ارا ئه راه حلی برای جلوگیری از حمله سیاه چاله در شبکه های متحرک اقتضایی درپروتکلADOV

ستار مرادی[1]، محمدرضا حسنی آهنگر[2]

[1]دانشجوی کارشناسی ارشد شبکه های کامپیوتری دانشگاه جامع امام حسین(ع)، smoradi@ihu.ac.ir

[2]دانشیار گروه مهندسی کامپیوتر دانشگاه جامع امام حسین(ع)، mrhassani@iust.ac.ir

چکیده

شبکه های متحرک اقتضایی به‌دلیل اینکه روزبه‌روز کاربرد بیشتری در زندگی بشر پیدا می‌کنند از اهمیت بسیار بالایی برخوردار هستند و مسئله امنیت در این شبکه ها بسیار مهم و چالش برانگیز است. حمله سیاه چاله یکی از تهدیدات جدی شبکه های متحرک اقتضایی است که یک گره بداندیش با معرفی کردن خود به عنوان مقصد یا نزدیک ترین گره تا مقصد از اطلاعات سوءاستفاده کرده یا اطلاعات‌را از بین می برد. در این مقاله تعدادی از راه حل های موجود مورد بررسی قرار گرفت. سپس راه حلی ارائه شده است که مشکلات روش های پیشین را برطرف کرده است. این روش محدود به تعداد حمله های گره های بد اندیش نیست و هر تعداد حمله را پاسخگو است و اثر آنها را خنثی میسازد. همچنین مهم نیست که گره بداندیش در کجای شبکه قرار دارد. در این روش فقط درستی مقصد اعتبارسنجی نمی شود بلکه احراز هویت برای طرفین رابطه برقرار می شود این امر با عث صرفه جویی در انرژی و زمان و بالا رفتن قابلیت دسترس پذیری شبکه می‌شود.

واژه‌های کلیدی

شبکه های متحرک اقتضایی، حمله سیاه چاله، شبکه های حسگر بی سیم، امنیت در شبکه های اقتضایی ،MANET، شبکه های Ad Hoc متحرک.

۱- مقدمه

شبکه های متحرک اقتضایی(MANET) [1] عبارت است از یک شبکه بدون زیرساخت ثابت. این شبکه ها از تعدادی گره متحرک که به صورت بیسیم به یکدیگر متصل هستند تشکیل شده اند نود هایی که در بازه فرکانسی یکدیگر قرار دارند می‌توانند با یکدیگر ارتباط برقرار کنند و هر نود برای دیگر نودها به عنوان یک نود انتهایی و یا یک مسیریاب عمل می‌کند و به طور کاملاً پویا شبکه را بدون هیچ گونه مدیریت مرکزی تشکیل می دهند. در این شبکه‌ها به علت اینکه قابلیت جابجایی و تحرک وجود دارد و مزایایی چون سرعت بالا، هزینه کم در برپایی و همچنین کاربرد در مناطق خطر ناک این شبکه ها را از سایر شبکه ها متمایز میکند. یکی ازمعروفترین پروتکلهای مسیریابی درMANET پروتکل(AODV)[2] است که با این فرض طراحی شده است که تمامی گره ها باصداقت کار خود را انجام می دهند یا میتوان گفت ارتباط براساس اعتماد است بنابراین ویژگیهای امنیتی در آن لحاظ نشده است. در نتیجه این پروتکل در مقابل حمله ها و سوء رفتارهایی که شبکه را تهدید میکند، آسیب پذیر است. در این مورد پژوهش هایی انجام شده است که می توان آنها را به دو دسته پژوهش های تشخیص حمله و پژوهش های مقابله با حمله تقسیم کرد که ما در این پژوهش قصد داریم روشی را جهت تشخیص و مقابله با حمله سیاه چاله ارائه کنیم.

شبکه های متحرک اقتضایی به دلیل نداشتن زیرساختی جهت مدیریت وکنترل انتقالها (access point) باعث می‌شود ارتباط بین دو گره مجاور که در محدوده یکدیگر هستند برقرار شود. همچنین به دلیل اینکه هیچگونه تسهیلاتی مربوط به مجوز در این شبکه ها وجود ندارد و همچنین محدود بودن منابع و تغییرات زیاد توپولوژی لذا ارتباطات براساس اعتماد بین طرفین شکل می گرد. همین جریان باعث به وجود آمدن مشکلاتی می شود که یکی از آنها حمله سیاه چاله است که ما روشی را برای حل آن ارائه می کنیم و این روش را با روشهای موجود مقایسه کرده و نتیجه گیری می‌کنیم.

۲- روش کار الگوریتم AODV

پروتکل مسیریابیAODV که ما انتخاب کردیم یک پروتکل مسیریابی On-Demand است که در آن همه مسیرها فقط وقتیکه مورد

[1] **Mobile Ad Hoc Network**

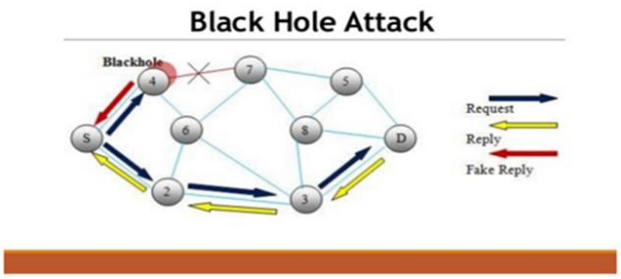
[2] **Ad hoc On-Demand Distance Vector**

نیاز باشند کشف می شوند و تنها در طول مدتی که مورد استفاده قرار می گیرند نگهداری می شوند. مسیرها در طول یک جریان کشف می شوند که در طی آن نودهای شبکه در فرآیند جستجوی یک مسیر به سمت مقصد مورد سوال قرار می گیرند. وقتی یک نود با یک مسیر به مقصد کشف می شود آن مسیر به عقب و به نود مبدائی که درخواست مسیر کرده بود گزارش می شود. AODV در هر نود شماره های ترتیبی را برای جلوگیری از حلقه های مسیریابی بکار می برد.

در فرآیند کشف مسیر وقتی یک نود مبدأ نیاز به یک مسیر به یک نود مقصد داشته باشد و مسیر معتبری در جدول مسیریابی نباشد، نود مبدأ یک بسته درخواست مسیر Route Request را به سمت نود مقصد همه پخشی می کند.وقتی هر نود RREQرا دریافت می کند، یک ورودی مسیر برعکس به سمت نود مبدأ را در جدول مسیریابی ایجاد یا بروزرسانی می کند و اگر یک مسیر معتبر در جدول مسیریابی به سمت نود مقصد، ندارد RREQ را دوباره همه پخشی می کند . وقتی دریک جریان بسته RREQ از نود مبدأ به نود مقصد برسد، نود مقصد ورودی مسیر برعکس را ایجاد یا بروزرسانی می کند و یک بسته پاسخ مسیر RouteReplyراکه یک شماره ترتیب افزایش یافته دارد در مسیر برعکس تک پخشی می کند . وقتی RREP در طول مسیر برعکس به نود مبدأ می رسد، یک مسیر رو به جلو را به سمت مقصد ایجاد یا بروزرسانی کرده و ارتباط شروع شده و داده انتقال می یابد.

۳- حمله سیاه چاله[۳] و روشهای مقابله با آن

در این حمله، مهاجم سعی میکند تا با دستکاری بسته های کنترلی یا ارسال RREP های جعلی، ترافیک شبکه را به سمت خود جذب نماید و سپس تبدیل به سیاه چاله شود. گره مهاجم تبدیل به سیاه چاله میشود اگر هیچ کدام از بسته های کنترلی یا داده ای که به آن می رسد را رو به جلو ارسال نکند.



شکل ۱:حمله سیاه چاله

فرض می کنیم منبع S می خواهد با گره D ارتباط برقرار کند. S با ارسال بسته حاوی درخواست مسیر به همسایگانش شروع به فرآیند کشف مسیر می کند؛ گره مقصد D یا هر گره دیگرمیانی می تواند با ارسال بسته پاسخ به S جواب بدهد.

از آنجا که X یک گره بدخواه است بسته درخواست را ارسال نمیکند. در عوض اشتباها به Sجواب می‌دهد و نشان می‌دهد که آن یک مسیر تازه و معتبر به D است. بنابراین بسته پاسخ از X به D میرسد.اکنون که X همه بسته ها را که از S به D ارسال شدند را جذب کرده است یک حمله blackhole اتفاق افتاده است.

این حمله بدین صورت است که و قتی گره بدخواه بسته حاوی در خواست مسیر را دریافت کرد چون نیاز به چک کردن جدول مسیریابی خود ندارد لذا زودتر از بقیه گره ها به مبداء صادر کننده جواب می دهد و مبدا او را به عنوان مقصد یا گره ای که به مقصد نزدیک تر است تصور می کند و انتقال بسته را انجام می دهد.

در [۲] نویسندگان به این صورت عمل کرده اند که دو مسیر یا مقصدی که ابتدا پیدا میشوند را نادیده میگیرند سپس به سومین مقصدی که پیدا میشود پاسخ میدهند و آنرا به عنوان مقصد اصلی در نظر میگیرند آنها بر این باورند که گره های سیاه چاله معمولا در مسیرهای پیشنهادی اول یا دوم وجود دارند برهمین اساس از این دو مسیر هیچگاه استفاده نمیکنند به عبارتی آن مسیر هارا در قرنطینه نگه میدارند.

در[۳] گره یک بسته درخواست تایید مسیر یا CREQ به گره بعد در جهت مقصد می فرستد. بعد از آنکه، گره بعدی CREQ را دریافت کرد، حافظه مسیر خودش را برای پیدا کردن یک مسیر به مقصد جستجو می کند. اگر مسیری داشته باشد آنگاه پاسخ تایید مسیر یا CREP را به همراه اطلاعات مسیر به گره مبداء می فرستد. گره مبداء با مقایسه اطلاعات CREP تشخیص می دهد مسیر موجود در RREP معتبر است یاخیر، سربار این روش بالاست. در[۴]زمانیکه هر گره میانی در مقابل RREQ پاسخ می دهد، گره منبع در خواست بیشتری FREQ در مورد گره بعدی به گره پاسخ دهنده می فرستد و در مورد گره پاسخ دهنده و مسیر مقصد میپرسد. با استفاده از این روش می توان قابلیت اعتماد گره پاسخ دهنده را تنها در صورتی که گره بعدی درست باشد مشخص کرد. این راه حل تنها یک حمله سیاه چاله را در یک زمان مشخص می کند. در [۵] گره مبدا با پیدا کردن بیش از یک مسیر به مقصد اعتبار گره ای که RREP را شروع کرده، تایید می کند. گره مبدا صبر می کند تا بسته RREP را از بیش از دو گره دریافت کند. وقتی گره مبداء RREP هارا دریافت کرد، در صورتی که در مسیر ها به مقصد، گره های مشترک وجود داشته باشد،گره مبدا می تواند مسیر ایمن به مقصد را تشخیص دهد. این روش باعث تاخیر مسیریابی می شود چون گره باید منتظر بماند تا RREP را از بیش از دو گره دریافت کند همچنین باعث از بین رفتن انرژی که از بحث های مهم شبکه های حسگر بی سیم است می شود. در[۶]یک راه حل ممکن برای مشکل سیاه چاله غیرفعال کردن توانایی پاسخ گره میانی است، ازاین رو تمامی پیام های پاسخ باید تنها به وسیله گره مقصد فرستاده شوند. با استفاده از این

---

[۳] **Black Hole Attack**

روش گره میانی قادر به پاسخگویی نیست و به طریقی ما از به وجود آمدن مشکل سیاه چاله جلوگیری به عمل می آوریم و یک پروتکل AODV امن را پیاده‌سازی می‌کنیم. اما در آنجا دو عیب مرتبط وجود دارد، نخست اینکه تأخیر مسیریابی به شدت افزایش می‌یابد به خصوص برای شبکه های بزرگ. دوم اینکه گره مخرب میتواند اقداماتی از قبیل جعل کردن یک پیام پاسخ از طرف گره مقصد را انجام دهد. گره مقصد نمیتواند مشخص کند اگر پیام پاسخ واقعاً از طرف گره مقصد است یا اینکه به وسیله گره مخرب جعل شده است. در این مورد این روش ممکن است کافی نباشد. الگوریتم ارائه شده در[۷]،برای تشخیص حمله سیاه چاله در یک MANET که بر اساس روابطی که دارای سطح اعتماد درستی در میان گره ها است،میباشد. با این حال، در شبکه واقعی، تعیین مقدار مناسب برای رسیدن به سطح اعتماد بسیار دشوار است زیرا گره ها هیچ گونه تسهیلاتی جهت اعتماد بر یکدیگر ندارند. در[۸]اطلاعات گام بعدی به مقصد، باید وقتیکه هر گره میانی به RREQ پاسخ میدهد، ضمیمه بسته RREP شود، سپس گره مبدأ یک درخواست مجدد 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 راه حال نمیتواند از حمله سیاه چاله جمعی در شبکه های سیار موردی موبایل پیشگیری کند. برای مثال اگر گام بعدی نیز با گره پاسخگو همکاری کند، پاسخ برای FREQ برای هر سؤال به سادگی بله خواهد بود درنتیجه مبدأ به گام بعدی اعتماد کرده و داده ها را از طریق گره پاسخگو می فرستند که خود یک گره سیاه چاله است. در [۹] وقتی گره ای RREP را صادر کرد، در اطراف آن گره یک فرایند نظرخواهی صورت می گیرد. سپس بر اساس نظرات اعلام شده توسط همسایگان گره صادرکننده، RREP در مورد خرابکار بودن گره پاسخگو تصمیم گیری می شود. روش فوق برای حمله سیاه چاله تکی ارائه شده است که این ضعف این روش را نشان می دهد. در [۱۰] از روش سگ نگهبان استفاده میکنند که عملیات ارسال اطلاعات را ردیابی میکنند به این صورت که گره ای که اطلاعات را رو به جلو ارسال میکند خود ناظر شبکه خواهد بود تااینکه گره بعدی نیز اطلاعات را ارسال کند و اگر گره بعدی اطلاعات را ارسال نکند یک گره مخرب خواهد بود ضعف این روش این است که برای گره های بد اندیش چندتایی کاربرد ندارد.

جدول مقایسه روشهای موجود

شماره مرجع روش	تعداد حملات مورد بررسی	احراز هویت مبداء	سرعت الگوریتم	توضیحات
۱	فرقی ندارد	ندارد	کم	چون گره مخرب بایک مقایسه ساده میتواند اثر خود را بگذارد
۲	محدود ۱یا ۲	ندراد	بسیار کند	این روش چون چند مسیر را پیشهناد میکند سرعتش بسیار کم است
۴	یک	ندارد	بسیار کند	در این روش اگر همه گره های بعدی بد اندیش باشند نمیتواند تشخیص دهد
۵	یک	ندارد	بسیار کند	مقصد توسط دو مسیر که پیدا میشود ارزیابی میشود
۶	یک	ندارد	بسیار کند	ممکن است گره میانی خود بداندیش باشد و همچنین جعل پیام نیز وجود دارد
۷	فرقی ندارد	ندارد	خوب	بر اساس اعتماد بین گره ها ارتباط صورت میگردکه درعمل هچین چیزی جود ندارد
۸	یک	ندارد	کم	به گره های مجاور مقصد بستگی دارد
۹	یک	ندارد	کم	درستی الگوریتم به درستی گره های مجاور گره پاسخ دهنده بستگی دارد
۱۰	یک	ندارد	کم	در صورتی درست است که مقصد مشخص باشد و گرنه ممکن است گره میانی مخرب باشد
روش پیشنهادی	فرقی ندارد	دارد	کم	مشکلات روش های بالا رفع شده اند

۴- معماری روش پیشنهادی

در[۱]از روش هانی پات استفاده می کند به این صورت است گره ای که خود را به عنوان مقصد معرفی می کند توسط مبداء مورد آزمایش قرار می گیرد تا درستی آن ثابت شود به این صورت که گره مبداء توسط گره قبل از گره مقصد بسته ای را که در آن گره قبل مقصد IP خود را به عنوان مقصد در بسته قرار می دهد سپس آنرا به گره ای که خود را مقصد اعلام کرده می فرستد اگر دوباره خود را به عنوان مقصد معرفی کند پس آن یک گره بد اندیش است البته این روش هرچند نسبت به روش های دیگر موثر تر است ولی اگر برای گره بد اندیش اینطور تعریف کنیم که قبل از پاسخ به درخواست ها ابتدا IP مبداء و مقصد را با یکدیگر مقایسه کن اگر با هم برابر هستند به آن پاسخ ندهد دیگر نمیتوان گره بد اندیش را تشخیص داد.

روشی که ما برای حل این مشکل استفاده کرده ایم به این صورت است که از روش کلمه عبور(اسم شب) در کاربرد های نظامی استفاده می کنیم به این صورت که ابتدا گره مبدا آدرس مقصد را در درون بسته قرار می دهد سپس RREQ را به گره های همسایه می فرستد هر گره پس از دریافت RREQ اگر آدرس مقصد مربوط به همان گره باشد RREP را به صورت یک مسیر مستقیم به سمت مبداء میفرستد در غیر این صورت دوباره بسته را به همسایه های خود ارسال می کند حال برای مشخص کردن گره بداندیش به این صورت عمل می کنیم که به هرگره در شبکه یک رمز دو قسمتی می دهیم وهرگره هنگام ارسال RREQ اولین قسمت رمز را در بسته قرار می دهد تا گره ای که بسته را دریافت می کند مطمئن شود گره ای که بسته را ارسال کرده یک گره بداندیش نیست هنگامی که گره ای خود را به عنوان مقصد اعلام کرد باید در بسته RREP جزء دوم رمز را قرار دهد تا گیرنده مطمئن شود که مقصد گره بد اندیش نیست.در این روش چون انرژی گره ها محدود است لذا پیدا کردن یا حدس زدن رمز برای گره مخرب بسیار مشکل یا می توان گفت ناممکن است . چون می توان وابستگی بین دو رمز را طوری قرار داد که از روی هم قابل تشخیص نبوده و همچنین یک نوع وابستگی بین آنها برقرار باشد مثل اینکه جزء اول از یک نوع باشند مثلا نام درخت و جزء دوم از یک نوع مثلا نام اجزاء کامپیوتر باشد لذا این خود باعث ایمن تر شدن این روش می شود.

برای کارهای آینده می توان روی امنیت بیشتر این روش در حمله سیاه چاله ، همچنین استفاده از این روش در پروتکل های دیگر مسیر یابی مانند OLSR و همچنین کاربرد این روش روی سایر حمله ها مانند حمله سیبل،کرم چاله کار کرد.

۵-نتیجه گیری

در این روش نسبت به روش های دیگر احراز هویت هم برای فرستنده و هم برای گیرنده مشخص می شود ولی در روش های قبلی به این صورت نیست و ممکن است یک گره بد اندیش خود با فرستادن بسته در شبکه در کار شبکه اختلال ایجاد کند. ویا با تغییراتی که می توان در گره بد اندیش انجام داد می توان به فعالیت گره ادامه داد و در کار شبکه اختلال ایجاد کرد. همچنین در این روش به علت اینکه داده های کمتری ارسال می شود سربار کمتری به شبکه وارد شده همچنین در انرژی گره ها که یک موضوع بسیار مهم در شبکه های اقتضایی است صرفه جویی می شود چون نیاز به ارسال داده اضافی نیست. همچنین برای کاربرد های که نیاز به قابلیت اطمینان بالایی است بسیار مناسب است. این روش مشکلات روش های پیشین را برطرف کرده از جمله این روش محدود به تعداد حمله های گره های بد اندیش نیست و هر تعداد حمله را پاسخگو است و اثر آنها را خنثی میسازد وهمچنین مهم نیست که گره بد اندیش در کجای شبکه قرار دارد که در روش های قبل برای هر موقعیت گره بد اندیش یک راه حل عنوان شد ولی در این روش گره بند اندیش هرکجا که باشد مشخص شده و اثرش خنثی می شود .

مراجع

[۱] میرزائی, سمیه و محمد علایی، ۱۳۹۳، دومین همایش ملی مهندسی کامپیوتر و فناوری اطلاعات *روش جدید برای جلوگیری از حمله سیبیل به پروتکل مسیریابی DSR در شبکه های بی سیم متحرک موردی(manet)* ، دومین همایش ملی مهندسی کامپیوتر و فناوری اطلاعات، شوشتر، باشگاه پژوهشگران جوان و نخبگان واحد شوشتر،

http://www.civilica.com/Paper-NCCEB۰۲ NCCEB۰۲_۱۰۳.html

[۲] R. Kesavan , V. Thulasi, "Avoidance of Black Hole Attack in Virtual Infrastructure for MANET ", International Journal of Computer Applications (۲۰۱۲), VOL. ۵۰ .۳..

[۳] Lee S., Han B. and Shin M., ۲۱۱۲, *"Robust routing in wirelessAd hoc networks"*, in ICPP workshops, pp.۷۳.

[۴] Deng H., Li W. and Agrawal D. P., Oct ۲۱۱۲, *"Routing security in Ad hoc networks"*, IEEE communications magazine, vol.۴۱, no.۱۱, pp.۷۱-۷۵.

[۵] Shurman M.A., Yoo S.M. and Park S., Apr. ۲۱۱۴, *"Black Hole attack in wireless Ad hoc networks"*, in ACM ۲nd southeast conference (ACMSE'۱۴), pp.۹۶-۹۷.

[٦] Y. khamayseh, A. Bader, Wail Mardini, M. BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks", International Journal of Communication Networks and Information Security, (۲۰۱۱) VOL. ۳.۱.

[۷] L. Tamilselvan, V. Sankaranarayanan*: "Prevention of Black Hole Attack in MANET"*, the ۲nd international conference on wireless, Broadband and Ultra Wideband Communications (January ۲۱۱۷)

.

[۸] Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L*"Optimized Link State Routing Protocol for Ad Hoc Networks,"* Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, pp: ۲۸-۳۰. December. ۲۰۰۱.

[۹] M. Medadian, M. h. Yektaie, A. M. Rahmani, *"Combat with Black Hole Attack in AODV routing protocol in MANET," First Asian Himalayas International Conference*, PP: ۱-۵, ۳-۵ Nov

[۱۰] H. Deng, W. Li, D.P. Agrawal, "Routing Security in Adhoc Networks.", IEEE Communications Magazine, (۲۰۰۲), VOL. ۴۰: ۱۰