مطالعات علوم کاربردی در مهندسی

Online ISSN: ٢٤٧٦-٤٥٠٧

دوره ۱۱، شماره ۱، بهار ۱۴۰۴

Print ISSN: ٢٥٣٨-٢٠٥٥

www.irijournals.com

صفحات ۱۵۰-۱۴۴

بررسی و شناسایی امنیت پروتکل‌های مسیریابی در شبکه‌ها در مقابله با حمله تونل خصوصی

محمد خدارحمی

کارشناسی ارشد مهندسی برق گرایش مخابرات سیستم دانشگاه ملایر، ایران.

چکیده

هدف از انجام این پژوهش بررسی و شناسایی امنیت پروتکل‌های مسیریابی در شبکه‌ها در مقابله با حمله تونل خصوصی می‌باشد. تونل‌ها در شبکه، روشی برای انتقال داده‌ها در یک شبکه با استفاده از پروتکل‌هایی هستند که توسط آن شبکه پشتیبانی نمی‌شوند. تونل زدن با کپسوله کردن بسته‌ها (بسته‌بندی بسته‌ها در داخل بسته‌های دیگر) کار می‌کند. بسته‌ها قطعات کوچکی از داده‌ها هستند که مجدداً در مقصد خود در یک فایل بزرگ‌تر جمع خواهند شد. تونل زدن بین دو سرور یک تکنیک مهم به‌منظور ایجاد ارتباط امن و مطمئن بین دو سرور یا دستگاه در شبکه‌های کامپیوتری و فضای نت است. این تکنیک با استفاده از رمزنگاری داده‌ها، از اطلاعات حساس در برابر حمله هکرها نیز محافظت می‌کند. استفاده از تونل زدن در موارد مختلف از جمله ایجاد شبکه‌های VPN و دسترسی به منابع شبکه از راه دور بسیار مفید خواهد بود. مسیریابی یعنی انتخاب مناسب‌ترین مسیر برای انتقال بسته‌ها از دستگاه یک شبکه به دستگاه شبکه دیگر. در این عملیات از پروتکل‌های مسیریابی استفاده می‌شود. وظیفه این پروتکل‌ها یافتن مسیرهای موجود در شبکه یک سازمان، ساختن جدول‌های مسیریابی و تصمیم‌گیری در مورد مسیریابی می‌باشد. یک پروتکل مسیریابی مشخص می‌کند چگونه گره‌ها با یکدیگر ارتباط برقرار می‌کنند و توزیع اطلاعاتی را انجام می‌دهد. یک پروتکل مسیریابی گره‌ها را قادر می‌سازد تا مسیرهایی را بین هر دو گره در یک شبکه کامپیوتری انتخاب کنند. بسته‌های داده‌ها از طریق شبکه‌های کامپیوتری از گره تا گره به مقصد منتقل می‌شوند. الگوریتم‌های مسیریابی، انتخاب مسیر خاص را تعیین می‌کنند.

واژه‌های کلیدی: امنیت، پروتکل‌های مسیریابی، شبکه‌های خصوصی، حمله تونل خصوصی

دوره ۱۱، شماره ۱، بهار ۱۴۰۴، صفحات ۱۵۰-۱۴۴

مقدمه

با پیشرفت‌های به وجود آمده در شبکه‌ها و تکنولوژی‌های ارتباطی، دستگاه‌های بی‌سیم قابل‌حمل در بیشتر فعالیت‌های ما پیدا شده‌اند. بیشتر مردم از کامپیوترهای لپ‌تاپ ، پیچرها و وسایلی که از تکنولوژی سیار بهره می‌گیرند، استفاده می‌کنند. ازجمله این شبکه‌های بی‌سیم می‌توان به شبکه‌های موردی اشاره نمود. شبکه‌های موردی شبکه‌هایی هستند که توسط میزبان‌های بی‌سیم با لینک‌های بدون سیم به هم متصل شده‌اند. این شبکه‌ها هیچ الزامی به استفاده از زیرساخت‌های ثابت و پیش‌ساخته‌ای همچون ایستگاه مرکزی[1]، مسیریاب[2] و سوئیچ[3] ندارند، بلکه فقط تعدادی گره بی‌سیم هستند که با کمک ارتباط با گره‌های همسایه به گره‌های غیرهمسایه متصل می‌گردند. [۱]

عملیات مسیریابی در این شبکه‌ها توسط خود گره‌ها انجام می‌شود و در واقع هر گره به عنوان یک مسیریاب عمل می‌کند و بسته‌های داده را برای سایر گره های موجود در شبکه رو به جلو می‌راند. در این شبکه‌ها ممکن است شبکه به سرعت و به صورت غیرقابل‌پیش‌بینی تغییرات توپولوژی را تجربه کند. به دلیل سهولت و سرعت پیاده‌سازی این شبکه‌ها و همچنین عدم وابستگی به ساختارهای ازپیش ساخته شده کاربردهای فراوانی همچون اتصال لپ‌تاپ‌ها به یکدیگر، محیط‌های نظامی و کنترل از راه دور نبردها، عملیات جستجو و نجات برای ترمیم و به دست آوردن اطلاعات در حوادث غیرمترقبه دارند. [۲]

حمله‌ها علیه شبکه‌های موردی را می‌توان از چند جنبه تقسیم‌بندی نمود: از یک جنبه حمله‌ها به دو دسته تقسیم می‌شوند: حمله‌های خارجی[4] و حمله‌های داخلی[5]. منظور از حمله‌های خارجی حمله‌هایی است که توسط یک یا چند گره خارج از شبکه انجام می‌شود و بیشتر اقدامات امنیتی در مقابل این‌گونه حمله‌ها اعمال می‌شوند. حمله‌های داخلی، حمله‌هایی هستند که توسط گره‌های مجاز داخل شبکه انجام می‌شوند و معمولا جلوگیری از آن‌ها مشکل است. از دیدگاه دیگر حمله‌ها به دو دسته حمله‌های فعال و غیرفعال تقسیم می‌شوند. هر گره میانی یا روتر فقط از اطلاعات مربوط به شبکه‌هایی را که مستقیماً به آن متصل است، اطلاع دارد. یک پروتکل مسیریابی این اطلاعات را ابتدا در میان همسایگان نزدیک و سپس در سراسر شبکه به اشتراک می‌گذارد. به این ترتیب، روترها دانش توپولوژی شبکه را بدست می آورند. توانایی مسیریابی پروتکل‌ها به صورت پویا با توجه به شرایط در حال تغییر است. ویژگی‌های خاص پروتکل‌های مسیریابی عبارتند از روشی که آن‌ها از حلقه‌های مسیریابی اجتناب می‌کنند، نحوه انتخاب مسیرهای مورد نظر، استفاده از اطلاعات مربوط به هزینه‌های گام، زمان لازم برای دستیابی به همگرایی مسیریابی، مقیاس پذیری آن‌ها و سایر عوامل است. پروتکل RIP اطلاعات قابل دسترسی را با نزدیکترین همسایه‌های خود مبادله می‌کند که این اطلاعات مجموعه‌ای از مقاصد شناخته شده برای مسیریاب‌های شرکت‌کننده است.[۴]

در حمله‌های غیرفعال، متخاصم فقط به استراق‌سمع داده‌های در حال انتقال گوش می‌دهد. اما در حمله‌های فعال، متخاصم علاوه براستراق‌سمع داده‌ها می‌تواند آن‌ها را به نفع خود تغییر دهد. دیدگاه بعدی از لحاظ لایه‌هایی است که مورد حمله قرار گرفته‌اند، یعنی حمله می‌تواند بر روی لایه فیزیکی، پیونددداده، شبکه و کاربرد صورت پذیرد. نوع دیگری ازحمله‌ها مانند عدم‌شرکت در عملیات مسیریابی یا قطع‌ارتباط نیز وجود دارند که منجر به حمله‌ی ممانعت از سرویس می‌شوند و تنها راه جلوگیری از آن‌ها پیدا کردن گره متخاصم است. حمله‌ی دیگر حمله‌ی جامعیت است که یک گره متخاصم می‌تواند خود را به جای یک گره درست معرفی کند. یکی دیگر از انواع حمله‌ها حمله‌ی ردکردن سرویس است.

در این نوع حمله، حمله‌کننده تعداد زیادی بسته‌ی بی‌ارزش به شبکه تزریق می‌کند که این بسته‌ها بخش عمده‌ای از منابع شبکه را مصرف می‌کنند. [۵]

دو نوع دیگر از انواع حمله‌ها عبارتند از: حمله‌ی شکست مسیریابی[6] و حمله‌ی مصرف مسیریابی[1]. در حمله‌ی شکست مسیریابی حمله‌کننده سعی بر آن دارد که بسته‌های خود را به عنوان بسته مجاز روی شبکه ارسال کند تا در راه‌های غیرکارا

[1] Base Station
[2] Router
[3] Switch
[4] External Attacks
[5] Internal Attacks
[6] Routing Distruption Attack

صرف شوند، در حمله‌ی مصرف مسیریابی مهاجم سعی برآن دارد با ارسال بسته‌ی غیرمجاز پهنای‌باند و یا حافظه و توان محاسباتی گره را مصرف کند. نوع دیگری از حمله، حمله هجوم[2] است که در عملیات کشف مسیر، گره مهاجم درخواست خود را بسیار سریع‌تر از گره مجاز ارسال می‌کند و با احتمال بیشتری بسته‌اش مورد پذیرش قرار خواهد گرفت. مهاجم می‌تواند با احتمال زیادی مسیری را بنا کند که خود او در آن مسیر وجود دارد. [۴]

۲. مسیریابی در شبکه‌های موردی

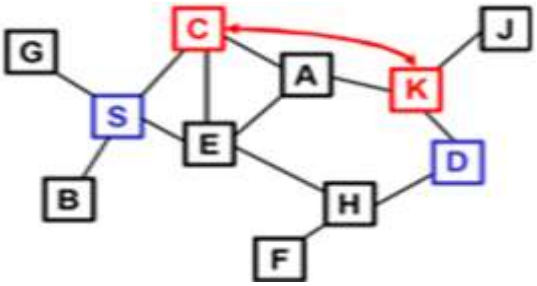
۲,۱ درخواست مسیر

گره مبدأ یک بسته کنترلی درخواست مسیر که به اختصار آن را RREQ[3] می‌نامیم در شبکه منتشر می‌کند و هر گره میانی که اولین بار آن را می‌شنود به انتشار مجدد آن در شبکه می‌پردازد. [۳]

۲,۲ مرحله پاسخ مسیر

به محض دریافت یک پیام RREQ، مقصد بسته‌ی پاسخ مسیر را در جهت عکس برای مبدا ارسال می‌کند. بسته‌ی پاسخ مسیر به اختصار RREP[4] نامیده می‌شود.

حمله‌ی تونل‌کرم عملیات مسیریابی در شبکه را به شدت تحت تاثیر قرار می‌دهد. برای مثال همان‌گونه که در شکل زیر نشان داده شده است اگر گره متخاصم C بسته‌های درخواست مسیرِ S را به مقصد یکی ازگره‌های J,D,H,A, توسط لینک پرسرعتش با K منتقل نماید، گره‌های مورد نظر گره تصور می‌کنند که گره K در همسایگی آن‌ها قرار دارد و یا فقط یک گام از آن‌ها فاصله دارد. پس بنابراین بسته را از طریق تونل ایجاد شده میان گره C و گره K منتقل می‌کنند.



شکل شماره ۱: حمله تونل‌کرم. [۶]

۳. حمله‌های تونل خصوصی و انواع آن

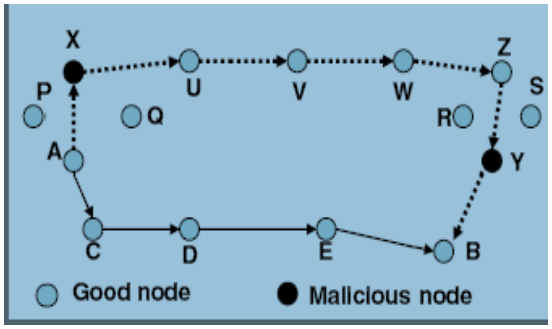
۳,۱ حمله تونل‌کرم با استفاده از محفظه سازی[5]

مطابق شکل صفحه بعد X و Y دو گره متخاصم می‌باشند، وقتی گره A بسته‌ی درخواست مسیر را ارسال می‌کند، بسته به گره X می‌رسد. گره X میان خودش و گره متخاصم بعدی که در این حالت Y می‌باشد، محفظه‌ای مجازی ایجاد می‌کند و بسته را داخل این محفظه منتقل می‌کند، بعد از دریافت بسته در Y، گره Y بسته را به سمت مقصد B هدایت می‌کند.

نکته این که به سبب محفظه‌سازی بسته، مقدار طول گام به هنگام عبور از گره‌های u-v-w-z افزایش نمی‌یابد. به طور همزمان بسته درخواست مسیر از مسیر C-D-E به مقصد D می‌رسد. گره B دو مسیر دارد یکی از طریق C-D-E به طول ۴ و دیگری از طریق گره‌های متخاصم X و Y و ظاهراً به طول ۳ گره B مسیری با طول کمتر را انتخاب می‌کند اما در واقع طول مسیر انتخاب شده ۷ می‌باشد پس می‌توان گفت: هر پروتکل مسیریابی که از معیار کوتاه‌ترین مسیر به عنوان بهترین مسیر استفاده می‌کند در برابر حمله تونل‌کرم آسیب‌پذیر است. [۱۰]

---

[1] Routing Consumption Attack
[2] Rushing Attack
[3] Rout Request
[4] Rout Reply
[5] Encapsulation

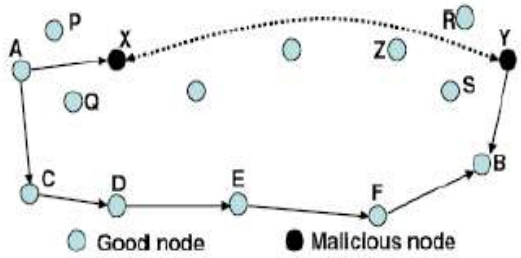


شکل شماره ۲: تونل‌کرم با استفاده از کانال IN BAND [۷]

۳,۲ تونل‌کرم با استفاده از کانال خارج از باند[1]

مطابق شکل، این حمله از طریق کانالی با پهنای باند بالای خارج از باند میان گره‌های متخاصم انجام می‌شود. امکان اجرای این نوع حمله نسبت به قبلی سخت‌تر است، زیرا نیازمند قابلیت سخت‌افزاری ویژه‌ای می‌باشد. [۸]

در این جا نیز دو مسیر وجود دارد: مسیری از طریق گره C، (A-C-D-E-F-B) و به طول پنج گام و مسیری از طریق گره‌های متخاصم به طول ظاهری. در این‌جا نیز گره مقصد مسیری با طول کمتر را انتخاب می‌کند و حمله با موفقیت صورت می‌پذیرد.



شکل شماره ۳: تونل‌کرم با استفاده از کانال OUT BAND [۹]

۳,۳ تونل‌کرم با استفاده از بازپخش کردن[2] بسته

در این نوع حمله، یک گره متخاصم بسته‌ها را بین دو گره دور از هم بازپخش می‌کند برای این‌که آن‌ها را متقاعد کند که همسایه هستند. این اقدام می‌تواند توسط هریک از گره‌های متخاصم انجام شود. حداقل تعداد گره‌های متخاصم در دو روش قبلی دو گره بود ولی در این روش یک گره می‌باشد.[۹]

۴. پروتکل‌های مسیریابی شبکه‌های موردی

۴,۱ دسته‌بندی پروتکل‌های مسیریابی

پروتکل‌های مسیریابی در شبکه‌های موردی به دو دسته کلی تقسیم می‌شوند:

الف) پروتکل‌های فعال: که اطلاعات مسیریابی را برای همه گره‌ها سازگار و به‌روز رسانی می‌کنند.

ب) پروتکل‌های واکنشی: که هرگاه نیاز باشد یعنی هر زمان که گره مبدا می‌خواهد بسته‌ای را به مقصد بفرستد، مسیری ساخته می‌شود که شامل مکانیسم‌های کشف مسیر برای پیدا کردن راهی به مقصد می‌باشد. [۱۵]

ج) پروتکل سیل‌آسا: در این روش گره فرستنده اطلاعات را برای تمام گره‌های همسایه خود ارسال می‌کند و این روال تا مقصد ادامه پیدا می‌کند. هر بسته یک شماره توالی[3] دارد برای جلوگیری از تکرار ارسال بسته توسط یک گره. هر گیرنده با کنترل شماره توالی بسته در صورت غیرتکراری بودن آن، بسته را برای همسایگان خود ارسال می‌کند. مزیت اصلی این روش

[1] Out Of Band
[2] Packet Relay
[3] Sequence Number

سهولت پیاده‌سازی و اطمینان از رسیدن بسته‌ها به مقصد است و مشکل اصلی آن حجم بالای بسته‌های داده و طی مسافت طولانی بدون دلیل می‌باشد.

د) پروتکل DSR[1]: در پروتکل مسیریابی امن پویا که به اختصار آن را DSR می‌نامیم گره مبدأ با تولید بسته‌ی درخواست مسیر و قرار دادن مبدأ و مقصد در آن و سپس ارسال آن به وسیله‌ی پروتکل سیل‌آسا کار را آغاز می‌کند. هر گره با دریافت بسته در صورت ندانستن مسیر، نام خود را به لیست بسته اضافه کرده و آن را منتشر می‌کند. [۱۴]

اگر گرهی قادر به ارسال بسته برای گره بعدی نباشد و در واقع احتمال شکست مسیریابی در آن وجود داشته باشد با ارسال بسته‌ای به نام خطای مسیردهی[2] برای گره مبدأ سعی می‌کند تمام گره‌ها را متوجه قطع ارتباط نماید تا مسیریابی از سرگرفته شود. با این که این روش، روش خوبی است و حتماً به جواب می‌رسد اما به دلیل انتقال بسته‌هایی با سرآیند بزرگ بار شبکه و مصرف پهنای باند را افزایش می‌دهد.

ه) پروتکل AODV[3]: پروتکل بردار فاصله‌ی بنا به درخواست پیشرفته که به اختصار AODV نامیده می‌شود، برخلاف DSR مسیر را در سرآیند بسته قرار نمی‌دهد، بلکه هر گره هنگام دریافت پیام درخواست مسیر از روی جدولی که از قبل در اختیار داشته آن را کنترل می‌کند، اگر مسیر نهایی را در جدول خود داشته باشد پیام پاسخ مسیر را می‌فرستد. برای گره‌های میانی از یک شماره‌ی توالی در یک پیام درخواست مسیر استفاده می‌شود و تنها در صورتی پیام پاسخ مسیر توسط گره میانی صادر می‌شود که RREQ کوچک‌تر از شماره‌ی توالی مسیر باشد.

و) پروتکل LAR[4]: این پروتکل با استفاده از اطلاعات مکانی برای کاهش سرباری مسیریابی پروتکل سیل‌آسا تلاش می‌کند. در این جا فرض می‌شود که هر گره مکان خودش را از طریق یک سیستم مکان‌یابی تعیین موقعیت سراسری یا GPS[5] می‌شناسد. [۱۳]

۵. تشخیص و مقابله با حمله‌ی تونل‌کرم

همان‌طور که گفته شد یکی از تهدیدات جدی علیه امنیت شبکه‌های موردی حمله تونل خصوصی می‌باشد که برای مقابله با آن روش‌های مختلفی پیشنهاد شده است. در ادامه به معرفی برخی از این روش‌ها می‌پردازیم.

۵,۱ پروتکل WARP[6]: یکی از پروتکل‌هایی که برای اجتناب از حمله‌ی تونل خصوصی طی فرآیند مسیریابی مطرح شده است پروتکل WARP می‌باشد که توسط Ming-Yang Su در دانشگاه Ming Chuan ارائه شد. این پروتکل مسیریابی بر پایه AODV می‌باشد و می‌تواند گره‌های تونل‌کرم را از دخالت در روند مسیریابی دور نگه دارد. این پروتکل مسیرهای چندگانه‌ی گسسته‌ای را که از مبدأ تا مقصد وجود دارند مورد بررسی قرار می‌دهد و نهایتاً فقط یک مسیر را برای انتقال بسته‌های داده انتخاب می‌کند. اساس WARP بر این است که گره‌های همسایه یک گره تونل‌کرم از توان بسیار بالای گره تونل‌کرم در کشف مسیر آگاهی داشته باشند و سعی بر این دارد که گره‌های تونل‌کرم به تدریج توسط همسایه‌های نرمالشان کنار گذاشته شوند.

۵,۲ پروتکل DELPHI[7] DELPHI توسط Chiu و Wong Lui در دانشگاه Hong kong پیشنهاد شد. برای هر مسیر مجزا به صورت جداگانه تعداد گام و اطلاعات مربوط به تأخیر را جمع‌آوری کرده و مقدار تأخیر بر گام را به عنوان شاخص تشخیص حمله‌ی تونل خصوصی در نظر گرفته است که مقدار این شاخص در مسیر نرمال کوچک‌تر است. [۱۲]

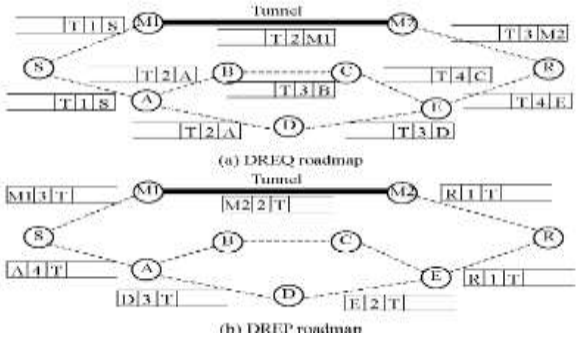
پروتکل DELPHI دارای دو فاز می‌باشد:

۱. فاز اول اطلاعات مربوط به تأخیر مسیرها و تعداد گام جمع‌آوری می‌شود.

۲. فاز دوم فرستنده به تجزیه وتحلیل اطلاعات به دست آمده در فاز اول برای تشخیص وجود تونل خصوصی می‌پردازد.

---

[1] Dynamic Secure Routing
[2] Rout Error
[3] Advanced On-Demand Distance Vector
[4] Location Aided Routing
[5] Global Positioning System
[6] Wormhole Avoidance Routing Protocol
[7] Delay Per Hop Indication



شکل شماره ۴: عملیات مسیریابی توسط پروتکل DELPHI [۱۱]

۶. نتیجه‌گیری و پیشنهادات

بر اساس مطالب گفته شده در فصل‌های قبل دیدیم که امروزه اکثر شبکه‌ها از جمله شبکه‌های موردی در برابر حمله‌ی تونل خصوصی ضعیف هستند. برای مقابله با این حمله پروتکل‌های مختلفی پیشنهاد شده بود که هر یک به نحوی می‌کوشیدند که مانع از تحمیل این حمله به شبکه شوند. همان‌طور که دیده شد پروتکل OLSR بالاترین میزان گذردهی را در انتقال بسته‌های داده به سمت مقصد و جلوگیری از انحراف آن‌ها از مسیر اصلی داشت و حداقل افزایش ناگهانی تاخیر از شبکه‌ی نرمال به شبکه‌ی تحت حمله را داراست. و در نتیجه مسیریابی بر اساس این پروتکل از امنیت بیشتری برخوردار بود.

- ✓ برای مقابله با حمله‌ی تونل خصوصی پروتکلی با بالاترین میزان گذردهی را انتخاب کنیم.
- ✓ برای مقابله با حمله‌ی تونل خصوصی پروتکلی با حداقل شکست در برابر مهاجمان را انتخاب کنیم.
- ✓ پروتکلی که حداقل افزایش تاخیر از شبکه‌ی نرمال به تحت حمله را دارد می‌تواند در مقابل تونل خصوصی بهتر عمل کند.
- ✓ ما با توجه به نتایج ارزیابی‌ها برای برقراری امنیت مسیریابی در شبکه‌های موردی در برابر حمله‌ی تونل خصوصی، در شبکه‌های متراکم پروتکل OLSR را پیشنهاد می‌دهیم.

با این‌که پروتکل OLSR تا حدود زیادی امنیت مسیریابی را در شبکه‌های موردی برقرار می‌کند اما باز هم در برابر حمله‌ی تونل خصوصی ضعیف است، پس به دست آوردن پروتکلی که کلا مانع از ایجاد تونل خصوصی در شبکه‌ی موردی گردد، امنیت مسیریابی در آن ۱۰۰٪ باشد و گره‌های متخاصم را از شبکه حذف نماید و به نحوی بتواند علاوه بر پارامترهای فوق بار و ترافیک شبکه را نیز کاهش دهد به عنوان کار آتی محسوب خواهد شد.

منابع و مأخذ

[1] Prayag Narula, Sanjay Kumar Dhurandher, Sudip Misra, Isaac Woungang. (2023) "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing", in computer communication 31, pp 760-769

[2] Radwan Mahmoud E.H. Houssein. (2023) "Evaluation comparision of some ad hoc networks routing protocols", 12th Egyption Informatics Journal, pp 95-106

[3] Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam. (2022) "Collaborative Techniques for Detecting Wormhole Attack in MANETs"

[4]Mahajan, V.Natu, M.sethi, A, "Analysis of wormhole intrusion attacks in MANETs", in IEEE Military Communications conference (MILCOM), pp 1-7

[5] Luis Fernando Garcia and Jean-Marc Robert. (2021) "Preventing Layer-3 wormhole attacks in ad hoc networks with multiple DSR", in the 8th IFIP Annual Mediterranean Ad Hoc Networking Workshop, pp 15-20

[6] Lang D. (2022) "evaluation and classification of routing protocols for mobile ad hoc networks" thesis Fakultat fur Informatik der Technischen Universitat Munchen, Germany.

[7] Ashtiani H, Alirezaee S, Mohsen mir hosseini S, khosravi H. (2022) "NR new position based routing algorithm for mobile ad hoc networks", in: proceedings of the world congress on engineering ,UK, vol 1,2009

[8] Sanzgiri D.Laflamme, B.Dahill Levine shields and E.M.Belding-Royer. (2023) "Authenticated Routing for ad hoc networks", IEEE Journal on selected Areas in Commnication, special issue on wireless Ad Hoc networks vol 23, no 3, pp 598-610.

[9] Song baiLu, LongXuanLi, kwok-Yan Lam, Ling yan jia, (2022) "SAODV: A routing protocol that can withstand Blackhole attack international conference of computational intelligence and security December 421-425

[10] Chiu, HS Lui, ks (2021) "DelPHI wormhole Detection Mechanism for ad hoc wireless Networks"in the 1st International symposium on wireless pervasive computing, phuket, Thailand 16-18 January

[11] Sun choi, Doo-young hyeon Lee, Jae-il (2021) "WAP wormhole prevention Algorithm in Mobile ad hoc networks", in IEEE International Conference on sensor Networks, Ubiquitous, and Trustworthy computing, pp 343-348

[12] H.VU. (2022) "WORMEROS: A New Framework for Defending against wormhole Attacks on wireless ad hoc networks", proc.Of Int'1 conf. on wireless algo. Systems and App LNCS Vol 5258 pp 491-502

[13] Saurabh Gupta, subrat kar, S Dharmaraja. (2020) "WHOP: wormhole Attack Detection protocol using Hound Packet", in International Conference on Innovations in Information Technology", pp 226-231

[14] L.Qian, N.song, and X.Li. (2020) "Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach", in the Journal of Network and computer applications, vol 30, pp 308-330.

[15] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, (2021) "SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks" in IEEE Communications Society (ICC)