مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۴، زمستان ۱۳۹۶، ص ۸۰-۶۹

ارائه روش ترکیبی به‌منظور کشف و اجتناب از حمله سیاه‌چاله در شبکه‌های موردی مبتنی بر پروتکل AODV

سینا شهابی رابری[۱]، مهدیه قزوینی[۲*]

۱- کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد بافت، باشگاه پژوهشگران جوان و نخبگان، ۲- استادیار، بخش مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه شهید باهنر کرمان

(دریافت: ۹۶/۰۲/۱۰، پذیرش: ۹۶/۰۵/۰۱)

چکیده

شبکه‌های موردی از تعدادی گره بی‌سیم بدون نیاز به هیچ‌یک از زیرساخت‌های شبکه‌ای پیشین تشکیل می‌شوند. این گره‌ها بدون هیچ‌گونه زیرساختی با یکدیگر ارتباط برقرار می‌کنند. به دلیل ویژگی‌هایی مانند تغییر پویای ساختار شبکه، اعتماد پیش‌فرض گره‌ها به یکدیگر و نادیده‌گرفتن عملکرد گره‌ها، شبکه‌های موردی در مقابل حملات گره‌های مخرب محافظت‌شده نیستند. در این مقاله روش جدیدی با استفاده از ترکیب یک روش تشخیص مسیر امن و یک روش مقابله با گره‌های خرابکار در حمله سیاه‌چاله برای پروتکل مسیریابی AODV ارائه‌شده است. در مرحله اول، گره مبدأ با پیداکردن بیش از یک مسیر به مقصد، اعتبار گره‌ای که بسته پاسخ مسیر را فرستاده است تأیید می‌کند. هنگامی‌که یک بسته پاسخ مسیر به گره مبدأ برسد، آن گره، مسیرهای کامل به مقصد را استخراج کرده و در انتظار یک بسته پاسخ مسیر دیگر می‌ماند. ایده این راه‌حل انتظار برای دریافت بسته پاسخ مسیر از بیش از دو گره است. در مرحله بعدی با توجه به رفتار گره‌ها در شبکه، رأی‌گیری از گره‌های همسایه انجام شده و با استفاده از قوانین تعریف‌شده در مبدأ به‌منظور تشخیص گره خرابکار، گره‌های خرابکار شناسایی و حذف می‌شوند. نتایج شبیه‌سازی با استفاده از نرم‌افزار OMNET نشان‌دهنده بهبود قابل‌توجه الگوریتم پیشنهادی نسبت به نسخه اصلی پروتکل AODV که دچار حمله شده است، می‌باشد.

واژه‌های کلیدی: شبکه موردی، پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا، حمله سیاه‌چاله، مسیر امن.

۱- مقدمه

اغلب شبکه‌های بی‌سیم به‌صورت با ساختار[۱] پیاده‌سازی می‌شوند. معماری معمول در شبکه‌های بی‌سیم بر مبنای استفاده از نقطه مرکزی[۲] است. با نصب یک نقطه مرکزی، عملاً مرزهای یک سلول مشخص می‌شود. با این‌وجود، نوع دیگری از شبکه‌های بی‌سیم نیز وجود دارند که از منطق نقطه‌به‌نقطه[۳] استفاده می‌کنند و عموماً شبکه‌های موردی[۴] نامیده می‌شوند. شبکه‌های موردی از گره های مستقل بی‌سیم تشکیل می‌شوند که خودشان بدون هیچ‌گونه زیرساختی، شبکه را مدیریت می‌کنند و می‌توانند به‌صورت پویا در هر مکان و در هر زمان به‌راحتی به شبکه ملحق شده و یا آن را ترک کنند. ارتباط میان گره‌ها در این شبکه از طریق امواج رادیویی صورت می‌گیرد. درصورتی‌که یک گره دربرد رادیویی گره دیگر باشد همسایه آن گره به‌حساب می‌آید و در غیر این صورت، در صورت نیاز به ارتباط میان دو گره که دربرد رادیویی یکدیگر نیستند می‌توان از کمک گره‌های دیگر در این مورد استفاده کرد؛ بنابراین، ارتباط میان گره‌ها در این شبکه به‌نوعی بر مبنای اعتماد و مشارکت میان گره‌ها صورت می‌گیرد. در این نوع شبکه‌ها هر گره نه‌تنها به‌عنوان میزبان بلکه به‌عنوان یک مسیریاب نیز عمل ارسال بسته های اطلاعاتی را انجام می‌دهد. گره‌ها به‌طور مستقیم، بدون هیچ‌گونه نقطه دسترسی با همدیگر ارتباط برقرار می‌کنند و سازمان ثابتی ندارند، بنابراین در یک هم‌بندی دلخواه شکل‌گرفته‌اند [۱]. شبکه‌های موردی (اقتضایی) دارای انواع مختلفی می‌باشند مانند شبکه اقتضایی بین خودرویی[۵] که در آن گره‌های شبکه، خودروها می‌باشند و شبکه اقتضایی موبایل[۶] که گره‌های آن موبایل‌های مجهز به گیرنده و

* رایانامه نویسنده مسئول: mghazvini@uk.ac.ir

1- Infrastructure
2 - Access Point
3 - Peer-to-Peer
4- Ad hoc Networks
5 - VANET (Vehicular Ad hoc Network)
6 - MANET(Mobile Ad hoc Network)

فرستنده‌های بی‌سیم هستند. تفاوت عمده شبکه‌های موردی با شبکه‌های بی‌سیم مبتنی بر استاندارد IEEE.802.11 این است که در این شبکه‌ها ارتباط بین گره‌های شبکه بدون هیچ‌گونه زیرساخت مرکزی و یا ایستگاه پایه‌ای برای مدتی کوتاه برقرار می‌شود. از ویژگی‌های این شبکه‌ها تحرک‌پذیری بسیار بالای گره‌ها بوده که منجر به تغییرات بسیار زیادی در هم‌بندی این شبکه‌ها می‌گردد. با توجه به اینکه هنگام طراحی پروتکل‌های شبکه‌های موردی توجه چندانی به امنیت آن‌ها نشده است، طراحی پروتکل‌های ارتباطی امن و کارآمد در این شبکه‌ها از چالش‌های اساسی این حوزه بوده و از موضوعات باز تحقیقاتی در مراکز علمی و دانشگاهی به شمار می‌آید [۲]. شکل (۱)، همکاری گره‌ها برای ارسال بسته از مبدأ به مقصد را نشان می‌دهد.

شکل (۱): ارسال بسته از مبدأ به مقصد از کوتاه‌ترین مسیر [۳].

استفاده گسترده از شبکه‌های موردی در محیط های نظامی و دیگر کاربردهای حساس به امنیت، امنیت را به‌عنوان یک نیاز اساسی از زمان معرفی این شبکه‌ها مطرح نموده است. در کنار این نیاز، ایجاد امنیت در این دسته از شبکه‌ها مشکلات مخصوص به خود را داراست. در این شبکه‌ها علاوه‌بر تمامی مشکلاتی که در یک شبکه سیمی و یا یک شبکه بی‌سیم با زیرساخت وجود دارد؛ به دلیل این‌که خود گره‌ها در عمل مسیریابی شرکت می‌کنند، وجود یک گره خرابکار می‌تواند به نابودی شبکه بیانجامد. به جهت این‌که ساختار مسیریابی شبکه های موردی به‌نوعی بر مبنای اعتماد میان گره‌ها استوار است، فرصت خوبی را برای حمله‌کنندگان فراهم می‌سازد تا با شرکت در فرآیند مسیریابی به‌نوعی باعث اخلال در فرایند مسیریابی شده و در نهایت امر مسیریابی را مختل کنند. از این‌رو، امنیت در این شبکه ها به صورت جداگانه مورد بحث و بررسی قرار می‌گیرد [۱ و ۴]. آسیب پذیری ارتباطات بی‌سیم در برابر استراق سمع، نقطه‌ضعفی اساسی در برقراری ارتباطات امن محسوب می‌شود. برای آن دسته از شبکه‌های ارتباطی مانند شبکه‌های موردی که امنیت در آن‌ها از اولویت بالایی برخوردار است ارتباط بی‌سیم تنها در صورتی می‌تواند کارآمد باشد که برای امن‌نمودن ارتباطات خود راه‌حلی مؤثر اتخاذ نموده باشند [۵].

پس از بیان مقدمه‌ای در مورد شبکه‌های موردی و مسئله مهم امنیت در این شبکه‌ها، در بخش دوم این مقاله پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا مورد بررسی قرار گرفته است. حمله سیاه‌چاله و روش کار آن نیز در بخش سوم شرح داده شده است. در بخش چهارم، کارهای علمی و تحقیقاتی انجام‌شده در این حوزه بررسی‌شده‌اند. الگوریتم پیشنهادی و جنبه نوآوری آن در بخش پنجم بیان گردیده است. در بخش ششم، پیاده‌سازی و شبیه‌سازی الگوریتم پیشنهادی انجام شده است و در بخش هفتم، بحث و نتیجه‌گیری از الگوریتم پیشنهادی ارائه‌شده، بیان شده است.

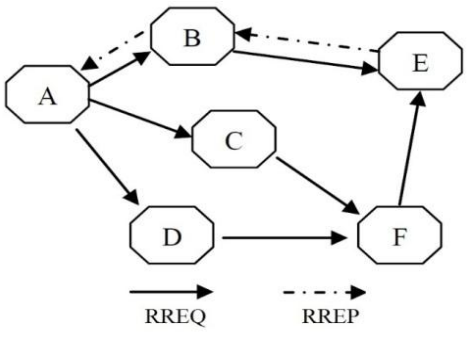
۲- پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا[1]

پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا، یک پروتکل درخواست مسیریابی در مسیر[2] است که قابلیت‌های پویابودن، خودآغازی[3] و مسیریابی تک‌پخشی[4] و چندپخشی[5] را برای گره هایی که می‌خواهند در ایجاد یک شبکه موردی شرکت نمایند، فراهم می‌کند. این پروتکل الگوریتمی است که بنا بر تقاضا، کار می‌کند؛ یعنی این پروتکل مسیر بین گره‌ها را تنها درصورتی‌که توسط گره مبدأ درخواست شده باشد می‌سازد و تا زمانی‌که مسیرها توسط گره مبدأ مورد نیازند آن‌ها را حفظ می‌کند. این پروتکل برای تضمین تازگی مسیرها و عدم وجود حلقه از شماره ترتیب استفاده می‌کند. از ویژگی‌های دیگر این پروتکل این است که مسیرهای بدون حلقه ایجاد کرده، خودآغاز بوده و برای مقیاس‌های بزرگ شبکه که از تعداد زیادی گره تشکیل شده است نیز پاسخگو است [۶].

پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا با استفاده از یک چرخه پرس‌وجوی درخواست مسیر و پاسخ مسیر، مسیرها را می‌سازد. وقتی‌که گره مبدأ مسیری به گره مقصد را درخواست می‌کند گره‌ای که در حال حاضر مسیری به مقصد ندارد، بسته درخواست مسیر[6] را به‌صورت همه‌پخشی[7] به سراسر شبکه ارسال می‌نماید. گره‌هایی که این بسته را دریافت می‌کنند اطلاعاتشان را

1- AODV(Ad-Hoc On-Demand Distance Vector)
2- Reactive
3- Self-initiated
4 -Unicast
5 -Multicast
6 -RREQ(Route Request)
7 -Broadcast

با توجه به اطلاعات گره مبدأ به‌روز کرده و یک ورودی مسیر معکوس را برای گره مبدأ در جدول‌های مسیریابی خود ایجاد می‌کنند. گره دریافت‌کننده بسته درخواست مسیر، درصورتی‌که خودش گره مقصد باشد و یا مسیری به گره مقصد با شماره ترتیب بزرگ‌تر یا مساوی شماره ترتیب بسته درخواست مسیر داشته باشد، پاسخ بسته درخواست مسیر را ارسال خواهد کرد. اگر یکی از دو حالت فوق رخ دهد گره دریافت کننده بسته درخواست مسیر، یک بسته پاسخ مسیر[1] در جهت معکوس برای گره مبدأ به صورت تک‌پخشی ارسال خواهد کرد. در غیر این صورت، گره دریافت کننده مجدداً بسته درخواست مسیر را به صورت همه‌پخشی ارسال می‌کند. گره‌ها در بسته درخواست مسیر، آدرس IP گره مبدأ و شناسه همه‌پخشی را نگه می‌دارند. اگر گره‌ای بسته درخواست مسیری که قبلاً آن را دریافت کرده، دریافت نماید آن را دور انداخته و هدایت نخواهد کرد. اگر بعداً گره مبدأ، بسته درخواست مسیری که شامل یک شماره ترتیب بزرگ تر است یا شماره ترتیب یکسان با تعداد شماره گام[2] کوچک تر را دریافت کند اطلاعات مسیریابی مربوط به گره مقصد را به‌روز کرده و مسیر بهتر را مورد استفاده قرار می‌دهد. تا زمانیکه به‌اندازه کافی ترافیک داده به مقصد وجود داشته باشد تداوم مسیر حفظ می‌شود. زمانی‌که ترافیک به مقصد متوقف شود مهلت مسیر تمام شده و سرانجام از جدول مسیریابی حذف می‌شود. اگر قطع‌شدن یک اتصال درحالی‌که مسیر فعال است رخ دهد، یک بسته خطای مسیر توسط گره‌ای که نزدیک گره آغازگر است ارسال می‌شود. بسته خطای مسیر اطلاعاتی در مورد مقصدهایی که در حال حاضر غیرقابل دسترس هستند را در بردارد. اگر گره آغازگر مجدداً تقاضای ارسال داده به مقصد را داشته باشد می‌تواند فرآیند کشف مسیر را دوباره آغاز نماید [۷]. شکل (۲) نحوه ایجاد مسیر بین دو گره را با استفاده از پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا نشان می‌دهد.



شکل (۲): ایجاد مسیر بین گره A,E [۸].

1 -RREP(Route Reply)
2 -Hop count

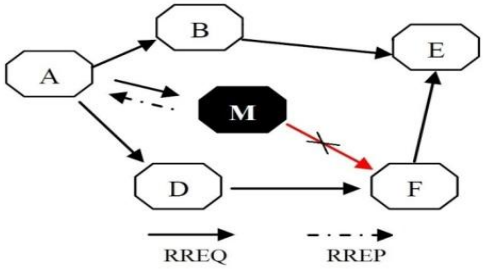
۳- حمله سیاه‌چاله[3]

در حمله سیاه‌چاله گره خرابکار با وانمودکردن خود به‌عنوان پرش بعدی واقع بر کوتاه‌ترین مسیر به سمت مقصد، فرستنده بسته را وادار می‌کند تا بسته خود را از طریق این گره ساختگی به مقصد برساند. درنتیجه، به‌راحتی شروع به نابودی کل بسته‌ها عبوری از خود می‌کند. این نوع حمله تعدادی یا همه بسته‌های دریافتی را به‌جای ارسال‌کردن، حذف نموده و باعث افت شدید نرخ تحویل بسته می‌شود. حمله سیاه‌چاله به دو دسته تقسیم می‌شود: حمله سیاه‌چاله تکی و حمله سیاه‌چاله گروهی یا جمعی. حمله سیاه‌چاله تکی از طریق یکی از گره‌های موجود در شبکه اعمال می‌شود اما در حمله سیاه‌چاله جمعی بیش از یک گره خرابکار وجود دارد که در انجام حمله باهم همکاری می‌کنند به‌عبارت‌دیگر، گره‌های سیاه‌چاله ممکن است مانند یک گروه کار کنند تا گره‌های دیگر را، اشتباه راهنمایی کنند [۹].

گره‌ای که حمله سیاه چاله را اجرا می‌کند منتظر می‌ماند تا یک بسته درخواست مسیر از گره‌های همسایه دریافت کند. با دریافت بسته درخواست مسیر، بلافاصله و بدون بررسی‌کردن جدول مسیریابی خود به گره ارسال‌کننده درخواست مسیر، یک بسته پاسخ مسیر دروغین، ارسال می‌کند. به عبارت دیگر، گره خرابکار بدون توجه به جدول مسیریابی خود و این‌که آیا اصلاً مسیری به گره مقصد دارد یا خیر، به بسته درخواست مسیر دریافتی، بسته پاسخ مسیر مساعد ارسال می‌کند که این امر باعث کوتاه‌شدن ارسال بسته‌های پاسخ مسیر نسبت به گره‌های دیگر می‌شود. گره خرابکار در بسته پاسخ مسیر خود بیشترین شماره ترتیب و کمترین تعداد گام را قرار می‌دهد و به این صورت گره درخواست‌کننده مسیر را فریب می‌دهد. گره‌ای که بسته درخواست مسیر را فرستاده است با دریافت این بسته پاسخ مسیر، فرض می‌کند که بهترین مسیر را کشف کرده است. درنتیجه، این گره را به‌عنوان مسیر مناسب و کوتاه برای ارسال بسته ها دانسته و بسته‌های خود را از مسیر این گره ارسال می‌کند. در این صورت، یک سیاه‌چاله ایجادشده و گره‌ای هم که به‌عنوان سیاه‌چاله شناخته می‌شود به‌جای ارسال بسته‌ها به مقصد، اقدام به دریافت اطلاعات آن‌ها و یا دورانداختن آن‌ها می‌کند. به دلیل این‌که گره خرابکار جدول مسیریابی خود را بررسی نمی‌کند قبل از سایر گره ها به گره درخواست کننده مسیر پاسخ می‌دهد. اگر گره خرابکار خود را به عنوان مسیر مناسب برای کلیه گره‌های شبکه معرفی کند و موفق شود همه ترافیک

3 -Black hole attack

شبکه را به‌دست آورد. در این صورت، سبب از دست رفتن تمامی بسته‌های شبکه خواهد شد و باعث به‌وجودآمدن حمله ممانعت از سرویس می‌شود [۱۰]. شکل (۳) نمایی از حمله سیاه چاله را نشان می‌دهد.



شکل (۳): حمله سیاه‌چاله [۸].

۴- تحقیقات انجام‌شده

پژوهش‌های بسیاری به‌منظور بهبود عملکرد شبکه‌های موردی در مقابل حمله سیاه‌چاله انجام شده است. چندین پیشنهاد برای کشف و کاهش حملات سیاه‌چاله در شبکه‌های موردی وجود دارد.

در [۱] یک الگوریتم جدید ارائه شده است که امنیت پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا را در مواجهه با حملات سیاه‌چاله در شبکه‌های موردی ارتقاء می‌دهد. در این الگوریتم سعی بر این است که بتوان با توجه به رفتار گره‌ها در شبکه، گره‌های خرابکار را شناسایی و آن‌ها را از مسیریابی حذف کرد. زمانی‌که یک گره از گره همسایه خود یک بسته پاسخ مسیر دریافت می‌کند درصورتی‌که گره پاسخ‌دهنده به درخواست مسیر، یک گره میانی باشد و گره مقصد نباشد بررسی می‌کند که آیا گره پاسخ‌دهنده از گره‌هایی نیست که در قرنطینه می‌باشند. اگر گره، یک گره خرابکار باشد بسته پاسخ مسیر دور ریخته می‌شود. در غیر این صورت، فرایند رأی‌گیری در اطراف گره پاسخ‌دهنده انجام می‌شود تا بتوان تمام فعالیت های گره موردنظر را به دست آورد. سپس براساس اطلاعات دریافتی، طبق قوانینی که برای تشخیص گره خرابکار در گره مبدأ تعریف شده است درستی گره موردنظر بررسی می‌شود و اگر گره خرابکار باشد در شبکه یک پیغام خطر پخش می‌شود تا گره موردنظر در قرنطینه قرار گیرد. الگوریتم پیشنهادی توسط نرم‌افزار شبیه ساز NS2 شبیه‌سازی شده است. نتایج شبیه‌سازی نشان‌دهنده بهبود قابل‌توجه تأخیر انتها به انتها و نرخ تحویل بسته در الگوریتم پیشنهادی نسبت به نسخه اصلی پروتکل بردار فاصله مبتنی بر تقاضا که دچار حمله شده است، می‌باشد.

در [۱۱] راه‌حلی برای پیشگیری در برابر حمله سیاه‌چاله ارائه شده است که در آن اعتبار اولیه گره‌های میانی که پیام پاسخ مسیر را می‌فرستند و تأییدیه را از مقصد به دست می‌آورند بررسی می‌شوند. اگر تأییدیه توسط مقصد نرسید، سابقه این گره‌های میانی بدخواه در فهرست سیاه برای داوری در زمان دیگری ذخیره می‌شود. پارامتر CL یک شمارنده است که رفتار بد گره‌های میانی را هنگامی‌که آن‌ها یک پاسخ مسیر نادرست می‌فرستند نشان می‌دهد. اگر CL برای هر گره بیشتر از سه شود، آن گره به عنوان گره بدخواه (خرابکار) معرفی می‌شود و از مسیر معرفی‌شده توسط این گره اجتناب می‌شود.

در [۱۲]، سیستم تشخیص نفوذی با استفاده از نرم‌افزار NS-2 با تغییر پروتکل بردار فاصله مبتنی بر تقاضا و حذف گره سیاه‌چاله‌ای که بیشترین بسته‌ها را از بین برده پیاده‌سازی شده است. همچنین یک روش از فعال‌شدن حالت بی‌قاعده با انتخاب مسیر از بالاترین شماره ترتیب ارائه شده است که در دستیابی به کیفیت بهتر خدمات مفید است. در این مقاله، عملکرد روش IDS مورد بررسی قرار گرفته است. IDS به تشخیص گره‌های آسیب‌پذیر کمک نموده و با حذف آن‌ها سبب کیفیت بهتر خدمات می‌گردد. پس از اجرای IDS، بهبود کیفیت خدمات را می‌توان به‌وضوح دید. IDS بهبود ۶۰ ٪ نرخ تحویل بسته را نشان می‌دهد.

در [۱۳]، الگوریتمی برای کشف حمله سیاه‌چاله جمعی در شبکه موردی مبتنی بر پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا ارائه شده است که در آن تمام بسته‌های پاسخ مسیر را براساس شماره توالی مقصد به‌صورت نزولی قرار می‌دهد و آن‌هایی را که بسیار زیاد بزرگ‌تر از شماره توالی منبع هستند به‌عنوان گره مشکوک در نظر می‌گیرد. سپس سراغ گره بعدی می‌رود این فرآیند تا زمانی ادامه دارد که گره‌ای مشکوک در نظر گرفته نشود. البته متوسط تأخیر انتها به انتها در این روش زیاد است.

در [۱۴]، سازوکاری بیان شده است که براساس رفتار هر گره شناسایی صورت می‌گیرد و جزئیات حمله تهیه می‌شود. داده‌های به‌دست‌آمده از شبکه شامل نرخ ارسال درخواست مسیر و نرخ دریافت پاسخ بسته‌ها است. الگوریتم ژنتیک برای شناسایی رفتارهای مخرب از عادی با توجه به دو معیار فوق استفاده شده است؛ که در آن از یک حد آستانه برای شناسایی استفاده شده است.

در [۱۵]، راه‌حلی بیان شده است که از وقوع حمله سیاه‌چاله جمعی جلوگیری می‌کند. در این روش برای مقابله با حملات سیاه‌چاله از جدول صحت استفاده می‌شود که در آن هر گره شرکت‌کننده یک درجه صحت دارد که به‌عنوان اندازه اطمینان آن گره محسوب می‌شود. اگر درجه صحت یک گره صفر شود به این معنی است که این گره، یک گره خرابکار است که اصطلاحاً به آن سیاه‌چاله گفته می‌شود که باید دور ریخته شود. گره مبدأ بسته درخواست مسیر را به همسایگانش می‌فرستد. پس‌ازآن مبدأ به‌اندازه زمان‌سنج[1] منتظر می‌ماند تا بسته‌های پاسخ مسیر جمع‌آوری شوند. در هرکدام از بسته‌های پاسخ مسیر دریافتی، درجه صحت گره پاسخ‌دهنده مشخص است، برای هرکدام از آن‌ها درجه صحت گام بعدی آن‌ها، بررسی می‌شود. اگر دو یا بیشتر از دو مسیر که درجه صحت یکسانی دارند، وجود داشت آنگاه آن مسیری انتخاب می‌شود که تعداد گام کمتری داشته باشد در غیر این صورت، مسیری که درجه صحت بیشتری دارد انتخاب می‌شود. با دریافت بسته‌های اطلاعاتی، گره مقصد یک تصدیق دریافت[2] به مبدأ می‌فرستد که به‌وسیله آن، درجه صحت گره میانی افزایش می‌یابد، اگر تصدیق دریافت به مبدأ نرسد آنگاه درجه صحت گره میانی کاهش می‌یابد.

در [۱۶]، یک الگوریتم IDPS ساده در برابر حمله سیاه‌چاله ارائه‌شده و عملکرد شبکه بعد از اعمال IDS اندازه‌گیری شده است. روش پیشنهادی اثر گره مهاجم را به صفر رسانده و همچنین باعث بهبود عملکرد مسیریابی شبکه شده است. شبیه‌سازی حمله سیاه‌چاله با نرم‌افزار شبیه‌ساز NS-2 انجام شده و نرخ گم‌شدن بسته‌ها در حضور گره مهاجم و سامانه تشخیص نفوذ در برابر حمله گره‌های خرابکار اندازه‌گیری شده است. در روش پیشنهادی، کارایی شبکه بهبودیافته و عملکرد بهتری نسبت به حضور مسیرهای قابل‌اعتماد فراهم می‌کند که در پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا در دسترس نیست.

در [۱۷]، روشی ارائه شده است که از هر دو نوع حملات سیاه‌چاله پیشگیری می‌کند و با استفاده از اشتراک‌گذاری امن و روش‌های مسیریابی چندمسیره تصادفی، ارتباط داده‌ها را به‌صورت امن برقرار می‌کند. بعد از این‌که بسته‌ها توسط روش اشتراک‌گذاری محرمانه به اشتراک گذاشته شدند با استفاده از مسیرهای تصادفی چندگانه، بسته‌ها تحویل داده می‌شوند. این روش شامل چهار مرحله است: ۱- جلوگیری از سیاه‌چاله توسط روش دریافت پاسخ مسیر ۲- اشتراک‌گذاری امن اطلاعات ۳- تصادفی‌کردن انتشار هر اطلاعاتی که به اشتراک گذاشته‌شده با استفاده از مسیریابی چندمسیره تصادفی ۴- مسیریابی معمولی به سمت مقصد. این روش تضمین می‌کند مسیرهایی که به‌طور تصادفی تولید شده‌اند تا حد ممکن پراکنده هستند. با استفاده از مسیرهای پراکنده تصادفی، حداکثر توان عملیاتی همراه با کاهش تأخیر حتی پس از حضور سیاه‌چاله به‌دست آمده است. استفاده از مسیرهای تصادفی نسبت به یک مسیر واحد باعث افزایش نرخ تحویل بسته همراه با کاهش نرخ بسته‌های گم شده است.

در [۱۸]، سازوکاری برای شناسایی و جلوگیری از انواع مختلف حمله سیاه‌چاله از قبیل حملات سیاه‌چاله تکی و جمعی، ارائه‌شده که این مکانیسم براساس پروتکل ساده بردار فاصله مبتنی بر تقاضا شبکه موردی است. این روش نه‌تنها حمله سیاه‌چاله را شناسایی و از آن جلوگیری می‌کند بلکه قادر به جداسازی گره سیاه‌چاله از شبکه است. در این مکانیسم، از دو روش استفاده شده است: روش اول شناسایی گره سیاه‌چاله در طول مرحله کشف مسیر از پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا و روش دوم حذف گره سیاه‌چاله از شبکه است. در مرحله کشف مسیر اضافی، سربار زیادی که این روش بر شبکه تحمیل می‌کند بسیار کاهش پیدا کرده است. همچنین، کشف مسیر دوم توسط بسته‌های درخواست مسیر چندپخشی، بدون پخش همگانی آن‌ها بهینه‌سازی شده است. درنتیجه، بسته‌های داده با موفقیت به مقصد می‌رسند که یک موضوع حساس در این نوع از شبکه با منابع محدود است.

در [۱۹]، نویسندگان روشی را ارائه نموده‌اند که با جمع‌آوری پاسخ‌های رسیده در گره مبدأ و بررسی شماره ترتیب مقصد، نحوه انتخاب پاسخ مسیر پروتکل بردار فاصله مبتنی بر تقاضا را تغییر داده‌اند. در این روش همچنین از جدولی به نام جدول درستی استفاده شده است که سطوح درستی اختصاص داده شده به گره‌های شبکه در آن نگهداری می‌شود. با به‌روزشدن این جدول توسط گره مبدأ و ارسال آن برای سایر گره‌ها و همچنین پخش همگانی بسته هشدار در مورد گره‌هایی که سطح درستی آن‌ها صفر شده است، گره‌های خرابکار به سرعت شناسایی شده و از انتخاب پاسخ مسیر آن‌ها در جدول پاسخ اجتناب می‌شود. نتایج نشان‌دهنده این است که این روش، نرخ تحویل بسته را در سناریوهای حاوی سیاه‌چاله از ۲۲/۳۲ ٪ تا ۴۲/۳۴ ٪ افزایش داده است؛ اما تأخیر انتها به انتها و سربار مسیریابی در این روش، بیشتر از بردار فاصله مبتنی بر تقاضا است و این به دلیل انتظار گره مبدأ جهت جمع‌آوری بسته‌های پاسخ و پردازش زیادتر این روش نسبت به بردار فاصله مبتنی بر تقاضا و همچنین پخش

1- Timer
2- ACK

همگانی جدول درستی است.

در [۲۰]، سعی بر ایجاد مسیرهایی با ضریب امنیتی بالا است. همچون دیگر شبکه‌ها، امنیت در شبکه‌های موردی نیز موضوعی قابل توجه است و با توجه به ماهیت پویا و متغیر این شبکه‌ها و کاربرد آن در مناطقی با اطلاعات سری و مهم، امنیت داده و اطلاعات اهمیت به‌سزایی دارد. لذا با به کارگیری سازوکارهایی برای پایش گره‌ها و انتشار این اطلاعات به سایر گره‌های شبکه و سرورهای مکان مربوطه به کشف و رتبه بندی گره‌ها پرداخته است که در این صورت گره‌های بدخواه در شبکه به راحتی شناسایی شده و با اعمال مؤلفه‌هایی آن‌ها را از شبکه حذف نموده‌اند. در این روش برای ارسال بسته‌های به‌روزرسانی از دو جهت استفاده می‌شود تا گره‌های مستقر در انتهای نوارهای فرضی به‌طور همزمان اطلاعات دقیقی از سایر گره‌های موجود در نوار داشته باشند که در این صورت با ذخیره اطلاعات گره‌ها در چندین گره و سرور مکان به سربار پایین‌تر دست یافته‌اند.

در [۲۱]، از روش‌های الهام گرفته‌شده از زیست‌شناسی مانند بهینه‌سازی کلونی مورچه‌ها برای تغییر پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا استفاده شده است. مکان مورچه در هر گره با میزان فرومن[1] آن با استفاده از نرخ ارسال در گره محاسبه می‌شود. این پروتکل اصلاح‌شده با استفاده از پارامترهای مختلف به‌عنوان مثال نرخ تحویل بسته، تأخیر انتها به انتها و توان عملیاتی با پروتکل موجود مقایسه شده است. نتایج نشان‌دهنده افزایش نرخ تحویل بسته‌ها و توان عملیاتی و کاهش تأخیر انتها به انتها است که عملکرد بهتر روش پیشنهادی را در مقایسه با پروتکل موجود نشان می‌دهد. پروتکل پیشنهادی قادر به بهبود دو مشکل اصلی از قبیل امنیت و کارایی است، اما این روش تنها قادر به تشخیص حمله‌تکی است و برای حمله سیاه‌چاله قابل اجرا است.

در [۲۲]، به‌منظور تشخیص و مقابله با حمله سیاه‌چاله جمعی در پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا راه‌حلی ارائه شده است که در این راه‌حل وقتی گره‌ای بسته پاسخ مسیر را صادر کرد، در اطراف آن گره یک فرایند نظرخواهی صورت می‌گیرد. سپس براساس نظرات اعلام شده توسط همسایگان گره صادرکننده بسته پاسخ مسیر، در مورد خرابکاربودن گره پاسخگو تصمیم‌گیری می‌شود. این روش که با استفاده از نرم‌افزار Glomosim شبیه‌سازی شده است با دقت بالایی توانایی تشخیص گره‌های خرابکار را دارد و در زمانی‌که تعداد گره‌های خرابکار پایین باشد با هزینه اندکی می‌توان آن‌ها را تشخیص داد. به دلیل پخش همگانی بسته درخواست مسیر سربار الگوریتم بالا است اما به دلیل به‌روزرسانی جداول مسیریابی سربار الگوریتم کاهش پیدا کرده است. در ابتدا به دلیل سربار زیاد، تأخیر نیز افزایش یافته است ولی به‌تدریج که سرعت بالاتر می‌رود تأخیر کاهش پیدا می‌کند. نرخ تحویل بسته نیز نسبت به پروتکل بردار فاصله مبتنی بر تقاضا افزایش یافته است.

در [۲۳]، روشی برای کشف مسیر امن در پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا بیان شده است. در این روش گره مبدأ با پیداکردن بیش از یک مسیر به مقصد، اعتبار گره‌ای که بسته پاسخ مسیر را ارسال کرده، تأیید می‌کند. گره مبدأ صبر می‌کند تا بسته پاسخ مسیر را از بیش از دو گره دریافت کند. وقتی گره مبدأ بسته‌های پاسخ مسیر را دریافت کرد، درصورتی‌که در مسیرها به مقصد گام های مشترک وجود داشته باشد، گره مبدأ می‌تواند مسیر ایمن به مقصد را تشخیص دهد.

در [۲۴]، روشی با توجه به تأمین کیفیت سرویس برای مواجه با حملات سیاه‌چاله ارائه شده است. در این روش، بسته‌ها از مسیر رزرو شده‌ای که پیکربندی شده‌اند، ارسال می‌گردند. تمرکز اصلی در این روش، تأثیر کیفیت سرویس بر روی حمله سیاه‌چاله است. ویژگی‌های مختلف و درصد پیشرفت یا کاهش پارامترها مورد ارزیابی قرار گرفته است. هدف از این روش، تحلیل کیفیت سرویس بر حمله سیاه‌چاله است. جهت بررسی تأثیر استفاده از کیفیت سرویس در حمله سیاه‌چاله و در شبکه های موردی از شبیه‌ساز Opnet استفاده شده است. شاخص‌های عملکرد شامل تأخیر انتها به انتها، نسبت تحویل بسته و بهره‌وری هستند که در تحلیل نتایج به‌کار رفته‌اند پس از اعمال روش پیشنهادی، پارامتر تأخیر انتها به انتها ۷۹/۵۴ ٪، همچنین پارامتر نسبت تحویل بسته ۵۰ ٪ و پارامتر بهره‌وری ۵/۶ ٪ بهبود پیدا کرده‌اند.

در [۲۵]، نویسندگان برای حذف مسیرهایی که دارای گره‌های سیاه‌چاله هستند به این صورت عمل کرده‌اند که اولین و دومین مسیر پیشنهادی برای ارسال اطلاعات را نادیده می‌گیرند و سومین مسیر به بعد را استفاده می‌کنند دلیل ارائه این روش را چنین توجیه نمودند که چون گره‌های سیاه‌چاله اغلب در مسیرهای پیشنهادی اول یا دوم هستند بنابراین از این دو مسیر برای ارسال اطلاعات استفاده نمی‌کنند و در واقع این دو مسیر را

1 -Pheromone

در قرنطینه نگهداری می‌کنند. روش پیشنهادی با اجرای آن در نرم‌افزار شبیه‌ساز NS-2 ارزیابی شده است و نتایج نشان‌دهنده تأثیر روش ارائه‌شده در جلوگیری از حمله سیاه‌چاله است.

در [۲۶]، روشی ارائه شده است که هدف آن شناسایی گره‌های سیاه‌چاله جمعی در پروتکل مسیریابی بردار فاصله مبتنی بر تقاضا است. در این روش، ابتدا سیستم تشخیص نفوذ شروع به جمع‌آوری اطلاعات می‌کند. سپس با توجه به تاریخچه گره‌های موجود در شبکه گره‌های مخرب شناسایی و در قرنطینه قرار می‌گیرند. درنهایت، الگوریتم پیشنهادی با پروتکل بردار فاصله مبتنی بر تقاضا پایه و الگوریتم دیگری که با استفاده از روش دیگر گره‌های سیاه‌چاله را شناسایی می‌کند با شبیه‌ساز OPNET مقایسه شده است. روش ارائه‌شده با حداقل هزینه یا سربار، گره‌های بدرفتار را شناسایی و در قرنطینه قرار می‌دهد. نتایج شبیه‌سازی حاکی از آن است که الگوریتم پیشنهادی توانسته است حمله گره‌های سیاه‌چاله را تشخیص داده و بسته‌های اطلاعاتی بیشتری را در زمان مساوی با دو الگوریتم دیگر، ارسال کند و کارایی شبکه را به میزان قابل‌توجه‌ای افزایش دهد.

۵- روش پیشنهادی

در حمله سیاه‌چاله، گره‌های خرابکار با وانمودکردن خود به‌عنوان کوتاه‌ترین مسیر در رساندن بسته‌ها از مبدأ به مقصد، فرستنده را فریب داده و وی را وادار می‌کنند تا بسته خود را برای ارسال به مقصد، به گره خرابکار تحویل دهد. بدین ترتیب به آسانی تعدادی یا تمام بسته‌های دریافتی را به‌جای ارسال به سمت مقصد، از بین می‌برند. از این‌رو، در این مقاله با ایجاد تغییراتی چند و ترکیب روش‌های تعیین مسیر امن و شناسایی و حذف‌کردن گره خرابکار روشی برای مقابله با حمله سیاه‌چاله در دو مرحله ارائه می‌شود.

مرحله اول: روش پیشنهادی [۲۳]، گره مبدأ صبر می‌نماید تا بیش از یک مسیر به سمت مقصد پیدا شود. سپس گره مبدأ یک بسته اطلاعاتی پینگ[1] را با استفاده از این مسیرهای افزونه به‌صورت تک‌پخشی به سمت مقصد می‌فرستد. بسته اطلاعاتی پینگ مدت‌زمان ارسال بسته از گره مبدأ، رسیدن آن به گره مقصد و ارسال مجدد آن به گره مبدأ را مشخص کرده و سوابق بسته‌های گم‌شده را ثبت می‌کند. اگر گره‌ای اولین بسته را دریافت کرده باشد، در صورت دریافت بسته دوم که کپی همان بسته اول است، آن را بیرون می‌اندازد. لذا لازم است جهت اجتناب از بیرون انداخته‌شدن بسته دوم اطلاعاتی پینگ، شماره‌های شناسایی و شماره‌های توالی متفاوتی را به بسته‌ها نسبت داد. گره دریافت کننده و مخرب به همراه هر گره میانی که ممکن است مسیری به مقصد داشته باشد، به این درخواست بسته اطلاعاتی پینگ پاسخ خواهند داد. گره مبدأ این پاسخ‌ها را برای تشخیص این‌که کدام امن نبوده و ممکن است از طرف گره مخرب باشد، پردازش می‌کند. به‌عبارت‌دیگر، گره مبدأ با به کارگیری افزونگی مسیر در شبکه، اعتبار گره‌ای که بسته پاسخ مسیر را ارسال کرده است تأیید می‌کند. به دلیل این‌که هر بسته‌ای می‌تواند از طریق بسیاری از راه‌های افزونه به مقصد رسیده باشد، ایده این راه حل انتظار برای دریافت بسته پاسخ مسیر از بیش از دو گره است. در این مدت، گره ارسال کننده، بسته‌ها را تا زمان تشخیص یک مسیر امن، در بافر قرار خواهد داد. به‌محض اینکه یک مسیر امن، مشخص شد بسته‌هایی که در بافر قرار دارند ارسال خواهند شد. هنگامی‌که یک بسته پاسخ مسیر به گره مبدأ برسد، وی مسیرهای کامل به مقصدها را استخراج کرده و در انتظار یک بسته پاسخ مسیر دیگر می‌ماند. از آن‌جا که در شبکه‌های موردی، مسیرهای افزونه در اغلب زمان‌ها، تعدادی گام یا گره اشتراکی دارند دو یا تعداد بیشتری از این گره‌ها باید تعدادی گام مشترک داشته باشند. با توجه به این گام‌های مشترک، گره مبدأ می‌تواند مسیر امن به مقصد را تشخیص دهد. اگر هیچ گره مشترکی در این مسیرهای افزونه نباشد، ارسال‌کننده در انتظار یک بسته پاسخ مسیر دیگر می‌ماند تا زمانی‌که یک مسیر با گام‌های مشترک مشخص شود یا زمان‌سنج مسیریابی منقضی شود. این راه‌حل، می‌تواند پیدانمودن مسیر امن به مقصد را تضمین نماید؛ اما عیب اصلی آن، تأخیر زمانی است. بسیاری از بسته‌های پاسخ مسیر، باید به‌وسیله گره مبدأ دریافت و پردازش شوند. علاوه‌بر آن، اگر گره یا گام اشتراکی بین مسیرها وجود نداشته باشد، بسته‌ها هیچ‌وقت ارسال نمی‌شوند. در فاز اول، با استفاده از افزونگی، مسیرهای دارای گام‌های مشترک به‌عنوان مسیر امن شناسایی شد؛ اما همچنان امکان آن وجود دارد که در این مسیر گره خرابکار وجود داشته باشد که هوشمندانه با اعلام چند گام مشترک، خود را در یک مسیر امن قرار داده باشد.

مرحله دوم: از روش پیشنهادی [۲۲] به منظور جلوگیری از ارائه‌دادن اطلاعات غلط به گره‌های بررسی‌کننده، گره‌های خرابکار شناسایی، قرنطینه و از فرآیند مسیریابی حذف می‌شوند. هرچقدر تعداد گره‌های خرابکار افزایش یابد، شناسایی گره‌های خرابکار سخت‌تر می‌شود به همین دلیل، نرخ تحویل بسته با افزایش گره‌های خرابکار کاهش می‌یابد؛ بنابراین، با شناسایی هرچه بهتر

1- Ping

گره‌های خرابکار می‌توان تأخیر را کاهش و نرخ تحویل بسته را افزایش داد. گره های خرابکار گره‌هایی هستند که تعداد زیادی بسته داده به آن‌ها تحویل داده می‌شود ولی هیچ یا تعداد کمی بسته توسط آن ها به گره مقصد یا گره‌های همسایه ارسال می‌شود. هنگامی‌که گره‌ای یک بسته پاسخ مسیر از همسایه خود دریافت نماید قبل از هر اقدام و اعتمادی بایستی وضعیت همسایه خود را بررسی کند. اگر گره پاسخ‌دهنده، گره مقصد باشد نیاز به بررسی بیشتر نیست؛ اما اگر گره پاسخ‌دهنده یک گره میانی باشد بایستی بررسی‌های بیشتری انجام شود. بدین ترتیب که اگر خرابکاربودن گره طبق قوانینی که در ادامه آمده است احراز شود، بسته پاسخ مسیر باید دور انداخته شود. در غیر این صورت، جهت کسب اطلاعات بیشتر درباره فعالیت های گره مورد نظر، از همسایگان اطراف آن گره پرس‌وجو و رأی‌گیری به عمل می‌آید. در ادامه برای تعیین خرابکاربودن گره مورد نظر، گره مبدأ داده‌های به دست آمده از رأی‌گیری را با قوانین ذیل پردازش می‌کند. اگر تشخیص داده شود که گره مذکور خرابکار است یک پیام هشدار در شبکه پخش خواهد شد تا گره مذکور در قرنطینه قرار گیرد.

در الگوریتم پیشنهادی برای احراز هویت گره از قوانین زیر استفاده می‌شود:

الف) گره‌ای که زودتر از سایر گره‌های شبکه، یک بسته پاسخ مسیر را به گره درخواست‌کننده مسیر ارسال می‌کند گره خرابکار است. به دلیل این‌که گره خرابکار جدول مسیریابی خود را بررسی نمی‌کند قبل از سایر گره‌ها به گره درخواست‌کننده مسیر پاسخ می‌دهد.

ب) گره‌ای که در بسته پاسخ مسیر خود بیشترین شماره ترتیب و کمترین تعداد گام را دارد، گره خرابکار است. در حمله سیاه‌چاله گره خرابکار در بسته پاسخ مسیر خود بیشترین شماره ترتیب و کمترین تعداد گام را قرار می‌دهد.

ج) گره‌ای که تعداد زیادی بسته دریافت کرده و هیچ‌یک از آن‌ها را ارسال نکرده است گره خرابکار است.

د) گره‌ای که تعداد زیادی بسته درخواست مسیر دریافت کرده و حداکثر یک بسته پاسخ مسیر فرستاده است یک گره خرابکار است.

با توجه به قوانین ذکرشده، اصول الگوریتم پیشنهادی به شرح ذیل است:

۱) در تمامی مراحل، اطلاعات مربوط به فعالیت گره‌ها شامل تعداد بسته های دریافتی، تعداد بسته‌های ارسالی و تعداد پاسخ‌های مسیر ارسالی، نگهداری و ثبت می‌شوند.

گره‌های موجود در شبکه‌های موردی به‌منظور برقراری ارتباط بین دو گره، فعالیت‌هایی را انجام می‌دهند که این فعالیت‌ها ذخیره شده و مورد بررسی قرار می‌گیرند. این فعالیت‌ها شامل داده هایی که یک گره میانی از گره مبدأ دریافت کرده است، داده‌هایی که گره میانی به گره مقصد ارسال کرده است و پاسخ‌های مسیری که گره میانی برای گره مبدأ فرستاده است، می‌باشند.

۲) بسته درخواست نظرات در مورد گره‌ای که بسته پاسخ مسیر را ارسال کرده است به همسایه ها فرستاده می‌شود.در شبکه های موردی به دلیل این‌که گره های شبکه با یکدیگر در ارتباط هستند، برای دریافت اطلاعات در مورد خرابکاربودن گره‌ای که بسته پاسخ مسیر را به گره مبدأ ارسال کرده است، می‌توان از همسایه‌های آن گره کمک گرفت.

۳) اطلاعات مربوط به گره فرستنده بسته پاسخ مسیر که در گره‌های همسایه آن ذخیره شده است، دریافت می‌شوند.

بعد از ارسال بسته درخواست نظرات به همسایه‌ها، گره‌های همسایه نظر خود در مورد خرابکار بودن آن گره را به گره مبدأ ارسال می‌کنند.

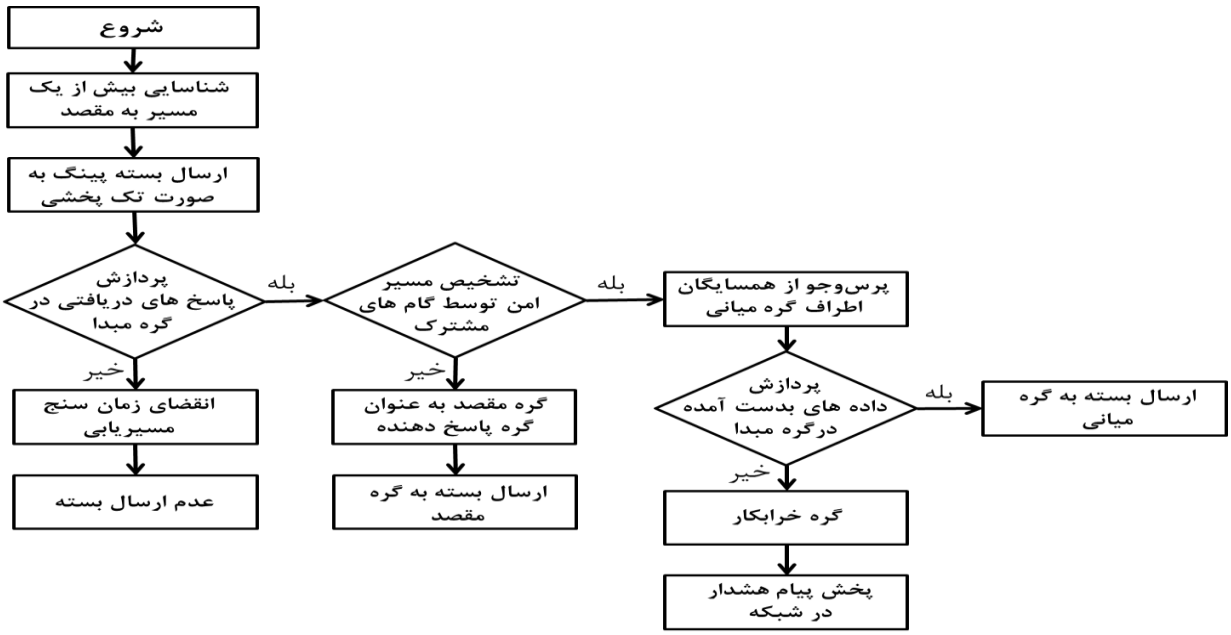
۴) اطلاعات دریافتی و نظرات همسایگان در مورد خرابکاربودن گره، ارزیابی می‌شوند.

پس از این‌که گره مبدأ اطلاعات را از گره‌های همسایه دریافت کرد آن ها را به‌منظور بررسی خرابکاربودن گره‌ای که بسته پاسخ مسیر را ارسال کرده است مورد پردازش و ارزیابی قرار می‌دهد.

۵) اگر گره مورد نظر خرابکار تشخیص داده شود یک پیام هشدار برای قرنطینه‌کردن گره خرابکار در سراسر شبکه پخش می‌شود.

۶) گره‌های داخل قرنطینه از فرآیند مسیریابی حذف می‌شوند.

گره های موجود در قرنطینه به دلیل جلوگیری از ایجاد حمله یا اخلال در فرآیند مسیریابی، از فرآیند مسیریابی کنار گذاشته می‌شوند. درنتیجه گره‌های موجود در شبکه بسته‌های ارسالی خود را از مسیر این گره‌ها ارسال نمی‌کنند. روند نمای الگوریتم پیشنهادی در شکل (۴) نشان داده شده است.



شکل (۴): روند نمای الگوریتم پیشنهادی.

۵-۱- جنبه نوآوری

برخلاف مقالات ارائه شده در این زمینه، الگوریتم پیشنهادی در این مقاله ترکیبی از روش‌های شناسایی مسیر امن و تشخیص گره‌های خرابکار با توجه به رفتار آن‌ها است. با استفاده از شناسایی مسیر امن دیگر نیازی به بررسی رفتار تمامی گره‌های موجود در شبکه به‌منظور شناسایی گره خرابکار نیست. درصورتی‌که مسیر امن شناسایی شود فقط تعداد گره‌های تشکیل‌دهنده مسیر شناسایی شده و عملکرد و رفتار آن‌ها مورد بررسی قرار می‌گیرد.

همچنین، در الگوریتم پیشنهادی شناسایی گره‌های خرابکار توسط گره مبدأ صورت می‌گیرد. ممکن است یکی از گره‌های همسایه خود نیز یک گره خرابکار باشد و بخواهد با ارائه‌دادن اطلاعات غلط در مورد گره مورد نظر باعث ایجاد حمله سیاه‌چاله شود، به همین دلیل، گره مبدأ درستی گره‌ای که بسته پاسخ مسیر را ارسال کرده است را بررسی می‌کند تا همسایه‌ها نتوانند در اجرای حمله سیاه‌چاله با گره مورد نظر همکاری کنند.

در الگوریتم پیشنهادی از تعدادی قوانین برای شناسایی گره خرابکار استفاده شده است در [۲۲]، این قوانین وجود ندارد. همچنین، به دلیل این‌که ممکن است گره خرابکار به‌صورت هوشمندانه ابتدا چند بسته داده را ارسال کند و بعد از جلب اعتماد گره‌ها شروع به سوءاستفاده و حذف بسته‌های دریافتی کند برخلاف [۲۲]، به هیچ گره‌ای از قبل اعتماد نمی‌شود و همه گره‌ها یکسان هستند. برخلاف [۲۳]، ممکن است در مسیر امن شناسایی‌شده توسط گام‌های مشترک، گره خرابکاری وجود داشته باشد که با ترکیب روش تشخیص گره خرابکار بعد از روش شناسایی مسیر امن در الگوریتم پیشنهادی این مورد برطرف شده است.

عیب این روش نسبت به روش‌های دیگر سربار بالا است. به دلیل این‌که تمامی همسایه‌ها اطلاعات خود را به گره مبدأ ارسال کرده و گره مبدأ درستی گره مورد نظر را بررسی می‌کند ترافیک در گره مبدأ زیاد شده و باعث می‌شود که سربار افزایش یابد. در [۲۲]، به دلیل پخش همگانی بسته درخواست مسیر سربار بالا است اما به دلیل به‌روزرسانی جداول مسیریابی سربار کاهش پیدا کرده است. در [۲۳]، سربار به دلیل پخش همگانی جدول درستی افزایش پیدا کرده است.

۶- محیط و نتایج شبیه‌سازی

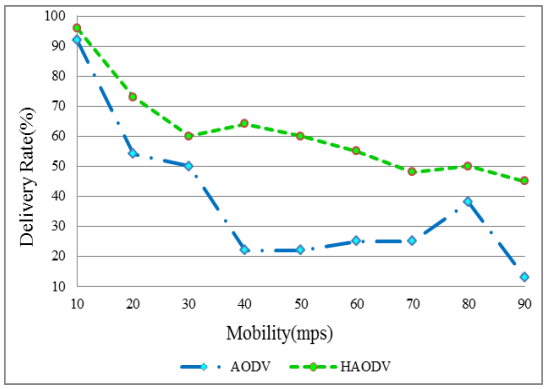
برای شبیه‌سازی از نرم‌افزار OMNET++ 4.6 استفاده شده است. شبکه شامل ۴۰ گره است که به‌طور تصادفی حرکت می‌کنند. یک گره در شبکه حمله سیاه‌چاله را اجرا می‌کند. زمان تعیین‌شده برای شبیه‌سازی ۳۰۰s می‌باشد. محیط شبیه‌سازی

۱۰۰۰m*۱۰۰۰m در نظر گرفته شده است. از Random Waypoint (RWP) به‌عنوان مدل تغییر مکان گره‌ها استفاده شده است. در این شبیه‌سازی دو جریان ترافیکی در شبکه وجود دارد که با نرخ ثابت بسته‌ها را به شبکه ارسال می‌کنند و نوع ترافیک استفاده شده Constant Bit rate (CBR) می‌باشد. در جدول (۱) پارامترهای شبیه‌سازی نشان داده شده است.

جدول (۱): پارامترهای شبیه‌سازی

Simulator	OMNET++ 4.6
Number of system nodes	40
Number of black hole nodes	1
The time of simulation	300 (s)
Topology	1000m × 1000m
Routing protocol	AODV
Data traffic	CBR
Transmission range	200m
Packet size	512 bytes
Node mobility model	RWP

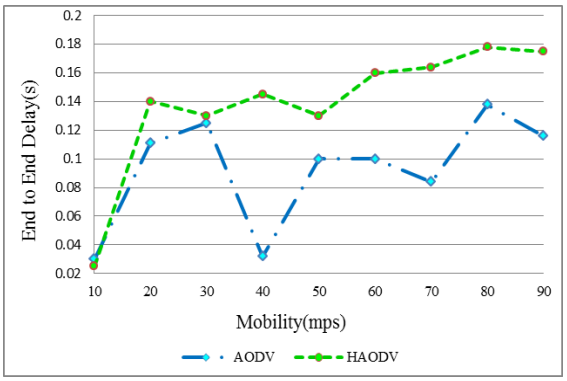
نتایج شبیه‌سازی براساس تحرک گره‌ها در نمودارهای زیر نشان داده شده است. در نمودارها منظور از AODV پروتکل استاندارد AODV است که دچار حمله سیاه‌چاله شده است و منظور از HAODV الگوریتم پیشنهادی می‌باشد.



شکل (۵): تأثیر حمله سیاه‌چاله بر نرخ تحویل بسته در شبکه.

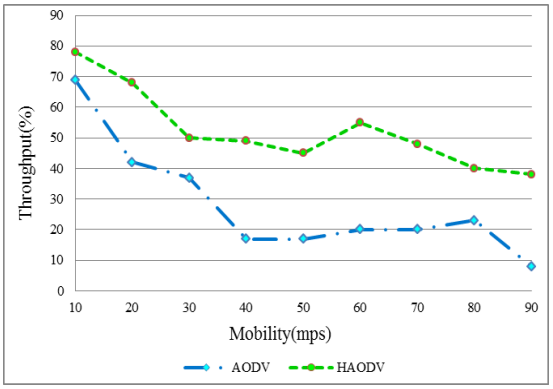
همان‌طور که در شکل (۵) نشان داده شده است به دلیل شناسایی مسیر امن و تشخیص و قرنطینه‌کردن گره خرابکار نرخ تحویل بسته در پروتکل HAODV افزایش یافته است. به دلیل این‌که در زمان حمله، بسته‌های زیادی توسط گره خرابکار حذف می‌شود نرخ تحویل بسته در پروتکل AODV کاهش یافته است.

در [۲۳-۲۲] نیز نرخ تحویل بسته نسبت به پروتکل AODV بهبود یافته است.



شکل (۶): تأثیر حمله سیاه‌چاله بر تأخیر انتها به انتها در شبکه.

شکل (۶) نتیجه مقایسه تأخیر انتها به انتهای پروتکل AODV و الگوریتم پیشنهادی را نشان می‌دهد. با توجه به این‌که فقط گره مبدأ درستی گره‌های شبکه را بررسی می‌کند سربار روش پیشنهادی افزایش یافته است. به همین دلیل، تأخیر انتها به انتها در پروتکل HAODV نسبت به پروتکل AODV نیز افزایش پیدا کرده است. در [۲۲] در ابتدا به دلیل سربار زیاد، تأخیر نیز افزایش یافته است ولی به‌تدریج که سرعت بالاتر می‌رود تأخیر کاهش پیدا می‌کند. در [۲۳] به دلیل انتظار گره مبدأ جهت جمع‌آوری بسته‌های پاسخ و پردازش بیشتر تأخیر نسبت به پروتکل AODV افزایش پیدا کرده است.



شکل (۷): تأثیر حمله سیاه‌چاله بر توان عملیاتی شبکه.

شکل (۷) نشان‌دهنده افزایش توان عملیاتی الگوریتم پیشنهادی می‌باشد. به دلیل این‌که نرخ تحویل بسته در الگوریتم پیشنهادی افزایش یافته است توان عملیاتی نیز در پروتکل HAODV نسبت به پروتکل AODV افزایش پیدا کرده است.

۷- نتیجه‌گیری

همانند دیگر شبکه‌ها، ایجاد امنیت در شبکه‌های موردی یکی از مسائل مطرح در طراحی این دسته از شبکه‌ها است و طی سال‌های گذشته روش‌های متعددی برای حل این مسئله پیشنهاد شده است. با توجه به ضعف این‌گونه شبکه‌ها ازنظر خطر در برابر حملات مختلف، جا دارد تا این ضعف‌ها مورد بررسی دقیق‌تری قرار بگیرد تا با اطمینان بیشتری بتوان از آن‌ها استفاده نمود. در این مقاله روش ترکیبی جدیدی ارائه گردید که می‌تواند مسیر امن برای فرستادن بسته‌ها به مقصد را شناسایی کند و گره‌های خرابکاری که قصد اخلال در مسیریابی دارند را از بین ببرد. از معیارهای نرخ تحویل بسته، تأخیر انتها به انتها و توان عملیاتی برای ارزیابی الگوریتم پیشنهادی استفاده شده است. با توجه به نتایج شبیه‌سازی می‌توان دریافت که الگوریتم پیشنهادی نسبت به پروتکل AODV در برابر حمله سیاه‌چاله بهتر عمل می‌کند. افزایش کارایی شبکه در الگوریتم پیشنهادی با افزایش توان عملیاتی و نرخ تحویل بسته، حاصل شده است.

۸- مراجع

[1] S. Shahabi, M. Ghazvini, M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," Wireless Networks, vol. 22, pp. 1505-1511, July 2016.

[2] S. M. Pournaghi, M. Barmshoori, M. Gardeshi, "An Improved Authentication Scheme with Conditional Privacy Preserving in VANETs," Journal of Electronical & Cyber Defence, vol. 3, pp. 1-12, 2015. (in Persian)

[3] L. J. García Villalba, J. García Matesanz, A. L. Sandoval Orozco, and J. D. Márquez Díaz, "Auto-configuration protocols in mobile ad hoc networks," Sensors, vol. 11, pp. 3652-3666, Mar. 2011.

[4] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: friend-based ad hoc routing using challenges to establish security in manets systems," IEEE Systems Journal, vol. 5, pp. 176-188, Jun 2011.

[5] A. Golestani, K. Mohamedpour, and A. Habibi Bastami, "Enhancing Communication Security in Cellular Communications Networks by using Interference Alignment Technique," Journal of Electronical & Cyber Defence, vol. 3, pp. 49-60, 2015. (in Persian)

[6] P. K. Maurya, G. Sharma, V. Sahu, A. Roberts, M. Srivastava, and M. Scholar, "An overview of AODV routing protocol," International Journal of Modern Engineering Research (IJMER), vol. 2, pp. 728-732, May 2012.

[7] G. S. Tomar, T. Sharma, D. Bhattacharyya, and T. H. Kim, "Performance comparision of AODV, DSR and DSDV under various network conditions: a survey," In Ubiquitous Computing and Multimedia Applications (UCMA), 2011 International Conference on, IEEE, pp. 3-7, Apr. 2011.

[8] R. Das, B. S. Purkayastha, and P. Das, "Security measures for black hole attack in Manet: An approach," arXiv preprint arXiv: 1206.3764, Jun 2012.

[9] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," IJ Network Security. vol. 5, pp. 338-346, Nov. 2007.

[10] S. Jamali and S. Behzad, "A survey over black hole attack detection in mobile ad hoc network," International Journal of Computer Science and Network Security (IJCSNS), vol. 15, p. 44, Mar. 2015.

[11] T. K. Araghi, M. Zamani, A. B. Manaf, S. M. Abdullah, H. S. Bojnord, and S. K. Araghi," A secure model for prevention of black hole attack in wireless mobile ad hoc networks," In12th International Conference on Applied Computer and Applied Computational Science (ACACOS '13), Kualalumpur, Malaysia, pp. 2-4, Apr. 2013.

[12] S. K. Arora, S. Vijan, and G. S. Gaba, "Detection and analysis of black hole attack using IDS," Indian Journal of Science and Technology, vol. 9, May 2016.

[13] N. Khemariya and A. Khuntetha, "An efficient algorithm for detection of blackhole attack in aodv based manets," International Journal of Computer Applications, vol. 66, Jan 2013.

[14] K. S. Sujatha, V. Dharmar, and R. S. Bhuvaneswaran," Design of Genetic Algorithm based IDS for MANET," InRecent Trends In Information Technology (ICRTIT), 2012 International Conference on, pp. 28-33, IEEE, Apr. 2012.

[15] M. Salehi and H. Samavati, "Dsr vs olsr: Simulation based comparison of ad hoc reactive and proactive algorithms under the effect of new routing attacks," InNext Generation Mobile Applications, Services and Technologies (NGMAST), 2012 6th International Conference on, IEEE, pp. 100-105, Sep. 2012.

[16] S. Dubey and P. Saxena, "A Review on Collaborative Decision Technique for Blackhole Attack Prevention in MANET," International Journal of Scientific & Engineering Research, vol. 7, pp. 230-236, Jan 2016.

[17] V. Kamatchi and R. Mukesh, "Securing data from black hole attack using aodv routing for mobile ad hoc networks," In Advances in Computing and Information Technology, Springer, Berlin, Heidelberg, vol. 177, pp. 365-373, 2013.

[18] S. Banerjee, M. Sardar, and K. Majumder, "Aodv based black-hole attack mitigation in manet," In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013, Springer, Cham, vol. 247, pp. 345-352, 2014.

[19] I. Zangeneh, M. Sadeghzade, and S. J. Mirabedini, "A new method for detecting and removing a single black hole attack in AODV protocol ad hoc network," First National Conference on Electrical and Computer southern Iran, Islamic Azad University of Khormoj, May 2013. (in Persian)

[20] A. Momeni and M. Parhizgar, "Providing a safe location service to cope with the attack of a black hole," The first Conference of artificial intelligence systems and their applications, Payamnoor University of Tehran, 2011. (in Persian)

[21] A. Vangili and K. Thangadurai, "Detection of black hole attack in mobile ad-hoc networks using ant colony optimization–simulation analysis," Indian Journal of Science and Technology, vol. 8, Jul. 2015.

[22] M. Medadian, K. Fardad, and I. Barazande, "Discovered and removed a mass black hole attacks on mobile networks Ad Hoc," First National Conference on Soft Computing and Information Technology, Islamic Azad University of Mahshahr, Mar. 2011. (in Persian)

[23] M. Al-Shurman, S. M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," In Proceedings of the 42nd annual Southeast regional conference, ACM, pp. 96-97, Apr. 2004.

[24] A. A. Arjomand, "Provide a way to confronting with black hole attacks in ad hoc networks and survey its effect on basic parameters of AODV routing protocol," The First Conference on Advances and Challenges in Engineering and Technology Sciences (SET), Advanced Institute of Science and Technology Kharazmi, Shiraz, Iran, Jan 2016. (in Persian)

[25] R. Kesavan and V. T. Bai, "Avoidance of Black Hole Attack in Virtual Infrastructure for MANET," International Journal of Computer Applications, vol. 50, pp. 26-31, Jan 2012.

[26] E. Azizi Abolmomen and A. Nori, "Provide a way to detect and prevent of black hole nodes attack in Ad hoc networks," First Regional Conference on Theoretical and Applicational in Computer Engineering and Information Technology, University of Science and Technology of Saghez, 2015. (in Persian)

Journal of Electronical & Cyber Defence
Vol. 5, No. 4, 2017, Serial No. 20

Presenting a New Algorithm with Aiming to Improve Security and Performance of AODV Protocol in Ad Hoc Network

S. Shahabi Rabori, M. Ghazvini*

*Shahid Bahonar University of Kerman

(Received: 15/11/2016, Accepted: 13/02/2017)

ABSTRACT

Ad hoc networks include some wireless nodes which do not need any pre-existing network's substructure. The nodes communicate to each other without any infrastructure. Because of some specifications such as dynamic changes of network's structure, presumptions trust each other and ignore the nodes' actions, Ad hoc networks are not protected against attacks of destructive nodes. In this study, a new method has been represented by combining a safe route detection method and an opposition method to destructive nodes to black hole attack countermeasure in AODV routing protocol. At the first step, the source node confirms the validity of the route reply packet sender's node by finding more than one route to the destination. When a route reply packet arrives to a source node, then that node extracts the complete route to destruction and waits for other packs of route reply. The idea of this solution is waiting to receive route reply packet from more than two nodes. In the next step, according to nodes' manner in the network, a voting from neighboring nodes has been done and by use of predefined rules, destructive nodes are identified and destroyed. Simulations results of OMNet++ simulator show some improvements of the proposed algorithm to the original AODV protocol which has been attacked by the black hole.

Keywords: Ad Hoc Network, AODV Routing Protocol, Black Hole Attack, Safe Path.

* Corresponding Author Email: mghazvini@uk.ac.ir