دوفصلنامه محاسبات و سامانه های توزیع شده
سال سوم، شماره اول، شماره پیاپی ۵، صفحه ۱۱۹ تا ۱۳۰، سال ۱۳۹۹

ارزیابی و بررسی انواع حملات در مسیریابی شبکه‌های موردی سیار و ارائه روش جدید برای شناسایی و جلوگیری از حملات سوراخ کرم در مسیریابی امن مبتنی بر پروتکل SPR

فتانه طاهری آشتیانی*
دانشکده فنی و مهندسی، گروه کامپیوتر، دانشگاه آزاد اسلامی واحد بناب، بناب، ایران.

چکیده

شبکه‌های موردی سیار مجموعه مستقلی از گره‌های متحرک هستند که از طریق ارتباطات بی‌سیم با همدیگر در ارتباط هستند و برای اتفاقات غیر قابل پیش‌بینی اتصالات راه‌حل مناسبی است همچنین این شبکه‌ها بدون زیرساخت مشخصی هستند که به صورت متحرک و خودمختار عمل کرده و از طریق امواج رادیویی با همدیگر در ارتباط هستند. بدلیل متغیر بودن تعداد گره‌ها در شبکه ارتباطات بین آنها مدام در حال تغییر هستند بنابراین امنیت این شبکه‌ها از اهمیت زیادی برخوردار هستند. ما در این مقاله ضمن مطالعه انواع مختلف پروتکل‌های مسیریابی، مشکلات امنیتی در مسیریابی شبکه‌های موردی سیار و انواع مختلف پروتکل‌های مسیریابی امن را به همراه مزایا و معایب آن را بررسی کرده و با تغییراتی در پروتکل SPR مشکل حملات سوراخ کرم را با استفاده از ترکیب جدیدی از تکنیک قلاده‌های بسته حل می‌کنیم. به این صورت که با افزودن تکنیک دیگری به عنوان تکنیک قلاده‌های وضعیت به پروتکل SPR که مبتنی بر وضعیت هر بسته بر اساس ویژگی‌های امنیتی و اطلاعات رمزنگاری است می‌توان بسته‌های مبادله شده در مسیر را پیگیری و کنترل کرد. همچنین برای مدیریت کلید و افزایش امنیت روش پیشنهادی از الگوریتم دیفی-هلمن استفاده کردیم و در نهایت برای پیاده‌سازی الگوریتم پیشنهادی از نرم افزار متلب استفاده کرده‌ایم.

کلمات کلیدی: شبکه‌های موردی سیار، مسیریابی امن، حملات امنیتی، مدیریت کلید، پروتکل SPR.

Evaluate the Types of Attacks in the Routing of Mobile Networks and Provide a New Way to Detect and Prevent Wormhole Attacks in Secure Routing base in SPR Protocol

Fattaneh Taheri Ashtiyani*

Islamic Azad University, Bonab Branch, Bonab, Iran.

Abstract

Mobile case networks are an independent set of mobile nodes that communicate with each other via wireless communications and are a good solution for unpredictable events. These networks also have no specific infrastructure that operates mobile and autonomously and through radio waves which they are in touch with each other. Due to the variable number of nodes in the communication network between them are constantly changing, so the security of these networks is very important. In this article, we study different types of routing protocols, security problems in routing mobile case networks and different types of secure routing protocols along with its advantages and disadvantages, and with changes in SPR protocol, the problem of wormhole attacks using a new combination. We solve by the closed collars technique. In this way, by adding another technique as the status collar technique to the SPR protocol, which is based on the status of each packet based on security features and encryption information, packets exchanged along the way can be tracked and controlled. We also used the Diffie-Hellman algorithm to manage the key and increase the security of the proposed method, and finally we used MATLAB software to implement the proposed algorithm.

تاریخچه مقاله:

تاریخ ارسال: ۱۳۹۹/۰۴/۰۱
تاریخ اصلاحات: ۱۳۹۹/۰۵/۰۲
تاریخ پذیرش: ۱۳۹۹/۰۶/۱۵
تاریخ انتشار: ۱۳۹۹/۰۷/۲۰

Keywords:

Adhoc Mobile Networks
Secure Routing
Security Attacks
Key Management
SPR protocol

*ایمیل نویسنده مسئول:
F.taheri.ashtiyani@gmail.com

۱- مقدمه

شبکه، تعدادی از رایانه‌ها و دستگاه‌هایی می‌باشد که توسط کانال‌های ارتباطی به هم متصل شده‌اند. این کانال‌ها می‌توانند سیم، فیبرنوری و یا بی‌سیم باشند. و سبب سهولت ارتباطات میان کاربران شده و اجازه می‌دهد کاربران منابع خود را به اشتراک بگذارند.

شبکه‌های موردی، مجموعه مستقلی از گره‌ها می‌باشد که زیرساخت مشخصی ندارند. این شبکه‌ها به دو بخش شبکه‌های حسگر بی‌سیم و شبکه‌های موردی سیار تقسیم شده است. علت نامگذاری شبکه موردی سیار، متحرک و خودمختار بودن گره‌ها است. در جهان ما، شبکه‌ها، دائما در حال تغییر می‌باشند و پیوندهای خودشان را برای اتصال گره‌های جدید تغییر می‌دهند[۱]. این شبکه‌ها با وجود مشکلات امنیتی کاربردهای زیادی دارند. همچنین در زمینه‌هایی که زیرساخت‌های ارتباطی وجود ندارد یا زیرساخت‌های موجود بسیار گران‌قیمت بوده، کاربران سیار بی‌سیم می‌توانند از طریق شبکه موردی سیار با یکدیگر ارتباط برقرار کنند. هر گره جهت برقراری ارتباط، مجهز به یک فرستنده و یک گیرنده می‌باشد که از طریق امواج رادیویی به دو طریق با بقیه گره‌ها ارتباط برقرار می‌کند: روش نظیر به نظیر و روش همه‌پخشی. در این شبکه، گره‌ها هیچ دانشی نسبت به اتصالات شبکه‌ای که در آن قرار دارند ندارند زیرا ساختار این شبکه پویا می‌باشد. هر گره برای ارسال اطلاعات به گره دیگر باید عمل کشف مسیر و عمل نگهداری مسیر را انجام دهد[۲]. این نوع شبکه بدلیل پویایی، با پیچیدگی‌ها و محدودیت‌های طراحی مثل عدم داشتن زیر ساخت ارتباطی مشخص، تغییر با گذشت زمان، محدودیت انرژی، محدودیت پهنای باند و کیفیت و امنیت و همکاری گره‌ها مواجه است. با توجه به این مسائل، بهینه‌سازی پهنای باند، کنترل قدرت و انرژی و بهبود کیفیت انتقال از اولویت‌های این نوع شبکه‌ها است. در این شبکه‌ها گره‌ها بدلیل وجود محدودیت‌هایی در فرستنده و گیرنده‌های خود نمی‌توانند با تمام گره‌ها ارتباط مستقیم برقرار کنند. بنابراین داده‌ها از طریق بقیه گره‌ها که نقش مسیریاب را ایفا می کنند منتقل می‌شوند. با این حال متحرک بودن گره‌ها باعث شده شبکه مدام در حال تغییر بوده و مسیرهای مختلفی بین آنها به وجود آید[۲و۳]. این شبکه‌ها دارای ویژگی‌های زیر است:

۱- ترمینال مستقل: در MANET، هر ترمینال یک گره مستقل است که در زمان پردازش به عنوان هاست و روتر عمل می‌کند و گره‌های سیار می‌توانند عملیات SWICHING انجام دهند.

۲- عملیات توزیعی: از آن‌جایی‌که هیچ ساختاری برای عملیات کنترل مرکزی وجود ندارد، کنترل و مدیریت شبکه بین ترمینال‌ها به صورت توزیع‌شده انجام می‌شود. گره‌های درگیر در آن با همدیگر کار می‌کنند و هر گره به عنوان یک تقویت‌کننده عمل می‌کند.

۳- مسیریابی چندگانه : این شبکه‌ها برای مسیریابی می‌توانند بر اساس خصوصیات متفاوت لایه پیوند و پروتکل‌های مسیریابی به صورت تک‌گامی‌و چندگامی عمل کنند. موقع تحویل دادن بسته‌ها از یک منبع به مقصد خارج از دامنه انتقالات بی‌سیم مستقیم، بسته باید توسط یک یا تعداد بیشتری گره میانی ارسال شود.

۴- توپولوژی شبکه‌ای پویا: بدلیل اینکه گره‌ها سیار هستند، توپولوژی شبکه ممکن است به سرعت و به صورت غیر قابل پیش‌بینی تغییر کند. فلذا ترافیک و شرایط انتشار و همچنین الگوهای حرکت گره‌های شبکه سیار باید سازگار باشد.

۵-تعدد ظرفیت اتصالاتی : طبیعتا نرخ بیت خطای بالای ارتباط بی‌سیم ممکن است در یک شبکه موردی سیار عمیق‌تر باشد. یک مسیر انتها به انتها می‌تواند توسط چندین جلسه مشترک شود. کانالی که ترمینال‌ها را متصل می‌کند هدفی برای نویز، ناپدید شدن و تداخل می‌باشد و پهنای باند کمتری از یک شبکه سیمی دارد. در تعدادی از طرح‌ها، مسیر بین هرجفت از کاربران می‌تواند اتصالات بی‌سیم متعددی را بپیماید.

۶- ترمینال‌های سبک وزن : در بعضی حالت‌ها، گره های MANET گره‌هایی با ظرفیت پردازش کمتر، اندازه حافظه کوچکتر و ذخیره‌سازی نیروی کمتری هستند این گره‌ها نیاز به الگوریتم‌های بهینه شده و مکانیسم‌هایی که عملیات محاسباتی و ارتباطی را بهینه می‌کنند دارند.

۲- مسیریابی

مسیریابی از چالش‌های مهم در شبکه‌های موردی سیار است که به دلیل پویا بودن محیط، نیاز به روش‌های مسیریابی سازگار با این شرایط می‌باشد. تعیین مسیر در این نوع شبکه‌ها به دلیل این که هر گره می‌تواند حرکت تصادفی داشته باشد و در بعضی مواقع از شبکه خارج شود، مشکل می‌باشد. به عبارت دیگر ممکن است مسیر بهینه‌ای وجود داشته باشد که چند ثانیه بعد بهینه نباشد و یا اصلا این مسیر از بین رفته باشد. در این شبکه‌ها، گره‌ها، اطلاعاتی در مورد نحوه ارتباطات و نوع اتصالات شبکه‌ای که در آن هستند، ندارند. به همین دلیل برای برقراری ارتباط با سایر گره‌ها و فرستادن اطلاعات به آنها باید عمل کشف مسیر انجام

دهند. بنابراین در شبکه‌های موردی سیار یک گره جدید، حضور خود را در سراسر شبکه همه‌پخشی می‌کند و برای دریافت پاسخ از طرف آنها منتظر می‌ماند. به این ترتیب این گره از حضور گره‌های همسایه‌اش مطلع می‌شود و راه رسیدن به آنها را می‌آموزد. به همین ترتیب دست‌کم یک راه برای رسیدن به آنها را کشف می‌کند[۴].

۲-۱- تقسیم‌بندی پروتکل‌های مسیریابی

شبکه موردی سیار به صورت یک فضای دو بعدی ارائه می‌شود. هر گره دارای یک مختصات مکانی است و در برد رادیویی خود از طریق پیوندهای بی‌سیم با همسایگانش ارتباط دارد. این شبکه یک گراف همبند است که برای رسیدن از یک گره به گره دیگر از چندین گره واسط استفاده می‌شود. ارتباط بین گره‌ها با استفاده از روش‌های مختلف مسیریابی انجام می‌شود که در این روش‌ها تعدادی معیار از قبیل کاهش تاخیر و افزایش نرخ تحویل بسته مطرح می‌باشد[۵]. پروتکل‌های مسیریابی به سه زیر شاخه اصلی مبتنی بر جدول، مبتنی بر تقاضا و ترکیبی تقسیم شده است که هر کدام به دو زیر شاخه یکنواخت و غیر یکنواخت تقسیم می‌شود. هر یک از این زیر شاخه‌ها نیز به زیر بخش‌های مسطح، سلسله‌مراتبی و جغرافیایی تقسیم‌بندی شده است.

در روش‌های مسیریابی مبتنی بر جدول، هر گره به طور مداوم برای شناسایی مقاصد، اطلاعات به روزرسانی شده را نگهداری می‌کند. این نوع از پروتکل‌ها اطلاعات مسیر را در یک یا چند جدول نگهداری می‌کند و مسیر را که به صورت دوره‌ای در طول شبکه به علت تغییر توپولوژی عوض می‌شوند را نگه می‌دارد. هر گره اطلاعات تمام مسیرها را نگه می‌دارد، بدون در نظر گرفتن این‌که این مسیرها مورد نیاز است یا خیر. بنابراین سربار کنترلی به طور قابل توجهی زیاد است. به ویژه در شبکه‌های بزرگ یا شبکه‌هایی که در آن گره‌ها تحرک بسیار دارند[۶]. در روش‌های مسیریابی مبتنی بر تقاضا، مسیرها زمانی کشف می‌شوند که واقعا مورد نیاز باشند. این پروتکل‌ها شامل فرآیند کشف مسیر و نگهداری مسیر می‌باشند. فرآیند کشف مسیر زمانی آغاز می‌شود که یک گره می‌خواهد داده را به مقصد خاصی بفرستد. کشف مسیر معمولا به وسیله روش سیل‌آسا و در قالب درخواست مسیر در شبکه رخ می‌دهد. یعنی زمانی که بسته درخواست مسیر در شبکه پخش شد، فرآیند کشف مسیر شروع می‌شود. سپس گره مقصد یافت شده یک پاسخ مسیر به گره مبدا به وسیله گره‌های میانی می‌فرستد. مرحله نگهداری مسیر، در این مرحله مسیرهای ناقص و شکست خورده حذف می‌شود و دوباره فاز کشف مسیر به خاطر تغییر توپولوژی انجام می‌گیرد.

روش‌های مسیریابی ترکیبی: متشکل از مزایای هر دو روش مبتنی بر جدول و مبتنی بر تقاضا است. این پروتکل‌ها روش مسیریابی بردار فاصله را برای پیدا کردن کوتاه‌ترین مسیر به کار می‌گیرند و اطلاعات مسیریابی را تنها وقتی تغییری در توپولوژی شبکه وجود دارد را گزارش می‌دهند. پروتکل‌های ترکیبی می توانند یک تعادل یا توازن بهتر بین هزینه ثابت ارتباطات و تاخیر ایجاد کنند.

در مسیریابی مسطح، هر گره بصورت مستقیم با سایر گره‌ها در ارتباط است. مشکل اصلی این روش این است که برای بروزرسانی اطلاعات مسیر اجازه مقایسه کردن وجود ندارد

در مسیریابی سلسه‌مراتبی گره‌ها به خوشه‌های مختلف تقسیم‌بندی می‌شوند. و از هرخوشه یک گره به عنوان سرخوشه انتخاب می‌شود و بقیه گره‌ها به عنوان گره‌های عضو آن خوشه هستند. یک گره ممکن است سرخوشه نباشد اما همسایه بیش از یک سرخوشه باشد که به آن گره دروازه می‌گویند. بسته‌ها بین سرخوشه‌ها به واسطه این دروازه‌ها تعیین مسیر می‌شوند. هر کدام از سرخوشه‌ها اطلاعاتی را راجع به دیگر گره‌های موجود در آن خوشه نگهداری می‌کنند و در بازه‌های زمانی مشخصی این اطلاعات بین سرخوشه‌های موجود در شبکه مبادله می‌شوند[۷و۸].

۲-۲- پروتکل‌های مسیریابی

از انواع الگوریتم‌های مسیریابی در شبکه‌های موردی سیار، نحوه عملکرد الگوریتم‌های DSR،AODV، DSDV و ZRP و مزایا و معایب هر کدام در جدول ۱ نشان داده شده است.

(جدول-۱): نحوه عملکرد و مزایا و معایب انواع مختلف الگوریتم‌های مسیریابی در شبکه‌های موردی سیار

معایب	مزایا	نحوه عملکرد	نام الگوریتم
بار شبکه بالا می‌باشد - پهنای باند زیادی را مصرف می‌کند - افزایش حجم سرآیندها با افزایش فاصله گره مبدا و مقصد زیاد می‌شود.	مسیریابی ساده و موثر است و قطعا دارای جواب است	از دو فاز کشف مسیر و نگهداری مسیر تشکیل شده است. گره مبدا در ابتدا مسیرهای موجود به گره مقصد را بررسی می‌کند، در صورت عدم وجود مسیر فاز کشف مسیر آغاز می‌شود. گره‌های شبکه موردی اطلاعات تمامی مسیرهایی را که می‌دانند را در حافظه خود نگه می‌دارند. در طول فرآیند کشف مسیر گره می‌تواند به صورت عادی با سایر گره‌ها در ارتباط باشد. تمامی‌مسیرهای ذخیره شده دارای تاریخ انقضا می‌باشند که بعد از اتمام آن از حافظه پاک می‌شوند. اگر یک گره تشخیص دهد که انتقال شکست خورده است این مسیر را از حافظه پاک می‌کند. به همین ترتیب اگر یک گره میانی تشخیص دهد که انتقال به گره بعدی را نمی‌تواند انجام دهد، یک پیام خطا به منبع می‌فرستد که آن مسیر را از فهرست مسیرهای شناخته شده پاک کند.	**DSR** (مبتنی بر تقاضا)
افزایش افزونگی در بسته‌های درخواست و پاسخ و بسته خطا -	حداقل سربار کنترلی - حداقل سربار پردازشی - قابلیت مسیریابی پویا و چندگامی – نگهداری	مسیرها فقط زمانی که مورد نیاز باشند کشف می‌شوند و تنها در طول مدتی که مورد استفاده قرار می‌گیرند نگهداری می‌شوند. این پروتکل نیز از دو فاز کشف مسیر و نگهداری مسیر تشکیل شده است. فرآیند کشف مسیر به صورت flooding انجام می شود. در این الگوریتم برای تصحیح مسیر از پیش ساخته از یک شماره توالی در بسته‌های	**AODV** (مبتنی بر تقاضا)
	پویای توپولوژی	درخواست مسیر استفاده می‌شود. همچنین این الگوریتم پیام دیگری به نام (RERR) دارد که در صورت خطای مسیریابی ارسال می‌شود.	
پارامترهایی مثل زمان و تعداد به روزرسانی اطلاعات مورد نیاز می‌باشد.	اجتناب از به وجود آمدن حلقه‌های مسیریابی در شبکه‌های شامل مسیریاب‌های متحرک است.	بر مبنای الگوریتم کلاسیک بلمن فورد بنا شده است. در این حالت هر گره لیستی از تمام مقاصد و نیز تعداد گام‌ها تا هر مقصد را تهیه می‌کند. هر مدخل لیست با یک عدد شماره‌گذاری شده است	**DSDV** (مبتنی بر جدول)
برای مناطق کوچک با حرکت سریع گره‌ها و جایی که تقاضای مسیر بالاست، مناسب نیست	برای شبکه‌های متحرک با چندین جابه‌جایی در مدت زمان طولانی استفاده می‌شود - افزایش کارآیی و کیفیت کشف مسیر با استفاده از مکانیزم سئوال/ جواب	مساحت کل شبکه به مناطق مختلف تقسیم می‌شود. شعاع و اندازه منطقه به فاصله بستگی ندارد، بلکه به تعداد جهش‌ها بستگی دارد. به منظور شناسایی گره‌های همسایه،ZRP از پروتکل MAC استفاده می‌کند و برای شناسایی گره‌ها در محدوده منطقه از پروتکل کشف مسیر استفاده می‌کند.	**ZRP** (ترکیبی)

۳- مشکلات امنیتی در مسیریابی شبکه‌های موردی سیار

مسائل امنیتی در شبکه‌های موردی سیار از اهمیت خاصی برخوردار است به‌خاطر اینکه گره‌ها در عمل مسیریابی شرکت می‌کنند، نفوذ یک گره متخاصم به شبکه می‌تواند به نابودی کل شبکه بیانجامد. همچنین به‌دلیل اینکه این شبکه‌ها اغلب بدون هماهنگی قبلی ایجاد می‌شوند و برای زمان کوتاهی نیاز به برقراری

امنیت دارند تصور یک واحد توزیع کلید و یا زیرساخت کلید عمومی و غیره مشکل است. از موارد امنیتی در شبکه‌های موردی سیار می‌توان به مدیریت کلید، مسیریابی امن، تصدیق اصالت، جلوگیری از حملات ممانعت از سرویس، تشخیص سوء رفتار و تشخیص نفوذ اشاره کرد. از جمله مواردی که منجر به ناامن شدن این شبکه‌ها شده است می‌توان به کانال رادیویی از نوع پخش همگانی به اشتراک گذارده شده، محیط عملیاتی ناامن، نبود شناسایی متمرکز، دسترسی محدود به منابع و مشکلات و آسیب پذیری‌های فیزیکی اشاره کرد. زمانی که در مورد امنیت شبکه بحث می‌شود معمولا به عناوین زیر توجه ویژه می‌شود:

قابلیت دسترسی : بدین معنی که شبکه در طول زمان و حتی در مواردی که دچار حمله شده بتواند به عمل خود ادامه بدهد.

محرمانگی: اطمینان از اینکه اطلاعات مشخص و معینی در اختیار کاربران خاصی قرار نگیرد.

احراز هویت: توانایی یک گره در شناسایی و تشخیص گره‌هایی که با وی در ارتباط است.

جامعیت: تضمین اینکه یک پیام پس از منتشر شدن تخریب نشده و از بین نمی رود.

انکارپذیری: ایستگاه فرستنده پیام نتواند ارسال خود را انکار کند.

یک شبکه ad hoc به دلیل نداشتن ساختار ثابت و مشخص و نیز ارتباطات پویا بین nodeها نیازمند ملاحظات امنیتی بیشتری نسبت به انواع دیگر شبکه است. حملات در شبکه‌های موردی سیار را می‌توان از دیدگاه‌های مختلف دسته‌بندی کرد. در دسته‌بندی اول، حملات می‌تواند به صورت حملات خارجی و حملات داخلی باشد. حملات داخلی حملاتی هستند که توسط گره‌های مجاز داخل شبکه انجام می‌شوند و معمولا جلوگیری از آنها کاری مشکل است. حملات خارجی حملاتی هستند که توسط یک یا چند گره از خارج از شبکه انجام می‌شوند و بیشتر اقدامات امنیتی در مقابل اینگونه حملات اعمال می‌شوند. دسته‌بندی دوم بر حسب فعال و یا غیرفعال بودن حمله است. حملات غیرفعال حملاتی هستند که در آنها حمله کننده تنها به اطلاعات روی کانال گوش داده و آنها را استراق سمع می‌کند ولی در حملات فعال حمله‌کننده می‌تواند به اطلاعات روی کانال دسترسی داشته باشد و تغییراتی را روی آن اعمال کند. دسته‌بندی بعدی از جهت لایه‌های شبکه‌ای مورد حمله می‌باشد. یعنی حملات می‌توانند به روی لایه‌های فیزیکی، شبکه و یا کاربرد صورت پذیرد[۹]. مشکلات امنیتی در مسیریابی شبکه‌های موردی سیار به سه دسته عمده تغییر، جعل هویت و جعل تقسیم می‌شود.

۳-۱- حملات مبتنی بر تغییر

ممکن است یک گره متخاصم بخواهد به روش‌های مختلف با تغییر دادن فیلدهای یک بسته مسیریابی، باعث پیدایش یک مسیر اشتباه شود. این روش‌ها عبارتند از:

۳-۱-۱- تغییر مسیر به وسیله تغییر شماره توالی

برخی از الگوریتم‌های مسیریابی مانند AODV برای تصحیح مسیر از یک شماره توالی در پیام‌های درخواست مسیر استفاده می‌کنند. در این روش گره متخاصم با نفوذ به داخل شبکه و با دریافت بسته درخواست مسیر از یک گره و تولید یک بسته پاسخ مسیر با شماره توالی بزرگ‌تر می‌تواند مسیر را به نفع خودش تغییر دهد.

۳-۱-۲- تغییر مسیر به وسیله تغییر تعداد گام

هر کدام از الگوریتم‌های مسیریابی مانندAODV از روش‌های مختلفی برای پیدا کردن کوتاه‌ترین مسیر از بین مسیرهای پیدا شده استفاده می‌کنند. که یکی از این روش‌ها استفاده از شمارنده گام است به این صورت که هر کدام از گره‌های میانی که بسته درخواست مسیر را به گره بعدی ارسال می‌کند یک واحد به شمارنده گام اضافه می‌کند. در نهایت، از روی کمترین مقدار شمارنده گام می‌توان به کوتاه‌ترین مسیر پی برد. حال اگر یک گره متخاصم در شبکه وجود داشته باشد می‌تواند با صفر قرار دادن مقدار شمارنده گام یک بسته درخواست مسیر، باعث شود تا با احتمال بسیار زیاد مسیر نهایی از خود آن گره عبور کند و یا با بینهایت کردن مقدار آن، خود را از قرار گرفتن در مسیر کنار بکشد.

۳-۱-۳- ممانعت از سرویس به وسیله تغییر مسیر مبدأ

بعضی از الگوریتم‌ها مانند DSR، مسیر پیدا شده را در سرآیند بسته‌های ارسالی خود قرار می‌دهند. در این صورت گره متخاصم می‌تواند با تغییر مسیر داخل سرآیند بسته باعث شود تا آن بسته به مقصد درست خود دست پیدا نکند.

۳-۲- حملات مبتنی بر جعل هویت

در این نوع حمله یک گره می‌تواند با قرار دادن آدرس یک گره دیگر در بسته ارسالی، خود را به جای گره دیگر معرفی کرده و باعث بروز یک‌سری مشکلاتی از جمله مشکل ایجاد حلقه کند.

در الگوریتم AODV، گره متخاصم M با نزدیک شدن به گره A و با قرار دادن آدرس فیزیکی گره B در بسته ارسالی، خود را بجای آن گره معرفی کرده و بسته پاسخ مسیر را با شمارنده گام برابر با صفر به گره A ارسال می‌کند و گره A بر اساس آن مسیر را تغییر می‌دهد[۸].

۴- حملات مشهور در شبکه‌های موردی سیار

۴-۱- حمله عجله‌ایی

این نوع حمله که به هک پنهان نیز معروف است هدفش از کار انداختن شبکه است. به این صورت که وقتی گره‌های منبع بسته‌های کشف مسیر را برای پیدا کردن مقصد در شبکه پخش می‌کنند هر گره میانی فقط اولین بسته غیرتکراری را پردازش می‌کند و بسته‌های ورودی تکراری را رد می‌کنند. یک مهاجم عجله‌ایی با سو استفاده از مکانیزم مهار گره‌های تکراری بوسیله ارسال سریع بسته‌های کشف مسیر سعی می‌کند به گره‌های ارسال دسترسی پیدا کنند. بسیاری از پروتکل‌های تقاضامحور از این روش مهار بسته‌های تکراری استفاده می‌کنند که در مقابل حملات عجله‌ایی آسیب پذیر می باشند[۹].

۴-۲- حمله سوراخ کرم

این نوع حملات خاص شبکه‌های موردی است. در این حمله، دو گره متخاصم، یک اتصال کوتاه را با همکاری یکدیگر در توپولوژی شبکه ایجاد می‌کنند. سپس درخواست مسیریابی که از جانب گره‌ها، به یکی از این گره‌های متخاصم می‌رسد. این گره متخاصم، درخواست را از طریق یک شبکه خصوصی برای گره دوم ارسال می‌کند. حال اگر این دو گره مقدار شمارنده گام درخواست مسیر را عوض نکنند، مقداری زیادی از مسیر توسط این شبکه خصوصی بدون افزایش مقدار شمارنده گام طی شده است. بدین ترتیب ممکن است بسته به جای ده‌ها شمارنده تنها با دو شمارنده به مقصد برسد و مطمئناً این مسیر به عنوان کوتاه‌ترین مسیر انتخاب می شود. راه‌حل این مشکل استفاده از تکنیک قلاده‌های بسته است[۱۰].

۴-۳- حمله هجوم

در این نوع حمله فرض کنید در طی یک عملیات کشف مسیر، بسته‌های دریافتی از سوی مهاجمین، اولین بسته دریافتی توسط گره‌های همسایه گره مقصد باشد. در این صورت تمامی درخواست‌های دیگر که بعداً به دست این گره‌ها می‌رسد نادیده گرفته خواهد شد و تنها بسته درخواست مسیری که مهاجم فرستاده است را به مقصد ارسال می‌نماید. همین امر باعث می‌شود تا مسیرهای به دست آمده به گونه‌ای باشد که حتماً در آن مسیرها یک گره مهاجم وجود داشته باشد. بنابراین اگر مهاجم درخواست خود را سریعتر از گره مجاز ارسال نماید، به طور حتم بسته او دریافت خواهد شد و مورد پذیرش قرار خواهد گرفت و مهاجم می‌تواند با احتمال زیادی مسیری را بنا کند که خود او در آن مسیر وجود دارد[۱۱].

۴-۴- حمله سیاه‌چاله

در این نوع حمله گره متخاصم با نفوذ به شبکه و قرار گرفتن واقع در کوتاهترین مسیر به سمت مقصد و با دریافت بسته‌های ارسالی از این مسیر، آنها را حذف کرده و باعث کاهش شدید نرخ تحویل بسته می‌شود. در الگوریتم AODV گره متخاصم با دریافت بسته درخواست مسیر از یک گره، بدون بررسی آن یک بسته پاسخ مطابق میل خودش ارسال می‌کند که باعث کوتاه شدن ارسال بسته‌های پاسخ نسبت به گره‌های دیگر می‌شود که در آن بیشترین شماره ترتیب و کمترین شمارنده گام وجود دارد که باعث انتخاب این مسیر توسط گره ارسال کننده بسته درخواست مسیر شده و نهایتا بسته‌های ارسالی توسط گره متخاصم از بین می‌رود[۱۲].

۴-۵- حمله حفره خاکستری

این حمله نوع خاصی از حمله سیاه‌چاله است که گره مهاجم پس از جلب بسته‌های یک گره به سمت خود, گروهی از آنها را به صورت انتخابی دور می ریزد و بقیه را ارسال می‌کند. در این حمله گره مهاجم یکی از گره‌های میانی یا یک گره با فاصله دورتر از گره مبدا است و در جریان مسیریابی شرکت می‌کند و بسته RREQ را برای گره مقصد می‌فرستد و بسته RREP را نیز از گره مقصد برای گره مبدا هدایت می‌کند اما در جریان تبادل اطلاعات سعی می‌کند فقط قسمتی از اطلاعات را به گره مقصد هدایت کند و باقی اطلاعات را پیش خود نگه می‌دارد حمله حفره خاکستری خطرات کمتری برای شبکه دارد اما فرآیند شناسایی گره مهاجم در آن سخت‌تر از حمله سیاه‌چاله است. در حقیقت گره مهاجم در حمله حفره خاکستری یک نوع جاسوس است و طوری رفتار می‌کند که دو گره مبدا و مقصد مشکوک نشوند و اطلاعات لازم میان آنها تبادل شود[۱۳].

۴-۶- حمله همسایه

گره‌های میانی پس از دریافت یک بسته، سوابق و مشخصات خود را به بسته اضافه کرده و آن را به گره بعدی ارسال می‌کنند. یک گره متخاصم بدون اینکه مشخصات خود را به بسته اضافه کند آن را به گره بعدی ارسال می‌کند در نتیجه موقع

برگشت گره تصور می‌کند که داده را می‌خواهد به همسایه خود ارسال کند که از محدوده آن خارج است در نتیجه باعث مختل شدن عملیات مسیریابی می‌شود[۱۴].

۴-۷- حمله پخش مکرر

این روش یک نوع از حمله به شبکه است که در آن داده‌های معتبر بصورت خرابکارانه یا متقلبانه با تاخیر به مقصد می‌رسند یا تکرار می‌شوند گره متخاصم حمله پخش مکرر را به داخل ترافیک مسیریابی شبکه تزریق می‌کند این حمله معمولا به مسیرهای تازه احداث صورت می‌پذیرد[۱۲].

۴-۸- حمله انسداد

گره یا گره‌های متخاصم در این حمله، شبکه را با بسته‌های نامربوط و غیرمعتبر یا سیگنال‌های رادیویی بمباران می‌کنند در نتیجه اگر بقیه گره‌های شبکه که در محدوده آلودگی رسانه انتقال قرار دارند قصد کشف مسیر یا ارسال بسته را داشته باشند با تصادم‌های متعدد مواجه می‌شوند و به راحتی قادر به ارسال پیغام نخواهند بود بنابراین این حمله را می‌توان در زمره حملات براندازی سرویس دسته‌بندی کرد این حمله در لایه‌های فیزیکی و پیوند داده انجام می‌شود[۱۴و۱۵].

۵- مسیریابی امن شبکه‌های موردی سیار

مسیریابی خوب در شبکه موردی سیار می‌بایستی منجر به تشخیص یک مسیر درست شده و بتوان از آن نگهداری کرد به طوری‌که گره‌های متخاصم نتوانند از ساخت و نگهداری صحیح مسیر جلوگیری کنند. در جدول شماره (۲) انواع پروتکل‌های امنیتی در مسیریابی شبکه‌های موردی سیار بیان شده است.

(جدول-۲): انواع پروتکل‌های امنیتی در مسیریابی شبکه‌های موردی سیار

پروتکل	نحوه عملکرد	مزایا	معایب
ARAN	برای ایجاد امنیت در پروتکل AODV استفاده می‌شود- بر اساس رمزنگاری با کلید عمومی و همچنین استفاده از گواهی دیجیتالی بنا نهاده شده است- شامل فرایند صدور گواهی است و تصدیق اصالت انتها به انتها را تضمین می‌کند- در این	مقاوم در برابر حملات جعل هویت	عدم مقاومت در برابر حمله سیاه چاله- مصرف زیاد انرژی و پردازنده- پاسخ یکسان به هر رفتار غیر قابل پیش‌بینی
SRP	بر پایه الگوریتم مسیریابی DSR بنا نهاده شده و به سرایند آن یک بخش شش کلمه‌ای اضافه شده که علاوه بر شناسه و شماره توالی، کد تصدیق اصالت پیام نیز قرار دارد. در این پروتکل یک وابستگی امنیتی بین گره مبدا و مقصد در نظر گرفته می‌شود و بر اساس آن، گره مبدا پاسخ‌های دریافتی برای این عملیات را تشخیص داده و در صورت	تضمین جامعیت و تصدیق اصالت پیام	عدم وجود راه‌کاری برای پیگیری بسته‌ها در شبکه و طول مسیر پیموده شده توسط آنها – احتمال بروز اشکال توسط گره‌های متخاصم در درک توپولوژی چه از طرف گره متخاصم و چه گره دوستی که درست عمل نمی‌کند
Ariadne	برای ایمن سازی پروتکل DSR استفاده می‌شود- به جای استفاده از کلید عمومی از رمزنگاری متقارن و برای تصدیق اصالت پیام‌ها از کد تصدیق اصالت پیام استفاده می‌شود که توسط یک تابع درهم سازی ساخته می‌شود.	ایمن در مقابل حملات سوراخ کرم	نیاز به تبادل کلید بین گره‌های شبکه برای رمزنگاری قبل از شروع پروتکل
SAODV	برای ایمن سازی پروتکل AODV بنا نهاده شده و از توابع درهم ساز استفاده می‌شود- از شمارش گام برای اندازه‌گیری تعداد گام‌های طی شده توسط بسته استفاده می‌شود اگر شمارش گام از یک مقدار max count بیشتر شود بسته نادیده گرفته می‌شود	مقاوم در برابر حملات سیاه‌چاله	تعیین مقدار برای متغیر max count که یک بسته می‌تواند طی کند
	روش یک پیام کشف مسیر توسط مبدا انتشار می‌یابد که توسط گره مقصد به حالت unicast پاسخ داده می‌شود به‌طوری که پیام‌های مسیریابی، هم در هر گام در طول مسیر مبدا به مقصد و هم در مسیر برگشت تصدیق اصالت می‌شوند		

شبکه		تشخیص نادرست بودن، آنها را نادیده بگیرد.	
مشکل در حمله هجوم- مشکل در توافق کلید	عدم وجود حلقه در مسیر با اضافه کردن شماره توالی به هر کدام از عناصر جدول مسیریابی	این پروتکل بر اساس پروتکل DSDV بنا نهاده شده که در آن هر گره دارای یک جدول مسیریابی است که شامل لیستی از تمام مقاصد ممکن در شبکه است. برای بروز کردن جدول مسیریابی، هر گره در بازه‌های زمانی مشخصی یک پیام درخواست مسیر را به تمام همسایگان خود ارسال میکند تا مسیرهای جدید را در جدول خود قرار دهد- برای ایجاد امنیت از توابع درهم ساز یکطرفه بجای توابع رمزنگاری غیر متقارن استفاده می‌کند	**SEAD**
عدم دریافت بسته‌های ارسالی از سوی همسایه‌های چندگامی	حفاظت داده‌ها از گره‌هایی که تصدیق اصالت نشده اند	برای تعیین موقعیت فعلی گره‌ها از GPS استفاده می‌کند-هر گره تنها می‌تواند بسته‌های ارسالی از سوی همسایه‌های تک گام خود را دریافت کند - در صورت عدم وجود هیچ اطلاعی از موقعیت گره‌ها از الگوریتم flooding استفاده می‌کند.	**SPAAR**
مشکل در حمله کرم‌چاله و حملات داخلی – عدم دریافت بروز رسانی کلید برای بیش از یک بازه زمانی	رعایت دقیق تصدیق اصالت پیام	این پروتکل مبتنی بر یک لایه میانی بین لایه شبکه و MAC است و از تکنیک TESLA برای تصدیق اصالت پیام‌ها استفاده می‌کند که در این تکنیک از یک تابع درهم‌ساز بهره گرفته می‌شود. در این پروتکل یک کلید تصادفی در نظر گرفته می‌شود و بقیه کلیدهای زنجیره از روی آن ساخته می‌شود.	LHAP

۶- روش پیشنهادی

یکی از معروف‌ترین حملات در مسیریابی شبکه‌های موردی سیار حمله سوراخ کرم است که در آن ممکن است چندین گره به عنوان گره‌های متخاصم به شبکه نفوذ کرده و با ارتباط با همدیگر تغییری در توپولوژی شبکه ایجاد کنند و هنگامی که گره‌های مجاز، بسته درخواست مسیر(RREQ) را در شبکه ارسال می‌کنند این بسته در طی فرآیند انتقال به یکی از گره‌های متخاصم رسیده و این گره نیز از طریق یک شبکه خصوصی با سیم و یا بدون سیم آنرا به گره‌های متخاصم دیگری ارسال نماید بدون اینکه تغییری در مقدار شمارنده گام بسته درخواست مسیر ایجاد کنند. بنابراین فیلد شمارنده گام در بسته دارای کمترین مقدار است و این به معنی وجود کوتاهترین مسیر است فلذا این مسیر انتخاب می‌شود. با توجه به جدول فوق و عملکرد هر کدام از این پروتکل‌ها و مزایا و معایب مشخص شده، ما در این مقاله سعی کردیم با تغییراتی در پروتکل SPR مشکل حملات سوراخ کرم را با استفاده از ترکیب جدیدی از تکنیک قلاده‌های بسته حل کنیم. یکی از راه‌های جلوگیری از حمله سوراخ کرم استفاده ازتکنیک قلاده‌های بسته است. در این تکنیک یکسری اطلاعاتی به بسته ارسالی اضافه می‌شود تا اولا از ارسال بسته‌ها برای مسافت‌های بیش از مقدار تعیین شده و دوما از وقوع حمله سوراخ کرم در مسافت‌های کمتر از حد تعیین شده جلوگیری کند و شامل دو دسته است

تکنیک قلاده‌های زمانی: این تکنیک مبتنی بر همزمانی دقیق دو گره مبدا و مقصد و همچنین استفاده از مهر زمان در بسته‌ها است. بدین ترتیب با کاهش مقدار مهر زمانی از زمان دریافت بسته، مدت زمانی که بسته در راه بوده است تخمین زده می شود.

تکنیک قلاده‌های مکانی: این تکنیک مبتنی بر اطلاعات مکانی است که در آن گره مقصد می‌تواند با توجه به محدود بودن سرعت گره‌ها، فاصله تقریبی گره مبدا تا خود را اندازه‌گیری کند و بنابراین از مسیرهای غیر معقول جلوگیری نماید. ما در این مقاله با ایجاد تغییراتی در پروتکل SPR و اضافه کردن تکنیک دیگری به عنوان تکنیک قلاده‌های وضعیت به آن، روش جدیدی برای شناسایی و جلوگیری از حملات سوراخ کرم در مسیریابی امن مبتنی بر پروتکل SPR ارائه می‌دهیم. در این روش مسیرهای با گام‌های مشترک شناسایی شده و به عنوان مسیر امن انتخاب می‌شوند. برای اطمینان از عدم وجود گره‌های متخاصم در مسیر بایستی که بعد از شناسایی این گره‌ها آنها را از فرایند مسیریابی حذف کنیم. مشکلی که در این روش وجود دارد اینست که با وجود تعداد زیاد گره‌های متخاصم شناسایی آنها سخت‌تر می‌شود. برای تشخیص گره‌های متخاصم در الگوریتم پیشنهادی به صورت زیر عمل می‌کنیم:

۱. گره‌هایی که تعداد بسته‌های دریافتی آن از تعداد بسته‌های ارسالی بیشتر باشد ممکن است گره متخاصم باشد
۲. گره‌هایی که در بسته پاسخ مسیر، کمترین تعداد گام و بیشترین شماره ترتیب را درج کند ممکن است گره متخاصم باشد.
۳. گره‌هایی که زودتر به بسته درخواست مسیر پاسخ داده باشد ممکن است گره متخاصم باشد چرا که گره‌های متخاصم بدلیل عدم بررسی جدول مسیریابی زمان پاسخ‌دهی کوتاهتری دارند.

بنابراین با توجه به موارد فوق لازم است که همواره اطلاعات مربوط به گره‌ها اعم از تعداد بسته‌های ارسالی و دریافتی و غیره ثبت شود برای این کار در این مقاله از تکنیک قلاده‌های وضعیت استفاده شده است. تکنیک قلاده‌های وضعیت مبتنی بر وضعیت هر بسته بر اساس ویژگی‌های امنیتی و اطلاعات رمزنگاری است که در آن مقدار برچسب زمان و برچسب آدرس فیزیکی گره ارسال کننده بسته درخواست مسیر توسط کلید خصوصی رمزگذاری شده و این مقادیر در داخل سرایند بسته ارسالی قرار می‌گیرند. با استفاده از این تکنیک می‌توان بسته‌های مبادله شده در مسیر را پیگیری و کنترل کرد. در صورتی که هر کدام از گره‌های میانی، بسته درخواست مسیر را دریافت کنند با استفاده از برچسب زمان ارسال و دریافت بسته و محاسبه اختلاف این زمان و با توجه به سرعت انتشار بسته در رسانه میزان تاخیر بسته از فرمول (۱) محاسبه می‌شود. که در آن h تعداد گام و D_{switch} تاخیر سویچینگ برای انتخاب مسیر در هر گره و $D_{Queuing}$ تاخیر صف‌بندی برای نوبت پردازش و $D_{Propagation}$ تاخیر انتشار رسانه می‌باشد. سپس فرمول (۲) مورد بررسی قرار می‌گیرد. اگر رابطه زیر برقرار باشد به معنی این است که تمام گره‌های موجود در مسیر معتبر هستند و بسته مورد قبول واقع می‌شود و این مسیر به عنوان مسیر امن شناخته می‌شود و در صورتی که رابطه فوق برقرار نباشد یعنی در مسیر کشف شده گره متخاصم وجود دارد و امن نیست بنابراین بسته نادیده گرفته می‌شود.

$$D_{total}=h.\ (D_{switch}+D_{Queuing}+D_{Propagation}) \quad (1)$$

$$(T_r - T_s - D_{total}) <= h*t_{rmax} \quad (2)$$

برای مدیریت کلید و امنیت در روش پیشنهادی از الگوریتم دیفی-هلمن به صورت فرمول (۳) استفاده کرده‌ایم.

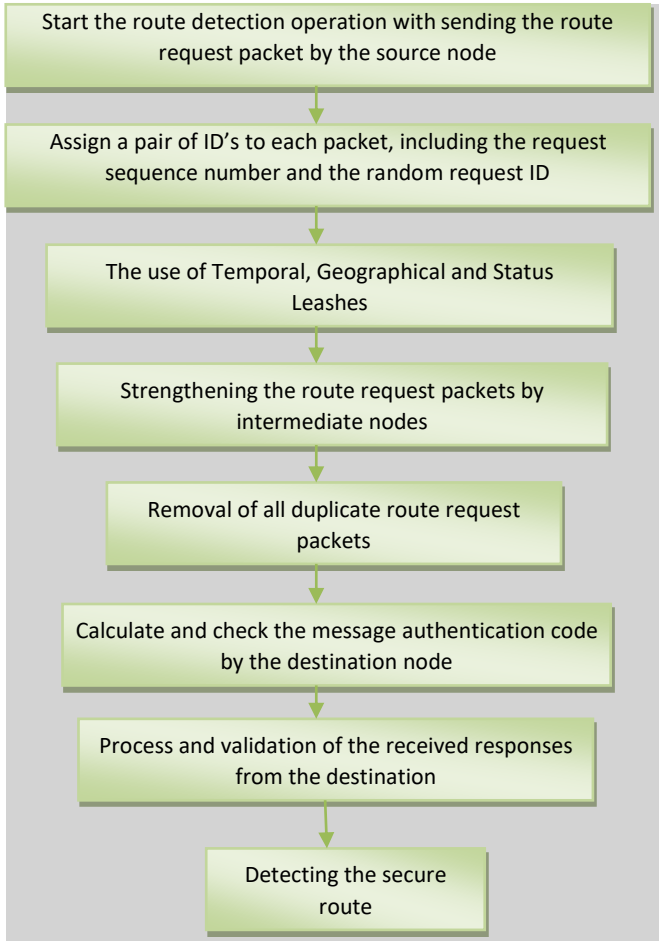
$$A \rightarrow B:\ g^a \bmod p = X$$

$$B \rightarrow A:\ g^b \bmod p = Y$$

$$A \rightarrow B:\ Y^a = g^{ab} = K$$

$$B \rightarrow A:\ X^b = g^{ab} = K$$

کارنمای روش پیشنهادی مطابق شکل (۱) نشان داده می‌شود.



(شکل-۱): کارنمای روش پیشنهادی

۷- نتایج تجربی

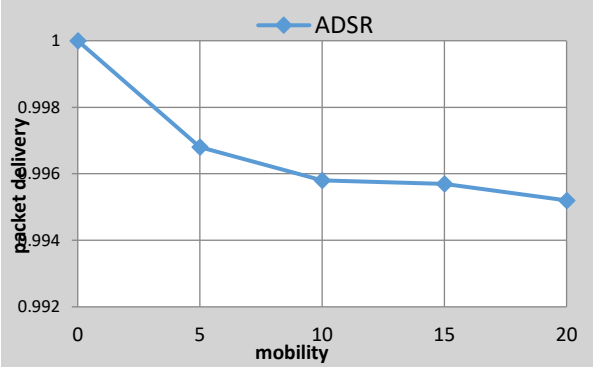
برای شبیه‌سازی از نرم افزار متلب استفاده شده است و پارامترهای شبیه‌سازی در جدول (۳) نشان داده شده است.

(جدول-۳): پارامترهای شبیه‌سازی

پارامترها	مقادیر
تعداد گره‌های متحرک	۵۰
تعداد گره‌های سوراخ کرم	۲
زمان	۳۰۰
توپولوژی	۱۰۰۰*۱۰۰۰
پروتکل مسیریابی	DSR
برد رادیویی	۲۰۰
اندازه بسته‌ها	۵۱۲ بایت

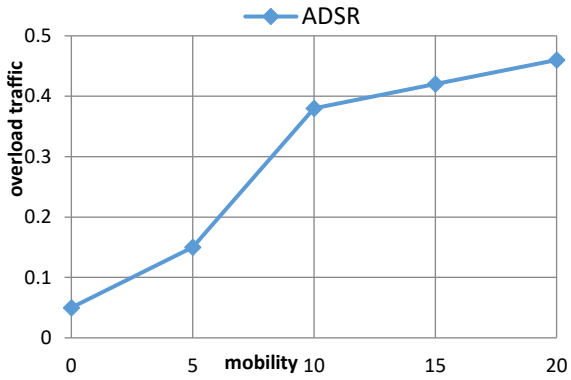
در نمودارهای زیر منظور از ADSR روش پیشنهادی می‌باشد.

در شکل (۲) تاثیر سرعت تحرک گره‌ها بر نرخ تحویل بسته در روش پیشنهادی نشان داده شده است.

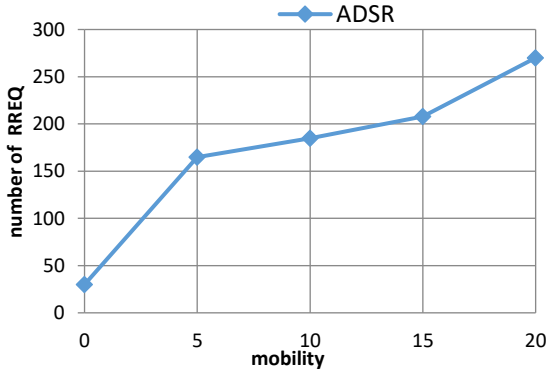


(شکل-۲): تاثیر سرعت تحرک گره‌ها بر نرخ تحویل بسته

در شکل (۳) با افزایش یک تکنیک جدید بنام تکنیک قلاده وضعیت، تغییرات سربار ترافیکی نشان داده شده است.

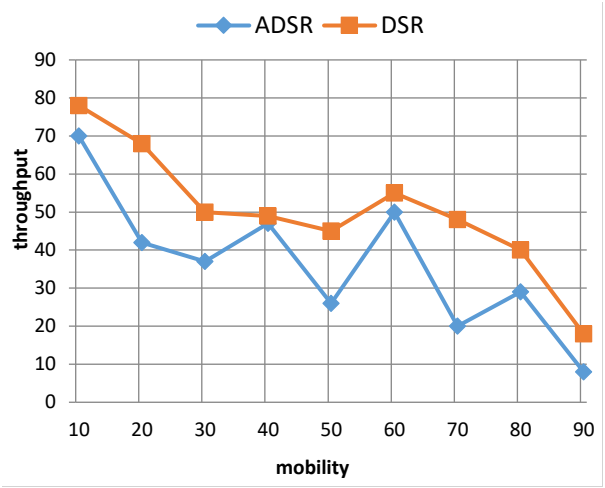


(شکل-۳): تاثیر ترافیک بر میزان اضافه بار



(شکل-۴): تاثیر سرعت گره‌ها بر تعداد پیام‌های درخواست مسیر

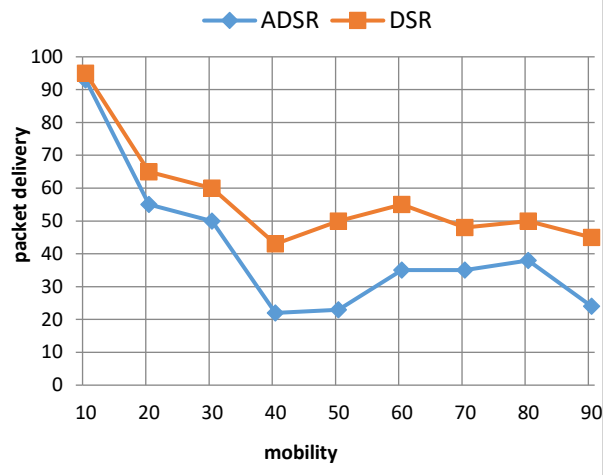
شکل (۴) الگوریتم ADSR را اجرا کرده و تاثیر سرعت گره‌ها را بر تعداد پیام‌های درخواست مسیر نشان می‌دهد که با افزایش سرعت تحرک گره‌ها تعداد بسته‌ها افزایش چشم‌گیری داشته است.



(شکل-۵): تاثیر حمله سوراخ کرم بر میزان گذردهی شبکه

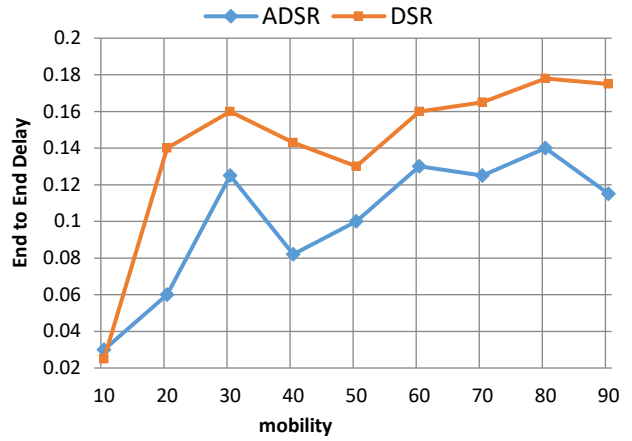
همانطور که در شکل (۵) دیده می‌شود میزان گذردهی در الگوریتم ADSR نسبت به الگوریتم DSR افزایش داشته است چرا که در الگوریتم ADSR مسیرهای دارای گره‌های مخرب شناسایی و نادیده گرفته شده‌اند.

در شکل (۶) تاثیر حمله سوراخ کرم بر نرخ تحویل بسته نشان داده شده است که با وجود گره‌های مخرب این نرخ افزایش می‌یابد.



(شکل-۶): تاثیر حمله سوراخ کرم بر نرخ تحویل بسته

با توجه به اینکه وجود گره‌های مخرب در شبکه باعث تشکیل مسیرهای کوتاه می‌شود و بدلیل اینکه این گره‌ها می‌توانند با همکاری همدیگر شبکه محلی تشکیل دهند بنابراین تاخیر انتها به انتها در الگوریتم ADSR نسبت به الگوریتم DSR کاهش یافته است. شکل (۷) تاثیر حمله سوراخ کرم را بر این تاخیر نشان می‌دهد.



(شکل-۷): تاثیر حمله سوراخ کرم بر میزان تاخیر انتها به انتها

۸- نتیجه‌گیری و پژوهش‌های آتی

با توجه به اینکه امروزه شبکه‌های موردی سیار کاربردهای زیادی دارند، امنیت در این شبکه‌ها از اهمیت خاصی برخوردار است. بنابراین لازم است مصونیت این شبکه‌ها تا حد زیادی تضمین گردند. روش‌های مختلفی جهت ایجاد امنیت در این شبکه‌ها در سال‌های گذشته مطرح شده است. در این مقاله ابتدا الگوریتم‌های مسیریابی و مسیریابی امن و سپس تاثیر حمله سوراخ کرم بر پروتکل SPR که بر پایه الگوریتم مسیریابی DSR بنا نهاده شده مورد بررسی قرار گرفت و در پایان یک روش نوین شناسایی و جلوگیری از حمله سوراخ کرم در مسیریابی امن شبکه‌های موردی سیار مبتنی بر پروتکل SPR ارائه گردید. و بعد از شبیه‌سازی در نرم‌افزار متلب با معیارهای مختلف مورد ارزیابی قرار گرفت. و با نتایج حاصل شده می‌توان نتیجه گرفت که الگوریتم ADSR نسبت به پروتکل DSR در برابر حمله سوراخ کرم عملکرد بهتری دارد.

۹- مراجع

[1] Kale A., Ruchia Ms., and Gupta SR., "An Overview of MANET Ad Hoc Network," International Journal of Computer Science and Applications, vol. 6, no. 2, pp. 257-264, 2013.

[2] Singh G., and Singh J., "MANET: A Study of Challenges and Routing Principles," International Journal of Advanced and

Innovative Research, vol. 1, no. 1, pp. 514-523, 2012.

[3] Bakshi A., Sharma A.K., and Mishra A., "Significance of Mobile Ad-Hoc Networks (MANETS)," International Journal of Innovative Technology and Exploring Engineering, vol. 2, no. 4, pp. 899-912, 2013.

[4] Tai W.Y., Tan C.T., and Lau S.P., "Towards Utilizing Flow Label IPv6 in Implicit Source Routing for Dynamic Source Routing (DSR) in Wireless Ad Hoc Network," Computers & Informatics (ISCI) on IEEE Symposium, pp. 101-106, 2017.

[5] Cerri D.,Ghioni A., "Securing AODV: the A-SAODV secure routing prototype" Communications Magazine in IEEE, pp. 120-125, vol. 46, Issue 2, 2016.

[6] Perkins C. E., and Bhagwat P., "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" Conference on Communications Architectures, Protocols and Applications, pp. 234-224, 2015.

[7] Nicola Milanovic et al, "Routing and Security in Mobile Ad Hoc Networks",IEEE Computer, vol. 37, no. 2, pp. 61-65, 2014.

[8] Bridget Dahill et al, "A Secure Routing Protocol for Ad Hoc Networks," MobiCom 2012, Atlanta, Georgia, USA, September 23-28, 2012.

[9] Yih-Chun Hu and Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy 2004, Editorial Calendar, vol. 2, no. 3, PP. 94-105, May/June 2014.

[10] Stefano Basagni et al, Mobile Ad-hoc Networking, IEEE press, John Wiley and Sons publication, PP. 329-354, 2004.

[11] Yih-Chun Hu, et al, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the 2003 ACM workshop on Wireless security, San Diego, USA, pp. 30-40, 2013.

[12] S. B. S. Jamali, "A Survey over Black hole Attack Detection in Mobile Ad hoc Network," International Journal of Computer Science and Network Security, vol. 15, pp. 44-51, 2015.

[13] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2012.

[14] Stephen Carter and Alec Yasinsac, "Secure Position Aided Ad hoc Routing," Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), Nov 3-4, 2012.

[15] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A lightweight network access control protocol for ad hoc networks," Ad Hoc Networks, vol. 4, no. 5, pp. 567-585, Sep. 2016.

۱۰ – بیوگرافی نویسنده

فتانه طاهری آشتیانی دارای مدرک کارشناسی رشته کامپیوتر با گرایش نرم افزار از دانشگاه آزاد اسلامی واحد تبریز و مدرک کارشناسی ارشد با گرایش هوش مصنوعی از دانشگاه آزاد اسلامی واحد قزوین است. از سال ۱۳۸۴ عضو هیات علمی دانشگاه آزاد اسلامی واحد بناب بوده و سالها در بخش مدیریت IT این دانشگاه خدمت کرده . ایشان تحقیقات خود را که در زمینه های پژوهشی Optical Character Recognition وسیستم های OCR و شبکه های عصبی وPattern وشبکه و مسیر یابی شبکه و شبکه های حسگر بی سیم و شبکه های موردی سیار بوده در مقالات و مجلات داخلی و خارجی به چاپ رسانده است. نشانی رایانامه ایشان:F.taheri.ashtiyani@gmail.com

روش ارجاع به مقاله : ف. طاهری آشتیانی، ارزیابی و بررسی انواع حملات در مسیریابی شبکه‌های موردی سیار و ارائه روش جدید برای شناسایی و جلوگیری از حملات سوراخ کرم در مسیریابی امن مبتنی بر پروتکل SPR، دوفصلنامه محاسبات و سامانه های توزیع شده، سال سوم، شماره اول، شماره پیاپی ۵، صفحه ۱۱۹ تا ۱۳۰، سال ۱۳۹۹