بکارگیری پازل‌های مشتری و اتوماتاهای یادگیر جهت شناسایی گره‌های سیبل در شبکه‌های حسگر بی‌سیم

مجتبی جمشیدی[1]، مهدی اثنی‌عشری[2]، محمد رضا میبدی[3]

[1] دانشکده برق، رایانه و فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد قزوین، قزوین، ایران jamshidi.mojtaba@gmail.com
[2] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران esnaashari@aut.ac.ir
[3] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران mmeybodi@aut.ac.ir

چکیده

یک حمله مضر شناخته شده علیه شبکه‌های حسگر، حمله سیبل می‌باشد که در آن یک گره بدخواه چندین شناسه کسب و از خود منتشر می‌کند. این حمله به طور چشمگیری پروتکل‌های مسیریابی را مختل کرده و بر روی عملیاتی نظیر رأی‌گیری، تجمیع داده‌ها، ارزیابی اعتبار و ... اثرات ویران کننده می‌گذارد. در این مقاله، یک الگوریتم توزیعی و پویا مبتنی بر تئوری پازل‌های مشتری و مدل اتوماتای یادگیر جهت شناسایی گره‌های سیبل در شبکه‌های حسگر بی‌سیم ارائه می‌شود. شبیه‌سازی الگوریتم پیشنهادی با نرم‌افزار شبیه‌ساز JSIM صورت گرفته و نتایج شبیه‌سازی‌ها نشان می‌دهد که الگوریتم پیشنهادی قادر به شناسایی کامل گره‌های سیبل بوده و میزان تشخیص غلط آن در حالت میانگین کمتر از ٪۵ می‌باشد. هم‌چنین، با انجام یک سری آزمایش‌ها، کارایی الگوریتم پیشنهادی با دیگر الگوریتم‌های موجود مقایسه گردیده و نتایج حاصل، نشان دهنده کارایی بهتر الگوریتم پیشنهادی نسبت به دیگر الگوریتم‌ها از نظر معیارهای نرخ تشخیص و نرخ تشخیص غلط است.

کلمات کلیدی

شبکه‌های حسگر- گره سیبل- پازل‌های مشتری- اتوماتاهای یادگیر

۱- مقدمه

شبکه‌های حسگر بی‌سیم که معمولاً حاوی صدها یا حتی هزاران گره حسگر ارزان قیمت هستند، یک راه‌حل ایده‌ال برای کاربردهای مختلف نظارتی و تجسس، از جمله کنترل ترافیک، مراقبت بهداشتی، نظارت محیطی، دیده‌بانی میدان جنگ و ... می‌باشند. با توجه به محدودیت‌های گره‌های حسگر از نظر منابع (حافظه، قدرت محاسباتی، انرژی و ارتباطات)، گسترش بدون مراقبت[1] گره‌های حسگر در محیط عملیاتی و هم‌چنین ماهیت کاربردهای شبکه‌های حسگر بی‌سیم (خصوصاً کاربردهای نظامی و نظارت بر زیرساخت‌های بحرانی)، برقراری امنیت در این شبکه‌ها امری مهم و در عین حال مشکل می‌باشد.

یکی از حمله‌های خطرناک و تأثیر گذار در لایه شبکه (مسیریابی)، حمله سیبل[2] است. در حمله سیبل، یک گره قانونی ضبط شده توسط دشمن یا یک گره غیر قانونی درج شده در شبکه توسط دشمن، تحت عنوان گره بدخواه[3] چندین شناسه از خود منتشر می‌کند که به این شناسه‌های جعلی عموماً گره‌های سیبل می‌گویند. دشمن این شناسه‌ها را یا بطور جعلی می‌سازد و یا از شناسه‌های دیگر گره‌های قانونی در نواحی دیگر شبکه جعل می‌کند. در این حمله، از آن‌جایی که یک گره بدخواه چندین شناسه دارد، گره‌های همسایه آن گمان می‌کنند هر یک از این شناسه‌ها (گره‌های سیبل) مربوط به یک گره مستقل هستند [1,2]. از این‌رو، گره بدخواه می‌تواند ترافیک زیادی را به سمت خود جذب کرده و به طور چشمگیری پروتکل‌های مسیریابی را مختل، و حتی بر روی عملیاتی نظیر رأی‌گیری[4] [3-5]، تجمیع داده‌ها[5]، ارزیابی اعتبار[6] و ... اثرات ویران کننده بگذارد.

برای مقابله با این حمله، مکانیزم‌های حفاظتی مبتنی بر رویکرد رأی‌گیری و یا رویکرد اعتبار نمی‌توانند به طور مؤثر کار کنند، چراکه برخی از گره‌ها غاصب بوده و نمی‌توان به آن‌ها در جهت کسب اطلاعات قابل اطمینان، اعتماد کرد. روش‌های تصدیق هویت [2,6,7] نیز معمولاً جهت ذخیره‌سازی اطلاعات حیاتی تصدیق هویت (مثلاً کلیدهای رمزگذاری اشتراکی، گواهی‌نامه‌های هویت و ...) به فضای زیادی از حافظه نیاز دارند و درگیر پردازش الگوریتم‌های وارسی پیچیده می‌شوند. هم‌چنین، الگوریتم‌های مبتنی بر قدرت سیگنال دریافتی (RSSI[7]) [8] نیز نمی‌توانند راه‌حل مناسبی باشند، چراکه سیگنال رادیویی توسط محیط مستعد مداخله است و در نتیجه دقت تشخیص این گونه الگوریتم‌ها تحت تأثیر قرار خواهد گرفت.

در این مقاله، به کمک تئوری پازل‌های مشتری و مدل اتوماتای یادگیر یک الگوریتم توزیعی و پویا جهت شناسایی گره‌های سیبل پیشنهاد می‌گردد. از مزایای الگوریتم پیشنهادی می‌توان به پویایی، توزیع شدگی، دقت تشخیص بالا، عدم نیاز به گره‌های کنترلی خاص (نظیر گره‌های مکان‌آگاه یا ردیاب)، سخت‌افزار اضافی (نظیر GPS)، اطلاعات مکانی گره‌ها و روش‌های تصدیق هویت اشاره کرد.

ادامه مقاله بدین ترتیب سازماندهی می‌شود. بخش ۲ کارهای گذشته را معرفی می‌کند. بخش‌های ۳ و ۴ به ترتیب پازل‌های مشتری و اتوماتاهای یادگیر را شرح می‌دهند. در بخش ۵ فرضیات سیستم و مدل حمله و در بخش ۶ الگوریتم پیشنهادی آمده است. نتایج شبیه‌سازی و مقایسه نتایج با روش‌های دیگر در بخش ۷ آمده است. بخش نهایی مقاله، نتیجه گیری می‌باشد.

۲- کارهای گذشته

حمله سیبل برای اولین بار در [1] برای شبکه‌های نظیر به نظیر[۸] معرفی شد. سپس در [9] اشاره شد که این حمله می‌تواند برای الگوریتم‌های مسیریابی شبکه‌های حسگر نیز یک تهدید خطرناک باشد. در [2] برای اولین بار به‌طور سیستماتیک این حمله در شبکه‌های حسگر بی‌سیم تحلیل و مکانیزم‌هایی برای مقابله با آن مطرح شد. هم‌چنین در همین مقاله، دسته‌بندی‌های مفصلی از حمله سیبل صورت گرفته که مورد ارجاع بیشتر مقالات و محققان می‌باشد. در همین مقاله چندین مکانیزم برای تشخیص حمله سیبل معرفی شده است که عبارتند از: شناسایی گره‌های سیبل با استفاده از تست منبع رادیویی، شناسایی گره سیبل با استفاده از پیش‌توزیع تصادفی کلیدها، مقابله با حمله سیبل با استفاده از مکانیزم ثبت‌نام شناسه(registration) و رویکرد آخری که در این مقاله ارائه شده است وارسی راه‌دور کد یا تصدیق کد(Code Attestation) می‌باشد. Seshardi در [10] الگوریتمی به نام SWAtt ارائه کرده که به طور مطمئن، کد در حال اجرا روی یک دستگاه جاسازی‌شده راه‌دور را وارسی می‌کند. اگرچه این تکنیک به آسانی قابل بکارگیری در یک شبکه بی‌سیم نمی‌باشد ولی امید می‌رود در آینده نزدیک وارسی کد در شبکه‌های حسگر بی‌سیم امکان‌پذیر شود و به حل خیلی مسائل از جمله مقابله با حمله سیبل کمک کند. در [8] یک الگوریتم تعیین مکان، مبتنی بر RSSI ارائه شده است که از نسبت RSSIها از چند دریافت کننده، جهت تخمین موقعیت مکانی گره‌ها در شبکه استفاده می‌کند. در [11] یک الگوریتم مطرح شده که از مکانیزم تعیین مکان ارائه شده در [8] جهت شناسایی گره‌های سیبل استفاده می‌کند. در این الگوریتم از چهار گره مکان‌آگاه(گره ردیاب) استفاده می‌شود که توانایی شنود بسته‌ها از تمام نواحی شبکه را دارند. هر گره‌ای که بسته‌ای را ارسال کند گره‌های ردیاب با همکاری هم‌دیگر مکان آن گره را تخمین می‌زنند. همین امر جهت شناسایی گره‌های سیبل کافی است لذا گره‌های سیبل همگی در یک مکان واقع شده‌اند. در [12] یک روش دیگر برای شناسایی شناسه‌های سیبل ارائه شده که نیازی به سخت افزار یا اطلاعات مربوط به قدرت سیگنال نمی‌باشد و صرفاً از اطلاعات مربوط به تعداد همسایه‌ها استفاده می‌کند تا گره بدخواه و شناسه‌های جعلی(سیبل) را شناسایی کند. در [13] نیز یک الگوریتم دیگر جهت شناسایی حمله سیبل در پروتکل مسیریابی چندپخشی مبتنی بر مکان جغرافیایی ارائه شده است. در [14] نیز یک الگوریتم جهت شناسایی حمله سیبل در شبکه‌های حسگری که از پروتکل Leach جهت کلاستربندی استفاده می‌کنند ارائه شده است. در [15] مکانیزم دیگری ارائه شده است که در آن از یک تکنیک مبتنی بر RSSI پیشرفته جهت شناسایی گره‌های سیبل، هنگامی‌که گره‌ها توان انتقال خود را تنظیم می‌کنند استفاده می‌شود. در [16] روشی با استفاده از مدل کانال جک[۹] ارائه شده است که در شبکه‌های حسگر مبتنی بر ساختار خوشه‌بندی عمل می‌کند. در [17] روشی به منظور مقابله با حمله سیبل ارائه شده است که در آن اطلاعات مسیرها به وسیله الگوریتم هوش جمعی[۱۰] در طول فعالیت شبکه جمع آوری می‌شود و گره سیبل با توجه به تغییرات انرژی‌اش در طول فعالیت شبکه شناسایی می‌شود. یک راه‌حل دیگر برای تشخیص این حمله، بر اساس تفاوت زمانی ورود (TDOA[۱۱]) بین گره منبع و گره‌های راهنما[۱۲] در [18] مطرح شده است. این الگوریتم، وجود حمله سیبل و مکان گره‌های سیبل را تشخیص می‌دهد. در [19] یک ارزیابی درستی بر اساس مکانیزم تشخیص زاویه ورود (AOA[۱۳]) به نام TEBA 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 (که به وسیله ارزیابی درجه درستی برای گره‌های حسگر مجاور محاسبه می‌شود) باشد را شناسایی می‌کند.

۳- پازل‌های مشتری

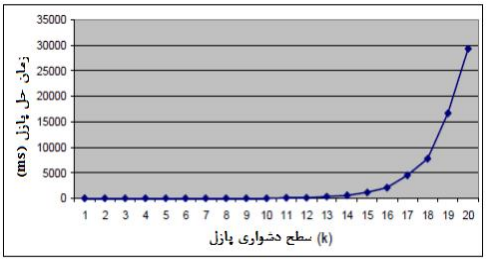
رویکردهای مبتنی بر پازل‌های مشتری توسط محققان، جهت مقابله با برخی حمله‌ها و مسائل امنیتی در شبکه‌های کامپیوتری مورد توجه قرار گرفته است. به عنوان مثال، در [20] الگوریتمی جهت مقابله با حمله "سیلاب پیغام Hello" و در [21,22] الگوریتم‌هایی جهت مقابله با حمله‌های تکذیب سرویس (DOS) ارائه شده که در تمامی این الگوریتم‌ها از پازل‌های مشتری به عنوان یک ابزار جهت حل مسئله مورد نظر استفاده شده است. در این رویکرد، قبل از تخصیص منابع به مشتری‌ها و یا مخابره با آن‌ها، سِرور از مشتری درخواست حل یک پازل را می‌کند. اگر مشتری بتواند پازل را درست حل کند، سِرور به آن مشتری منابع تخصیص می‌دهد و یا با آن مخابره می‌کند [20,21,22].

انتخاب معمول برای یک پازل مشتری، توابع درهم ساز معکوس‌پذیر، نظیر MD5 یا SHA1 می‌باشد، چرا که این توابع یک ساختار ساده دارند و می‌توانند بر روی انواع مختلفی از سخت‌افزارها اجرا شوند. پازلی که برای مشتری‌ها پخش می‌شود در واقع زوج $<<Ns,K>>$ می‌باشد که در آن، Ns نشانه[۱۴] سِرور(معمولاً ۶۴ بیتی و غیرقابل پیش‌بینی) و K سطح دشواری پازل است. مشتری باید به طور مرتب یک تابع درهم‌ساز را بر یک کمیت اعمال کند و زمانی پازل را حل شده پندارد که K بیت اول Y برابر 0 باشد: $h(id, Ns, Nc, X)=Y$

در این‌جا، h تابع درهم‌ساز رمزنگاری، نظیر MD5 یا SHA می‌باشد. پارامتر id شناسه مشتری، Nc نشانه تولید شده توسط مشتری و X حل پازل می‌باشد. از آن‌جا که سِرور به طور پریودیک Ns را تغییر می‌دهد، باید یک لیست از نمونه‌های درست حل شده را به

شکل زوج (Ns, Nc) نگه‌داری کند تا حل‌های قبلی نتوانند مجدداً استفاده شوند. این نشانه Nc دو هدف دارد. اول، اگر سرور از یک Ns استفاده مجدد کند (Nsی که در زمان قبل‌تر برای مشتری‌ها ارسال کرده بود را مجدداً ارسال کند)، مشتری می‌تواند با تولید یک Nc جدید، یک نمونه جدید از پازل را ایجاد کند. هدف دوم، جلوگیری از سوءاستفاده گره‌های بدخواه در شبکه است. بدون نشانه مشتری (Nc)، گره بدخواه احتمالی می‌تواند قبل از مشتری پازل را محاسبه و نتیجه را به سِرور برگشت دهد و درنتیجه سرور به این گره بدخواه منابع تخصیص دهد یا شروع به مخابره با آن کند. از آن‌جا که هیچ دانش میانبری جهت پیدا کردن X وجود ندارد، تنها راه ممکن، جستجو به روش ناشیانه (brute-force) می‌باشد.

پارامتر K در واقع میزان زمان مورد نیاز جهت حل پازل توسط مشتری را دیکته می‌کند. به عنوان مثال، اگر K برابر 0 باشد، هیچ کاری جهت حل پازل نیاز نیست، و اگر K برابر ۱۲۸ (برای MD5) یا ۱۹۲ (برای SHA) باشد، مشتری باید کل یک تابع یک‌راهه را معکوس کند که این از نظر محاسباتی غیرممکن است. سطح دشواری پازل، K، یک منحنی نمایی دارد. یعنی جهت حل یک پازل با سطح دشواری K، مشتری به طور میانگین نیاز به اجرای 2^k-1 عملیات دارد. با توجه به آزمایشات انجام شده در [22]، می‌توان تأثیر پارامتر K در مقدار زمان مورد نیاز جهت حل پازل را در شکل (۱) مشاهده کرد.



شکل (۱) زمان مورد نیاز جهت حل پازل با سطح دشواری‌های مختلف[22]

۴- اتوماتاهای یادگیر

یک اتوماتای یادگیر[23,24,25] یک ماشین با حالات محدود است که می‌تواند تعداد محدودی عمل را انجام دهد. هر عمل انتخاب شده، توسط یک محیط تصادفی ارزیابی شده و پاسخی به اتوماتای یادگیر داده می‌شود. اتوماتای یادگیر از این پاسخ استفاده نموده و عمل خود را برای مرحله بعد انتخاب می‌کند. در طی این فرآیند، اتوماتای یادگیر یاد می‌گیرد که چگونه بهترین عمل را از بین اعمال مجاز خود انتخاب کند. شکل (۲) ارتباط بین اتوماتای یادگیر و محیط را نشان می‌دهد.

محیط را می‌توان توسط سه‌تایی $E \equiv \{\alpha, \beta, c\}$ نشان داد که در آن $\alpha \equiv \{\alpha_1, \alpha_2, ..., \alpha_r\}$ مجموعه ورودی‌های محیط، $\beta \equiv \{\beta_1, \beta_2, ..., \beta_m\}$ مجموعه خروجی‌های محیط و $c \equiv \{c_1, c_2, ..., c_r\}$ مجموعه احتمال‌های جریمه می‌باشند. ورودی محیط یکی از r عمل انتخاب شده اتوماتا است. خروجی (پاسخ) محیط به هر عمل i توسط β_i مشخص می‌شود. اگر β_i یک پاسخ دودویی باشد، محیط مدل P[15] نامیده می‌شود. در چنین محیطی $\beta_i(n) = 1$ بعنوان پاسخ نامطلوب یا شکست و $\beta_i(n) = 0$ به عنوان پاسخ مطلوب یا موفقیت در نظر گرفته می‌شوند. به این ترتیب اتوماتای یادگیر تصادفی را می‌توان با چهارتایی $LA \equiv \{\alpha, \beta, p, T\}$ نشان داد که $\alpha \equiv \{\alpha_1, \alpha_2, ..., \alpha_r\}$ مجموعه عمل‌های اتوماتا (r تعداد عمل‌های اتوماتا)، $\beta \equiv \{\beta_1, \beta_2, ..., \beta_r\}$ مجموعه ورودی‌های اتوماتا، $p \equiv \{p_1, p_2, ..., p_r\}$ بردار احتمال عمل‌های اتوماتا و $T \equiv p(n+1) = T[\alpha(n), \beta(n), p(n)]$ الگوریتم یادگیری می‌باشد.



شکل (۲) اتوماتای یادگیر تصادفی[23]

اگر اتوماتای یادگیر در تکرار nاُم، یک عمل خود مانند α_i را انتخاب کند، تغییر احتمال عمل‌ها بصورت زیر خواهد بود(a پارامتر پاداش و b پارامتر جریمه می‌باشند):

الف- پاسخ مطلوب از محیط

$$p_i(n+1) = p_i(n) + a[1 - p_i(n)]$$
$$p_j(n+1) = (1-a)p_j(n) \qquad \forall j, \ j \neq i \qquad (۱)$$

ب- پاسخ نامطلوب از محیط

$$p_i(n+1) = (1-b)p_i(n)$$
$$p_j(n+1) = \frac{b}{r-1} + (1-b)p_j(n) \qquad \forall j, \ j \neq i \qquad (۲)$$

۵- فرضیات سیستم و مدل حمله

۵-۱- فرضیات سیستم

شبکه حسگر حاوی N گره حسگر است که به طور تصادفی در یک ناحیه دوبعدی توزیع می‌شوند. گره‌ها همیشه ساکن بوده و از موقعیت مکانی خود آگاه نیستند. شبکه همگن (همه گره‌های شبکه امکانات سخت‌افزاری و نرم‌افزاری برابری دارند) بوده و هر گره یک شناسه یکتا دارد. گره‌ها با یکدیگر از طریق کانال رادیویی بی‌سیم مخابره و از انتشار به شیوه همه-جهته[16] استفاده می‌کنند. تمام گره‌ها دارای برد رادیویی ثابت و برابر r می‌باشند. گره‌ها توانایی تولید پازل، بررسی صحت حل یک پازل و همچنین تنظیم سطح دشواری پازل را دارند. همچنین فرض می‌شود شبکه حسگر در یک محیط خصمانه گسترش می‌یابد، بنابر این، گره‌های حسگر در معرض ضبط فیزیکی توسط مهاجم می‌باشند. گره‌ها در برابر مداخله مقاوم نیستند و مهاجم در صورت ضبط یک گره می‌تواند به اطلاعات محرمانه آن دسترسی داشته باشد.

۵-۲- مدل حمله

در این مقاله، مطابق دسته‌بندی‌های صورت گرفته در [2]، مدل حمله سیبل مستقیم[17]، همزمان[18] و شناسه‌های جعلی[19] یا سرقتی[20] در نظر گرفته شده است. 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. قدرت و توانایی‌های گره‌های بدخواه با گره‌های نرمال برابر فرض می‌شود. هنگامی که یک گره، بسته‌ای را به هر یک از گره‌های سیبل ارسال می‌کند، بسته توسط گره بدخواه دریافت و در صورت نیاز پردازش و پاسخ داده می‌شود.

۶- الگوریتم پیشنهادی

ایده اصلی الگوریتم پیشنهادی برگرفته از این حقیقت است که چون شناسه‌های سیبل همگی مربوط به یک سخت‌افزار واحد هستند (یعنی همه گره‌های سیبل یک واحد حافظه، یک پردازشگر و یک فرستنده/گیرنده دارند)، لذا تمام پرسش‌ها و بسته‌های ارسالی گره‌های قانونی به گره‌های سیبل، فقط و فقط توسط یک واحد پردازشگر، پردازش و فقط توسط یک کانال ارسال و دریافت می‌شوند. از این‌رو، با توجه به فرض برابری قدرت گره‌های بدخواه و گره‌های نرمال، سرعت پاسخ‌گویی گره‌های سیبل در شرایطی که نیاز است تمام گره‌های سیبل همزمان عملی را انجام و پاسخ دهند، نسبت به دیگر گره‌های قانونی پایین‌تر خواهد بود.

الگوریتم پیشنهادی از این موضوع جهت شناسایی گره‌های سیبل استفاده می‌کند. به این ترتیب که، همه گره‌های قانونی به طور توزیعی، در طول حیاط شبکه (به‌طور پریودیک)، پازل‌هایی به همسایه‌های خود ارسال می‌کنند و منتظر پاسخ (حل پازل) از سوی همسایه‌ها می‌شوند. از آن‌جا که گره‌های سیبل دیرتر پاسخ می‌دهند، می‌توان آن‌ها را از گره‌های قانونی متمایز کرد. هم‌چنین، با توجه به این‌که ارسال و حل پازل‌ها باعث سربار محاسباتی، ارتباطی و در نتیجه افزایش انرژی مصرفی می‌شود، هر گره حسگر از یک اتوماتای یادگیر جهت کم کردن تعداد ارسال پازل‌ها به همسایه‌های خود بهره می‌گیرد که این امر سبب کاهش سربار محاسباتی، ارتباطی و انرژی مصرفی به میزان قابل توجهی خواهد شد. در ادامه به شرح جزئیات و مراحل این الگوریتم می‌پردازیم.

در الگوریتم پیشنهادی، هر گره حسگر v، در حافظه خود یک جدول همسایگی، مطابق شکل (۳)، دارد که در ستون Neighbor_ID شناسه گره‌های همسایه و در ستون Score، نمره‌ای که گره v به هر یک از این همسایه‌ها، در هر دور ارسال پازل، منتسب می‌کند ثبت خواهد شد. پس از گسترش گره‌ها در محیط عملیاتی، هر گره یک پیغام "Hello" منتشر می‌کند تا وجودش برای گره‌های همسایه آشکار شود. با این کار، هر گره، شناسه همسایه‌هایش را در جدول همسایگی ذخیره کرده و مقدار اولیه فیلد Score را برای همه آنها برابر با 0 قرار می‌دهد.

Neigbor_ID	Score

شکل (۳) ساختار جدول همسایگی

هم‌چنین، هر گره حسگر v مجهز به یک اتوماتای یادگیر (LA_v) با دو عمل ممکن است. عمل α_0 بیان‌گر عدم ارسال پازل توسط گره v به همسایه‌هایش در دور بعدی اجرای الگوریتم و عمل α_1 بیان‌گر ارسال پازل توسط گره v در دور بعدی اجرای الگوریتم می‌باشد. در واقع عمل α_0 نشان دهنده این است که گره‌های سیبل در همسایگی گره v قرار ندارند و دیگر لازم نیست گره v پازل به همسایه‌هایش ارسال کند. بالعکس، عمل α_1 بدین معنی است که احتمالاً گره‌های سیبل در همسایگی گره v وجود دارند و لذا گره v باید پازل‌هایی را به همسایه‌هایش ارسال کند تا با توجه به پاسخ‌های دریافتی، همسایه‌های سیبل را از همسایه‌های قانونی تمیز دهد. احتمال انتخاب عمل‌های اتوماتای یادگیر در ابتدا مساوی و برابر با ۰/۵ خواهد بود:

$$P = \left\{ \widetilde{0.5}^{Action0} \ , \ \widetilde{0.5}^{Action1} \right\} \qquad (۳)$$

اجرای الگوریتم به دوره‌های زمانی برابر تقسیم می‌شود. دور iام اجرای الگوریتم پیشنهادی با R_i نشان داده می‌شود. هر دوره زمانی در هر گره با فعال شدن اتوماتای یادگیر آن گره به صورت همزمان (با اتوماتاهای یادگیر دیگر گره‌ها) آغاز می‌شود. با فعال شدن اتوماتای یادگیر گره v در R_i (دور iام)، LA_v یکی از عمل‌های خود را به صورت تصادفی و بر اساس بردار احتمال عمل‌های خود انتخاب می‌نماید. در صورتی که عمل انتخابی α_1 باشد، گره v یک پازل به همسایه‌هایش ارسال می‌کند و منتظر برگشت حل آن توسط همسایه‌هایش می‌شود. گره‌های همسایه (گره‌های نرمال و در صورت وجود، گره‌های سیبل) با دریافت این پازل، باید آن‌را حل و نتیجه را برای گره v ارسال کنند. گره بدخواه، با دریافت یک پازل، ابتدا یکی از شناسه‌های سیبل خود را به تصادف انتخاب و پازل را به ازای آن حل و برگشت می‌دهد، سپس یکی دیگر از شناسه‌های سیبل انتخاب نشده را انتخاب و پازل را به ازای آن نیز حل و برگشت می‌دهد. گره بدخواه باید این فرایند را به ازای همه شناسه‌های سیبل خود تکرار می‌کند. گره v، زمان برگشت حل پازل‌ها (از سوی همسایه‌هایش) را در برداری در حافظه خود به نام *Result* ذخیره می‌کند. در دور R_{i+1}، گره v بردار *Result* خود (نتیجه ارسال پازل در R_i) را به همسایه‌هایش ارسال می‌کند، همسایه‌های گره v نیز، بردار *Result* مربوط به R_i خود را (در صورتی که در R_i عمل α_1 را انتخاب کرده باشند) برای v ارسال می‌کنند. گره v در انتهای دور R_{i+1}، با توجه به *Result* خود و همسایه‌هایش در دور قبلی (R_i)، ۱ واحد به/ از فیلد Score هر یک از همسایه‌هایش در جدول همسایگی اضافه/کم می‌کند. اگر درصد همسایه‌های با Score منفی بزرگتر از آستانه T_m باشد، LA_v به عمل α_1 (ارسال پازل) مطابق فرمول (۱) پاداش می‌دهد، در غیر این‌صورت مطابق فرمول (۲) این عمل را جریمه می‌کند. بدین ترتیب با گذشت زمان و افزایش تعداد دورهای اجرای الگوریتم، اتوماتای یادگیر هر گره v در شبکه یاد می‌گیرد که آیا گره‌های سیبل در همسایگی‌اش وجود دارد یا خیر. اگر وجود نداشته باشد، گره v دیگر پازلی به همسایه‌هایش ارسال نمی‌کند و این منجر به کاهش سربار ارتباطات و ذخیره انرژی در گره v و همسایه‌های آن می‌شود. هم‌چنین، گره v، با توجه به تعداد نمره‌هایی (مثبت و منفی)

که طی دورهای مختلف به همسایه‌هایش داده است، گره‌های سیبل را تشخیص می‌دهد.

هر گره در شبکه فقط آن دسته از همسایه‌هایش که دارای *Score* مثبت باشند را در پروتکل‌هائی نظیر مسیریابی، رأی‌گیری، تعیین اعتبار، تجمیع داده و ... مشارکت می‌دهد. به این ترتیب مانع از تأثیرگذاری گره‌های سیبل بر عملکرد پروتکل‌های شبکه می‌شود.

۷- نتایج شبیه‌سازی

به منظور ارزیابی عملکرد الگوریتم پیشنهادی، تعدادی آزمایش انجام گرفته و نتایج حاصل با نتایج به‌دست آمده از الگوریتم‌های ارائه شده در [11,12,14,15,17] مقایسه می‌گردد. سه معیار زیر به منظور ارزیابی مورد استفاده قرار گرفته‌اند:

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

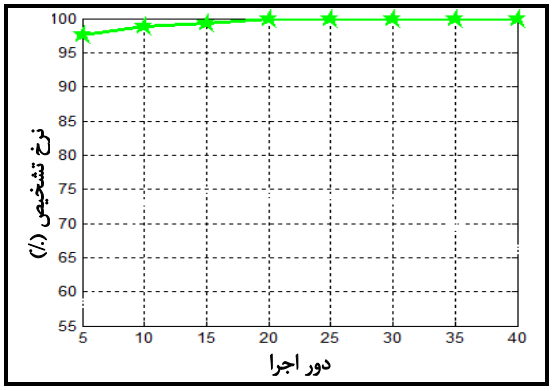
نرخ تشخیص غلط: یعنی درصدی از گره‌های نرمال که به اشتباه توسط الگوریتم امنیتی به عنوان گره‌های سیبل شناسایی شده باشند.

سربار ارتباطات، تعداد بسته‌هایی است که به دلیل استفاده از الگوریتم امنیتی مورد نظر در جهت شناسایی گره‌های سیبل به شبکه تحمیل می‌شود. در الگوریتم پیشنهادی، این معیار برابر است با تعداد پازل‌های ارسالی توسط کل گره‌های شبکه در یک دور از اجرای الگوریتم.

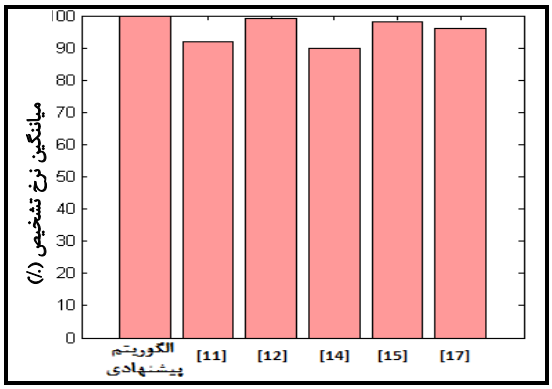
برای شبیه‌سازی محیط شبکه از نرم‌افزار شبیه‌ساز JSIM [26] استفاده شده است. در اجرای شبیه‌سازی‌ها، فرض می‌شود شبکه حاوی ۳۰۰ گره حسگر است که به طور تصادفی در یک ناحیه ۱۰۰×۱۰۰ مترمربع پراکنده شده‌اند. ناحیه عملیاتی حاوی ۱۰ گره بدخواه می‌باشد که به طور تصادفی پراکنده می‌شوند. هر گره بدخواه تعداد S شناسه جعل و از خود منتشر می‌کند. همه گره‌ها (نرمال و بدخواه) برد رادیویی یکسان و برابر ۱۰ متر دارند. هم‌چنین، سطح دشواری پازل‌ها K=10 در نظر گرفته شده است. 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: در این آزمایش کارایی الگوریتم پیشنهادی از نقطه نظر تشخیص گره‌های سیبل مورد بررسی قرار گرفته است. در این آزمایش، S=10، T_m=0.7 و پارامترهای پاداش و جریمه اتوماتاهای یادگیر با مقدار a=b=0.05 تنظیم شده و نرخ تشخیص گره‌های سیبل به ازای دورهای ۵ تا ۴۰ اجرای الگوریتم پیشنهادی ارزیابی شده است. شکل (۴) نتیجه این آزمایش را نشان می‌دهد. همان‌طور که از نتایج آزمایش مشخص است، نرخ تشخیص الگوریتم پیشنهادی از دور ۱۵ام به بعد ۱۰۰٪ خواهد بود. از آن‌جا که در هر دور اجرای الگوریتم، گره‌های بدخواه به ازای برخی از شناسه‌های سیبل مربوط به خود، پازل را به موقع حل و برگشت می‌دهند و هم‌چنین با توجه به این‌که ارسال پازل‌ها در هر دور اجرای الگوریتم بستگی به عمل انتخابی اتوماتای‌های یادگیر دارد (ممکن است در یک دور، برخی گره‌ها به همسایه‌های خود پازل ارسال نکنند)، از این‌رو، شناسایی ۱۰۰٪ گره‌های سیبل نیازمند چندین دور اجرای الگوریتم پیشنهادی است (در این آزمایش، ۱۵ دور).

شکل (۵) کارایی الگوریتم پیشنهادی و دیگر الگوریتم‌ها را از نظر متوسط نرخ تشخیص گره‌های سیبل نشان می‌دهد. نرخ تشخیص الگوریتم ارائه شده در [12] پایین‌تر از 100%، الگوریتم ارائه شده در [14] کمتر از 90%، الگوریتم ارائه شده در [17] کمتر از 96% و الگوریتم‌های ارائه شده در [11] و [15] به ترتیب و به طور میانگین در حدود 92% و 98% خواهد بود. از این‌رو، الگوریتم پیشنهادی در مقایسه با سایر الگوریتم‌های ذکر شده کارایی بالاتری در نرخ تشخیص گره‌های سیبل دارد. چرا که دیگر الگوریتم‌های مذکور اغلب یا از RSSI جهت تعیین مکان گره‌ها استفاده می‌کنند و چون سیگنال رادیویی مستعد مداخله محیط است لذا دقت تشخیص این گونه الگوریتم‌ها تحت تأثیر قرار خواهد گرفت، یا مبتنی بر بررسی سطح انرژی گره‌ها در شبکه و یا مبتنی بر فقط اطلاعات همسایگی هستند. در حالی که الگوریتم پیشنهادی نیازی به تعیین مکان گره‌ها و یا بررسی سطح انرژی گره‌ها ندارد و مبتنی بر سرعت پاسخ‌دهی گره‌هاست.



شکل (۴)نرخ تشخیص گره‌های سیبل در الگوریتم پیشنهادی

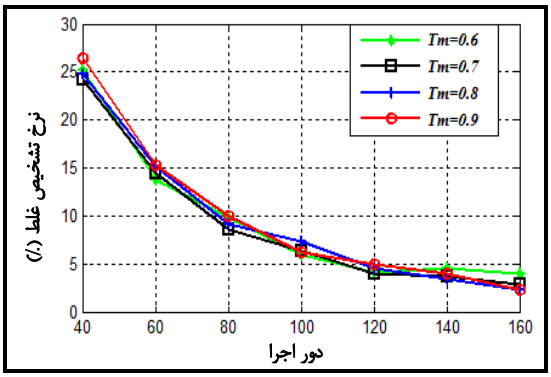


شکل (۵) مقایسه نرخ تشخیص گره‌های سیبل در الگوریتم پیشنهادی و دیگر الگوریتم‌ها

آزمایش ۲: این آزمایش به منظور بررسی نرخ تشخیص غلط الگوریتم پیشنهادی طراحی شده است. در این آزمایش، S=10، a=b=0.1 قرار داده شده و آستانه T_m از 0.6 تا 0.9 تغییر داده شده

است و تأثیر آن بر نرخ تشخیص غلط در دورهای 40 تا 160 اجرای الگوریتم پیشنهادی ارزیابی شده است. نتایج حاصل در شکل (۶) آمده است. همان‌طور که از شکل (۶) معلوم است، نرخ تشخیص غلط در دور ۴۰ام اجرای الگوریتم، به ازای مقادیر مختلف T_m تقریباً 25% بوده و با افزایش تعداد دورهای اجرای الگوریتم، این میزان به شدت کاهش پیدا خواهد کرد. به طوری که بعد از ۸۰ دور اجرا، نرخ تشخیص غلط کمتر از 10% و بعد از ۱۲۰ دور اجرای الگوریتم این نرخ به کمتر از 5% می‌رسد.

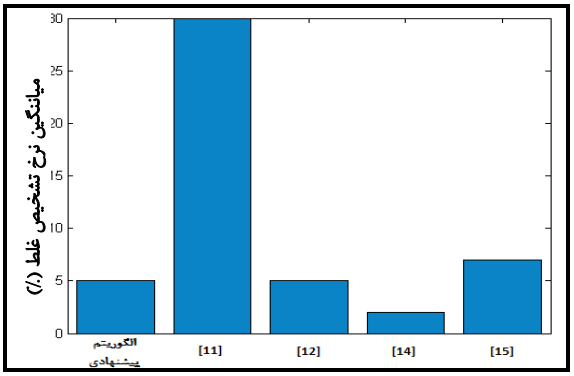
هم‌چنین، شکل (۷) مقایسه‌ای از میانگین نرخ تشخیص غلط در الگوریتم پیشنهادی و دیگر الگوریتم‌ها را نشان می‌دهد. همان‌طور که از نتیجه این مقایسه معلوم است، نرخ تشخیص غلط در الگوریتم پیشنهادی پایین‌تر از سایر الگوریتم‌ها به جز الگوریتم ارائه شده در [14] می‌باشد. البته در [14] فقط حالت خاصی از حمله سیبل در نظر گرفته شده است که در آن، گره بدخواه تلاش می‌کند تا به عنوان سرخوشه در الگویتم خوشه‌بندی LEACH انتخاب شود و چون شناسایی گره‌های سیبل توسط ایستگاه پایه صورت می‌گیرد لذا نرخ تشخیص غلط در این الگوریتم کمتر از الگوریتم پیشنهادی و دیگر الگوریتم‌هاست.



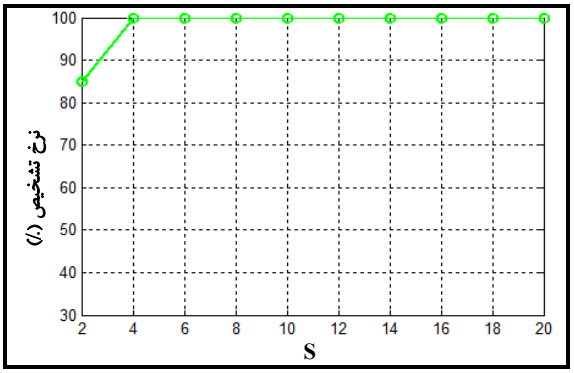
شکل (۶) نرخ تشخیص غلط الگوریتم پیشنهادی برای مقادیر مختلف T_m

آزمایش ۳: در این آزمایش، تأثیر تعداد شناسه‌های سیبل بر کارایی الگوریتم پیشنهادی در نرخ تشخیص و نرخ تشخیص غلط مورد ارزیابی قرار گرفته شده است. در این آزمایش، T_m=0.7، پارامترهای پاداش و جریمه اتوماتاهای یادگیر با مقدار a=b=0.05 تنظیم شده و تعداد شناسه‌های سیبل تولید شده توسط گره‌های بدخواه (یعنی S) از ۲ تا ۲۰ تغییر داده شده و تأثیر آن بر نرخ تشخیص و نرخ تشخیص غلط الگوریتم پیشنهادی ارزیابی شده است. نتایج این آزمایش بعد از ۱۰۰ دور اجرای الگوریتم پیشنهادی بدست آمده است. شکل‌های (۸) و (۹) نتایج حاصل از این آزمایش را نشان می‌دهند. همان‌طور که از شکل (۸) معلوم است، وقتی تعداد شناسه‌های سیبل بیش از ۲ عدد باشد، نرخ تشخیص 100% خواهد بود و در حالتی‌که تعداد شناسه‌های سیبل منتشر شده از سوی گره بدخواه، کمترین تعداد (یعنی ۲) باشد، نرخ تشخیص در الگوریتم پیشنهادی ۸۵٪ خواهد بود. چراکه، اگر گره بدخواه تعداد شناسه‌های سیبل کمتری از خود منتشر کند، سرعت پاسخ‌گویی و عکس‌العمل آن بالاتر خواهد رفت (هر پازل دریافتی را به تعداد کمتری حل و برگشت می‌دهد) و چون پازل‌ها را سریع‌تر حل و برگشت می‌دهد، دیرتر(یا اصلاً) شناسایی نمی‌شود.

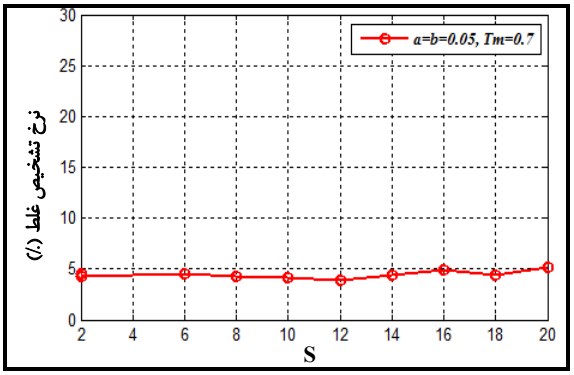
هم‌چنین، شکل (۹) نشان می‌دهد که افزایش و یا کاهش تعداد شناسه‌های سیبل تأثیر چندانی بر نرخ تشخیص غلط الگوریتم پیشنهادی ندارد و نرخ این معیار تقریباً کمتر از 5% می‌باشد. زیرا در الگوریتم پیشنهادی، مهم



شکل (۷) مقایسه نرخ تشخیص غلط الگوریتم پیشنهادی با دیگر الگوریتم‌ها



شکل (۸) تأثیر تعداد شناسه‌های سیبل بر نرخ تشخیص الگوریتم پیشنهادی

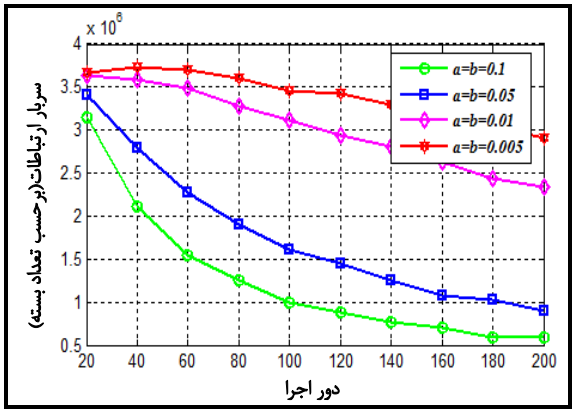


شکل (۹) تأثیر تعداد شناسه‌های سیبل بر نرخ تشخیص غلط الگوریتم پیشنهادی

این در حالیست که تعداد شناسه‌های سیبل تأثیر زیادی بر نرخ تشخیص و نرخ تشخیص غلط اکثر الگوریتم‌های ارائه شده دارد. به عنوان مثال، هنگامی که تعداد شناسه‌های سیبل ۱۰ عدد باشد، نرخ تشخیص و تشخیص غلط الگوریتم ارائه شده در [12] به ترتیب کمتر

از 99.2% و بیش از 14% می‌باشد، در حالی که این میزان در الگوریتم پیشنهادی به ترتیب 100% و کمتر از 5% است.

آزمایش ۴: در این آزماش، میزان سربار نسبی ارتباطات الگوریتم پیشنهادی مورد ارزیابی قرار گرفته است. در این آزمایش، S=10، T_m=0.7 می‌باشد و تأثیر مقادیر مختلف پارامترهای پاداش (a) و جریمه (b) اتوماتاهای یادگیر بر میزان سربار ارتباطات الگوریتم پیشنهادی مورد ارزیابی قرار گرفته است. شکل (۱۰) نتایج حاصل از این آزمایش را نشان می‌دهد. همان‌طور که از نتیجه این آزمایش مشخص است، مقدار پارامترهای پاداش و جریمه تأثیر زیادی بر میزان سربار ارتباطات دارد. a و b کوچکتر سبب کاهش سربار ارتباطات می‌شود چراکه سریع‌تر احتمال عمل ۱ (ارسال پازل) اتوماتای یادگیر را به مقدار ۱ می‌رساند و در نتیجه تعداد پازل‌های کمتری در شبکه منتشر می‌شود که این سبب کاهش سربار ارتباطات می‌شود. هم‌چنین، با افزایش تعداد دورهای اجرای الگوریتم، میزان سربار ارتباطات کاهش می‌یابد، چرا که اتوماتاهای یادگیر یاد می‌گیرند که فقط در نواحی که حمله سیبل وجود دارد گره‌ها اقدام به ارسال پازل کنند.



شکل (۱۰) تأثیر پارامترهای پاداش و جریمه بر میزان سربار نسبی ارتباطات الگوریتم پیشنهادی

۸- نتیجه‌گیری

در این مقاله، الگوریتمی جهت مقابله با حمله سیبل در شبکه‌های حسگر بی‌سیم ارائه گردید که در آن همه گره‌های قانونی به طور توزیعی، در طول حیاط شبکه، پازل‌های محاسباتی به همسایه‌های خود ارسال می‌کنند و منتظر پاسخ (حل پازل) از سوی همسایه‌ها می‌باشند. از آن‌جا که گره‌های سیبل دیرتر پاسخ می‌دهند، می‌توان آن‌ها را از گره‌های قانونی متمایز کرد. هم‌چنین، از اتوماتاهای یادگیر جهت کاهش سربار محاسباتی و ارتباطی ناشی از ارسال و حل پازل‌ها استفاده شده است. اتوماتای یادگیر به هر گره کمک می‌کند که نرخ ارسال پازل به همسایه‌هایش را بر اساس احتمال وجود گره‌های سیبل در اطراف خود تنظیم نماید. از مزایای الگوریتم پیشنهادی می‌توان به پویایی، توزیع شدگی، دقت تشخیص بالا، عدم نیاز به گره‌های کنترلی خاص (نظیر گره‌های مکان‌آگاه یا ردیاب) و عدم نیاز به سخت‌افزار اضافی (نظیر GPS) اشاره کرد. نتایج شبیه‌سازی‌ها نشان می‌دهد که الگوریتم پیشنهادی قادر به شناسایی 100% گره‌های سیبل بوده و نرخ تشخیص غلط آن در حالت میانگین کمتر از 5% است. کارایی الگوریتم پیشنهادی با دیگر الگوریتم‌های مطرح شده در [11,12,14,15,17] مقایسه گردید. نتایج حاکی از کارایی مطلوب الگوریتم پیشنهادی نسبت به دیگر الگوریتم‌ها از نقطه نظر معیارهای نرخ تشخیص و نرخ تشخیص غلط است.

منابع

[1] Douceur J. R., "***The Sybil attack***", in: Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS '02), 2002.

[2] Newsome J., Shi E., Song D. and Perrig A., "***The Sybil attack in sensor networks: analysis and defenses***", in: Proceedings of the third International Symposium on Information Processing in Sensor Networks (IPSN), ACM Press, Berkeley, California, USA, pp. 259–268, April 2004.

[3] Huang S.K., Ssu K.F. and Wu T.T., "***A fault-tolerant multipath routing protocol in wireless sensor networks***", in: Proceedings of the International Computer Symposium, pp. 966–971, Dec. 2004.

[4] Ssu K.F., Chou K.F., Jiau H.C. and Hu W.T., "***Detection and diagnosis for data inconsistency failures in wireless sensor networks***", in: Proceedings of the Computer Networks 50 (9), pp. 1247–1260, 2006.

[5] Ssu K.F., Chou C.H. and Cheng L.W., "***Using overhearing technique to detect malicious packet-modifying attacks in wireless sensor networks***", in: Proceedings of the Computer Communications 30 (11-12), pp. 2342–2352, 2007.

[6] Y. Zhang, W. Liu, W. Lou, Y. "***Fang, Location-based compromise tolerant security mechanisms for wireless sensor networks"***, in: Proceedings of the IEEE Journal on Selected Areas in Communications 24 (2), pp. 247–260, 2006.

[7] 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.

[8] 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.

[9] Karlof C. And Wagner D, "***Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures***", in: Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications(SNPA 03), pp. 113-127, 2003.

[10] Seshadri A., Perrig A., van Doorn L. and Khosla P., "***SWAtt: Software-based attestation for embedded devices***", in: Proceedings of the IEEE Symposium on Security and Privacy, 2004.

[11] 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.

[12] 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, Vol. 53, Issue 18, pp. 3042–3056, August 2009.

[13] Ramachandran S. and Shanmugan V., "***Impact of Sybil and Wormhole Attacks in Location based Geographic Multicast Routing Protocol for Wireless Sensor Networks***", in: Proceedings of the Journal of Computer Science 7, pp. 973-979, 2011.

[14] 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.

[15] 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.

[16] 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.

[17] Muraleedharan R., Ye X. and Osadciw L.A., "***Prediction of Sybil Attack on WSN Using Bayesian Network and Swarm Intelligence***", in: Proceedings of the Wireless Sensing and Processing, Orlando, FL, USA, March 2008.

[18] Wen M., Li H., Zheng Y.-F., "***TDOA-based Sybil attack detection scheme for wireless sensor***

[19] 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.

[20] Singh V. P., Jain S. and Singhai J., "***Hello Flood Attack and its Countermeasures in Wireless Sensor Networks***", in: Proceedings of the International Journal of Computer Science Issues(IJCSI), Vol. 7, Issue 3, No. 11, May 2010.

[21] Dwork C. and Naor M., "***Pricing via processing or combating junk mail***", in: Proceedings of the Advances in Cryptology (CRYPTO '98), volume 740 of LNCS, Santa Barbara, CA USA, pages139-147, August 1992.

[22] Bocan V., "***Threshold Puzzles: The Evolution of DOS-resistant Authentication***", in: Proceedings of the Transactions on AUTOMATIC CONTROL and COMPUTER SCIENCE, Vol.49 (63), ROMANIA, 2004.

[23] *Narendra K. S. and Thathachar M. A. L., "**Learning automata: An introduction**", in: Proceedings of the Prentice Hall, 1989.*

[24] *Narendra K. S. and Thathachar M. A. L., "**Learning automata a survey**", in: Proceedings of the IEEE Transactions on Systems, Man and Cybernetics, Vol. 4, no. 4, July 1974.*

[25] *Lakshmivarahan S. and Thathachar M. A. L., "**Absolutely expedient learning algorithms for stochastic automata**", in: Proceedings of the IEEE Transactions on Systems, Man and Cybernetics, Vol. 6, pp. 281-286, 1973.*

[26] *J-Sim Simulator,* http://www.j-sim.org.

زیرنویس‌ها

[1] Unattended
[2] Sybil
[3] Malicious node
[4] Voting
[5] Data aggregation
[6] Reputation evaluation
[7] Received Signal Strenght Indicator
[8] Peer to Peer
[9] Jakes Channel
[10] Swarm Intelligence
[11] Time difference of arrival
[12] beacon
[13] Angle of Arrival
[14] nonce
[15] P-Model
[16] Omni-directional
[17] Direct
[18] Simultaneous
[19] Fabricated
[20] Stolen