مقاله پژوهشی

# افزایش بهینه طول عمر شبکه حسگر بی‌سیم پس از حمله اسمورف همراه با استفاده از سیستم تشخیص نفوذ مبتنی بر شبکه و الگوریتم خوشه‌بندی k-mean

Doi: 10.30508/kdip.2024.469585.1108

علی عزتی[۱] | محمدمهدی شیرمحمدی[۲]

۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد همدان، همدان، ایران
۲- استادیار گروه کامپیوتر، دانشگاه آزاد اسلامی واحد همدان، همدان، ایران

تاریخ دریافت: ۱۴۰۳/۰۵/۰۳
تاریخ پذیرش: ۱۴۰۳/۰۸/۰۳
صفحه: ۵۹ - ۵۲

## چکیده

در دهه‌ی اخیر شبکه‌های حسگر بی‌سیم با مشکلات مختلفی روبه رو شده‌اند. یکی از مشکلات اساسی آنها موضوع امنیت است. پیشرفت‌های اخیر در اتصال شبکه و قابلیت‌های محاسباتی، کاربردهای شبکه‌های حسگر بی‌سیم (WSN) را گسترش داده است. جمع‌آوری داده‌ها و انتقال آن به یک سرور دور، که اغلب در مکان‌های ایزوله قرار دارد، هدف اصلی شبکه‌های حسگر بی‌سیم (WSNs) است. این شبکه‌ها ممکن است زیرزمینی، زیرآبی، زمینی یا چندمدلی باشند. از آن‌ها در اتوماسیون صنعتی، مدیریت ترافیک، نظارت بر دستگاه‌های پزشکی و سایر حوزه‌ها استفاده می‌شود. با وجود رشد بازار، شبکه‌های حسگر بی‌سیم با چندین چالش مواجه هستند. کارایی انرژی، محدودیت‌های منابع ذخیره‌سازی و پردازش، پهنای باند، نرخ خطا، مقیاس‌پذیری و بقا در شرایط سخت باید مورد توجه قرار گیرند. با استفاده از برخی روش های امنیت شبکه می‌توان با حملات مقابله کرد اما این روش‌ها بر طول عمر حسگرهای شبکه اثر منفی می‌گذارند و باعث اتلاف انرژی کلی شبکه می‌شوند. در این مقاله با شبیه‌سازی یک شبکه حسگر بی‌سیم ابتدا با استفاده از الگوریتم خوشه‌بندی کا- مین گره‌ها را در خوشه‌های مختلف تقسیم‌بندی کنید که از نظر فاصله با بقیه نودها و نود سرخوشه و همچنین انرژی مصرفی هر نود برای ارسال پیام و فاصله از ایستگاه پایه در بهینه‌ترین حالت ممکن باشند. سپس با شبیه‌سازی حمله اسمورف چند گره بیش از اندازه پیام ارسال می‌کنند، که باعث مصرف انرژی بیش از حد نودها می‌شود، سپس با ایجاد یک سیستم تشخیص نفوذ گره‌های حمله کننده شناسایی و حذف می‌شوند. در این مقاله علاوه بر شناسایی گره‌های حمله کننده گره‌های دیگر که وضعیت آن‌ها عادی نیست را به عنوان گره مشکوک شناسایی و تحت نظر می‌گیرد و در پایان باعث افزایش طول عمر کلی مجموعه با حذف نودهای حمله‌کننده می‌شود.

**کلمات کلیدی:** سیستم تشخیص نفوذ مبتنی بر شبکه، شبکه حسگر بی‌سیم، حمله اسمورف، خوشه‌بندی، الگوریتم کا- مین.

## ۱- مقدمه

شبکه حسگر بیسیم شامل گره‌های مذکور دارای شیوه عملیاتی مشابه با نگهبانان دیجیتال هستند که به‌طور فعال داده‌هایی را در مورد مجموعه‌ای متنوع از ویژگی‌ها جمع‌آوری می‌کنند، از جمله اما نه محدود به فشار، رطوبت، دما، سطح آلودگی، صدا و سایر عوامل مرتبط، همان‌طور که نیازهای خاص برنامه مورد نظر ایجاب می‌کند. در حوزه شبکه‌های حسگر بی‌سیم (WSNs)، گنجاندن تعداد قابل توجهی از گره‌ها که دارای ارتباط قوی هستند، در حیطه شبکه در نظر گرفته می‌شود. این شبکه ممکن است شامل تعداد متغیری از گره‌ها باشد که از چند صد تا چند هزار متغیر است. این گره‌ها تحت هدایت توپولوژی‌های از پیش تعیین‌شده همکاری می‌کنند تا داده‌های ضروری را جمع‌آوری کرده و آن را به یک گره سرور مشخص منتقل کنند (ژو، ژانگ، و هانگ[1]، ۲۰۲۱). طبیعت پویا و شبکه‌های حسگر بی‌سیم (WSNs) نیازمند مطالعه مداوم است، با تمرکز خاص بر توسعه الگوریتم‌های مسیریابی ترکیبی که اکنون به عنوان یک حوزه تحقیقاتی برجسته و پرجنب‌وجوش شناخته می‌شود. هماهنگی مؤثر انتقال داده‌ها از گره‌های عضو به گره مقصد، جایی که فرآیند تجمیع داده‌ها انجام می‌شود، نیازمند استفاده از استراتژی‌های مسیریابی است که از اهمیت بالایی برخوردارند و تأثیر قابل توجهی دارند (جیانگ، ژائو، ژوو، وانگ، و دوو[2]، ۲۰۲۲). توسعه الگوریتم‌های مسیریابی برای شبکه‌های حسگر بی‌سیم (WSNs) شامل چالش‌های زیادی است، از جمله اما نه محدود به موارد مربوط به کارایی انرژی، دوام شبکه، حفاظت از شبکه، تأخیر شبکه و ساختار شبکه. این موانع قابل غلبه هستند؛ با این حال، خالی از چالش نیستند. احتمال مواجهه با چالش‌های بیشتر همیشه وجود دارد (لیو، چنگ، و سانگ[3]، ۲۰۲۲). رشته تکنیک‌های بهینه‌سازی که در دهه‌های اخیر به‌طور سیستماتیک در بسیاری از بخش‌ها مورد استفاده قرار گرفته است، راهی قابل قبول برای پرداختن به چالش‌های چندوجهی ارائه می‌دهد. به‌طور قابل توجهی، استراتژی‌های بهینه‌سازی راه‌حلی مناسب برای مسئله حیاتی کنترل مصرف انرژی در شبکه‌های حسگر بی‌سیم فراهم می‌کنند و بدین ترتیب به ظهور دوره‌ای جدید که با مدیریت شبکه‌ای آگاهانه و دوستدار محیط زیست مشخص می‌شود، کمک می‌کنند (هان، و همکاران[4]، ۲۰۲۲؛ فانگ، مین، ویوو، وانگ، ژائو، مائو[5]، ۲۰۲۲). پیشرفت مداوم شبکه‌های حسگر بی‌سیم (WSNs) به عنوان یک نمونه قابل توجه از منظر هوش مصنوعی، از پتانسیل هم‌افزایی که می‌تواند از طریق ادغام فناوری‌های پیشرفته و رویکردهای هوشمندانه حل مسئله به وجود آید، برای به‌طور مؤثر رسیدگی به چالش‌های پیچیده‌ای که توسط محیط جهانی متصل ما ایجاد می‌شود، نشان می‌دهد (ایکسو، گائو، لیو، دنگ، چین و ما[6]، ۲۰۲۱). دستیابی به هم‌افزایی می‌تواند به عنوان راهی برای غلبه مؤثر بر چالش‌های پیچیده‌ای که توسط زمینه جهانی متصل ما ایجاد می‌شود، دنبال شود. ایجاد این هم‌افزایی می‌تواند از طریق ادغام فناوری پیشرفته با استراتژی‌های هوشمندانه

1- Zhou, Zhang, & Huang
2- Jiang, Zhao, Zhu, Wang, & Du
3- Lv, Cheng, & Song
4- Han, et al
5- Fang, Min, Wu, Wang, Zhao, & Mao
6- Xu, Guo, Liu, Deng, Chen, & Ma

حل مسئله حاصل شود، که به افراد این امکان را می‌دهد تا به طور مؤثر به بسیاری از دشواری‌های ارائه شده توسط جامعه جهانی متصل ما پاسخ دهند (لیو[1]، ۲۰۲۳). در حوزه امنیت هم، مهاجم قادر است اطلاعات رمزنگاری گران‌بهایی را برای تغییر عملکرد به دست آورد. سیستم و برای خرابکردن مدار، که همه از طریق دسترسی فیزیکی به یک شی منجربه تخریب طولانی مدت می‌شود. در ادامه چند حمله ذکر می‌شود.

حمله کانال جانبی: اینترنت اشیا عملیات عادی خود را اجرا می‌کنند، بنابراین احتمال افشای اطلاعات قابل توجهی وجود دارد. ممکن است حتی در مواردی که هیچ پروتکل بی‌سیمی برای انتقال داده توسط آنها پیاده‌سازی نشده، اجرا شود. استراق سمع: این حمله معمولاً با پروتکل‌های ارتباطی مرتبط است، بنابراین احتمال وقوع آن در این سطح، مخصوصاً برای برچسب‌های RFID وجود دارد. هدف اساسی از حمله شنود این است که پیام‌ها رهگیری شده، خوانده می‌شوند و برای انجام کاوش بیشتر اصلاح می‌شوند (لیو،کیائو، و نوواک[2]، ۲۰۲۲). شبیه‌سازی برچسب: این یک نوع حمله، برای هکرها بسیار مفید است، و می‌تواند برای شهرت شرکت نیز خطرناک باشد. مهاجم قادر است به کمک کپی کردن برچسب‌ها به داده‌های حساس و مناطق بسته دسترسی پیدا کند (ایفزامی، تابا، هافیدی، و لامگاری[3]، ۲۰۲۱). این مقاله ظرفیت استفاده از الگوریتم‌های مبتنی برهوش مصنوعی و چندین الگوریتم دیگر را برای محافظت، بهینه‌سازی مصرف انرژی و قابل اتکاء بودن شبکه حسگر بی‌سیم نشان می‌دهد.

## ۲- مبانی نظری

به دنبال گسترش دامنه کاربردهای شبکه‌های حسگر بی‌سیم (WSNs)، مجموعه‌ای غنی از پیشرفت‌های فنی منحصر به فرد به عنوان نتیجه تحقیقات مشترکی که در سال‌های اخیر انجام شده، توسعه یافته است. این امر به دلیل سرعت شگفت‌انگیزی است که شبکه‌های حسگر بی‌سیم در حال افزایش محبوبیت هستند. نمی‌توان این وضعیت را از دیدگاه موجودی که هوش آن در آزمایشگاه ساخته شده است، نادیده گرفت. به‌ویژه، این شبکه‌ها شاهد افزایش استفاده از الگوریتم‌های مسیریابی پیشرفته بوده‌اند که برای ورود به عصر مدرن ارتباطات بسیار مهم هستند، زیرا این الگوریتم‌ها برای به‌روزکردن آنها در عصر کنونی ارتباطات حیاتی هستند (لیو، شی، ژائو، لیو، یین، وژنگ[4]، ۲۰۲۳). FA، GA، ACO، ABC، PSO و BFO برخی از استراتژی‌هایی هستند که پتانسیل کشف در چشم‌انداز وسیع بهینه‌سازی شبکه‌های حسگر بی‌سیم (WSN) را دارند. برای عبور مؤثر از حوزه‌های پیچیده‌ای که برای حل آن‌ها طراحی شده‌اند، این استراتژی‌ها از مفاهیم هوش غیرمتمرکز و هوش جمعی استفاده می‌کنند. ریشه‌های این استراتژی‌ها را می‌توان در دنیای طبیعی یافت. آن‌ها نمایان‌گر همکاری ممکن بین سیستم‌های کامپیوتری و سیستم‌های زیستی هستند تا راه‌حل‌هایی ایجاد کنند که نه تنها از نظر عملی مفید باشند بلکه از نظر زیبایی‌شناختی نیز دلپذیر باشند. این همکاری ممکن است به منظور تولید راه‌حل‌هایی باشد که هم از نظر بصری جذاب و هم از نظر عملی مفید باشند. نتیجه نهایی این همکاری تولید راه‌حل‌هایی خواهد بود که نه تنها کارآمد بلکه از نظر زیبایی نیز دل‌پذیر هستند (اکسائو،لی، جیانگ، لی، الذاب، ژوو، و دوستار[5]، ۲۰۲۳؛ چنگ، ژوو، ژائو، و چن[6]، ۲۰۱۶). TOPSIS و MCDM در برنامه‌های WSN بسیار مفید هستند. MCDM با ارزیابی معیارهای متعدد مانند؛ بهره‌وری انرژی، پوشش و هزینه، تصمیم‌گیری آگاهانه را ممکن می‌سازد. در همین حال، TOPSIS راه حل‌های جایگزین WSN را بر اساس شباهت آنها به یک راه حل ایده‌آل رتبه‌بندی می‌کند. با استفاده‌از این روش‌ها، فرآیندهای تصمیم‌گیری و بهینه‌سازی در استقرار WSN می‌تواند به طور قابل توجهی افزایش یابد. درWSN ، مصرف انرژی یک مسئله اصلی برای چندین محقق است. رویکرد MCDMبا استفاده از TOPSIS برای انتخاب CH های کارآمد که دقت و طول عمر

1- Liu
2- Lv, Qiao, & Nowak
3- Ifzarne, Tabbaa, Hafidi, & Lamghari
4- Liu, Shi, Zhou, Liu, Yin, Yin, & Zheng
5- Xiao, Li, Jiang, Li, Alazab, Zhu, & Dustdar
6- Cheng, Zhu, Zhao, & Chen

شبکه را افزایش می‌دهد و سربار مصرف انرژی مرتبط با CH را کاهش می‌دهد (سین، ساهوو، تیاری، سیمیک، و سناپاتی[1]، ۲۰۲۳). از دیدگاه یک موجودی که تحت کنترل هوش مصنوعی است، شبکه‌های حسگر بی‌سیم به عنوان یک شبکه وسیع از گره‌های حسگری به نظر می‌رسند که به دقت در مکان‌های دورافتاده و در بسیاری از موارد، غیرقابل دسترس قرار داده شده‌اند (چن، هوو، ژائو، قوش[2]، ۲۰۲۲؛ جیانگ، لیو، ژائو، و وو[3]، ۲۰۲۲). این مطالعه یک الگوریتم خوشه‌بندی اصلاح شده مبتنی بر LEACH را با تنظیم محدوده گیربکس خودکار و یک جمع‌آورنده داده موبایل مبتنی بر (Frefy MDC) ادغام می‌کند. این به منظور افزایش جمع‌آوری داده‌ها و طول عمر شبکه انجام می‌شود. به دلیل تلاشی که برای این تحقیق انجام شد، هر دوی این پیشرفت‌ها توانستند محقق شوند (پندی، کومار، پریاداریش، و نات[4]، ۲۰۲۲؛ ساتیش، دوتا، پریاداریش، نات[5]، ۲۰۲۱).

## اقدامات مربوط به تحقیق حاضر

در ابتدا نودها را در یک محیط ۱۰۰ * ۱۰۰ برنامه متلب به شکل تصادفی پخش کرده، سپس با استفاده از الگوریتم K-MEAN به خوشه‌بندی و طبقه‌بندی نودها پرداخته شد.

معیارهای بهینه‌سازی سازی در این تحقیق، به شرح زیر است:

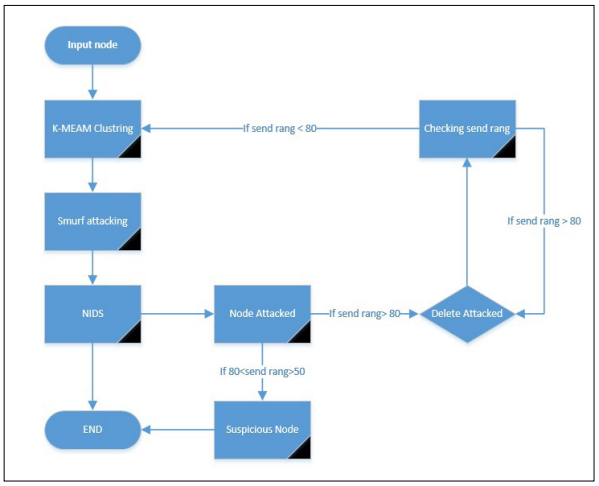
۴-فاصله گره‌ها از هم.

۵-فاصله گره‌ها از سر خوشه .

۶-فاصله خوشه از ایستگاه پایه .

۷-محاسبه بهینه‌ترین مسیر ارسال پیام برای هر نود.

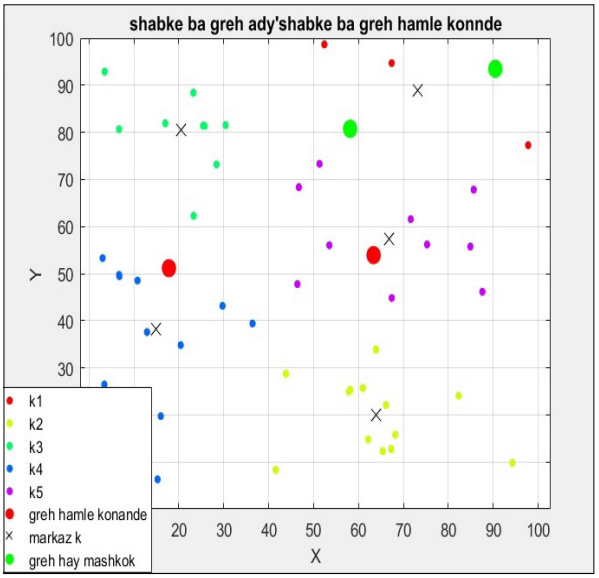
این امر با استفاده از الگوریتم K-MEAN اتفاق افتاده است. بعد از خوشه‌بندی یک حمله اسمورف را شبیه‌سازی کرده که باعث ارسال بیش از اندازه پیام از بعضی از گره‌های شبکه شد. حمله اسمورف یکی از حملات DoS می‌باشد که علاوه بر درگیری نودهای شبکه سبب افت انرژی کلی شبکه می‌شود. از این رو ویژگی اطمینان شبکه را با خطر مواجه می‌کند. طبق شکل شماره (۱)، با استفاده از یک سیستم تشخیص نفوذ (IDS) مبتنی بر شبکه شبکه را مورد ارزیابی قرار دهید.




شکل (۱): فلوچارت

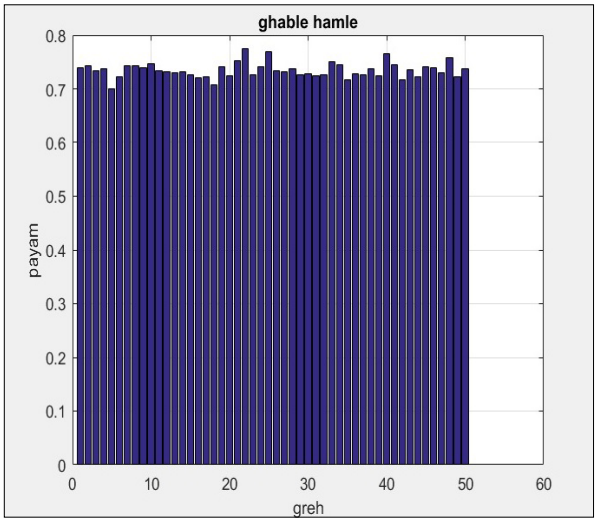
طبق تشخیص این سیستم اگر پیام‌های ارسالی گره‌های خوشه‌ها از حد مجاز بیشتر شود، سیستم تشخیص می‌دهد که حمله‌ای رخ داده است. و با استفاده از نرخ مجاز پیام‌ها شروع به شناسایی گره‌های حمله کننده، می‌کند. تفاوت سیستم تشخیص نفوذ این مقاله با سیستم‌های دیگر در این است که سیستم تشخیص علاوه بر تشخیص گره‌های حمله کننده به تشخیص گره‌های مشکوک نیز می‌پردازد. ممکن است در آینده به گره حمله کننده تبدیل شوند. علاوه بر این این سیستم قابلیت این را دارد که حمله به گره‌ها را کاهش داده و آنها را به وضعیت عادی برگرداند که با استفاده از این روش توانسته‌اید عمر مفید شبکه را افزایش دهید. همان طور که در شکل شماره (۲)، نمایش داده شده، الگوریتم طبقه‌بندی گره‌ها را در پنج دسته طبقه‌بندی کرده است. هر خوشه، سرخوشه خود را دارد، سپس با ایجاد حمله اسمورف سیستم تشخیص نفوذ، وارد عمل شده و با شناسایی گره‌های مشکوک و حمله کننده و سپس تغییر وضعیت به حالت عادی، کار خود را انجام داد.

1- Sen, Sahoo, Tiwary, Simic, & Senapati
2- Chen, Hu, Zhao, & Ghosh
3- 12Jiang, Liu, Li, Zhao, & Wu
4- Pandey, Kumar, Priyadarshi, & Nath
5- Sateesh, Dutta, Priyadarshi, & Nath



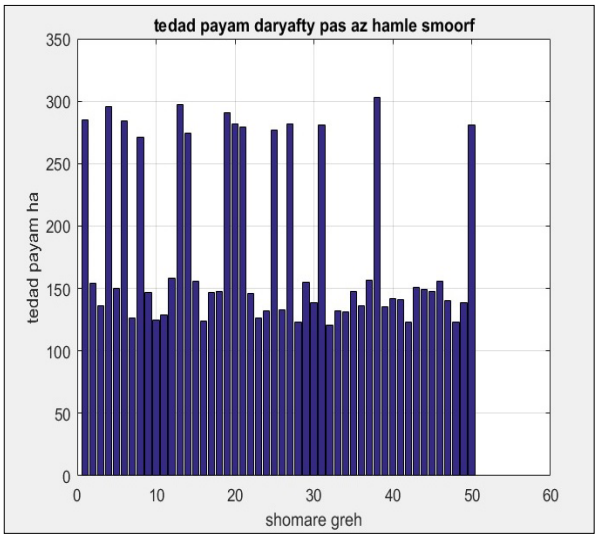

شکل (۲): خوشه‌بندی عادی، نمایش گره مشکوک و حمله کننده

در شکل شماره (۳)، تعداد پیام‌های ارسالی هر گره در حالت عادی نمایش داده شده است که بسیاری از گره‌ها، شبیه به هم هستند و این به معنی انجام درست مراحل خوشه‌بندی الگوریتم K-MEAN است. در حالت عادی قبل از ایجاد حمله مشاهده می‌شود که نرخ ارسال بسته‌ها در گره‌ها متعادل است و گره‌هایی که طبق معیارهای تحقیق خوشه‌بندی شده‌اند. بر اساس محل قرارگیری بازه خاصی از پیام را ارسال می‌کنند که در این حالت چون الگوریتم K-MEAN آنها را به صورت بهینه، خوشه‌بندی کرده است، از نرخ ارسال پیام، تفاوت چندانی ندارند.



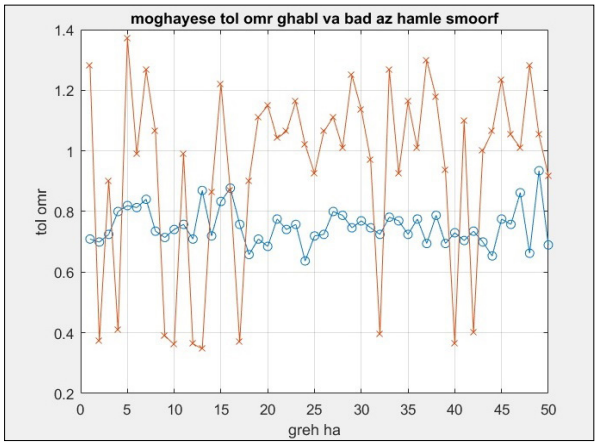

شکل (۳): نرخ ارسال پیام از هر گره قبل حمله اسمورف

در شکل شماره (۴)، نرخ ارسال پیام پس از حمله اسمورف را مشاهده می‌کنید که حاکی از افزایش چشمگیر ارسال پیام چندین نود می‌باشد. این نودها بر اساس مقیاس‌های سیستم تشخیص نفوذ مبتنی بر شبکه به دو دسته گره حمله کننده و گره مشکوک تقسیم می‌شوند.




شکل (۴): نرخ ارسال پیام هرگره بعد از حمله اسمورف

شکل شماره (۵)، نشان دهنده طول عمر هر گره پس از حمله اسمورف می‌باشد. طبق این حمله چندین گره به طور کامل به دلیل تخلیه انرژی از شبکه خارج شده‌اند.



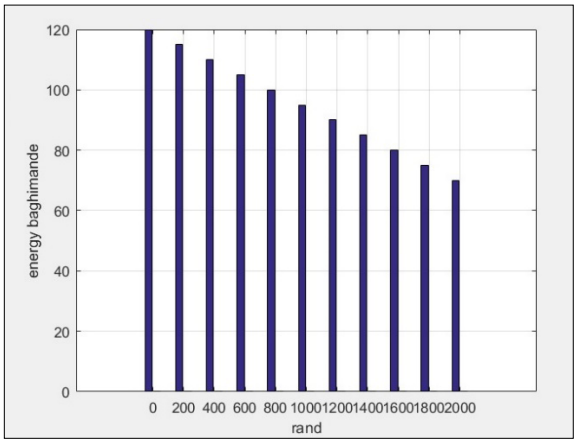

شکل (۵): طول عمر هر گره قبل و بعد از حمله اسمورف

## ۳- یافته‌های تحقیق: مدل شبکه و شبیه‌سازی

به هرحال انواع حملات امنیتی به شبکه‌های حسگر بیسیم، باعث افت چشمگیر انرژی گره‌های شبکه

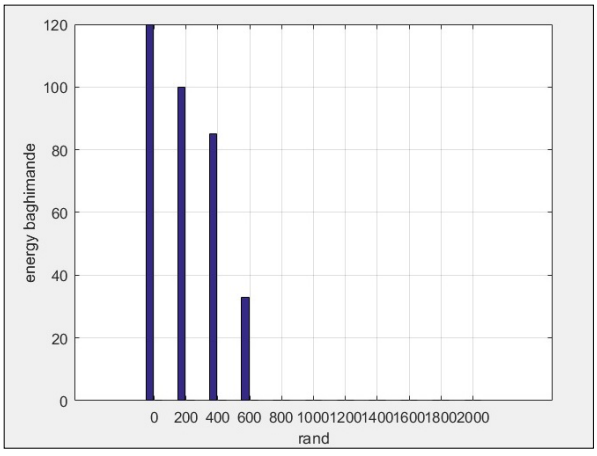
می‌شوند که بر اساس نوع حمله این آسیب‌ها متفاوت هستند. یکی از راه‌های مقابله با این نوع حملات سیستم‌های تشخیص نفوذ مبتنی بر شبکه هستند. سیستم مبتنی بر نفوذ این مقاله با استفاده از الگوریتم K-MEAN سبب بهبود انرژی گره‌های مورد تهاجم شده که این امر در نرخ انرژی کلی شبکه حسگر بی‌سیم و حفظ انرژی گره‌ها تاثیرگذار است.

شکل شماره (۶)، مصرف انرژی گره‌ها در حالت عادی را بعد از ۲۰۰۰ دور نشان می‌دهد. در اینجا با استفاده از الگوریتم K-MEAN به صورت بهینه خوشه‌بندی شده‌اند.




شکل (۶): انرژی کل گره‌ها بعد از ۲۰۰۰ دور در حالت عادی

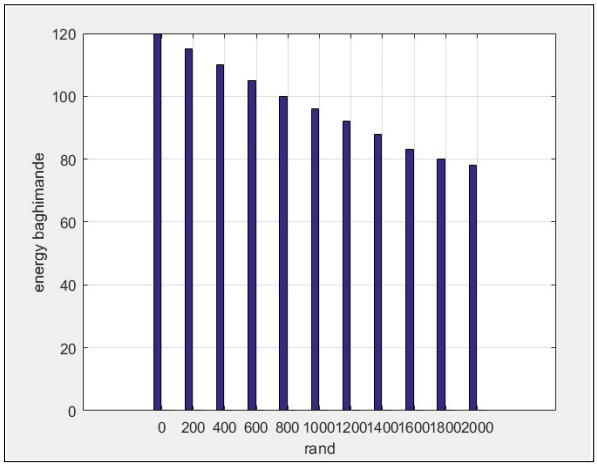
شکل شماره (۷)، انرژی مصرفی کل گره‌ها را بعد از حمله اسمورف و عدم دخالت سیستم تشخیص نفوذ مبتنی بر شبکه نشان می‌دهد.




شکل (۷): انرژی کل گره‌ها بعد از ۲۰۰۰ دور با حمله اسمورف

همانطور که در شکل شماره (۷)، مشخص است در دور ۸۰۰ کل انرژی گره‌ها مصرف شده و شبکه عملا از دسترس خارج شده و ویژگی قابلیت اطمینان به طور کامل نقض شده، لذا پس از حمله اسمورف انرژی چند گره به سرعت تخلیه می‌شود و حتی با خوشه‌بندی هم نمی‌توان مانع آن شد و بار شبکه به دوش بقیه گره‌ها انداخته می‌شود، این باعث می‌شود عمرکلی شبکه زودتر از حد انتظار به پایان برسد.

اما شکل شماره (۸)، که پس از حمله اسمورف است و با استفاده از سیستم تشخیص نفوذ مبتنی بر شبکه انرژی گره‌ها سنجیده شده، نشان می‌دهد علاوه بر حفظ انرژی کلی، شبکه باعث تامین قابلیت اعتماد شبکه می‌شود.




شکل (۸): انرژی کل گره‌ها پس از ۲۰۰۰ دور با سیستم تشخیص نفوذ

## ۴- نتیجه‌گیری

با توجه به محدودیت‌های ذاتی شبکه‌های حسگر بیسیم از جمله؛ انرژی، توان پردازشی و حافظه، افزایش قابلیت اطمینان و مصرف بهینه انرژی در پروتکل‌های مسیریابی از چالش‌های اساسی برای شبکه‌های مذکور محسوب می‌گردد. سیستم تشخیص نفوذ با شناسایی گره‌های حمله کننده و مشکوک و حذف عوامل حمله کننده که با استفاده از الگوریتم K-MEAN خوشه‌بندی بهینه‌ای را بعد از حمله انجام داده و سبب افزایش طول عمر شبکه و ایجاد قابلیت اعتماد می‌شود. این سیستم در این مقاله باعث شد که انرژی کلی شبکه که پس از دور ۶۰۰ به طور کلی از بین رفته بود، بهینه شود و پس از ۲۰۰۰ دور کمی

بهتر از حالت اولیه خود تکامل پیدا کرده است. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی، قابلیت اطمینان را افزایش و انرژی مصرفی را کاهش می‌دهد. به عنوان کاری که در آینده می‌توان از سیستم‌های تشخیص نفوذ ترکیبی در شبکه به جای سیستم نفوذ مبتنی بر شبکه استفاده کرد.

## منابع:

1-Chen, B., Hu, J., Zhao, Y., & Ghosh, B. K. (2022). Finite-time velocity-free rendezvous control of multiple AUV systems with intermittent communication. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(10), 6618-6629.
2-Cheng, B., Zhu, D., Zhao, S., & Chen, J. (2016). Situation-aware IoT service coordination using the event-driven SOA paradigm. *IEEE Transactions on Network and Service Management*, *13*(2), 349-361.
3-Fang, Y., Min, H., Wu, X., Wang, W., Zhao, X., & Mao, G. (2022). On-ramp merging strategies of connected and automated vehicles considering communication delay. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 15298-15312.
4-Han, Y., Wang, B., Guan, T., Tian, D., Yang, G., Wei, W., ... & Chuah, J. H. (2022). Research on road environmental sense method of intelligent vehicle based on tracking check. *IEEE transactions on intelligent transportation systems*, *24*(1), 1261-1275.
5-Ifzarne, S., Tabbaa, H., Hafidi, I., & Lamghari, N. (2021). Anomaly detection using machine learning techniques in wireless sensor networks. In *Journal of Physics: Conference Series* (Vol. 1743, No. 1, p. 012021). IOP Publishing.
6-Jiang, S., Zhao, C., Zhu, Y., Wang, C., & Du, Y. (2022). A Practical and Economical Ultrawideband Base Station Placement Approach for Indoor Autonomous Driving Systems. *Journal of advanced transportation*, *2022*(1), 3815306.
7-Jiang, Y., Liu, S., Li, M., Zhao, N., & Wu, M. (2022). *A new adaptive co-site broadband interference cancellation method with auxiliary channel. Digital Communications and Networks*.
8-Liu, G. (2023). A Q-Learning-based distributed routing protocol for frequency-switchable magnetic induction-based wireless underground sensor networks. *Future Generation Computer Systems*, *139*, 253-266.
9-Liu, X., Shi, T., Zhou, G., Liu, M., Yin, Z., Yin, L., & Zheng, W. (2023). Emotion classification for short texts: an improved multi-label method. *Humanities and Social Sciences Communications*, *10*(1), 1-9.
10-Lv, Z., Cheng, C., & Song, H. (2022). Digital twins based on quantum networking. *Ieee Network*, *36*(5), 88-93.
11-Lv, Z., Qiao, L., & Nowak, R. (2022). Energy-efficient resource allocation of wireless energy transfer for the internet of everything in digital twins. *IEEE Communications Magazine*, *60*(8), 68-73.

12-Pandey, A., Kumar, D., Priyadarshi, R., & Nath, V. (2022). Development of smart village for better lifestyle of farmers by crop and health monitoring system. In *Microelectronics, Communication Systems, Machine Learning and Internet of Things: Select Proceedings of MCMI 2020* (pp. 689-694). Singapore: Springer Nature Singapore.
13-Sateesh, V. A., Dutta, I., Priyadarshi, R., & Nath, V. (2021). Fractional frequency reuse scheme for noise-limited cellular networks. In *Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems: MCCS 2019* (pp. 995-1004). Springer Singapore.
14-Sen, S., Sahoo, L., Tiwary, K., Simic, V., & Senapati, T. (2023). Wireless sensor network lifetime extension via K-Medoids and MCDM techniques in uncertain environment. *Applied Sciences*, *13*(5), 3196.
15-Xu, K. D., Guo, Y. J., Liu, Y., Deng, X., Chen, Q., & Ma, Z. (2021). 60-GHz compact dual-mode on-chip bandpass filter using GaAs technology. *IEEE Electron Device Letters*, *42*(8), 1120-1123.
16-Xiao, Z., Li, H., Jiang, H., Li, Y., Alazab, M., Zhu, Y., & Dustdar, S. (2023). Predicting urban region heat via learning arrive-stay-leave behaviors of private cars. *IEEE transactions on intelligent transportation systems*, *24*(10), 10843-10856.
17-Zhou, G., Zhang, R., & Huang, S. (2021). Generalized buffering algorithm. *IEEE access*, *9*, 27140-27157.