شناسایی گره‌های سیبل در شبکه‌های حسگر بی‌سیم متحرک به کمک گره‌های ناظر

مجتبی جمشیدی[1]، مهدی اثنی عشری[2]، عدنان نصری[3]، علی حنانی[4]، محمدرضا میبدی[5]

[1] آموزشکده فنی و حرفه‌ای سما، دانشگاه آزاد اسلامی، واحد کرمانشاه، کرمانشاه، ایران jamshidi.mojtaba@gmail.com
[2] پژوهشکده فناوری اطلاعات، پژوهشگاه فضای مجازی، تهران، ایران esnaashari@aut.ac.ir
[3] دانشگاه آزاد اسلامی، واحد صحنه، گروه کامپیوتر، صحنه، ایران Adnan.nasri@gmail.com
[4] دانشگاه آزاد اسلامی، مرکز سنقر و کلیایی، گروه کامپیوتر، سنقر و کلیایی، ایران Ali_hanani@yahoo.com
[5] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران mmeybodi@aut.ac.ir

چکیده

با توجه به گسترش روزافزون شبکه‌های حسگر بی‌سیم در کاربردهای نظامی، محیط زیست، کنترل سلامت و ... ، برقرای امنیت در این شبکه‌ها یک موضوع بسیار مهم است. حمله سیبل یکی از حمله‌های خطرناک شناخته شده علیه این شبکه‌ها است که در آن یک گره بدخواه اقدام به انتشار چندین شناسه از خود می‌کند. این حمله می‌تواند پروتکل‌های مسیریابی و عملیاتی نظیر رأی‌گیری، تجمیع داده‌ها، تخصیص منابع و ... را تحت تأثیر قرار دهد. با توجه به حرکت گره‌ها در شبکه‌های حسگر متحرک، استفاده از الگوریتم‌های مبتنی بر تعیین مکان گره‌ها، الگوریتم‌های مبتنی بر RSSI و الگوریتم‌های مبتنی بر تعداد همسایه‌ها جهت شناسایی گره‌های سیبل با مشکل مواجه می‌شوند. در این مقاله، یک الگوریتم پویا، سبک وزن و کارا جهت شناسایی گره‌های سیبل در شبکه‌های حسگر متحرک مطرح می‌گردد. در الگوریتم پیشنهادی، گره‌های ناظر به کمک اطلاعات همسایگی در پریودهای زمانی مختلف اقدام به شناسایی گره‌های سیبل می‌کنند. الگوریتم پیشنهادی توسط شبیه‌ساز JSIM پیاده‌سازی گردیده و با انجام یک سری آزمایش‌ها، کارایی آن با دیگر الگوریتم‌های موجود مقایسه شده است. نتایج شبیه‌سازی‌ها حاکی از برتری الگوریتم پیشنهادی در مقایسه با دیگر الگوریتم‌های موجود در قالب معیارهای نرخ تشخیص و نرخ تشخیص غلط است. هم‌چنین، نتایج شبیه‌سازی‌ها نشان می‌دهد میانگین نرخ تشخیص و نرخ تشخیص غلط الگوریتم پیشنهادی به ترتیب ۹۹٪ و کمتر از ۲٪ می‌باشد.

کلمات کلیدی

شبکه حسگر، حمله سیبل، گره متحرک، گره ناظر

۱- مقدمه

شبکه‌های حسگر بی‌سیم نمونه‌ای از شبکه‌های موردی بی‌سیم هستند که حاوی صدها تا هزاران گره حسگر ارزان قیمت هستند. گره‌های حسگر دارای محدودیت‌هایی نظیر انرژی، حافظه، برد رادیویی و قدرت محاسباتی هستند. با توجه به این محدودیت‌ها و به دلیل ماهیت پخشی[1] ارتباطات بی‌سیم و مقاوم نبودن گره‌های حسگر در برابر مداخله[2] دشمن، برقراری امنیت در این گونه شبکه‌ها امری مهم و چالش‌زا است [1] [2].

یکی از حمله‌های مهم و تأثیر گذار بر لایه مسیریابی، حمله سیبل است. در این حمله، دشمن یا یک گره بدخواه در شبکه درج می‌کند یا یک گره نرمال درون شبکه را ضبط کرده، آن را برنامه‌ریزی مجدد نموده و تحت عنوان گره بدخواه در شبکه درج می‌کند. این گره بدخواه پس از گسترش در محیط، چندین شناسه از خود منتشر می‌کند که دشمن این شناسه‌ها را یا بطور جعلی می‌سازد و یا از شناسه‌های دیگر گره‌های نرمال در نواحی دیگر شبکه جعل می‌کند. به این شناسه‌های منتشر شده توسط گره بدخواه، اصطلاحاً گره‌های سیبل گفته می‌شود. گره بدخواه پس از گسترش در محیط، شناسه‌های سیبل را از خود منتشر می‌کند. این امر سبب می‌شود گره بدخواه ترافیک زیادی را به خود جلب کرده و به طور چشمگیری پروتکل‌های مسیریابی را مختل کند و حتی بر عملیاتی نظیر تجمیع داده‌ها، تخصیص منابع و رأی‌گیری تأثیر گذارد [3] [4].

تاکنون راه‌کارهای مختلفی جهت مقابله با حمله سیبل در شبکه‌های حسگر ثابت مطرح شده است. به عنوان مثال، در مرجع [5] یک الگوریتم مبتنی بر تست منبع رادیویی جهت شناسایی گره‌های سیبل مطرح شده است که در آن هر گره به هر یک از همسایه‌هایش یک کانال مجزا جهت مخابره اختصاص می‌دهد. با توجه به محدودیت‌های گره‌های حسگر این روش

نمی‌تواند کارامد باشد. هم‌چنین روش‌های مبتنی بر متدهای تصدیق هویت نظیر الگوریتم‌های ارائه شده در [5] و [6] معمولاً جهت ذخیره سازی اطلاعات ضروری تصدیق هویت(مثلاً کلیدهای رمزگذاری اشتراکی، گواهی‌نامه‌های هویت و ...) اولاً به فضای زیادی از حافظه نیاز دارند و ثانیاً درگیر پردازش الگوریتم‌های وارسی[3] پیچیده می‌شوند. هم‌چنین، الگوریتم‌های مبتنی بر قدرت سیگنال دریافتی(RSSI[4]) [7] نظیر الگوریتم مطرح شده در مرجع [8] نیز نمی‌توانند راه‌حل مناسبی باشند، چراکه از طرفی سیگنال رادیویی توسط محیط مستعد مداخله است و از طرف دیگر، گره بدخواه می‌تواند با تنظیم توان ارسال خود منجر به شکست این الگوریتم شود. هم‌چنین باید توجه شود تاکنون الگوریتم‌های زیادی جهت شناسایی گره‌های سیبل در شبکه‌های حسگر ثابت مطرح شده است که قابل بکارگیری در شبکه‌های حسگر متحرک نمی‌باشند. چرا که اکثر این الگوریتم‌ها یا مبتنی بر تعیین مکان گره‌ها می‌باشند یا مبتنی بر RSSI و یا با توجه به تعداد همسایه‌ها اقدام به شناسایی گره‌های سیبل می‌کنند. در حالی‌که، تحرک گره‌ها (اعم از سیبل و غیر سیبل) در شبکه‌های حسگر متحرک می‌تواند اجرای این الگوریتم‌ها را مختل کند.

از این‌رو، در این مقاله یک الگوریتم سبک وزن جدید جهت تشخیص گره‌های سیبل در شبکه‌های حسگر بی‌سیم متحرک به کمک گره‌های ناظر[5] ارائه می‌شود. الگوریتم پیشنهادی متکی بر تعیین مکان گره‌ها، RSSI و متدهای تصدیق هویت نبوده و فقط با نظارت بر ترافیک شبکه توسط گره‌های ناظر اقدام به شناسایی گره‌های سیبل می‌کند.

ادامه این مقاله بدین ترتیب سازماندهی می‌شود. کارهای گذشته در بخش ۲ آمده است. بخش‌های ۳ و ۴ به ترتیب فرضیات سیستم و الگوریتم پیشنهادی را شرح می‌دهند. ارزیابی سربار الگوریتم در بخش ۵ و نتایج شبیه‌سازی در بخش ۶ آمده است. بخش آخر نیز نتیجه‌گیری می‌باشد.

۲- کارهای گذشته

در این بخش به ارائه الگوریتم‌های موجود در دو بخش الگوریتم‌های مطرح جهت شناسایی گره‌های سیبل در شبکه‌های حسگر ثابت و متحرک می‌پردازیم.

۲-۱- الگوریتم‌های مطرح برای شبکه‌های حسگر ثابت

در [5] برای اولین بار به‌طور سیستماتیک حمله سیبل در شبکه‌های حسگر بی‌سیم تحلیل و مکانیزم‌هایی نظیر تست منبع رادیویی، پیش‌توزیع تصادفی کلیدها، مکانیزم ثبت نام شناسه و وارسی راه‌دور کد جهت مقابله با این حمله مطرح شد. در [8] الگوریتمی ارائه شده است که از مکانیزم تعیین مکان ارائه شده در [4] جهت شناسایی گره‌های سیبل استفاده می‌کند. در این الگوریتم از چهار گره مکان‌آگاه که توانایی شنود بسته‌ها از تمام نواحی شبکه را دارند استفاده شده است. هر گره‌ای که بسته‌ای را ارسال کند گره‌های مکان‌آگاه با همکاری هم‌دیگر مکان آن گره را تخمین می‌زنند و همین جهت شناسایی گره‌های سیبل کافی است چراکه گره‌های سیبل همگی در یک مکان واقع شده‌اند. در [9] یک الگوریتم برای شناسایی گره‌های سیبل ارائه شده که نیازی به سخت‌افزار یا اطلاعات مربوط به قدرت سیگنال ندارد و صرفاً از اطلاعات مربوط به تعداد همسایه‌ها جهت شناسایی گره‌های سیبل استفاده می‌کند. در [10] یک پروتکل جدید انتساب شناسه بر اساس رمزنگاری مبتنی بر شناسه ارائه شده است. این پروتکل از این نظر که به گره‌های بدخواه اجازه نمی‌دهد به راحتی شناسه جعلی کسب کنند، می‌تواند جهت مقابله با حمله سیبل بکار گرفته شود. در [11] نیز یک الگوریتم مبتنی بر مکانیزم RSSI جهت شناسایی حمله سیبل در شبکه‌های حسگری که از پروتکل Leach جهت کلاستربندی استفاده می‌کنند ارائه شده است. در [12] یک ارزیابی درستی بر اساس مکانیزم تشخیص زاویه ورود (AOA[6]) به نام TEBA[7] ارائه شده است. با توجه به این ویژگی که گره سیبل می‌تواند چندین شناسه ایجاد کند ولی فقط یک مکان فیزیکی دارد، گره راهنما شناسه‌های سیبلی که تفاوت فاز سیگنال آن‌ها کم‌تر از مقدار آستانه درستی[8](که به وسیله ارزیابی درجه درستی برای گره‌های حسگر مجاور محاسبه می‌شود) باشد را شناسایی می‌کند. در [13] روشی با استفاده از مدل کانال جک[9] ارائه شده است که در شبکه‌های حسگر مبتنی بر ساختار خوشه‌بندی عمل می‌کند. در [14] روش دیگری ارائه شده است که در آن از یک تکنیک مبتنی بر RSSI پیشرفته جهت شناسایی گره‌های سیبل استفاده می‌کند، به‌طوری که گره‌های بدخواه نتوانند با تنظیم توان انتقال خود از شناسایی توسط الگوریتم تشخیص در امان باشند. در [16] یک الگوریتم مبتنی بر کانال جک جهت مقابله با حمله سیبل در شبکه‌های مبتنی بر کلاستربندی Leach مطرح شده است. در [17] نیز یک الگوریتم دیگر مبتنی بر قدرت سیگنال دریافتی جهت شناسایی گره‌های سیبل در شبکه‌های حسگر ثابت ارائه شده است. در [18] یک الگوریتم مبتنی بر اتوماتاهای یادگیر و پازل‌های مشتری جهت شناسایی گره‌های سیبل در شبکه‌های حسگر ثابت مطرح شده است.

۲-۲- الگوریتم‌های مطرح برای شبکه‌های حسگر متحرک

در [15] یک الگوریتم جهت شناسایی گره‌های سیبل در شبکه‌های حسگر بی‌سیم متحرک ارائه شده است که با گروه‌بندی گره‌ها و با توجه به توان ارسالی بسته‌ها از سوی گره‌های عضو و هم‌چنین با توجه با تصادم‌های رخ داده، سرگروه‌ها اقدام به شناسایی گره‌های سیبل می‌کنند. در [19] یک روش مبتنی بر شناسه گره جهت شناسایی گره‌های سیبل در شبکه‌های حسگر متحرک ارائه شده است که فرایند تشخیص آن مبتنی بر ثبت‌نام گره در ایستگاه پایه می‌باشد و انتساب شناسه به گره‌ها به‌طور پویا صورت می‌گیرد. در [20] نیز یک الگوریتم دیگر جهت شناسایی گره‌های سیبل در شبکه‌های موردی متحرک ارائه شده است که تمرکز بر الگوریتم‌های مبتنی بر کلاستربندی دارد. در [21] نیز یک الگوریتم دیگر مبتنی بر گره‌های معتبر و نظارت بر تصادم‌ها در لایه MAC در جهت شناسایی گره‌های سیبل در شبکه‌های موردی متحرک مطرح شده است.

۳- فرضیات سیستم و مدل حمله

در این‌جا فرض می‌شود تعداد کل گره‌های شبکه $N=SN+ON$ می‌باشد (SN تعداد گره‌های حسگر معمولی و ON تعداد گره‌های ناظر). گره‌های حسگر معمولی مأموریت شبکه نظیر جمع‌آوری اطلاعات، ارسال داده‌ها به سمت ایستگاه پایه و ... را انجام می‌دهند و گره‌های ناظر به‌طور پریودیک ترافیک شبکه را نظارت کرده و گره‌های سیبل را شناسایی می‌کنند. تمام گره‌های حسگر (معمولی و ناظر) به طور تصادفی در یک ناحیه دوبعدی توزیع می‌شوند. گره‌های حسگر متحرک می‌باشند و در طول حیات شبکه مطابق مدل‌های تحرک، نظیر Random waypoint در محیط عملیاتی مورد نظر

حرکت می‌کنند. گره‌ها شناسه یکتا دارند و از موقعیت مکانی خود آگاه نیستند. گره‌ها با یکدیگر از طریق کانال رادیویی بی‌سیم مخابره و از انتشار به شیوه همه–جهته[10] استفاده می‌کنند. برد رادیویی تمام گره‌ها ثابت و برابر r می‌باشد. هم‌چنین فرض می‌شود گره‌های ناظر در صورت لزوم از الگوریتم‌های مسیریابی reactive چندگامه نظیر [22] جهت تولید مسیر بین خود استفاده می‌کنند تا بتوانند با یکدیگر مخابره کنند. هم‌چنین فرض می‌شود گره‌های حسگر معمولی در برابر مداخله مقاوم نیستند و دشمن در صورت ضبط یک گره می‌تواند به اطلاعات محرمانه آن دسترسی داشته باشد و آن را برنامه ریزی مجدد کند. این در حالیست که فرض می‌شود گره‌های ناظر سخت‌افزار مقاوم در برابر مداخله دارند و دشمن نمی‌توان آن‌ها را کدگشایی و برنامه‌ریزی مجدد کند.

مدل حمله در نظر گرفته شده در این‌جا بر اساس دسته‌بندی‌های صورت گرفته در مرجع [5]، حمله سیبل مستقیم[11]، همزمان[12] و شناسه‌های جعلی[13] می‌باشد. فرض می‌شود که شبکه ناامن است و گره‌ها ممکن است توسط دشمن ضبط شوند. به گره ضبط شده توسط دشمن، گره بدخواه و مابقی گره‌ها در شبکه را گره‌های نرمال می‌گوییم. هر گره بدخواه چندین شناسه (گره‌های سیبل) از خود منتشر می‌کند. هم‌چنین فرض می‌شود هر گره بدخواه حداقل T_{min} شناسه سیبل از خود منتشر می‌کند. گره‌های بدخواه نیز هم‌چون گره‌های حسگر معمولی در محیط عملیاتی متحرک می‌باشند. مطابق آن‌چه که در [9] آمده است، دشمن به دو حالت می‌تواند به کمک حمله سیبل عملیات شبکه را مختل کند. حالت اول این است که دشمن تعداد زیادی گره نرمال داخل شبکه را ضبط و تحت عنوان گره‌های بدخواه برنامه‌ریزی مجدد کرده و مجدداً آن‌ها را در شبکه وارد کند به‌طوری که هر گره بدخواه تعداد شناسه‌های سیبل اندکی (مثلاً ۲ یا ۳ عدد) از خود منتشر کند. در این حالت الگوریتم‌های امنیتی به سختی گره‌های سیبل را شناسایی می‌کنند و حتی بعضی الگوریتم‌ها نظیر الگوریتم ارائه شده در [9] ممکن است گره‌های سیبل را شناسایی نکنند. ولی برای دشمن سخت و زمان‌بر است که بخواهد تعداد زیادی گره نرمال داخل شبکه را ضبط، کدگشایی، برنامه‌ریزی مجدد و کنترل کند. حالت دوم این است که دشمن تعداد گره‌های نرمال کمتری را ضبط و تحت عنوان گره‌های بدخواه برنامه‌ریزی مجدد کند، به‌طوری که هر گره بدخواه تعداد شناسه‌های سیبل بیشتری از خود منتشر کند. ما نیز در الگوریتم پیشنهادی خود، هم‌چون الگوریتم ارائه شده در [9] فرض می‌کنیم دشمن حالت دوم را پیش می‌گیرد. گره‌های بدخواه نیز مانند گره‌های نرمال و ناظر در شبکه متحرک هستند. به علاوه، فرض می‌شود که هر گره، با رسیدن به یک مکان جدید باید یک پیغام "Hello" یا پیغام درخواست مسیر[14] و ... منتشر نماید. این عمل درواقع یکی از نیازمندی‌های شبکه‌های حسگر متحرک است تا هر گره بتواند در هر لحظه از زمان همسایه‌های جاری خود را شناسایی کرده، در صورت نیاز با آن‌ها کلیدهای امنیتی برپا کند، مخابره کند، جدول مسیریابی خود را ایجاد کند (و غیره)[21]. بدیهی است که در این صورت، هر گره بدخواه با ورود به یک مکان جدید در شبکه، باید به ازای تمام شناسه‌های سیبل خود یک پیغام "Hello" یا پیغام درخواست مسیر[15] و ... منتشر نماید (حمله سیبل مدل همزمان [5]). الگوریتم پیشنهادی ما از این نوع پیغام‌های منتشر شده از جانب گره‌ها جهت شناسایی گره‌های سیبل استفاده می‌کند.

۴- الگوریتم پیشنهادی

ایده اصلی الگوریتم پیشنهادی برگرفته از تعداد دفعات ظهور گره‌ها در مجاورت گره‌های ناظر است. همان‌طور که گفته شد، در الگوریتم پیشنهادی دو نوع گره حسگر (معمولی و ناظر) داریم. گره‌های حسگر معمولی که عملیات عادی شبکه نظیر جمع‌آوری اطلاعات، ارسال داده‌ها به سمت ایستگاه پایه و به‌طور کلی مأموریت شبکه را انجام می‌دهند و گره‌های ناظر که به‌طور پریودیک ترافیک شبکه را نظارت کرده و گره‌های سیبل را شناسایی می‌کنند. الگوریتم پیشنهادی در واقع از دو فاز تشکیل شده است. فاز نظارت بر ترافیک شبکه و فاز شناسایی گره‌های سیبل که هر دو فاز توسط گره‌های ناظر صورت می‌گیرد. در ادامه به شرح این دو فاز می‌پردازیم.

فاز اول: گره‌های حسگر پس از گسترش در محیط عملیاتی، شروع به ارسال بسته‌ها (بسته حاوی داده، بسته "Hello"، بسته درخواست مسیر و ...) و حرکت در محیط عملیاتی می‌کنند. هر گره ناظر در حافظه خود یک بردار n خانه‌ای، به نام history، دارد که تعداد دفعات حضور دیگر گره‌ها در همسایگی خود را در این بردار ذخیره می‌کند. به این ترتیب که هر گره ناظر، در هر دوره زمانی t، اگر گره‌ای مثل u در همسایگی آن واقع شده باشد، در بردار history خود یک واحد به فیلد متناظر با گره u اضافه می‌کند. دوره زمانی t به قدری بزرگ انتخاب می‌شود که رفتار تمام شناسه‌های سیبل مربوط به یک گره بدخواه، شامل انتقال داده، پیغام "Hello"، درخواست مسیر و ... مشاهده شود[21]. به عبارت دیگر فاصله زمانی t به قدری بزرگ انتخاب می‌شود که تمام شناسه‌های سیبل مربوط به یک گره بدخواه خود را آشکار کنند. با توجه به این‌که تمام گره‌های حسگر معمولی و سیبل پس از ورود به یک مکان جدید در شبکه، اقدام به ارسال بسته‌ها (نظیر بسته "Hello" و ...) می‌کنند، لذا اگر گره ناظری در آن مکان حضور داشته باشد ورود گره‌های جدید به آن مکان را در بردار history خود ثبت می‌کند. بنابر این پس از گذشت P دوره زمانی از حیات شبکه، گره‌های ناظر در بردار خود تعداد دفعاتی که دیگر گره‌ها در همسایگی آن‌ها ظاهر شده‌اند را خواهند داشت.

فاز دوم: پس از اجرای فاز اول، به منظور شناسایی گره‌های سیبل، هر گره ناظر u بردار history خود را پیمایش کرده و مجموعه‌هایی مجزا از شناسه گره‌ها (با توجه به تعداد دفعات حضور گره‌ها در همسایگی گره ناظر) ایجاد می‌کند، به طوری که هر مجموعه حاوی شناسه گره‌هایی خواهد بود که به تعداد برابری در همسایگی گره ناظر u حضور پیدا کرده باشند. گره ناظر سپس مجموعه‌هایی را که تعداد اعضای آنها بزرگتر یا مساوی T_{min} باشد به عنوان گره‌های مشکوک به سیبل در لیستی از مجموعه‌ها به نام Suspicious_list ذخیره می‌کند. چراکه فرض شد هر گره بدخواه حداقل T_{min} شناسه سیبل از خود منتشر می‌کند. برای هر گره ناظر، Suspicious_list حاوی مجموعه‌هایی خواهد بود که عضوهای آن‌ها مشکوک به سیبل هستند. با توجه به این‌که تمام گره‌های سیبل مربوط به یک گره بدخواه می‌باشند، لذا تعداد دفعات حضور آنها در همسایگی گره ناظر u برابر خواهد بود و از این‌رو همه گره‌های سیبل در یک مجموعه قرار خواهند گرفت. هم‌چنین، ممکن است برخی گره‌های نرمال نیز وجود داشته باشند که به تعداد برابر با گره‌های سیبل در همسایگی گره ناظر u حضور پیدا کرده باشند. در این صورت، مجموعه‌های موجود در Suspicious_list گره ناظر u علاوه بر شناسه گره‌های سیبل، حاوی شناسه گره‌های نرمالی نیز

خواهد. از این‌رو، اگر هر گره ناظر به‌طور مستقل تمام شناسه‌های موجود در Suspicious_list خود را به عنوان گره‌های سیبل علامت زند، نرخ تشخیص غلط بالا می‌رود.

جهت بالا بردن دقت تشخیص، گره‌های ناظر با همکاری یکدیگر اقدام به شناسایی گره‌های سیبل می‌کنند. به این صورت که گره‌های ناظر، Suspicious_listهای خود را برای همدیگر ارسال می‌کنند. گره‌های ناظر ابتدا به کمک یک الگوریتم مسیریابی reactive چندگامه، نظیر [22]، مسیرهایی بین خود ایجاد می‌کنند و سپس Suspicious_listها را بین خود مبادله می‌کنند. هر گره ناظر پس از دریافت تمام Suspicious_listها (از جانب دیگر گره‌های ناظر)، اقدام به شناسایی گره‌های سیبل می‌کند. به این صورت که، هر گره ناظر با عمل اشتراک‌گیری روی Suspicious_listهای دیگر گره‌های ناظر و خودش گره‌های سیبل را علامت می‌زند. عمل اشتراک‌گیری به این صورت می‌باشد که هر گره ناظر u، به ازای هر یک از مجموعه‌های موجود در Suspicious_list خودش، مثلاً Set_u^i، دیگر مجموعه‌ها در Suspicious_listهای دریافتی از دیگر گره‌های ناظر، مثلاً Set_v^j، را پیمایش نموده و چنانچه اشتراک این دو مجموعه بزرگتر یا مساوی $T_{\min}$ باشد، شناسه‌های حاصل از اشتراک این دو مجموعه را در Set_u^i می‌ریزد. پس از انجام این عملیات، اگر تعداد عضوهای باقی‌مانده از Set_u^i بزرگتر یا مساوی پارامتر $T_{\min}$ باشد، محتوای آن به مجموعه شناسه‌های سیبل گره ناظر u (به نام $Sybil_list_u$) اضافه می‌شود. گره u این عملیات را به ازای تمام مجموعه‌های خود در Suspicious_list تکرار می‌کند. در آخر، $Sybil_list_u$ حاوی شناسه‌هایی خواهد بود که گره ناظر u آنها را به عنوان سیبل تشخیص داده است. شکل (۱) شبه‌کد مربوط به هسته اصلی فاز دوم الگوریتم پیشنهادی را نشان می‌دهد.

```
node u for each Set_u^i in it's Suspicious_list Do
{
    for each node v Do
        for each Set_v^j in Suspicious_list_v Do
            if (Set_u^i ∩ Set_v^j ≥ T_min) then
                Set_u^i = Set_u^i ∩ Set_v^j
    if (Set_u^i ≥ T_min) then
        Sybil_list_u = Sybil_list_u ∪ Set_u^i
}
```

شکل (۱): شبه‌کد هسته اصلی فاز دوم الگوریتم پیشنهادی

۵- ارزیابی سربار الگوریتم پیشنهادی

سربار حافظه: از آن‌جا که الگوریتم پیشنهادی فقط توسط گره‌های ناظر اجرا می‌شود، لذا سربار حافظه فقط مربوط به گره‌های ناظر بوده و گره‌های عادی هیچ سرباری را از جانب الگوریتم پیشنهادی متحمل نمی‌شوند. در الگوریتم پیشنهادی، هر گره ناظر به یک فضای از مرتبه $O(SN)$ جهت ذخیره تعداد دفعات رویارویی با دیگر گره‌ها در بردار history خود نیاز دارد. هم‌چنین، در فاز تشخیص گره‌های سیبل (علامت زدن گره‌های سیبل)، هر گره ناظر نیاز دارد مجموعه‌هایی مجزا از شناسه گره‌ها ایجاد کند و هم‌چنین به‌طور موقت Suspicious_listهای خود و دیگر گره‌های ناظر را در حافظه خود ذخیره کند تا عمل اشتراک‌گیری روی Suspicious_listها صورت گیرد که در این مرحله سربار حافظه به $O(ON \times SN)$ می‌رسد. ولی از آنجا که پس از تشخیص گره‌های سیبل، گره‌های ناظر فضای مربوط به Suspicious_listها و مجموعه‌های مجزا را آزاد می‌کنند، می‌توان سربار حافظه تحمیلی الگوریتم پیشنهادی بر گره‌های ناظر را از مرتبه $O(SN)$ دانست. با توجه به این‌که گره‌های ناظر فقط وظیفه نظارت و شناسایی گره‌های سیبل را برعهده دارند و حافظه خود را برای دیگر عملیات‌ها در شبکه، نظیر تجمیع داده‌ها، کلاسترینگ و ... مصرف نمی‌کنند، لذا به اندازه کافی حافظه آزاد جهت ذخیره بردار history خواهند داشت.

سربار ارتباطات: فاز اول الگوریتم پیشنهادی هیچ سربار ارتباطات قابل ملاحظه‌ای بر شبکه تحمیل نمی‌کند و تنها سربار ارتباطات الگوریتم پیشنهادی مربوط به ارسال Suspicious_listها توسط گره‌های ناظر در فاز دوم است. هر گره ناظر باید Suspicious_list خود را به شیوه چندگامه به دست دیگر گره‌های ناظر برساند. با فرض این‌که قطر شبکه d باشد، هر گره ناظر باید با $(ON-1)\times d$ انتقال، Suspicious_list خود را به دست دیگر گره‌های ناظر برساند. از این‌رو، کل سربار ارتباطات تحمیلی به شبکه $(ON \times (ON-1) \times d)$ خواهد بود. البته لازم به ذکر است که الگوریتم پیشنهادی سربار ارتباطی مربوط به اجرای الگوریتم مسیریابی reactive جهت پیداکردن مسیر بین گره‌های ناظر را نیز خواهد داشت.

سربار محاسباتی: سربار محاسباتی الگوریتم پیشنهادی به فاز دوم الگوریتم بر می‌گردد. هر گره ناظر، ابتدا بردار history خود را پیمایش کرده و مجموعه‌هایی مجزا از شناسه گره‌ها ایجاد می‌کند که این عملیات با مرتبه زمانی $O(N)$ قابل انجام است (با داشتن یک فضای کمکی از مرتبه $O(N)$). سپس گره ناظر باید از بین این مجموعه‌های مجزا، مجموعه‌های مشکوک را انتخاب و به Suspicious_list خود اضافه کند که این مرحله نیز با مرتبه زمانی $O(N)$ قابل انجام است. در آخر، گره ناظر باید با توجه به Suspicious_listهای دیگر گره‌های ناظر و خودش، با عمل اشتراک‌گیری ذکر شده در شکل (۱)، گره‌های سیبل را شناسایی کند. با فرض این‌که Suspicious_list هر گره ناظر به‌طور میانگین حاوی k مجموعه باشد در این صورت هر گره ناظر در زمان $O(k^2 \times ON)$ عملیات اشتراک‌گیری و شناسایی گره‌های سیبل را انجام می‌دهد.

۶- نتایج شبیه‌سازی

الگوریتم پیشنهادی توسط نرم‌افزار شبیه‌ساز JSIM [24] شبیه‌سازی گردیده و با انجام یک‌سری آزمایش‌ها کارایی آن با دیگر الگوریتم‌های ارائه شده در مراجع [8,9,11,14,16,17,18] مقایسه شده است. معیارهای مورد ارزیابی عبارتند از:

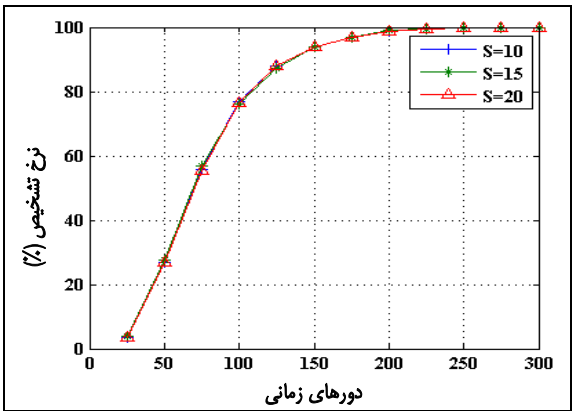
نرخ تشخیص: درصدی از گره‌های سیبل است که توسط یک الگوریتم امنیتی شناسایی می‌شود.

نرخ تشخیص غلط: درصدی از گره‌های نرمال است که به اشتباه توسط الگوریتم امنیتی به عنوان گره‌های سیبل شناسایی می‌شوند.

در اجرای شبیه‌سازی‌ها، فرض می‌شود که شبکه حاوی N گره حسگر است که به طور تصادفی در یک ناحیه ۱۰۰×۱۰۰ مترمربع پراکنده شده‌اند. ناحیه عملیاتی حاوی M=5 گره بدخواه می‌باشد که به طور تصادفی در محیط عملیاتی پراکنده می‌شوند. برای پارامتر T_{min} مقدار 10 در نظر گرفته شده

است. هر گره بدخواه به تعداد S شناسه جعل و از خود منتشر می‌کند. همه گره‌ها (نرمال و بدخواه) برد رادیویی یکسان و برابر ۱۰ متر دارند. هم‌چنین، ما از مدل حرکت در نظر گرفته شده در [23] جهت حرکت گره‌ها در محیط عملیاتی استفاده می‌کنیم. به منظور اطمینان از اعتبار نتایج، هر شبیه‌سازی ۱۰۰ بار تکرار شده و نتیجه نهایی از میانگین نتایج این ۱۰۰ تکرار بدست آمده است.

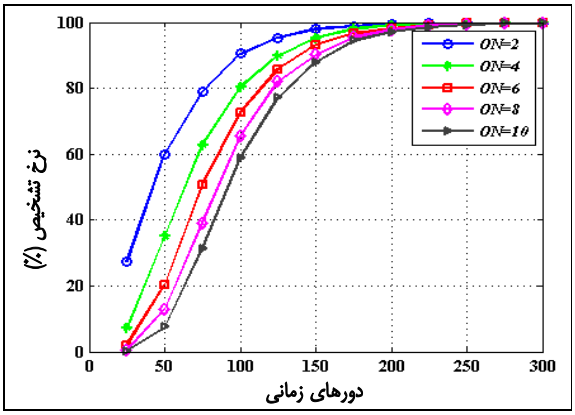
آزمایش ۱: هدف این آزمایش، ارزیابی الگوریتم پیشنهادی از نظر معیار نرخ تشخیص گره‌های سیبل است. در این آزمایش، تعداد گره‌های حسگر N=300 می‌باشد که از این تعداد، ۵ گره ناظر می‌باشند (یعنی ON=5). هم‌چنین، تعداد شناسه‌های سیبل منتشر شده توسط هر گره بدخواه را از ۱۰ تا ۲۰ (با گام افزایش ۵) تغییر داده و نرخ تشخیص گره‌های سیبل در الگوریتم پیشنهادی را برای دوره‌های زمانی ۲۵ تا ۳۰۰ ارزیابی کرده و نتایج بدست آمده را در شکل (۲) به تصویر کشیده‌ایم. نتیجه آزمایش نشان می‌دهد تغییر تعداد شناسه‌های سیبل تأثیری در نرخ تشخیص الگوریتم پیشنهادی نداشته و نرخ این معیار بعد از ۲۰۰ دوره زمانی، بالاتر از ۹۹٪ خواهد بود.



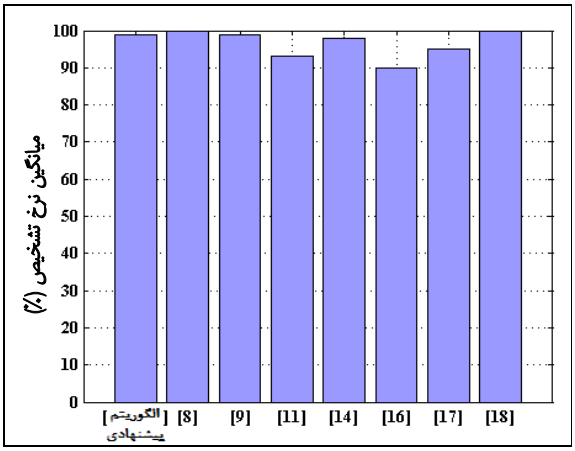
شکل (۲): نرخ تشخیص گره‌های سیبل الگوریتم پیشنهادی(برای مقادیر مختلف S)

آزمایش ۲: این آزمایش به بررسی تأثیر تعداد گره‌های ناظر بر نرخ تشخیص الگوریتم پیشنهادی می‌پردازد. در این آزمایش، S=20 و N=300 در نظر گرفته شده است و تعداد گره‌های ناظر را از ۲ تا ۱۰(با گام افزایش 2) تغییر داده و تأثیر آن بر نرخ تشخیص گره‌های سیبل در دوره‌های زمانی ۲۵ تا ۳۰۰ ارزیابی شده است. شکل (۳) نتیجه این آزمایش را نشان می‌دهد. همان‌طور که از نتیجه این آزمایش مشخص است، نرخ تشخیص الگوریتم پیشنهادی، به ازای مقادیر مختلف ON(تعداد گره‌های ناظر)، بعد از ۱۵۰ دوره زمانی، بالاتر از ۹۰٪ و بعد از ۲۰۰ دوره زمانی بالاتر از ۹۹٪ خواهد بود. نتیجه این آزمایش نشان می‌دهد نرخ تشخیص گره‌های سیبل با کاهش تعداد گره‌های ناظر، افزایش و بلعکس با افزایش تعداد گره‌های ناظر، نرخ این معیار کاهش می‌یابد. دلیل این موضوع این است که گره‌های ناظر با همکاری همدیگر و با انجام عمل اشتراک روی مجوعه‌های مجزا (Suspicious_listهای گره‌های ناظر) گره‌های سیبل را شناسایی می‌کنند. بنابر این هرچه تعداد گره‌های ناظر کمتر باشد، اشتراک مجوعه‌های مجزا حاوی تعداد بیشتری عضو خواهد بود که این سبب می‌شود هم نرخ تشخیص و هم نرخ تشخیص غلط (همان‌طور که در آزمایش ۳ آمده است) افزایش یابد. البته، بعد از ۲۰۰ دوره زمانی، به ازای مقادیر مختلف گره‌های ناظر، نرخ تشخیص بالاتر از ۹۹٪ می‌شود.

همچنین، در شکل (۴)، کارایی الگوریتم پیشنهادی و دیگر الگوریتم‌های موجود در قالب نرخ تشخیص ارائه گردیده است. همان‌طور که از شکل (۴) مشخص است، نرخ تشخیص گره‌های سیبل(در حالت میانگین) در الگوریتم‌های ارائه شده در [8]، [9] و الگوریتم پیشنهادی تقریباً ۹۹٪ و در الگوریتم [18] نرخ این معیار 100% می‌باشد. درحالی که، نرخ تشخیص الگوریتم‌های مطرح شده در [11]، [14]، [16] و [17] به ترتیب برابر ۹۳٪، ۹۸٪، ۹۰٪ و ۹۵٪ می‌باشد. نتیجه این مقایسه، کارایی مطلوب الگوریتم پیشنهادی در قالب معیار نرخ تشخیص گره‌های سیبل را نشان می‌دهد.



شکل (۳): تأثیر تعداد گره‌های ناظر بر نرخ تشخیص الگوریتم پیشنهادی

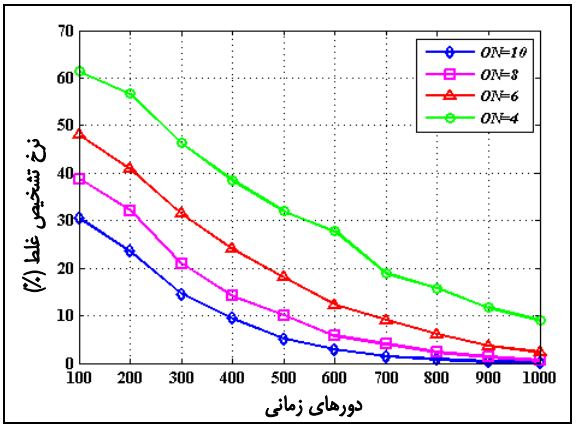


شکل (۴): میانگین نرخ تشخیص الگوریتم پیشنهادی و دیگر الگوریتم‌ها

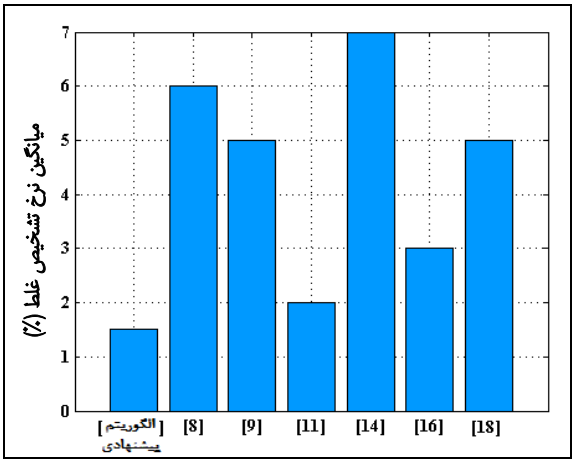
آزمایش ۳: هدف این آزمایش، ارزیابی نرخ تشخیص غلط الگوریتم پیشنهادی است. در این آزمایش نیز تعداد گره‌های حسگر N=300 می‌باشد. هم‌چنین، تعداد شناسه‌های سیبل منتشر شده توسط گره‌های بدخواه S=20 در نظر گرفته شده و گره‌های ناظر از ۴ تا ۱۰(با گام افزایش ۲) تغییر داده شده و تأثیر آن بر نرخ تشخیص غلط الگوریتم پیشنهادی در دورهای زمانی ۱۰۰ تا ۱۰۰۰ ارزیابی شده است. شکل (۵) نتایج این آزمایش را نشان می‌دهد. همان‌طور که از نتیجه آزمایش مشخص است، هرچه تعداد گره‌های ناظر بیشتر باشد، نرخ تشخیص غلط کاهش می‌یابد. چراکه گره‌های ناظر با همکاری یکدیگر و با عمل اشتراک‌گیری اقدام به شناسایی گره‌های سیبل می‌کنند. نتیجه آزمایش نشان می‌دهد که اگر تعداد گره‌های ناظر ON=10

باشد، بعد از ۵۰۰ دوره زمانی نرخ تشخیص غلط تقریباً ۵٪ و بعد از ۹۰۰ دوره زمانی نرخ این معیار تقریباً ۰٪ خواهد بود.

هم‌چنین، در شکل (۶) میانگین نرخ تشخیص غلط الگوریتم پیشنهادی و چند الگوریتم دیگر به تصویر کشیده شده است. میانگین نرخ تشخیص غلط الگوریتم‌های ارائه شده در [8]، [9]، [14]، [16] و [18] به ترتیب ۶٪، ۵٪، ۷٪ ، ۳٪ و ۵٪ می‌باشد، درحالی‌که میانگین نرخ این معیار در الگوریتم پیشنهادی برای ON=10 و دوره‌های زمانی بیشتر از ۶۰۰ کمتر از ۲٪ است که این حاکی از برتری الگوریتم پیشنهادی نسبت به دیگر الگوریتم‌ها از نظر میانگین نرخ تشخیص غلط است. هم‌چنین، میانگین نرخ تشخیص غلط الگوریتم ارائه شده در [11] برابر ۲٪ است.

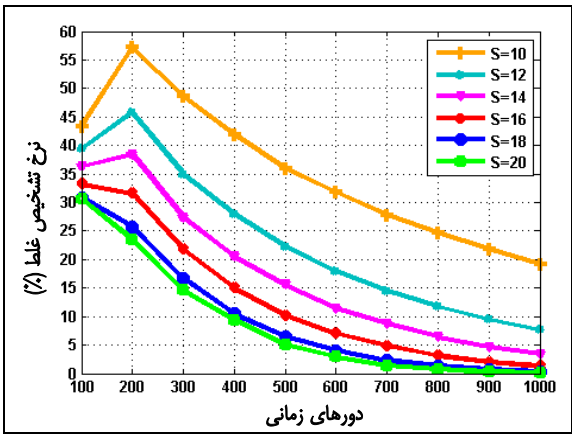


شکل (۵): تأثیر تعداد گره‌های ناظر بر نرخ تشخیص غلط الگوریتم پیشنهادی



شکل (۶): میانگین نرخ تشخیص غلط الگوریتم پیشنهادی و دیگر الگوریتم‌ها

آزمایش ۴: در این آزمایش به بررسی تأثیر تعداد شناسه‌های سیبل منتشر شده توسط گره‌های بدخواه، یعنی S، بر نرخ تشخیص غلط الگوریتم پیشنهادی می‌پردازیم. در این آزمایش، N=300 و ON=10 در نظر گرفته شده و تعداد شناسه‌های سیبل منتشر شده توسط هر گره بدخواه را از 10 تا 20 (با گام افزایش ۲) تغییر داده و تأثیر آن بر نرخ تشخیص غلط الگوریتم پیشنهادی برای دوره‌های زمانی ۱۰۰ تا ۱۰۰۰ ارزیابی نموده و نتایج حاصل را در شکل (۷) به تصویر کشیده‌ایم. همانطور که از نتیجه این آزمایش مشخص است، با افزایش تعداد شناسه‌های سیبل منتشر شده توسط گره‌های بدخواه، نرخ تشخیص غلط کاهش و بلعکس با کاهش تعداد شناسه‌های سیبل منتشر شده توسط گره‌های بدخواه، نرخ این معیار افزایش می‌یابد. دلیل این امر واضح است، هرچه تعداد شناسه‌های سیبل کمتر باشد، باتوجه به نحوه اشتراک‌گیری و شناسایی گره‌های سیبل که در فاز دوم الگوریتم پیشنهادی به شرح آن پرداختیم، تعداد شناسه‌های بیشتری ممکن است به اشتباه به عنوان سیبل تشخیص داده شوند. به هرحال، پس از گذشت ۵۰۰ دوره زمانی، نرخ تشخیص غلط برای حالتی که $S>18$ باشد، زیر ۵٪ و بعد از ۱۰۰۰ دوره زمانی، نرخ این معیار برای $S\geq12$ ، کمتر از ۱۰٪ می‌باشد. البته با افزایش تعداد دوره‌های زمانی، نرخ این معیار به ازای تمام مقادیر $S\geq10$ به سمت صفر میل می‌کند. به عنوان مثال، بعد از ۱۰۰۰ دوره زمانی، نرخ تشخیص غلط برای $S=18$ و $S=20$ به ترتیب ۰.۳٪ و ۰.۱٪ خواهد بود.



شکل (۷): تأثیر تعداد شناسه‌های سیبل، یعنی S، بر نرخ تشخیص غلط الگوریتم پیشنهادی

۷- نتیجه‌گیری

در این مقاله یک الگوریتم توزیعی، سبک وزن و کارا جهت شناسایی گره‌های سیبل در شبکه‌های حسگر بی‌سیم متحرک معرفی گردید. در این الگوریتم، گره‌های ناظر، در طی دوره‌های زمانی مختلف، تعداد دفعات رویارویی خود با دیگر گره‌ها را در یک بردار به نام history ثبت می‌کنند. جهت شناسایی گره‌های سیبل، گره‌های ناظر با همکاری همدیگر و بر اساس محتوای بردارهای history اقدام به شناسایی گره‌های سیبل می‌کنند. الگوریتم پیشنهادی شبیه‌سازی شده و با انجام یک سری آزمایش‌ها، کارایی آن با دیگر الگوریتم‌ها ارائه شده در [8,9,11,14,16,17,18] مقایسه گردید. نتایج آزمایش‌ها نشان دهنده عملکرد مطلوب الگوریتم پیشنهادی از نقطه نظر نرخ تشخیص و نرخ تشخیص غلط می‌باشد.

مراجع

[1] Akyildiz I. F., Su W., Sankarasubramaniam Y. and Cayircl E., "***A survey on sensor networks***", in: Proceedings of the IEEE Communication Magazine, Vol. 40, pp. 102-114, August 2002.

[2] Akyildiz Ian F. and Kasimoglu Ismail H., "***Wireless sensor and actor networks: research challenges***", in: Proceedings of the Ad Hoc Networks 2, pp. 351–367, 2004.

[3] Karlof C. And Wagner D, "***Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures***", in: Proceedings of the AdHoc Networks, pp. 299-302, year 2003.

[4] Padmavathi G. and shanmugapriya D, "***A survey of attacks, security mechanisms and Challenges in Wireless sensor networks***", in: Proceedings of the International Journal of

Computer Science And Information Security (IJCSIS), Vol. 4, No. 1 & 2, August 2009.

[5] Newsome J., Shi E., Song D. and Perrig A., "***The Sybil attack in sensor networks: analysis and defenses***", in: Proceedings of the International Symposium on Information Processing in Sensor Networks, pp. 259–268, April 2004.

[6] D. Liu, P. Ning, "***Establishing pairwise keys in distributed sensor networks***", in: Proceedings of the ACM Conference on Computer and Communications Security, pp. 52–61, October 2003.

[7] Zhong S., Li L., Liu Y. G. and Yang Y. R., ***"Privacy-preserving location based services for mobile users in Wireless Networks***", In: Proceedings of the Technical Report YALEU/DCS/TR-1297, Yale Computer Science, 2004.

[8] Demirbas M. and Song Y., "***An RSSI-based scheme for Sybil attack detection in wireless sensor networks***", In: Proceedings of the IEEE Computer Society International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 570–574, 2006.

[9] Ssu K. F, Wang W. T. and Chang W. C., "***Detecting Sybil attacks in wireless Sensor Networks using neighboring information***", in: Proceedings of the Computer Networks 53, pp. 3042–3056, 2009.

[10] Butler K. and et al., "***Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems***", in: Proceedings of the *IEEE transaction on parallel and distributed systems*, Vol. 20, 2009.

[11] Chen S., Yang G. and Chen S., "***A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks***", in: Proceedings of the International Conference on Communications and Mobile Computing, 2010.

[12] ZHANG Y., FAN K.-.F., ZHANG S.-B. and MO W., "***AOA based trust evaluation sheme for Sybil attack detection in WSN***", in: Proceedings of the journal on Application Research of Computers, 2010.

[13] Wang J., Yang G., Sun Y. and Chen S., "***Sybil attack detection based on RSSI for wireless sensor network***", in: Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2684–2687, September 2007.

[14] Misra S. and Myneni S., "***On Identifying Power Control Performing Sybil Nodes in Wireless ensor Networks Using RSSI***", in: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM 2010), pp. 1-4, Dec. 2010.

[15] Sharmila S., Umamaheswari G., "***DETECTION OF SYBIL ATTACK IN MOBILE WIRELESS SENSOR NETWORKS***", in: Proceedings of the INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY, Vol. 2, pp. 256 – 262 2012.

[16] Jangra A., Swati, Priyanka, "***Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS)***", in: Proceedings of the International Conferences on Advances in ICT for Emerging Regions(ICTer2011), 2011.

[17] Jiangtao W., Geng Y., Yuan S. and Shengeshou C., "***Defending Against Sybil Attacks Based on Received Signal Strength in Wireless Sensor Networks***", in: Proceedings of the journal of elctronics, Vol. 17,No. 4, Oct. 2008.

[18] Jamshidi, M., Esnaashari, M. and Meybodi, M. R., ***"An Algorithm for Defending Sybil Attacks based on Client Puzzles and Learning Automata for Wireless Sensor Networks"***, in: Proceeding of 18th National Conference of Computer Society of Iran , Sharif University, Tehran, Iran, March 14-16, 2013.

[19] Sharmilaa S., Umamaheswari G., "***Node ID based detection of Sybil attack in mobile wireless sensor network***", in: Proceedings of the International Journal of Electronics, 2012.

[20] Vasudeva1 A. and Sood M., "***SYBIL ATTACK ON LOWEST ID CLUSTERING ALGORITHM IN THE MOBILE AD HOC NETWORK***", in: Proceedings of the International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.

[21] Piro C., Shields C. and Levine B. N. , "***Detecting the Sybil Attack in Mobile Ad hoc Networks***", in: Proceedings of the *Securecomm and Workshops*, pp 1-11, 2006.

[22] Shah R. C. and Rabaey J., "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", in: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), pp. 17-21, 2002.

[23] Yu C. M., Lu C. S. , and Kuo S. Y., "***Mobile Sensor Network Resilient Against Node Replication Attacks***" In: Proceedings of the IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 2008.

[24] ***J-SIM Simulator***, http://www.j-sim.org.

زیرنویس‌ها

[1] broadcast
[2] Tamper
[3] verification
[4] Received Signal Strenght Indicator
[5] Observer
[6] Angle of Arrival
[7] Trust evaluation base on AOA
[8] Trust thershold
[9] Jakes Channel
[10] Omni-directional
[11] Direct
[12] Simultaneous
[13] Fabricated
[14] Roue request
[15] Roue request