# ارائه روش سنجش طیف مقاوم در برابر حملات خون‌آشام برای شبکه‌های حسگر بی‌سیم شناختگر

شیرین اسدالهی خیبری [۱]، مرتضی شفیعی [۲]

[۱] کارشناسی ارشد امنیت اطلاعات، دانشکده فناوری و امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران، Shirin.Asadollahi@gmail.com

[۲] عضو هیئت علمی، دانشکده فناوری و امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران، Mshafiee@iust.ac.ir

**چکیده - شبکه حسگر بی‌سیم شناختگر نسل جدیدی از شبکه‌های حسگر بی‌سیم است که با بهره‌گیری از سنجش طیف موجب بهبود کارایی، دسترس‌پذیری و کیفیت سرویس در این شبکه‌ها شده است. افزودن ویژگی رادیو شناختگری به گره‌های حسگر، شبکه‌های حسگر بی‌سیم را با چالش‌های امنیتی جدیدی مواجه می‌کند. این ویژگی بستری مناسب برای تشدید تخریب ناشی از حملات خون‌آشام که با هدف اتلاف منابع گره‌ها و منع دسترسی به شبکه اجرا می‌شوند، فراهم کرده است. با توجه به حساسیت پیام‌های حاوی داده‌های سنجش طیف، این حملات می‌توانند موجب کاهش کیفیت عملکرد شبکه‌های حسگر بی‌سیم شناختگر شوند و شبکه را به سرعت از دسترس خارج کنند. در این مقاله روشی امن برای سنجش طیف در شبکه‌های حسگر بی‌سیم شناختگر با هدف کاهش تاثیر حمله خون‌آشام در عملکرد شبکه ارائه می‌کنیم. روش پیشنهادی ضمن سازگاری با منابع محدود گره‌های حسگر در برابر این حمله نیز مقاوم می‌باشد. نتایج حاصل از شبیه‌سازی نشان می‌دهد که با حمله به شبکه و مرگ ۷۱ درصد از گره‌ها، اختلال قابل ملاحظه‌ای در عملکرد سنجش طیف به وجود نمی‌آید و این روش در حضور مهاجم با موفقیت به سنجش طیف ادامه خواهد داد.**

کلید واژه- سنجش طیف، امنیت شبکه، شبکه حسگر بی‌سیم شناختگر، حمله خون‌آشام.

## ۱- مقدمه

شبکه حسگر بی‌سیم از تعداد زیادی گره حسگر تشکیل شده است که به صورت تصادفی در محیط پراکنده می‌شوند و با استفاده از ارتباطات رادیویی برای شناسایی، جمع‌آوری اطلاعات و بررسی وضعیت محیط اطراف خود با یکدیگر همکاری می‌کنند. این گره‌ها عموما کوچک با حافظه و توان پردازشی پایین هستند که انرژی مورد نیاز خود را از طریق باتری تامین می‌کنند. گره‌های حسگر بی‌سیم برای ارتباطات خود از باندهای فرکانسی محدود و بدون مجوز ISM[۱] و UNII[۲] به صورت مشترک با کاربردهای بی‌سیم دیگر مانند بلوتوث و وای- فای استفاده می‌کنند. رشد روزافزون کاربردهای بی‌سیم و عدم افزایش باند فرکانسی موجب تنزل کارایی، قابلیت اعتماد و دسترس-پذیری در این شبکه‌ها شده است [۱].

در حال حاضر به‌کارگیری الگوریتم‌های سنجش طیف در شبکه‌های حسگر بی‌سیم به عنوان راه‌حلی برای استفاده بهینه از طیف رادیویی و دسترسی به باندهای فرکانسی بیشتر ارائه شده است. محدودیت‌های گره‌ها در شبکه حسگر بی‌سیم، افزودن قابلیت رادیو شناختگری به این شبکه‌ها را با چالش‌های بسیاری روبرو می‌کند. چالش‌های پیاده‌سازی سنجش طیف در شبکه‌های حسگر بی‌سیم را می‌توانیم به سه دسته تقسیم کنیم: میزان مصرف منابع شبکه، کیفیت عملکرد الگوریتم و امنیت. روش‌های مطرح شده برای پیاده‌سازی یک الگوریتم باید از هر سه دیدگاه ارزیابی شوند.

از نقطه نظر میزان مصرف منابع، محاسباتی که برای اجرای سنجش طیف به گره‌ها سپرده می‌شود باید تا حد ممکن ساده باشد. هم‌چنین روش اجرا نباید ترافیک شبکه را به گونه‌ای افزایش دهد که با ارزش‌ترین منبع شبکه یعنی توان باتری گره‌ها برای انتقال تعداد زیادی پیام مصرف شود [۲] [۳].

از دیدگاه کیفیت عملکرد سنجش طیف باید در نظر داشت که به دلیل وابستگی شدید صحت عملکرد شبکه‌های حسگر بی‌سیم شناختگر به داده‌های سنجش طیف، پروتکل‌ها و الگوریتم‌هایی که برای این شبکه‌ها طراحی می‌شوند باید سطحی از تحمل‌پذیری خطا را داشته باشند. همچنین با توجه به بلادرنگ بودن فرآیند سنجش طیف، محاسبات تخمین طیف باید در زمان قابل قبولی خاتمه یابد.

از منظر امنیت نیز اطمینان از مصونیت محاسبات هر گره در برابر نابودی و جلوگیری از فاش شدن نتیجه نهایی فرآیند سنجش طیف بسیار حائز اهمیت است. به عبارت دیگر فرآیند سنجش طیف باید به نحوی پیاده‌سازی شود که ازدست رفتن بخشی از محاسبات تاثیر چندانی بر نتیجه محاسبات مرحله نهایی الگوریتم نداشته باشد [۳]

---

[1] Industrial, Scientific and Medical

[2] Unlicensed National Information Infrastructure

[۴].

در [۵] روشی برای سنجش طیف در شبکه های حسگر بی‌سیم شناختگر بر اساس الگوریتم MTM عنوان شد که بر دو ویژگی خاص این الگوریتم استوار است. اولا الگوریتم MTM دارای محاسباتی با بخش‌های مجزا و یکسان است و ثانیا محاسبات هر بخش مستقل از بخش‌های دیگر اجرا می‌شود و پیچیدگی زمانی، مکانی و محاسباتی تمام بخش‌های آن با هم برابر است. در این مقاله سعی داریم تا امنیت روش مطرح شده را در برابر حمله خون‌آشام مورد بررسی و آنالیز دقیق‌تر قرار دهیم.

ابتدا معرفی مختصری در رابطه با حملات خون‌آشام در شبکه‌های حسگر بی‌سیم در بخش ۲ و روش سنجش طیف پیشنهادی در بخش ۳ ارائه می‌شود. بخش ۴ را به تشریح نتایج حاصل از شبیه‌سازی به همراه ارزیابی امنیتی روش پیشنهادی اختصاص داده‌ایم و در بخش ۵ نیز به جمع‌بندی نتایج به دست آمده می‌پردازیم.

## ۲- حملات خون‌آشام

یکی از جدیدترین انواع حملات تخلیه باتری که در سال ۲۰۱۴ مطرح و مورد بررسی قرار گرفته است حملات خون آشام هستند. در این حملات مهاجم با تشکیل و ارسال پیام‌هایی جعلی، گره‌های بخشی از شبکه را برای ارسال این بسته‌های پیام فریب می‌دهد و باعث افزایش تاخیر و مصرف انرژی اجزای شبکه می‌شود. ویژگی‌های این حملات عبارتند از:

- مختص پروتکل یا نوع پیاده‌سازی خاصی نیستند.
- از پیام‌های سازگار با پروتکل‌های شبکه استفاده می‌کنند تا پیام‌های مخرب به سادگی قابل ردیابی نباشند.
- در این حمله گره قربانی داده‌های کمی را با مصرف انرژی زیادی منتقل می‌کند.
- اگر تعداد گره‌های واقع در محل وقوع حمله برابر Log(N) باشد حمله خون‌آشام می‌تواند مصرف انرژی گره‌های آن بخش از شبکه را با سرعت O(N) افزایش دهد.
- روش‌های مانیتورینگ مصرف انرژی گره و دنبال کردن مسیر می‌توانند مصرف انرژی گره را در هر بار اجرای حمله تا ۳۰ درصد کاهش دهند اما این روش‌ها امکان جلوگیری از اجرای مجدد حمله را ندارند، زمان‌بر هستند و تضمینی برای تشخیص صحیح حمله وجود ندارد.

به دلایلی که ذکر شد بسیار اهمیت دارد تا تاثیر این نوع حملات در طراحی و آنالیز پروتکل‌ها و فرآیندهای شبکه حسگر بی‌سیم مورد بررسی و تحلیل قرار گیرند [۳].

## ۳- روش سنجش طیف پیشنهادی

الگوریتم MTM روشی برای سنجش طیف توان است که از یک مجموعه متعامد از دنباله‌های اسلپین مقاوم در برابر نشتی استفاده می‌کند. این دنباله‌ها به عنوان پنجره‌های متعامد چندگانه در نظر گرفته می‌شوند. در این الگوریتم تخمین طیف طبق رابطه (۱) محاسبه می‌شود. در این رابطه $K$ تعداد دنباله‌های اسلپین با طول $N$، $|Y_k(f)|^2$ توزیع‌های انرژی برای $k$های مختلف و $\lambda_k$ مقادیر ویژه متناظر با بردارهای اسلپین هستند [۸-۶].

$$\hat{S}(f)=\frac{\sum_{k=0}^{k-1}\lambda_\kappa\cdot|Y_k(f)|^2}{\sum_{k=0}^{k-1}\lambda_k} \qquad (۱)$$

در روش ارائه شده در [۵] اجرای محاسبات هر پنجره به گرهی جداگانه محول شده است. در هر گره نمونه‌های دریافت شده از محیط در دنباله‌های اسلپین که به ازای هر پنجره جداگانه محاسبه می‌شوند ضرب شده، پس از گرفتن تبدیل فوریه به توان ۲ می‌رسند. حاصل این عملیات بر مجموع دنباله‌های اسلپین تقسیم می‌گردد و نتیجه آن به سرخوشه ارسال می‌شود.

سرخوشه حاصل‌جمع پنجره‌هایی که توسط این پیام‌ها دریافت کرده است را محاسبه می‌کند تا مقادیر تابع $\hat{S}(f)$ تولید شود. محاسبات سرخوشه در این روش در ۳ مرحله انجام می‌شود: دریافت پیام‌های حاوی تخمین جزئی طیف، محاسبه $\hat{S}(f)$ و مقایسه مقادیر $\hat{S}(f)$ با حد آستانه برای تشخیص حفره‌ها.

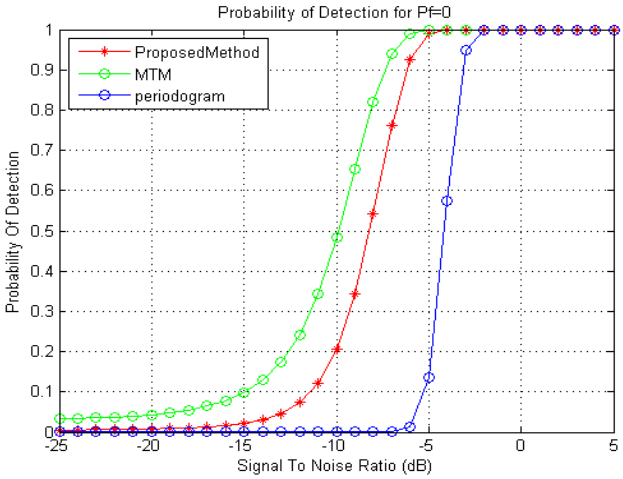
## ۴- نتایج شبیه‌سازی

روش پیشنهادی در شبکه‌ای با ۶ گره عادی و یک سرخوشه با استفاده از ابزار TrueTime نسخه ۲-β۷ شبیه‌سازی شده است. تعداد گره‌های عادی براساس تعداد پنجره‌های الگوریتم MTM در شرایط $P_f$=0 انتخاب شده‌اند و حمله خون‌آشام با حضور گره مهاجمی از نوع گره‌های عادی شبکه شبیه سازی شده است [۵].

در این شبیه‌سازی پس از گذشت ۰/۰۴ ثانیه از آغاز حمله، مصرف انرژی گره‌های قربانی افزایش یافته و توان باتری گره‌ها ۳/۹ ثانیه پس از آغاز حمله خاتمه یافته و از توپولوژی حذف می‌شوند.

نمودار احتمال کشف روش پیشنهادی، الگوریتم MTM و آشکارساز انرژی در نرخ سیگنال به نویزهای متفاوت در شکل ۱ نمایش داده شده است. در این شکل عملکرد این سه روش در شرایط عادی و بدون حضور مهاجم با N= ۴۰۰ و k=۶ برای روش پیشنهادی و الگوریتم MTM (که N تعداد نمونه و k تعداد پنجره‌ها است) و N= ۴۰۰۰ برای الگوریتم آشکارساز انرژی با در نظر گرفتن $P_f$= ۰ رسم شده است. در این شبیه‌سازی از حد آستانه ارائه شده در [۹] استفاده کرده‌ایم. مشاهده می‌شود که احتمال کشف روش پیشنهادی در نرخ سیگنال به نویزهای مختلف از الگوریتم MTM ۷/۱ درصد

کمتر است. دلیل این امر اضافه شدن مجدد نویز به تخمین‌های جزئی طیف در حین ارسال از گره‌های عادی به سرخوشه است. در نرخ‌های سیگنال به نویز پایین‌تر از ۲۰- دسیبل احتمال کشف روش پیشنهادی صفر می‌شود در حالیکه دقت تخمین الگوریتم MTM در بازه [۰-۰/۱] قرار دارد. هم‌چنین مشاهده می‌شود که احتمال کشف روش پیشنهادی در نرخ سیگنال به نویزهای مختلف تقریبا ۳۶ درصد از الگوریتم آشکارساز انرژی بیشتر است.



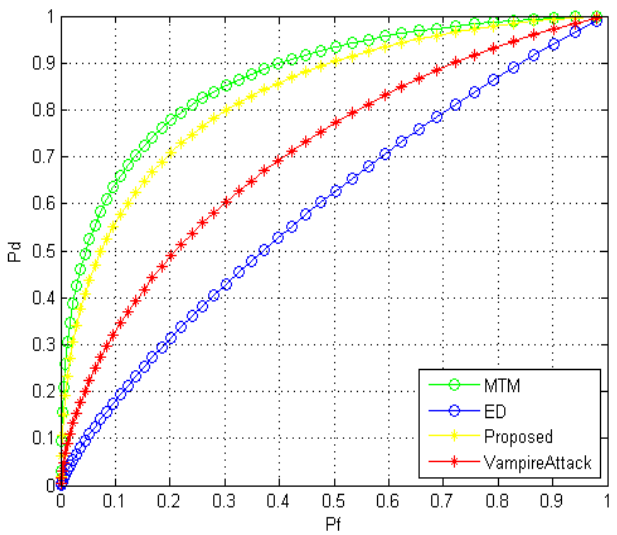

شکل ۱: احتمال کشف روش پیشنهادی، الگوریتم MTM و آشکارساز انرژی

نمودار ROC روش پیشنهادی، الگوریتم MTM و آشکارساز انرژی در شکل ۲ ارائه شده است. لازم به ذکر است که در آنالیز نمودار ROC سطح زیر نمودارها برای مقایسه کیفیت عملکرد دو الگوریتم مورد بررسی قرار گرفته و با توجه به مقدار سطح زیر هر نمودار کیفیت عملکرد روش مربوطه با توجه به جدول ۱ طبقه‌بندی می‌شود [۱۰].

جدول ۱: نحوه طبقه‌بندی نمودارهای ROC

| طبقه‌بندی | عالی (A) | خوب (B) | متوسط (C) | ضعیف (D) | غیر قابل قبول (F) |
|---|---|---|---|---|---|
| AUC[1] | ۱-۰/۹ | ۰/۹-۰/۸ | ۰/۸-۰/۷ | ۰/۷-۰/۶ | ۰/۶-۰/۵ |

[1]Area Under Curve




شکل ۲: نمودار ROC روش پیشنهادی، MTM و آشکارساز انرژی

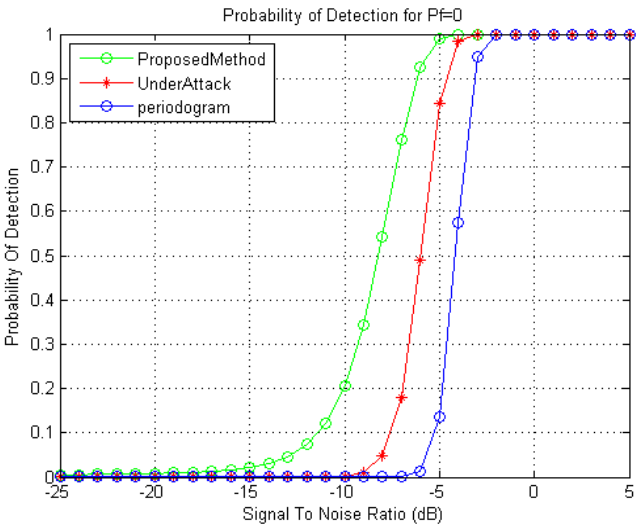
جدول ۲: سطح زیر نمودار ROC

| نمودار ROC | MTM | روش پیشنهادی | حمله خون‌آشام | آشکارساز انرژی |
|---|---|---|---|---|
| AUC | ۰/۸۴۹۲ | ۰/۸۱۲۸ | ۰/۶۸۶۹ | ۰/۵۷۰۹ |
| طبقه‌بندی | B | B | D | F |

با توجه به طبقه‌بندی ارائه شده در جدول ۱ و سطح زیر نمودار اندازه‌گیری شده در جدول ۲ مشاهده می‌شود که روش پیشنهادی و الگوریتم MTM در یک دسته قرار می‌گیرند و این دو روش در شرایط عادی از کیفیت عملکرد خوبی برخوردار هستند. هم‌چنین با توجه به کاهش میزان منابع مورد نیاز برای اجرای محاسبات در روش پیشنهادی این روش با منابع محدود گره‌های حسگر سازگاری بیشتری داشته و بنابراین برای شبکه‌های حسگر بی‌سیم شناختگر مناسب است.

در شرایط بروز حمله خون‌آشام در روش پیشنهادی مشاهده می‌شود که کیفیت عملکرد فرآیند سنجش طیف کاهش یافته و سطح زیر نمودار به دسته ضعیف (D) تنزل می‌یابد در حالیکه کیفیت عملکرد روش آشکارساز انرژی در شرایط عادی غیر قابل قبول بوده و روش پیشنهادی در حضور مهاجم از کیفیت عملکرد بسیار بهتری برخوردار است.

در نمودارهای شکل ۳ نمودار قرمز رنگ مربوط به شبیه‌سازی حمله خون‌آشام است که پس از مرگ ۴ گره سرخوشه توانسته است با ۲ تخمین جزئی $\hat{S}(f)$ را تشکیل دهد. در این شکل مشاهده می‌شود که با حمله به شبکه احتمال کشف روش پیشنهادی نسبت به حالت عادی ۲۱/۹۹ درصد کاهش یافته است. قابل توجه است که با وجود کاهش احتمال کشف در هنگام حمله خون‌آشام در روش پیشنهادی، این روش با اختلاف ۲۲ درصد احتمال کشف بالاتری نسبت به آشکارساز انرژی در شرایط عادی و بدون حضور مهاجم دارد.




شکل۳: احتمال کشف روش پیشنهادی در حمله خون‌آشام

در شبکه‌هایی که به صورت متمرکز سنجش طیف را اجرا می‌کنند زمانی که گرهی از دست برود تمامی اطلاعات مربوط به آن نابود می‌شوند و تعداد محدودی گره شناختگر باقی می‌ماند. اما با توجه به شکل ۳ روش پیشنهادی در برابر این حمله آسیب‌پذیری کمتری دارد زیرا تمامی گره‌های عضو خوشه در اجرای سنجش طیف مشارکت کنند. یک مزیت روش پیشنهادی آن است که اگر سرخوشه به تعداد کافی تخمین جزئی طیف دریافت نکند می‌تواند خود یک تخمین را محاسبه کند تا تخمین صحیح‌تری از طیف داشته باشد. به عبارت دیگر اگر تنها ۱گره عادی بتواند پیام خود را به سرخوشه برساند سرخوشه با محاسبه یک تخمین جزئی طیف دیگر می‌تواند حفره‌های طیفی را مانند شکل ۳ تخمین بزند.

## ۵- نتیجه‌گیری

در این مقاله امنیت روش ارائه شده برای پیاده‌سازی فرآیند سنجش طیف در شبکه‌های حسگر بی‌سیم مورد بررسی و ارزیابی قرار گرفت. این روش دست‌یابی پویا به طیف در حضور مهاجم را براساس طبیعت توزیع شده شبکه با درصد بالایی تضمین می‌کند. بررسی‌های حاصل از تحلیل امنیتی روش پیشنهادی بیانگر آن است که این روش توانسته است در برابر نابودی ۷۱/۵ درصد از داده‌های سنجش طیف به خوبی مقاومت کند. هم‌چنین مشاهده می‌شود که کیفیت عملکرد روش پیشنهادی در حضور مهاجم بهتر از کیفیت عملکرد الگوریتم آشکارساز انرژی در شرایط عادی است. به این ترتیب می‌توان نتیجه گرفت که روش پیشنهادی توانسته است بدون استفاده از مکانیزم‌های امنیتی رایج علاوه بر افزایش صحت فرآیند سنجش طیف با استفاده از الگوریتمی کارآمد، مقاومت آن را نیز در برابر حملات خون‌آشام به طور قابل ملاحظه‌ای افزایش دهد.

از این موارد می‌توان به نتیجه مهمی دست یافت. توزیع محاسبات هر الگوریتمی در شرایطی که اولا محاسبات هر گره عاری از هرگونه وابستگی و ارتباط معنی‌دار با محاسبات بخش‌ها یا گره‌های دیگر باشد، دوما هر موجودیت سطح دانش محدود با حساسیت امنیتی برابر با موجودیت‌های دیگر سیستم داشته باشد و سوما دانش هر موجودیت اطلاعاتی را در مورد نتیجه نهایی محاسبات نشت ندهد، شبکه بدون نیاز به مکانیزم‌های امنیتی سنگین و پیچیده در برابر حملات خون‌آشام با درصد بالایی ایمن خواهد بود.

## مراجع


[1] A. Akyildiz and B. Balakrishna, "*Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey*," Physical Communication, Vol. 4, No. 1, pp. 40-62, 2011.

[2] A. Sen, "Security and Privacy Challenges in Cognitive Wireless Sensor Networks," arXiv preprint arXiv: pp.1302-2253, 2013.

[3] A. Vasserman and B.Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks," IEEE Trans. Mobile Computing, Vol. 12, No. 2, pp. 318-332, 2013.

[4] A. Al-Qasrawi, "*Cognitive Sensor Techniques to Face Security Challenges in C-WSN*," IJCSI International Journal of Computer Science Issues, Vol. 10, No. 2, pp. 33-38, 2013.

[۵] شیرین اسدالهی خیبری، مرتضی شفیعی، "ارائه روش سنجش طیف امن برای شبکه‌های حسگر بی‌سیم شناختگر"، بیستمین کنفرانس ملی سالانه انجمن کامپیوتر ایران، دانشگاه فردوسی مشهد، اسفند ۹۳، صفحات ۱۰۸۷-۱۰۹۲

[6] A. Shafiee and B. Vakili, "*An Approach to Efficient Spectrum Sensing in Cognitive Wireless Sensor Networks*," Applied Mechanics and Materials, Vol. 256, No.259, pp. 4-8, 2013.

[7] A. Shafiee and B. Vakili, "*MTM-based spectrum sensing in cognitive Wireless Multimedia Sensor Networks (C-WMSNs)*," *Proc. Int. Conf. on* Telecommunications (IST), pp. 266-270, 2012.

[8] A. Alghamdi and B. Abu-Rgheff, "*MTM Parameters Optimization for 64-FFT Cognitive Radio Spectrum Sensing using Monte Carlo Simulation*," *Proc. Int. Conf. on* Emerging Network Intelligence , pp. 107-113, 2010.

[9] A. Alghamdi and B. Abu-Rgheff, "Probabilities of Detection and False Alarm in MTM-Based Spectrum Sensing for Cognitive Radio Systems," *Proc. Int. Conf. on* Emerging Network Intelligence, pp. 114-119, 2010.

[10] A. Mahafza, Radar Systems Analysis and Design Using MATLAB Third Edition, CRC Press, 2013.