نشریه علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»

سال اول، شماره ۲، تابستان ۱۴۰۰؛ ص ۵۸- ۵۱

علمی – تخصصی

ارائه روشی به‌منظور تشخیص و مقابله با حملات کرم‌چاله و سیاه‌چاله در شبکه‌های Ad-Hoc

رضا مولایی فرد*

کارشناسی ارشد گروه کامپیوتر دانشگاه آزاد اسلامی واحد دزفول،ایران

(دریافت: ۱۴۰۰/۰۳/۰۶، پذیرش: ۱۴۰۰/۱۰/۲۲)

چکیده

امروزه شبکه‌های حسگر بی‌سیم در معرض حملات خطرناکی هستند که می‌توانند شبکه را مختل کنند. یکی از این حملات مخرب، حملات کرم‌چاله و سیاه‌چاله می‌باشد که می‌تواند شبکه را با خطرات جدی مواجه کند. شناسایی و تشخیص به‌موقع این حملات می‌تواند باعث بهبود عملکرد شبکه شود. در این تحقیق به ارائه روشی به‌منظور بهبود، شناسایی، تشخیص و مقابله به حملات کرم‌چاله و سیاه‌چاله پرداخته می‌شود. روش پیشنهادی موردنظر با استفاده از ترکیب دو روش مبتنی بر RTT و روش شناسایی انتها به انتها می‌باشد. در شبکه‌های حسگر بی‌سیم وقتی حمله کرم‌چاله رخ می‌دهد طبیعی است که تعداد همسایگان گره از حد معمول بیشتر خواهد شد، بنابراین ما از این اطلاعات برای شناسایی و حملات کرم‌چاله‌ها استفاده کنیم. نتایج حاصل از این تحقیق حاکی از بهبود تشخیص و مقابله حملات می‌باشد به‌نحوی‌که در بخش‌های، میانگین نرخ بسته‌های رسیده، تعداد RREQ های پذیرفته‌شده در مقصد، مقایسه متوسط انرژی مصرفی، میزان حذف گره‌ها و میزان سربار سیستم توانست عملکرد قابل قبولی نسبت به سایر روش‌های موجود به‌دست آورد.

کلیدواژه‌ها: شبکه حسگر، کرم‌چاله، سیاه چاله، روش RTT، روش شناسایی انتها به انتها

۱- مقدمه

پیشرفت‌های روزافزون در ساخت مدارات مجتمع و همچنین توسعه ارتباطات بی‌سیم باعث توسعه ریزحسگرهایی گردیده است که شاکله اصلی یک شبکه حسگر بی‌سیم را ایجاد می‌کنند. به‌عبارت‌دیگر یک شبکه حسگر متشکل از گره‌هایی است که به‌صورت متراکم در محیط پخش‌شده و با همکاری یکدیگر یک وظیفه مشترک را انجام می‌دهند. امروزه شبکه‌های حسگر بی‌سیم در حوزه‌های مختلف نظامی، بهداشت و درمان، نظارت بر زیستگاه، نظارت بر فرایندهای صنعتی کاربردهای ویژه‌ای دارند. شبکه حسگر بی‌سیم از چندین گره کوچک به نام حسگر تشکیل می‌شوند. این گره‌ها باهم در ارتباط بوده و در راستای انجام‌وظیفه یا وظایفی با همدیگر همکاری می‌کنند. حملات مختلفی وجود دارد که می‌توانند این شبکه‌ها را تهدید کنند. حمله کرم‌چاله و سیاه‌چاله ازجمله حملاتی است که در لایه شبکه باعث اختلال در پروتکل‌های مسیریابی می‌شود. در جمله کرم‌چاله، بسته‌های یک منطقه از شبکه از طریق لینک سریع و خارج از باند، به منطقه دیگری از شبکه منتقل‌شده و بازپخش می‌شوند. این عمل باعث می‌شود گره‌هایی که ازنظر فیزیکی در همسایگی هم قرار ندارند، به‌طور ناخودآگاه یکدیگر را به‌عنوان همسایه شناسایی کنند. حمله کرم‌چاله و سیاه‌چاله یک نوع حمله فعال است که در لایه سوم شبکه‌های حسگر بی‌سیم رخ می‌دهد. در این جمله مهاجمان با متقاعد کردن گره فرستنده برای ارسال اطلاعات از یک مسیر جعلی که کوتاه‌تر و سریع‌تر از مسیر عادی به نظر می‌رسد، سعی دارند ارسال بسته‌ها از تونل ایجادشده انجام شود تا بتوانند حملات تحلیل ترافیک، انکار سرویس، رها کردن بسته‌ها و یا جلورانی انتخابی را انجام دهند. هر پروتکلی که از مقیاس کمترین تأخیر و کمترین تعداد گام برای مسیریابی استفاده کند؛ بنابراین به‌منظور دست‌یابی به هدف ارسال بسته‌ها در شبکه، هر گره به‌عنوان یک میزبان، همانند یک دستگاه مسیریابی همکاری می‌کند. این مسئله، مسیر ارتباطی مشترک بین گره‌هایی که در محدوده انتقالی یکدیگر قرار ندارند، تشکیل می‌دهد. در این شبکه‌ها، انتقال توسط پروتکل‌های مسیریابی ادهاک، مدیریت می‌شوند. به‌طوری‌که این پروتکل‌ها به گره‌ها اجازه می‌دهند تا کلیه مسیرهای ارتباطی به سمت گره‌های دیگر را از طریق به‌روزرسانی پویای مسیر ارتباطی کشف نمایند. تاکنون تحقیقاتی در مورد کشف کرم‌چاله و سیاه‌چاله صورت

* رایانامه نویسنده مسئول: rezamolae4@gmail.com

گرفته که ازجمله مشکلات تحقیقات پیشین می‌تواند به عدم شناسایی تمامی حملات در شبکه اشاره کرد که این مشکل می‌تواند سبب بروز تکرار حملات گردد که در این تحقیق سعی شده که کلیه حملات شناسایی و با کلیه این حملات مقابله گردد. در این تحقیق به ارائه روش جدیدی به‌منظور تشخیص، جلوگیری و بهبود حملات کرم‌چاله و سیاه‌چاله در شبکه‌های حسگر بی‌سیم پرداخته می‌شود که تا حدود زیادی می‌تواند روش‌های پیشین را بهبود بخشد.

۲- کارهای پیشین

کالیار و همکاران در مقاله خود در سال ۲۰۲۰ به ارائه روشی به‌منظور تشخیص حملات کرم‌چاله در اینترنت اشیاء پرداختند. این محققان در مقاله خود با استفاده از دو تهدید عمده به نام حملات PRL و کرم‌چاله را سعی کردند حملات کرمم چاله را از بین ببرند. روش پیشنهادی آنها برای پیدا کردن عامل مشترک با بالاترین رتبه در میان اجدادی که یک گره در درخت شبکه هدف دارند، از مفهوم بالاترین رتبه اجداد مشترک (HRCA) بهره گرفتند. دو الگوریتم تشخیص نه تنها یک حمله مداوم را شناسایی می‌کنند بلکه موقعیت تهدید را در شبکه محلی تشخیص می‌دهند؛ بنابراین روند تخفیف را سبک و سریع می‌کند. دو روش شبیه‌سازی را در Cooia، شبیه‌ساز شبکه پیاده‌سازی شده که نتایج به‌دست‌آمده از آزمایش‌های اجرای پیشنهادهای مربوط به نرخ مثبت واقعی، زمان تشخیص، نسبت تلفات بسته، مصرف حافظه و سربار شبکه را بهبود بخشیده است [۱].

گوماتی و همکاران در مقاله خود در سال ۲۰۲۰ به ارائه روشی به‌منظور مقابله با کرم‌چاله‌ها در شبکه‌های حسگر بی‌سیم پرداختند. ای محققان در طرح پیشنهادی خود از گره‌های ناهمگن خوش‌هایی مبتنی بر مسیریابی امن، شبکه‌ایی مبتنی بر اعتماد را برای شناسایی حملاتی مانند کرم‌چاله و سیاه‌چاله ناشی از وجود گره‌های مخرب در شبکه بی‌سیم ادهاک مورداستفاده قراردادند. نتایج حاصل از شبیه‌سازی این روش راندمان تشخیص گره مخرب را می‌توان ۹۶ consumption همچنین مصرف انرژی نیز ۱۰٪ بهتر نسبت به سایر روش‌ها می‌باشد [۲].

سانکارا و همکاران در مقاله خود در سال ۲۰۲۰ به ارائه ساز و کار پیشرفته‌ایی به‌منظور تشخیص و مقابله با حملات مخرب کرم‌چاله پرداختند. این محققان برای مقابله با حملات کرم‌چاله‌ها در شبکه MANET با استفاده از روش تشخیص حملات با استفاده از کیفیت خدمات (Qos) برای کل شبکه استفاده کردند. در این روش پیشنهادی از نرخ تحویل بسته و زمان رفت‌وبرگشت برای هر گره استفاده می‌کند و همچنین حملات فعال و غیرفعال را تشخیص می‌دهد [۳].

تامیلاراسی و سانتی در مقاله خود در سال ۲۰۲۰ به ارائه روش جدیدی به‌منظور تشخیص حملات کرم‌چاله پرداختند. برای دست‌یابی به این هدف، روش تشخیص حمله کرم‌چاله‌ای و انتخاب مسیر بهینه یا ایمن در این مقاله ارائه‌شده است. در ابتدا، مسیرهای "K" یا مسیرهای متعدد با استفاده از پروتکل مسیریابی AOMDV بین مبدأ و مقصد ایجاد می‌شوند. سپس، گره مبدأ با تأیید بسته شناسایی (DP) و بازخورد بسته (FP) از مقصد، مسیر موردحمله کرم‌چاله را شناسایی می‌کند. گره منبع پس از شناسایی مسیرهای موردحمله سوراخ کرم، با استفاده از الگوریتم Particle Swarm Optimization (PSO) مسیر بهینه را در بین مسیرهای رایگان مهاجم انتخاب می‌کند. نتایج شبیه‌سازی نشان می‌دهد که عملکرد روش پیشنهادی بهره‌وری انرژی و طول عمر شبکه را بهبود می‌بخشد [۴].

شارما و همکارن در مقاله خود در سال ۲۰۲۰ به ارائه روشی کارآمد به‌منظور تشخیص حمله کرم‌چاله پرداختند. در این مقاله، مکانیسم مبتنی بر اعتماد مؤثر مبتنی بر مفهوم تأخیر بسته Node to Node برای تشخیص گره بدخواه کرم‌چاله ارائه‌شده است. مقدار اعتماد هر گره با مشاهده معامله بسته در بین گره‌های مجاور محاسبه می‌شود و بعداً این مقدار اعتماد برای شناسایی گره بدخواه استفاده می‌شود. بر اساس مقادیر اعتماد، تصمیمات بیشتر در مورد مسیریابی و انتخاب یک مسیر ایمن انجام می‌شود. نتایج حاصل از تحقیق حاکی از بهبود نتایج تشخیص حملات کرم‌چاله است [۵].

روی و خان در مقاله خود در سال ۲۰۲۰ به ارائه روشی به‌منظور بهبود تشخیص حملات کرم‌چاله پرداختند. این محققان در مقال خود مکانیسم تشخیصی را بر اساس محاسبه زمان رفت‌وبرگشت (RTT) و زمان پردازش برای شناسایی گره‌های مخرب تشکیل‌دهنده حمله کرم‌چاله پیشنهاد کردند. کار پیشنهادی آن‌ها از پروتکل مسیریابی AODV در برابر حمله کرم‌چاله در شبکه‌های WMN جلوگیری می‌کند. شبیه‌سازی کار پیشنهادی ما با استفاده از شبیه‌ساز NS-3 انجام‌شده است و نتایج نشان می‌دهد که عملکرد این الگوریتم تشخیص نسبت به روش‌های تشخیص موجود در برابر حمله کرم‌چاله بهبود می‌یابد [۶].

قاگر و پرادهان در مقاله خود در سال ۲۰۲۱ به بررسی روش‌های حملات کرم‌چاله پرداختند. عقیده این محققان این بود که یک شبکه حسگر بی‌سیم (WSN) نقش بسیار مهمی در شبکه‌ها دارد. از ویژگی‌های اصلی WSN می‌توان به ارتباطات ماهواره‌ای، کانال پخش، محیط خصمانه، سیستم پزشکی و

جمع‌آوری اطلاعات اشاره کرد .حمـلات زیـادی در WSN وجـود دارد. سناریوی حمله کرم‌چاله از حملات دیگر بی‌رحمانه است که در شبکه‌ها به نرمی حل می‌شود اما مشاهده آن‌ها سـخت اسـت. در این مقاله بررسی آزمایشـی بـرای مشـاهده تهدیـدات اسـت و همچنین بر روی روش متفاوتی برای شناسایی حملات کرم‌چالـه تمرکز دارد [۷].

۳- روش پیشنهادی

درروش پیشنهادی به ارائه روش جدیدی به‌منظور تشخیص و جلوگیری از حملات کرم‌چاله و سیاه‌چاله در شبکه‌های حسگر بی‌سیم پرداخته می‌شود. در حمله کرم‌چاله، گره‌های خرابکار با وانمود کردن خود به‌عنوان کوتاه‌ترین مسیر در رساندن بسته‌ها از مبدأ به مقصد، فرستنده را فریب داده و وی را وادار می‌کنند تا بسته‌های خود را برای ارسال به مقصد، به گره خرابکار تحویل دهد. بدین ترتیب به‌آسانی تعدادی یا تمامی بسته‌های دریافتی به‌جای ارسال به سمت مقصد، از بین می‌برند. روش پیشنهادی موردنظر با استفاده از ترکیب دو روش مبتنی بر RTT و روش شناسایی انتها به انتها می‌باشد. در شبکه‌های حسگر بی‌سیم وقتی حمله کرم‌چاله رخ می‌دهد طبیعی است که تعداد همسایگان گره از حد معمول بیشتر خواهد شد. بنابراین ما از این اطلاعات برای شناسایی و حملات کرم‌چاله‌ها استفاده کنیم. در روش پیشنهادی هنگامی‌که RTT بین دو گره کوچک‌تر یا مساوی مقدار حد آستانه باشد، گره مبدأ مسئول محاسبه RTT گره‌های متوالی مسیر در طول فرایند کشف مسیر می‌باشد. برای محاسبه اختلاف RTT، تمام گره‌های میانی مقدار RTT خود را به گره مبدأ ارسال می‌کند. وقتی گره مقصد یا هر گره میانی دیگر که مقصد معتبری که منقضی نشده است به مقصد دارد، بسته PREQ را تولید می‌کند تا به گره مبدأ ارسال کند. هر گره میانی X وقتی بسته را دریافت می‌کند مقدار RTT(X) را محاسبه می‌کند و آن را به بسته اضافه می‌کند و به گره بعدی در مسیر برگشت ارسال می‌کند. وقتی بسته PREQ به مقصد می‌رسد شامل تمام گره‌های میانی است. گره مبدأ مقدار RTT گره‌های میانی را از بسته PREQ می‌گیرد سپس از روی آن RTT گره‌های متوالی را محاسبه می‌کند. RTT بین دو گره متوالی A و B به‌صورت زیر محاسبه می‌شود.

$$\boldsymbol{RTT\ (A,B) = RTT\ (A) - RTT\ (B)} \qquad (۱)$$

روش پیشنهادی حملات کرم‌چاله را قبل از آسیب به شبکه و در زمان کشف مسیر تشخیص داده و از آن جلوگیری می‌کند. وقتی گره مبدأ تصمیم به ارسال بسته به مقصد را دارد و مسیر معتبری در جدول مسیریابی وجود ندارد، بسته PREQ را به‌طرف مقصد ارسال می‌کند. اگر گره مبدأ گره عضو عادی باشد، بسته را به سرخوشه خود هدایت می‌کند و اگر که سرخوشه است به گره‌های دروازه خود ارسال می‌کند. این روند تا زمانی که بسته به مقصد برسد یا مسیری به مقصد داشته باشد، ادامه دارد.

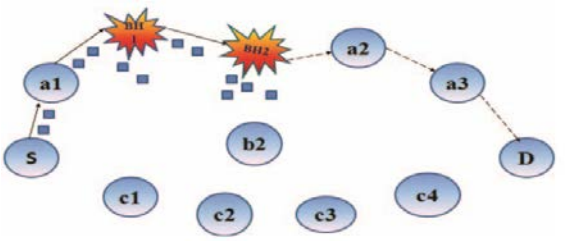
۴- تشخیص حمله کرم‌چاله

اگر RTT بین دو گره متوالی از k برابر RTT میانگین گره‌های شبکه در مسیر استقراریافته کوچک‌تر بود آنگاه مسیر مظنون به کرم‌چاله است. اما وجود RTT کوچک‌تر همواره به معنای حمله کرم‌چاله نیست بلکه می‌تواند به علت توان پردازش بالای برخی گره‌ها، سرعت پردازش گره‌ها و برخی دلایل دیگر باشد. اگر k برابرRTT بین دو گره از مقدار حد آستانه کمتر باشد، جدول همسایگی خوشه‌های دو گره مضمون را بررسی می‌کنیم، اما اگر سرخوش‌هایی در جدول همسایگی خوشه‌های دو گره مضمون قرار داشت اما در فرایند مسیریابی شرکت مکرده بود، دو گره مضمون، گره‌های کرم‌چاله هستند. آنگاه وجود گره‌های مخرب را به تمام گره‌های شبکه اطلاع می‌دهیم.

۵- مدل شبکه

در مدل شبکه حسگر بی‌سیم شامل یک مجموعه از n گره حسگر $S = \{i, j, k \dots\}$ است. گره‌های شبکه دارای محدودیت‌هایی از قبیل مقدار انرژی، حافظه ذخیره‌سازی و بازه ارسال و دریافت محدود می‌باشند [۸]. در این روش نیازی به سخت‌افزار اضافی نبوده و هیچ‌گونه شروط محدودیتی مثل هم‌زمانی گره‌ها وجود ندارد. همچنین انرژی گره‌ها ابتدا برای همه گره‌ها یکسان در نظر گرفته می‌شود. همچنین محدوده ارسال و دریافت را برای تمامی گره‌ها یکسان و برابر فرض می‌شود. بنابراین هردو گره در محدوده هم و یا به‌عنوان همسایه همدیگر خواهند بود که در رابطه زیر به‌صورت منطق مرتبه اول بیان‌شده است.

$$\forall \boldsymbol{i,j} \in \boldsymbol{s}; \boldsymbol{NB(i,j)} \leftrightarrow \boldsymbol{NB(i,j)} \qquad (۲)$$

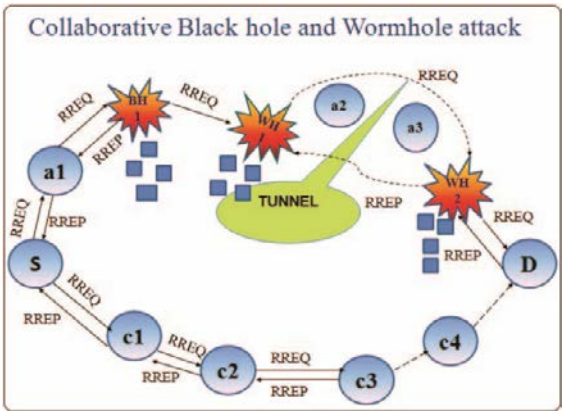


شکل (۱): مدل شبکه

۶- مدل حمله

کرم‌چاله یک لینک اختصاصی بین دو گره موجود در مکان فیزیکی مجزا است که تحت کنترل حمله‌کننده قرار دارد [۹]. حمله‌کننده‌ایی را در نظر می‌گیریم که با استفاده از دو گره همکار به شبکه حمله می‌کند [۱۰]. گره‌های حمله‌کننده را دو سر کرم‌چاله می‌نامیم. بسته‌های دریافتی در یک سر کرم‌چاله، بدون ایجاد هرگونه تغییری در محتوای آن‌ها، از طریق یک لینک پرسرعت و خارج از باند، به گره همکار در انتهای دیگر کرم‌چاله ارسال‌شده و در مقصد بازپخش می‌شود. هدف اصلی این حمله فریب داده گره شبکه است به‌طوری‌که درنتیجه وقوع آن، گره‌های دور از هم همدیگر را به‌عنوان همسایه می‌پندارند. مدل حمله را می‌توان از فرمول زیر به‌دست آورد.

$$\forall \boldsymbol{i,j} \in \boldsymbol{S}, \forall \boldsymbol{(x,y)} \in \boldsymbol{M}; (\boldsymbol{InRange(x,y) \wedge InRange(y,j)}) \rightarrow \boldsymbol{NB(i,j)} \quad (۳)$$



شکل (۲): مدل حمله

در روش پیشنهادی نیز به‌منظور تشخیص حمله از سه آیتم زیر استفاده می‌کنیم.

۱. تعداد پیام‌های *RREQ* ارسال‌شده
۲. تعداد پیام‌های *RREP* دریافت شده
۳. متوسط مقدار تفاوت شماره سریال مقصد موجود در پیام‌های *RREP* و *RRWQ*

زمانی که یک بسته *PREQ* ارسال و دریافت می‌شود، هر گره مقدار شناسه مقصد و شماره سریال آن را در لیست خود نگهداری می‌کند. زمانی که یک بسته *RREP* دریافت می‌شود، ابتدا گره بررسی می‌کند که آیا شناسه مقصد موجود دربسته‌های *RREQ* و *RREP* باهم برابرند یا خیر [۱۱-۱۲]. اگر این‌چنین باشد، تفاوت مقدار شماره سریال مقصد را در هر د مورد محاسبه می‌کند. به‌منظور انجام این کار، برای ترافیکی که از هر گره عبور می‌کند، موقعیت شبکه در هر بازه زمانی i، به‌صورت بردار سه‌بعدی $X1 = (xi1, xi2, xi3)$ بیان می‌شود. حال متوسط مقدار x، از بین D دریافتی در N بازه زمانی محاسبه می‌شود.

$$\boldsymbol{x_d} = \frac{\boldsymbol{1}}{\boldsymbol{n}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{x_i} \quad (۴)$$

درواقع در رابطه بالا، متوسط مقدار شماره سریال مقصد را در هر بازه زمانی به‌دست می‌آورد. سپس فاصله مقدار ورودی نمونه x را، با متوسط مقدار محاسبه‌شده از رابطه زیر به‌دست می‌آورد.

$$\boldsymbol{d(x) = |x - x_D|^2} \quad (۵)$$

زمانی که این فاصله از حد آستانه Th بزرگ‌تر باشد، وقوع حمله تشخیص داده می‌شود.

$$\begin{cases} \boldsymbol{d(x) > Th \rightarrow Attack} \\ \boldsymbol{d(x) \leq Th \rightarrow Normal} \end{cases} \quad (۶)$$

در اینجا بیشینه‌ترین فاصله‌ایی که از مجموع داده‌ها استخراج‌شده، به‌عنوان Th انتخاب می‌شود.

$$\boldsymbol{Th = d(xi) where, i} = \boldsymbol{\arg, max\, d(xi) i, xi \in D} \quad (۷)$$

پس از شناسایی حملات کرم‌چاله باید با این حملات مقابله کنیم. برای این منظور از ترکیب دو روش مبتنی بر RTT و روش شناسایی انتها به انتها استفاده می‌کنیم تا از این حملات جلوگیری کنیم.

۷- روش مبتنی بر RTT

در این روش گره فرستنده با تشخیص میزان تأخیر مسیرهای مختلف تا مقصد، با حمله کرم‌چاله مقابله می‌کند. شماره گام و اطلاعات تأخیر مسیرهای جداشده، جمع‌آوری و مقدار تأخیر برای هر گام به‌عنوان نشان‌گر حمله به‌کار گرفته می‌شود. در حالت عادی مقدار تأخیر بسته که در یک گام منتشر می‌شود، در طول مسیر برای هر گام مشابه است، ولی در هنگام حمله کرم‌چاله این مقدار تأخیر بدون توجیه با توجه به حضور گره‌های بدرفتار در طول مسیر بالا خواهد بود. بنابراین اگر مسیری تأخیر بالا به ازای هر گام داشته باشد، در معرض کرم‌چاله قرار خواهد گرفت. مشکل این روش این است که، شناسایی تنها زمان انتقال می‌تواند منجر به تولید زیاد نرخ مثبت شود. یعنی ممکن است تأخیر

ایجادشده بنا به ازدحام بسته‌ها در مواردی خاص رخ دهد، نه این‌که لزوماً حمله اتفاق افتاده است [۱۳-۱۶]. RTT روشی برای جلوگیری از حملات کرم‌چاله در پروتکل‌های شبکه‌های حسگر بی‌سیم می‌باشد. با استفاده از اندازه‌گیری RTT بین گره‌های متوالی حمله کرم‌چاله را تشخیص می‌دهد. در این روش، ابتدا RTT بین هر دو گره متوالی را با استفاده از رابطه‌های زیر محاسبه می‌کند. سپس RTT بین گره‌ها را با استفاده از شبیه‌سازی به‌دست می‌آورد. از مقدار $\mu = 2$ برای تشخیص کرم‌چاله استفاده می‌کند. اگر اختلاف مقدار RTT بین دو گره متوالی به‌دست‌آمده از شبیه‌سازی و RTT محاسبه‌شده از طریق رابطه زیر بیشتر یا کمتر از مقدارμ باشد حمله کرم‌چاله را تشخیص می‌دهد. گره مبدأ، حمله را به تمام گره‌ها اطلاع می‌دهد و مسیر دارای لینک کرم‌چاله را حذف می‌کند.

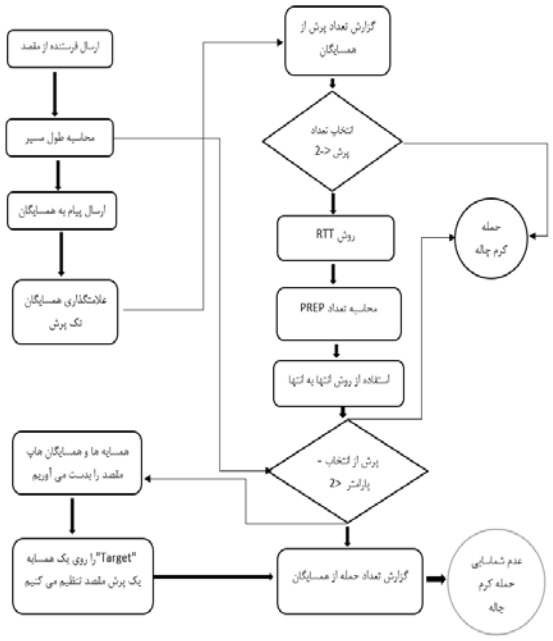
$$TT_{ni,n(I+1)} = \frac{\boldsymbol{Packet\ Size\ PREQ\ (bits)}}{\boldsymbol{Bandwitth\ (bps)}} \qquad (۸)$$

وقتی گره مبدأ تصمیم به ارسال بسته به مقصد را دارد و مسیر معتبری در جدول مسیریابی وجود ندارد، بسته PREQ را به‌طرف مقصد ارسال می‌کند. اگر گره مبدأ گره عضو عادی باشد، بسته را به سرخوشه خود هدایت می‌کند و اگر که سرخوشه است به گره‌های دروازه خود ارسال می‌کند. این روند تا زمانی که بسته به مقصد برسد یا مسیری به مقصد داشته باشد، ادامه دارد. گره مقصد چندین بسته PREQ را دریافت می‌کند اما فقط به اولین PREQ دریافتی پاسخ می‌دهد.

برای پوشش قرار دادن روش مبتنی بر RTT، این روش را با استفاده از روش انتها به انتها ترکیب می‌کنیم تا مشکلات این روش برطرف گردند.

۷-۱- روش شناسایی انتها به انتها

این روش، روشی برای شناسایی حمله کرم‌چاله ارائه‌شده که به EDWA معروف است. این روش بر مبنای کم‌ترین تعداد گام بنا نهاده شده است و می‌توان با استفاده از این روش و ترکیب آن با روش RTT یک روش قدرتمند ایجاد کرد که تمام بر تمام مشکلات سایر روش‌های موجود برتری داشته باشد. در EDWA هر گره با استفاده از سامانه موقعیت‌یاب، جایگاه خود را در شبکه پیدا می‌کند، و از تخمین مسافت اقلیدسی جهت کوتاه‌ترین مسیر استفاده می‌کند. در مرحله ردیابی، فرستنده کوتاه‌ترین مسیر تا گیرنده را با تخمین شمارش گام محاسبه می‌کند و آن را با مقدار تخمینی موجود دربسته RREP مقایسه می‌کند. اگر این مقدار کمتر از مقدار تخمین شده باشد، مسیر بالا را یک مسیر کرم‌چاله پیش‌بینی می‌کند. در مرحله آخر گره فرستنده کوتاه‌ترین مسیر، از میان مسیرهای قانونی شروع به ارسال داده می‌کند [۱۷-۲۰].



شکل (۳): فلوچارت روش RTT و روش انتها به انتها

با پایان این روش تمامی حملات شناسایی و از بین خواهند رفت و مسیر موردحمله بهینه خواهد شد تا دیگر شاهد نفوذ و حملات کرم‌چاله نباشیم.

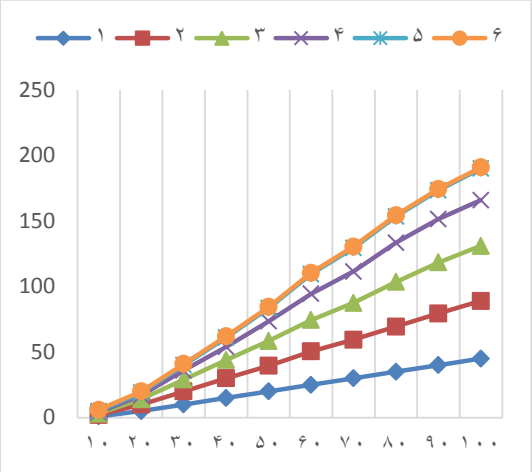
۸- ارزیابی روش پیشنهادی

برای ارزیابی حملات کرم‌چاله و سیاه‌چاله معمولاً از یک برنامه شبیه‌ساز استفاده می‌شود که می‌تواند میزان حملات و میزان برطرف کردن حملات را با استفاده از آن تشخیص داد. معمولاً برای ارزیابی نتایج برای مباحث کرم‌چاله و سیاه‌چاله از پارامترهایی مانند تعداد RREQ های پذیرفته‌شده، میانگین نرخ بسته‌های رسیده، میانگین تأخیر نقطه‌به‌نقطه و میزان سربار مسیریابی استفاده می‌شود. با استفاده از این معیارها می‌توان نوع حملات و نرخ برطرف کردن حملات را تشخیص داد.

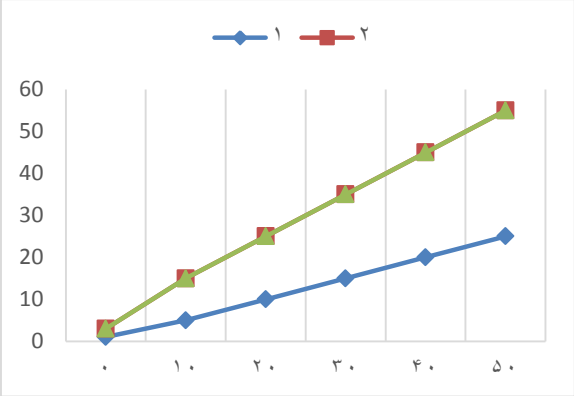
۹- شبیه‌سازی روش پیشنهادی

برای نمایش عملکرد گره‌ها در شناسایی حمله کرم‌چاله تحت روش ارائه شده با استفاده از شبیه‌ساز NS-2 و Cisco packet Tracer حملات کرم‌چاله و سیاه چاله را در لایه لینک پیاده‌سازی شد. گره‌ها به‌صورت تصادفی در محیطی به ابعاد ۱۰۰ در ۱۰۰ پخش شده و الگوریتم روی هر گره به‌صورت جداگانه اجرا شد.

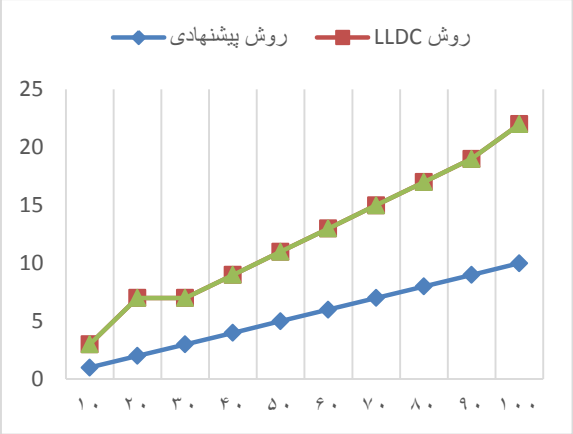
محدوده ارسال گره‌ها یکسان و برابر ۱۰ در نظر گرفته شد و انرژی اولیه گره‌ها نیز به‌صورت مساوی در نظر گرفته شد. نتایج حاصل از شبیه‌سازی در زیر توضیح داده شده است. شبیه‌سازی روش پیشنهادی در چند بخش صورت گرفت که نتایج حاصل از آن را در قالب چند نمودار نشان داده می‌شود. مرحله اول شبیه‌سازی تعداد RREQ های پذیرفته در مقصد می‌باشد. هدف از این پارامتر این است که ببینیم چه تعداد از مسیرهایی که توسط مبدأ با وزن مختلف درخواست می‌شود، در مقصد موردپذیرش قرار می‌گیرند. در این بخش شبیه‌سازی با ۱۰ گره در مدت‌زمان صد ثانیه انجام خواهد شد. نتایج حاصل از شبیه‌سازی نشان می‌دهد که هرچه وزن درخواستی توسط مبدأ افزایش یابد تعداد RREP های پذیرفته‌شده به ازای آن درخواست در مقصد کاهش می‌یابد (شکل ۴). مرحله دوم شبیه‌سازی میانگین نرخ بسته‌های رسیده می‌باشد. نرخ بسته‌های رسیده که آن را PDR می‌نامیم، برای تعریف تعداد بسته‌های داده ایی است، که یک گره فرستاده و گره مقصد آن را صحیح دریافت کرده است. میزان بسته‌های رسیده مقصد را در ترافیک UDP با تعداد ۱۰ الی ۵۰ گره با حضور دو گره حمله‌کننده که سعی دارند در فرایند مسیریابی اختلالاتی ایجاد کنند را مشاهده می‌کنید (شکل ۵). مرحله بعد مقایسه متوسط انرژی می‌باشد. به‌منظور مقایسه انرژی مصرفی روش پیشنهادی با روش LLDC آزمایشی را با تعداد مختلف گره‌های متفاوت انجام دادیم و متوسط انرژی مصرفی گره‌ها درروش پیشنهادی را با روش LLDC مقایسه کردیم که نتایج آن در شکل (۶) آورده شده است. نتایج به‌دست‌آمده نشان می‌دهد که روش پیشنهادی متوسط انرژی کمتری را نسبت به سایر روش‌های مشابه دارد به‌نحوی‌که روش پیشنهادی در حالت‌های مختلف از تراکم گره‌ها و ازنظر متوسط انرژی مصرفی نسبت به روش LLDC بهتر عمل کرده است (شکل ۶). مقایسه و ارزیابی کارایی روش پیشنهادی و مقایسه آن با روش‌های دیگر در سناریوی یک گره سیاه‌چاله ازنظر تعداد بسته‌های حذف‌شده در واحد زمان، که روش پیشنهادی عملکرد بهتری داشته است. به‌منظور مقایسه روش پیشنهادی با سایر روش‌های مشابه مقایسه‌ایی بین میزان شناسایی و حذف گره‌های مخرب همچنین میزان سربار سیستم صورت گرفت که نتایج حاصل از این ارزیابی حاکی از عملکرد بالای روش پیشنهادی نسبت به سایر روش‌های موجود می‌باشد. نتایج حاصل از این مقایسه را در (شکل ۸ و ۷) مشاهده می‌کنید.



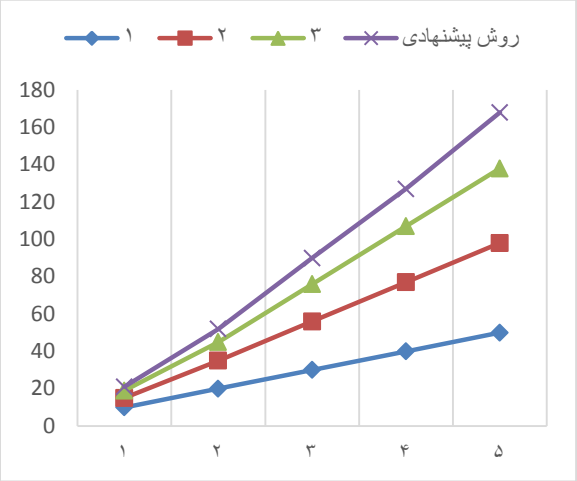
شکل (۴): تعداد RREQ های پذیرفته‌شده در مقصد



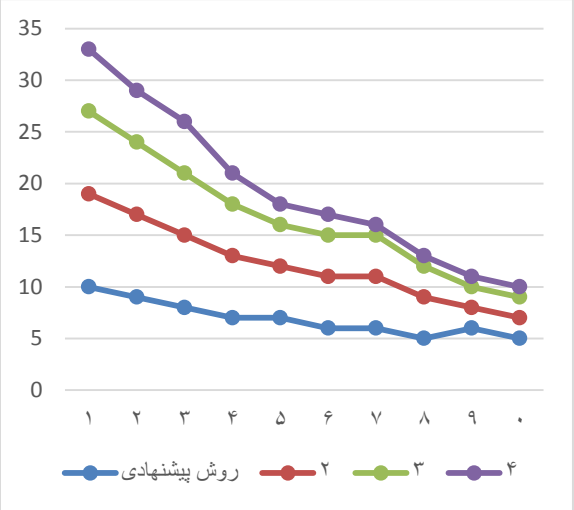
شکل (۵): میانگین نرخ بسته‌های رسیده



شکل (۶): مقایسه متوسط انرژی مصرفی روش پیشنهادی با روش LLDC



شکل (۷): میزان حذف گره‌ها درروش پیشنهادی و سایر روش‌ها



شکل (۸): میزان سربار سیستم

۱۰- نتیجه‌گیری

حمله کرم‌چاله یک نوع حمله فعال است که در لایه شبکه رخ می‌دهد. در این حمله مهاجمان با متقاعد کردن گره فرستنده برای ارسال اطلاعات از یک مسیر جعلی که کوتاه‌تر و سریع‌تر از مسیر عادی به نظر می‌رسد، سعی دارند ارسال بسته‌ها از تونل ایجادشده انجام شود تا بتوانند، حملات خود را انجام دهند. در حمله کرم‌چاله، بسته‌ها یک منطقه از شبکه از طریق لینک سریع و خارج از باند، به منطقه دیگری از شبکه منتقل‌شده و بازپخش می‌شوند. این عمل باعث می‌شود گره‌هایی که ازنظر فیزیکی در همسایگی هم قرار ندارند، به‌طور ناخودآگاه یکدیگر را به‌عنوان همسایه شناسایی کنند. برای مقابله با این حمله، روش‌های متنوعی ارائه‌شده‌اند که برخی از آن‌ها دارای مشکلاتی ازجمله شناسایی اکثر حملات نیستند. درروش پیشنهادی به ارائه روش جدیدی به‌منظور تشخیص و جلوگیری از حملات کرم‌چاله و سیاه‌چاله در شبکه‌های حسگر بی‌سیم پرداخته می‌شود. در حمله کرم‌چاله، گره‌های خرابکار با وانمود کردن خود به‌عنوان کوتاه‌ترین مسیر در رساندن بسته‌ها از مبدأ به مقصد، فرستنده را فریب داده و وی را وادار می‌کنند تا بسته‌های خود را برای ارسال به مقصد، به گره خرابکار تحویل دهد. بدین ترتیب به‌آسانی تعدادی یا تمامی بسته‌های دریافتی به‌جای ارسال به سمت مقصد، از بین می‌برند. روش پیشنهادی موردنظر با استفاده از ترکیب دو روش مبتنی بر RTT و روش شناسایی انتها به انتها می‌باشد. در شبکه‌های حسگر بی‌سیم وقتی حمله کرم‌چاله رخ می‌دهد طبیعی است که تعداد همسایگان گره از حد معمول بیشتر خواهد شد؛ بنابراین ما از این اطلاعات برای شناسایی و حملات کرم‌چاله‌ها استفاده کنیم. نتایج حاصل از این تحقیق حاکی از بهبود تشخیص و مقابله حملات می‌باشد به‌نحوی‌که در بخش‌های، میانگین نرخ بسته‌های رسیده، تعداد RREQ های پذیرفته‌شده در مقصد، مقایسه متوسط انرژی مصرفی، میزان حذف گره‌ها و میزان سربار سستم توانست عملکرد قابل قبولی نسبت به سایر روش‌های موجود به‌دست آورد.

۱۱- مراجع

[1] P. Kaliyar, W. B. Jaballah, M. Conti, & C. Lal, “LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks”, Computers & Security, Vol. 94, 2020.

[2] Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V., & Amiri, I. S. “Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks”, Journal of Ambient Intelligence and Humanized Computing, Vol. 11, no. 11, pp. 4995-5001, 2020.

[3] S. Sankara Narayanan, & G. Murugaboopathi, “Modified secure AODV protocol to prevent wormhole attack in MANET”, Concurrency and Computation: Practice and Experience, Vol. 32, no. 4, p. 5017, 2020.

[4] N. Tamilarasi, & S. G. Santhi, “Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network”, Wireless Personal Communications, Vol. 114, no. 1, pp. 329-345, 2020.

[5] N. Sharma, M. Sharma, & D. P. Sharma, “A Trust based Scheme for Spotting Malicious Node of Wormhole in Dynamic Source Routing Protocol”, In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) pp. 1232-1237, IEEE, 2020.

[6] A. K. Roy, & A. K. Khan, “RTT based wormhole detection for wireless mesh networks”, International Journal of Information Technology, Vol. 12, no. 2, pp. 539-546, 2020.

[7] U. Ghugar, & J. Pradhan, “Survey of wormhole attack in wireless sensor networks”, Computer Science and Information Technologies, Vol. 2, no. 1, pp. 33-42, 2021.

[8] A. Almheiri, T. Hartman, J. Maldacena, E. Shaghoulian, & A. Tajdini, “Replica wormholes and the entropy of Hawking radiation”, Journal of High Energy Physics, Vol. 5, pp. 1-42, 2020.

[9] S. B. Giddings, & G. J. Turiaci, “Wormhole calculus, replicas, and entropies”, Journal of High Energy Physics, Vol. 9, pp. 1-18, 2020.

[10] Y. Chen, X. L. Qi, & P. Zhang, “Replica wormhole and information retrieval in the SYK model coupled to Majorana chains”, Journal of High Energy Physics, Vol. 6, 1-26, 2020.

[11] K. Jusufi, P. Channuie, & M. Jamil, “Traversable wormholes supported by GUP corrected Casimir energy”, The European Physical Journal C, Vol. 80, no. 2, pp. 1-14, 2020.

[12] G. Antoniou, A. Bakopoulos, P. Kanti, B. Kleihaus, & J. Kunz, “Novel Einstein–scalar-Gauss-Bonnet wormholes without exotic matter”, Physical Review D, Vol. 101, no. 2, p. 024033, 2020.

[13] O. R. Ahutu, & H. El-Ocla, “Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks. IEEE Access, Vol. 8, pp. 63270-63282, 2020.

[14] A. Bhawsar, Y. Pandey, & U. Singh, “Detection and Prevention of Wormhole Attack using the Trust-based Routing System”, In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 809-814), IEEE, 2020.

[15] S. Jamali, & R. Fotohi, “Defending against wormhole attack in MANET using an artificial immune system”, New Review of Information Networking, Vol. 21, no. 2, pp. 79-100, 2016.

[16] J. Govindasamy, & S. Punniakody, “A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack”, Journal of Electrical Systems and Information Technology, Vol. 5, no. 3, pp. 735-744, 2018.

[17] A. B. Aswale, & R. D. Joshi, “Security Enhancement by Preventing Wormhole Attack in MANET”, In Innovations in Electronics and Communication Engineering, pp. 225-237, Springer, Singapore, 2020.

[18] P. Kaur, D. Kaur, & R. Mahajan, “Wormhole attack detection technique in mobile ad hoc networks”, Wireless Personal Communications, Vol. 97, no. 2, pp. 2939-2950, 2017.

[19] C. Samuel, B. M. Alvarez, E. G. Ribera, P. P. Ioulianou, & V. G. Vassilakis, “Performance evaluation of a wormhole detection method using round-trip times and hop counts in RPL-based 6LoWPAN networks”, In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 1-6, IEEE, 2020.

[20] S. Majumder, & D. Bhattacharyya, “Relation estimation of packets dropped by wormhole attack to packets sent using regression analysis”, In Emerging Technology in Modelling and Graphics, pp. 557-566, Springer, Singapore, 2020.

Journal of "Innovations of Applied Information and Communication Technologies"
Vol. 1, No. 2, 2021 (Serial No. 2)

Provide a Way to Detect and Combat Wormhole and Black Hole Attacks in Ad-Hoc Networks

R. Molaei Fard

Department of Computer Engineering - Dezful Branch of Azad University, Khuzestan, Iran

Abstract

Today, wireless sensor networks are exposed to dangerous attacks that can disrupt the network. One of these malicious attacks is wormhole and black hole attacks which can pose serious threats to the network. Timely detection and detection of these attacks can improve network performance. In this research, a method is provided to improve, identify, detect and deal with wormhole and black hole attacks. The proposed method is a combination of two methods based on RTT and end-to-end identification method. In wireless sensor networks, when a wormhole attack occurs, it is natural that the number of node neighbors will be higher than usual; So we use this information to identify and attack wormholes. The results of this study indicate an improvement in the detection and response of attacks so that in sections, the average rate of packets received, the number of RREQs accepted at the destination, comparison of average energy consumption, node removal rate and system overhead can achieve acceptable performance compared to others. Acquired existing methods.

Keywords: Sensor network, Wormhole, Black Hole, RTT Method, End-to-End Detection Method

* Corresponding author E-mail: rezamolae4@gmail.com