ارائه یک طرح مدیریت کلید برای شبکه حسگر بی سیم

صادق محمدی*, کرامت حسنی

گروه کامپیوتر دانشگاه فنی و مهندسی واحد ملایر

1-چکیده:

پیشرفت های اخیر در زمینه الکترونیک و مخابرات، توانایی طراحی و ساخت حسگرهایی با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربری های گوناگون را به وجود آورده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلفی،پردازش اطلاعات و ارسال آن ها را دارند، موجب پیدایش ایده ای برای ایجاد و گسترش شبکه های موسوم به شبکه های حسگر بی سیم شده اند. یک شبکه حسگر متشکل از تعداد زیادی گره حسگر است که در یک محیط به طور گسترده پخش می شوند . با توجه به این که ممکن است گره ها در محیط های عملیاتی ناامن قرار گی رند، مخصوصا در کاربردهای نظامی، امنیت یکی از پارامترهای مهم و ضروری در این شبکه هاست. از این رو سرویس های امنیتی نظیر احراز اصالت و محرمانگی باید در این شبکه ها مورد استفاده قرار گیرند تا بتوان از عملکرد گره ها و در نهایت شبکه مطمئن بود . ارایه این سرویس ها در سطح شبکه مستلزم وجود یک زیر ساخت امنیتی بین گره های شبکه است که به شکل مناسبی کلیدهای مشترکی را برای احراز اصالت و محرمانگی گره ها فراهم نمایدچارچوبی که طی آن نیازمندی فوق برآورده می شود را مدیریت کلید می گویند. طراحی پروتکل مدیریت کلید است که می تواند امنیت توزیع کلید های مخفی میان گره های حسگر را بوجود آورد و این یک موضوع مهم برای شبکه گیرنده ی سریم است. در چند سال اخیر روش های زیادی برای مدیریت کلید در شبکه های حسگر بی سیم ارائه شده است؛ که بطور خلاصه ممکن نیست یک طرح به تنهایی بتواند همه معیارهای امنیتی را در بهترین حالت در خود داشته باشد، و هر یک از آنها دارای برخی از نقاط قوت قطعی، نقاط ضعف و نقاط مناسب برای موقعیت های خاص هستند. برخی از این روش ها از همبندی محلی و مقاومت مناسبی در قبال افشای کلید برخوردار هستند اما نیاز به صرف منابع زیادی در گره های حسگر دارند به طوری که استفاده از آن ها در گره های حسگر مقدور نیست. در مقابل، برخی دیگر از این روش ها از نظر مصرف منابع مناسب هستند اما با چالش های امنیتی و یا کارایی روبرو هستند در این بررسی صورت گرفته ما ابتدا با بررسی و شناخت چالش های فرا روی شبکه‌های حسگربی سیم سعی در طراحی پروتکل های مدیریت کلیدی است که قابل به کارگیری در گره های حسگر باشند و همچنین کارآمدی و امنیت آن ها در سطح قابل قبولی باشد به این منظور، پس از شناخت مسائل پیرامون مدیریت کلید در شبکه ی حسگر، چهار طرح مدیریت کلید را معرفی کرده‌و به تجزیه و تحلیل آن ها میپردازیم

واژگان کلیدی: شبکه های حسگر ، مدیریت کلید ، امنیت ،

2- مقدمه:

با پیشرفت حاصل‌شده در دهه اخیر درزمینه شبکه‌های حسگر بی‌سیم[1] استفاده از این شبکه‌ها به‌شدت رو به گسترش است. در این شبکه‌ها عموماً گره‌ها از کانال مشترک برای تبادل اطلاعات استفاده می نمایند. این خصوصیت باعث می شود تا دسترسی به اطلاعات دیگران به‌طور غیرمجاز امکان‌پذیر شده و زمینه بروز حملات مختلف فراهم گردد . ازاین رو امنیت اطلاعات در شبکه‌های بی‌سیم با چالش‌های جدی مواجه است که نیازمند بررسی و ارائه راه‌کارهایی برای بهبود سطح امنیت در این شبکه‌ها است.

در یک دسته‌بندی کلی، شبکه‌های بی‌سیم را می‌توان به دودسته شبکه‌های ساختارمند و بدون ساختار تقسیم کرد. در شبکه‌های ساختارمند به راه اندازی ساختار اولیه برای ایجاد شبکه نیاز است . یک از معروف ترین شبکه های ساختارمند شبکه‌های سلولی هستند . در شبکه های سلولی، محیط تحت پوشش به سلول هایی تقسیم می شود و در هر سلول از یک ایستگاه پایه مرکزی برای برقراری ارتباط کاربران با یکدیگر استفاده می گردد. در شبکه های بدون ساختار نیازی به ایجاد ساختار از پیش تعیین‌شده وجود ندارد. شبکه‌های اقتضایی[2] و حسگر نمونه‌هایی از شبکه‌های بدون ساختار هستند که به‌شدت موردتوجه قرارگرفته‌اند. این شبکه‌ها با اجتماع تعدادی گره بی‌سیم با هزینه کم‌راه اندازی می‌شوند. این ویژگی باعث شده است که این شبکه ها در حوزه های مختلف به ویژه دفاعی، زیست محیطی و علمی کاربردهای زیادی پیدا کنند . با توجه به آنکه شبکه‌های حسگر در آینده در کاربردهای مختلف مورداستفاده قرار می گیرند، در این مقاله مباحث پیرامون مدیریت کلید در یک شبکه پویا موردتحقیق و بررسی قرار خواهد گرفت.

3- معرفی شبکه های حسگر بیسیم

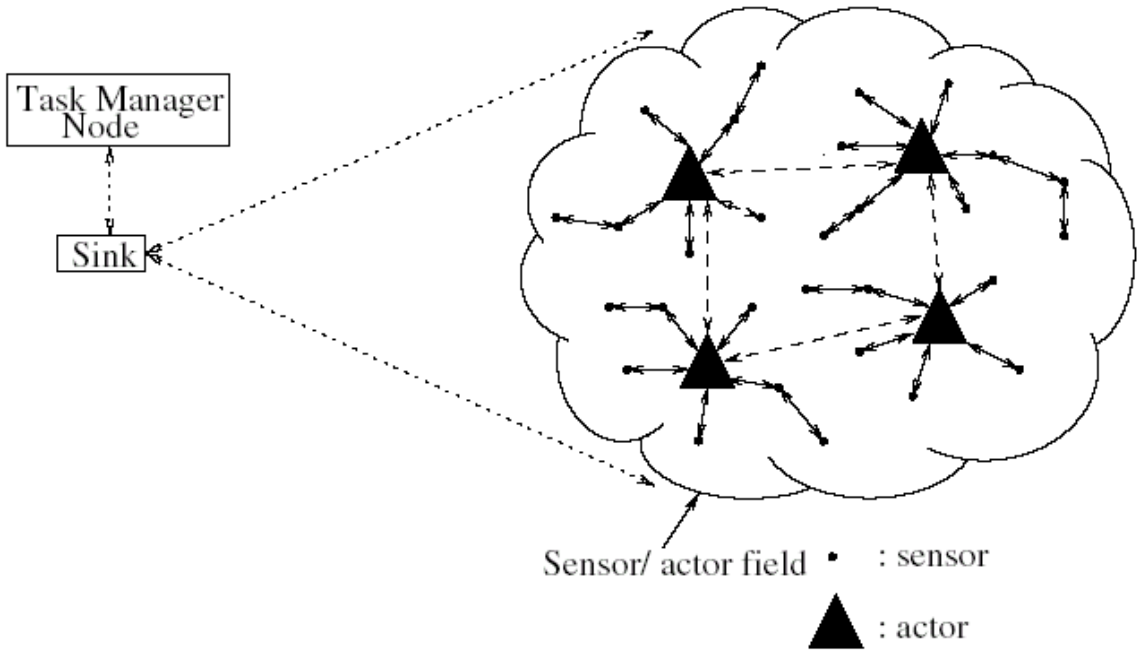
یک شبکه حسگر متشکل از تعداد زیادی گره های حسگری است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می پردازد. لزوماً مکان قرار گرفتن گره های حسگر از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آن‌ها را در مکان‌های خطرناک و یا غیرقابل‌دسترس رها کنیم. از طرف دیگر این بدان معنی است که پروتکل ها و الگوریتم های شبکه های حسگر باید دارای توانایی های خودسازماندهی، همکاری، و هماهنگی بین گره‌های حسگر باشند. هر گره حسگر دارای یک پردازشگر است و به‌جای فرستادن تمامی اطلاعات خام به مرکز یا به گره‌ای که مسئول پردازش و نتیجه گیری اطلاعات است، ابتدا خود یک سری پردازش های اولیه و ساده را روی اطلاعاتی که به دست آورده است، انجام می‌دهد و سپس داده‌های نیمه پردازش شده را ارسال می‌کند.

4- موارد قابل لحاظ در طراحی شبکه حسگر بیسیم مورد نظر:

---

1 Wireless Sensor Network
2 ad-hoc network

شبکه‌های حسگر بی‌سیم از حسگرهای کوچک و کم‌حجم باقابلیت‌های محدود ازلحاظ منبع تغذیه، قدرت پردازش و میزان حافظه تشکیل می‌شوند. گره‌های حسگر معمولاً دریک میدان با توجه به شکل-1 توزیع می‌شوند . با پیشرفت فنّاوری کاربرد این شبکه‌ها بسیار فراگیر شده است به‌گونه‌ای که در بسیاری از زمینه‌های تحقیقاتی مورداستفاده قرار می‌گیرند. هرگره داده‌های خود را از طریق رسانه مشترک و به‌صورت بی‌سیم تک گام یا در گام‌های متعدد به گره مرکزی یا چاهک [۳] ارسال می‌کند. گره‌های حسگر قبل از ارسال هرگونه داده، ابتدا مسیریابی انجام می‌دهند.



شکل1: ساختار کلی شبکه حسگر

لایه شبکه به دلیل انجام مسیریابی و کنترل تراکم تأثیر بسزایی در مصرف انرژی دارد. لذا اهمیت طراحی یک پروتکل مسیریابی مناسب قابل‌چشم‌پوشی نیست. پروتکل‌های مختلفی برای شبکه‌های حسگر بی‌سیم طراحی‌شده‌اند که هرکدام به طریقی نحوه ارسال داده‌ها را مشخص می‌کنند تا از اتلاف انرژی جلوگیری کرده و طول عمر شبکه را افزایش دهند . پروتکل‌های مسیریابی را می‌توان به هفت گروه مسیریابی داده محور، مسیریابی سلسله مراتبی، مسیریابی مبتنی بر مکان، مسیریابی مبتنی بر مذاکره، مسیریابی مبتنی بر چندمسیرگی، مسیریابی مبتنی بر کیفیت سرویس و مسیریابی مبتنی بر حرکت تقسیم کرد. طراحی پروتکل‌های مسیریابی در شبکه حسگر بی‌سیم چالش‌برانگیز است زیرا شامل محدودیت‌هایی برای بهره‌وری انرژی شبکه هست.

5- مدیریت کلید:

---

2 Sink

مدیریت کلید یک کار مهم در DSN است و کار تحقیقاتی گسترده‌ای در این حوزه انجام‌شده است . مدیریت کلید، مدیریت از کلیدهای رمزنگاری در یک سیستم رمزنگاری، که شامل بررسی تولید، ذخیره‌سازی، استفاده و جایگزینی کلیدها و همچنین شامل طراحی پروتکل رمزنگاری و پروتکل‌های دیگر طراحی کلید مربوطه می‌باشد.

مدیریت کلید موفق برای امنیت یک سیستم رمزنگاری بسیار مهم است، چراکه ممکن است انواع مختلفی از کلید، برای برخی از سیستم‌ها، بیش از یک کلید استفاده شود. این کلیدها ممکن است شامل هردو نوع متقارن و نامتقارن باشند . در کلیدهای نامتقارن که ازنظر ریاضی دو کلید مجزا می‌باشند درحالی‌که کلید متقارن شامل یک کلید یکسان هست که هردو برای رمزگذاری و رمزگشایی از یک پیام هستند. مسئله مهم در سیستم مدیریت کلید استفاده از طول کلید می‌باشد و بنابراین نیاز به تکرار جایگزینی کلید، برای جلوگیری از هر حمله را افزایش می‌دهد. کلیدها باید به‌طور مرتب تغییر کنند که این کار مانع از دست دادن اطلاعات که به‌عنوان تعدادی از پیام‌های رمز شده و ذخیره‌شده می‌باشند .

6- معماری شبکه پیشنهاد شده:

مفروضات و نشانه‌گذاری: راه‌حل ما بر مفروضات زیر متکی است..

- گره‌های حسگر از سه نوع که به‌طور تصادفی در شبکه توزیع‌شده را شامل م ی‌شوند . (1) گره ایستگاه (2) پایه گره ها ی سرخوش (3) گره‌های متحرک
- ایستگاه پایه محدودیتی در قابلیت‌های محاسباتی و ذخیره‌سازی ندارد و نمی‌تواند به خطر بیفتد.
- گره سرخوش دارای انرژی نسبتاً بالایی است.
- گره‌های غیر سرخوش به‌صورت متحرک و در حالت حرکت 360 درجه می‌باشند.
- کانال‌های ارتباطی دوطرفه هستند؛ اگر یک گره u بتواند یک پیام را از گره v دریافت کند، پس‌ازآن u می‌تواند یک پیام را به v ارسال کند.
- به‌طورکلی ایستگاه پایه مسئول ایجاد فرآیند مدیریت کلید است.
- هر گره حسگر دارای یک شناسه منحصربه‌فرد است.

هر گره قادر به استفاده از موارد زیر است:

- رمزنگاری نامتقارن: برای تأمین اعتبار از ایستگاه پایه است.
- رمزنگاری متقارن: برای اطمینان از محرمانه بودن ترافیک در سراسر شبکه است.
- MAC (پیام کد احراز اصالت) برای اطمینان از درستی داده‌ها.

- هر حسگر قابلیت ذخیره حداقل کلید عمومی از ایستگاه پایه و یک و یا چند کلید متقارن برای رمزگذاری داده‌ها را دارد.
- این سه نوع گره، یک شبکه حسگر را در 100m*100m از طریق یک توزیع تصادفی تشکیل می‌دهند.

6-1مرحله مقداردهی اولیه

فرض بر این است که تمام گره ها یی که در شبکه می پیوندند امن هستند . هر گره دارای شناسه منحصربه فرد که شماره اصلی آن می باشد، و تمام این اطلاعات را به BS در زمان اولیه انتقال می‌دهند، و پس‌ازآن BS این اطلاعات را برای تشکیل یک لیست ثبت می‌کند.

اگر گره‌ای جدید بخواهد به شبکه بپیوندد، اولین چیزی که باید تعیین شود این است که اگر شناسه منحصربه‌فرد گره جدید، با فرمت اصلی یکسان بود یک تأییدیه را فراخوانی کند که در این حالت عملکرد پایداری صورت گرفته است.

عملیات خاص اولیه به شرح زیر انجام می‌گیرد:

1 -سطح انرژی تمام گره‌ها به‌عنوان حالت انرژی به چهار سطح تقسیم می‌شوند:

با اشاره به توان انرژی: قوی‌تر ، قوی ، معمولی، ضعیف است که در اینجا سطح انرژی گره ایستگاه پایه (BS) بدون محدودیت می‌باشد.

باید این مسئله را در نظر گرفت، گره‌هایی در حالت خاص در شبکه قرار دارند که درصد انرژی باقی‌مانده آن‌ها ، در وضعیت ضعیف می‌باشد و باید بتوان این گره‌ها را در حالت sleep قرارداد و در زمان نیاز برای ارسال پیام‌های اضطراری از آن‌ها استفاده کرد.

2 -گره ایستگاه پایه (BS) یک جفت کلید را با استفاده از الگوریتم رمزنگاری نامتقارن RSA تولید کرده که کلید خصوصی (SK)و کلید عمومی (PK) است که کلید خصوصی به‌صورت مخفی می‌ماند، و BS کلید عموی(PK) را در بین گره ها پخش می‌کند.

3 - همه گره‌ها، یک پیام Hello که در هر گره از پیش تنظیم شده است که شامل شماره اصلی خود (شناسه منحصربه فرد) می‌باشد، برای پیوستن به گره ایستگاه پایه (BS) ، به آن ارسال می‌کنند.

4 - ایستگاه پایه (BS) یک لیست از اطلاعات در سراسر شبکه اولیه تشکیل می‌دهد. در ایستگاه پایه(BS) یک شمارنده، برای زمان دریافت پیام Hello و پاسخ به گره‌ها طراحی می‌شود.

5 - بر اساس قانون اینکه اولین ورودی اولین سرویس را می‌گیرد، تعدادی ID به هر گره اختصاص داده خواهد شد و این ID ها تکرار نمی‌شوند، وبه‌عنوان مقدار اولیه برای گره‌ها که کلیدها از آن تولید می‌شوند می‌باشند. به‌طوری‌که ما بتوانیم به هدف انتقال امن دست بیابیم.

- مرحله انتخاب سرخوشه‌ها

بعد از مقداردهی اولیه، شبکه به صورت یک شبکه موردنظر نمی باشد که بتواند به طور مؤثر اجرا شود، درواقع، شکل‌گیری خوشه نیز، باید از طریق انتخاب سرخوشه، به دقت انجام گیرد. این‌که یک گره به عنوان گره CH انتخاب می‌شود، مقداردهی نسبت به سطح انرژی و یک الگوریتم تصادفی در مرحله اولیه صورت می‌گیرد.

1 - به‌روزرسانی سطح انرژی گره ها : معمولاً ، اگر انرژی بالاتری در آن گره وجود داشته باشد، شانس بیشتری برای آن، در انتخابش به عنوان گره CH است . باید سرخوشه‌ها بر اساس موقعیت و وضعیت گره، از پیش انتخاب شوند.

2 - هم‌زمان، سرخوشه‌هایی که به‌عنوان زاپاس در نظر گرفته می شوند باید با الگوریتم تصادفی به شرح زیر از پیش انتخاب شوند:[39]

$$T(n) = \begin{cases} \dfrac{P}{\left\{1 - p\left[r \bmod \left(\frac{1}{p}\right)\right]\right\} \times [(i \times p)(1 - E(n))]} & n \in G \\ \text{Otherwise} & \end{cases}$$

که در آن:

P درصد مطلوب گره ها ی CH در میان جمعیت حسگرها ، که به طورکل ی به مجموع 5% است، r نمایش داده‌شده ، برای تعداد دوره‌ها ی جاری که برای انتخاب می باشند . E(n) درصد سطح انرژی باقی‌مانده است. i تعداد کل دوره‌های بیکاری توسط گره است.

زمانی که گره به‌عنوان گره‌ی سرخوشه انتخاب می‌شود، ارزش i باید پاک شود.

G یک مجموعه از گره‌هایی که به‌عنوان سرخوشه در آخرین 1/p دورها انتخاب‌شده‌اند. پس ازاین روند از آزمایش، بسیاری از گره‌ها وجود دارند که محروم می‌شوند.

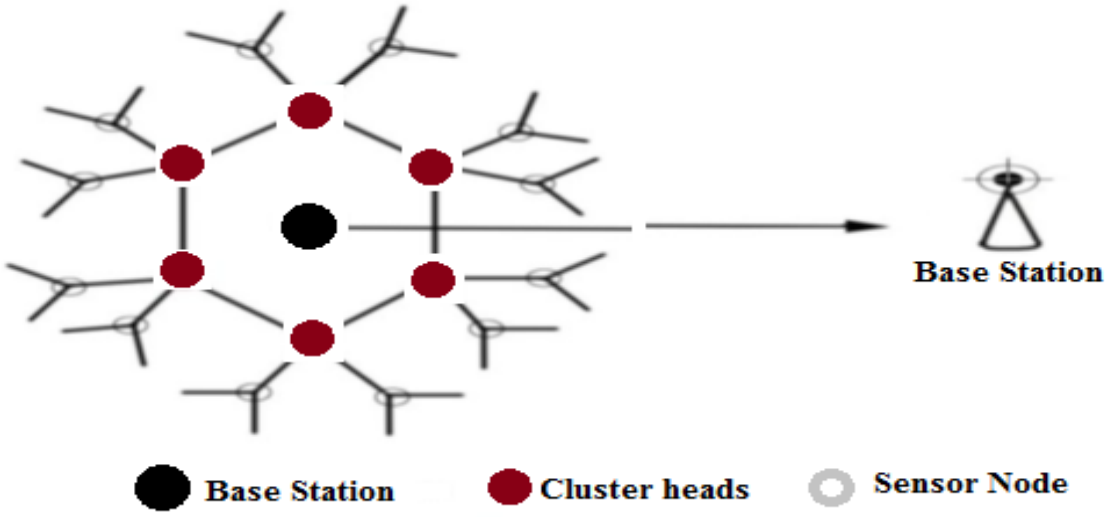
3 - درنهایت، یک گره به‌عنوان یک گره CH انتخاب می‌شود، باید احراز اصالت با همسایگان با انتقال یک کلید از طریق اتصال مستقیم صورت پذیرد. این کار برای ایجاد کلید بین دو گره مجاور صورت می‌گیرد. ایجاد کلید توسط یک تابع درهم‌ساز یک‌طرفه تولید می‌شود[40].

گره n با استفاده از ID خود و یک تابع یک‌طرفه درهم‌ساز تولید یک کلید اصلی می‌کند.

$$K(n) = F(ID(n))$$

به‌این‌ترتیب، هر گره مقدار کلید را با گره‌ای که در مجاورت خود به‌طور مستقیم قرار دارد را بر اساس شناسه آن، می‌تواند محاسبه کند. به این معنی که هرگره را می‌توان با احراز اصالت گره‌ها به هم وصل کرد. گره‌ای که به‌عنوان سرخوشه

کاندید شده است تنها به گره واقعی سرخوشه تبدیل می‌شود که گره‌ها به‌طور مستقیم به هم وصل می‌شوند که از احراز اصالت با جفت کلید درست می‌شود.



شکل 5-1 : نمای کلی از شبکه پیشنهادی

2-6مرحله شکل‌گیری خوشه

1 - سرخوشه ها یک پیام Hello حاوی شماره اصلی خودشان را پخش می‌کنند که با کلید متقارن رمزگذاری شده است. باید توجه داشت که کلید متقارن با استفاده از کد الگوریتم DES ذخیره‌شده و در هر گره تولید می‌شود.

2 - گره‌های غیر سرخوشه، لیست اطلاعات گره های سرخوشه که در همسایه خود هستند را دریافت کرده که به طور مکرر از CH این پیام را دریافت می‌کنند، و به‌طور خودکار سرخوشه ه ای مربوطه به‌عنوان سرخوشه‌های پشتیبان گیر ثبت و ضبط می‌کنند. اگر گره غیر سرخوشه لیست اطلاعات از همسا یه‌ها ی CH به آن نرسد، یک پیام Hello را پخش می‌کند(شامل شماره اصلی که با کلید متقارن رمزگذاری شده است) و منتظر پاسخ از گره‌های دیگر می‌شود و همچنین لیست اطلاعات همسایه‌های سرخوشه از آن‌ها را پالایش می‌کند.

3 - گره غیر سرخوشه(گره معمولی) به یک خوشه می‌پیوندد:

وقتی‌که یک گره غیر سرخوشه تصمیم می‌گیرد که به یک خوشه بپیوندد، گره نیاز به ارسال یک پیام "درخواست عضویت" به سرخوشه را دارد.

این پیام شامل :

a) شماره اصلی گره سرخوشه: CHMN

b) شماره اصلی گره گره غیر سرخوشه NCHMN با کلید متقارن و کلید احراز اصالت K_{auth} رمزگذاری می‌شود.

c) کلید احراز اصالت توسط تابع f() تولید می‌شود: $K_{auth}=f(CHMN , NCHMN)$

پس از دریافت پیام، در مرحله اول، CH م ی‌خواهد این پیام را با استفاده از کلید احراز هویت K_{auth} به NCHMN رمزگشایی کند . و مطابق با نتیجه، با استفاده از الگوریتم رمزگشایی DES به NCHMN رمزگشایی م ی‌شو د. اگر مطابق با موفقیت بود و گره درست بود، پس مجاز به پیوستن است و موافقت گره را برای پیوستن صادر م ی‌کند .سپس گره CH پیام " تای د پیوستن " را به گره ارسال می‌کند با این کار از حمله تکرار و حمله پخش جلوگیری خواهد کرد.

7-ارائه نتایج شبیه سازی:

در این بخش کارایی الگوریتم پیشنهادی با استفاده ازآزمایشات مختلف مورد ارزیابی قرار می‌گیرد. جهت انجام آزمایشات از نرم‌افزار متلب استفاده‌شده است.

در طول استقرار شبکه، ما به‌طور تصادفی 100 گره تصادفی را مستقر کرده ای م، BS بالاترین سطح انرژی را در این شبکه را دارد، پس‌ازآن 10 گره CH با سطح انرژی نسبتاً بالا وجود دارد و گره‌های MS بقیه‌ی شبکه را تشکیل م ی‌دهند . این 100 گره با اندازه پوشش 100m*100m شبکه را تشکیل می‌دهد. علاوه بر گره BS، تمام گره‌های دیگر در فاصله 360 درجه حرکت می‌کنند، اما سرعت حرکت آن‌ها ثابت است، و در این شبکه قرار است 1m/s باشد، جهت حرکت در هر 0.1s یک‌بار به‌روز می‌شوند.

از طریق شبیه‌سازی، ما پارامترهای زیر را برای مقایسه، با طرح LECH انتخاب می‌کنیم.

7-1:امنیت شبکه پویا

در مرحله اولیه شبکه، ارتباط بین سرخوشه (CH) و ایستگاه پایه(BS) را که می‌تواند امنیت بالای بین دو سطح را تضمین کند اعمال می‌شود.

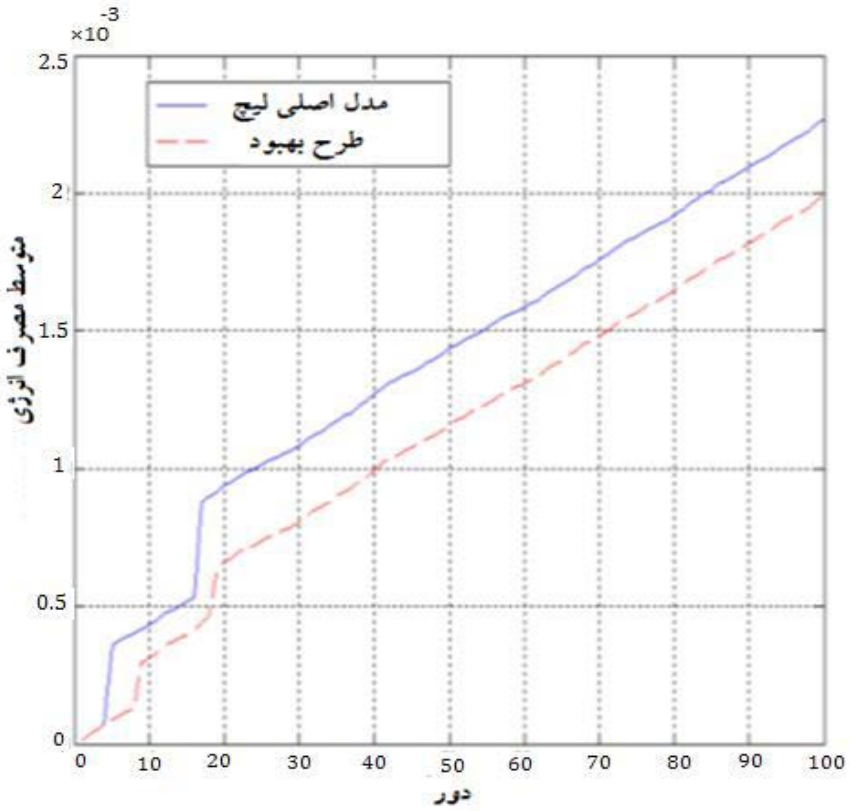
برنامه ما یک الگوریتم درست بهبودیافته از نوع درخت خود متوازن است که با به‌روزرسانی کلید پویا عمل م ی‌کند . درحالی‌که امنیت گره متحرک را تضمین می‌کند دارای کاهش بار محاسباتی می‌باشد. علاوه برای، این برنامه می‌تواند سیستم ایمنی در برابر حمله متعارف را وقتی گره حرکت می‌کند و همچنین بهبود نرخ به‌روزرسانی کلید را که در تنظیم امنیت شبکه پویا اثرگذاری دارد را تضمین کند.

جدول 5-1- ایمنی نسبت به حملات رایج

طرح ما	درخت AVL	نوع حمله
Y	Y	انتخاب - ارسال
Y	Y	چاهک- روزنه حمله

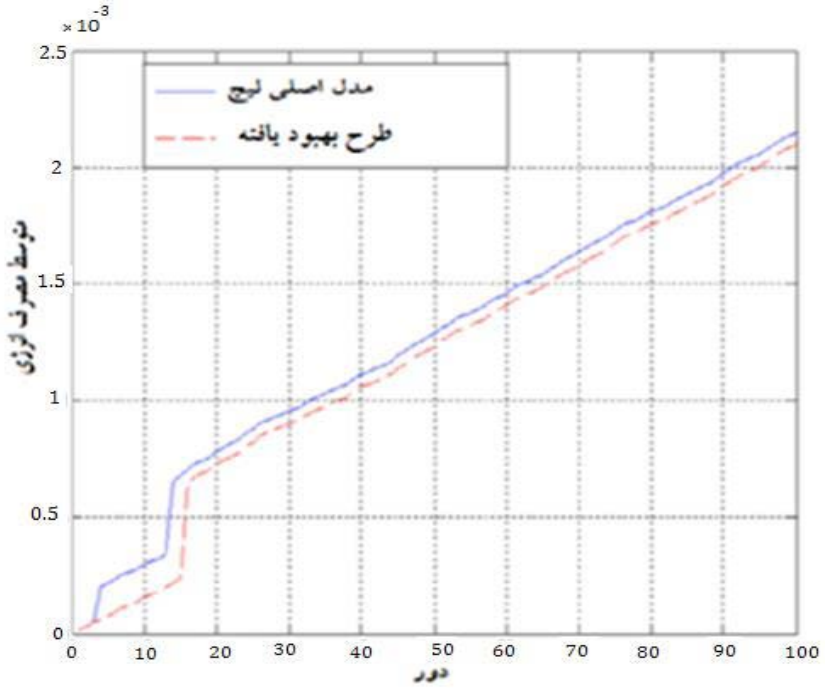
پاسخ حمله	N	Y
تکرار حمله	N	Y
حمله سیبیل	Y	Y

1 - **کل بار شبکه ارتباطی در مرحله انتخاب سرخوشه‌ها**



شکل 5-3 : آزمایش اول

b – در این آزمایش تغییر از دور پنجم صورت گرفته است.



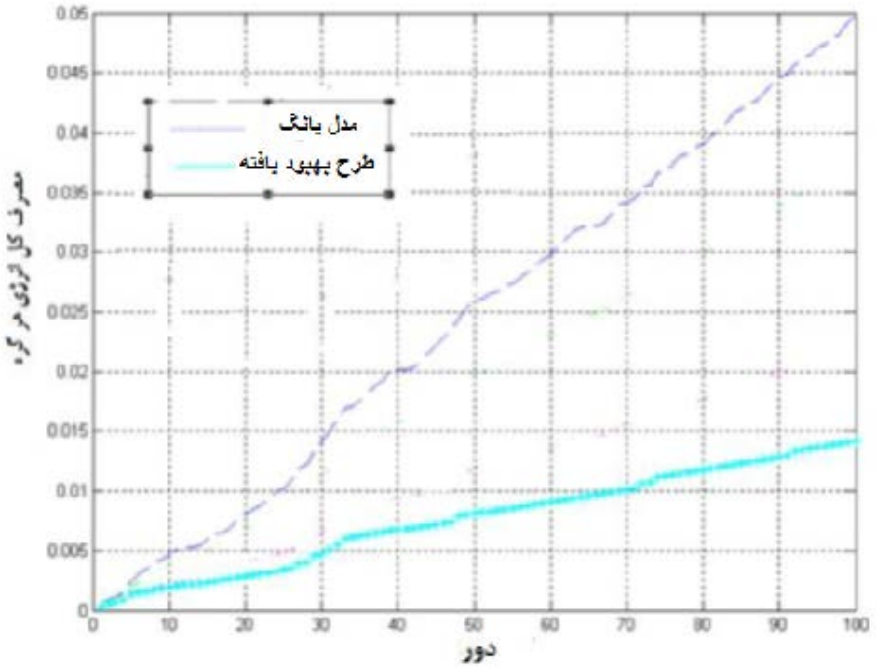
شکل 5-4: آزمایش دوم

b – در این آزمایش تغییر از دور سوم صورت گرفته است.

در این 2 آزمایش می‌توانیم ببینیم که معمولاً مصرف انرژی به‌طور متوسط در $[2.5\times10^{-3}]$، 100 دور برای انتخاب سرخوشه است. در مقایسه با مدل اصلی، مدل ما انرژی را در مرحله شکل‌گیری سرخوشه‌ها کاهش می‌دهد . در مدت زمان کوتاه، الگوریتم استخراج‌شده بهبود یافته است. بهبود قابل‌توجه‌ی در وضع مصرف انرژی در مقایسه با مدل اصلی دارد.

7-2:بار مصرف انرژی هر گره

در طرح پیشنهادی با توجه به شکل 5-5 در ابتدای دور به‌روزرسانی، تفاوت آن‌چنان بزرگ نیست، بااین‌حال، بعدازآن، تفاوت بیشتر و بیشتر می‌شود. مصرف انرژی نسبت به مدل یانگ به حداقل رسیده است. پتانسیل زیادی برای انطباق با مقیاس بزرگ شبکه حسگر بی‌سیم پویا را دارد. در این طرح، ذخیره کلید کمتری نسبت به طرح‌های دیگر دارد، به همین علت سربار حافظه بسیار کوچک است. علاوه برای، در همان زمانی که هدف صرفه‌جویی در مصرف انرژی است از طریق احراز اصالت، ما می‌توانیم امنیت شبکه را تضمین کنیم، به این دلیل که مصرف تأخیر آن بسیار کم است.



8-پیشنهادات:

ازآنجاکه نتایج حاصل از این تحقیق نسبت به روش‌های قبلی رضایت‌بخش‌تر بوده است، ازاین‌رو می‌توان برای مطالعات آتی با توسعه علم و فناوری، بسیاری از برنامه های بین شبکه های مختلف و نحوی اطمینان از امنیت در ارتباطات سیار بین شبکه های مختلف وجود داشته که در آینده این کارها مورد مطالعه بیشتر قرار می گیرند

9- منابع:

[1] G.J. Pottie, W. J. Kaiser, 2007 "**Wireless Integrated Network Sensors**", in communications of the ACM, , vol 43(5) pages 51-58.

[2] Maytham Safar, Hasan Al-Hamadi, Dariush Ebrahimi, 2011 "**PECA:Power Efficient Clustering Algorithm for Wireless Sensor Networks**", International Journal of Information Technology and Web Engineering, 6(1January-March, pages 49 -58

[3] Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari, 2011 "**Energy Efficient clustering Algorithms in Wireless Sensor Networks: A Survey,** IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September, pages – 259 – 268.

[4] D. J. Dechene, A. El Jardali, M. Luccini, and A. Sauer, "**A Survey of Clustering Algorithms for Wireless Sensor Networks**".

[5] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, (2008) " **Wireless sensor networks: a survey**", Computer Networks 38 393–422,

[6] Ossama Younis, Marwan Krunz, and Srinivasan Ramasubramanian, University of Arizona, 2009 "**Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges, IEEE Network** " May/June, pages 20-25.

[7] Vivek Katiyar, Narottam Chand, Surender Soni, (2011), "**A survey on Clustering Algorithms for heterogeneous wireless sensor Networks**" , Int. J. Advanced Networking and applications Volume: 02, Issue: 04, Pages: 745-754.

[8] Srie Vidhya Janani. E, Ganeshkumar.P, Vasantha Suganthi.G, Sultan.M, Kaleeswaran. D, 2013 "**A Survey on Algorithms for Cluster Head Selection in WSN**", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, May.

[9] Huseyin O¨ zgu¨r Tan and I˙brahim Ko¨rpeog˘lu, "**Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks**" .

[10] C.E.Nishimura and D.M.Conlon, "**IUSS dual use: Monitoring of whales and earthquakes using SOSUS,**" Mar. Technol. Soc. J., vol. 27, no. 4.

[11] Bettstetter, C., 2008"**The cluster density of a distributed clustering algorithm in ad hoc networks,**" Communications, 2008 IEEE International Conference on , vol.7, no., pp.4336,4340 Vol.7, 20-24 June