اولین کنفرانس بین‌المللی هوش مصنوعی
و علوم کامپیوتری نوظهور: از الگوریتم تا آینده‌نگری
First International Conference on Artificial Intelligence
and Emerging Computer Science: From Algorithm to Foresight
ICAICS
https://icaics.ir
info@icaics.ir
March 17, 2026-GEORGIA
۲۶ اسفند ماه ۱۴۰۴–گرجستان

مروری بر حملات و راهکارهای امنیتی در شبکه‌های سیار موردی(MANET)

فرهنگ پدیداران مقدم
استادیار گروه کامپیوتر، مجتمع آموزش عالی فنی مهندسی اسفراین
padidaran@esfarayen.ac.ir

مصطفی ضیغمی
دانشجوی کارشناسی ارشد دانشگاه غیردولتی اشراق بجنورد
mostafaZeighami@outlook.com

چکیده

شبکه‌های سیار موردی (MANET) به‌عنوان یکی از مهم‌ترین انواع شبکه‌های بی‌سیم بدون زیرساخت، به دلیل ویژگی‌هایی مانند توپولوژی پویا، تحرک بالای گره‌ها، ارتباطات چندهاپه و نبود کنترل مرکزی، در کاربردهای حساس و پویا مورد توجه قرار گرفته‌اند. با این حال، همین ویژگی‌ها موجب بروز چالش‌های امنیتی جدی در این شبکه‌ها شده است، به‌گونه‌ای که امنیت به یکی از مسائل اساسی و حل‌نشده در MANET تبدیل شده است. این مقاله با رویکردی مروری، به بررسی و تحلیل مهم‌ترین حملات امنیتی و راهکارهای مقابله با آن‌ها در شبکه‌های MANET می‌پردازد. در این راستا، هشت مقاله منتخب در حوزه امنیت MANET مورد مطالعه قرار گرفته و رویکردهای مختلف از جمله امنیت مبتنی بر مسیریابی، مدل‌های اعتماد، سیستم‌های تشخیص نفوذ و روش‌های مبتنی بر یادگیری ماشین به‌صورت مقاله‌به‌مقاله تحلیل شده‌اند. نتایج این بررسی نشان می‌دهد که هر یک از رویکردهای امنیتی، تنها بخشی از چالش‌های موجود را پوشش می‌دهند و اغلب میان سطح امنیت، کارایی شبکه، مصرف انرژی و مقیاس‌پذیری یک بده‌بستان اجتناب‌ناپذیر وجود دارد. همچنین مشخص می‌شود که روش‌های سنتی امنیتی در مواجهه با تحرک بالا و محدودیت منابع MANET کارایی لازم را ندارند و رویکردهای نوین، اگرچه دقت بالاتری دارند، با چالش‌های پیاده‌سازی عملی مواجه هستند. در نهایت، این مقاله ضمن جمع‌بندی وضعیت فعلی پژوهش‌ها، خلأهای موجود در حوزه امنیت MANET را مشخص کرده و ضرورت توسعه راهکارهای جامع، تطبیق‌پذیر و کم‌هزینه را برجسته می‌سازد.

واژگان کلیدی: MANET، امنیت شبکه، حملات امنیتی، مسیریابی امن، سیستم تشخیص نفوذ

مقدمه

شبکه‌های سیار موردی (Mobile Ad Hoc Networks – MANET) نوعی شبکه بی‌سیم بدون زیرساخت هستند که در آن گره‌ها به‌صورت پویا و خودسازمان‌ده با یکدیگر ارتباط برقرار می‌کنند. در این شبکه‌ها هر گره علاوه بر ارسال و دریافت داده، نقش مسیریاب را نیز ایفا می‌کند و ارتباطات معمولاً به‌صورت چندهاپه انجام می‌شود. ویژگی‌هایی مانند تحرک بالا، توپولوژی متغیر و نبود کنترل مرکزی، MANET را برای کاربردهایی نظیر عملیات نظامی، امداد و نجات و شبکه‌های اضطراری مناسب ساخته است[1].

با وجود این مزایا، همین ویژگی‌ها چالش‌های امنیتی جدی را برای MANET به همراه دارند. نبود مرجع مرکزی برای نظارت و احراز هویت، استفاده از محیط بی‌سیم باز و محدودیت منابعی مانند انرژی و پهنای باند، باعث می‌شود این شبکه‌ها در برابر حملات مختلفی نظیر دستکاری مسیریابی، شنود و رفتارهای مخرب گره‌های داخلی آسیب‌پذیر باشند. این تهدیدات می‌توانند عملکرد شبکه را مختل کرده و قابلیت اطمینان ارتباطات را به‌شدت کاهش دهند، ازاین‌رو امنیت به یکی از مسائل اساسی در MANETتبدیل شده است[2].

در سال‌های اخیر، پژوهش‌های متعددی با هدف افزایش امنیت MANET ارائه شده‌اند که شامل رویکردهای مبتنی بر اصلاح پروتکل‌های مسیریابی، مدل‌های اعتماد، سیستم‌های تشخیص نفوذ و روش‌های هوشمند مانند یادگیری ماشین می‌باشند [۳]–[۸]. با این حال، تنوع حملات و محدودیت‌های ذاتی MANET موجب شده است که هیچ راهکار واحدی پاسخگوی تمامی چالش‌ها نباشد. هدف این مقاله ارائه یک مرور تحلیلی بر مطالعات انجام‌شده در حوزه امنیت MANET، بررسی نقاط قوت و محدودیت‌های رویکردهای موجود و شناسایی خلأهای پژوهشی برای تحقیقات آینده است.

۱ -مروری بر پروتکل‌های مسیریابی، حملات و روش‌های مقابله در شبکه‌هایMANET

۱-۱ -هدف مقاله و جایگاه آن در ادبیات پژوهش

این مقاله با هدف ارائه یک مرور ساخت‌یافته از وضعیت امنیت در شبکه‌های MANET تدوین شده است و تمرکز آن بر ارتباط مستقیم میان طراحی پروتکل‌های مسیریابی و بروز تهدیدات امنیتی قرار دارد. نویسندگان تلاش می‌کنند نشان دهند که چرا مسیریابی، به‌عنوان هسته عملکردMANET ، به یکی از آسیب‌پذیرترین اجزای شبکه تبدیل شده است. از این منظر، مقاله نقش یک منبع مرجع را در ادبیات پژوهش ایفا می‌کند که زمینه‌ساز مطالعات بعدی در حوزه امنیت MANET شده است.[1]

۱-۲ -وابستگی امنیت MANET به پروتکل‌های مسیریابی

پروتکل‌های مسیریابی در MANET عمدتاً با هدف بهبود معیارهایی مانند تأخیر، سربار کنترلی و سازگاری با تحرک بالا طراحی شده‌اند. در این طراحی‌ها، ملاحظات امنیتی نظیر احراز هویت و صحت‌سنجی پیام‌های کنترلی کمتر مورد توجه قرار گرفته است. این رویکرد باعث شده است که فرآیند کشف و نگهداری مسیر به نقطه‌ای حساس از نظر امنیتی تبدیل شود و امنیت کلی شبکه به‌طور مستقیم به امنیت مسیریابی وابسته باشد[1] .

۱-۳ -منشأ آسیب‌پذیری‌های امنیتی درMANET

آسیب‌پذیری‌های امنیتی MANET حاصل ترکیب عواملی نظیر اعتماد ضمنی میان گره‌ها، ماهیت توزیع‌شده شبکه و نبود نظارت مرکزی هستند. این شرایط امکان انتشار اطلاعات نادرست مسیریابی را بدون شناسایی سریع فراهم می‌کند. در چنین محیطی، حتی یک گره مخرب می‌تواند با دستکاری پیام‌های کنترلی، بخش قابل توجهی از شبکه را تحت تأثیر قرار دهد[2] .

۱-۴ -حملات مبتنی بر مسیریابی و تأثیر آن‌ها

حملات مبتنی بر مسیریابی از مهم‌ترین تهدیدات امنیتی MANET محسوب می‌شوند، زیرا مستقیماً فرآیند برقراری ارتباط را هدف قرار می‌دهند. حملاتی مانندBlackhole ، Wormholeو Greyhole با جعل یا دستکاری اطلاعات مسیریابی، مسیرهای نادرست ایجاد کرده و منجر به کاهش نرخ تحویل بسته، افزایش تأخیر و ناپایداری شبکه می‌شوند. وابستگی MANET به همکاری گره‌ها، شدت اثر این حملات را افزایش می‌دهد[1]، [2].

۱-۵ -رویکردهای مقابله و چالش‌های عملی

برای مقابله با حملات امنیتی، رویکردهای مختلفی از جمله اصلاح پروتکل‌های مسیریابی، مدل‌های مبتنی بر اعتماد، سیستم‌های تشخیص نفوذ و مکانیزم‌های امنیتی مکمل مطرح شده‌اند. اگرچه این روش‌ها می‌توانند تا حدی تهدیدات را کاهش دهند، اما اغلب با چالش‌هایی مانند افزایش سربار کنترلی، مصرف انرژی و پیچیدگی محاسباتی همراه هستند که کارایی عملی آن‌ها را در محیط‌های پویا محدود می‌کند [۱]، [۳].

۲-تحلیل چالش‌ها و حملات امنیتی در شبکه‌هایMANET

۲-۱-ویژگی‌های ساختاری MANET و تأثیر آن‌ها بر امنیت

شبکه‌های MANET به دلیل تحرک بالای گره‌ها، تغییر مداوم توپولوژی و نبود کنترل مرکزی، از نظر امنیتی محیطی پیچیده و آسیب‌پذیر محسوب می‌شوند. این ویژگی‌ها باعث می‌شوند فرآیندهای نظارتی و اعمال سیاست‌های امنیتی به‌صورت متمرکز امکان‌پذیر نباشد و تصمیم‌گیری‌ها به‌طور کامل به گره‌های شبکه واگذار شود. چنین شرایطی، احتمال سوءاستفاده از ساختار شبکه را افزایش می‌دهد[2] .

۲-۲-محدودیت منابع و نقش آن در بروز آسیب‌پذیری‌ها

یکی از عوامل کلیدی در ناامن بودنMANET ، محدودیت منابعی مانند انرژی، توان پردازشی و پهنای باند است. این محدودیت‌ها باعث می‌شوند پیاده‌سازی مکانیزم‌های امنیتی سنگین عملی نباشد و بسیاری از راهکارهای کلاسیک امنیت شبکه قابل استفاده نباشند. در نتیجه، گره‌ها اغلب فاقد مکانیزم‌های دفاعی قوی بوده و در برابر حملات مختلف آسیب‌پذیر باقی می‌مانند [۲]، [3].

۲-۳-اعتماد ضمنی بین گره‌ها و پیامدهای امنیتی آن

در MANET معمولاً فرض بر این است که گره‌ها به‌صورت صادقانه در فرآیند مسیریابی و انتقال داده همکاری می‌کنند. این اعتماد ضمنی، اگرچه برای عملکرد شبکه ضروری است، اما زمینه‌ساز بروز حملات داخلی می‌شود. گره‌های مخرب می‌توانند با سوءاستفاده از این اعتماد، اطلاعات نادرست مسیریابی را منتشر کرده یا بسته‌ها را به‌صورت گزینشی حذف کنند، بدون آنکه به‌راحتی شناسایی شوند [۲]، [5].

۲-۴-طبقه‌بندی حملات امنیتی درMANET

حملات امنیتی در MANET را می‌توان به دو دسته کلی حملات غیرفعال و فعال تقسیم کرد. حملات غیرفعال عمدتاً محرمانگی داده‌ها را هدف قرار می‌دهند، در حالی که حملات فعال با دستکاری یا حذف بسته‌ها مستقیماً عملکرد شبکه را مختل می‌کنند. تمرکز اصلی پژوهش‌ها بر حملات فعال است، زیرا این حملات تأثیر مستقیمی بر پایداری و کارایی شبکه دارند [۱]، [2].

۲-۵-پیامدهای حملات امنیتی بر عملکرد شبکه

حملات امنیتی می‌توانند موجب کاهش نرخ تحویل بسته، افزایش تأخیر انتها به انتها و افزایش مصرف انرژی گره‌ها شوند. این پیامدها نه‌تنها کیفیت خدمات شبکه را کاهش می‌دهند، بلکه در کاربردهای حساس می‌توانند منجر به از دست رفتن کامل ارتباطات

شوند. بنابراین، بررسی تأثیر حملات بر معیارهای عملکردی، نقش مهمی در ارزیابی شدت تهدیدات امنیتی در MANET دارد [۱]، [۲].

۳-رویکردهای پیشگیری و مقابله با حملات امنیتی در لایه شبکهMANET

۳-۱ -نقش لایه شبکه در امنیتMANET

درMANET ، لایه شبکه مسئول کشف مسیر و انتقال بسته‌ها بین گره‌هاست و به همین دلیل یکی از حیاتی‌ترین لایه‌ها از نظر امنیتی محسوب می‌شود. بسیاری از حملات امنیتی مستقیماً فرآیند مسیریابی را هدف قرار می‌دهند و با دستکاری اطلاعات کنترلی، باعث ایجاد مسیرهای نادرست یا ناپایدار می‌شوند. از این رو، تمرکز بر امنیت لایه شبکه نقش کلیدی در افزایش پایداری و قابلیت اطمینان MANET دارد [۱]، [3].

۳-۲ -حملات رایج لایه شبکه

حملات لایه شبکه معمولاً با هدف اختلال در فرآیند مسیریابی انجام می‌شوند. حملاتی مانندBlackhole ، Floodingو DoSبا ارسال اطلاعات جعلی یا ترافیک غیرعادی، باعث اشباع منابع شبکه یا هدایت نادرست بسته‌ها می‌گردند. این حملات می‌توانند نرخ تحویل بسته را به‌شدت کاهش داده و سربار کنترلی شبکه را افزایش دهند [۱]، [2].

۳-۳ -رویکردهای پیشگیرانه مبتنی بر مسیریابی

در رویکردهای پیشگیرانه، تلاش می‌شود قبل از وقوع یا گسترش حمله، مکانیزم‌هایی در فرآیند مسیریابی اعمال شود. این مکانیزم‌ها شامل اعتبارسنجی پیام‌های کنترلی، بررسی رفتار گره‌ها در ارسال بسته‌ها و اعمال محدودیت بر گره‌های مشکوک هستند. هدف اصلی این روش‌ها کاهش احتمال موفقیت حمله و افزایش مقاومت شبکه در برابر رفتارهای مخرب است[3] .

۳-۴ -تأثیر راهکارهای پیشگیرانه بر عملکرد شبکه

مطالعات نشان می‌دهند که استفاده از مکانیزم‌های پیشگیرانه در لایه شبکه می‌تواند باعث بهبود معیارهایی مانند نرخ تحویل بسته و پایداری مسیر شود. با این حال، اعمال این مکانیزم‌ها اغلب با افزایش سربار کنترلی و مصرف انرژی همراه است. بنابراین، طراحی راهکارهای پیشگیرانه نیازمند ایجاد تعادل میان سطح امنیت و کارایی شبکه است [۳]، [4].

۳-۵ -محدودیت‌ها و چالش‌های رویکردهای لایه شبکه

اگرچه تمرکز بر لایه شبکه می‌تواند امنیت MANET را تا حدی افزایش دهد، اما این رویکردها معمولاً به سناریوهای خاص حمله وابسته هستند و قادر به پوشش تمامی تهدیدات امنیتی نیستند. علاوه بر این، تحرک بالای گره‌ها و تغییرات سریع توپولوژی می‌تواند اثربخشی مکانیزم‌های پیشگیرانه را کاهش دهد [۳].

۴-امنیت مبتنی بر رمزنگاری و مدیریت کلید در شبکه‌هایMANET

۴-۱-تمرکز بر حفاظت از داده درMANET

در برخی رویکردهای امنیتی، به‌جای تمرکز مستقیم بر شناسایی یا حذف گره‌های مخرب، حفاظت از داده‌های در حال انتقال در اولویت قرار می‌گیرد. در این دیدگاه، حتی در صورت حضور گره‌های ناامن در مسیر، محرمانگی و صحت داده‌ها از طریق رمزنگاری تضمین می‌شود. این رویکرد به‌ویژه در کاربردهایی که حساسیت داده بالا است، اهمیت ویژه‌ای دارد[4] .

۴-۲-نقش رمزنگاری در افزایش امنیت مسیریابی

رمزنگاری به‌عنوان یکی از ابزارهای اصلی امنیت، برای تضمین محرمانگی، یکپارچگی و اصالت داده‌ها در MANET به‌کار گرفته می‌شود. با رمزنگاری بسته‌های ارسالی، امکان شنود یا دستکاری داده‌ها توسط گره‌های میانی کاهش می‌یابد. علاوه بر این، استفاده از مکانیزم‌های احراز هویت می‌تواند از جعل پیام‌های کنترلی مسیریابی جلوگیری کند [1]، [4].

۴-۳-چالش‌های مدیریت کلید در محیط MANET

یکی از مهم‌ترین مسائل در استفاده از رمزنگاری درMANET ، مدیریت کلید است. نبود زیرساخت مرکزی، تحرک بالای گره‌ها و تغییر مداوم توپولوژی باعث می‌شود توزیع، به‌روزرسانی و ابطال کلیدها به‌صورت ایمن و کارآمد دشوار باشد. این چالش‌ها باعث می‌شوند بسیاری از روش‌های مدیریت کلید سنتی در MANET قابل استفاده نباشند[4] .

۴-۴-تأثیر رمزنگاری بر عملکرد شبکه

اگرچه استفاده از رمزنگاری سطح امنیت MANET را افزایش می‌دهد، اما سربار محاسباتی و مصرف انرژی گره‌ها را نیز افزایش می‌دهد. این مسئله می‌تواند منجر به افزایش تأخیر و کاهش طول عمر شبکه شود. بنابراین، انتخاب الگوریتم‌های سبک و طراحی مکانیزم‌های مدیریت کلید کارآمد، نقش مهمی در موفقیت این رویکرد دارند[4] .

۴-۵-محدودیت‌های رویکردهای مبتنی بر رمزنگاری

رویکردهای مبتنی بر رمزنگاری معمولاً تمرکز اصلی خود را بر حفاظت از داده‌ها قرار می‌دهند و به‌تنهایی قادر به شناسایی گره‌های مخرب یا جلوگیری از حملات مسیریابی نیستند. به همین دلیل، این روش‌ها اغلب به‌عنوان یک راهکار مکمل در کنار سایر مکانیزم‌های امنیتی مورد استفاده قرار می‌گیرند [۱]، [۴].

۵-رویکردهای مبتنی بر اعتماد (Trust-Based Security) در شبکه‌های MANET

۵-۱-مفهوم اعتماد و نقش آن در امنیت MANET

در شبکه‌های MANET ، به دلیل نبود کنترل مرکزی و مشارکت مستقیم گره‌ها در فرآیند مسیریابی، ارزیابی رفتار گره‌ها اهمیت ویژه‌ای دارد. رویکردهای مبتنی بر اعتماد با هدف سنجش میزان همکاری و صداقت گره‌ها معرفی شده‌اند. در این رویکردها، تصمیم‌گیری‌های امنیتی نه صرفاً بر اساس اطلاعات کنترلی، بلکه بر مبنای رفتار واقعی گره‌ها در شبکه انجام می‌شود [۵]، [6].

۵-۲-معیارهای محاسبه اعتماد گره‌ها

اعتماد در MANET معمولاً بر اساس معیارهایی مانند میزان ارسال صحیح بسته‌ها، همکاری در مسیریابی و رفتار گذشته گره‌ها محاسبه می‌شود. این معیارها می‌توانند از طریق مشاهده مستقیم یا با استفاده از اطلاعات دریافت‌شده از سایر گره‌ها به‌دست آیند. کاهش سطح اعتماد یک گره نشان‌دهنده احتمال رفتار مخرب یا خودخواهانه آن است[5] .

۵-۳-اعتماد متمرکز در مقابل اعتماد توزیع‌شده

برخی رویکردهای مبتنی بر اعتماد از ساختارهای متمرکز یا خوشه‌بندی‌شده استفاده می‌کنند که در آن‌ها گره‌های خاصی مسئول مدیریت و ارزیابی اعتماد هستند. در مقابل، رویکردهای توزیع‌شده تلاش می‌کنند محاسبه اعتماد را بین گره‌ها پخش کنند تا وابستگی به یک نقطه خاص کاهش یابد. هر یک از این روش‌ها مزایا و محدودیت‌های خاص خود را از نظر مقیاس‌پذیری و سربار دارند [۵]، [6].

۵-۴-نقش اعتماد در انتخاب مسیرهای امن

یکی از کاربردهای اصلی مدل‌های اعتماد، انتخاب مسیرهای مسیریابی امن است. در این حالت، مسیرهایی که شامل گره‌های با سطح اعتماد پایین هستند حذف می‌شوند و مسیرهایی با میانگین اعتماد بالاتر در اولویت قرار می‌گیرند. این رویکرد باعث افزایش احتمال انتقال موفق داده‌ها و کاهش تأثیر حملات داخلی می‌شود [۵]، [6].

۵-۵-محدودیت‌ها و چالش‌های رویکردهای مبتنی بر اعتماد

اگرچه مدل‌های مبتنی بر اعتماد در شناسایی گره‌های مخرب داخلی مؤثر هستند، اما با چالش‌هایی مانند سربار محاسباتی، نیاز به زمان برای شکل‌گیری اعتماد و حساسیت به اطلاعات نادرست مواجه‌اند. علاوه بر این، تغییرات سریع توپولوژی MANET می‌تواند دقت مدل‌های اعتماد را کاهش دهد و نیازمند به‌روزرسانی مداوم مقادیر اعتماد باشد [۵]، [۶].

۶-سیستم‌های تشخیص نفوذ (IDS) در شبکه‌هایMANET

۶-۱-جایگاه IDS در چارچوب امنیتMANET

در شبکه‌هایMANET ، بسیاری از حملات از سوی گره‌هایی انجام می‌شوند که عضو شبکه هستند و رفتار آن‌ها در ظاهر عادی به نظر می‌رسد. در چنین شرایطی، رویکردهایی مانند رمزنگاری یا اعتماد به‌تنهایی کافی نیستند و نیاز به مکانیزم‌هایی وجود دارد که بتوانند رفتار شبکه را پایش کرده و فعالیت‌های غیرعادی را شناسایی کنند. سیستم‌های تشخیص نفوذ با هدف شناسایی این رفتارهای مشکوک و مخرب در MANET مطرح شده‌اند[7] .

۶-۲-تفاوت IDS در MANET با شبکه‌های سنتی

IDSهای مورد استفاده در شبکه‌های سنتی معمولاً بر ساختارهای متمرکز و زیرساخت‌های ثابت متکی هستند. این در حالی است که درMANET ، تحرک گره‌ها، تغییر مداوم توپولوژی و نبود نقطه کنترل مرکزی، پیاده‌سازیIDS های متمرکز را با محدودیت جدی مواجه می‌کند. این تفاوت‌ها باعث شده‌اند کهIDS های MANET نیازمند طراحی‌های خاص و سازگار با محیط پویا باشند[7] .

۶-۳IDS-های توزیع‌شده و مبتنی بر خوشه‌بندی

برای غلبه بر محدودیت‌هایIDS های متمرکز، رویکردهای توزیع‌شده و مبتنی بر خوشه‌بندی پیشنهاد شده‌اند. در این روش‌ها، شبکه به چند خوشه تقسیم می‌شود و برخی گره‌ها وظیفه پایش و تحلیل رفتار سایر گره‌ها را بر عهده می‌گیرند. این ساختار باعث کاهش سربار ارتباطی، افزایش مقیاس‌پذیری و بهبود کارایی IDS در MANET می‌شود[7] .

۶-۴-انواع رفتارهای قابل تشخیص توسطIDS

IDSهای مورد استفاده در MANET قادر به شناسایی رفتارهایی مانند حذف گزینشی بسته‌ها، ارسال ترافیک غیرعادی، عدم همکاری در مسیریابی و الگوهای رفتاری مشکوک هستند. با تحلیل این رفتارها، گره‌های مخرب شناسایی شده و می‌توان اقدامات اصلاحی مانند محدودسازی یا حذف آن‌ها از فرآیند مسیریابی را اعمال کرد[7] .

۶-۵-چالش‌ها و محدودیت‌های IDS درMANET

با وجود مزایای IDS، پیاده‌سازی آن در MANET با چالش‌هایی همراه است. مصرف انرژی، سربار محاسباتی، انتخاب گره‌های نظارتی مناسب و تأثیر تحرک گره‌ها بر دقت تشخیص از جمله این چالش‌ها هستند. این محدودیت‌ها نشان می‌دهند که IDS معمولاً به‌عنوان بخشی از یک چارچوب امنیتی ترکیبی مورد استفاده قرار می‌گیرد، نه به‌عنوان یک راهکار مستقل [۷].

۷-رویکردهای هوشمند و مبتنی بر یادگیری ماشین در امنیت شبکه‌های MANET

۷-۱-ضرورت استفاده از روش‌های هوشمند در امنیتMANET

پیچیدگی و پویایی بالای شبکه‌های MANET باعث شده است که بسیاری از روش‌های سنتی امنیتی در شناسایی دقیق و به‌موقع حملات با محدودیت مواجه شوند. تغییر مداوم الگوهای ترافیکی، ظهور حملات جدید و رفتارهای پیچیده گره‌های مخرب، نیاز به رویکردهایی تطبیق‌پذیر و هوشمند را برجسته می‌سازد. در این راستا، یادگیری ماشین به‌عنوان ابزاری کارآمد برای تحلیل الگوهای رفتاری در MANET مطرح شده است[8] .

۷-۲-کاربرد یادگیری ماشین در تشخیص حملات

در رویکردهای مبتنی بر یادگیری ماشین، مدل‌های مختلف با استفاده از داده‌های رفتاری شبکه آموزش داده می‌شوند تا بتوانند الگوهای عادی و غیرعادی را از یکدیگر تشخیص دهند. این مدل‌ها قادرند با تحلیل ویژگی‌هایی مانند الگوی ارسال بسته‌ها، تأخیر، نرخ ریزش بسته و رفتار مسیریابی گره‌ها، حملات امنیتی را شناسایی کنند. چنین قابلیتی امکان تشخیص حملات ناشناخته یا ترکیبی را نیز فراهم می‌سازد[8] .

۷-۳-یکپارچگی یادگیری ماشین با سیستم‌های تشخیص نفوذ

بخش قابل توجهی از رویکردهای مبتنی بر یادگیری ماشین در قالب سیستم‌های تشخیص نفوذ پیاده‌سازی می‌شوند. در این حالت، یادگیری ماشین نقش هسته تصمیم‌گیری IDS را ایفا می‌کند و فرآیند تشخیص را از حالت قانون‌محور به حالت داده‌محور منتقل می‌سازد. این یکپارچگی می‌تواند دقت تشخیص را افزایش داده و نرخ هشدارهای نادرست را کاهش دهد [۷]، [8].

۷-۴-مزایای رویکردهای مبتنی بر یادگیری ماشین

از مهم‌ترین مزایای این رویکردها می‌توان به توانایی تطبیق با شرایط پویا، شناسایی الگوهای پیچیده و تشخیص حملات جدید اشاره کرد. برخلاف روش‌های سنتی که به قواعد از پیش تعریف‌شده متکی هستند، مدل‌های یادگیری ماشین می‌توانند با یادگیری مستمر، خود را با تغییرات شبکه سازگار کنند. این ویژگی برای محیط‌هایی مانند MANET اهمیت ویژه‌ای دارد[8] .

۷-۵-محدودیت‌ها و چالش‌های عملی

با وجود مزایای قابل توجه، استفاده از یادگیری ماشین در MANET با چالش‌هایی نیز همراه است. نیاز به داده‌های آموزشی مناسب، سربار محاسباتی بالا، مصرف انرژی بیشتر و دشواری پیاده‌سازی مدل‌های پیچیده بر روی گره‌های با منابع محدود از جمله این چالش‌ها هستند. این محدودیت‌ها باعث می‌شوند که استفاده عملی از روش‌های مبتنی بر یادگیری ماشین نیازمند بهینه‌سازی و ترکیب با سایر رویکردهای امنیتی باشد [۸].

عنوان مقاله	مزایا و نقاط قوت	معایب و چالشها
Routing Protocols, Attacks and Mitigation Techniques	پوشش جامع پروتکل‌های مسیریابی و حملات امنیتی؛ ارائه طبقه‌بندی ساخت‌یافته از حملات و راهکارها	عدم ارائه مدل یا مکانیزم امنیتی جدید؛ نبود ارزیابی شبیه‌سازی یا تحلیل عددی
Analysis on Essential Challenges and Attacks	تحلیل عمیق چالش‌های ذاتی ؛ تمرکز بر ریشه‌های ساختاری ناامنی	عدم ارائه راهکار عملی؛ محدود بودن به تحلیل مفهومی
A Comprehensive Mechanism of MANET…	تمرکز مشخص بر لایه شبکه؛ بررسی حملات مسیریابی و روش‌های پیشگیرانه	افزایش سربار کنترلی؛ وابستگی به سناریوهای خاص حمله
Data Security-Based Routing in MANETs…	تضمین محرمانگی و یکپارچگی داده؛ استفاده از رمزنگاری در مسیریابی	مشکل مدیریت کلید؛ سربار محاسباتی و مصرف انرژی بالا
A Study on Improving Secure Routing…	شناسایی گره‌های مخرب داخلی؛ بهبود عملکرد مسیریابی با Trust	وابستگی به گره مدیریت اعتماد؛ کاهش مقیاس‌پذیری
Establishing Secure Routing Path Using Trust..	مدل Trust توزیع‌شده؛ استفاده از مشاهدات مستقیم و غیرمستقیم	پیچیدگی محاسبات Trust؛ افزایش تأخیر در مسیریابی
Distributed Clustering Algorithm Based IDS...	تشخیص مؤثر حملات با IDS؛ کاهش سربار با خوشه‌بندی	حساسیت به تحرک گره‌ها؛ چالش انتخاب سرخوشه
Machine Learning Based Security Solutions	دقت بالای تشخیص؛ قابلیت شناسایی حملات ناشناخته	نیاز به داده آموزشی؛ سربار محاسباتی و انرژی بالا

جدول ۱: قایسه مزایا و معایب روش‌های امنیتی ارائه‌شده درMANET

بحث و نتیجه گیری

بررسی مقالات انجام‌شده در حوزه امنیت شبکه‌های MANET نشان می‌دهد که ماهیت پویا، توزیع‌شده و بدون زیرساخت این شبکه‌ها، امنیت را به یکی از چالش‌های اساسی و پیچیده تبدیل کرده است. مطالعات مرورشده رویکردهای متنوعی از جمله پیشگیری در لایه شبکه، رمزنگاری و مدیریت کلید، مدل‌های مبتنی بر اعتماد، سیستم‌های تشخیص نفوذ و روش‌های مبتنی بر یادگیری ماشین را برای مقابله با تهدیدات امنیتی پیشنهاد کرده‌اند. هر یک از این رویکردها توانسته‌اند بخشی از مشکلات امنیتی MANETرا کاهش دهند، اما همگی با محدودیت‌هایی نظیر سربار محاسباتی، مصرف انرژی، کاهش مقیاس‌پذیری یا وابستگی به سناریوهای خاص حمله مواجه هستند. این موضوع نشان می‌دهد که تاکنون راهکار جامع و یکپارچه‌ای برای تأمین امنیت کامل MANETارائه نشده است. در نتیجه، می‌توان نتیجه گرفت که ترکیب هوشمندانه چند رویکرد امنیتی و طراحی مکانیزم‌های تطبیق‌پذیر متناسب با ویژگی‌های ذاتیMANET، مسیر اصلی پژوهش‌های آینده در این حوزه خواهد بود.

منابع

[1] Sharma, N. and Verma, A. K. (2022). MANET routing protocols, attacks and mitigation techniques: A review. International Journal of Computer Networks and Communications.

[2] Patel, R. and Gupta, S. K. (2021). Analysis on essential challenges and attacks on MANET. Journal of Wireless Networking and Communications.

[3] Kumar, A. and Rana, P. S. (2020). A comprehensive mechanism of MANET network layer based security attack prevention. International Journal of Network Security.

[4] Singh, H. and Chauhan, R. K. (2019). Data security-based routing in MANETs using key management. Journal of Information Security and Applications.

[5] Mehta, V. and Patel, N. (2018). A study on improving secure routing performance using trust model in MANET. International Journal of Ad Hoc and Ubiquitous Computing.

[6] Kaur, S. and Sood, A. K. (2019). Establishing secure routing path using trust to enhance security in MANET. Journal of Network and Computer Applications.

[7] Rahman, M. S. and Islam, M. S. (2020). A hybrid efficient distributed clustering algorithm based IDS to enhance security in MANET. Computer Communications.

[8] Alotaibi, S. and Alzahrani, M. A. (2021). Machine learning based security solutions in MANETs: State of the art. IEEE Access.