

تشخیص حملات سبیل در شبکه‌های حس‌گر

بی‌سیم با رویکرد مدیریت اعتماد

سید محمد طباطبائی‌پارسا^{۱*} و حسن شاکری^۲

^۱دانش‌آموخته کارشناسی ارشد مهندسی کامپیوتر، امنیت اطلاعات دانشگاه بین‌المللی امام رضا(ع)، مشهد، ایران
m.tabatabaei.parsa@imamreza.ac.ir

^۲استادیار گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، مشهد، ایران
shakeri@msdiau.ac.ir

چکیده

شبکه‌های حس‌گر بی‌سیم راه حل ایده‌آلی برای انواع گوناگونی از کاربردهای نظارت و مراقبت شامل کنترل ترافیک، نظارت بر محیط، نظارت بر میدان جنگ و غیره هستند. گرهای حس‌گر محدودیت‌هایی هم به لحاظ حافظه و هم قابلیت‌های محاسباتی دارند. حمله سبیل یک تهدید جدی برای این شبکه‌ها بهشمار می‌آید که در آن گره مخرب چندین هویت برای خود ایجاد کرده و گرهای شبکه را گمراه می‌کند. این حمله می‌تواند پروتکل‌های مسیریابی و عملیاتی نظری رأی‌گیری، تجمعیت داده‌ها ... را تحت تأثیر قرار دهد. در این مقاله یک الگوریتم پویا و سبک وزن با رویکرد اعتماد آگاه از اطمینان ارائه می‌شود. در رویکرد مورد استفاده از مقدار اعتماد هر گره به منظور کاهش نرخ هشدارهای اشتباه و تشخیص حملات سبیل غیرمستقیم در شبکه‌های حس‌گر بی‌سیم استفاده می‌شود. نتایج شبیه‌سازی نشان می‌دهد که میانگین نرخ تشخیص و تشخیص غلط به ترتیب 0.92% و 0.08% است.

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

شبکه‌های حس‌گر، با انگیزه استفاده در کاربردهای

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

۱- مقدمه

پیشرفت‌های اخیر در ساخت مدارات مجتمع در اندازه‌های کوچک، از یک سو و توسعه فناوری ارتباطات بی‌سیم از سوی دیگر زمینه‌ساز طراحی شبکه‌های حس‌گر بی‌سیم شده است. شبکه حس‌گر بهشت با محیط فیزیکی اطراف خود تعامل دارد و از طریق حس‌گرها اطلاعات محیط را گرفته و در صورت نیاز پس از اعمال پردازشی ساده، آن‌ها را ارسال می‌کند. ارتباط بین گرهای به صورت بی‌سیم برقرار می‌شود و هر کدام از آن‌ها به صورت مستقل و بدون دخالت انسان کار می‌کند و به طور معمول از لحاظ فیزیکی بسیار کوچک هستند. گرهای حس‌گر با همکاری یکدیگر امکان نظارت بر محیط را فراهم می‌آورند و برای اندازه‌گیری برخی از کمیت‌های فیزیکی یا شرایط محیطی به کار می‌روند.

* نویسنده عهده‌دار مکاتبات

هدف از این مقاله تشخیص حمله سیبیل با رویکرد امنیت نرم بوسیله 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 بخش ۲ کارهای گذشته و سازوکارهای دفاعی در برابر این حمله شرح داده می‌شود. در بخش ۳ مدل پیشنهادی جهت تشخیص حمله سیبیل در شبکه‌های حسگری سیم با رویکرد مدیریت اعتماد ارائه می‌شود. در بخش ۴ ارزیابی روش پیشنهادی و در بخش آخر نتیجه‌گیری و فرصت‌های پژوهشی در آینده مطرح می‌گردد.

۲- کارهای مرتبط

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

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

دسته نخست به طور کلی، حملات سیبیل را با محدود کردن تولید اطلاعات گره‌های معتبر کاهش می‌دهد. در اکثر روش‌های عمومی این دسته وابسته به تشخیص یک ID یا شناسه امن توسط یک سور مرکزی است. این دسته برای تشخیص حملات سیبیل از روش‌های احراز هویت و رمزگاری استفاده می‌کنند [13].

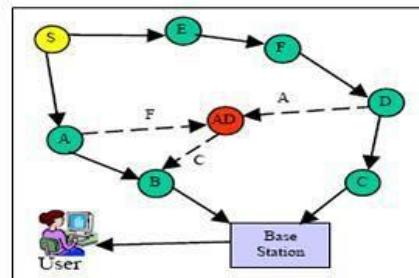
در سال ۲۰۰۴^۳ روش برای حفاظت از شبکه‌های حسگری سیم در برابر حملات سیبیل پیشنهاد داده‌اند که شامل یک سازوکار آزمایش منابع رادیویی (RRT)، موقعیت مورد تأیید و سازوکار ثبت گره و پیش‌توزیع تصادفی کلید است [14].

در [15] یک طرح مدیریت کلید به نام پروتکل تصدیق هویت و رمزگاری متمنکز (LEAP) برای حفاظت از شبکه‌های حسگری سیم در برابر حملات مختلف طراحی کرده‌اند. چهار نوع از کلیدها (فردي، گروهي، دوبهدو و کلیدهای کلاستر) برای ایجاد احراز هویت بين هر جفت از

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

حملات سیبیل نخستین بار در شبکه‌های نظیر به نظیر مطرح شد. دوسر^۱ ادعا کرد در چنین محیط‌های محاسباتی توزیع شده‌ای، یک دستگاه می‌تواند به راحتی چندین هویت (شناسه) اختیار کند که این به دلیل فقدان یک قدرت مرکزی و مورد اعتماد در شبکه است [6].

حملات سیبیل به راحتی قابل پیاده‌سازی در شبکه‌های حسگری سیم هستند؛ چون گره‌های حسگر در یک محیط توزیع شده قرار گرفته‌اند و از طریق امواج رادیویی با یکدیگر ارتباط برقرار می‌کنند. این حملات عملیاتی مثل مسیریابی، رأی‌گیری، تجمعیت داده‌ها، تشخیص 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 به دست آمده از آن‌ها نمی‌توان اعتماد کرد [7]. 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-۱): حمله Sybil

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

³ Random Key Pre-distribution

¹ Douceur

² Radio Resource Testing

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

دسته سوم از این واقعیت که هر گره می‌تواند در هر زمان در یک موقعیت (مکان فیزیکی) قرار گیرد برای تشخیص حمله سبیل پهنه می‌گیرد. این تکنیک و استه به تأیید مکان است، محل مورد نظر برای هر تعیین‌کننده هویت با استفاده از اندازه‌گیری فاصله و مثلث‌بندی (زاویه‌بندی) بررسی می‌شود. دیمرباس^۷ و همکاران (۲۰۰۶) یک رویکرد مبتنی بر شاخص قدرت سیگنال دریافتی (RSSI)^۸ برای دفاع در برابر حملات سبیل ارائه کردند. یک مجموعه از گره‌های حس‌گر قابل اعتماد به عنوان 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 به عنوان مهاجم سبیل در نظر می‌گیرند [18].

استفاده از نسبت RSSI ابتدا توسط سونگ^۹ و همکاران برای تشخیص مکان فرستنده با استفاده از چهار گره ناظر مطرح شد [19] که از الگوریتم موقعیت‌یابی پیشنهاد شده برای تشخیص حملات سبیل استفاده می‌کند. بدین صورت 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 محاسبه شده و در صورت تشابه، تشخیص حمله سبیل اعلام می‌شود.

ساریکیانیدیس و همکاران (۲۰۱۵) یک روش مبتنی بر قانون براساس تشخیص به صورت ناهنجاری با استفاده از اطلاعات در محدوده فرکانسی UWB^{۱۰}. برای تشخیص حملات سبیل 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 IEEE 802.15.4 با M گره حس‌گر در نظر می‌گیرد. گره‌ها به طور یکنواخت در یک ناحیه با نام E شکل (۲) مستقر گردیده‌اند.

گره‌ها داخل شبکه ایجاد می‌شوند که مستلزم هزینه محاسباتی بالا و عدم مقیاس‌پذیری بود؛ زیرا هر گره جدید در شبکه چندین کلید با گره‌های دیگر به اشتراک می‌گذارد. چینگ^{۱۱} و همکاران (۲۰۱۳) یک روش مبتنی برای زنجیره کلید پیش‌توزیع شده در برابر حمله سبیل ارائه کردند، از چندین زنجیره کلید استفاده می‌شد. از هش اطلاعات هویتی یکتا برای هر گره پشت سرهم در ایستگاه پایه مورد اعتماد استفاده می‌شد که درنهایت یک استخراج از Zنجیره کلیدها ایجاد می‌شد. سپس از طریق پروتکل CK- AE گره‌های همسایه به همراه مابقی گره‌ها احراز هویت می‌شوند و یک جفت کلید منحصر به مفرد برای محافظت از جعل کلیدها بوسیله مهاجمان سبیل ایجاد می‌شد [16].

۲-۲- روش‌های مبتنی بر اطلاعات دریافتی از گره‌ها

دسته دوم با استفاده از تجزیه و تحلیل اطلاعات گره‌های همسایه، هویت گره‌ها را بررسی و بازبینی می‌کنند. بوسه^{۱۲} (۲۰۰۷) دو روش برای تشخیص حملات سبیل به نامهای MG و SRP ارائه داد که این دو روش مکمل یکدیگر هستند. روش MG برای زمانی است که گره مخرب شناسه یکی از گره‌های همسایه را در اختیار خود می‌گیرد. روش SRP 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 همسایگی اش نیست؛ سپس با مبادله اطلاعاتی درباره تعداد بسته‌های دریافتی هر گره و مقایسه تعداد بسته‌های ارسال شده و دریافت شده حمله سبیل تشخیص داده می‌شود [17].

سو^{۱۳} و همکاران (۲۰۰۹) روشی برای مقابله با حملات سبیل در شبکه‌های حس‌گر بی‌سیم ارائه داده‌اند که در آن با استفاده از تجزیه و تحلیل اطلاعات گره‌های همسایه 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 سبیل ارائه دهدند [7].

⁴ Received Signal Strength Indicator

⁵ zhong

⁶ Ultra-wideband

¹ Cheng

² Bhuse

³ Ssu

⁴ Demirbas

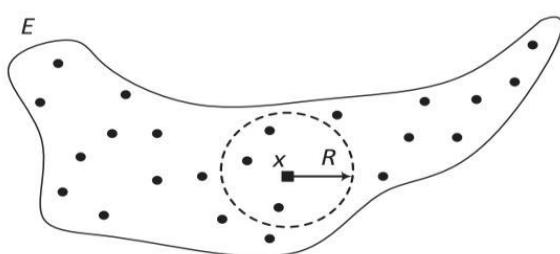
است؛ به این معنی که بررسی فاصله به صورت متواالی انجام می‌شود. در واقع تشخیص حمله سبیل به فرکانسی که هر گره مرحله کشف همسایگان را برای همسایگان جدید در مجاورتش جستجو می‌کند، وابسته است.

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

روش ساریکیانیدیس و همکاران^(۲۰۱۵) جزء روش تشخیص مبتنی بر مکان است که براساس رویکرد امنیت سخت عمل می‌کند. 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 همه چیز 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.

روش پیشنهادی در یک محیط شبیه‌سازی دقیق بررسی شده که نشان می‌دهد سامانه تشخیص پیشنهادی در برابر حملات سبیل اثر بخش بوده است. به طور کلی ویژگی‌های سامانه‌های تشخیص با روش‌های موجود مقایسه شده که در جدول ۱ نشان داده شده است.

سید محمود سجاد^۲ 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 به عنوان 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، به طور عمومی 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 حمله کننده، قابل اعتماد و مخاطره‌آمیز می‌شود. در صورتی که رفتار گره قابل اعتماد باشد این گره را به محرك ارسال، به منظور ارسال بسته



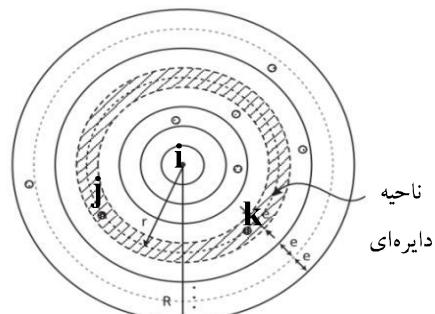
(شکل_۲): میدان شبکه حس‌گر

در RADS^۱ از چهار مرحله برای تشخیص حملات سبیل در شبکه‌های حس‌گر بی‌سیم استفاده می‌کند. مرحله نخست مرحله کشف همسایه است. کشف همسایه شامل تبادل بسته‌های hello بین گره‌های همسایه است. در مرحله دوم هر گره یک جدول که حاوی تخمین محدوده محاسبه شده است، به طور 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 می‌باشد که با گره n_i اندازه‌گیری می‌شود.

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

$$d_{ij}^a \leq d_{ij}^e + \frac{\epsilon}{2} \quad \text{برای هر گره } n_i \text{ و } n_j \text{ که } i \neq j \text{ و } i, j \in M$$

در مرحله سوم هر گره به تنها یک در شبکه به طور مستقل بررسی فاصله را چندین بار انجام می‌دهد (شکل_۳).



(شکل_۳): نحوه تشخیص گره سبیل [20]

در صورتی که گره n_i دو گره دیگر را (گره‌هایی به طور مجزا) مثل n_j و n_k که تفاوت فاصله آن‌ها کمتر از ϵ باشد پیدا کند، علامت‌گذاری می‌شود. گره با بررسی فاصله متوجه یک حمله سبیل می‌شود که نتیجه آن اضافه شدن گره n_k به فهرست سیاه است. مرحله سوم از الگوریتم، یک گام تکرار

² Syed Muhammad Sajjada

^۱ Rule-based anomaly detection system

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].

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 محرك ارسال، برای ارسال بسته‌ها توصیه می‌کند که گره مورد نظر رفتار پر خطر دارد. وضعیت گره‌های مشاهده شده در پایگاه

(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

جدول ۱ اعتقاد مستقیم گره n_2 برای توپولوژی شبکه در شکل ۵ نشان می‌دهد.

جدول_۱: اعتقاد 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.

$$T = 1 - e^{-|d_{ij}^e - d_{ik}^e| - \alpha} \quad (1)$$

در این رابطه α همان محدوده خطأ، d^e تخمین فاصله بین

گره n_i و n_j و d_{ik}^e تخمین فاصله بین گره n_i و n_k است. در صورتی که قدر مطلق $|d_{ij}^e - d_{ik}^e| - \alpha$ (که از این

پس با نماد ρ نشان داده خواهد شد) به صفر نزدیک شود مقدار ρ به یک نزدیک می‌شود درنتیجه مقدار اعتقاد ناحیه همزیستی (T) به صفر میل خواهد کرد.

میزان اعتقاد بر اساس منطق ذهنی^۱ جوسانگ [۲۲] محاسبه می‌شود. میزان باور، عدم باور و عدم قطعیت براساس این تعاملات طبق رابطه (۲) تعیین می‌شود.

$$b = \frac{s}{s+f+1}, \quad d = \frac{f}{s+f+1} \quad (2)$$

$$u = \frac{1}{s+f+1}$$

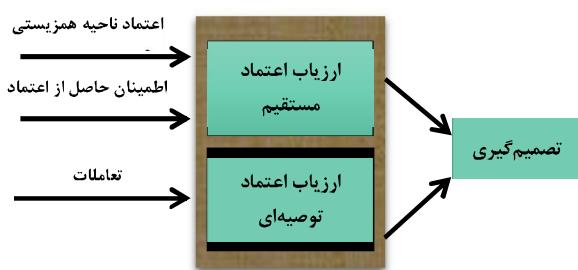
میزان باور (b)، میزان عدم باور (d)، عدم قطعیت (c)، تعداد تعاملات موفق (s)، تعداد تعاملات ناموفق (f) است. مقدار اعتقاد طبق رابطه (۳) محاسبه می‌شود.

$$T_c = \frac{b}{1-u} \quad (3)$$

در صورتی که عدم قطعیت صفر باشد، آنگاه مقدار اعتقاد برابر با میزان باور خواهد بود. در صورتی که مقدار اعتقاد ناحیه همزیستی (T) کمتر از مقدار آستانه (T_t) باشد، آن گره به عنوان گره مشکوک بوده و تصمیم‌گیری نهایی در خصوص تشخیص گره سبیل براساس مقدار اعتقاد (T_c) که حاصل از تعداد تعاملات موفق و ناموفق است، تعیین خواهد شد.

۳- توصیف روش پیشنهادی

بهمنظور کاهش نرخ هشدارهای اشتباه و تشخیص حملات سبیل غیرمستقیم و نظارت بر عملکرد گره‌ها در طول مدت فعالیتشان از یک پروتکل با رویکرد مدیریت اعتقاد به‌شرح ذیل استفاده می‌کنیم. ساختار کلی مدل پیشنهادی در شکل ۴ آمده است. در این پروتکل، اعتقاد مستقیم بر اساس تعاملات ناحیه همزیستی و اطمینان حاصل از اعتقاد، براساس تعاملات بین گره‌ها محاسبه می‌شود. همچنین از اعتقاد توصیه‌ای (غیرمستقیم) بهمنظور تشخیص حملات سبیل غیرمستقیم استفاده می‌شود که در آن گره مجاز به‌طورمستقیم با گره سبیل در ارتباط نیست.

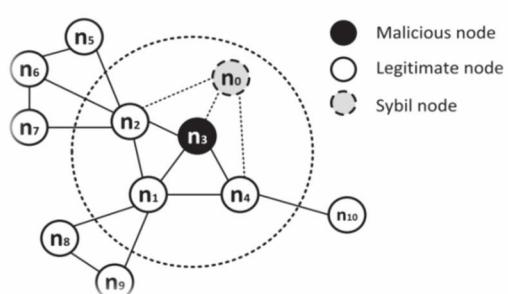


(شکل_۴): ساختار کلی روش پیشنهادی

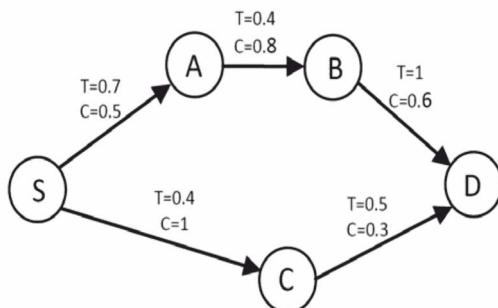
۳-۱-۱- قابلیت به کارگیری مدل پیشنهادی

بهمنظور کاهش نرخ هشدارهای اشتباه

هر گره از یک جدول که حاوی تعداد تعاملات موفق و ناموفق در هر دوره و میزان اعتقاد ناحیه همزیستی محاسبه شده برای گره‌های همسایه است، استفاده می‌کند. شکل ۵ حمله سبیل مستقیم را برای گره n_2 نشان می‌دهد.

(شکل_۵): حمله سبیل مستقیم برای گره n_2 ^۱ Subjective Logic

می‌انجامد و همچنین اطمینان می‌تواند به عنوان پارامتری در نظر گرفته شود که بعد دیگری به خروجی مدل اعتماد اضافه می‌کند. به عنوان نمونه شکل (۷) یک شبکه اعتماد را نشان می‌دهد که در آن برچسب هر یال گراف علاوه بر مقدار اعتماد (T)، میزان اطمینان (C) به اعتماد تخمین‌زده شده را نیز در بر دارد؛ برای مثال برچسب لبه SA نشان می‌دهد که گره S به گره A اعتماد ۰.۷ دارد؛ در صورتی که مقدار اطمینان به اعتماد تخمین‌زده شده فقط ۰.۵ است [۲۳].



(شکل_۷): یک شبکه اعتماد نمونه با مقادیر اطمینان [۲۳]

در بسیاری از مدل‌های مدیریت اعتماد، تخمین 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؛ [۲۴] که در رابطه (۴) نشان داده شده است.

$$C_{\text{ind}} = 1 - u \quad (4)$$

در صورتی که نتیجه حاصل از برآیند اعتماد توصیه‌ای آگاه از اطمینان گره مقصد کمتر از مقدار آستانه باشد، گره مذکور را به عنوان گره سبیل 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.

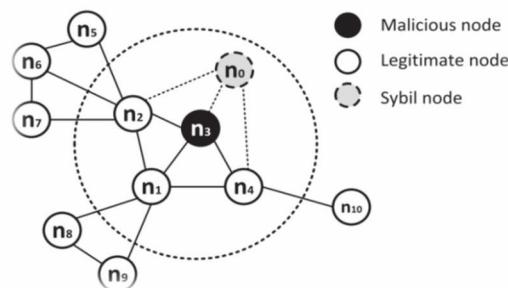
$$W_i = e^{-\lambda \Delta T_i} \quad \Delta T_i = T_{\text{Current}} - T_i \quad (5)$$

λ خریب میرایی اعتماد است که مشخص می‌کند از چه زمان قبل قر تعاملات تأثیر نداشته باشد i وزن تعاملات

برای مقدار اعتماد، یک آستانه (T_C) در نظر می‌گیریم چنانچه مقدار به دست آمده کمتر از مقدار آستانه باشد، آن گره را به عنوان گره سبیل تشخیص می‌دهیم.

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

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



(شکل_۶): حمله سبیل غیرمستقیم

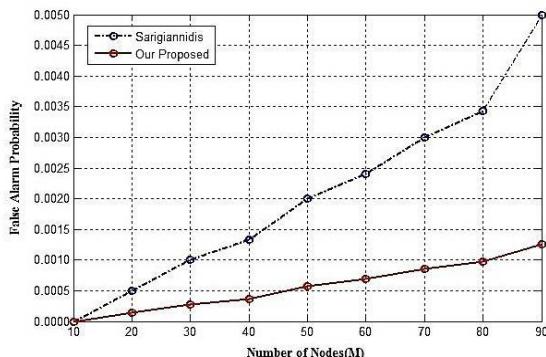
با توجه به اینکه هر گره دارای جدول همسایگی است که در آن تعداد تعاملات موفق و ناموفق در هر دوره نسبت به همسایگانی که به طورمستقیم با آن‌ها در ارتباط هستند، ثبت شده است، به منظور تشخیص گره سبیل در این روش نظر گره‌های دیگر را که به طور مستقیم با گره مقصد در ارتباط هستند، بررسی می‌شود. بر اساس تعاملات موفق و ناموفق در

هر دوره میزان اعتماد آگاه از اطمینان بر اساس منطق ذهنی ^{۱۴} جوسانگ [۲۲] محاسبه می‌شود و میزان باور، عدم باور و عدم قطعیت بر اساس این تعاملات طبق رابطه (۲) و مقدار اعتماد طبق رابطه (۳) تعیین می‌شود.

اطمینان میزان باور به درستی 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 ارزیابی شده است که مقدار آن در بازه [۰,۱] 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

^۱ Subjective Logic

محدوده شعاع ارتباطات $R=20m$ و محدوده خطا $e=50cm$ می باشد، که تعداد گرهها از ۱۰ تا ۹۰ تغییر می یابد.



(شکل_۸): مقایسه احتمال تولید هشدارهای اشتباه

جدول (۳) نتایج نرخ هشدارهای اشتباه (FPR) را هنگامی که تعداد گرهها (M) در حال تغییر است، نشان می دهد. همان طور 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 می یابد، احتمال اینکه گرهای به اشتباه در ناحیه همزیستی گره دیگری قرار گیرد، بیشتر می شود و درنتیجه اعتماد ناحیه همزیستی کاهش می یابد و از مقدار آستانه همزیستی (T_e) کمتر می شود. در مرحله دوم که باید بر اساس میزان تعاملات موفق و ناموفق تصمیم گیری شود، احتمال اینکه میزان اعتماد کمتر از مقدار آستانه اعتماد (T_{tC}) شود محتمل تر 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

۲-۴- نتایج حاصل از آزمایش‌ها در تشخیص

حملات سیبیل غیرمستقیم

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

را مشخص می کند. در صورتی که از زمان تعاملات (نسبت به زمان جاری) زمان زیادی گذشته باشد، مقدار $t_i^{-\lambda e^{-T_i}}$ و درنتیجه W_i به صفر نزدیک می شود.

$$s = \sum_{x_i \in ST} W_i, \quad f = \sum_{x_i \in FT} W_i \quad (6)$$

مجموعه تعاملات موفق و FT مجموعه تعاملات ناموفق است.

این تعاملات می توانند به صورت اسلات‌های زمانی در نظر گرفته شود که هر کدام دارای یک برچسب زمانی هستند.

۴- ارزیابی مدل پیشنهادی

روش پیشنهادی در نرم افزار متلب شبیه سازی شده است. M تعداد کل گرههای حسگر، R شعاع ارتباطات (شعاع حسی) e ، E محدوده خطا و N ناحیه‌ای است که گرههای حسگر در آن توزیع شده‌اند. جدول (۲) پارامترهای مورد استفاده در شبیه سازی را نشان می دهد. 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 برعرسی خواهد شد.

(جدول_۲): پارامترهای به کار رفته در شبیه سازی

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

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

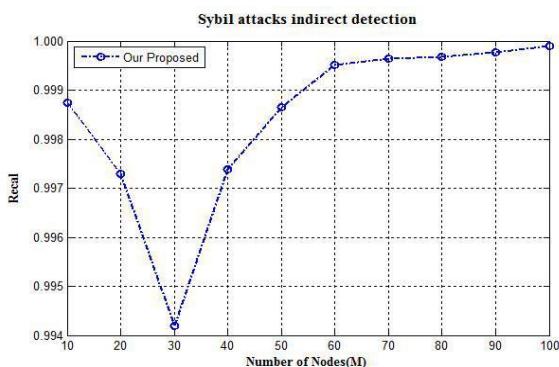
نمودار شکل (۸) مقایسه احتمال تولید هشدارهای اشتباه روش پیشنهادی را با روش ساریکیانیدیس به عنوان تابعی از تغییرات تعداد گرهها نشان می دهد. که مقدار $E=100m^2$ ، $e=50cm$ محدوده شعاع ارتباطات $R=20m$ و محدوده خطا $e=50cm$ است که تعداد گرهها از ۱۰ تا ۱۰۰ تغییر می یابد.

ثابت بودن 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 به عنوان نمودار Recall، نسبت حملات را که به درستی تشخیص داده شده (TP) به کل حملات (هم حملاتی که به درستی تشخیص دادیم و هم حملاتی که تشخیص داده نشده است (TP+FN)) با استفاده از اعتماد توصیه‌ای، به عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.

Sensitivity را به عنوان نرخ Recall در نظر گرفته می‌شود که طبق رابطه (۷) محاسبه می‌شود.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (7)$$



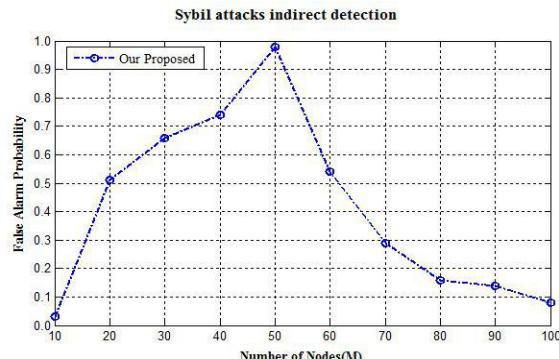
(شکل_۱۱): نسبت حملات که به درستی تشخیص داده شده به کل حملات (Recall) با استفاده از اعتماد توصیه‌ای

نمودار شکل ۱۲ به عنوان نمودار Precision، نسبت حملاتی که به درستی تشخیص داده شده (TP) به کل تشخیص (هم حملاتی که به درستی تشخیص دادیم و هم آن‌هایی که حمله نبود و به اشتباہ حمله تشخیص دادیم (TP+FP)) را با استفاده از اعتماد توصیه‌ای، به عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.

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

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (8)$$

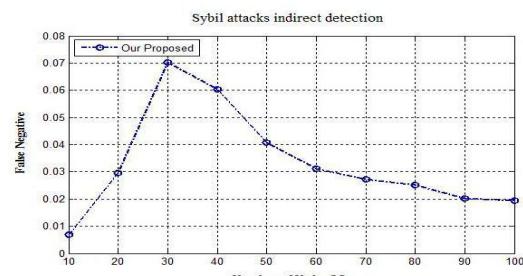
زمانی که تعداد گره‌ها به صد گره افزایش می‌یابد، دقت تشخیص روش پیشنهادی ۹۹.۹۲ درصد می‌باشد.



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

همان‌طور که در نمودار شکل (۹) نشان داده شده مقدار نرخ هشدارهای اشتباه بسیار کم و زمانی که تعداد گره‌ها M=100 است به ۰.۰۸% می‌رسد. مقدار نرخ هشدارهای اشتباه در ابتدا با افزایش گره‌ها افزایش می‌یابد. با توجه به ثابت بودن مساحتی که گره‌ها در آن توزیع شده‌اند (E=100m²) 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 ازانجا به بعد نرخ هشدارهای اشتباه کمتر می‌شود.

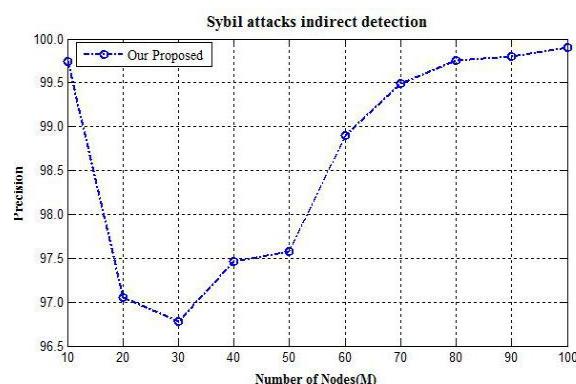
نمودار شکل ۱۰ نرخ FN را در تشخیص حملات سیبیل غیرمستقیم با استفاده از اعتماد توصیه‌ای، به عنوان تابعی از تغییرات تعداد گره‌ها نشان می‌دهد.



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

همان‌طور که در نمودار شکل ۱۰ نشان داده شده است، نرخ FN با افزایش تعداد گره‌ها افزایش می‌یابد. با توجه به

بهبود روش ارائه شده بهمنظور کاهش میزان انرژی و استفاده از روش های یادگیری ماشین برای تعیین پارامترهای مورد استفاده در مدل پیشنهادی مانند ضربی پویایی و شکنندگی، از جمله مواردی هستند که در آینده می تواند موضوع پژوهش و تحقیق قرار گیرند. همچنین مدل کردن روش ارائه شده برای دیگر حملات مطرح در شبکه های حسگر بی سیم از جمله، حمله گودال و کرم چاله می تواند از اهداف پژوهشی در آینده باشد.



(شکل-۱۲): نسبت حملاتی که به درستی تشخیص داده شده به کل تشخیص (Precision) (با استفاده از اعتماد توصیه ای

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

۵- نتیجه گیری

روش های مختلف ارائه شده برای تشخیص حملات سیبیل بر اساس رویکرد امنیت سخت است. این روش ها باید محدودیت های این شبکه ها را در منابع پردازشی، حافظه و توان در نظر بگیرند. سازوکارهای مبتنی بر امنیت سخت برای حفظ امنیت سامانه های اطلاعاتی به خصوص در جوامع باز، کافی نیستند که در سال های اخیر رویکردی جدیدی از امنیت به نام امنیت نرم مورد توجه واقع شده است؛ که در آن به جای یک نهاد مرکزی، افراد مسئول امنیت خود هستند که سامانه های مدیریت اعتماد نمونه ای 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 توصیه های دریافتی از همسایه ها و وزن دهی به این توصیه ها می باشد، 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 آزمایش های ارائه شده، مدل پیشنهادی باعث افزایش دقت و کاهش نرخ هشدارهای اشتباه شد و از طرفی امکان تشخیص حملات سیبیل غیرمستقیم را فراهم کرد. با درنظر گرفتن عامل زمان در تعاملات برای محاسبه اعتماد آگاه از اطمینان یک سامانه مدیریت اعتماد پویا ارائه شد که مقادیر اعتماد بین گره ها را با درنظر گرفتن عامل زمان محاسبه می کند. این روش برای محاسبه اعتماد غیرمستقیم بین گره ها، میزان اطمینان به اعتماد را در نظر می گیرد تا توصیه های قابل اطمینان تر، تأثیر بیشتری در محاسبه اعتماد داشته باشند.

- [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 طباطبائی پارسا

تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات به ترتیب از دانشگاه علمی و کاربردی 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 به عنوان دانشجو ممتاز می‌باشد. زمینه‌های پژوهشی مورد علاقه ایشان مدیریت اعتماد، پنهان نگاری، رمزگاری و امنیت شبکه می‌باشد.



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 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.

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 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.