دوره دوازدهم، شماره اول، بهار و تابستان۱۳۹۸
مجله فناوری اطلاعات در طراحی مهندسی
Information Technology in Engineering Design
http://ited.sinaweb.net

بهینه‌سازی الگوریتم مسیریابی AODV به‌منظور شناسایی گره‌های مزاحم و جلوگیری از بروز حملات سیاه‌چاله در شبکه‌های حسگر بی‌سیم

محسن عبدالرضایی* [(۱)] شمس الله قنبری [(۱)]

(۱) گروه مهندسی کامپیوتر، واحد آشتیان، دانشگاه آزاد اسلامی، آشتیان، ایران.*

(تاریخ دریافت: ۱۳۹۸/۶/۱۷ تاریخ پذیرش: ۱۳۹۸/۱۰/۱۷)

چکیده

شبکه حسگر بی‌سیم(WSN)، دربرگیرندهمجموعه‌ایی از گره‌های حسگر است که به‌صورت تصادفی در ناحیه تحت نظارت توزیع‌شده‌اند و از طریق ارتباطات رادیویی با همدیگر در ارتباط هستند.AODVیک پروتکل مسیریابی برحسب تقاضا در WSN است و فرآیند کشف مسیر میان فرستنده و گیرنده را فقط زمانی که به آن نیاز باشد انجام می‌دهد. این پروتکل علی‌رغم دارا بودن سربار محاسباتی و مسیریابی بسیار کم، به‌شدت در معرض حمله سیاه‌چاله قرار دارد. در این مقاله روشیبه‌منظور بهبود عملکرد پروتکل AODV در برابر حملات سیاه‌چالهارائه‌شده است. روش پیشنهادیارائه‌شده دارای دو فاز به نام‌های فاز تشخیص گره مزاحم و فاز کنار گذاشتن آن از روند مسیریابی در شبکه حسگر بی‌سیم است. نتایج حاصل از شبیه‌سازی‌هایانجام‌شده نشان می‌دهند که روش پیشنهادی در مقایسه با پروتکل‌های مسیریابیAODV و DSR توانسته است در حضور چندین گره مزاحم در پارامترهای سنجش کارایی نظیر توان عملیاتی، تأخیر انتها به انتها، نرخ تحویل بستهو تعداد بسته‌هایازدست‌رفتهعملکرد بسیار خوبی را ثبت کند.

واژه‌های کلیدی: پروتکل مسیریابی، شبکه‌های حسگر بی‌سیم، حمله سیاه‌چاله، AODV

* عهده‌دار مکاتبات:
نشانی: تهران، جردن، خیابان بابک بهرامی، پلاک ۱۱، طبقه اول، مرکز کنترل عملیات شبکه.
تلفن: ۰۹۱۲۵۲۷۱۳۷۶ **پست الکترونیکی:***m_abdolrezaei@yahoo.com*

1.مقدمه

نسل بشر همواره به دنبال آن بوده است تا بتواند کارها و فعالیت‌های خود را به ایمن‌ترین و سریع‌ترین روش انجام دهد تا بتواند ضمن استفاده بهینه از منابع (انسانی و مالی و تجهیزات فنی و...) به بهترین کارایی ممکن دست یابد. به وجود آمدن شبکه‌های کامپیوتری و مشخصاً شبکه‌های بی‌سیم توانسته است تا حد زیادی انسان‌ها را دررسیدن به اهدافشان یاری کند. در سال‌های اخیر، یکی از زیرمجموعه‌های مربوط به شبکه‌های بی‌سیم با عنوان شبکه‌های حسگر بی‌سیم(WSN) توانسته است تا حد بسیار زیادی ضمن تأمین امنیت لازم در محیط‌های خطرناک (مثل محیط‌های صنعتی، نظامی، کنترل و آنالیز آب‌وهوای مناطق مختلف)، کارایی و سرعت جمع‌آوری اطلاعات، آنالیز و تصمیم‌گیریفوق‌العاده‌ای‌ را نیز برای انسان‌ها به ارمغان آورد[۱،۲].

در شبکه‌های حسگر بی‌سیم، از چند گره حسگر بی‌سیم استفاده می‌شودبه‌صورت که هرکدام از آن‌ها با توجه به نوع مأموریتی که دارند، مجهز به چندین حسگر

(مثل حسگر دما، رطوبت، حسگرهای سنجش لرزه‌ای و...) هستند و به جمع‌آوری اطلاعات می‌پردازند. در این‌گونه شبکه‌ها، هر گره حسگر بعد از جمع‌آوری

اطلاعاتموردنیاز، آن‌ها را برای گره چاهکیا ایستگاه پایه ارسال می‌کند[۳] و سپس از طریقدستگاه‌های مخابراتی مختلف به مرکز کنترل مخابره می‌شود تا بتوان بر اساس آن‌ها تصمیمات سریعو لازم را اتخاذ کرد. به همین دلیل شبکه‌های حسگر بی‌سیم دارای کاربردهای فراوانی نظیرعملیات نظامی، امداد و نجات، فعالیت‌هایصنعتی، کنترل خطوط راه‌آهن، فعالیت‌های کشاورزی و موارد دیگر هستند[۱،۲،٤].

هر گره در شبکه حسگر بی‌سیم با توجه به ابعاد کوچکی که دارد و با توجه به آنکه غال با در محیط‌هاییبه‌کاربردهمی‌شوند که هیچ‌گونه بستر ارتباطی(شبکه‌های کامپیوتری) یاتغذیه‌ای‌ای (نیروی برق) وجود ندارد [۵]، معمولاً دارای قدرت محاسباتی،ذخیره‌سازی و تغذیه‌ای‌ای محدودیمی‌باشند. همچنین گره تا زمانیمی‌تواند در شبکه باقی بماند که انرژیتغذیه‌ای‌ای آن بهآن به پایان نرسیده باشد و درصورتی‌که انرژی گره به پایان برسد، پوشش ناحیه تحت نظارت آن‌ها با شکست مواجه می‌شود و ممکن است تبعات وخیمی را نیز به همراه داشته باشد؛ بنابراین صرفه‌جویی در مصرف انرژی این گره‌ها و نگه‌داشتن آن‌ها در شبکه

جزو چالش‌های اساسی موجود در شبکه‌های حسگر بی‌سیم است. چالش‌ها و مسائلی که باعث هدر رفتن انرژی شبکه‌های حسگر بی‌سیممی‌شوندمواردی نظیر تصادم، ازدحام ، تأخیرو نفوذ گره‌های مزاحم به شبکه می‌باشند.علاوه بر آنکه نفوذ گره‌های مزاحم به یک شبکه حسگر بی‌سیممی‌تواند سبب بالا بردن انرژی مصرفی شبکه و کاهش طول عمر آن‌ها شود، این چالش را می‌توان از نگاه امنیتی نیزموردتوجهقرارداد. درواقع نفوذ گره یا گره‌های مزاحم به شبکه می‌تواند سبب کاهش امنیت در شبکه نیز شود و قابلیت اطمینان آن را به‌شدت تحت تأثیر قرار دهد[٦].

در شبکه‌های حسگر بی‌سیم به علت عدم وجود توپولوژی ایستا و ثابت و متحرک بودن گره‌های حسگر، همواره این احتمال وجود دارد که گره‌هایی باهدف**ایجاد اختلال در عملکرد عادی شبکه به آن نفوذ کنند و از طریق پروتکل‌های مسیریابی همچون [7] AODVدر** مسیرهای

موجود میان دو گره مبدأ و مقصد شرکت کرده و بسته‌ها را بعد از دریافت از گره مبدأ به گره مقصد تحویل ندهند. ازاین‌رویکی از آن چالش‌هایی که در کنار بهینه‌سازی انرژی مصرفی شبکه‌های حسگر بی‌سیم از اهمیت فراوانی برخوردار است، افزایش امنیت شبکه و شناسایی گره‌های مزاحم و کنار گذاشتن آن‌ها از فعالیت در شبکه‌های حسگر بی‌سیم است[۱،۶،۸،۹].

پروتکل مسیریابیAODVیک پروتکل مسیریابی برحسب تقاضااست که در آن‌همه مسیرها فقط وقتی‌کهموردنیاز باشند کشف می‌شوند و تنها در طول مدتی که مورداستفاده قرار می‌گیرند نگهداریمی‌شوند. مسیرها در طول یک فرآیندسیل‌آساییکشف می‌شوند. هدف فرآیندسیل‌آسایی جستجوی مسیرهایی است که بین فرستنده و گیرنده قرار دارند. در طی این فرآینددرصورتی‌که مسیری میانمبدأ و مقصد کشف شود، اطلاعات مسیراستخراج‌شده به گره مبدأ برگردانده می‌شود تا بتواند بر اساس مسیرهایکشف‌شده بهترین مسیر را برای انتقال اطلاعات انتخاب کند[۸].

از اهداف اصلی پروتکل مسیریابیAODVمی‌توان به مواردی همچون حداقل سربار کنترلی، حداقل سربار پردازشی، قابلیتمسیریابی چند گامی، نگهداری پویای توپولوژی و عاری بودن مسیرهایاستخراج‌شده از حلقه اشاره کرد. درواقع این پروتکل به‌گونه‌ایطراحی‌شده است که بتواند از منابع محدود موجود در شبکه‌های متحرک موقتی استفاده بهینه نماید و ضمن کاهشسربارهایفوق‌الذکر کارایی شبکه را به حداکثر برساند. ازاین‌رو این پروتکل در حالت عادی و در مواقعی که حملات خاصی بر روی آن صورت نمی‌گیردمی‌تواند کارایی بسیار خوبی را از خود نشان دهد. پروتکل AODV در ساختار خود دارای دو فاز اصلی به نام‌های فاز کشف مسیر و فاز نگهداری مسیر است[۸].

در فرآیند کشف مسیر،هنگامی‌که بین گره‌هایمبدأ و مقصد مسیری معتبر و مورداطمینان وجود نداشته باشد، گره مبدأ بسته درخواست مسیر(RREQ)را به سمت گره مقصد در شبکه به‌صورت فراگیر منتشر می‌کند[۷،۸]. گره‌هایی که این بسته را دریافتمی‌کنند، ورودی مسیر برعکسیرا به سمت گره مبدأ ایجادمی‌کنند و آن را در جدول مسیریابی خود ثبت یابه‌روزمی‌کنند، بعد از انجام این کار گره هر که بسته RREQ را دریافت کرده است درصورتی‌که در جدول مسیریابی خود، مسیری به سمت گره مقصد داشته باشد، مسیر را به اطلاع گره فرستنده می‌رساند و در غیر این صورت بسته دریافتی را به‌منظور کشف مسیر در شبکه به‌صورت فراگیر منتشر می‌کند. اینروند تا زمانی که مسیریا مسیرهایی میان گره‌هایمبدأ و مقصد کشف شوند ادامه پیدامی‌کند. هنگامی‌که بسته RREQ از گره مبدأ به گره مقصد برسد، گره مقصد یک مسیر ورودیبرعکس به سمت گره مبدأ را ایجادمی‌کند و بسته پاسخ مسیر (RREP)را در مسیر برعکس به‌صورتتک‌پخشی به سمت گره مبدأ ارسال می‌کند. هنگامی‌که این بسته به گره مبدأمی‌رسد، مسیریروبه‌جلو توسط گره به‌روزیا ایجادمی‌شود و ارتباطات شروع می‌شود[۷].

به‌منظور آنکه پروتکل مسیریابیAODV از برقرار ماندنمسیرهای موجود در شبکه اطمینان حاصل کند به‌صورتمتناوب فاز نگهداری مسیر را اجرا می‌کند. در این فاز هر گره موجود در شبکه به‌صورت متناوب یک بسته Hello را برای تمام اتصالات محلی موجود در جدول مسیریابی خودش به‌صورت فراگیر ارسال می‌کند و بسته RREP را نیز همانند بسته Hello منتشر می‌کند. درصورتی‌که گره فرستنده بعد از گذشت مقدار زمان در

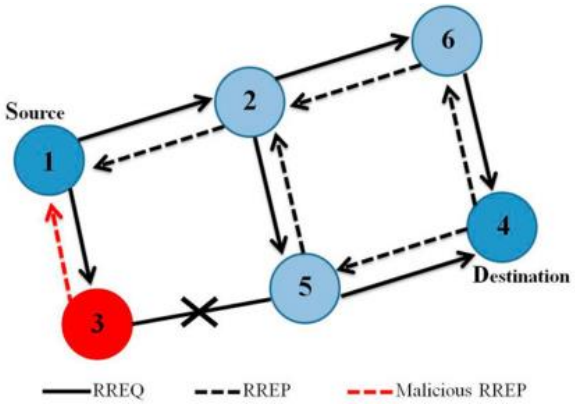
نظر گرفته‌شده برای پاسخ به پیام، پاسخی را از گره مجاورش دریافت نکند آن لینک را نامعتبر در نظر می‌گیرد. بدین ترتیب مسیری که گره با شکست مواجه شده در آن شرکت داشته است نامعتبر در نظر گرفته می‌شود.علاوه بر آن درصورتی‌که شکست لینک به گره مقیدنزدیک‌تر باشد (یعنی تعداد گام از نقطه شکست تا گره مقصد نسبت به گره مبدأ کمتر باشد) این مسیربه‌صورت کامل نادیده گرفته می‌شود و باید مسیر جدیدی برای ارتباط میان گره‌هایمبدأ و مقصد کشف شود[۷]. فرآیند کشف مسیر جدید بعد از شناسایی شکست لینک با عنوان تعمیر محلیشناخته می‌شود.

یکی از حملاتی که بر روی پروتکل مسیریابیAODV انجام می‌شود، حمله سیاه‌چاله است[۱۰]. حمله سیاه–چاله، حمله‌ای است که در آن گره مزاحم و خرابکار با انتشار اخبار دروغ داشتن بهترین مسیر، سعیمی‌کند ترافیک شبکه را به‌طرف خود جذب کند. این گره، پیام‌های جعلی را به‌گونه‌ای در شبکه منتشر می‌کند که در فرآیندمسیریابیبه‌عنوان کوتاه‌ترین مسیر میان گره گیرنده و فرستنده در نظر گرفته شود. حاصل این روند انتخاب گره مزاحم به‌عنوانبهینه‌ترین گره برایمسیریابی و ارسال داده‌ها از مبدأ به مقصد است. هنگامی‌که فرآیندمسیریابی به پایانمی‌رسد و گره مزاحم بسته‌هایداده‌ای گره فرستنده را دریافتمی‌کندبه‌جای آنکه بسته‌های داده‌های دریافت شده را به سمت گره گیرنده فورارد کند یا آن‌ها را به‌صورت کامل حذف می‌کند و یا اینکه داده‌های مخرب مدنظر خود را ارسال می‌کند[۹،۱۰،۱۱].

تصویر۱ نحوه انجام این حمله را در فرآیند کشف مسیر در پروتکل AODV نشان داده است. در این تصویر گره شماره ۱ گره فرستنده و گره شماره ٤ گره گیرنده است. مطابق با عملکرد پروتکل AODV، گره فرستنده با انتشار فراگیر بسته RREQ به دنبال مسیر مناسبی به گره ٤ است. گره‌های شماره ۲ و ۳ که در یک گامی گره گیرنده قرار دارند و به‌عنوان مجاوران مستقیم و تک گامی آن در نظر گرفته می‌شوند بسته RREQ را دریافتمی‌کنند، در حالت عادیهیچ‌یک از این دو گره (گره‌های۲ و ۳) مسیری به گره ٤ را نمی‌شناسند و باید مجدد بسته RREQ را در شبکه منتشر کنند، ازآنجایی‌که گره ۲یک گره عادی است بسته را مجدداً در شبکه منتشر می‌کند اما گره ۳ عملکردی خرابکارانه دارد و خود را به‌عنوانناندیک‌ترین مسیر به گره شماره ٤ و یک گامی آن معرفیمی‌کند و با تولید بسته جعلیRREP به گره فرستنده پاسخ می‌دهد. هنگامی‌که گره فرستنده مسیرهایمنتهی به گره گیرنده را دریافتمی‌کندبر اساس عملکرد الگوریتم،کوتاه‌ترین مسیر را در پیشمی‌گیرد و اطلاعات به سمت گره ۳ ارسال می‌شوند تا به سمت گره گیرنده فورارد شوند. این امر در حالی است که گره ۳ اطلاعات را پس از دریافت به سمت گره ٤ فورارد نمی‌کندو تمام بسته‌ها را حذف می‌کند[۱۰]با نگاهی به توضیحات فوق و بالا بودن اهمیتافزایش امنیت در چنین شبکه‌هایی، در این مقاله، بهینه‌سازی الگوریتم مسیریابیAODVبه‌منظور شناسایی گره‌های مزاحم و جلوگیری از بروز حملات سیاه‌چاله هدف قرار داده‌شده است تا بتوان با استفاده از آن ضمن شناسایی گره‌های مزاحم در شبکه و بالا بردن امنیت شبکه به معیارهایی نظیربهینه‌سازی انرژی مصرفی از طریق باز ارسال بسته‌هایحذف‌شده توسط گره‌های مزاحم،کارایی و قابلیت اعتماددست‌یافت.

این مقاله به‌صورت زیرسازماندهی‌شده است: در بخش دوم پژوهش‌های و مقالات ارائه‌شده در حوزه تشخیص نفوذ در

شبکه‌های حسگر بی‌سیمارائه‌شده است. بخش سوم روش پیشنهادی، بخش چهارم نتایج حاصل از شبیه‌سازی‌ها و مقایساتانجام‌شده را ارائه کرده است. نتایج کلی و اهداف آتی پژوهشی نیز به ترتیب در بخش‌های پنجم و ششم توضیحداده‌شده‌اند.



تصویر ۱. اجرای حملهBlackHole توسط گره مزاحم بر روی پروتکل مسیریابی[۱۰AODV]

۲. مروری بر کارهای مرتبط

به‌صورت کلیIDS را می‌توانبر اساسفن‌های تشخیصو معماریاستفاده‌شده بررسی و ارزیابی کرد. دسته‌بندی‌های مبتنی بر فن‌های تشخیص را می‌توان در سه دسته سیستم مبتنی بر امضاء [٦]، سیستم تشخیصناهنجاری[۱۲] و سیستم مبتنی بر خصوصیات[۱] تقسیم کرد. همچنین IDS مبتنی بر معماری را نیزمی‌توان در سه دسته معماریIDS خودکفا[۲]، IDSتوزیع‌شده و همکارانه[۵] و IDS سلسله مراتبی[٤،۱۳] تقسیم کرد.

در[٦] پژوهش‌هاییبررسی‌شده‌اند که برایدستگاه‌های مبتنی بر امضاء پیشنهادشده‌اند، ایندستگاه‌ها در دسته فن‌های تشخیص قرار می‌گیرند و در آن سیستم داراییک پایگاه داده است که در آن رفتار و عملکرد حملات اصلیقرارداده می‌شوند و اطلاعات جمع‌آوری‌شده با آن‌ها مقایسهمی‌شوند. درصورتی‌که داده جمع‌آوری‌شده با اطلاعاتی که در پایگاه داده وجود دارد، منطبق باشند، این رفتار به‌عنوان حمله در نظر گرفته می‌شود و پاسخ مناسب به آن داده می‌شود.

در[۱۲] سیستم تشخیصغیرمتعارفپیشنهادشده استکه در دسته فن‌های تشخیص قرار می‌گیرد و در آن هرگونه رفتاری که از رفتارهای استاندارد از پیشتعریف‌شده، تخطی کند به‌عنوان حمله در نظر گرفته می‌شود و عملیات لازم برای مقابله با آن اتخاذ می‌شود.

در[۱] نمونه دیگری از دستگاه‌هایIDS مبتنی بر تشخیصپیشنهادشده است که با عنوان سیستم مبتنی بر تشخیص شناخته می‌شود و در آن درمجموعه‌هایی از شروط در نظر گرفته می‌شود که بایدیک برنامه یا پروتکل بتواند آن‌ها را محقق کند درصورتی‌کهبرنامه یا پروتکل موردنظر توانایی تحقق این شروط را نداشته باشد به‌عنوان حمله در نظر گرفته می‌شود.

به‌هرحال علاوه بر دستگاه‌هایIDS مبتنی بر فن‌های تشخیص،دستگاه‌هایIDS مبتنی بر معماری نیز وجود دارند که برایتأمین امنیت در WSNپیشنهادشده‌اند. در [۲]معماریIDS خودکفا پیشنهادشده است که در آن گره‌ها با توجه به منابع محلی که در اختیاردارند اقدام به جمع‌آوری داده‌ها از سایر گره‌های دیگر موجود در شبکه می‌کنند و نفوذ را تشخیصمی‌دهند. در این معماریهیچ‌گونه اطلاعاتی میان گره‌ها ردوبدل نمی‌شود و گره‌ها نیزهیچ‌گونهاطلاعاتی نسبت به موقعیت گره‌های دیگر در شبکه ندارند؛ بنابراین نمی‌توانند نسبت به برخی حملات گسترده و توزیع‌شده واکنش خوبی را نشان دهند.

در[۵]معماریIDSتوزیع‌شده و همکارانه پیشنهادشده است. اساس و اصول این معماری تشخیص مبتنی بر همکاری و تعامل گره‌ها با یکدیگر در شناسایی و خنثی کردن حملات است. در این سیستم ابتدا گره‌ها کار

تشخیصی را به‌صورت انفرادی انجام می‌دهند و درصورتی‌که نتوانند تشخیص را انجام دهند آنگاه به‌صورت گروهی این کار انجام می‌دهند. به‌هرحالردوبدل کردن اطلاعات و هشدارها توسط گره‌ها در شبکه می‌تواند منجر به بالا بردن ترافیک شبکه و کاهش کارایی آن شود.

در[IDS۱۳،۳] سلسله مراتبپیشنهادشده است. این روش‌ها با در نظر گرفتن مشکل معماری‌های همکارانه گره‌های موجود در شبکه را به کلاستر یاگروه‌های کوچکی تقسیمکرده‌اند و سپس برایهرکدام از آن‌ها هد کلاستری را انتخاب کرده‌اند تا بتوانند عملیات تشخیص را در هر کلاستر و با محوریت هد کلاستر انجام دهند و در صورت تشخیص حمله آن را به سایر هد کلاسترهای دیگر انتشار دهند و کل شبکه را آگاه کنند. در ایندستگاه‌هابه‌منظور کاهش ارتباط میان گره‌ها، هشدارها به‌صورت سلسله مراتبی و بر اساس میزان شدت آن‌ها بررسیمی‌شوند. در این صورت ردوبدل شدن اطلاعات میان گره‌ها کاهش‌یافته و کارایی شبکه را نیز تحت تأثیر قرار نمی هند. به‌هرحال مشکلی که در این روش‌ها وجود دارد آن است که این روش با توجه به گروه‌بندی شبکه، قادر به بررسی و رویارویی با برخی از حملات توزیع‌شدهشبکه‌ای نیست.

در[۱۵] پژوهش و تحقیقی بر روی پروتکل مسیریابیAODVانجام‌شده است و روشیارائه‌شده است که هدف اصلی آن بهبود عملکرد پروتکل مسیریابیAODV از طریق کوتاه کردن مدت‌زمانیافتن مسیر مناسب و کاهش زمان تعمیر مسیرانتخاب‌شده بوده است. علی‌رغم آنکه روش پیشنهادی آنان توانسته است در معیارهایی نظیر نرخ تحویل بسته، تأخیر انتها به انتها و توان عملیاتی عملکرد بهتری را نسبت به پروتکل AODV از خود نشان دهد اما در آن هیچ‌گونه مکانیزی برای شناسایی نفوذ و جلوگیری از حملاتی نظیر حمله سیاه‌چاله ارائه نشده است و به‌شدت در هنگام چنین حملاتی با تنزل کارایی روبرو می‌شود.

به‌منظورایمن‌سازی پروتکل AODV در برابر حمله سیاه‌چاله در [۱٤] روشی برای مقابله با حمله سیاه‌چالهارائه‌شده است که اساس کار آن برای شناسایی گره مزاحم، جمع‌آوری نظر گره‌های دیگر درباره گره مظنون است. این روش هنگامی‌که شبکه حسگر بی‌سیم تحت حمله یک گره قرار دارد، روش مناسبی است. به‌هرحالهنگامی‌که شبکه حسگر بی‌سیم تحت حمله چند گره مزاحم قرار می‌گیرد، گره‌های مزاحم می‌توانند در هنگام رأی‌گیری به درست‌کار بودن گره هم‌رده خود رأی دهند و مانع از آن شوند که گره مزاحم اصلی شناسایی شوند، همچنینمی‌توانند به‌صورت گروهی به گره یا گره‌هایی که دارای عملکرد عادی هستند، رأی منفی دهند و آن را به‌عنوان گره مزاحم معرفی کنند. ازاین‌رو روش ارائه‌شده در[۱٤] قابلیت و توانایی رویارویی با چنین حملاتی را ندارد.

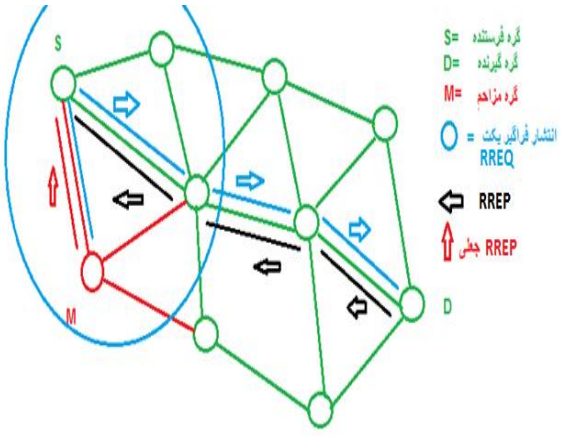
با در نظر گرفتن موارد فوق، محتوی این مقاله بر آن است تا بتواند با ارائه روشی جدید و بهینه، بر کیفیتدستگاه‌های تشخیص نفوذ سلسله مراتبی بیفزاید و مشکلات موجود در این‌گونهدستگاه‌ها را کاهش یا رفع نمایدبه‌صورت که بتواند ضمن شناسایی سریع گره‌های مزاحم و کنار گذاشتن آن‌ها از پروسه مسیریابی در شبکه‌های حسگر، سبب ارتقاء پارامترهای دیگری نظیر کاهش انرژی مصرفی گره‌ها (به علت باز ارسال بسته‌هایی که توسط گره‌های مزاحم از بینرفته‌اند انرژی مصرفی گره‌ها بالا می‌رود) و به حداکثر رساندن طول عمر شبکه، میزان نرخ تأخیر انتها به انتها ونرخ بسته‌های تحویلداده‌شدهدر شبکه شود.

۳. روش پیشنهادی

به‌منظور شناسایی و مجازات گره‌های مزاحم و بدرفتار موجود در شبکه، روش پیشنهادی دارای دو فاز به نام‌های فاز شناسایی گره بدرفتار و فاز حذف گره مزاحم است.

۳-۱. فاز شناسایی گره بدرفتار

هدف اصلی این فاز، شناسایی گره یا گره‌هایی است که در داخل شبکه خود را به‌عنوان‌نزدیک‌ترین مسیر به گره مقصد معرفیمی‌کنند و پس از دریافت ترافیک شبکه و بسته‌های ارسالی از سوی فرستنده، به‌جای فوراورد آن‌ها به سمت گیرنده، آن‌ها را از بینمی‌برند و سبب بروز اخلال در عملکرد شبکه می‌شوند. در ابتدا حالتی در نظر گرفته‌شده است که گره بدرفتار به شبکه نفوذ کرده است و پروتکل مسیریابیAODV در حال مسیریابی است. این روند در تصویر۲ نشان داده‌شده است.



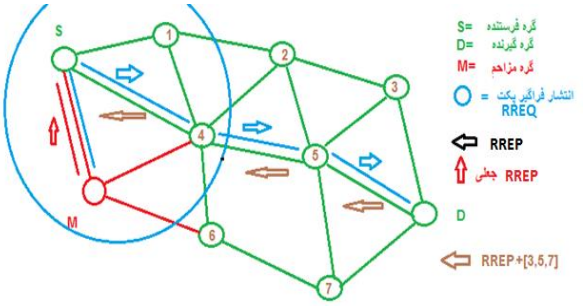
تصویر۲. عملکرد پروتکل مسیریابیAODV در زمان وجود گره مزاحم

همان‌طور که در تصویر۲ نشان داده‌شده است، گره S قصد کشف مسیر به سمت گره D را دارد ازاین‌رو با انتشار فراگیر بسته (RREQدایره آبی) از مجاوران تک گامی خود مسیر را درخواست می‌کند. در حالت عادی بسته RREQ در بین تمام گره‌ها منتشر می‌شود تا زمانی که به گره مقصد برسد (فلش‌های آبی). بعد از آن گره D با بسته (RREPفلش‌های سیاه) به فرستنده پاسخ می‌دهد تا مسیر شکل گیرد؛ اما در اینجا گره Mبه‌عنوان گره مزاحم با بسته RREP جعلی(فلش قرمز) به فرستنده پاسخ داده است و مسیر را به خود اختصاص داده است تا بتواند ترافیک را در دست گرفته و بسته‌های دریافتی از گره S را از بین ببرد.

همان‌طور که این تصویر نشان می‌دهد گره مزاحم بدون توجه به گره‌های دیگر، بسته RREP جعلی را تولید کرده است و این در حالی است که بسته RREQاصلاً به دست گره گیرنده نرسیده‌است تا بتواند با RREP به بسته دریافتی جواب دهد. در اینجابه‌منظورتائید آنکه بسته درخواست مسیرRREQ به دست گره گیرنده رسیده است و بسته پاسخ به مسیریابRREP که توسط فرستنده دریافت شده است، متعلق به گره گیرنده است، گره گیرنده اعمال زیر انجام می‌دهد:

-_ابتدا بسته RREP را تولیدمی‌کند.

-_ازآنجایی‌که هر گره، لیستمجاوران تک گامی خود را در اختیار دارد، گره گیرنده لیست مجاوران خود را به بسته RREQ ضمیمه کرده و از طریق همان مسیری که بسته RREQ را دریافت کرده است مسیر معکوس را ایجاد کرده و بسته RREP که حاوی اطلاعات مربوط به مجاوران تک گامی خود است را ارسال می‌کند. به‌صورتواضح‌تر در این مرحله، گره گیرنده در پاسخ به گره فرستنده، لیست مجاوران خود را نیز برای گره فرستنده ارسال می‌کند. (تصویر۳). الگوریتم۱ این روند را نشان داده است.



تصویر۳. اضافه کردن لیست مجاوران تک گامی گره گیرنده به بسته RREP

شروع
تولید بسته RREP
اضافه نمودن شناسه گره‌های تک گامی خود به بسته RREP
ارسال بسته به گره فرستنده از طریق مسیری که بسته درخواست مسیر (RREQ)را از آن دریافت کرده است.
پایان

الگوریتم۱.

اضافهنمودنگرههایتکگامیبهبستهRREPتوسطگرهگیرندهیاگرهمزاحم

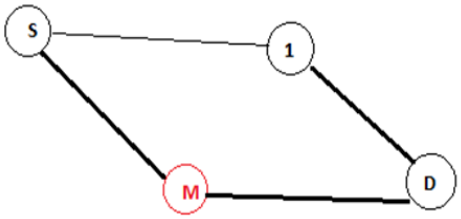
گره فرستنده به‌منظور انتخاب بهترین مسیر تا گیرنده، منتظر دریافت مسیرهای دیگرمی‌ماند. این مسیرهابه‌صورت زیر خواهند بود:

S-M-D
S-1-2-3-D
S-1-4-5-D
S-4-5-D
S-4-6-7-D
...

بعدازآنکهتمام‌مسیرهای منتهی به گره گیرنده در قالب بسته‌هایRREP به گره فرستنده می‌رسد، گره فرستنده پروسه انتخاب بهترین مسیر را آغاز می‌کند. این پروسه به شرح زیر است (انتخاب بهترین مسیر توسط گره فرستنده):

_حذف تمام‌مسیرهایی که در آن‌ها گره گیرندهبه‌عنوان مجاور تک گامی آمده است، ازآنجایی‌که گره فرستنده، انتظار دارد بسته RREP را از گره گیرنده دریافت کرده باشد، بنابراین نباید گره گیرنده خود را **به‌عنوان مجاور خودش معرفی کند. ازاین‌رو گره فرستنده تمام بسته‌هایی که در آن‌ها، گره گیرنده را به‌عنوان مجاوران تک گامی معرفیکرده‌اند، نادیدهمی‌گیرد. این روند در تصویر٤نشان داده‌شده است؛ کهدران گره Mبه‌عنوانتولیدکننده بسته جعلیRREP، گره D را به‌عنوانیکی از مجاوران خودش معرفیمی‌کند و این در حالی است که بسته تولیدکنندهRREP باید گره D باشد.**

-ازآنجایی‌که درخواست کشف مسیر از سوی گره فرستنده به‌سوی گره گیرنده به علت آن است که گره فرستنده به گره گیرندهدسترسی مستقیم ندارد و جزو مجاوران تک گامی آن به شمار نمی‌رود، لذا گره فرستنده انتظار ندارد که در لیستمجاوران تگ کای دریافتی از RREPهای مختلف، خودش به‌عنوان مجاور گره گیرنده بیاید. درصورتی‌که به همراه بسته RREP، خود گره فرستنده به‌عنوان مجاور تک گامی گره گیرندهمعرفی‌شده باشد، گره فرستنده این مسیر را نادیدهمی‌گیردچراکه در این حالت گره هی که بسته RREP را تولید کرده است خود را به‌عنوان مجاور تک گامی گره فرستنده معرفی کرده است. در صورت وجود چنین شرایطی، گره فرستنده نیازی به پروسه کشف مسیر نداشت و داده را برای گره گیرنده ارسال می‌کرد. ازاین‌رو گره هی که خود را در یک گامی فرستنده معرفی کرده است، گره مزاحم خواهد بود. این سناریو در تصویر٤ نشان داده‌شده است.



تصویر٤. عملکرد روش پیشنهادی در شناسایی گره مزاحم

در تصویر فوق، هنگام کشف مسیر توسط S به گره D، گره M بعد از دریافت بسته کشف مسیر از S، بدون انتقال آن به گره D، بسته جعلیRREP را تولیدمی‌کند و گره‌هایDو S را به‌عنوان مجاوران خود معرفیمی‌کند. در اینجا گره Sتولیدکننده بسته RREP را به‌عنوان گره مقصد در نظرمی‌گیرد و در لیست مجاوران آن گره، اسم خودش را مشاهده می‌کند. این بدان معناست که در حال حاضر گره D در یک گامی گره S است. با دیدن این حالت گره S مسیر را دیجکتمی‌کند.

با در نظر گرفتن دو شرط فوق، گره فرستنده تمام‌مسیرهایی که در آن‌ها مشخصات خودش یا گره گیرندهبه‌عنوان مجاور تک گامی آن مسیر آمده باشد را کنار می‌گذارد.

بعد از حذف مسیرهایی که دارای اشکالات زیر هستند پروسه انتخاب مسیر به شکل زیر انجام می‌شود، درواقع هدف دو گام قبلی مشخص کردن تمام‌مسیرهایی است که در آن‌ها خود گره گیرنده، بسته RREP را تولید و به گره فرستنده انتقال داده است:

_انتخاب کوتاه‌ترین مسیربرحسب تعداد گام، یعنی مسیر-S M-D.

_بررسی مجاوران ضمیمه‌شده به مسیر انتخابیبه‌عبارت‌دیگر گره فرستنده علاوه بربستهRREP، مجاوران گره D که به بسته RREP الحاق شده است را بررسیمی‌کند.

_مقایسه گره‌های مجاور ضمیمه‌شده به مسیر منتخب با سایر گره‌های مجاور ضمیمه‌شده به دیگر مسیرها

- اگر حاصل مقایسه، برابر نباشد، مسیر نامعتبر است و گره تولیدکننده بسته به‌عنوان گره مزاحم در نظر گرفته می‌شود و بهترین مسیر بعدی بررسیمی‌شود.

-اگر حاصل مقایسه برابر باشد، مسیر معتبر استو ارسال اطلاعات از طریق همان مسیر آغاز می‌شود.این روند در الگوریتم۲ نشان داده‌شده است.

۱. شروع
۲. انتخاب بهترین مسیر با دارا بودن کمترین گام تا گیرنده.
۳. لیست مجاوران مسیر برتر را بررسی کن
٤. اگر در لیست مجاوران مسیر برتر، گره فرستنده، گیرنده یا هردوی آن‌ها بود، مسیر را حذف کن و برو به ۷ در غیر این صورت برو به ۵
۵. لیست مجاوران مسیر برتر را با سایر مجاوران موجود در مسیرهای دیگر مقایسه کن،
٦. اگر حاصل مقایسه، منفی است برو به ۷ در غیر این صورت مسیر نهایی را ایجاد کن و ارسال اطلاعات را آغاز کن و برو ۱۰
۷. اطلاعات مسیر را حذف کن و تولیدکننده بسته RREP، گره مزاحم است.
۸. ارسال مشخصات شناسه گره مزاحم به فاز مقابله با نفوذ و حذف گره مزاحم.
۹. در صورت باقی ماندن مسیر بررسی نشده بعدی برو به ۲.
۱۰. پایان.

الگوریتم۲- فاز شناسایی گره بدرفتار توسط گره فرستنده

۳-۲. فاز حذف گره مزاحم

گره‌هایی که در فاز قبلی، دارای بسته‌هایRREP باشند که مشخصات گره‌های مجاور مربوط به گره‌های مقصد با سایر بسته‌هایRREP دیگر همخوانی نداشته باشند به این فاز فرستاده می‌شوند. در این فاز مشخصاتگره بدرفتار توسط گره فرستنده به‌صورت عمومی در شبکه منتشر

می‌شود. این روند سبب می‌شود تا گره‌های دیگر، تمام بسته‌های دریافتی از سویاین گره را نادیده بگیرند و در پروسه‌هایمسیریابی از آن استفاده نکنند.در الگوریتم۳، فاز حذف گره بدرفتار از بدنه شبکه و منزوی کردن آن نشان داده‌شده است.

۱. شروع
۲. دریافت مشخصات و شناسه گره مزاحم
۳. برچسب "مزاحم" را به گره دریافتی اضافه کن.
٤. انتشار فراگیر مشخصات گره برچسب دار در شبکه.
۵. پایان

نرم‌افزارشبیه‌سازی	**NS-2.34**
محیط	**1000*۱۰۰۰**
تعداد گره‌ها	**۲۵**
پروتکل مسیریابی	**AODV, DSR**
محدوده انتقال	**٦۰ متر**
نوع آنتن	**Omenia Antenna**
زمان‌های شبیه‌سازی	**۱۰۰ ثانیه**
لایه MAC	**IEEE 802.11**
نوع ترافیک	**CBR (UDP)**
اندازه بافر	**٤۰ بسته**
موقعیت قرارگیری نودها	**تصادفی**

الگوریتم۳. فاز حذف گره مزاحم در شبکه حسگر بی‌سیم

٤. شبیه‌سازی و نتایج

٤-۱. تنظیماتشبیه‌سازی

درشبیه‌سازی‌هایانجام‌شده از سناریویشبکه‌ای‌ با تراکم گره هی۲۵ گره حسگر بی‌سیماستفاده‌شده است که به‌صورت تصادفی در ناحیه‌ای به ابعاد ۱۰۰۰*۱۰۰۰توزیع‌شده‌اند. برد رادیویی گره‌های حسگر بی‌سیم٦۰متر است و نوع ترافیکاستفاده‌شده نیز از نوع CBR است. در این شبیه‌سازی‌ها،مدت‌زمان۱۰۰ ثانیه در نظر گرفته‌شده است. جدول ۱ پارامترهایاستفاده‌شده برایشبیه‌سازی را نشان داده است.

جدول ۱. تنظمیاتشبیه‌سازی

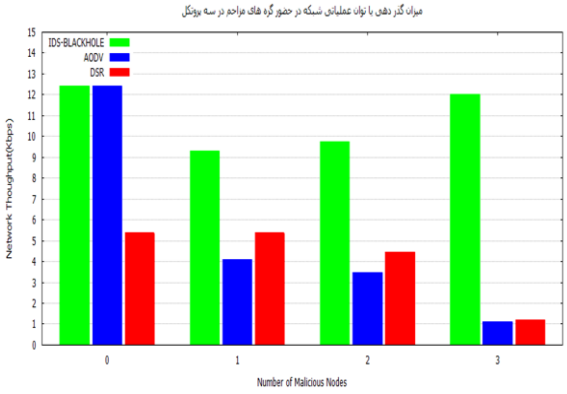
٤-۲. مقایسهشبیه‌سازی‌ها و نتایج

محتویگنجانده‌شده در این بخش به بررسی و تحلیل نتایجبه‌دست‌آمده از شبیه‌سازی‌هایانجام‌شدهمی‌پردازد. این نتایج مربوط به عملکرد دو پروتکل مسیریابی پایه و پرکاربرد AODV و DSR و نتایج حاصل از شبیه‌سازی‌های مربوط به روش پیشنهادی است و در آن‌ها عملکرد هر سه روشمدنظر در حضور صفرتا سه گره مزاحم که به‌صورت تصادفی در محیط تحت شبیه‌سازییراکنده‌شده‌اند در چهار معیار بررسی عملکرد و کارایی به نام‌های میزانگذردهی،تأخیر انتها به انتها، میزان نرخ تحویلموفقیت‌آمیز بسته و تعداد بسته‌هایداده‌ای‌ از بین رفته در حینانجام عمل انتقال تحلیل‌شده است.

۱-۲-٤.توان عملیاتی(میزانگذردهی شبکه)

میزانگذردهییا توان عملیاتی شبکه، بستگی زیادی به عملکرد صحیح و بدون خطای گره‌های موجود در یک شبکه حسگر بی‌سیم دارد. در مواقعی که گره‌های موجود در شبکه دارای رفتار عادی هستند و سعیمی‌کنندبه‌صورت

سالم و بدون مزاحمت در امر به جلو رانیبا فوروارد بسته‌هایداده‌ای از فرستنده به گیرنده شرکت کنند، میزان نرخ بسته‌هایداده‌ای که به‌صورتموفقیت‌آمیز در شبکه تحویلداده‌شده‌اند بالا رفته و سبب افزایش توان عملیاتییاگذردهی شبکه می‌شوند. خلاف این امر زمانی است که گره‌های موجود در شبکه رفتار و عملکرد عادی نداشته باشند و سعی در به وجود آوردن اخلال در به جلو رانی بسته‌هایداده‌ای شوند. این امر سبب از بین رفتن بسته‌هایداده‌ای و کاهش نرخ توان عملیاتی شبکه می‌شود. این امر سبب از بین رفتن بسته‌هایداده‌ای و کاهش نرخ توان عملیاتی شبکه می‌شود. با در نظر گرفتن این موارد تصویر۵ نتایج حاصل از توان عملیاتی مربوط به پروتکل‌هایDSR،AODV و روش پیشنهادی را در حضور گره‌های مزاحم نشان می‌دهد.



تصویر۵. میزان گذردهی و توان عملیاتی شبکه برای پروتکل‌های تحت بررسی

نتایجبه‌دست‌آمده از تحلیل توان عملیاتی شبکه در حضور گره‌های مزاحم برای هر سه پروتکل نشان می‌دهد که روش پیشنهادی توانسته است، با تشخیص گره‌های مزاحم و عدم استفاده از آن‌ها در مسیریابی به سمت گره مقصد، توان عملیاتی بالایی را کسب نماید. همان‌گونه که از تصویر۵ مشاهده می‌شود، روشپیشنهادی توانسته است بهترین عملکرد را درزمانی که شبکه تحت تأثیر مخرب عملکرد گره‌های مزاجم است را به خود اختصاص دهد. علاوه بر آن جدول ۲ عملکرد هر سه پروتکل را در بحث توان عملیاتی نشان داده است.

جدول ۲. توان عملیاتیثبت‌شده برای روش پیشنهادی، پروتکل AODV و DSR (برحسب کیلوبایت)

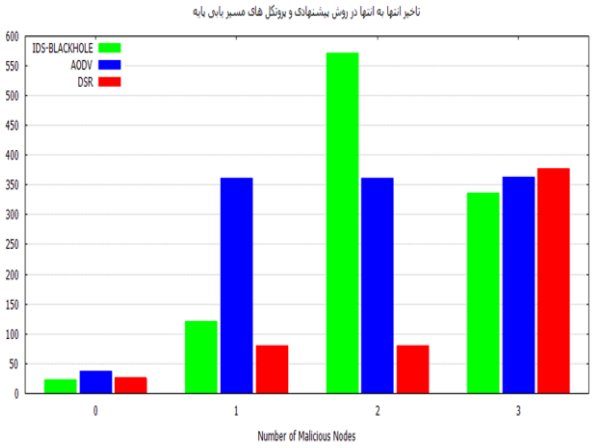
تعداد گره های مزاحم	روش پیشنهادی	پروتکل AODV	پروتکل DSR
0	12.4	12.4	5.36
1	9.28	4.096	5.36
2	9.73	3.49	4.46
3	12.0	1.101	1.201

اطلاعات به‌دست‌آمده از ۲ نشان می‌دهد که بهترین عملکرد در بحث توان عملیاتی مربوط به روش پیشنهادی است. هنگامی‌که هیچ گره مزاحمی در شبکه وجود ندارد عملکرد روش پیشنهادی و پروتکل AODV مشابه است؛ اما هنگامی‌که شبکه تحت تأثیر گره‌های مزاحم قرارگرفته است، اطلاعات این جدول نشان می‌دهد که روش پیشنهادی با عملکرد بهینه توانسته است ضمن شناسایی و کنار گذاشتن گره‌های مخرب از بدنه مسیریابی در شبکه، به توان عملیاتیدست یابد. در این مقایسه پروتکل مسیریابیDSR بدترین عملکرد را داشته است.

۲-۲-٤.تأخیر انتها به انتها

میزان برخورد در شبکه، توپولوژی و چیدمان گره‌های حسگر، الگوریتم‌هایزمان‌بندی برای ارسال و دریافت بسته‌ها بدون به وجود آمدن ترافیک و برخورد عواملی هستند که می‌توانند بر معیارتأخیر انتها به انتها اثرگذار باشند. علاوه بر این موارد، وجود و حضور گره‌های مزاحم در شبکه حسگر، جذب ترافیک شبکه و از بین بردن بسته‌هایداده‌ای بدون تحویل به گیرنده نیزمی‌تواند علاوه بر ناامن کردن شبکه سبب افزایشتأخیر و کاهش نرخ تحویل بسته شود. با در نظر گرفتن اینموضوع، تصویر٦،

تأخیر انتها به انتها در پروتکل‌های تحت بررسی را نشان می‌دهد.



تصویر٦. تأخیر انتها به انتها برای پروتکل‌های تحت بررسی در حضور گره‌های مزاحم

یکی از نکاتی که در تصویر٦ اهمیت زیادی دارد، عملکرد روش پیشنهادی در حضور دو گره مزاحم است که در بین سه پروتکل عملکرد خوبی نداشته است این در حالی است که در حضور یک و سه گره مزاحم روش پیشنهادی توانسته است عملکرد خوبی را به ثبت برساند. با توجه به موقعیت گره مزاحم که به‌صورت تصادفی در ناحیه تحت پوشش توزیع‌شده است، امکان دارد روش پیشنهادیبه‌منظور تحلیل وضعیت و صحت آن به پروسه بیشتری نیاز داشته باشد و بعد از رد مسیر دریافتی و ارسال مجدد بسته تقاضای مسیر و انتخاب مسیر صحیحمدت‌زمانی طول بکشد؛ بنابراین موقعیت گره‌های مزاحم و تحلیل وضعیت آن‌ها می‌تواند سبب افزایشتأخیر در حالت مذکور شده باشد. به‌هرحالعلی‌رغم آنکه روش پیشنهادی در این مورد نوعی سربار محاسباتی را از خود نشان داده است اما قابل‌چشم‌پوشی است چراکه در مراحل بعدیمی‌تواند با انتخاب مسیر صحیح، نرخ تحویل بسته و توان عملیاتی را افزایشداده و مانع از درپشدن بسته‌ها توسط گره مزاحم شود. این استدلال در تصاویر۷ و ۸ که به ترتیب مربوط به میزان نرخ تحویل بسته و میزان بسته‌هایدادهای از بین رفته هستند اثبات‌شده است.

جدول۳ میزانتأخیر انتها به انتهای هر سه پروتکل تحت بررسی را نشان می‌دهد. اطلاعات به‌دست‌آمده از این جدول نشان می‌دهند که روش پیشنهادیعلی‌رغم توانایی در شناسایی و کنار گذاشتن گره‌های مزاحم توانسته است نسبت به دو پروتکل دیگر رتبه قابل قبولی را کسب کند. انتظارمی‌رود با بالا رفتن مدت‌زمان فعالیت شبکه حسگر بی‌سیم، روشپیشنهادی بتواند به‌مرورزمان و با تشخیص دادن گره‌های مزاحم از این زمان بکاهد. همان‌طور که نتایجبه‌دست‌آمده برای حضور سه گره مزاحم این قضیه را اثبات کرده است. این در حالی است که در دو پروتکل دیگر افزایشمدت‌زمان فعالیت شبکه می‌تواندتأخیر انتها به انتها را افزایش دهد چراکه مکانیزمی برای تشخیص و کنار گذاشتن گره‌های مزاحم ندارند و با افزایش زمان فعالیت،به‌صورت تدریجی اکثر شاخص‌های ارزیابی رو به صفر میل خواهند نمود.

جدول ۳. میزانتأخیر انتها به انتها برای روش پیشنهادی و پروتکل‌هایAODV، DSR در حضور گره‌های مزاحم

تعداد گره های مزاحم	روش پیشنهادی	پروتکل AODV	پروتکل DSR
0	23.5965	36.635	25.7153
1	121.403	361.401	79.9291
2	570.967	361.406	79.9291
3	335.597	362.902	377.547

٣-٢-٤. میزان نرخ تحویل بسته

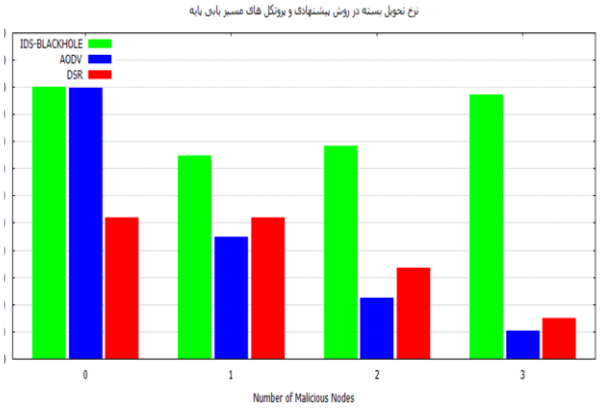
جدول٤ میزان نرخ تحویل بسته برای روش پیشنهادی، پروتکل AODV و پروتکل DSR را نشان می‌دهد. هنگامی‌که شبکه تحت تأثیر گره مزاحمی نیست، روش پیشنهادی و پروتکل AODV درصد مشابهی از نرخ تحویل بسته را ثبت نموده‌اند و پروتکل DSRدر رده سوم قرارگرفته است. هنگامی‌که شبکه تحت تأثیر گره مزاحم

قرارگرفته است، روش پیشنهادیمجدداً توانسته است در میزان درصد تحویلموفقیت‌آمیز بسته‌هایداده‌ای‌ای عملکرد مثبتی را نسبت به دو پروتکل دیگر از خود ثبت کند. تصویر۷ میزان نرخ تحویل بسته را نشان داده است.

جدول ٤. میزان نرخ تحویل بسته برای روش پیشنهادی و پروتکل‌های AODV و DSR

تعداد گره های مزاحم	روش پیشنهادی	پروتکل AODV	پروتکل DSR
0	99.9194	99.734	52.0126
1	74.7784	44.6909	52.0126
2	78.4045	22.2508	33.38
3	97.0185	10.23	14.87

یکی از نکاتی که در تصویر۷به‌وضوح روشن است آن است که با افزایش تعداد گره‌های مزاحم عملکردروش پیشنهادی در نرخ تحویل بسته بهتر شده و دو پروتکل دیگر عملکرد بسیار بدی را از خود ثبت کرده اند. این امر به دلیل آن است که روش پیشنهادی در حینمسیریابی میان فرستنده و گیرندهبه‌مرور گره‌های مخرب را شناسایی و آن‌ها را از بدنه مسیریابی کنارمی‌گذاردازاین‌رو با مرور زمان و افزایشمدت‌زمان فعالیت شبکه، روش پیشنهادیمی‌تواند عملکرد بهتری را از خود ثبت کند.

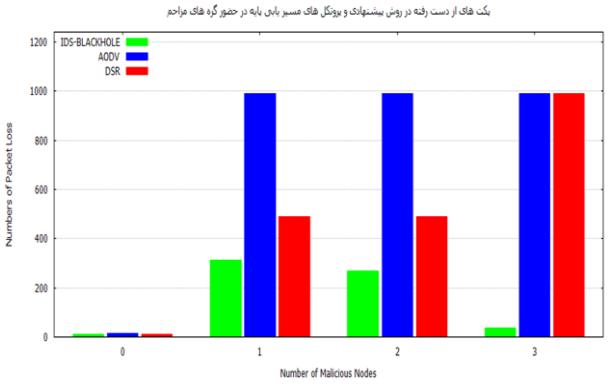


تصویر۷. میزان نرخ تحویل بسته در حضور گره‌های مزاحم

٤-۲-٤.تعداد بسته‌هایازدست‌رفته

تصویر۸ میزان بسته‌هایداده‌ای‌ایازدست‌رفتهدرروش پیشنهادی و دو پروتکل دیگر را نشان می‌دهد. همان‌گونه که از این تصویر مشخص است، هنگامی‌که شبکه حسگر بی‌سیم تحت تأثیر گره مزاحم نیست، هر سه پروتکل توانسته‌اند عملکرد بسیار مناسبی را از خود نشان دهند. هنگامی‌که در شبکه یک گره مزاحم وجود دارد، این تصویر نشان می‌دهد که ۸۰ درصد بسته‌های ارسالی توسط پروتکل AODV و ۵۰ درصد از بسته‌هایارسالی توسط DSR به علت عملکرد تخریبی گره مزاحم از بینرفته‌اند. این امر برای روش پیشنهادی در حدود ۲۰ درصد بوده است که به نسبت دو پروتکل دیگر عملکرد بسیار خوبی داشته است.

هنگامی‌که هر سه پروتکل تحت تأثیر دو گره مزاحم قرارگرفته‌اند همچنان تعداد بسته‌هایگم‌شده برای هر سه پروتکل مشابه باحالت اول هستند. یکی از نکات ویژه در تصویر۸ بالا رفتن مدت‌زمان فعالیت شبکه و افزایش تعداد گره‌های مزاحم در شبکه بوده است. برای دو پروتکل مسیریابی پایه، افزایش تعداد گره‌های مزاحم سبب شده تا در حدود ۹۰ درصد از بسته‌هایداده‌ای‌ای آن‌ها از بین برود این در حالی است که روش پیشنهادیبه‌صورت تدریجی توانسته است گره‌های**مزاحم را کنار زده و آنان را از روند مسیریابی حذف کند و بتواند ۹۵ درصد از بسته‌های ارسالی را با موفقیت به گیرنده برساند و فقط ۵ درصد از بسته‌های ارسالی را از دست دهد. علاوه بر موارد فوق، نتایج عددی حاصل از تعداد بسته‌هایازدست‌رفته در جدول ۵ نشان داده‌شده‌اند.**



تصویر۸. درصد بسته‌هایازدست‌رفته در شبکه حسگر در حضور گره‌های مزاحم

جدول۵. نتایج عددی حاصل از شبیه‌سازی روش پیشنهادی و پروتکل‌های پایه در شاخص تعداد بسته‌هایازدست‌رفته

تعداد گره های مزاحم	روش پیشنهادی	پروتکل AODV	پروتکل DSR
0	99.9194	99.734	52.0126
1	74.7784	44.6909	52.0126
2	78.4045	22.2508	33.38
3	97.0185	10.23	14.87

۵. نتیجه‌گیری کلی

نتایجبه‌دست‌آمده از پژوهش انجام‌شده نشان می‌دهند که روش پیشنهادی بدون تحمیل سربار محاسباتی بسیار زیاد،به‌جز در مورد تأخیر انتها به انتها که می‌تواند به علت موقعیت‌های مختلف گره‌های مزاحم به وجود آید، توانسته است گره‌های مزاحم را شناسایی و از روند مسیریابی در شبکه حذف کند. این روش در مقایسه با سایر روش‌های دیگری نظیررأی‌گیری گره هی[۱٤] که در آن گره‌های موجود در شبکه در مورد رفتار صحیحیا غیر صحیح گره مظنون تصمیم‌گیریمی‌کنند، روش‌هایخوشه‌بندی و کنترل گره‌ها توسط سرخوشه‌ها از کارایی بالاتری برخوردار است چراکه روش پیشنهادیبه‌صورت مستقیم و بدون درگیر کردن سایر گره‌ها و تحمیل سربارهای شدید محاسباتی که سبب افزایش ترافیک شبکه، افزایش انرژی مصرفی، کاهش طول عمر شبکه و افزایشتأخیرمی‌شوند، توانسته است با در نظر گرفتن نقیصه ذاتی پروتکل AODV و پر کردن آن، به‌راحتی گره‌های مزاحم را شناسایی و از پروسه مسیریابی کنار بزند.

در روش‌های انتخاباتی و جمع‌آوری عقیده سایر گره‌های دیگر درباره بدرفتار بودن یابدرفتار نبودن یک گره خاص نظیر روش ارائه‌شده در [۱٤]، درصورتی‌که چند گره مزاحم در شبکه حضورداشته باشند می‌توانند به عملکرد صحیح و عادی بودن رفتار گره مظنون رأی دهند و گره را علی‌رغم رفتار غیرعادیتبرئه کنند، و گره‌هایی که رفتار عادی دارند را بر اساسرأی خود به بدرفتاری متهم کنند، همچنیندر روش‌های کنترل توسط سرخوشه و با در نظر گرفتن محدودیت انرژی گره‌هایحسگر، مسئولیت سرخوشه به‌نوبت میان گره‌های موجود در شبکه تعویضمی‌شود و این در حالی است که اگرچند گره مزاحم به‌صورتهم‌زمان در چند خوشه مختلف، سرخوشه شوند، کل ارتباطات شبکه را مختل خواهند کرد.

در مورد روش پیشنهادیارائه‌شده در اینپایان‌نامه، از یک پروسه تصمیم‌گیری منطقیاستفاده‌شده است که در آن گره فرستنده می‌تواندبر اساس اطلاعاتی که گره همراه بسته پاسخ به درخواست مسیر (RREP)به گره فرستنده ارسال کرده است، در مورد مسیر صحیحتصمیم‌گیری کند. ازاین‌روبر اساس نتایجبه‌دست‌آمده توانسته است، درصد بالای تشخیص گره‌های مزاحم را به خود اختصاص دهد.

عملکرد روش پیشنهادیبه‌گونه‌ای بوده است که گره‌های مزاحمی که در یک گامی گره فرستنده یا گیرندهبوده‌اند را به‌راحتی تشخیص داده است. هنگامی‌که گره‌های مزاحم در چند گامی فرستنده و گیرندهبوده‌اند، روش با دشواری

بیشتری روبرو بوده است، چراکه باید مسیرهای موجود در جدول مسیریابی
را نیزآزمون کند.
به‌هرحال با در نظر گرفتن تمامی موارد، روش پیشنهادی توانسته است با تحمیل حداقل سربار محاسباتی، عملکرد خوبی را در تشخیص و کنار زدن گره‌های مزاحم در شبکه از خود نشان دهد.

٦. پژوهش‌های آتی

بهبود عملکرد روش پیشنهادی در انتخاب سریع‌تر مسیر درست که سبب کاهش تأخیر انتها به انتها و انرژی مصرفی گره‌ها و بالا بردن طول عمر شبکه می‌شود از اهداف آتی پژوهشی محسوب می‌شود. همچنین توسعه روش پیشنهادی و قابلیت پشتیبانی آن از سایر حملاتی که در این‌گونه شبکه‌ها انجام می‌شود از دیگر اهداف پژوهشی جذاب در آینده خواهد بود.

۷.مراجع

[1] Ping Yi, Yichuan, Yiping Zhong, Shiyong Zhag, “Distributed Intrusion Detection for Mobile Ad Hoc Networks ”, Journal of Systems Engineering and Electronics Vol. 19, No. 4, 2008, pp.851–859.
[2] 2. Mishra, A., K. Nadkarni and A. Patcha. 2004. « Intrusion detection in wireless ad hoc networks».IEEE Wireless Communications, vol. 11, no 1, p. 48-60.
[3] P. Dewal, G. S. Narula and V. Jain, "Detection and prevention of black hole attacks in cluster based wireless sensor networks," 20163rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3399-3403.
[4] 4. Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” 6th Int’l. Conf. Mobile Comp. and Net. Aug. 2000, pp. 275–283.
[5] Foong He6ng Wai ,Yin Nwe Aye, Ng Hian James , “Intrusion Detection in Wireless Ad Hoc Networks,” 6th Int’l. CS4274 INTRODUCTION TO MOBILE COMPUTING, pp. 1–12.
[6] Faroq Anjum,Dhanant Subhadrabandhu and Saswati Sarkar, “Signature Intrusion Detection for Wireless Ad Hoc Networks: A Comparative study of various routing protocols”, in 2003.
[7] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, New Orleans, LA, 1999, pp. 90-100.
[8] A.A. Chavan, D.S. Kurule, P.U. Dere, Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack Original Research ArticleProcedia Computer Science, Volume 79, 2016, Pages 835-844.
[9] K.S. Praveen, H.L. Gururaj, B. Ramesh, Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols Original Research Article Procedia Computer Science, Volume 85, 2016, Pages 325-330.
[10] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, A survey of black hole attacks in wireless mobile ad hoc networks, Human-centric Computing and Information Sciences 2011, pp 1-16.
[11] Debarati Roy Choudhury, Leena Ragha, Nilesh Marathe, Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole AttackOriginal Research ArticleProcedia Computer Science, Volume 45, 2015, Pages 564-570
[12] P C Kishore Raja, Dr.Suganthi.M, R.Sunder, “WIRELESS NODE BEHAVIOR BASED INTRUSION DETECTION USING GENETIC ALGORITHM”, Ubiquitous Computing and Communication Journal, 2006.
[13] Jaydip Sen, "An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks”, Second International Conference on Computational Intelligence, Communication Systems and Networks, 2010.

[14] Mehdi Medadian, Ahmad Mebadi, Elham Shahri, "Combat with Black Hole Attack in AODV Routing Protocol ", roceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 15 -17 December 2009 Kuala Lumpur Malaysia.

[15] Sheng Liu, Yang Yang, Weixing Wang, "Research of AODV Routing Protocol for Ad Hoc Networks", 2013 AASRI Conference on Parallel and Distributed Computing and Systems, AASRI Procedia 5 (2013) 21 – 31.