

بهبود پروتکل AODV جهت مقابله با حملات کرم چاله در شبکه‌های اقتضایی

فرید محمدی^۱ و حسین قرایی^{۲*}

^۱ دانشگاه تهران، پردیس بین الملل کیش، تهران، ایران

^۲ پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران



چکیده

حمله کرم چاله یک نوع حمله فعال است که در لایه سوم شبکه از شبکه‌های اقتضایی رخ می‌دهد. در این حمله مهاجمان با متقاعد کردن گره فرستنده برای ارسال اطلاعات از یک مسیر جعلی که کوتاه‌تر و سریع‌تر از مسیر عادی به نظر می‌رسد، سعی دارند ارسال بسته‌ها از تونل ایجاد شده انجام شود تا بتوانند، حملات تحلیل ترافیک، انکار سرویس، رها کردن بسته‌ها و یا جلورانی انتخابی را انجام دهند. هر پروتکلی که از مقیاس کم‌ترین تأخیر و کم‌ترین تعداد گام برای مسیریابی استفاده کند، در برابر این حمله آسیب‌پذیر است. در این مقاله یک راه‌کار جدید برای مقابله با حملات کرم چاله ارائه خواهد شد. در راه‌حل پیشنهاد شده هر گره دارای یک وزن است و مجموع وزن‌ها در شبکه برابر صد خواهد بود. هرگاه گره‌ای قصد ارسال ترافیک به گره دیگر را داشته باشد، در بسته^۱ RREQ حداقل وزن درخواستی برای ایجاد ارتباط را بیان می‌کند. گره فرستنده با توجه به اهمیت داده‌هایی که ارسال خواهد کرد، مشخص می‌کند که مجموع وزن گره‌های شرکت‌کننده، در فرایند کشف مسیر، باید چقدر باشد. روش پیشنهادی MAODV نام‌گذاری خواهد شد. روش ذکر شده به صورت نرم‌افزاری بوده و با توجه به این‌که از روش رمزنگاری استفاده نمی‌کند، پیش‌بینی می‌شود سربار کمتری نسبت به سایر روش‌ها داشته باشد؛ و همچنین به علت عدم استفاده از الگوریتم‌های سخت، توان گره‌ها که اتفاقاً محدود است، کمتر صرف محاسبات خواهد شد. کارایی الگوریتم پیشنهادی در محیط ns-2 نشان داده خواهد شد.

واژگان کلیدی: شبکه MANET، حمله کرم چاله، پروتکل مسیریابی AODV، NS-2

Modified AODV Routing Protocol in Order to Defend Wormhole Attacks

Farid Mohammadi¹ & Hossein Gharaee^{2*}

¹Kish International Campus, Tehran University, Tehran, IRAN

²IRAN Telecom Research Center (ITRC), Tehran, IRAN

Abstract

Mobile Ad hoc Networks (MANET) are vulnerable to both active and passive attacks. The wormhole attack is one of the most severe security attacks in wireless ad hoc networks, an attack that can be mounted on a wide range of wireless network protocols without compromising any cryptographic quantity or network node. In Wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If the source chooses this fake route, malicious nodes have the option of sniff, modify, selectively forward packets or them. Existing solution defends wormhole attacks, such as SECTOR, Packet Leashes, DelPHI, directional antenna. These solutions require special hardware or strict synchronized clocks or cause message overhead, or generate false-positive alarms. A novel approach MAODV: Modified AODV is proposed to defend wormhole attacks, launched in AODV. The proposed approach is based on weight per hop. Each node in network has its own weight, given

¹RREQ

by administration due to trusty power capability. Sum of weight will not be exceeded from 100. Whenever a source node wants to send a traffic to destination, puts its minimum weight in RREQ packet to constitute the route. The destination node is selected in the route that its weight is close to destination announcement weight. Since no special hardware and no encryption techniques are used, it is likely to have less overhead and delay, compared to other techniques.

The proposed wormhole defend mechanism is discussed in detail. Our proposed system does not require any synchronized clocks or special hardware to defend wormhole attacks. In our proposed system some parameters will be added to AODV routing protocol and make it more secure against wormhole attacks. We will name this new protocol as MAODV. In the first place, there is a master node in network, which weighs 100 (weights of whole network). Whenever a node attends to enter the network, sends a join message to nearest neighbor. After receiving the message, master node will share its weights with the node requester, and sends the weight to this node requester. This process and weight sharing will be repeated after any requests to join a network, and total weight of network is not exceeded from 100. In our proposed method, each path which is created between source and destination, has a particular weight and this weight equals to intermediate node weights being added to each other. In MAODV whenever a source node wants to send RREQ packet, it adds the minimum weight to constitute route. After receiving RREQ packets, each intermediate node increases its weight beside increasing hop count. Each intermediate node does the same action, as far as destination node receives, RREQ packet among the received RREQ, one of them will be selected which its weight is the same as minimum requested weight by source, or slightly more than that. For instance, consider fig 1 which has 14 nodes. Assuming the node weights are equal for each node and its 7. As mentioned, the weight of whole network is tantamount to 100. Example 1: consider fig. 1 in which node A sends RREQ to node B. At first, node A checks its cache table to see whether there is a route between A and B, or not. If the answer is positive, it starts to send data. If the answer is negative, it sets up RREQ as follow: $\langle A, B, 1, 7, 25, [] \rangle$ which means: A: source, B: destination, 1: hop count, 7: constitute path weight, 25: request weight, []: intermediate nodes. Each node which receives RREQ will check if it is the destination or not. If it wasn't: 1. Increase hop count, 2. puts its weight to constitute path weight, 3. Adds its address as an intermediate node. And then broadcasts RREQ packet to the neighbors. In this example node A sends RREQ to X and C, which are legitimate neighbor of A. When X receives the packet, modifies it as: $\langle A, B, 2, (4, 25, [X]) \rangle$ and forwards it to its neighbors on the other hand node. C modifies packet as: $\langle A, B, 2, (4, 25, [C]) \rangle$ and forwards it to its neighbor D. This action will be repeated until B gets two RREQ - $\langle A, B, 4, 28, 25, [C, D, E] \rangle$ and $\langle A, B, 7, 25, 48, [X, U, V, W, Z, Y] \rangle$ - among the received RREQ, B will be selected which its weight is the same as minimum requested weight by A, or slightly more than that, so the first route will be chosen by B. node B setup RREP packet as $\langle A, B, 1, 4, 25, 7, [E, D, C] \rangle$ which means: A: source, B: destination, 1: back path weight, 4: hop count, 25: request weight, 7: constitute path weight, [E, D, C]: intermediate nodes.

The effectiveness of the propose mechanism is evaluated using ns2 network simulator. The simulator's outcome demonstrates that PDR in MAODV rose by 5% up to 8% in presence of two malicious nodes, compared to PDR in AODV routing protocol. The average delay point to point in MAODV is more than AODV, but on the other hand, it is less than SAODV due to not using encryption.

Keywords: MANET, Wormhole attacks, AODV, NS2

است. گره‌های بداندیش می‌توانند حملات فعال و یا غیر فعال

را به شبکه وارد کنند. در حملات غیر فعال یک گره بداندیش فقط محتوای بسته‌ها و ترافیک را شنود می‌کند؛ درحالی‌که در حملات فعال، هدف مهاجم خنثی کردن و یا حذف ویژگی‌های امنیتی، رهاکردن و یا تغییر بسته‌های قانونی است [4]. حمله کرم چاله یک حمله فعال است که در لایه سوم شبکه رخ می‌دهد. در این حمله، حمله‌کننده بسته‌ها و یا بیت‌ها را در یک محل شبکه ذخیره کرده و آن‌ها را از طریق یک تونل به محل دیگر منتقل می‌کند. تونل کرم‌چاله به‌طور معمول بین دو گره بدرفتار^۱ که به‌طورعمومی در فاصله دور از هم قرار دارند و با هم برای ایجاد یک مسیر جعلی با فاصله یک گام تبانی کرده باشند، تأسیس می‌شود. مهاجمان

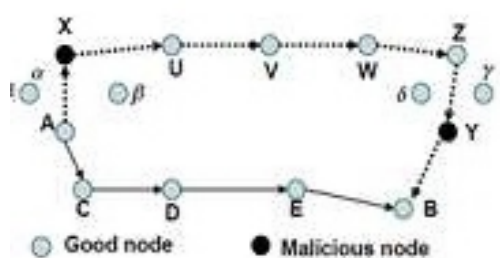
۱- مقدمه

شبکه‌های MANET به مجموعه شبکه‌های متحرک اطلاق می‌شود که بدون داشتن زیرساخت ثابت و داشتن خاصیت تحرک گره‌ها، با یکدیگر ارتباط برقرار می‌کنند. این گره‌ها همانند گوشی‌های بی‌سیم، لپ‌تاپ و دستیار دیجیتالی دارای برد انتقال محدود هستند؛ از این‌رو، هر گره توانایی ارتباط مستقیم با گره دیگر و جلورانی پیام‌ها به همسایه‌ها را تا زمانی که بسته‌ها به گره‌های مقصد برسد دارد. برقراری امنیت در چنین شبکه‌هایی به بزرگترین چالش تبدیل شده است. ماهیت باز شبکه‌های بی‌سیم کار را برای مهاجمان برای بررسی ترافیک شبکه و یا دخالت در آن آسان کرده

بین مبدأ و مقصد داده‌اند. این موضوع به گره‌ها، اجازه کشف مسیرهای مجازی را که بیش از دو گام فاصله دارند، نخواهد داد. شکل (۱) را در نظر بگیرید، جایی که A گره مبدأ و B گره مقصد است، هر دو با حضور دو گره بداندیش X و Y برای یافتن کوتاه‌ترین مسیر میان یکدیگر تلاش می‌کنند. گره A بسته RREQ را پخش می‌کند، X بسته RREQ را دریافت کرده و آن را به مقصد Y با توجه به مسیری که میان X و Y وجود دارد، یعنی (U-V-W-Z) بازگشایی می‌کند. گره Y بسته را کپسوله و آن را دوباره پخش می‌کند که به گره B می‌رسد. با توجه به کپسوله کردن بسته، مقدار گام در طول پیمایش (U-V-W-Z) اضافه نخواهد شد. به طور هم‌زمان RREQ مسیر خود از A به B را از طریق (C-D-E) طی خواهد کرد. اکنون گره B دو مسیر را پیش خواهد داشت، اولی مسیری با طول چهار گام خواهد بود (A-C-D-E) و E-B) و مسیری دوم که به نظر مسیری با طول سه گام است (A-X-Y-B). گره B مسیر دوم را با توجه به این‌که کوتاه‌تر به نظر می‌رسد، انتخاب خواهد کرد؛ درحالی‌که درواقع این مسیر با طول گام هفت است. هر پروتکل مسیریابی که از مقیاس کوتاه‌ترین مسیر برای انتخاب بهترین مسیر استفاده می‌کند، در برابر این روش حمله کرم چاله آسیب‌پذیر است [2].

۲-۲- کرم چاله با استفاده از کانال خارج از باند

این مدل برای حمله، از کانال out-of-band استفاده می‌کند. این حمله با استفاده از کانال پهنای باند قوی بین گره‌های بداندیش انجام می‌شود. این مدل از حمله نیازمند ظرفیت سخت‌افزاری ویژه است.



(شکل ۱): کرم چاله با استفاده از کپسوله کردن
(Figure-1): Wormhole using encapsulation method

شکل (۲) را در نظر بگیرید، جایی که گره A، RREQ را به گره B ارسال می‌کند و گره‌های X و Y گره‌های بداندیش هستند که دارای کانال خارج از باند میان یکدیگر می‌باشند. گره X بسته RREQ را به Y که همسایه مجاز B است، تونل می‌زند. گره Y بسته را به همسایه‌های خود که شامل B نیز است، پخش می‌کند. گره B، دو RREQ را دریافت می‌کند

در این حمله، مسیر کوتاه‌تر را معرفی می‌کنند و منجر به مسیریابی بسته‌ها از این مسیر جعلی می‌شوند. پس از برقراری موفق تونل کرم‌چاله، نظیرهای کرم‌چاله، بسته‌های داده را می‌توانند تغییر دهند، آن‌ها را رها کنند، حملات انکار سرویس را انجام دهند و یا بسته‌ها را به صورت دلخواه جلورانی و یا رها کنند [11]. پروتکل‌های مسیریابی بر مبنای نیاز همانند AODV و DSR در هنگام فرایند کشف مسیر در خطر حمله کرم‌چاله قرار دارند. بدین معنی که گره‌های بداندیش گره مبدأ را متقاعد می‌کنند، مسیری با تعداد گام کمتر و یا سریع‌تر برای ایجاد ترافیک به گره مقصد وجود دارد. درحالی‌که در واقعیت چنین مسیری وجود ندارد. ارزیابی تأثیرات حمله کرم‌چاله نشان می‌دهد، پارامترهای مختلف شبکه، همانند خروجی شبکه، میانگین تأخیر انتها به انتها و نرخ ازدست‌دادن بسته‌ها تحت تأثیر تونل کرم‌چاله در شبکه قرار می‌گیرد [1]. بنابراین در این مقاله سعی خواهد شد، با اعمال سازوکارهایی پروتکل مسیریابی AODV که یکی از مهم‌ترین پروتکل‌های مسیریابی بر مبنای نیاز است، نسبت به حمله کرم چاله مقاوم شود. در ادامه این مقاله، در بخش ۲ حمله کرم چاله و انواع مختلف آن بررسی، در بخش ۳ کارهای مرتبط معرفی خواهد شد؛ در بخش ۴ روش پیشنهادی مطرح و در بخش ۵ نتایج شبیه‌سازی نمایش و در نهایت بخش ۶ مقاله نتیجه‌گیری بیان می‌شود.

۲- سبک‌های مختلف حمله کرم چاله

بر اساس تکنیک‌های مورد استفاده برای انجام حمله کرم چاله، سبک‌های این حمله به صورت زیر تقسیم بندی شده است [6]:

۲-۱- کرم چاله با استفاده از کپسوله کردن

زمانی که گره مبدأ، بسته RREQ را پخش می‌کند، یک گره بداندیش که یک قسمت از شبکه است، بسته RREQ را دریافت می‌کند. گره بداندیش بسته را به گره‌ای که از قبل با هم تبانی کرده‌اند و این گره در یک فاصله دور نسبت به گره بداندیش و نزدیک به گره مقصد است، تونل می‌زند و بعد RREQ را دوباره پخش همگانی می‌کند. همسایه‌های گره تبانی‌کننده دوم، RREQ را دریافت کرده و تمامی تقاضاهای مجاز بعدی را که ممکن است، بعداً از مسیرهای چندگامی مجاز برسد حذف می‌کنند. نتیجه به این صورت خواهد بود که مسیر بین مبدأ و مقصد از طریق دو گره تبانی‌کننده عبور خواهد کرد که می‌توان گفت تشکیل یک کرم چاله را

به صورت مصنوعی توسط گره نفوذگر X با کنترل کرم چاله پیامها میان A-B می تواند شکل گیرد [13].

۲-۵- کرم چاله با استفاده از انحراف پروتکل^۲

برخی پروتکل های مسیریابی مانند ARAN، مسیر با کوتاه ترین تأخیر را نسبت به کم ترین تعداد گام، در اولویت قرار می دهند. در طی تقاضای ارسال مسیری، گره ها به طور معمول منتظر یک مقدار تصادفی از زمان قبل از ارسال می باشند. این عمل با توجه به این واقعیت که ارسال تقاضا با انتشار همگانی به پایان می رسد رخ می دهد، بنابراین کاهش دادن تصادم لایه MAC^۳ امر مهمی به شمار می رود. یک گره بداندیش به راحتی می تواند حمله کرم چاله را با موافقت نکردن پروتکل و انتشار همگانی بدون منتظرماندن^۴ برای مقدار تصادفی زمان، انجام دهد. هدف از انجام این کار به این شکل خواهد بود که بسته درخواست ارسال، به عنوان نخستین بسته به مقصد برسد، این عامل احتمال این را که مسیر بین مبدأ و مقصد شامل گره بداندیش باشد، افزایش می دهد [10].

(جدول- ۱): روش های مختلف حمله کرم چاله

(Table- 1): Wormhole attack methods

نام روش	حداقل گره های تبانی کننده	نیازهای خاص
کپسوله کردن بسته	دو	_____
کانال خارج از باند	دو	ارتباط خارج از باند
توان بالای ارسال	یک	منبع با انرژی زیاد
باز پخش بسته ها	یک	_____
انحراف پروتکل	یک	_____

۳- پژوهش های پیشین

۳-۱- روش مهار بسته ها

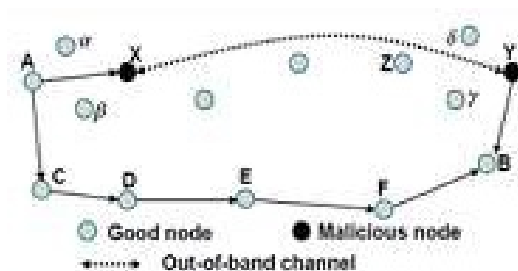
سازوکار مهار بسته ها یک سازوکار کلی جهت تشخیص و دفاع از حملات کرم چاله است. یک مهار، یک سری اطلاعات است که به یک بسته اضافه می شود [5] تا بیشینه فاصله انتقال بسته را محدود و مشخص کند. مهارها جهت محافظت در برابر حملات کرم چاله در انتقال های بی سیم طراحی شده اند. مهار بسته ها به دو صورت جغرافیایی و زمانی انجام می شود. در مهار جغرافیایی هر گره موقعیت جغرافیایی خود

² Protocol Deviation

³ Message Authentication Code

⁴ Backing off

نخستین مسیر شامل (A-X-Y-B) و دومی (A-C-D-E-F- (B است. اولین مسیر، هم کوتاه تر و هم سریع تر از مسیر دوم است و به همین دلیل توسط B انتخاب می شود.



(شکل ۲): کرم چاله با استفاده از کانال خارج از باند

(Figure-2): Wormhole using out of band channel method

۲-۳- کرم چاله با استفاده از توان بالای ارسال

در این شیوه، وقتی یک گره بداندیش بسته RREQ را دریافت می کند، تقاضا را به یک سطح توان بالا که این توانایی در بین گره های دیگر شبکه موجود نیست، پخش می کند. هر گره که پخش توان بالا را می شنود، دوباره آن را به سمت مقصد، پخش همگانی می کند. با استفاده از این روش، شانس گره بداندیش برای این که در مسیر ایجاد شده میان مبدأ و مقصد باشد، افزایش خواهد یافت.

۲-۴- کرم چاله با استفاده از بازپخش کردن بسته^۱

در این شیوه گره بداندیش بسته ها را بین دو گره دور ارسال می کند تا آن ها را متقاعد کند که با یکدیگر همسایه هستند. این شیوه می تواند با حضور یک گره بداندیش نیز انجام شود. هر چند با وجود چند گره بداندیش می توان فهرست همسایه گره قربانی را به صورت چندگامی گسترش داد. این عمل توسط گره نفوذگر X که داخل محدوده انتقال دو گره مجاز A و B قرار دارد، انجام می شود، جایی که A و B خود در داخل محدوده انتقال یکدیگر نیستند. گره نفوذگر X فقط کنترل ترافیک میان A و B (و برعکس) را تونل می زند و این کار را بدون تغییر فرض شده در پروتکل مسیریابی انجام می دهد. برای مثال بدون وارد کردن نشانی به عنوان منبع در سرآمد بسته ها، و به این ترتیب گره X به صورت مجازی نامرئی خواهد بود. گره X پس از آن می تواند بسته های تونل شده را حذف و یا هر زمان که خواست این ارتباط را قطع کند. درواقع یک ارتباط خارج از قلمرو میان A-B

¹ Packet relay

این سازوکار می‌تواند حمله کرم چاله را شناسایی کند، گرچه توانایی شناسایی محل دقیق کرم چاله را ندارد.

۳-۳- روش‌های مبتنی بر RTT^5

در [9] گره فرستنده با تشخیص میزان تأخیر مسیرهای مختلف تا مقصد، حمله کرم چاله را شناسایی می‌کند. شماره گام^۶ و اطلاعات تأخیر مسیرهای جدا شده، جمع‌آوری و مقدار مقدار تأخیر برای هر گام به‌عنوان نشان‌گر حمله به کار گرفته می‌شود. در حالت عادی مقدار تأخیر بسته که در یک گام منتشر می‌شود، در طول مسیر برای هر گام مشابه است، ولی در هنگام حمله کرم چاله این مقدار تأخیر بدون توجه با توجه به حضور گره‌های بدرفتار در طول مسیر بالا خواهد بود. بنابراین اگر مسیری تأخیر بالا به‌ازای هر گام داشته باشد، در معرض کرم چاله قرار خواهد گرفت. مشکل این روش این است که، شناسایی، تنها توسط زمان انتقال می‌تواند منجر به تولید زیاد نرخ خطای مثبت شود. یعنی ممکن است تأخیر ایجاد شده بنا به ازدحام بسته‌ها در مواردی خاص رخ دهد، نه این‌که لزوماً حمله اتفاق افتاده باشد.

۳-۴- روش مبتنی بر چالش / پاسخ^۷

در [3] هدف استفاده از سیستم چالش / پاسخ برای به کمینه رساندن تأخیرهای ممکن بدون استفاده از ابزار CPU است. با استفاده از الگوریتم محدودکننده فاصله، فاصله میان دو همسایه با ارسال یک بیت چالش محاسبه شده و مشخص می‌شود که آیا فاصله محاسبه شده در محدوده انتقال ممکن وجود دارد یا خیر. از آنجایی که این الگوریتم، فاصله در هر گام را محاسبه می‌کند، نمی‌تواند راه حلی برای مقابله با حملات کرم چاله آشکار داشته باشد. این روش به یک سخت‌افزار ویژه نیاز دارد تا بتواند به یک بیت چالش به‌صورت آنی پاسخ دهد.

۳-۵- روش LiteWorp

این روش [7] پروتکلی جهت کشف حمله کرم چاله در شبکه‌های ایستا ارائه کرد که به آن LiteWorp گفته می‌شود. هنگامی که LiteWorp اجرا می‌شود، گره‌ها اطلاع کاملی از مسیرهای با دو گام با توجه به همسایه‌های خود

را با استفاده از GPS^۱ در شبکه پیدا می‌کند. همچنین، تمامی گره‌ها دارای کلاک هماهنگی ضعیف^۲ در حد میلی ثانیه هستند. هر گره قبل از ارسال بسته، موقعیت خود (p_s) و زمان ارسال بسته (t_s) را به بسته اضافه می‌کند. گره گیرنده با دریافت بسته و مقایسه p_s با موقعیت خودش (p_r) و مقایسه t_s با زمان دریافت بسته (t_r) و با در نظر گرفتن بیشینه تفاوت کلاک هماهنگی بین فرستنده و گیرنده برابر $\pm \Delta$ و سرعت نور برابر v و بیشینه خطا در اطلاعات محل برابر δ ، فاصله بین فرستنده و گیرنده (d_{sr}) را با فرمول (۱) محاسبه می‌کند:

$$d_{sr} \leq \|p_s - p_r\| + 2v \cdot (t_r - t_s + \Delta) + \delta \quad (1)$$

گیرنده با محاسبه d_{sr} از این مسافت جهت کشف و شناسایی رخ داد و یا عدم رخ داد حمله کرم چاله استفاده می‌کند. در مهار زمانی تمامی گره‌ها نیاز به یک کلاک هماهنگی دقیق^۳ در حد نانو ثانیه دارند. هنگام استفاده از مهار زمانی گره فرستنده، زمان ارسال بسته (t_s) و همچنین زمان انقضای بسته (t_e) را که بعد از چه مدت بسته رها خواهد شد طبق فرمول (۲) محاسبه کرده و به بسته اضافه می‌کند. (c سرعت انتشار سیگنال در شبکه بی‌سیم و کلاک هماهنگی Δ نشان‌دهنده بیشینه تفاوت بین دو گره بوده و مقدار آن باید برای تمامی گره‌های شبکه واضح بوده و در حدود چند میلی ثانیه باشد.) و گیرنده می‌تواند با استفاده از زمان ارسال بسته (t_s) توسط گره فرستنده و زمان دریافت بسته (t_r) و سرعت نور از وجود مسیر قانونی مطلع شود. اگر زمان رسیدن بسته از زمان محاسبه شده توسط گیرنده زیادتر باشد، گیرنده بسته بالا را رها می‌کند.

$$t_e = t_s + L / c - \Delta \quad (2)$$

۳-۲- روش DelPHI^۴

اندازه تأخیر برای گام توسط [8] ارائه شد. در DelPHI تلاش‌ها به‌منظور یافتن مسیرهای از بین رفته میان فرستنده و گیرنده انجام می‌شود. سپس میزان تأخیر و طول هر مسیر محاسبه شده و میانگین تأخیر به‌ازای گام، در راستای هر مسیر تعیین می‌شود. این مقادیر برای مشخص کردن حمله کرم چاله به کار می‌رود. مسیری که شامل پیوند کرم چاله است، دارای مقدار تأخیر بیشتری برای هر گام خواهد بود.

¹ Global Positioning system

² Loosely Synchronized Clock

³ Tightly Synchronized Clock

⁴ Delay per Hop Indicator

⁵ Round Trip Time

⁶ Hop number

⁷ Challenge/Response

انتها به انتها	نیاز به همگام سازی زمانی ضعیف (ms)، نیاز به GPS
آنتن های جهتی	نیاز به آنتن های جهتی برای تمامی گره ها
LiteWorp	بدون نیاز به سخت افزار اضافی، فقط قابل استفاده در شبکه های ایستا
چالش/ پاسخ	نیاز به سخت افزار برای ارسال پاسخ آتی، عدم کارایی مقابل کرم چاله آشکار

۴- مدل پیشنهادی

راه کار ارائه شده برای این نوع حمله، یک روش نرم افزاری و بدون نیاز به سخت افزار اضافی و کلاک هماهنگی است. در روش پیشنهادی یک سری سازوکارهای امنیتی بر روی پروتکل AODV اضافه شده است و باعث ایجاد امنیت بیشتر در برابر حمله کرم چاله خواهد شد. این پروتکل جدید^۲ MAODV نام گذاری خواهد شد. در ابتدای راه اندازی شبکه، یک گره به عنوان گره مادر در شبکه وجود دارد که وزن آن برابر ۱۰۰ (وزن کل شبکه) خواهد بود. هنگامی که گره ای قصد ورود به شبکه را داشته باشد، به نزدیکترین گره پیام عضویت ارسال می کند. گره مادر پس از دریافت پیام عضویت گره جدید وزن خود را با درخواست کننده تقسیم می کند و به گره مذکور می فرستد. این فرایند و تقسیم وزن با حضور هر گره جدید در شبکه تکرار می شود، تا وزن کل شبکه در عدد ۱۰۰ باقی بماند.

فرایند کشف مسیر-در پروتکل مطرح شده هر مسیر که بین گره های مبدأ و مقصد ایجاد می شود، دارای یک وزن بوده و وزن هر مسیر از جمع وزن های گره های میانی به دست می آید. همانند پروتکل AODV، برای کشف مسیر از بسته های RREP و RREQ استفاده می شود. این بسته ها ساختاری متفاوت با بسته های پروتکل AODV دارند. در این پروتکل گره مبدأ هنگام ارسال بسته RREQ، وزن مسیر درخواستی را اعلام می کند و هر یک از گره های میانی هنگام ارسال بسته RREQ به سمت مقصد، علاوه بر این که مقدار hopCount را افزایش می دهند، وزن خود را نیز به وزن مسیر ایجاد شده اضافه می کنند. این روند آن قدر تکرار می شود تا بسته مذکور به مقصد برسد. برای طراحی بسته های RREQ پروتکل MAODV فیلدهای PathReq، Patweight به ساختار بسته های RREQ پروتکل AODV اضافه شده است.

به دست می آورند. در حالی که در پروتکل های مسیریابی استاندارد شبکه های اقتضایی، گره ها به طور معمول همسایه های یک قدمی خود را بررسی می کنند؛ ولی در پروتکل LiteWorp، آن ها شناختی در مورد همسایه، گره همسایه خود را دارند، و با این کار می توانند از مزیت اطلاعات همسایه با دو گام، به جای یک گام بهره مند باشند. این اطلاعات، برای آشکار کردن حمله کرم چاله مورد استفاده می تواند قرار گیرد. بعد از احراز هویت، گره ها پیام ها را از گره ای که خود را به عنوان همسایه ثبت نکرده باشد، نخواهند پذیرفت. همچنین گره ها رفتار همسایه ها را به منظور این که آیا بسته های داده به درستی توسط همسایه ارسال می شود، نظارت می کنند، (روشی که به Watchdog معروف است. در LiteWorp گره ها نه تنها تأیید می کنند تمامی بسته ها از همسایه های خود به درستی ارسال می شوند، بلکه اطمینان حاصل می کنند که هیچ گره ای بسته ای را که دریافت نکرده ارسال نکند.

۳-۶- روش شناسایی انتها به انتها

در [12] روشی جهت شناسایی حمله کرم چاله ارائه شده که به EDWA^۱ معروف است. این روش بر مبنای کمترین تعداد گام بنا نهاده شده است. در EDWA هر گره با استفاده از سامانه موقعیت یاب، جایگاه خود را در شبکه پیدا می کند، و از تخمین مسافت اقلیدسی جهت تخمین کوتاه ترین مسیر استفاده می کند. در مرحله ردیابی، فرستنده کوتاه ترین مسیر تا گیرنده را با تخمین شمارش گام محاسبه می کند و آن را با مقدار تخمینی موجود در بسته RREP مقایسه می کند. اگر این مقدار کمتر از مقدار تخمین شده باشد، مسیر بالا را یک مسیر کرم چاله پیش بینی می کند. در مرحله آخر گره فرستنده از کوتاه ترین مسیر، از میان مسیرهای قانونی شروع به ارسال داده می کند.

(جدول- ۲): مقایسه روش های مختلف مقابله با کرم چاله

(Table- 2): Comparison between Prevention of Wormhole attack

روش	توضیحات
مهار بسته (جغرافیایی)	نیاز به GPS برای هر گره، نیاز به همگام سازی زمانی (ms)، محدودیت های فناوری GPS
مهار بسته (زمانی)	نیاز به همگام سازی زمانی قوی (ns)، غیر قابل پیاده سازی

² Modified AODV

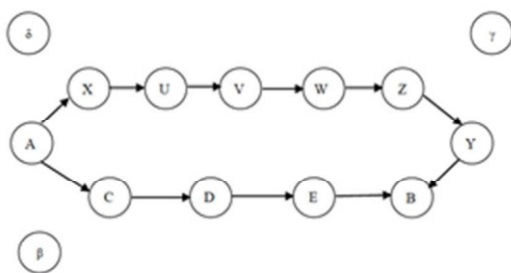
¹ End-to-End Detection Wormhole Attack

باشد. در این صورت نیز جدول Cache با توجه به اطلاعات موجود در RREP تغییر خواهد کرد.

در این بخش مثال‌های مختلفی از پروتکل MAODV مطرح خواهد شد تا عملکرد آن بهتر معلوم شود. همان‌طور که بیان شد، وزن کل شبکه برابر ۱۰۰ است. در مثال ذکر شده فرض کردیم، وزن به‌طور تقریبی به‌طور مساوی بین گره‌ها تقسیم شده است. با توجه به اینکه چهارده گره در شبکه فرضی وجود دارند، وزن هر گره برابر هفت در نظر گرفته شده است. **مثال ۱:** برای شکل (۳) سناریوی نیز را در نظر بگیرید. فرض کنید گره A بخواهد اطلاعاتی را به گره B ارسال کند.

مرحله نخست: ابتدا این گره جدول Cache خود را مورد جستجو قرار می‌دهد تا ببیند آیا مسیری برای رسیدن به گره B وجود دارد یا نه. در صورتی که پاسخ مثبت باشد بلافاصله شروع به ارسال داده می‌کند. در غیر این صورت بسته RREQ را به‌صورت $\langle A, B, 1, 7, 25, [] \rangle$ تنظیم می‌کند، بدین معنی که: A: مبدأ ارسال ترافیک. B: مقصد مورد نظر. ۱: تعداد گام ۷: وزن مسیر ایجاد شده (یا وزن بسته

RREQ) که در ابتدا وزن مبدأ است. ۲۵: وزن مسیر درخواستی توسط مبدأ. $[X, U, V, W, Z, Y]$: گره‌های میانی شرکت کننده در فرایند مسیریابی. گره A آن‌را به تمامی همسایه‌های خود ارسال می‌کند. **مرحله دوم:** هر کدام از همسایه‌ها که بسته بالا را دریافت کنند، بلافاصله بررسی می‌کند که آیا مقصد بسته است یا خیر (با توجه به فیلد دوم). در صورتی که مقصد بسته نباشد، بسته RREQ رسیده را بدین شکل تغییر می‌دهند: ۱. مقدار hopcount را یک واحد افزایش می‌دهند. ۲. وزن خود را به وزن بسته اضافه می‌کنند. ۳. نشانی خود را به فهرست گره‌های میانی اضافه می‌کنند.



(شکل-۳): چگونگی اتصال گره‌ها به یکدیگر

(Figure-3): Node connection to each other

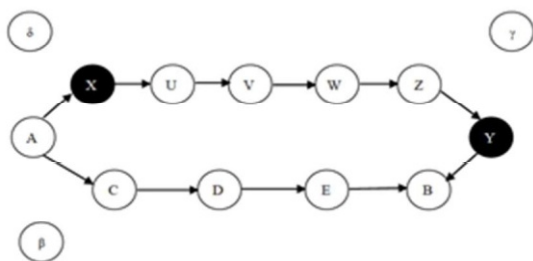
پس از انجام مراحل بالا بسته RREQ به تمامی همسایه‌ها ارسال می‌شود. با توجه به مثال بالا گره A بسته RREQ را به همسایه‌های یک قدمی خود یعنی X و C ارسال می‌کند. X با دریافت بسته RREQ و با توجه به مطالب گفته شده، آن‌را به‌صورت $\langle A, B, 2, 14, 25, [X] \rangle$

فیلد PathReq حاوی وزن مسیری است که توسط گره مبدأ درخواست می‌شود. فیلد Patweight حاوی وزن مسیر ایجاد شده است. وزن مسیر ایجاد شده از مجموع وزن‌های گره‌های شرکت کننده در فرایند کشف مسیر به دست می‌آید. این فیلد به عنوان وزن بسته RREQ نامیده می‌شود. بسته RREQ نیز همانند بسته RREQ دارای فیلد PathReq است.

بسته RREP حاوی فیلدی به نام Bakpatweight است. هنگام ارسال بسته RREP از طرف مقصد، مقدار آن برابر وزن گره مقصد خواهد بود. هنگامی که گره‌های میانی بسته RREP را دریافت می‌کنند، مقدار آن را به اندازه وزن خود افزایش می‌دهند و بسته را به سمت مبدأ ارسال می‌کنند. این فیلد به گره‌های میانی کمک می‌کند تا متوجه شوند در چه فاصله وزنی از گره مقصد قرار دارند. هنگامی که بسته RREP به مبدأ می‌رسد، مقدار آن برابر وزن مسیر ایجاد شده خواهد بود. فیلد Bakpatweight حاوی وزن مسیر بازگشتی است. این فیلد به عنوان وزن بسته RREP نامیده می‌شود.

با توجه به این که مسیرهای ایجاد شده ممکن است از نظر فاصله و وزن بهینه نباشند، باید این امکان در آنها وجود داشته باشد تا بتوان آن‌ها را بهینه کرد. برای بهینه کردن مسیرها جدول Cache را تغییر می‌دهیم. با رسیدن یک RREP جدول Cache مورد جستجو قرار می‌گیرد. اگر این RREP جدید باشد (یعنی در جدول وجود نداشته باشد) به جدول اضافه خواهد شد در غیر این صورت سه حالت زیر می‌تواند اتفاق بیافتد: حالت نخست این که وزن RREP رسیده از وزن مسیر موجود در Cache بیشتر باشد. در این صورت جدول تغییری نخواهد کرد. حالت دوم زمانی است که وزن RREP رسیده مساوی وزن مسیر موجود در Cache باشد. در این صورت دو حالت ممکن است اتفاق بیافتد. حالت نخست زمانی رخ می‌دهد که فیلد hopcount از RREP hopcount موجود در Cache کوچک‌تر باشد، در این صورت RREP جدید هم وزن مسیر قدیم بوده با این تفاوت که از لحاظ فاصله کوتاه‌تر است. در نتیجه جدول Cache با توجه به اطلاعات موجود در RREP تغییر خواهد کرد. حالت دوم زمانی است که فیلد hopcount از RREP hopcount موجود در Cache بزرگ‌تر یا مساوی باشد در این صورت جدول Cache تغییر نخواهد کرد. حالت سوم زمانی است که وزن RREP رسیده از وزن موجود در Cache کوچک‌تر

مثال ۲: در این مثال عملکرد پروتکل MAODV در مقابل حملات کرم چاله بررسی خواهد شد. برای این منظور فرض می‌کنیم گره A می‌خواهد ترافیکی را به گره B در حضور دو گره بداندیش X و Y که سعی دارند، روند مسیریابی را به‌گونه‌ای تغییر دهند تا در هنگام ارسال داده‌ها بخشی از مسیر باشند، ارسال کند. ابتدا گره A بسته RREQ به‌صورت $\langle A, B, 1, 7, 25, [] \rangle$ تنظیم کرده و آن را به تمامی همسایه‌های خود ارسال می‌کند. این بسته در گره بدخواه X دریافت و به‌صورت $\langle A, B, 2, 14, 25, [x] \rangle$ به همسایه‌های آن می‌رسد. با ادامه مراحل فرایند کشف مسیر بسته‌ای به‌صورت $\langle A, B, 6, 42, 35, [X, U, V, W, Z] \rangle$ به گره بدخواه Y می‌رسد. این گره با پردازش گره‌های میانی در می‌یابد که گره بدخواه X نیز در بین گره‌های شرکت کننده در کشف مسیر است. به همین دلیل بسته رسیده را به‌صورت $\langle A, B, 3, 42, 25, [X, Y] \rangle$ به همسایه‌های خود ارسال می‌کند. در این ارسال تمامی گره‌های میانی بین گره‌های بدخواه حذف شده و علاوه بر این که مقدار hopcount افزایش نیافته است، بلکه از مقدار آن به تعداد گره‌های حذف شده کاسته می‌شود^{۱۴}. با انجام کارهای بالا دو بسته به شکل‌های $\langle A, B, 3, 49, [X, Y] \rangle$ و $\langle A, B, 4, 28, 25 [C, D, E] \rangle$ به گره B می‌رسند. هرچند بسته $\langle A, B, 3, 49, [X, Y] \rangle$ از لحاظ گام کوچک‌تر است، ولی در گره B انتخاب نمی‌شود، زیرا در پروتکل MAODV تعداد گام ملاک انتخاب RREQ نیست؛ و عامل دوم این که نسبت به بسته دیگر اختلاف وزن بسته به وزن مسیر درخواست شده بیشتر است.



(شکل - ۴): گره‌های X و Y گره‌های بداندیش هستند.
(Figure-4): Malicious X and Y nodes

در مثال ذکر شده اگر از پروتکل‌های DSR و یا AODV استفاده کنیم، مسیر دوم یعنی $\langle A, B, 3, 49, [X, Y] \rangle$ به‌علت این که دارای تعداد گام کمتری است، انتخاب می‌شود؛ و درواقع مسیر انتخابی شامل تونل کرم چاله خواهد بود. سؤال

^{۱۴} به این کار به اصطلاح کپسوله کردن می‌گویند.

تغییر می‌دهد؛ سپس بسته RREQ را به تمامی همسایه‌های خود که در این مثال فقط U است ارسال می‌کند. در سوی دیگر گره C با دریافت بسته از گره A آن را به‌صورت $\langle A, B, 2, 14, 25 [C] \rangle$ تغییر می‌دهد و به همسایه خود، یعنی گره D ارسال می‌کند. مرحله دوم آن قدر تکرار می‌شود تا بسته به مقصد برسد. با توجه به شکل (۳) و انجام مراحل بالا دو بسته به شکل‌های $\langle A, B, 4, 28, 25 [C, D, E] \rangle$ و $\langle A, B, 7, 25, 48 [X, U, V, W, Z, Y] \rangle$ به گره B می‌رسند.

مرحله سوم: گره مقصد از بین RREQ های رسیده RREQ را قبول می‌کند که نخست این که وزن بسته آن از وزن مسیر درخواست شده زیادتر باشد و دوم این که اختلاف کمی داشته باشد. با توجه به مطالب گفته شده گره B از بین دو درخواست رسیده به درخواست $\langle A, B, 4, 28, 25 [C, D, E] \rangle$ پاسخ می‌دهد؛ زیرا وزن این بسته به وزن درخواست شده نزدیک‌تر است.

مرحله چهارم: گره مقصد پس از انتخاب RREQ، اقدام به ارسال بسته می‌کند. با توجه به مثال بالا گره B بسته RREP را به‌صورت $\langle A, B, 1, 4, 25, 7 [E, D, C] \rangle$ تنظیم می‌کند، که:

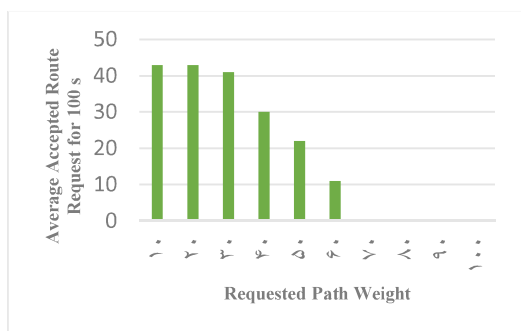
A: مبدأ. B: مقصد. ۱: تعداد گام‌های مسیر بازگشت. ۴: تعداد گام‌های مسیر رفت. ۲۵: وزن درخواست شده توسط مبدأ. ۷: وزن مسیر بازگشت (یا وزن بسته RREP) که در ابتدا وزن مقصد است. [E, D, C]: گره‌هایی که بسته RREP باید از آن‌ها عبور کند. پس از تنظیم بسته RREP، گره B آن را تنها به گره E ارسال می‌کند.

مرحله پنجم: هر کدام از گره‌ها که بسته RREP را دریافت کند، ابتدا جدول Cache خود را بر اساس اطلاعات مورد نیاز تکمیل می‌کند و سپس تغییراتی را به‌صورت زیر روی بسته RREP اعمال می‌کند: ۱. مقدار hopcount مسیر بازگشت را یک واحد افزایش می‌دهد. ۲. مقدار hopcount مسیر رفت را یک واحد کاهش می‌دهد. ۳. وزن خود را به وزن بسته اضافه می‌کند. پس از انجام مراحل بالا، بسته RREP به گره بعدی ارسال می‌شود. مرحله پنجم آن قدر تکرار می‌شود تا بسته RREP به مبدأ برسد. با توجه به مثال بالا و انجام مراحل گفته شده، بسته RREP به‌صورت $\langle A, B, 4, 1, 25, 28, [D, C, B] \rangle$ به مبدأ می‌رسد. پس از رسیدن بسته به مبدأ، مبدأ شروع به ارسال داده می‌کند.

بسته RREQ در مقصد مورد پذیرش قرار خواهد گرفت. همان‌طور که دیده می‌شود، تعداد RREQهای پذیرفته‌شده به‌ازای وزن‌های بالای شصت، به‌طور تقریبی صفر است. یعنی اگر مبدأ مسیری با وزن هفتاد را درخواست کند، چنین مسیری ایجاد نخواهد شد. با توجه به این‌که وزن صد بین گره‌ها توزیع می‌شود، نتایج این شبیه‌سازی را می‌توان برای تعداد گره‌های بیشتر بسط داد.

(جدول-۳): پارامترهای شبیه‌سازی
(Table- 3): Simulation Parameters

پروتکل استفاده شده در شبیه سازی	MAODV
زمان شبیه سازی	۱۰۰۰S
ابعاد شبیه سازی	۱۰۰۰*۱۰۰۰
تعداد گره‌ها	۵۰-۱۰
محدوده انتقال بی‌سیم	۲۵۰ متر
نرخ انتقال داده	۴Mb/s
اندازه بسته‌ها	۵۱۲
سرعت گره‌ها	۱-۱۰S
نوع تحرک گره‌ها	تصادفی
نوع ترافیک	CBR



(شکل-۵): تعداد RREQهای پذیرفته‌شده به‌ازای ۱۰ گره
(Figure- 5): Number of acceptance RREQ nodes

میانگین نرخ بسته‌های رسیده

نرخ بسته‌های رسیده که در اصطلاح با PDR^1 نمایش داده می‌شود، برای تعریف تعداد بسته‌های داده‌ای است، که یک گره فرستاده و گره مقصد آن‌ها را صحیح دریافت کرده است. میانگین نرخ بسته‌های رسیده عبارت از نرخ بسته‌های رسیده به یک مقصد از تمامی گره‌های شبکه است. شکل (۶) میزان بسته‌های رسیده به مقصد را در ترافیک UDP با تعداد ده الی پنجاه گره، با حضور دو گره بداندیش که سعی دارند با تونل‌زدن مسیر بین منبع و مقصد، در فرایند مسیریابی شرکت کنند؛ و با حداقل وزن‌های مختلف بین ده

قابل طرح این است که گره Y چرا وزن بسته را همانند hopcount کاهش (یا افزایش) نمی‌دهد تا توسط مقصد انتخاب شود. پاسخ می‌تواند بدین شکل باشد که: چون گره E هیچ‌گونه اطلاعاتی در مورد محل گره مقصد و وزن گره‌های میانی بین آن‌ها ندارد، هر گونه کاهش (یا افزایش) نمی‌تواند دلیلی برای انتخاب بسته باشد؛ زیرا اگر مقدار وزن بسته را کاهش دهد، ممکن است که به هیچ وجه بسته مذکور انتخاب نشود و یا اگر وزن بسته را افزایش دهد ممکن است در رقابت با سایر بسته‌ها از دور خارج شود. در نتیجه انتخاب بسته به‌ازای افزایش یا کاهش وزن آن در مقصد امری تصادفی خواهد بود، درحالی‌که در پروتکل‌هایی مثل DSR و AODV اگر گره‌های بدرفتار هر چقدر مقدار hopcount را بیشتر کاهش دهند، امکان انتخاب‌شدن آن‌ها نیز بیشتر خواهد شد؛ در صورتی‌که در پروتکل MAODV این‌گونه نیست. و عامل دوم این‌که، با توجه به توزیع به‌طور تقریبی یکنواخت وزن میان گره‌ها، گره‌های بداندیش توانایی کاهش یا افزایش قابل توجه وزن را نخواهند داشت.

۵- پیاده‌سازی و نتایج شبیه‌سازی

برای نشان دادن کارایی راه‌کار ارائه‌شده، آن را روی پروتکل AODV اعمال کرده و از محیط ns-2 بدین منظور استفاده خواهد شد. همان‌طور که پیش‌تر اشاره شد، پروتکل مسیریابی AODV یک پروتکل مسیریابی بر مبنای نیاز است. در این پروتکل مسیرها تنها زمانی کشف می‌شوند که مبدأ اقدام به برقراری ارتباط با گره دیگری را انجام دهد. زمانی که یک گره بخواهد با گره دیگری ارتباط برقرار کند، باید فرایند کشف مسیر را در شبکه فراخوانی کند. در این حالت قبل از برقراری ارتباط، تأخیر قابل توجهی مشاهده می‌شود. جدول (۳) پارامترهای استفاده‌شده در محیط شبیه‌سازی را نشان می‌دهد.

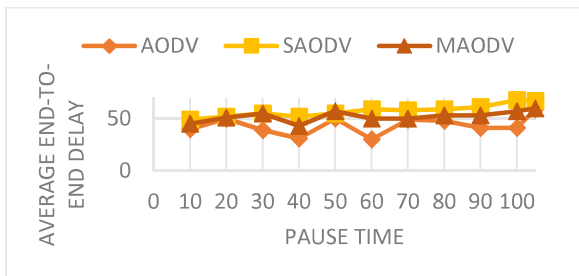
تعداد RREQهای پذیرفته‌شده در مقصد

هدف از این پارامتر این است که ببینیم، چه تعداد از مسیرهایی که توسط مبدأ با وزن‌های مختلف درخواست می‌شود، در مقصد مورد پذیرش قرار می‌گیرند. در این بخش شبیه‌سازی با ده گره در مدت زمان صد ثانیه انجام خواهد شد.

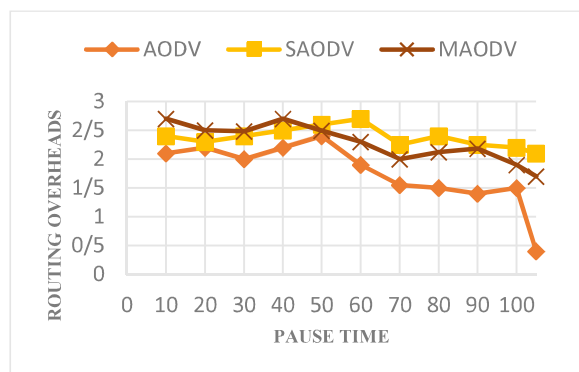
نتایج این شبیه‌سازی نشان می‌دهد که هرچه وزن درخواستی توسط مبدأ افزایش یابد تعداد RREQ پذیرفته‌شده به‌ازای آن درخواست در مقصد کاهش می‌یابد. برای مثال اگر وزن درخواستی توسط مبدأ شصت باشد، ده

¹ Packet Delivery Ratio

اطلاعات کمتری دارند، سربار مسیریابی بیشتری خواهیم داشت؛ اما با گذشت زمان اجرا و روزآمد کردن جداول route cache، میزان سربار مسیریابی بهبود می‌یابد و نزدیک به پروتکل استاندارد AODV می‌شود. عدم استفاده از روش رمزنگاری، موجب مشاهده سربار کمتری نسبت به SAODV می‌شود.



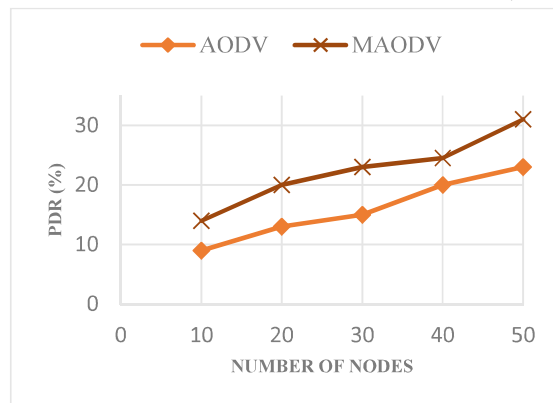
(شکل-۷): نمودار میانگین تأخیر نقطه به نقطه
(Figure-7): Average delay point to point



(شکل-۸): نمودار سربار مسیریابی بر حسب بایت
(Figure-8): Routing overhead bytes

همان‌طور که جدول (۴) نشان می‌دهد، روش مهار جغرافیایی به یک سازوکار تصدیق پخش همگانی کلی نیاز دارد که باعث افزایش حجم محاسبات و سربار خواهد شد. دستیابی به اطلاعات محل قرارگیری گره‌ها در شبکه نیز میزان سربار شبکه را افزایش می‌دهد. روش مهار زمانی نیازمند یک همگام‌سازی زمانی قوی ns است، که فراهم کردن آن در شبکه بسیار دشوار است. روش EDWA بر مبنای کوتاه‌ترین مسیر بین فرستنده و گیرنده، بنا نهاده شده است، که برای محاسبه فاصله، نیاز به GPS دارد. روش RTT زمان تأخیر برای هر گام را به عنوان نشان‌گر حمله معرفی می‌کند؛ با توجه به این که ممکن است در مواردی ازدحام بسته‌ها منجر به تأخیر شود، این روش منجر به تولید زیاد نرخ خطای مثبت خواهد بود. روش چالش/ پاسخ از الگوریتم محدودکننده فاصله، فاصله میان دو گره را بررسی می‌کند، که آیا این دو گره در حقیقت با یکدیگر همسایه هستند یا خیر. این روش نیازمند سخت‌افزار ویژه است که به یک بیت

تا سی را نمایش خواهد داد. همان‌طور که در شکل مشخص است، میزان بسته‌های رسیده در پروتکل AODV برابر ۹ الی ۲۳ درصد و در پروتکل MAODV به‌طور تقریبی برابر ۱۴ الی ۳۱ درصد است.



(شکل-۶): نمودار نرخ بسته‌های رسیده
(Figure-6): Arrival packet rate

میانگین تأخیر End-to-End

تأخیر انتهابه‌انتهای یک بسته به زمان رسیدن بسته از مبدأ تا مقصد گفته می‌شود. میانگین تأخیر انتهابه‌انتهای برابر متوسط زمان رسیدن بسته‌ها از مبدأ تا مقصد در شبکه است. در این سناریو تعداد گره‌ها پنجاه و وزن درخواستی برای تشکیل مسیر پنج تا بیست در نظر گرفته شده است. شکل (۷) الگوریتم پیشنهادی را با پروتکل AODV و SAODV مقایسه می‌کند. همان‌طور که مشاهده می‌شود، میزان تأخیر برای رسیدن بسته‌ها در پروتکل MAODV بیشتر از پروتکل AODV و کمتر از پروتکل SAODV است؛ زیرا در پروتکل استاندارد AODV مسیر، با کم‌ترین تعداد گام انتخاب می‌شود؛ و در پروتکل SAODV به‌علت فرایند رمزنگاری تأخیر قابل توجهی مشاهده می‌شود؛ درحالی که در پروتکل فرض‌شده، هر مسیر کوتاهی الزاماً امن نبوده و باید کمینه وزن مورد نیاز را تأمین کند. با اجرای مداوم پروتکل و انتخاب وزن بهینه مقدار تأخیر پروتکل MAODV به AODV استاندارد بسیار نزدیک می‌شود.

میزان سربار مسیریابی

در این بخش سربار مسیریابی پروتکل MAODV بر اساس بایت مورد ارزیابی قرار خواهد گرفت؛ و نتیجه آن با پروتکل AODV و SAODV^۱ مقایسه خواهد شد. شبیه‌سازی با پنجاه گره و وزن‌های درخواستی مختلف پنج تا بیست در نظر گرفته شده است. در ابتدای اجرای شبیه‌سازی به دلیل اینکه گره‌ها از وزن مناسب برای یافتن مقصد مورد نظر

^۱ Secure AODV

یکدیگر تبانی کرده‌اند، گره فرستنده را تحریک می‌کنند که مسیری کوتاه‌تر و سریع‌تر برای ارسال داده‌ها، نسبت به مسیر عادی وجود دارد، که درواقع این یک مسیر جعلی است. تمامی پروتکل‌هایی که از کوتاه‌ترین مسیر و یا سریع‌ترین بسته رسیده به مقصد استفاده می‌کنند، در برابر این حمله آسیب‌پذیر خواهند بود. در راه‌کار ارائه‌شده که بدون نیاز به سخت‌افزار خاص و همگام‌سازی زمان است، هر گره دارای یک وزن است، که مجموع وزن‌ها در شبکه برابر صد خواهد بود. هرگاه فرستنده قصد ارسال ترافیک به مقصد را داشته باشد، در کنار بسته RREQ در قسمت حداقل وزن، مقدار وزن درخواستی خود را وارد می‌کند که با توجه به اهمیت و ارزش بسته ارسالی می‌تواند تعیین کند، حداقل چند گره در فرایند کشف مسیر باید حضور داشته باشند. در آینده سعی خواهد شد درخواست وزن بهینه مسیر توسط مبدأ انجام گیرد. مقدار وزن درخواستی رمز خواهد شد که این مقدار فقط توسط گره مقصد قابل بازگشایی خواهد بود و گره بداندیش که در فاصله یک‌قدمی مقصد قرار دارد، نخواهد توانست وزن را تغییر دهد؛ زیرا هیچ ایده‌ای در مورد وزن پیشنهادی نخواهد داشت. همچنین در آینده راه‌کار پیشنهادی روی پروتکل‌های مسیریابی که در برابر کرم‌چاله آسیب‌پذیر هستند از جمله ARAN, DSR و DSDV اعمال شده و نتایج به‌دست‌آمده با راه‌کار پیشنهادی مقایسه خواهد شد.

7-References

۷- مراجع

- [1] A. F. S. D. Vandana, "Evaluation of Impact of wormhole Attack on AODV," *International journal of advanced Networking and Applications*, vol. 4, no. 4, pp. 1652-1656, 2013.
- [2] A. F. S. D. Vandana, "Wormhole attack Detection Using Hop Latency and Adjoining Node Analysis in MANET," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 3, 2013.
- [3] B. H. Capkun, "SECTOR: Secure Tracking of Node encounters in Multihop Wireless Networks," *First ACM Workshop on Security of Ad-hoc and Sensor Networks*, pp. 21-32, 2003.
- [4] B. Patel, "A survey on detecting wormhole attack in MANET", *Int. Journal of Engineering Research and Applications*, pp.653-656, 2014.

چالش فرستاده‌شده به‌صورت آنی پاسخ دهد. روش LiteWorp به هیچ سخت‌افزار اضافی نیاز ندارد؛ ولی این روش تنها در شبکه‌های ایستا کاربرد دارد و برای شبکه‌های متحرک کارآمد نخواهد بود. در راه‌کار پیشنهادی که بدون نیاز به موقعیت‌سنج، هماهنگ‌کننده زمانی، سخت‌افزار اضافی و بدون استفاده از تکنیک‌های رمزنگاری است، با توزیع وزن به گره‌ها و بیان حداقل وزن درخواستی برای ایجاد ترافیک، پروتکل AODV در برابر حمله کرم‌چاله مقاوم‌تر شده است. جدول (۴) راه‌کار پیشنهادی را با روش‌های دیگر مقایسه خواهد کرد.

(جدول ۴): مقایسه روش‌های مختلف مقابله با حمله کرم‌چاله

(Table-4): Comparison between Prevention of Wormhole attack

متد	نیاز به موقعیت سنج	نیاز به همگام‌سازی زمان	نیازهای خاص	کاربرد
مهار جغرافیایی	دارد	ضعیف (میلی-ثانیه)	ندارد	شناسایی و جلوگیری کرم‌چاله
مهار زمانی	ندارد	قوی (نانوثانیه)	ندارد	شناسایی و جلوگیری کرم‌چاله
EDWA	دارد	ندارد	ندارد	شناسایی کرم‌چاله
RTT	ندارد	ندارد	ندارد	جلوگیری کرم‌چاله
LiteWorp	ندارد	ندارد	ندارد	جلوگیری در شبکه‌های ایستا
چالش / پاسخ	ندارد	ندارد	سخت‌افزاری برای پاسخ آنی	جلوگیری کرم‌چاله
MAODV	ندارد	ندارد	ندارد	جلوگیری کرم‌چاله

۶- نتیجه‌گیری

حمله کرم‌چاله یکی از سخت‌ترین حملات DOS است که در لایه شبکه رخ می‌دهد. این حمله می‌تواند روی مسیریابی داده‌ها و تراکم داده‌ها تأثیرگذار باشد. در این حمله مهاجمان با ایجاد یک تونل بین گره‌های بداندیش که از قبل با

کارشناسی ارشد را در رشته امنیت اطلاعات در دانشگاه بین-الملل تهران در سال ۱۳۹۲ اخذ کرد. از ایشان یک مقاله در در هفتمین همایش بین‌المللی ارتباطات در سال ۱۳۹۲ به چاپ رسیده است.

نشانی رایانامه ایشان عبارت است از:

Fa.mohammadi1988@yahoo.com



حسین قرائی تحصیلات خود را در

مقطع کارشناسی مهندسی برق-

الکترونیک در دانشکده مهندسی برق

دانشگاه خواجه نصیرالدین طوسی در

سال ۱۳۷۷ به اتمام رساند. مقاطع

کارشناسی ارشد و دکتری مهندسی برق - الکترونیک در

دانشکده مهندسی برق دانشگاه تربیت مدرس را به ترتیب در

سال‌های ۱۳۷۹ و ۱۳۸۸ تکمیل کرد. از سال ۱۳۸۱ تاکنون

عضو هیئت علمی مرکز تحقیقات مخابرات است و زمینه‌های

پژوهشی مورد علاقه ایشان طراحی مدارات VLSI دیجیتال،

آنالوگ و سیگنال مختلط، پردازش سیگنال‌های دیجیتال،

سامانه‌های تشخیص و پیش‌گیری از نفوذ و مرکز عملیات

امنیت و اجزای آن است.

نشانی رایانامه ایشان عبارت است از:

gharaee@itrc.ac.ir

[5] J. Perrig, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 370-380, 2006.

[6] K. H. N.S Raote, "Approaches toward Mitigating Wormhole Attack in Wireless Ad-hoc Network," *International Journal of Advanced Engineering Sciences and Technologies*

[7] (*IJAEST*), vol. 2, no. 2, pp. 172-175, 2011.

[8] I. Khalil, and K. S. Bagchi, "A Lightweight Countermeasure for the wormhole Attack in Multihop Wireless Networks," In *Proceedings of DSN*, 2005.

[9] L. Wong, "DELPHI: Wormhole Detection Mechanism for adhoc Wireless Networks," in *Proceeding of International Symposium on Wireless Pervasive Computing*, 2006, pp. 6-11.

[10] L. X. H. Phuong Van Tran, "An efficient Mechanism to Detect Wormhole Attacks in Wireless ad-hoc Networks," *IEEE Consumer Communications and Networking Conference*, 2007.

[11] V. Mahajan, M. Natsu, and A. Sethi "Analysis of wormhole Intrusion Attacks in MANETS," in *IEEE Military Communications Conference*, 2008.

[12] V. G. Supriya Tayal, "A Survey of Attacks on MANET Routing Protocols," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 2, no. 6, pp. 2280-2286, 2013.

[13] W. Wang, "EDWA: End-to-End detection of wormhole attack in wireless adhoc networks," in *Computer Software and Applications Conference*, 2007. *31st Annual International, IEEE*, 2007.

[14] Y. Zhiwei, and J. Zhongyuan, "A Survey on the Evolution of Risk Evaluation for Information Systems Security," in *International Conference on Future Electrical Power and Energy System*, 2012, vol. 17, pp. 1288-1294.



فرید محمدی تحصیلات خود را در

مقطع کارشناسی مهندسی کامپیوتر در

دانشکده مهندسی برق کامپیوتر

دانشگاه زنجان در سال ۱۳۹۰ در

دانشگاه زنجان و در رشته فناوری اطلاعات و مدرک

فصلنامه



سال ۱۳۹۵ شماره ۴ پیاپی ۳۰

۱۲۰