشمن قرار نمی‌گیرد. بـرای مثـال اگـر گـره مرجـع (sink node) در حال تولید کلید توس مهاجم ضبط شـود، چـون آن گـره شامل کلید بین سرخوشه و زیرخوشه‌ها نمـی‌باشـد؛ بنـابراین، نحـوه مدیریت کلید، لو نمی‌رود. همچنـین قابلیـت افـزودن، جـایگزینی، و تجدید کلید را دارد. طرح شـل ارتباطـات گروهـی را نیـز پـشتیبانی می‌کند. با این حال دارای معایبی نیز می‌باشد. ساختار و عمل‌کرد آن بسیار پیچیده است که شامل عمل‌کردهای متفاوت توسـط گـره‌هـا و چندین نوع از کلیـد (حـداقل ۷ کلیـد) مـی‌باشـد. مـصرف انـرژی و

1- q-composite
2- Intersection threshold
3- Yener
4- Balanced Incomplete Block Design
5- SHELL
6- Location-Aware
7- Cluster base

محاسبات رمزنگاری آن قابل مقایسه با طرح‌های دیگر نیست. نهایتاً، پیاده‌سازی این چنین پروتکل پیچیده‌ای با محدودیت‌های برنامه‌ریزی پردازنده‌های حال حاضر بسیار سخت است. به‌طور خلاصه، در این طرح بر روی افزایش نیرومندی و ایجاد توازن بین نیازمندی‌های عملیاتی و درجه فراهمی تمرکز شده است. اما افزایش پیچیدگی افزایش استفاده از انرژی را درپی داشته است که در این صورت به‌دلیل تخلیه باطری گره‌های منفرد از کار خواهند افتاد.

۲-۷- طرح پانجا[1] و همکاران

پانجا و همکاران [۹] یک طرح توزیع کلید گروهی سلسله‌مراتبی را بر اساس پروتکل دیفی هلمن گروهی درختی[2] (TGDH) معرفی کردند. ویژگی اصلی این طرح، این است که هر کلید از تعداد زیادی کلید جزئی تشکیل شده است. با تقسیم کلیدها به بخش‌های کوچکتر، بازسازی کلید را از طریق ابطال، تغییر و یا افزودن یک بخش از کلید(ها) ساده و مؤثر می‌سازد. طرح کلیددهی TGDH در یک شبکه WSN سلسله‌مراتبی که دارای یک سطح از گره‌های حسگر عمومی و چندین سطح از سرخوشه‌ها می‌باشد، به این صورت است که یکی از سرخوشه‌ها مسئولیت چندین سرخوشه زیری خود را بر عهده دارد. فرآیند جمع‌آوری اطلاعات با یک گروه از گره‌ها آغاز می‌شود، به این صورت که اطلاعات را از ناحیه مورد نظر جمع‌آوری می‌کنند و آن را به نزدیکترین سرخوشه می‌فرستند. سرخوشه نیز با فشرده‌سازی و بهینه‌سازی اطلاعات مورد نظر، آنها را به سرپرست (سرخوشه) خود می‌فرستد. آن سرخوشه نیز چندین زیرخوشه دارد، و او نیز با فشرده‌سازی و اجتماع، اطلاعات را به سرخوشه خود می‌فرستد. این کار ادامه می‌یابد تا زمانی که به گره منبع برسیم. برای ثبت کلیدها در این ساختار WSN درختی دو طرح استفاده می‌شود، (کلیددهی درون‌خوشه‌ای[3] و بین‌خوشه‌ای[4]). فرآیند توزیع کلید درون خوشه‌ای اینگونه شروع می‌شود که گره‌های leaf کلیدهای جزئی خود را به سرخوشه خود می‌فرستند. سپس سرخوشه کلید جزئی خود را محاسبه می‌کند و کلیدهای جزئی را با هم ترکیب می‌کند تا کلیدخوشه را تشکیل دهد و سپس کلیدخوشه را به تمام leaf هایش می‌فرستد. همه ارتباطات با یک کلید پیش‌توزیع‌شده رمز شده‌اند تا در طول این مرحله، محرمانگی حفظ شود، سپس کلیددهی بین‌خوشه‌ای آغاز می‌گردد. این فرآیند بسیار شبیه به آن چیزی است که در توزیع کلید درون‌شبکه‌ای داشتیم به‌جز اینکه کلیدهای موقت سرخوشه‌ها (leafهای سطوح بالاتر) به‌جای کلیدهای جزئی استفاده می‌شوند. مزیت این طرح در مقایسه با شل این است که ساده و کم حجم است و بنابراین پیاده‌سازی آن ساده است. پانجا و دوستانش، همچنین کارآیی طرحشان را در مقایسه با دیگر پروتکل‌های امنیتی برای شبکه‌های حسگر (SPINS) [۷]، به‌عنوان یک پروتکل توزیع کلید که ارتباط یک به یک امن را در یک WSN مقدور می‌سازد شبیه‌سازی کردند. نتایج این شبیه‌سازی، نویدبخش بود. انتقال سریع و مقیاس‌پذیر کلید که همراه با استفاده بهینه از زمان و انرژی است، با استفاده از کلیدهای جزئی کوچک، هزینه‌های ذخیره‌سازی و محاسبات را کاهش می‌دهد. این امر برای گره‌های leaf به‌دلیل وجود منابع بسیار کم، اهمیت بیشتری دارد. عیب طرح پانجا این است که اگر چه این طرح دارای ابطال کلید و تجدید کلید می‌باشد، اما افزودن و تعویض کلید در نظر گرفته نشده است. به علاوه، امنیت آن در مقابل لو رفتن کلید پیش‌توزیع‌شده اولیه تحلیل نشده است. نتیجه اینکه، طرح پانجا در مقابل کم شدن نیرومندی، نیازمندی‌های دیگر از قبیل خود سازماندهی، دسترس‌پذیری، انعطاف‌پذیری، و مقیاس‌پذیری را بهبود می‌بخشد. استفاده از ساختار سلسله‌مراتبی درختی ما را مطمئن می‌سازد که این طرح بسیار مقیاس‌پذیر است.

۲-۸- طرح یانگ، ساجید، و صفایت

این پروتکل از تابع درهم‌ساز یک‌طرفه[5] برای به‌روز رسانی کلیدهای نشست بعد از ثبت ارتباط استفاده می‌کند. همچنین با تغییر تعداد دفعات اجرای تابع درهم‌ساز می‌توان کلید متقارن برای هر نشست را تغییر داد. این پروتکل دارای چهار مرحله است:

۱- تولید مخزن کلید؛

۲- تخصیص حلقه کلید به هر گره؛ این مرحله نیز مانند مرحله قبل، قبل از استقرار گره‌ها در شبکه انجام می‌شود.

۳- کشف کلید مشترک

۴- به‌روز رسانی کلید برای هر نشست؛ در اینجا از تابع درهم‌ساز کلید استفاده می‌شود.

استفاده از تابع درهم‌ساز کلید برای تولید کلید جهت برگزاری نشست‌های متفاوت، باعث امنیت بیشتر و مقاومت در مقابل حملات مختلف در شبکه‌های حسگر بی‌سیم می‌باشد. اما این افزایش نیرومندی، سربارهای محاسباتی و عملیاتی بسیار زیادی را به همراه دارد چون تعداد تکرارهای تابع درهم‌ساز زیاد است.

۳- آینده مدیریت کلید

با اینکه مقالات بسیار زیادی وجود دارد که طرح‌های گوناگونی را در زمینه توزیع کلید ارائه کرده‌اند، اما یا قابلیت پیاده‌سازی ندارند یا مورد نیاز مصرف‌کنندگان نیستند. یک طرح پیشنهادی، در عمل نیز کاربرد خواهد داشت اگر برطبق استاندارد باشد. اخیراً گروه IEEE 802.15.4 و ZigBee Alliance استانداردهای جدیدی را ارائه

1- Panja
2- Tree-base Group Diffie-Hellman protocol
3- Intra-cluster
4- Inter-cluster
5- One-way Hash function

کرده‌اند. با اینکه استاندارد جدید 802.16.4b هنوز یک طرح مدیریت کلید مشخص را معین نکرده است، اما در مقایسه با استاندارد اصلی، بسیاری از ابهامات را برطرف ساخته و ویژگی‌های زیادی را در دسترس ما قرار می‌دهد. در سال ۲۰۰۳ استاندارد 802.15.4-2003 با عمل‌کرد گروهی ارائه شد. برای رفع ابهام‌های امنیتی آن در سپتامبر ۲۰۰۶ یک اصلاحیه از آن به‌عنوان 802.15.4-2006 ارائه گردید.

جدول ۴- خلاصه‌ای از طرح‌های مدیریت کلید

طرح	تاریخ	ساختار	تولید کلید	توصیف
اشنور	۲۰۰۲	زوجی، توزیع کلید تصادفی	ایستا	به‌طور تصادفی، k کلید تصادفی را از یک مخزن بزرگ انتخاب و یک حلقه کلید تشکیل می‌دهد. کلیدهای مشترک در یک زوج از حلقه کلیدهای مربوط به گره ها، اجازه برقراری ارتباط را می‌دهند.
q- مرکب	۲۰۰۳	زوجی، توزیع کلید تصادفی	ایستا	به‌طور تصادفی، k کلید تصادفی را از یک مخزن بزرگ انتخاب و یک حلقه کلید تشکیل می‌دهد. q کلید مشترک در یک زوج از حلقه کلیدهای مربوط به گره ها، تعیین می‌شوندو اجازه برقراری ارتباط را می‌دهند.
دوو	۲۰۰۳	زوجی، ماتریس	پویا و متحرک	T ماتریس کلید را انتخاب و با استفاده از ضرب ماتریسی، کلید مشترک زوجی را در حالت پویا محاسبه می‌کند.
لیپ	۲۰۰۳	چندگانه: شبکه‌ای، گروهی،زوجی همسایه‌ای	بیشتر ایستا	از یک کلید پیش‌توزیع‌شده برای ثبت چهار نوع از کلیدها استفاده می‌کند.
ینر	۲۰۰۴	زوجی همسایه‌ای	پویا و متحرک	از طرح ترکیباتی BIBD درتوزیع کلید استفاده می‌کند.
شل	۲۰۰۶	گروهی	پویا و متحرک	از یک نهاد مدیریت کلید توزیع‌شده برای تولید و مدیریت کلیدها استفاده می‌کند.
پانجا	۲۰۰۶	گروهی، ساختار شبکه‌ای سلسله مراتبی	پویا و متحرک	از کلیدهای جزئی متعدد برای محاسبه کلیدهای گروهی به‌طور پویا استفاده می‌کند.
یانگ	۲۰۰۹	زوجی همسایه‌ای	ایستا/پویا	از تابع درهم‌ساز کلید برای محاسبه کلید در هر نشست استفاده می‌کند.

جدول ۵- مقایسه کارآیی طرح‌های مدیریت کلید

طرح	سادگی	مقیاس	نیرومندی	راندمان حافظه
اشنور	بالا	متوسط	پایین	متوسط/بالا
q- مرکب	پایین	متوسط	متوسط	پایین/متوسط
دوو	پایین	پایین	بالا	متوسط
لیپ	متوسط	متوسط	متوسط	متوسط
ینر	پایین	متوسط/پایین	متوسط/پایین	پایین
شل	پایین	متوسط	بالا	پایین/متوسط
پانجا	متوسط	بالا	متوسط	متوسط/بالا
یانگ	پایین	متوسط	بالا	پایین/متوسط

۴- نتیجه‌گیری

در این مقاله، ما هشت طرح توافق کلید را با توجه به نیازمندی‌های عملیاتی و امنیتی بررسی کردیم. واضح است که طرح‌های مدیریت کلید مختلف نسبت به یکدیگر مزایا و معایب متعددی دارند و با توجه به شمار بسیار زیاد طرح‌ها، مقایسه آنها به‌منظور انتخاب مناسب‌ترین پروتکل برای یک کاربر عادی بسیار سخت است. در این قسمت، ما راه‌کارهایی را برای چنین انتخابی ارائه می‌کنیم. کاربردها و علایق کنونی در حوزه پدافند غیرعامل نشان می‌دهد که عمل‌کرد گروهی یا شاخه‌ای، یک مشخصه لازم است که طرح‌های اخیر مانند شل، لیپ و پانجا آن را در نظر گرفته‌اند. هر کدام از این طرح‌ها ویژگی خود را دارد؛ قابل تنظیم بودن سطوح امنیتی در لیپ، نیرومندی قوی شل و مقیاس‌پذیری سلسله‌مراتبی پانجا. زمانی که می‌خواهیم یک طرح مدیریت کلید مناسب در یک کاربرد از حوزه پدافند غیرعامل انتخاب کنیم باید به دقت ویژگی‌های مثبت و منفی آن را در نظر بگیریم. برای مثال اگر چه طرح شل نیرومندی بالایی را پیشنهاد می‌دهد اما در مقایسه با دو طرح دیگر بسیار پیچیده‌تر است و بنابراین ممکن است پیاده‌سازی آن بسیار مشکل باشد. لیپ دارای انعطاف‌پذیری بالایی برای ارتباط بین گروه‌ها، شبکه و توزیع کلید زوجی است؛ اما به‌دلیل داشتن ضعف‌های امنیتی می‌بایست مطالعه بیشتری روی آن صورت گیرد. طرح‌های توزیع کلید مناسب در آینده می‌توانند انعطاف‌پذیری لیپ را با نیرومندی طرح‌های اشنور یا دوو ترکیب کنند. برای کاربردهای با امنیت بالا، به نظر می‌رسد که شل دارای بالاترین نیرومندی است، اما اگر بتوان پیچیدگی پیاده‌سازی آن را کاهش داد بسیار بهبود خواهد یافت. برای شبکه‌های بسیار بزرگ، یک نسخه اصلاح شده از طرح سلسله‌مراتبی پانجا به‌دلیل مشخصه مقیاس‌پذیری بالای آن می‌تواند یک انتخاب مناسب باشد. در جایی که انعطاف‌پذیری توأم با مقیاس‌پذیری مد نظر باشند، استفاده از طرح‌های ترکیباتی مانند آنچه در طرح ینر دیدیم پیشنهاد می‌شود.

جدول ۶- مقایسه مزایا و معایب طرح‌های مدیریت کلید

طرح	مزایا	معایب
اشنور	• از حافظه کمتری در مقایسه با طرح زوجی استفاده می‌کند. • نیرومندی قابل تنظیم برای معاوضه آن با هزینه حافظه • ساده و قابل پیاده سازی	• احراز هویت ندارد. • عمل‌کرد گروهی را پشتیبانی نمی‌کند. • برخی گره‌ها ممکن است قابل دسترسی نباشند. • دسترس‌پذیری پایین دارد.
q- مرکب	• نیرومندی آن نسبت به طرح اشنور بهبود یافته • مقیاس‌پذیری آن مناسب است • انعطاف‌پذیری آن مناسب است.	• احراز هویت ندارد. • عمل‌کرد گروهی را پشتیبانی نمی‌کند. • دسترس‌پذیری پایین دارد و بار محاسبات آن نسبت به اشنور بیشتر است.
دوو	• احراز هویت را در طرحی شبیه اشنور فراهم می‌سازد. • حجم حافظه همچنان مناسب باقی می‌ماند. • نیرومندی عالی	• پیچیدگی بالا • عمل‌کرد گروهی را پشتیبانی نمی‌کند • مصرف انرژی بالا • دسترس‌پذیری پایین
لیپ	• عمل‌کردهای شبکه‌ای و زوجی و شاخه‌ای را پشتیبانی می‌کند (برای اجتماع اطلاعات مناسب است). • می‌تواند گره‌های لو رفته را به سرعت توسط احراز هویت µTESLA باطل کند. • مقیاس‌پذیری و پیچیدگی مناسب	• امنیت در طول مدت ثبت کلید اولیه ممکن است ضعیف باشد. • هزینه حافظه برای تعداد کمی از گره‌ها با توجه به استفاده از چهار نوع کلید متفاوت، بالا است. • فرض می‌کند که گره منبع هیچگاه لو نمی‌رود.
ینر	• احتمال رسیدن دو گره به کلید مشترک افزایش یافته • دارای مقیاس‌پذیری و انعطاف‌پذیری مناسب است • مشخصه امنیتی به نسبت طر حهای زوجی مناسب است.	• پیچیدگی آن به نسبت طرح‌های زوجی بیشتر است. • دسترس‌پذیری ندارد. • به‌دلیل پیچیدگی، سربار محاسباتی و حافظه زیادی دارد.
شل	• افزودن و تعویض گره‌ها را پشتیبانی می‌کند. • کلیدها را با استفاده از چند پیام تجدید می‌کند. • نهاد مدیریت کلید توزیع شده را به کار می‌گیرد. • دارای نیرومندی بالا • دارای دسترس‌پذیری بالا	• عمل‌کردهای پیچیده با رفتارهای ناهمگون گره ها • هزینه حافظه برای تعداد کمی از گره‌ها با توجه به استفاده از هفت نوع کلید متفاوت، بالا است. • بار محاسبات رمزنگاری بالاتر • مصرف انرژی بالا با توجه به عمل‌کردهای پیچیده
پانجا	• ساده و کم حجم • فرآیند تجدید کلید ساده و سریع می‌باشد. • دارای مقیاس‌پذیری بسیار بالا با استفاده از TGDH • حجم پایین استفاده از حافظه برای گره‌های Leaf	• قدرت امنیتی قابل تنظیم نیست. • به‌طور واضح نحوه افزودن گره و ابطال کلید مشخص نشده است. • اگر کلید اولیه لو برود ممکن است با استراق سمع طولانی یک حمله شدید روی آن رخ دهد. • امنیت در مقابل حمله مهاجمی که قدرت محاسباتی بالایی دارد ممکن است کافی نباشد.
یانگ	• نیازمندی‌های امنیتی بسیار عالی(نیرومندی بسیار بالا) • امنیت در مقابل کلیه حملات در WSN ها	• نیازمندی‌های عملیاتی از قبیل بهینه‌سازی مصرف انرژی و محاسبات و حافظه در سطح پایینی قرار دارد.

مراجع

1. Carman, D. W.; Kruus, P. S.; Matt, B. J. "Constraints and Approaches for Distributed Sensor Security."; NAI Labs tech., rep. 00-010, (**2000**).
2. Sastry, N.; Wagner, D. "Security Considerations for IEEE 802.15.4 Networks."; Proc. 2004 ACM Wksp. Wireles Sec., pp. 32–42,(**2002**).
3. Eshenauer, L.; Gligor, V. D. "A Key-Management Scheme for Distributed Sensor Networks."; Proc. 9th ACM Conf. Comp. and Commun. Sec., pp. 41–47, (**2002**).
4. Du, W. et al. "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks."; Proc. 10th ACM Conf. Comp. Commun. Sec., pp. 42–51, (**2003**).
5. Blom, R. "An Optimal Class of Symmetric Key Generation Systems."; Proc. EUROCRYPT '84 Wksp. Advances in Cryptology: Theory and App. of Cryptographic Techniques, , pp. 335–38, (**1985**).
6. Zhu, S.; Setia, S.; and Jajodia S.; "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Comp. and Commun. Sec., pp. 62–72, (**2003**).
7. Perrig, A. et al. "SPINS: Security Protocols for Sensor Networks."; Wireless Network, vol. 8, pp. 521–34, (**2002**).
8. Younis, M. F.; Ghumman, K.; and Eltoweissy, M. "Location- Aware Combinatorial Key Management Scheme for Clustered Sensor Networks."; IEEE Trans. Parallel and Distrib. Sys., vol. 17, pp. 865–82, (**2006**).
9. Panja, B.; Madria, S. K.; and Bhargava, B.; "Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks."; SUTC '06: Proc. IEEE Int'l. Conf. Sensor Networks, Ubiquitous, and Trustworthy Comp., pp. 384–93, (**2006**).
10. Camtepe, S. A.; Yener, B.; "Key Distribution Mechanisms for Wireless Sensor Networks: A Survey."; Tech. rep ,TR-05-07, Dept. of Comp. Sci., Rensselaer Polytechnic Inst, (**2005**).
11. Camtepe, S. A.;Yener, B.; "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," Tech. rep. TR-05-07, Dept. of Comp. Sci., Rensselaer Polytechnic Inst., (**2004**).
12. CHAN, H., PERRIG, A., AND SONG, D. Random key predistribution schemes for sensor networks.In Proceedings of the Symposium on Security and Privacy. IEEE Computer Society,197–213., (**2003**).
13. Johnson,C.; Lee ; Victor, C.; Leung, M.; Kirk, H. Wong, Jiannong, C.; Henry, C. B.; CHAN.; "Key management issues in wireless sensor network: CURRENT PROPOSALS AND FUTURE DEVELOPMENTS."; IEEE Wireless Communications, (**2007**).

Protocol Selection of Appropriate Key Management in Passive Defense Applications of Wireless Sensor Networks

Y. Kakavandi[1]

B. Khadem[2]

Abstract

The Need to modern and reliable communication systems, seems to be more important, as the probability of society chaos, terrorist threats and natural disasters increase. These communication tools should be able to transmit, within the shortest possible time, the vital and emergency messages from crisis- stricken regions to control and management centers and from there, to endangered and relief needing people so that their lives and properties could be protected against accidents and disasters or the damage rate could be mitigated. One of the most important features of these systems is that they are able to act well under severe conditions and that their performance are not intentionally and unintentionally vulnerable. Wireless sensor networks are one of the most advanced technologies for such cases. Key management has remained a challenging issue in wireless sensor networks (WSNs) due to the constraints of sensor node resources. Various key management schemes that trade off security and operational requirements have been proposed in recent years. In this article, we first examine the security and operational requirements of WSNs and then review eight key management protocols: Eschenauer,q-composite,Yener, Du, LEAP, SHELL, Panja, and Yang and analyze them in the case of security and operational requirements. Finally we propose some proposals for selecting a suitable protocol.

Key Words: *Wireless Sensor Network, Key Management Protocols, Operational Requirements, Security Requirements*

1- MS. Candidate- Imam Hossein University (Email: y.kakavand@gmail.com)
2- Faculty and Research Center of Information & Communications Technology (ITC) Lecturer, Imam Hossein Comprehensive University (Email khadem@tmu.ac.ir)