یک سیستم تشخیص نفوذ سبک مبتنی بر اعتماد دوسطحی برای شبکه‌های حسگر بی‌سیم

مهدی صادقی‌زاده و امیدرضا معروضی

چکیده: شبکه‌های حسگر بی‌سیم یکی از فناوری‌های کاربردی و جذاب است که در سال‌های اخیر بسیار مورد توجه قرار گرفته است. این شبکه‌ها به دلیل ویژگی‌هایی همچون سهولت استفاده و هزینه پایین آن، در زمینه‌های متنوعی به کار گرفته شده‌اند. با توجه به بحرانی‌بودن اغلب کاربردهای این شبکه‌ها، امنیت به‌عنوان یکی از پارامترهای اساسی کیفیت سرویس در آنها مطرح بوده و بنابراین تشخیص نفوذ نیز به‌عنوان یک لازمه اساسی برای تأمین امنیت در این شبکه‌ها تلقی می‌شود. این مقاله یک سیستم تشخیص نفوذ سبک مبتنی بر اعتماد را برای محافظت از شبکه حسگر بی‌سیم در برابر همه حملات لایه شبکه و مسیریابی ارائه می‌نماید که مبتنی بر خصوصیات استخراج‌شده از آنها است. از طریق شبیه‌سازی‌ها، سیستم تشخیص نفوذ پیشنهادی با تمامی معیارهای کارایی مورد ارزیابی قرار گرفته است. نتایج به‌دست‌آمده نشان می‌دهد که سیستم تشخیص نفوذ پیشنهادی در مقایسه با کارهای موجود که اغلب بر روی یک حمله خاص تمرکز دارند، همه حملات لایه شبکه و مسیریابی را در شبکه‌های حسگر بی‌سیم پوشش داده و همچنین با توجه به دقت تشخیص بالا، نرخ هشدار نادرست پایین و مصرف انرژی کم، به‌عنوان یک سیستم تشخیص نفوذ مطلوب و سبک برای شبکه‌های حسگر بی‌سیم مطرح است.

کلیدواژه: **شبکه‌های حسگر بی‌سیم، حملات مسیریابی، سیستم‌های تشخیص نفوذ، تشخیص مبتنی بر خصوصیات، عملیات مبتنی بر اعتماد، معیار کارایی.**

۱- مقدمه

شبکه‌های حسگر بی‌سیم به دلیل مزایای ذاتی خود مانند هزینه کمتر و استقرار راحت‌تر در محیط، برای ایفای نقش در طیف وسیع و متنوعی از کاربردها مانند کنترل و نظارت نظامی [۱]، مراقبت از سلامتی [۲]، نظارت بر ایمنی سازه‌ها و ساختمان‌ها و خانه‌های هوشمند [۳]، بسیار مطلوب و مقرون‌به‌صرفه می‌باشند. با این وجود گره‌های موجود در این شبکه‌ها به دلیل توان پردازشی پایین، حافظه و انرژی محدودشان دارای محدودیت‌های منابع شدیدی هستند [۴].

با توجه به این که این شبکه‌ها معمولاً در مکان‌های دور و فاقد حفاظت و یا اغلب در جاهایی که شرایط عملیاتی نامطلوب و یا حتی خصمانه دارد به کار گرفته می‌شوند، برای تهاجم و حملات امنیتی بسیار مستعد هستند که این امر با توجه به منابع محدود آنها باعث کاهش شدید عملکرد و کارایی آنها می‌گردد. بنابراین تأمین امنیت در شبکه‌های حسگر بی‌سیم در برابر مهاجمان و حملات مختلف به یک موضوع مهم مبدل شده است، به‌ویژه اگر این شبکه‌ها در فرایندهای بحرانی نیز دخیل باشند [۵]. شبکه‌های حسگر بی‌سیم امن در کاربردهای نظامی دارای اهمیت بحرانی و حساسی هستند، به‌گونه‌ای که یک شکاف امنیتی در شبکه می‌تواند باعث تحریک و تضعیف نیروهای خودی در میدان جنگ گردد.

مهم‌ترین حملاتی که بیشترین تقابل را در شبکه‌های حسگر بی‌سیم دارند و در مراجع زیادی مانند [۶] تا [۸] مورد توجه بوده‌اند، حملات لایه شبکه و مسیریابی هستند. این حملات عبارتند از:

- حمله حفره چاهک[1] (سیاه‌چاله) [۹]
- حمله سایبیل[2] [۱۰]
- حمله کرم‌چاله[3] [۱۱]
- حمله سیل ارسال پیام[4] [۱۲]
- حمله ارسال انتخابی[5] [۱۳]

در این مقاله قصد داریم با شبیه‌سازی یک نمونه کامل از شبکه حسگر بی‌سیم و قراردادن آن در معرض حملات مسیریابی، نحوه عملکرد و کارایی آن را در مواجهه با آنها ارزیابی کرده و با تحلیل رفتار حملات به طراحی یک سیستم تشخیص نفوذ سبک مبتنی بر اعتماد در شبکه‌های حسگر بی‌سیم بپردازیم به‌گونه‌ای که عملکرد شبکه را در برابر حملات مختلف به‌خوبی حفظ نماید. در همین راستا ما در ابتدا یک سیستم تشخیص نفوذ سبک را بر اساس تحلیل رفتار حملات مختلف و خصوصیات آنها ارائه می‌نماییم و در ادامه به جهت بهبود آن، از یک روش مبتنی بر اعتماد برای ارزشیابی پیام‌های هشدار در گره‌های مختلف استفاده می‌کنیم. برای اعتبارسنجی مناسب روش پیشنهادی، تمامی معیارهای کارایی نیز مورد ارزیابی قرار گرفته‌اند.

ادامه مقاله به این صورت سازمان‌دهی شده است: در بخش ۲، ابتدا سیستم‌های تشخیص نفوذ را به همراه انواع مکانیسم‌های موجود تشریح می‌کنیم. سپس مهم‌ترین کارهای انجام‌شده در زمینه تشخیص نفوذ را به همراه مزایا و معایب آنها بررسی می‌کنیم. در بخش ۳ سیستم تشخیص نفوذ پیشنهادی خود را ارائه می‌نماییم. در بخش ۴ به شبیه‌سازی، ارائه نتایج و مقایسه روش پیشنهادی با کارهای موجود خواهیم پرداخت. در انتهای مقاله نیز در بخش ۵، نتیجه‌گیری کلی را ارائه خواهیم نمود.

۲- کارهای مرتبط

در این بخش ابتدا سیستم‌های تشخیص نفوذ به همراه انواع آنها مورد تشریح قرار می‌گیرند. در انتها نیز مهم‌ترین سیستم‌های تشخیص نفوذ موجود را مورد بررسی و ارزیابی قرار خواهیم داد.

این مقاله در تاریخ ۲۴ اردیبهشت ماه ۱۳۹۷ دریافت و در تاریخ ۲۵ بهمن ماه ۱۳۹۷ بازنگری شد.

مهدی صادقی‌زاده (نویسنده مسئول)، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شاهرود، شاهرود، ایران، (email: m.sadeghizadeh@shahroodut.ac.ir).

امیدرضا معروضی، دانشکده مهندسی برق و رباتیک، دانشگاه صنعتی شاهرود، شاهرود، ایران، (email: marouzi@shahroodut.ac.ir).

1. Sinkhole Attack
2. Sybil Attack
3. Wormhole Attack
4. Hello Flooding Attack
5. Selective Forward Attack

۲-۱ سیستم‌های تشخیص نفوذ

در یک شبکه یا یک سیستم، هر نوعی از فعالیت‌های غیر مجاز و نامطلوب، نفوذ نامیده می‌شوند. یک سیستم تشخیص نفوذ یک مجموعه از ابزار، متدها و منابع برای کمک به شناسایی، ارزیابی و گزارش نفوذها است. تشخیص نفوذ یک واحد حفاظتی منفرد و جداگانه نیست بلکه معمولاً بخشی از یک سیستم حفاظت کلی‌تر است که در کنار یک سیستم یا دستگاه نصب می‌گردد. نفوذ به‌صورت: "هر مجموعه از فعالیت‌ها که تلاش می‌کند تا اصالت، محرمانگی و یا موجودیت یک منبع را به خطر بیندازد" تعریف می‌شود [۱۴] و تکنیک‌های پیشگیری از نفوذ (مانند رمزنگاری، تأیید هویت، مسیریابی امن و غیره) به‌عنوان اولین خط تدافعی در برابر نفوذها ارائه می‌شوند.

با این وجود باید توجه داشت که در هیچ سیستم امنیتی، نمی‌توان به طور کامل از نفوذها پیشگیری نمود. نفوذ و تسخیر یک گره منجر به افشای اطلاعات محرمانه مانند کلیدهای امنیتی برای نفوذگرها می‌شود. این امر منجر به شکست مکانیسم امنیتی پیشگیرانه می‌گردد. بنابراین سیستم‌های تشخیص نفوذ به جهت شناسایی نفوذها طراحی شده‌اند، قبل از این که آنها بتوانند منابع سیستم و اطلاعات امنیتی را فاش کنند. شرایط عملیاتی مورد انتظار در یک سیستم تشخیص نفوذ به‌صورت زیر خواهد بود [۱۵] و [۱۶]:

- نباید معایب و نقاط ضعف جدیدی به سیستم اضافه نماید.
- منابع سیستم را کمتر مصرف نماید و همچنین نباید با سربارهایی که به سیستم تحمیل می‌کند، کارایی آن را تنزل دهد.
- دارای نرخ بالای تشخیص درست و نرخ پایین تشخیص اشتباه باشد.
- به‌صورت پیوسته و مداوم اجرا گردد و برای سیستم و کاربران به‌صورت نامحسوس عمل نماید (اصل شفافیت[1]).
- طراحی آن مطابق استانداردها باشد تا امکان مشارکت و گسترش آن در آینده وجود داشته باشد.

سیستم‌های تشخیص نفوذ بر اساس نحوه عملکرد به سه گروه دسته‌بندی می‌شوند [۱۷] که در زیر به اختصار تشریح شده‌اند:

- **تشخیص مبتنی بر ناهنجاری[2]:** این روش مبتنی بر مدل رفتار آماری است که در آن عملیات عادی اعضای شبکه ثبت شده و در صورت مشاهده انحراف مشخصی نسبت به آن، ناهنجاری تشخیص داده می‌شود. عیب این روش تشخیص این است که چون رفتار شبکه ممکن است سریع تغییر نماید، بنابراین اطلاعات وضعیت عادی اعضا باید به‌صورت دوره‌ای به‌روزرسانی گردد. این امر باعث می‌شود بار کاری گره‌ها افزایش یافته و سرباری بر منابع محدود گره‌های حسگر اضافه نماید [۱۴]. مزیت این نوع تشخیص این است که کاملاً برای تشخیص حملات ناشناخته که قبلاً با آنها مواجه نشدیم مناسب است.
- **تشخیص نفوذ مبتنی بر قانون[3]:** در این روش الگوی مربوط به حملات شناخته‌شده قبلی تولید شده و به‌عنوان مرجعی برای شناسایی حملات آینده استفاده می‌گردد. مزیت این روش در این است که می‌تواند حملات شناخته‌شده را به‌طور دقیق و کارا تشخیص دهد. بنابراین این روش‌ها دارای نرخ پایینی در خطا هستند. عیب این روش نیز این است که اگر حمله نوع جدیدی باشد، در این صورت قادر به شناسایی و رسیدگی به آن نخواهد بود و مهاجم به‌راحتی می‌تواند در شبکه فعالیت کند.
- **تشخیص مبتنی بر خصوصیات[4]:** در این روش یک مجموعه از خصوصیات و محدودیت‌ها که عملیات صحیح یک برنامه یا پروتکل را توصیف می‌نمایند تعریف می‌شود. سپس اجرای آن برنامه با توجه به خصوصیات و محدودیت‌های تعریف‌شده مورد نظارت قرار می‌گیرد. این روش به‌گونه‌ای است که قابلیت تشخیص حملات شناخته‌شده قبلی را با نرخ پایین خطا فراهم می‌نماید. تکنیک تشخیص نفوذ مبتنی بر خصوصیات مزایای هر دو روش تشخیص مبتنی بر ناهنجاری و مبتنی بر قانون را ادغام می‌نمایند.

۲-۲ سیستم‌های تشخیص نفوذ موجود

تاکنون سیستم‌های تشخیص نفوذ زیادی برای شبکه‌های حسگر بی‌سیم ارائه شده که اغلب آنها مانند [۹] تا [۱۳] بر روی یک حمله خاص تمرکز دارند. معدودی از سیستم‌های تشخیص نفوذ نیز وجود دارند که بر روی تعدادی و یا همه حملات موجود قابل استفاده هستند که در ادامه به تشریح مهم‌ترین آنها می‌پردازیم.

در [۱۸] یک معماری سلسله‌مراتبی[5] برای تشخیص نفوذ همراه با پردازش داده به شیوه سلسله‌مراتبی پیشنهاد شده است. آنها یک خوشه‌بندی دوسطحی را ارائه کردند که در سطح اول سرخوشه‌ها مدیریت خوشه‌ها را بر عهده دارند و در سطح دوم سرخوشه‌ها با دروازه‌ها در ارتباط خواهند بود و از طریق آنها با ایستگاه پایه مرتبط می‌شوند. آنها در تمام آزمایش‌های معماری پیشنهادی خود بر روی مفهوم خوشه‌بندی تک‌پرشه متمرکز شده‌اند. دلیل اصلی تمرکز آنها بر روی خوشه‌بندی تک‌پرشه این گونه عنوان شده که بالاترین نرخ تشخیص زمانی است که گره‌ها به‌صورت تک‌پرشه با سرخوشه در ارتباط باشد و هرچه تعداد پرش‌ها بیشتر گردد نرخ تشخیص نفوذ نیز به‌صورت خطی کاهش خواهد یافت. ایراد اساسی معماری سلسله‌مراتبی آنها برای تأمین امنیت در شبکه‌های حسگر بی‌سیم این است که صرفاً برای کاربردهای صنعتی قابل استفاده می‌باشد.

در [۱۹] حمله و تشخیص آن به‌عنوان طرفین یک بازی در نظر گرفته شده و تدابیری برای طرفین بازی تنظیم گردیده است. به‌منظور افزایش احتمال تشخیص، استراتژی‌ها درون یک مدل بازی غیر صفر و غیر مشارکتی[6] نرمال شده‌اند. ایده آنها بر روی شناسایی ضعیف‌ترین گره در شبکه و ایجاد تدابیری برای دفاع از آن گره تمرکز دارد. مشکل موجود در این شیوه این است که در صورت وجود چندین مهاجم در شبکه حسگر بی‌سیم، تنها یکی از آنها توسط سیستم تشخیص نفوذ شناسایی می‌گردد در حالی که مابقی مهاجمان بدون شناسایی رها می‌شوند.

در [۲۰] متدهای سبک‌وزنی[7] را برای تشخیص نفوذهای غیر عادی در شبکه‌های حسگر بی‌سیم پیشنهاد کردند. ایده اصلی آنها مبتنی بر استفاده مجدد از اطلاعات سیستمی موجود قبلی (مانند لیست همسایه‌ها، جداول مسیریابی، زمان‌بندی‌های فعال و غیر فعال شدن، اطلاعات شدت سیگنال دریافتی و زمان‌بندی ارسال در لایه MAC) می‌باشد که در لایه‌های مختلف پشته پروتکلی شبکه در مدل OSI، به‌ویژه در لایه‌های فیزیکی، MAC و مسیریابی تولید شده است. به‌منظور ارائه یک نرخ تشخیص بهتر، مؤلفان پیشنهاد کردند که چندین تشخیص‌گر به لایه‌های مختلف

1. Transparency
2. Anomaly Intrusion Detection Systems
3. Rule Based Intrusion Detection Systems
4. Specification Intrusion Detection Systems
5. Hierarchical Intrusion Detection
6. Non-Cooperative and Non-Zero Game Model
7. Lightweight Methods

مدل OSI نظارت نمایند. این برای شبکه‌های حسگر امکان‌پذیر نیست زیرا نظارت بر نفوذ در لایه‌های مختلف و حفظ هماهنگی بین این ناظرها می‌تواند به‌سرعت منابع محدود موجود در شبکه حسگر را مصرف نموده و تخلیه کند. از طرف دیگر، مؤلفان طرحشان را تنها برای حملات خارجی پیشنهاد کردند و حملات داخلی را در نظر نمی‌گیرند. این گزینش کافی نیست زیرا گره‌ها در یک شبکه حسگر بی‌سیم برای حملات داخلی (حمله تسخیر فیزیکی گره‌ها، حمله سایبیل و غیره) بسیار مستعد هستند.

در [۲۱] یک سیستم تشخیص نفوذ سبک مبتنی بر دانش تشخیص (OWIDS)[1] ارائه شده که از یک سری گره‌های نگهبان به جهت تشخیص نفوذ استفاده می‌کند. گره نگهبان در واقع گره حسگری است که دانش چگونگی تشخیص حملات را در خود دارد. این گره‌ها از طریق جمع‌آوری اطلاعات از گره‌های حسگر و اعمال دانش تشخیص بر روی آنها، بر گره‌های حسگر نظارت می‌کنند. در این روش برای بالابردن قدرت گره‌های نگهبان در تشخیص حملات، روابط بین گره‌های حسگر را نیز در دانش تشخیص تعریف می‌کند. روش پیشنهادی آنها از لحاظ مصرف انرژی سبک است اما با توجه به استفاده از گره‌های نگهبان که عملاً یک سربار برای شبکه است، هزینه شبکه را افزایش خواهد داد. همچنین دقت تشخیص نیز وابسته به تعداد گره‌های نگهبان در شبکه تغییر می‌نماید.

در [۲۲] یک سیستم تشخیص نفوذ ترکیبی سراسری (GHIDS)[2] ارائه شده است که به جهت دستیابی به هدف نرخ تشخیص بالا و نرخ هشدار نادرست پایین، به‌صورت ترکیبی از یک روش تشخیص ناهنجاری مبتنی بر تکنیک ماشین بردار پشتیبان (SVM)، همراه با یک مجموعه از قوانین تشخیص مبتنی بر امضا برای شناسایی حملات در شبکه‌های حسگر بی‌سیم مبتنی بر خوشه‌بندی استفاده می‌نماید. نتایج حاصل از شبیه‌سازی‌ها نشان می‌دهد که روش پیشنهادی آنها از لحاظ نرخ تشخیص و نرخ هشدار نادرست در وضعیت مطلوبی قرار دارد. اما مشکل اساسی آنها بالابودن مصرف انرژی به جهت استفاده از روش مبتنی بر تکنیک ماشین بردار پشتیبان (SVM) است که سربار آن برای شبکه حسگر مناسب نیست.

در [۲۳] یک روش تشخیص نفوذ مبتنی بر اعتماد در سطح لایه پروتکل (PLTIDS)[3] برای شبکه‌های حسگر بی‌سیم ارائه شده است. در روش پیشنهادی آنها مقدار اعتماد یک گره حسگر با توجه به انحراف پارامترهای کلیدی در هر لایه پروتکل و با توجه به حملات آغازشده در آن لایه، محاسبه می‌گردد. آنها در روش پیشنهادی به‌طور عمده سه جنبه از اعتماد، یعنی اعتماد در لایه فیزیکی، اعتماد در لایه کنترل دسترسی به رسانه و اعتماد در لایه شبکه را بر اساس پارامترهای مختص هر لایه در نظر می‌گیرند. سپس معیارهای اعتماد در هر لایه را برای تعیین مقدار کل اعتماد یک گره حسگر ترکیب می‌کنند. نتایج ارائه‌شده با شبیه‌سازی در سناریوهای مختلف حملات، حاکی از آن است که روش تشخیص نفوذ پیشنهادی آنها از لحاظ نرخ تشخیص شرایط مناسبی را دارد. اما مشکل اصلی روش پیشنهادی آنها نرخ هشدارهای نادرست آن است که نسبتاً بالا می‌باشد.

در [۲۴] یک سیستم تشخیص نفوذ ترکیبی برای شبکه‌های حسگر بی‌سیم مبتنی بر خوشه‌بندی ارائه شده که با ادغام قوانین تشخیص رفتار سوء و اعتبارسنجی عملکرد، گره‌های مهاجم را شناسایی می‌کند. ایده اصلی روش پیشنهادی در این است که به جای تشخیص حملات فقط در سطح گره‌ها، یک طرح مبتنی بر همکاری و متمرکز با استفاده از ارزیابی اعتماد متقابل بین همه اجزای شبکه، پیشنهاد کردند که در آن هر گره حسگر مقادیر مربوط به اعتبار عملکرد همسایه‌های خود را به وسیله مشاهده فعالیت‌های آنها (نقل و انتقالات و تجمیع داده‌ها) محاسبه می‌نماید. برای رسیدن به این هدف آنها پنج معیار اعتبارسنجی عملکرد را تعریف کرده و از مزیت نرخ تشخیص بالای شیوه تشخیص رفتار سوء نیز با اعمال قوانین مربوط بهره برده‌اند. مشکل اصلی روش آنها این است که صرفاً نتایج خود را از لحاظ مصرف انرژی بیان کرده‌اند و هیچ بحثی بر روی انواع حملات قابل شناسایی و نرخ تشخیص آنها ارائه نکرده‌اند.

۳- سیستم تشخیص نفوذ پیشنهادی

تاکنون روش‌های مختلفی برای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه شده است. اما چالش اساسی در روش‌های موجود همچنان در مصرف انرژی بالا و عدم پوشش اغلب حملات است.

ما از یک تشخیص نفوذ مبتنی بر خصوصیات استفاده می‌کنیم که با توجه به موارد ذکرشده در بخش ۲-۲، هم به جهت سرعت عمل آن و کاهش انرژی مصرفی در تشخیص و هم به دلیل پایین‌بودن خطا در تشخیص، می‌تواند کارایی شبکه را در حد مطلوبی نگه دارد. همچنین به جهت بهبود دقت تشخیص ما از یک روش مبتنی بر اعتماد سبک نیز بهره خواهیم برد به‌گونه‌ای که بتواند بر اساس سطح اعتماد گره‌ها، پیام‌های هشدار تولیدشده توسط آنها را ارزشیابی نماید. این ارزشیابی می‌تواند سیستم تشخیص نفوذ را در تشخیص گره‌های مهاجم و حملات یاری کند و دقت تشخیص‌های آن را نیز ارتقا دهد.

سیستم پیشنهادی در دو سطح گره‌های عادی (سطح اول) و گره‌های سرخوشه (سطح دوم) سازمان‌دهی می‌گردد. در سطح اول، ابتدا گره‌های عادی قوانین مربوط به خصوصیات حملات مختلف را بررسی نموده و در صورت وجود هرگونه ناهنجاری آن را به گره سرخوشه به جهت بررسی‌های بیشتر ارجاع می‌دهند. در سطح دوم گره‌های سرخوشه هشدارهای رسیده از گره‌های مختلف را بررسی می‌نماید و در صورتی که این هشدارها از حد آستانه بگذرند، به‌عنوان یک حمله شناخته شده و لیست مربوط به گره‌های مهاجم توسط سرخوشه به‌روزرسانی شده و به همه گره‌های خوشه ارسال می‌گردد.

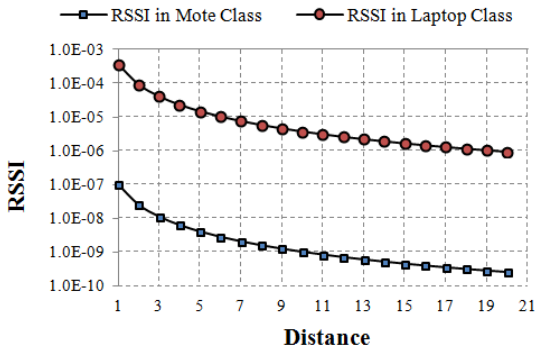
در ادامه با اصلاح عملیات سرخوشه‌ها از طریق یک سیستم مبتنی بر اعتماد که در بخش ۳-۳ تشریح می‌گردد، سعی می‌کنیم عملکرد سیستم تشخیص نفوذ پیشنهادی را بهبود بدهیم.

۳-۱ تشخیص نفوذ سطح اول

تشخیص نفوذ در سطح گره‌های عادی (سطح اول) به‌صورت قوانینی اعمال می‌گردد که از خصوصیات هر نوع حمله استخراج شده است. این خصوصیات بر اساس تحلیل صورت‌گرفته در بخش تحلیل رفتار حملات و نحوه عملکرد آنها به دست آمده است. این قوانین به همراه شبه‌کدهای مربوط به شرح زیر می‌باشند:

تشخیص حمله انکار سرویس: در این حمله مهاجم با توجه به سرعت بالا در ارسال بسته‌ها به سایر گره‌ها قصد دارد تا بار کاری آنها را به حدی برساند که امکان سرویس‌دهی معمول خود را از دست بدهند. بنابراین با بررسی فاصله زمانی بین بسته‌های دریافتی می‌توان این مهاجم را شناسایی نمود که مقدار حد آستانه آن (۰/۱۵ ثانیه) در جدول ۱ ارائه شده

1. Ontology-Based Wireless IDS
2. Global Hybrid IDS
3. Protocol Layer Trust-Based IDS



شکل ۱: مقدار RSSI دریافتی بر حسب تغییرات فاصله.

جدول ۱: حدود آستانه مربوط به تشخیص حملات مختلف.

No	Parameters	Values
۱	$Treshold_{RSSI}$ of All attacker	$۷٫۲\times۱۰^{-۷}$
۲	$Treshold_{IRP}$ of DoS attack	۰٫۱۵ Sec
۳	$Treshold_{PDR}$ of Sinkhole attack	۰٫۵
۴	$Treshold_{PDR}$ of Selectforward attack	۰٫۱۲
۵	$Treshold_{RMI}$ of HelloFlood attack	۰٫۱۵ Sec

است. علاوه بر این در اغلب موارد، مهاجم با توان بالایی ارسال بسته‌ها را انجام می‌دهد که از روی قدرت سیگنال دریافتی (RSSI)[1] نیز می‌توان آن را به شکل مؤثری شناسایی کرد. به جهت تعیین حد آستانه RSSI دریافتی، فرض کنید یک گره مفروض $S_۱$ با قدرت $P_.$ سیگنالی را ارسال کند. در این حالت مقدار RSSI دریافتی در گره i $(R_i^{S_۱})$ به صورت زیر خواهد بود

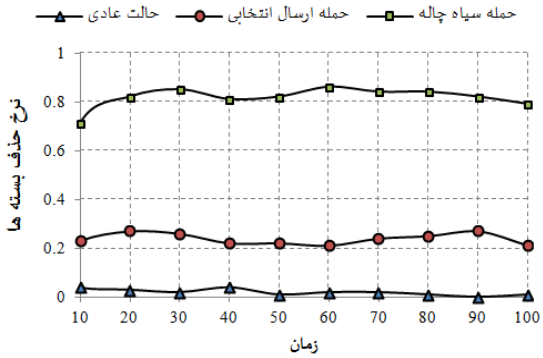
$$R_i^{S_۱} = P_. \times \frac{K}{d_i^{\alpha}} \qquad (۱)$$

در (۱) d_i فاصله اقلیدسی گره مفروض تا گره i، α فاکتور تضعیف سیگنال و K نیز یک ثابت است. در نمودار شکل ۱ تغییرات مقدار RSSI دریافتی بر حسب تغییرات فاصله بین گره‌های شبکه برای هر دو کلاس گره‌های عادی (کلاس ذره) و گره‌های قدرتمند (کلاس لپ‌تاپ) ارائه شده است. با توجه به اختلاف فاحش RSSI دریافتی بین گره‌های عادی شبکه با گره‌های مهاجم قدرتمند که در شکل ۱ آمده است، مقدار حد آستانه مربوط، قابل تعیین می‌باشد و در جدول ۱ نیز ارائه شده است.

تشخیص حمله سیل ارسال سلام: با توجه به این که در حمله سیل ارسال سلام، در اغلب موارد مهاجم یک گره خارجی با قدرت ارسال بالا است، می‌توانیم از طریق قدرت سیگنال دریافتی (RSSI) آن را شناسایی نماییم. همچنین با توجه به این که عملکرد این حمله موجب افزایش سربار مسیریابی می‌گردد (مراجعه شود به شکل ۱۶)، می‌توانیم با اعمال قانون فاصله زمانی در دریافت پیام‌های مسیریابی نیز آن را شناسایی نماییم. بر طبق فواصل زمانی معمول در پیام‌های مسیریابی در شبکه‌های حسگر، مقدار حد آستانه مربوط به آن تعیین می‌شود (۰٫۱۵ ثانیه) که در جدول ۱ ارائه شده است.

تشخیص حمله حفره چاهک و ارسال انتخابی: مهم‌ترین پارامتر در شناسایی این حملات بالارفتن نرخ حذف بسته‌هاست که گره‌های عادی از طریق عملیات شنود[2] می‌توانند آن را تشخیص دهند. بدین ترتیب اگر

1. Received Signal Strength Indicator
2. Overhearing Method



شکل ۲: نرخ حذف بسته‌ها در حالات مختلف شبکه.

نرخ حذف بسته‌ها از نرخ معمول بیشتر شود هشداری ایجاد و به سرخوشه ارسال می‌گردد. رابطه (۲) نحوه محاسبه نرخ حذف بسته‌ها را از طریق شنود نشان می‌دهد

$$Packet\ Drop\ Rate = ۱ - \frac{packets\ actualy\ forwarded}{packets\ to\ be\ forwarded} \qquad (۲)$$

با توجه به حاصل فرمول فوق و مقایسه آن با حدود آستانه می‌توان حمله‌های حفره چاهک و ارسال انتخابی را شناسایی نمود. به جهت تعیین حدود آستانه مربوط به نرخ حذف بسته‌ها، نمودار نرخ حذف بسته‌ها در سه حالت مختلف در شکل ۲ ترسیم شده است. همان طور که دیده می‌شود، نرخ حذف بسته‌ها در حملات سیاه‌چاله، ارسال انتخابی و حالت عادی شبکه اختلاف فاحشی با هم دارند که از آن می‌توان به جهت تعیین حدود آستانه استفاده کرد. بنابراین بر طبق شکل ۲ مقادیر آستانه نرخ حذف بسته‌ها در حملات سیاه‌چاله و ارسال انتخابی به ترتیب ۰٫۵ و ۰٫۱۲ تعیین می‌شوند که در جدول ۱ نیز ارائه شده است.

در حمله حفره چاهک با توجه به این که گره مهاجم معمولاً یک گره قدرتمند است می‌توان علاوه بر معیار فوق مهاجم را با توجه به قدرت سیگنال دریافتی نیز شناسایی کرد.

مهم‌ترین مشکل در عملیات شنود مصرف انرژی در گره‌های شنودکننده است که باعث کاهش عمر شبکه می‌گردد. بنابراین به جهت کاهش مصرف انرژی تا حد امکان، به‌جای این که هر گره همه پیام‌های محدوده تحت پوشش خود را شنود کند صرفاً به شنود پیام‌های ارسالی خود اکتفا می‌نماید. با این کار هر گره صرفاً به ارسال رو به جلوی پیام‌های خود از گره‌های همسایه مستقیمش نظارت خواهد کرد. با این کار هزینه انرژی عملیات شنود به حداقل رسیده و به‌صورت متوازن بین همه گره‌ها پخش خواهد شد.

تشخیص حمله سایبیل: مهم‌ترین خصوصیتی که بتوان بر اساس آن حمله سایبیل را شناسایی کرد این است که همه گره‌های سایبیل با شناسه‌های مختلف در یک مکان از شبکه قرار دارند چرا که همه آنها تحت کنترل یک گره مهاجم با یک سخت‌افزار یکتا هستند. با توجه به محاسبات سنگین مربوط به مکان‌یابی گره‌ها در شبکه، می‌توانیم صرفاً بر اساس ذخیره و مقایسه نسبت قدرت سیگنال دریافتی (RSSI) برای پیام‌های دریافت‌شده، حمله سایبیل را تشخیص دهیم. اگر ۲ گره $S_۱$ با توان ارسال $P_۱$ و $S_۲$ با توان ارسال $P_۲$ دارای فاصله یکسان از گره i باشند و نماد d_i^k فاصله اقلیدسی گره k از گره i باشد آن گاه داریم

$$d_i^{S_۱} = d_i^{S_۲} \qquad (۳)$$

حالا با توجه به (۱) و جایگذاری آن در (۳) داریم

```
Receive (alert);
If (Looking (alert, intrusion alert)) {
   Attacker_Count [Node-ID] ++;
   If (Attacker_Count [Node-ID] > Treshold_Alarm)
   {
      Insert (Blacklist, Node-ID);
      Propagate (Blacklist);
   }
}
```

شکل ۳: شبه‌کد عملیات سرخوشه.

جدول ۳: پارامترهای شبیه‌سازی حملات.

No	Parameters	Values
۱	Number of attacker	۱/۲/۳
۲	Initial Energy of nodes	۱۰ j
۳	Transfer rate of packets	Between ۰/۰۱ to ۰/۱ sec
۴	Attacker location	Random/manual

$$P_1 \times \frac{K}{R_i^{s_1}} = P_2 \times \frac{K}{R_i^{s_2}} \quad (۴)$$

$$\frac{P_1}{R_i^{s_1}} = \frac{P_2}{R_i^{s_2}} \quad (۵)$$

$$\frac{R_i^{s_1}}{R_i^{s_2}} = \frac{P_1}{P_2} \quad (۶)$$

رابطه (۶) نشان می‌دهد که اگر دو گره S_1 و S_2 با توان‌های ارسال P_1 و P_2 که در فاصله یکسانی از گره i هستند، پیام‌هایی را به آن ارسال کنند در این صورت نسبت RSSI دریافتی از آنها در گره i با نسبت توان‌های ارسالی از آنها برابر خواهد بود. بنابراین به جهت تشخیص حمله سایبیل کافی است که هر گره نسبت RSSI دریافتی از گره‌های مشکوک را محاسبه کرده و با مقایسه آن با مقادیر گره‌های همسایه خود تصمیم نهایی را اتخاذ نماید.

با توجه به مطالب ذکرشده در این بخش برای تشخیص حملات مختلف، به جهت تعیین حدود آستانه در سیستم تشخیص نفوذ پیشنهادی، بر اساس شبکه شبیه‌سازی‌شده با پارامترهای جداول ۲ و ۳، حدود آستانه مفروض نیز در جدول ۱ ارائه شده‌اند.

۳-۲ تشخیص نفوذ سطح دوم

تشخیص نفوذ پیشنهادی در سطح دوم که عملیات سرخوشه و تصمیم‌گیری نهایی است به این صورت عمل می‌کند که هر وقت پیامی مبنی بر هشدار وجود مهاجم از گره‌های دیگر به سرخوشه ارسال گردد، سرخوشه با به‌روزرسانی وضعیت هشدار صادرشده و مقایسه آن با حد آستانه، تصمیم‌گیری نهایی را انجام می‌دهد. در صورت تجاوز هشدارها از حد آستانه، گره مفروض به‌عنوان مهاجم شناسایی شده و آن را در لیست مهاجمان قرار می‌دهد و از طریق ارسال پیام به سایر گره‌های موجود در خوشه، لیست آنها را نیز به‌روزرسانی می‌نماید. این امر در شکل ۳ ارائه شده است.

۳-۳ بهبود دقت تشخیص به کمک اعتبارسنجی هشدارها

یکی از مشکلات سیستم‌های تشخیص نفوذ مبتنی بر همکاری گره‌ها، عدم ارزشیابی پیام‌های هشدار صادرشده از گره‌های مختلف در شبکه است که این امر موجب کاهش دقت تشخیص می‌گردد. به جهت غلبه بر

جدول ۲: پارامترهای شبیه‌سازی شبکه حسگر بی‌سیم.

No	Parameters	Values
۱	Number of nodes	۷۰/۱۰۰/۲۰۰/۵۰۰
۲	Size of network	۱۰۰×۱۰۰ m^2
۳	Routing protocol	AODV
۴	MAC protocol	۸۰۲/۱۱
۵	Type of traffic	CBR
۶	Packet size	۷۰ byte
۷	Number of Cluster	۲/۳/۴/۵
۸	Simulation Time	۱۰۰ sec
۹	Type of nodes	Mica۲
۱۰	Sensing Power	۰/۰۱۵ w
۱۱	Processing Power	۰/۰۲۴ w
۱۲	RX Power	۰/۰۲۴ w (۳v×۸mA)
۱۳	TX Power	۰/۰۳۶ w (۳v×۱۲mA)
۱۴	Initial Energy of nodes	۱ j
۱۵	Bandwidth of nodes	۲۸/۸ kbps
۱۶	Radio Propagation Model	Two Ray Ground
۱۷	Antenna Model	Omni Antenna

این مشکل ما از یک روش مبتنی بر اعتماد سبک بهره خواهیم برد به‌گونه‌ای که بتواند بر اساس سطح اعتماد گره‌ها، پیام‌های هشدار تولیدشده توسط آنها را ارزشیابی نماید. این ارزشیابی می‌تواند گره سرخوشه را در جهت تصمیم‌گیری نهایی خود در تشخیص گره‌های مهاجم و حملات یاری کند و دقت تشخیص‌های آن را نیز ارتقا دهد.

عملیات مبتنی بر اعتماد: سطح اطمینان یک گره به‌عنوان خصوصیت اعتماد تعریف می‌گردد. Tv_{XY} مقدار اعتماد گره Y است که توسط گره X محاسبه شده است. هر گره X برداری به جهت ارزیابی اعتماد گره‌های همسایه‌اش دارد که بردار اعتماد نامیده می‌شود و آن را با Tv_X نشان می‌دهیم

$$Tv_X = (Tv_{X,1}, Tv_{X,2}, \ldots, Tv_{X,N}) \quad (۷)$$

در (۷)، $Tv_{X,i}$ مقدار اعتماد iامین همسایه گره X را نشان می‌دهد. به جهت محاسبه و به‌روزرسانی بردارهای اعتماد موجود در گره‌های شبکه از تابع توزیع بتا استفاده می‌کنیم

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (۸)$$

در (۸)، Γ تابع گاما و $0 \le p \le 1$ و $\alpha, \beta > 0$ هستند. در واقع با استفاده از تابع توزیع بتا که به‌وسیله دو پارامتر α و β مشخص می‌گردد، می‌توانیم احتمالات پسین را برای وقایع دودویی ارائه کنیم. امید ریاضی احتمال توزیع بتا نیز به‌صورت زیر ارائه می‌شود

$$E(p) = \frac{\alpha}{\alpha+\beta} \quad (۹)$$

به جهت انطباق تابع بتا با عملیات محاسبه اعتماد گره‌ها در شبکه حسگر بی‌سیم، متغیر تصادفی p را به‌عنوان احتمال موفقیت تحویل بسته‌ها و تابع $f(p|\alpha,\beta)$ را نیز به‌عنوان احتمال این که p یک مقدار خاص دارد در نظر می‌گیریم. بنابراین امید ریاضی احتمال توزیع بتا یعنی $E(p)$ به‌صورت محتمل‌ترین مقدار p تفسیر می‌گردد که در شبکه حسگر به‌عنوان مقدار اعتماد گره‌ها در نظر گرفته می‌شود و پارامتر α به تعداد موفقیت‌آمیز تحویل بسته‌ها ($SPDs$) و β نیز به تعداد ناموفق تحویل بسته‌ها ($UPDs$) اشاره دارند. بنابراین با توجه به (۹) و استفاده از آن برای پیش‌بینی اعتماد در آینده داریم

```
Receive (alert);
If (Looking (alert, intrusion alert)) {
   Switch Trust_Level (Node (alert)) {
      case 'high': Attacker_Count [Node-ID] + = λ ;
      case 'medium': Attacker_Count [Node-ID] + = β ;
      case 'uncertain': Attacker_Count [Node-ID] + = δ ;
   }
   If (Attacker_Count [Node-ID] > TresholdAlarm) {
      Insert (Blacklist, Node-ID);
      Propagate (Blacklist);
   }
}
```

شکل ۴: شبه‌کد عملیات سرخوشه مبتنی بر اعتماد.

$$Tv_{X,i} = \frac{SPDs + 1}{SPDs + UPDs + 2}, \quad \text{where } SPDs, UPDs \geq 0 \qquad (10)$$

با توجه به این که (۱۰) برای محاسبه اعتماد گره‌های شبکه وابسته به عملیات شنود در گره‌ها است، بنابراین به‌طور کامل منطبق بر ماژول تشخیص نفوذ مبتنی بر خصوصیات در سطح اول می‌باشد و در نتیجه از لحاظ مصرف انرژی بسیار سبک است.

هر گره حسگر X، میانگین اعتماد گره‌های همسایه‌اش را توسط (۱۱) محاسبه می‌نماید

$$E(X) = \frac{\sum_{i=1}^{N} Tv_{X,i}}{N} \qquad (11)$$

همچنین مقادیر اعتماد گره‌ها توسط تابع نگاشت (۱۲) سطح‌بندی می‌شوند

$$Mp(Tv_{node}) = \begin{cases} high & 0.8 \leq Tv_{node} \leq 1 \\ medium & 0.5 \leq Tv_{node} < 0.8 \\ uncertain & 0.3 \leq Tv_{node} < 0.5 \\ low & 0 \leq Tv_{node} < 0.3 \end{cases} \qquad (12)$$

پس از محاسبه میانگین اعتماد، این میزان توسط رابطه فوق به یک سطح مشخص از اعتماد نگاشت می‌یابد. هر پیام انتقالی در شبکه نیز باید در سرآیند خود حاوی سطح اعتماد گره ارسال‌کننده باشد. در نهایت پیام‌های هشدار رسیده از گره‌های مختلف به گره سرخوشه، بر اساس سطح اعتماد گره‌های ارسال‌کننده آنها ارزیابی می‌شوند تا در عملیات تشخیص نفوذ تصمیم دقیق‌تری اتخاذ گردد.

در الگوریتم شکل ۴، $Node(alert)$ گره‌ای است که پیام هشدار را به سرخوشه ارسال کرده و $Node-ID$ نیز گره‌ای است که مشکوک به حمله در شبکه می‌باشد و پیام هشدار مربوط به آن است.

همان طور که در الگوریتم اصلاح‌شده در شکل ۴ مشاهده می‌شود، هر گاه یک پیام هشدار درباره نفوذ در گره‌ای به سرخوشه ارسال گردد، بر اساس سطح اعتماد گره هشداردهنده مقادیر مختلفی به شمارنده نفوذ آن افزوده خواهد شد. به عبارت دیگر هرچه سطح اعتماد گره هشداردهنده بالاتر باشد این پیام هشدار دارای اهمیت بالاتری بوده و به‌تبع آن مقدار بیشتری نیز به شمارنده تشخیص نفوذ افزوده می‌شود.

ما چهار پارامتر $(\varphi, \delta, \beta, \lambda)$ را برای چهار سطح مختلف اعتماد در گره‌ها ارائه کردیم که (۱۳) ارزش آنها را بر اساس سطح اعتماد نشان می‌دهد. برای مثال گره‌ای با سطح اعتماد بالا در صورت ارسال پیام هشدار به سرخوشه بالاترین اهمیت را دارد و به شمارنده نفوذ مقدار $\lambda = 1$ را اضافه می‌کند و گره‌ای با سطح اعتماد پایین، کمترین اهمیت را دارد و معمولاً مقدار ارزش آن $\varphi = 0$ است

$$Parameters: 0 \leq \varphi < \delta < \beta < \lambda \leq 1$$
$$Trust\ Levels: low\ uncertain\ medium\ high \qquad (13)$$

رابطه (۱۴) نحوه محاسبه شمارنده هشدار نفوذ برای یک گره مشکوک به حمله را بر اساس مقادیر (۱۳) نشان می‌دهد

$$Attacker\ Count(Node) = \sum_{i=1}^{n_1} \lambda + \sum_{j=1}^{n_2} \beta + \sum_{k=1}^{n_3} \delta + \sum_{p=1}^{n_4} \varphi \qquad (14)$$

در رابطه فوق مقادیر n_i به ترتیب تعداد هشدارهای رسیده از گره‌هایی با سطوح اعتماد مختلف بر اساس دسته‌بندی (۱۲) است. با این الگوریتم مبتنی بر اعتماد و با توجه به این که در گره سرخوشه متناسب با سطح اعتماد گره‌ها به پیام‌های هشدار آنها اهمیت می‌دهد، وضعیت دقت تشخیص بهبود خواهد یافت.

۴- شبیه‌سازی و ارائه نتایج

در این بخش ابتدا ما به شبیه‌سازی حملات لایه شبکه و مسیریابی می‌پردازیم که در بخش ۱ معرفی شده‌اند. در ادامه نیز به شبیه‌سازی سیستم تشخیص نفوذ پیشنهادی خود و ارائه نتایج به‌دست‌آمده از آن و مقایسه با کارهای دیگران خواهیم پرداخت.

۴-۱ شبیه‌سازی حملات در شبکه حسگر بی‌سیم

ما به جهت شبیه‌سازی‌های خود از شبیه‌ساز NS2 استفاده کرده‌ایم که به‌عنوان یکی از معتبرترین شبیه‌سازهای شبکه است. در این شبیه‌سازی، پارامترهای شبکه پایه خود را با توجه به ماهیت شبکه‌های حسگر بی‌سیم و نیازمندی‌های موجود و بررسی کاربردهای معمول در این شبکه‌ها تعیین کردیم که در جدول ۲ لیست کامل آنها همراه با مقادیر مربوط ارائه شده است.

با توجه به [۲۵] و [۲۶] و این که حملات لایه شبکه با ایجاد اختلال در فرایند مسیریابی، شبکه حسگر بی‌سیم را دچار مشکل می‌کنند، بنابراین به جهت شبیه‌سازی آنها در NS2 و اعمال رفتار و عملکرد آنها در شبکه حسگر بی‌سیم مفروض، با ایجاد تغییراتی در پروتکل مسیریابی گره‌های مهاجم که در فایل‌های AODV.h و AODV.cc قرار دارند، عملکرد مربوط به آنها را شبیه‌سازی نمودیم. در جدول ۳ پارامترهای مربوط به شبیه‌سازی حملات ارائه شده‌اند.

۴-۲ شبیه‌سازی سیستم تشخیص نفوذ پیشنهادی

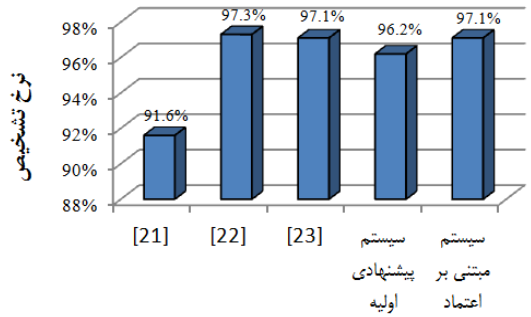
به جهت ارزیابی کارایی سیستم تشخیص نفوذ پیشنهادی، معیارهای زیر در نظر گرفته شده‌اند:

- **نرخ تشخیص:** نرخ تشخیص یا دقت تشخیص درصد حملات تشخیص داده شده را نسبت به کل حملات مشخص می‌نماید

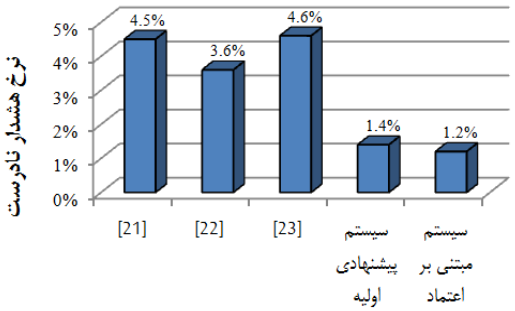
$$Detection\ Rate = \frac{No.\ of\ Detected\ Attacks}{No.\ of\ Attacks} \times 100\% \qquad (15)$$

- **نرخ هشدار نادرست:** این معیار نرخ هشدار نادرست را در تشخیص حملات نشان می‌دهد. به عبارت دیگر مشخص می‌کند که چه درصدی از حملات تشخیص داده شده حمله نبوده‌اند و سیستم تشخیص نفوذ اشتباهاً آنها را حمله تشخیص داده است

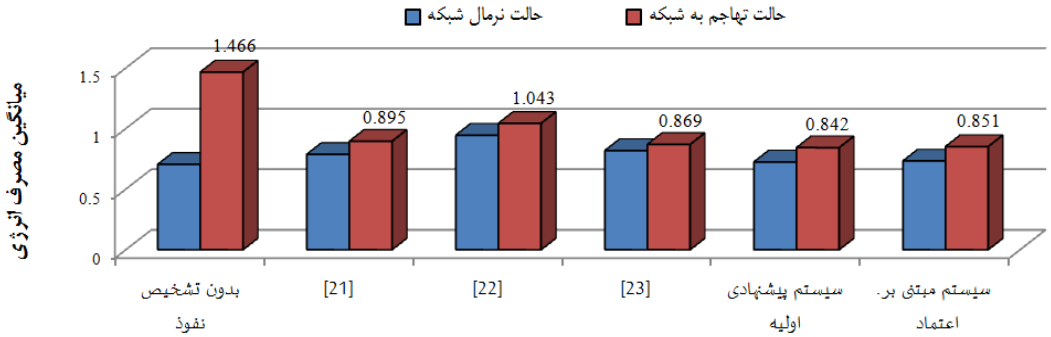
$$False\ positive\ Rate = \frac{No.\ of\ misdetected\ Attacks}{No.\ of\ Normal\ connections} \times 100\% \qquad (16)$$



شکل ۵: نمودار نرخ تشخیص حملات.



شکل ۶: نمودار نرخ هشدار نادرست.



شکل ۷: میانگین مصرف انرژی سیستم تشخیص نفوذ پیشنهادی و کارهای موجود.

- **میانگین مصرف انرژی:** این معیار میانگین انرژی مصرف‌شده در گره‌های شبکه را توسط تشخیص نفوذ پیشنهادی نشان می‌دهد

$$energy\ consump. = \frac{\sum_{i=1}^{nodes} Initial\ Energy_i - Residal\ Energy_i}{No.\ of\ nodes} \quad (17)$$

- **معیار تأخیر انتها به انتها در ارسال:** این معیار زمان صرف‌شده برای ارسال یک بسته در طول شبکه از مبدأ به مقصد است.
- **معیار گذردهی شبکه:** این معیار میزان داده‌های دریافت‌شده در کل شبکه را در واحد زمان بیان می‌کند

$$Throughput = \sum_{f=1}^{Max\ Flow} \frac{received\ pkts \times Pkt\ size \times 8}{flow\ time} \quad (18)$$

- **نرخ تحویل بسته‌ها:** این معیار میزان داده‌های دریافت‌شده را نسبت به داده‌های ارسال‌شده در کل شبکه مشخص می‌نماید و از تقسیم گذردهی شبکه بر نرخ ارسال ترافیک حاصل می‌شود

$$Packet\ Delivery\ Ratio = \frac{No.\ of\ received\ packets}{No.\ of\ sent\ packets} \times 100\% \quad (19)$$

- **سربار مسیریابی:** این معیار میزان سربار ناشی از مسیریابی داده‌ها را بین گره‌های شبکه حسگر بیان می‌کند

$$Normalized\ Routing\ Overhead = \frac{No.\ of\ Routing\ packets}{No.\ of\ Received\ packets} \quad (20)$$

- **نرخ حذف بسته‌ها:** این معیار درصد بسته‌های حذف‌شده را نسبت به کل بسته‌های ارسال‌شده تعیین می‌نماید

$$Packet\ Loss\ Ratio = \frac{Packet\ Loss}{No.\ of\ sent\ packets} \times 100\% \quad (21)$$

همچنین به جهت مقایسه مناسب روش پیشنهادی با کارهای موجود، از بستر یکسانی برای شبیه‌سازی همه روش‌ها استفاده کردیم که پارامترهای آن در جداول ۲ و ۳ ارائه شده است.

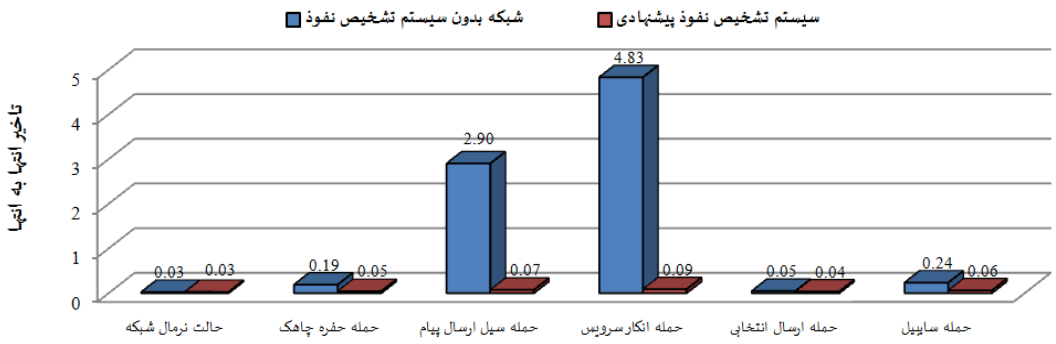
تحلیل نرخ تشخیص: همان طور که در شکل ۵ و ۶ مشاهده می‌شود نرخ تشخیص و نرخ هشدار نادرست در سیستم تشخیص نفوذ پیشنهادی با اصلاح انجام‌شده بر اساس سطح اعتماد بهبود یافته است.

همان طور که در شکل ۵ مشاهده می‌گردد، نرخ تشخیص سیستم پیشنهادی با میانگین ۹۷/۱٪ با اختلاف کمی بعد از [۲۲] قرار دارد. اما با توجه به نرخ هشدار نادرست خیلی پایین ۱/۲٪ روش پیشنهادی به نسبت مراجع دیگر که در شکل ۶ ارائه شده و همچنین میانگین مصرف انرژی کمتر نسبت به کارهای موجود در شکل ۷، سیستم پیشنهادی شرایط مطلوب‌تری را ارائه می‌نماید.

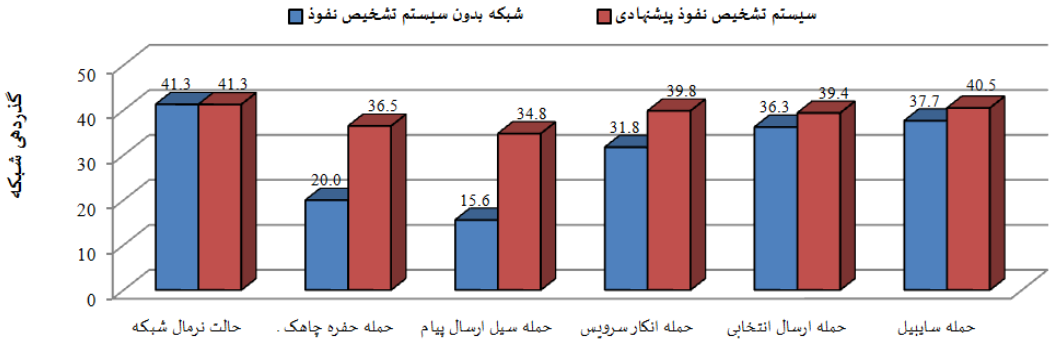
جدول ۴ نیز نرخ تشخیص و نرخ هشدار نادرست را در سیستم پیشنهادی اولیه و تشخیص نفوذ اصلاح‌شده بر اساس سطح اعتماد در مقایسه با کارهای موجود، به تفکیک حملات مختلف نشان می‌دهد.

تحلیل مصرف انرژی: مشخصاً یک سیستم تشخیص نفوذ در دو بخش پردازش و انتقال پیام‌ها انرژی مصرف می‌کند. مصرف انرژی در بخش پردازش الگوریتم تشخیص نفوذ با توجه به سبک‌بودن الگوریتم ارائه‌شده به دلیل استفاده از یک روش مبتنی بر خصوصیات ساده، بسیار ناچیز و قابل چشم‌پوشی است. در بخش انتقال پیام‌ها که مهم‌ترین بخش در مصرف انرژی است، سه عملیات ارسال، دریافت و شنود پیام‌ها هستند که دو عملیات ارسال و دریافت پیام‌ها مربوط به عملکرد عادی شبکه حسگر بی‌سیم بوده و تنها عملیات شنود مربوط به عملکرد سیستم تشخیص نفوذ است. با توجه به این که عملیات شنود نیز در هر گره صرفاً به بررسی اطلاعات ابتدایی سرآیند بسته‌های دریافتی می‌پردازد تا مشخص کند که گره‌های همسایه پیام‌های آن را انتقال می‌دهند، بنابراین حداقل انرژی در این عملیات مصرف خواهد شد.

رابطه محاسبه انرژی برای انتقال پیام‌ها در زیر ارائه شده است



شکل ۸: نمودار تأخیر انتها به انتها در سیستم تشخیص نفوذ پیشنهادی در برابر حملات مختلف و حالت عادی شبکه.



شکل ۹: نمودار گذردهی شبکه در سیستم تشخیص نفوذ پیشنهادی در برابر حملات مختلف و حالت عادی شبکه.

جدول ۴: مقایسه سیستم تشخیص نفوذ پیشنهادی با کارهای موجود به تفکیک حملات مختلف.

نوع حمله	سیستم پیشنهادی اولیه		سیستم مبتنی بر اعتماد		روش OWIDS [۲۱]		روش GHIDS [۲۲]		روش PLTIDS [۲۳]	
	نرخ تشخیص (٪)	نرخ هشدار نادرست (٪)	نرخ تشخیص (٪)	نرخ هشدار نادرست (٪)	نرخ تشخیص (٪)	نرخ هشدار نادرست (٪)	نرخ تشخیص (٪)	نرخ هشدار نادرست (٪)	نرخ تشخیص (٪)	نرخ هشدار نادرست (٪)
حمله انکار سرویس	۹۵/۶	۱/۲	۹۶/۱	۰/۹۴	–	–	–	–	۹۵/۴	۷/۴
حمله سیل ارسال سلام	۹۷/۵	۰/۹	۹۸/۲	۰/۸۶	۹۲/۷	۳/۴	۹۷/۲	۲/۲	۹۷/۶	۳/۱
حمله حفره چاهک	۹۴/۷	۱/۱	۹۵/۸	۱/۰۳	۹۳/۴	۴/۷	۹۶/۳	۳/۵	۹۸/۱	۲/۴
حمله ارسال انتخابی	۹۳/۸	۲/۳	۹۵/۷	۱/۸	۸۸/۹	۵/۶	۹۸/۴	۵/۱	۹۷/۳	۵/۶
حمله سایبیل	۹۹/۴	۱/۷	۹۹/۶	۱/۵	۹۱/۳	۴/۳	–	–	–	–

$$Energy\ Consump.(Q) = \frac{Power \times Elec.Current \times Packet\ Size}{Bandwidth} \quad (۲۲)$$

با توجه به این که طول پیام‌ها در شبکه حسگر ۷۰ بایت است که ۲ بایت اول سرآیند پیام، مربوط به گره بلافصل بعدی (گام بعدی) است و با جایگذاری مقادیر مربوط با پارامترهای (۲۲) با مقادیر موجود در جدول ۲ میزان مصرف انرژی برای ارسال، دریافت و شنود مشخص خواهد شد

$$\begin{aligned} Q_{Transmision} &= ۰/۶۹۹۹۵۵۲ \text{ mJ/message} \\ Q_{Reception} &= ۰/۴۶۶۶۳۶۸ \text{ mJ/message} \\ Q_{Listening} &= ۰/۰۱۳۳۳۲۴۷ \text{ mJ/message} \end{aligned} \quad (۲۳)$$

همان طور که از نتایج معلوم است، میزان مصرف انرژی در عملیات شنود نسبت به عملیات ارسال و دریافت پیام‌ها بسیار ناچیز است و بنابراین نشان‌دهنده مصرف انرژی بسیار پایین سیستم تشخیص نفوذ پیشنهادی و سبک‌بودن آن خواهد بود.

در ادامه به جهت ارزیابی دقیق انرژی مصرفی سیستم تشخیص نفوذ پیشنهادی، حالات مختلفی را در نظر گرفتیم که عبارتند از:

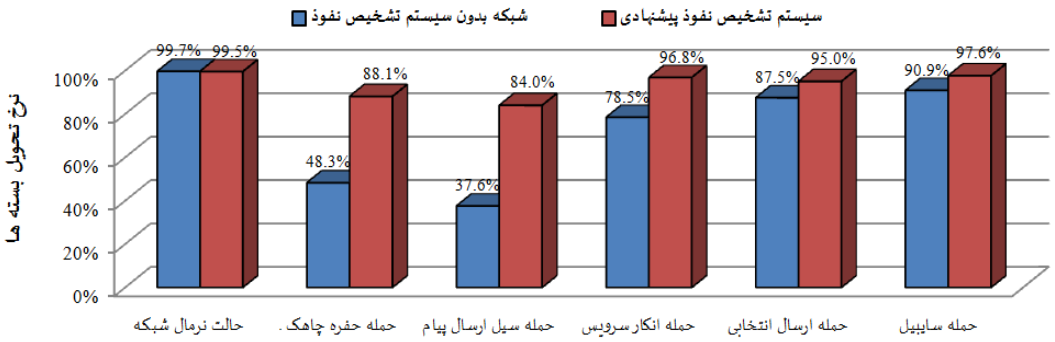
- شبکه بدون سیستم تشخیص نفوذ و بدون حضور حملات
- شبکه همراه با سیستم تشخیص نفوذ و بدون حضور حملات
- شبکه در حضور حملات و بدون سیستم تشخیص نفوذ
- شبکه در حضور حملات و همراه با سیستم تشخیص نفوذ

با مقایسه حالات فوق در شکل ۷ مشهود است که سیستم تشخیص نفوذ پیشنهادی سبک بوده و سربار ناچیزی را به شبکه تحمیل می‌نماید و همچنین به نسبت روش‌های موجود نیز کمترین میزان مصرف انرژی را دارا است که این امر در شبکه‌های حسگر بی‌سیم بسیار حایز اهمیت است.

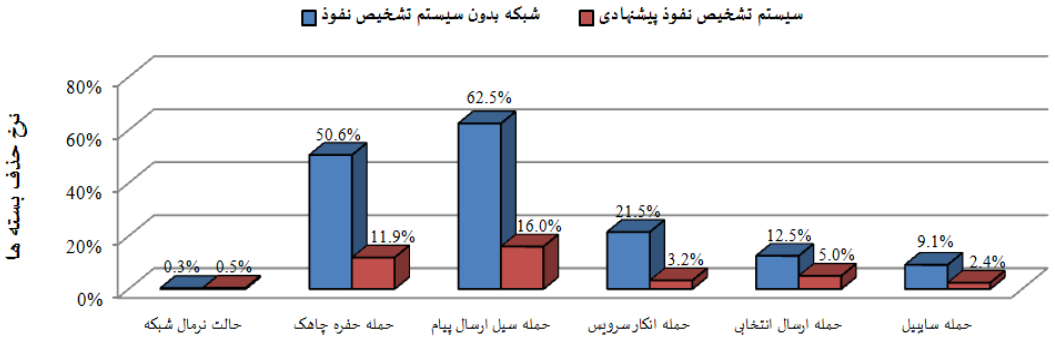
در شکل‌های ۸ تا ۱۲ نیز سیستم تشخیص نفوذ پیشنهادی بر اساس معیارهای مختلف کارایی در شبکه‌های حسگر بی‌سیم، به تفکیک حملات مورد ارزیابی قرار گرفته است. با توجه به شکل‌ها و با مقایسه حالات شبکه در حضور و عدم حضور سیستم تشخیص نفوذ پیشنهادی، مشاهده می‌گردد که حملات مختلف کارایی شبکه را به‌شدت تنزل می‌دهند و با به‌کارگیری تشخیص نفوذ پیشنهادی به خوبی می‌توان کارایی و عملکرد شبکه را در حد مطلوب حفظ کرد.

۵- نتیجه

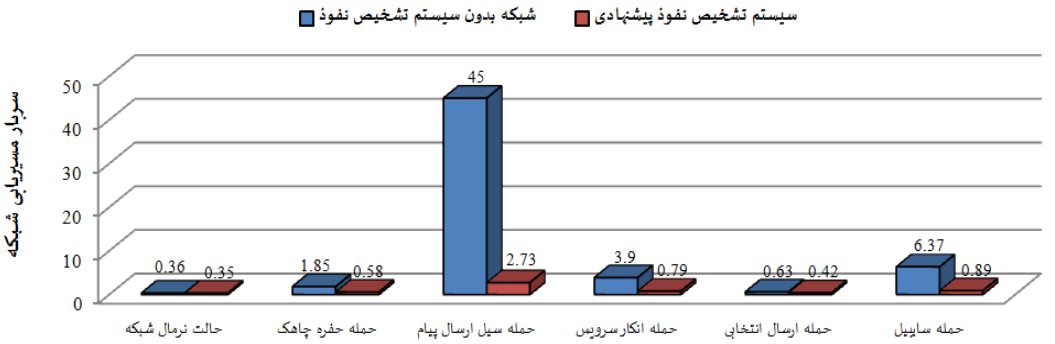
در این مقاله ابتدا حملات رایج بر روی شبکه‌های حسگر بی‌سیم معرفی شده و سپس انواع سیستم‌های تشخیص نفوذ موجود برای مقابله با



شکل ۱۰: نمودار نرخ تحویل بسته‌ها در سیستم تشخیص نفوذ پیشنهادی در برابر حملات مختلف و حالت عادی شبکه.



شکل ۱۱: نمودار نرخ حذف بسته‌ها در سیستم تشخیص نفوذ پیشنهادی در برابر حملات مختلف و حالت عادی شبکه.



شکل ۱۲: نمودار سربار مسیریابی شبکه در سیستم تشخیص نفوذ پیشنهادی در برابر حملات مختلف و حالت عادی شبکه.

آنها را مورد ارزیابی قرار دادیم. در ادامه یک سیستم تشخیص نفوذ سبک برای تشخیص حملات لایه شبکه و مسیریابی ارائه کردیم که در آن خصوصیات مربوط به حملات مختلف را بر اساس تحلیل رفتار آنها برای تشخیص در نظر گرفتیم. در ادامه با اصلاح عملیات سرخوشه‌ها از طریق یک سیستم مبتنی بر اعتماد که در بخش ۳-۳ تشریح گردید، عملکرد سیستم تشخیص نفوذ پیشنهادی را بهبود دادیم. سیستم مبتنی بر اعتماد پیشنهادی در مقایسه با کارهای موجود که اغلب بر روی یک حمله خاص تمرکز دارند، همه حملات لایه شبکه و مسیریابی را در شبکه‌های حسگر بی‌سیم پوشش می‌دهد. در انتها نیز سیستم پیشنهادی را با تمامی معیارهای کارایی مورد ارزیابی قرار دادیم. نتایج به‌دست‌آمده از شبیه‌سازی‌ها نشان می‌دهد که سیستم پیشنهادی با نرخ تشخیص بالای ۹۷٫۱ درصدی و نرخ هشدار نادرست پایین ۱٫۲ درصدی و همچنین میانگین مصرف انرژی کم ۰٫۰۲ ژول، به‌عنوان یک روش مؤثر و سبک برای شبکه‌های حسگر بی‌سیم مطرح است و با به‌کارگیری آن در شبکه‌های حسگر بی‌سیم، به خوبی می‌توان کارایی و عملکرد شبکه را در حد مطلوب حفظ نمود.

مراجع

[1] M. G. Ball, B. Qela, and S. Wesolkowski, "A review of the use of computational intelligence in the design of military surveillance networks," *Recent Advances in Computational Intelligence in Defense and Security*, vol. 621, pp. 663-693, Dec. 2015.

[2] D. He, N. Kumar, J. Chen, C. C. Lee, and N. Chilamkurti, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49-60, Feb. 2015.

[3] M. Li and H. J. Lin, "Design and implementation of smart home control systems based on wireless sensor networks and power line communications," *IEEE Trans. on Industrial Electronics*, vol. 62, no. 7, pp. 4430-4442, Jul. 2015.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[5] H. C. Qu, S. Jian, X. M. Tang, and P. Wang, "Hybrid computational intelligent methods incorporating into network intrusion detection," *J. of Computational and Theoretical Nanoscience*, vol. 12, no. 12, pp. 5492-5496, Dec. 2015.

[6] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52-73, Jun. 2009.

[7] G. Padmavathi and D. Shanm, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International J. of Computer Science and Information Security*, vol. 4, no. 1, pp. 1-9, Aug. 2009.

[8] Y. Maleh and A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor network," *International J. of Wireless & Mobile Networks*, vol. 5, no. 6, 12 pp., Dec. 2013.
[9] E. J. Kumar Patel and K. Tripathi, "Sinkhole attack detection and prevention in WSN & improving the performance of AODV protocol," *International J. of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 5, pp. 9660-9669, May 2016.
[10] V. C. Manju, "Sybil attack prevention in wireless sensor network," *International J. of Computer Networking, Wireless and Mobile Communications*, vol. 4, no. 2, pp. 125-132, Apr. 2014.
[11] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Computer Science*, vol. 79, pp. 700-707, 2016.
[12] M. A. Salam and N. Halemani, "Performance evaluation of wireless sensor networks under hello_flood attack," *International J. of Computer Networks & Communications*, vol. 8, no. 2, pp. 77-78, Mar. 2016.
[13] A. Liu, M. Dong, K. Ota, and J. Long, "PHACK-an efficient scheme for selective forwarding attack detection in WSNs," *Sensors*, vol. 15, no. 12, pp. 30942-30963, Dec. 2015.
[14] Y. Zhang, W. Lee, and Y. A. Huang, "Intrusion detection techniques for mobile wireless networks," *J. of Wireless Networks*, vol. 9, no. 5, pp. 545-556, Sept. 2003.
[15] A. Ghosal and S. Halder, "A survey on energy efficient intrusion detection in wireless sensor networks," *J. of Ambient Intelligence and Smart Environments*, vol. 9, no. 2, pp. 239-261, Feb. 2017.
[16] S. Duhan and P. khandnor, "Intrusion detection system in wireless sensor networks a comprehensive review," in *Proc. Int. Conf. on Electrical, Electronics, and Optimization Techniques, ICEEOT'16*, pp. 2707-2712, Chennai, India, 3-5 Mar. 2016.
[17] A. Abduvaliyev, S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223-1237, Third Quarter 2013.
[18] S. Shin, T. Kwon, G. Y. Jo, Y. Park, and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Trans. on Industrial Informatics*, vol. 6, no. 4, pp. 744-757, Nov. 2010.
[19] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: a repeated game theory approach," *International J. of Network Security*, vol. 5, no. 2, pp. 145-153, 2007.
[20] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *J. of High Speed Networks*, vol. 15, no. 1, pp. 33-51, Jan. 2006.
[21] C. F. Hsieh, R. C. Chen, and Y. F. Huang, "Applying an ontology to a patrol intrusion detection system for wireless sensor networks," *International J. of Distributed Sensor Networks*, vol. 10, no. 1, pp. 1-14, Jan. 2014.
[22] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047-1052, Jun. 2015.
[23] J. Wang, S. Jiang, and A. O. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors*, vol. 17, no. 6, Article 1227, May 2017.
[24] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," in *Proc. Int. Symp. on Networks, Computers and Communications, ISNCC'17*, 6 pp., Marrakech, Morocco, 16-18 May 2017.
[25] K. K. Waraich and B. Singh, "Performance analysis of AODV routing protocol with and without malicious attack in mobile adhoc networks," *International J. of Advanced Science and Technology*, vol. 82, no. 6, pp. 63-70, Sep. 2015.
[26] H. Ehsan and F. A. Khan, "Malicious AODV: implementation and analysis of routing attacks in MANETs," in *Proc. IEEE 11th Int. Conf. on Trust, Security and Privacy in Computing and Communications*, pp. 1181-1187, Liverpool, UK, 25-27 Jun. 2012.

مهدی صادقی‌زاده در سال ۱۳۸۴ مدرک کارشناسی خود را در مهندسی نرم‌افزار کامپیوتر از دانشگاه آزاد اسلامی مشهد و در سال ۱۳۸۸ مدرک کارشناسی ارشد خود را در مهندسی نرم‌افزار کامپیوتر از دانشگاه فردوسی مشهد دریافت نمود. در سال ۱۳۹۷ نیز موفق به اخذ درجه دکتری در مهندسی کامپیوتر گرایش هوش مصنوعی از دانشگاه صنعتی شاهرود گردید. موضوع پایان‌نامه دکتری ایشان، "یک معماری کارآ برای سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم" می‌باشد. ایشان از سال ۱۳۸۹ در گروه مهندسی کامپیوتر دانشگاه صنعتی قوچان مشغول به فعالیت گردید و اینک نیز عضو هیأت علمی این دانشگاه می‌باشد. زمینه‌های علمی و تحقیقاتی مورد علاقه ایشان عبارتند از: سیستم‌های تشخیص نفوذ، شبکه‌های حسگر بی‌سیم، سیستم‌های نهفته و بلادرنگ و امنیت شبکه‌های کامپیوتری.

امیدرضا معروضی تحصیلات خود را در مقاطع کارشناسی مهندسی برق گرایش الکترونیک و کارشناسی ارشد مهندسی برق گرایش مخابرات سیستم به‌ترتیب در سال‌های ۱۳۶۹ و ۱۳۷۲ از دانشگاه صنعتی شریف و در مقطع دکتری مهندسی برق گرایش مخابرات سیستم در سال ۱۳۸۵ از دانشگاه تربیت مدرس به پایان رسانده است و هم‌اکنون استادیار دانشکده مهندسی برق دانشگاه صنعتی شاهرود می‌باشد. نام‌برده قبل از پیوستنش به دانشگاه صنعتی شاهرود در سال‌های ۱۳۷۲ الی ۱۳۸۱ در مرکز تحقیقات راه‌آهن و شرکت خدمات انفورماتیک پروژه های تحقیقاتی متعددی را به انجام رسانده است. همچنین طی سال‌های ۱۳۸۲ الی ۱۳۸۵ در دانشگاه غیر انتفاعی سجاد مشهد مشغول تدریس بوده است. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: شبکه‌های مخابرات داده، مخابرات دیجیتال و شبکه‌های کامپیوتری.