تشخیص حملات سیبیل در شبکه‌های حس‌گر بی‌سیم با رویکرد مدیریت اعتماد

سید محمد طباطبائی‌پارسا[1*] و حسن شاکری[2]

[1]دانش‌آموخته کارشناسی‌ارشد مهندسی کامپیوتر،امنیت اطلاعات دانشگاه بین‌المللی‌امام رضا(ع)، مشهد، ایران
m.tabatabaei.parsa@imamreza.ac.ir
[2]استادیار گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، مشهد، ایران
shakeri@msdiau.ac.ir

چکیده

شبکه‌های حس‌گر بی‌سیم راه‌حل ایده‌آلی برای انواع گوناگونی از کاربردهای نظارت و مراقبت شامل کنترل ترافیک، نظارت بر محیط، نظارت بر میدان جنگ و غیره هستند.گره‌های حس‌گر محدودیت‌هایی هم به‌لحاظ حافظه و هم قابلیت‌های محاسباتی دارند. حمله سیبیل یک تهدید جدی برای این شبکه‌ها به‌شمار می‌آید که در آن گره مخرب چندین هویت جعلی برای خود ایجاد کرده و گره‌های شبکه را گمراه می‌کند. این حمله می‌تواند پروتکل‌های مسیریابی و عملیاتی نظیر رأی‌گیری، تجمیع داده‌ها و... را تحت تأثیر قرار دهد. در این مقاله یک الگوریتم پویا و سبک‌وزن با رویکرد اعتماد آگاه از اطمینان ارائه می‌شود. در رویکرد مورد استفاده از مقدار اعتماد هر گره به‌منظور کاهش نرخ هشدارهای اشتباه و تشخیص حملات سیبیل غیرمستقیم در شبکه‌های حس‌گر بی‌سیم استفاده می‌شود. نتایج شبیه‌سازی نشان می‌دهد که میانگین نرخ تشخیص و تشخیص غلط به‌ترتیب ۰/۹۲٪ و ۰/۰۸٪ است.

واژگان کلیدی: شبکه‌های حس‌گر بی‌سیم، امنیت، حملات سیبیل و مدیریت اعتماد

۱- مقدمه

پیشرفت‌های اخیر در ساخت مدارات مجتمع در اندازه‌های کوچک، از یک سو و توسعهٔ فناوری ارتباطات بی‌سیم از سوی دیگر زمینه‌ساز طراحی شبکه‌های حس‌گر بی‌سیم شده است. شبکهٔ حس‌گر به‌شدت با محیط فیزیکی اطراف خود تعامل دارد و از طریق حس‌گرها اطلاعات محیط را گرفته و درصورت نیاز پس از اعمال پردازشی ساده، آن‌ها را ارسال می‌کند. ارتباط بین گره‌ها به‌صورت بی‌سیم برقرار می‌شود و هرکدام از آن‌ها به‌صورت مستقل و بدون دخالت انسان کار می‌کنند و به‌طورمعمول ازلحاظ فیزیکی بسیار کوچک هستند.گره‌های حس‌گر با همکاری یکدیگر امکان نظارت بر محیط را فراهم می‌آورند و برای اندازه‌گیری برخی از کمیت‌های فیزیکی یا شرایط محیطی به‌کار می‌روند.

شبکه‌های حس‌گر، با انگیزهٔ استفاده در کاربردهای نظامی مانند نظارت بر میدان جنگ توسعه پیدا کردند؛ اما امروزه کاربردهای متنوعی در بخش‌های صنعتی، بهداشتی و ... دارند و بیشتر برای مطالعه محیط‌هایی مناسب هستند که امکان حضور انسان در آن محیط پرهزینه و خطرناک است. در هر مأموریت گره‌های بسیار زیادی (صدها و یا هزاران گره) در محیط عملیاتی مورد نظر پراکنده می‌شوند و به‌طورمعمول پس از گسترش گره‌ها در محیط و یا پایان مأموریت، امکان جمع‌آوری و استفاده مجدد از گره‌ها نیست. محدودیت‌های بسیاری از نظر ظرفیت حافظه، توان محاسباتی، برد رادیوئی و میزان انرژی و ... متوجه گره‌های حس‌گر خواهد بود [1]، [2]، [3]، [4]. با توجه به این محدودیت‌ها و گسترش بدون مراقبت گره‌های حس‌گر، ماهیت بی‌سیم ارتباطات و نیز

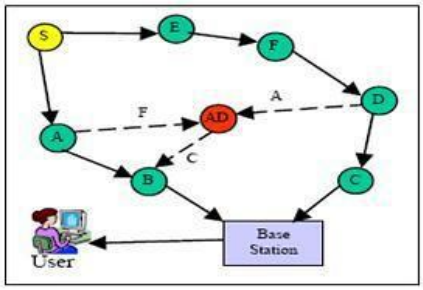
* نویسندهٔ عهده‌دار مکاتبات

[Downloaded from monadi.isc.org.ir on 2026-11-20]

کاربرد روزافزون این نوع شبکه‌ها در زمینه‌های نظامی، برقراری امنیت در شبکه‌های حس‌گر بی‌سیم امری بسیار مهم و چالش‌زا است که توجه بسیاری از پژوهش‌گران را به خود معطوف کرده است .[5]

حملات سیبیل نخستین بار در شبکه‌های نظیر به نظیر مطرح شد. دوسر[1] ادعا کرد در چنین محیط‌های محاسباتی توزیع‌شده‌ای، یک دستگاه می‌تواند به‌راحتی چندین هویت (شناسه) اختیار کند که این به‌دلیل فقدان یک قدرت مرکزی و مورد اعتماد در شبکه است [6].

حملات سیبیل به‌راحتی قابل پیاده‌سازی در شبکه‌های حس‌گر بی‌سیم هستند؛ چون گره‌های حس‌گر در یک محیط توزیع‌شده قرارگرفته‌اند و از طریق امواج رادیویی با یکدیگر ارتباط برقرار می‌کنند. این حملات عملیاتی مثل مسیریابی، رأی‌گیری، تجمیع داده‌ها، تخصیص منابع، تشخیص بدرفتاری و ... تحت تأثیر قرار می‌دهند. سازوکارهایی که مبتنی بر رأی‌گیری هستند، کارایی خود را از دست می‌دهند؛ چون برخی گره‌ها جعلی هستند و به اطلاعات به‌دست‌آمده از آن‌ها نمی‌توان اعتماد کرد [7] [8].در چنین حملاتی، مهاجم یک گره بدخواه در شبکه درج می‌کند و یا یک گره نرمال در شبکه را ضبط کرده، آن را برنامه‌ریزی مجدد کرده شکل (۱) و تحت عنوان گره بدخواه در شبکه درج می‌کند [9].



(شکل ـ ۱): حمله Sybil

گرهٔ مخرب چندین هویت جعلی برای خود ایجاد می‌کند. گره‌های نرمال در همسایگی گره بدخواه فریب‌خورده به‌اشتباه گمان می‌کنند همسایه‌های زیادی دارند. این سبب می‌شود گره بدخواه ترافیک زیادی به خود جذب کرده و به‌طور چشم‌گیری پروتکل‌های مسیریابی را مختل کند [10]، [11] [12].

هدف از این مقاله تشخیص حمله سیبیل با رویکرد امنیت نرم به‌وسیله سامانه مدیریت اعتماد است که در کنار روش‌های مبتنی بر امنیت سخت نرخ هشدارهای اشتباه را با استفاده از مقدار اعتماد کاهش داده و حملات سیبیل غیرمستقیم را تشخیص خواهد داد.

بقیه مقاله بدین صورت سازماندهی شده است: در بخش۲ کارهای گذشته و سازوکارهای دفاعی در برابر این حمله شرح داده می‌شود. در بخش۳ مدل پیشنهادی جهت تشخیص حمله سیبیل در شبکه‌های حس‌گر بی‌سیم با رویکرد مدیریت اعتماد ارائه می‌شود. در بخش۴ ارزیابی روش پیشنهادی و در بخش آخر نتیجه‌گیری و فرصت‌های پژوهشی در آینده مطرح می‌گردد.

۲- کارهای مرتبط

راه‌حل‌های متنوعی برای تشخیص حمله سیبیل و حذف آن از بستر شبکه پیشنهاد شده است. سازوکارهای دفاعی به سه دستهٔ کلی دسته‌بندی می‌شوند.

۲-۱- روش‌های مبتنی بر تشخیص هویت (شناسه)

دستهٔ نخست به‌طورکلی، حملات سیبیل را با محدودکردن تولید اطلاعات گره‌های معتبر کاهش می‌دهد. در اکثر روش‌های عمومی این دسته وابسته به تخصیص یک ID یا شناسه امن توسط یک سرور مرکزی است. این دسته برای تشخیص حملات سیبیل از روش‌های احراز هویت و رمزنگاری استفاده می‌کنند [13].

در سال ۲۰۰۴روش برای حفاظت از شبکه‌های حس‌گر بی‌سیم در برابر حملات سیبیل پیشنهاد داده‌اند که شامل یک سازوکار آزمایش منابع رادیویی(RRT[2])، موقعیت مورد تأیید و سازوکار ثبت گره و پیش‌توزیع تصادفی کلید است(RKP[3]) [14].

در [15] یک طرح مدیریت کلید به نام پروتکل تصدیق هویت و رمزنگاری متمرکز (LEAP) برای حفاظت از شبکه‌های حس‌گر بی‌سیم در برابر حملات مختلف طراحی کرده‌اند. چهار نوع از کلیدها(فردی، گروهی، دوبه‌دو و کلیدهای کلاستر) برای ایجاد احراز هویت بین هر جفت از

[1] Douceur

[2] Radio Resource Testing

[3] Random Key Pre-distribution

[Downloaded from monadi.isc.org.ir on 2026-11-20]

گره‌ها داخل شبکه ایجاد می‌شدند که مستلزم هزینه محاسباتی بالا و عدم مقیاس‌پذیری بود؛ زیرا هر گره جدید در شبکه چندین کلید با گره‌های دیگر به اشتراک می‌گذارد.

چینگ[4] و همکاران (۲۰۱۳) یک روش مبتنی برای زنجیره کلید پیش‌توزیع‌شده در برابر حمله سیبیل ارائه کردند، از چندین زنجیره کلید استفاده می‌شد. از هش اطلاعات هویتی یکتا برای هرگره پشت سرهم در ایستگاه پایه مورد اعتماد استفاده می‌شدکه درنهایت یک استخری از زنجیره کلیدها ایجاد می‌شد. سپس از طریق پروتکل CK-AE گره‌های همسایه به همراه مابقی گره‌ها احراز هویت می‌شدند و یک جفت کلید منحصربه‌مفرد برای محافظت از جعل کلیدها بوسیله مهاجمان سیبیل ایجاد می‌شد [16].

۲-۲- روش‌های مبتنی بر اطلاعات دریافتی از گره‌ها

دسته دوم با استفاده از تجزیه‌وتحلیل اطلاعات گره‌های همسایه، هویت گره‌ها را بررسی و بازبینی می‌کنند. بوسه[5] (۲۰۰۷) دو روش برای تشخیص حملات سیبیل به نام‌های MG وSRP ارائه داد که این دو روش مکمل یکدیگر هستند. روشMG برای زمانی است که گره مخرب شناسه یکی از گره‌های همسایه را در اختیار خود می‌گیرد. روشSRP برای پروتکل MAC که با امکان دسترسی انحصاری به کانال از تصادم جلوگیری می‌کنند، کاربرد دارد. این روش برای زمانی است که گره مخرب شناسه‌ای اختیار می‌کند که در همسایگی‌اش نیست؛ سپس با مبادله اطلاعاتی درباره تعداد بسته‌های دریافتی هر گره و مقایسه تعداد بسته‌های ارسال‌شده و دریافت‌شده حمله سیبیل تشخیص داده می‌شود [17].

سو[6] و همکاران (۲۰۰۹) روشی برای مقابله با حملات سیبیل در شبکه‌های حس‌گر بی‌سیم ارائه داده‌اند که در آن با استفاده از تجزیه‌وتحلیل اطلاعات گره‌های همسایه هر گره، هویت گره‌ها بررسی و بازبینی می‌شود. این روش از این واقعیت که هر گره مخرب تعداد زیادی هویت جعلی ایجاد می‌کند، استفاده می‌کند تا سازوکاری برای حفاظت از شبکه‌های حس‌گر بی‌سیم در برابر حملات سیبیل ارائه دهند [7].

۲-۳- روش‌های مبتنی بر تأیید مکان (مکان‌یابی)

دسته سوم از این واقعیت که هر گره می‌تواند در هر زمان در یک موقعیت (مکان فیزیکی) قرار گیرد برای تشخیص حمله سیبیل بهره می‌گیرد. این تکنیک وابسته به تأئید مکان است، محل موردنظر برای هر تعیین‌کننده هویت با استفاده از اندازه‌گیری فاصله و مثلث‌بندی(زاویه‌بندی) بررسی می‌شود.

دیمرباس[7] و همکاران (۲۰۰۶) یک رویکرد مبتنی بر شاخص قدرت سیگنال دریافتی (RSSI)[8] برای دفاع در برابر حملات سیبیل ارائه کردند. یک مجموعه از گره‌های حس‌گر قابل‌اعتماد به‌عنوان آشکارساز در نظر گرفته می‌شوند. پس از دریافت پیام آشکارسازها محل فرستنده پیام با بررسی قدرت سیگنال دریافتی تخمین زده می‌شود. اگر یک گروه از هویت‌ها (شناسه‌ها) در همان منطقه مستقر شوند، آشکارسازها یک گره را به‌عنوان مهاجم سیبیل در نظر می‌گیرند [18].

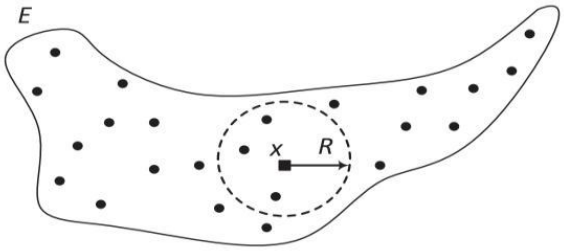
استفاده از نسبت RSSI ابتدا توسط سونگ[9] و همکاران برای تشخیص مکان فرستنده با استفاده از چهار گره ناظر مطرح شد [19] که از الگوریتم موقعیت‌یابی پیشنهادشده برای تشخیص حملات سیبیل استفاده می‌کند. بدین‌صورت که با دریافت یک پیغام، چهار گره ناظر، موقعیت فرستنده را محاسبه کرده و موقعیت حاصله را با شناسه فرستنده مرتبط می‌کنند؛ سپس با دریافت پیغامی با شناسه جدید، مکان فرستنده محاسبه‌شده و در صورت تشابه، تشخیص حمله سیبیل اعلام می‌شود.

ساریکیانیدیس و همکاران (۲۰۱۵) یک روش مبتنی بر قانون براساس تشخیص به‌صورت ناهنجاری با استفاده از اطلاعات در محدوده فرکانسیUWB[10] برای تشخیص حملات سیبیل ارائه کردند [20]. پهنانی باند گسترده(UWB) یک فناوری رادیویی برای مخابرات بی‌سیم در سطوح بسیار پایین انرژی است که برای برد کوتاه استفاده می‌شود. این فناوری از بخش بزرگی از طیف رادیویی استفاده می‌کند و هزینه پیاده‌سازی آن پایین است. در این روش احتمال ناحیه همزیستی(احتمال اینکه دو گره در همان ناحیه حلقه دایره‌ای قرار گیرند) تعریف می‌شود. این مدل یک شبکه حس‌گر بی‌سیم مبتنی بر پهنای باند گسترده با استاندارد IEEE 802.15.4 با M گره حس‌گر در نظر می‌گیرد. گره‌ها به‌طور یکنواخت در یک ناحیه با نام E شکل (۲) مستقر گردیده‌اند.

[1] Cheng
[2] Bhuse
[3] Ssu
[4] Demirbas

[4] Received Signal Strength Indicator
[5] zhong
[6] Ultra-wideband

[Downloaded from monadi.isc.org.ir on 2026-11-20]



(شکل_۲): میدان شبکه حس‌گر

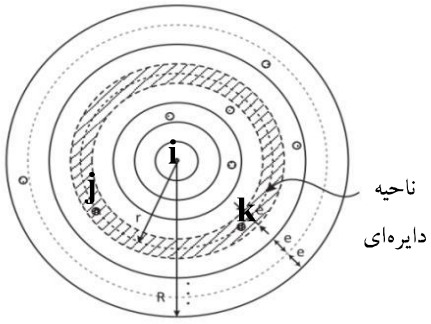
در RADS[1] از چهار مرحله برای تشخیص حملات سیبیل در شبکه‌های حس‌گر بی‌سیم استفاده می‌کند.

مرحلهٔ نخست مرحلهٔ کشف همسایه است.کشف همسایه شامل تبادل بسته‌هایhello بین گره‌های همسایه است. در مرحله دوم هر گره یک جدول که حاوی تخمین محدوده محاسبه‌شده است، به‌طور محلی ایجاد می‌کند. یعنی فاصلهd_{ij}^{e} از هر گره همسایه تشخیص داده می‌شود. نماد d_{ij}^{e} تخمین فاصله بین گره n_i وn_j می‌باشد که با گره n_i اندازه‌گیری می‌شود.

با d_{ij}^{a} فاصله واقعی بین گره n_i و n_j علامت‌گذاری می‌شود که به‌شرح ذیر محاسبه می‌شود:

$d_{ij}^{e} - \frac{e}{2} \leq d_{ij}^{a} \leq d_{ij}^{e} + \frac{e}{2}$ برای هر گره n_i و n_j که i و j عضو M است.

در مرحله سوم هر گره به‌تنهایی در شبکه به‌طور مستقل بررسی فاصله را چندین‌بار انجام می‌دهد(شکل۳).



(شکل_۳): نحوه تشخیص گره سیبیل [20]

درصورتی‌که گره n_i دو گره دیگر را (گره‌هایی به‌طور مجزا) مثل n_j و n_k که تفاوت فاصله آن‌ها کمتر از e باشد پیدا کند، علامت‌گذاری می‌شود.گره با بررسی فاصله متوجه یک حمله سیبیل می‌شود که نتیجه آن اضافه‌شدن گره n_k به فهرست سیاه است. مرحله سوم از الگوریتم، یک گام تکرار است؛ به این معنی که بررسی فاصله به‌صورت متوالی انجام می‌شود. درواقع تشخیص حمله سیبیل به فرکانسی که هر گره مرحلهٔ کشف همسایگان را برای همسایگان جدید در مجاورتش جستجو می‌کند، وابسته است.

در مرحله چهارم فاصله بین همسایگان جدیدی که اضافه‌شده‌اند و گره‌های موجود دیگر که در فهرست همسایگان می‌باشند، مرتباً بررسی می‌شود که همیشه به‌روز باشد.

روش ساریکیانیدیس و همکاران (۲۰۱۵) جزء روش تشخیص مبتنی بر مکان است که براساس رویکرد امنیت سخت عمل می‌کند. در روش های مبتنی بر امنیت سخت بعد از اینکه یک گره مجاز شناخته می‌شود، از آن به بعد رفتارش بررسی نمی‌شود؛ به عبارت دیگر اگر موجودیتی مجاز شناخته شد همه چیز در اختیارش قرار می‌گیرد. در یک شبکهٔ حس‌گر بی‌سیم اگر یکی از عامل‌ها آلوده شود و رفتار و عملکرد مخربی داشته باشد در شبکه همچنان مجاز باقی می‌ماند و به عملکرد مخرب خود ادامه می‌دهد.

روش پیشنهادی در یک محیط شبیه‌سازی دقیق بررسی شده که نشان می‌دهد سامانه تشخیص پیشنهادی در برابر حملات سیبیل اثر بخش بوده است. به طور کلی ویژگی‌های سامانه‌های تشخیص با روش‌های موجود مقایسه شده که در جدول۱ نشان داده شده است.

سید محمود سجاد[2] و همکاران یک تکنیک تشخیص نفوذ بر اساس محاسبه اعتماد به وسیله گره‌های همسایه ارائه داده‌اند. در این سامانه تشخیص نفوذ پیشنهادی هر گره از سطح اعتماد گره‌های همسایه اطلاع دارد. بر اساس این مقادیر اعتماد، گره‌های همسایه ممکن است به‌عنوان گره قابل اعتماد، گره پرمخاطره و یا گره مخرب اعلام شوند. فرضیه این تکنیک بر این اساس عمل می‌کند که گره‌هایی که در یک منطقه خاص واقع شده‌اند، به‌طورعمومی دارای رفتار مشابهی هستند. سامانه تشخیص نفوذ پیشنهادی دارای یک مدیر اعتماد است که اعتماد مستقیم و غیر مستقیم یک گره را مدیریت می‌کند. طبقه‌بندی رفتار بر اساس مقادیر اعتماد و محاسباتی است که از طرف مدیر اعتماد به دست آورده است، که درنهایت باعث دسته‌بندی رفتار گره‌ها به حمله‌کننده، قابل اعتماد و مخاطره‌آمیز می‌شود. در صورتی که رفتار گره قابل اعتماد باشد این گره را به محرک ارسال، به منظور ارسال بسته

[1] Rule-based anomaly detection system

[2] Syed Muhammad Sajjada

[Downloaded from monadi.isc.org.ir on 2026-11-20]

توصیه می‌کند. هنگامی که رفتار یک گره مخاطره‌آمیز تشخیص داده شود، فاکتورهای خطر، ارزیابی و به‌روز می‌شود. اگر دیده شود که یک گره تمایل به خطر دارد، به محرک ارسال، برای ارسال بسته‌ها توصیه می‌کند که گره مورد نظر رفتار پرخطر دارد. وضعیت گره‌های مشاهده‌شده در پایگاه داده پیشنهادی ذخیره می‌شود. در مورد رفتارهایی که منجر به حمله می‌شود، دسته‌بندی حملات الگوی حمله را براساس یک سری محاسبات تشخیص می‌دهد. بر این اساس این گره به منظور نامزدی برای ارسال رد می‌شود[21].

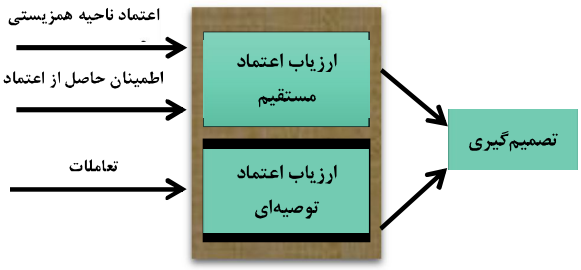
(جدول-۱): تجزیه و تحلیل مقایسه‌ای انواع سیستم‌های تشخیص حمله سیبیل

Citation	Lightweight?	Authentication based method?	Location information?	Specialized h/w?	Comm. Mode	Identity type	Operation	Approch
(this paper)	✓	×	✓	×	Both	Both	Distributed	Hard & Soft Security
Douceur (2002)	×	✓	×	×	Direct	Fabricated	Centralized	Hard-Security
Karlof and Wagner (2003)	×	✓	×	×	Direct	Fabricated	Centralized	Hard-Security
Zhu et al. (2003)	×	✓	×	×	Direct	Stolen	Distributed	Hard-Security
Zhang et al. (2005)	✓	✓	×	×	Direct	Both	Distributed	Hard-Security
Piro et al. (2006)	✓	✓	×	✓	Direct	Fabricated	Distributed	Hard-Security
Xing et al. (2008)	×	✓	×	×	Direct	Stolen	Centralized	Hard-Security
Parno et al. (2005)	×	✓	×	✓	Direct	Stolen	Distributed	Hard-Security
Conti et al. (2007)	✓	✓	×	×	Direct	Stolen	Distributed	Hard-Security
Lazos and Poovendran (2005)	✓	×	✓	×	Direct	Stolen	Distributed	Hard-Security
Mukhopadhyay and Saha (2006)	✓	×	✓	✓	Direct	Fabricated	Centralized	Hard-Security
Demirbas and Song (2006)	✓	×	✓	×	Direct	Fabricated	Distributed	Hard-Security
Wang et al. (2007)	✓	×	✓	×	Direct	Fabricated	Distributed	Hard-Security
Ssu et al. (2009)	✓	×	✓	×	Direct	Fabricated	Distributed	Hard-Security
Zhang et al. (2006)	×	✓	✓	×	Direct	Both	Centralized	Hard-Security
Wang and Lu (2006)	✓	×	×	✓	Both	Fabricated	Centralized	Hard-Security
Lu et al. (2011)	✓	×	×	✓	Both	Fabricated	Centralized	Hard-Security
Sarigiannidis, et al., (2015)	✓	×	✓	×	Direct	Both	Distributed	Hard-Security

[Downloaded from monadi.isc.org.ir on 2026-11-20]

۳- توصیف روش پیشنهادی

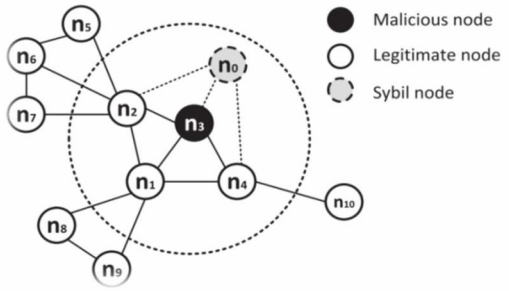
به‌منظور کاهش نرخ هشدارهای اشتباه و تشخیص حملات سیبیل غیرمستقیم و نظارت بر عملکرد گره‌ها در طول مدت فعالیت‌شان از یک پروتکل با رویکرد مدیریت اعتماد به‌شرح ذیل استفاده می‌کنیم. ساختار کلی مدل پیشنهادی در شکل۴ آمده است. در این پروتکل، اعتماد مستقیم بر اساس اعتماد ناحیه همزیستی و اطمینان حاصل از اعتماد، بر اساس تعاملات بین گره‌ها محاسبه می‌شود. همچنین از اعتماد توصیه‌ای (غیرمستقیم) به‌منظور تشخیص حملات سیبیل غیرمستقیم استفاده می‌شود که در آن گره مجاز به‌طورمستقیم با گره سیبیل در ارتباط نیست.



(شکل_۴): ساختار کلی روش پیشنهادی

۳-۱- قابلیت به‌کارگیری مدل پیشنهادی به‌منظور کاهش نرخ هشدارهای اشتباه

هر گره از یک جدول که حاوی تعداد تعاملات موفق و ناموفق در هر دوره و میزان اعتماد ناحیه همزیستی محاسبه‌شده برای گره‌های همسایه است، استفاده می‌کند. شکل۵ حمله سیبیل مستقیم را برای گره n_2 نشان می‌دهد.



(شکل_۵): حمله سیبیل مستقیم برای گره n_2

جدول۱ اعتماد مستقیم گره n_2 برای توپولوژی شبکه در شکل۵ نشان می‌دهد.

(جدول_۱): اعتماد مستقیم گره n_2

	n_0	n_1	n_3	n_5	n_6	n_7
	$S_{n_{20}}, F_n$	$S_{n_{21}}, F_n$	$S_{n_{23}}, F_n$	$S_{n_{25}}, F_n$	$S_{n_{26}}, F_n$	$S_{n_{27}}, F$
T_n	$T_{n_{20}}$	$T_{n_{21}}$	$T_{n_{23}}$	$T_{n_{25}}$	$T_{n_{26}}$	$T_{n_{27}}$

اعتماد ناحیه همزیستی مطابق رابطه(۱) تعیین می‌شود.

$$T = 1 - e^{-\left|\left|d_{ij}^{e} - d_{ik}^{e}\right| - \alpha\right|} \qquad (۱)$$

در این رابطه α همان محدوده خطا، d_{ij}^{e} تخمین فاصله بین گره n_i و n_j و d_{ik}^{e} تخمین فاصله بین گره n_i و n_k است. درصورتی‌که قدر مطلق $\left|\left|d_{ij}^{e} - d_{ik}^{e}\right| - \alpha\right|$ (که از این پس با نماد ρ نشان داده خواهد شد) به صفر نزدیک شود مقدار e^{ρ} به یک نزدیک می‌شود درنتیجه مقدار اعتماد ناحیه همزیستی (T) به صفر میل خواهد کرد.

میزان اعتماد بر اساس منطق ذهنی[1] جوسانگ[22] محاسبه می‌شود. میزان باور، عدم باور و عدم قطعیت براساس این تعاملات طبق رابطه(۲) تعیین می‌شود.

$$b = \frac{s}{s+f+1},\ d = \frac{f}{s+f+1} \qquad (۲)$$
$$u = \frac{1}{s+f+1}$$

میزان باور(b)، میزان عدم باور(d)، عدم قطعیت (c)، تعداد تعاملات موفق(s)، تعداد تعاملات ناموفق(f) است.

مقدار اعتماد طبق رابطه (۳) محاسبه می‌شود.

$$T_C = \frac{b}{1-u} \qquad (۳)$$

در صورتی که عدم قطعیت صفر باشد، آنگاه مقدار اعتماد برابر با میزان باور خواهد بود.

درصورتی‌که مقدار اعتماد ناحیه همزیستی(T) کمتر از مقدار آستانه (T_t) باشد، آن گره به‌عنوان گره مشکوک بوده و تصمیم‌گیری نهایی در خصوص تشخیص گره سیبیل براساس مقدار اعتماد(T_C) که حاصل از تعداد تعاملات موفق و ناموفق است، تعیین خواهد شد.

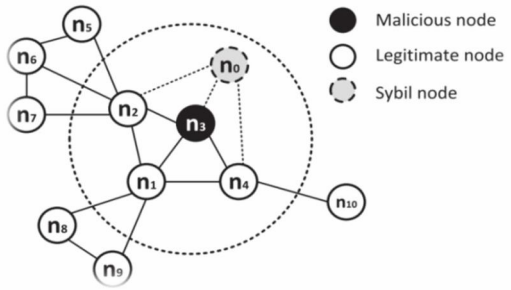
[1] Subjective Logic

[Downloaded from monadi.isc.org.ir on 2026-11-20]

برای مقدار اعتماد، یک آستانه (T_{tC}) در نظر می‌گیریم چنانچه مقدار به‌دست‌آمده کمتر از مقدار آستانه باشد، آن گره را به‌عنوان گره سیبیل تشخیص می‌دهیم.

۳-۲- قابلیت تشخیص حملات سیبیل غیرمستقیم در مدل پیشنهادی

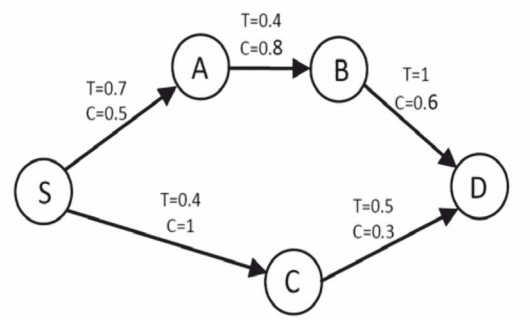
در تشخیص حملات سیبیل غیرمستقیم با توجه به اینکه گره سیبیل به‌طورمستقیم با گره مجاز در ارتباط نیست و این ارتباط از طریق گره بدخواه فراهم می‌شود؛ لذا برای تشخیص گره سیبیل در این پروتکل از اعتماد توصیه‌ای (غیرمستقیم) بر اساس تعاملات به‌شرح زیر استفاده می‌شود: شکل (۶)



(شکل_۶): حمله سیبیل غیرمستقیم

با توجه به اینکه هر گره دارای جدول همسایگی است که در آن تعداد تعاملات موفق و ناموفق در هر دوره نسبت به همسایگانی که به‌طورمستقیم با آن‌ها در ارتباط هستند، ثبت شده است، به‌منظور تشخیص گره سیبیل در این روش نظر گره‌های دیگر را که به‌طور مستقیم با گره مقصد در ارتباط هستند، بررسی می‌شود. بر اساس تعاملات موفق و ناموفق در هر دوره میزان اعتماد آگاه از اطمینان بر اساس منطق ذهنی[۱۴] جوسانگ [22] محاسبه می‌شود و میزان باور، عدم باور و عدم قطعیت بر اساس این تعاملات طبق رابطه (۲) و مقداراعتماد طبق رابطه (۳) تعیین می‌شود.

اطمینان میزان باور به‌درستی تخمین اعتماد است. در مقایسه دو مفهوم اعتماد و اطمینان توجه به این نکته لازم است، اعتماد در مورد یک عامل در نظر گرفته می‌شود و اطمینان در مورد مقدار اعتماد ارزیابی‌شده است که مقدار آن در بازه [0,1] معنی دارد. میزان اطمینان به یک تخمین اعتماد می‌تواند مبنای تعیین وزن این تخمین در ترکیب نظرات اعتماد باشد که به محاسبه دقیق‌تر مقدار اعتماد می‌انجامد و همچنین اطمینان می‌تواند به‌عنوان پارامتری در نظر گرفته شود که بعد دیگری به خروجی مدل اعتماد اضافه می‌کند. به‌عنوان نمونه شکل (۷) یک شبکه اعتماد را نشان می‌دهد که در آن برچسب هر یال گراف علاوه‌بر مقدار اعتماد(T)، میزان اطمینان (C) به اعتماد تخمین‌زده‌شده را نیز در بر دارد؛ برای مثال برچسب لبه SA نشان می‌دهد که گره S به گره A مقدار 0.7 اعتماد دارد؛ درصورتی‌که مقدار اطمینان به اعتماد تخمین‌زده‌شده فقط 0.5 است [23].



(شکل_۷): یک شبکه اعتماد نمونه با مقادیر اطمینان[23]

در بسیاری از مدل‌های مدیریت اعتماد، تخمنین اطمینان در محاسبه اعتماد مستقیم یا مفاهیم نزدیک به آن مانند قطعیت قابلیت اتکا، باورپذیری و ... مورد توجه قرار می‌گیرد.

میزان اطمینان درک غنی‌تری از اعتماد و درنهایت تصمیم‌گیری بهتری برای چگونگی واکنش به ما می‌دهد؛ [24] که در رابطه(۴) نشان داده شده است.

$$C_{ind} = 1 - u \qquad (۴)$$

درصورتی‌که نتیجه حاصل از برآیند اعتماد توصیه‌ای آگاه از اطمینان گره مقصد کمتر از مقدار آستانه باشد، گره مذکور را به‌عنوان گره سیبیل تشخیص داده می‌شود و در فهرست سیاه قرار می‌گیرد.

با توجه به اینکه تعاملاتی که به زمان حال نزدیک است، باید تأثیرگذارتر نسبت به تعاملات گذشته باشند، لذا تأثیر زمان و پویایی در ارزیابی اعتماد آگاه از اطمینان و تصمیم‌گیری مبتنی بر آن طبق رابطه ۵ و ۶ در محاسبه میزان باور و عدم باور استفاده می‌شود.

$$W_i = e^{-\lambda \Delta T_i} \qquad \Delta T_i = T_{Current} - T_i \qquad (۵)$$

λ ضریب میرایی اعتماد است که مشخص می‌کند از چه زمان قبل‌تر تعاملات تأثیر نداشته باشد W_i وزن تعاملات

[1] Subjective Logic

[Downloaded from monadi.isc.org.ir on 2026-11-20]

را مشخص می‌کند. درصورتی‌که از زمان تعاملات (نسبت به زمان جاری) زمان زیادی گذشته باشد، مقدار $e^{-\lambda \diamond T_i}$ و درنتیجه W_i به صفر نزدیک می‌شود.

$$s = \sum_{x_i \in ST} W_i \quad , \quad f = \sum_{x_i \in FT} W_i \qquad (۶)$$

ST مجموعه تعاملات موفق و FT مجموعه تعاملات ناموفق است.

این تعاملات می‌توانند به‌صورت اسلات‌های زمانی در نظر گرفته شود که هر کدام دارای یک برچسب زمانی هستند.

۴- ارزیابی مدل پیشنهادی

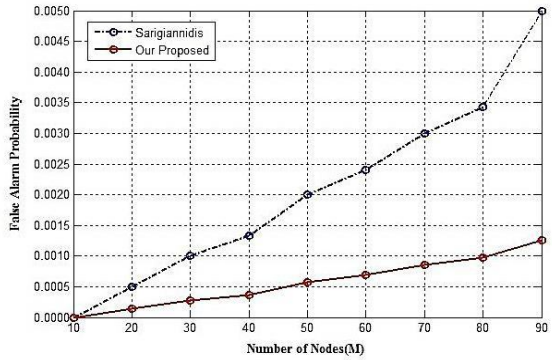
روش پیشنهادی در نرم‌افزار متلب شبیه‌سازی‌شده است. M تعداد کل گره‌های حس‌گر، R شعاع ارتباطات (شعاع حسی) ، e محدوده خطا و E ناحیه‌ای است که گره‌های حس‌گر در آن توزیع شده‌اند. جدول (۲) پارامترهای مورد استفاده در شبیه‌سازی را نشان می‌دهد. مقدار هر یک از پارامترها در جدول آورده شده است. با توجه به بررسی تأثیر تعداد گره بر عملکرد مدل پیشنهادی، تعداد گره‌ها بین ۱۰ تا ۱۰۰ بررسی خواهد شد.

(جدول_۲): پارامترهای به‌کاررفته در شبیه‌سازی

پارامتر	مقدار	توضیحات
M	10-100	تعداد کل گره‌های حس‌گر
Ms	2-20	تعداد گره‌های سیبیل
Mj	8-80	تعداد گره‌های مجاز
R	20m	شعاع ارتباطات
e	50cm	محدوده خطا
E	$100m^2$	ناحیه‌ای که در آن گره‌های حس‌گر توزیع‌شده‌اند
T_{tC}	0.60	مقدار آستانه اعتماد در اعتماد مستقیم
T_{ind}	0.68 , 0.85	مقدار آستانه در اعتماد آگاه از اطمینان
S	--	تعداد تعاملات موفق
F	--	تعداد تعاملات ناموفق

۴-۱- نتایج حاصل از آزمایش‌ها در تشخیص حملات سیبیل مستقیم

نمودار شکل (۸) مقایسه احتمال تولید هشدارهای اشتباه روش پیشنهادی را با روش ساریکیانیدیس به‌عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.که مقدار $E=100m^2$، محدوده شعاع ارتباطات R=20m و محدوده خطا e=50cm می‌باشد، که تعداد گره‌ها از ۱۰ تا ۹۰ تغییر می‌یابد.



(شکل_۸): مقایسه احتمال تولید هشدارهای اشتباه

جدول (۳) نتایج نرخ هشدارهای اشتباه (FPR) را هنگامی‌که تعداد گره‌ها (M) در حال تغییر است، نشان می‌دهد. همان‌طور که نشان داده شده است، مقدار نرخ هشدارهای اشتباه در روش ساریکیانیدیس 0.005% و در روش پیشنهادی کمتر از 0.002% است. زمانی که تعداد گره‌ها افزایش می‌یابد، احتمال اینکه گره‌ای به‌اشتباه در ناحیهٔ همزیستی گره دیگری قرار گیرد، بیشتر می‌شود و درنتیجه اعتماد ناحیهٔ همزیستی کاهش می‌یابد و از مقدار آستانهٔ همزیستی (T_t) کمتر می‌شود. در مرحله دوم که باید بر اساس میزان تعاملات موفق و ناموفق تصمیم‌گیری شود، احتمال اینکه میزان اعتماد کمتر از مقدار آستانه اعتماد (T_{tc}) شود محتمل‌تر است.

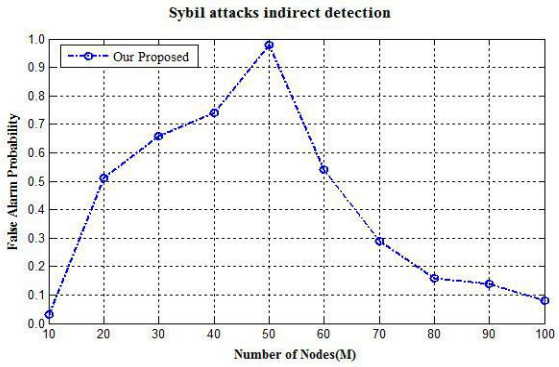
(جدول_۳): مقایسه احتمال هشدارهای اشتباه

Number of nodes	10	30	50	70	90
Sarigiannidis	0.00000	0.00100	0.00200	0.00320	0.00500
Our proposed	0.00000	0.00027	0.00057	0.00085	0.00126

۴-۲- نتایج حاصل از آزمایش‌ها در تشخیص حملات سیبیل غیرمستقیم

نمودار شکل (۹) نرخ FP، در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای، به‌عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد که مقدار $E=100m^2$، محدوده شعاع ارتباطات R=20m و محدوده خطا e=50cm است که تعداد گره‌ها از ۱۰ تا ۱۰۰ تغییر می‌یابد.

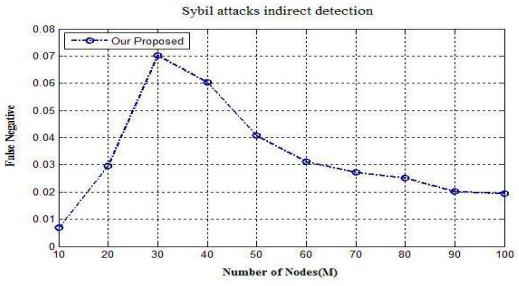
[Downloaded from monadi.isc.org.ir on 2026-11-20]



(شکل_۹): نرخ FP در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

همان‌طور که در نمودار شکل (۹) نشان داده‌شده مقدار نرخ هشدارهای اشتباه بسیار کم و زمانی که تعداد گره‌ها M=100 است به 0.08% می‌رسد. مقدار نرخ هشدارهای اشتباه در ابتدا با افزایش گره‌ها افزایش می‌یابد. باتوجه به‌ثابت‌بودن مساحتی که گره‌ها در آن توزیع شده‌اند ($E=100m^2$) و از طرفی هر گره می‌بایست در شعاع حسی گره دیگر قرار بگیرد به جهت پوشش بیشتر ناحیه، تعداد همسایگانی که در جدول همسایگی هر گره قرار می‌گیرد، کم‌تر می‌شود؛ درنتیجه تعداد نظرات کمتری در مورد گره مقصد وجود دارد. زمانی که تعداد گره‌ها به پنجاه گره می‌رسد با توجه به اینکه E ثابت است، تعداد همسایگانی که در جدول همسایگی هر گره قرار می‌گیرد، بیشتر می‌شود و تعداد نظرات بیشتری در مورد گره مقصد وجود خواهد داشت. درنتیجه احتمال اشتباه کاهش پیدا می‌کند و ازآنجا به بعد نرخ هشدارهای اشتباه کمتر می‌شود.

نمودار شکل ۱۰ نرخ FN را در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای، به‌عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.



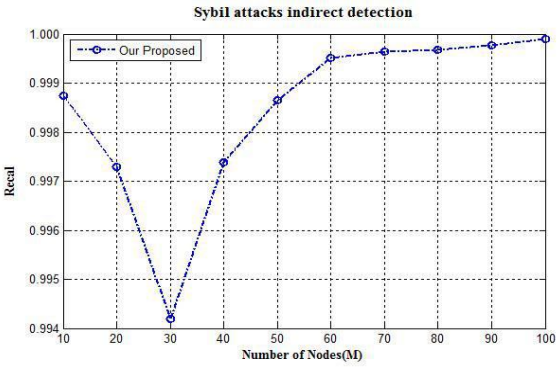
(شکل_۱۰): نرخ FN در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

همان‌طورکه در نمودار شکل ۱۰ نشان داده شده است، نرخ FN با افزایش تعداد گره‌ها افزایش می‌یابد. با توجه به ثابت‌بودن اینکه مقدار E و تراکم کم گره‌ها، در نتیجه تعداد همسایگانی کمتری در جدول همسایگی هر گره قرار می‌گیرد؛ لذا زمانی که تعداد گره‌ها کمتر از ۳۰ است، نرخ FN افزایش می‌یابد.

نمودار شکل ۱۱ به‌عنوان نمودار Recall، نسبت حملاتی را که به‌درستی تشخیص داده‌شده(TP) به‌کل حملات (هم حملاتی که به‌درستی تشخیص دادیم و هم حملاتی که تشخیص داده نشده است(TP+FN)) با استفاده از اعتماد توصیه‌ای، به‌عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.

Recall را به‌عنوان نرخ True Positive یا Sensitivity در نظر گرفته می‌شود که طبق رابطه (۷) محاسبه می‌شود.

$$\text{Recall} = \frac{TP}{TP + FN} \qquad (۷)$$



(شکل_۱۱): نسبت حملات که به‌درستی تشخیص داده‌شده به‌کل حملات (Recall) با استفاده از اعتماد توصیه‌ای

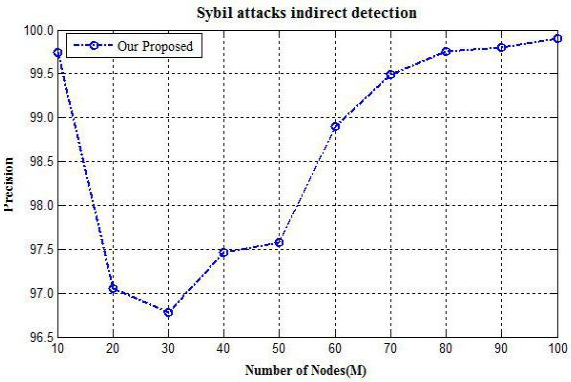
نمودار شکل۱۲ به‌عنوان نمودار Precision، نسبت حملاتی که به‌درستی تشخیص داده‌شده(TP) به‌کل تشخیص (هم حملاتی که به‌درستی تشخیص دادیم و هم آن‌هایی که حمله نبود و به‌اشتباه حمله تشخیص دادیم(TP+FP)) را با استفاده از اعتماد توصیه‌ای، به‌عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.

Precision دقت مدل پیشنهادی را نشان می‌دهد که طبق رابطه(۸) محاسبه می‌شود.

$$\text{Precision} = \frac{TP}{TP + FP} \qquad (۸)$$

زمانی که تعداد گره‌ها به صد گره افزایش می‌یابد، دقت تشخیص روش پیشنهادی 99.92 درصد می‌باشد.

[Downloaded from monadi.isc.org.ir on 2026-11-20]



(شکل-۱۲): نسبت حملاتی که به‌درستی تشخیص داده‌شده به‌کل تشخیص (Precision) با استفاده از اعتماد توصیه‌ای

۵- نتیجه‌گیری

روش‌های مختلف ارائه‌شده برای تشخیص حملات سیبیل بر اساس رویکرد امنیت سخت است. این روش‌ها باید محدودیت‌های این شبکه‌ها را در منابع پردازشی، حافظه و توان در نظر بگیرند. سازوکارهای مبتنی بر امنیت سخت برای حفظ امنیت سامانه‌های اطلاعاتی به‌خصوص در جوامع باز، کافی نیستند که در سال‌های اخیر رویکردی جدیدی از امنیت به نام امنیت نرم مورد توجه واقع‌شده است؛ که در آن به‌جای یک نهاد مرکزی، افراد مسئول امنیت خود هستند که سامانه‌های مدیریت اعتماد نمونه‌ای از راهکارهای مبتنی بر امنیت نرم هستند.

در روش پیشنهادی از مقدار اعتماد هر گره استفاده و مقدار اعتماد مستقیم و غیرمستقیم که برگرفته از توصیه‌های دریافتی از همسایه‌ها و وزن دهی به این توصیه‌ها می‌باشد، استفاده شد؛ که با ترکیب مقادیر اعتماد مستقیم و غیرمستقیم و تعیین وزنی برای این دو مقدار اعتماد، نرخ هشدارهای اشتباه کاهش یافت و از طرفی حملات سیبیل غیرمستقیم تشخیص داده شد.

با توجه به نتایج آزمایش‌های ارائه‌شده، مدل پیشنهادی باعث افزایش دقت و کاهش نرخ هشدارهای اشتباه شد و از طرفی امکان تشخیص حملات سیبیل غیرمستقیم را فراهم کرد. با درنظرگرفتن عامل زمان در تعاملات برای محاسبه اعتماد آگاه از اطمینان یک سامانه مدیریت اعتماد پویا ارائه شد که مقادیر اعتماد بین گره‌ها را با درنظرگرفتن عامل زمان محاسبه می‌کند. این روش برای محاسبه اعتماد غیرمستقیم بین گره‌ها، میزان اطمینان به اعتماد را در نظر می‌گیرد تا توصیه‌های قابل‌اطمینان‌تر، تأثیر بیشتری در محاسبه اعتماد داشته باشند.

بهبود روش ارائه‌شده به‌منظور کاهش میزان انرژی و استفاده از روش‌های یادگیری ماشین برای تعیین پارامترهای مورد استفاده در مدل پیشنهادی مانند ضریب پویایی و شکنندگی، ازجمله مواردی هستند که در آینده می‌تواند موضوع پژوهش و تحقیق قرار گیرند. همچنین مدل‌کردن روش ارائه‌شده برای دیگر حملات مطرح در شبکه‌های حس‌گر بی‌سیم ازجمله، حمله گودال و کرم‌چاله می‌تواند از اهداف پژوهشی در آینده باشد.

۶- منابع

[1] Yick, Mukherjee and Ghosal, "Wireless sensor network survey," Computer networks, pp. 2292-2330, 2008.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., "A survey on sensor networks," IEEE communications magazine, vol. 40(8), pp. 102-114, 2002.

[3] Walters, J. P., Liang, Z., Shi, W. and Chaudhary, V., "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, vol. 1, p. 367, 2007.

[4] Goldsmith, A. J. and Wicker, S. B., "Design challenges for energy-constrained ad hoc wireless networks.," IEEE wireless communications, vol. 9(4), pp. 8-27, 2002.

[5] Sharma and Dhawan, "An Enhanced and efficient mechanism to detect Sybil attack in Wireless Sensor Networks," International Journal of Advanced Research in Computer Engineering & Technology(IJARCET), p. 2(2), 2013.

[6] Douceur, "The sybil attack," In Peer-to-peer Systems, no. Springer Berlin Heidelberg, pp. 251-260, 2002.

[7] Ssu, Wang and Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," Computer Networks, pp. 3042-3056, 2009.

[8] Misra, S., Zhang, I. and Misra, S. C. (Eds.)., "Guide to wireless sensor networks," Springer Science & Business Media, 2009.

[9] Su, Lin, Ren and Zhan, "Security mechanisms analysis of wireless sensor networks specific routing attacks," In 2006 First International Symposium on Pervasive Computing and Applications, 2006.

[10] Padmavathi and Shanmugapriya, "A survey of attacks," security mechanisms and challenges in wireless sensor networks, 2009.

[11] P. Rathee and S. Malhotra, "Prevention of Sybil Attack using Cryptography in Wireless Sensor

[Downloaded from monadi.isc.org.ir on 2026-11-20]

Networks," International Journal for Innovative Research in Science and Technology, vol. 2(2), pp. 100-105, 2015.

[12] Sujatha, V. and Anita, E. M., "Detection of Sybil Attack in Wireless Sensor Network.," Middle-East Journal of Scientific Research 23, pp. 202-206, 2015.

[13] Malan, D. J., Welsh, M. and Smith, M. D., "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In Sensor and Ad Hoc Communications and Networks," IEEE SECON 2004. 2004 First Annual IEEE Commu, 2004, October.

[14] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," In Third International Symposium on Information Processing in Sensor Networks, pp. 259-268, 2004.

[15] S. Zhu, S. Setia and S. Jajodia, " LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," ACM Transactions on Sensor Networks (TOSN), vol. 2(4), pp. 500-528, 2006.

[16] C. Cheng, Y. Qian and D. Zhang, "An Approach Based on Chain Key Predistribution against Sybil Attack in Wireless Sensor Networks.," International Journal of Distributed Sensor Networks., 2013.

[17] V. Bhuse, "Lightweight intrusion detection: A second line of defense for unguarded wireless sensor networks," Doctoral dissertation, Western Michigan University, 2007.

[18] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks.," In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, no. IEEE, pp. 564-570, 2006, June.

[19] S. Zhong, L. Li, Y. G. Liu and Y. R. Yang, "Privacy-preserving location-based services for mobile users in wireless networks," Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297., 2004.

[20] P. Sarigiannidis, E. Karapistoli and . A. A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," Expert Systems with Applications, vol. 42(21), pp. 7560-7572, 2015.

[21] S. M. Sajjad, S. H. Bouk and M. Yousaf, "Neighbor node trust based intrusion detection system for wsn," Procedia Computer Science, vol. 63, pp. 183-188, 2015.

[22] A. Jøsang, E. Gray and M. Kinateder, "Simplification and analysis of transitive trust networks," Web Intelligence and Agent Systems, vol. 4(2), pp. 139-161., 2006.

[23] H. Shakeri and A. G. Bafghi, "A layer model of a confidence-aware trust management system," International Journal of Information Science and Intelligent System, vol. 3(1), pp. 73-90, 2014.

[24] H. Shakeri and A. G. Bafghi, "CATEF: Confidence-aware trust estimation framework," In Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on, no. IEEE, pp. 1-6, 2013.



سید محمد طباطبائی‌پارسا تحصیلات خود را در مقاطع کارشناسی و کارشناسی‌ارشد در رشته مهندسی‌فناوری اطلاعات گرایش امنیت اطلاعات به‌ترتیب از دانشگاه علمی وکاربردی مرکز علمی- صنعتی مشهد در سال ۱۳۹۳ و از دانشگاه بین‌المللی امام‌رضا(ع) در سال ۱۳۹۵ به پایان رسانده است. وی در تمامی مقاطع تحصیلی به‌عنوان دانشجو ممتاز می‌باشد. زمینه‌های پژوهشی مورد علاقه ایشان مدیریت اعتماد، پنهان نگاری، رمزنگاری و امنیت شبکه می‌باشد.



حسن شاکری مدارک کارشناسی، کارشناسی ارشد و دکترای خود را در رشته مهندسی کامپیوتر ـ نرم‌افزار به‌ترتیب از دانشگاه‌های فردوسی مشهد، صنعتی شریف و فردوسی مشهد دریافت کرد و در حال حاضر عضو هیأت علمی گروه کامپیوتر دانشگاه آزاد اسلامی مشهد است. از وی بیش از ۷۰ مقاله علمی در کنفرانس‌ها و مجلات داخلی و بین‌المللی منتشر شده است. زمینه‌های تحقیقاتی مورد علاقه وی مدیریت اعتماد، امنیت شبکه‌ها ، سامانه‌های کامپیوتری و پردازش زبان‌های طبیعی است.

[Downloaded from monadi.isc.org.ir on 2026-11-20]