رویکرد جدید برای تشخیص حملات سیبیل غیرمستقیم در شبکه‌های حس‌گر بی‌سیم مبتنی بر اعتماد آگاه از اطمینان با درنظرگرفتن عامل زمان

سیدمحمدطباطبائی‌پارسا*[1] و حسن شاکری[2]

[1]دانش‌آموخته کارشناسی‌ارشد مهندسی‌کامپیوتر،امنیت اطلاعات دانشگاه بین المللی‌امام 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، اطلاعات محیط را از طریق حس‌گرها،گرفته و در صورت نیاز پس از اعمال پردازشی ساده، آن‌ها را ارسال می‌کنند.گره‌های حس‌گر دارای محدودیت‌هایی به‌لحاظ حافظه، توان محاسباتی، برد رادیویی و میزان انرژی دارند. با توجه به گسترش بدون مراقبت گره‌های حس‌گر و ماهیت بی‌سیم ارتباطات، این شبکه‌ها مستعد حملات زیادی هستند. یکی از این حملات، حمله سیبیل است. در این حمله گره مخرب چندین هویت جعلی برای خود ایجاد کرده و گره‌های همسایه را فریب می‌دهد. این سبب می‌شود که گره بدخواه ترافیک زیادی را به خود جذب کرده و به‌طور چشم‌گیری پروتکل‌های مسیریابی را مختل کند. مدل پیشنهادی برای تشخیص این دسته از حملات سیبیل از اعتماد آگاه از اطمینان با درنظرگرفتن عامل زمان استفاده می‌کند. در این مدل از اعتماد غیرمستقیم که برگرفته از توصیه‌های دریافتی از همسایه‌ها و وزن‌دهی به این توصیه‌ها است، استفاده شده و الگوریتم پیشنهادی توسط شبیه‌ساز متلب پیاده‌سازی شده است. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی برتری قابل توجهی از نظر دقت تشخیص و نرخ هشدارهای اشتباه دارد. میانگین نرخ تشخیص و تشخیص غلط مدل پیشنهادی به ترتیب ۹۳ ٪ و ۰/۲۶ ٪ است.

واژگان کلیدی: شبکه‌های حس‌گر بی‌سیم، حملات سیبیل، اطیمنان و اعتماد آگاه از اطمینان

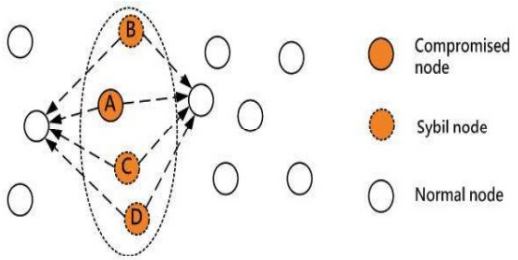
۱- مقدمه

یک شبکه حس‌گر بی‌سیم در مقیاس بزرگ، از هزاران گره حس‌گرها تشکیل شده و ممکن است در یک محیط پهناوری پراکنده شده باشد. گره‌های حس‌گر، کوچک و دارای توانایی محدود در محاسبات هستند که ارتباطات آن‌ها توسط باطری تغذیه می‌شوند. این گره‌های حس‌گر کوچک، مستعد انواع مختلفی از حملات هستند. برای یک شبکه حس‌گر با مقیاس بزرگ، نظارت و محافظت از هر گره حس‌گر از حملات فیزیکی یا منطقی، عملی نیست. حملات در شبکه‌های حس‌گر بی‌سیم به حملات بر روی لایه‌های فیزیکی، ارتباطات (کنترل دسترسی به رسانه یا واسط)، شبکه انتقال یا لایه کاربرد می‌توانند طبقه‌بندی شوند. شبکه‌های حس‌گر، باانگیزه استفاده در کاربردهای نظامی مانند نظارت بر میدان جنگ توسعه پیدا کردند؛ اما امروزه کاربردهای متنوعی در بخش‌های صنعتی و بهداشتی 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 در محیط عملیاتی موردنظر پراکنده می‌شوند و به‌طورمعمول پس از گسترش گره‌ها در محیط و یا پایان مأموریت، امکان جمع‌آوری و استفاده مجدد از گره‌ها نیست. شبکه حس‌گر بی‌سیم متشکل از عناصر ارتباطی،

*نویسندهٔ مسؤول

محاسباتی و حس‌گرها است که اهداف اصلی آن قابلیت اطمینان، دقت، انعطاف‌پذیری، اثربخشی هزینه‌ها و سهولت استقرار است [1]. محدودیت‌های بسیاری ازنظر ظرفیت حافظه، توان محاسباتی، برد رادیویی و میزان انرژی، متوجه گره‌های حس‌گر خواهد بود [2] [3] [4] [5]. با توجه به این محدودیت‌ها و گسترش بدون مراقبت گره‌های حس‌گر و نیز 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 .[6]

حملات سیبیل به‌راحتی قابل پیاده‌سازی در شبکه‌های حس‌گر بی‌سیم هستند، چون گره‌های حس‌گر در یک محیط توزیع‌شده قرارگرفته 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، به‌دلیل اینکه برخی گره‌ها جعلی هستند و به اطلاعات به‌دست‌آمده از آن‌ها نمی‌توان اعتماد کرد، کارایی خود را از دست می‌دهند [7] [8].در چنین حملاتی، مهاجم یک گره بدخواه در شبکه درج می‌کند و یا یک گره نرمال را در شبکه ضبط و آن را برنامه‌ریزی مجدد کرده (شکل۱) و تحت عنوان گره بدخواه در شبکه درج می‌کند [9].



(شکل-۱): حمله سیبیل

گره مخرب چندین هویت جعلی برای خود ایجاد می‌کند. گره‌های نرمال در همسایگی گره بدخواه فریب‌خورده و 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].

حملات سیبیل به دو دسته تقسیم می‌شوند؛ حملات سیبیل مستقیم که گره‌های سیبیل به‌طور مستقیم با گره‌های مجاز ارتباط برقرار می‌کنند و حملات سیبیل غیر مستقیم که گره‌های مجاز قادر به ارتباط مستقیم با گره‌های سیبیل نیستند و ارتباط آنها از طریق گره‌های بدخواه است.

در روش‌های 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، همه‌چیز در اختیارش قرار می‌گیرد. در یک شبکه 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. با درنظرگرفتن امنیت نرم عملکرد عامل‌ها را می‌توان تحت نظر قرار داده و برای هر عامل میزان سطح قابل‌اعتمادبودن[1] تعیین کرد و با این روش گره‌های مخرب و بدخواه را شناسایی کرد. سامانه‌های مدیریت اعتماد یکی از راه‌کاری‌های امنیت نرم است که در آن هر فرد قبل از برقراری ارتباط با فرد ناشناس، ابتدا میزان قابل‌اعتمادبودن آن را ارزیابی می‌کند.[13] هر موجودیت با بررسی سوابق تعاملاتی که با موجودیت مقصد دارد، میزان اعتماد به او را محاسبه می‌کند و همچنین برای به‌دست‌آوردن اعتمادی با ضریب اطمینان بالاتر از موجودیت‌هایی که سابقاً با موجودیت مقصد تعامل داشته‌اند، پیشنهادهایی را می‌تواند دریافت کند و این پیشنهادها را در محاسبه اعتماد تأثیر دهند.

هدف از این مقاله تشخیص حمله سیبیل غیرمستقیم با استفاده از اعتماد آگاه از اطمینان است که با استفاده از اعتماد توصیه‌ای حملات سیبیل غیرمستقیم را تشخیص داده و نرخ هشدارهای اشتباه را به میزان قابل توجهی کاهش خواهد داد. بقیه مقاله بدین صورت سازماندهی می‌شود. در بخش۲ مروری برکارهای گذشته و سازوکارهای دفاعی در برابر این حمله شرح داده می‌شود. مدل پیشنهادی به‌منظور تشخیص حمله سیبیل غیرمستقیم در شبکه‌های حس‌گر بی‌سیم با استفاده از اعتماد آگاه از اطمینان در بخش ۳ و در بخش۴ ارزیابی مدل پیشنهادی ارائه و در بخش۵ نتیجه‌گیری مطرح می‌شود.

۲- کارهای مرتبط

حمله سیبیل نخستین بار در شبکه‌های نظیربه‌نظیر مطرح شد. دوسر[2] ادعا کرد در چنین محیط‌های محاسباتی توزیع‌شده‌ای، یک دستگاه به‌راحتی چندین هویت (شناسه) می‌تواند اختیار کند که این به‌دلیل فقدان یک قدرت مرکزی و مورد اعتماد در شبکه است [14]. روش‌ها و سازوکارهای

[1] trustworthy

[2] Douceur

دفاعی زیادی برای تشخیص حمله سیبیل ارائه شده است که به سه دسته‌بندی کلی، تقسیم شده‌اند.

۲-۱- روش‌های مبتنی بر اطلاعات دریافتی از گره‌ها

دستهٔ نخست هویت گره‌ها را با استفاده از تجزیه‌وتحلیل اطلاعات گره‌های همسایه، بررسی و بازبینی می‌کنند [15]. سو[1] 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 گرهٔ مخرب تعداد زیادی هویت جعلی ایجاد می‌کند، استفاده می‌کند تا سازوکاری برای حفاظت از شبکه‌های حس‌گر بی‌سیم در برابر حملات سیبیل ارائه دهند [16].

۲-۲- روش های مبتنی بر تشـــخیص هو یت (شناسه)

دسته دوم به‌طورکلی، حملات سیبیل را با محدودکردن تولید اطلاعات گره‌های معتبر کاهش می‌دهد. در بیش‌تر 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 [17] [18].کارلوف و واگنر[2] (۲۰۰۳) در مورد مزایای نسبی روش‌های رمزنگاری متقارن و غیرمتقارن برای حفاظت از شبکه‌های حس‌گر بی‌سیم در برابر حملات سیبیل صحبت کرده‌اند. آن‌ها بیان کردند که شبکه‌های حس‌گر بی‌سیم به‌دلیل این‌که دارای محیط توزیع‌شده و غیرقابل اطمینانی هستند، مستعد قرارگرفتن در معرض حملات سیبیل می‌باشند به‌منظور دفاع در برابر این حمله نیز استفاده از کلیدهای رمزنگاری و سازوکار احراز هویت گره‌ها را پیشنهاد داده‌اند که به‌دلیل محدودیت گره‌های حس‌گر در منابع ذخیره‌سازی و محاسباتی، روش مناسبی نیست. از جهتی دیگر استفاده از کلیدهای رمزنگاری، همیشه نمی‌تواند باعث تشخیص و جلوگیری از حمله سیبیل شود [19]. چینگ[3] و همکاران (۲۰۱۳) یک روش مبتنی برای زنجیره کلید پیش‌توزیع‌شده در برابر حمله سیبیل ارائه کردند. در این روش از چندین زنجیرهٔ کلید استفاده و از هش اطلاعات هویتی یکتا برای هرگره پشت سرهم در ایستگاه پایه مورد اعتماد استفاده می‌شد که درنهایت یک استخری از زنجیره کلیدها ایجاد و سپس از طریق پروتکل CK-AE گره‌های همسایه به همراه مابقی گره ها احراز هویت می‌شدند و یک جفت کلید منحصربه‌مفرد برای محافظت از جعل کلیدها توسط مهاجمان سیبیل ایجاد می‌شد [20].

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

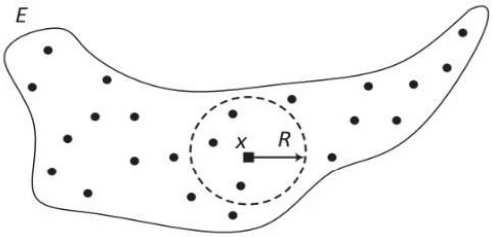
دسته سوم از این واقعیت که هر گره در هر زمان در یک موقعیت (مکان فیزیکی) می‌تواند قرار گیرد، برای تشخیص حمله سیبیل بهره می‌گیرد. این روش وابسته به تأیید مکان است؛ محل موردنظر برای هر تعیین‌کننده هویت با استفاده از اندازه‌گیری فاصله و مثلث‌بندی(زاویه‌بندی) بررسی می‌شود. دیمرباس[4] و همکاران (۲۰۰۶) یک رویکرد مبتنی بر شاخص قدرت سیگنال دریافتی (*RSSI*)[5] 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 به‌وسیله بررسی قدرت سیگنال دریافتی تخمین زده می‌شود. اگر یک گروه از هویت‌ها (شناسه‌ها) در همان منطقه مستقر شونـد[21]، آشکارسازها یک گره را به‌عنوان مهاجم سیبیل در نظر می‌گیرند.

استفاده از *RSSI* به‌واسطه ماهیت متغیر و غیرقابل‌اعتماد آن برای این منظور پاسخ‌گو نیست. از آن‌جایی‌که *RSSI* تابعی از توان ارسالی است و توان‌های متفاوت منجر به شاخص‌های قدرت سیگنال دریافتی متفاوت می‌شوند، لذا گره‌ها در شبکه‌های حس‌گر به‌راحتی توان ارسالی خود را می‌توانند تغییر و درنتیجه گیرنده را فریب دهند. استفاده از نسبت *RSSI* نخستین بار توسط سونگ[6] و همکاران برای تشخیص مکان فرستنده با استفاده از چهار گرهٔ ناظر مطرح شد [22] 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

[1] Ssu
[2] Karlof, C & ,.Wagner
[3] Cheng
[4] Demirbas
[5] Received Signal Strength Indicator
[6] zhong

فرستنده محاسبه‌شده و در صورت تشابه، تشخیص حمله سیبیل اعلام می‌شود. ساریکیانیدیس و همکاران (۲۰۱۵) یک روش مبتنی بر قانون[1] براساس تشخیص به‌صورت ناهنجاری برای تشخیص حملات سیبیل ارائه‌کردند [23].

در این روش احتمال ناحیه هم‌زیستی(که 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 (شکل۲) مستقر شده‌اند.



(شکل-۲): میدان شبکه حس‌گر [23]

در RADS[2] از چهار مرحله برای تشخیص حملات سیبیل در شبکه‌های حس‌گر بی‌سیم استفاده می‌کند.

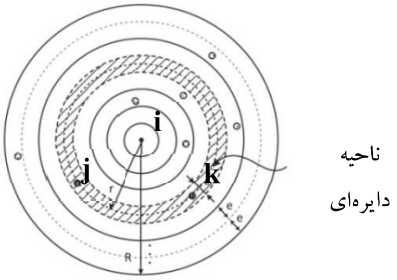
مرحله نخست، مرحلهٔ کشف همسایه است. کشف همسایه شامل تبادل بسته‌های*hello* بین گره‌های همسایه است. در مرحله دوم، هر گره یک جدول که حاوی تخمین محدوده محاسبه‌شده است، به‌طور محلی ایجاد می‌کند. یعنی فاصله d_{ij}^{e} از هر گره همسایه تشخیص داده می‌شود. نماد d_{ij}^{e} تخمین فاصله بین گره n_i و n_j است که با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

به‌وسیله d_{ij}^{a} فاصله واقعی بین گره n_i و n_j علامت‌گذاری می‌شود که به شرح ذیل 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 به‌تنهای در شبکه، به‌طور مستقل بررسی فاصله را چندین بار انجام می‌دهد(شکل۳).

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 مرحله کشف همسایگان را برای همسایگان جدید در مجاورتش جستجو می‌کند، وابسته است.



(شکل-۳): نحوه تشخیص گره سیبیل(Sarigiannidis, et al., 2015)

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

روش ساریکیانیدیس و همکاران (۲۰۱۵) جزء روش تشخیص مبتنی بر مکان و براساس رویکرد امنیت سخت عمل می‌کند. روش پیشنهادی یک محیط شبیه‌سازی دقیق به‌منظور بررسی و تأیید تجزیه و تحلیل ارائه کرده که نشان می‌دهد سامانهٔ تشخیص پیشنهادی در برابر حملات سیبیل اثر بخش بوده است. به‌طورکلی ویژگی‌های سامانه‌های تشخیص با روش‌های موجود مقایسه شده که در جدول (۱) نشان داده شده است .

۳- توصیف مدل پیشنهادی

به‌منظور تشخیص حملات سیبیل غیرمستقیم، گره‌های بدخواه، کاهش نرخ هشدارهای اشتباه و نظارت بر عملکرد گره‌ها در طول مدت فعالیت‌شان، از یک پروتکل با رویکرد اعتماد آگاه از اطمینان به شرح زیر استفاده می‌کنیم. ساختار کلی مدل پیشنهادی در شکل (۴) آمده است.

در یک شبکهٔ اعتماد اگر A به B و B به C اعتماد مستقیم داشته باشد، آن‌گاه A به C اعتماد غیرمستقیم خواهد داشت(شکل۵).

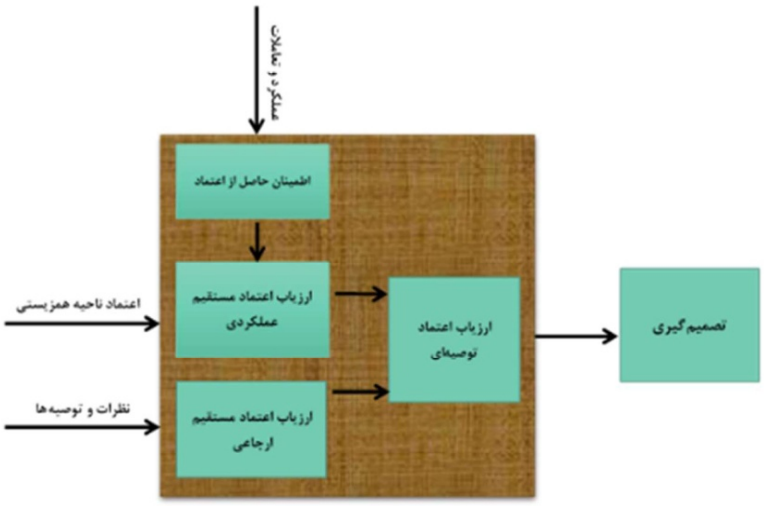
برای محاسبه اعتماد غیرمستقیم در یک زنجیرهٔ اعتماد، لازم است که فرد ماقبل مقصد، نسبت به مقصد اعتماد عملکردی و بقیهٔ افراد زنجیره، نسبت به فرد بعد از خود، اعتماد ارجاعی داشته باشند(شکل۶).

[1] Rule-based

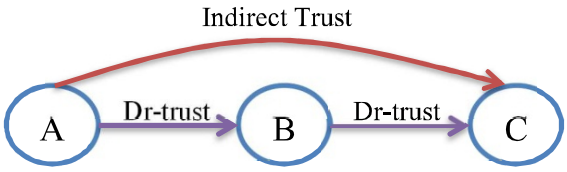
[2] Rule-based anomaly detection system

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

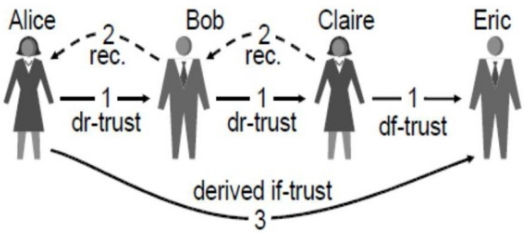
Citation	Lightweight?	Authentication based method?	Location information?	Specialized h/w?	Comm. Mode	Identity type	Operation	Approch
(this paper)	✓	×	✓	×	**Both**	**Both**	**Distributed**	**Hard & Soft Security**
Douceur (2002)	×	✓	×	×	Direct	Fabricated	Centralized	**Hard-Security**
Karlof and Wagner (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**



(شکل-۴): ساختار کلی روش پیشنهادی



(شکل-۵): شبکه اعتماد



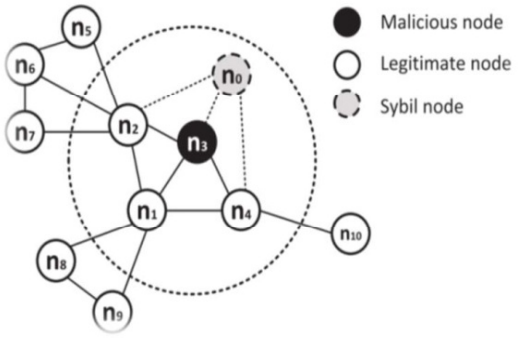
(شکل-۶): اعتماد عملکردی و ارجاعی در انتشار اعتماد

در این مدل، باتوجه به اینکه گره مجاز به‌طورمستقیم با گره سیبیل در ارتباط نیست، ابتداد اعتماد مستقیم عملکردی بر اساس اعتماد ناحیه هم‌زیستی و اطمینان حاصل از اعتماد محاسبه شده، سپس اعتماد مستقیم ارجاعی براساس میزان اعتماد به درستی توصیه‌ها، محاسبه می‌شود. درنهایت اعتماد توصیه‌ای با درنظرگرفتن این دو مقدار اعتماد به‌دست می‌آید.

۱-۳- قابلیت تشخیص حملات سیبیل غیرمستقیم در مدل پیشنهادی

هر گره از یک جدول که حاوی تعدادی تعاملات موفق و ناموفق در هر دوره و میزان اعتماد ناحیهٔ هم‌زیستی محاسبه‌شده برای گره‌های همسایه است استفاده می‌کند.

شکل (۷) حمله سیبیل غیرمستقیم را برای گره n_1 نشان می‌دهد.



(شکل-۷): حمله سیبیل غیرمستقیم

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 (۱) و (۲) در محاسبه میزان باور و

عدم باور استفاده می‌شود:

$$W_i = e^{-\lambda \Delta T_i} \qquad (۱)$$
$$\Delta T_i = T_{Current} - T_i$$

λ ضریب میرایی اعتماد است که مشخص می‌کند که از چه زمان قبل‌تر تعاملات تأثیر نداشته باشد W_i وزن تعاملات را مشخص می‌کند. درصورتی‌که از زمان تعاملات (نسبت به زمان جاری) زمان زیادی گذشته باشد، مقدار $e^{-\lambda \Delta T_i}$ و درنتیجه W_i به صفر نزدیک می‌شود:

$$s = \sum_{x_i \in ST} W_i \qquad (۲)$$
$$f = \sum_{x_i \in FT} W_i$$

ST مجموعه تعاملات موفق و FT مجموعه تعاملات ناموفق می‌باشد؛ بنابراین برای محاسبه تعاملات موفق و ناموفق، تعامل را با درنظرگرفتن ΔT به S و F اضافه می‌کنیم. برای مثال با فرض $\lambda = 1$ دو تعامل موفق که ΔT آنها به‌ترتیب 0 و 2 است، S به شکل زیر محاسبه می‌شود:

$$S = e^0 + e^{-2}$$

با توجه به اینکه هر گره دارای جدول همسایگی می‌باشد که در آن تعداد تعاملات موفق و ناموفق در هر دوره نسبت به همسایگانی که به‌طورمستقیم با آن‌ها در ارتباط هستند، ثبت‌شده است، به‌منظور تشخیص گره سیبیل در این روش نظر گره‌های دیگر را که به‌طور مستقیم با گره مقصد در ارتباط هستند، (CT) بررسی می‌شود. گره مبدأ میزان اعتماد مستقیم ارجاعی نسبت به توصیه‌های دریافتی از گره های همسایه را محاسبه کرده (RT) ، با درنظرگرفتن این دو مقدار اعتماد، اعتماد توصیه‌ای طبق ویژگی‌های انتشار اعتماد محاسبه شده و درصورتی‌که کمتر از مقدار آستانه باشد، آن گره را به‌عنوان گره سیبیل تشخیص می‌دهیم.

همان‌طورکه در جدول (۲) نشان داده شده است، دورهٔ در نظر گرفته‌شده برای تعاملات موفق و ناموفق به‌صورت اسلات‌های زمانی (T) در نظر گرفته شده که هر کدام دارای یک برچسب زمانی هستند.

جدول (۲) اعتماد مستقیم گره n_2 برای توپولوژی شبکه درشکل (۷) نشان می‌دهد.

(جدول-۲): اعتماد مستقیم گره n_2

Trust Direct of node n_2						
	n_0	n_1	n_3	n_5	n_6	$\boldsymbol{n_7}$
	$S_{n_{20}}, F_{n_{20}}, T_{n_{20}}$	$S_{n_{21}}, F_{n_{21}}, T_{n_{21}}$	$S_{n_{23}}, F_{n_{23}}, T_{n_{21}}$	$S_{n_{25}}, F_{n_{25}}, T_{n_{25}}$	$S_{n_{26}}, F_{n_{26}}, T_{n_{26}}$	$\boldsymbol{S_{n_{27}}, F_{n_{27}}, T_{n_2}}$
CT_{n_2}	$CT_{n_{20}}$	$CT_{n_{21}}$	$CT_{n_{23}}$	$CT_{n_{25}}$	$CT_{n_{26}}$	$\boldsymbol{T_{Fn_{27}}}$

اعتماد ناحیه همزیستی مطابق رابطه (۳) تعیین می‌شود:

$$T = 1 - e^{-\left|\left|d_{ij}^e - d_{ik}^e\right| - \alpha\right|} \qquad (۳)$$

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 می‌باشد. در صورتی که 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 می‌گردد در نتیجه مقدار اعتماد ناحیه همزیستی (T) به صفر میل خواهد کرد.

برای محاسبه اطمینان حاصل از اعتماد مقدار اعتماد بر اساس منطق ذهنی[1] جوسانگ [24] محاسبه می‌شود. میزان باور، عدم باور و عدم قطعیت بر اساس این تعاملات طبق رابطه (۴) تعیین می‌شود:

$$b = \frac{s}{s+f+1}\ ,\ d = \frac{f}{s+f+1}\ ,\ u = \frac{1}{s+f+1} \qquad (۴)$$

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

[1] Subjective Logic

مقدار اعتماد طبق رابطه (۵) محاسبه می‌شود:

$$T_C = \frac{b}{1-u} \qquad (۵)$$

درصورتی‌که عدم قطعیت صفر باشد، آن‌گاه مقدار اعتماد برابر با میزان باور خواهد بود. به‌منظور محاسبه دقیق‌تر مقدار اعتماد از یک مشخصهٔ دیگری به نام اطمینان[1] استفاده می‌کنیم. میزان اطمینان به یک تخمین اعتماد مبنای تعیین وزن این تخمین در ترکیب نظرات اعتماد می‌تواند باشد. همچنین اطمینان به‌عنوان مشخصه‌ای می‌تواند در نظر گرفته شود که بعد دیگری به خروجی مدل اعتماد اضافه می‌کند. میزان اطمینان درک غنی‌تری از اعتماد و درنهایت تصمیم‌گیری بهتری برای چگونگی واکنش به ما می‌دهد [25] که در رابطه (۶) نشان داده شده است:

$$C = 1 - u \qquad (۶)$$

برای محاسبه اعتماد مستقیم عملکردی (CT) برآیند اعتماد ناحیه همزیستی واطمینان حاصل از اعتماد محاسبه شده و در جدول همسایگی ثبت می‌شود:

برای محاسبه اعتمادتوصیه‌ای(غیرمستقیم)، اعتماد مستقیم ارجاعی (RT) را در همان جدول همسایگی، (نظر گره مبدأ نسبت به توصیه ای دریافتی از گره واسط) درج می‌شود.

جدول (۳) اعتماد مستقیم و غیرمستقیم گره n_1 را برای توپولوژی شبکه در شکل (۶) نشان می‌دهد.

(جدول-۳): اعتماد مستقیم و غیرمستقیم گره n_1

	n_2	n_3	n_4	n_8	n_9
	$S_{n_{12}}, F_{n_{12}}, T_{n_{12}}$	$S_{n_{13}}, F_{n_{13}}, T_{n_{13}}$	$S_{n_{14}}, F_{n_{14}}, T_{n_{14}}$	$S_{n_{18}}, F_{n_{18}}, T_{n_{18}}$	$\boldsymbol{S_{n_{19}}, F_{n_{19}}, T_{n_{19}}}$
CT_{n_1}	$CT_{n_{12}}$	$CT_{n_{13}}$	$CT_{n_{14}}$	$CT_{n_{18}}$	$\boldsymbol{CT_{n_{19}}}$
RT_{n_1}, RC_{n_1}	$RT_{n_{12}}, RC_{n_{12}}$	$RT_{n_{13}}, RC_{n_{13}}$	$RT_{n_{14}}, RC_{n_{14}}$	$RT_{n_{18}}, RC_{n_{18}}$	$\boldsymbol{RT_{n_{19}}, RC_{n_{19}}}$

محاسبهٔ اعتماد غیرمستقیم بر مبنای توصیه دیگران انتشار اعتماد[2] نامیده می‌شود. اگر در شبکه اعتماد بین فرد مبدأ با فرد مقصد یک مسیر شامل چند واسطه وجود داشته باشد، این مسیر را به‌عنوان یک زنجیره اعتماد می‌توان در نظر گرفت و با به‌کارگیری خاصیت تعدی اعتماد به‌صورت ضرب مکرر، میزان اعتماد غیرمستقیم مبدأ به مقصد را محاسبه کرد؛

بنابراین زنجیره‌های اعتماد[3] به گره مقصد تشکیل شده و انتشار اعتماد آگاه از اطمینان طبق رابطه (۷) محاسبه می‌شود:

$$(T_{ind}, C_{ind}) = (T_1, C_1) \otimes (T_2, C_2) \otimes (T_3, C_3) \qquad (۷)$$

عملگر $\otimes$ انتشار اعتماد را نشان می‌دهد.

اگر مقدار اعتماد A به B برابر با $T_{A,B}$ و مقدار اعتماد B به C برابر با $T_{B,C}$ باشد، اعتماد غیرمستقیم A به C به‌صورت زیر تخمین زده می‌شود:

$$T_{A,C} = T_{A,B}.T_{B,C}$$

در یک شبکه اعتماد اگر بین v_1 (گره مبدأ) و v_n (گره مقصد) یک مسیر $v_1 v_2 \dots v_n$ وجود داشته باشد، با ضرب مکرر مقادیر برچسب یال‌ها مقدار اعتماد v_1 به v_n به‌صورت غیرمستقیم طبق رابطه (۸) تخمین زده می‌شود:

$$T_{1,n} = RT_{1,2}.RT_{2,3} \dots .RT_{n-2,n-1}.CT_{n-1,n} = \left(\prod_{i=1}^{n-2} RT_{i,i+1}\right).CT_{n-1,n} \qquad (۸)$$

RT اعتماد ارجاعی، CT اعتماد عملکردی و $T_{1,n}$ مقدار اعتماد عملکردی غیرمستقیم است.

با توجه به اینکه ممکن است در یک شبکه اعتماد بیش از یک زنجیره اعتماد از مبدأ به مقصد وجود داشته باشد، در چنین شرایطی مقدار اعتماد غیرمستقیم باید با ترکیب یا تعیین برآیند نتایج انتشار اعتماد در کلیه این زنجیره‌ها به‌صورت مناسب به‌دست آید. این ترکیب به‌اصطلاح تجمیع اعتماد[4] خوانده می‌شود.

نتایج برآیند کلیه زنجیره‌های انتشار اعتماد آگاه از اطمینان طبق رابطه (۹) تعیین می‌شود:

[1] Confidence
[2] Published trust
[3] Web Of Trust
[4] Trust aggregation

(۱۲)

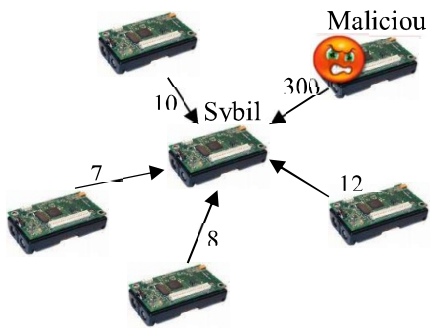
$$(T_{Tind},\ C_{Tind}) = (T_{t1},\ C_{t1}) \oplus (T_{t2},\ C_{t2}) \oplus (T_{t3},\ C_{t3})$$

عملگر $\oplus$ تجمیع اعتماد را نشان می‌دهد.

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

۲-۳-قابلیت تشخیص گره مخرب در مدل پیشنهادی

برای تشخیص گره‌های مخرب در این روش با توجه به اینکه گره‌های بدخواه، تعداد تعاملات موفق و ناموفق را برای گره سیبیل و مجاز به نادرست ثبت می‌کنند، لذا با استفاده از سازوکار رأی‌گیری به‌صورت میانگین‌گیری و نظر گره‌های دیگر نسبت به گره مقصد گره مخرب را می‌توان شناسایی کرد.



(شکل-۷): تشخیص گره مخرب در مدل پیشنهادی

۴- ارزیابی مدل پیشنهادی

مدل پیشنهادی در نرم‌افزار متلب شبیه‌سازی شده 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 (۴) مشخصه‌های مورداستفاده در شبیه‌سازی را نشان می‌دهد. مقدار هر یک از مشخصه‌ها در این جدول آورده شده است. برای تشخیص حملات سیبیل غیرمستقیم و گره مخرب مقادیر TP[1]، FP[2]، FN[3]، Recall و Precision را به‌دست می‌آوریم که در ادامه توضیح داده شده است. همچنین به‌منظور دقت بیشتر، الگوریتم را یکصد بار اجرا کرده و میانگین آن را به‌عنوان نتیجه ارائه می‌کنیم.

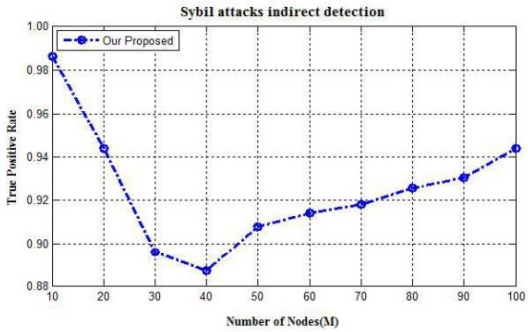
[1] True Positive
[2] False Positive
[3] False Negative

(جدول-۴): 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
RT_t	0.62	مقدار آستانه برای اعتماد در اعتماد توصیه‌ای
RC_t	0.88	مقدار آستانه برای اطمینان در اعتماد توصیه‌ای
S	--	تعداد تعاملات موفق
F	--	تعداد تعاملات ناموفق

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

نمودار شکل (۹) نرخ TP در تشخیص حملات سیبیل غیرمستقیم را با استفاده از اعتماد توصیه‌ای، نشان می‌دهد.که تعداد گره‌ها از ۱۰ تا ۱۰۰ تغییر می‌یابد.



(شکل-۹): نرخ TP در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

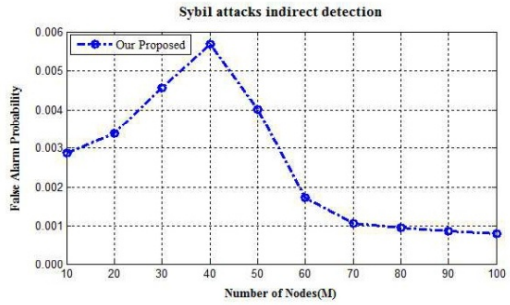
همان‌طور که در نمودار شکل (۹) و جدول (۵) نشان داده‌شده است، مقدار TP در ابتدا با افزایش تعداد گره‌ها کاهش می‌یابد. با توجه به ثابت‌بودن مساحتی که گره‌ها در آن توزیع شده‌اند ($E=100m^2$) و از طرفی هر گره می بایست در شعاع حسی گره دیگر قرار بگیرد، و همچنین به جهت پوشش بیشتر ناحیه، تعداد همسایگانی که در جدول همسایگی هر گره قرار می‌گیرد کمترمی‌شود؛ لذا تعداد نظرات کمتری در مورد گره مقصد وجود خواهد داشت، که باعث می‌شود نرخ TP کاهش یابد. زمانی که تعداد گره‌ها از چهل تا بیشتر

می‌شود 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 که باعث می‌شود نرخ TP افزایش یابد. این نشان می‌دهد، روش پیشنهادی با افزایش تعداد گره‌ها نه‌تنها دقت آن کاهش نیافته بلکه تعداد حملات بیشتری را تشخیص خواهد داد.

(جدول-۵): نرخ *TP* در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

Number of nodes	10	20	30	40	50	60	70	80	90	100
TPR (%)	0.9864	0.9437	0.8959	0.8873	0.9076	0.9142	0.9182	0.9257	0.9305	0.9439

نمودار شکل (۱۰) نرخ FP در تشخیص حملات سیبیل غیرمستقیم را با استفاده از اعتماد توصیه‌ای نشان می‌دهد.



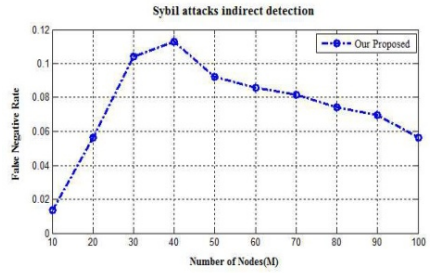
(شکل-۱۰): نرخ FP در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

همان‌طور که در نمودار شکل (۱۰) و جدول (۶) نشان داده شده است 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. با توجه به ثابت‌بودن مساحتی که گره‌ها در آن توزیع شده‌اند، ($E=100m^2$) و از طرفی هر گره می بایست در شعاع حسی گره دیگر قرار بگیرد و همچنین به جهت پوشش بیشتر ناحیه، تعداد همسایگانی که در جدول همسایگی هر گره قرار می‌گیرد، کمترمی‌شود، درنتیجه تعداد نظرات کمتری در مورد گره مقصد وجود خواهد داشت. 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؛ لذا احتمال اشتباه، کاهش پیدا می‌کند.

(جدول-۶): نرخ *FP* در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

Number of nodes	10	20	30	40	50	60	70	80	90	100
FPR (%)	0.0029	0.0034	0.0046	0.0057	0.0040	0.0017	0.0011	0.0010	0.0009	0.0008

نمودار شکل (۱۱) نرخ FN در تشخیص حملات سیبیل غیرمستقیم را با استفاده از اعتماد توصیه‌ای نشان می‌دهد.



(شکل-۱۱): نرخ FN در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

همان‌طور که در نمودار شکل (۱۱) و جدول (۷) نشان داده شده است، نرخ FN با افزایش تعداد گره‌ها افزایش می‌یابد. با توجه به ثبات‌بودن مساحتی که گره‌ها در آن توزیع شده‌اند، ($E=100m^2$) و تراکم کم گره‌ها، درنتیجه تعداد همسایگانی کمتری در جدول همسایگی هر گره قرار می‌گیرد؛ لذا زمانی که تعداد گره‌ها کمتر از چهل است نرخ FN افزایش و زمانی که تعداد گره‌ها از چهل گره بیشتر می‌شود، نرخ FN کاهش می‌یابد.

نمودار شکل (۱۲) به‌عنوان نمودار Recall، نسبت حملاتی که به‌درستی تشخیص داده‌شده(TP) به‌کل حملات (هم حملاتی که به‌درستی تشخیص دادیم و هم حملاتی را

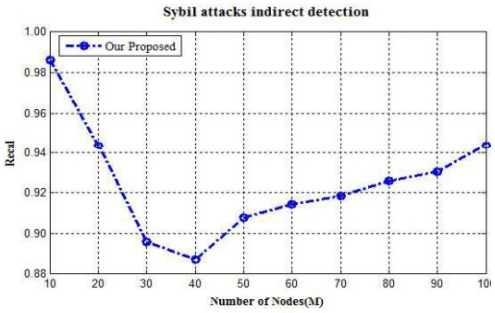
(جدول-۷): نرخ FN در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای

Number of nodes	10	20	30	40	50	60	70	80	90	100
FNR (%)	0.0136	0.0563	0.1041	0.1127	0.0924	0.0858	0.0818	0.0743	0.0695	0.0561

که تشخیص داده نشده است($TP+FN$)) با استفاده از اعتماد توصیه‌ای نشان می‌دهد.

Recall به‌عنوان نرخ Sensitivity در نظر گرفته که طبق رابطه (۹) محاسبه می‌شود:

$$Recall = \frac{TP}{TP+} \quad (۹)$$



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

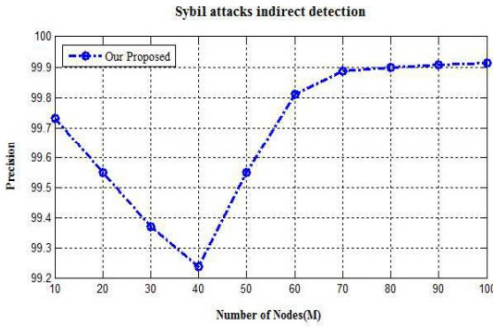
زمانی که تعداد گره‌ها از چهل گره بیشتر می‌شود با توجه به اینکه تعداد نظرات بیشتری در مورد گره مقصد وجود دارد، تعداد حملات بیشتری تشخیص داده می‌شود و نمودار Recall با افزایش گره‌ها رو به افزایش خواهد بود.

نمودار شکل (۱۳) به‌عنوان نمودار Precision، نسبت حملاتی که به‌درستی تشخیص داده‌شده(TP) به‌کل تشخیص (هم حملاتی که به‌درستی تشخیص دادیم و هم آن‌هایی را که حمله نبود و به‌اشتباه حمله تشخیص دادیم($TP+FP$)) با استفاده از اعتماد توصیه‌ای، نشان می‌دهد.

Precision دقت مدل پیشنهادی را نشان می‌دهد که طبق رابطه (۱۰) محاسبه می‌شود:

$$Precision = \frac{TP}{TP + FP} \quad (۱۰)$$

زمانی که تعداد گره‌ها به یکصد افزایش می‌یابد، دقت تشخیص روش پیشنهادی 99.92 درصد است.

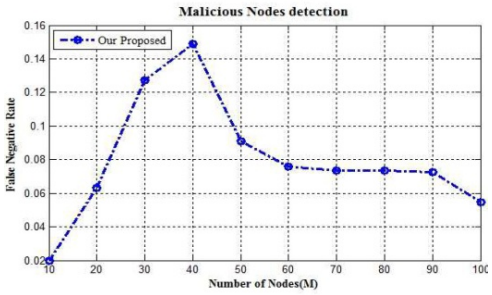


(شکل-۱۳): نسبت حملاتی که به‌درستی تشخیص داده‌شده به‌کل تشخیص (Precision) با استفاده از اعتماد توصیه‌ای

۴-۲- نتایج حاصل از آزمایش‌ها در تشخیص گره‌های مخرب

برای تشخیص گره‌های مخرب در این روش با توجه به اینکه این گره‌ها تعداد تعاملات موفق و ناموفق را برای گره سیبیل و مجاز به نادرست ثبت می‌کنند، لذا با استفاده از سازوکار رأی‌گیری به‌صورت میانگین‌گیری و نظر گره‌های دیگر نسبت به گره مقصد گره مخرب می‌تواند شناسایی شود.

نمودار شکل (۱۴) نرخ FN را در تشخیص گره‌های مخرب با استفاده از اعتماد توصیه‌ای، به‌عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.



(شکل-۱۴): تشخیص گره‌های مخرب با استفاده از اعتماد توصیه‌ای

همان‌طورکه نشان داده شده است، نرخ FN در ابتدا با افزایش تعداد گره‌ها افزایش می‌یابد. نرخ FN با تراکم گره‌ها رابطه معکوس دارد. زمانی که تعداد گره‌ها افزایش می‌یابد تعداد همسایگان، در جدول همسایگی گره بیشتر می‌شود و تعداد نظرات در مورد گره مقصد افزایش می‌یابد؛ که این باعث دقت بیشتر شده و درنتیجه نرخ FN در تشخیص گره‌های مخرب کاهش می‌یابد.

۵- نتیجه‌گیری

روش‌های مختلف ارائه‌شده برای تشخیص حملات سیبیل بر اساس رویکرد امنیت سخت است. سازوکارهای مبتنی بر امنیت سخت برای حفظ امنیت سامانه‌های اطلاعاتی به‌خصوص در جوامع باز، کافی نیستند. در سال‌های اخیر رویکردی جدیدی از امنیت به نام امنیت نرم موردتوجه واقع‌شده است که در آن به‌جای یک نهاد مرکزی، افراد مسئول امنیت خود هستند. سامانه‌های مدیریت اعتماد نمونه‌ای از راهکارهای مبتنی بر امنیت نرم هستند.

در روش پیشنهادی از مقدار اعتماد هر گره استفاده شد و مقدار اعتماد مستقیم عملکردی و اعتماد مستقیم ارجاعی که برگرفته از توصیه‌های دریافتی از همسایه‌ها و

وزن‌دهی به این توصیه‌ها است، استفاده شد با ترکیب مقادیر اعتماد مستقیم عملکردی و اعتماد مستقیم ارجاعی و تعیین وزنی برای این دو مقدار اعتماد، حملات سیبیل

غیرمستقیم را تشخیص داده شد و از طرفی نرخ هشدارهای اشتباه کاهش یافت.

با توجه به نتایج آزمایش‌های ارائه‌شده، مدل پیشنهادی امکان تشخیص حملات سیبیل غیرمستقیم را فراهم کرده و از طرفی باعث افزایش دقت و کاهش نرخ هشدارهای اشتباه شده است. با درنظرگرفتن عامل زمان در تعاملات برای محاسبه اعتماد آگاه از اطمینان، یک سامانهٔ 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.

۶- مراجع

[1] A. C. Prabhjotkaur and S. Singh, "Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralizedids," International Journal of Engineering Science, vol. 8399, 2016.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] K. F. W. W. T. &. C. W. C. Ssu, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," Computer Networks, vol. 53(18), 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 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] A. Jøsang, "Trust Management in Online Communities," New Forms of Collaborative Innovation and Production on the Internet, p. 75, 2011.

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

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

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

[17] 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.

[18] 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.

[19] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, no. Elsevier, pp. 293-315, 2003.

[20] 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.

[21] K. F. Ssu, W. T. Wang and W. C. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," Computer Networks, vol. 53(18), pp. 3042-3056, 2009.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

سیدمحمد طباطبائی پارسا تحصیلات خود را در مقاطع کارشناسی و کارشناسی‌ارشد در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات به ترتیب از دانشگاه علمی وکاربردی مرکز علمی- صنعتی مشهد در سال ۱۳۹۳ و از دانشگاه بین‌المللی امام رضا(ع) در سال ۱۳۹۵ به پایان رسانده است. وی در تمامی مقاطع تحصیلی دانشجوی ممتاز بودند. زمینه‌های پژوهشی مورد علاقه ایشان مدیریت اعتماد، پنهان نگاری، رمزنگاری و امنیت شبکه است.

حسن شاکری مدارک کارشناسی، کارشناسی ارشد و دکترای خود را در رشته مهندسی کامپیوتر- نرم‌افزار به ترتیب 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 ایشان بیش از هفتاد مقاله علمی در کنفرانس‌ها و مجلات داخلی و بین‌المللی منتشر شده است. زمینه‌های پژوهشی مورد علاقه وی مدیریت اعتماد، امنیت شبکه‌ها، سامانه‌های رایانه‌ای و پردازش زبان‌های طبیعی است.