

کشف و حذف حمله سیاه چاله جمعی در شبکه ad hoc

سهیلا شکری

کارشناسی، مهندسی کامپیوتر، گرایش نرم افزار، دانشگاه پیام نور

نام نویسنده مسئول:

سهیلا شکری

تاریخ دریافت: ۱۴۰۰/۰۵/۱۵

تاریخ پذیرش: ۱۴۰۰/۰۷/۰۳

چکیده

شبکه‌های ویژه سیار شامل تعداد از گره‌ها بوده که آزادانه بدون داشتن هیچ گونه زیرساخت شبکه‌ای و همچنین از طریق فرکانس رادیویی می‌توانند با یکدیگر مرتبط باشند. سرعت در برپایی و همچنین بدون ساختار بودن این شبکه‌ها سبب شده که نقش مهمی را در زمینه‌های مختلف مانند کاربردهای نظامی و اضطراری، محیط‌های دانشگاهی، حوادث طبیعی و همچنین محیط‌های شهری ایفا می‌نمایند. مبحث امنیت در این شبکه‌ها یکی از مهم‌ترین مباحث تحقیقاتی می‌باشد. لذا در این پژوهش به بررسی امنیت در مسیریابی AODV خواهیم پرداخت. آنچه در این پژوهش ارائه می‌گردد، بررسی حمله سیاه چاله جمعی در پروتکل مسیریابی AODV و همچنین ارائه راهکاری به منظور تشخیص و مقابله با آن است.

واژگان کلیدی: سیاه چاله، سیاه چاله جمعی، AODV، ad hoc

مقدمه

امروزه تمایل به استفاده از شبکه های بی سیم روز به روز در حال افزایش است؛ چون هر شخصی، هر جایی و در هر زمانی می تواند از آنها استفاده نماید. در سالهای اخیر رشد شگرفی در فروش کامپیوترهای قابل حمل بوجود آمده است. این کامپیوترهای کوچک، به چندین گیگابایت حافظه روی دیسک، نمایش رنگی با کیفیت بالا و کار تنهای شبکه بی سیم مجهز هستند. بعلاوه، این کامپیوترهای کوچک می توانند چندین ساعت فقط با نیروی باتری کار کنند از اینرو کاربران آزادند براحتی آنها را به هر طرف که می خواهند منتقل نمایند. زمانی که کاربران شروع به استفاده از کامپیوتر های متحرک نمودند به اشتراک گذاشتن اطلاعات بین کامپیوترها یک نیاز طبیعی را بوجود آورد. از جمله کاربردهای به اشتراک گذاری اطلاعات در مکانهایی نظیر سالن کنفرانس، کلاس درس، ترمینال های فرودگاه و همچنین در محیط های نظامی است. شبکه های ویژه بسیار مجموعه ای از گردهای بی سیم است که می توانند بصورت پویا در هر مکان و در هر زمان بدون استفاده از هر زیرساخت شبکه ای تشکیل شوند. اغلب این گردها در آن واحد هم بعنوان مسیریاب و هم بعنوان گرد عمل می کنند. این خاصیت سبب شده که در موارد اضطراری که امکان تشکیل شبکه ای با ساختار ثابت و از پیش تعریف شده وجود ندارد، مانند موارد نظامی و یا وقوع سیل و...، بتوان از این شبکه ها استفاده کرد. ارتباط میان گردها در این شبکه از طریق امواج رادیویی صورت می گیرد و در صورتی که یک گره در برد رادیویی گرد دیگر باشد همسایه آن گره به حساب می آید و در غیر این صورت در صورت نیاز به ارتباط میان دو گره که در برد رادیویی یکدیگر نیستند می توان از کمک گردهای دیگر در این مورد استفاده کرد، بنابراین ارتباط میان گردها در این شبکه به نوعی پر مبنای اعتماد و مشارکت میان گردها صورت می گیرد. مبحث امنیت در این شبکه ها امروزه یکی از مباحث مهم تحقیقاتی است. تحرک گردها، بی سیم بودن ارتباطات، تغییر پویای ساختار شبکه، فقدان مدیریت متمرکز برای بررسی رفتارها و عملکردها، فقدان خطوط دفاعی مشخص و محدودیت در توان مصرفی گردها، بستر مناسبی را برای حملات مختلف علیه این شبکه ها فراهم می آورد. به خاطر ساختار مسیریابی شبکه های ویژه بسیار [۱،۲،۳] که به نوعی بر مبنای یک جور اعتماد میان گردها استوار است فرصت خوبی را برای حمله کنندگان فراهم می سازد تا با شرکت در فرآیند مسیریابی به نوعی باعث اختلال در فرآیند مسیریابی شده و نهایتاً امر مسیریابی را مختل کنند. یکی از معروفترین پروتکل های مسیریابی در شبکه های ویژه، پروتکل AODV [۴،۵] می باشد که در بسیاری از تحقیقات تاثیر حملات مختلف بر روی آن بررسی شده است. پروتکل مسیریابی بردار فاصله بنا به تقاضا (AODV) برای استفاده توسط گره های موبایل در یک شبکه AdHoc، طراحی شده است. در شبکه AdHoc، این پروتکل سازگاری سریعی با شرایط لینک های پویا، سربار حافظه، استفاده پایین از شبکه و مشخص کردن مسیره های Unicast به مقصدها دارد. این پروتکل به منظور تضمین عدم وجود حلقه (که در پروتکل های بردار فاصله کلاسیک وجود داشت)، شماره ترتیب مقصد را مورد استفاده قرار می دهد. AODV با استفاده از یک چرخه پرس و جوی درخواست مسیر و پاسخ مسیر، مسیرها را می سازد. وقتی که گرد مبدأ درخواست مسیری به مقصدی را می کند، گردابی که در حال حاضر مسیری به مقصد ندارد، پسته درخواست مسیر را به صورت broadcast به سراسر شبکه ارسال می کند. گردهایی که این بسته را دریافت می کنند، اطلاعاتشان را بنا به اطلاعات گره مبدأ، بروز کرده و یک مدخل مسیر معکوس را برای مبدأ در جداول مسیر خود ایجاد می کنند. همچنین اگر گرد، مسیری به مقصد داشته باشد به گرد مبدأ اطلاع می دهد که داده های خود را می تواند از طریق این گره به مقصد بفرستد، در غیر این صورت گرد، درخواست را در شبکه پخش می کند. یکی از مهمترین حملات در AdHoc حمله سیاه چاله [۶،۷،۸] میباشد. این حمله از طریق یکی از گردهای موجود در شبکه اعمال می- شود به این نحو که این گردها با پاسخ دادن به هر درخواست مسیر بدون توجه کردن به جدول مسیر یابی خود و بدون توجه به اینکه آیا این گره اصلاً مسیری به گره مقصد دارد یا خیر، باعث می شود گردهای دیگر این گره را بعنوان مسیر مناسب و کوتاه برای ارسال بسته ها بدانند و بسته های خود را از مسیر این گره ارسال کنند که در این صورت یک سیاهچاله ایجاد شده است و گردای هم که بعنوان سیاهچاله شناخته می شود بجای ارسال بسته ها به مقصد اقدام به دریافت اطلاعات آنها و یا دور انداختن آنها می کند. در صورتی که گره سیاهچاله خود را بعنوان مسیر مناسب برای کلیه گره های شبکه معرفی کند در این صورت این امر سبب از دست رفتن کلیه بسته های شبکه خواهد شد، که در نهایت باعث بوجود آمدن عدم پذیرش

سرویس (Denial of Service) خواهد شد. برای همین در این مقاله روشی برای حل این مشکل ارائه شده است. این روش با توجه به رفتار گردها در شبکه تصمیم می‌گیرد که گره مورد نظر خرابکار است یا خیر.

۲- الگوریتم مسیریابی AODV

پروتکل مسیریابی بردار فاصله بنا به تقاضا برای استفاده توسط گردهای موبایل در یک شبکه Ad Hoc، طراحی شده است [۹،۱۰]. در شبکه Ad Hoc این پروتکل سازگاری سریعی با شرایط لینکهای پویا، سردار حافظه، استفاده پایین از شبکه و مشخص کردن مسیرهای Unicast به مقصد ها دارد. این پروتکل به منظور تضمین عدم وجود حلقه، شماره ترتیب مقصد را مورد استفاده قرار می‌دهد.

الگوریتم AODV قابلیت‌های پویا بودن، خود آغازی، مسیریابی Multi Hop را برای گردهای موبایلی که می‌خواهند در ایجاد یک شبکه Ad Hoc شرکت نمایند، فراهم می‌نماید. AODV قادر به مسیریابی unicast و multicast می‌باشد. این پروتکل، الگوریتمی است که بنا به تقاضا کار می‌کند، به این معنی که مسیر بین گردها را تنها در صورتی که توسط گره منبع درخواست شده باشد، می‌سازد. این الگوریتم مسیرها را تنها تا زمانی که توسط منبع مورد نیاز است حفظ می‌کند.

AODV برای تضمین تازگی مسیرها از شماره ترتیب استفاده می‌کند، از خصیصه‌های دیگر این پروتکل که قابل ذکر است این است که این پروتکل مسیرهای بدون دور ایجاد کرده، خود آغاز بوده و برای مقیاس‌های بزرگ شبکه که از تعداد زیادی گره موبایل تشکیل شده است، هم پاسخگوست AODV با استفاده از یک چرخه پرس و جوی درخواست مسیر و پاسخ مسیر، مسیرها را می‌سازد. وقتی که گره مبدأ درخواست مسیری به مقصدی را می‌کند، گرهایی که در حال حاضر مسیری به مقصد ندارد، بسته درخواست مسیر را به صورت broadcast به سراسر شبکه ارسال می‌کند [۱۱]. گردهایی که این بسته را دریافت می‌کنند، اطلاعات شان را بنا به اطلاعات گره مبدأ، بروز کرده و یک مدخل مسیر معکوس را برای مبدأ در جداول مسیر خود ایجاد می‌کنند.

گرد دریافت کننده RREQ، در صورتیکه خودش گره مقصد باشد و یا مسیری به مقصد با شماره ترتیب بزرگتر یا مساوی شماره ترتیب RREQ داشته باشد، پاسخ RREQ را ارسال خواهد کرد. اگر یکی از دو حالت فوق رخ دهد، گره دریافت کننده RREQ، یک RREP در جهت معکوس برای گرد منبع بصورت unicast ارسال خواهد کرد در غیر اینصورت، گره دریافت کننده مجدداً RREQ را بصورت broadcast ارسال می‌کند.

گردها در RREQ، آدرس IP گرد مبدأ و شناسه broadcast را نگه می‌دارند. اگر گره‌هایی RREQ را دریافت کنند که قبلاً بسته درخواست مسیر را دریافت کرده اند، آنها RREQ را به دور انداخته و آن را هدایت نخواهند کرد.

اگر بعداً منبع، RREP‌ی که شامل یک شماره ترتیب بزرگتر است یا شماره ترتیب یکسان با تعداد hop count کوچکتر را دریافت کند، اطلاعات مسیریابی مربوط به مقصد را بروز کرده و مسیر بهتر را مورد استفاده قرار می‌دهد. تا زمانیکه مسیر، فعال باقی بماند، تداوم مسیر حفظ می‌شود.

الگوریتم AODV به گردهای بسیار اجازه می‌دهد که مسیریابی برای مقصدهای جدید را به سرعت انجام دهند و نیازی ندارد که گرد - ها، مسیرهای به مقصد را که در ارتباط فعال نیستند، نگه دارند. وقتی که لینکها قطع می‌شوند، AODV به مجموعه گردهایی که مسیر را تشکیل می‌دهند، خبر از دست رفتن لینک را می‌دهد و آنها را از شکستن لینک آگاه می‌کند تا گردها بتوانند با استفاده از لینک از دست رفته مسیر را باطل کنند.

از مشخصات متمایز AODV استفاده از یک شماره ترتیب به مقصد به ازای مدخل هر مسیر است. با استفاده از شماره ترتیب، مقصد، از عدم وجود دور مطمئن شده و برای برنامه نویسی هم آسان خواهد شد. فرض کنید که در مسیر به مقصد درخواستی وجود دارد؛ در اینصورت مسیری که بیشترین شماره ترتیب را دارد، انتخاب میشود.

کشف مسیر در AODV بنا به تقاضا انجام می‌شود و چرخه درخواست مسیر و پاسخ مسیر به دنبال هم انجام می‌شود. هنگامیکه یک مسیر بین دو گره مورد نیاز شود، گرد آغاز گر، یک درخواست مسیر را در سرتاسر شبکه بصورت broadcast ارسال می‌کند. گردهایی که این RREQ را دریافت می‌کنند، اطلاعات خودشان را در مورد گره آغاز گر با تنظیم کردن نقاط برگشت به گرد آغازگر، در جداول مسیر بروز می‌کنند.

RREQ شامل شماره ترتیب اخیر متعهد است که گرد آغازگر از آن با اطلاع است. گرهایی که پیغام RREQ را دریافت

می‌کند، در دو حالت زیر RREP را ارسال می‌کند:

۱- این گرد، گره مقصد باشد.

۲- گره، مسیری تازه داشته باشد (شماره ترتیبی بزرگتر یا مساوی با شماره ترتیبی که RREQ را در بر گرفته است).

در غیر اینصورت گرد مجدداً RREQ را بصورت broadcast ارسال می‌کند. همه گردها در RREQ گرهایی را که پیش از این دیده شده - اند، نگه می‌دارند (آدرس IP گره آغازگر و شناسه مربوط به RREQ را نگه می‌دارد). اگر RREQ یکسانی دوباره دریافت شود، بدون سر و صدا دور انداخته می‌شود. یک مسیر هدایتی برای ارسال بسته‌های داده از گره آغازین، عملکرد کشف مسیر برای مقصد خواسته شده را تنظیم می‌کند. مسیرها تنها تا زمانیکه فعال باشند حفظ می‌شوند تا زمانیکه ترافیک داده‌ای به مقصد به اندازه کافی وجود داشته باشد. زمانیکه ترافیک به مقصد متوقف شود، مهلت مسیر تمام می‌شود و سرانجام از جدول مسیر حذف می‌شود، اگر قطع شدن یک اتصال در حالیکه مسیر فعال است اتفاق بیافتد، یک پیغام خطای مسیر RERR توسط گردانی که نزدیک گره آغازگر است ارسال می‌شود. پیغام RERR اطلاعاتی در مورد مقصدهایی که در حاضر غیر قابل رسیدن هستند، را در بر دارد. اگر گره آغازگر مجدداً تقاضای ارسال دادن به مقصد را داشته باشد، می‌تواند کشف مجدد مسیر را از دوباره آغاز نماید.

۳- حمله سیاهچاله و انواع آن

حمله سیاهچاله به دو دسته تقسیم می‌شود. حمله سیاهچاله تکی و حمله سیاهچاله گروهی یا جمعی. حمله سیاهچاله تکی از طریق یکی از گردهای موجود در شبکه اعمال می‌شود به این نحو که این گره بدون توجه به جدول مسیریابی خود و به اینک آیا اصلاً مسیری به گره مقصد دارد یا خیر، به RREQ دریافتی، RREP مساعد ارسال می‌کند، که این امر باعث کوتاه شدن ارسال بسته‌های RREP نسبت به گرد-های دیگر می‌شود در نتیجه گردهای دیگر این گره را بعنوان مسیر مناسب و کوتاه برای ارسال بسته‌ها دانسته و بسته‌های خود را از مسیر این گره ارسال می‌کنند، در این صورت یک سیاهچاله ایجاد شده است و گردای هم که بعنوان سیاهچاله شناخته می‌شود به جای ارسال بسته - ها به مقصد، اقدام به دریافت اطلاعات آنها و یا دور انداختن آنها می‌کند. اگر گرد سیاهچاله خود را بعنوان مسیر مناسب برای کلیه گردهای شبکه معرفی کند، در این صورت سبب از دست رفتن کلیه بسته‌های شبکه خواهد شد که در نهایت باعث بوجود آمدن Denial Of Service خواهد شد [۹،۱۰،۱۲]. نوع دیگر حمله سیاهچاله، حمله سیاهچاله گروهی یا جمعی است که در آن بیش از یک گرد سیاهچاله وجود دارد که این گردها با هم همکاری دارند [۱۱،۱۶،۱۷]

تحقیقات انجام شده

در [۱۲] راه حلی برای سیاهچاله تکی پیشنهاد داده است. در این روش، اطلاعات گام بعدی به مقصد، باید وقتی که هر گرد میانی به RREQ پاسخ می‌دهد، ضمیمه بسته RREP شود، سپس گرد مبداء یک درخواست مجدد (FREQ) به گام بعدی گرد پاسخگو می‌فرستد و درباره گرد پاسخگو و مسیر به مقصد می‌پرسد. با استفاده از این روش می‌توان قابلیت اعتماد گره پاسخگو را تنها اگر گام بعدی قابل اعتماد باشد، شناسایی کرد. این راه حل نمی‌تواند از حمله سیاهچاله جمعی در MANET ها پیشگیری کند. برای مثال اگر گام بعدی نیز با گرد پاسخگو همکاری کند، پاسخ برای FREQ برای هر سوال به سادگی بله خواهد بود در نتیجه مبداء به گام بعدی اعتماد کرده و داده‌ها را از طریق گرد پاسخگو می‌فرستد که خود یک گرد سیاهچاله است.

در [۱۳]، روش پیشنهادی نیازمند گرد واسطه‌ای است تا در خواست تایید مسیر یا CREQ را به گرده hop بعدی در جهت مقصد بفرستد. بعد از آن که، گرد hop بعدی، CREQ را دریافت کرد، حافظه مسیر خودش را برای پیدا کردن یک مسیر به مقصد جستجو می‌کند. اگر مسیری داشته باشد آنگاه پاسخ تایید مسیر یا CREQ را به همراه اطلاعات مسیر به گرد مبداء می‌فرستد. گرد مبداء با مقایسه اطلاعات CREQ تشخیص می‌دهد مسیر موجود در RREP معتبر است یا خیر. چون عملیاتی به پروتکل مسیریابی اضافه شده در نتیجه سربار این روش بالاست. در [۱۴]، گرد مبداء با پیدا کردن بیشتر از یک مسیر به

مقصد، اعتبار گردانی که RREP را شروع کرده، تایید می کند. گره مبدا صبر می کند تا بسته RREP را از پیش از دو گره دریافت کند. در شبکه های ادهاک، در مسیرهای تکراری در بیشتر اوقات تعدادی گره و hop مشترک وجود دارد. وقتی گره مبدا RREP ها را دریافت کرد، در صورتی که در مسیرها به مقصد، hop های مشترک وجود داشته باشد، گره مبدا می تواند مسیر ایمن به مقصد را تشخیص دهد. این روش باعث تاخیر مسیریابی می شود چون گرد باید منتظر بماند تا RREP را از بیش از دو گره دریافت کند. از این رو روشی که بتواند بدون افزایش سربار و تاخیر مسیریابی، از حمله سیاه چاله جلوگیری کند مورد نیاز است.

در [۱۵] وقتی گره های RREP را صادر کرد، در اطراف آن گره یک فرآیند نظر خواهی صورت می گیرد. سپس بر اساس نظرات اعلام شده توسط همسایگان گره صادر کننده RREP، در مورد خرابکار بودن گرد پاسخگو تصمیم گیری می شود. روش های فوق همگی برای حمله سیاهچاله تکی ارائه شده اند.

در [۱۱] یک روش ارائه شده است که حمله سیاهچاله جمعی را شناسایی می کند. این پروتکل نسخه اندکی تعدیل شدن، از پروتکل AODV است که با جدول اطلاعات مسیریابی داده DRI و بررسی فرسی FREQ و پاسخ مجدد (FREP) بیان می شود. هر گره یک جدول اطلاعات مسیریابی را نگهداری می کند. DRI پیگیری می کند که آیا گره با همسایگانش تبادل داده داشته است یا خیر. در این جدول مدخلی برای هر همسایه نگهداری می شود. DRI نشان می دهد که آیا گره از طریق این همسایه داده فرستاده یا خیر و آیا گره از این همسایه داده دریافت کرده است یا خیر.

در [۱۷] یک راه حل دیگر که از وقوع حمله سیاه چاله جمعی جلوگیری می کند، ارائه شده است. این راه حل توسعه یافته AODV است. این راه حل یک مسیر ایمن را که از سیاه چاله گروهی جلوگیری می کند، کشف می کند. روش فرض می کند که گره هایی که قبلا تایید شده هستند در ارتباط شرکت می کنند. در این روش برای مقابله با حملات سیاه چاله از جدول صحت استفاده می شود که در آن هر گره شرکت کننده یک درجه صحت دارد که به عنوان اندازه اطمینان آن گره محسوب می شود. اگر درجه صحت یک گرد صفر شود به این معنی است که این گرد، یک گره متخاصم است که اصطلاحا به آن سیاه چاله گفته می شود که باید دور ریخته شود.

روش پیشنهادی

در روش پیشنهادی سعی بر این است تا بتوان با توجه به رفتار گردها در شبکه در مورد خرابکار بودن یک گره تصمیم گیری کرد. شبه کد روش پیشنهادی به صورت زیر است:

۱- ثبت اطلاعات مربوط به فعالیت گردها که شامل موارد زیر می باشد:

تعداد داده های ارسالی به گره همسایه

تعداد داده های دریافتی از یک گره همسایه

تعداد پاسخ های (reply) دریافتی از یک گره همسایه

۲- ارسال بسته درخواست نظرات همسایه ها در مورد یک گره همسایه که بسته reply را ارسال کرده است.

۳- دریافت اطلاعات ثبت شده در مورد گرد فرستنده بسته reply در گردهای همسایه آن.

۴- بررسی اطلاعات دریافت و اعلام نظر در مورد خرابکار بودن گرد

۵- ارسال یک بسته خطر برای قرنطینه کردن گره خرابکار.

۶- حذف گردهای داخل قرنطینه در فرآیند مسیریابی

در روش پیشنهادی هر گره در شبکه دارای ساختمان داده های زیر می باشد:

۱- هر گره دارای یک جدول مربوط به همسایه ها و رفتارهای آنها می باشد. هر مدخل این جدول مشخص می کند که

گره همسایه با Id مشخص چند بسته داده با این گره ارسال کرده است، چند بسته reply به این گره ارسال کرده است و گرد مورد نظر به گرد همسایه چند بسته داده تحویل داد.

۲- هر گره دارای لیستی از گردهایی است که در قرنطینه می- باشند و باید این گردها را از فرآیند مسیریابی حذف کرد. گردهای خرابکار گردهایی هستند که بسته های RREQ را با ارسال بسته های RREP پاسخ می دهند و تعداد زیادی بسته داده به آن تحویل داده شده ولی حداقل داده توسط آن به گردهای همسایه ارسال شده است. زمانی که یک گره، از گره همسایه خود یک بسته RREP دریافت می کند در صورتی که گره پاسخ دهنده به RREQ، یک گره میانی باشد و گره مقصد نباشد بررسی می کند که آیا گره پاسخ دهنده از گردهایی نیست که در قرنطینه می باشند. اگر گره، یک گره خرابکار باشد بسته RREP دور ریخته می شود. در غیر این صورت فرآیند رای گیری در اطراف گره پاسخ دهنده انجام می شود تا بتوان تمام فعالیت های گره مورد نظر را بدست آورد. سپس بر اساس اطلاعات دریافتی درستی گره مورد نظر بررسی می شود و اگر گره خرابکار باشد در شبکه یک پیغام alarm پخش می شود تا گره مورد نظر در قرنطینه قرار گیرد. الگوریتم پیشنهادی بر روی پروتکل AODV پیاده سازی شدت است و برای انجام عملیات های خود از چندین بسته جدید استفاده می کند که عبارتند از:

۱- بسته درخواست اطلاعات در مورد یک گره؛ بسته شامل شناسه گره مورد سوال، شناسه فرستنده در خواست و زمان زندگی بسته می باشد.

۲- بسته اطلاعات گردهای همسایه در مورد گره مورد سوال: این بسته شامل تعداد بسته های داده دریافتی از گره مورد تفکر، تعداد بسته های ارسالی به گره مورد نظر و تعداد بسته های RREP دریافتی از گره مورد نظر می باشد.

۳- بسته اعلام خطر: این بسته شامل گردهایی است که خرابکار شناخته شده اند و باید در لیست قرنطینه گردها قرار گیرند.

بسته اعلام خطر در کل شبکه پخش می شود. مزایای روش پیشنهادی در این است که اولاً گردای فرایند نظر خواهی را شروع می کند که یک بسته reply از یک گره غیر مطمئن دریافت کرده است. یعنی اگر گره های درستی خود را قبلاً اثبات کرده است (با ارسال بسته های داده) دیگر لازم به نظر خواهی از دیگران نیست. این مورد باعث کاهش سرریار الگوریتم پیشنهادی خواهد شد. ثانیاً در زمان درخواست اطلاعات جدول گردهای همسایه نیز بروز رسانی می شوند تا سردار الگوریتم کاهش یابد. شبه کد الگوریتم پیشنهادی به صورت زیر است:

```

Node_function (packet,time)
{
  IF time is start of simulation THEN
  BEGIN
    Initialize quarantine list;
    Initialize activity table of neighbors;
    This table has following fields:
    (Node id, number of received data, number of sent data, number of sent rrep )
  END
  IF packet is data THEN
  BEGIN
    INCREMENT number of received data for sender of packet
    IF this node isn't destination THEN
    BEGIN
      GET next node which it isn't in quarantine list
      IF find next node for forwarding THEN
      BEGIN
        FORWARD packet to next node
        INCREMENT number of sent data to next node
      END
    ELSE
      SEND error packet to source
    END
  ELSE
    RECIEVE packet
  END
  IF packet is rrep THEN
  BEGIN
    INCREMENT number of received rrep for sender of packet
    IF next isn't in quarantine list THEN
    BEGIN
      IF sender of rrep has not been good node THEN
      BEGIN
        CREATE an opinion request packet broadcast to neighbors of rrep's sender
        SET a timer for process responses
        CREATE a temporary list to save responses
      END
      FORWARD packet
    ELSE
      DISCARD packet
    END
  END
  IF packet is opinion request THEN
  BEGIN
    CHECK if this node has any opinion about requested node
    IF this node have any opinion THEN
    BEGIN
      EXTRACT activities of the requested node from activity table (including number of
      received data, number of sent data, and number of sent rrep)
      CREATE response packet including the required information
      FORWARD response packet
    END
  ELSE
    FORWARD packet
  END
  IF packet is response packet THEN
  BEGIN
    IF this node is sender of the opinion request packet THEN
    BEGIN
      EXTRACT information from packet (including number of received data, number of
      sent data, number of sent rrep)
      SAVE the extracted information in temporary list
    END
  ELSE
    FORWARD packet
  END
  IF time is timer expiration THEN
  BEGIN
    INSPECT all information in the temporary list to judge about node
    IF ((sum of sent rrep's is high) and (sum of sent data is low) and (sum of received data is high)) or high number of
    the voters announce this node as a attacker) THEN
    BEGIN
      ADD attacker to quarantine list
      REMOVE all routes to this node in routing table
      ALARM this node is a attacker
    END
  END
  IF packet is an alarm THEN
  BEGIN
    ADD attacker to quarantine list
    REMOVE all routes to this node in routing table
    ALARM this node is an attacker
    FORWARD packet
  END
}

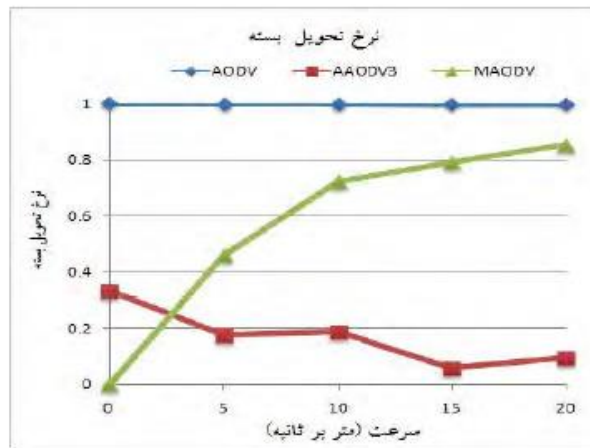
```

محیط شبیه سازی و نتایج شبیه سازی

برای شبیه سازی از نرم افزار شبیه ساز GloMosim استفاده شده است. در سناریوهای مختلف الگوریتم پیشنهادی با AODV پایه مقایسه شده است. تعداد گردهای موجود در شبکه برابر ۵۰ و تعداد گردهای خرابکار ۳ گرد در نظر گرفته شده

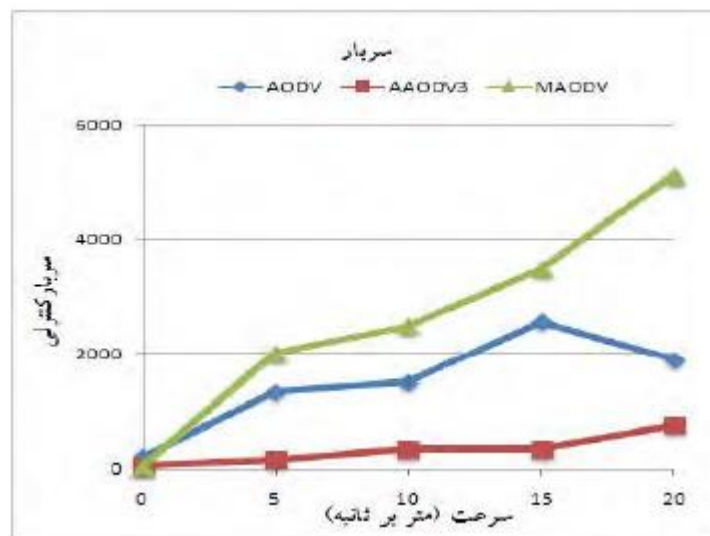
است. محیط شبیه سازی ۱۰۰۰ متر در ۱۰۰۰ متر می باشد. همچنین در این شبیه سازی ها سه جریان ترافیکی در شبکه وجود دارد که با نرخ ثابت پسته ها را به شبکه ارسال می کنند. در شکل های زیر، منظور از AODV، پروتکل AODV استاندارد و منظور از AODV3 و MAODV به ترتیب پروتکل AODV استاندارد با سه گرد خرابکار و پروتکل پیشنهادی است که توانسته است سیاه چاله های جمعی را شناسایی کند.

نرخ تحویل پسته در روش پیشنهادی با MAODV بسیار نزدیک به AODV می باشد. در حالی که در پروتکل AAODV3 مقدار نرخ تحویل پسته بسیار پایین است. در روش پیشنهادی به دلیل شناسایی گرد خرابکار و قرنطینه کردن آن، کارآیی این روش بسیار نزدیک به روش AODV می باشد (شکل ۱).



شکل ۱- نرخ تحویل بسته با افزایش سرعت

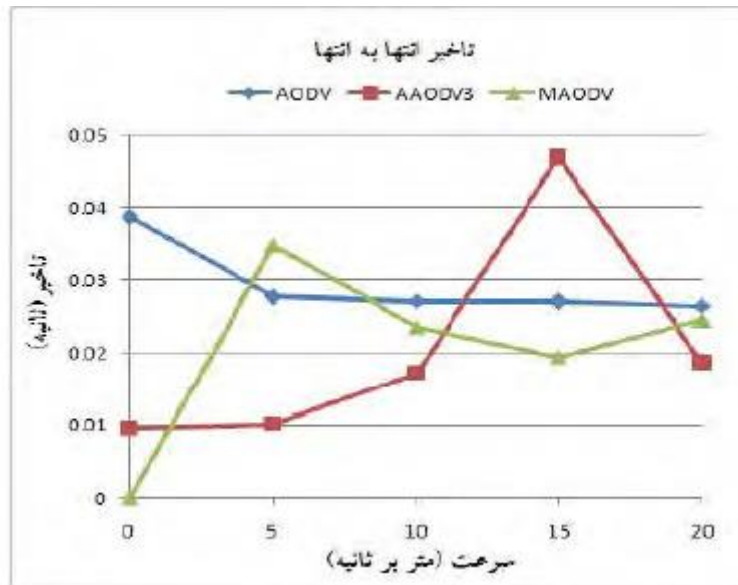
روش پیشنهادی به دلیل پخش همگانی درخواست بررسی، دارای سربار اضافی می باشد. اما به دلیل به روز رسانی جدول های مسیریابی، حجم سربار اضافی کاسته می شود. در روش AAODV1 به دلیل اینکه گره خرابکار همواره مسیریها را به منابع پیشنهاد می کند، برای همین دارای سربار کمتری است. البته باید توجه کرد که این پروتکل داده بسیار کمی را به مقصدها تحویل می دهد (شکل ۲)



شکل ۲- سربار الگوریتم

به دلیل اینکه روش AAODV3 دارای کمترین سربار است دارای کمترین تاخیر می باشد و سپس روش پیشنهادی به دلیل ارسال RREQ های سراسری کمتر، دارای کمترین تاخیر می باشد. در روش پیشنهادی در زمانی که گره ها دارای سرعت

پایین می باشند به دلیل اینکه ممکن است مسیر های بین گره ها به سختی برقرار شود و یا اصلا برقرار نشود RREQ های بیشتری ارسال شود علاوه بر این به دلیل عدم وجود اطلاعات کافی در خواست نظرات نیز به دفعات ارسال خواهد شد و این باعث افزایش تاخیر در ابتدا برای روش ما می شود (شکل ۳).



شکل ۳- تاخیر انتها به انتها

به دلیل اینکه روش پیشنهادی در ابتدا دارای تاخیر بسیار زیاد و سربرار زیاد می باشد، تعداد بسته های داده دریافتی بسیار پایین می باشد، اما به تدریج که سرعت بالاتر می رود گرد خرابکار شناسایی شده و قرنطینه می شود (شکل ۴).



شکل ۴- نرخ گذردهی

نتیجه گیری

در این مقاله روشی برای تشخیص و مقابله با حملات سیاه چاله ارائه شد که با حداقل هزینه یا سربار می‌توانست گردهای خرابکار را تشخیص و در قرنطینه قرار دهد. این روش به خاطر سادگی پیاده‌سازی و سربار پایین می‌تواند در بسیاری از شبکه‌های موردی به کار رود.

روش پیشنهادی با دقت بالایی توانایی تشخیص گردهای خرابکار را دارد. در زمانی که تعداد گردهای خرابکار پایین باشد، با هزینه بسیار اندکی می‌تواند گره خرابکار را تشخیص دهد. به علت پخش همگانی پیغام‌های درخواست نظر همسایه‌ها، سردار الگوریتم بالاست اما با به روزرسانی جدول‌های مسیریابی گردهای شبکه، می‌توان تا اندازه زیادی از سربار الگوریتم کاهش داد. از لحاظ پیاده‌سازی الگوریتم پیشنهادی دارای پیچیدگی خاصی نیست و به راحتی قابل پیاده‌سازی می‌باشد. ساختار پیغام‌های جدید معرفی شده بسیار شبیه RREQ, RREP میباشد.

منابع و مراجع

- [1] H. Deng, W. Li, and D. P. Agrawal, Routing security in ad hoc networks, IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
- [2] S. Lee, B. Han, and M. Shin, Robust routing in wireless ad hoc networks, in ICPP Workshops, pp. 73, 2002. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
- [3] S. Makki, N. Pissinou, H. Huang, The Security issues in the ad-hoc on demand distance vector routing protocol (AODV), In Proc. of the 2004 International Conference on Security and Management (SAM'04), pp.427-432 C. E. Perkins, E. M. B. Royer, and S. R. Das, Adhoc On Demand Distance Vector (AODV) routing, RFC 3561, July 2003 .
- [4] Y.C. Hu and A. Perrig, A survey of secure wireless ad hoc routing, IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.
- [5] M. A. Shurman, S. M. Yoo, and S. Park, Black hole attack in wireless ad hoc networks, in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr.2004.
- [6] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, Crossfeature analysis for detecting ad-hoc routing anomalies, in The 23rd International Conference on Distributed Computing Systems (ICDCS'03), pp. 478-487, May 2003.
- [7] Y. A. Huang and W. Lee, Attack analysis and detection for ad hoc routing protocols, in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.
- [8] Latha Tamilselvan, Dr. V Sankaranarayanan, Prevention of Co-operative Black Hole Attack in MANET, JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.
- [9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method, International Journal of Network Security, Vol.5, No.3, PP.338-346, Nov. 2007.
- [10] C. E. Perkins, E. M. B. Royer, and S. R. Das, Ad hoc On- Demand Distance Vector (AODV) routing, RFC 3561, July 2003.
- [11] Hesiri Weerasinghe, Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation, International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008.
- [12] H. Deng, W. Li, and D. P. Agrawal, Routing security in ad hoc networks, IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
- [13] S. Lee, B. Han, and M. Shin, Robust routing in wireless ad hoc networks, in ICPP Workshops, pp. 73, 2002.
- [14] M. A. Shurman, S. M. Yoo, and S. Park, Black hole attack in wireless ad hoc networks, in ACM 2nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.
- [15] Mehdi Medadian, M.H. Yektaie and A.M Rahmani, Combat with Black Hole Attack in AODV routing protocol in MANET, 2009, AH-ICI 2009. First Asian Himalayas International Conference, pp: 1-5, 3-5 Nov. 2009.
- [16] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA.
- [17] Lata Tamilselvan, Dr.V Sankaranarayanan, Prevention of Cooperative Black Hole Attack in MANET , Journal Of networks, Vol. 3, NO. 5, May 2008.