یک روش مبتنی بر سیستم ایمنی مصنوعی جهت دفاع در برابر حملات کرم‌چاله در شبکه‌های موردی سیار

شهرام جمالی[۱]، دانشیار؛ رضا فتوحی سلاله، دانش‌آموخته کارشناسی ارشد؛ مرتضی آنالوئی[۲]، دانشیار

۱- گروه مهندسی کامپیوتر - دانشگاه محقق اردبیلی - اردبیل - ایران - jamali@uma.ac.ir
۲- دانشکده مهندسی کامپیوتر - دانشگاه علم و صنعت ایران - تهران - ایران - analoui@iust.ac.ir

چکیده: شبکه‌های موردی سیار، شبکه‌های بدون ساختاری هستند که در آن گره‌ها به‌شکل بی‌سیم باهم ارتباط برقرار می‌کنند؛ اما این شبکه‌ها با نگرانی‌های امنیتی جدی که ریشه در بی‌سیم بودن کانال دارد، مواجه‌اند. یکی از این نگرانی‌ها حمله کرم‌چاله هست. حمله کرم‌چاله به‌عنوان یک حمله ماهرانه تلقی می‌شود که در آن دو مهاجم فعال با ایجاد یک تونل خصوصی مجازی، جریان عادی حرکت پیام‌ها را اتصال کوتاه می‌کنند و با این روش دو گره غیر مجاور را به‌عنوان گره‌های همسایه معرفی می‌کنند. به‌این‌ترتیب مسیر عبوری از این گره‌ها به‌عنوان کوتاه‌ترین مسیر ممکن بین مبدأ و مقصد تلقی می‌شود. نتیجه این است که کل بسته‌ها به این مسیر هدایت می‌شوند و لذا ممکن است توسط این گره‌های مهاجم حذف شوند. در این مقاله، جهت طراحی مکانیسم دفاعی در برابر حملات کرم‌چاله، از سیستم ایمنی بدن انسان الهام گرفته‌شده است. در نگاشت انجام‌شده مسیرهای ناامن معادل آنتی‌ژن در نظر گرفته می‌شود که توسط الگوهای آموزش‌یافته مبتنی بر آنتی‌بادی کشف و از چرخه مسیریابی خارج می‌شوند. نتایج حاصل از شبیه‌سازی در محیط شبیه‌ساز NS-2 نشان می‌دهد که کارایی الگوریتم دفاعی پیشنهادی که WAAIS (Defense Against Wormhole Attack using Artificial Immune System) نام‌گذاری شده است، از نقطه‌نظر نسبت تحویل بسته، نرخ بسته‌های حذف‌شده توسط مهاجمین و میانگین تأخیر انتها به انتها، در مقایسه با روش‌های WormPlanar و AODV از کارایی بالاتری برخوردار است.

واژه‌های کلیدی: WAAIS، سیستم ایمنی مصنوعی، حمله کرم‌چاله، شبکه‌های موردی سیار.

An Artificial Immune System based Method for Defense against Wormhole Attack in Mobile Adhoc Networks

S. Jamali[1], Associate Professor; R. Fotohi, MSc; M. Analoui[2], Associate Professor

1- Department of Computer Engineering, University of Mohaghegh Ardabili, Ardabil, Iran, Email: jamali@iust.ac.ir
2- Department of Computer Engineering, Iran University of Science and Technology (IUST), Tehran, Iran, Email: analoui @iust.ac.ir

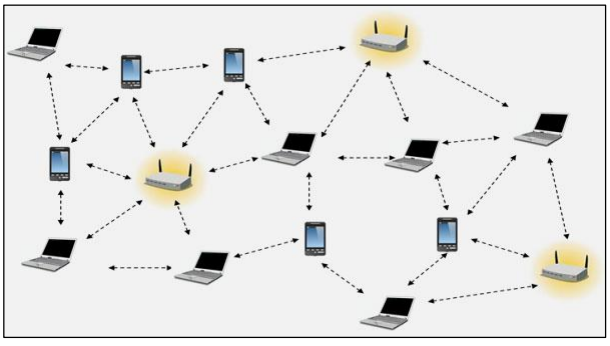
Abstract: Mobile ad hoc networks (MANETs) are structure-less networks in which the mobile nodes are communicate wirelessly with each other's. This wireless channel makes the MANETs vulnerable against different types of attacks. Wormhole is one of these attacks, according to which, two active attackers create a virtual private communication tunnel; reduce message normal stream and pretend two non-neighbored nodes as neighbors. In this way, the path between these two nodes is pretended as the shortest possible route between the source and the destination. Thus, all data packets passing through this route can be eliminated by these attacker nodes. This paper inspires from human immune system to design a defense mechanism against wormhole attack, called WAAIS (Wormhole Attack Artificial Immune System). In this proposed mapping, all unsecure routes, are considered as antigen. These unsecure routes are recognized by some rules, which are considered as antibody. The simulation results show that WAAIS outperforms WormPlanar and AODV in terms of packet delivery rate, average end-to-end delay and drop packets rate.

Keywords: WAAIS, Artificial Immune System, Wormhole attack, Mobile Ad-Hoc Networks (MANETs).

تاریخ ارسال مقاله: ۱۳۹۵/۰۳/۲۸
تاریخ اصلاح مقاله: ۱۳۹۵/۰۸/۰۹
تاریخ پذیرش مقاله: ۱۳۹۵/۱۰/۲۶
نام نویسنده مسئول: شهرام جمالی
نشانی نویسنده مسئول: ایران - اردبیل خیابان دانشگاه - دانشگاه محقق اردبیلی - دانشکده فنی و مهندسی.

۱- مقدمه

شبکه‌های موردی سیار[1] شامل مجموعه‌ای از گره‌های توزیع‌شده هستند که بدون هیچ زیرساخت یا مدیریت مرکزی، یک شبکه موقت را تشکیل می‌دهند. این نوع شبکه‌ها ارتباط بی‌سیم در بین تجهیزات غیر همگن را در هر زمان و هر مکان و بدون هیچ زیرساختی، فراهم می‌کنند. همان‌طور که در شکل ۱ نشان داده شده است، این تجهیزات شامل تلفن همراه، لپ‌تاپ‌ها و غیره است. در چنین شبکه‌هایی، هر گره سیار نه‌تنها به‌عنوان یک میزبان عمل می‌کند، بلکه می‌تواند به‌عنوان یک مسیریاب، ارسال و حمل بسته‌ها به گره‌های سیار دیگر را در شبکه انجام دهد. همه گره‌های شبکه در قالب پروتکل‌های مختلف مسیریابی در فرآیند کشف مسیر چندگانه مشارکت می‌کنند. به این معنی که بسته می‌تواند از گره مبدأ به گره مقصد از طریق چند گره در سراسر شبکه حرکت کند [۱، ۲]. متأسفانه، علیرغم مزایای خوب شبکه‌های موردی، این شبکه‌ها ساختار مرکزی امنی ندارند و به‌شدت در معرض حملات مخرب ازجمله حمله کرم‌چاله[2] قرار می‌گیرند. حمله کرم‌چاله یکی از تهدیدآمیزترین و خطرناک‌ترین حملات بشمار می‌رود که معمولاً توسط دو گره مخرب انجام می‌شود. دو گره مخرب یکی در نزدیکی گره مبدأ و دیگری در نزدیکی گره مقصد به ارسال و دریافت پیام مسیریابی به یکدیگر از طریق کانال مجزا می‌پردازند. در این حمله اگرچه دو گره مخرب دور از یکدیگر می‌باشند، اما به‌نظر می‌رسد که در محدوده ارتباطی یک گامی همدیگر قرارگرفته‌اند؛ بنابراین، مسیر عبوری از طریق گره‌های مخرب کوتاه‌تر از سایر مسیرها خواهد بود. نتیجه این است که این مسیر به‌عنوان مسیر نهایی انتخاب می‌شود و لذا گره‌های مهاجم می‌توانند به‌آسانی اطلاعات ارسالی از گره مبدأ به گره مقصد را بربایند و بسته‌های ارسالی از این مسیر را به‌صورت انتخابی حذف کنند. هدف این مقاله این است که یک الگوریتم مبتنی بر سیستم ایمنی مصنوعی[3] برای کشف و حذف حمله کرم‌چاله ارائه کند که منجر به بهتر شدن امنیت شبکه‌های موردی سیار در پارامترهای کیفیت سرویس گردد.



شکل ۱: نمونه‌ای از شبکه‌های موردی سیار [۳].

ادامه این مقاله به ترتیب زیر سازمان‌دهی شده است: در بخش ۲ به بستر تحقیق (پروتکل مسیریابی AODV، حمله کرم‌چاله و سیستم ایمنی مصنوعی) پرداخته‌شده است. بخش ۳ به بررسی روش‌های پیشین دفاع در برابر حملات کرم‌چاله پرداخته است. بخش ۴ به معرفی روش پیشنهادی دفاع در برابر حملات کرم‌چاله مبتنی بر سیستم ایمنی مصنوعی (WAAIS) می‌پردازد. در بخش ۵ شبیه‌سازی و ارزیابی روش پیشنهادی آمده است و نهایتاً بخش ۶ به جمع‌بندی این مقاله می‌پردازد.

۲- بستر و مقدمات تحقیق

ازآنجاکه در این مقاله پروتکل مسیریابی AODV، حمله کرم‌چاله و سیستم ایمنی مصنوعی مورد استفاده قرار می‌گیرند، در این بخش به معرفی آن‌ها می‌پردازیم.

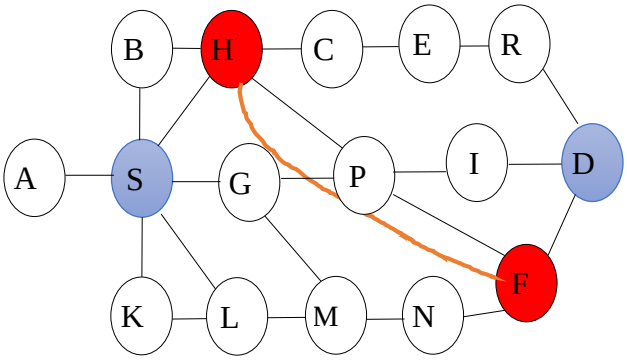
۲-۱- پروتکل مسیریابی AODV

پروتکل مسیریابی AODV یک پروتکل مسیریابی مبتنی بر نیاز[4] است که در آن همه مسیرها فقط وقتی‌که مورد نیاز باشند، کشف می‌شوند و تنها در طول مدتی که مورد استفاده قرار می‌گیرند، نگهداری می‌شوند. مسیرها در طول یک فرآیند همه پخشی[5] کشف‌شده و پاسخ مسیر به گره مبدائی که درخواست مسیر کرده بود ارسال می‌گردد.

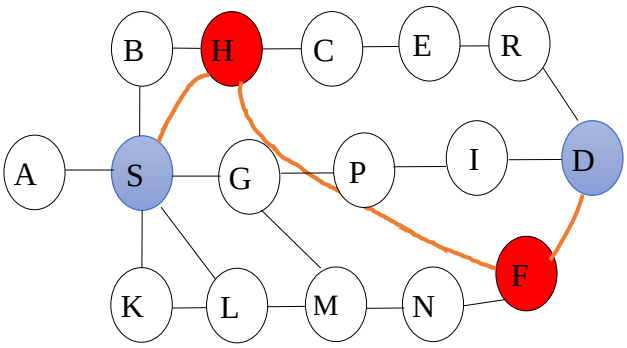
۲-۲- حمله کرم‌چاله در شبکه‌های موردی سیار

یکی از حملات بسیار مشهوری که در شبکه‌های موردی سیار انجام می‌گیرد، حمله کرم‌چاله هست. در این حمله، حمله‌کننده بسته‌هایی را در یک منطقه از شبکه شنود می‌کنند و آن‌ها را با همان شکل در منطقه دیگری از شبکه که خارج از محدوده ارسال خود است، پخش می‌کنند. این حمله غالباً با استفاده از دو گره که با استفاده از یک لینک اختصاصی به یکدیگر متصل شده‌اند، صورت می‌پذیرد. محدوده این لینک اختصاصی بیش از محدوده ارسال فرستنده‌های معمول به‌کار گرفته‌شده در شبکه است. این کار با استفاده از یک لینک بی‌سیم با آنتن‌های جهت‌دار[6] یا با یک لینک سیمی اختصاصی انجام می‌گیرد. گره‌های حمله‌کننده که در دو سوی تونل قرار دارند، برای سرعت دادن به لینک اختصاصی به‌جای ارسال بسته‌ها به‌صورت بسته به بسته آن‌ها را به‌صورت بیت به بیت ارسال می‌نمایند. در نگاه اول اینکه بسته‌ها از یک منطقه از شبکه با یک لینک پرسرعت به مقاصد خود در منطقه دیگری ارسال می‌شوند، نمی‌تواند به‌صورت یک حمله تلقی شود؛ اما با اندکی دقت متوجه می‌شویم که در این حالت گره‌های حمله‌کننده در شرایط بسیار مناسبی قرار می‌گیرند که بتوانند شکل‌های متنوعی از حملات را اجرا کنند. این گره‌ها می‌توانند بسته‌ها را به‌صورت انتخابی، از این کانال عبور دهد یا با عبور ندادن بسته‌های مربوط به گره خاص، آن گره را در شرایط حمله انکار خدمت[7] قرار دهد. حمله کرم‌چاله در پروتکل مسیریابی مانند AODV می‌تواند به‌راحتی اعمال‌شده و عملکرد شبکه را تحت تأثیر قرار دهد. برای مثال همان‌گونه که در شکل ۲ نشان داده شده است، حمله‌کننده H، بسته درخواست مسیر را که از گره مبدأ S دریافت کرده است، مستقیماً از طریق تونل‌زنی به گره F (حمله‌کننده دوم) ارسال کرده، سپس گره F آن را سریعاً به گره مقصد D ارسال می‌کند. گره مقصد از طریق مسیر H، P و F، تعداد گام

کمتری نسبت به سایر مسیرها دارد، بنابراین بسته پاسخ را از این مسیر برگشت می‌دهد. بدین ترتیب براساس شکل ۳ حمله کرم‌چاله می‌تواند شکل‌گرفته و داده‌های عبوری از این تونلینگ بین گره H و F حذف شوند [۴، ۵].



شکل ۲: گره‌های H و F بسته‌های تقاضای مسیر را به یکدیگر ارسال می‌نمایند.



شکل ۳: گره‌های H و F موفق به تشکیل کرم‌چاله در شبکه شده‌اند.

۲-۳- سیستم ایمنی مصنوعی

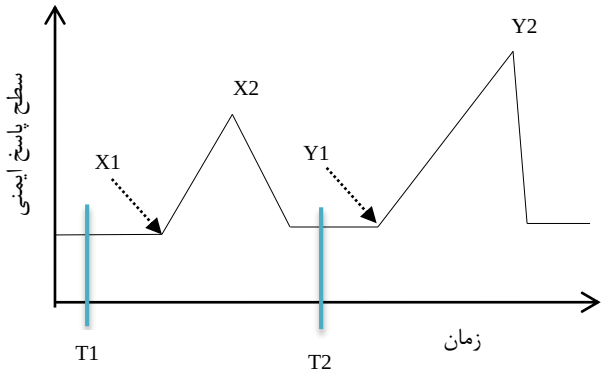
در این بخش سیستم ایمنی مصنوعی توضیح داده می‌شود. بر اساس تعریف نویسندگان دی کاسترو[۸] و تیمیس[۹] سیستم ایمنی مصنوعی به سیستم‌های وفقی که با الهام از ایمونولوژی نظری و توابع، اصول و مدل‌های ایمنی مشاهده‌شده به‌وجود آمده‌اند و برای حل مسائل مورد استفاده قرار می‌گیرند [۶]. سه نکته که در هر الگوریتم ایمنی مصنوعی باید لحاظ شود: در هر الگوریتم ایمنی مصنوعی، حداقل باید یک جزء ایمنی مانند لنفوسیت‌ها[۱۰] وجود داشته باشد. در هر الگوریتم ایمنی مصنوعی، باید ایده‌ای برگرفته از بیولوژی نظری یا تجربی استفاده شود. الگوریتم ایمنی مصنوعی طراحی‌شده، باید به حل مسئله‌ای کمک کند [۷].

۲-۳-۱- اصول ایمنی

در این بخش به اصول ایمنی اشاره خواهیم کرد. این بخش را با خلاصه کوتاهی از سیستم ایمنی ذاتی شروع می‌کنیم. سیستم ایمنی ذاتی در سیستم‌های مصنوعی به‌طور گسترده استفاده نشده‌اند ولی ازآنجاکه به عملکرد سیستم ایمنی اکتسابی کمک می‌کنند و بر روی آن تأثیر می‌گذارند و در این مقاله نیز از این سیستم استفاده می‌شود، مروری کوتاه بر آن لازم به‌نظر می‌رسد.

ایمنی ذاتی: سیستم ایمنی ذاتی همان‌طور که از نامش برمی‌آید با گذر زمان تغییر نمی‌کند و برای تشخیص تعداد کمی از مهاجمان معمول، تنظیم‌شده است. سیستم ایمنی ذاتی بیشتر پاتوژن‌ها[۱۱] را (که مهاجمان بالقوه مضر هستند) در برخورد اول منهدم می‌کند اما سیستم ایمنی اکتسابی، برای ایجاد واکنش در برابر مهاجمان احتیاج به‌وقت دارد و بنابراین وظیفه سیستم ایمنی ذاتی است که در برابر مهاجمان به‌سرعت واکنش نشان دهد و حمله را تحت کنترل بگیرد تا سیستم ایمنی اکتسابی بتواند پاسخ مؤثری ایجاد کند [۷-۱۲].

ایمنی اکتسابی: ایمنی اکتسابی زمانی که فعال شود، برای هفته‌ها فعال می‌ماند؛ درحالی‌که ایمنی ذاتی زمانی که فعال می‌شود، برای چند روزی فعال می‌ماند. وظیفه ایمنی اکتسابی است که زمانی که ایمنی ذاتی ازپادرآمده یا به هر جهت ناکارآمد شد، پاتوژن‌ها را از بین ببرد. ناکارا بودن ایمنی ذاتی به‌این‌علت است که ایمنی ذاتی نمی‌تواند پاسخی خاص برای یک پاتوژن مهاجم ایجاد کند. در این حالت سیستم ایمنی اکتسابی وارد عمل می‌شود. برخلاف ایمنی ذاتی، ایمنی اکتسابی حافظه دارد و بنابراین طبق شکل ۴ پاتوژنی را که یک‌بار حمله کرده و سیستم برای آن پاسخی تولید کرده است، به‌یاد می‌آورد و در برخوردهای بعدی، برای مقابله با آن پاتوژن پاسخ سریع‌تری تولید می‌کند.

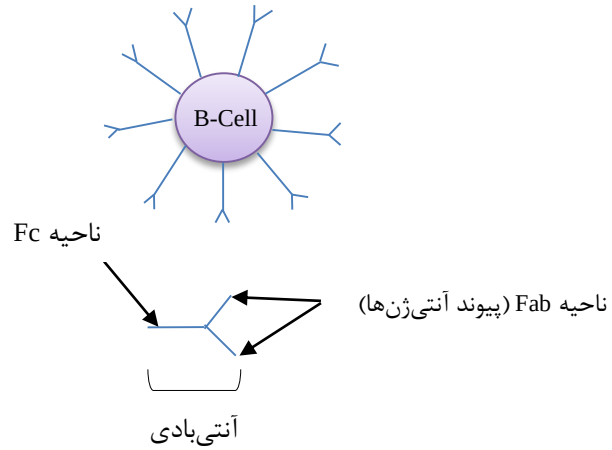


شکل ۴: پاسخ‌های اولیه و ثانویه ایمنی

۲-۳-۲- سلول B آنتی‌بادی‌ها[۱۲] و انتخاب کلونی[۱۳]

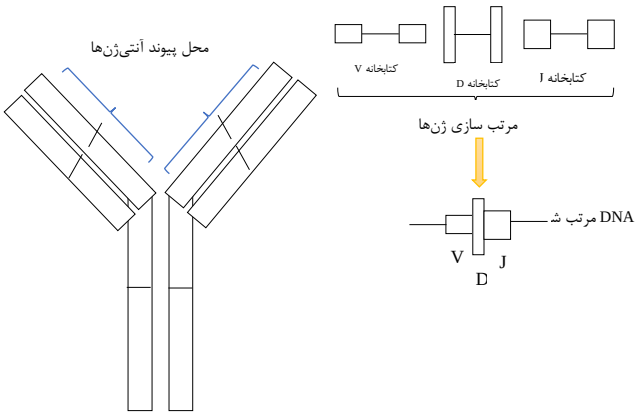
مانند همه سلول‌های ایمنی، سلول‌های B در مغز استخوان ساخته می‌شوند. یک سلول B طبیعی حامل ۱۰۵ آنتی‌بادی (پذیرنده) در سطح خود است. هرکدام از این آنتی‌بادی‌ها دارای شکلی هستند که در ساختار ژنتیکی سلول B است و بنابراین شکلی مشابه به سلول B دارند. بنابراین همه آنتی‌بادی‌هایی که توسط یک سلول B تولیدشده‌اند به مجموعه مشابهی از الگوهای مولکولی متصل می‌شوند. طبق شکل ۵ آنتی‌بادی‌های سلول B دو ارزشی و دو عملکردی هستند. آن‌ها دو

ارزشی‌اند زیرا می‌توانند از طریق دو بازوی نـواحی Fab بـه دو آنتـی‌ژن متصل شوند و دو عملکردی‌اند زیرا به‌علاوه اتصال از طریق نواحی Fab به الگوهای آنتی‌ژن می‌توانند از طریق قسمت Fc به پذیرنده‌های خاص روی سطح سلول‌های ایمنی دیگر نیز متصل شوند.



شکل ۵: دیاگرام سلول B

آنتی‌بادی‌های زیادی در سطح سلول B دیده می‌شود. در شـکل ۶ یک آنتی‌بادی، یا یـک ایمونوگلـوبین، از دو زنجیـر سـبک مشـابه و دو زنجیر سنگین مشابه، تشکیل شده است.



شکل ۶: مولکول آنتی‌بادی و ژنومش

۲-۳-۳- سیستم ایمنی مصنوعی الگوی الهام گرفته‌شده از بیولوژی

بـه‌طورکلی، سیسـتم‌های ایمنـی مصـنوعی جـزء الگوریتم‌هـای الهـام گرفته‌شده از بیولـوژی هسـتند. ایـن نـوع الگوریتم‌هـا، الگوریتم‌هـایی هستند که اصول و ویژگی‌های آن‌ها نتیجه بررسی در خواص وفقی[۱۴] و مقاومتی[۱۵] نمونه‌های بیولوژیکی هستند. نمونـه چنـین الگوریتم‌هـایی، شبکه‌های عصبی زیدنبرگ[۱۶] که از مغز الهام گرفته‌شده است و سیستم ایمنی مصنوعی که از اصول و پردازش‌های سیستم ایمنی طبیعی برای حل مسائل استفاده می‌کند هستند [۱۳].

۳- کارهای پیشین

در سال‌های اخیر امنیت در شبکه‌های مـوردی سـیار به‌خصـوص امـن کـردن پروتکل‌هـای مسـیریابی در برابـر حمـلات کرم‌چالـه، بشـدت موردتوجه بـوده اسـت. در ادامـه بـه معرفـی تعـدادی از پژوهش‌هـای انجام‌شده پرداخته می‌شود.

در [۱۴]، برای کشف و جلوگیری از حملات کرم‌چاله روشی مبتنی بر تابع فشرده‌سازی درهم‌سـاز پیشنهادشـده اسـت. ایـن روش از تـابع درهم‌ساز امن بـرای محاسـبه مقـدار فیلـد درهم‌سـاز دربسـته RREQ استفاده می‌کند. بدین‌صورت گره مبـدأ S بـرای یـافتن مقصـد گـره D فرایند کشف مسیر را شروع می‌کنـد، در ابتـدا گـره S تـابع درهم‌سـاز HCF را مقداردهی کرده و به‌طرف همسـایگان پخـش مـی‌کنـد تـا بـه مقصد D برسد. مقصد هم به RREQ رسیده، تـابع درهم‌سـاز را اعمـال کرده و گام واقعی را با تعداد گامی که در فیلد seed محاسبه‌شده بود، مقایسه می‌کند. اگر تطابق داشت، مسیر مـوردنظر امـن بـوده و بسـته پاسخ مسیر را به مبدأ ارسال می‌کنـد امـا اگـر تطـابق نداشـته باشـد، به‌عنوان مسیر مشکوک حذف می‌کند.

در [۱۵]، یک روش توزیع‌شده، پیشنهادشده است که از اطلاعات همسایگی استفاده می‌کند و نیاز به سخت‌افزار خاصی ندارد. ایـده ایـن مقاله برای یافتن گره‌های همسایه واقعی، استفاده از لیست همسـایگی گره‌های همسایه‌ای است که هم‌زمان با گره جـاری تحـت حملـه قـرار ندارد. وقتی حمله کرم‌چاله در شبکه رخ می‌دهـد، تعـداد همسـایه‌های گره‌های در معرض حمله بیش از حد معمول خواهـد شـد. بنـابراین از این ایـده اسـتفاده کـرده و به‌صـورت توزیع‌شـده همسـایه‌های واقعـی گره‌هایی که تحت حمله قرارگرفته‌اند را شناسایی کرده و گره‌های دیگر را به‌عنوان گره مشکوک در نظر گرفتـه و از لیسـت همسـایگی حـذف می‌شود.

در [۱۶]، نویسـندگان یـک روشـی مبتنـی بـر تئـوری گـراف کـه WormPlanar نامیده می‌شـود، پیشـنهاد کردنـد. Wormplanar بـه دو بخش اساسی تست سطحی محلـی (شناسـایی گره‌هـای مشـکوک بـه حمله) و فرآیند پالایش (حذف گره‌های مشکوک) تقسیم مـی‌شـود. در تست سطحی محلی؛ گره‌های مشکوک بـه حملـه شناسـایی مـی‌شـود بدین‌صورت که هر گره اطلاعات همسایگان k گامی خود را جمـع‌آوری می‌کند سپس الگوریتم مسطح سازی برای زیر گـراف همسـایگان هـر گره اعمال می‌شود بعدازاینکه تمامی گره‌هـا تسـت سـطحی محلـی را انجام دادند، تعدادی گره‌های مشکوک شناسایی می‌شوند. سپس در فاز فرآیند پالایش، گره‌های مشکوکی که از فاز قبل شناسایی‌شده بودند را فیلتر کرده تا از ادامه فعالیت مخرب‌کاری جلوگیری به‌عمـل آیـد. ایـن روش که صرفاً از اطلاعات اتصال محلی گره‌ها بهره می‌گیـرد، قـادر بـه ثبت فعالیت کرم‌چاله‌ها در شبکه‌های مـوردی سـیار هسـت و محـرک خوبی برای تشخیص حمله کرم‌چاله اسـت و در روش‌هـای توزیع‌شـده تنها با اطلاعات اتصال شبکه کار می‌کند.

در [۱۷]، نویسندگان یک روشی مبتنی بر موقعیت و ناحیه بر اساس پروتکل LAR پیشنهاد کردند که فرآیند کشف مسیر را با همه پخشی محدود انجام می‌دهد. این روش از اطلاعات مکان با کمک GPS برای مسیریابی داده‌ها استفاده کرده که از سربار پیچیده در عملیات مسیریابی را کاهش می‌دهد. به‌عنوان مثال، وقتی یک گره مبدأ S می‌خواهد اطلاعاتی به گره مقصد D ارسال کند، اول ناحیه مورد انتظار را پیداکرده و سپس درون آن ناحیه درخواست کشف مسیر به مقصد D را می‌کند. همه گره‌های همسایه عضو ناحیه که بسته ناحیه درخواستی را دریافت کردند، به همسایگان خود به سمت مقصد همه پخشی می‌کنند. این فرایند ادامه می‌یابد تا بسته درخواست مسیر به دست مقصد برسد زمانی که مسیری کشف شد به گره مبدأ تک‌پخشی شده و گره مبدأ مسیرهای کشف‌شده را با اعمال الگوریتم Hexagon جدا کرده سپس با مسیر انتخابی امن، داده‌ها را به مقصد ارسال می‌کند.

هو و همکارانش [۱۵]، روش Packet Leash را جهت کشف حملات کرم‌چاله[۱۷] پیشنهاد کردند که مبتنی بر Leash جغرافیایی[۱۸] و Leash زمانی است. یک Leash جغرافیایی، تضمین می‌کند که دریافت‌کننده بسته درون فاصله مشخص از فرستنده قرار دارد و یک Leash زمانی، تضمین می‌کند که بسته یک حد بالای طول عمر دارد و ازآنجایی‌که بسته می‌تواند با سرعت زیاد نور حرکت کنند به حداکثر فاصله‌ای که می‌تواند حرکت کند محدود شده است. هر دو نوع Leash پیشنهادی می‌توانند از حملات کرم‌چاله جلوگیری کنند به‌دلیل این‌که اجازه می‌دهد اگر بسته بیشتر از محدوده فاصله یا سرعت تجاوز کند، دریافت‌کننده بسته به‌عنوان گره مشکوک شناسایی شود. بدین طریق، برای ساختن یک بسته Leash جغرافیایی هر گره باید مکان خود و تمام گره‌ها را برای همگام‌سازی ساعت بداند. وقتی‌که یک بسته ارسال می‌شود، فرستنده بسته، مکان خودش را در P_s و زمان ارسال بسته را در t_s قرار می‌دهد. وقتی یک بسته دریافت می‌شود، گره دریافت‌کننده این مقدار را با مکان خودش که در متغیر P_r است، و مان دریافت بسته که در t_r است، مقایسه می‌کند. اگر ساعت‌های فرستنده و گیرنده درون محدوده $\pm\Delta$ و V حداکثر سرعت گره‌ها همگام‌سازی شده باشد، دریافت‌کننده بسته می‌تواند حد بالای فاصله بین ارسال‌کننده بسته و خودش (d_{sr}) را محاسبه کند. به‌ویژه، بر اساس مهر زمانی t_s دربسته، زمان دریافت محلی در t_r، حداکثر خطای مربوطه در اطلاعات مکانی در ∂، و مکان در فت‌کننده بسته در P_r، و مکان ارسال‌کننده بسته در P_s باشد سپس d_{sr} می‌تواند به‌صورت زیر مرزبندی شود:

$$d_{sr} \le ||P_s - P_r|| + 2v * (t_r - t_s + \Delta) + \partial$$

بر اساس رابطه بالا، مهر زمانی و مکانی بسته دریافت شده از گره‌ها مورد تصدیق قرار می‌گیرد تا گره‌ها تبادل اطلاعات امنی داشته باشند [۱۸، ۱۹].

آقای عبدالسلام و تاریک، روش مبتنی بر محدوده فاصله و زمان را پیشنهاد کردند. بدین‌صورت برای کشف و جلوگیری از حملات کرم‌چاله، اول پیوندهایی که در عملیات مسیریابی با احتمال بالا درگیر یک حمله کرم‌چاله هستند کشف می‌شوند. این بر اساس فرض اینکه حملات کرم‌چاله از نوع داخل باند باعث زیادشدن تأخیر بسته‌ها در مقایسه با شبکه‌های بی‌سیم معمولی می‌شود؛ در نظر گرفته‌شده است. پس‌ازآن، جهت اطمینان اینکه پیوند موردنظر آلوده به حمله کرم‌چاله هست یا نه یک بسته رمزنگاری‌شده بین دو سر پیوند، ارسال‌شده تا سالم یا آلوده بودن آن مشخص گردد [۲۰].

آقای چیانگ و همکارانش یک روش مبتنی بر زمان پیشنهاد کردند که از همگام‌سازی ساعت برای تشخیص حملات استفاده می‌کند. بدین‌معنی که به سرآیند این پروتکل یک فیلد تصدیق اصالت اضافه کردند که می‌تواند روی هر کانالی که داده‌ها ارسال می‌شود، عمل کند. این فرآیند، برای حملاتی که قصد ایجاد تأخیر بین گره مبدأ و مقصد حین تبادل ترافیک داده دارد، عمل کرده و آن‌ها را از ادامه فعالیت بازمی‌دارد [۲۱].

آقای وو و همکاران یک روش مبتنی بر زمان به نام Wormeros پیشنهاد کردند که شامل دو فاز برای کشف حمله کرم‌چاله است. فاز پیدا کردن گره‌های مشکوک و فاز تأییدیه. در فاز اول، از اطلاعات محلی گره‌ها برای بررسی وجود حملات کرم‌چاله در شبکه استفاده می‌کند. در ابتدا، RTT ین گره مبدأ S و تمامی همسایه‌های گره میانی اندازه‌گیری می‌شود. اگر RTT(S,D) جایی‌که D، یکی از همسایگان گره مبدأ S است، به‌صورت غیرعادی بزرگ‌تر از میانگین RTT تمامی پیوندها از گره S به همسایگان آن باشد، ممکن است یک کرم‌چاله مابین گره S و گره D وجود داشته باشد. در طول عملیات، نیازی به همکاری تمامی گره‌ها در مسیر بین S و D نیست؛ دوم، از مشاهداتی که دو گره همسایگان S و D به‌احتمال زیاد، برای اشتراک‌گذاری همسایه‌های مشترک در شبکه متراکم، استفاده می‌کند.

در فاز تأییدیه پس از پیدا شدن گره‌های مشکوک به کرم‌چاله در شبکه، Wormeros یکسری از چالش‌ها را برای مطمئن ساختن اینکه کرم‌چاله به‌طور صحیح شناسایی شده است، آغاز می‌کند. در این فاز، دو گره همکار و مطمئن برای به چالش کشیدن گره کرم‌چاله، حمله‌ای به پیوند آلوده به کرم‌چاله آغاز می‌کنند [۲۲]. برای این منظور نویسندگان از روش TrueLink استفاده کردند [۲۳].

آقای ونگ و همکارانش یک روش مبتنی بر مکان انتها به انتها به نام EDWA، برای تشخیص حمله کرم‌چاله پیشنهادی کردند. در این روش گره مبدأ بر اساس اطلاعات تبادلی بین خود و مقصد، حداقل تعداد گام به گره مقصد را تخمین می‌زند. گره مبدأ مقدار تعداد گام را برای هر مسیر دریافتی از پاسخ بسته با مقدار تخمینی استفاده‌شده مقایسه می‌کند، اگر مقدار دریافتی بسیار کمتر از مقدار گام تخمینی باشد، مسیر مربوطه به‌عنوان مسیر آلوده به کرم‌چاله تشخیص داده می‌شود. پس‌ازآن، گره مبدأ، کرم‌چاله راه‌اندازی شده را در دو نقطه پایانی ردیابی کرده و گره‌های کرم‌چاله در یک ناحیه کوچک شناسایی شده و از ادامه فعالیت در شبکه بلوکه می‌شود و از سایر مسیرهای سالم کشف شده که آلوده به کرم‌چاله نیست، استفاده می‌کند [۲۴].

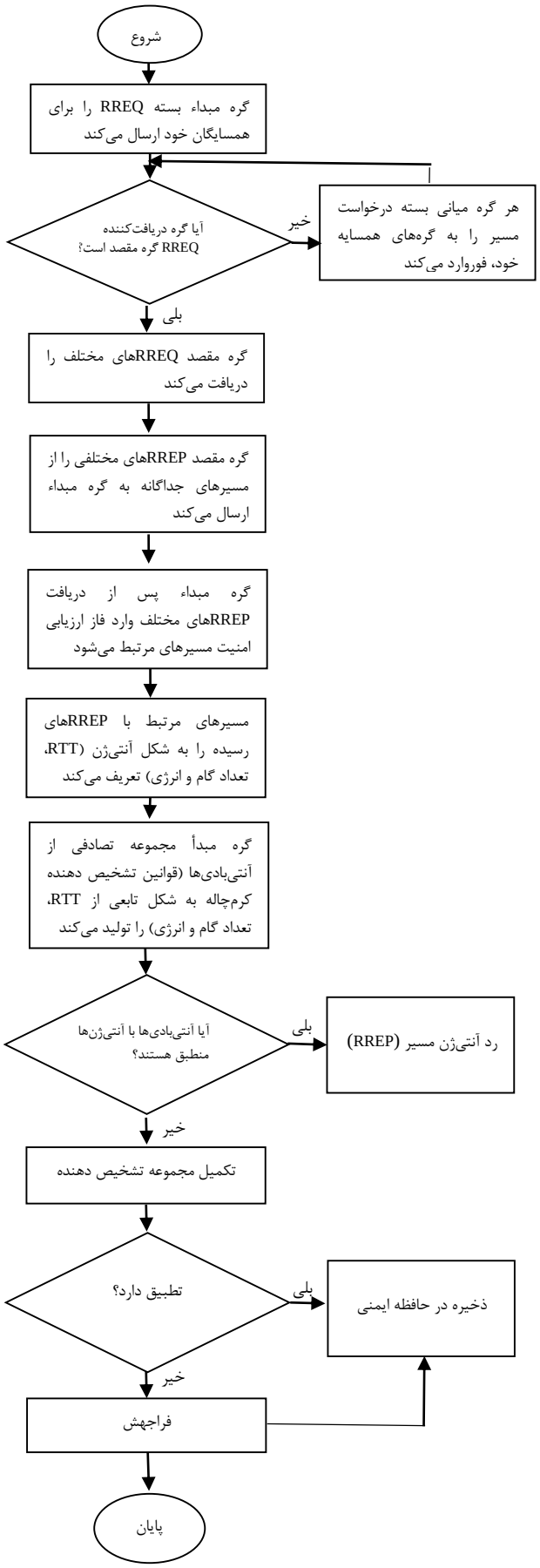
۴- روش پیشنهادی: دفاع در برابر حملات کرم‌چاله با بهره‌گیری از سیستم ایمنی مصنوعی (WAAIS)

در پروتکل مسیریابی AODV بعد از این‌که گره مبدأ RREP ها را دریافت می‌کند، با اولین RREP رسیده کوتاه‌ترین مسیر را شناسایی کرده و بسته‌ها را ارسال می‌کند. بر این اساس این پروتکل توجهی به امن بودن مسیر (نبود حملات کرم‌چاله) نمی‌کند؛ اما در روش پیشنهادی گره مبدأ پس از دریافت RREPها، ابتدا با بهره‌گیری از الگوریتم سیستم ایمنی مصنوعی امنیت مسیرها را بررسی کرده و بسته را به امن‌ترین مسیر ارسال می‌کند. در روش پیشنهادی ایده کلی کار این است که همان‌طور که در سیستم ایمنی بدن، آنتی‌بادی‌ها آموزش می‌بینند تا آنتی‌ژن‌های مخرب را شناسایی و از بین ببرند، در اینجا نیز مجموعه قوانینی ایجاد می‌شود و طوری به‌روزرسانی می‌شود که بتواند مسیرهایی را که توسط مهاجمان کرم‌چاله آلوده‌شده است، شناسایی کرده و از چرخه انتخاب خارج نماید. نگاشت و قیاس پیشنهادی بین سیستم ایمنی بدن انسان و شبکه‌های موردی سیار تحت حمله کرم‌چاله در جدول ۱ نشان داده شده است. جزئیات چگونگی استفاده از نگاشت جدول ۱ در زیر بخش ۴،۲ آمده است.

روش پیشنهادی طبق فلوچارت شکل ۷ از قسمت‌های مختلفی تشکیل شده است: تولید تصادفی جمعیتی از آنتی‌بادی‌ها (قوانین)، ارزیابی آنتی‌ژن‌ها (مسیرهای برگشت RREPها)، تطبیق آنتی‌بادی با آنتی‌ژن‌ها، رد کردن مسیرهای تطبیق داده شده، تکمیل مجموعه تشخیص دهنده (قوانینی که منجر به تشخیص مسیرهای آلوده به کرم‌چاله شده‌اند)، ذخیره در حافظه ایمنی و فراجهش تشخیص‌دهنده. آنتی‌بادی موردنظر طوری طراحی می‌شود که امنیت و کارایی را به‌شکل هم‌زمان در نظر می‌گیرد. این طراحی در دو فاز انجام می‌شود.

۴-۱- فاز اول: ارزیابی اولیه امنیت مسیرهای نامزد با استفاده از بسته‌های آزمایشی

در این مرحله هر یک از مسیرهایی که برای آن‌ها RREP دریافت شده است، ازنقطه‌نظر امنیتی آزمایش می‌شود. برای این منظور از هر مسیر یک بسته آزمایش ارسال می‌شود و مقصد نیز موظف است در صورت دریافت بسته آزمایش یک بسته تائیدیه برای آن مسیر ارسال نماید. بدیهی است که چنان‌چه یک مسیر آلوده به حمله کرم‌چاله باشد، بسته آزمایش به مقصد نخواهد رسید و بسته تائیدیه دریافت نخواهد کرد. در این شرایط احتمال اینکه این مسیر یک مسیر آلوده باشد، افزایش می‌یابد؛ یعنی مقدار $P_{wh}(r)$ برای مسیر r افزایش می‌یابد؛ اما اگر بسته آزمایش به مقصد برسد، بسته تائید دریافت خواهد شد و این بدین معنی است که آن مسیر دارای حمله کرم‌چاله نیست؛ بنابراین مقدار $P_{wh}(r)$ کاهش پیدا می‌کند. فرآیند ارسال بسته آزمایش به‌تعداد ۳ بار انجام می‌گیرد.



شکل ۷: فلوچارت WAAIS

جدول ۱: نگاشت بین بدن انسان و شبکه‌های موردی سیار

بدن انسان	شبکه‌های موردی سیار
آنتی‌ژن	مجموعه تمام مسیرها از مبدأ تا مقصد
ساختار آنتی‌بادی	قوانین تشخیص حمله کرم‌چاله براساس (RTT ، تعداد گام و انرژی)
کلونی‌سازی	تکثیر مجدد آنتی‌بادی‌هایی با بیشترین تطبیق با آنتی‌ژن‌ها
میزان میل ترکیبی	مجموع انرژی گره‌های مسیر، تعداد گام‌ها و RTT
جهش	در شرایط مساوی سریع‌ترین RREP انتخاب می‌شود

مقدار اولیه $P_{wh}(r)$: اگر طبق مکانیسم تشخیص مهاجم، مسیر مورد تأیید بود، مقدار اولیه $P_{wh}(r)$ برابر ۰ خواهد بود اما اگر مسیر مورد تأیید نبود $P_{wh}(r)$، برابر ۱۰۰ مقداردهی می‌شود. سپس برای به‌روزرسانی آن، طبق جدول ۲ گره مبدأ به‌صورت دوره‌ای، ۳ بار یک بسته آزمایشی را از تمام مسیرهای ممکن به گره مقصد ارسال می‌کند. اگر از طرف گره مقصد بسته تأیید آمد، ۵۰ واحد از متغیر $P_{wh}(r)$ کسر می‌شود؛ اما اگر از طرف گره مقصد بسته تأیید نیامد، ۲۰ واحد به متغیر $P_{wh}(r)$ اضافه می‌شود. این امر ۳ بار انجام می‌شود و برای تمامی مسیرها $P_{wh}(r)$ به‌روزرسانی می‌شود. حال اگر مقدار $P_{wh}(r)$ مسیری بیشتر از ۵۰ بود، آن مسیر به‌عنوان یک مسیر آلوده کنار گذاشته می‌شود (رد می‌شود). در غیر این صورت، آن مسیر به قسمت بعدی، یعنی فاز دو، جهت ارزیابی امنیت و کارایی مسیرها، ارسال می‌شود.

جدول ۲: آزمایش مکانیسم تشخیص مهاجم

$RREP_s$	Confirmation	NotConfirmation	$P_{wh}(r)$
$RREP_1$	√		$P_{wh}(r)$ - ۵۰
$RREP_2$		√	$P_{wh}(r)$ + ۲۰

۴-۲- فاز دوم: ارزیابی امنیت و کارایی مسیرهایی که از فاز اول عبور کرده‌اند.

با توجه به این‌که حمله کرم‌چاله تعداد گام‌ها را کمتر از مقدار واقعی نشان می‌دهد، لذا چنانچه یک مسیر دارای تعداد گام کمتری باشد، احتمال اینکه این مسیر آلوده باشد، افزایش می‌یابد. این در حالی است که پائین بودن زمان رفت‌وبرگشت و بالا بودن مجموعه انرژی گره‌های موجود در مسیر، علاوه بر اینکه امنیت مسیر را از نقطه نظر حمله کرم‌چاله ارتقاء می‌دهد، از نقطه نظر کارایی مسیر نیز مطلوب است. لذا می‌توان مسیر مطلوب را مسیری در نظر گرفت که طبق رابطه (۱) باعث بیشینه شدن شاخص F_i می‌شود:

$$F_i\left(Energy_i.HopCount_i.RTT_i\right) = \left(\frac{Max\ RTT}{RTT_i}\right) + \left(\frac{HopCount_i}{\text{Max HopCount}}\right) + \left(\frac{Energy_i}{\text{Max energy}}\right) \quad (۱)$$

که در آن $Energy_i$ میزان انرژی باقیمانده مسیر i، $HopCount_i$ تعداد گام مسیر i، RTT_i زمان رفت و برگشت مسیر i، $Max\ RTT$ بیشترین زمان رفت و برگشت مسیرها، Max HopCount بیشترین تعداد گام مسیرها و Max energy، بیشترین انرژی مسیرها را نشان می‌دهد.

به‌منظور ترکیب نتایج فازهای اول و دوم و در نظر گرفتن شاخص امنیت و کارایی، معیار کلی انتخاب یک مسیر طبق رابطه (۲) به‌دست می‌آید.

$$IR = \left(1 - \text{Pwh(r)}\right) * F_i\left(Energy_i.HopCount_i.RTT_i\right) \quad (۲)$$

الگوریتم شکل ۸، شبه کد آموزش تشخیص‌دهنده‌ها را نشان می‌دهد. هدف این است که مجموعه آنتی‌بادی‌ها را جهت مقاوم کردن با یکسری آنتی‌ژن خودی آموزش دهد تا جهت دفاع در مقابل آنتی‌ژن غیرخودی (حمله کرم‌چاله) مقاوم باشند.

Algorithm 1: For training the detectors

1: **Set** counter n_a as the number of self $ALCs$ to train;
2: **Create** an set of self $ALCs$ as C;
3: **Determine** the training of self-element as D_t;
4: **While** size of C not equal to n_a do
5: Randomly generate an ALC, X_i;
6: Matched = False;
7: **For** each self-set $z_p \in D_t$ do
8: **If** affinity between X_i and Z_p is higher than affinity threshold $\boldsymbol{r}$ then
9: Matched = True;
10: Break;
11: **End if**
12: **End for**
13: **If** not matched then
14: **Add** X_i to set C;
15: **End if**
16: **End Procedure**

شکل ۸: شبه کد آموزش تشخیص دهنده‌ها (در قسمت تکمیل مجموعه تشخیص دهنده)

ساختار آنتی‌بادی و آنتی‌ژن: آنتی‌بادی همان سه ویژگی محدود کردن حمله کرم‌چاله (تعداد گام، زمان رفت‌وبرگشت و انرژی باقیمانده) و آنتی‌ژن مجموعه کل مسیرهایی در نظر گرفته می‌شود که برای آن‌ها RREP دریافت شده است.

میل ترکیبی: همان‌طور که در سیستم ایمنی مصنوعی تعریف شد، آنتی‌بادی‌هایی که درجه اتصال به آنتی‌ژن قوی‌تری نسبت به بقیه آنتی‌بادی‌ها داشته باشند به‌عنوان آنتی‌بادی بهتر جهت ترکیب شدن انتخاب می‌شوند. در روش پیشنهادی، میل ترکیبی همان مجموع مسیرهایی که تعداد گام بیشتر، زمان رفت‌وبرگشت کمتر و انرژی

باقیمانده بیشتر باشند انتخاب می‌شوند. در غیر این صورت مسیر کاندید حذف می‌شود.

تطبیق: در این قسمت RREPهایی که در گره مبدأ جمع شده‌اند، آن‌ها را با سه شرط موجود مقایسه و بررسی کرده و امن‌ترین مسیر انتخاب می‌شود. در ضمن مهم‌ترین ویژگی مکانیسم تشخیص مهاجم این است که در طول زمان اصلاح شوند و به‌نحوی تعریف شوند که قابل اصلاح بوده و به‌راحتی قدرت یادگیری داشته باشند.

جزئیات ویژگی اول، دوم و سوم آنتی‌بادی در قسمت تطبیق:

ویژگی اول، زمان رفت و برگشت بین مبدأ و مقصد: طبق رابطه (۴) برای تمامی مسیرهای دریافتی از گره مبدأ به گره مقصد زمان رفت‌وبرگشت را محاسبه می‌نماید. جهت به‌دست آوردن مسیری با زمان رفت‌وبرگشت کم از رابطه (۱) استفاده می‌شود.

محاسبه $RTT\ avg$**:** زمان رفت‌وبرگشت بدین‌صورت تعریف شده است: فاصله زمانی بین ارسال یک بسته Hello به همسایگان و دریافت جواب Hello مربوطه از همسایگان تعریف شده است. بدین صورت هر گره میانگین زمان رفت‌وبرگشت بین خود و همسایگان تک گامی را نگهداری می‌کند که این مقدار با $RTT\ avg$ نشان داده شده است (رابطه ۴).

$$RTT\ avg(0) = RTT_0 \quad (۳)$$

$$RTT\ avg(i) = (RTT\ avg(i-1) * a) + ((1-a) * RTTi) \quad (۴)$$

در رابطه (۳)، $RTT\ avg(0)$ بیانگر این است که وقتی گره مبدأ بعد از اینکه از اولین همسایه تک گامی خود پاسخ بسته Hello را دریافت کرد، تنظیم شده است. بعلاوه اینکه گره مبدأ پس از دریافت هر پاسخ Hello میانگین زمان رفت‌وبرگشت یا $RTT\ avg$ را به‌روزرسانی می‌کند. همچنین مقدار اولیه متغیر α به ۰/۸۷۵ تنظیم شده است.

ویژگی دوم، تعداد گام مسیرهای بین مبدأ و مقصد: همان‌طور که عنوان شد مسیرهای آلوده به حمله کرم‌چاله خود را به‌عنوان مسیرهای کوتاه تبلیغ می‌کنند. لذا از بین مسیرهایی که توسط RREPهای مختلف به مبدأ اطلاع داده شده‌اند مسیرهایی که کوتاه‌تر می‌باشند همواره احتمال آلوده بودن آن‌ها بیشتر است. بر این اساس همان‌طور که در رابطه (۱) دیده می‌شود مسیرهایی‌که نسبت HopCount آن‌ها به بزرگ‌ترین HopCount یعنی (MaxHopCount) عدد بزرگ‌تری است احتمال سالم بودن آن مسیر بیشتر است.

ویژگی سوم، انرژی باقیمانده بین گره‌های مبدأ و مقصد: بر اساس رابطه (۱) مسیرهایی‌که نسبت Energy آن‌ها به بزرگ‌ترین Energy یعنی (MaxEnergy) عدد بزرگ‌تری باشد انرژی باقیمانده آن مسیر بیشتر است.

قسمت تکمیل مجموعه تشخیص‌دهنده: برای تمامی مسیرهایی که مقدار P_{wh} (r) آن‌ها کمتر از ۵۰ بود جهت انتخاب امن‌ترین مسیر از الگوریتم ۲، طبق شکل ۹ استفاده می‌شود:

Algorithm 2: For selecting immune route

1: **Initialization:**

2: Let $P_{wh}(r)$ as the probability candidate route;

3: Let R denote the number of candidate route;

4: Let F_r denote the $fitness\ route$;

5: Let IR denote the $immune\ route$;

6: **Procedure** Selecting $immune\ route$

7: **For** r = 1 to R **do**

8: **If** $P_{wh}(r) > 0.5$ **Then**

9: Push out $route_r$;

10: **Else**

11: $F_i\ (Energy_i.HopCount_i.RTT_i) = \left(\frac{Max\ RTT}{RTT_i}\right) + \left(\frac{HopCount_i}{\text{Max HopCount}}\right) + \left(\frac{Energy_i}{\text{Max energy}}\right)$

12: Select the route with maximum $IR = (1 - Pwh(r)) * F_i\ (Energy_i.HopCount_i.RTT_i)$

13: **End if**

14: **End for**

15: **End Procedure**

شکل ۹: الگوریتم انتخاب مسیر امن

طبق الگوریتم ۲، برای هر مسیر تابع F_i محاسبه می‌شود و مسیری که عدد بزرگ‌تری داشته باشد، به‌عنوان امن‌ترین مسیر انتخاب می‌شود.

قسمت فراجهش: از بین مسیرهای ارزیابی شده مسیرهایی‌که دارای شرایط تقریباً یکسان باشند به مرحله فراجهش ارسال می‌شود تا در این مرحله مسیرها با یک معیار دیگر (در شرایط مساوی سریع‌ترین RREP انتخاب می‌شود) ارزیابی شده تا بهترین مسیر انتخاب شود.

قسمت ثبت در حافظه ایمنی: مسیرهایی که طبق رابطه F_i بزرگ‌ترین عدد را داشته باشد، آن مسیر امن‌ترین مسیر بوده و جهت استفاده در دفعات بعدی، در حافظه ایمنی ثبت می‌گردد.

۵- شبیه‌سازی و ارزیابی روش پیشنهادی

در این بخش ارزیابی مکانیسم دفاعی WAAIS مورد ارزیابی قرار می‌گیرد. برای این منظور از ابزار شبیه‌سازی NS-2 نسخه ۲/۳۴ استفاده می‌شود. در ادامه این بخش ابتدا پارامترهای شبیه‌سازی بیان می‌شود و سپس در بخش بعدی معیارهای ارزیابی ارائه می‌شود. در بخش سوم محیط شبیه‌سازی و طراحی سناریو ارائه شده است و در نهایت بعد از آن در بخش چهارم، نتایج شبیه‌سازی تشریح می‌گردد.

جدول ۳: پارامترهای استفاده‌شده در شبیه‌سازی

سناریوی اول		سناریوی دوم	
پارامتر	مقدار	پارامتر	مقدار
مساحت شبیه‌سازی	۱۵۰۰×۱۵۰۰	مساحت شبیه‌سازی	۱۰۰۰×۱۰۰۰
تعداد گره‌ها	۵۰ گره	تعداد گره‌ها	۱۰۰ گره
تعداد پیوند کرم‌چاله	۱	تعداد پیوند کرم‌چاله	۲
زمان شبیه سازی	تغییرات از ۱۵۰ تا ۶۰۰ ثانیه	زمان شبیه سازی	تغییرات از ۱۵۰ تا ۶۰۰ ثانیه
سناریوی سوم		**سناریوی چهارم**	
مساحت شبیه‌سازی	۱۵۰۰×۱۵۰۰	مساحت شبیه‌سازی	۱۰۰۰×۱۰۰۰
تعداد گره‌ها	۵۰ گره	تعداد گره‌ها	۱۰۰ گره
تعداد پیوند کرم‌چاله	۱	تعداد پیوند کرم‌چاله	۲
نرخ گره‌های مخرب	تغییرات از ۰ تا ۰/۴۰	نرخ گره‌های مخرب	تغییرات از ۰ تا ۰/۴۰

جدول ۴: چهار سناریو برای شبیه‌سازی روش پیشنهادی

پارامتر	مقدار
شبیه ساز	NS-2.34
نوع کانال	Channel/Wireless channel
مدل انتشار رادیوئی	Propagation/Two ray ground
نوع لایه مک	Mac/802.11
نوع رابط صف	Queue/Drop Tail
نوع ترافیک	CBR
نوع آنتن	Antenna/Omni Antenna
روش مورد مقایسه	AODV-WormPlanar
پارامترهای ارزیابی کارایی	تحویل بسته، بسته‌های حذف شده و تاخیر انتها به انتها
ماکزیمم تعداد بسته	۱۰۰۰۰
اندازه بسته (بیت)	۵۱۲
نرخ داده ارسالی (مگابایت)	۵۴
تأخیر بین بسته‌ها	۰.۲۵
مساحت فضای شبیه‌سازی	سناریو اول: ۱۵۰۰ × ۱۵۰۰ سناریو دوم: ۱۰۰۰ × ۱۰۰۰
تعداد گره‌ها	سناریو اول: ۵۰ گره سناریو دوم: ۱۰۰ گره
تعداد پیوند کرم‌چاله	سناریو اول: ۱ پیوند کرم‌چاله سناریو دوم: ۲ پیوند کرم‌چاله
زمان شبیه‌سازی	۶۰۰ ثانیه

۵-۱- پارامترهای شبیه‌سازی

در این مقاله از پارامترهای ارائه شده در جدول ۳ برای شبیه‌سازی استفاده می‌شود. در این قسمت جهت ارزیابی روش پیشنهادی WAAIS نمودارهایی ارائه می‌شود که رفتار این روش نسبت به رفتار روش‌های WormPlanar [۲۲] و AODV [۳] در شرایط حمله کرم‌چاله و با در نظر گرفتن چهار سناریوی ارائه شده در جدول ۴ مورد بررسی قرار می‌گیرد.

۵-۲- معیارهای ارزیابی

در این بخش عملکرد روش پیشنهادی WAAIS، بر اساس معیارهای زیر بررسی می‌گردد.

نسبت تحویل بسته: این معیار بیانگر درصدی از بسته‌هاست که سالم به مقصد تحویل داده شده‌اند. رابطه (۵) نسبت کل بسته‌های ارسال شده در شبکه به کل بسته‌های دریافت شده در شبکه را نشان می‌دهد [۲۴].

$$\text{PDR} = \left(\frac{\sum_{j=1}^{n} \text{Number of recieve packets}}{\sum_{j=1}^{n} \text{Number of sent packets}}\right) * 100 \quad (۵)$$

میانگین تأخیر انتها به انتها: رابطه (۶) میانگین تأخیر انتها به انتها را نشان می‌دهد. این معیار بیانگر تأخیر بین ارسال یک بسته به درون شبکه و دریافت بسته در مقصد، به ازای تمامی بسته‌های داده است [۲۵].

$$\text{E2E Delay} = \left(\frac{\sum_{j=1}^{n} \text{Delivery Time} - \sum_{j=1}^{n} \text{Arrival Time}}{\sum_{j=1}^{n} \text{Recieved packets}}\right) \quad (۶)$$

تعداد بسته‌های حذف‌شده: رابطه (۷) تعداد بسته‌های حذف‌شده را نشان می‌دهد. تعداد بسته‌هایی که توسط گره‌های مخرب حذف‌شده است [۲۶].

$$\text{Drop packets} = \left(\frac{\sum_{j=1}^{n} \text{Number of droped packets}}{\sum_{j=1}^{n} \text{Number of droped packets} + \text{sent packets}}\right) * 100 \quad (۷)$$

۵-۳- محیط شبیه‌سازی و طراحی سناریو

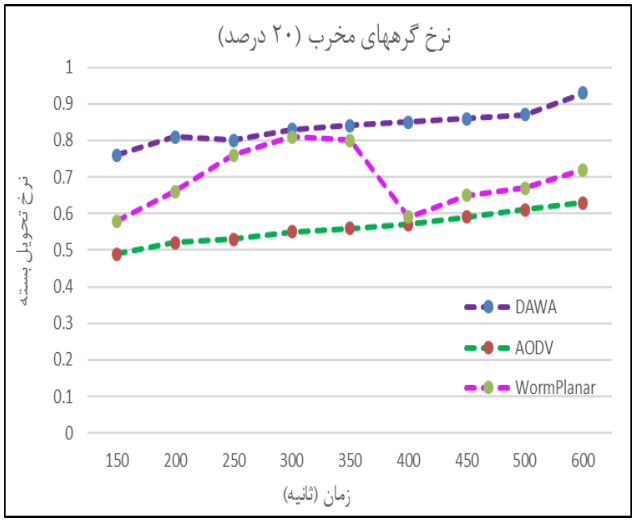
برای ارزیابی کارایی روش پیشنهادی از نسخه شماره دو نرم‌افزار شبیه‌ساز NS استفاده شده است. NS یک موتور شبیه‌سازی است که برنامه‌نویسی آن بر اساس مدل رویداد گرا بوده و ترکیبی از زبان‌های برنامه‌نویسی C++ و OTCL است. زبان OTCL نیز که نسخه شیءگرای زبان TCL است دارای انعطاف و کارایی بالائی در طراحی سناریوهای شبیه‌سازی هست. جهت ارزیابی کارایی روش پیشنهادی، سناریوهایی در قالب شبکه‌های موردی سیار طراحی و با زبان TCL پیاده‌سازی شده‌اند. معیارهای مورد مقایسه قرار گرفته شده، به‌کمک زبان AWK و از نتایج شبیه‌سازی که در قالب فایل‌های Trace استخراج شده و با نرم افزار اکسل طراحی شده است [۲۷].

۵-۴- نتایج شبیه‌سازی

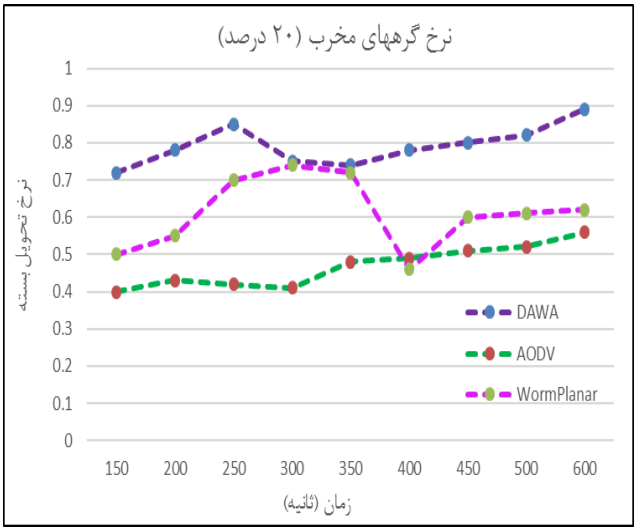
در این قسمت نتایج اجرای شبیه‌سازی در قالب نمودار ارائه می‌شود.

نسبت تحویل بسته: شکل ۱۰، نسبت تحویل بسته را در چهار سناریو در مقابل زمان و نرخ گره‌های مخرب برای WAAIS، روش WormPlanar و پروتکل مسیریابی AODV در شرایط حمله کرم‌چاله نشان می‌دهد.

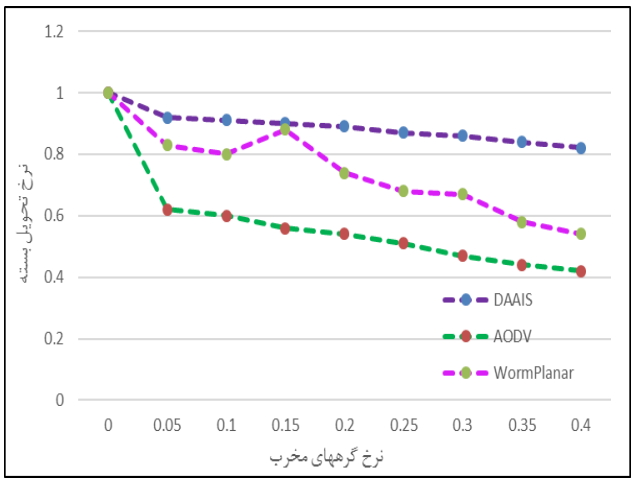
همان‌طور که از شکل مشخص هست، تحویل بسته WAAIS در دو سناریو اول و دوم در زمان‌های بین ۱۵۰ تا ۶۰۰ ثانیه در حال افزایش هست، اما در دو سناریو سوم و چهارم نرخ تحویل بسته کاهش یافته اما نسبت به دو روش دیگر بهبود خوبی دارد. دلیل بهتر بودن تحویل بسته در روش WAAIS، شناسایی سریع گره‌های مخرب و حذف آنان توسط نگاشت انجام شده مسیرهای ناامن و آنتی‌ژن در نظر گرفته شده است که توسط الگوی آموزش‌یافته مبتنی بر آنتی‌بادی کشف و از چرخه خارج می‌شوند؛ اما در روش WormPlanar در زمان ۳۲۰ ثانیه تا ۴۰۰ ثانیه کاهش یافته و کارایی آن به‌مراتب پایین می‌آید. همچنین پروتکل مسیریابی AODV از همان ابتدا که دچار حمله گره‌های مخرب شده، کارایی آن از همان ابتدا بین ۵۰ تا ۵۴ درصد نشان داده شده است و چون هیچ مکانیسم دفاعی ندارد کارایی آن به‌مراتب بدتر از روش پیشنهادی و WormPlanar است.



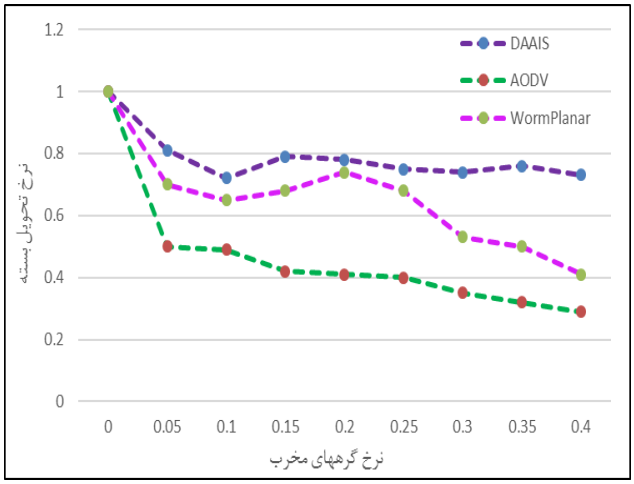
(الف) سناریوی اول



(ب) سناریوی دوم



(ج) سناریوی سوم



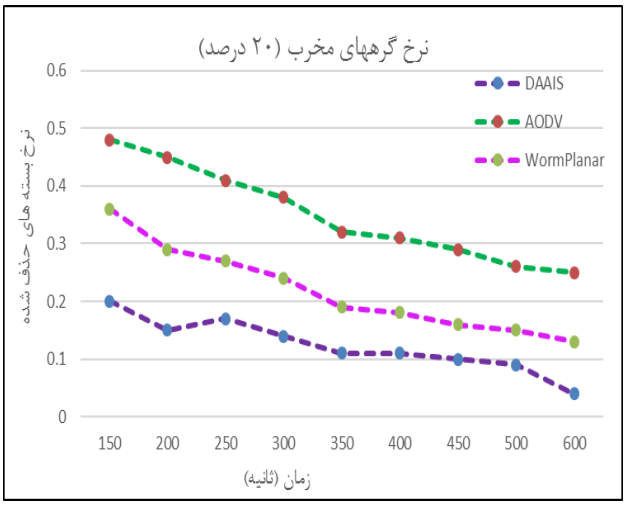
(د) سناریوی چهارم

شکل ۱۰: مقایسه نرخ تحویل بسته روش پیشنهادی WAAIS با WormPlanar و پروتکل مسیریابی AODV در شرایط حمله در چهار سناریو

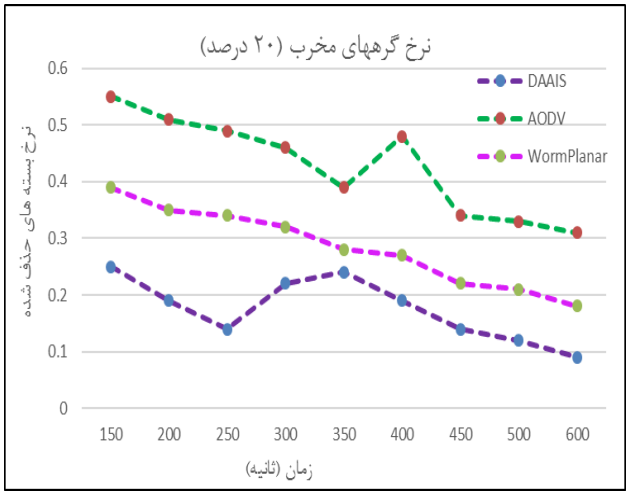
تعداد بسته‌های حذف‌شده: شکل ۱۱، حذف بسته‌ها را در چهار سناریو در مقابل زمان و نرخ گره‌های مخرب برای WAAIS، روش WormPlanar و پروتکل مسیریابی AODV در شرایط حمله کرم‌چاله نشان می‌دهد. روش پیشنهادی به‌دلیل اینکه فرآیند درخواست مسیر جعلی گره‌های نفوذکننده را شناسایی و طبق ویژگی‌های تعیین‌شده محدود می‌کند، در نتیجه مسیری که بین مبدأ و مقصد انتخاب می‌شود امن بوده و در نتیجه بسته‌های داده‌ای خیلی کم توسط گره‌های مخرب حذف می‌شوند. بنابراین همان‌طوری که از نمودار مشخص هست تعداد بسته‌های حذف‌شده توسط گره مخرب در روش پیشنهادی WAAIS به‌مراتب کمتر از روش WormPlanar و پروتکل مسیریابی AODV در شرایط حمله کرم‌چاله است.

دلیل بیشتر بودن حذف بسته در پروتکل مسیریابی AODV نداشتن مکانیسم دفاعی در مقابل حمله کرم‌چاله هست. همچنین در روش WormPlanar به‌خاطر این‌که هر گره اطلاعات همسایگان k گامی خود را جمع‌آوری کرده سپس الگوریتم مسطح سازی برای زیر گراف همسایگان هر گره اعمال می‌کند، سربار روش بالا رفته در نتیجه فعالیت حمله کرم‌چاله گسترش می‌یابد و نتیجتاً بسته‌های بیشتری در شبکه حذف می‌گردد.

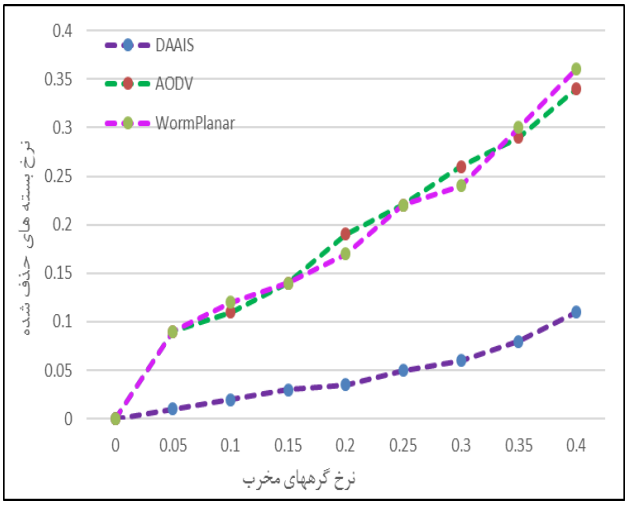
میانگین تأخیر انتها به انتها: شکل ۱۲، میانگین تأخیر انتها به انتها را در چهار سناریو در مقابل زمان و نرخ گره‌های مخرب برای WAAIS، روش WormPlanar و پروتکل مسیریابی AODV در شرایط حمله نشان می‌دهد. WAAIS، تاخیرکمتری نسبت به دو روش دیگر دارد. بالا بودن نرخ تحویل بسته در روش پیشنهادی، متعاقباً باید تأخیر کمتر ارسال بسته بین مبدأ و مقصد باشد بعلاوه اینکه چون روش پیشنهادی، از مسیرهای ذخیره‌شده در حافظه ایمنی استفاده می‌کند و هیچ فرآیند کشف مسیر انجام نمی‌شود، باید تأخیرش کمتر باشد.



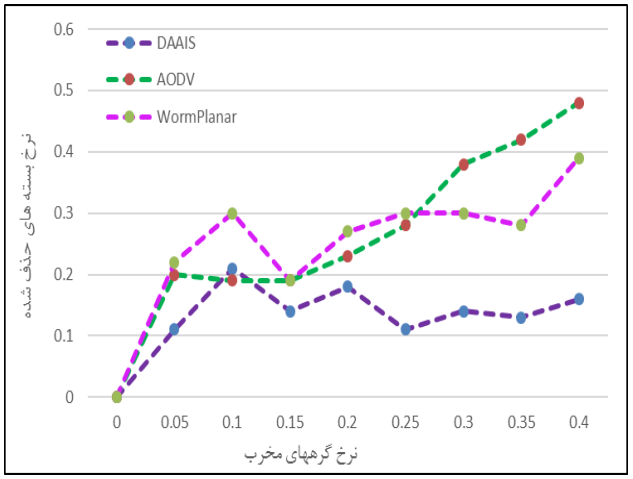
(الف) سناریوی اول



(ب) سناریوی دوم



(ج) سناریوی سوم



(د) سناریوی چهارم

شکل ۱۱: مقایسه بسته‌های حذف‌شده روش پیشنهادی WAAIS با WormPlanar و پروتکل مسیریابی AODV در شرایط حمله در چهار سناریو

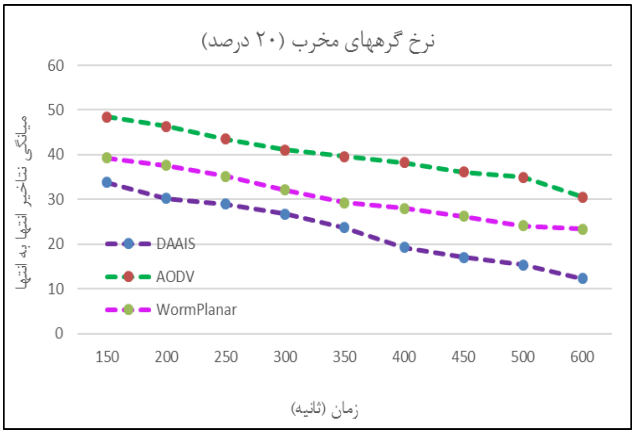
دلیل بیشتر بودن تأخیر در پروتکل مسیریابی AODV، این است که همیشه برای ارسال بسته از مبدأ به مقصد باید مسیرجداگانه‌ای کشف شود و این فرآیند کشف مسیر و پیدا کردن پاسخ مسیر مناسب، تأخیر بیشتری را در شبکه حادث می‌کند. تأخیر روش WormPlanar، نسبت به WAAIS بیشتر است اما نسبت به پروتکل AODV تأخیر کمتری دارد. دلیل بهتر بودن WormPlanar نسبت به AODV، استفاده از دو مکانیسم تست دوطرفه محلی و پالایش مسیرها هست که هم در فرآیند ارسال بسته RREQ هم دریافت RREP انجام می‌شود.

۶- نتیجه‌گیری

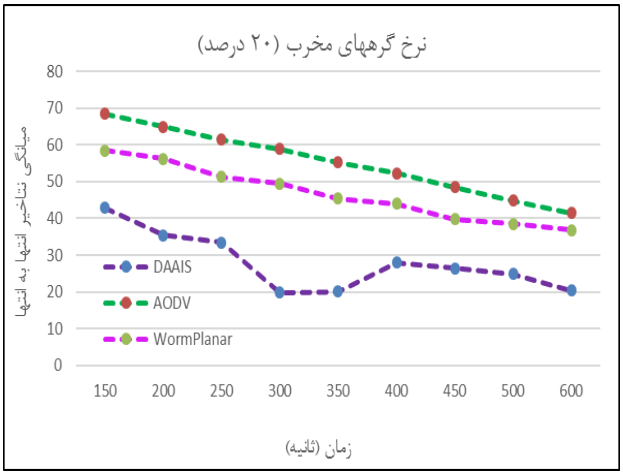
در این مقاله، یک روش مبتنی بر سیستم ایمنی مصنوعی جهت انتخاب امن‌ترین مسیر از بین مسیرهای ناامن حاوی کرم‌چاله ارائه شد. هدف اصلی روش ارائه‌شده انتخاب امن‌ترین مسیر است. در روش

پیشنهادی در فاز اول؛ برای هر یک از مسیرهایی که برای آن‌ها بسته RREP دریافت شده بود، ازنقطه‌نظر امنیتی آزمایش شد.

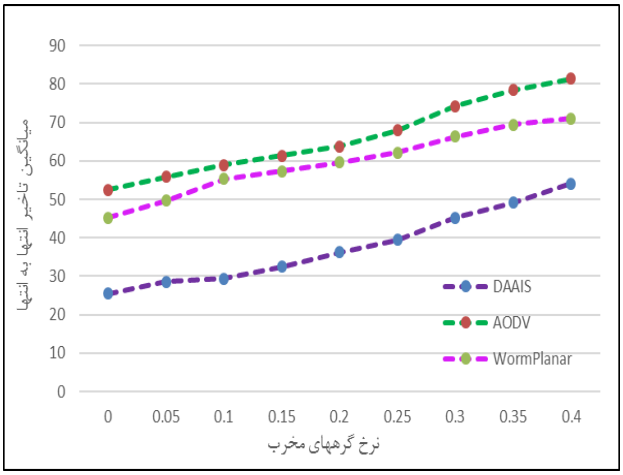
برای این منظور از هر مسیر یک بسته آزمایش ارسال شد و مقصد نیز موظف بود. برای این منظور از هر مسیر یک بسته آزمایش ارسال شد و مقصد نیز موظف بود در صورت دریافت بسته آزمایش یک بسته تائید برای آن ارسال نماید.



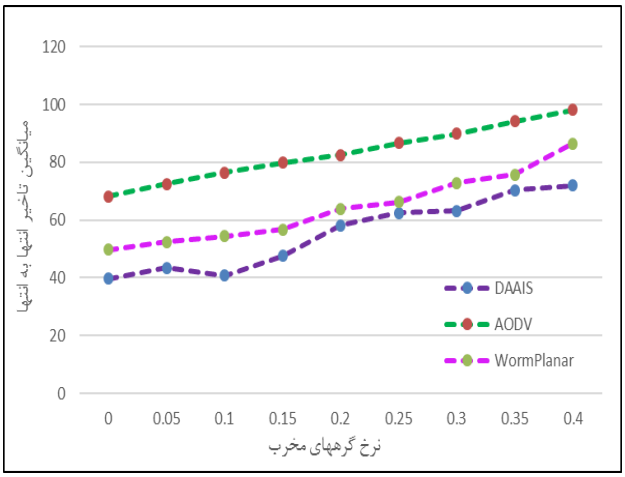
(الف) سناریوی اول



(ب) سناریوی دوم



(ج) سناریوی سوم



(د) سناریوی چهارم

شکل ۱۲: مقایسه تأخیر انتها به انتها روش پیشنهادی WAAIS با WormPlanar و پروتکل مسیریابی AODV در شرایط حمله در چهار سناریو

بدیهی است که چنانچه یک مسیر آلوده به حمله کرم‌چاله بود، بسته آزمایش به مقصد نمی‌رسید و لذا بسته تائید دریافت نمی‌کرد. در این شرایط احتمال اینکه این مسیر یک مسیر آلوده باشد افزایش می‌یافت. در فاز دوم؛ با توجه به اطلاعات به‌دست آمده مسیرها از فاز اول چنانچه مسیری دارای تعداد گام کمی بود. احتمال اینکه این مسیر یک میسر آلوده باشد افزایش می‌یافت. این در حالی است که پائین بودن زمان رفت‌وبرگشت و بالا بودن مجموعه انرژی گره‌های موجود در مسیرهای به‌دست‌آمده از فاز اول علاوه بر اینکه امنیت مسیر را از نقطه‌نظر حمله کرم‌چاله ارتقاء می‌داد از نقطه‌نظر کارایی مسیر نیز مطلوب بود. لذا مسیر مطلوب، مسیری در نظر گرفته شد که طبق رابطه بالا باعث بیشینه شدن شاخص F_i گردید. نتایج حاصل از شبیه‌سازی در چهار سناریو، نشان داد کارایی روش پیشنهادی نسبت به WormPlanar و AODV در شرایط حملات کرم‌چاله از نقطه‌نظر نسبت بسته‌های تحویل داده‌شده، تعداد بسته‌های حذف‌شده توسط مهاجمین و تأخیر انتها به انتها بهتر بود.

مراجع

[۱] رضا فتوحی، دفاع در برابر حملات کرم‌چاله در شبکه‌های موردی سیار با استفاده از سیستم ایمنی مصنوعی، فوق لیسانس، دانشگاه آزاد اسلامی واحد شبستر، شبستر، ۸۵-۱، سال ۱۳۹۳.

[۲] معصومه واعظی و محمدعلی جبرئیل جمالی، «پروتکل مسیریابی جدید مبتنی بر کیفیت خدمات در شبکه‌های حسگر بی‌سیم با تحلیل سلسله مراتبی»، *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۶، شماره ۲، صفحه ۳۵۵-۳۶۷، سال ۱۳۹۵.

[۳] یاسر عظیمی، وحید هاشمی‌فرد، جمشید باقرزاده، «تشخیص توزیع‌شده و مشارکتی حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم»،

مجله مهندسی برق دانشگاه تبریز، جلد ۴۶، شماره ۴، صفحه ۱۹۵-۲۰۶، سال ۱۳۹۵.

[4] S. Zandiyan, R. Fotohi, & M. Koravand, "P-Method: Improving AODV Routing Protocol for Against Network Layer Attacks in Mobile Ad-Hoc Networks," *International Journal of Computer Science and Information Security*, vol. 14, no. 6, pp. 95-103, 2016.

[5] S. Jamali, and V. Shaker, "Defense against SYN flooding attacks: A particle swarm optimization approach," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 2013-2025, 2016.

[6] L. N. DeCastro, and J. Timmis, "Artificial immune systems: a new computational intelligence approach," *Springer Science & Business Media*, 2002.

[7] M. Zeidenberg, *Neural Network Models in Artificial Intelligence*, Ellis Horwood, 1990.

[8] P. Matzinger, "The Danger Model: A Renewed Sense of Self," *Science*, vol. 296, no. 5566, pp. 301-305, 2002.

[9] U. Aickelin, S. Cayzer, "The Danger Theory and Its Application to Artificial Immune Systems," *1st International Conference on Artificial Immune Systems (ICARIS), Canterbury, UK*, pp. 141-148, 2002.

[10] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, J. McLeod, "Danger Theory: The Link between AIS and IDS," *2nd International Conference on Artificial Immune Systems (ICARIS), Edinburgh, UK, Lecture Notes in Computer Science 2787, Springer-Verlag*, pp. 147-155, 2003.

[11] A. Secker, A. Freitas, J. Timmis, "A Danger Theory Inspired Approach to Web Mining," *2nd International Conference on Artificial Immune Systems (ICARIS), Edinburgh, UK, Lecture Notes in Computer Science 2787, Springer-Verlag*, pp. 156-167, 2003.

[12] J. Greensmith, U. Aickelin, S. Cayzer, "Introducing Dendritic Cells as a novel Immune-Inspired Algorithm for Anomaly Detection," *4th International Conference on Artificial Immune Systems (ICARIS), Banff, Canada, Lecture Notes in Computer Science* 3627, Springer-Verlag, pp. 153-167, 2005.

[13] J. D. Farmer, N. H. Packard, and A. S. Perelson, "The immune system, adaptation, and machine learning," *Physica D: Nonlinear Phenomena*, vol. 22, no. 1: pp. 187-204, 1986.

[14] J. Twycross, U. Aickelin, "Towards a Conceptual Framework for Innate Immunity," *4th International Conference on Artificial Immune Systems (ICARIS), Banff, Canada, Lecture Notes in Computer Science 3627, Springer-Verlag*, pp. 112-125, 2005.

[15] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM), IEEE Societies*, vol. 3, pp. 1976-1986, 2003.

[16] K. Sun, P. Ning, and C. Wang, "Secure and resilient clock synchronization in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 395-408, 2006.

[17] F. Naït-Abdesselam, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Communications*, vol. 46, vol. 4, pp. 127-133, 2008.

[18] J. T. Chiang, J. J. Haas, Y. C. Hu, P. R. Kumar, & J. Choi, "Fundamental limits on secure clock synchronization and man-in-the-middle detection in fixed wireless networks," *INFOCOM* 2009, USA, pp. 1962-1970, 2009.

[19] Y. T. Hou, C. M. Chen, & B. Jeng, "Distributed detection of wormholes and critical links in wireless sensor networks," *Third International Conference in Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), USA*, vol. 2, pp. 639-642, 2007.

[20] J. Eriksson, S. V. Krishnamurthy, & M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," *14th IEEE International Conference on Network Protocols (ICNP'06)*, USA, pp. 75-84, 2006.

[21] X. Wang, & J. Wong, "An end-to-end detection of wormhole attack in wireless ad-hoc networks," *31st Annual International Computer Software and Applications Conference (COMPSAC), USA*, vol. 1, pp. 39-48, 2007.

[22] X. Lu, D. Dong, & X. Liao, "WormPlanar: Topological Planarization Based Wormhole Detection in Wireless Networks," *42nd International Conference on Parallel Processing, USA*, pp. 498-503, IEEE, 2013.

[23] V. Teotia, S. K. Dhurandher, I. Woungang, & M. S. Obaidat, "Wormhole prevention using COTA mechanism in position based environment over MANETs," *In 2015 IEEE International Conference on Communications (ICC), USA, pp. 7036-7040, IEEE, 2015*.

[24] R. Fotohi, Y. Ebazadeh, & M. S. Geshlag, "A New Approach for Improvement Security against DoS Attacks in Vehicular Ad-hoc Network," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no. 7, pp. 10-16, 2016.

[25] R. Fotohi, S. Jamali, F. Sarkohaki, S. Behzad, "An Improvement over AODV Routing Protocol by Limiting Visited Hop Count," *IJITCS*, vol. 5, no. 9, pp. 87-93, 2013.

[26] R. Fotohi, and S. Jamali, "A Comprehensive Study on Defence against Wormhole Attack Methods in Mobile Ad hoc Networks," *International journal of Computer Science & Network Solutions*, vol. 2, no. 5, pp. 36-56, 2014.

[27] S. Behzad, R. Fotohi, and F. Dadgar, "Defense Against the Attacks of the Black Hole, Gray Hole and Wormhole in MANETs Based on RTT and PFT," *International Journal of Computer Science and Network Solutions (IJCSNS)*, vol. 3, no. 3, pp. 89-103, 2015.

زیرنویس‌ها

[1] Mobile Adhoc Networks

[2] Wormhole Attack

[3] Artificial Immune System (AIS)

[4] On-Demand

[5] Broadcast

[6] Directional Antena

[7] Denial of Servis (DoS)

[8] De Castro

[9] Timmis

[10] Lymphocytes

[11] Pathogen

[12] Antibody

[13] Clonal Selection

[14] Adaptability

[15] Robustness

[16] Zeidenberg

[17] Temporal Packet Leashes

[18] Geographical Packet Leashes