اولین کنفرانس ملی ایده های نو در مهندسی برق
۱۶ و ۱۷ آذر ماه ۱۳۹۱- دانشگاه آزاد اسلامی واحد خوراسگان- اصفهان
NCNIEE
NATIONAL CONFERENCE NEW IDEA IN ELECTRICAL ENGINEERING

مروری بر روش‌های تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم

شهرزاد گلستانی نجف آبادی [۱] ، حمید رضا ناجی [۲] و علی ماهانی [۳]
[۱] دانشگاه تحصیلات تکمیلی صنعتی کرمان، golestani@gut.ac.ir
[۲] دانشگاه تحصیلات تکمیلی صنعتی کرمان، hamidnaji@ieee.org
[۳] دانشگاه شهید باهنر کرمان ، amahani@uk.ac.ir

چکیده - شبکه‌های حسگر بی‌سیم راه‌حل ایده‌آلی برای انواع گوناگونی از کاربردهای نظارت و مراقبت شامل کنترل ترافیک، نظارت بر محیط، نظارت بر میدان جنگ و غیره هستند. شبکه‌های حسگر بی‌سیم رایج، از صدها یا هزاران گره حسگر تشکیل شده‌اند که در یک محیط وسیع و غالباً بدون نظارت و مراقبت توزیع شده‌اند. گره‌های حسگر دارای محدودیت‌هایی هم از لحاظ حافظه و هم از لحاظ قابلیت‌های محاسباتی هستند. این شبکه‌ها تحت تأثیر انواع مختلفی از حملات هستند که یکی از آنها حمله سیبیل است. حملات سیبیل تهدیدی جدی برای شبکه‌های حسگر بی‌سیم به‌شمار می‌آیند. در چنین حملاتی، یک نود مخرب چندین هویت جعلی برای خود ایجاد کرده و نودهای شبکه را گمراه می‌کند. حملات سیبیل به راحتی قابل پیاده‌سازی در شبکه‌های حسگر بی‌سیم هستند و می‌توانند در عملیاتی مثل رأی‌گیری، تجمیع‌سازی داده‌ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد کنند. هدف از این تحقیق بررسی روش‌های موجود برای تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم می‌باشد.

کلید واژه- شبکه‌های حسگر بی‌سیم، امنیت، حملات سیبیل.

۱- مقدمه

یک شبکه حسگر بی‌سیم از تعداد زیادی گره حسگر تشکیل شده که بصورت متراکم در محیط پخش شده‌اند و برای اندازه-گیری گروهی برخی از کمیت‌های فیزیکی یا شرایط محیطی بکار می‌روند. شبکه‌های حسگر با انگیزه استفاده در کاربردهای نظامی مانند نظارت بر میدان جنگ توسعه پیدا کردند اما امروزه در صنعت و بسیاری از مقاصد غیر نظامی نیز استفاده می‌شوند. در حالیکه حضور شبکه‌های حسگر بی‌سیم در زمینه‌های نظامی و عمرانی افزایش پیدا می‌کند، نیاز به امنیت هم به یک ضرورت تبدیل می‌شود.

این شبکه‌ها تحت تأثیر انواع مختلفی از حملات هستند که یکی از آنها حمله سیبیل (Sybil) است. حملات سیبیل به راحتی قابل پیاده‌سازی در شبکه‌های حسگر بی‌سیم هستند چون گره‌های حسگر در یک محیط توزیع‌شده قرار گرفته‌اند و از طریق امواج رادیوئی با یکدیگر ارتباط برقرار می‌کنند. همین قابلیت، این امکان را برای حمله خرابکاران به شبکه فراهم می-کند.

حملات سیبیل تهدیدی جدی برای شبکه‌های حسگر بی-سیم به‌شمار می‌آیند. در چنین حملاتی، یک گره مخرب چندین هویت جعلی برای خود ایجاد کرده و گره‌های شبکه را گمراه می‌کند [۲-۱]. این حملات می‌توانند در عملیاتی مثل مسیریابی، رأی‌گیری، تجمیع‌سازی داده‌ها، ارزیابی اعتبار گره‌ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد کنند [۳]. مکانیزم‌هایی که مبتنی بر رأی‌گیری هستند کارایی خود را از دست می‌دهند چون برخی گره‌ها جعلی هستند و نمی‌توان به اطلاعات به دست آمده از آنها اعتماد کرد [۴].

امنیت اطلاعات در برخی سیستم‌ها از اهمیت بسیار بالایی برخوردار است. به عنوان مثال محرمانگی و امنیت اطلاعات در جائی که سنسورها اطلاعات پزشکی یا فعالیت نظامی تانک‌ها را جمع آوری می کنند بسیار مهم است. حملات سیبیل از این جهت یکی از مهم‌ترین حملات در شبکه‌های حسگر بی‌سیم به-شمار می‌آیند که می‌توانند بستر لازم برای بسیاری دیگر از حملات را فراهم کنند [۵]. همچنین این حمله ترافیک کنترلی را مورد هدف قرار داده و خرابی وسیعی را در شبکه باعث می-

شود.

با توجه به سادگی پیاده‌سازی این حملات و حساس بودن اطلاعات در این نوع شبکه‌ها، ارائه راه‌کارهایی که بتوانند حملات سیبیل را تشخیص دهند و در صورت امکان با آن مقابله کنند بسیار ضروری می‌باشد. این راه‌کارها باید محدودیت‌های پردازشی، حافظه و توان در شبکه‌های حسگر بی‌سیم را نیز در نظر گرفته باشند تا بطور عملی قابل استفاده در این شبکه‌ها باشند.

هدف از این تحقیق بررسی روش‌هایی است که تاکنون برای تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم ارائه شده‌اند می‌باشد.

۲- حملات سیبیل

حمله سیبیل اولین بار در شبکه‌های نظیر به نظیر مطرح شد [۷]. Douceur ادعا کرد در چنین محیط‌های محاسباتی توزیع‌شده‌ای، یک دستگاه می‌تواند به راحتی چندین هویت (شناسه) اختیار کند که این به دلیل فقدان یک قدرت مرکزی و مورد اعتماد در شبکه است. راه‌حل‌های متنوعی برای تشخیص این حمله و حذف آن از بستر شبکه پیشنهاد شده است. روش‌های مذکور را بدین طریق طبقه‌بندی کرده و تشریح می‌کنیم:

- روش‌های مبتنی بر رمزنگاری و احراز هویت
- روش‌های مبتنی بر مکان یابی (سیگنال دریافتی)
- روش‌های مبتنی بر اطلاعات دریافتی از گره‌ها

روش‌های هوشمند.

۲-۱- روش‌های مبتنی بر رمزنگاری و احراز هویت

یکی از اولین راه‌حل‌ها برای تشخیص حملات سیبیل استفاده از روش‌های احراز هویت و رمزنگاری است. هنگام استفاده از روش‌های رمزنگاری نامتقارن، ابتدا کلیدهای عمومی و خصوصی بین همه گره‌های شبکه توزیع می‌شود، سپس امضای دیجیتال ایجاد می‌شود. بالعکس در یک مکانیزم رمزنگاری متقارن، هر گره یک کلید منحصربه فرد با چاهک دارد. هر زمان دو گره اطلاعاتی برای تبادل داشته باشند، ابتدا با چاهک ارتباط برقرار کرده و تمایل خود را برای برقراری ارتباط اعلام می‌کنند. چاهک هویت دو گره را از طریق کلیدهای متقارن آنها بررسی کرده و سپس یک کلید مشترک برای هر دو آنها ارسال می‌کند تا آنها بتوانند بصورت مستقیم با یکدیگر ارتباط برقرار کنند [۴].

رمزنگاری کلید عمومی برای حسگرهای بی‌سیم کوچک از لحاظ محاسباتی مقرون به صرفه نیست. رمزنگاری با کلید عمومی و یا تعیین هویت پیغام در گره‌های حسگر چندین ثانیه زمان می‌برد [۶]. سیستم‌های کلید عمومی، حافظه بیشتری نسبت به سیستم‌های کلید متقارن مصرف می‌کنند. همچنین آنها بطور قابل توجهی اندازه پیغام را افزایش می‌دهند. در نتیجه سیستم‌های کلید عمومی بطور قابل توجهی مصرف انرژی و پهنای باند را افزایش می‌دهند. بنابر دلایل ذکر شده، بیشتر راه‌حل‌های رمزنگاری موجود برای شبکه‌های حسگر بی‌سیم، بر مبنای سیستم‌های کلید متقارن هستند. اما در سیستم‌های کلید متقارن هم توزیع کلید یک چالش مهم به حساب می‌آید [۵].

Karlof و Wagner در مورد مزایای نسبی تکنیک‌های رمزنگاری متقارن و غیرمتقارن برای حفاظت از شبکه های حسگر بی‌سیم در برابر حملات سیبیل صحبت کرده‌اند [۷]. آنها بیان کردند که شبکه‌های حسگر بی‌سیم به دلیل اینکه دارای محیط توزیع شده و غیر قابل اطمینانی هستند مستعد قرار گرفتن در معرض حملات سیبیل هستند. به منظور دفاع در برابر این حمله نیز استفاده از کلیدهای رمزنگاری و مکانیزم احراز هویت گره‌ها را پیشنهاد داده‌اند که به دلیل محدودیت گره‌های حسگر در منابع ذخیره سازی و محاسباتی، روش مناسبی نیست. از جهتی دیگر استفاده از کلیدهای رمزنگاری همیشه نمی‌تواند باعث تشخیص و جلوگیری از حمله سیبیل شود.

Newsome و همکارانش چندین روش برای حفاظت از شبکه‌های حسگر بی‌سیم در برابر حملات سیبیل پیشنهاد داده‌اند، که شامل یک مکانیزم تست منابع رادیوئی[a] (RRT) و یک مکانیزم پیش‌توزیع تصادفی کلید[b] (RKP) می‌شود [۳]. مکانیزم RRT بر پایه این فرض بنا نهاده شده است که گره‌ها در یک شبکه عام قابلیت انتقال همزمان روی بیش از یک کانال را ندارند. هنگامیکه یک گره می‌خواهد ببیند قربانی یک حمله سیبیل شده است یا خیر، به هر کدام از همسایگان خود یک کانال منحصربه فرد اختصاص می‌دهد و از آنها درخواست می‌کند تا در یک زمان مشخص یک پیغام تصدیق روی کانال‌های اختصاص داده شده به آنها پخش کنند. سپس گره مذکور بطور تصادفی گیرنده خود را روی یکی از کانال‌ها تنظیم می‌کند و منتظر دریافت پیغام تصدیق می‌شود. اگر هیچ پیغام تصدیقی دریافت نکرد، به گره مذکور مشکوک می‌شود. این به این دلیل است که گره مخرب قادر نیست برای همه هویت‌های جعلی خود

بطور همزمان روی چند کانال پیغام تصدیق ارسال کند. با تکرار مکرر این روال، همه گره‌های جعلی با احتمال بالایی قابل تشخیص هستند.

در روش RKP هر گره k کلید را بطور تصادفی از یک مخزن بزرگی که m کلید دارد انتخاب می‌کند. m بگونه‌ای انتخاب می‌شود که هر دو گره حتماً یک کلید مشترک داشته باشند. سپس شناسه هر گره با شناسه مجموعه کلیدهایی که انتخاب کرده ترکیب می‌شود و شناسه‌های منحصر بفردی تولید می‌شود. بدین طریق هر گره را با تأیید کردن برخی یا همه کلیدهایی که ادعا می‌کند در اختیار دارد می‌توان شناسایی و احراز هویت کرد.

Zhang و همکارانش برای جلوگیری از حملات سیبیل از رمزنگاری کلید متقارن استفاده کرده‌اند [۸]. این روش از یکی از ویژگی‌های مهم درخت‌های درهم‌سازی مرکل استفاده می‌کند، بدین صورت که هر گره برگ را می‌توان تأیید و تصدیق کرد به شرط اینکه مقدار والد آن از پیش مشخص باشد. همچنین این ویژگی در روش دیگری استفاده می‌شود تا هر گره شبکه بتواند هویت دیگر گره‌های شبکه را بررسی و تأیید کند [۹]. این روش تنها در شبکه‌های حسگر بی‌سیم با مقیاس کوچک کارا است.

روش‌های احراز هویت [۱۰-۸] غالباً نیاز به فضای حافظه زیادی برای ذخیره اطلاعات هویت ضروری (مثل کلیدهای رمزنگاری مشترک، شناسه‌ها و غیره) و پردازش‌های پیچیده دارند. بعلاوه اینکه اگر مهاجمی بتواند به مکانیزم احراز هویت نفوذ کند، آنگاه جامعیت کلی مکانیزم حفاظتی از بین می‌رود [۴].

۲-۲- روش‌های مبتنی بر مکان یابی (سیگنال دریافتی)

روش‌های دفاعی غیر- احراز هویتی گوناگونی نیز برای مقابله با حملات سیبیل ارائه شده است. برای مثال Demirbas و Song استفاده از شاخص قدرت سیگنال دریافتی[c] (RSSI) را برای تشخیص حملات سیبیل پیشنهاد داده‌اند [۱۱]. گره به هنگام دریافت پیغام از یک فرستنده جدید، RSSI آن پیغام را محاسبه می‌کند. سپس RSSI محاسبه شده را با شناسه فرستنده پیغام (که در پیغام وجود دارد) مرتبط کرده و آن را در یک جدول جستجو ذخیره می‌کند. اگر در آینده، گره پیغام دیگری با همان RSSI اما شناسه فرستنده متفاوتی دریافت کرد، وقوع یک حمله سیبیل را اعلام می‌کند.

استفاده از RSSI بواسطه ماهیت متغیر و غیرقابل اعتماد آن برای این منظور پاسخگو نیست. علاوه بر این، گره‌ها در شبکه‌های حسگر به راحتی می‌توانند توان ارسالی خود را تغییر دهند و در نتیجه گیرنده را فریب دهند. از آنجائیکه RSSI تابعی از توان ارسالی است، توان‌های متفاوت منجر به RSSIهای متفاوت می‌شوند. در برخی پروتکل‌ها نیز برای مقاصد راندمان انرژی، گره‌ها به ارسال با توان‌های متفاوت می‌پردازند. همچنین با کاهش توان باتری و تغییر فاکتورهای محیطی، توان ارسالی به ناچار تغییر می‌کند. به دلیل موارد فوق‌الذکر، در این روش به جای استفاده از RSSI از نرخ RSSI استفاده می‌شود.

استفاده از نسبت RSSI ابتدا توسط Zhong و همکارانش، برای تشخیص مکان فرستنده با استفاده از چهار گره ناظر مطرح شد [۱۲]. می‌توان از الگوریتم موقعیت‌یابی پیشنهاد شده در این مقاله برای تشخیص حملات سیبیل استفاده کرد. بدین صورت که با دریافت یک پیغام، چهار گره ناظر، موقعیت فرستنده را محاسبه کرده و موقعیت حاصله را با شناسه فرستنده مرتبط می‌کنند. سپس با دریافت پیغامی با شناسه جدید، مکان فرستنده محاسبه شده و در صورت تشابه، تشخیص حمله سیبیل اعلام می‌شود.

باید توجه داشت برای تشخیص این حمله، محاسبه مکان کار طاقت فرسا و غیر ضروری می‌باشد. در واقع می‌توان حمله را با محاسبه و ثبت نرخ RSSI برای پیغام‌های دریافتی تشخیص داد. پس آنها در روش پیشنهادی خود از دو گیرنده و نسبت RSSIها استفاده کردند.

با فرض اینکه گره i از گره 0 سیگنال رادیوئی دریافت می‌کند. آنگاه مقدار RSSI با استفاده از فرمول ۱ محاسبه می‌شود.

$$R_i = P_0 K / d_i^{\alpha} \qquad (۱)$$

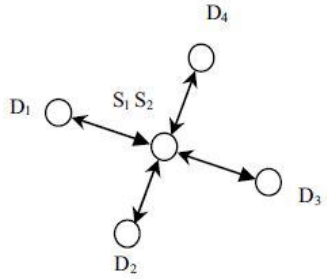
که P0 نشان دهنده توان فرستنده، Ri نشان دهنده RSSI، K یک عدد ثابت و di فاصله اقلیدسی است. α گرادیان فاصله‌توان می‌باشد. و نرخ RSSI گره i به j نیز طبق فرمول ۲ محاسبه می‌شود:

$$R_i / R_j = \left(\frac{p_0 k}{d_i^{\alpha}}\right) \Big/ \left(\frac{p_0 k}{d_j^{\alpha}}\right) = \left(\frac{d_j}{d_i}\right)^{\alpha} \qquad (۲)$$

با فرض اینکه دو گره سیبیل (S_1, S_2) و چهار گره ناظر (D_1, D_2, D_3, D_4) داریم (شکل ۱)، فرآیند تشخیص حمله بدین صورت است. هر کدام از گره‌های ناظر D_2, D_3, D_4 پیغامی برای D_1 ارسال می‌کنند و مقدار RSSI دریافتی از یک گره (مثلاً S_1) را برای او ارسال می‌کنند.

سپس D_1 نسبت‌های زیر را محاسبه می‌کند:

$$\frac{R_{D_1}^{S_1}}{R_{D_2}^{S_1}}, \frac{R_{D_1}^{S_1}}{R_{D_3}^{S_1}}, \frac{R_{D_1}^{S_1}}{R_{D_4}^{S_1}} \qquad (۲)$$



شکل ۱: تشخیص حمله سیبیل توسط ۴ گره [۱۳]

این نسبت‌ها برای گره S_2 هم محاسبه می‌شود:

$$\frac{R_{D_1}^{S_2}}{R_{D_2}^{S_2}}, \frac{R_{D_1}^{S_2}}{R_{D_3}^{S_2}}, \frac{R_{D_1}^{S_2}}{R_{D_4}^{S_2}} \qquad (۳)$$

اگر تفاوت بین هر دو نسبت بسیار نزدیک به صفر بود (مشاهده فرمول ۵)، پس یک حمله سیبیل رخ داده است.

(۵)

$$\frac{R_{D_1}^{S_1}}{R_{D_2}^{S_1}} - \frac{R_{D_1}^{S_2}}{R_{D_2}^{S_2}} < \sigma, \frac{R_{D_1}^{S_1}}{R_{D_3}^{S_1}} - \frac{R_{D_1}^{S_2}}{R_{D_3}^{S_2}} < \sigma, \frac{R_{D_1}^{S_1}}{R_{D_4}^{S_1}} - \frac{R_{D_1}^{S_2}}{R_{D_4}^{S_2}} < \sigma$$

در حالتی که دو گره گیرنده (ناظر) داریم، برای تشخیص حمله سیبیل تنها یک انتقال کافی است (انتقال از گره D_2 به D_1). بنابراین در این مورد سربار بسیار کم است که باعث می‌شود این روش، روش مناسب‌تری برای شبکه‌های حسگر بی‌سیم باشد.

Wang و همکارانش نیز مکانیزم مشابهی برای تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم مبتنی بر کلاستر پیشنهاد داده‌اند [۱۳]. آنها مدل کانال جکس را پیاده‌سازی کرده‌اند که در آن تأثیر خطاهای ناشی از محو شدگی و افت مسیر در کانال‌های ارتباطی شبکه‌های حسگر بی‌سیم مورد توجه و بررسی قرار گرفته‌اند. سپس یک روش ترکیبی برای تشخیص حملات سیبیل ارائه داده‌اند که این حملات را با توجه به RSSI دریافتی از گره‌ها و در نظر گرفتن اطلاعاتی که توسط گره‌های شبکه تهیه و ارسال می‌شوند تشخیص می‌دهد.

مکانیزمی مبتنی بر TDOA، برای تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم مبتنی بر کلاستر ارائه شده است [۱۴]. در این روش در هر کلاستر سه گره راهنما داریم. گره‌های حسگر درون یک کلاستر توسط این سه گره شنیده می‌شوند. گره‌های راهنما از مکان خود مطلع هستند (مثلاً از طریق سیستم GPS و غیره). با ارسال پیغام توسط گره‌ها، TDOA بین گره فرستنده و گره‌های راهنما محاسبه می‌شود. سپس نرخ TDOA با شناسه فرستنده مرتبط می‌شود. هنگامیکه دو شناسه متفاوت با نرخ TDOA یکسان مشاهده شد، وقوع یک حمله سیبیل شناسایی می‌شود.

در روشی دیگر، استفاده از یک تکنیک مسافت یابی برای تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم مورد استفاده قرار می‌گیرد. نویسندگان این مقاله از این واقعیت بهره جستند: از آنجائیکه گره‌های سیبیل توسط یک گره مخرب ایجاد می‌شوند، پس در یک مکان فیزیکی قرار گرفته‌اند. در نتیجه فاصله این گره‌ها (سیبیل) از یک سری گره‌ها باید یکسان باشد [۱۵].

در این روش یک مقدار آستانه در نظر گرفته می‌شود. هر گره، گره‌های با مسافت یکسان تا خودش را پیدا کرده و آنها را در لیست گره‌های مشکوک قرار می‌دهد و لیست خود را اعلام می‌کند. اگر دو یا چند گره مشکوک بطور همزمان در N لیست که N بزرگتر از مقدار آستانه است ظاهر شوند آنگاه آنها به عنوان گره‌های سیبیل در نظر گرفته می‌شوند. به عنوان مثال در شکل ۲ گره‌های A، B و C گره‌های نرمال و گره‌های E و D گره‌های سیبیل هستند.

این روش از یک روش اندازه‌گیری فاصله بر مبنای اختلاف فاز استفاده می‌کند [۱۶].دو گره N1 و N2 دو موج سینوسی ω_1 و ω_2 با فرکانس یکسان را ارسال می‌کنند.

$$S_1(t) = a_1 \sin[\omega_1 t + \phi_1] \qquad (۶)$$

$$S_2(t) = a_2 \sin[\omega_2 t + \phi_2] \qquad (۷)$$

این دو موج سینوسی با زمان تأخیر متفاوتی به گره N3 می‌رسند. بنابراین N3 سیگنال‌های ذیل را دریافت می‌کند:

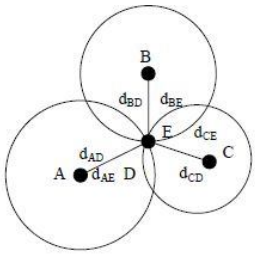
$$r_{31}(t) = a_1 \sin[\omega_1 (t - d_{31}/c) + \phi_1] \qquad (۸)$$

$$r_{32}(t) = a_2 \sin[\omega_2 (t - d_{32}/c) + \phi_2] \qquad (۹)$$

$r_{31}(t)$ و $r_{32}(t)$ به ترتیب سیگنال‌های دریافتی از N1 و N2 در N3 هستند. d_{31} و d_{32} به ترتیب فاصله گره‌های فرستنده (N1 و N2) تا گره گیرنده (N3) هستند. C سرعت نور می‌باشد.

اگر گره‌های N1 و N2 دو موج سینوسی با فرکانس‌های تقریباً مشابه ارسال کنند و این موج‌های سینوسی همپوشانی داشته باشند، پس از اینکه N3 و N4 این سیگنال‌های همپوشان را دریافت کردند، مقدار RSSI را محاسبه می‌کنند. اختلاف فاز

RSSI تنها به فاصله بین این چهار گره و طول موج این امواج سینوسی وابسته است. پس با محاسبه اختلاف فاز بین دو RSSI می‌توان رابطه خطی بین فرستنده و گیرنده و در نتیجه فاصله بین آنها را بدست آورد.



شکل ۲: نمونه‌ای از مسافت‌یابی گره‌ها [۱۵]

Chen و همکارانش ابتدا مدلی کلی برای تشخیص حمله با استفاده از همبستگی فضایی قدرت سیگنال دریافتی در گره‌های حسگر پیشنهاد دادند. سپس موقعیت گره‌های مهاجم با استفاده از یک موقعیت‌یاب بدست می‌آید. آنها با کمک همبستگی فضایی قدرت سیگنال دریافتی و موقعیت گره‌های مهاجم به تشخیص حملات مبتنی بر شناسه می‌پردازند. و در نهایت با استفاده از الگوریتم K- میانگین روش خود را تحلیل می‌کنند [۱۷].

بسیاری از گره‌های حسگر برای جمع‌آوری اطلاعات محیطی و ارسال این اطلاعات به ایستگاه پایه از پروتکل ZigBee استفاده می‌کنند. Lee و همکارانش روشی برای کاهش تأثیر حمله سیبیل در شبکه‌های حسگر بی‌سیم مبتنی بر پروتکل ZigBee ارائه داده‌اند [۱۸]. روش پیشنهادی آنها از شیوه تست منابع استفاده می‌کند.

آنها یک مکانیزم چالش و پاسخ ارائه داده‌اند. در این مکانیزم یک گره ناظر درخواستی برای گره‌های حسگر ارسال می‌کند و از گره‌های حسگر انتظار دارد تا در مدت زمان مشخص و معقولی به درخواستش پاسخ دهند. گره حسگر باید در طول این مدت زمان به درخواست گره ناظر پاسخ دهد. همچنین باید پاسخ درستی به درخواست یا سؤال این گره بدهد. اگر گره حسگر نتواند در مدت زمان مشخص شده پاسخ دهد یا اینکه پاسخ اشتباه باشد، گره ناظر به این گره مشکوک می‌شود. پس از تشخیص گره‌های مخرب، این گره‌ها از شبکه حذف می‌شوند، به این صورت که دیگر ترافیک به سمت آنها ارسال نمی‌شود.

Amini و همکارانش روشی برای تشخیص حملات سیبیل در شبکه‌های حسگر خوشه‌بندی شده با گره‌های غیرمتحرک پیشنهاد داده‌اند [۱۹]. روش پیشنهادی مبتنی بر قدرت سیگنال دریافتی در سرخوشه‌ها است. بسیاری روش‌ها با این فرض که گره‌ها در شبکه‌های حسگر بصورت نظیر به نظیر با یکدیگر ارتباط برقرار می‌کنند و اینکه بطور مستقیم با همسایگان خود در ارتباط هستند به تشخیص حمله سیبیل می‌پردازند اما در این روش ساختار شبکه بصورت ستاره در نظر گرفته شده و از پروتکل IEEE 802.15.4 مبتنی بر راهنما استفاده می‌کنند. در این پروتکل گره‌ها از طریق سرخوشه با یکدیگر ارتباط برقرار می‌کنند که باعث می‌شود این پروتکل نسبت به برخی دیگر پروتکل‌ها برای شبکه‌های حسگر بی‌سیم مناسب‌تر باشد.

در این روش خوشه‌ها بصورت دایره‌هایی هم مرکز در نظر گرفته می‌شوند که مرکز آنها هماهنگ کننده شبکه است. در مرحله توزیع گره‌ها یک شماره دیسک و یک شناسه به هر گره اختصاص داده می‌شود. هماهنگ کننده شبکه این اطلاعات مربوط به همه گره‌ها را در جدولی ذخیره می‌کند. هنگامیکه هماهنگ کننده بسته‌ای از یک گره دریافت می‌کند، مکان گره (فاصله بین گره تا خودش) را تخمین می‌زند. سپس شناسه گره را از بسته دریافتی استخراج کرده با کمک فاصله محاسبه شده، شماره دیسک گره را محاسبه می‌کند. مجموعه (شماره دیسک، شناسه) محاسبه شده با مقادیر ذخیره شده در جدول برای همین شناسه مقایسه می‌شود. در صورت مغایرت حمله سیبیل تشخیص داده می‌شود.

ابتدا در این روش، برای محاسبه مقدار RSSI از روش ذکر شده در مرجع [۲۰] استفاده شده است. اما بواسطه نوسان در مقدار RSSI، آنها از روشی که در مرجع [۲۱] پیشنهاد شده برای تخمین میانگین مقدار RSSI استفاده می‌کنند.

Lv و همکارانش روشی تحت عنوان $CRSD^d$ برای شبکه‌های حسگر بی‌سیم ثابت ارائه کرده‌اند که از قدرت سیگنال دریافتی برای اندازه‌گیری فاصله بین دو گره استفاده می‌کند [۲۲]. این روش از کمک چندین گره همسایه (قابلیت همکاری گره‌ها) استفاده می‌کند و فاصله بین گره موردنظر را تا این گره‌ها محاسبه می‌کند. در این روش فرض بر اینست که توان ارسالی برای همه گره‌ها (نرمال و مخرب) یکسان و ثابت است. همه گره‌های سیبیل دارای مکان فیزیکی مشترک هستند [۱۱]، پس این روش برای تشخیص حملات سیبیل از مکان گره‌ها و RSS استفاده می‌کند. یک گره برای تشخیص حمله، گره‌هایی که تا این گره فاصله یکسانی دارند و مقدار RSS مشابهی هم دارند را در یک گروه قرار می‌دهد. گره‌هایی که در یک گروه قرار می-

گیرند گره‌های سیبیل هستند.

۲-۳- روش‌های مبتنی بر اطلاعات دریافتی از گره‌ها

Ssu و همکارانش روشی برای مقابله با حملات سیبیل در شبکه‌های حسگر بی‌سیم ارائه داده‌اند که در آن هویت گره‌ها با استفاده از تجزیه و تحلیل اطلاعات گره‌های همسایه هر گره بررسی و بازبینی می‌شود [۴]. این روش از این واقعیت که هر گره مخرب تعداد زیادی هویت جعلی ایجاد می‌کند استفاده کرده تا مکانیزمی برای حفاظت از شبکه‌های حسگر بی‌سیم در برابر حملات سیبیل ارائه دهد.

این مکانیزم دفاعی بر این فرض بنیادی بنا نهاده شده‌است: با این فرض که شبکه‌ای با تراکم گره بالا داریم، احتمال اینکه دو گره متفاوت دارای مجموعه همسایگی دقیقاً یکسان باشند بسیار کم است. در حملات سیبیل، گره‌های جعل شده دارای مجموعه مشابهی از همسایگان هستند چون همه آنها مربوط به یک گره فیزیکی یعنی گره مخرب هستند. در نتیجه می‌توان وجود یک گره مخرب را با بررسی گره‌های همسایه گره قربانی و بررسی اینکه آیا برخی از این گره‌ها مجموعه همسایگی مشابه هم دارند یا خیر و بنابراین گره‌های سیبیل هستند، تشخیص داد. آنها امکان‌پذیری روش خود را هم با قوانین ریاضی و هم بصورت عددی ارزیابی کرده‌اند. همچنین اعتبار آن را بصورت تجربی و با استفاده از ۸ گره Tmote sky نیز بررسی کرده‌اند.

مکانیزم دفاع توسط یک گره نرمال که به قربانی بودن خود مشکوک است انجام می‌گیرد. نکته قابل توجه در این روش این است که روش پیشنهادی به جای اینکه اقدام به بازجویی هر گره کند، متکی به فرآیند ساده جمع‌آوری اطلاعات و تحلیل آنها است. در نتیجه، این استراتژی از این ریسک که گره مخرب به قصد جواب غلط بدهد و سیستم تشخیص را گمراه کند جلوگیری می‌کند.

همچنین آنها روشی برای بهبود مکانیزم تشخیص خود ارائه دادند. در واقع آنها عقیده دارند، اگر بتوان گره مخرب را حذف کرد آنگاه دیگر این گره موثر نخواهد بود و بقیه همسایگان گره قربانی، گره‌های نرمال خواهند بود. از آنجائیکه تنظیم دامنه ارتباطی گره‌های حسگر به طور وسیعی انجام می‌گیرد [۲۴-۲۳]، از این شیوه در این مکانیزم نیز استفاده شده است. کاهش دامنه ارتباطی گره قربانی، تا جائیکه گره مخرب بیرون از این محدوده قرار گیرد ادامه می‌یابد. در این صورت گره مخرب اثر خود را از دست داده و تعداد تشخیص‌های غلط کاهش پیدا می‌کند. آنها کار خود را در مرجع [۲۵] ادامه دادند.

Bhuse در رساله خود دو روش برای تشخیص حملات سیبیل به نام‌های MG[e] و SRP[f] ارائه داد که این دو روش مکمل یکدیگر هستند [۲۶]. روش MG برای زمانی است که گره مخرب شناسه یکی از گره‌های همسایه را در اختیار خود می‌گیرد. دو گره‌ای که در دامنه ارتباطی هم هستند می‌توانند بسته‌های ارسالی توسط دیگری را دریافت کنند. یک گره مخرب که در ناحیه مشترک بین این دو گره قرار گرفته باشد نمی‌تواند خود را به جای هر کدام از این گره‌ها جا زند چون توسط آنها تشخیص داده می‌شود.

روش SRP برای پروتکل‌های MAC که با امکان دسترسی انحصاری به کانال از تصادم جلوگیری می‌کنند کاربرد دارد. این روش برای زمانی است که گره مخرب شناسه‌ای اختیار می‌کند که در همسایگی‌اش نیست. سپس با مبادله اطلاعاتی درباره تعداد بسته‌های دریافتی هر گره و مقایسه تعداد بسته‌های ارسال شده و دریافت شده حمله سیبیل تشخیص داده می‌شود.

۲-۴- روش‌های هوشمند

Banerjee و همکارانش یک مکانیزم تشخیص نفوذ مبتنی بر کلونی مورچه‌ها برای شبکه‌های حسگر بی‌سیم پیشنهاد دادند [۲۷]. Zheng و همکارانش نیز با استفاده از الگوریتم کلونی مورچه‌ها سعی در کاهش تأثیر حملات سیبیل در شبکه‌های حسگر بی‌سیم دارند. در شبکه‌ای که گره‌های سیبیل داریم، گره سیبیل می‌تواند به گره‌های نرمال شبکه متصل شود و در نتیجه یک یال بین گره سیبیل و گره نرمال برقرار می‌شود. با کمک ماهیت الگوریتم کلونی مورچه‌ها می‌توان تعداد این یال‌های مخرب را کاهش داد [۲۸].

Quercia و همکارش روشی غیرمتمرکز برای تشخیص حملات سیبیل در شبکه‌هایی با گره‌های متحرک ارائه دادند. آنها از ایده شبکه‌های اجتماعی استفاده کردند. در این روش هر گره دو مجموعه که متشکل از اطلاعات مربوط به گره‌ها می‌باشد را جمع‌آوری و نگهداری می‌کند. یک مجموعه شبکه دوستان و دیگری شبکه مهاجمان را تشکیل می‌دهد. مجموعه اول شامل گره‌های قابل اعتماد و مجموعه دوم شامل گره‌هایی است که گره به آنها مشکوک است [۲۹].

۳- نتیجه‌گیری

حملات سیبیل تهدیدی جدی برای شبکه‌های حسگر بی-سیم به‌شمار می‌آیند که در آن یک گره مخرب چندین هویت جعلی برای خود ایجاد کرده و با گمراه کردن گره‌های شبکه در عملیاتی مثل رأی‌گیری، تجمیع‌سازی داده‌ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد می‌کند.

در این مقاله روش‌های مختلف ارائه شده برای تشخیص حملات سیبیل در شبکه‌های حسگر بی‌سیم در چهار گروه طبقه‌بندی شدند. روش‌هایی که برای شبکه‌های حسگر بی‌سیم ارائه می‌شوند باید محدودیت‌های این شبکه‌ها در منابع پردازشی، حافظه و توان را درنظر بگیرند. بسیاری از روش‌های ارائه شده برای تشخیص حملات سیبیل در این شبکه‌ها، این محدودیت‌ها را در نظر نگرفته‌اند.

با توجه به طبقه‌بندی انجام شده در این مقاله می‌توان گفت روش‌های مبتنی بر رمزنگاری و احراز هویت غالباً به دلیل نیاز به پردازش‌های سنگین روش‌های مناسبی نیستند. همچنین در این روش‌ها پس از نفوذ به مکانیزم احراز هویت، جامعیت مکانیزم احراز هویت از بین می‌رود و همه شبکه به مخاطره افتاده است.

روش‌های مبتنی بر مکان‌یابی بعضاً نیاز به سخت‌افزارهای اضافی مثل GPS و گره‌های ناظر دارند که در نتیجه هزینه شبکه حسگر را بالا برده و همچنین مصرف انرژی را افزایش می‌دهند.

طبقه سوم روش‌هایی هستند که مبتنی بر اطلاعات دریافتی از گره‌ها هستند. روش‌های مذکور می‌توانند روش‌های مفیدی برای تشخیص حملات باشند اگر حجم اطلاعات ارسالی و دریافتی روی شبکه در حد معقولی باشد. حجم تبادلات زیاد باعث سربار ارتباطی و افزایش مصرف انرژی می‌شود.

روش‌های هوشمند روش‌های جدیدی برای تشخیص حملات به شمار می‌سوند. این روش‌ها در صورتیکه منجر به سربار پردازشی نشوند روش‌های مناسبی هستند.

مراجع

[1] J.R. Douceur, “The Sybil attack,” in Proc. of the International Workshop on Peer-to-Peer Systems,” March 2002, pp. 251–260.

[2] Z. Su, C. Lin, F. Ren, X. Zhan, “Security mechanisms analysis of wireless sensor networks specific routing attacks,” in Proc. of 2006 1st International Symposium on Pervasive Computing and Applications, pp. 579–584.

[3] J. Newsome, E. Shi, D. Song and A. Perrig, “The Sybil attack in sensor networks: analysis and defenses,” in Proc. of 2004 International Symposium on Information Processing in Sensor Networks, pp. 259–268.

[4] K. F. Ssu, W. T. Wang, W. C. Chang, “Detecting Sybil Attacks in Wireless Sensor Networks Using Neighboring Information,” Computer Networks, vol. 53, no. 18, pp. 3042-3056, Dec. 2009.

[5] S. Misra, I. Woungang, S. C. Misra, Guide to Wireless Sensor Networks, Springer, 2009, pp. 491-512.

[6] D. J., Malan, M., Welsh, M., Smith, “A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography,” First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks,, pp. 71 – 80, 2004.

[7] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in Proc. of 2003 IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127.

[8] Q. Zhang, P. Wang, D.S. Reeves, P. Ning, “Defending against Sybil attacks in sensor networks,” in Proc. of 2005 IEEE International Conference on Distributed Computing Systems Workshops, pp. 185–191.

[9] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 247-260, Feb. 2006.

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

[11] M. Demirbas and Y. Song, “An RSSI-based scheme for Sybil attack detection in wireless sensor networks,” in Proc. of International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 564–570, 2006.

[12] S., Zhong, L., Li, Y. G., Liu, Y. R., Yang, “Privacy-preserving location based services for mobile users in wireless networks”, Technical Report YALEU/DCS/TR-1297, Yale Computer Science, July 2004.

[13] J., Wang, G., Yang, Y., Sun, S., Chen, “Sybil Attack Detection Based on RSSI for Wireless Sensor Network”, International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2684-2687, 2007.

[14] W. Mi, L. Hui, Z. Yanfei and C. Kefei, “TDOA-based Sybil attack detection scheme for wireless sensor networks,” Journal of Shanghai University (English Edition), Vol .12, No.1, pp. 66-70, 2008.

[15] R., Xiu-li, Y., Wei, “Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network” 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1 – 4, 2009.

[16] Z., Zhi-Guang, “A WSN Node Ranging Method Based on Phase Difference Measuremen,” Chinese Journal of Sensors and Actuators, Vol. 20, No. 12, pp. 2728-2732, December 2007.

[17] J., Yang, Y., Chen, W., Trappe, “Detecting sybil attacks inwireless and sensor networks using cluster analysis,” IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 834 – 839, October 2008.

[18] G., Lee, J., Lim, D., Kim, S., Yang, M., Yoon, “An Approach to Mitigating Sybil Attack in Wireless Networks using ZigBee,” International Conference on Advanced Communication Technology, pp. 1005 – 1009, April 2008.

[19] F., Amini, J., Misic, H., Pourreza, “Detection of Sybil Attack in Beacon Enabled IEEE802.15.4 Networks,” International Conference on Wireless Communications and Mobile Computing, pp. 1058 – 1063, August 2008.

[20] A., Flammini, D., Marioli, G., Mazzoleni, E., Sisinni, A., Taroni, “Received Signal Strength Characterization for Wireless Sensor Networking,” Proceedings of the IEEE Instrumentation and Measurement Technology Conference, pp. 207 – 211, April 2006.

Radio Resource Testing [a]
Random Key Pre-distribution [b]
Received Signal Strength Indicator [c]
Cooperative RSS-based Sybil Detection [d]
Mutual Guarding [e]
Packets sent and received [f]

[21] J. F., Kurose, K. W., Ross, "Computer Networking: A Top-Down Approach Featuring the Internet," May 2004.
[22] S.,Lv, X., Wang, X., Zhao, X., Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks," International Conference on Computational Intelligence and Security, pp. 442 – 446, December 2008.
[23] S., Lin, J., Zhang, G., Zhou, L., Gu, T., He, , J.A., "StankovicATPC: adaptive transmission power control for wireless sensor networks," Proceedings of the International Conference on Embedded Networked Sensor Systems, pp. 223–236, November 2006.
[24] C., Song, M., Liu, J., Cao, Y., Zheng, H., Gong, G., Chen, "Maximizing network lifetime based on transmission range adjustment in wireless sensor networks," Special Issue of Computer Communications on Heterogeneous Networking for Quality, Reliability, Security, and Robustness, Vol. 32, No. 11, pp. 1316–1325, 2009.
[25] W. T., Wang, K. F., Ssu, W. C., Chang, "Defending Sybil Attacks Based on Neighboring Relations in Wireless Sensor Networks," Security and Communication Networks, , Vol. 3, No. 5, pp. 408-420, 2010.
[26] V. S, Bhuse, "Lightweight Intrusion Detection: A Second Line of Defense for Unguarded Wireless Sensor Networks." Doctoral Dissertation, Western Michigan University, January 2007.
[27] S., Banerjee, C., Grosan, A., Abraham, P. K., Mahanti, "Intrusion Detection on Sensor Networks Using Emotional Ants." International Journal of Applied Science and Computations, Vol. 12, No. 3, pp. 152-173, 2005.
[28] B., Zeng, B., Chen, "SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless sensor network," International Conference On Computer and Communication Technologies in Agriculture Engineering, pp. 357 – 360, August 2010.
[29] D., Quercia, S., Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proceedings of IEEE INFOCOM, pp. 1-5, May 2010.