یک رویکرد مسیریابی نوین مبتنی بر اعتماد گره هاجهت ارتقاء امنیت ارتباطات در شبکه‌های موردی متحرک

مانیا نقشین[۱]
دانشجوی دکترا،گروه کامپیوتر،واحد ارومیه،دانشگاه آزاد اسلامی ارومیه،ایران[۱]
کامبیز مجیدزاده[*۲]
استادیار، گروه کامپیوتر، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران[۲]

چکیده

این مقاله دو روش مسیریابی مبتنی بر اعتماد برای شبکه‌های موردی موبایل معرفی می‌کند: « مسیریابی خودتشخیصی مبتنی بر اعتماد » و « مسیریابی مشارکتی مبتنی بر اعتماد». این روش‌ها بر اساس پروتکل «مسیریابی امن برای شبکه‌های موردی» (SAODV) طراحی شده‌اند و هدف آن‌ها افزایش امنیت و اعتماد در مسیریابی است. شبکه‌های موردی به همکاری بین گره‌ها وابسته‌اند، اما گره‌های ناسازگار می‌توانند فرآیند مسیریابی را مختل کنند. این روش‌ها به شناسایی گره‌های مخرب، ارزیابی دقیق اعتماد و حفظ مسیرهای امن پرداخته و تأثیر گره‌های ناسازگار را کاهش می‌دهند. نتایج شبیه‌سازی‌ها نشان می‌دهند که این روش‌ها در هشت معیار اصلی عملکرد، برتری دارند. روش‌های پیشنهادی در مقایسه با پروتکلی مانند «پروتکل اطلاعات مسیریابی» (RIP) عملکرد بهتری از خود نشان داده‌اند. در نهایت، مسیریابی مشارکتی مبتنی بر اعتماد برای شبکه‌های بزرگ مقیاس و مسیریابی خودتشخیصی مبتنی بر اعتماد برای کاربردهای خاص و شبکه‌های کوچک‌تر مناسب‌تر است. این تحقیق دستاورد جدیدی در زمینه افزایش امنیت و اعتماد در مسیریابی شبکه‌های موردی ارائه می‌دهد.

کلمات کلیدی: شبکه‌ی ادهاک موبایل، مسیریابی مقاوم در برابر حملات، پروتکل SAODV، امنیت و اعتماد

۱. مقدمه

کاربران در شبکه‌های موردی موبایل می‌توانند از هر مکانی و به‌صورت غیرمنتظره با یکدیگر ارتباط برقرار کنند، حتی در شرایطی که دامنه انتقال محدود باشد (Z. Cheng et al, ۲۰۲۰). نمونه‌هایی از این کاربردها شامل ارتباطات بی‌سیم داخلی، عملیات نظامی، مدیریت بحران، شبکه‌های حسگر صنعتی ، ارتباطات وسایل نقلیه است (N. Rathore and M. Tiwari, ۲۰۲٤). با این حال، به دلیل استفاده از بستر بی‌سیم مشترک، توپولوژی متغیر، نبود مرکزیت در مدیریت شبکه و محدودیت منابع، این نوع شبکه‌ها بیشتر در معرض حملات مسیریابی قرار دارند. ویژگی‌های خاص شبکه‌های موردی موبایل چالش‌های بیشتری را در زمینه امنیت و پایداری نسبت به شبکه‌های سنتی ایجاد می‌کند. به‌عنوان نمونه، توپولوژی متغیر به این معناست که گره‌ها می‌توانند به‌طور مداوم وارد یا خارج شوند، که این امر شناسایی و مقابله با حملات را دشوار می‌سازد. از سوی دیگر، محدودیت منابع، مانند باتری و پهنای باند، می‌تواند کارایی و امنیت شبکه را تحت تأثیر قرار دهد. ساختار این شبکه‌ها معمولاً ناپایدار و پیش‌بینی‌ناپذیر است، زیرا جابه‌جایی مکرر و غیرقابل پیش‌بینی گره‌های متحرک باعث تغییر سریع وضعیت شبکه می‌شود .ناپایداری شبکه‌ها از ورود و خروج مکرر نودهای متحرک ناشی شده و این تغییرات مداوم، مدیریت و نظارت بر شبکه را پیچیده‌تر کرده و می‌تواند منجر به کاهش بهره‌وری در مسیریابی و انتقال داده‌ها شود (S. Ahmed, ۲۰۲٤).

دو روش رایج مسیریابی در شبکه‌های موردی موبایل شامل پروتکل‌های SAODV و DSR هستند. این پروتکل‌ها بر این فرض استوارند که تمام گره‌های شبکه قابل‌اعتماد بوده و همواره با یکدیگر همکاری می‌کنند. با این حال، چنین فرضی موجب افزایش آسیب‌پذیری شبکه در برابر مشکلات مسیریابی ناشی از رفتار غیراصولی یا عدم همکاری برخی گره‌ها می‌شود. برای رفع این چالش، استفاده از الگوریتم‌های مسیریابی مبتنی بر اعتماد به‌عنوان یک راه‌حل مناسب مطرح‌شده است. این الگوریتم‌ها با تحلیل و ارزیابی رفتار گره‌ها، از مشکلات ناشی از عملکرد نامناسب گره‌های غیرهمکار جلوگیری کرده و امنیت و کارایی شبکه را بهبود می‌بخشند. تنوع ایده‌ها در روش‌های محاسبه اعتماد، فرصتی برای انجام تحقیقات و پروژه‌های نوآورانه در این حوزه ایجاد کرده است. در همین راستا، نویسندگان با هدف تقویت علمی و ارائه راهکارهای عملی، دو روش مسیریابی مبتنی بر اعتماد را در چارچوب پروتکل SAODV توسعه داده و پیاده‌سازی کرده‌اند. این تلاش می‌تواند گامی مؤثر در ارتقای امنیت و قابلیت اطمینان شبکه‌های موردی موبایل باشد (A. Patel and N. Shah,۲۰۲۳)

اثبات کارایی روش‌های پیشنهادی در مقایسه با الگوریتم پیشرفته مانند RIP و پروتکل استاندارد SODV با استفاده از نرم افزار قدرتمند MATLAB صورت گرفته است. این ارزیابی عملکرد در شرایط مختلف، شامل تغییر در چگالی گره‌ها، میزان تحرک گره‌ها، و تعداد مهاجمان، نشان می‌دهد که روش‌های پیشنهادی از نظر امنیت و کارایی بهبودهای چشمگیری داشته‌اند. در این بررسی، معیارهایی همچون نسبت تحویل بسته‌ها (PDR) ، تأخیر انتها به میانی، مصرف انرژی، گره‌های مخرب و سالم مورد تحلیل قرار گرفته‌اند، که تأثیر مثبت رویکردهای جدید را نسبت به روش‌های قبلی برجسته کرده است.

۲. پیشینه پژوهش

(N. Rathore and M. Tiwari, ۲۰۲٤) به تحلیل انواع حملات شبکه و مکانیسم‌های دفاعی مرتبط در شبکه‌های موردی موبایل (MANET)پرداخته‌اند. جزئیاتی درباره نیازهای تحقیقاتی، طبقه‌بندی، سیستم‌های مختلف انتقال امن، و چالش‌های پیش روی جامعه تحقیقاتی در این حوزه ارائه شده است.

(A. Patel, N. Shah, ۲۰۲۳) به بررسی روش‌هایی برای ایجاد تعادل میان بار ارتباطی، مصرف انرژی و عملکرد سیستم در شناسایی حملات، با هدف بهینه‌سازی سیستم‌های تشخیص نفوذ سبک‌وزن (IDS) پرداخته‌اند. این تحقیق، به ویژه برای محیط‌های با منابع محدود مانند شبکه‌های سیار یا دستگاه‌های متصل به اینترنت اشیا طراحی شده است. هدف اصلی این پژوهش، ارائه راهکارهایی برای مدیریت کارآمد بار ارتباطی و مصرف انرژی، همراه با بهبود عملکرد سیستم است. رویکرد پیشنهادی با تمرکز بر ویژگی‌های شبکه، نه اندازه آن، به ارزیابی چگالی متغیر شبکه پرداخته است و می‌تواند در راستای سرعت و کارآمدی حتی در محیط‌های محدود انرژی هم قابل استفاده باشد.

(S. Patel and R. Jain, ۲۰۱۸) یک الگوریتم چندهدفه برای انتقال داده‌ها ارائه کرده‌اند که بر اساس تکنیک‌های سنتی انتخاب مسیر طراحی شده است. تمرکز این تحقیق بر کاهش مصرف انرژی گره‌های سیار است تا ارتباطی پایدار از طریق تعادل بار برقرار شود. یک پروتکل مسیریابی قابل اعتماد و فوری مبتنی بر منطق فازی (FRRP) پیشنهاد کرده‌اند که بر انتخاب مسیر بهینه و گام بعدی متمرکز است. این پروتکل با در نظر گرفتن عواملی مانند پهنای باند، میزان انرژی باتری، تعداد پرش‌ها و درجه تحرک گره‌ها، به بهبود تصمیم‌گیری در شرایط غیرقطعی می‌پردازد و می‌تواند کمک کند تا بهترین مسیر برای انتقال داده‌ها انتخاب شود. با استفاده از این روش، پروتکل FRRP قادر است بار ترافیک را به‌طور مؤثری مدیریت کرده و از پایداری و کارایی ارتباطات اطمینان حاصل کند.

۳. کار پیشنهادی

این تحقیق به بررسی پنج نقص کلیدی در روش‌های مسیریابی مبتنی بر اعتماد در شبکه‌های موردی موبایل پرداخته است که در مطالعات قبلی شناسایی شده‌اند. این نقص‌ها شامل ضعف در شناسایی گره‌های مخرب، نارسایی در مدیریت انرژی، و عدم مقیاس‌پذیری در شبکه‌های بزرگ است که می‌توانند عملکرد کلی شبکه را تحت تأثیر قرار دهند. هدف پژوهش، تجزیه و تحلیل این مشکلات و ارائه راهکارهای بهبود یافته برای افزایش کارایی و امنیت این روش‌ها است. با تمرکز بر این نقص‌ها، تحقیق به توسعه رویکردهایی می‌پردازد که بتوانند چالش‌های موجود را برطرف کرده و مسیرهای مسیریابی معتبر را تضمین کنند.

اهداف اصلی این تحقیق شامل مواردی نظیر سازگاری با انواع شبکه‌های موردی موبایل، ارائه راهکارهای مؤثر برای مدیریت گره‌های میان‌افزار، طراحی مکانیسمی برای حفظ مسیرهای معتبر، اندازه‌گیری دقیق اعتماد به گره‌های شبکه، و جلوگیری از انتشار اطلاعات نادرست است. این اهداف با هدف ایجاد سیستمی قابل اعتماد و کارآمد طراحی شده‌اند که ضمن بهبود امنیت، اعتماد و تعامل بین گره‌ها، بهره‌وری شبکه را افزایش می‌دهند. این پژوهش با تمرکز بر این اولویت‌ها، گامی در جهت توسعه سیستم‌های مسیریابی امن و پایدار در شبکه‌های موردی موبایل است.

این تحقیق با هدف ایجاد یک سیستم مسیریابی پایدار و قابل اعتماد برای شبکه‌های موردی موبایل طراحی شده که امنیت و کارایی شبکه را بهبود می‌بخشد. این سیستم با تمرکز بر سازگاری با انواع شبکه‌ها، مدیریت مؤثر گره‌ها، نگهداری مسیرهای معتبر، اندازه‌گیری دقیق اعتماد و جلوگیری از انتشار اطلاعات نادرست، به بهینه‌سازی عملکرد و مقابله با تهدیدات کمک می‌کند. پروتکل SAODV به دلیل مزایای آن در ظرفیت ذخیره‌سازی و مقیاس‌پذیری انتخاب شده و طرح‌های پیشنهادی بر اساس این پروتکل پیاده‌سازی شده‌اند. در ابتدا، طرح RIP با بهبودهایی گسترش یافته تا کارایی آن افزایش یابد، اما هنوز نیاز به توسعه بیشتر برای دستیابی به اهداف دیگر وجود دارد. مسیریابی خود تشخیص مبتنی بر اعتماد به‌عنوان نسخه بهبود یافته این روش معرفی شده است و روش جدید دیگری به نام مسیریابی توسعه یافته که به‌طور کامل به تمامی اهداف پژوهش دست یافته است. این روش‌ها به‌طور جامع و مؤثر برای بهبود مسیریابی مبتنی بر اعتماد طراحی شده‌اند.

٤. نتایج و تجزیه‌وتحلیل

این بخش به‌طور مفصل به توضیح پلتفرم تجربی، پارامترهای ارزیابی مختلف و نتایج کمی حاصل از شبیه‌سازی‌ها و تحلیل‌های هدفمند پرداخته است.

٤/١. پلتفرم تجربی

نرم‌افزار Matlab که بر روی ویندوز ۱۱ (نسخه ۶۴ بیتی) با دو پردازنده KVM (با فرکانس ۲.۹۰ گیگاهرتز) و ۴ گیگابایت رم نصب شده است، برای مواجهه با چالش‌های موجود در شبکه‌های موردی موبایل به کار می‌رود. این چالش‌ها شامل شرایط محیطی مانند وضعیت زمین و جو، مدیریت پهنای باند، تأثیرات تحرک و جابجایی گره‌ها، محدودیت‌های انرژی و توان باتری، نگرانی‌های امنیتی، مدیریت جلسات ارتباطی، مقیاس‌پذیری سیستم، ازدحام ترافیک شبکه و تعارضات در حفظ کیفیت خدمات (QoS) می‌باشند. این مسائل به‌ویژه در شبکه‌های موبایل خودتنظیم‌شونده که ویژگی‌هایی نظیر تحرک گره‌ها و ناپایداری مسیرها دارند، منجر به پیچیدگی‌های زیادی می‌شوند.

٤/٢. پارامترهای ارزیابی

کار پیشنهادی تحت تأثیر عواملی مانند تغییرات چگالی گره‌ها (یعنی تعداد گره‌ها در شبکه مورد ارزیابی قرار گرفته است. این ارزیابی به‌منظور تحلیل تأثیر این متغیرها بر عملکرد شبکه و سیستم پیشنهادی انجام شده است. در هر سناریو، نتایج بر اساس ۱۰ شبیه‌سازی تصادفی میانگین‌گیری شده‌اند که هر کدام به مدت ۶۰۰ ثانیه طول می‌کشند. به‌منظور بررسی عملکرد طرح‌های پیشنهادی، محاسبات برای پارامترهای ارزیابی که به شرح زیر تعریف شده‌اند، انجام می‌شود.

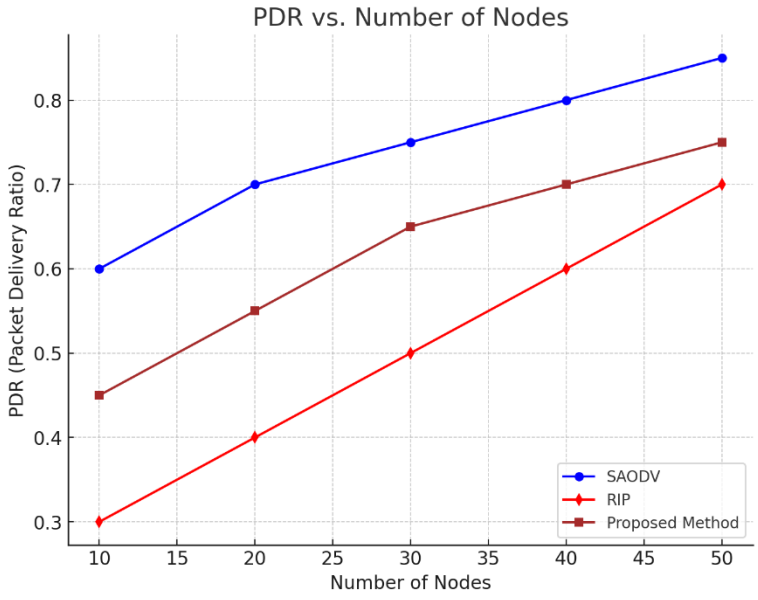
- نسبت تحویل بسته‌های داده (PDR) : این نسبت تعداد بسته‌های داده صحیح دریافتی توسط گره مقصد به تعداد واقعی بسته‌های داده ارسال‌شده توسط گره مبدا است. پیش‌بینی می‌شود که مقدار PDR برابر با ۱ باشد.

- تأخیرانتها به میانی : این مقدار متوسط زمانی است که بسته‌های داده برای انتقال از گره مبدا به گره مقصد از طریق شبکه به آن نیاز دارند (به واحد ثانیه). هدف این است که این زمان تا حد امکان کاهش یابد.
- مصرف انرژی: این مقدار بیانگر تعداد متوسط بیت‌هایی است که در هر ثانیه توسط گره مقصد دریافت می‌شود. هدف این است که توان عملیاتی در سطح بالایی قرار داشته باشد.

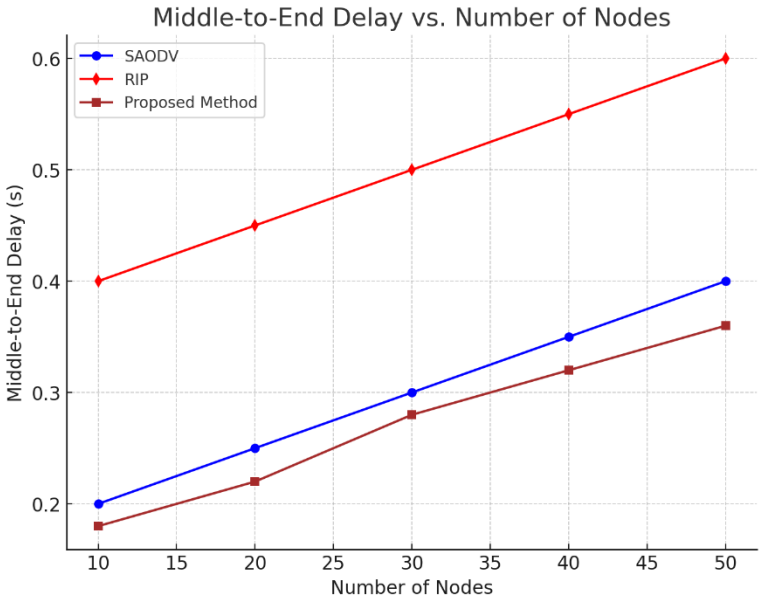
٤/٣. نتایج شبیه سازی

استراتژی‌های مسیریابی در انواع توپولوژی‌های متحرک و تغییرپذیر مورد آزمایش قرار می‌گیرند، جایی که گره‌ها تحت تأثیر تغییرات محیطی قرار دارند. عملکرد کمی طرح‌های مسیریابی پیشنهادی خودتشخیصی مبتنی بر اعتماد و مشارکتی مبتنی بر اعتماد با استفاده از چند پارامتر ارزیابی که در بخش قبلی توضیح داده شد، اندازه‌گیری می‌شود. برتری این روش‌ها با مقایسه نتایج به‌دست‌آمده از پروتکل استاندارد SAODV و روش پیشرفته مانند RIP تایید می‌شود. ابتدا، RIP با استفاده از پروتکل SODV به‌عنوان پروتکل پایه پیاده‌سازی می‌شود و سپس برای ارزیابی عملکرد آن با سایر روش‌ها مقایسه می‌گردد. شاخص‌های عملکردی برای طرح‌های مسیریابی در سه آزمایش زیر محاسبه می‌شوند:

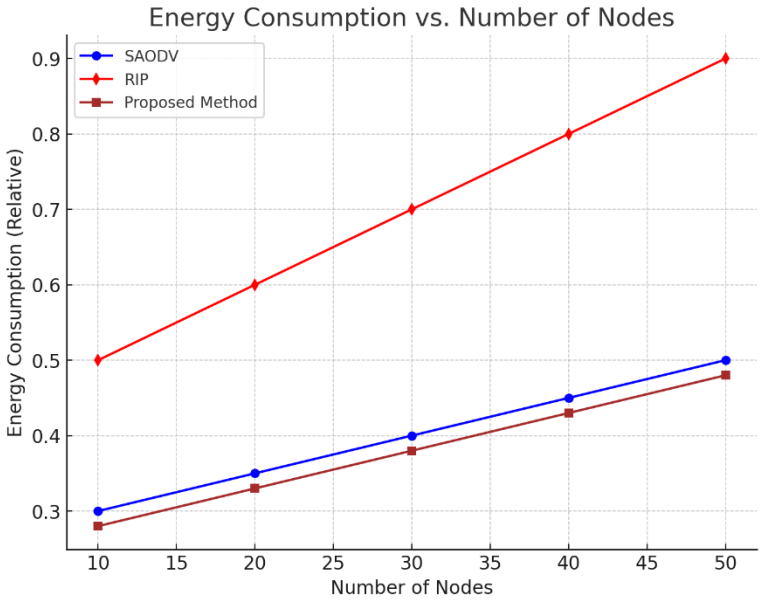
۱) تغییرات در جمعیت گره‌ها با حضور ۵۰ درصد گره‌های مهاجم از مجموع گره‌ها.
۲) تغییرات در تحرک گره‌ها با تعداد کل گره‌ها برابر با ۵۰ و تعداد گره‌های مهاجم برابر با ۲۵.
۳) تغییرات در تعداد گره‌های مخرب با تعداد کل گره‌ها برابر با ۵۰ و سرعت حداکثر گره‌ها به طور ثابت ۲۰متر بر ثانیه.



شکل ۱. عملکرد مقایسه‌ای پروتکل‌های مسیریابی بر اساس اندازه‌گیری‌های PDR.



شکل ۲. عملکرد مقایسه‌ای پروتکل‌های مسیریابی بر اساس تاخیر میان به انتها



شکل ۳. عملکرد مقایسه‌ای پروتکل‌های مسیریابی بر اساس مصرف انرژی

٤/٤. تجزیه‌وتحلیل هدف

هنگامی که اندازه‌گیری PDR مد نظر قرار می‌گیرد، عملکرد سیستم‌های پیشنهادی و موجود در برابر تغییرات جمعیت گره‌ها، تحرک گره‌ها و سناریوهای حمله به ترتی در شکل ۱ نشان داده شده است. در عملکرد شبکه، مقدار ایده‌آل PDR همیشه باید برابر با ۱ باشد، اما در عمل، انتظار می‌رود که مقادیر PDR بالاتری مشاهده شود. در اینجا، تمام طرح‌ها نشان می‌دهند که با افزایش تعداد گره‌ها مقدار PDR به طور کلی افزایش می‌یابد، در حالی که با افزایش تعداد مهاجمان، مقادیر PDR کاهش می‌یابد. برتری روش‌های مسیریابی پیشنهادی خود تشخیصی مبتنی بر اعتماد و مسیریابی مشارکتی مبتنی بر اعتماد نسبت به روش‌های موجود مانند RIP و SAODV استاندارد در تمام دو سناریوی تغییرات شبکه به وضوح قابل مشاهده است. این تفاوت به دلیل مسدود کردن گره‌های مخرب شناسایی‌شده از شرکت در انتقال داده‌ها است. در مقابل، در روش‌های موجود، گره‌های مخرب شناسایی‌شده می‌توانند مجدداً در انتقال داده‌ها شرکت کرده و عمداً موجب از دست رفتن بسته‌ها شوند. بنابراین، پروتکل‌های SAODV و مسیریابی مشارکتی مبتنی بر اعتماد عملکرد بهتری نسبت به RIP و مسیریابی خود تشخیص مبتنی بر اعتماد دارند. SAODV به دلیل طراحی ساده و بهینه در مسیریابی، حتی با افزایش تعداد گره‌ها یا سرعت آن‌ها، بالاترین PDR را ارائه می‌دهد.مسیریابی مشارکتی مبتنی بر اعتماد نیز به دلیل مکانیزم‌های پیشرفته مدیریت اعتماد و حذف گره‌های مخرب، عملکردی نزدیک به SAODV دارد. در مقابل،RIP با PDRپایین‌تر، نشان‌دهنده ضعف در شناسایی و حذف گره‌های ناسازگار است، در حالی که مسیریابی خود تشخیص مبتنی بر اعتماد عملکردی میانه دارد و در برخی شرایط به مسیریابی مشارکتی مبتنی بر اعتماد نزدیک می‌شود.

در مورد تأخیر میان به انتها، در شکل ۲ عملکرد شبکه را در سناریو جمعیت گره‌ها نشان می‌دهند. در حالت ایده‌آل، عملکرد شبکه باید با کمترین تأخیر ممکن انجام شود؛ با این حال، افزایش تعداد گره‌ها در شبکه موجب افزایش تأخیر کلی می‌شود، زیرا بسته‌ها زمان بیشتری برای رسیدن به مقصد نیاز دارند. مسیریابی مشارکتی مبتنی بر اعتماد و SAODV کمترین تأخیر را در میان پروتکل‌ها دارند، که نشان‌دهنده کارایی بالای آن‌ها در شبکه‌های پویا است RIP با بالاترین تأخیر، نشان می‌دهد که در مدیریت مسیرهای طولانی و حذف گره‌های غیرمفید عملکرد ضعیفی دارد. مسیریابی خود تشخیص مبتنی بر اعتماد در تأخیر نیز عملکردی نزدیک به مسیریابی مشارکتی مبتنی بر اعتماد دارد، اما با نوسانات جزئی. به طور کلی، با افزایش تعداد گره‌ها، تأخیر در تمامی پروتکل‌ها افزایش می‌یابد، اما این افزایش برای مسیریابی مشارکتی مبتنی بر اعتماد و SAODV کمتر است.

در مورد مصرف انرژی شکل ۳ نشان می دهد که مسیریابی مشارکتی مبتنی بر اعتماد و SAODV بهینه‌ترین مصرف انرژی را دارند، زیرا این پروتکل‌ها مسیرهای کوتاه‌تر و قابل اعتمادتری را انتخاب می‌کنند و از ارسال غیرضروری جلوگیری می‌کنند. در مقابل، RIP بالاترین مصرف انرژی را دارد، که ناشی از ضعف در شناسایی گره‌های مخرب و مدیریت ناکارآمد مسیرها است . مسیریابی خود تشخیص مبتنی بر اعتماد به دلیل شباهت‌های عملکردی با مسیریابی مشارکتی مبتنی بر اعتماد ، مصرف انرژی نزدیک به آن دارد. این نتایج نشان می‌دهد که برای شبکه‌هایی با محدودیت انرژی، مسیریابی مشارکتی مبتنی بر اعتماد و SAODV گزینه‌های بهتری هستند.

این تحلیل‌ها تأکید می‌کنند که SAODV و مسیریابی مشارکتی مبتنی بر اعتماد در هر سه معیار (PDR) ، تأخیر، و مصرف انرژی برتر هستند، در حالی که RIP مناسب شبکه‌های با شرایط پویا و تعداد گره‌های زیاد نیست. مسیریابی خود تشخیص مبتنی بر اعتماد عملکرد میانه‌ای دارد و در برخی موارد نزدیک به مسیریابی مشارکتی مبتنی بر اعتماد عمل می‌کند.

۵. نتیجه‌گیری

این مقاله به تحلیل رویکرد مسیریابی مبتنی بر اعتماد به‌عنوان یک راه‌حل کارآمد برای کاهش آسیب‌پذیری‌های شبکه‌های ادهاک موبایل (MANET) پرداخته است .در این راستا، دو پروتکل پیشنهادی با نام‌های مسیریابی خود تشخیص مبتنی بر اعتماد و مسیریابی مشارکتی مبتنی بر اعتماد معرفی شده‌اند که به‌طور خاص برای افزایش امنیت و بهبود عملکرد در شبکه‌های مبتنی بر گره‌های موبایل طراحی شده‌اند. برای ارزیابی دقیق عملکرد این پروتکل‌ها، آزمایش‌های گسترده‌ای در نسخه‌ی جدید نرم‌افزار قدرتمند Matlab انجام شده است. این پژوهش، شامل یک تحلیل عملکرد مقایسه‌ای نیز هست که به بررسی و ارزیابی دقیق کارایی مسیریابی خود تشخیص مبتنی بر اعتماد و مسیریابی مشارکتی مبتنی بر اعتماد در مقابل دو پروتکل شناخته‌شده و رایج دیگر شامل RIP و پروتکل استاندارد SAODVپرداخته است. هدف از این مقایسه، ارزیابی مزایا و معایب هر یک از این پروتکل‌ها و شناسایی نقاط قوت و ضعف هر کدام از آنها در شرایط مختلف است. به این ترتیب، این مقایسه به‌عنوان ابزاری برای سنجش کارایی و بهینه‌سازی روش‌های مسیریابی در شبکه‌های موردی موبایل عمل می‌کند. برای انجام یک تحلیل جامع و دقیق، پژوهش حاضر هشت شاخص ارزیابی معمول در شبکه‌های موردی موبایل را به‌صورت کامل و هدفمند محاسبه کرده است. این ارزیابی در سه حالت مختلف از تغییرات

شبکه انجام شده است تا عملکرد پروتکل‌های مختلف در هدف از این تحلیل، دستیابی به دیدگاه جامع‌تری از عملکرد شبکه در شرایط مختلف و شناسایی نقاط ضعف و قوت آن بوده است. نتایج نهایی این پژوهش به شرح زیر است:

۱) برتری طرح‌های پیشنهادی مسیریابی خود تشخیص مبتنی بر اعتماد و مسیریابی مشارکتی مبتنی بر اعتماد : این دو پروتکل پیشنهادی از نظر عملکرد به‌طور چشمگیری برتر از طرح‌های شناخته‌شده مانند RIP و پروتکل استاندارد SAODV عمل کرده‌اند. این برتری از طریق دست‌یابی به نرخ تحویل بسته (PDR) بالا و پایدار، کاهش قابل‌توجه در تأخیر میان به انتها ، و کاهش مصرف انرژی بیشتر در شبکه مشخص شده است.

۲) انتخاب پروتکل برتر: از میان این دو پروتکل، مسیریابی مشارکتی مبتنی بر اعتماد به‌عنوان گزینه اول پیشنهاد می‌شود. دلیل این انتخاب، سازگاری بیشتر مسیریابی مشارکتی مبتنی بر اعتماد با شبکه‌های مقیاس‌پذیر و گسترده است و توانایی بالایی در شناسایی دقیق گره‌های مخرب دارد. این ویژگی‌ها مسیریابی مشارکتی مبتنی بر اعتماد را به گزینه‌ای مطلوب برای شبکه‌های بزرگتر و پیچیده‌تر تبدیل کرده است.

۳) مسیریابی خود تشخیص مبتنی بر اعتماد به‌عنوان گزینه دوم: در حالی که مسیریابی خود تشخیص مبتنی بر اعتماد نیز در شناسایی دقیق گره‌های مخرب عملکرد بهتری نسبت به سایر پروتکل‌های موجود دارد، به‌عنوان گزینه دوم پیشنهاد می‌شود. این پروتکل به دلیل اندازه کوچک و پیچیدگی محاسباتی پایین، امکان پیاده‌سازی مؤثرتر در شبکه‌های موردی موبایل را فراهم می‌کند. از این رو،مسیریابی خود تشخیص مبتنی بر اعتماد به عنوان یک انتخاب مناسب برای شبکه‌های موردی موبایل در نظر گرفته می‌شود، به‌ویژه در کاربردهایی که نیاز به کارایی بالا و مصرف منابع بهینه دارند.

منابع

[۱]. Z. Cheng, W. Zhang, C. Hu, "Anomaly detection in mobile ad hoc networks using provenance-based techniques," IEEE Trans. Mob. Comput. ۱۹ (۲۰۲۰) ۱۰۵۳–۱۰۶۶..

[۲]. S. Patel, R. Jain, "A survey on MANET routing protocols: Security and anomaly detection perspectives," Int. J. Commun. Syst. ۳۱ (۲۰۱۸) e۳۴۹۲.

[۳]. N. Rathore, M. Tiwari, "Analysis of TCP/IP vulnerabilities in mobile networks with enhanced countermeasures," Wireless Pers. Commun. ۱۲۹ (۲۰۲٤) ۱۲۳–۱٤۰.

[٤]. X. Zhao, H. Li, "Secure routing in industrial wireless sensor networks with edge computing," IEEE Trans. Ind. Inform. ۱۹ (۲۰۲۳) ۳٤٥٦–۳٤٦۸.

[٥]. X. Liu, Y. Zhang, "Geographical-based routing with edge computing in vehicular networks," IEEE Trans. Veh. Technol. ۷۲ (۲۰۲۳) ۲۲۳٤–۲۲٤٦.

[٦]. N. Gupta, S. Sharma, Hybrid cryptographic approach for securing AODV in MANETs, Ad Hoc Networks ۱۲۸ (۲۰۲۲) ۱۰۲۷۹٦.

[۷]. Y. Li, J. Wang, "Trust-aware secure routing protocol for IoT-enabled MANETs," IEEE Internet of Things Journal ۸ (۲۰۲۱) ۲۳۰۴–۲۳۱۲.

[۸]. R. Meena, S. K. Pandey, "An enhanced secure routing protocol for MANETs using trust and machine learning," Wireless Networks ۲۸ (۲۰۲۲) ۱٤٥۷–۱٤۷۱.

[۹]. S. Ahmed, R. Islam, "Enhancing AODV with lightweight security mechanisms," IEEE Access ۹ (۲۰۲۱) ٥۰٦۷–٥۰۸۰.

[۱۰]. A. Patel, N. Shah, "Comparative analysis of secure dynamic source routing protocols for MANETs," Springer Wireless Personal Communications ۱۲۹ (۲۰۲۳) ۲۲۱۱–۲۲۲٥.

Maniya Naghshin[1]

Department of IT and Computer Engineering, Urmia Branch, Islamic Azad University, Urmia,Iran

Kambiz Majidzadeh[2*]

Department of IT and Computer Engineering, Urmia Branch, Islamic Azad University, Urmia,Iran

Abstract

This article introduces two trust-based routing methods for mobile ad hoc networks: "Trust-Based Self-Diagnostic Routing" and "Trust-Based Cooperative Routing". These methods are designed based on the "Secure Ad hoc On-demand Distance Vector" (SAODV) protocol, with the aim of enhancing security and trust in routing. Ad hoc networks rely on cooperation between nodes; however, incompatible nodes can disrupt the routing process. These methods focus on identifying malicious nodes, accurately assessing trust, and maintaining secure paths, thereby reducing the impact of incompatible nodes. Simulation results show that these methods outperform in eight key performance metrics. The proposed methods demonstrate better performance compared to protocols like "Routing Information Protocol" (RIP). Finally, Trust-Based Cooperative Routing is more suitable for large-scale networks, while Trust-Based Self-Diagnostic Routing is better for specific applications and smaller networks. This article provides a novel contribution to enhancing security and trust in routing for ad hoc networks.

Keywords: **“**Mobile ad hoc network**”, “**attack-resistant routing**”, “**SAODV protocol**”**, “security and trust**”.**