رویکردی جدید برای کاهش دادن حمله حفره خاکستری در MANET

چکیده

شبکه ادهاک سیار (MANET) به عنوان دسته ای از شبکه های بی سیم تعریف می شود که قادر به عملیات بدون هرگونه زیرساخت ثابت شده است. فرضیه ی اصلی در نظر گرفته شده در این شبکه این است که همه ی گره ها، گره هایی مورد اطمینان هستند، اما در سناریوی واقعی، برخی گره ها می توانند مخرب باشند و از این رو می توانند بسته های داده را به جای انتقال به گره مقصد، به صورت انتخابی کنار بگذارند. این گره های مخرب در طول مرحله ی شناسایی مسیر عادی رفتار می کنند و بعد از آن بخشی از بسته های داده ی مسیر دهی شده از میان آنها را کنار می گذارند. چنین نوعی از حمله به عنوان حمله ی حفره ی خاکستری هوشمند شناخته می شود که نوعی موارد متوالی تشکیل دهنده ی حمله ی حفره ی خاکستری است. در این مقاله، حمله ی حفره ی خاکستری را اجرا و برای کاهش اثر آن مکانیزمی جدید مطرح کرده ایم. مکانیزم کاهش حمله ی حفره ی خاکستری (MGAM) چندین گره خاص که گره های G-IDS (سیستم شناسایی نفوذ حفره ی خاکستری) نامیده می شوند را استفاده می کند. گره های G-IDS برای شناسایی و جلوگیری از حمله ی حفره ی خاکستری در MANET به کار برده می شوند. گره های G-IDS انتقال گره های همسایگی خود را استراق سمع کرده و در زمانی که شناسایی می کند که گره، بسته های داده را کنار می گذارد، پیام هشدار را در شبکه مخابره می کند تا شبکه را درمورد هویت گره مخرب آگاه کند. لازم به ذکر است که کنار گذاری بسته های داده در گره، بزرگتر از مقدار آستانه است. سپس گره مخرب شناسایی شده بوسیله ی کنار گذاری بسته ی درخواست و پاسخ از مشارکت های بعدی اش منع می شود. شبیه ساز NS-2.35به منظور اعتبار سنجی کارآمدی مکانیزم پیشنهادی ما، استفاده می شود. نتایج شبیه سازی نشان می

دهد که مکانیزم پیشنهادی در مقایسه با طرح حمله ی حفره ی خاکستری هوشمند موجود نسبتا خوب عمل می کند.

کلمات کلیدی: MANET، حمله ی خودداری از خدمت، حمله ی حفره ی خاکستری هوشمند، سیستم شناسایی نفوذ حفره ی خاکستری

1. مقدمه

شبکه ادهاک متحرک (MANET)، یک فناوری در حال پیشرفت و فراگیرترین فناوری در میان شبکه های بی سیم است که به عنوان شبکه ی کم زیرساخت شناخته می شود. این شبکه از نوع خود تنظیم، موقت و مقیاس پذیر شبکه ها است. این نوع از شبکه ها برای عملیات های مهمی مانند میدان نبرد، عملیات نجات اضطراری و غیره مناسب است. در این نوع از شیکه، هر دستگاه نه تنها به عنوان یک میزبان بلکه به عنوان یک راهبر نیز عمل می کند. این پروتوکل های مسیریابی مانند بردار فاصله برحسب درخواست در شبکه اد هاک (AODV)، مسیریابی منبع پویا (DSR) و غیره که برای ارتباطات استفاده می شوند، بر مبنای این فرض هستند که همه ی گره ها تعاونی و قابل اعتماد هستند. بنابراین، پروتوکل های مسیریابی MANET به شدت نسبت به مدل های مختلف حمله های خودداری از خدمت (DOS)، خصوصا حمله ی کنار گذاری بسته، آسیب پذیر هستند. حمله ی کنار گذاری بسته می تواند به عنوان حمله ی کنارگذاری بسته ی کامل و کنارگذاری بسته ی جزیی دسته بندی شوند. حمله ی کنار گذاری بسته ی کامل به عنوان حمله ی حفره ی خاکستری شناخته می شود. در هنگام حمله ی کنارگذاری بسته ی کامل، گره مخرب در روند شناسایی مسیر شرکت نمی کند و سعی می کند تا ترافیک داده را از طریق دادن اطلاعات مسیر یابی غلط جذب کند و همه ی بسته های داده ی رسیده را با این کار کنار می گذارد، در حالیکه در هنگام حمله ی کنار گذاری بسته ی جزیی، گره مخرب حقیقتا در روند شناسایی مسیر شرکت می کند و همچنین بسته ی پاسخ حقیقی دریافت شده از مقصد را ارسال می کند. وقتی گره منبع بسته های داده را از طریق مسیری

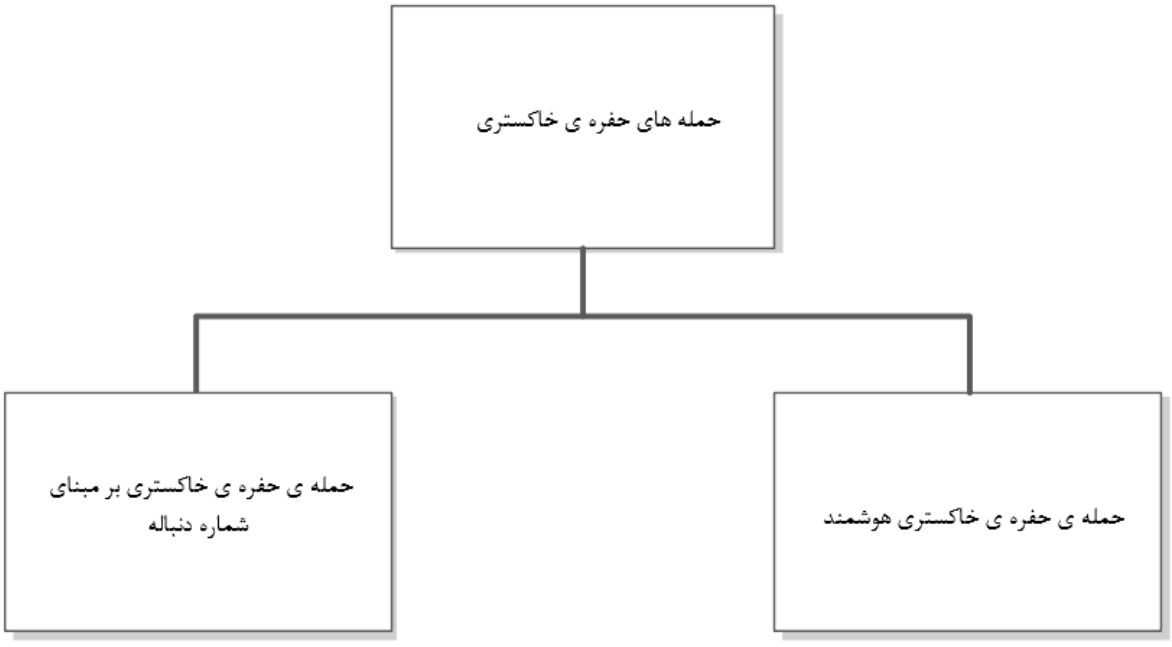
که شامل گره حفره ی خاکستری است، ارسال می کند، برخی از بسته های داده را کنار می گذارد و عملکرد شبکه اندکی کاهش می یابد. بنابراین، تامین امنیت در شبکه ی تک کاره در جهت اداره کردن حمله ها ضروری است. در این مقاله، مکانیزم جدیدی به عنوان مکانیزم کاهش حمله ی حفره ی خاکستری (MGAM) در جهت کاهش تاثیر حمله ی حفره ی خاکستری هوشمند در شبکه مطرح کرده ایم . می توان اذعان کرد که این طرح، مشارکت اصلی این مقاله است.

باقی مانده ی مقاله به صورت پیش رو بنا شده است. بخش 2 انواع مختلف حمله ی حفره ی خاکستری و فرایندهای راه اندازی حمله ی حفره ی خاکستری هوشمند را تشریح می کند. در بخش 3، درباره ی طرح های مختلف موجود برای اداره کردن حمله ی حفره ی خاکستری در MANET توضیح داده ایم. در بخش 4، مکانیزم در حال کارِ روش علمیِ مطرح شده را به تفصیل تشریح کرده ایم. بخش 5 در باره ی پارامترها و تحلیل های عملی در NS-2 بحث می کند. در بخش 6، مقایسه ی عملکرد رویکرد ما با ABM نشان داده می شود. مزایا و نقص های رویکرد ارائه شده و نتیجه گیری به ترتیب در بخش 7 و 8 بحث می شوند.

2. حمله حفره خاکستری

حمله حفره خاکستری یا حمله ارسال انتخابی یک حمله خودداری از خدمات است که نوعی از حمله ی سیاه چاله می باشد. در حمله ی سیاه چاله، در ابتدا، گره به عنوان یک مخرب ظاهر نمی شود اما بعدها تبدیل به یک گره مخرب می شود و بسته های داده ی انتخابی را کنار می گذارد. همان طور که در شکل 1 نشان داده شده، دو نوع از حمله های حفره ی خاکستری در MANET امکان پذیر است. اولین نوع از حمله ی حفره ی خاکستری، شماره دنباله ی تشکیل دهنده ی حمله ی حفره ی خاکستری است که در (10) نشان داده شده است. در این نوع از حمله ی حفره ی خاکستری، گره بوسیله ی ارسال شماره دنباله ی مقصد بالا با تعداد هاپ کمینه به گره منبع، پاسخ مسیر غلط می دهد. گره منبعِ دریافت کننده ی بسته های پاسخ، شروع به ارسال بسته های داده از مسیر حاوی گره حفره ی خاکستری می کند و بعد از آن گره حفره ی خاکستری بسته های داده را به صورت انتخابی کنار می گذارد.

دومین نوع حمله ی حفره ی خاکستری، حمله ی حفره ی خاکستری هوشمند است که نوعی از شماره دنباله ی تشکیل دهنده ی حمله ی حفره ی خاکستری می باشد. گره در این مدل، در زمان روند شناسایی مسیر، به طور عادی رفتار می کند و سپس بخش هایی از بسته های داده را کنار می گذارد. گره حفره ی خاکستری به روشی غیرقابل پیش بینی در شبکه رفتار می کند و از همین رو، شناسایی این حمله ها دشوارتر از حمله های سیاه چاله است. لازم به ذکر است که گره سیاه چاله تمام داده های دریافت شده را کنار می گذارد. همان طور که در زیر بخش های 2.1 و 2.2 نشان داده شده، فرایندی را به منظور راه اندازی حمله ی حفره ی خاکستری هوشمند مطرح کرده ایم. گره حفره ی خاکستری هوشمند، در ابتدا در جهت مشارکت عادی در روند شناسایی مسیر ساخته می شود تا مسیر های به سمت مقصد را پیدا کند اما هنگامی که بسته ی داده را دریافت می کند، کنترل می کند که متغیر مورد اعتماد صحیح یا غلط است. اگر حمله ی حفره ی خاکستری هوشمند بین زمان های T1 و T2 راه اندازی شود، متغیر مورد اعتماد، روی غلط تنظیم می شود و بعد از آن گره کتار گذاشتن انتخابی بسته را اجرا می کند در غیر اینصورت بسته های داده را به گره بعدی و یا به گره مقصد ارسال می کند.



شکل1: انواع حمله های حفره ی خاکستری

2.1. عملیات اجرا شده بوسیله ی گره های مخرب روی بسته ی درخواست دریافت

اگر (درخواست برای من نیست) سپس

در جدول مسیریابی به دنبال مسیر بگرد

اگر در جدول مسیریابی نبود

درخواست مسیر را منتشر کن // به منظور یافتن گره مقصد

Else

پاسخ را ارسال کن

Else

جدول مسیریابی را ارسال کن

پاسخ را ارسال کن

End if

2.2. عملیات اجرا شده بوسیله ی گره های مخرب روی بسته ی درخواست دریافت

اگر (درخواست برای من نیست)

اگر *(Current_Time > Set_Time1 && Current_Time < Set_Time2)*

اگر *(Trusted==False)*

شکاف های کنارگذاری بسته های داده

Else

بسته های داده را به گره مقصد یا هاپ بعدی ارسال کن

End if

End if

Else

بسته ی داده را بپذیر

End if

3. کارهای مرتبط

طرح های متعدد موجودی وجود دارند که از طرف بسیاری از محققین به منظور اداره کردن حمله کنار گذاشتن بسته ی انتخابی مطرح شده اند.

نویسنده در 17 روشی ارائه می کند که زنجیره ی گره های مخرب جمعی را مشخص می کند، این گره های مخرب، کنارگذاری انتخابی بسته در شبکه را اجرا می کنند. در این رویکرد، ترافیک داده ی کل به چندین بلوک با اندازه ی کوچک تقسیم می شود. گره منبع یک پیام مقدمه قبل از فرستادن داده به گره مقصد ارسال می کند تا آن را در مورد بلوک داده ی در حال آمدن، آگاه کند و زمان سنج را راه اندازی می کند. بعد از ارسال کردن پیام مقدمه، به منظور نظارت بر فعالیت های گره بعدی یک پیام نظارت به همه ی گره های همسایگی خود مخابره و ارسال بسته های داده را شروع می کند. از سوی دیگر، گره مقصد، یک پیام مقدمه ارسال می کند که شامل تعدادی از بسته های داده های دریافت شده از طرف گره مقصد است. اگر گره منبع، پیام مقدمه را در سر رسید زمان سنج دریافت کند، تعداد بسته های دریافت شده را با تعداد کل بسته های ارسال شده از طرف خودش را کنترل می کند و اگر اختلاف در محدوده ای قابل قبول باشد، بلوک بعدی بسته ی داده را ارسال می کند، در غیر اینصورت، شروع به شناسایی گره مخرب می کند و بعد از ان گره مخرب را بوسیله ی جمع کردن پاسخ از گره های نظارت، از شبکه حذف می کند. این رویکرد به علت بسته های کنترل اضافی متعدد دارای مسیریابی مازاد زیادی می باشد که این موضوع نقطه ضعف این رویکرد است و نویسنده ارزیابی عملکرد رویکرد پیشنهادی را انجام نداده است.

در 18، گره های خاص با عنوان IDS ، در شبکه مستقر می شوند که توانایی استراق سمع از تراکنش های همسایگی اش را دارد.در این روش، تنها گره های مقصد اجازه دارند تا بسته ی پاسخ را در هنگام دریافت کردن بسته ی درخواست، ارسال کنند و گره های میانی از ارسال بسته ی پاسخ منع می شوند. قوانین خاصی براساس کارنکردن

گره ها وجود دارد. گرهی که کار نمی کند به عنوان گره مخرب اعلام می شود. گره IDS ، مقدار مشکوک[1] بودن گره های نزدیکش را بر اساس اختلاف غیر عادی بین بسته های درخواست (RREQs) و پاسخ (RREPs) انتقال داده از گره، نظارت می کند و افزایش می دهد. اگر یک گره میانی، گره مقصد نباشد و این گره هیچ گاه یک بسته ی درخواست را برای مسیری خاص مخابره نکرده باشد، لذا گره IDS (که در ان نزدیکی قرار دارد) مقدار شک خود را به اندازه ی 1 در جدول گره مشکوکش افزایش می دهد. هنگامی که مقدار مشکوک بودن یک گره بزرگتر از مقدار آستانه شود، گره IDS یک پیام مسدود کردن به همه ی گره های در شبکه مخابره می کند تا گره مشکوک را مسدود کنند و از به همین ترتیب گره مشکوک را از شبکه جدا کنند. اگر چه این رویکرد قادر به شناسایی حمله ی سیاه چاله و حمله ی حفره ی خاکستری بر مبنای شماره دنباله در شبکه است اما در مورد حمله ی حفره ی خاکستری هوشمند شکست می خورد. گره حفره ی خاکستری هوشمند به درستی در شناسایی مسیر شرکت می کنند و همچنین بسته ی درخواست را به این علت که قادر به شناسایی آن نیست ارسال می کند. لذا محدودیت این رویکرد می باشد.

در 12، نویسنده بوسیله ی به کار گیری گره های خاص، روش پژوهشی جدیدی را برای کاهش دادن اثر گره حفره ی خاکستری پیشنهاد کرده است که می توان سیستم شناسایی نفوذ (IDS) در شبکه را مثال زد. گره منبع درباره ی تعداد بسته ها ی که از طریق مسیر جایگزین ارسال خواهد کرد به گره مقصد اطلاع رسانی می کند. هر زمانی که گره مقصد تعداد دقیق بسته های داده را نگیرد، بسته ی درخواست جستجو را به گره ای که در فاصله ی دو هاپی از آن است، (QRREQ) ارسال می کند، منتظر بسته ی پاسخ جستجو (QRREP) می ماند. بسته ی پاسخ جستجو (QRREP) شامل داده درباره ی تعداد بسته های داده ی ارسال شده از طریق گره به هاپ همسایگی بعدی در مسیر اصلی می شود. هنگام دریافت کردن بسته ی پاسخ جستجو (QRREP)، گره مقصد تایید می کند که آیا گره هاپ قبل از گره مقصد، همه ی بسته های داده ای که از گره هاپ قبل از خود، دریافت کرده را باز پخش کرده است یا نه. زمانی که گره مقصد بفهمد که گره قبلی اش همه ی بسته های دریافت کرده از گره قبل خود را ارسال نکرده است،

[1] Suspicious value

ورودی اش را به لیست مظنون تبدیل می کند و به گره های IDS نزدیک در مورد گره مورد ظن هشدار می دهد. گره های IDS به تراکنش گره مخرب گوش می کنند و هر زمانی که هر گونه ناهنجاری شناسایی کنند، پیام مسدود کردن را در شبکه مخابره می کنند. این پیام شامل هویت گره مخرب است. و سپس گره مخرب را از شبکه جدا می کنند. محدودیت این رویکرد این است که گره مخرب می تواند بعد از دریافت بسته ی جستجو به طور عادی رفتار کند و می تواند بسته های داده را ارسال کند که گره IDS به همین دلیل در وضعیتی نخواهد بود که بتواند آن را شناسایی کند.

در 10، رویکردی بر پایه ی آستانه ی شماره دنباله مطرح می شود که کاهش حمله ی حفره ی خاکستری را در شبکه ی AODV پایه اجرا می کند. نویسندگان یک طرح SNBDS را پیشنهاد داده اند که جدول مسیر یابی را بوسیله ی اضافه کردن دو حوزه ی جدید تغییر می دهد. این دو حوزه ، وضعیت گره و زمان آخرین پاسخ هستند. وضعیت گره ها بدین معنی است که آیا گره مخرب است یا خیر و زمان آخرین پاسخ به معنی زمان اعلام وصول آخرین پاسخ (RREP) برای گره مقصد است. که این گره مقصد شماره دنباله اش را به روز رسانی کرده است. با توجه به رویکرد، نویسندگان سه نوع مختلف حفره ی خاکستری را از طریق استعمال اطلاعات غلط مسیر یابی راه اندازی کردند. این اطلاعات غلط ترافیک را به سمت حفره ی خاکستری جذب می کند و کنارگذاری انتخابی بسته در شبکه را اجرا می کند. بسته های پاسخ دریافت کردن یک گره (RREP) بسته ی پاسخ ارسال کردن گره (RREP) را به عنوان یک گره مخرب شناسایی می کند اگر اختلاف بین شماره دنباله های مقصد در بسته ی پاسخ و جدول مسیر یابی بزرگتر از مقدار آستانه ی محاسبه شده باشد. در ادامه یک بسته ی درخواست طعمه (RREQ) با آدرس مقصد و شماره دنباله ی مقصد غیر واقعی به گره مشکوک ارسال می شود. اگر گره مشکوک به درخواست طعمه (RREQ) پاسخ دهد، به عنوان یک گره مخرب اعلام می شود و گره ها در آینده همه ی بسته های پاسخ را حذف می کنند. محدودیت این طرح این است که نمی تواند حمله ی حفره ی خاکستری هوشمندی را کاهش دهد که در زمان روند شناسایی مسیر، حقیقتا در شبکه مشارکت می کند و در بسته ی پاسخ دریافت شده از گره مقصد یا دیگر گره های میانی ، اطلاعات صحیح ارسال می کند.

در 19، یک مکانیزم جمعی و توزیع شده ی جدید مطرح می شود که برای اداره کردن حمله ی حفره ی خاکستری شامل چهار ماژول امنیت می شود. مازول های امنیت عبارتند از : a) مجموعه داده ی همسایگی b) شناسایی ناهنجاری محلی c) شناسایی ناهنجاری جمعی و d) فعال کننده ی هشدار سراسری. در مازول های مجموعه داده ی همسایگی، هر گره در شبکه، اطلاعات ارسال داده در همسایگی اش را جمع می کند و آن را در یک جدول اطلاعات مسیر یابی داده (DRI) ذخیره می کند. ماژول شناسایی ناهنجاری محلی بوسیله ی یک گره تحریک می شود و این اتفاق زمانی رخ می دهد که این گره با کنترل کردن جدول DRI یک گره مشکوک، آن را شناسایی می کند. ماژول شتناسایی ناهنجاری جمعی برای افزایش قابلیت اطمینان شناسایی بوسیله ی کاهش احتمال شناسایی غلط فرایند شناسایی ناهنجاری محلی، فعال می شود. و در نهایت، ماژول فعال کننده ی هشدار سراسری با انتشار پیام هشدار درباره ی گره حفره ی خاکستری به همه ی گره ها در شبکه فراخوانی می شود. لازم به ذکر است که گره خاکستری بوسیله ی ماژول شناسایی ناهنجاری جمعی شناسایی شده است. گره مخرب شناخته شده از شبکه جدا می شود. این نویسنده حفره ی خاکستری ساده را از طریق استعمال پاسخ مسیر غلط راه اندازی کرده است اما گره حفره ی خاکستری هوشمند پاسخ مسیر غلط ارسال نمی کند و در زمان شناسایی مسیر به صورت عادی رفتار می کند و بسته های داده ی انتخابی را کنار می گذارد. در نتیجه، طرحِ DRI بنیانِ تحت حمله ی حفره ی خاکستری هوشمند شکست می خورد.

اکثر کارهای موجود با کاهش شماره دنباله بر مبنای حمله ی حفره ی خاکستری سر و کار دارند. لازم به ذکر است که در حمله ی حفره ی خاکستری گره پاسخ مسیر غلط می دهد تا ترافیک را جذب کند و بسته ی داده ی انتخابی را کنار بگذارد. همچنین در ادبیات علمی قابل دسترس، هیچگونه ارزیابی از حمله ی حفره ی خاکستری در دوره های زمانی مختلف و با توجه به پویایی گره وجود ندارد.

محدودیت های طرح های کنونی ما را تشویق کرد تا مکانیزم جدیدی پیشنهاد کنیم که بتواند حمله ی حفره ی خاکستری هوشمند در شبکه ی تک کاره را اداره کند. در این مقاله، توجهمان را روی نوع دوم حمله ی حفره ی خاکستری فوق الذکر متمرکز می کنیم. برای مثال، حمله ی حفره ی خاکستری که گره مخرب در ان در زمان

شناسایی مسیر به طور عادی مشارکت می کند، کنار گذاری انتخابی بسته های داده را برای مدت زمانی اجرا می کند و سپس رفتار خود را به حالت عادی تغییر می دهد.

4. سیستم شناسایی نفوذ حفره ی خاکستری مطرح شده ی G-IDS

به منظور کاهش دادن اثر حمله ی حفره ی خاکستری هوشمند، مکانیزم جدیدی با نام MGAM (مکانیزم کاهش دهنده ی حمله ی حفره ی خاکستری) را مطرح کرده ایم، که عمدتا برای محاسبه ی تعداد بسته های کنار گذاشته شده بوسیله ی گره ای خاص به کار برده می شود . همه ی گره های G-IDS در حالت بی قاعده قرار دارند تا تراکنش های گره های همسایه را مورد استراق سمع قرار دهند. هنگامی که هرگونه ناهنجاری بوسیله ی گره های G-IDS شناسایی می شود، یک پیام هشدار بوسیله ی ان مخابره می شود. این پیام همه ی گره های در شبکه را برای مسدود کردن گره مخرب آگاه می کند. پیام هشدار شامل هویت گره حفره ی خاکستری، آدرس منبع و آدرس مقصد است. همه ی گره های عادی در هنگام دریافت کردن پیام هشدار مطرح شده از طرف گره های G-IDS، گره مخرب را در لیست سیاه خود قرار خواهند داد. طبق این پروتوکل مسیریابی AODV ، گره های معمولی اندکی تغییر می کند. نشان گذاری متعدد استفاده شده در رویکرد پیشنهادی در جدول 1 تشریح شده است و الگوریتم مکانیزم پیشنهادی در بخش 4.2 داده می شود. موارد پیش رو دو فرضیه ای هستند که در هنگام طراحی مکانیزم پیشنهادی ما لحاظ شده اند.

جدول ۱. خلاصه نشانه گذاری ها

نشانه گذاری ها	معنی ها
N_{BLT}	جدول لیست سیاه گره
IDS_{BLT}	جدول لیست سیاه آی دی اس
D_P	بسته ی داده
DP_S	تعداد بسته های داده ی فرستاده شده به وسیله گره
DP_R	تعداد بسته های داده ی دریافت شده به وسیله گره
DP_F	تعداد بسته های داده ی ارسال شده به وسیله گره
DP_D	تعداد بسته های داده ی کنار گذاشته شده به وسیله ی گره
R_Q	بسته ی در خواست
R_P	بسته ی پاسخ
A_P	بسته ی هشدار
S_A	آدرس منبع
D_A	آدرس مقصد
T_H	آستانه ی کنار گذاری بسته
M_{ID}	هویت بد نهاد

• هر گره G-IDS در محدوده ی تراکنش حداقل یک گره G-IDS خواهد بود تا هشدار را به یکدیگر ارسال کنند. برای مثال، همان طور که در شکل 2 نشان داده شده، یک گره G-IDS همواره همسایه ی چند گره G-IDS دیگر خواهد بود

• هر گره G-IDS در حالت استراق سمع قرار داده شده است تا همه ی تراکنش ها در محدوده اش را استراق سمع کند

در این مقاله، سه نوع مختلف گره در شبکه وجود دارد که به صورت مجزا کارهای مختلفی اجرا می کنند. این گره ها به شرح زیر هستند:

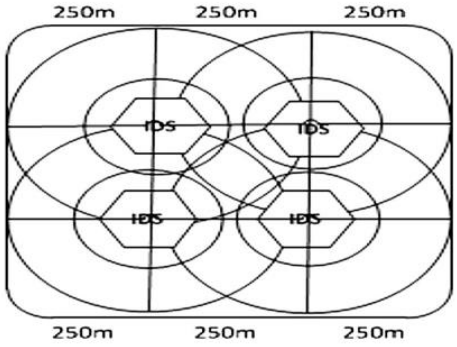
• گره حفره ی خاکستری هوشمند: به صورت انتخابی الگوریتم مسیریابی SGAODV (حفره ی خاکستری هوشمند AODV) را برای حمله ی حفره ی خاکستری در شبکه اجرا می کند.

• گره معمولی: این گره یک AODV اندکی اصلاح شده که MAODV (AODV تغییر داده شده) نامیده می شود را اجرا می کند تا مسیر یابی معمولی را انجام دهد و همچنین در زمانی که یک بسته ی هشدار منتشر شده بوسیله ی گره های G-IDS دریافت می کند، گره های مخرب را وارد لیست سیاه می کند.

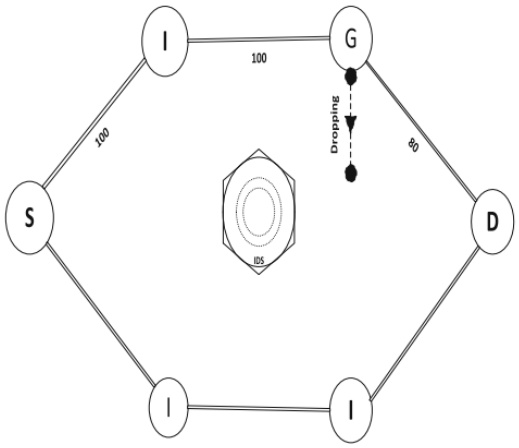
• گره G-IDS: این گره MGAM را اجرا می کند (مکانیزم کاهش دهنده ی حمله ی حفره ی خاکستری) تا گره های حفره ی خاکستری را کاهش دهد و شناسایی کند و بسته های یک هشدار را در زمانی که هر گونه ناهنجاری شناسایی می کند، در شبکه مخابره کند.

4.1. تعریف روش پژوهشی پیشنهاد شده

براساس پروتوکل AODV، گره منبع، بسته ی درخواست (RREQ) را به منظور یافتن مسیری برای برقراری ارتباط با گره مقصد مخابره می کند. هنگام دریافت کردن بسته ی درخواست (RREQ)، گره مقصد یا هر گره میانی که دارای مسیری به سمت مقصد است می تواند بسته ی پاسخ (RREP) را به گره منبع ارسال کند. گره های مخرب که حمله ی حفره ی خاکستری را انجام می دهند، در زمان روند شناسایی مسیر به صورت طبیعی رفتار می کنند

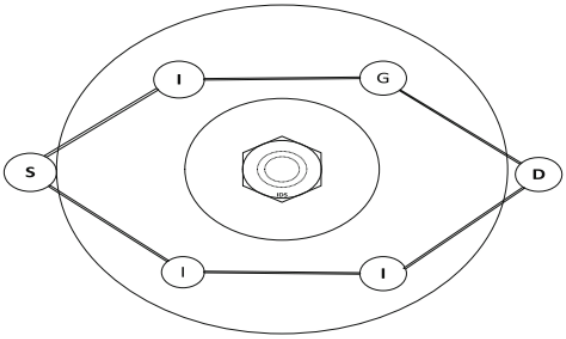


شکل2: گره G-IDS انتقال بسته را استراق سمع می کند

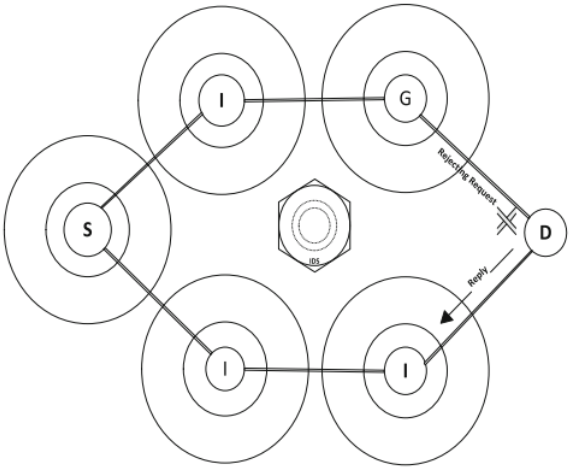


شکل3: جایگذاری گره های G-IDS

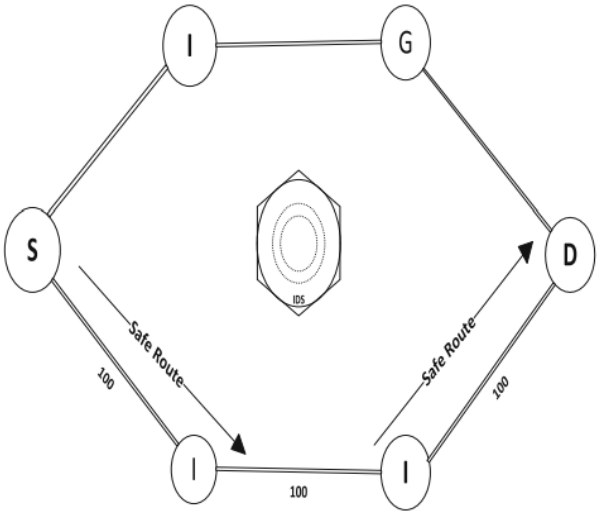
و بسته ی در خواست (RREQ) را در صورتی که مسیر به سمت مقصد نداشته باشند، مجددا در شبکه مخابره می کنند.وقتی مسیر که حاوی گره مخرب برای ارسال بسته های داده است، انتخاب می شود، همان طور که در شکل 3 نشان داده شده، این گره بسته های داده را به صورت انتخابی کنار می گذارد. به منظور کم کردن حمله ی حفره ی خاکستری، چهار گره ثابت شده ی G-IDS مورد استعمال قرار گرفته که بیشتر محدوده ی شبیه سازی را پوشش می دهند و گره های همسایگی را برای کنترل این موضوع که آیا تعداد بسته هایی که گره دریافت کرده به هاپ بعدی اش ارسال شده یا نه، نظارت می کنند. این گره G-IDS تعداد بسته های دریافت شده و ارسال شده بوسیله ی گره را محاسبه می کند. اگر اختلاف بین تعداد بسته های دریافت شده و بسته های ارسال شده بیشتر از مقدار آستانه ی کنار گذاری (TH) باشد، در ادامه، همان طور که در شکل 4 نشان داده شده، گره های G-IDS یک بسته ی هشدار را مخابره کرده و همه ی گره ها در شبکه را در مورد هویت گره های حفره ی خاکستری آگاه می کنند. دیگر گره ها هنگام دریافت کردن یک بسته ی هشدار، ورودی گره مخرب را در جدول لیست سیاهشان قرار می دهند و گره منبع ورودی مقصد را از جدول مسیریابی حذف می کند و روند شناسایی مسیر جدیدی را از طریق مخابره ی بسته ی درخواست جدیدی در شبکه آغار می کند. این فرایند در شکل 5 نشان داده شده است. هر گره در هنگام دریافت کردن بسته ی درخواست، کنترل می کند که آیا درخواست از سمت گره مخرب است یا نه. اگر از طرف گره مخرب باشد، در ادامه این بسته بوسیله ی گره کنار گذاشته می شود در غیر اینصورت، بسته ی درخواست مسیر را مخابره می کند تا مسیر به سمت گره مقصد را پیدا کند. همان طور که در شکل 6 نشان داده شده،گره منبع بعد از دریافت کردن پاسخ از گره مقصد، بسته های داده را از طریق مسیر امن ارسال می کند. پیاده سازی سیستم شناسایی نفوذ حفره ی خاکستری پیشنهاد شده (G-IDS) در NS-2 ، در شکل 7 نشان داده می شود.



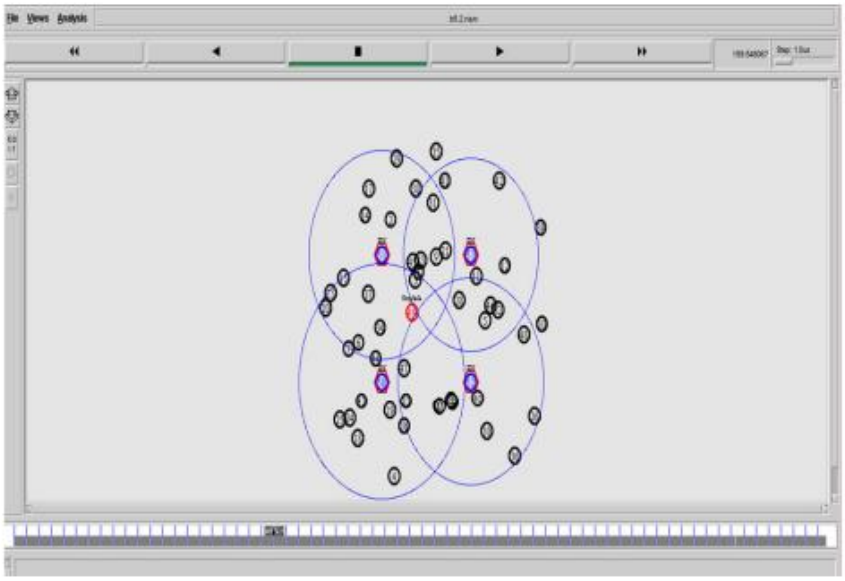
شکل4: مخابره کردن بسته ی هشدار



شکل5: شناسایی مسیر جدید بوسیله ی گره S



شکل6: انتقال از طریق مسیر ایمن



شکل7: پیاده سازی G-IDS در NS-2

4.2. الگوریتم

4.2.1. اقدام انجام شده بوسیله ی گره های G-IDS در حالت استراق سمع

تعداد بسته های دریافت شده (DPR) بوسیله ی گره را حساب کن

تعداد بسته های فرستاده شده (DPS) بوسیله ی گره را حساب کن

تعداد بسته های ارسال شده (DPF) بوسیله ی گره را حساب کن

تعداد بسته های داده ی کنار گذاشته شده (DPD) را با معادله ی زیر حساب می کند

$$DP_D = DP_R - DP_F$$

$$Set\ T_H = \frac{N}{100} \times \sum_{i=1}^{n} DPs$$

که N>0 است و i تعداد گره های منبع است که بسته های داده را می فرستند

IF (DPD>TH)

ID گره مخرب (MID) را در جدول لیست سیاه IDS (IDSBLT) اضافه کن

بسته ی هشداری که شامل ID مخرب ها (MID)، آدرس منبع (SA) و آدرس مقصد (DA) در شبکه می باشد را مخابره کن

End if

4.2.2. اقدام انجام شده بوسیله ی گره های G-IDS هنگام دریافت بسته ی هشدار

اگر پیش از این بسته های هشدار (AP) را دریافت کرده باشد

بسته های هشدار را کنار بگذار

در غیر اینصورت

ID گره مخرب (MID) را در جدول لیست سیاه IDS (IDSBLT) اضافه کن

بسته ی هشداری که شامل ID مخرب ها (MID)، آدرس منبع (SA) و آدرس مقصد (DA) در شبکه می باشد را مخابره کن

END IF

4.2.3. اقدام انجام شده بوسیله ی گره ها در هنگام دریافت بسته ی هشدار

برای ورودی مخرب در جدول لیست سیاه گره (NBLT) جستجو کن

اگر ID گره مخرب (MID) یافت شد

بسته های هشدار (AP) را کنار بگذار

در غیر اینصورت

برای ID گره مخرب (MID) در جدول لیست سیاه گره (NBLT) ورودی ایجاد کن

اگر گره منبع (SA)

ورودی آدرس مقصد (DA) را از جدول مسیر یابی حذف کن

روند شناسایی مسیر (RDP) جدید را شروع کن

End if

End if

4.2.4. اقدام انجام شده بوسیله ی گره ها در هنگام دریافت بسته ی درخواست

برای ورودی مخرب در جدول لیست سیاه گره (NBLT) جستجو کن

اگر ID گره مخرب (MID) یافت شد

بسته های درخواست (RQ) را کنار بگذار

در غیر اینصورت

اگر گره مقصد

بسته ی پاسخ (RP) را بفرست

در غیر اینصورت

بسته ی درخواست (RQ) را ارسال کن

End if

End if

4.2.5. اقدام انجام شده بوسیله ی گره ها در هنگام دریافت بسته ی پاسخ

برای ورودی مخرب در جدول لیست سیاه گره (NBLT) جستجو کن

اگر ID گره مخرب (MID) یافت شد

بسته های پاسخ (RP) را کنار بگذار

در غیر اینصورت

اگر گره منبع

بسته ی داده (DP) را بفرست

در غیر اینصورت

بسته ی پاسخ (RP) را ارسال کن

End if

End if

5. تحلیل و تنظیم محیطیِ عملی

در این مقاله، شبیه ساز NS-2.35 به منظور اعتبارسنجی اثربخشی روش پژوهشی ارائه شده دربرابر گره های حفره ی خاکستری هوشمند، استعمال می شود. در یک سطح 750*750m ، 48 گره عادی پروتوکل مسیریابی AOVD را اجرا می کنند که به طور تصادفی توزیع گشته اند و در بیشترین حالت، دو گره مخرب حمله ی حفره ی خاکستری هوشمند را اجرا می کنند که به طور تصادفی مکان یابی شده اند. دو جفت به صورت تصادفی برای ارتباط انتخاب شدند، هر کدام در هر ثانیه10 KB از بسته های UDP-CBR را ارسال می کنند. در هر سناریو، همه ی گره ها در موقعیت های مختلف مکان یابی شدند و با سرعت انتقال مختلفی از 5،15،25 و 35 m/s جابه جا شدند. پارامترهای مهم استفاده شده در این آزمایش در جدول 2 لیست می شوند و همه ی مقدار عملی در این مطالعه به یک مقدار میانگین ارجاع داده می شود که از ده آزمایش بدست آمده است.

جدول ۲. پارامترهای شبیه سازی

پارامتر	مقدار
ابعاد	750 × 750 m
تعداد کل گره ها	50
زمان شبیه سازی	500 s
مدل رادیویی انتشار	Two ray ground
نوع ترافیک	CBR
تعداد ارتباطات	2
اندازه ی بسته	512 bytes
آرتباط	UDP
مدل تحرک	Random waypoint
لایه ی مک	IEEE 802.11
گره ی بد نهاد	1–2
سرعت تحرک	5, 15, 25, 35 m/s
پروتوکول	AODV, SGAODV

به منظور ارزیابی عملکرد مکانیزم پیشنهادی ما، معیارهای عملکرد مختلفی مانند نرخ انتقال بسته، نرخ اتلاف بسته، توان عملیاتی میانگین، مازاد مسیر یابی و مازاد مسیریابی نرمالیزه شده را استفاده کرده ایم. پروتوکل حفره ی خاکستری هوشمند AODV (SGAODV)برای راه اندازی حمله ی حفره ی خاکستری هوشمند در شبکه استفاده می شود. حمله ی حفره ی خاکستری هوشمند به روشی راه اندازی می شود که بین زمان شبیه سازی 0 و 100 ثانیه به طور عادی رفتار می کند و در ادامه بین ثانیه های 100 و 200 ، کنارگذاری بسته ی انتخابی را اجرا می کند. بعد از این دوره ی زمانی، این گره مجددا برای 100 ثانیه به عنوان یک گره معمولی رفتار می کند و سپس رفتارش را به اجرای کنار گذاری بسته ی انتخابی بین ثانیه های 300 و 400 تغییر می دهد. در نهایت بعد از ثانیه ی 400، این گره به صورت عادی رفتار می کند.

5.1. معیار های عملکرد

معیارهای مختلف عملکرد که به منظور ارزیابی اثربخشی روش ارائه شده تحت حمله ی حفره ی خاکستری هوشمند مورد استعمال قرار گرفته اند در این بخش تشریح می شوند و معنای نشان گذاری استفاده شده در این معادلات در جدول 3 داده می شوند.

5.1.1. نرخ انتقال بسته

این معیار بوسیله ی مجموع تعداد بسته های رسیده به مقصد تقسیم بر مجموع تعداد بسته های ارسال شده از طرف منبع * 100٪ بدست می آید.

$$PDR = \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\,\%.$$

جدول۳ . معنی نشانه گذاری ها

نشانه گذاری ها	معنی
PDR	نرخ انتقال بسته
PLR	نرخ اتلاف بسته
AT	توان عملیاتی میانگین
RO	مازاد مسیریابی
NRL	بار مسیریابی نرمالیزه شده
TPR	نرخ مثبت واقعی
FPR	نرخ مثبت غلط
i	تعداد گره های منبع یا مقصد
j	تعداد گره های تولید کننده ی بسته های کنترل
X	تعداد بسته های دریافت شده
Y	تعداد بسته های فرستاده شده
P_S	اندازه ی بسته
S_P	زمان توقف شبیه سازی
S_T	زمان شروع شبیه سازی
R	تعداد بسته های کنترل
N_{DM}	تعداد گره های بد نهاد شناسایی شده
T_{MN}	تعداد کل گره های بد نهاد
N_{FDM}	تعداد گره های به اشتباه بد نهاد شناسایی شده
T_{NN}	تعداد کل گره های عادی

5.1.2. نرخ اتلاف بسته

این معیار بوسیله ی مجموع تعداد بسته های کنار گذاشته شده تقسیم بر مجموع تعداد بسته های ارسال شده از طرف منبع * 100٪ محاسبه می شود

$$PLR = \frac{\sum_{i=1}^{n} Y_i - \sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\,\%.$$

5.1.3. توان عملیاتی میانگین

این معیار بوسیله ی مجموع اندازه ی بسته های رسیده به مقصد در شبکه تقسیم بر اختلاف زمان شروع و توقفِ زمان شبیه سازی محاسبه می شود.

$$AT = \frac{\sum_{i=1}^{n} X_i \times P_s}{S_P - S_T}.$$

5.1.4. مازاد مسیریابی

این معیار به معنای مجموع تعداد بسته های کنترل تولید شده بوسیله ی گره در شبکه می باشند

$$RO = \sum_{j=1}^{n} R_j.$$

5.1.5. بار مسیریابی نرمالیزه شده

این معیار بوسیله ی مجموع تعداد بسته های تولید شده بوسیله ی گره، تقسیم بر مجموع بسته های دریافت شده در مقصد، در شبکه محاسبه می شود.

$$NRL = \frac{\sum_{j=1}^{n} R_j}{\sum_{i=1}^{n} X_i}.$$

5.1.6. نرخ مثبت واقعی

نرخ TP بوسیله ی نعداد گره های مخرب شناسایی شده تقسیم بر مجموع تعداد گره های مخرب در شبکه * 100٪ محاسبه می شود

$$TPR = \frac{N_{DM}}{T_{MN}} \times 100\,\%.$$

5.1.7. نرخ مثبت غلط

نرخ FP بوسیله ی نعداد گره های به اشتباه مخرب شناسایی شده تقسیم بر مجموع تعداد گره های عادی در شبکه * 100% محاسبه می شود

$$FPR = \frac{N_{FDM}}{T_{NN}} \times 100\,\%.$$

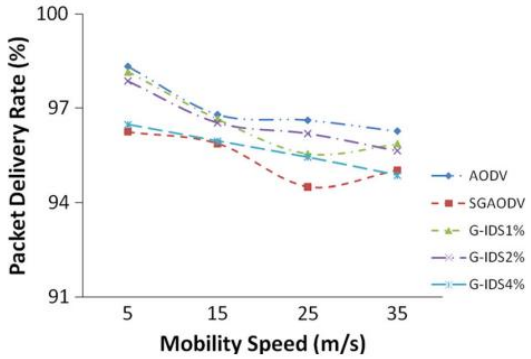
5.2. نرخ انتقال بسته

شکل 16 نشان می دهد که مازاد مسیریابی نرمالیزه شده با افزایش در سرعت تحرک گره ها، افزایش می یابد. بار مسیریابی نرمالیزه شده میانگین بوسیله ی AODV برای همه ی سرعت های تحرک و در نبود گره مخرب در حدود 2.17است. زمانی که حمله ی حفره ی خاکستری هوشمند (SGAODV) راه اندازی می شود، بار مسیریابی نرمالیزه شده ی میانگین SAODV در حدود 2.24 است. هنگامی که رویکرد پیشنهاد شده در G-IDS پیاده سازی می شود، بار مسیریابی نرمالیزه شده ی میانگین در زمانی که مقدار آستانه ی کنارگذاری بسته روی 1 و 2 و 4 درصد از بسته های داده ی کل باشد، به ترتیب برای همه ی سرعت های تحرک در حدود 2.23 و 2.25و 2.21 است. این مسئله در شکل 17 نیز دیده می شود که بار مسیریابی نرمالیزه شده در هنگام وجود دو گره مخربا افزایش سرعت تحرک، افزایش می یابد. هنگامی که دو گره مخرب هوشمند در شبکه وجود داشته باشد، مازاد مسیریابی نرمالیزه شده ی میانگین SGAODV در حدود 2.34 است. هنگامی که رویکرد پیشنهاد شده استفاده می شود، بار نرمالیزه شده ی

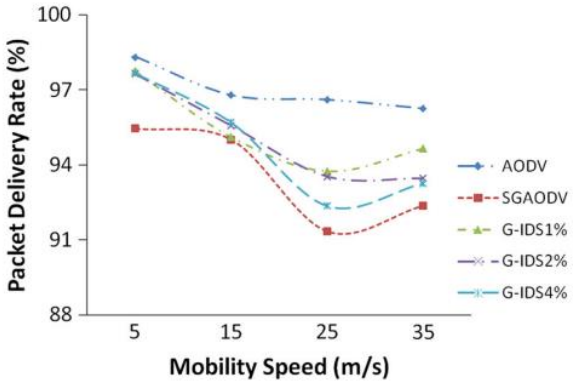
مسیریابی میانگین برای همه ی سرعت های تحرک در زمانی که مقدار آستانه ی کنارگذاری بسته روی 1 و 2 و 4 درصد از بسته های داده ی کل تنظیم شود، به ترتیب در حدود 2.33 و 2.30 و 2.27 است.

5.3. نرخ اتلاف بسته

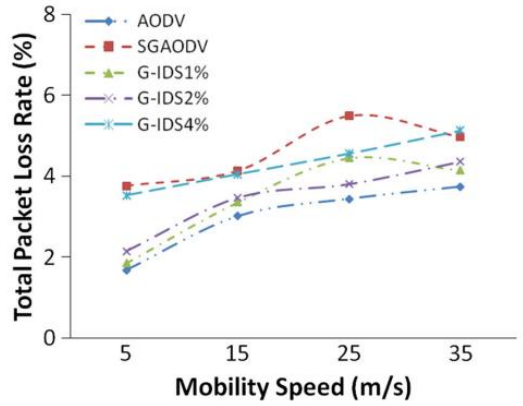
می توان در شکل 10 دید که میانگین مجموع PLR در زمانی که گره مخرب وجود ندارد و برای همه ی سرعت های تحرک بوسیله ی AODV در حدود 2.99% است. زمانی که حمله ی حفره ی خاکستری هوشمند (SGAODV) راه اندازی می شود، میانگین مجموع PLR برای SAODV در حدود 4.59% است. این موضوع به علت رفتار عادی آن در شناسایی مسیر به جای کنارگذاری بسته ی انتخابیِ بسته های داده است. زمانی که رویکرد پیشنهاد شده به کار گرفته می شود، میانگین مجموع PLR برای همه ی سرعت های تحرک هنگامی که مقدار آستانه ی کنارگذاری بسته روی 1 و 2 و 4 ار کل بسته های داده تنظیم می شود، به ترتیب در حدود 3.45 و3.44 و 4.31% است. همچنین می توان در شکل 11 دید که وقتی دو گره مخرب هوشمند در شبکه وجود دارد، میانگین مجموع PLR برای SGAODV در حدود 6.31% است. هنگامی که رویکرد پیشنهاد شده بوسیله ی G-IDS استفاده می شود، میانگین مجموع PLR برای همه ی سرعت های تحرک در زمانی که مقدار آستانه یکنارگذاری بسته روی 1 و 2 و 4 از کل بسته های داده تنظیم شود، به ترتیب برابر با 4.69 و 4.96 و 5.26٪ است. از گراف می توان دید که مکانیزم ما تحت حمله ی حفره ی خاکستری در شبکه دارای PLR کمی است.



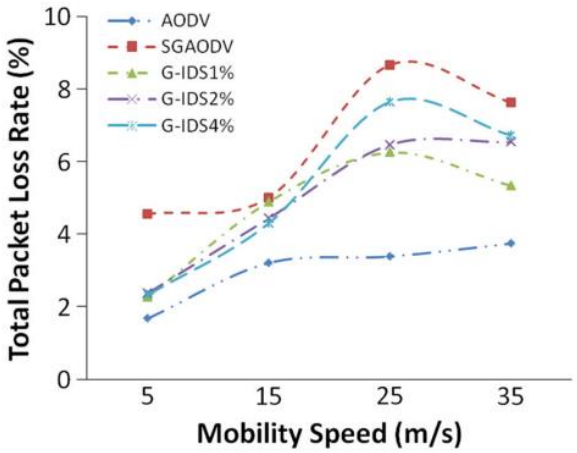
شکل8:PDR تحت یک گره مخرب



شکل9:PDR تحت دو گره مخرب



شکل10: نرخ اتلاف بسته تحت یک گره مخرب



شکل11: نرخ اتلاف بسته تحت دو گره مخرب

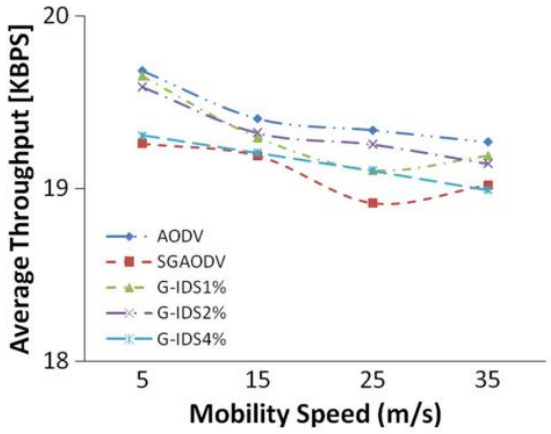
5.4. توان عملیاتی میانگین

می توان از شکل 12 دید که توان عملیاتی میانگین و در زمانی که گره مخرب وجود ندارد، برای همه ی سرعت های تحرک بوسیله ی AODV در حدود 19.42 kbps است. زمانی که حمله ی حفره ی خاکستری (SGAODV) راه اندازی می شودتوان عملیاتی میانگینِ SAODV در حدود 19.09 kbps است. این موضوع به علت رفتار معمولی آن در شناسایی مسیر به جای کنارگذاری بسته ی بسته های داده است. زمانی که رویکرد پیشنهاد شده در G-IDS به کار گرفته می شود، توان عملیاتی میانگین برای همه ی سرعت های تحرک در زمانی که مقدار آستانه ی کنارگذاری بسته 1 و 2 و 4٪ از کل بسته های داده تنظیم می شود، به ترتیب برابر با 19.30 و 19.32 و 19.15 kbps است. می توان در شکل 13 دید که وقتی دو گره مخرب در شبکه وجود دارد، توان عملیاتی میانگینِ SGAODV در حدود 18.75 kbps است. زمانی که رویکرد پیشنهادی استعمال می شود، توان عملیاتی میانگین برای همه ی سرعت های تحرک در زمانی که مقدار آستانه ی کنارگذاری بسته 1 و 2 و 4٪ از کا بسته های داده تنظیم می شود، به ترتیب برابر با 19.07 و 19.02 و 18.93 kbps است از گراف می توان دید که مکانیزم ما قادر به بهبود دادن توان عملیاتی میانگینِ شبکه تحت حمله ی حفره ی خاکستری هوشمند است.

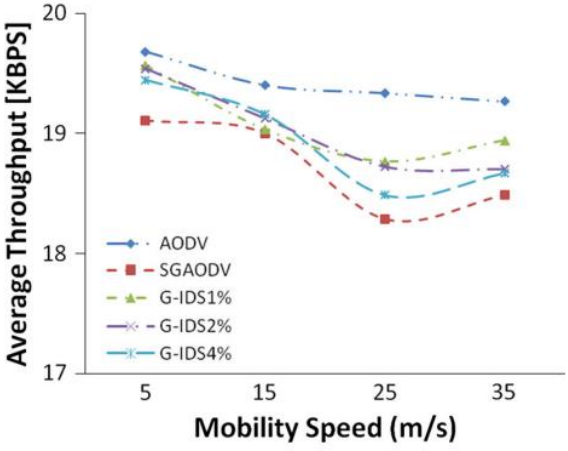
5.5. مازاد مسیر یابی

شکل 14 نشان می دهد که مازاد مسیریابی با افزایش سرعت تحرک، افزایش می یابد. مازاد مسیریابی میانگین در زمانی که گره مخربی وجود ندارد، برای همه ی سرعت های تحرک بوسیله ی AODV در حدود 4600 بسته هی کنترل است. زمانی که حمله ی حفره ی خاکستری (SGAODV) راه اندازی می شود، مازاد مسیریابی میانگینِ SAODV در حدود 4664 بسته ی کنترل است. زمانی که رویکرد پیشنهاد شده در G-IDS به کار گرفته می شود، مازاد مسیریابی میانگین برای همه ی سرعت های تحرک در زمانی که مقدار آستانه ی کنارگذاری بسته 1 و 2 و 4٪ از کل بسته های داده تنظیم می شود، به ترتیب در حدود 4694 و 4753 و 4549 بسته ی کنترل است. همچنین از شکل 15 می توان دید که مازاد مسیریابی میانگین در مواردی که دو گره مخرب حضور دارد، با افزایش سرعت

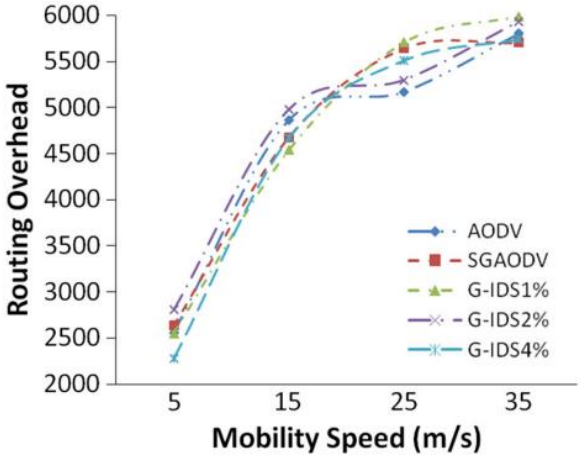
تحرک، افزایش می یابد. زمانی که دو گره هوشمند مخرب در شبکه وجود دارد، مازاد مسیریابی میانگینِ SGAODV در حدود 4734 است. زمانی که رویکرد پیشتنهاد شده در G-IDS استفاده می شود، مازاد مسیریابی میانگین برای همه ی سرعت های تحرک در زمانی که مقدار آستانه ی کنارگذاری بسته روی 1 و 2 و 4٪ از کل بسته های داده تنظیم می شود، به ترتیب در حدود 4837 و 4766 و 4686 بسته ی کنترل است. از گراف می توان دید که با افزایش سرعت تحرک، مازاد مسیریابی رویکرد پیشنهادی نیز افزایش می یابد و به طور موازی با مقدار استاندارد AODV حرکت می کند.



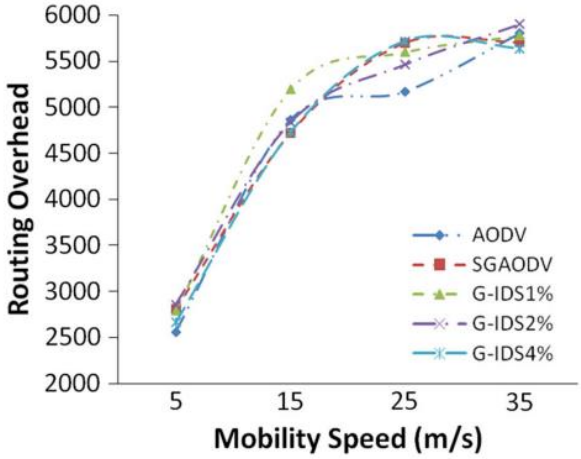
شکل12: توان عملیاتی میانگین تحت یک گره مخرب



شکل13: توان عملیاتی میانگین تحت دو گره مخرب



شکل14: مازاد مسیر یابی تحت یک گره مخرب

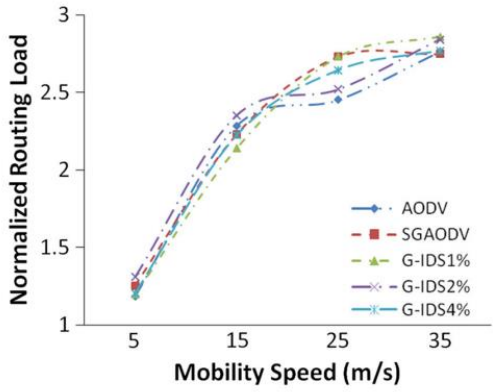


شکل15: مازاد مسیر یابی تحت دو گره مخرب

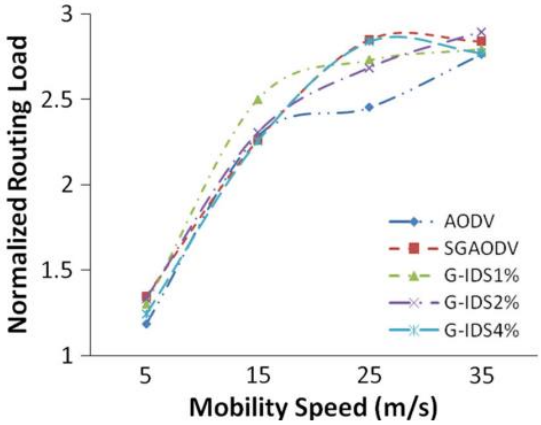
5.6. بار مسیر یابی نرمالیزه شده

شکل 16 نشان می دهد که مازاد مسیریابی نرمالیزه شده با افزایش سرعت تحرک گره ها افزایش می یابد. بار مسیریابی نرمالیزه شده ی میانگین در زمانی که گره مخربی وجود ندارد، برای همه ی سرعت های تحرک بوسیله ی AODV در حدود 2.17 است. زمانی که حمله ی حفره ی خاکستری (SGAODV) راه اندازی می شود، بار مسیریابی نرمالیزه شده ی میانگین در حدود 2.24 است. زمانی که رویکرد پیشنهاد شده در G-IDS به کار گرفته می شود، بار مسیریابی نرمالیزه شده ی میانگین در زمانی که مقدار آستانه ی کنارگذاری بسته روی 1 و 2 و 4٪ از

کل بسته های داده تنظیم می شود، به ترتیب در حدود 2.23 و 2.25 و 2.21 است. همچنین می توان در شکل 17 دید که بار مسیریابی نرمالیزه شده ی میانگین در هنگام حضور دو گره مخرب، با افزایش سرعت تحرک افزایش می یابد. در زمانی که دو گره مخرب هوشمنددر شبکه وجود دارد، مازاد مسیریابی نرمالیزه شده ی میانگینِ SGAODV در حدود 2.34 است. زمانی که رویکرد پیشنهاد شده استفاده می شود، بار نرمالیزه شده ی میانگین برای همه ی سرعت های میانگین در زمانی که مقدار آستانه ی کنارگذاری بسته روی 1 و 2 و 4٪ از کل بسته های داده تنظیم می شود، به ترتیب در حدود 2.33 و 2.30 و 2.27 است. از گراف می توان دید که با افزایش سرعت تحرک، بار مسیریابی نرمالیزه شده ی رویکرد پیشنهاد شده نیز افزایش می یابد و به طور موازی با مقدار استاندارد AODV حرکت می کند.



شکل16: مازاد مسیر یابی نرمالیزه شده تحت یک گره مخرب



شکل17: مازاد مسیر یابی نرمالیزه شده تحت دو گره مخرب

جدول 4: نرخ TP و FP برای یک گره مخرب

N	TP (%)	FP (%)
1	45	0.8
2	40	0.6
4	35	0

جدول 5: نرخ TP و FP برای دو گره مخرب

N	TP (%)	FP (%)
1	40	1.2
2	35	0.8
4	30	0

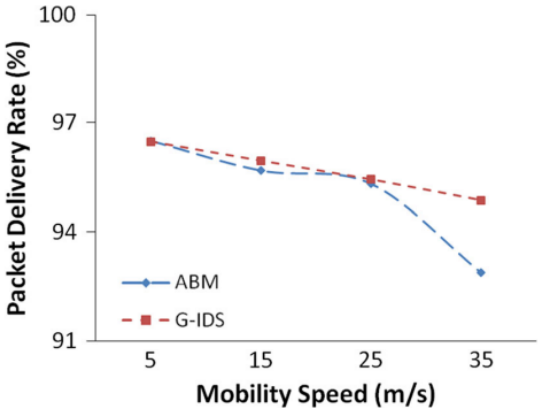
5.7. نرخ مثبت واقعی و نرخ مثبت غلط

به منظور انتخاب مقدار آستانه ی کنارگذاری بسته ی بهینه ، در ادامه میانگین نرخ مثبت واقعی و نرخ مثبت غلط را برای همه ی سرعت های تحرک محاسبه کردیم. هنگامی که 1 درصد از کل بسته های داده به عنوان مقدار آستانه در نظر گرفته می شوند، یافته شد که نر مثبت واقعی در حدود 45 درصد و نرخ مثبت غلط در حدود 0.8 درصد است. هنگامی که مقدار آستانه را روی 2 درصد از بسته های داده ی کل تنظیم کردیم، یافته شد که تحت یک گره مخرب نرخ مثبت واقعی در حدود 35 درصد و نرخ مثبت غلط در حدود صفر درصد است که در جدول 4 نشان داده شده اند. در هنگام وجود دو گره بدنهتد، هنگامی که مقدار آستانه روی 1 درصد از بسته های داده ی کل تنظیم می شود، یافته شد که نرخ مثبت واقعی در حدود 40 درصد و نرخ مثبت غلط در حدود 1.2 درصد است و هنگامی که مقدار آستانه را روی 2 درصد از بسته های داده ی کل تنظیم کردیم، نرخ مثبت واقعی در حدود 35 درصد و نرخ مثبت غلط در حدود 0.8 درصد است. هنگامی که 4 درصد از بسته های داده ی کل به عنوان مقدار آستانه در نظر گرفته می شود (تحت وجود دو گره مخرب) نرخ مثبت واقعی در حدود 30 درصد و نرخ مثبت غلط در حدود صفر

درصد است که در جدول 5 نشان داده شده اند. با توجه به جداول 4 و 5، می توان نتیجه گرفت که مقدار بهینه برای N 4 است. برای مثال، مقدار آستانه ی کنارگذاری بسته 4 درصد از بسته های داده ی کل است.

6. مقایسه ی عملکرد با طرح موجود

در این بخش، عملکرد رویکرد ما با طرح موجود ABM مقایسه شده است. مقایسه با طرح موجود بوسیله ی مقدار بهینه ی آستانه ی کنارگذاری بسته ی 4 درصد از بسته های داده ی کل در رویکرد ما انجام داده شده است.



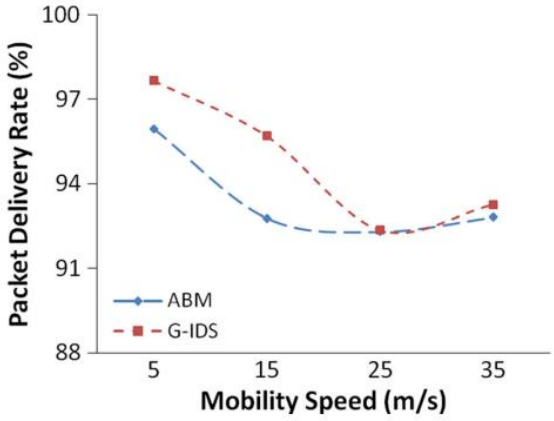
شکل18:PDR تحت یک گره مخرب

6.1. نرخ انتقال بسته

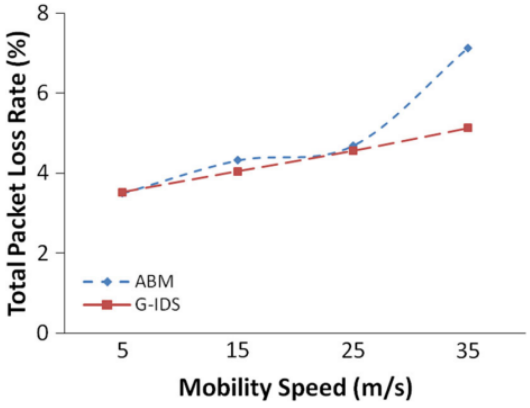
در شکل 18 دیده می شود که میانگین PDR برای همه ی سرعت های تحرک برای ABM و در حضور یک گره مخرب حفره ی خاکستری هوشمند در حدود 95.02 درصد است در حالیکه برای رویکر پیشنهاد داده شده، میانگین PDR برای همه ی سرعت های تحرک در حدود 95.68 در صد است. همچنین در شکل 19 دیده می شود که وقتی دو گره مخرب حفره ی خاکستری هوشمند در شبکه وجود داشته باشد، PDR برای ABM در حدود 93.45 درصد است در حالیکه میانگین PDR برای رویکرد پیشنهادی و برای همه ی سرعت های تحرک در حدود 94.74 درصد است. از این گراف نتیجه گرفته می شود که مکانیزم ما در مقایسه با ABM عملکرد بهتری دارد.

6.2. نرخ اتلاف بسته

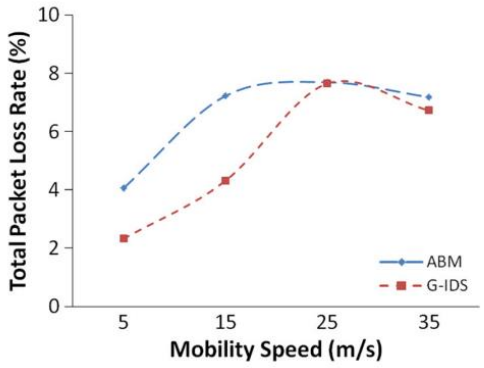
در شکل 20 دیده می شود که نرخ میانگین اتلاف بسته برای همه ی سرعت های تحرک در روش ABM و در حضور یک گره مخرب حفره ی خاکستری هوشمند در حدود 4.97 درصد است در حالیکه برای رویکرد پیشنهاد شده، نرخ میانگین اتلاف بسته برای همه ی سرعت های تحرک در حدود 4.31 درصد است. همچنین می توان در شکل 21 دید که وقتی دو گره مخرب حفره ی خاکستری هوشمند در شبکه وجود داشته باشد، نرخ میانگین اتلاف بسته برای روش ABM در حدود 6.54 درصد است، در حالیکه برای رویکرد پیشنهاد شده، نرخ میانگین اتلاف بسته برای همه سرعت های تحرک در حدود 5.26 درصد است. از این گراف می توان نتیجه گرفت که مکانیزم ما در مقایسه با ABM اتلاف کمتری دارد.



شکل19: PDR تحت دو گره مخرب



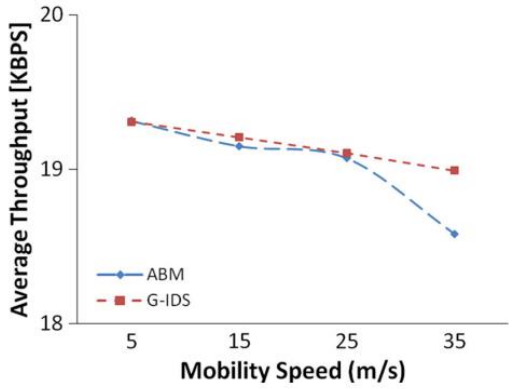
شکل20: نرخ اتلاف بسته تحت یک گره مخرب



شکل21: نرخ اتلاف بسته تحت دو گره مخرب

6.3. توان عملیاتی میانگین

می توان در شکل 22 دید که توان عملیاتی میانگین برای همه ی سرعت های تحرک و در حضور یک گره مخرب هوشمند برای ABM در حدود Kbps 19.03 است در حالیکه برای رویکر پیشنهاد شده، توان عملیاتی میانگین برای همه ی سرعت های حرکت در حدود Kbps 19.15 است. همچنین در شکل 23 می توان دید که وقتی دو گره مخرب حفره ی خاکستری هوشمند در شبکه وجود داشته باشد، توان عملیاتی میانگین برای ABM در حدود 18.69 درصد است در حالیکه برای رویکرد پیشنهاد شده، توان عملیاتی میانگین برای همه ی سرعت های حرکت در حدود 18.93 درصد است. از این گراف می توان نتیجه گرفت که مکانیزم ما در مقایسه با ABM توان عملیاتی بهتری دارد.



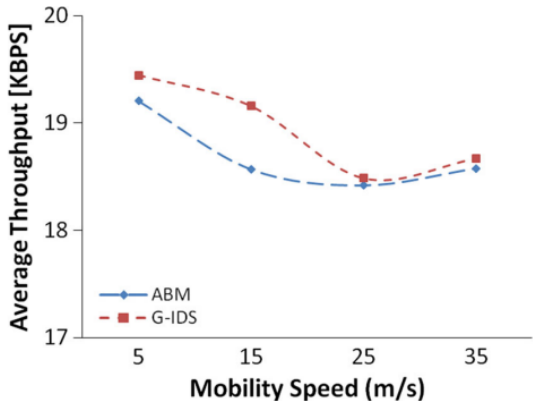
شکل22: توان عملیاتی میانگین تحت یک گره مخرب

6.4. مازاد مسیر یابی

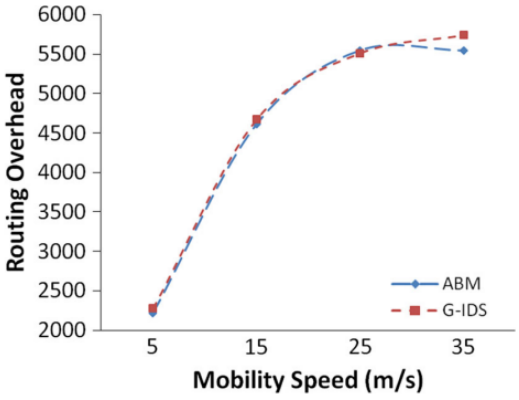
شکل 24 نشان می دهد که مازاد مسیریابی با افزایش سرعت تحرک، افزایش می یابد. مازاد میانگین مسیریابی برای همه ی سرعت های تحرک و در حضور یک گره مخرب حفره ی خاکستری هوشمند برای ABM در حدود 4482 بسته ی کنترل است در حالیکه برای رویکرد پیشنهادی، مازاد میانگین مسیریابی برای همه ی سرعت ها در حدود 4549 بسته ی کنترل است. همچنین از شکل 25 می توان دید که مازاد مسیریابی در هنگامی که دو گره مخرب حفره ی خاکستری هوشمند وجود داشته باشد، با افزایش سرعت تحرک، افزایش می یابد. هنگامی که دو گره مخرب حفره ی خاکستری هوشمند در شبکه وجود داشته باشد، مازاد میانگین مسیریابی برای ABM در حدود بسته ی کنترل4416 است در حالیکه برای رویکرد پیشنهادی، مازاد میانگین مسیریابی برای همه ی سرعتهای تحرک در حدود 4686 بسته ی کنترل است. افزایش اندک در مازاد مسیریابی در رویکرد پیشنهادی ما ناشی از مخابره ی بسته های هشدار در شبکه است.

6.5. بار مسیریابی نرمالیزه شده

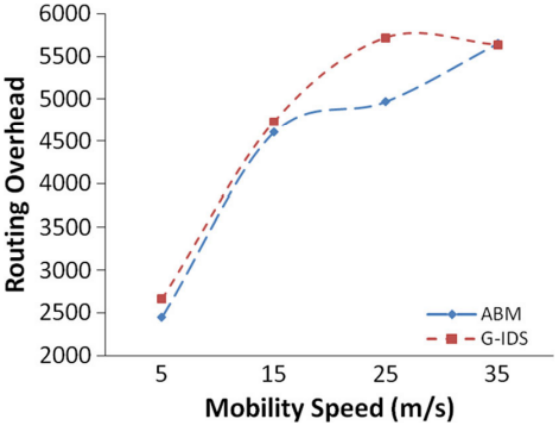
شکل 26 نشان می دهد که مازاد مسیر یابی نرمالیزه شده با افزایش در سعت تحرک، افزایش می یابد. NRL میانگین برای همه ی سرعت ها و در حضور یک گره مخرب حفره ی خاکستری هوشمند، برای ABM در حدود 2.18 است در حالیکه برای رویکرد پیشنهاد شده، NRL پیشنهادی برای همه ی سرعت های تحرک در حدود 2.21 است. همچنین از شکل 27 می توان دید که NRL میانگین در زمان حضور دو گره مخرب حفره ی خاکستری هوشمند، با افزایش سرعت تحرک، افزایش می یابد. هنگامی که دو گره مخرب حفره ی خاکستری هوشمند در شبکه وجود داشته باشد، NRL میانگین برای همه ی سرعت های تحرک، برای ABM در حدود 2.14 است در حالیکه برای همه ی سرعت های تحرک، برای رویکرد پیشنهادی در حدود 2.27 است.



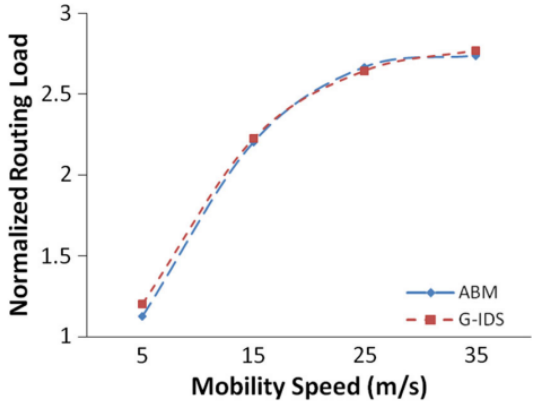
شکل23: توان عملیاتی میانگین تحت دو گره مخرب



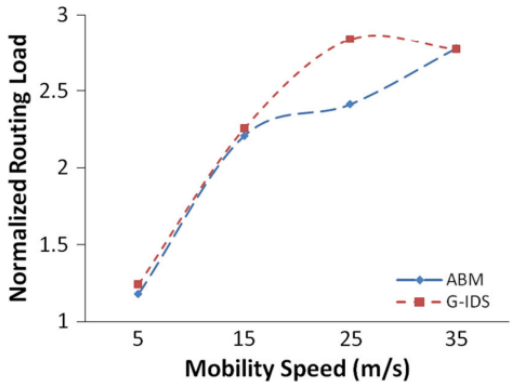
شکل24: مازاد مسیر یابی تحت یک گره مخرب



شکل25: مازاد مسیر یابی تحت دو گره مخرب



شکل26: مازاد مسیر یابی نرمالیزه شده تحت یک گره مخرب



شکل27: مازاد مسیر یابی نرمالیزه شده تحت دو گره مخرب

6.6. نرخ مثبت واقعی و نرخ مثبت غلط

برای G-IDS، وقتی یک گره مخرب حفره ی خاکستری هوشمند در شبکه وجود داشته باشد، TP 35 درصد و FP صفر درصد است درحالیکه برای AMB ، TP صفر درصد و FP صفر درصد است. هنگامی که دو گره مخرب حفره ی خاکستری هوشمند وجود داشته باشد، TP برای G-IDS 30 درصد و نرخ FP صفر درصد است درحالیکه همانطور که در جدول 6 نشان داده شده، برای AMB ، TP صفر درصد و FP صفر درصد است.

7. مزایا و معایب رویکرد پیشنهاد شده

رویکرد پیشنهاد شده مزایای پیش رو را دارا می باشد: 1) می تواند حمله ی حفره ی خاکستری هوشمندی را اداره کند که درآن گره مخرب به درستی در شناسایی مسیر به درستی شرکت می کند و در ادامه بسته های داده ی انتخابی را کنار می کذارد در حالیکه طرح های موجود در ادبیات علمی در دسترس، حمله ی حفره ی خاکستری بر مبنای شماره دنباله را اداره می کنند که گره حفره ی خاکستری پاسخ مسیر اشتباه می دهد و بسته های داده ی گزینشی را کنار می گذارد، در نتیجه نمی تواند حمله ی حفره ی خاکستری هوشمند را مدیریت کند. 2) رویکرد پیشنهاد شده ی ما می تواند حمله ی حفره ی خاکستری بر مبنای شماره دنباله را اداره کند چون اگر کنارگذاری بسته های داده بزرگتر از مقدار آستانه باشد، گره های G-IDS دیگر گره ها در شبکه را درباره ی هویت گره مخرب آگاه می کنند. 3) رویکرد پیشنهاد شده نه تنها گره های مخرب را شناسایی می کند بلکه این گره ها را بوسیله ی مشخص کردن هویت آن برای دیگر گره ها در شبکه، برای همیشه جدا می کند. 4) رویکرد ما از هیچگونه بسته ی کنترل اضافی برای شناسایی گره های مخرب در شبکه استفاده نمی کند. رویکرد پیشنهاد شده دارای معایب پیش رو می باشد: 1) گره های G-IDS ،گره های خاص هستند که باید در شبکه به درستی قرار داده شوند، باید به طریقی باشند که حداقل یک G-IDS در محدوده ی تراکنش ان باشد تا بسته ی هشدار را در شبکه به یکدیگر ارسال کنند. اگر مهاجم حفره ی خاکستری به علت جایگذاری نامناسب این گره های خاص، خارج از محدوده ی گره G-IDS باشد لذا مهاجم حفره ی خاکستری شناسایی و مسدود نخواهد شد. 2) این گره های خاص در شبکه ثابت می شوند و به همین دلیل نمی توانند جا به جا شوند 3) گره های G-IDS باید به طریقی جایگذاری شوند که بیشتر محدوده ی شبیه سازی را پوشش دهند 4) با افزایش اندازه ی محدوده ی شبکه، تعداد بیشتری از این گره های خاص نیاز می شود تا پوشش بیشینه ی سطح شبکه را داشته باشند.

8. نتیجه گیری

در یک MANET، گره ها با یکدیگر همکاری می کنند تا ارتباط چند هاپی را بین منبع و مقصد فراهم کنند. اما برخی گره ها وجود دارند که در ارسال بسته های داده همکاری نمی کنند و کنارگذاری انتخابی بسته را اجرا می کنند که به عنوان حمله ی حفره ی خاکستری شناخته می شود. حمله ی حفره ی خاکستری می تواند بر مبنای دنباله یا هوشمند باشد. در زمانی که بر پایه ی دنباله باشد، گره حفره ی خاکستری پاسخ مسیر غلط می دهد تا از این رو ترافیک را به سمت خودش جذب کند و کنارگذاری بسته ی انتخابی را اجرا می کند اما در زمان حمله ی حفره ی خاکستری هوشمند، مهاجم به طور عادی در شناسایی مسیر شرکت می کند و بعد از گرفتن داده از گره های منبع، کنارگذاری بسته ی انتخابی را اجرا می کند. به منظور اداره کردن حمله ی حفره ی خاکستری هوشمند، مکانیزم جدید MGAM را پیشنهاد دادیم که اثر حمله ی حفره ی خاکستری هوشمند را کم می کند. نتایج شبیه سازی نشان می دهد که مکانیزم پیشنهاد شده ی ما عملکرد شبکه را به لحاظ PDR، PLR و توان عملیاتی میانگین بهبود می بخشد. به طو.ر عملی اثبات کردیم که مقدار آستانه ی بهینه ی شده ی کنارگذاری بسته در چهار درصد از بسته های داده ی کل بهترین انتخاب است چون نرخ شناسایی گره های مخرب حداقل 30 درصد و با صفر درصد نرخ مثبت غلط در شبکه است. علاوه بر این، طرح خودمان را با طرح موجود مقایسه کردیم که نشان داد طرح ما در مقایسه با طرح موجود، از لحاظ PDR، PLR و توان عملیاتی میانگین اندکی بهتر است.

به عنوان کار آینده، تصمیم داریم تا این رویکرد را با طراحی یک مکانیزم جدید بهبود ببخشیم که در این مکانیزم جدید، هیچ گره خاصی به کار برده نشود و گره های متحرک به صورت پویا، به عنوان گره های خاص انتخاب شوند که عملکرد گره های G-IDS را خواهند داشت و همچنین اکثر محدوده ی شبیه سازی را پوشش خواهند داد.

References

1. Funde, R., & Chandre, P. (2015). Dynamic cluster head selection to detect gray hole attack using intrusion detection system in MANETs. In Proceeding of ICCCT '15, ACM, September 25–27, 2015. Allahabad, India. http://dx.doi.org/10.1145/2818567. 2818581.

2. Murthy, C. S. R., & Manoj, B. S. (2004). Ad hoc wireless networks: Architectures and protocols. Prentice Hall PTR.

3. Sharma, B. (2015). A distributed cooperative approach to detect gray hole attack in MANET. In Proceeding of WCI, ACM, Kochi, India. http://dx.doi.org/10.1145/2791405.2791433.

4. Deng, H. M., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communication Magazine, 40(10), 70–75.

5. Perkins, C. E., Beliding-Royer, E., & Das, S. (2004). Ad hoc ondemand distance vector (AODV) routing. IETF Internet Draft, MANET working group.

6. Johnson, D. B., Maltz, D. A., & Hu, Y-C. (2004). The dynamic source routing protocol for mobile ad-hoc network (DSR). IETF Internet Draft.

7. Heydari, V., & Yoo, S.-M. (2015). E2EACK: An end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs. Springer Wireless Network, New York. doi:10.1007/s11276-015-1098-6.

8. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). DoS attacks in mobile ad hoc networks: A survey. In IEEE 2nd International Conference on Advanced Computing & Communication Technologies.

9. Shila, D. M., Cheng, Y., & Anjali, T. (2010). Mitigating selective forwarding attacks with a channel-aware approach in WMNs. IEEE Transactions on Wireless Communications, 9(5), 1661–1675.

10. Jhaveri, R. H., & Patel, N. M. (2015). A sequence number based bait detection scheme to thwart gray hole attack in mobile ad hoc networks. Springer Wireless Network, 21, 2781–2798. doi:10. 1007/s11276-015-0945-9.

11. Vani, A., & Jadhao, M. M. (2013). Eliminating co-operative black hole and gray hole attacks using modified EDRI table in MANET. In Proceeding of IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 944–948.

12. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Elsevier Computers and Electrical Engineering, 40, 530–538.

13. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000) Mitigating routing misbehavior in mobile adhoc networks. In Proceedings of MOBICOM'2000, pp. 255–265.

14. Ramaswamy, S., Fu, Hu., Sreekantaradhya, M., Dixon, J., & Nygard, K. (2003). Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of ICWN'03, pp. 570–575.

15. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack. Springer Wireless Network. doi:10.1007/s11276-015-1032-y.

16. Gurung, S., & Saluja, K. K. (2014). Mitigating impact of blackhole attack in MANET. In Proceedings 5th International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 229–237. doi: 02.ITC.2014.5.560.

17. Banerjee, S. (2008). Detection/removal of cooperative black and gray hole attack in mobile ad hoc networks. In Proceedings of the World Congress on Engineering and Computer Science, WCECS, October 22–24, SanFrancisco, USA.

18. Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Elsevier Computer Communication.

19. Sen, J., Chandra, M. G., Reddy, H., & Balamuralidhar, P. (2007). A mechanism for detection of gray hole attack in mobile ad hoc network. In Proceedings of the IEEE ICICS.

20. The network simulator-ns-2. (2015). http://www.isi.edu/nsnam/ ns/.