اولین کنفرانس ملی محاسبات نرم و فناوری اطلاعات
1st National Conference on Soft Computing and Information Technology
دانشگاه آزاد اسلامی واحد ماهشهر
۱۲و۱۳ اسفند ماه ۸۹

کشف و حذف حمله سیاهچاله جمعی در شبکه‌های سیار ادهاک

مهدی مدادیان [۱] – خسرو فرداد [۲] – ایمان برازنده [۳]
(۱) گروه کامپیوتر - دانشگاه آزاد اسلامی واحد بهبهان
medadian@gmail.com
(۲) گروه کامپیوتر – دانشگاه آزاد اسلامی واحد بهبهان
khossro_fardad@gmail.com
(۳) گروه کامپیوتر – دانشگاه آزاد اسلامی واحد ماهشهر
barazandeh_i@yahoo.com

خلاصه: شبکه‌های ویژه سیار، شامل مجموعه‌ای از گره‌ها می‌باشد که می‌توانند آزادانه بدون داشتن هیچ گونه زیرساخت شبکه‌ای و از طریق فرکانس‌های رادیویی با یکدیگر در ارتباط باشند. سرعت در برپایی و بدون ساختار بودن این شبکه‌ها باعث شده است که نقش بسیار مهمی را در زمینه‌های مختلف مانند کاربردهای نظامی و اضطراری، حوادث طبیعی، محیط‌های دانشگاهی و شهری ایفا کنند. مبحث امنیت در این شبکه‌ها امروزه یکی از مباحث مهم تحقیقاتی است. در این تحقیق بر روی امنیت در مسیریابی AODV تحقیق خواهد شد. آنچه در این مقاله ارائه می‌شود، بررسی حمله سیاه چاله جمعی در پروتکل مسیریابی AODV و ارائه راهکاری برای تشخیص و مقابله با آن می‌باشد.

کلمات کلیدی: شبکه‌های بی‌سیم موردی، پروتکل مسیر یابی AODV ، امنیت، حمله سیاه چاله گروهی

۱ – مقدمه

امروزه تمایل به استفاده از شبکه های بی‌سیم روز به روز در حال افزایش است؛ چون هر شخصی، هر جایی و در هر زمانی می‌تواند 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 کارتهای شبکه بی‌سیم مجهز هستند. بعلاوه، این کامپیوترهای کوچک می‌توانند چندین ساعت فقط با نیروی باتری کار کنند از اینرو کاربران آزادند براحتی آنها را به هر طرف که می‌خواهند منتقل نمایند. زمانی که کاربران شروع به استفاده از کامپیوترهای 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، ترمینال‌های فرودگاه و همچین در محیط‌های نظامی است . شبکه‌های ویژه سیار مجموعه‌ای از گره‌های بی‌سیم است که می‌توانند بصورت پویا در هر مکان و در هر زمان بدون استفاده از هر زیرساخت شبکه‌ای تشکیل شوند. اغلب این گره‌ها در آن واحد هم بعنوان مسیریاب و هم بعنوان گره عمل می‌کنند. این خاصیت سبب شده که در موارد اضطراری که امکان تشکیل شبکه‌ای با ساختار ثابت و از پیش تعریف شده وجود ندارد، مانند موارد نظامی و یا وقوع سیل و... ، بتوان از این شبکه‌ها استفاده کرد. ارتباط میان گره‌ها در این شبکه از طریق امواج رادیویی صورت می‌گیرد و در صورتی که یک گره در برد رادیویی گره دیگر باشد همسایه آن گره به حساب می‌آید و در غیر این صورت در صورت نیاز به ارتباط میان دو گره که در برد رادیویی یکدیگر نیستند می‌توان از کمک گره‌های دیگر در این مورد استفاده کرد، بنابراین ارتباط میان گره‌ها در این شبکه به نوعی بر مبنای اعتماد و مشارکت میان گره‌ها صورت می‌گیرد. مبحث امنیت در این شبکه‌ها امروزه یکی از مباحث مهم تحقیقاتی است. تحرک گره‌ها، بی‌سیم بودن ارتباطات، تغییر پویای ساختار شبکه، فقدان مدیریت متمرکز برای بررسی رفتارها و عملکردها، فقدان خطوط دفاعی مشخص و محدودیت در توان مصرفی گره‌ها، بستر مناسبی را برای حملات مختلف علیه این شبکه‌ها فراهم می‌آورد. به خاطر ساختار مسیریابی شبکه‌های ویژه سیار [1,2,3] که به نوعی بر مبنای یک جور اعتماد میان گره‌ها استوار است فرصت خوبی را برای حمله کنندگان فراهم می‌سازد تا با شرکت در فرآیند مسیریابی به نوعی باعث اخلال در فرآیند مسیریابی شده و نهایتاً امر مسیریابی را مختل کنند. یکی از معروفترین پروتکل‌های مسیریابی در شبکه‌های ویژه، پروتکل AODV [4,5] 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 گره‌های موبایل در یک شبکه AdHoc، طراحی شده است. در شبکه AdHoc، این پروتکل سازگاری سریعی با شرایط لینک‌های پویا، سربار حافظه، استفاده پایین از شبکه و مشخص کردن مسیرهای Unicast به مقصدها دارد. این پروتکل به منظور تضمین عدم وجود حلقه(که در پروتکلهای بردار فاصله کلاسیک وجود داشت) ، شماره ترتیب مقصد را مورد استفاده قرار می‌دهد. 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، گره‌ای که در حال

حاضر مسیری به مقصد ندارد ، بسته درخواست مسیر را به صورت broadcast به سراسر شبکه ارسال می‌کند. گره‌هایی که این بسته را دریافت می‌کنند، اطلاعاتشان را بنا به اطلاعات گره مبدأ، بروز کرده و یک مدخل مسیر معکوس را برای مبدأ در جداول مسیر خود ایجاد می‌کنند. همچنین اگر گره، مسیری به مقصد داشته باشد به گره مبدا اطلاع می‌دهد که داده‌های خود را می‌تواند از طریق این گره به مقصد بفرستد. در غیر این صورت گره، درخواست را در شبکه پخش می‌کند. یکی از مهمترین حملات در AdHoc حمله سیاه چاله [6,7,8] می‌باشد. این حمله از طریق یکی از گره‌های موجود در شبکه اعمال می‌شود به این نحو که این گره‌ها با پاسخ دادن به هر درخواست مسیر بدون توجه کردن به جدول مسیریابی خود و بدون توجه به اینکه آیا این گره اصلاً مسیری به گره مقصد دارد یا خیر، باعث می‌شود گره‌های دیگر این گره را بعنوان مسیر مناسب و کوتاه برای ارسال بسته‌ها بدانند و بسته‌های خود را از مسیر این گره ارسال کنند که در این صورت یک سیاهچاله ایجاد شده است و گره‌ای هم که بعنوان سیاهچاله شناخته می شود بجای ارسال بسته‌ها به مقصد اقدام به دریافت اطلاعات آنها و یا دور انداختن آنها می‌کند. در صورتی که گره سیاهچاله خود را بعنوان مسیر مناسب برای کلیه گره‌های شبکه معرفی کند در این صورت این امر سبب از دست رفتن کلیه بسته‌های 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 گره‌ها 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 گره‌های موبایل در یک شبکه Ad Hoc، طراحی شده است[9,10]. در شبکه Ad Hoc، این پروتکل سازگاری سریعی با شرایط لینک‌های پویا، سربار حافظه، استفاده پایین از شبکه و مشخص کردن مسیرهای Unicast به مقصدها 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 گره‌های 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 گره‌ها 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 پرس‌وجوی 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[11]. گره‌هایی که این بسته را دریافت می‌کنند، اطلاعات‌شان را بنا به اطلاعات گره مبدأ، بروز کرده و یک مدخل مسیر معکوس را برای مبدأ در جداول مسیر خود ایجاد می‌کنند.

گره دریافت‌کننده 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 درجهت معکوس برای گره منبع بصورت unicast ارسال خواهد کرد؛ درغیر اینصورت، گره دریافت کننده مجدداً RREQ را بصورت broadcast ارسال می‌کند.

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

اگر بعداً منبع، RREPای 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 گره‌های سیار اجازه می‌دهد که مسیریابی برای مقصدهای جدید را به سرعت انجام دهند و نیازی ندارد که گره‌ها، مسیرهای به مقصد را که در ارتباط فعال نیستند، نگه دارند. وقتی که لینکها قطع می‌شوند، AODV به مجموعه گره‌هایی که مسیر را تشکیل می‌دهند، خبر ازدست رفتن لینک را می‌دهد و آنها را از شکستن لینک آگاه می‌کند تا گره‌ها 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 دو مسیر به مقصد درخواستی وجود دارد؛ دراینصورت مسیری که بیشترین شماره ترتیب را دارد، انتخاب می‌شود.

کشف مسیر درAODV 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، گره آغازگر، یک درخواست مسیر را در سرتاسر شبکه بصورت broadcast ارسال می‌کند. گره‌هایی که این RREQ را دریافت می‌کنند، اطلاعات خودشان را در مورد گره آغازگر با تنظیم کردن نقاط برگشت به گره آغازگر، در جداول مسیر بروز می‌کنند .

RREQ شامل شماره ترتیب اخیر مقصد است که گره آغازگر از

آن با اطلاع است. گره‌ایی که پیغام RREQ را دریافت می‌کند، در دو حالت زیر RREP را ارسال می‌کند:

۱- این گره، گره مقصد باشد .

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

در غیر اینصورت گره مجدداً RREQ را بصورت broadcast ارسال می‌کند. همه گره‌ها در RREQ گره‌هایی را که پیش از این دیده شده‌اند، 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 درحالیکه مسیر فعال است اتفاق بیافتد، یک پیغام خطای مسیر RERR توسط گره‌ایی که نزدیک گره آغازگر است ارسال می‌شود. پیغام RERR اطلاعاتی در مورد مقصدهایی که در حاضر غیر قابل رسیدن هستند، را دربر دارد. اگر گره آغازگر مجدداً تقاضای ارسال داده 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 گره‌های موجود در شبکه اعمال می‌شود به این نحو که این گره بدون توجه به جدول مسیریابی خود و به اینکه آیا اصلاً مسیری به گره مقصد دارد یا خیر، به RREQ دریافتی، RREP مساعد ارسال می‌کند، که این امر باعث کوتاه شدن ارسال بسته های RREP نسبت به گره‌های دیگر می‌شود درنتیجه گره‌های 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 گره‌ای هم که بعنوان سیاه‌چاله شناخته می‌شود به‌جای ارسال بسته‌ها به مقصد، اقدام به دریافت اطلاعات آن‌ها و یا دور انداختن آنها می‌کند. اگر گره سیاه‌چاله خود را بعنوان مسیر مناسب برای کلیه گره‌های 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[9,10,12]. نوع دیگر حمله سیاهچاله، حمله سیاهچاله گروهی یا جمعی است که در آن بیش از یک گره سیاهچاله وجود دارد که این گره‌ها با هم همکاری دارند[11,16,17].

۴ – تحقیقات انجام شده

در [12] راه‌حلی برای سیاه‌چاله تکی پیشنهاد داده است. در این روش، اطلاعات گام[۱] بعدی به مقصد، باید وقتی که هر گره میانی به RREQ پاسخ می‌دهد، ضمیمه بسته RREP شود، سپس گره مبداء یک درخواست مجدد[۲] (FREQ) به گام بعدی گره پاسخگو می‌فرستد و درباره گره 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 راه‌حل نمی‌تواند از حمله سیاه‌چاله جمعی در MANETها پیشگیری کند. برای مثال اگر گام بعدی نیز با گره 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 گره پاسخگو می‌فرستد که خود یک گره سیاه‌چاله است. در [13]، روش پیشنهادی نیازمند گره واسطه‌ای است تا درخواست تایید مسیر یا CREQ[۳] را به گره hop بعدی در جهت مقصد بفرستد. بعد از آن که، گره 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 CREP[۴] را به همراه اطلاعات مسیر به گره مبداء می‌فرستد. گره مبداء با مقایسه اطلاعات CREP تشخیص می‌دهد مسیر موجود در RREP معتبر است یا خیر. چون عملیاتی به پروتکل مسیریابی اضافه شده در نتیجه سربار این روش بالاست. در [14]، گره مبداء با پیدا کردن بیشتر از یک مسیر به مقصد، اعتبار گره‌ای که RREP را شروع کرده، تایید می‌کند. گره مبداء صبر می‌کند تا بسته RREP را از بیش از دو گره دریافت کند. در شبکه‌های ادهاک، در مسیرهای تکراری در بیشتر اوقات تعدای گره و hop مشترک وجود دارد. وقتی گره مبداء RREPها را دریافت کرد، در صورتی که در مسیرها به مقصد، hopهای مشترک وجود داشته باشد، گره مبداء می‌تواند مسیر ایمن به مقصد را تشخیص دهد. این روش باعث تاخیر مسیریابی می‌شود چون گره باید منتظر بماند تا RREP را از بیش از دو گره دریافت کند. از این‌رو روشی که بتواند بدون افزایش سربار و تاخیر مسیریابی، از حمله سیاه‌چاله جلوگیری کند موردنیاز است. در [15] وقتی گره‌ای RREP را صادر کرد، در اطراف آن گره یک فرآیند نظرخواهی صورت می‌گیرد. سپس بر اساس نظرات اعلام شده توسط همسایگان گره صادر کننده RREP ، در مورد خرابکار بودن گره پاسخگو تصمیم گیری می‌شود. روش‌های فوق همگی برای حمله سیاهچاله تکی ارائه شده‌اند. در [11] یک روش ارائه شده است که حمله سیاهچاله جمعی را شناسایی می‌کند. این پروتکل نسخه اندکی تعدیل شده، از پروتکل AODV است که با جدول اطلاعات مسیریابی داده DRI و بررسی FREQ و پاسخ مجدد (FREP) بیان می‌شود.

هر گره یک جدول اطلاعات مسیریابی را نگهداری می‌کند. DRI پیگیری می‌کند که آیا گره با همسایگانش تبادل داده داشته است یا خیر. در این جدول مدخلی برای هر همسایه نگهداری می‌شود. DRI

---

[۱] Hop
[۲] Further Request
[۳] Rote Confirmation Request
[۴] Rote Confirmation Reply

نشان می‌دهد که آیا گره از طریق این همسایه داده فرستاده یـا خیـر و آیا گره از این همسایه داده دریافت کرده است یـا خیـر. در [17] یـک راه‌حل دیگر که از وقوع حمله سیاه‌چاله جمعی جلوگیری می‌کند، ارائه شده است. این راه‌حل توسعه‌یافتـه AODV اسـت. ایـن راه‌حـل یـک مسیر ایمن را که از سیاه‌چاله گروهی جلوگیری می‌کند، کشف می‌کند. روش فرض می‌کند که گره‌هایی که قبلا تایید شده هسـتند در ارتبـاط شرکت می‌کنند. در این روش برای مقابله با حملات سیاه‌چاله از جدول صحت استفاده می‌شود که در آن هر گره شـرکت کننـده یـک درجـه صحت دارد که به عنوان اندازه اطمینان آن گره محسوب می‌شود. اگـر درجه صحت یک گره صفر شود به این معنی است که ایـن گـره، یـک گره متخاصم است که اصطلاحا به آن سیاه‌چاله گفته می‌شود که بایـد دور ریخته شود.

۵ – روش پیشنهادی

در روش پیشنهادی سعی بر این است تا بتوان با توجه به رفتار گره‌ها 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 گره‌ها که شامل موارد زیر می‌باشد:

- تعداد داده های ارسالی به گره همسایه
- تعداد داده های دریافتی از یک گره همسایه
- تعداد پاسخ‌های (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 گره فرستنده بسته reply در گره‌های همسایه آن.

۴- بررسی اطلاعات دریافتی و اعلام نظر در مورد خرابکار بودن گره.

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

۶- حذف گره‌های داخل قرنطینه در فرآیند مسیریابی

در روش پیشنهادی هر گره در شبکه دارای ساختمان داده‌های زیر می‌باشد:

۱- هر گره دارای یک جدول مربوط به همسایه‌ها و رفتارهای آنها می باشد. هر مدخل این جدول مشخص می‌کند 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 گره مورد نظر به گره همسایه چند بسته داده تحویل داده است.

۲- هر گره دارای لیستی از گره‌هایی است که در قرنطینه می‌باشند و باید این گره‌ها را از فرآیند مسیریابی حذف کرد.

گره‌های خرابکار گره‌هایی هستند که بسته‌های RREQ را با ارسال بسته‌های RREP پاسخ می‌دهند و تعداد زیادی بسته داده به آن تحویل داده شده ولی حداقل داده توسط آن به گره‌های همسایه ارسال شده است. زمانی که یک گره، از گره همسایه خود یک بسته RREP دریافت می‌کند در صورتی که گره پاسخ دهنده به RREQ ، یک گره میانی باشد و گره مقصد نباشد بررسی می‌کند که آیا گره پاسخ دهنده از گره‌هایی نیست که در قرنطینه می باشند. اگر گره، یک گره خرابکار باشد بسته RREP دور ریخته می‌شود. در غیر این صورت فرآیند رای گیری در اطراف گره پاسخ دهنده انجام می‌شود تا بتوان تمام فعالیت‌های گره مورد نظر را بدست آورد. سپس بر اساس اطلاعات دریافتی درستی گره مورد نظر بررسی می‌شود و اگر گره خرابکار باشد در شبکه یک پیغام alarm پخش می‌شود تا گره مورد نظر در قرنطینه قرار گیرد.

الگوریتم پیشنهادی بر روی پروتکل AODV پیاده سازی شده است و برای انجام عملیات های خود از چندین بسته جدید استفاده می‌کند که عبارتند از:

۱- بسته درخواست اطلاعات در مورد یک گره: بسته شامل شناسه گره مورد سوال، شناسه فرستنده درخواست و زمان زندگی[۵] بسته می‌باشد.

۲- بسته اطلاعات گره‌های همسایه در مورد گره مورد سوال: این بسته شامل تعداد بسته‌های داده دریافتی ازگره مورد نظر، تعداد بسته‌های ارسالی به گره مورد نظر و تعداد بسته‌های RREP دریافتی از گره مورد نظر می‌باشد.

۳- بسته اعلام خطر: این بسته شامل گره‌هایی است که خرابکار شناخته شده‌اند و باید در لیست قرنطینه گره‌ها قرار گیرند. بسته اعلام خطر در کل شبکه پخش می‌شود.

مزایای روش پیشنهادی در این است که اولاً گره‌ای فرایند نظرخواهی را شروع می‌کند که یک بسته reply از یک گره غیر مطمئن دریافت کرده است. یعنی اگر گره‌ای درستی خود را قبلاً اثبات کرده است(با ارسال بسته‌های داده) دیگر لازم به نظرخواهی از دیگران نیست. این مورد باعث کاهش سربار الگوریتم پیشنهادی خواهد شد. ثانیاً در زمان درخواست اطلاعات جدول گره‌های همسایه نیز بروز رسانی می‌شوند تا سربار الگوریتم کاهش یابد. شبه کد الگوریتم پیشنهادی به صورت زیر است:

---

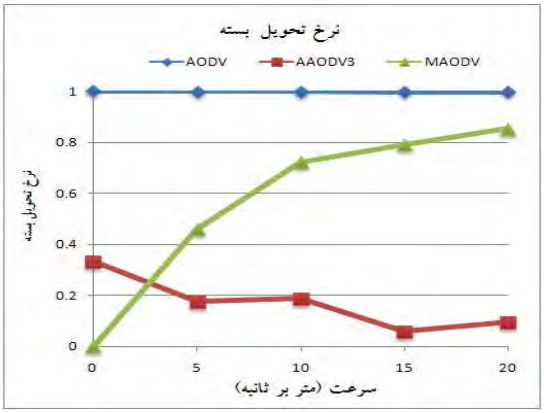
[۵] Time to live

```
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
                                                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
                                        FORWARD packet
                                END
                        ELSE
                                DISCARD packet
                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

    }
```

۶ – محیط شبیه سازی و نتایج شبیه سازی

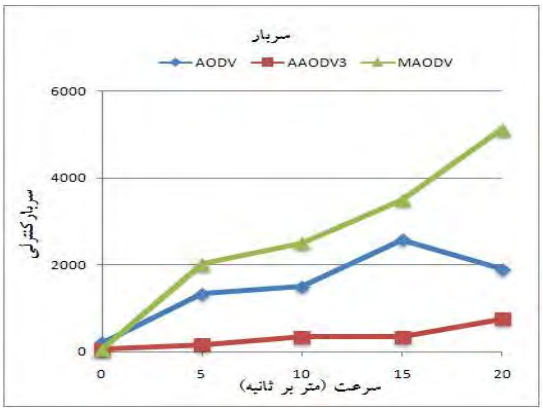
برای شبیه سازی از نرم افزار شبیه ساز GloMosim استفاده شده است. در سناریوهای مختلف الگوریتم پیشنهادی با AODVپایه مقایسه شده است. تعداد گره‌های موجود در شبکه برابر ۵۰ و تعداد گره‌های خرابکار ۳ گره در نظر گرفته شده است. محیط شبیه سازی ۱۰۰۰ متر در ۱۰۰۰ متر می باشد. همچنین در این شبیه سازی‌ها سه جریان ترافیکی در شبکه وجود دارد که با نرخ ثابت بسته‌ها را به شبکه ارسال می‌کنند. در شکل‌های زیر، منظور از AODV، پروتکل AODV استاندارد و منظور از AODV3 و MAODV به ترتیب پروتکل AODV استاندارد با سه گره خرابکار و پروتکل پیشنهادی است که توانسته است سیاهچاله‌های جمعی را شناسایی کند.

نرخ تحویل بسته در روش پیشنهادی یا MAODV بسیار نزدیک به AODV می باشد. در حالی که در پروتکل AAODV3 مقدار نرخ تحویل بسته بسیار پائین است. در روش پیشنهادی به دلیل شناسایی گره خرابکار و قرنطینه کردن آن، کارآئی این روش بسیار نزدیک به روش AODV می باشد (شکل ۱).



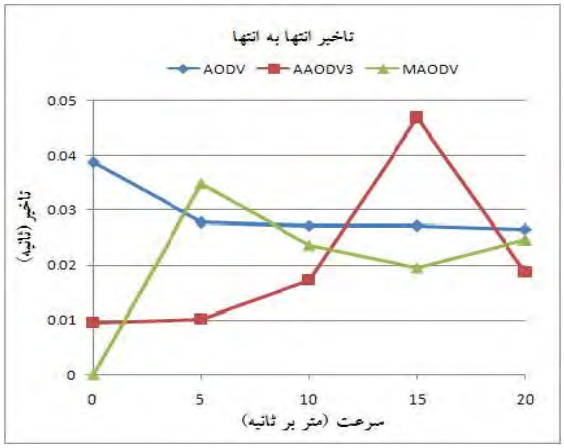
شکل ۱- نرخ تحویل بسته با افزایش سرعت

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 مسیرها 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).



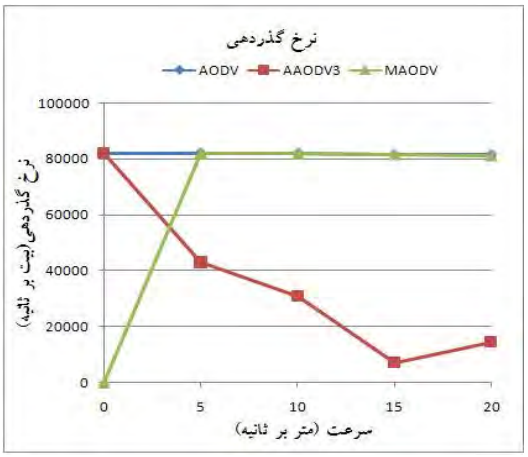
شکل ۲- سربار الگوریتم

به دلیل اینکه روشAAODV3 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 مسیرهای 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 درخواست 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 سربار زیاد می باشد، تعداد بسته های داده دریافتی بسیار پایین می باشد. اما به تدریج که سرعت بالاتر می رود گره خرابکار شناسایی شده و قرنطینه می شود(شکل ۴).



شکل ۴- نرخ گذردهی

۷- نتیجه گیری

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

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

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, *Cross-feature analysis for detecting ad-hoc routing anoma-lies*, 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.