9th SASTech Symposium on Advances in & Science Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

حمله‌ی حفره‌ی خاکستری(Gray hole) و راههای تشخیص و حذف آن در شبکه های تک کاره‌ی متحرک (MANET)

مهدی ذوالفقاری، محمد صادق زاده، رضا فروزنده، احمد امامی

۱- دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی علوم و تحقیقات تهران- خراسان رضوی

۲- دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی واحد مشهد

۳- دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی علوم و تحقیقات تهران- خراسان رضوی

٤- دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی علوم و تحقیقات تهران- خراسان رضوی

mahdi.zolfaghari.ir@gmail.com

نام ارائه‌دهنده: مهدی ذوالفقاری

خلاصه

شبکه‌های تک کاره‌ی متحرک، چون ازمجموعه‌ای ازگره‌های متحرک و بدون سیم تشکیل شده است و همچنین به دلیل تغییرات پویای توپولوژی آن در ارتباطات خود ، هدف طیف گسترده ای ازحملات قرارگرفته است که کاملا آسیب پذیر نشان داده است؛ یکی از این حملات ، حمله‌ی حفره‌ی خاکستری است که به آسانی بر روی پروتکل‌های مسیریابی واکنشی مانند پروتکل مسیریابی منبع پویا اجرا می‌شود. حمله‌ی حفره-ی خاکستری ، ابتدا مخرب نیست ورفتاری صادقانه در طول فرآیند کشف مسیر دارد اما مدتی بعد، به گره‌ی مخرب تبدیل می شود؛ و می تواند فرآیند کشف مسیر را برای انتقال داده اطلاعاتی در شبکه را ، به هم زده و کارآیی شبکه را کاهش داده و باعث از بین رفتن داده های اطلاعاتی شود. بنابراین آشنایی با روش‌های تشخیص و حذف این حمله‌ی مخرب، بسیار مفید است که می تواند باعث افزایش کارآیی شبکه و اطمینان از صحت ارسال داده‌های اطلاعاتی ، در شبکه‌های تک کاره‌ی متحرک شود. در این مقاله به بررسی حمله‌ی حفره‌ی خاکستری وآخرین روش‌های موجود برای تشخیص وحذف آن پرداخته شده است.

کلمات کلیدی: **شبکه های تک کاره‌ی متحرک[۱] , حمله‌ی حفره‌ی خاکستری[۲] , پروتکل مسیریابی منبع پویا[۳] , حمله‌ی حفره‌ی سیاه[٤]**

۱. مقدمه

۱ - Mobile Adhoc Network(MANET)
۲ - Gray Hole Attack
۳ - Dynamic Source Routing (DSR)
۴ - Black hole Attack

www.NetSimulate.net
نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

شبکه‌ی تک کاره‌ی متحرک که به صورت پویا یک شبکه‌ی غیر متمرکز ، فاقد تاسیسات زیر بنایی و موقتی است که گره‌ها آزاد و متحرک هستند ؛ در این شبکه گره‌های میانی همکاری کرده و عملکردی مانند یک مسیریاب انجام داده و پیام ها را از یک گره به گره دیگری می‌فرستند[۱].

حمله‌ی حفره‌ی خاکستری [۲] که به آن حمله‌ی حفره‌ی سیاه انتخابی[۱] نیز می گویند[۳] ؛ نوع خاصی از حمله‌ی حفره‌های سیاه است که در آن گره‌ی مخرب ابتدا مخرب نیست، مدتی بعد به گره‌ی مخرب تبدیل می‌شود[۴]. دراین حمله گره‌های مخرب به درستی در فرآیند کشف مسیر شرکت می کنند اما زمانیکه از بین آنها ، یک مسیر برای ارسال به مقصد اتخاب می‌شود؛ آنها به صورت انتخابی بسته‌های اطلاعاتی را حذف و از بین خواهند برد[۵].

پروتکل مسیریاب منبع پویا [۶] ، بر حسب تقاضا می‌باشد که عمل مسیریابی از مبدا را انجام می‌دهد؛ یعنی فرستنده از کل مسیری که باید گام به گام تا مقصد طی شود، اطلاع دارد. درصورت وجود چند مسیر از مبدا به مقصد ، این مسیرها در حافظه پنهان ذخیره می‌شوند. فیلد مسیر از مبدا به مقصد ، در سرآیند بسته‌ها نگهداری می‌شود.[۷].

حمله‌ی حفره‌ی سیاه [۸] که در زمره حملات جلوگیری از دسترسی خوانده می‌شود به این صورت است که گره مخرب، ترافیک شبکه را به سوی خود هدایت کرده و پس از دریافت بسته های داده ، تمام بسته ها را از بین می‌برد[۹].

در حمله‌ی حفره‌ی سیاه ، یک گره مخرب می تواند همه بسته‌های اطلاعاتی را بوسیله درخواست مسیر جدید اشتباه یا کوتاهترین مسیر تا مقصد، به طرف خود جذب کند و سپس آنها را بدون ارسال به مقصددفع کند؛ در حالیکه در حمله حفره های خاکستری،گره های مخرب به درستی در فرآیند کشف مسیر شرکت می کنند؛ اما به یکباره از بین آنهایک مسیر برای رسیدن به مقصد انتخاب می‌شود،آنها بصورت انتخابی بسته های اطلاعاتی را حذف می کنند.به این دلیل تنها بخشی از بسته‌های اطلاعاتی حذف می‌شوند.ردیابی حمله‌ی حفره‌های خاکستری به مراتب از حمله‌ی حفره‌های سیاه سخت تر است[۵].

بنابراین آشنایی کامل و دقیق با روش‌های نوین و پرکاربرد کشف و تشخیص حمله‌ی حفره‌ی خاکستری، و در نهایت حذف حمله‌ی حفره‌ی خاکستری می‌تواند باعث عدم تخریب شبکه‌های تک کاره‌ی متحرک توسط این چالش مهم امنیتی و درنتیجه باعث افزایش و بهبود کارایی شبکه و افزایش بازدهی و مانع از دستبرد و ازبین رفتن داده‌های اطلاعاتی می‌شود.

۲. مرور ادبیات مساله

در این قسمت به بررسی ومرور کارهای پیشین شبکه‌های تک کاره‌ی متحرک و حمله‌ی حفره‌ی خاکستری در شبکه‌های تک کاره‌ی متحرک پرداخته می‌شود.

۳. شبکه‌های تک‌کاره‌ی متحرک

شبکه‌های تک‌کاره‌ی متحرک یا شبکه‌های موردی سیار ، یک شبکه‌ی بدون زیرساخت و دارای قابلیت خودپیکربندی است که از دستگاه‌های متحرکی که ازطریق لینک‌های بی‌سیم به هم متصل شده‌اند، تشکیل شده است. هر دستگاه موجود در یک MANET آزاد است که به طور مستقل در هر جهتی حرکت کند و در نتیجه لینک‌های آن بر سایر دستگاه‌ها ، مدام تغییر می کند. دستگاه‌ها شامل مسیریاب‌ها و میزبان‌های متحرک می‌باشند که یک گراف دلخواه را تشکیل می‌دهند. شبکه‌های MANET ممکن است به طور مستقل عمل کنند یا به شبکه دیگری مثل اینترنت متصل باشند[۱۰].

۴. کاربرد شبکه‌های تک کاره‌ی متحرک:

- کاربردهای عمومی

  ارتباط بین وسایل نقلیه عمومی و تاکسی‌ها
- کاربردهای نظامی

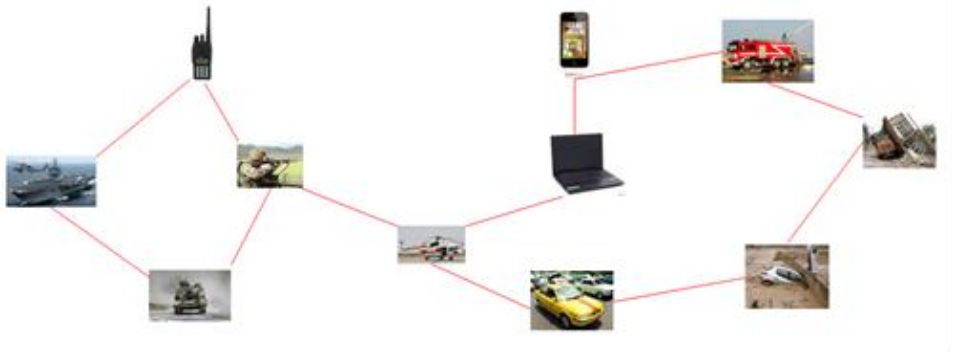
  میادین جنگی ، سازمان‌های ارتش و ارتباطات ناوگان جنگی
- کاربردهای شخصی

  اتصال کامپیوترهای کیفی با یکدیگر
- کاربردهای اضطراری

  عملیات امداد و نجات سیل و زلزله و غیره[۵،۳،۱].

۱ - Selective Black hole

www.NetSimulate.net نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی



شکل ۱- کاربرد و معماری شبکه‌ی تک کاره‌ی متحرک

۵. حمله‌ی حفره‌ی خاکستری

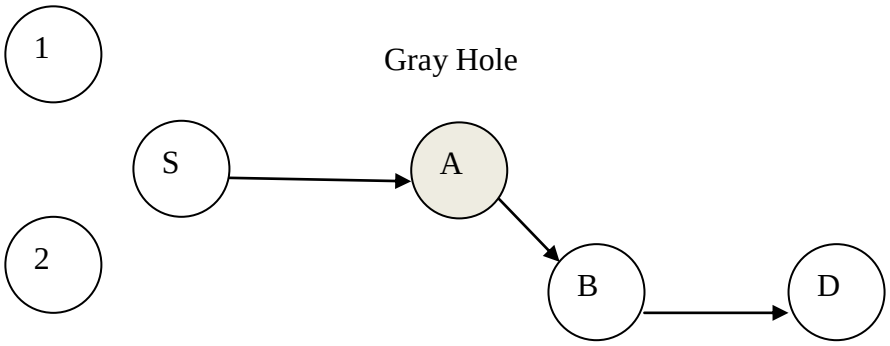
گره‌های حفره‌های خاکستری می‌توانند حملات را در سه جهت ایجاد نمایند :

۱) گره‌ی مخرب در حالی که بقیه بسته‌ها را بر می‌گرداند بسته‌ها را از گره‌های مشخص به سمت پایین بیندازد و از بین ببرد .

۲) یک گره می‌تواند در زمانی مشخص ، مخرب رفتار کرده و بصورت انتخابی بسته‌ها را سقوط دهد و از بین ببرد .

۳)هر دو حمله (حفره‌ی سیاه و حفره‌ی خاکستری) را با یکدیگر ادغام کند به عنوان مثال گره‌ی مخرب ممکن است بسته‌ها را در مدت زمانی معین از گره‌ای مشخص سقوط داده و از بین ببرد . سپس بصورت گره‌ای عادی رفتار کند . به علت این ویژگی ها ، آشکارسازی حملات حفره های خاکستری بسیار دشوار است . حملات حفره‌های سیاه و حفره‌های خاکستری هر دو می‌توانند به آسانی بر روی پروتکل‌های مسیریابی واکنشی‌مانند مسیریابی بردار فاصله درخواستی بر روی تقاضای مورد نظر [۱] و مسیر یابی منبع پویا[۲] اجرا شوند [۵].

یک گره قادر نخواهد بود همه‌ی گره‌های که در همسایگی‌اش قرار دارد مشاهده کند اما تنها قادر به تماشای پرش بعدی در مرحله مسیر کنونی خواهد بود . S گره مبدا است و D گره مقصد است و گره A یک حفره سیاه است. گره S در حال ارسال بسته‌های داده به گره D از طریق مسیر D ، B ، A ، S است . در این طرح گره S قادر خواهد بود تنها گره A که در پرش بعدی است را مشاهده کند و قادر به مراقبت از گره ۱ و ۲ نخواهد بود [۱۱].



شکل ۲- حمله‌ی حفره‌ی خاکستری[۱۱].

۶. روش‌های تشخیص و حذف حمله‌ی حفره‌ی خاکستری

دراین مقاله به بررسی جدیدترین روش های تشخیص و حذف حمله‌ی حفره‌ی خاکستری می پردازیم

۱ - Ad hoc On demand Distance Vector (AODV)
۲ - Dynamic Source Routing (DSR)

www.NetSimulate.net
نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

۷. استفاده از حدس شماره توالی

در این روش هر گره شبکه موظف است با توجه به ماهیت ترافیکی شبکه، حداکثر شماره‌ی توالی ممکن را حدس بزند؛ و هنگام دریافت بسته‌ی پاسخ مسیریابی، شماره‌ی توالی حداکثر خود را با شماره‌ی توالی بسته‌ی پاسخ مقایسه کند؛ اگر شماره‌ی توالی بسته‌ی پاسخ ، بیشتر بود گره ارسال کننده آن مخرب است.دراین روش اصول کار آن بر اساس حدس شماره‌ی توالی است.

اگر بسته‌ای دریافت کرد که شماره‌ی توالی آن بیش از مقدار مجاز باشد، بسته را به عنوان گره مخرب علامت گذاری کرده و آن را به گره‌های بعدی ارسال می‌کند؛ تا سایر گره‌های مسیر، مسیر را به عنوان مخرب شناسایی کنند و گره ارسال کننده‌ی پاسخ را به عنوان گره‌ی مخرب علامت گذاری کنند.روش هایی که بر اساس حدس شماره‌ی توالی هستند برای حملات با یک گره‌ی مخرب مناسب هستند و در حملات گره‌های همدست ، نمی‌توانند تمام گره‌های مخرب را کشف کنند و فقط گره‌ی تولید کننده‌ی بسته شناسایی خواهد شد. همچنین این روش دارای سربار پردازش بالایی برای کل شبکه است؛ زیرا تک تک گره‌های شبکه باید دائما حداکثر شماره‌ی توالی را محاسبه کنند و با شماره‌ی توالی بسته‌های دریافتی مقایسه کنند[۹].

۸. استفاده از پروتکل مسیریابی منبع پویای تغییر داده شده

در این روش زمانیکه گره مبدا دارای بسته‌های اطلاعاتی جهت ارسال به مقصد است ، داده‌هایی را که برای انتقال دادن می‌باشد را به بلاک‌های مختلف تقسیم می‌کند و هر دفعه یکی از بلاک‌های داده را به مقصد می‌فرستد؛ همچنین شماره منحصر به فرد بسته‌های اطلاعاتی را که آن را در یک بلاک دیگر به مقصد می‌فرستد قبل از اینکه داده‌ها به صورت واقعی استفاده شود در مسیری متفاوت (دومین مسیر کوتاه برای رسیدن به مقصد) منتقل شوند .

فرآیند کشف حملات حفره‌های خاکستری آغاز می‌شود.ابتدا بسته درخواست بررسی[۱] ، ابتدا (QREQ) را به گره‌ای در مسیر مبدا (مسیر ارسال داده) می‌فرستد که در فاصله‌ی 2-hop (۲ پرش) از او واقع شده است . QREQ جهت پیدا کردن شماره‌ی بسته‌های داده ارسال کرده به همان گره به گره پرش بعدی استفاده می شود؛ گره a_{n-1} بسته‌ی جواب بررسی[۲] ، ابتدا (QREP) را به گره‌ی مقصد D می - فرستد . QREP شامل شماره‌ی بسته‌های داده حاوی یک گره‌ی ارسال شده از پرش مجاور بعدی در مسیر مبدا است . گره مقصد با استفاده از QREP که دریافت می‌کند تایید می‌کند که آیا همسایه پرش قبلی‌اش (مثلا گره a_n) همه‌ی بسته‌های داده‌ای که از گره قبلی خود دریافت کرده است (گره a_{n-1}) را به درستی ارسال می‌کند ؛ اگر درست ارسال نمی‌شود گره مقصد هر دو گره a_n و a_{n-1} را به فهرست گره‌های مشکوک می‌فرستد. اگر درست ارسال می شوند بدین معناست که این دو گره عملکرد صحیحی در ارسال داده‌ها دارند. بنابراین گره مقصد دوباره یک QREQ جدید را به گره a_{n-3} می‌فرستد که در فاصله ۲ پرش از گره a_{n-1} در مسیر مبدأ قرار دارد. گره مقصد با استفاده از QREP که دریافت می‌کند تایید می‌کند که آیا دو گره a_{n-3} و a_{n-2} همه‌ی بسته‌های داده‌ای که دریافت کرده‌اند را به درستی ارسال می‌کند. این فرآیند ادامه پیدا می‌کند تا زمانی که QREQ به گره‌ای برسد که دارای یک گره مسیر قبلی به فاصله ۲ پرش در مسیر مبدأ نباشد. (شکل ۳- a) گره مقصد بسته QREQ را به GN(گره‌ی حفره‌ی خاکستری) می‌فرستد که در فاصله 2-hop از گره مقصد قرار گرفته است . گره GN در صورت مخرب بودن،اطلاعات درستی در مورد چگونگی ارسال بسته اطلاعاتی به گره بعدی نمی- فرستد (شکل ۳- a).

در (شکل۳- b) گره‌های ۱ و ۶ به ترتیب منبع و مقصد هستند. اگر به عنوان مثال گره منبع ۱۰۰ بسته اطلاعاتی ارسال کند و گره مقصد تنها ۶۰ بسته از آن را دریافت نماید ، گره مقصد یک بسته QREQ را به گره ۴ می فرستد. گره ۴ بسته QREP را که حاوی تعداد بسته های اطلاعاتی(در این مثال ۶۰ بسته) بوده به گره بعد از خود(گره ۵) مجددا ارسال می کند.گره ۵ بسته QREP را دریافت کرده و به گره مقصد ۶ ارسال می نماید . گره ۶ تایید می کند که تعداد بسته های اطلاعاتی دریافتی از گره ۵ با تعداد ذکر شده در QREP مطابقت دارد ؛ اما از بسته QREP متوجه می شود که گره ۴ تنها ۶۰ بسته از ۱۰۰ بسته ارسال شده توسط گره مبدا را مجددا ارسال می‌نماید بنابراین گره ۴ را به فهرست گره های مشکوک منتقل می کند؛ سپس یک بسته QREQ به گره ۲ که در فاصله 2-hop (۲ پرش) از گره ۴ قرار دارد ارسال می کند .گره ۲ یک QREP حاوی تعداد بسته‌های اطلاعاتی (۱۰۰ بسته) که به گره بعدی‌اش به عنوان مثال گره GN ارسال کرده می‌فرستد . گره GN بسته QREP را دریافت کرده و آنها را به مقصد مجددا ارسال می نماید . گره مخرب GN نمی تواند بسته QREP را اصلاح کند زیرا پیام با کد تایید هویتی (MAC) متصل شده است که با عدد خصوصی گره (گره ۲) و عددی اتفاقی برای کاهش خطر حمله تهیه گشته است . همزمان با دریافت QREP توسط گروه گره مقصد ، مشاهده می کنیم که تعداد بسته های ارسالی از گره ۲ به گره GN ۱۰۰ بسته است.درحالیکه گره ۴ ، بطور واقعی ۶۰ بسته را ارسال کرده است.بنابراین این احتمال وجود دارد که هردو گره

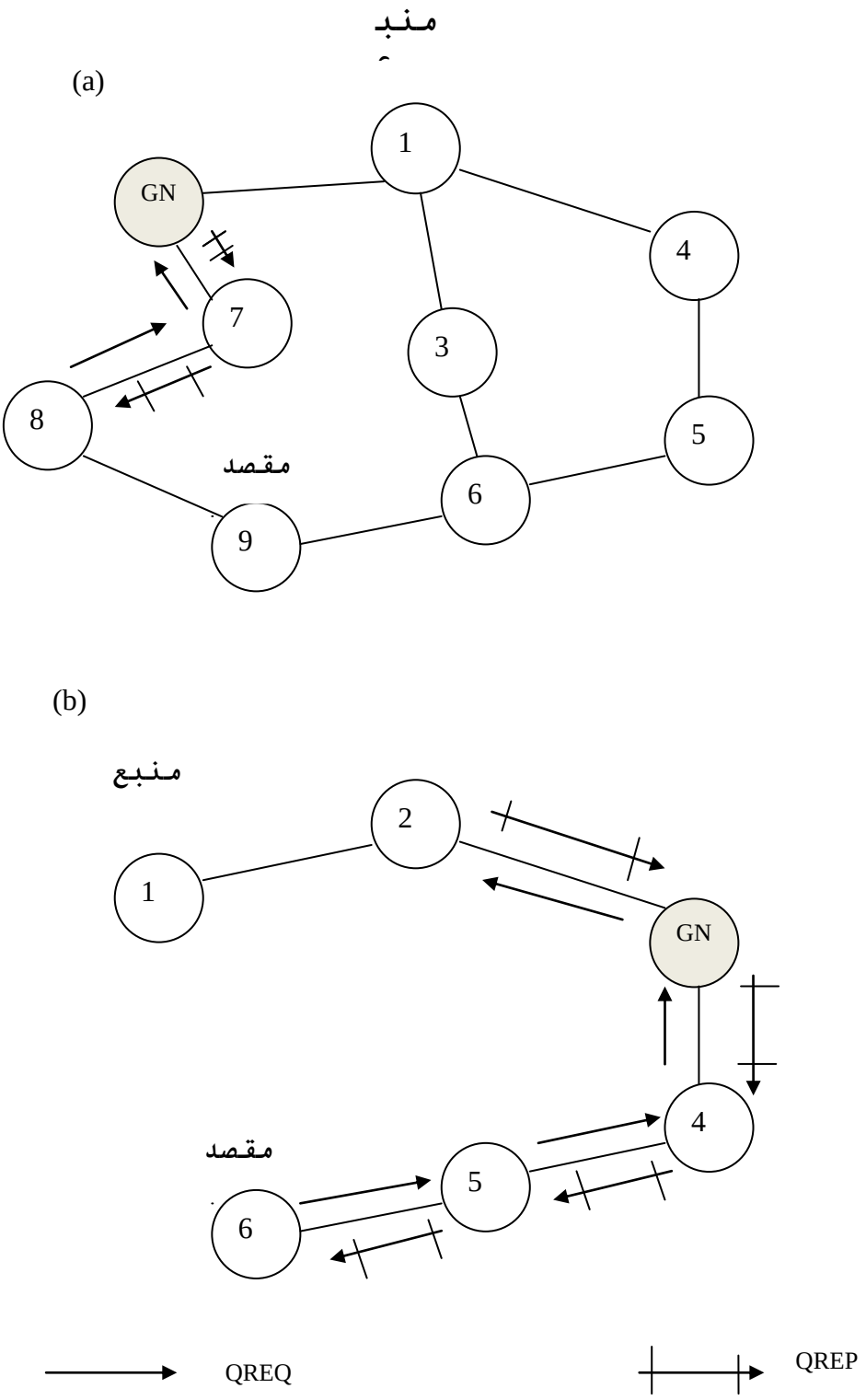
---

۱ – Query Requst (QREQ)

۲ - Query Reply (QREP)

www.NetSimulate.net نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

GN و گره ۲ بسته‌هایی را حذف کرده باشند و اطلاعات ارسالی توسط گره ۲ نیز غلط می‌باشد.از این رو ،گره مقصد گره ۲ و GN در فهرست گره-های مشکوک ذکرمی‌شوند[۵].



شکل ۳ – انتقال QREQ و QREP بین گره های مسیر مبدا در فاصله 2-hop [۵]

www.NetSimulate.net
نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

اکنون گره مقصد ، گره‌های خصوصی مشکوک در مسیر مبدا را به گره‌های IDS به عنوان بسته MNREQ (درخواست گره مشکوک) معرفی می کنند. بسته MNREQ به تمامی گره های IDS مجددا فرستاده می شود.بسته MNREQ تنها توسط یک گره IDS به گره های IDS مجاور ارسال میشود.بعد از گذشت فاصله زمانی دوره ای (برای دریافت MNREQ توسط تمامی گره های IDS ، گره IDS که در مجاورت گره مبدا قرار گرفته ، بسته ALARM را به گره مبدا ارسال می کند تا آن را از حضور حمله کننده ها در مسیر ارسال داده ها،آگاه نماید و از آنها می خواهد که بلاک های بعدی اطلاعات را بفرستند؛

زمانی که گره مبدا بلاک‌های اطلاعاتی بعدی را می‌فرستد ، گره های IDS که در مجاورت گره‌های مشکوک قرار گرفتند به حالت مخرب تبدیل شده و گوش می‌کنند که آیا بسته‌های اطلاعاتی ارسالی یا حذف شده توسط گره‌های مشکوک را می‌پذیرند. اگر هریک از گره‌های مشکوک پیدا شدند عمدا بسته‌های اطلاعاتی را حذف کنند ، در فهرست گره های مشکوک جای می‌گیرند؛ سپس گره های IDS نشان داده شده ، پیام مسدودکننده را به همه‌ی گره‌های نزدیک ارسال می- کنند . هر گره IDS پس از دریافت پیام مسدود کننده آن را به همسایگان خود انتقال می‌دهد و به این ترتیب گره مشکوک حذف می‌گردد . پیام مسدود کننده تنها توسط گره‌های IDS در شبکه فرستاده می‌شود. هر گره عادی ، پس از دریافت پیام مسدودکننده از اطلاعات گره مخرب آگاه شده و سپس پیام را بدون بازارسال ، حذف می کند. همین که گره مشکوک مکان یابی و حذف شد همه گره ها هرگونه اطلاعات مسیریابی شامل گره‌های حمل کننده را برمی دارند و هیچ RREP شامل گره مخرب جایگزین نمی شود[۵].

۹. استفاده از شماره تولید شده اولیه

شماره‌ی تولید شده اولیه (PPN) طرح پیشنهادی برای کاهش اثرات نامطلوب گره مخرب است . ایده‌ی اولیه طرح PPN این است که ، هر گره در شبکه می‌تواند با یک عدد خاص اولیه که به عنوان هویت آن گره است فعالیت کند و این هویت امکان ندارد که تغییر کند؛ روش PPN به عنوان یک مکمل پروتکل AODV (مسیریابی بردار فاصله درخواستی بر روی تقاضای مورد نظر) موردی (Adhoc) است برنامه PPN مبتنی بر AODV است و می تواند به طور موثر از حملات گره مخرب در طول مسیر تشکیل شده بین مبدا و مقصد جلوگیری کند . برنامه PPN از مسیریابی بردار فاصله درخواستی بر روی تقاضای مورد نظر به صورت مسیری در طول فرآیند استفاده می‌کند .

در برنامه PPN هر گره ، سر خوشه‌ای دارد که وظیفه حفظ و مراقبت جدول همسایه که برای نگه داشتن اطلاعات در مورد همه گره‌ها در مرحله‌ی کشف برنامه PPN است استفاده می‌شود یک گره میانی که برای ایجاد یک مسیر تلاش خواهد کرد و ازمسیر یک گره- ای که اطلاعات دریافتی- اش اشتباه باشد استفاده نمی‌کند و PPN به طور کامل قابل انجام نیست ؛ بنابراین، گره های مخرب به تدریج در شبکه از گره های غیر مخرب دیگر اجتناب خواهد کرد [۴].

۱۰. استفاده از جدول مسیر یابی مداوم داده تغییر داده شده

در این روش طرح کشف و حذف همکاری حملات blackhole وgrayhole با ثابت نگهداشتن جدول MEDR (اطلاعات مسیریابی داده مختصر و طولانی مدت تغییر دادن آن) در هر گره بیان شده است؛ قسمت‌ها (محتویات) این جدول نه تنها برای کشف یک گره مخرب و بلکه شاهد تغییر ندادن سابقه‌ی مخرب قبلی‌اش که به رفتار حفره‌ی خاکستری کمک می‌کرده است استفاده می شوند به عنوان روشی که پروتکل های Ad Hoc (موردی) انتخاب کرده اند برنامه‌ای برای طراحی الگوریتم و توسعه و برآورده کردن الزامات پروتکل AODV است [۳].

۱۱. استفاده از یک سیستم تشخیص نفوذ

همه سیستم تشخیص تفوذ با اجرای یک مکانیسم ABM به نام (مکانیسم ضد Blackhole) است که عمدتا مورد استفاده برای برآورد ارزش مشکوک (مخرب)بودن یک گره بر اساس میزان غیرطبیعی تفاوت بین RREQs و RREPs از گره ارسالی باشد .

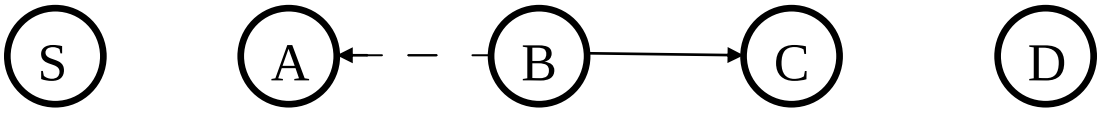
هنگامی که مقدار مشکوک بیش از آستانه از پیش تعریف شده یک بلاک باشد پیام‌ای توسط IDS نزدیک ، به اطلاع تمام گره‌هایی که در شبکه پخش هستند ارسال می‌شود که با همکاری یکدیگر به منزوی کردن گره مخرب منجر می‌شود. بلاک پیام ، حاوی IDS صادر شده و گره شناسایی حفره سیاه و زمان شناسایی آن می باشد . به محض دریافت پیام بلاک صادر شده توسط IDS، گره های معمولی مکان‌های گره‌های مخرب را در لیست سیاه شان قرار می‌دهند [۱۲].

۱۲. استفاده از سیستم تشخیص نگهبان

www.NetSimulate.net نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

روش سیستم تشخیص نگهبان[۱] [۱۳] یا تایمر مراقب ، روشی برای کشف و تشخیص گره‌ی مخرب مبتنی بر بسته سوء رفتار، در حرکت به سمت جلو و یا رفتار بسته از بین رفته در دوره زمانی که از قبل مشخص شده باشد، می‌باشد؛ استفاده از تایمر مراقب برای شمارش یک زمان برای انتقال بسته‌ها از گره مبدا به گره مقصد می باشد[۳].

سیستم تشخیص نگهبان یکی از روش‌های اساسی است که در برابر بسیاری از روش پیشنهادی تشخیص نفوذ که تا کنون ایجاد شده وجود دارد.
گره های مخرب بر روی پرش بعدی ، توسط استراق سمع (پنهانی گوش دادن) از طریق روش تشخیص نگهبان تشخیص داده می شوند. سپس راه مسیریابی که می خواستیم کمکی در امکان تشخیص مسیر هایی باشد که آن مسیر ها شامل گره های مخرب هم باشد.
در پروتکل مسیریابی منبع پویا [۲] مسیریابی داده‌ها در گره منبع تعریف شده است. این اطلاعات به شکل یک پیام به گره های میانی منتقل شده است تا زمانی که به مقصد مورد نظر می رسد. بنابراین، هر گره میانی که در مسیر است باید گره‌ای که در پرش بعدی وجود دارد را تشخیص دهد. علاوه بر این، به دلیل به ویژگی‌های خاص شبکه‌های بیسیم ممکن است برای شنیدن پیام های پرش بعدی هم به کار برده شود
به عنوان مثال اگر گره A نزدیک گره B باشد آنگاه گره A می تواندارتباطات گره B را بشنود .
فرض کنیم که گره S(منبع) مایل به ارسال بسته به گره D (مقصد)داشته باشد. یک مسیراز طریق A , B و C ازگره منبع S به گره مقصدD وجود دارد. تصور کنید در حال حاضر که گره A پیش از این بسته داده را در مسیر گره منبع S به گره مقصد D دریافت کرده بود. و با اطمینان گره B بسته داده را به گره C حرکت به جلو داده است. اگر گره B (با خطوط نقطه چین) بسته داده اطلاعاتی را استراق سمع و شنود کند و همان را به آنچه که در بافر خودش است می فرستد.
نشان دهنده این است که گره B بسته داده را به طرف گره C (با خط پر) به جلو حرکت داده است. بسته داده از بافر گره منبع حذف شده است. از سوی دیگر آن بسته ، در یک
زمان مشخص با بسته ای که در بافر گره منبع وجود دارد مقایسه نشده است.روش تشخیص نگهبان به گره B ، شمارنده خطا را می افزاید. اگر عدد این شمارنده از آستانه گره A بیشتر شود؛ گره A نتیجه گیری می کند که گره B ، گره ای مخرب است و این را به گره منبع S گزارش می دهد [۱۴].



شکل ۴- عملکرد روش تشخیص نگهبان[۱۴]

۱۳. استفاده از درخت Merkel

با استفاده از درخت مرکل [۳] [۱۵] به تشخیص حفره‌ی خاکستری پرداخته می‌شود . درخت Merkle یک درخت دودویی است که هر برگ آن شامل یک شماره‌ی اعتباری است و گره‌های میانی از مجوز شماره اعتباری ، برای ایجاد یک شماره ترکیبی جدید استفاده می‌کنند این روش همچنین می‌تواند همکاری حملات حفره های سیاه با یکدیگر را نیز پیدا کند [۳].

۱ - Watchdog
۲ - Dynamic Source Routing (DSR)
۳ – Merkel Tree

www.NetSimulate.net
نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

جدول شماره ۱-بررسی تعدادی از روش های تشخیص و حذف حمله ی حفره ی خاکستری

روش تشخیص و حذف حمله حفره خاکستری	مزایا و معایب	مرجع
حدس شماره ی توالی	سربار پردازشی زیاد	۹
سیستم تشخیص نفوذ	مصرف و اتلاف انرژی زیاد دوباره ارسال کردن بسته های داده کاربردسخت و چالش برانگیز	۱۲
شماره تولید شده اولیه	اجتناب گره های مخرب در شبکه از گره های غیر مخرب	۴
درخت مرکل	وابسته بودن گره های میانی به برگ های درخت	۳
جدول مسیریابی مداوم داده تغییر داده شده	وابسته بودن به تغییر مداوم اطلاعات مسیریابی	۳
پروتکل مسیریابی منبع پویا تغییر داده شده	سربار پردازشی زیاد	۵

۱۴. نتیجه‌گیری

شبکه‌های سیار موردی به سرعت در حال پیشرفت است زیرا با افزایش روز افزون دستگاه های متحرک قابل حمل و ارزان قیمت که کارآیی و قدرت بیشتری دارند و از نظر کمی رو به افزایش هستند باید از نظر کیفی هم مورد توجه قرار گیرند لذا مهمترین چالش مهم شبکه های سیار موردی امنیت است و یکی از این آسیب های امنیتی این شبکه‌ها ، حمله‌ی حفره‌ی خاکستری است که باعث تخریب این شبکه ها و کاهش بازدهی و از بین رفتن داده‌های اطلاعاتی و افزایش مصرف انرژی می شود ؛ پس لزوم آشنایی با روش‌های کشف و تشخیص حمله‌ی حفره‌ی خاکستری و در نهایت حذف این چالش امنیتی بسیار مهم است ؛ مساله مهمی که در اینجا لازم است بیان شود این است که این روش‌های تشخیص وحذف را بتوان برای سایر حملات و

چالش های امنیتی نه تنها برای شبکه‌های تک کاره‌ی متحرک بلکه برای سایر زیر مجموعه‌های شبکه های تک کاره مانند به کاربرد.

۱۵. قدردانی

با سپاس از خداوند متعال با نعمت های بی‌حسابش و با تقدیر و تشکر از دوستان و همکلاسی های محترم که با ارائه راهنمایی‌ها و نظریه‌های سازنده خود نقش شایان و قابل توجهی در سامان دهی و پیشبرد این مقاله داشته اند کمال تشکر و قدردانی داریم.

۱۶. مراجع

[1] Khattak, Hizbullah., Nizamuddin.," A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", 978-1-4799-0615-4/13/$31.00, **IEEE, 2013**.

[2] Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.**2010.**

[3] Hiremani, Vani A., Jadhao, Manisha Madhukar., "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET" , **IEEE, 2013.**

[4] Gambhir, Sapna ., Sharma, Saurabh .," PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs", **IEEE, 2012.**

[5] Mohanapriya, M., Krishnamurthi, Ilango., " Modified DSR Protocol for detection and removal of selective black hole attack in MANET ", Comput Electr Eng (2013), http://dx.doi.org/10.1016/j.compeleceng.2013.06.001 , **Elsevier, 2013.**

[6] D.B.Johnson and D.A. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Kluwer Academic Publishers, chapter 5, pp. 153–181,**1996.**

[۷] مزیدی. آرش، رجب زاده. مصطفی، "تحلیل ، ارزیابی و پیاده سازی الگوریتم‌های مسیریابی در شبکه‌های موردی "، هشتمین سمپوزیوم پیشرفت های علوم و تکنولوژی ، مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه‌های کامپیوتری، مدل سازی و امنیت سیستم‌ها ، موسسه آموزش عالی خاوران ، مشهد آذر۱۳۹۲.

[8] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," in Proceedings of the 42nd annual South east regional conference. New York, NY, USA: ACM Press, pp. 96-97, 2004.

www.NetSimulate.net نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی

[۹] دری. علی، محمد کریمی زاده تکابی. طاهره ، "تحلیل حمله Black hole و راه های کشف آن در شبکه MANET"، کنفرانس منطقه ای روش های محاسبه نرم در مهندسی برق و کامپیوتر ، دانشگاه آزاد اسلامی واحد صفا شهر ، ۶ اسفند **۱۳۹۲**.

[۱۰] رضایی. مهرداد، جعفری. مهدی، امینی لاری. منصور، "بررسی حملات و مسائل امنیتی پروتکلهای مسیریابی در شبکه های ad hoc"، اولین همایش ملی برق و کامپیوتر جنوب ایران ، دانشگاه آزاد اسلامی واحد خورموج ، اردیبهشت **۱۳۹۲**.

[11] CAI, Jiwen ., YI, Ping ., CHEN, Jialin ., WANG, Zhiyang ., LIU, Ning ., " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 1550-445X/10 $26.00, DOI 10.1109/AINA.2010.143 **, IEEE, 2010.**

[12] Yang Su, Ming ., " Prevention of selective black hole attacks on mobile ad hoc networks throughintrusion detection systems**", Elsevier, 2011.**

[13] Sergio Marti et al., "Mitigating routing misbehavior in mobile ad-hoc networks," Proceedings of the International Conference on Mobile Computing And Networking ACM (MobiCOM 2000),**2000.**

[14] Ms.Sonali P. Botkar, Mrs. Shubhangi R. Chaudhary," An Enhanced Intrusion detection System using Adaptive Acknowledgment based, Algorithm", 978-1-4673-0126-8/11/$26.00 c 2011 IEEE, **IEEE, 2011.**

[15] Merkle, R. C. **(1988)**. "A Digital Signature Based on a Conventional Encryption Function". "Advances in Cryptology CRYPTO '87". Lecture Notes in Computer Science 293. p. 369. doi:10.1007/3-540-48184-2_32. ISBN 978-3-540-18796-7.

www.NetSimulate.net نت سیمولیت - مرجع شبیه سازی شبکه های کامپیوتری و مخابراتی