اولین همایش منطقه ای رویکردهای نوین در مهندسی کامپیوتر و فناوری اطلاعات
۵ خرداد ۱۳۹۰ - رودسر
Roudsar 2011

# کاهش میزان نفوذپذیری گره‌های ناشناس با طراحی یک واحد امنیتی در شبکه حسگرهای بی‌سیم

حکمت محمدزاده[۱]، شاپور جودی بیگدیلو[۲]، بهبود خردمند[۳]

[۱] هیأت علمی گروه کامپیوتر، دانشگاه آزاد اسلامی واحد پارس آباد مغان، پارس آباد مغان
Hekmat@iaupmogan.ac.ir
[۲] هیأت علمی گروه کامپیوتر، دانشگاه آزاد اسلامی واحد پارس آباد مغان، پارس آباد مغان
Joudi@iaupmogan.ac.ir
[۳] بورسیه هیأت علمی گروه کامپیوتر، دانشگاه آزاد اسلامی واحد پارس آباد مغان، پارس آباد مغان
Kheradmand@iaupmogan.ac.ir

## چکیده

**در شبکه‌های بی‌سیم که از سیگنال‌های رادیویی جهت تبادل اطلاعات استفاده می کنند. با استفاده از این سیگنال‌ها نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرتمند این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس‌دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب توسط گره‌های نفوذگر فراهم می شود. بر همین اساس در این مقاله روشی برای افزایش امنیت در شبکه حسگرهای بی‌سیم با طراحی یک واحد امنیتی برای سرخوشه ارائه شده است، که نفوذپذیری گره‌های مزاحم ناشناس به گره‌های حسگر که اطلاعات را به سرخوشه ارسال می کنند، کاهش می دهد. واحد امنیت با بکارگیری شیفت رجیسترهای بازخور(LFSR)، کلیدی را برای هر گره در نظر می‌گیرد، تا هر گره داده خود را با آن کلید رمز کرده و به گره بعدی ارسال کند. با این روش ضریب امنیت برای شبکه‌هایی با فعالیت ویژه و وظایف حساس افزایش خواهد یافت.**

## کلمات کلیدی

**شبکه حسگرهای بی‌سیم، سرخوشه، شیفت رجیسترهای بازخور خطی، واحد امنیتی.**

## ۱ - مقدمه

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم توانایی طراحی و ساخت حسگرهایی را با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربری‌های گوناگون داده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی بر اساس نوع حسگر، پردازش و ارسال آن اطلاعات را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های موسوم به شبکه‌های حسگر بی‌سیم شده‌اند [1]. یک شبکه حسگر متشکل از تعداد زیادی گره‌های حسگری است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می‌پردازند. لزوماً مکان قرار گرفتن گره‌های حسگری، از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد، که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم[2].

یکی از خصوصیت‌های منحصر به فرد شبکه‌های حسگر، توانایی همکاری و هماهنگی بین گره‌های حسگری است. هر گره حسگر روی برد خود دارای یک پردازشگر است و به جای فرستادن تمامی اطلاعات خام به مرکز یا به گره‌ای که مسئول پردازش و نتیجه‌گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه و ساده را روی اطلاعاتی که به دست آورده است، انجام می‌دهد و سپس داده‌های نیمه پردازش شده را ارسال می‌کند. ترکیب صدها و یا هزاران حسگر کوچک امکانات جدیدی را عرضه می‌کند. در واقع قدرت شبکه‌های حسگر بی‌سیم در توانایی به‌کارگیری تعداد زیادی گره کوچک است که خود قادرند سرهم و سازماندهی شوند و در موارد متعددی چون مسیریابی

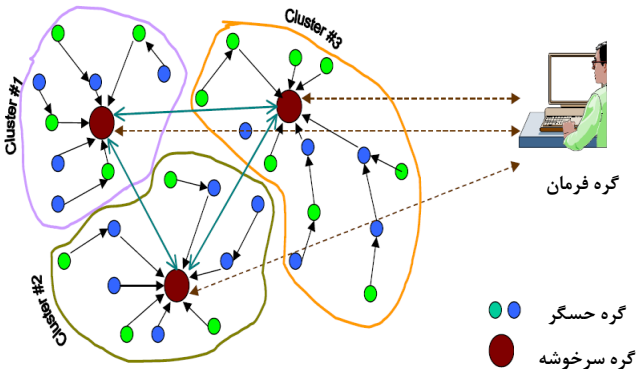
همزمان، نظارت بر شرایط محیطی، نظارت بر سلامت ساختارها یا تجهیزات یک سیستم به کار گرفته شوند[3]. با این توصیفات امنیت در این شبکه‌ها امری ضروری است.

شبکه‌های بی سیم با استفاده از سیگنال‌های رادیویی جهت تبادل اطلاعات عمل می کنند. که نفوذگران و یا گره‌های ناشناس با استفاده از این سیگنال‌ها قادرند در صورت شکستن موانع امنیتی این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده که منجر به دست‌یابی غیرمجاز به اطلاعات حیاتی، حمله به سرویس‌دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد. بر همین اساس در این مقاله روشی برای افزایش امنیت در شبکه حسگرهای بی‌سیم با طراحی یک واحد امنیتی برای سرخوشه ارائه شده است، که نفوذپذیری گره‌های مزاحم ناشناس به گره‌های حسگر که اطلاعات را به سرخوشه ارسال می کنند، کاهش می یابد. این واحد امنیت با بکارگیری شیفت رجیسترهای بازخور(LFSR)، کلیدی را برای هر گره در نظر می گیرد، تا هر گره داده خود را با آن کلید رمز کرده و به گره بعدی ارسال کند. این روال ادامه می یابد تا داده به سرخوشه برسد. در نهایت تنها شناسه گره اول و گره ماقبل سرخوشه به همراه داده رمز شده به سرخوشه ارسال می شود. سرخوشه با استفاده از جدول مسیر بهینه و جدول مشخصه گره‌ها قادر به رمزگشایی داده مربوطه است، تا آن را به ایستگاه پایه ارسال کند. با پیاده سازی این روش ضریب امنیت برای شبکه حسگرهای بی سیم افزایش می یابد.

ساختار این مقاله بدینصورت سازماندهی شده است قسمت ۲ با شبکه حسگرهای بی‌سیم مبتنی بر سرخوشه آشنا می شویم. در قسمت ۳ به بررسی LFSR ها و ویژگی های آنها مورد بررسی قرار می گیرد، و در قسمت ۴ هم طرح پیشنهادی جهت افزایش امنیت در شبکه‌های حسگر بی‌سیم ارائه می گردد.

## ۲–شبکه‌های حسگر بی‌سیم مبتنی بر سرخوشه

شبکه حسگر متشکل از گره‌هایی است که با محدودیت انرژی مواجه هستند. بنابراین نگهداری انرژی مصرفی در ارتباط با گره‌های ناظر با آرایش‌بندی‌های چندتایی و تکنولوژی‌های مسیریابی با آگاهی از میزان انرژی در مقاله‌های دیگر پیشنهاد شده است[5,6]. این تکنولوژی ها سرباری را تحمیل می کنند. برای جلوگیری از چنین سربارهایی و مصرف انرژی نامتعادل، تعدادی گره‌هایی با انرژی بالا که سرخوشه نامیده می شوند، در شبکه مستقر می شوند. این گره‌ها گروهی از حسگرها را در سیستم برای شکل‌گیری خوشه‌های متمایز و مدیریت این خوشه‌ها بکار می گیرند[1]. همچنین در این مقاله نیز جهت بالا بردن امنیت تبادل اطلاعات، صحت داده‌های ارسالی را بررسی می نماییم.

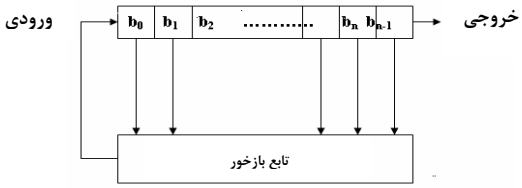



**شکل (۱): خوشه بندی شبکه حسگرها با سرخوشه‌های چندتایی**

بر اساس شکل (۱) خوشه‌ها بر اساس این که روی کدام سرخوشه قرار گرفته، شکل می‌گیرد و ارتباط بین آنها به فاصله‌شان بستگی دارد[8]. هر حسگر فقط به یک سرخوشه متعلق است و ارتباط با ایستگاه پایه از طریق سرخوشه هر خوشه صورت می‌گیرد. در قسمت ۴ طرح پیشنهادی واحد امنیت برای سرخوشه را خواهیم دید تا اطلاعات ارسالی به ایستگاه پایه حدالمقدور مطمئن باشد.

## ۳ – شیفت رجیسترهای بازخور خطی (LFSR[۱])

اجزاء تشکیل دهنده شیفت رجیستر بازخور، تابع بازخور[۲] و شیفت رجیستر می‌باشند. شیفت رجیستر عبارتست از تعدادی عنصر تأخیری که در کنار هم چیده شده‌اند و هر کدام قابلیت ذخیره‌سازی یک بیت را دارد. و دارای یک ورودی و یک خروجی می‌باشد. طول یک شیفت رجیستر برحسب بیت حساب می‌شود و شامل تعداد بیت‌هایی است که می‌توانند در شیفت رجیستر قرار بگیرند. اگر یک شیفت رجیستر n بیتی نامیده شود به این معناست که n عنصر تأخیری (۰و۱و۲و... و n-۱) در کنار هم قرار گرفته‌اند. با وجود n بیت در داخل شیفت رجیسترها، در هر واحد زمانی یک بیت به عنوان خروجی درنظر گرفته می‌شود. شکل(۲) نمای کلی یک شیفت رجیستر بازخور را نشان می دهد.

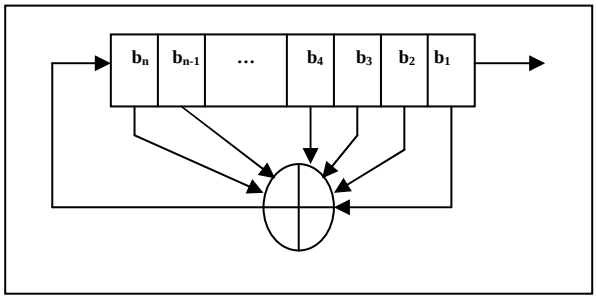



**شکل (۲): شیفت رجیستر بازخور**

تابع بازخور نیز عبارتست از تابعی که بر روی بیتهای مشخصی از شیفت رجیستر عمل می‌کند و مقدار حالت n-۱ را تولید می‌کند، البته درحالت ساده‌تر این تابع همان XOR درنظر گرفته می‌شود. تابع بازخور را می‌توان بصورت زیر درنظر گرفت.

$$F(b_0, b1 \ldots b_{n-1}) = c_0b_0 + c_1b_1 + \ldots + c_{n-1}b_{n-1}$$

ثابتهای $C_{n-1},\ldots,C_1,C_0$ ضرایب بازخور نامیده می‌شوند و به عنوان سوئیچ درنظر گرفته می‌شوند. به طوریکه اگر $C_1$=۱ باشد سوئیچ بسته است. در غیر اینصورت سوئیچ باز است. شکل (۳) یک شیفت رجیستر بازخور خطی را نشان می دهد[10].




**شکل(۳): شیفت رجیستر بازخور خطی**

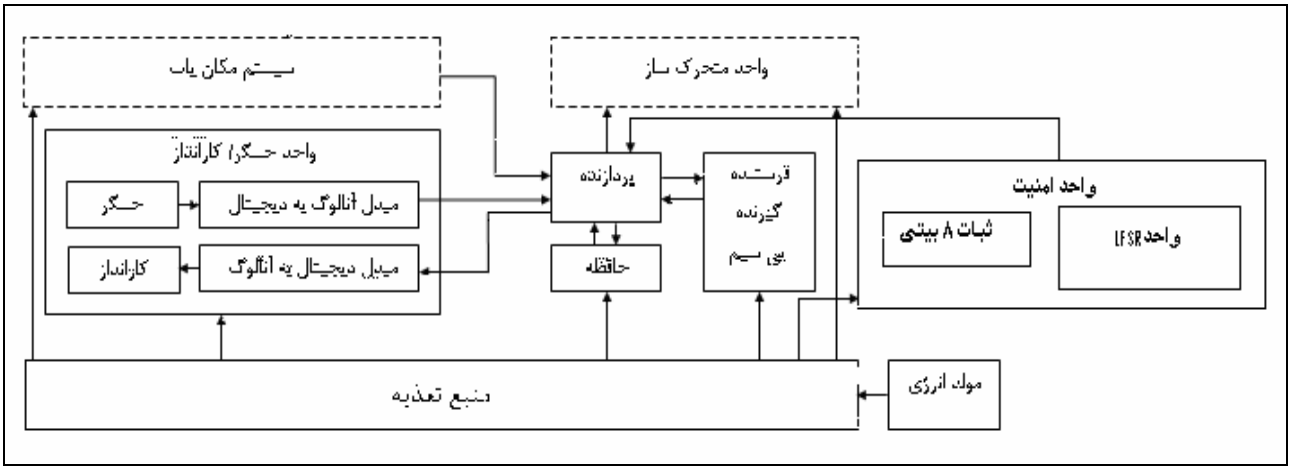
برای تجزیه و تحلیل LFSRها از نظریه‌های ریاضی استفاده می‌شود و رمزنگارها با آنالیز نمودن دنباله‌ها متقاعد می‌شوند که دنباله حاصل بقدر کافی تصادفی می‌باشد که امن هم باشد. به همین دلیل LFSRها پرکاربردترین نوع شیفت رجیسترها هستند که در رمزنگاری استفاده می‌شود[11].

## ۴- طراحی واحد امنیت برای سرخوشه

طرح پیشنهادی برای افزایش امنیت در شبکه حسگرها این است که به سرخوشه هر شبکه واحد کوچکی بنام واحد امنیت اضافه می کنیم. این واحد شامل یک ثبات ۸ بیتی و یک مولد اعداد شبه تصادفی سخت افزاری مانند LFSR است. کارکرد این سیستم به این ترتیب است که ابتدا توسط گره ناظر یک کلید به سرگروه ها داده می شود. این عطای کلید به هر سرگروه دارای چندین مزیت است:

- در صورت دریافت اطلاعات نادرست شناسایی خوشه معیوب امکان پذیر است و گره ناظر باید مساله را بررسی کند.
- درصورت خرابی یا وجود اشکال در یک سرخوشه جایگزینی آن توسط سرخوشه دیگر امکان پذیر است.

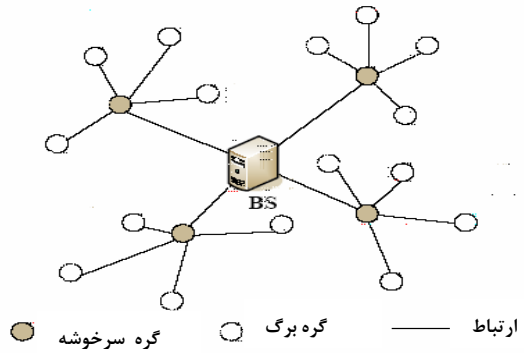
بعد از تخصیص کلیدها به سرخوشه‌ها، هر سرخوشه با واحد امنیت پیشنهادی مطابق با شکل (۴) برای هر گره موجود در خوشه خودش یک مقداری را به عنوان مقدار شناسایی تخصیص می دهد.




**شکل(۴): واحد امنیت برای سرخوشه**

با تخصیص این مقدار به هر گره، زمانی که گرهی می خواهد داده‌ای را به سرخوشه خود ارسال کند، ابتدا با این کلید آن داده را رمز می‌کند، سپس گره اول عدد شناسایی خود را به داده اضافه می کند و به گره بعدی ارسال می کند، گره بعدی نیز داده را با کلید مربوط به خود دوباره رمز کرده با اضافه کردن عدد شناسایی مربوط به خود آن را به گره بعدی ارسال می کند. این گره ابتدا عدد شناسایی گره ماقبل خود را چک می‌کند (شناسایی همسایه‌اش) سپس داده را رمز کرده و شماره شناسایی گره ماقبل خود را حذف کرده و عدد شناسایی خود را اضافه می‌کند. این کار ادامه می یابد تا داده رمز شده به گره ماقبل سرخوشه برسد، گره ماقبل سرخوشه عدد شناسایی همسایه‌اش را حذف کرده و شماره خود را اضافه می کنند. تا زمانیکه داده رمز شده به سرخوشه رسید. با توجه به این که کلید مربوط به هر گره با شماره آن در جدول مربوطه اش در واحد حافظه سرخوشه موجود است و همچنین در جدول مسیر

[12]، مسیر طی شده از گره نخست و گره آخر موجود است. همچنین گره نخست شماره خود را همراه داده ارسال می نماید. بنابراین سرخوشه قادر است مسیر طی شده توسط داده را شناسایی و داده رمز شده را رمزگشایی کند. همچنین برای جلوگیری از حمله تصاحب سرخوشه[۳] با توجه به اینکه این گره شامل اطلاعات اساسی خوشه است، پیشنهاد می‌شود جنس این گره از سخت‌افزارهای مقاوم[۴] ساخته شود[3]. با این روش پیشنهادی حتی در صورت شنود داده‌ها هم باید رمزگشایی شود. همچنین اگر گرهی مورد حمله تصاحب گره دیگر شد، فقط کلید مربوط به آن گره و شماره شناسایی همسایگانش را بدست می آورد. در مقابل اگر گره مزاحم در چرخه ارسال داده شرکت کند توسط همسایگانش قابل شناسایی است. شکل(۵) نحوه انتقال داده تا سرخوشه و چاهک[۵] را نشان می دهد.




**شکل (۵): انتقال داده ها تا سرخوشه و چاهک**

## ۵ – نتیجه گیری و کارهای آتی

با توجه به اهمیت امنیت در شبکه حسگرهای بی‌سیم، ارسال اطلاعات بین گره‌ها بایستی به حد کافی امن و قابل اعتماد باشد. در این مقاله روشی برای افزایش امنیت در شبکه حسگرهای بی‌سیم با طراحی یک واحد امنیتی برای سرخوشه ارائه شد، که نفوذپذیری گره‌های مزاحم ناشناس به گره‌های حسگر را کاهش می‌دهد. در روش ارائه شده اطلاعات ارسالی بین گره‌ها توسط LFSR رمز می‌شوند، تا در صورت استراق سمع هم نیاز به رمزگشایی باشد. در این نوع رمزنگاری سرخوشه نقش حیاتی در خوشه و رمزگشایی اطلاعات دارد، که پیش فرض این است که جدول مسیر در سرخوشه موجود است. در کارهای بعدی سعی می شود داده بین گره‌ها طوری رمز شود که سرخوشه بدون نیاز به جدول مسیر و جدول کلیدها تا با دانستن کلید گره ماقبل آخر داده را رمزگشایی نماید، همچنین داده ارسالی از سرخوشه به گره ناظر نیز رمز شود.

## مراجع


[1] G.Gupta, M.Younis "Fault -Tolerant Clustering of Wireless Sensor Networks", IEEE, pp.1579-1584, 2003.

[2] L.Eschenauer and Virgil D.Gligor, "A key management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47, November 2002.

[3] H.Chan, A.Perrig, and D.Song, "Random key predistribution schemes for sensor networks", In IEEE Symposium on Research in Security and Privacy, 2003.

[4] F.An, X.Cheng, J.M. Rivera, J.Li, and Z.Cheng, "PKM: A Pairwise Key Management Scheme for Wireless Sensor Networks", ICCNMC, 2005.

[5] S.Singh, M.Woo and C.S.Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks", Proceedings of ACM MOBICOM'98, Dallas, Texas, October 1998.

[6] D.Estrin, R.Govindan, J.Heidemann, and S.Kumar, "Scalable Coordination in sensor networks", Proceedings of ACM/IEEE MobiCom 1999, Seattle, Washington, August 1999.

[7] H.Wang, D.Luo, Feife.i Chen and Z.i Li, "Study on Dynamic Key Management of Clustered Sensor Networks", International Journal of Computer Science and Network Security, Vol.6, No.6, June 2006.

[8] G.Gupta, M.Younis, “Load-Balanced Clustering in Wireless Sensor Networks”, Submitted to the IEEE International Conference on communications (ICC 2003), Anchorage, Alaska, May 2003.

[9] C.Karlof and D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, In First IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003.

[10] M.Goresky, A.Klapper, Fibonacci and Galois, "Representations of Feedback-With-Carry Shift Registers", IEEE Trans. on Inform. Theory, vol. 48, pp. 2826−2836, November 2002.

[11] T.Lai Win, N.Christina Kyaw, "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)", World Academy of Science, Engineering and Technology, 2008.

[12] N. Sengottaiyan, R.Somasundaram, "A Modified Routing Algorithm for Reducing Congestion in Wireless Sensor Networks" European Journal of Scientific Research ISSN 1450-216X ,Vol.35, No.4 , pp.529-536, 2009.


## زیرنویس‌ها

۱- Linear Feedback Shift Register
۲- Feedback Function
۳- Node Capture attack
۴- Temper-proof hardware
۵- Sink