مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هشتم، شماره ۴، زمستان ۱۳۹۶؛ ص ۳۰۰-۲۸۵

مقابله با حملات سیاه‌چاله در پروتکل مسیریابی AODV با بهره‌گیری از منطق فازی

شهرام جمالی[1*]، سونیا میرمحسنی نمین[2]، سید ناصر سید هاشمی[3]

۱- دانشیار، دانشگاه محقق اردبیلی ۲- کارشناس ارشد، دانشگاه آزاد اسلامی واحد تبریز ۳- دانشجوی دکتری، دانشگاه اصفهان

(دریافت: ۹۵/۰۲/۰۲، پذیرش: ۹۵/۱۰/۱۰)

چکیده

شبکه‌های موردی سیار، به علت سادگی و سرعت پیاده‌سازی، در بسیاری از موارد گزینه انتخابی قدرتمند و مناسبی هستند. با این حال، به علت پویایی و فقدان زیرساخت ثابت در برابر تهدیدهای امنیتی بسیار آسیب‌پذیر هستند. در سال‌های اخیر تلاش‌های قابل توجهی در زمینه طراحی پروتکل‌های مسیریابی امن و قدرتمند انجام شده و طرح‌های امنیتی زیادی برای مقابله با این مسائل امنیتی ارائه شده است. دلیل این حساسیت، کاربردهای اخیر شبکه‌های موردی است. کاربرد وسیع این شبکه‌ها، از میدان‌های جنگ گرفته تا عملیات امداد و نجات و یا کاربردهای تجاری، لزوم داشتن ارتباطات امن، در این شبکه‌ها را بیان می‌کند. در این مقاله، ضمن بررسی تأثیر حمله سیاه‌چاله در شبکه‌های مبتنی بر پروتکل AODV، یک راهکار دفاعی جهت مقابله با این حملات ارائه خواهد شد. راهکار پیشنهادی از سامانه منطق فازی جهت شناسایی گره‌های مخرب در شبکه استفاده خواهد کرد. در این سامانه، میزان مشکوک بودن یک گره از نقطه‌نظر امکان مخرب بودن، با استفاده از منطق فازی مدل شده و عدد فازی حاصل، نحوه رفتار سایر گره‌ها با گره مذکور را مشخص می‌کند. نتایج شبیه‌سازی‌های انجام شده با شبیه‌ساز ns-2 نشان می‌دهد که الگوریتم ارائه شده کارایی بهتری از نظر تشخیص و کاهش تعداد بسته‌های حذف شده، نسبت به دو روش متداول 2's RREP و DPRAODV دارد.

کلیدواژه‌ها: شبکه‌های موردی سیار MANET، پروتکل AODV، حمله سیاه‌چاله، منطق فازی

Defense against Black Hole Attacks on AODV Routing Protocol Using Fuzzy Logic

Sh. Jamali*, S. Mirmohseni Namin, S. N. Seyed Hashemi
University of Mohaghegh Ardebili
(Received: 21/04/2016; Accepted: 30/12/2016)

Abstract

Mobile ad hoc networks (MANETs) are suitable option in many cases due to its simplicity and speed of deployment. However, MANETs are vulnerable against various types of security threats because of their dynamic topology and absence of a fixed infrastructure. Especially, the wide employment of this network in military and commercial applications makes its security more important. In recent years, considerable efforts have been made to design secure and robust routing protocol, and many security schemes have been proposed to tackle these security issues. In this paper, we design a defense strategy against black hole attack over the AODV routing protocol. The proposed solution employs the fuzzy logic system to identify malicious nodes in the network. In this design, each node is assigned by a fuzzy value which measures its probability of being an attacker. Extensive simulation, performed in the ns-2 simulator, show that the proposed algorithms outperforms previous methods in terms of number of dropped pockets.

Keywords: Mobile Ad - Hoc Networks, AODV Protocol, Black Hole Attack, Fuzzy Logic

*Corresponding Author E-mail: jamali@iust.ac.ir

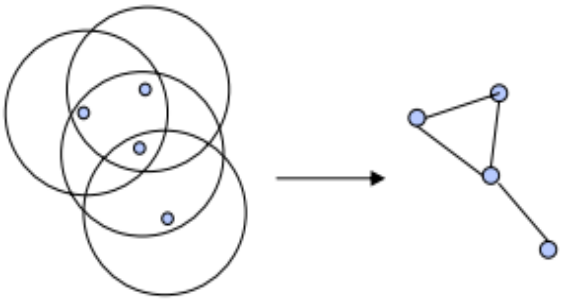
۱. مقدمه

شبکه موردی، شبکه‌ای است که توسط میزبان‌های بی‌سیمی که می‌توانند سیار هم باشند، تشکیل می‌شود. در این شبکه‌ها، از هیچ زیرساخت پیش ساخته‌ای، استفاده نمی‌شود. بدین معنا که، هیچ زیرساختی مانند یک ایستگاه مرکزی، مسیریاب[1]، سوییچ و یا هر چیز دیگری که در دیگر شبکه‌ها از آن‌ها برای کمک به ساختار شبکه استفاده می‌شود، وجود ندارد. در این شبکه‌ها، ارتباطات مابین گره‌ها به ویژگی‌های خاص شبکه بستگی دارد. فقدان مدیریت متمرکز همراه با قابلیت انتقال محدود وسیله‌های بی‌سیم، گره‌ها را مجبور می‌کند تا به منظور انتقال بسته‌ها از گره مبدأ به مقصد، با دیگر گره‌ها هماهنگ باشند[۱].

بنابراین به منظور دستیابی به هدف ارسال بسته‌ها در شبکه، هر گره به عنوان یک میزبان، همانند یک دستگاه مسیریابی همکاری می‌کند. این مسئله، یک مسیر ارتباطی مشترک را مابین گره‌هایی که در محدوده انتقالی یکدیگر قرار ندارند، تشکیل می‌دهد. در این شبکه‌ها، انتقال توسط پروتکل‌های مسیریابی ادهاک، مدیریت می‌شود، به طوری که این پروتکل‌ها به گره‌ها اجازه می‌دهند تا کلیه مسیرهای ارتباطی به سمت گره‌های دیگر را، از طریق به‌روزرسانی پویای مسیرهای ارتباطی، کشف نمایند.

دو نوع سناریو جهت انتقال داده در شبکه‌های موردی سیار[2] وجود دارد. اول اینکه، گره‌هایی که در محدوده انتقالی یکدیگر قرار دارند، به طور مستقیم پیام‌ها را به یکدیگر ارسال و دریافت می‌کنند. دوم اینکه، گره‌هایی که در محدوده انتقالی یکدیگر قرار ندارند، به منظور تحویل بسته‌ها، به گره‌های میانی اتکاء می‌کنند. بنابراین گره‌های میانی، بسته‌ها را مابین گره‌های مبدأ و مقصد بازپخش می‌کنند. به این ترتیب مسیرهای چندگامه‌ایی ایجاد می‌شود که در آن‌ها هر گره به عنوان یک مسیریاب عمل می‌کند. این مسئله به یک سطح بالایی از نیازمندی‌ها مابین گره‌ها در محیط شبکه‌های موردی سیار منجر خواهد شد [۲].

در شکل (۱) ساختار یک شبکه موردی نمونه آورده شده است. دایره‌های کوچک، نشان دهنده گره‌های بی‌سیم می‌باشند. هر دایره بزرگ نشان دهنده برد مفید یک گره است. بدین معنا که هر گره دیگری که در این فاصله قرار داشته باشد، می‌تواند داده‌های ارسالی این گره را دریافت کرده و آن‌ها را از نویزهای محیطی تشخیص دهد. برای راحتی کار، این شبکه را با یک گراف متناظر آن نشان می‌دهند. یال‌های گراف بدین معنا هستند که دو رأس آن در فاصله‌ای با یکدیگر قرار دارند که می‌توانند پیام‌های یکدیگر را دریافت کنند. در واقع گره‌هایی که در فاصله برد مفید یک گره قرار دارند، در نمایش گرافی، با یک یال به آن متصل می‌شوند [۳].



شکل ۱. ساختار یک شبکه موردی [۳]

تحقیقات اولیه در شرایطی که فرض بر این بود که شبکه در وضعیت هماهنگ و دوستانه‌ای قرار دارد، بر روی دسترسی به کانال ارتباطی بی‌سیم، ارتباطات و پروتکل‌های مسیریابی چندگامه، تمرکز داشت. کاربردهای شبکه‌های موردی سیار و افزایش استفاده از آن‌ها، تأمین امنیت در این شبکه‌ها را در یک محیط بالقوه متخاصم، به یک بحران اصلی تبدیل کرده است. تحقیقاتی که اخیراً انجام شده است نشان می‌دهد که شبکه‌های موردی سیار بیشتر از شبکه‌های سیمی و بی‌سیم معمول، مستعد مشکلات امنیتی هستند [۱].

ادامه این مقاله، به شکل زیر سازمان‌دهی شده است: در بخش ۲، پروتکل مسیریابیAODV و در بخش ۳، منطق فازی معرفی شده است. سپس در بخش ۴، چگونگی وقوع حملات سیاه‌چاله در شبکه‌های MANET مبتنی بر این پروتکل با جزئیات بیشتری بررسی شده و در بخش۵، نگاه اجمالی به پیشینه تحقیقات انجام شده در زمینه مقابله با حملات سیاه‌چاله صورت خواهد گرفت. سپس در بخش ۶، سامانه پیشنهادی را بررسی و درنهایت در قسمت ۷، شبیه‌سازی راهکار پیشنهادی انجام و نتایج حاصل از آنالیز این راهکار با روش‌های متداول قبلی مقایسه خواهد شد.

پروتکل AODV، یک پروتکل مبتنی بر تقاضا است. در این پروتکل، کلیه مسیرها فقط زمانی که مورد نیاز باشند، کشف شده و مورد استفاده قرار می‌گیرند. مسیرها در طول یک همه‌پخشی کشف و در طی آن گره‌های شبکه با استفاده از پیام‌های کنترلی مسیریابی، به صورت هماهنگ با یکدیگر، در فرآیند جستجوی یک مسیر به سمت مقصد مورد نظر شرکت می‌کنند. با استفاده از این پیام‌های کنترلی، پروتکل مسیریابی AODV می‌تواند، سریعاً خود را با شرایط پویای شبکه تطبیق دهد. در این پروتکل به علت اینکه پیام‌های مسیریابی پروتکل AODV، دارای ساختاری ساده و با حجم پایین هستند و نیاز به محاسبات کمی دارند، سربار استفاده از حافظه و پردازش اطلاعات پایین بوده، و با استفاده از

[1] Router
[2] Mobile Ad Hoc Networks

محدود کردن به‌روزرسانی‌های متناوب مسیر و همچنین استفاده از پیام‌های مسیریابی تنها در زمان نیاز، از پهنای باند شبکه نیز استفاده بهینه‌ای به عمل می‌آید.

پروتکل AODV به منظور تحقق اهداف زیر طراحی شده است:

- ✓ حداقل سربار کنترلی
- ✓ حداقل سربار پردازشی
- ✓ قابلیت مسیریابی چندگامی
- ✓ نگهداری پویای توپولوژی
- ✓ عاری بودن از حلقه

در یک شبکه موردی سیار، ممکن است گره‌های مبدأ و مقصد به علت محدودیت حوزه ارسال تجهیزات بی‌سیم، در خارج از محدوده ارتباطی مستقیم یکدیگر قرار داشته باشند. از این رو پروتکل AODV گره‌ها را قادر می‌سازد تا بتوانند از کشف مسیرهای چندگامی به سمت مقصد استفاده کنند، و این مسیرها را تا وقتی که توپولوژی شبکه تغییر می‌کند، نگهداری نمایند.

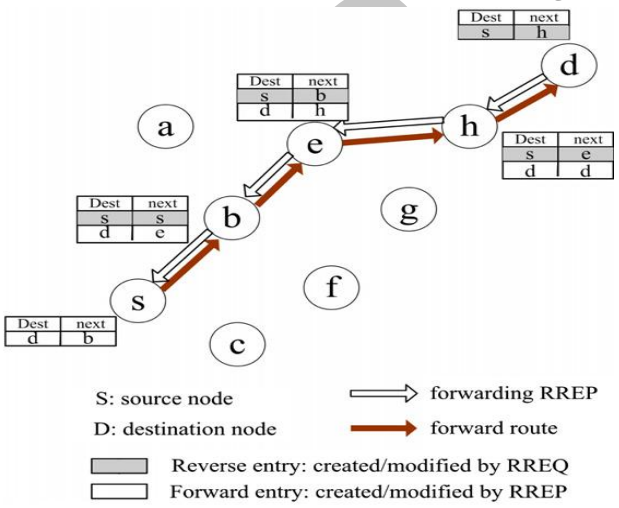
پروتکل مسیریابی AODV به منظور انجام فرآیند مسیریابی از دو نوع پیام‌های کنترلی مسیریابی استفاده می‌کند: پیام‌های مربوط به کشف مسیر و پیام‌های مربوط به نگهداری مسیر. اولی شامل پیام‌های RREQ و RREP است. در حالی که دومی شامل پیام‌های RERR و پیام‌های HELLO است، که فرمت آن‌ها در تحقیقاتی که توسط دسوال و سینگ [۴] انجام شده، نشان داده شده است. این پیام‌ها، از طریق پروتکل UDP/IP ارسال می‌شوند. بارزترین مشخصه پروتکل مسیریابی AODV، در مقایسه با سایر پروتکل‌های مسیریابی این است که، پروتکل AODV برای هر مسیر، از یک فیلد شماره سریال مقصد[1] استفاده می‌کند. بنابراین زمانی که به یک اتصال[2] به سمت مقصد مورد نظر نیاز باشد، مقدار فیلد شماره سریال مقصد، توسط گره مقصد ساخته می‌شود. استفاده از شماره سریال ما را مطمئن می‌سازد، که مسیر ما تازه[3] و فارغ از هر گونه حلقه تکراری است، و با استفاده از فیلد تعداد گام‌ها[4]، این اطمینان را به ما می‌دهد که مسیر ارائه شده کوتاه‌ترین مسیر ممکن به سمت مقصد است [۴]. در پروتکل‌های مسیریابی، شماره‌های سریال، به عنوان مهرهای زمانی[5] عمل می‌کنند. شماره سریال به گره‌ها این امکان را می‌دهد که تازه بودن و جدید بودن اطلاعات خود را، در گره‌های دیگر مقایسه کنند. زمانی که یک گره، هر نوعی از پیام‌های کنترل مسیریابی مانند RREQ[6]، RREP[7]، RERR را ارسال می‌کند، مقدار شماره سریال خود را یک واحد افزایش می‌دهد. هر گره مقدار شماره سریال همه گره‌های دیگری را که با آن‌ها در ارتباط است، را نگهداری می‌کند. بالا بودن مقدار شماره سریال نشان دهنده دقیق‌تر و تازه‌تر بودن اطلاعات است و هر گرهی که شماره سریال بالاتری را ارسال کند، اطلاعات آن گره در فرآیند کشف مسیر، بررسی خواهد شد و مسیر از طریق این گره، به گره‌های دیگر برپا می‌شود.

زمانی که گره مبدأ می‌خواهد با گره مقصد اتصالی را ایجاد کند، اما مسیر موجود در جدول مسیریابی آن قدیمی شده باشد، یا اصلاً چنین مسیری در جدول مسیریابی وجود نداشته باشد، در این حالت، گره مبدأ یک پیام RREQ را به صورت همه‌پخشی ارسال می‌کند. این پیام RREQ منتشر شده از طرف گره مبدأ، به وسیله تمام همسایگان گره مبدأ، یعنی گره‌هایی که در فاصله یک گامی از گره مبدأ قرار دارند، دریافت می‌شود. گره‌های میانی نیز، پیام RREQ دریافتی را به صورت همه‌پخشی ارسال می‌کنند. این فرآیند تا زمانی ادامه پیدا می‌کند که بسته RREQ توسط گره مقصد دریافت شود، یا یک گره میانی، که مسیر تازه‌ای به سمت مقصد دارد، این بسته RREQ را دریافت کند. از آن جایی که، پیام RREQ به صورت همه‌پخشی توسط گره‌ها منتشر می‌شود، بنابراین جهت استفاده بهینه از منابع گره‌ها، می‌بایست از پردازش تکراری این پیام‌ها، توسط گره‌های میانی جلوگیری شود. از این رو، زمانی که یک گره میانی پیام RREQ را دریافت می‌کند، ابتدا فیلد RREQID آن را بررسی می‌کند، اگر قبلاً RREQایی، با همین RREQID دریافت کرده باشد به طوری که شناسه گره ارسال کننده بسته RREQ هم مشابه قبل باشد در این حالت، متوجه می‌شود که RREQ دریافتی تکراری است و آن را دور می‌ریزد، اگر نه، تعداد گام‌های RREQ را یک واحد افزایش می دهد و دوباره پیام RREQ دریافتی را به صورت همه‌پخشی ارسال می‌کند.

در فرآیند RREQ، زمانی که یک گره میانی بسته RREQایی را برای اولین بار را دریافت می‌کند، ابتدا بررسی می‌کند که آیا مسیر معکوس به سمت گره مبدأ را در جدول مسیریابی‌اش دارد یا نه؟ چرا که در ادامه کار، از این مسیر معکوس، برای ارسال پیام RREP استفاده خواهد شد. ضمناً پیام RREP از طریق یک مسیر تکی به سمت گره مبدأ ارسال می‌شود. پس از اتمام مرحله ارسال کردن بسته درخواست مسیر، RREP از گره مقصد و یا گره میانی که مسیری به سمت مقصد مورد نظر دارد، در جهت

[1] Destination Sequence Number
[2] Connection
[3] Fresh
[4] Hop Count
[5] Time Stamps
[6] Rout Request
[7] Rout Reply

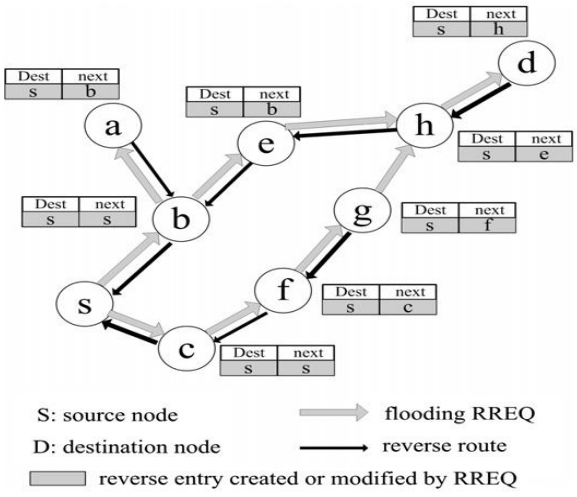
معکوس به گره مبدأ ارسال خواهد شد. جهت نگهداری مسیر در پروتکل AODV، هر گره به صورت متناوب پیام‌های HELLO را به همسایگان خود ارسال می‌کند. اگر یک گره، پیام HELLO را از گرهی که در همسایگی آن قرار دارد، برای یک مدت زمان معین دریافت نکند، یک پیام RERR را به همه گره‌هایی که در جدول همسایگی آن قرار دارند، ارسال می‌کند. پیام RERR به پروتکل AODV اجازه می‌دهد تا زمانی که گره‌ها جابه‌جا می‌شوند، بتواند مسیرها را از نو تنظیم کند. گرهی که پیام RERR را دریافت می‌کند، مسیر توافق شده را، از جدول مسیریابی خود حذف کرده، و به این ترتیب، از مسیرهای



(b) RREP message and forward route

شکل ۲. فرآیند کشف مسیر در پروتکل مسیریابی AODV [۶]

آسیب‌دیده، برای ارسال بسته‌های داده استفاده نمی‌شود [۵]. شکل (۲) نمایی از نحوه عملکرد پروتکل AODV در فاز کشف مسیر را نشان می‌دهد. پروتکل مسیریابی AODV، با وجود تمام مزایایی که به همراه دارد، بازهم نمی‌تواند با تهدیدهای حمله سیاه‌چاله مبارزه کند. زیرا در طول فاز جستجوی مسیر، ممکن است گره‌های مخرب مقدار شماره سریال و تعداد گام‌ها را از یک پیام مسیریابی جعل کنند و بدین ترتیب بتوانند به یک مسیر دست یابند، تا از طریق این مسیر همه بسته‌های داده‌ایی را که از آن مسیر عبور می‌کنند را استراق سمع و یا حذف نمایند.



(a) RREQ message and reverse route

به منظور مقابله مؤثر با پیچیدگی روزافزون در مدل‌سازی و حل مسائل جدید، ایجاد و ابداع روش‌های محاسباتی جدیدی مورد نیاز است، به طوری که روش‌های جدید بیش از پیش به شیوه‌های تفکر و تعلم خود انسان نزدیک باشد. هدف اصلی آن است که، تا حد امکان رایانه‌ها بتوانند مسائل و مشکلات بسیار پیچیده علمی را با همان سهولت و شیوایی که ذهن انسان قادر به ادراک و اخذ تصمیمات سریع و مناسب است، بررسی و حل و فصل نمایند.

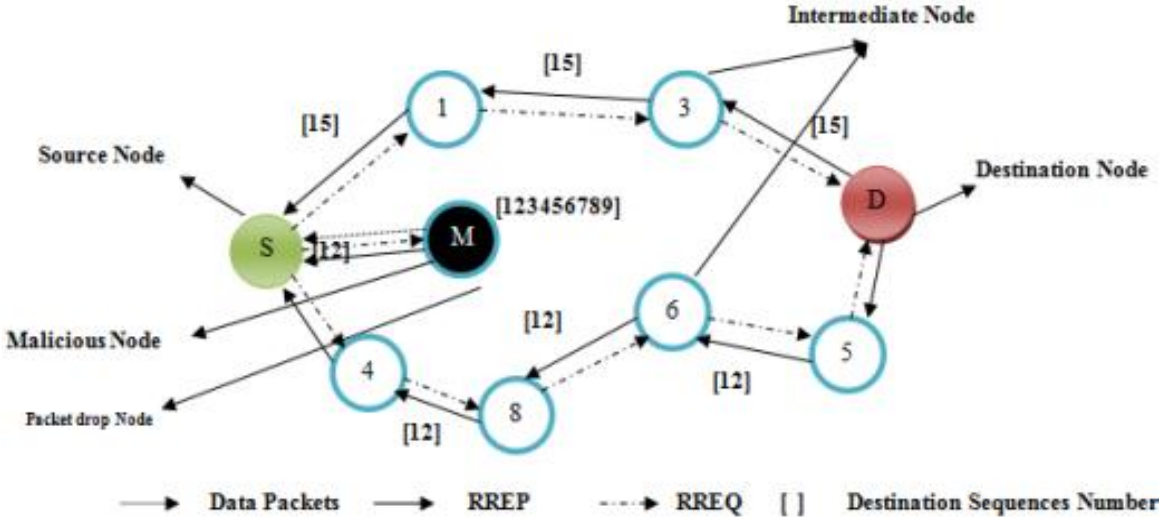
در جهان واقعیات، آدمی، بسیاری از مفاهیم را به صورت فازی (به معنای غیر دقیق، نا واضح و مبهم) درک می‌کند و به‌کار می‌بندد. به عنوان نمونه، هر چند کلمات و مفاهیمی همچون گرم، سرد، بلند، کوتاه، پیر، جوان و نظایر این‌ها به عدد خاص و دقیقی اشاره ندارند، اما ذهن انسان با سرعت و انعطاف‌پذیری شگفت‌آوری همه را می‌فهمد و در تصمیمات و نتیجه‌گیری‌های خود به‌کار می‌گیرد. این در حالی است که ماشین فقط اعداد را می‌فهمد و اهل دقت است. اهداف شیوه‌های نو در علوم رایانه آن است که، اولاً رمز و راز اینگونه توانایی‌ها را از انسان بیاموزد و سپس آن‌ها را تا حد امکان به ماشین یاد بدهد. قوانین علمی گذشته در فیزیک و مکانیک نیوتونی، همه بر اساس منطق قدیم استوار گردیده‌اند. در منطق قدیم فقط دو حالت دارید: سفید و سیاه، آری و خیر، روشن و تاریک، یک و صفر و درست و غلط. از آن جا که ذهن ما با منطق دیگری کارهای خود را انجام می‌دهد و تصمیمات مناسب را اتخاذ می‌کند، جهت شروع، ایجاد و ابداع منطق‌های تازه و چند ارزشی مورد نیاز است که منطق فازی یکی از آن‌ها است. کلمه Fuzzy به معنای غیر دقیق، نا واضح و مبهم است. اگر بخواهیم نظریه مجموعه‌های فازی را تعریف کنیم، باید بگوییم که نظریه‌ای است، برای اقدام در شرایط عدم اطمینان؛ این نظریه قادر است، بسیاری از مفاهیم، متغیرها و سامانه‌هایی را که نادقیق هستند را صورت‌بندی ریاضی ببخشد و زمینه را برای استدلال، استنتاج، کنترل و تصمیم‌گیری در شرایط عدم اطمینان فراهم آورد. منطق فازی از جمله منطق‌های چند ارزشی بوده و بر نظریه مجموعه‌های فازی تکیه می‌کند. مجموعه‌های فازی خود از تعمیم و گسترش مجموعه‌های قطعی، به صورتی طبیعی، مشتق می‌شوند. منطق فازی بیشتر با داده‌های نسبی سروکار دارد تا

داده‌های منطقی. به عبارت دیگر برخلاف منطق دو ارزشی که متغیرهای آن، از منطق باینری پیروی می‌کنند، متغیرهای منطق فازی ممکن است مقدار درستی در بازه [۱و۰] داشته باشند، در منطق فازی، هیچ تحمیلی برای پیروی مقادیر درستی از منطق گزاره‌ای وجود ندارد [۶].

در شبکه‌های موردی سیار، یک حمله سیاه‌چاله، می‌تواند به وسیله یک گره واحد، یا به وسیله چندین گره در مجموعه اتفاق بیفتد. حمله سیاه‌چاله گره واحد، مقدار شماره سریال و تعداد گام‌های یک پیام مسیریابی را جعل می‌کند، تا به این ترتیب مسیری را به‌دست آورد، سپس همه بسته‌هایی را که از آن مسیر عبور می‌کنند را یا استراق سمع و یا حذف می‌کند.

شکل (۳) رفتار حمله سیاه‌چاله گره واحد را نشان می‌دهد. در این سناریو، هدف گره مبدأ S، ارسال بسته‌ای به مقصد گره D است. در یک پروتکل مسیریابی AODV نرمال و فاقد حمله، زمانی که گره S می‌خواهد بسته‌ای را به گره مقصد D ارسال کند و هیچ مسیر قبلی به سمت مقصد مورد نظر در جدول مسیریابی آن وجود ندارد، در این حالت گره S، بسته RREQ را به صورت همه‌پخشی، به همسایگان خود ارسال می‌نماید، تا به این ترتیب مسیری را به در یک پروتکل مسیریابی AODV نرمال و فاقد حمله، زمانی که گره S می‌خواهد بسته‌ای را به گره مقصد D ارسال کند و هیچ مسیر قبلی به سمت مقصد مورد نظر در جدول مسیریابی آن وجود ندارد، در این حالت گره S، بسته RREQ را به صورت همه‌پخشی، به همسایگان خود ارسال می‌نماید، تا به این ترتیب مسیری را به مقصد گره D جستجو کند.

در یک پروتکل مسیریابی AODV نرمال و فاقد حمله، زمانی که گره S می‌خواهد بسته‌ای را به گره مقصد D ارسال کند و هیچ مسیر قبلی به سمت مقصد مورد نظر در جدول مسیریابی آن وجود ندارد، در این حالت گره S، بسته RREQ را به صورت همه پخشی، به همسایگان خود ارسال می‌نماید، تا به این ترتیب مسیری را به مقصد گره D جستجو کند. هر کدام از گره‌های میانی که این پیام RREQ را دریافت می‌کنند، آن را به صورت مستمر ارسال می‌کنند تا به مقصد D برسد [۷].



شکل ۳. نمایش چگونگی وقوع حمله سیاه‌چاله در پروتکل مسیریابی AODV [۸]

همان‌طور که در شکل (۳) نشان داده شده است، گره سیاه چاله M، به محض دریافت بسته RREQ، یک بسته RREP را با مقدار شماره سریال خیلی بزرگ و تعداد گام یک، به سمت گره مبدأ S، ارسال می‌کند. زمانی که گره مقصد D، کلیه RREQها را ، از گره‌های نرمال، دریافت کرد، این گره از میان مسیرهای دریافتی، یک مسیر بهینه را بر اساس شماره سریال و تعداد گام ها، انتخاب کرده و سپس بسته RREP را به گره مبدأ S برمی گرداند. بر اساس طراحی پروتکل AODV، گره مبدأ نیز از میان RREPهای دریافتی، مسیری را که مقدار شماره سریال آن از همه بزرگ‌تر و تعداد گام‌های آن از همه کمتر باشد را برای ارسال بسته‌های داده انتخاب خواهد کرد. از آن جایی که پیام RREPای که از طرف گره سیاه‌چاله ارسال شده است، مقدار شماره سریال خیلی بزرگی داشته و تعداد گام‌های آن نیز یک واحد فرض شده است، بنابراین گره مبدأ، مسیر ارسال شده از طرف گره سیاه‌چاله را برای ارسال بسته‌های داده، انتخاب خواهد کرد. با به‌دست آوردن مسیر ارسال داده توسط گره سیاه‌چاله، این گره، یا کلیه بسته‌های دریافتی را استراق سمع و یا آن‌ها را حذف خواهد کرد.

۲. پیشینه تحقیق

داکورر و همکاران [۹]، پروتکل مسیریابیAODV را اصلاح کرد تا فرصت دستیابی به یک مسیر توسط گره سیاه‌چاله را کاهش دهد. پروتکل ارائه شده توسط داکورر، پروتکل 2's RREP نام دارد. در

این پروتکل، گره مبدأ اولین یا ۲ تا از اولین RREPهایی را که دریافت کرده است را دور می‌ریزد، اما هر بسته RREPایی را که در ادامه کار دریافت می‌شود را انتخاب می‌کند، زیرا RREPایی که توسط گره سیاه‌چاله ساخته می‌شود، اولین یا دومین RREPایی است که به گره مبدأ می‌رسد. این پروتکل، در مواقعی که گره سیاه‌چاله، در نزدیکی گره مبدأ قرار دارد، می‌تواند بسیار مفید باشد.

لو و همکاران [۱۰]، یک پروتکل مسیریابی امن مبتنی بر پروتکل AODV به نام SAODV را، به منظور مقابله با حملات سیاه‌چاله ارائه دادند. پروتکل بهبود یافته SAODV، در هر گره از مدیریت پسورد مبتنی بر احراز هویت بهره می‌برد. به این ترتیب که در این پروتکل تمامی گره‌ها کلمه عبور یکسانی را بین خود به اشتراک می‌گذارند، این کلمه عبور، قبل از ارسال بسته درخواست مسیر، توسط گره‌های دیگر به نمایندگی از گره‌های همسایه بررسی می‌گردد. درخواست‌ها با رمز عبور معتبر ارسال و بقیه حذف می‌شوند. این رمز عبور به گره‌های شبکه کمک می‌کند تا گره‌های قانونی را از عناصر غیر قانونی شناسایی نمایند.

پروتکل SAODV، جهت انتقال اطلاعات مابین گره‌های مبدأ و مقصد، گره‌های میانی را غیر فعال می‌کند. به این ترتیب، پاسخ به درخواست‌های مسیر تنها توسط گره مقصد واقعی انجام می‌شود. گره مبدأ پاسخ به درخواست را دریافت کرده و یک پیام پرس و جویی را ارسال می‌کند تا به این ترتیب بررسی نماید که آیا لینک ارتباطی از گره میانی به گره مقصد وجود دارد؟ اگر وجود داشته باشد گره مبدأ معتبر بودن گره میانی را بررسی کرده و ترافیک را از طریق آن مسیر ارسال می‌کند. در غیر این صورت، گره مخرب شناسایی شده و این اطلاعات به صورت همه‌پخشی در کل شبکه منتشر می‌شود. به این طریق پروتکل SAODV، با شناسایی گره‌های سیاه‌چاله می‌تواند از وقوع حملات وسیع‌تر پیشگیری نماید. در این پروتکل بهبود یافته، ترافیک شبکه به صورت رمزنگاری شده ارسال می‌شود تا از خواندن اطلاعات توسط گره‌های غیر مجاز پیشگیری شود، از طرف دیگر در این روش، همه گره‌های موجود در مسیر، از گره مبدأ به گره مقصد امن هستند و نیازمندی‌های امنیتی گره فرستنده تحقق پیدا می‌کند.

به منظور مقابله با حملات سیاه‌چاله در سال ۲۰۱۰، پروتکل جدید دیگری مبتنی بر بهبود پروتکل AODV، ارائه شد. این پروتکل MOSAODV نام دارد. پروتکل MOSAODV در اصل، فقط کار گره مبدأ را اصلاح می‌کند و این کار را با استفاده از یک تابع اضافی به نام Pre- Receive Reply (PacketP) انجام می‌دهد. این تابع، یک جدول جدید به نام Cmg- RREP- Tab، یک زمان‌سنج جدید، به نام MOS – WAIT- TIME و یک متغیر جدید به نام Mali- Node، به ساختار داده در پروتکل پیش‌فرض AODV اضافه می‌کند.

در پروتکل AODV اولیه، گره مبدأ هر پیام RREPایی را که به اندازهٔ کافی تازه و جدید باشد را می‌پذیرد. در حالی که پروتکل MOSAODV، کلیه RREPهای دریافتی را در جدول جدیدی که در این پروتکل ایجاد شده است، نگهداری می‌کند. اطلاعات این جدول به اندازه مدت زمان Mos- Wait- Time، در جدول نگهداری می‌شوند. این روش، در ابتدای کار، به صورت ابتکاری، مقدار Mos- Wait- time، را برابر نصف مدت زمان RREP- Wait- time در نظر می‌گیرد. RREP- Wait- time مدت زمانی است که گره مبدأ قبل از اینکه یک پیام RREQ جدیدی را بسازد، منتظر دریافت پیام RREP باقی می‌ماند.

در پروتکل بهبود یافته MOSAODV، بعد از اینکه گره مبدأ اولین پیام کنترلی RREP را دریافت کرد، به اندازه مدت زمان Mos- Wait- time، منتظر می‌ماند. در این مدت زمان، گره مبدأ همه پیام‌های RREP دریافت شده را در جدول Cmg- RREP- Tab، نگهداری کرده و آنالیز می‌کند و درنهایت RREPهایی را که مقدار شماره سریال مقصد آن‌ها خیلی بزرگ باشد را از حافظه پاک می‌کند. بعد از شناسایی گره مخرب، گره مبدأ از لیست موجود RREPایی را که مقدار شماره سریال مقصد آن بزرگ‌تر از RREPهای دیگر است را انتخاب می‌کند. در این روش، گرهی که به صورت مخرب شناسایی شده، در متغیر Mali- Node نگهداری شده و در ادامه کار، هر پیامی که از طرف آن گره آمده باشد، حذف می‌شود.

نتایج شبیه‌سازی‌ها نشان می‌دهد که مقدار PDR در زمانی که سایز شبکه تغییر می‌کند، تا ٪۸۱/۸۱۱ بهبود می‌یابد. در حالی که وقتی حرکت گره تغییر می‌کند مقدار بهبودی ٪۷۰/۸۷۷ خواهد بود. در مقایسه با پروتکل مسیریابی AODV، این راه حل، نرخ تحویل بسته بالاتری را در نتایج شبیه‌سازی به‌دست می‌آورد اما میزان تأخیر انتها به انتها به صورت اجتناب‌ناپذیری افزایش می‌یابد [۱۱].

تامیل‌سلوان و ساناکارانارایانان[۱۲]، یک پروتکل مسیریابی اصلاح شده AODV، به نام PCBHA [1] را ارائه کردند، تا از وقوع حملات سیاه‌چاله پیشگیری کنند. پروتکل PCBHA، در ابتدا، هر کاربر قانونی و مشروع را با یک سطحی از وفاداری و صداقت پیش‌فرض در نظر می‌گیرد. سپس یک پیام RREQ به صورت همه‌پخشی ارسال می‌شود، گره مبدأ منتظر دریافت RREPهای برگشتی، از گره‌های همسایه می‌ماند و درنهایت گره همسایه با

[1] Prevention of a Co- Operative Black Hole Attack

بالاترین سطح صداقت و وفاداری که مقدار سطح صداقت آن از حد آستانه بیشتر باشد، برای عبور بسته‌های داده، انتخاب می‌شود.

گره مقصد بعد از دریافت بسته داده، یک پیام ACK را به گره مبدأ ارسال می‌کند. در این حالت گره مبدأ به محض دریافت بسته ACK، یک واحد به سطح صداقت گره همسایه اضافه می‌کند. اگر هیچ ACKایی دریافت نشد، یک واحد از سطح صداقت گره همسایه را کاهش می‌دهد، چرا که تشخیص داده است که ممکن است یک گره سیاه‌چاله در مسیر وجود داشته باشد و بسته‌های داده را قبل از اینکه به مقصد برسند، حذف کرده باشد.

همین محققان در سال ۲۰۰۷، یک روش پویا، برای تشخیص حملات سیاه‌چاله ارائه دادند. در این روش، به منظور تشخیص حمله، مقدار شماره سریال مقصد موجود در پیام‌های RREP، بررسی می‌شود. در حالت نرمال، مقدار شماره سریال هر گره، بسته به شرایط ترافیکی شبکه تغییر می‌کند. زمانی که تعداد اتصالات افزایش پیدا کند، مقدار شماره سریال نیز رشد خواهد کرد و زمانی که تعداد اتصالات کم باشد، مقدار شماره سریال هر گره موجود در شبکه، به صورت یکنواخت رشد می‌کند. با این حال، زمانی که حمله در محلی از شبکه اتفاق می‌افتد، بدون در نظر گرفتن شرایط محیطی و ترافیک موجود در شبکه، مقدار شماره سریال به صورت قابل توجهی افزایش پیدا خواهد کرد.

در این روش، به منظور تشخیص حمله، از ۳ آیتم زیر استفاده می‌شود:

۱- تعداد پیام‌های RREQ ارسال‌شده؛

۲- تعداد پیام‌های RREP دریافت شده؛

۳- متوسط مقدار تفاوت شماره سریال مقصد موجود در پیام‌های RREP و RREQ.

گزینه سوم به صورت زیر محاسبه می‌شود:

زمانی که یک بسته RREQ ارسال و دریافت می‌شود، هر گره مقدار شناسه مقصد و شماره سریال آن را در لیست خود نگهداری می‌کند. زمانی که یک بسته RREP دریافت می‌شود، ابتدا گره بررسی می‌کند که آیا شناسه مقصد موجود در بسته‌های RREQ و RREP با هم برابرند؟ اگر این چنین باشد، تفاوت مقدار شماره سریال مقصد را در هر دو مورد محاسبه می‌کند. به منظور انجام این کار، برای ترافیکی که از هر گره عبور می‌کند، موقعیت شبکه در هر بازه زمانی i، به صورت بردار سه بعدی $x1 = (xi1, xi2, xi3)$ بیان می‌شود. حال، متوسط مقدار x، از بین D داده دریافتی در N بازه زمانی را محاسبه می‌شود:

$$\bar{x}_D = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (۱)$$

در حقیقت رابطه(۱)، متوسط مقدار شماره سریال مقصد را در هر بازه زمانی به‌دست می‌آورد. سپس فاصله مقدار ورودی نمونه x را، با متوسط مقدار محاسبه شده از رابطه (۲) محاسبه می‌شود:

$$d(x) = |x - \bar{x}_D|^2 \qquad (۲)$$

زمانی که این فاصله از حد آستانه Th بزرگ‌تر باشد، وقوع حمله تشخیص داده می‌شود.

$$\begin{cases} d(x) > Th \Rightarrow \text{Attack} \\ d(x) \leq Th \Rightarrow \text{Normal} \end{cases} \qquad (۳)$$

در اینجا، بیشینه‌ترین فاصله‌ایی که از مجموعه داده‌ها استخراج شده، به عنوان Th انتخاب می‌شود [۱۳]:

$$Th = d(xI) \text{ where } I = \arg\max d(xI) \quad i, xi \in D \qquad (۴)$$

در سال ۲۰۱۰، با نوآوری و ایجاد تغییر در روش آموزش پویا، راه‌حل جدیدی به منظور مقابله با حملات سیاه‌چاله در شبکه‌های موردی ارائه شد. این روش پیشنهادی، که با عنوان DPRAODV شناخته می‌شود، از همان روش ارائه شده توسط تامیل‌سلوان و ساناکارانارایانان استفاده می‌کند، فقط با این تفاوت که در روش آموزش پویا، هیچ سازوکاری برای بلوکه کردن گره سیاه‌چاله، ارائه نداده بودند و فقط راهکاری برای تشخیص حملات سیاه‌چاله بیان شده بود.

راهکار روش پیشنهادی جدید به این صورت است که در این روش، هر گره علاوه بر جدول مسیریابی، جدولی به عنوان لیست سیاه[1] نیز دارد. زمانی که گرهی با استفاده از رابطه (۳) وجود یک اختلال را در شبکه تشخیص داد، این گره، ابتدا آدرس گره مخرب را به لیست سیاه خود اضافه کرده سپس یک بسته هشدار[2] می‌سازد. این بسته هشدار نیز، دارای فیلدی به نام لیست سیاه است. به محض تشخیص گره مخرب، علاوه بر اینکه آدرس گره مهاجم به لیست سیاه گره تشخیص دهنده اضافه می‌شود، بلکه به فیلد لیست سیاه بسته هشدار نیز اضافه شده و به صورت همه‌پخشی به همسایگان گره تشخیص دهنده نیز ارسال می‌شود. هر گره به محض دریافت بسته هشدار، جدول لیست سیاه خود را به‌روزرسانی می‌کند.

حال وقتی گرهی بسته RREP را دریافت می‌کند، ابتدا بررسی می‌کند که آیا آدرس فرستنده RREP در لیست سیاه موجود است یا نه؟ اگر وجود داشته باشد، هیچ پردازشی روی

[1] Confirimation Route Request
[2] Alarm Packet

بسته RREP دریافتی انجام نشده، بسته دور ریخته می‌شود و در ادامه کار گره مخرب بلوکه خواهد شد.

بر اساس این روش، نه تنها اینکه حملات سیاه‌چاله تشخیص داده می‌شوند، بلکه با استفاده از به‌روز بودن مقدار حد آستانه، که بر محیط واقعی شبکه نظارت دارد، از وقوع حمله سیاه‌چاله نیز جلوگیری می‌شود. در نتایج شبیه‌سازی‌ها نرخ تحویل بسته در حدود ٪۸۵ -۸۰، نسبت به پروتکل AODV تحت حمله سیاه‌چاله، بهبود داشته است و زمانی که بار ترافیکی افزایش می‌یابد، ٪۶۰ بهبود وجود دارد. مزیت روش DPRAODV، این است که این روش نرخ تحویل بسته بالاتری را نسبت به AODV به‌دست می‌آورد؛ اما در این روش مقدار سربار مسیریابی کمی افزایش می‌یابد و تأخیر انتها به انتها[1] نیز کمی افزایش می‌یابد [۱۴].

با وجود اینکه پروتکل‌های مسیریابی اصلاح شده و امن، شبکه را از وقوع تعدادی از حملات حفاظت می‌کنند، ولی این پروتکل‌های اصلاح شده منابع شبکه را مصرف کرده و از طرفی نفوذ هم به صورت مستمر اتفاق می‌افتد. از این رو، سامانه‌های تشخیص نفوذ (IDS)[2] معرفی شدند تا گره‌های مخرب و خودخواه را در شبکه تشخیص دهند. یک IDS از مجموعه سازوکارها و روش‌ها تشکیل شده است که از این سازوکارها، به منظور تشخیص فعالیت‌های مظنون و ایجاد هشدار در مورد نفوذها استفاده می‌کند. به طور عمده سه نوع IDS وجود دارد [۱۵]:

۱) تشخیص نفوذ مبتنی بر رفتارهای غیر عادی: تشخیص رفتارهای غیر عادی، روشی است که از لحاظ کمی، رفتارهای طبیعی سامانه را تعریف می‌کند، رفتارهایی مانند اطلاعات ترافیک شبکه، سابقه اطلاعات مربوط به آن رویداد و مصرف منابع. زمانی که هر گونه رفتار غیر طبیعی یا فعالیت غیر عادی در شبکه اتفاق می‌افتد به طوری که از رفتار طبیعی یا مشخصات پایه‌ای انحراف داشته باشد، سامانه هشداری را ایجاد می‌کند. با این حال تعریف رفتار طبیعی و نرمال کار چالش برانگیزی است، چون رفتار نرمال می‌تواند در بیشتر زمان‌ها تغییر کند که این مسئله می‌تواند منجر به بالا رفتن مثبت‌های دروغین شود: یعنی رفتارهایی که به صورت غیر عادی نیستند ولی به عنوان رفتارهای ناهنجار تشخیص داده شده‌اند [۱۵].

۲) تشخیص نفوذ مبتنی بر سوء استفاده: این نوع از سامانه‌های تشخیص نفوذ، با استفاده از مقایسه امضای حملات نگهداری شده با فعالیت‌های جاری، حملات و نفوذها را تشخیص می‌دهند. تشخیص نفوذهای مبتنی بر سوء استفاده، مؤثر و مفید هستند و نرخ مثبت دروغین کمتری دارند. ولی آن‌ها نمی‌توانند حملات جدید را تشخیص دهند و به صورت مکرر به به‌روزرسانی پایگاه‌های داده خود نیاز دارند. علاوه بر این، در این روش گره‌های تشخیص نفوذ به موجودیت‌های متمرکزی نیاز دارند تا ترافیک شبکه را جمع‌آوری و بررسی کنند. به علت محدودیت‌های سامانه‌های رایج مبتنی بر فهرست (لیست) امضاء، روش‌های تشخیص مبتنی بر رفتارهای غیر عادی بیشتر از تشخیص سوء استفاده مورد استفاده قرار می‌گیرند [۱۵].

۳) سامانه‌های تشخیص نفوذ مبتنی بر مشخصات: سامانه‌های تشخیص نفوذ مبتنی بر مشخصات، مزایای روش‌های تشخیص رفتارهای سوء استفاده و تشخیص رفتارهای خلاف قاعده را با هم ترکیب می‌کنند. این سامانه‌ها، یک مجموعه‌ای از محدودیت‌ها را تعریف می‌کنند. در این سامانه‌ها، عملیات صحیح یک پروتکل تعریف شده و رصد کردن شبکه با توجه به محدودیت‌های تعریف شده انجام می‌شود. این روش، نرخ مثبت‌های دروغین کمتری دارد و ممکن است توانایی تشخیص حملات ناشناخته را فراهم کند. تیسنگ و همکارانش [۱۶]، یک IDS مبتنی بر این روش را ارائه کرده‌اند. روش آن‌ها به منظور تعریف رفتار پروتکل مسیریابی AODV صحیح، از ماشین‌های حالت پایان‌پذیر استفاده می‌کند و رصد کردن شبکه به منظور تشخیص و توزیع زمان اجرای نقض (تخطی) از مشخصات تعریف شده، انجام می‌گیرد.

محققان، یک روش مبتنی بر منطق فازی را جهت شناسایی و مقابله با حملات سیاه‌چال ارائه دادند. مدل فازی ارائه شده در این روش، ۴ ماژول استخراج مؤلفه‌های فازی، ماژول محاسبات فازی، ماژول بررسی فازی و ماژول تولید بسته‌های هشدار را با پروتکل AODV تجمیع می‌کند. سامانه محاسبات فازی این راهکار، دو پارامتر میزان نرخ ارسال بسته و متوسط مقدار شماره سریال مقصد را از ماژول استخراج مؤلفه‌های فازی دریافت کرده و سپس با استفاده از این پارامترها و با بهره‌گیری از قوانین مختلف فازی و تابع‌های عضویت، به محاسبه سطح صداقت و وفاداری گره‌ها می‌پردازد. سپس میزان سطح صداقت و وفاداری محاسبه شده در این قسمت، با یک مقدار حد آستانه‌ای در ماژول بررسی فازی مقایسه شده تا در رابطه با رفتار گره تصمیم‌گیری شود. اگر سطح صداقت آن گره کمتر از حد آستانه باشد، یک بسته هشداری با شناسه گره مخرب شناسایی شده به صورت همه‌پخشی در شبکه منتشر می‌شود و به این ترتیب فعالیت گره‌های مخرب را در شبکه بلوکه می‌کنند. البته بدیهی است که بسیاری از روش‌های امنیتی ارائه شده در شبکه موردی تحت تأثیر توابع پایه امنیتی مانند درهم‌سازها و رمزنگارهاست [۱۷و ۱۸].

[1] End – to – End Delay
[2] Intrusion Detection Systems (IDS)

۳. سامانه پیشنهادی: دفاع مبتنی بر منطق فازی در برابر حملات سیاه‌چاله

راهکار فازی ارائه شده در این مقاله، توسط تک‌تک گره‌ها در شبکه اجرا می‌شود. بنابراین هر گره موجود در شبکه می‌تواند در رابطه با رفتار همسایگان خود تصمیم‌گیری کند. اگر همسایه مخرب باشد، در این حالت همانند روش‌های قبلی، یک بسته هشداری به صورت همه‌پخشی، در شبکه منتشر شده و از ادامه فعالیت گره مخرب، به صورت کامل جلوگیری می‌شود. اما اگر مقدار مشکوکیت یک گره، هنوز به حد آستان مخرب بودن نرسیده، در این حالت تا رسیدن مقدار مشکوکیت به حد آستان مخرب بودن، با بسته‌های ارسالی گره مشکوک به صورت فازی برخورد خواهد شد. به این ترتیب، ادامه فعالیت گره مشکوک در شبکه محدود خواهد شد.

در چهارچوب در نظر گرفته شده در این مقاله، دو نوع گره وجود دارد که این گره‌ها از دو الگوریتم اجرایی مجزا بهره می‌برند:

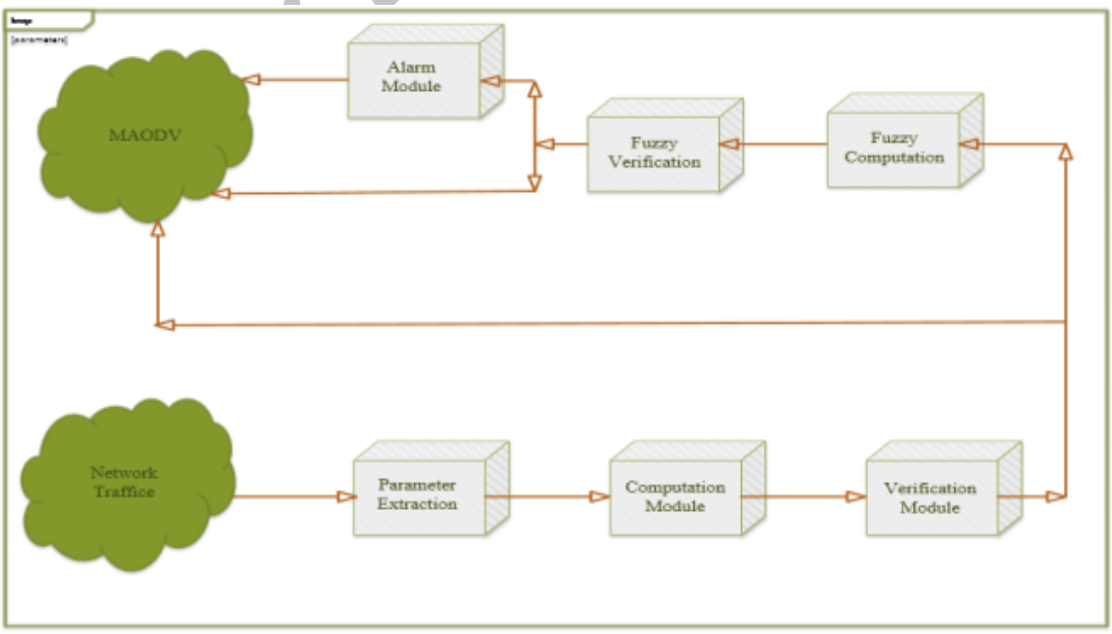
گره‌های مخرب: این گره‌ها، به منظور اعمال حملات سیاه‌چاله، در شبکه فعالیت می‌کنند و به این منظور از پروتکل مسیریابی Blackhole AODV استفاده می‌کنند.

گره‌های عادی: این گره‌ها از پروتکل مسیریابی MAODV، به منظور انجام عملیات مسیریابی استفاده می‌کنند. پروتکل MAODV، یک پروتکل بهبود یافته بر مبنای پروتکل AODV است. گره‌های عادی موجود در توپولوژی شبکه، با اجرای عملیات مسیریابی مبتنی بر پروتکلMAODV، قادر خواهند بود تا با بهره‌گیری از منطق فازی، گره‌های مخرب را در شبکه شناسایی نموده و درنهایت یک پیام بلوکه را به صورت همه‌پخشی در شبکه منتشر نمایند. به این ترتیب گره‌های مخرب در شبکه بلوکه خواهند شد. پروتکل MAODV، پروتکلی است که در این مقاله پیشنهاد و پیاده‌سازی شده است.

فرضیات انجام گرفته در راهکار پیشنهادی بدین شرح است:

- یک سازوکار احراز هویت، در شبکه‌های موردی سیار وجود دارد، به طوری که شناسه گره‌ها نمی‌تواند جعل شود و پیام بلوکه ارسال شده توسط گره‌های شبکه نمی‌تواند تغییر یا جعل یابد.
- گره‌هایی که در رنج انتقال یکدیگر واقع شده‌اند، می‌توانند پیام‌های بلوکه را به یکدیگر ارسال نمایند.
- از آنجایی که در راهکار ارائه شده، گره‌های معمولی از پروتکل مسیریابی MAODV جهت انجام عملیات مسیریابی استفاده می‌کنند، بنابراین می‌توان گفت راهکار پیشنهادی بدون استفاده از گره‌های ناظر و ایجاد هزینه اضافی، می‌تواند نزدیک به ۱۰۰٪ فضای کل شبکه را تحت پوشش قرار دهد.

مدل فازی ارائه شده در این مقاله، مطابق شکل (۴) پیاده‌سازی شده است. این مدل، شامل ۶ مؤلفه است، که عبارتند از: استخراج مؤلفه‌های مورد نیاز برای سامانه فازی، ماژول محاسبات، ماژول بررسی و استنتاج‌ها، ماژول محاسبات فازی، ماژول بررسی و استنتاج‌ها فازی و ماژول تولید کننده بسته‌های هشدار. در ادامه هر یک از این ماژول‌ها توضیح داده می‌شوند.



شکل۴. مدل فازی ارائه‌شده

۳-۱. ماژول استنتاج پارامترهای فازی

ورودی‌های سامانه فازی در گره i از دو طریق استنتاج می‌شود:

- از طریق گوش کردن به ترافیک دریافت شده، از گره‌های همسایه‌ای که در فاصله یک گامی گره i قرار دارند. از این طریق مقدار شماره سریال مقصد هر گره به همراه شناسه گره همسایه استخراج خواهد شد.

- در زمان ارسال بسته RREQ، گره مبدأ فیلدهای مورد نیاز خود شامل مقدار شناسه گره مبدأ، شناسه گره مقصد و مقدار شماره سریال مقصد بسته RREQ را استخراج می‌کند.

کلیه فیلدهای استخراج شده در یک لیست پیوندی به نام Seqinfo نگهداری می‌شوند. به این ترتیب در این لیست پیوندی، مقدار شناسه گره مقصد (Dest_id) و مقدار شماره سریال مقصد بسته RREQ (Dest_seqno) نگهداری می‌شود. با استفاده از اطلاعات موجود در این لیست پیوندی و مقایسه آن با اطلاعات موجود در بسته RREP دریافتی، می‌توان رشد غیر عادی شماره سریال مقصد موجود در بسته‌های RREP را تشخیص داده و بر اساس آن گره‌های مشکوک موجود در شبکه را شناسایی کرد.

به این ترتیب علاوه بر جداول مسیریابی، یک لیست جدیدی به نام Seqinfo، در هر گره وجود دارد، که در آن اطلاعات مربوط به هر همسایه و گره‌هایی که با آن‌ها قبلاً ارتباطی برقرار شده است، نگهداری می‌شود. هر گره در حالت بی‌قاعده[1] کار می‌کند، به طوری که می‌تواند به مسیریابی و ترافیک همسایگان خود گوش کند و از این طریق، اطلاعاتی را برای سامانه فازی جمع‌آوری کند. هنگامی که بسته RREQ ارسال می‌شود، گره مبدأ با استفاده از شبه کد زیر، مقدار شناسi گره مقصد(Dest_id) و مقدار شماره سریال مقصد بسته RREQ (Dest_seqno)، را از اطلاعات فیلدهای RREQ ارسالی و یا اطلاعات موجود در جدول مسیریابی خود (Routing Table) استنتاج کرده و در لیست Seqinfo قرار می‌دهد:

```
Send Request()
If (Packet. Dest_id  is in Routing Table) and
(Packet.Dest_id. Dest_seqno < Routing Table.Dest_id.
Dest_seqno) then
   Replace Seqinfo.Dest_seqno With Routing
RoutingTable.Dest_seqno
Else
   Replace Seqinfo.Dest_seqno With Packet.Dest_seqno
End if;
```

علت استفاده از فیلد مقدار شماره سریال مقصد را می‌توان به این صورت بیان کرد: در بسته RREP از پروتکل AODV، گره مقصد مقدار شماره سریال به‌روز شده خود را منتقل می‌کند. مقدار شماره سریال یک گره خاص، به تعداد اتصالات آن گره، وابسته است. گرهی که مقدار شماره سریال بزرگ‌تری داشته باشد، به عنوان یک گره قابل اعتماد در پروتکل AODV شناخته می‌شود. گره مقصد در شبکه، مقدار بزرگی را برای شماره سریال خود معرفی می‌کند تا به این طریق خود را به عنوان گره مقصد معرفی کند. بنابراین اگر گرهی بخواهد به عنوان گره سیاه‌چاله در شبکه فعالیت کند، می‌بایست مقدار شماره سریال خود را به بالاترین مقدار تنظیم کند تا به این طریق بتواند خود را به عنوان گره مقصد وانمود کند. در نتیجه می‌توان رفتار گره را بر اساس مقدار شماره سریال آن بررسی کرد.

۳-۲. واحد محاسبات

این واحد در هر بازه زمانی، متوسط مقدار تفاوت شماره سریال مقصد را از طریق شماره سریال‌های متعلق به هر گره خاص موجود در لیست Seqinfo محاسبه می‌کند. به این منظور، متوسط مقدار x از بین D داده دریافتی در N بازه زمانی محاسبه می‌شود:

$$\bar{x}_D = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (۵)$$

بازه‌های زمانی که متوسط مقدار شماره سریال مقصد به‌روزرسانی می‌شود برابر است با زمانی که گره i، مقدار شماره سریال جدیدی برای یک گره موجود در لیست Seqinfo دریافت می‌کند.

سپس به محض اینکه گره i بسته RREP را دریافت کرد، شناسه گره فرستنده RREP را از ساختار Seqinfo جستجو می‌کند. سپس فاصله مقدار ورودی نمونه x را با متوسط مقدار محاسبه شده از رابطه (۵) برآورد می‌شود:

$$d(x) = |x - \bar{x}_D|^2 \qquad (۶)$$

۳-۳. واحد بررسی

روش کاری این واحد به این ترتیب خواهد بود که زمانی که گره i پیام RREP را دریافت کرد، این گره ابتدا بررسی می‌کند که آیا گره‌ای که RREP را ارسال کرده، گره مقصد است؟ اگر بله، هیچ پردازشی نیاز نیست.

در مرحله دوم، گره i بررسی می‌کند که آیا شناسه گره‌ای که بسته RREP را ارسال کرده است، در لیست سیاه وجود دارد یا

[1] Promiscuous

نه؟ اگر بله، بسته RREP دریافتی را دور می‌ریزد، در غیر این صورت، مرحله سوم اجرا می‌شود.

مرحله سوم، زمانی اتفاق می‌افتد که بسته RREP از جانب گره میانی ارسال می‌شود، به طوری که شناسه این گره در لیست سیاه وجود ندارد. در این حالت، مقایسه‌ای مابین مقدار d(x) و مقدار α(Seqinfo.dest.seq) انجام می‌گیرد. چنانچه مقدار d(x) عددی کوچک‌تر از α(Seqinfo.NodeID.dest.seq) باشد، در این حالت از بسته RREP ارسال شده استفاده می‌شود، در غیر این صورت مرحله فازی اجرا خواهد شد. مقدار α(Seqinfo.NodeID.dest.seq) از رابطه (۷) محاسبه می‌شود.

$$\alpha(\text{Seqinfo. NodeID. dest. seq}) = \begin{cases} T_{\text{h}}(BL)\ \ (MAX(\text{Seqinfo.}\mathit{dest.seq})) \\ \quad if\ \text{Seqinfo. NodeID. dest. seq} = 0 \\ \quad - - - - - - \\ T_{\text{h}}(BL)\ \ (\text{Seqinfo.}\mathit{NodeID.dest.seq}) \\ \quad if\ \text{Seqinfo. NodeID. dest. seq} \neq 0 \end{cases} \quad (۷)$$

روش عملکرد این رابطه به این صورت است که، به محض اینکه بسته RREP توسط گره مبدأ دریافت شد، این گره شناسه گره ارسال کننده بسته RREP را در لیست Seqinfo جستجو می‌کند. چنانچه قبلاً بسته‌ای به آن گره ارسال شده باشد، حتماً فیلد شماره سریال مقصد مربوط به آن گره در لیست پیوندی مقداری غیر صفر خواهد داشت. چنانچه مقدار شماره سریال مقصد موجود در بسته RREP از $T_{\text{h}}(BL)$ برابر مقدار ثبت شده در این لیست برای همان گره بزرگ‌تر باشد، در این حالت به آن گره مشکوک خواهد شد. ولی چنانچه بسته RREQ ارسالی برای اولین بار به سمت مقصد مورد نظر ارسال می‌شود، در این حالت فیلد شماره سریال مقصد برای گره مورد نظر در لیست Seqinfo دارای مقدار صفر خواهد بود. در این حالت مقدار شماره سریال موجود در بسته RREP دریافتی توسط گره مبدأ، با $T_{\text{h}}(BL)$ برابر بیشینه مقدار ثبت شده در لیست Seqinfo مقایسه خواهد شد. بیشینه مقدار شماره سریال موجود در این لیست، بدون توجه به شناسه گره‌ها و فقط بر اساس مقدار شماره سریال مقصد محاسبه خواهد شد. حال چنانچه مقدار شماره سریال مقصد موجود در بسته RREP از $T_{\text{h}}(BL)$ برابر بیشینه مقدار شماره سریال مقصد ثبت شده در لیست Seqinfo بزرگ‌تر باشد، در این حالت باز هم به آن گره مشکوک خواهد شد. بنابراین در واحد بررسی، مقایسه‌ای مطابق رابطه (۸) انجام می‌گیرد و بر اساس نتایج استخراج شده از این مقایسه، گره‌های مشکوک شناسایی خواهند شد.

$$\begin{cases} \text{d(x)} > \alpha(\text{Seqinfo. dest. seq}) \ \Rightarrow \text{Suspecious} \\ \text{d(x)} \leq \alpha(\text{Seqinfo. dest. seq}) \ \Rightarrow \text{Normal} \end{cases} \quad (۸)$$

۳-۴. واحد محاسبات فازی

چنانچه بررسی‌های انجام شده طبق رابطه (۸)، بر مشکوک بودن گره دلالت داشته باشد، در این حالت مقدار مشکوکیت گره در این واحد محاسبه خواهد شد. در راهکار پیشنهادی علاوه بر لیست پیوندی Seqinfo، لیست دیگری به پروتکل AODV اضافه خواهد شد. لیست پیوندی جدید Susinfo نام دارد. در این لیست، شناسه گره مشکوک به همراه مقدار مشکوکیت آن نگهداری می‌شود. چنانچه طبق رابطه (۸)، به گره ارسال کننده بسته RREP مشکوک شدیم، در این حالت، گره مبدأ شناسه گره فرستنده پیام RREP را از لیست پیوندی SUSinfo جویا می‌شود. اگر شناسه گره در این لیست موجود نباشد، شناسه گره مشکوک، به همراه مقدار مشکوکیت ۱ به لیست SUSinfo اضافه می‌شود. در غیر این صورت فقط به مقدار مشکوکیت گره موجود در لیست SUSinfo یک واحد اضافه خواهد شد. مقدار مشکوکیت گره را با متغیر susval نشان داده شده است. بنابراین خواهید داشت:

$$\text{If} \ \rightarrow \ \text{susval} \ ++ \quad (۹)$$

Node: Suspeciou

۴-۵. واحد بررسی و استنتاج‌های فازی

این واحد مقدار مشکوکیت محاسبه شده در مرحله قبل را به عنوان ورودی دریافت می‌کند. سپس به منظور تصمیم‌گیری، در مورد مخرب بودن یا نبودن گره مظنون، مقدار مشکوکیت محاسبه شده برای گره مورد نظر را با مقدار حد آستانه مخرب بودن، یعنی مقدار $T_{\text{h}}(BL)$ مقایسه می‌کند:

$$\begin{cases} \text{susval(i)} \geq T_{\text{h}}(BL) \ \Rightarrow \text{BlakHole} \\ \text{susval(i)} < T_{\text{h}}(BL) \ \Rightarrow \text{Normal} \end{cases} \quad (۱۰)$$

چنانچه مقدار مشکوکیت گرهی، بزرگ‌تر یا مساوی حد آستانه مخرب بودن ($T_{\text{h}}(BL)$) باشد، در این حالت شناسه گره مخرب به لیست سیاه اضافه شده و بسته RREP دریافتی دور ریخته می‌شود. لیست سیاه، سومین لیست پیوندی است که با عنوان BlackList به پروتکل AODV اضافه می‌شود. در این لیست شناسه گره‌های مخرب نگهداری می‌شوند. چنانچه بر اساس رابطه (۱۰)، مخرب بودن گرهی تشخیص داده شود، در این حالت علاوه بر اینکه شناسه گره مخرب به لیست سیاه اضافه می‌شود، ماژول تولید کننده بسته هشدار نیز، یک بسته هشداری با شناسه گره مخرب تولید و در شبکه منتشر می‌کند تا از ادامه فعالیت گره مخرب در شبکه جلوگیری شود، در غیر این صورت، با گره مشکوک به صورت فازی برخورد خواهد شد.

واحد بررسی فازی، بر اساس مقدار مشکوکیت محاسبه شده برای گره مورد نظر و مقدار حد آستانه مخرب بودن، یک خروجی به نام سطح مشکوکیت ایجاد می‌کند. قوانین فازی جهت تعیین سطح مشکوکیت گره در ادامه آورده شده است.

الف) هر چه مقدار مشکوکیت گره موجود در ساختار Suspect، به مقدار حد آستانه مخرب بودن$(BL)_{\mathrm{h}}T$ نزدیک‌تر باشد، با گره مشکوک شناسایی شده با شدت بیشتری برخورد خواهد شد.

ب) اگر مقدار مشکوکیت گره مذکور، به مقدار۲/ $(BL)_{\mathrm{h}}T$ نزدیک باشد، در این حالت با گره مشکوک با شدت ملایم برخورد خواهد شد.

ج) چنانچه مقدار مشکوکیت گره موجود در ساختار Susinfo، به مقدار صفر نزدیک باشد، در این حالت با گره مذکور با شدت کمی برخورد خواهد شد.

سپس با بهره‌گیری از قوانین فازی، یک تابع عضویت به نام تابع عضویت در مجموعه حذف بسته را تعریف می‌شود. این تابع در رابطه (۱۱) آورده شده است.

$$A(x)=\begin{cases}1 & \text{if} \quad \mathrm{x} \geq T_{\mathrm{h}}(BL)\\ 0.25\mathrm{x} & \text{if} \quad \mathrm{x} < T_{\mathrm{h}}(BL)\end{cases} \qquad (۱۱)$$

اگر تابع A(x) را به عنوان تابع عضویت در مجموعه حذف بسته دریافتی از جانب گره مظنون و متغیر x را مقدار مشکوکیت گره در نظر بگیرید، می‌توان گفت با افزایش سطح مشکوکیت گره مهاجم، میزان عضویت پیام ارسال شده از طرف آن گره در مجموعه حذف بسته، بیشتر خواهد شد. به طوری که چنانچه نتایج بررسی‌ها در سامانه فازی تعریف شده، بر حذف بسته دریافتی دلالت داشته باشد، در این حالت بسته RREP ارسالی از طرف گره مظنون با امکان بالایی حذف خواهد شد، حتی اگر مقدار مشکوکیت آن گره هنوز به حد مخرب بودن نرسیده باشد.

در حقیقت تفاوت روش پیشنهاد شده با روش‌های قبلی ارائه شده در این است که در روش‌هایی که تا به حال ارائه شده است، تا زمانی که مقدار مشکوکیت گرهی به حد آستان مخرب بودن برسد، از ۱۰۰٪ بسته‌های RREP ارسالی توسط گره مخرب، در شبکه استفاده می‌شود. در نتیجه گره مخرب فرصت بیشتری برای انجام فعالیت‌های مخربانه خود دارد و شبکه را بیشتر تحت تأثیر قرار می‌دهد. در حالی که در روش پیشنهاد شده بعد از شناسایی گره مخرب در شبکه، به تدریج که میزان مشکوکیت آن گره افزایش می‌یابد، از بسته‌های ارسال‌شده توسط آن گره کمتر استفاده می‌شود، تا زمانی که مقدار مشکوکیت گره مذکور به حد آستانه مخرب بودن برسد؛ که در این حالت دیگر از ۱۰۰٪ بسته‌های ارسال شده توسط گره مخرب استفاده نخواهد شد. با اجرای راه‌کار پیشنهادی می‌توان تا زمان تشخیص قطعی گره‌های مخرب، انجام عملیات مخربانه گره مهاجم را در شبکه دچار اختلال کرد، به طوری که در طول مدت زمانی که از زمان تشخیص گره مشکوک تا رسیدن مقدار مشکوکیت مذکور به حد آستانه مخرب بودن و بلوکه کردن این گره طول می‌کشد، کمترین آسیب به شبکه وارد شود.

۴. شبیه‌سازی روش پیشنهادی و ارزیابی نتایج

در این مقاله جهت پیاده‌سازی و ارزیابی عملکرد راه‌کار پیشنهادی، از شبیه‌ساز ns-2 استفاده شده است. در ادامه، سناریوهای مختلفی پیاده‌سازی شده است که در جدول (۱) می‌توان پارامترهای شبیه‌سازی را که در آن سناریوها استفاده شده است، مشاهده کرد. به منظور ارزیابی کارایی، روش پیشنهاد شده را با روش‌های مرسوم قبلی یعنی استفاده از دومین بسته RREP و DPRAODV مقایسه خواهد شد.

جدول ۱. پارامترهای شبیه‌سازی

ناحیه تحت پوشش شبکه	۷۵۰×۷۵۰m^2
تعداد گره نرمال	۱۵
تعداد گره‌های مخرب	۱/۲
رنج انتقال	۲۵۰m
زمان شبیه‌سازی	۵۰۰s
الگوی حرکت گره‌ها	تصادفی
نوع ترافیک	UDP-CBR
سایز بسته‌ها	۵۱۲Byte
حداکثر سرعت	۲۰m/s

۴-۱. پارامترهای شبیه‌سازی

شبکه‌های موردی سیار از پروتکل UDP، برای انجام فعالیت‌های شبکه‌ای خود استفاده می‌کنند. به همین منظور، در طول شبیه‌سازی، از این پروتکل استفاده خواهد شد. در این پروتکل، اگر گره مخربی بسته‌های ارسالی از طرف گره مبدأ را حذف نماید، به دلیل وجود ویژگی‌های ذاتی پروتکل UDP، گره مبدأ از نرسیدن بسته‌های ارسالی خود به مقصد مورد نظر مطلع نمی‌شود و همچنان به ارسال بسته‌های داده ادامه می‌دهد. در حالی که اگر از پروتکل TCP استفاده می‌شد، در چنین حالتی، گره مبدأ ارسال بسته‌های خود را متوقف می‌کرد. زیرا در پروتکل TCP، چنانچه گره مبدأ بعد از ارسال بسته‌های داده پیام TCP ACK را دریافت نکند، به اتصال خود خاتمه خواهد داد. پارامترهای پیش‌فرض مختلف مانند رسانه انتقال داده، نوع واسط شبکه، پروتکلMAC، نوع لایه لینک، نوع صف و آنتن برای کلیه سناریوها یکسان هستند. پارامترهای پیش فرض دیگر، مانند فایل مسیر حرکت گره‌ها و فایل ایجاد ترافیک، می‌بایست متناسب با سناریوها، به صورت جداگانه، ایجاد شده و در فایل tcl به آن‌ها اشاره شود.

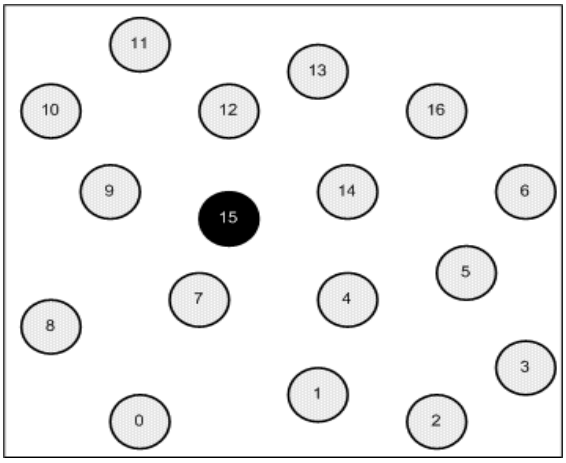
سناریوهای ما، در یک ناحیه مربعی شکل، با مقیاس ۷۵۰×۷۵۰m^2 پیاده‌سازی شده است. نرخ انتقال در استاندارد IEEE 802.11 در محیط ns-2، ۲۵۰m است و این حداکثر فاصله

ممکن بین گره‌های متحرک است. زوج‌های مبدأ و مقصد به صورت تصادفی در کل شبکه گسترش می‌یابند. میزان بار ترافیکی در گره‌های مبدأ، بر اساس مقادیر تعریف شده در منابع CBR متغیر است. هر گره حرکت خود را از یک محل تصادفی، متناسب با پارامترهای سرعت تعریف شده در هر سناریو آغاز می‌کند. همه مقادیر پارامترهای شبیه‌سازی در جدول (۱) نمایش داده شده است.

در این مقاله، تأثیر حملات سیاه‌چاله از دو بعد بررسی می‌شود: در بعد اول نرخ بسته‌های حذف شده را بر اساس تعداد گره‌های سیاه‌چاله موجود در شبکه بررسی می‌شود. در بعد دوم، علاوه بر تعداد گره‌های مخرب، تأثیر سرعت حرکت گره‌ها و جابه‌جایی آن‌ها در میزان بسته‌های حذف شده را، بررسی خواهد شد.

۴-۲. بررسی تأثیر تعداد گره‌های سیاه‌چاله در نرخ حذف بسته‌ها

به منظور ارزیابی و مقایسه روش پیشنهاد شده با تعدادی از روش‌های مرسوم، سناریویی را با پارامترهای موجود در جدول (۱) پیاده‌سازی کرده و سپس ابتدا یک و سپس دو گره سیاه‌چاله به سناریو اضافه می‌شود. سپس نتایج حاصل از شبیه‌سازی روش پیشنهاد شده را با روش‌های مرسوم قبلی، مانند استفاده از دومین بسته RREP و روش DPRAODV، مقایسه خواهد شد. شکل (۵)، نمایی از سناریو شبیه‌سازی اول را نشان می‌دهد.



شکل ۵. نمایی از سناریو پیاده‌سازی شده اول: جهت ارزیابی نتایج روش پیشنهادی با یک گره سیاه‌چاله

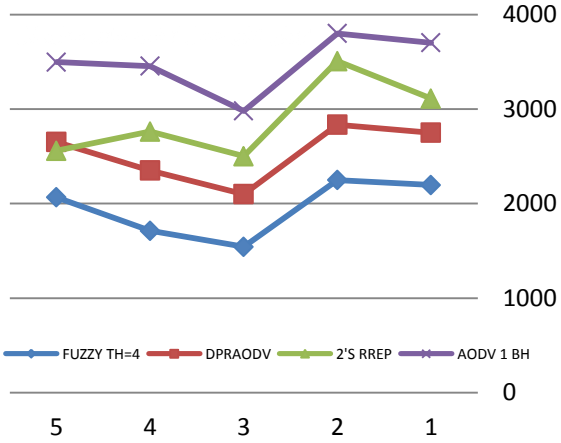
به منظور ارزیابی و سنجش کارایی روش پیشنهاد شده در سناریوی پیاده‌سازی شده در شکل (۵)، در مرحله اول میزان بسته های حذف شده را بدون وجود حمله، یعنی گره مهاجم ۱۵ و تحت پروتکلAODV به‌دست آورده می‌شود. نتایج شبیه‌سازی نشان می‌دهد که تعداد بسته‌های حذف شده در این حالت ۷۹۸۰ بسته خواهد بود. با اضافه کردن گره سیاه‌چال ۱۵، تعداد بسته‌های حذف شده تحت پروتکل AODV، به ۱۷۴۳۷ بسته افزایش می‌یابد. حال به منظور مقایسه روش پیشنهاد شده در این مقاله با روش‌های قبلی، ابتدا روش استفاده از دومین بسته RREP را پیاده‌سازی می‌شود. بعد از اعمال روش 2's RREP، تعداد بسته های حذف شده، به ۱۴۴۴۴ بسته می‌رسد که نسبت به پروتکل AODV نرمال ٪۲۰/۷۲ بهبود داشته است.

در مرحله بعد، روش استفاده از DPRAODV پیاده‌سازی شده، و نتایج حاصل از شبیه‌سازی ارزیابی می‌گردد. به منظور پیاده‌سازی این روش، تغییرات روی تابع recv Reply از پروتکل AODV اعمال خواهد شد. درنهایت، نتایج حاصل از پیاده‌سازی این روش نشان می‌دهد که تعداد بسته‌های حذف شده در سناریوی شکل (۵)، در مقدار حد آستانه ۳ به ۱۲۵۲۱ بسته می‌رسد که نسبت به پروتکل AODV نرمال تعداد بسته‌های حذف شده ٪۳۹/۲۶ کاهش یافته است و شرایط شبکه بهتر شده است. مقایسه این روش با روش استفاده از 2's RREP، نشان دهنده بهبود وضعیت، به میزان ٪۱۳/۸۲ است.

حال همین روش به صورت فازی، به شبکه اعمال می‌گردد. نتایج به‌دست آمده از شبیه‌سازی، نشان دهنده آن است که اگر مقدار حد آستانه ۳ انتخاب شود، تعداد بسته‌های حذف شد به ۹۷۵۹ بسته می‌رسد که این نشان دهنده بهبود وضعیت شبکه از لحاظ تعداد بسته‌های حذف شده به میزان ٪۷۸/۶۷ است. جدول (۲)، نتایج حاصل از انجام شبیه‌سازی روش‌های فوق را به صورت جدولی نشان می‌دهد. همان‌طور که در جدول (۲) نیز نشان داده شده است، در روش‌های DPRAODV و Fuzzy، با افزایش مقدار حد آستانه، تعداد بسته‌های حذف شده ما افزایش می‌یابد. چرا که با افزایش مقدار حد آستانه، گره مخرب مدت زمان زیادی تا زمان بلوکه شدن فرصت دارد، از این رو، این گره همچنان به عملیات مخربانه خود ادامه می‌دهد. از آن جایی که اگر حد آستانه را خیلی کم مانند ۳ در نظر بگیرد، ممکن است در برخی موارد گره‌های نرمال را هم به عنوان گره مخرب تشخیص دهد و اگر حد آستانه را زیاد در نظر بگیرد مانند ۶، در این حالت هم گره مخرب می‌تواند تعداد بسته‌های بیشتری را حذف کند، بهترین مقدار برای حد آستانه ۴ در نظر گرفته می‌شود. شکل (۶) تفاوت روش پیشنهاد شده را با روش‌های قبلی در قالب یک نمودار نشان می‌دهد.

جدول ۲. نتایج حاصل از شبیه‌سازی سناریو اول با یک گره سیاه‌چاله

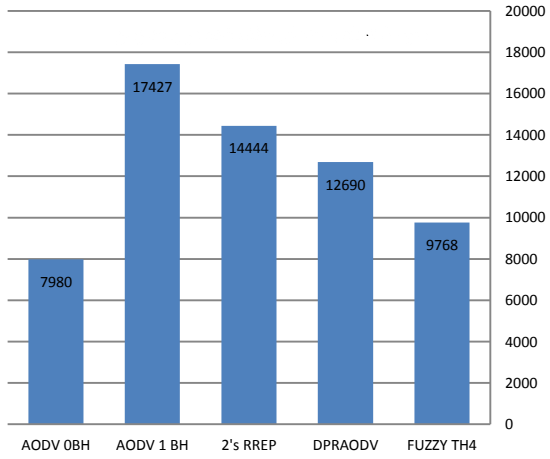
Protocol Name	BH no	Drop	Th=3	Th=4	Th=5	Th=6
AODV	۰	۷۹۸۰				
AODV	۱	۱۷۴۳۷				
2's RREP	۱	۱۴۴۴۴				
DPRAODV	۱		۱۲۵۲۱	۱۲۶۹۰	۱۲۷۶۹	۱۲۸۴۶
Fuzzy	۱		۹۷۵۹	۹۷۶۸	۱۲۵۲۱	۱۲۶۸۶



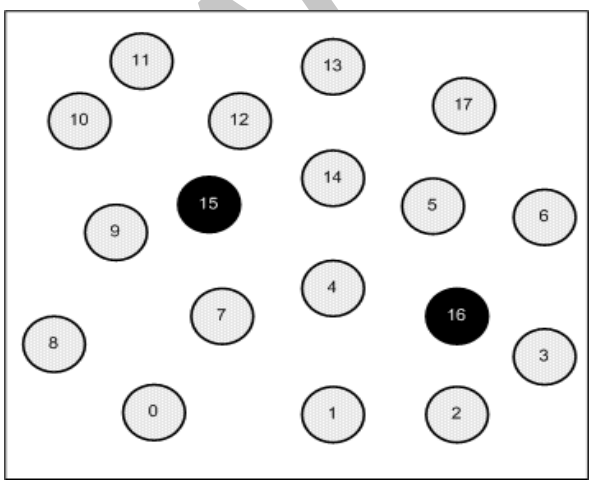
شکل ۶. مقایسه و ارزیابی کارایی روش فازی و مقایسه آن با دیگر روش‌ها در سناریو اول با یک گره سیاه‌چاله از نظر تعداد بسته‌های حذف شده در واحد زمان

همان‌طور که در شکل(۶) نیز نشان داده شده است، تعداد بسته‌های حذف شده در روش منطق فازی نسبت به روش‌های قبلی بهبود یافته است. شکل (۷) متوسط تعداد بسته‌های حذف شده را در سناریو اول و در طول مدت شبیه‌سازی نشان می‌دهد. به منظور ارزیابی کارایی روش منطق فازی در تعداد گره‌های مخرب بیشتر، گره سیاه‌چاله دوم را به سناریوی خود اضافه می‌کنیم. در این حالت نمایی از سناریوی جدید به صورت شکل (۸) است. همان‌طور که در جدول (۳) نشان داده شده است، تعداد بسته‌های حذف شده در سناریوی شکل (۸) با وجود ۲ گره سیاه‌چاله و تحت پروتکل AODV به ۱۸۸۰۷ بسته می‌رسد که نسبت به حالتی که هیچ گره مخربی در شبکه وجود ندارد، نرخ حذف بسته‌ها ٪۱۳۵/۶۷ رشد پیدا کرده است. با اعمال پروتکل مسیریابی 2's RREP، تعداد بسته‌های حذف شده به ۱۴۵۱۴ بسته می‌رسد که نسبت به پروتکل AODV نرمال نرخ حذف بسته‌ها ٪۲۹/۵۷ بهبود داشته است. با اعمال پروتکل DPRAODV و انتخاب مقدار حد آستانه ۴، تعداد بسته‌های حذف شده به ۱۲۹۳۲ بسته می‌رسد که نشان دهنده بهبود نسبی ٪۱۲/۲۳ نسبت به روش 2's RREP است. با اعمال منطق فازی، تعداد بسته‌های حذف شده در حد آستانه ۴، به ۹۹۳۸ بسته می‌رسد که نسبت به روش DPRAODV ٪۳۰/۱۳ وضعیت بهبود یافته است و نسبت به پروتکل AODV نرخ بسته‌های حذف شده، ٪۸۹/۲۴ کاهش یافته است.

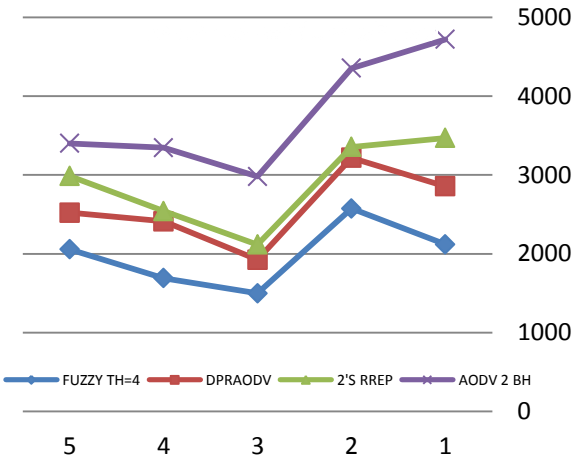
شکل (۹) تأثیر اعمال هر یک از پروتکل‌های مسیریابی ذکر شده را در سناریوی شکل (۸) نشان می‌دهد. شکل (۱۰)، متوسط تعداد بسته‌های حذف شده را در طول مدت شبیه‌سازی نشان می‌دهد.



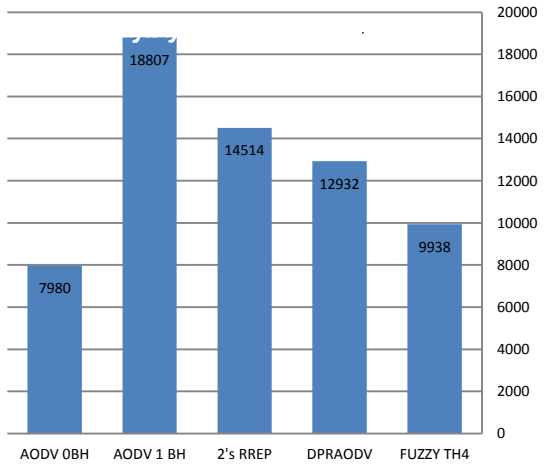
شکل ۷. متوسط تعداد بسته‌های حذف شده در پروتکل‌های شبیه‌سازی شده در طول مدت زمان شبیه‌سازی در سناریو اول با یک گره سیاه‌چاله



شکل ۸. نمایی از سناریو پیاده‌سازی شده دوم: جهت ارزیابی نتایج روش پیشنهادی با دو گره سیاه‌چاله



شکل ۹. مقایسه و ارزیابی کارایی روش فازی و مقایسه آن با دیگر روش‌ها در سناریو دوم با دو گره سیاه‌چاله از نظر تعداد بسته‌های حذف شده در واحد زمان



شکل ۱۰. متوسط تعداد بسته‌های حذف شده در پروتکل‌های شبیه‌سازی شده در طول مدت زمان شبیه‌سازی در سناریو دوم با دو گره سیاه‌چاله

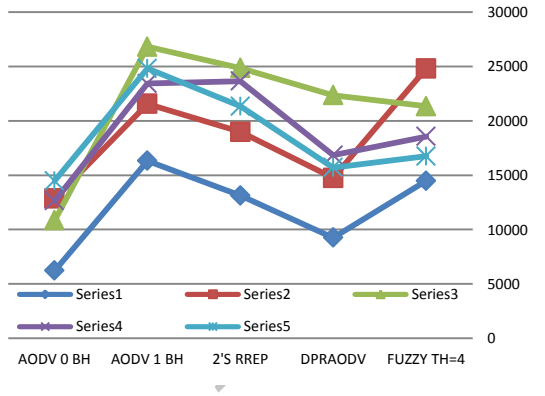
جدول ۳. نتایج حاصل از شبیه‌سازی سناریو دوم با دو گره سیاه‌چاله

Protocol Name	BH no	Drop	Th=3	Th=4	Th=5	Th=6
AODV	۰	۷۹۸۰				
AODV	۲	۱۸۸۰۷				
2's RREP	۲	۱۴۵۱۴				
DPRAODV	۲		۱۲۶۹۸	۱۲۹۳۲	۱۲۸۰۱	۱۲۷۵۶
Fuzzy	۲		۷۱۲۶	۹۹۳۸	۹۸۹۲	۱۰۳۲۶

۴-۳. تأثیر سرعت جابه‌جایی گره‌ها در نرخ حذف بسته‌ها

به منظور مشاهده تأثیر سرعت جابه‌جایی گره‌ها در نرخ حذف بسته‌ها، در همان سناریو موجود در شکل (۵)، نرخ بسته‌های حذف شده را با یک گره سیاه‌چاله و با سرعت حرکت گره‌ها برابر با ۲۰، ۳۰، ۴۰، ۵۰ و ۶۰ متر بر ثانیه به‌دست آورده می‌شود. نتایج حاصل از پیاده‌سازی مطابق با جدول (۴) نشان داده شده است.

شکل (۱۱) تأثیر سرعت حرکت گره‌ها، را در هر یک از پروتکل‌های مسیریابی ذکر شده در سناریوی شکل (۵) را نشان می‌دهد.



شکل ۱۱. مقایسه و ارزیابی کارایی روش فازی و مقایسه آن با دیگر روش‌ها در سرعت‌های متمایز از نظر تعداد بسته‌های حذف شده در واحد زمان

جدول ۴. نتایج حاصل از شبیه‌سازی سناریو اول با سرعت‌های حرکت مختلف و با حد آستانه ۴

Protocol Name	BH no	V=20	V=30	V=40	V=50	V=60
AODV	۰	۶۹۴۶	۱۰۸۹۷	۱۰۲۵۲	۱۱۱۳۳	۱۱۹۴۹
AODV	۱	۱۷۸۷۹	۲۲۹۷۳	۲۷۳۱۹	۲۴۶۲۹	۲۴۸۳۰
2's RREP	۱	۱۵۰۹۸	۱۹۱۹۵	۲۵۶۰۷	۲۴۵۱۷	۲۲۷۹۳
DPRAODV	۱	۹۲۱۷	۱۲۲۲۲	۱۷۰۲۱	۱۳۶۴۷	۱۴۶۵۸
Fuzzy	۱	۸۸۴۸	۱۱۷۷۰	۱۲۴۷۳	۱۲۴۹۹	۱۵۱۶۰

۵. نتیجه‌گیری

در این مقاله، شبکه‌های موردی سیار و ضعف‌های امنیتی موجود در این شبکه‌ها، با جزئیات مورد مطالعه قرار گرفت. پروتکل AODV، که یکی از پروتکل‌های مسیریابی محبوب و رایج در شبکه‌های موردی سیار است، با جزئیات کامل بیان شد. سپس حمله سیاه‌چاله را در پروتکل AODV مورد مطالعه قرار داده شد. راهکار پیشنهاد شده در این مقاله، از منطق فازی برای مقابله با حملات سیاه‌چاله در شبکه‌های موردی سیار استفاده کرده است. این روش با بهره‌گیری از روش استنتاج فازی، به شناسایی گره‌های مخرب در شبکه پرداخته و در صورت شناسایی، یک پیام بلوکه را به صورت همه پخشی مابین تمام گره‌های موجود در شبکه منتشر می‌کنند تا گره مهاجم را بلوکه کنند. نتایج شبیه‌سازی‌ها بعد از اعمال روش فوق، نشان دهنده بهبود وضعیت شبکه از لحاظ تعداد بسته‌های حذف شده است. این روش می‌تواند در کلیه ساختارهای دفاعی که از یک مقدار حد آستانه برای تشخیص گره مخرب استفاده می‌کنند، مفید واقع شود. چرا که در روش‌های تشخیص پیشین، تا رسیدن مقدار مشکوکیت به حد آستانه، از ٪۱۰۰ بسته‌های ارسالی توسط گره مخرب استفاده می‌شود. ولی در روش ارائه شده که بر مبنای استنتاج فازی است، با افزایش مقدار مشکوکیت گره، به صورت تدریجی از بسته‌های ارسال شده توسط گره مخرب کمتر استفاده خواهد شد، در نتیجه وجود گره مخرب، در کارایی شبکه، تأثیر کمتری خواهد داشت.

۶. مراجع

[1] Jamali, S.; Fotohi, R. “Defending against Wormhole Attack in MANET Using an Artificial Immune System”; New Review of Information Networking 2016, 21, 79-100.

[2] Al Jaroodi, J. “Routing Security in Open/Dynamic Mobile Ad Hoc Networks”; Int. Arab J. Inf. Tech. 2007, 1, 185-191.

[3] Mousapour, M. “Ad-hoc network security”; MSc Presentation, Amir Kabir University, 2001 (in Persian).

[4] Deswal, S.; Singh, S. “Implementation of Routing Security Aspects in AODV”; Int. J. Comput. Theory Eng. 2010, 1, 135-138.

[5] Berndt, L. K. “A Quick Guide to AODV Routing”; http://www.itl.nist.gov/div892/wctg/aodv_kernel/aodv_guide.pdf, 2013.

[6] Azar, A.; Faraji, H. “Fuzzy Management Science”; Mehrban Nashr, 2011 (In Persian).

[7] Su, M. U. “Prevention of Selective Blackhole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems”; Comput. Commun. 2011, 34, 107-117.

[8] Bathla, P.; Gupta, B. “Security Enhancements in AODV Routing Protocol”; Int. J. Comput. Sci. Tech. 2011, 2, 295-298.

[9] Dokurer, S.; Erten, Y. M.; Acar, C. E. “Performance Analysis of Ad-Hoc Networks under Black Hole Attacks”; Proc. IEEE Southeast Conf. 2007, 22-25, 148-153.

[10] Lu, S.; Li, L.; Lam, K.Y.; Jia, L. “SAODV: A MANET Routing Protocol that Can Withstand Black Hole Attack”; Lect. Notes Artif. Int. 2009, 2, 421-425.

[11] Mistry, N.; Jinwala, D. C.; Zaveri, M. “Improving AODV Protocol against Blackhole Attacks”; Proc. Int. Multi Conf. Engineers and Computer Scientist 2010, 17-19, 58-63.

[12] Tamilselvan, L.; Sanakaranarayanan, V. “Prevention of Co-Operative Blackhole Attack in MANET”; J. Netw. 2008, 3, 13-20.

[13] Tamilselvan, L.; Sankaranarayanan, V. “Prevention of Black Hole Attacks in MANET”; Proc. Int. Conf. Wireless Broadband and Ultra Wideband Communications 2007, 27-30, 148-169.

[14] Raj, P. N.; Swadas, P. B. “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV Based MANET”; Int. J. Comput. Sci. 2009, 3, 54-59.

[15] Abdelaziz, A. K.; Nafaa, M.; Salim, G. H. “Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks”; Proc. Int. Conf. on Computer Modeling and Simulation 2013, 10-12, 693-698.

[16] Tseng, C. H.; Wang, S. H.; Ko, C.; Levitt, K. “DEMEM: Distributed Evidence Driven Message Exchange Intrusion Detection Model for MANET”; Proc. Int. Conf. on Recent Advances in Intrusion Detection 2006, 20-22, 249-271.

[17] Kulbhushan, S. J. “Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET”; IJCA Netw. Secur. Lect. Notes 2011, 4, 124-139.

[18] Asgari M.; Jamali, S.; Nikzad N. “A Novel Keyed Parallel Hashing Scheme Based on a New Chaotic System”; Chaos, Solitons & Fractals 2016, 87, 216-225.