یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

مدلی برای مقابله با حملات سیبل در شبکه‌های موردی سیار با استفاده از مدل مخفی مارکوف

رویا زارع فرخادی[1]

[1]هیئت علمی گروه نرم افزار، موسسه آموزش عالی و غیرانتفاعی رشدیه ،تبریز،roya.farkhady@gmail.com

چکیده

شبکه های موردی سیار به شبکه‌های تک¬کاره موبایل اطلاق می¬شود که زیرساخت فیزیکی ثابتی ندارند. همچنین توپولوژی این شبکه به‌صورت پویا تغییر میکند. گره¬ها در این شبکه¬های پویا بدون مدیریت مرکزی باهم ارتباط برقرار می¬کنند و با به‌روزرسانی موقعیت¬های جدید گره¬ها، ارتباط بین شبکه¬ای تداوم می¬یابد.در این مقاله یک الگوریتم جدید به‌منظور مقابله با گره¬های مهاجم در حملات سیبل ارائه شده است. راهکار ارائه‌شده شامل یک الگوریتم شناسایی مهاجم و یک الگوریتم مسیریابی بر پایه هوش جمعی زنبورهای عسل مصنوعی است. در این روش، از ترکیب تکنیک¬های مدل مارکوف و رتبه¬بندی کاربران برای شناسایی کاربران مهاجم استفاده می¬شود. نتایج شبیه‌سازی نشان داد که الگوریتم ارائه‌شده یک‌راه حل ساده و مؤثر برای موقعیت‌های مختلف در شبکه‌های موردی سیار با حضور حملات سیبل هست. ارزیابی تأخیر انتها به انتها درروش پیشنهادی نشان داد که با تغییر تعداد گره¬های شبکه، میزان تأخیر انتها به انتها در شبکه تقریباً بدون تغییر باقی می¬ماند. در پروتکل پیشنهادی عمل کاهش مصرف انرژی با استفاده از پیش‌بینی مقدار انرژی مصرفی قبل از ارسال داده انجام می¬شود.

واژه‌های کلیدی

MANET، مارکوف، سبیل

۱- مقدمه

شبکه¬های موردی سیار (MANETراه‌حل ایده¬آلی برای انواع گوناگونی از کاربردهای نظارت و مراقبت شامل کنترل ترافیک، نظارت بر محیط، نظارت برمیدان جنگ و غیره هستند. شبکه¬های موردی سیار از صدها یا هزاران گره بی¬سیم باقابلیت تحرک تشکیل‌شده‌اند که در محیط وسیع و غالباً بدون نظارت و مراقبت فعالیت می¬کنند.

باتوجه به حوزه استفاده شده از این شبکه¬ و عمومیت استفاده از آن در محیط‌های مختلف؛ صحت داده‌ها و همچنین سلامتی شبکه امری ضروری است. محدودیت¬هایی از جمله منابع محدود، ارتباطات غیرقابل اعتماد، عملکرد خودکار (بی-مراقبت) باعث می¬شود تا استفاده از تکنیک‌های امنیتی بکار رفته در شبکه‌های سنتی در این نوع شبکه¬ها غیرممکن باشد. یکی از حمله¬های مهم و تأثیرگذار بر لایه مسیریابی، حمله سیبل است. در این حمله، دشمن یک گره بدخواه را در شبکه درج می¬کند یا یک گره نرمال درون شبکه را ضبط می¬کند. سپس آن را برنامه¬ریزی مجدد نموده و تحت عنوان گره بدخواه در شبکه درج می¬کند. این گره بدخواه پس از گسترش در محیط، چندین شناسه از خود منتشر می¬کند که دشمن این شناسه¬ها را یا به‌طور جعلی می¬سازد و یا از شناسه¬های دیگر گره¬های نرمال در نواحی دیگر شبکه جعل می¬کند[۱]. به این شناسه¬های منتشرشده توسط گره بدخواه، اصطلاحاً گره¬های سیبل گفته می¬شود. گره بدخواه پس از گسترش در محیط، شناسه¬های سیبل را از خود منتشر می¬کند. این ¬امر سبب می¬شود گره بدخواه ترافیک قابل‌توجهی را به خود جلب کرده و پروتکل¬های مسیریابی را مختل کند و حتی بر عملیاتی نظیر تجمیع داده¬ها و تخصیص منابع تأثیر گذارد.

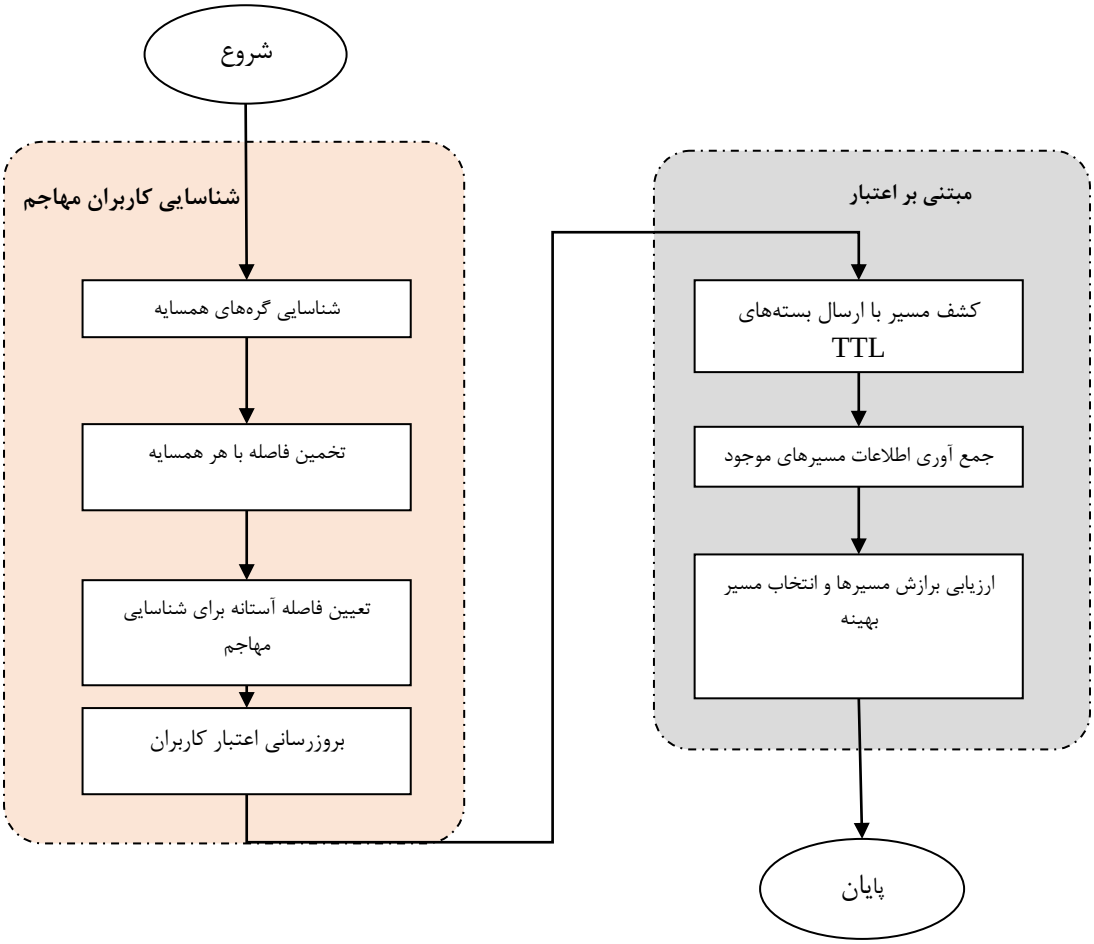
در این مقاله یک مدل برای مقابله با حملات سیبل در شبکه‌های موردی سیار با استفاده از مدل مخفی مارکوف خواهیم پرداخت. ازآنجایی‌که گره¬های سیبل شناسه¬های جعلی را از طریق یک سخت‌افزار یکسان انتشار می¬دهند؛ درنتیجه موقعیت¬یابی گره¬های شبکه می¬تواند راهکاری مناسب برای تشخیص هویت¬های جعلی باشند (دو یا چند شناسه که دریک موقعیت یکسان قرار دارند جعلی خواهند بود). مشکل اصلی در استفاده از این راهکار، وجود نویز در محیط می¬باشد که موقعیت‌یابی گره¬ها را با خطا مواجه می¬کند. از طرفی، قابلیت تحرک گره¬های شبکه بر این پیچیدگی می¬افزاید [۲]. برای حل این دو مشکل، در این مقاله یک روش ایمن برای مقابله با حملات سیبل با استفاده از مدل مارکوف و اعتبار کاربران ارائه خواهیم نمود. درروش پیشنهادی، از یک معیار مبتنی بر اعتبار برای شناسایی کاربران مهاجم و نادیده گرفتن آن‌ها در شبکه استفاده می¬شود. بدین‌صورت که اعتبار کاربران براساس تعداد دفعات مغایرت اطلاعات موقعیتی آن‌ها تعیین می¬شود. بدین‌ترتیب، پس از تکرار عملیات ارزیابی و تعیین اعتبار گره به تعداد دفعات زیاد، اثر مخرب نویز از بین خواهد رفت. در این فرآیند، از قدرت سیگنال دریافتی در مدل مارکوف برای تعیین فواصل آستانه جهت تشخیص مهاجمین استفاده می-شود.

.

۲- روش پیشنهادی

هر الگوریتم مسیریابی ارائه شده یک الگوریتم مسیریابی توزیع شده است که از ترکیب تکنیک‌های مدل مارکوف و معیار اعتبار کاربران بهره می‌گیرد. در این راهکار، از تکنیک‌های مدل مارکوف و معیار اعتبار کاربران برای شناسایی کاربران مهاجم و همچنین کشف مسیرهای بهینه به سمت مقصد استفاده می‌شود. لازم به ذکر است که منظور از بهینگی مسیر، مسیرهایی قابل اطمینان (عدم وجود گره مهاجم در طول مسیر) با انرژی بالا و تأخیر کم می‌باشد.

مراحل مسیریابی در الگوریتم پیشنهادی به‌صورت فلوچارت در شکل ۱ نمایش داده شده است.



شکل ۱ فلوچارت روش پیشنهادی

همان‌طور که در فلوچارت شکل ۱ نمایش داده شده است، روش پیشنهاد شامل دو فاز تشخیص گره‌های مهاجم و مسیریابی مبتنی بر اعتبار کاربران می‌باشد. فاز اول روش پیشنهادی، شناسایی کاربران مهاجم را با استفاده از یک معیار مبتنی بر اعتبار انجام می‌دهد. این فرآیند با استفاده از گام‌های زیر صورت می‌گیرد:

- شناسایی گره‌های همسایه توسط هر گره.
- تخمین فاصله گره با هرگره همسایه با استفاده از قدرت سیگنال دریافتی.
- تعیین فاصله آستانه برای شناسایی گره‌های مهاجم براساس فواصل تخمین زده شده و با استفاده از الگوریتم بهینه‌سازی کلونی زنبورعسل.
- بروز رسانی اعتبار کاربران براساس فواصل تخمین زده شده.
- پس از اعتبارسنجی کاربران طی مراحل ذکرشده، کاربران شناسایی شده به‌عنوان مهاجم دارای اعتبار کمتر و کاربران نرمال دارای اعتبار بالاتر خواهند بود. در فاز دوم روش پیشنهادی، عمل مسیریابی براساس اعتبار کاربران و با استفاده از وزن‌دهی ارتباطات انجام می‌شود. فاز مسیریابی داده در روش پیشنهادی شامل دو گام اصلی می‌باشد:
- جستجوی مسیر در سطح گره براساس انرژی مصرفی و تأخیر حاصل

- انتخاب مسیر بهینه در سطح شبکه با استفاده از اطلاعات مسیر و اعتبار کاربران

همان‌طور که اشاره شد، اولین بخش روش پیشنهادی شناسایی کاربران مهاجم با استفاده از یک راهکار مبتنی بر اعتبار می‌باشد. در این گام، کاربران مهاجم براساس اطلاعات موقعیتی استخراج شده از قدرت سیگنال دریافتی آن‌ها اعتبارسنجی می‌شود. بدین‌ترتیب که کاربران نرمال دارای اعتبار بیشتر و کاربران مهاجم دارای اعتبار کمتری خواهند بود.

اولین گام در فاز شناسایی گره‌های مهاجم، شناسایی همسایگان توسط هرگره موردی می‌باشد. این گام در روش پیشنهادی با استفاده از راهکار همه پخشی بسته‌های Hello انجام می‌شود. بدین‌ترتیب، هرگره موردی می‌تواند اطلاعات همسایگان خود در شبکه را جمع‌آوری کند. در مرحله‌ی جمع‌آوری اطلاعات هرگره برای کشف گره‌های دیگر در شبکه تلاش می‌کند؛ بنابراین هرگره مانند u، برای تماس و تبادل اطلاعات به همه‌ی گره‌ها در همسایگی قابل مشاهده‌اش نیاز دارد. برای این کار، هرگره به‌طور دوره‌ای یک پیغام Hello را با استفاده از حداکثر قدرت انتقال پخش می‌کند. در این پیغام، هر گره، ID خود و اطلاعات محلی‌اش را همراه با پیام ارسال می‌کند. هر گره دریافت‌کننده این پیام، اطلاعات خود را در بسته دریافتی وارد کرده و آن را به فرستنده پاسخ می‌دهد. گره اولیه، با دریافت این بسته، اطلاعات گره همسایه خود و همچنین قدرت سیگنال دریافتی از آن گره را در یک جدول ذخیره می‌کند.

گام بعدی برای تعیین اعتبار کاربران شبکه در روش پیشنهادی، تخمین فاصله با گره می‌باشد. فاصله بین دو گره را می‌توان براساس قدرت سیگنال دریافتی هریک از گره‌ها تخمین زد. قدرت سیگنال دریافتی از یک گره را می‌توان با استفاده از رابطه (۱)محاسبه نمود [۱]:

$$RSSI_d = P_T - L - 10n\log(d) + \sigma \qquad (۱)$$

که در رابطه فوق، d نشان‌دهنده فاصله بین دو گره بوده، و σ نویز محیط و به‌عنوان یک پارامتر مستقل تصادفی با توزیع گاوسی و مرکزیت صفر است. همچنین PT توان ارسال فرستنده، L ثابت فقدان مسیرو n ضریب فقدان مسیر در استاندارد 802.11 می‌باشند. فاصله دو گره را می‌توان با استفاده از قدرت سیگنال دریافتی تخمین زد. این رابطه را بدون در نظر گرفتن عامل نویز محیط می‌توان به‌صورت رابطه (۲)تخمین زد:

$$d_{c_1,c_2} = e^{\frac{(P_T - L - rssi)}{10n}} \qquad (۲)$$

همان‌طور که اشاره شد، رابطه فوق بدون در نظر گرفتن عامل نویز می‌تواند فاصله با گره همسایه را با استفاده از قدرت سیگنال دریافتی تخمین بزند. باید توجه داشت که وجود نویز در محیط موجب بروز خطا در تعیین فاصله دقیق با کاربر خواهد شد. نویز محیط به‌صورت یک متغیر تصادفی با توزیع نرمال و میانگین صفر مدل‌سازی می‌شود.

پس از تخمین فاصله بین هرگره موردی با همسایگانش، باید عمل مقایسه برای فواصل محاسبه شده صورت گیرد. باتوجه به اینکه در حملات سیبل، گره مهاجم بیش از یک هویت را از طریق یک سخت‌افزار منتشر می‌کند، در نتیجه می‌توان با شناسایی گره‌های همسایه‌ای که در موقعیت‌های یکسانی قرار دارند مهاجمین را کشف نمود.

باتوجه به‌وجود عامل نویز، خطا در تخمین فاصله می‌تواند منجر به خطا در شناسایی مهاجمین شود. یک راهکار برای به حداقل رساندن اثر نویز و بیشینه نمودن دقت تشخیص مهاجمین، استفاده از الگوریتم‌های بهینه‌سازی برای تعیین آستانه فاصله می‌باشد. در ادامه این بخش به نحوه تعیین فاصله آستانه بهینه برای تشخیص کاربران مهاجم احتمالی با استفاده از الگوریتم کلونی زنبورعسل خواهیم پرداخت. فرض کنید که گرهی مانند i، دو گره همسایه مانند u و v داشته باشد. فاصله گره i با هریک از این گره‌ها مقایسه می‌شود. اگر این دو گره در فاصله یکسانی از i قرار داشته باشند، هر دو به لیست مهاجمین احتمالی افزوده می‌شوند. در ادامه این متن، لیست مهاجمین احتمالی درهر دوره تشخیص را به‌صورت B نمایش می‌دهیم. اگر di,u و di,v به ترتیب فواصل تخمین زده شده برای گره i با گره‌های u و v باشد، آنگاه اختلاف موقعیت بین دو گره u و v به‌صورت di,v -di,u محاسبه می‌شود. در روش پیشنهادی، دو گره u و v به‌عنوان مهاجم تشخیص داده شده و به مجموعه لیست مهاجمین (B) افزوده می‌شوند؛ اگر شرط رابطه (۳) برای فواصل تخمین زده شده آن‌ها برقرار باشد.

$$u.v \in B \mid L_1 \le d_{i,v} - d_{i,u} \le L_2 \qquad (۳)$$

هدف الگوریتم کلونی زنبورعسل در روش پیشنهادی، تعیین دوثابت بهینه L1 و L2 برای فواصل آستانه می‌باشد، به شرطی که شرط $L_1 \le d_{i,v} - d_{i,u} \le L_2$ برای بیشترین تعداد کاربران در لیست B جاری صادق باشد. الگوریتم کلونی زنبورعسل یک الگوریتم هوش ازدحامی و تکاملی است که با شبیه‌سازی رفتار زنبورهای عسل در هنگام جستجوی غذا سعی دریافتن پاسخ بهینه برای یک مسئله دارد. در این الگوریتم، زنبورها برحسب وظایفشان به سه دسته دیده بان، کارگر و ناظر تقسیم می‌شوند:
الگوریتم پیشنهادی برای تعیین فواصل بهینه با استفاده از هوش جمعی زنبورها شامل گام‌های زیر می‌باشد:

گام ۱- (تعیین حدود مسئله): تعیین حدود برای هر متغیر بهینه‌سازی به‌صورت $r_i \in \{0,1\}$ و تعریف تابع برازش به‌صورت:

$$Fit_{(L_1,L_2)} = \frac{\sum_{u,v \in B} L_1 \le d_{i,v} - d_{i,u} \le L_2}{|B|} \quad (۴)$$

در رابطه فوق، حالت بهینه زمانی رخ خواهد داد که برازش پاسخ برابر با ۱ باشد. بدین‌معنا که مقادیر L1 و L2 به صورتی تعیین شوند که تمامی کاربران مهاجم احتمالی در رابطه (۴) صدق کنند. لازم به ذکر است که در اولین دوره تشخیص، لیست B خالی می‌باشد. درنتیجه مقادیر L1 و L2 به‌صورت ثابت و بدون استفاده از الگوریتم جستجو تعیین می‌شوند.

گام ۲- (فاز آماده‌سازی): در این گام تمام بردارهای جمعیت منابع غذایی (جواب‌های ممکن) توسط زنبورهای دیده‌بان به‌صورت بردار $\vec{x}_m.m = 1.2. \ldots . SN$ مقداردهی اولیه می‌شوند که در این بردار، SN برابر با اندازه جمعیت زنبورها می‌باشد. ازآنجایی‌که هر عضو $\vec{x}_m$ خود یک بردار شامل دو متغیر (L1 و L2) می‌باشد، هدف پیدا کردن مقادیری در بردار $\vec{x}_m$ است که کمترین مقدار تابع برازش را تولید کنند. مقداردهی اولیه بردار $\vec{x}_m$ از طریق رابطه زیر انجام می‌شود:

$$x_{m,i} = x_{min} + R \times (x_{max} - x_{min}) \quad (۵)$$

که در رابطه فوق R یک عضو تصادفی در مجموعه $\{0,1\}$ می‌باشد.

گام ۳- (فاز جستجوی زنبورهای کارگر): در این مرحله، زنبورهای جستجوگر به‌دنبال راه‌حل‌های جدید با میزان برازش بهینه‌تر در همسایگی بردار $\vec{x}_m$ می‌گردند. این زنبورها، مقادیر موجود در همسایگی بردار $\vec{x}_m$ را توسط رابطه (۳-۴) ارزیابی می‌کنند. به بیانی دیگر، زنبورهای کارگر مقادیر فواصل آستانه در بردار $\vec{x}_m$ را تغییر داده تا بردار $\vec{v}_m$ تولید شود. سپس برازش بردار $\vec{v}_m$ را محاسبه نموده و بررسی می‌کنند که آیا مقادیر پاسخ در $\vec{v}_m$ مناسب‌تر از $\vec{x}_m$ است یا خیر؟ درصورتی‌که پاسخ مثبت باشد، بردار $\vec{x}_m$ حذف و $\vec{v}_m$ جایگزین آن خواهد شد. تعیین بردار $\vec{v}_m$ با استفاده از رابطه زیر صورت می‌گیرد:

$$\vec{v}_m = x_{mi} + \varphi_{mi}(x_{mi} - x_{ki}) \quad (۶)$$

که در رابطه فوق، x_k یک بردار تصادفی انتخاب شده از جمعیت، i یک مکان تصادفی انتخاب شده در بردارهای پاسخ و φ_{mi} یک عضو تصادفی در مجموعه $\{0,1\}$ می‌باشد.

گام ۴- (فاز ارزیابی زنبورهای ناظر): زنبورهای کارگر اطلاعات مربوط به پاسخ‌های پیدا شده را در اختیار زنبورهای ناظر قرار می‌دهند. زنبورهای ناظر احتمال انتخاب هرپاسخ را محاسبه نموده و پاسخ مناسب را برای جستجو در گام‌های بعدی انتخاب می‌کنند. احتمال مربوط به بردار $\vec{x}_m$ توسط زنبور ناظر با استفاده از رابطه زیر محاسبه می‌شود:

$$P_m = \frac{fitness(\vec{x}_m)}{\sum_{i=1}^{SN} fitness(\vec{x}_i)} \quad (۷)$$

همان‌طور که اشاره شد، انتخاب پاسخ‌ها براساس مقدار احتمال محاسبه شده در رابطه (۷) صورت می‌گیرد. به‌منظور انتخاب پاسخ‌ها از الگوریتم چرخ رولت استفاده می‌شود. این الگوریتم تلاش می‌کند که پاسخ‌های با احتمال بالاتر را به‌منظور استفاده در جمعیت بعدی انتخاب نماید اما به‌منظور حفظ جامعیت مسئله، تعداد کمی از پاسخ‌های غیربهینه نیز به چرخه بعدی انتقال می‌یابند.

گام ۵- (فاز جستجوی زنبورهای دیده‌بان): در این گام پاسخ‌هایی که پس از گذشت تعداد چرخه‌های مشخصی بدون بهبود باقی می‌مانند توسط زنبورهای دیده‌بان مجدداً مقداردهی تصادفی می‌شوند. این عمل از طریق رابطه (۵) صورت می‌گیرد.

گام ۶- (ارزیابی نتایج): درصورتی‌که مقدار برازش یک پاسخ به مقدار آستانه موردنظر برسد و یا تعداد چرخه‌های جستجو به مقدار بیشینه مشخص شده برسد، الگوریتم خاتمه می‌یابد. در غیر این صورت الگوریتم جستجو برای چرخه‌ی جدید، مجدداً از گام ۲ تکرار می‌شود.

پس از تعیین آستانه‌های بهینه، لیست B براساس مقادیر جدید L1 و L2 به‌روزرسانی می‌شود. پس از انجام این کار، اعتبار کاربران در شبکه موردی بروز رسانی خواهد شد.

در مرحله بروز رسانی اعتبار کاربران براساس فواصل تخمین زده شده ، یک مقدار اعتبار که نشان‌دهنده وضعیت (امن/ناامن بودن) هر کاربر است، به هر گره موردی اختصاص داده می‌شود. در روش پیشنهادی، مقدار اعتبار r_i^k برای گره K-ام در دوره i به وضعیت آن در لیست کاربران مهاجم احتمالی (B) بستگی دارد و می‌توان به این صورت آن را به‌روزرسانی کرد:

$$r_{i+1}^k = \begin{cases} r_i^k + 1 & if\ k \notin B \\ r_i^k - 1 & if\ k \in B \end{cases} \quad (۸)$$

در رابطه فوق، r_{i+1}^k اعتبار بروز رسانی شده گره kام، و B لیست مهاجمین احتمالی تشخیص داده شده در گام قبلی می‌باشد؛ بنابراین مقدار اعتبار هر کاربر ثانویه با استفاده از رابطه (۳-۸) افزایش یا کاهش می‌یابد. درصورتی‌که کاربر در لیست B قرار نگرفته باشد، مقدار اعتبار به میزان ۱ واحد افزایش یافته و در غیر این صورت کاهش داده خواهد شد. این رابطه باعث می‌شود که اعتبار کاربران مهاجم در بازه اعداد منفی قرار گرفته و اعتبار کاربران نرمال در بازه اعداد مثبت افزایش یابد. در گام بعدی، از این معیار اعتبار برای مسیریابی داده بین گره‌های شبکه استفاده می‌شود.

دومین فاز روش پیشنهادی، مسیریابی داده با استفاده از خصوصیات گره و میزان اعتبار تخصیص داده شده به آن‌هاست. درروش پیشنهادی از الگوریتم ساخت توپولوژی ارائه شده در [۲] برای کنترل ارتباطات شبکه استفاده شده است. پس از تشکیل توپولوژی مطابق روند تشریح شده در [۲] فاز مسیریابی داده، شامل گام‌های کشف مسیر، وزن‌دهی ارتباطات و انتخاب مسیر می‌باشد. در مرحله اول، تمامی مسیرهای موجود بین دو گره از طریق بازپخش بسته‌های کنترلی کشف می‌شوند. سپس مسیرهای کشف شده با استفاده از معیارهای: انرژی، تأخیر و اعتبار وزن‌دهی می‌شوند. سپس مسیرهای ارسال داده به‌صورت مسیرهایی با ارزش بیشتر انتخاب می‌شوند. در ادامه به تشریح هریک از این مراحل خواهیم پرداخت.

در روش پیشنهادی، فرآیند انتخاب مسیر از طریق راهکار وزن‌هی ارتباطات و انتخاب مسیر با وزن بیشتر انجام می‌شود. معیارهای در نظر گرفته شده برای انتخاب مسیر انرژی، تاخیر و اعتبار خواهد بود.

الف) انرژی: در فرآیند انتخاب مسیر، میزان انرژی بالاترگره‌های واقع در مسیر مطلوب خواهد بود؛ به‌بیان‌دیگر، انتخاب مسیری در اولویت قرار خواهد داشت که گره‌های آن از سطح انرژی بالاتری برخوردار باشند؛ زیرا این حالت موجب کاهش احتمال اتمام زودهنگام انرژی گره و بروز اختلال در فرآیند مسیریابی خواهد شد. مدل مورد استفاده برای محاسبه میزان انرژی مصرفی در ارتباطات بی‌سیم شبکه، براساس مدل ارائه شده در [۳] می‌باشد. در این مدل، میزان انرژی مصرفی برای ارسال بی‌سیم N بیت داده بین دو گره برابر است با:

$$E_{TX}(N,d) = \begin{cases} N \times (E_{elec} + E_{amp} . d^2) & if\ d < d_0 \\ N \times (E_{elec} + E_{amp} . d^4) & if\ d \geq d_0 \end{cases} \quad (۹)$$

که در رابطه فوق d برابر با فاصله بین دو گره، E_{elec} برابر با انرژی مصرفی به ازای هربیت در مدارهای فرستنده و گیرنده و E_{ap} انرژی مصرفی به ازای هر بیت در تقویت‌کننده RF می‌باشد. همچنین d0 فاصله آستانه برای توان ارسال می‌باشد و مقدار آن برابر با $d_0 = \sqrt{\frac{E_{fs}}{E_{amp}}}$ خواهد بود.

همچنین انرژی مصرفی برای دریافت N بیت داده به‌صورت رابطه (۱۰) محاسبه خواهد شد:

$$E_{RX}(N.d) = N \times E_{elec} \quad (۱۰)$$

ب) تأخیر: دومین معیار برای ارزیابی ارتباط با یک گره، معیار تأخیر می‌باشد. تأخیر گره i عبارت است از؛ فاصله زمانی بین نقطه اقدام به ارسال داده تا نقطه تحویل موفق بسته و تصدیق تحویل. برای ارسال داده از i به j تأخیر به‌صورت رابطه (۱۱) محاسبه می‌شود.

$$De_i = \left\lceil \frac{D_{i,j}}{\omega} \times \varphi \right\rceil \quad (۱۱)$$

در این رابطه، $D_{i,j}$ فاصله اقلیدسی بین دو گره بوده و دو پارامتر ω و φ به ترتیب نسبت و ثابت تأخیر هستند. همان‌طور که در بخش قبل ذکر شد، فاصله بین دو گره را می‌توان با استفاده از قدرت سیگنال دریافتی گره‌های تخمین زد.

ج) اعتبار: به‌منظور بررسی امنیت مسیر در شبکه از راهکار تعیین اعتبار برای هر گره در شبکه استفاده شده است. روند تعیین اعتبار گره-های سیار در بخش قبل به‌تفصیل ارائه گردید.

در روش پیشنهادی، پس از محاسبه معیارهای ذکر شده برای هر مسیر، عملیات انتخاب مسیر با استفاده از این معیارها انجام می‌شود. ارزش هر مسیر مانند R را می‌توان با استفاده از رابطه (۱۲) توصیف نمود:

$$F(R) = \frac{E(R)}{\sum_{j=1}^{M} E(R_j)} - \frac{D(R)}{\sum_{j=1}^{M} D(R_j)} + P(R) \quad (۱۲)$$

که در رابطه فوق M تعداد کل مسیرهای موجود بین مبدأ و مقصد، $E(R)$ مجموع انرژی گره‌های میانی موجود در مسیر R می‌باشد و $D(R)$ مشخص‌کننده بیشترین تأخیر تخمین زده شده برای گام‌های میانی مسیر R است (اطلاعات انرژی و تأخیر گام‌های مسیر در طی فرآیند کشف مسیر جمع‌آوری می‌شوند). درنهایت $P(R)$ مجموع اعتبار محاسبه شده برای تمامی گره‌های واقع در مسیر می‌باشد. این معیار با استفاده از رابطه (۱۳) تعریف می‌شود:

$$P(R) = \sum_{\forall p \in R} reputation(p) \quad (۱۳)$$

در رابطه (۱۲)، معیارهای اعتبار و انرژی برای مسیر عوامل مثبت در تعیین رتبه (مقدار بیشتر آن‌ها به معنای ارزش بالاتر مسیر می‌باشد) و تأخیر عامل منفی می‌باشد (مقدار کمتر تأخیر به معنای ارزش بالاتر مسیر می‌باشد). به همین دلیل دو عامل اول با ضریب مثبت و عامل تأخیر با ضریب منفی در معادله آورده شده است تا کل رابطه بیانگر معیاری باشد که بیشتر شدن آن بیانگر مناسب‌تر بودن مسیر باشد؛ بنابراین، پس از تعیین ارزش هر مسیر کشف شده توسط رابطه (۱۲)، مسیر با بالاترین وزن به‌عنوان مسیر ارسال داده انتخاب خواهد شد.

۳- ارزیابی

شبیه‌سازی در محیط نرم‌افزار MATLAB انجام شده است. در محیط شبیه‌سازی مورد استفاده، تعدادی گره موردی در شبکه در نظر گرفته شده است که به‌صورت تصادفی و توزیع یکنواخت در محیط شبکه پراکنده شده‌اند. هدف روش پیشنهادی، مسیریابی ایمن داده‌ها از طریق گره‌های نرمالی است که بتوانند کمترین تأخیر و بیشترین احتمال ارسال موفق به سمت مقصد را درپی داشته باشند.

به‌منظور بررسی جامع عملکرد الگوریتم پیشنهادی، دو سناریوی مختلف برای ارزیابی نتایج در نظر گرفته شده است:

- عملکرد الگوریتم پیشنهادی در تشخیص مهاجمین

در این حالت به بررسی دقت روش پیشنهادی در شناسایی کاربران مهاجم پرداخته می‌شود. در این سناریو، دقت تشخیص الگوریتم پیشنهادی در حالات تغییر در تعداد مهاجمین و تغییر در ضریب نویز بررسی می‌شود.

عملکرد الگوریتم پیشنهادی در مسیریابی داده: در این حالت به بررسی عملکرد الگوریتم مسیریابی روش پیشنهادی در ارسال موفق بسته پرداخته می‌شود. در این سناریو، پارامترهای تأخیر انتها به انتها، انرژی مصرفی و نرخ تحویل بسته در شرایط تغییر تعداد کاربران مورد مطالعه قرار خواهد گرفت.

مهم‌ترین پارامترهای مورد استفاده در محیط شبیه‌سازی، در جدول (۱)آورده شده است.

جدول۱:پارامترهای شبیه‌سازی

Parameter	Value
Max data rate (Kbps)	128
Transmission power (dbm)	2
Receive threshod (dbm)	-74
Transmission current (mA)	17.4
Receive current (mA)	19.7
Fragment size (bit)	1024
Buffer size (Bytes)	128 K
MAC layer	CSMA/CA

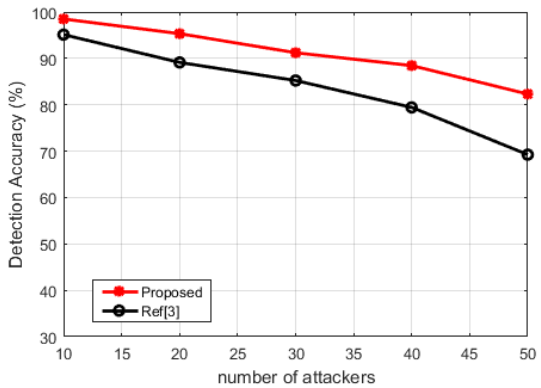
- دقت تشخیص الگوریتم پیشنهادی به ازای تغییرات تعداد مهاجمین

در این آزمایش تعداد کاربران مهاجم از ۱۰ تا ۵۰ تغییر داده شده و دقت تشخیص روش پیشنهادی به ازای هر حالت محاسبه می‌گردد. همچنین نتایج حاصل از روش پیشنهادی با نتایج الگوریتم پیشنهاد شده در [۳] مقایسه شده است. دقت تشخیص به‌صورت رابطه (۱۴) محاسبه می‌شود:

(۱۴)

$$Acc = \frac{D}{M} \times 100$$

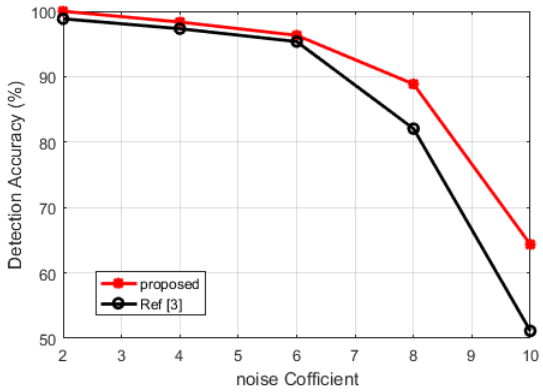
که در رابطه (۱۴)، D تعداد مهاجمین تشخیص داده شده توسط الگوریتم و M تعداد واقعی مهاجمین می‌باشد. لازم به ذکر است که در روش پیشنهادی کاربرانی به‌عنوان مهاجم تلقی می‌شوند که میزان اعتبار آن‌ها منفی باشد. در شکل ۲ نمودار دقت تشخیص روش پیشنهادی به ازای تغییرات تعداد مهاجمین نمایش داده شده است. در این آزمایش ضریب نویز محیط برابر با ۷ در نظر گرفته شده است.



شکل ۲ :نمودار دقت تشخیص روش پیشنهادی به ازای تغییرات تعداد مهاجمین

- دقت تشخیص الگوریتم پیشنهادی به ازای تغییرات ضریب نویز محیط

منظور از بررسی تغییرات نویز بر عملکرد روش پیشنهادی، ارزیابی عملکرد الگوریتم شناسایی مهاجمین در محیط‌های مختلف می‌باشد. همان‌طور که در فصل سوم ذکر شد، وجود عامل نویز در محیط موجب بروز خطا در مکان‌یابی صحیح کاربران شبکه می‌شود؛ بنابراین با افزایش عامل نویز طبیعی است که دقت تشخیص نیز کاهش خواهد یافت. در این آزمایش، تعداد کل گره‌های شبکه برابر با ۱۰۰ گره و نسبت مجاهمین برابر با ۰,۱ (۱۰ گره) تعیین شده است. مقدار ضریب نویز محیط از ۲ تا ۱۰ تغییر داده شده و به ازای هرحالت دقت تشخیص روش پیشنهادی و روش مورد مقایسه ارزیابی شده است. در شکل ۳ نمودار دقت تشخیص روش پیشنهادی به ازای تغییرات ضریب نویز نمایش داده شده است.



شکل ۳: نمودار دقت تشخیص روش پیشنهادی به ازای تغییرات ضریب نویز

براساس نتایج نمایش داده شده در شکل ۳، روش پیشنهادی در تمامی حالات دارای دقت تشخیص بالاتری نسبت به روش مورد مقایسه می‌باشد. استفاده از تکنیک میانگین‌گیری از قدرت سیگنال دریافتی در روش پیشنهادی موجب می‌شود که اثر نویز محیط تا حد ممکن کاسته شده و روش پیشنهادی بتواند در مقابل تغییرات اثر نویز مقاومت کند. این نتایج نشان می‌دهد که روش پیشنهادی می‌تواند به‌عنوان یک راهکار قابل اعتماد در مقابله با حملات سیبل در شبکه موردی سیار عمل کند.

- ارزیابی عملکرد مسیریابی در روش پیشنهادی

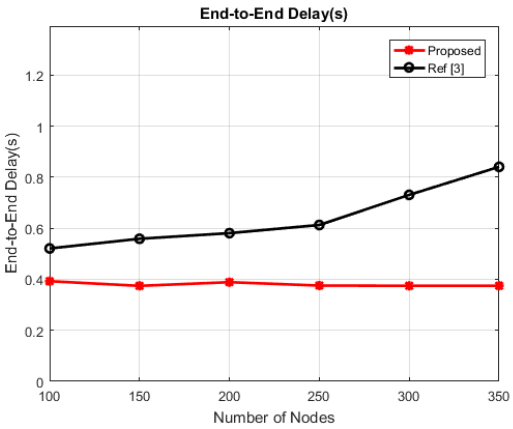
هدف این سناریو ارزیابی نحوه عملکرد الگوریتم مسیریابی در شرایط وجود حمله سیبل در شبکه موردی سیار می‌باشد. یک الگوریتم مسیریابی ایمن باید بتواند داده‌های درحال جریان در شبکه را از طریق گره‌های نرمال و دارای تأخیر کمتر ارسال کند. علاوه‌براین، میزان انرژی مصرفی و نرخ تحویل بسته دو پارامتر اساسی در بررسی صحت عملکرد یک الگوریتم مسیریابی می‌باشد. دراین سناریو، تعدادی گره به‌طور یکنواخت (تصادفی) روی محیطی با ابعاد ۱۰۰ در ۱۰۰ متر مستقر شده‌اند.

تأخیر انتها به انتها در ارسال نسبت به افزایش منابع شبکه

در این آزمایش تعداد گره‌های شبکه از ۱۰۰ گره تا ۳۵۰ گره تغییر یافته و آزمایش را به ازای تعداد مختلف گره تکرار می‌نماییم. نرخ گره‌های مهاجم دراین آزمایشات برابر با ۰,۱ (۱۰ تا ۳۵ گره موردی) تعیین شده است. سایر پارامترها در کلیه آزمایشات یکسان در نظر گرفته می‌شود. همچنین اندازه کلونی زنبورها نیز برابر با تعداد گره‌های شبکه قرار داده می‌شود. در روش‌های مرسوم، اغلب با افزایش تعداد گره‌های شبکه، میزان تأخیر انتها به انتهای شبکه نیز افزایش می‌یابد. دلیل این امر افزایش مسیرهای ممکن بین گره‌ها و در پی آن افزایش تعداد گام‌های لازم برای رساندن داده‌ها از مبدأ به مقصد می‌باشد. این عامل روی کارایی شبکه تأثیر مستقیم داشته و موجب افزایش ازدحام در مسیریابی داده بین گره‌ها می‌شود؛ زیرا هر بسته زمان بیشتری را داخل شبکه سپری نموده و استقرار طولانی‌تر بسته‌ها در درون شبکه موجب درگیری بیشتر گره‌ها با این بسته‌ها خواهد شد. درصورتی‌که این عامل نادیده گرفته شود، می‌تواند موجب کاهش نرخ تحویل بسته در شبکه نیز شود.

در پروتکل پیشنهادی برای رویارویی با این مشکل از ارسال بسته‌های TTL برای یافتن مسیرهای ممکن بین مبدأ و مقصد استفاده می-شود. استفاده از این امکان موجب می‌شود قبل از انتخاب مسیر، هرمسیری که دارای تأخیر بیشتر و احتمال اتلاف بسته‌ی بیشتری است نادیده گرفته شود.

دلیل این امر وجود فاکتور طول عمر برای بسته‌های TTL ارسالی می‌باشد؛ بنابراین اگر یک مسیر درحال اکتشاف دارای تأخیر بالایی باشد، احتمال بالایی وجود دارد که درحین عمل اکتشاف مسیر بسته TTL آن به‌دلیل اتمام طول عمر نادیده گرفته شود. از طرفی با استفاده از معیار اعتبار گره، از انتخاب مسیرهایی که شامل گره‌های ناامن هستند جلوگیری می‌شود. این روش باعث می‌شود که میزان تأخیر انتها به انتهای شبکه در روش پیشنهادی وابسته به تعداد گره‌های شبکه نباشد و با افزایش تعداد گره‌های شبکه، میزان تأخیر انتها به انتها افزایش نیابد. در شکل ۴ نمودار تأخیر انتها به انتهای حاصل از مسیریابی داده به ازای تعداد گره‌های مختلف نمایش داده شده است.



شکل ۴:. تأخیر انتها به انتهای گره‌های شبکه به ازای تعداد مختلف گره شبکه

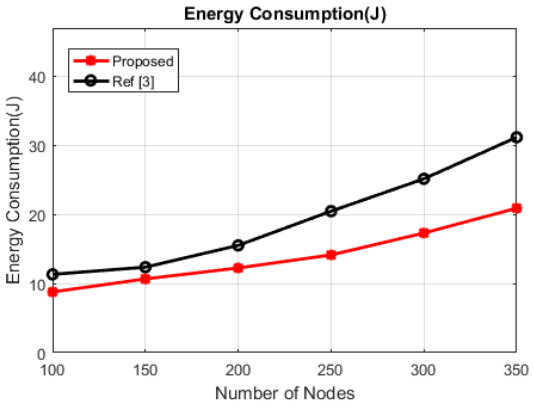
همان‌طور که در شکل ۴ نمایش داده شده است، تأخیر انتها به انتها در روش پیشنهادی به ازای تعداد مختلف گره تغییرات ناچیزی داشته و کمتر از روش مورد مقایسه می‌باشد. همان‌طور که قبلاً اشاره شد، در نظر گرفتن تأخیر به‌عنوان یکی از پارامترهای انتخاب مسیر در شبکه موجب این بهبود می‌شود.

- میزان انرژی مصرفی گره‌ها نسبت به افزایش گره‌های شبکه

در این آزمایش نیز مشابه آزمایش قبلی تعداد منابع شبکه از ۱۰۰ گره تا ۳۵۰ گره تغییر یافته و آزمایش را به ازای تعداد مختلف گره تکرار می‌نماییم. سایر پارامترها در کلیه آزمایشات یکسان در نظر گرفته می‌شود.

نتایج حاصل از این آزمایش برای روش پیشنهادی در شکل ۵ نمایش داده شده است. به‌طورکلی، میزان انرژی مصرفی گره‌های شبکه با تعداد گره‌های شبکه رابطه مستقیمی داشته و هم‌زمان با افزایش تعداد منابع در شبکه میزان انرژی مصرفی نیز افزایش می‌یابد.

براساس نتایج به‌دست‌آمده، روش پیشنهادی دارای انرژی مصرفی کمتری نسبت به روش مورد مقایسه می‌باشد؛ زیرا روش پیشنهادی عمل کاهش مصرف انرژی با استفاده از پیش‌بینی مقدار انرژی مصرفی قبل از ارسال داده انجام می‌دهد. عمل پیش‌بینی مقدار انرژی مصرفی قبل از ارسال داده و انتخاب مسیر در فصل قبل توضیح داده شد. استفاده از این روش و انتخاب مسیر بهینه باتوجه هم‌زمان به فاکتورهای تأخیر، انرژی و اعتبار مسیر موجب می‌شود در ارسال داده محدودیتی برای نرخ ارسال قائل نشویم و توان عملیاتی شبکه کاهش نیابد؛ بنابراین استفاده از این پروتکل برای شبکه‌هایی با اولویت داده محدودیتی ایجاد نمی‌کند



شکل ۵: میزان انرژی مصرفی شبکه به ازای تعداد مختلف گره شبکه

- نرخ تحویل بسته نسبت به افزایش گره‌های شبکه

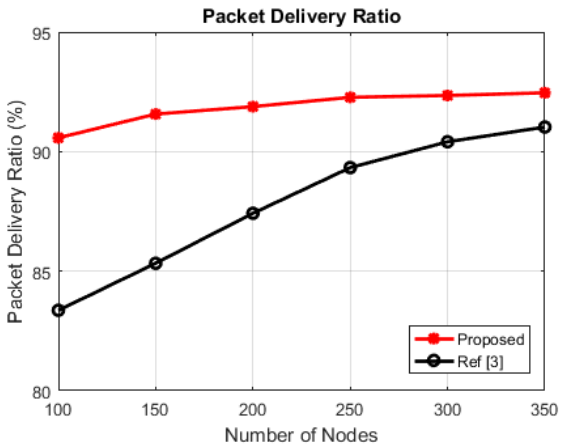
یک الگوریتم مسیریابی در صورت از کارایی کافی برخوردار خواهد بود که علاوه‌بر بهبود پارامترهای انرژی مصرفی و تأخیر، بتواند بسته-های داده را با احتمال موفقیت بیشتری به مقصد تحویل دهد. آخرین آزمایش مورد بررسی در این فصل، ارزیابی نرخ تحویل موفق بسته می‌باشد. این معیار با استفاده از رابطه (۱۵) محاسبه می‌گردد:

(۱۵)

$$DeliveryRatio = \frac{D}{T}$$

که در رابطه (۱۵)، T تعداد بسته‌های تولید شده توسط گره‌های منبع و D تعداد بسته‌های دریافت شده توسط گره‌های مقصد می‌باشد. در شکل (۶)، نمودار درصد تحویل موفق بسته به ازای تغییر در تعداد گره‌های شبکه نمایش داده شده است.

براساس نتایج نمایش داده شده در شکل ۶ با افزایش تعداد گره‌های شبکه درصد تحویل موفق بسته نیز افزایش می‌یابد. دلیل این امر این نکته است که با افزایش تعداد گره‌های شبکه در محیطی با ابعاد ثابت (۱۰۰×۱۰۰ متر)، تراکم شبکه افزایش یافته و درنتیجه تعداد مسیرهای بهینه احتمالی بین هردو گره نیز افزایش می‌یابد. درنتیجه بسته‌های داده می‌توانند به‌احتمال بیشتری با موفقیت به مقصد برسند. از طرفی، روش پیشنهادی در تمامی حالات دارای درصد تحویل موفق بیشتری نسبت به روش مقایسه شده می‌باشد؛ زیرا طبق آزمایشات صورت گرفته قبلی، روش پیشنهادی دارای دقت بالاتری در تشخیص گره‌های مهاجم بوده و درنتیجه احتمال استفاده از این دسته از گره‌ها در فرآیند مسیریابی و اتلاف بسته کمتر خواهد بود.



شکل ۶. درصد تحویل موفق بسته به ازای تعداد مختلف گره شبکه

۴- نتیجه گیری

در این مقاله، یک الگوریتم جدید به‌منظور مقابله با گره‌های مهاجم در حملات سیبل ارائه شده است. راهکار ارائه شده شامل یک الگوریتم شناسایی مهاجم و یک الگوریتم مسیریابی بر پایه هوش جمعی زنبورهای عسل مصنوعی است. در این روش، از ترکیب تکنیک‌های مدل مارکوف و رتبه‌بندی کاربران برای شناسایی کاربران مهاجم استفاده می‌شود. این فرآیند با استفاده از چهار گام متوالی انجام می‌شود: شناسایی گره‌های همسایه، تخمین فاصله گره بی‌سیم، تعیین فاصله آستانه برای شناسایی گره‌های مهاجم و به‌روزرسانی اعتبار کاربران براساس فواصل تخمین زده‌شده. همچنین از یک راهکار چندمعیاره به‌منظور کشف مسیرهای موجود بین دو گره و ارسال داده از طریق مسیر بهینه استفاده می‌شود. لازم به ذکر است که منظور از بهینگی مسیر، مسیرهایی قابل‌اطمینان (عدم وجود گره مهاجم در طول مسیر) باانرژی بالا و تأخیر کم می‌باشد. پس از اعتبارسنجی کاربران طی مراحل ذکرشده، کاربران شناسایی‌شده به‌عنوان مهاجم دارای اعتبار کمتر و کاربران نرمال دارای اعتبار بالاتر خواهند بود. در فاز دوم روش پیشنهادی، عمل مسیریابی براساس معیارهای: انرژی مصرفی، تأخیر و اعتبار کاربران انجام می‌شود.

مراجع

۱. خزاعی، فائزه؛ رضا رافع و وحید رافع، ۱۳۹۴، شناسایی حمله سیبل در شبکه‌های حسگر بی‌سیم متحرک به کمک گره‌های کاشف، دومین همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات، تهران، گروه پژوهشی بوعلی.

2. سرمست، عادل؛ مهدی اثنی‌عشری و محمدرضا میبدی، ۱۳۸۹، استفاده از آتوماتاهای یادگیر در تشخیص حمله سیبل و کاهش خطاهای تشخیص حمله سیبل در شبکه‌های حسگر بی‌سیم، سومین همایش ملی مهندسی کامپیوتر و فناوری اطلاعات، همدان.

3. Mulla, M., & Sambare, S. (2015, January). Efficient analysis of lightweight Sybil attack detection scheme in Mobile Ad hoc Networks. In Pervasive Computing (ICPC), 2015 International Conference on IEEE, Vol. 13, pp. 1-6.
4. Prathap, U., Shenoy, P. D., & Venugopal, K. R. (2016, May). CMNTS: Catching malicious nodes with trust support in wireless sensor networks. In Region 10 Symposium (TENSYMP) IEEE, Vol. 11, pp. 77-82.
5. Lazos, L., & Poovendran, R. (2005). SeRLoc: Robust localization for wireless sensor networks. ACM Transactions on Sensor Networks, 1(1), 73–100. 1051.
6. Levine, B. N., Shields, C., & Margolin, N. B. (2006). A survey of solutions to the Sybil attack, tech report, University of Massachusetts Amherst.
7. Lu, A., Wang, W., Dnyate, A., & Hu, X. (2011). Sybil attack detection through global topology pattern visualization. Information Visualization, 10(1), 32–46.