تشخیص نفوذ و ارائه راهکارهای امنیتی در شبکه های حسگر بی سیم

چکیده

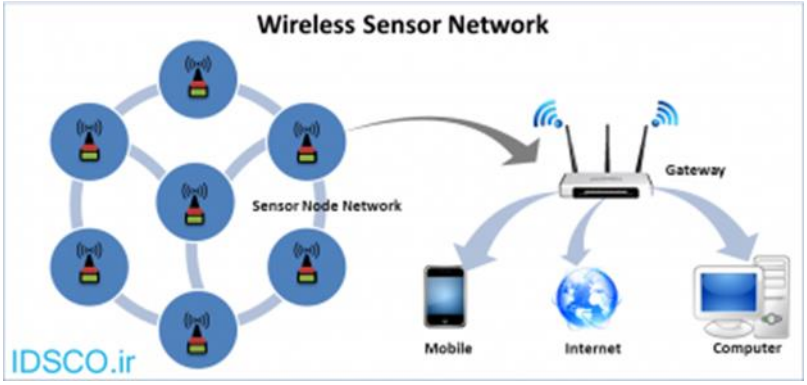
امروزه برای انواع گوناگونی از کاربردهای نظارت و مراقبت شامل کنترل ترافیک، نظارت بر محیط، نظارت بر میدان جنگ و غیره از شبکه های حسگر بیسیم که راه حل ایده آلی هستند استفاده می شود. در این شبکه های حسگر بیسیم، از هزاران گره حسگر استفاده می شود که در یک محیط وسیع و غالباً بدون نظارت و مراقبت گسترده شده اند. این شبکه ها غالبا تحت تأثیر انواع مختلفی از حملات منجمله حمله سیبیل هستند. در حملات سیبیل یک گره مخرب چندین هویت جعلی برای خود ایجاد کرده و با گمراه کردن گره های شبکه در عملیاتی مثل رأی گیری، تجمیع سازی داده ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد می کند که این خود تهدیدی جدی برای شبکه های حسگر بیسیم به شمار می آیند. در این پژوهش پس از بررسی روشهای موجود برای تشخیص حملات سیبیل در شبکه های حسگر بیسیم از یک روش توزیع شده با عامل های متحرک و اطلاعات مکانی برای شناسایی حملات سیبیل در یک مطالعه موردی استفاده خواهد شد. و نرخ از دست رفتن بسته ها قبل و بعد از اعمال متد مورد ارزیابی قرار خواهد گرفت.

کلید واژه: شبکه های حسگر بیسیم، امنیت، حملات سیبیل، مسیر یابی امن، راهکارهای مقابله با حملات.

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. شبکه های 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 می شوند. در حالیکه حضور شبکه های حسگر بیسیم در زمینه های نظامی و عمرانی افزایش پیدا می کند، نیاز به امنیت هم به یک ضرورت تبدیل میشود.

لزوما مکان قرار گرفتن گرههای حسگر، از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم.



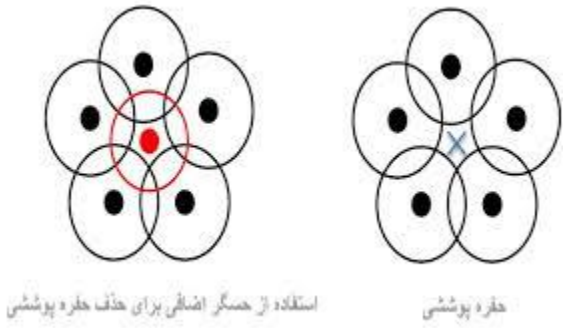
شکل ۱- گره ها در یک شبکه حسگر بیسیم

پروتکل‌ها و الگوریتم‌های شبکه‌های حسگر باید دارای توانایی‌های خود سازماندهی باشند. هر گره حسگر روی برد خود دارای یک پردازشگر است و به جای فرستادن تمامی‌اطلاعات خام به مرکز یا به گرهی که مسئول پردازش و نتیجه گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه و ساده را روی اطلاعاتی که به دست آورده است انجام می‌دهد و سپس داده‌های نیمه پردازش شده را ارسال می‌کند. با اینکه هر حسگر به تنهایی توانایی ناچیزی دارد، ترکیب صدها حسگر کوچک امکانات جدیدی را عرضه می‌کند. در واقع قدرت شبکه‌های بی‌سیم حسگر در توانایی به کارگیری تعداد زیادی گره کوچک است که خود قادرند ترکیب و سازماندهی شوند و در موارد متعددی جون مسیریابی همزمان، نظارت بر شرایط محیطی، نظارت بر سلامت ساختارها یا تجهیزات یک سیستم به کار گرفته شوند.

۲- ویژگی‌های عمومی یک شبکه حسگر

پروتکل‌های شبکه‌ای همتا به همتا یک سرویس ارتباطات مش مانند را جهت انتقال اطلاعات بین هزاران دستگاه کوچک با استفاده از روش چند جهشی ایجاد می‌کنند. معماری انطباق پذیر مش، قابلیت تطبیق با گره‌های جدید جهت پوشش دادن یک ناحیه جغرافیایی بزرگتر را داراست. علاوه بر این، سیستم می‌تواند بطور خودکار از دست دادن یک یا حتی چند گره را جبران کند.بر خلاف شبکه‌های بی‌سیم سنتی، همه گره‌ها در شبکه‌های بی‌سیم حسگر نیازی به برقراری ارتباط مستقیم با نزدیک‌ترین برج کنترل قدرت یا ایستگاه پایه ندارند، بلکه حسگرها به خوشه‌هایی تقسیم می‌شوند که هر خوشه یک سرگروه خوشه موسوم به Parent انتخاب می‌کند.

هر حسگر موجود در شبکه دارای یک محدوده حسگری است که به نقاط موجود در آن محدوده احاطه کامل دارد. با اینکه توجه زیادی به پوشش کامل منطقه توسط حسگرها می‌شود، احتمال دارد نقاطی تحت پوشش هیچ حسگری قرار نگیرند. این نقاط تحت عنوان حفره‌های پوششی نامیده می‌شوند.



شکل ۲- شماتیک حفره پوششی و شیوه حذف آن

تحمل خرابی از کار افتادن گره‌های حسگر نباید تاثیری روی کارکرد عمومی شبکه داشته باشد. بنابراین تحمل خرابی را «توانایی برقرار نگه داشتن عملیات شبکه علی رغم از کار افتادن برخی از گره‌ها» معرفی می‌کنیم.قابلیت گسترش یک شبکه باید طوری طراحی شود که بتواند چگالی بالای گره‌های حسگر را نیز تحقق بخشد. این چگالی می‌تواند از چند گره تا چند صد گره در یک منطقه تغییر کند.هزینه تولید از آنجایی که شبکه‌های حسگر از تعداد زیادی گره‌های حسگر تشکیل شده‌اند، هزینه یک گره در برآورد کردن هزینه کل شبکه بسیار مهم است.

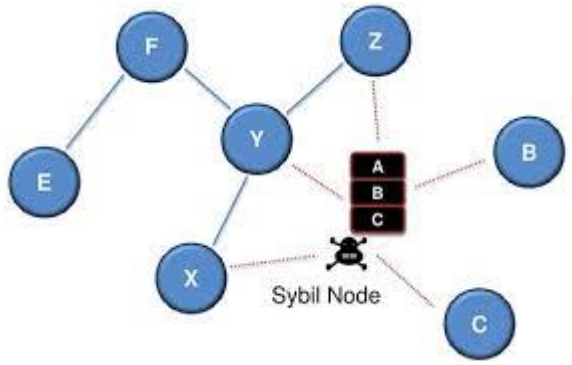
۳- نیازمندی‌های امنیتی و انواع حملات شبکه‌های حسگر

قابلیت اعتماد داده‌ها، جامعیت داده‌ها، تازگی داده، دسترس پذیری، خودسازماندهی، استقرار امن، استفاده از الگوریتم SeRLoc[۱]، احراز هویت سیستم و...

حملات سیبیل[۲] به راحتی قابل پیاده سازی در شبکه های حسگر بی سیم هستند چون گره های حسگر در یک محیط توزیع شده قرار گرفته اند و از طریق امواج رادیوئی با یکدیگر ارتباط برقرار می کنند. همین قابلیت، این امکان را برای حمله خرابکاران به شبکه فراهم می کند.

حملات سیبیل تهدیدی جدی برای شبکه های حسگر بی سیم به شمار می آیند. در چنین حملاتی، یک گره مخرب چندین هویت جعلی برای خود ایجاد کرده و گره های شبکه را گمراه می کند [۱-۲]. این حملات میتوانند در عملیاتی مثل مسیریابی، رأی گیری، تجمیع سازی داده ها، ارزیابی اعتبار گره ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد کنند [۳]. مکانیزمهایی که مبتنی بر رأی گیری هستند کارایی خود را از دست میدهند چون برخی گره ها جعلی هستند و نمی توان به اطلاعات به دست آمده از آنها اعتماد کرد [٤].

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 تانک ها را جمع آوری می کنند بسیار مهم است. حملات سیبیل از این جهت یکی از مهمترین حملات در شبکه های حسگر بیسیم به شمار می آیند که می توانند بستر لازم برای بسیاری دیگر از حملات را فراهم کنند [٥]. همچنین این حمله ترافیک کنترلی را مورد هدف قرار داده و خرابی وسیعی را در شبکه باعث می شود.



شکل ۳- گره های حمله سیبیل

[۱] (Secure Range-In depended Localization

[۲] Sybil

با توجه به سادگی پیاده سازی این حملات و حساس بودن اطلاعات در این نوع شبکه ها، ارائه راهکارهایی که بتوانند حملات سیبیل را تشخیص دهند و در صورت امکان با آن مقابله کنند بسیار ضروری می باشد. این راهکارها باید محدودیتهای پردازشی، حافظه و توان در شبکه های حسگر بی سیم را نیز در نظر گرفته باشند تا بطور عملی قابل استفاده در این شبکه ها باشند.

برای دفاع در مقابل حمله Sybil، ما باید اینکه هویت هر گره تنها هویت ارائه شده توسط یک گره فیزیکی مترادف است را قانونی کنیم. دو راه برای معتبر کردن یک هویت وجود دارد: راه اول «تایید مستقیم» است که در آن یک گره مستقیما بررسی می‌کند که ایا هویت گره دیگر معتبر است یا خیر؟ نوع دوم «تایید غیر مستقیم» است که در آن گره‌هایی که هم اکنون محقق شده اند، اجازه ضمانت یا تکذیب سایر گره‌ها را دارند.

در ادامه روشهایی است که تاکنون برای تشخیص حملات سیبیل در شبکه های حسگر بیسیم ارائه شده اند بررسی می شود و بهترین روش در یک مطالعه موردی مورد ارزیابی قرار می گیرد.

٤- حملات سیبیل

دوسر[1] ادعا کرد در چنین محیط های محاسباتی توزیع شده ای، یک دستگاه می تواند به راحتی چندین هویت (شناسه) اختیار کند که این به دلیل فقدان یک قدرت مرکزی و مورد اعتماد در شبکه است. راه حلهای متنوعی برای تشخیص این حمله و حذف آن از بستر شبکه پیشنهاد شده است. که در ادامه می آید

- روشهای رمزنگاری و احراز هویت
- روشهای اطلاعات دریافتی از گره ها
- روشهای هوشمند
- روشهای مکان یابی سیگنال دریافتی(RSSI[2]) [٧].

٤-١- روشهای رمزنگاری و احراز هویت

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 می کنند. چاهک هویت دو گره را از طریق کلیدهای متقارن آنها بررسی کرده و سپس یک کلید مشترک برای هر دو آنها ارسال می کند تا آنها بتوانند بصورت مستقیم با یکدیگر ارتباط برقرار کنند بالعکس هنگام استفاده از

---

[1] Douceur

[2] Received Signal Strength Indicator

روشهای رمزنگاری نامتقارن، ابتدا کلیدهای عمومی و خصوصی بین همه گره های شبکه توزیع میشود، سپس امضای دیجیتال ایجاد می شود [٤]. رمزنگاری کلید عمومی برای حسگرهای بیسیم کوچک از لحاظ محاسباتی مقرون به صرفه نیست. رمزنگاری با کلید عمومی و یا تعیین هویت پیغام در گره های حسگر چندین ثانیه زمان میبرد [٦]. سیستمهای کلید عمومی، حافظه بیشتری نسبت به سیستمهای کلید متقارن مصرف می کنند. 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 می دهند. بنابر دلایل ذکر شده، بیشتر راه حلهای رمزنگاری موجود برای شبکه های حسگر بی سیم، بر مبنای سیستمهای کلید متقارن هستند. اما در سیستم های کلید متقارن هم توزیع کلید یک چالش مهم به حساب می آید [٥].

کارلوف و واگنر[١] در مورد مزایای نسبی تکنیک های رمزنگاری متقارن و غیرمتقارن برای حفاظت از شبکه های حسگر بیسیم در برابر حملات سیبیل صحبت کرده اند [٧]. آنها بیان کردند که شبکه های 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 گره ها را پیشنهاد داده اند که به دلیل محدودیت گره های حسگر در منابع ذخیره سازی و محاسباتی، روش مناسبی نیست. از جهتی دیگر استفاده از کلیدهای رمزنگاری همیشه نمی تواند باعث تشخیص و جلوگیری از حمله سیبیل شود. نیوسام[٢] و همکارانش چندین روش برای حفاظت از شبکه های حسگر بیسیم در برابر حملات سیبیل پیشنهاد داده اند، که شامل یک مکانیزم تست منابع رادیوئی (RRT[٣]) و یک مکانیزم پیش توزیع تصادفی کلید (RKP[٤]) می شود [٣]. مکانیزم RRT بر پایه این فرض بنا نهاده شده است که گره ها در یک شبکه عام قابلیت انتقال همزمان روی بیش از یک کانال را ندارند. هنگامی که 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 کانال های اختصاص داده شده به آنها پخش کنند. سپس گره مذکور بطور تصادفی گیرنده خود را روی یکی از کانالها تنظیم می کند و منتظر دریافت پیغام تصدیق میشود. اگر هیچ پیغام تصدیقی دریافت نکرد، به گره مذکور مشکوک می شود. 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 گره های جعلی با احتمال بالایی قابل تشخیص هستند. در روش RKP هر

---

[١] Karlof & Wagner

[٢] Newsome

[٣] Radio Resource Testing

[٤] Random Key Pre-distribution

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

برای جلوگیری از حملات سیبیل می توان از رمزنگاری کلید متقارن استفاده کرد [۸]. ژانگ[۱] و همکارانش در این روش از یکی از ویژگیهای مهم درخت های درهم سازی مرکل استفاده می کند، 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 گره های شبکه را بررسی و تأیید کند [۹]. این روش تنها در شبکه های حسگر بیسیم با مقیاس کوچک کارا است. روشهای احراز هویت [۸-۱۰] غالباً نیاز به فضای حافظه زیادی برای ذخیره اطلاعات هویت ضروری (مثل کلیدهای رمزنگاری مشترک، شناسه ها و غیره) و پردازش های پیچیده دارند. بعلاوه اینکه اگر مهاجمی بتواند به مکانیزم احراز هویت نفوذ کند، آنگاه جامعیت کلی مکانیزم حفاظتی از بین می رود [٤].

٤-۲- روشهای بر اساس اطلاعات دریافتی از گره ها

در روشی دیگر برای مقابله با حملات سیبیل در شبکه های حسگر بیسیم سو[۲] و همکارانش هویت گره ها را با استفاده از تجزیه و تحلیل اطلاعات گره های همسایه هر گره بررسی و بازبینی کرده اند [٤]. این روش از این واقعیت که هر گره مخرب تعداد زیادی هویت جعلی ایجاد میکند استفاده کرده تا مکانیزمی برای حفاظت از شبکه های حسگر بی سیم در برابر حملات سیبیل ارائه دهد. در این روش این فرض که شبکهای با تراکم گره بالا داریم رعایت شده است، احتمال اینکه دو گره متفاوت دارای مجموعه همسایگی دقیقاً یکسان باشند بسیار کم است. در حملات سیبیل، گره های 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 گره های همسایه گره قربانی و بررسی اینکه آیا برخی از این گره ها مجموعه همسایگی مشابه هم دارند یا خیر و بنابراین گره های سیبیل هستند، تشخیص داد. آنها امکانپذیری روش خود را هم با قوانین ریاضی و هم بصورت عددی ارزیابی کرده اند. همچنین اعتبار آن را بصورت تجربی و با استفاده از ۸ گره (Tmote sky) نیز بررسی کرده اند. مکانیزم دفاع توسط یک گره نرمال که به قربانی بودن خود مشکوک است انجام می گیرد. نکته قابل توجه در این روش این است که روش پیشنهادی به جای اینکه اقدام به بازجویی هر گره کند، متکی به

---

[۱] Zhang

[۲] Ssu

فرآیند ساده جمع آوری 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. آنها در مکانیزم دیگری در بهبود روش خود بیان کردند که اگر بتوان گره مخرب را حذف کرد آنگاه دیگر این گره موثر نخواهد بود و بقیه همسایگان گره قربانی، گره های نرمال خواهند بود. از آنجائیکه تنظیم دامنه، ارتباطی گرههای حسگر به طور وسیعی انجام میگیرد [۲۳-۲٤]، 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 می یابد. در این صورت گره مخرب اثر خود را از دست داده و تعداد تشخیص های غلط کاهش پیدا می کند. آنها کار خود را در مرجع [۲۵] ادامه دادند.

باوس[۱] در رساله خود دو روش برای تشخیص حملات سیبیل به نامهای (MG[۲]) و (SRP) ارائه داد که این دو روش مکمل یکدیگر هستند [۲٦]. روش (MG) برای زمانی است که گره مخرب شناسه یکی از گره های همسایه را در اختیار خود می گیرد . دو گرهای که در دامنه ارتباطی هم هستند می توانند بسته های 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 گره ها جا زند چون توسط آنها تشخیص داده می شود. 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 شناسه ای اختیار می کند که در همسایگی اش نیست. سپس با مبادله اطلاعاتی درباره تعداد بسته های دریافتی هر گره و مقایسه تعداد بسته های ارسال شده و دریافت شده حمله سیبیل تشخیص داده میشود.

٤-۳- روشهای هوشمند

بانرجی[۳] و همکارانش یک مکانیزم تشخیص نفوذ مبتنی بر کلونی مورچه ها برای شبکه های حسگر بیسیم پیشنهاد دادند. [۲۷] .ژانگ و همکارانش نیز با استفاده از الگوریتم کلونی مورچه ها سعی در کاهش تأثیر حملات سیبیل در شبکه های حسگر بیسیم دارند. در شبکه ای که گره های سیبیل داریم، گره سیبیل میتواند به گرههای نرمال شبکه متصل شود و در نتیجه یک یال بین گره سیبیل و گره نرمال برقرار می شود. با کمک ماهیت الگوریتم کلونی مورچه ها می توان تعداد این یال های مخرب را کاهش داد[۲۸]. کورچا[٤] و همکارش

---

[۱] Bhuse

[۲] Mutual Guarding

[۳] Banerjee

[٤] quercia

روشی غیرمتمرکز برای تشخیص حملات سیبیل در شبکه هایی با گرههای متحرک ارائه دادند. در این روش هر گره دو مجموعه که متشکل از اطلاعات مربوط به گره ها می باشد را جمع آوری و نگهداری می کند. یک مجموعه شبکه دوستان و دیگری شبکه مهاجمان را تشکیل میدهد. مجموعه اول شامل گره های قابل اعتماد و مجموعه دوم شامل گره هایی است که گره به آنها مشکوک است [۲۹].

٤-٤- روشهای مبتنی بر مکان یابی (سیگنال دریافتی)

دمیراباس و سونگ[۱] استفاده از شاخص قدرت سیگنال دریافتی (RSSI[۲]) را برای تشخیص حملات سیبیل پیشنهاد داده اند [۱۱]. گره به هنگام دریافت پیغام از یک فرستنده جدید، RSSI آن پیغام را محاسبه می کند. سپس 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.

ژانگ[۳] و همکارانش استفاده از نسبت RSSI را برای تشخیص مکان فرستنده با استفاده از چهار گره ناظر مطرح کردند [۱۲]. میتوان از الگوریتم موقعیت یابی پیشنهاد شده در این پژوهش 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 می شود. باید توجه داشت برای تشخیص این حمله، محاسبه مکان کار طاقت فرسا و غیر ضروری می باشد. 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 RSSI ها استفاده کردند.

وانگ[٤] و همکارانش نیز مکانیزم مشابهی برای تشخیص حملات سیبیل در شبکه های حسگر بیسیم مبتنی بر کلاستر پیشنهاد داده اند [۱۳]. آنها مدل کانال جکس را پیاده سازی کرده اند که در آن تأثیر خطاهای ناشی از محو شدگی و افت مسیر در کانالهای ارتباطی شبکه های حسگر بیسیم مورد توجه و بررسی قرار گرفته اند. سپس یک روش ترکیبی برای تشخیص حملات سیبیل ارائه داده اند که این حملات را با توجه به (RSSI)دریافتی از گره ها و در نظر گرفتن اطلاعاتی که توسط گره های شبکه تهیه و ارسال میشوند تشخیص

---

[۱] Demirbas & Song

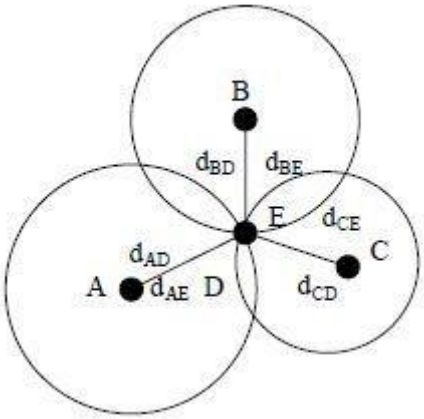
[۲] Received Signal Strength Indicator

[۳] Zhong

[٤] Wang

میدهد. مکانیزمی مبتنی بر (TDOA)برای تشخیص حملات سیبیل در شبکه های حسگر بیسیم مبتنی بر کلاستر ارائه شده است [١٤]. در این روش در هر کلاستر سه گره راهنما داریم. گره های حسگر درون یک کلاستر توسط این سه گره شنیده می شوند حسگر درون یک کلاستر توسط این سه گره شنیده می شوند.

گره های راهنما از مکان خود مطلع هستند (مثلاً از طریق سیستم (GPS)و غیره). با ارسال پیغام توسط گرهها (TDOA) بین گره فرستنده و گره های راهنما محاسبه می شود. 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 شخیص حملات سیبیل در شبکه های حسگر بی سیم مورد استفاده قرار میگیرد. از آنجائیکه گره های سیبیل توسط یک گره مخرب ایجاد میشوند، پس در یک مکان فیزیکی قرار گرفته اند. در نتیجه فاصله این گرهها (سیبیل) از یک سری گره ها باید یکسان باشد[١٥].



شکل ٤- نمونه ای از مسافت یابی گره ها

الوی[١] و همکارانش روشی تحت عنوان CRSD[٢] برای شبکه های حسگر بیسیم ثابت ارائه کرده اند که از قدرت سیگنال که از قدرت سیگنال دریافتی برای اندازه گیری فاصله بین دو گره استفاده می کند [٢٢]. این روش از کمک چندین گره همسایه (قابلیت همکاری گره ها) استفاده میکند و فاصله بین گره موردنظر را تا این گره ها محاسبه می کند. در این روش فرض بر اینست که توان ارسالی برای همه گرهها (نرمال و مخرب) یکسان و ثابت است. همه گره های سیبیل دارای مکان فیزیکی مشترک هستند [١١]، پس این روش برای تشخیص حملات سیبیل از مکان گره ها و (RSS) استفاده می کند. یک گره برای تشخیص حمله، گره هایی

[١] LV

[٢] Cooperative RSS-based Sybil Detection

که تا این گره فاصله یکسانی دارند و مقدار (RSS) مشابهی هم دارند را در یک گروه قرار می دهد. گره هـایی که در یک گروه قرار می گیرند گره های سیبیل هستند.

۵- مطالعه موردی

در یک مطالعه موردی در یک بسته عامل که دارای یک تابع به نام Detect بوده کـه وظیفـه آن تشـخیص وجود حمله سیبیل است این مطالعه را به پایان می بریم. این تابع در صورت یافتن گره های مشکوک بـه سـیبیل آنها را در لیستی قرار می دهد که الگوریتم آن در ادامه خواهد آمد. در این جا فیلد هـای Srcld و Dstld بـرای ذخیره گره های مبدا و مقصد در انتقال از یک گره به گره همسایه می باشد.

۵-۱- الگوریتم

الگوریتم ارائه شده شامل دو فاز آماده سازی شبکه و نگهداری شبکه می باشد. در فاز آماده سازی گره ها بصورت یکنواخت توزیع شده و در محدوده شبکه قرار می گیرند و ایستگاه پایه بر حسب درصد مطلوبی، تعداد گره هایی که برای ایستگاه پایه قابل اعتماد است به صورت رندوم ارسال می کند. این گـره هـا بعـد از دریافـت بسته عامل به عنوان گره عامل انتخاب می شوند و در فاز نگهداری نیز همسایه هایی کـه بـه عنـوان عامـل حملـه شناخته می شوند حذف می کند که این فرآیند در چند مرحله انجام می شود. در هر دور گره ها یک بسته برای ساخت ماتریس همسایگی و یافتن همسایه های درون دامنه فرکانسی پخش می کنند.

پس از یاقتن همسایه های هر گره، هر مدخلی از ماتریس همسایگی شامل شناسه های گره های همسـایه ۱ می باشند و در این شرایط trustbit و agentbit مربوط بـه همسـایه در جـدول بصـورت false اسـت. در هنگـام یافتن همسایه ها تک گره ها یک حافظه ای از گره های ملاقاتی ذخیره مـی کننـد. پـس از یـافتن همسـایه هـا و جمع آوری حافظه ها مربوط به آن دور، هر گره یک بسته به نام Msg که شامل اطلاعات جمع آوری شده و نیز اطلاعات خود گره شامل شناسه و مکان و ... ایجاد می شود.

الگوریتم تشخیص بصورت ذیل می باشد:

```
۱- listmsg ← Receive-from-neighbors ();
۲- foreach (msgi, msgj) listmsg do
۳- if msgi.pos ==msgj.pos then
٤- if msgi.id !=msgj.id then
٥- Raise-alarm ();
```

٦- if Check (msgi. History, msgj. History) == false then

٧- Raise-alarm ();

۵-۲- تشخیص حمله

در این متد در هر دوره، همه گره عامل ها با فراخوانی تابع تشخیص msg موجود در لیست خود را با هم مقایسه می کنند.این مقایسه به این صورت است که در ابتدا اطلاعات فرستنده های msg باهم مقایسه می شود. سپس اطلاعات هر گره فرستنده با حافظه جمع آوری شده توسط دیگر گره ها مقایسه می شود. اگر بیش از یک گره در یک مکان با یک شماره دور مشاهده شد، آن گره به عنوان حمله سیبیل به آن عامل قرار می گیرد و عامل trudtbit برای تمام گره های موجود در لیست LId را false می کند. در این روش، برای مسیر یابی از پروتکل (aodv[۱]) استفاده می شود و همین طور برای عدم برخورد در دسترسی به رسانه انتقال (MAC) از پروتکل CSMA/CA[۲] استفاده شده است [۱۲]. پیشگیری از تصادم برای بهبود کارایی CSMA مورد استفاده قرار می گیرد. روش کار بدین صورت است که اگر گره ای در حال ارسال اطلاعات می باشد، گره دیگر اجازه ارسال نخواهند داشت، بنابراین با این کار احتمال تصادم به حداقل می رسد.

در ادامه برای آزمایشات دو سری شبیه سازی صورت گرفته شده است، یک سری از شبیه سازی ها فقط پروتکل AODV را بدون هیچ مکانیزم ارائه امنیتی اجرا کرده ایم و در سری دوم شبیه سازی ها از مکانیزم ارائه شده استفاده شده است. تمام آزمایش ها در یک محیط ۲۰۰×۲۰۰متر مربع انجام گرفته است. آزمایش ها شامل چند اجرای شبیه سازی است و در هر شبیه سازی زمان اجرا ۲۰ دقیقه در نظر گرفته شده است. تعداد گره ها ۱۰۰عدد است. در هر اجرا تعداد گره های سیبیل ۵ عدد است و این گره ها به صورت رندوم در محیط پخش شده اند.

۵-۳- نتایج خروجی

تعداد بسته های تحویلی به گره های مهاجم

تعداد بسته های تحویل داده شده به گره های متخاصم[۳] می باشد. در این حالت فرض شده است با رسیدن بسته به گره های متخاصم بسته در شبکه از بین خواهد رفت. نرخ PL تعداد بسته ی تحویل داده شده به متخاصم نسبت به کل بسته های انتقالی در شبکه است. در شکل زیر نمودارهای مربوط به PL شبکه برای تعداد گره های

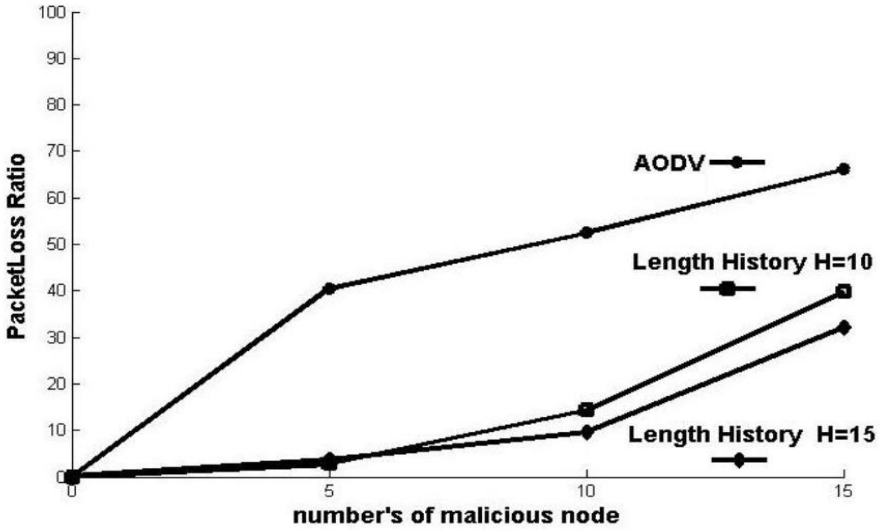
---

[۱] Ad Hoc on Demand Distance Vector

[۲] CSMA/CA اصلاحی برای دسترسی چندگانه با قابلیت شنود سیگنال حامل می باشد.

[۳] packet loss (PL)

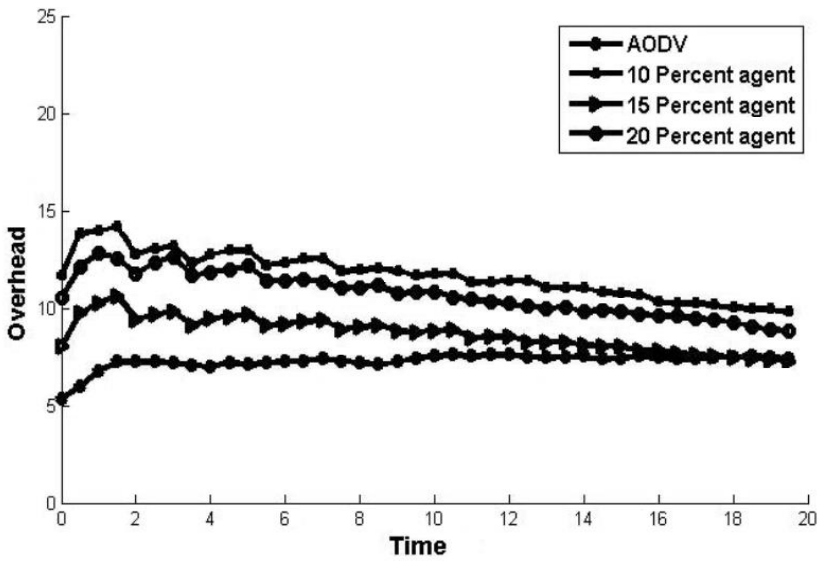
متخاصم متفاوت۵، ۱۰ و ۱۵ با اندازه حافظه های (H) متفاوت ۱۰و۱۵ در مقایسه با پروتکل AODV نشان داده شده است. همان طور که مشاهده می شود نرخ PL در متد ارائه شده باH برابر ۱۵ از بقیه کمتر است. این به این دلیل است که حافظه بیشتری نگهداری می شود و در نتیجه گره های متخاصم زودتر شناخته شده و از لیست همسایگی حذف می شوند. همین طور پروتکل AODV تعداد PL بیشتری دارد به دلیل اینکه هیچ مکانیزم امنیتی در آن تعبیه نشده است.



شکل ۵- نرخ تعداد بسته های تحویلی به گره های مهاجم (Packet Loss Ratio)

سربار ناشی از پیام های اضافی

سربار ناشی از پیام های اضافی مبادله شده بین گره ها به علت استفاده از عامل های متحرک جهت تشخیص حمله مهم می باشد. برای محاسبه این نرخ تعداد بسته های عامل متحرک مبادله شده به کل بسته های مبادله در شبکه را محاسبه می کنیم. همان طور که در شکل زیر می بینیم، پروتکل AODV نرخ سربار کمتر و ثابتی دارد. اما در ابتدا بسته های عامل متحرک بیشتری در شبکه مبادله می شود و رفته رفته این مقدار کاهش می یابد. دلیل کاهش، این است که بعد از شناسایی گره های مورد اعتماد، تعداد بسته های معمولی مبادله شده بین گره ها نسبت به بسته عامل افزایش می یابد. در نتیجه نرخ استفاده از بسته عامل نسبت به کل یسته ها کاهش می یابد.



شکل ٦- میزان سربار ناشی از شبیه سازی صورت گرفته

٦- نتیجه گیری

در حملات سیبیل یک گره مخرب چندین هویت جعلی برای خود ایجاد کرده و با گمراه کردن گره های شبکه در عملیاتی مثل رأی گیری، تجمیع سازی داده ها، تخصیص عادلانه منابع و تشخیص بدرفتاری اختلال ایجاد می کند که این خود تهدیدی جدی برای شبکه های حسگر بیسیم به شمار می آیند. روشهایی که برای شبکه های حسگر بی سیم ارائه میشوند باید محدودیتهای این شبکه ها در منابع پردازشی، حافظه و توان را درنظر بگیرند. بسیاری از روشها برای تشخیص حملات سیبیل در این شبکه ها، این محدودیتها را در نظر نگرفته اند.

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 هوشمند روشهای جدیدی برای تشخیص حملات به شمار میسوند. این روش ها در صورتیکه منجر به سربار پردازشی نشوند روشهای مناسبی هستند. روشهای مبتنی بر مکانیابی بعضاً نیاز به سخت افزارهای اضافی مثل GPS و گره های ناظر دارند که در نتیجه هزینه شبکه حسگر را بالا برده و همچنین مصرف انرژی را افزایش میدهند. از دیگر روشها، متد های مبتنی بر اطلاعات دریافتی از گرهها نام برد. روشهای مذکور میتوانند روش های 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 می شود.

در این پژوهش یک مکانیزم تشخیصی حملات سیبیل در شبکه های حسگر به کار برده شده است. این روش ارائه شده با استفاده از حافظه جمع آوری شده توسط هر گره و عامل متحرک گره های مهاجم را از لیست همسایگی هر گره حذف می کند و مانع استفاده آن ها برای مسیریابی می شود. هر گره متخاصم با استفاده ازfasle کردن اعتبار مربوط در جدول همسایگی گره ها حذف خواهد شد. عامل قطعه کد اجرایی است که با استفاده از الگوریتم ارائه شده در گره های متخاصم را تشخیص می دهد. در نتیجه مسیریابی امن برقرار می شود.

۷- منابع و مواخذ

[۱] J.R. Douceur, “The Sybil attack,” in Proc. of the International Workshop on Peer-to-Peer Systems,” March ۲۰۰۲, pp. ۲۵۱-۲٦۰.

[۲] Z. Su, C. Lin, F. Ren, X. Zhan, “Security mechanisms analysis of wireless sensor networks specific routing attacks,” in Proc. of ۲۰۰٦ ۱st International Symposium on Pervasive Computing and Applications, pp. ۵۷۹–۵۸٤.

[۳] J. Newsome, E. Shi, D. Song and A. Perrig, “The Sybil attack in sensor networks: analysis and defenses,” in Proc. of ۲۰۰٤ International Symposium on Information Processing in Sensor Networks, pp. ۲۵۹–۲٦۸.

[٤] K. F. Ssu, W. T. Wang, W. C. Chang, “Detecting Sybil Attacks in Wireless Sensor Networks Using Neighboring Information”,Computer Networks, vol. ۵۳, no. ۱۸, pp. ۳۰٤۲-۳۰۵٦, Dec. ۲۰۰۹.

[۵] S. Misra, I. Woungang, S. C. Misra, Guide to Wireless Sensor Networks, Springer, ۲۰۰۹, pp. ٤۹۱-۵۱۲.

[٦] 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. ۷۱ – ۸۰, ۲۰۰٤.

[۷] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in Proc. of ۲۰۰۳ IEEE International Workshop on Sensor Network Protocols and Applications, pp. ۱۱۳–۱۲۷.

[۸] Q. Zhang, P. Wang, D.S. Reeves, P. Ning, “Defending against Sybil attacks in sensor networks,” in Proc. of ۲۰۰۵ IEEE International Conference on Distributed Computing Systems Workshops, pp. ۱۸۵–۱۹۱.

[٩] 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. ٢٤, no. ٢, pp. ٢٤٧-٢٦٠, Feb. ٢٠٠٦.

[١٠] D., Liu, P., Ning, “Establishing pairwise keys in distributed sensor networks,” Proceedings of the ACM Conference on Computer and Communications Security, pp. ٥٢–٦١, October ٢٠٠٣.

[١١] 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. ٥٦٤–٥٧٠, ٢٠٠٦.

[١٢] 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-١٢٩٧, Yale Computer Science, July ٢٠٠٤.

[١٣] 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. ٢٦٨٤-٢٦٨٧, ٢٠٠٧.

[١٤] 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 .١٢, No.١, pp ٦٦-٧٠, ٢٠٠٨.

[١٥] R., Xiu-li, Y., Wei, “Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network” ٥th International Conference on Wireless Communications, Networking and Mobile Computing, pp. ١ – ٤, ٢٠٠٩.

[١٦]Z., Zhi-Guang, “A WSN Node Ranging Method Based on Phase Difference Measuremen,” Chinese Journal of Sensors and Actuators, Vol. ٢٠, No. ١٢, pp. ٢٧٢٨-٢٧٣٢, December ٢٠٠٧.

[١٧] 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. ٨٣٤ – ٨٣٩, October ٢٠٠٨.

[١٨]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. ١٠٠٥ – ١٠٠٩, April ٢٠٠٨.

[١٩]F., Amini, J., Misic, H., Pourreza, “Detection of Sybil Attack in Beacon Enabled IEEE٨٠٢،١٥،٤ Networks,” International Conference on Wireless Communications and Mobile Computing, pp. ١٠٥٨ – ١٠٦٣, August ٢٠٠٨.

[٢٠]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. ٢٠٧ – ٢١١, April ٢٠٠٦.

[٢١] J. F., Kurose, K. W., Ross, “Computer Networking: A Top–Down Approach Featuring the Internet,” May ٢٠٠٤.

[٢٢]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. ٤٤٢ – ٤٤٦, December ٢٠٠٨.

[٢٣]S., Lin, J., Zhang, G., Zhou, L., Gu, T., He, J.A.“Stankovic ATPC: adaptive transmission power control for wireless sensor networks,” Proceedings of the International Conference on Embedded Networked Sensor Systems, pp. ٢٢٣–٢٣٦, November ٢٠٠٦.

[٢٤] 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. ٣٢, No. ١١, pp. ١٣١٦–١٣٢٥, ٢٠٠٩.

[٢٥]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. ٣, No. ٥, pp. ٤٠٨-٤٢٠, ٢٠١٠.

[٢٦] V. S, Bhuse, “Lightweight Intrusion Detection: A Second Line of Defense for Unguarded Wireless Sensor Networks”. Doctoral Dissertation, Western Michigan University, January ٢٠٠٧.

[٢٧] 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. ١٢, No. ٣, pp. ١٥٢-١٧٣, ٢٠٠٥.

[٢٨] 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. ٣٥٧ – ٣٦٠, August ٢٠١٠.

[٢٩] D., Quercia, S., Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proceedings of IEEE INFOCOM, pp. ١-٥, May ٢٠١٠.