ارائه یک الگوریتم چند مسیری مبتنی برروش ترکیبی جستجوی عمقی چندگانه و تپه نوردی برای بهبود قابلیت اطمینان و امنیت مسیرهای ارسال بسته در اینترنت اشیا

وزیر احمد تاجیک
دانشجوی کارشناسی ارشد کامپیوتر دانشگاه آزاد اسلامی واحد مشهد
رضا شیبانی
عضو هیات علمی دانشگاه آزاد اسلامی واحد مشهد

چکیده

امروزه می‌توانیم اینترنت اشیا را به عنوان شبکه‌ای فراگیر و جهانی توصیف کنیم که سیستمی برای نظارت، کنترل، پردازش و تجزیه و تحلیل داده‌های تولید شده توسط دستگاه‌های اینترنت اشیا ارائه می‌دهد. ارتباطات با شبکه‌های اینترنت اشیا بدون پشتیبانی از طرح‌های مسیریابی زیربنایی کارآمد امکان پذیر نیست. با این حال، محدودیت‌های مربوط به منابع کم توان و همچنین ماهیت بی‌سیم و با تلفات بالا در شبکه‌های اینترنت اشیا ممکن است به شدت بر قابلیت اطمینان ارتباطات تأثیر بگذارد. در نتیجه، کارایی مسیریابی می‌تواند تحت تأثیر قرار گیرد. علاوه بر این، قرار گرفتن در معرض حملات سایبری داخلی و خارجی، به ویژه حملاتی که در دسترس بودن داده‌ها و سرویس‌ها را تهدید می‌کنند، مسیریابی و ماموریت‌های امنیتی را در چنین زمینه‌ای محدود پیچیده‌تر می‌کند. در این پایان نامه الگوریتمی با عنوان ارائه یک الگوریتم چند مسیری مبتنی برروش ترکیبی جستجوی عمقی چندگانه و تپه نوردی برای بهبود قابلیت اطمینان و امنیت مسیرهای ارسال بسته در اینترنت اشیا ارائه شده است که هدف آن بهبود میزان سربار بسته ارسالی از مبدا به مقصد در شبکه، میزان سربار ارتباطی بین گره‌ها برای ارسال بسته، میزان درصد بسته تحویلی به مقصد، میزان انرژی مصرفی مبدا به مقصد و میزان نرخ ازدست دادن بسته است. نتایج ارزیابی به وضوح اثربخشی راه حل پیشنهادی برای بهبود قابلیت اطمینان و امنیت ارتباطات، با هزینه کم را نشان می‌دهد.

واژگان کلیدی: مسیریابی چند مسیره، قابلیت اطمینان ارتباطی، امنیت شبکه، اینترنت اشیا، جستجوی عمقی چندگانه، تپه نوردی

۱.مقدمه

اینترنت اشیا به تکنیک رو به رشدی اشاره دارد که به بررسی نحوه استفاده از فناوری برای زندگی انسان در آینده می‌پردازد. اجزای اینترنت اشیا شامل مواردی مانند یخچال و ماشین است که به طور محکم در حوزه فناوری جاسازی شده اند. اینترنت اشیا ایده اینترنت را از طریق یک شبکه گسترش داد(Shinde, ۲۰۲٤).

آدرس دهی و مسیریابی بسته‌های داده در میان دستگاه‌های با محدودودیت منابع، به دلیل ضرورت توسعه پروتکل‌های یکپارچه برای مسیریابی بسته‌های داده در شبکه‌های مختلف RPL یک مسئله اساسی است. بسته‌های داده مسیریابی در دستگاه‌های اینترنت اشیا از تهدیدات امنیتی بالقوه رنج می‌برند و از آنجایی که به زندگی کاربر مربوط می‌شود تأثیر قابل توجهی دارد. چندین حمله RPL از طریق فعالیت گره‌های مخرب در طول مسیریابی بسته‌های داده در بین دستگاه‌ها رخ می‌دهد. این امر بر امنیت داده‌های کاربران تأثیر می‌گذارد زیرا دستگاه‌ها در برابر حملات مختلف آسیب پذیر هستند(Yousefi at el, ۲۰۲٤).

ارسال مقادیر عظیمی از پیام‌های تایید یا انتظار برای دریافت آنها ممکن است به طور قابل توجهی هزینه‌های شبکه و همچنین تاخیرهای ارتباطی را افزایش دهد. با انگیزه این، اتخاذ مسیریابی چند مسیری برای قابلیت اطمینان تقویت و مقاومت بومی در برابر تهدیدات انکار سرویس بسیار تشویق خواهد شد(Sahraoui and Henni, ۲۰۲۳).

با توجه به وجود داده‌های حساس در اینترنت اشیا و تبادل آن در شبکه باز، مسائل مربوط به حریم خصوصی و امنیت در این شبکه باید مورد توجه ویژه قرار گیرد. علاوه بر این، گره‌ها در اینترنت اشیا منابع محدودی دارند و از کلید رمزگذاری متقارن برای رمزگذاری داده‌های همه گره‌ها استفاده می‌شود که دارای ضعف‌های امنیتی است. بنابراین، یک طرح احراز هویت کارآمد و ایمن مورد نیاز است تا گره‌های اینترنت اشیا بتوانند یکدیگر را احراز هویت کنند و یک کلید جلسه امن را به اشتراک بگذارند(Haitham at el, ۲۰۲۲).

اینترنت اشیا به دلیل ویژگی‌های منحصربه‌فردش هم در حوزه‌های کاربردی و هم در تحقیقات دانشگاهی مورد توجه قرار می‌گیرد. این یک چارچوب بین رشته‌ای است که در آن اشیای اطراف ما با اینترنت در ارتباط هستند تا خدمات هوشمند و کارآمدی ارائه دهند(Samie at el, ۲۰۱٦).

اینترنت اشیا بعد جدیدی را به ارمغان می‌آورد که هر کسی را از هر مکانی در هر مکانی به هم متصل می‌کند .دنیای فیزیکی را با دنیای اطلاعات ترکیب می‌کند .یکی از اجزای مهم اینترنت اشیا، سنسوری است که داده‌ها را از محیط جمع‌آوری می‌کند و در صورت نیاز به تغییر، محیط را کنترل می‌کند(Suo at el, ۲۰۱۲).

دستگاه‌های اینترنت اشیا دارای محدودیت منابع از جمله ظرفیت پردازش محدود، حافظه کم و مصرف انرژی بالای مسیریابی هستند. که مجموعه جدیدی از مسائل به دلیل تحرک بالای اشیا رخ می‌دهد. مکانیسم‌های امنیتی سنتی برای دستگاه‌های اینترنت اشیا مناسب نیستند، زیرا انرژی بیشتری مصرف می‌کنند و سربار محاسبات را افزایش می‌دهند. علاوه بر این، تعداد زیادی از دستگاه‌های متصل به اینترنت اشیا مسائل امنیتی را در شبکه با مقیاس بزرگ ایجاد می‌کنند(Kumar at el, ۲۰۲۵).

بنابراین، شبکه اینترنت اشیاء توزیع شده و تغییر یافته پویا و دستگاه‌های سبک وزن اینترنت اشیا نیازمند راه حلی مبتنی بر اعتماد برای اطمینان از امنیت و قابلیت اطمینان اطلاعات هنگام مسیریابی هستند(Tosh at el, ۲۰۱۸).

فقدان کنترل‌کننده مرکزی، محدودیت‌های شدید منابع و مسیریابی داده‌های چند مسیری، تبادل داده‌ها را به یکی از چالش‌های اساسی اینترنت اشیا تبدیل کرده است. با وجود تلاش‌های تحقیقاتی متعدد در جنبه‌های مختلف مسیریابی و تبادل داده‌ها، برخی از چالش‌های

اساسی مانند تأثیرات منفی انتخاب بهترین مسیر ممکن و عدم وجود اقدامات لازم برای مشاهده شرایط پویای گره‌ها هنوز وجود دارد(Zahedy at el, ۲۰۲٤).

در این مقاله یک الگوریتم چند مسیری مبتنی برروش ترکیبی جستجوی عمقی چندگانه و تپه نوردی برای بهبود قابلیت اطمینان و امنیت مسیرهای ارسال بسته در اینترنت اشیا ارائه شده است که هدف آن کاهش سربار ارتباطی، کاهش سربار بسته‌ها، افزایش درصد بسته تحویلی، کاهش نرخ ازدست دادن بسته‌ها وکاهش مصرف انرژی شبکه اینترنت اشیا می‌باشد. این مقاله محققان را قادر می‌سازد تا رویکرد مناسبی را برای مطالعه و تحقیق انتخاب نمایند و پیشنهاد طرح‌های بهتری برای مسیریابی امن در اینترنت اشیا ارائه دهند. موضوعات تحقیقاتی آینده نیز در این پژوهش پیشنهاد شده است.

ادامه این مقاله به صورت زیر تنظیم شده است: بخش ۲ کار مرتبط را توضیح می‌دهد. در بخش ۳، الگوریتم پیشنهادی را توضیح می‌دهیم. بخش ۴ شامل ارزیابی نتایج آزمایش شبیه سازی است. در نهایت، نتیجه گیری را در بخش ۵ ارائه می‌دهیم.

۲.کار مرتبط

در پژوهش (Sahraoui and Henni, ۲۰۲۳) الگوریتم مسیریابی چند مسیری امن و تطبیقی مبتنی بر RPL به نام SAMP-RPL [۱] برای افزایش امنیت و قابلیت اطمینان در شبکه‌های ناهمگن متصل به اینترنت اشیا پیشنهاد شده است. در این مقاله، یک راه‌حل متکی بر مسیریابی چند مسیره تطبیقی و امن برای پروتکل مسیریابی IPv٦ برای شبکه‌های RPL ارائه شده است. نتایج ارزیابی به وضوح اثربخشی راه حل پیشنهادی برای بهبود قابلیت اطمینان و امنیت ارتباطات، با هزینه کم را نشان می‌دهد.

در پژوهش (Meena and Sharma, ۲۰۲۳) الگوریتم مسیریابی امن برای احراز هویت و تصمیم گیری کلید پویا مخفی برای شبکه حسگر بیسیم مبتنی بر اینترنت اشیا ارائه شده است. رویکرد پیشنهادی شامل خوشه بندی گره، انتخاب سر خوشه، احراز هویت کلید و مسیریابی امن است. الگوریتم خوشه‌بندی مرغ دریایی برای خوشه‌بندی گره‌های حسگر پیشنهاد شده است و سرخوشه با استفاده از الگوریتم جستجوی عقاب رایدر طاس RBES [۲] انتخاب می‌شود. در مرحله بعد، فرآیند توافق کلید با استفاده از یک طرح احراز هویت کلید پویا انجام می‌شود که انتقال داده‌های امن‌تر را از طریق شبکه ارائه می‌دهد.

در پژوهش(Prathapchandran at el, ۲۰۲۱) یک مکانیسم امنیتی آگاه از اعتماد برای شناسایی حمله سینک در محیط اینترنت اشیا مبتنی بر RPL با استفاده از جنگل تصادفی به نام RFT [۳] ارائه شده است. این مدل یک راه حل مبتنی بر اعتماد برای تضمین امنیت در شبکه اینترنت اشیا ارائه می‌دهد. اساساً برای رسیدگی به حمله سینک در پروتکل مسیریابی برای محیط‌های مبتنی بر اینترنت اشیا مبتنی بر شبکه‌های کم مصرف و شبکه‌های با اتلاف طراحی شده است. با یافتن و حذف گره‌های حفره در شبکه، مسیریابی قابل اعتماد را در محیط اینترنت اشیا افزایش می‌دهد. مدل پیشنهاد شده از جنگل تصادفی و منطق ذهنیSL [۴] برای بهبود عملکرد شبکه با شناسایی حمله سینک استفاده می‌کند. معیارهای بهبود این روش شامل: نسبت تحویل، توان عملیاتی، متوسط تاخیر، مصرف انرژی، نرخ مثبت کاذب، نرخ منفی کاذب، و دقت تشخیص است.

در پژوهش(Seyfollahi at el, ۲۰۲۲) یک پروتکل مسیریابی امن مبتنی بر RPL با استفاده از بهینه‌ساز شعله پروانه به نام [۵] MFO-RPLبرای برنامه‌های اینترنت اشیا ارائه شده است که برای بهینه‌سازی فرآیند مسیریابی و تشخیص حمله رتبه‌بندی در RPL پیشنهاد می‌کند.

---

۱ secure and adaptive multipath RPL

۲ Rider Bald Eagle Search

۳ Random Forest Trust

۴ Subjective Logic

۵ Moth-Flame Optimization-based secure scheme for RPL

در پژوهش (Ahmadi and Javidan, ۲۰۲۲) شناسایی حملات مسیریابی اینترنت اشیا مبتنی بر اعتماد با استفاده از شبکه‌های عصبی بازگشتی ارائه شده است. در این مقاله ارزیابی اعتماد بر اساس بررسی جریان ترافیک دستگاه‌ها و تشخیص انحرافات رفتاری آن‌ها مبتنی بر اعتماد[۱] TRAD پیشنهاد شده است.

در پژوهش(Manda and Singh, ۲۰۲۳) پروتکل مسیریابی داده آگاه از انرژی و اعتماد براساس الگوریتم رقابتی گرده افشانی گل به نام CVFP[۲] در اینترنت اشیا ارائه شده است که پارامترهای اعتماد، انرژی، تأخیر، فاصله و طول عمر پیوند را برای یافتن یک مسیر مسیریابی بهینه در نظر می‌گیرد. کیفیت ارتباطات با استفاده از محدودیت لینک اندازه گیری می‌شود تا تصمیم بگیرد که آیا داده‌ها می‌توانند مسیریابی شوند یا مکانیسم نگهداری مسیر برای اطمینان از قابلیت اطمینان در مسیریابی داده‌ها انجام شود.

در پژوهش (Bang and Rao, ۲۰۲۲) یک پروتکل RPL بهبود یافته به نام EMBOF-RPL [۳] برای تشخیص زودهنگام و جداسازی حمله رتبه‌ای در اینترنت اشیا مبتنی بر RPL ارائه شده است. این الگوریتم دقت تشخیص، تأخیر، نسبت تحویل بسته، تأخیر بین گره‌ها، مصرف انرژی و سربار حافظه را بهبود می‌دهد.

در پژوهش(Rashid at el, ۲۰۲۲) آموزش خصمانه برای شناسایی حملات سایبری مبتنی بر یادگیری عمیق در برنامه‌های شهر هوشمند مبتنی بر اینترنت اشیا ارائه شده است. در این کار، تأثیر حملات خصمانه بر یادگیری عمیق و مدل‌های یادگیری ماشین کم عمق با استفاده از مجموعه داده‌های قبلی اینترنت اشیاء بررسی می‌شود و روشی را با استفاده از بازآموزی خصمانه پیشنهاد می‌کند که می‌تواند به طور قابل توجهی عملکرد سیستم‌های تشخیص نفوذ را در هنگام مقابله با حملات خصمانه بهبود بخشد.

در پژوهش (Xiao et at, ۲۰۲٤) مسیریابی چند مسیری ایمن برای اینترنت اشیا بر اساس ارزیابی اعتماد به نام TESM [۴] ارائه شده است. این الگوریتم یک کنترل کننده شامل یک ماژول تأیید امنیتی، یک ماژول مسیریابی چند مسیره و یک ماژول مدیریت ناهنجاری را در خود جای داده است. ماژول تأیید امنیتی اعتبار سنجی امنیتی مداوم بسته‌های داده را تضمین می‌کند و امتیازات اعتماد را برای گره‌ها بدست می‌آورد. متعاقباً، ماژول مسیریابی چند مسیری از یادگیری تقویتی چند هدفه برای ایجاد پویا چندین مسیر ایمن بر اساس امتیازهای اعتماد گره استفاده می‌کند. ماژول مدیریت ناهنجاری وظیفه مدیریت گره‌های سوئیچ مخرب و مسیرهای غیرعادی را دارد. این مقاله تاخیر، امنیت و توان عملیاتی را بهبود می‌دهد.

در پژوهش (Ateyaet at, ۲۰۲٤) طرح مسیریابی چند مسیری برای انتقال بهینه داده در اینترنت متراکم اشیا ارائه شده است. یک روش جدید برای انتخاب گروه بهینه مسیرها و ضرایب توزیع ترافیک در طول آن‌ها پیشنهاد شده است. روش پیشنهادی با استفاده از برنامه نویسی پویا پیاده سازی شده است. این مدل تعداد گره‌های میانی درگیر در مسیریابی روی شبکه‌های متراکم اینترنت اشیا را کاهش می‌دهد و در نهایت سربار ارتباطی و زمان تحویل داده را بهبود می‌دهد.

۳.روش تحقیق

در این بخش ابتدا مدل پیشنهادی بیان می‌شود سپس روش پیشنهادی و جزئیات آن ارائه می‌شود.

---

۱ Trust-based RPL Attacks Detection

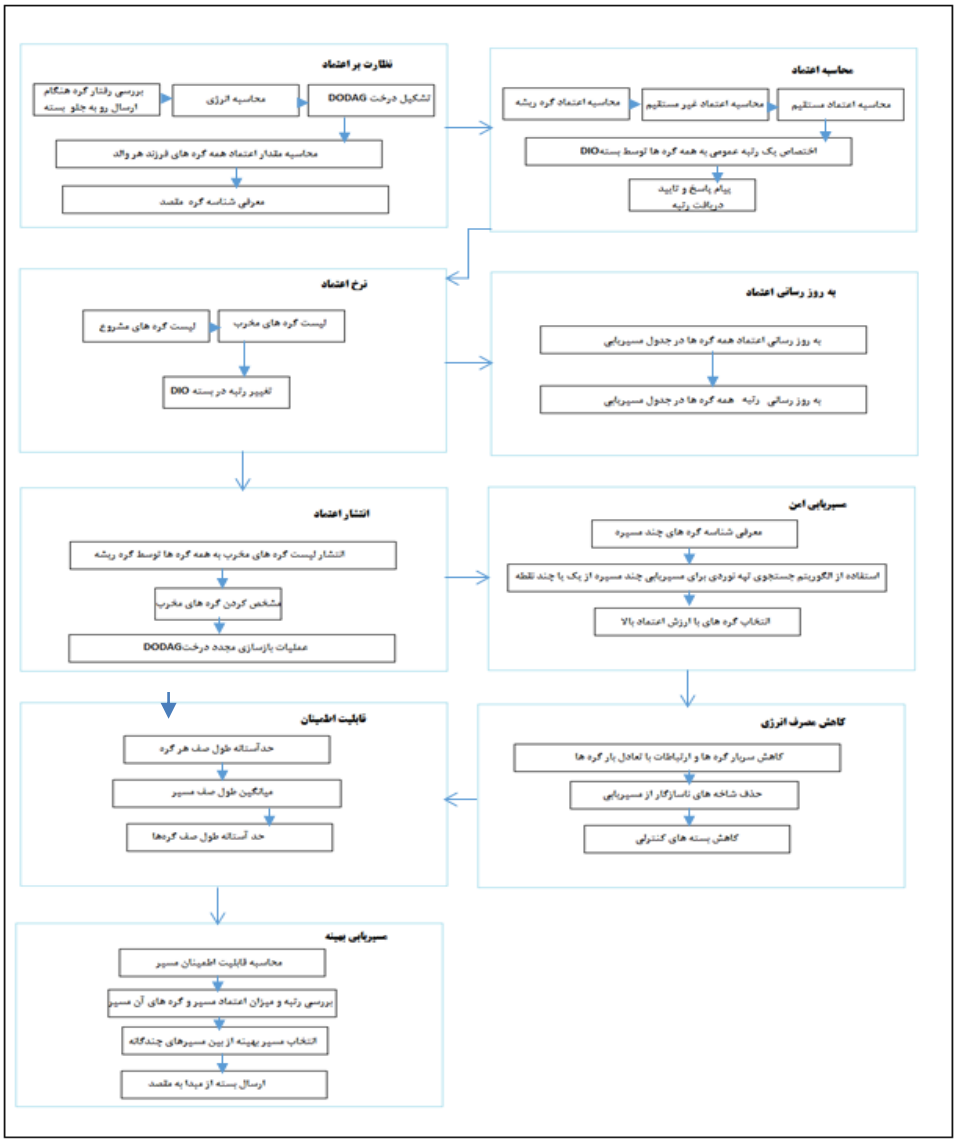
۲ Competitive Verse Flower Pollination

۳ Echelon Metric Based Objective Function

٤ trust evaluation based secure multi-path routing

۳-۱ مدل پیشنهادی تحقیق

در شکل۱ مدل پیشنهادی پژوهش ارائه شده است. ماژول اول نظارت بر اعتماد: در این بخش ابتدا یک درخت DODAG ایجاد می‌شود سپس انرژی گره‌ها بصورت لحظه‌ای محاسبه می‌شود. رفتار تمام گره‌ها هنگام ارسال بسته رو به جلو بررسی می‌شود. برای تمام گره‌های شبکه مقدار اعتماد محاسبه می‌شود. هر گره مقدار اعتماد خود ا به گره والد ارسال می‌کند. سپس بای تمام گره‌های مورد اعتماد شناسه مقصد ارسال می‌شود. ماژول دوم محاسبه اعتماد: در این ماژول اعتماد مستقیم و اعتماد غیرمستقیم برای تمام گره‌های شبکه محاسبه می‌شود. مقدار اعتماد همه گره‌ها از طریق والدین مستقیم و غیر مستقیم به ریشه ارسال می‌شود و اعتماد ریشه بدست می‌آید. برای اطمینان از مشروع بودن هر گره یک رتبه توسط ریشه با پیام کنترلیDIO[1] به تمام گره‌ها ارسال می‌شود. گره‌هایی که مخرب باشند این مقدار رتبه تغییر می‌کند. و تمام گره‌هایی که پیام را دریافت کنند یک پیام پاسخ به ریشه ارسال می‌کنند.



شکل۱: مدل پیشنهادی تحقیق

[1] DODAG Information Object

ماژول سوم نرخ اعتماد: در این ماژول نرخ اعتماد همه گره‌ها مشخص است و گره‌ها در دولیست گره‌های مشروع و گره‌های مخرب دسته بندی می‌شوند و رتبه تمام گره‌های مخرب تغییر می‌کند. ماژول چهارم به روز رسانی اعتماد: در این ماژول همه گره‌ها رتبه خود و مقدار اعتماد را به روز رسانی می‌کنند. ماژول پنجم انتشار اعتماد: در این بخش لیست تمام گره‌های مخرب توسط گره ریشه به همه گره‌ها ارسال می‌شوند. گره‌های مخرب مشخص می‌شوند و به عنوان گره مخرب علامتگذاری می‌شوند. بعد از شناسایی گره‌های مخرب و گره‌های مشروع، عملیات بازسازی مجدد درخت DODAG انجام می‌شود. ماژول ششم مسیریابی امن: در این بخش شناسه گره‌های چند مسیره مشخص می‌شود. با استفاده از الگویتم جستجوی تپه نوردی با جستجوی عمقی چندگانه از چندین مسیر به سمت مقصد مسیریابی را انجام می‌دهند. در هر مسیر گره‌هایی انتخاب می‌شوند که میزان انرژی بالا، مقدار اعتماد بالا و میانگین طول صف پایینی داشته باشند. ماژول هفتم قابلیت اعتماد: در این بخش ابتدا حدآستانه طول صف همه گره‌ها محاسبه می‌شود. برای هر مسیر میانگین طول صف آن مسیر مشخص می‌شود تا از ترافیک و سربار شبکه جلوگیری شود که در نهایت منجر به کاهش مصرف انرژی می‌شود. برای هر گره میانگین طول صف محاسبه می‌شود. ماژول هشتم کاهش مصرف انرژی: سربار گره‌ها و سربار ارتباطات با استفاده از بررسی صف هر منبع کاهش می‌یابد که منجر به کاهش انرژی می‌شود. شاخه‌های ناسازگار و کور مورد بررسی قرار نمی‌گیرند و بسط داده نمی‌شوند که منجر به بررسی نشدن بعضی شاخه‌های بی پایان می‌شود و مصرف انرژی کاهش می‌یابد. با در نظر گرفتن مسیرهای سازگار و کارا بسته‌های کنترلی کاهش می‌یابد و باعث بهبود مصرف انرژی می‌شود. ماژول نهم مسیریابی بهینه: در این بخش محاسبه قابلیت اطمینان مسیر انجام می‌شود. رتبه و میزان اعتماد مسیر بررسی می‌شود. از بین مسیرهای چندمسیره یک مسیر بهینه انتخاب می‌شود و بسته از مبدا به مقصد ارسال می‌شود.

۳-۳ روش پیشنهادی تحقیق

این تحقیق بر روی شبکه‌های اینترنت اشیا متمرکز است که بدون تحرک و یا کم تحرک است. فرض می‌کنیم که تمام ارتباطها دو طرفه هستند. اگر گره i بتواند بسته‌هایی را که به طور مستقیم توسط گره j منتقل شده است دریافت کند، گره j می‌تواند بسته‌هایی را که به طور مستقیم توسط گره i منتقل می‌شود، دریافت کند. شبکه اینترنت اشیا با یک گراف $G=\{d,L\}$ مدل شده است، که در آن d مقصد و L نشان دهنده مجموعه‌ای از لینک‌های ارتباطی است. روش پیشنهادی یک مکانیزم اساسی امنیتی ارائه می‌دهدکه توسط تمام گره‌ها انجام می‌شود و امنیت و اطمینان را در سراسر شبکه انجام می‌دهد.

در ادامه مفاهیم اولیه تعریف می‌شود:

در رابطه۱ نرخ تحویل بسته[۱]PDR به عنوان نسبت بین تعداد بسته‌های داده با موفقیت تحویل داده شده و تعداد بسته‌های ارسال شده تعریف می‌شود.

$$PDR = \frac{p_{recieved}}{p_{generated}} \times 100 \qquad (۱)$$

فاصله بین هر گره و والد آن براساس رابطه ۲ محاسبه می‌شود:

$$d = \sqrt{(x - x_{parent})^2 + (y - y_{parent})^2} \qquad (۲)$$

که در آن x ، yمختصات جغرافیایی فعلی گره هستند وx_{parent} ، y_{parent} مختصات جغرافیایی والد ترجیحی هستند.

[۱] Packet Delivery Ratio

RPL یک توپولوژی DODAG[1] را تشکیل می‌دهد که ساختار مسیریابی شبکه را توصیف می‌کند. یک گراف DODAG یک گراف غیر چرخه‌ای است که یک گره ریشه دارد. هر گره اطلاعات والدین خود را می‌داند. با این حال، آنها از فرزندان خود خبر ندارند. در RPL، هر گره والد ترجیحی خود و حداقل یک مسیر به گره ریشه دارد و از چهار پیام کنترلی برای به روز رسانی اطلاعات مسیریابی استفاده می‌کند.

اولین پیام کنترلیDIO است که رتبه گره را در مورد گره ریشه که در انتخاب والد انتخابی مشارکت دارد، مشخص می‌کند.

اعلان شی مقصد DAO[2] نوع دوم پیام است که اطلاعات مقصد را به والدین انتخاب شده بصورت یکپارچه در اختیار می‌گذارد.

درخواست اطلاعات گراف DIS [3]نوع سوم است. یک گره از این پیام کنترلی برای دریافت پیام DIO از گره‌های همسایه استفاده می‌کند.

پیام DAO-ACK [4] چهارمین و آخرین نوع پیام کنترلی است. این پیام کنترلی به گیرنده پیام DAO به عنوان گره والد یا گره ریشه پاسخ می‌دهد.

کنترل سربار پیام‌ها از رابطه ۳ بدست می‌آید که این مجموع کنترل‌های پیامDIO ، DISو DAO است که در طول شبیه سازی شبکه منتقل می‌شود:

$$\text{ntroloverhead}=\sum_{i=1}^{n} \text{DIS} + \sum_{i=1}^{n} \text{DIO} + \sum_{i=1}^{n} \text{DAOco} \quad (۳)$$

توپولوژی DODAG به گونه‌ای تشکیل می‌شود که گره ریشه شروع به ارسال پیام‌های DIO به همه گره‌ها می‌کند. گره ریشه مکان خود را در تمام گره‌ها تعیین می‌کند. هر گره در هر سطح از مسیریاب‌های گیرنده مسیر و تمام مسیرهای هر گره درگیر را ثبت می‌کند. سپس این گره‌ها پیام‌های DIO را منتشر می‌کنند و به این ترتیب کل توپولوژی ساخته می‌شود. گره والد ترجیحی به عنوان مسیر پیش فرض گره ریشه در تشکیل ریشه به سمت بالا انتخاب می‌شود. در حالی که در مسیرهای رو به پایین، گره‌ها پیام کنترل DAO را با استفاده از گره والد به سمت گره ریشه منتشر می‌کنند.

در ادامه برای کنترل ترافیک و ازدحام از روش حدآستانه طول صف هر گره استفاده می‌شود. برای هر گره میانگین طول صف پیام‌ها از رابطه ۴ محاسبه می‌شود:

$$\text{avg}_{q} = \frac{q + \sum_{i=1}^{n} nq_i}{n+1} \quad (۴)$$

که در آن q طول صف گره را نشان می‌دهد، nq طول صف گره همسایه را نشان می‌دهد و n تعداد گره همسایه را نشان می‌دهد.

در رابطه ۵ برای هر مسیر میانگین طول صف گره‌ها محاسبه می‌شود:

$$\text{avg}_{\text{qpath}} = \frac{\sum_{i=1}^{m} \text{avg}_{qi}}{m} \quad (۵)$$

مقدار آستانه طول صف گره‌ها از رابطه ۶ محاسبه می‌شود:

[1] Destination Oriented Directed Acyclic
[2] Destination Advertisement Object
[3] DODAG Information Solicitation
[4] DAO Acknowledgement

$$thr = \frac{|q-avg_q|+\sum_{i=1}^{n}|nq_i-avg_q|}{n+1} + avg_q \quad (۶)$$

که در آن، q و avg_q به ترتیب طول صف و میانگین طول صف گره را نشان می‌دهند.

اعتماد مستقیم DT[۱] : تعیین می‌کند که یک گره چقدر قابل اعتماد است و تا چه اندازه وظیفه تعیین شده خود را انجام می‌دهد. در روش پیشنهادی برای محاسبه اعتماد مستقیم براساس دو معیار مصرف انرژی گره و رفتار ارسال بسته از گره به سمت جلو استفاده می‌شود که از رابطه ۷ محاسبه می‌شود.

$$DT(n_i, n_j) = \frac{FPB + E_j}{2} \quad (۷)$$

بطوریکه در رابطه فوق FPB [۲] رفتار ارسال بسته از گره به سمت جلو و E_j میزان تغییر انرژی را در حین ارسال پیام‌ها نشان می‌دهد. مقدار میانگین ترکیبی مقدار DT مثبت یا منفی گره را می‌دهد.

در رابطه ۸ مقدار E تغییر مصرف انرژی از رابطه زیر محاسبه می‌شود و در حین ارسال پیام به گره C از طرف گرهA ، مقدار انرژی مصرف شده توسط گره B را تعیین می‌کند.

$$E_{n,t} = P \times E_{n,p} \quad (۸)$$

رابطه فوق نشان می‌دهد که در هنگام ارسال پیام‌هایp چقدر انرژی مصرف می‌شود. در نهایت، تفاوت انرژی مصرف شده در ارسال پیام‌ها در رویدادهای گذشته و فعلی، کاهش انرژی گره همسایه را نشان می‌دهد.

برای محاسبه FPB از رابطه ۹ استفاده می‌شود که نشان دهنده نرخ ارسال بسته‌های فوروارد شده به بسته‌های ارسالی است.

$$FPB(n_i, n_j) = \frac{FP_{ji}}{SP_{ij}} \quad (۹)$$

پس از نظارت بر رفتار گره‌های همسایه بر اساس این دو معیار، اعتماد مستقیم گره همسایه محاسبه می‌شود.

اگر مقدار اعتماد مستقیم گره با آستانه مطابقت داشته باشد، مدل اعتماد مثبت گره را افزایش می‌دهد. همه گره‌ها اعتماد مستقیم گره همسایه را محاسبه کرده و به گره ریشه منتقل می‌کنند. انتقال به مقدار اعتماد مستقیم بستگی دارد. اگر مقدار منفی مدل را افزایش دهد، گره فرزند والد خود را تغییر می‌دهد و به طور فعال به گره ریشه اطلاع می‌دهد. گره ریشه اعتماد مستقیم را بررسی می‌کند و سپس اعتماد غیر مستقیم را محاسبه می‌کند. اعتماد غیرمستقیم با در نظر گرفتن نظرات سایر گره‌ها که مقادیر اعتماد مستقیم همان گره با همسایگان مختلف هستند، تعیین می‌کند که یک گره چقدر قابل اعتماد است. گره ریشه اعتماد سراسری را به صورت دوره‌ای و محاسبه می‌کند. شکل۲ الگوریتم مسیریابی چندمسیره را نشان می‌دهد.

[۱] Direct Trust
[۲] forwarding packet behavior

```
function multipath rout()

١.  create DODAG
٢.  calculate energy of nodes
٣.  Checking the behavior of the node when forwarding packets
٤.  Calculating the trust of each parent's child nodes
٥.  Identification of destination node ID
٦.  Calculation of direct trust value
٧.  Calculation of indirect trust value
٨.  Calculate the trust value of the root node
٩.  propagation DIO message with public rank
١٠. Assigning a public rank to all nodes by the package DIO
١١. Send a reply message and confirm the rank
١٢. Create a list of legitimate nodes
١٣. Create a list of malicious nodes
١٤. if node is malicious then
١٥. increase rank value
١٦. end if
١٧. for i←١ to n d
١٨. Update the trust value of node(i) in the routing table
١٩. Update the rank value of node(i) in the routing table
٢٠. End for
٢١. propagation the list of malicious nodes to all nodes by the root
٢٢. Identify malicious nodes
٢٣. Reconstruction operation DODAG
٢٤. Identification of the ID of multipath nodes
٢٥. Selection of nodes with high trust value
٢٦. Calculate threshold of node queue length
٢٧. Calculate threshold of rout queue length
٢٨. call hill climbing search algorithm
٢٩. Reliability calculation
٣٠. Checking the rank and reliability of the route
٣١. select optimal route from multipath routing
٣٢. Send package from source to destination
٣٣. end
```

شکل۲:الگوریتم مسیریابی چندمسیره

شکل۳ الگوریتم جستجوی محلی تپه نوردی با جستجوی عمقی چندگانه را نشان می‌دهد. که عمل جستجو را از چند گره تصادفی آغاز می‌کند بطوریکه با انتخاب بهترین فرزندان مسیرهای بهینه جستجو می‌شوند.

```
١.  function  HILL-CLIMBING (root) returns  a state  that is a public maximum
٢.  Current ← MAKE-NODE (root.INITIAL-STATE)
٣.  loop  do
٤.  neighbor ←  a highest(trust+energy+١/avg(queue)) valued successor of current
٥.  if current.VALUE  ≤neighbor.VALUE and promising current=true then        return current.SATTE
٦.  add current.SATTE in to routing  table
٧.  end
٨.  current ←neighbor
٩.  if  unpromising current node then// Plateau, local hill, edge
١٠. select k random node from neighbors current node
١١. for i←١ to k do
١٢. HILL-CLIMBING (k);
١٣. end
```

شکل۳: الگوریتم جستجوی محلی تپه نوردی با جستجوی عمقی چندگانه

۴.یافته‌ها

در این بخش ابتدا تنظیمات شبیه‌سازی انجام شده سپس به تحلیل و ارزیابی نتایج پرداخته می‌شود.

۴-۱ داده‌های شبیه سازی

برای ارزیابی عملکرد الگوریتم پیشنهادیHCMPR[۱]، از روش پایه SAMP-RPL برای مقایسه استفاده می‌شود. از آنجا که پیاده‌سازی و اشکال زدایی اینترنت اشیا در شبکه‌های واقعی دشوار است، در نظر گرفتن شبیه‌سازی به عنوان یک ابزار طراحی اساسی ضروری است. مزیت اصلی شبیه‌سازی ساده‌سازی تجزیه و تحلیل و تأیید پروتکل، به ویژه در سیستم‌های بزرگ است. در این بخش، عملکرد روش پیشنهادی توسط متلب۲۰۲۰ به عنوان ابزار شبیه‌سازی ارزیابی می‌شود و سپس نتایج مورد بحث قرار می‌گیرد.

پارامترهای شبیه سازی در جدول۱ ارائه شده است. عملکرد روش HCMPR در ۹۰۰ ثانیه سنجیده می‌شود. تعداد گره‌های شبکه برابر ۸۰ گره می‌باشد. همچنین ۸ گره به عنوان گره‌های چند مسیره هستند که استقرار گره‌هابه صورت تصادفی در فضای شبیه سازی قرار دارند.

جدول۱:پارامترهای شبیه سازی

پارامترهای شبیه سازی	مقادیر
پروتکل کنترل دسترسی رسانه	IEEE ۸۰۲,۱۱p
زمان شبیه سازی	۹۰۰ ثانیه
فرکانس به روز رسانی امنیتی	هر ۵ دقیقه
تابع هش	SHA-۲۵۶
الگوریتم رمزگذاری	AES-۱۲۸
ترافیک ایجاد شده در هر گره	۱ بسته ۲۰ بایتی در هر ۵ ثانیه تولید می‌شود
محدوده تداخل	۲۵ متر گره‌های معمولی ۴۰ متر گره‌های چند مسیره
برد TX	۲۰ متر گره‌های معمولی ۴۰ مترگره‌های چند مسیره
تعداد گره‌های معمولی	۸۰
تعداد گره‌های چند مسیره	۸
تعداد مسیرهای بین یک گره چند مسیره	۳
استقرار گره‌ها	به صورت تصادفی

[۱] Hill Climbing Multi-Path Routes

۴-۲ ماژول‌های مدل HCMPR برای شبیه سازی

ماژول‌هایی که در شبیه سازی روش پیشنهاده استفاده شده است شامل: ماژول محاسبه اعتماد، ماژول نظارت بر اعتماد، ماژول محاسبه نرخ اعتماد، ماژول به روز رسانی اعتماد، ماژول انتشار اعتماد، ماژول مسیریابی امن، ماژول قابلیت اطمینان، ماژول کاهش مصرف انرژی و ماژول مسیریابی بهینه است.

۴-۳ متغیرهای مورد ارزیابی تحقیق

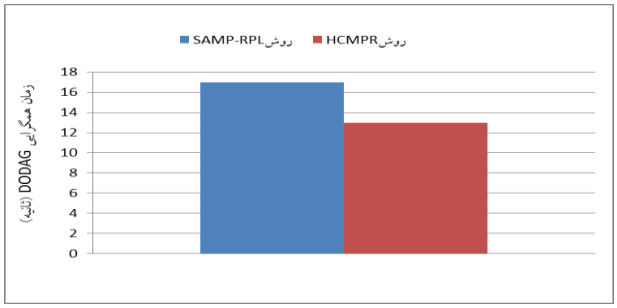
متغیرهایی که در این پژوهش مورد ارزیابی قرار می‌گیرند شامل موارد ذیل می‌باشد:

- سربار بسته
- سربار اتباطی
- درصد بسته تحویلی
- انرژی مصرفی
- نرخ ازدست دادن بسته

۴-۴ ارزیابی متغیرهای تحقیق

در این بخش، نتایج ارزیابی به دست آمده را ارائه و مورد بحث قرار می‌دهیم. ما بسیاری از پارامترهای ارزیابی را از جمله قابلیت اطمینان ارتباطات، هزینه‌های ناشی از مصرف انرژی و سربار شبکه، تأخیر در راه‌اندازی توپولوژی و در نهایت اثربخشی در برابر حملات مسیریابی مؤثر بر قابلیت اطمینان در نظر گرفته‌ایم.

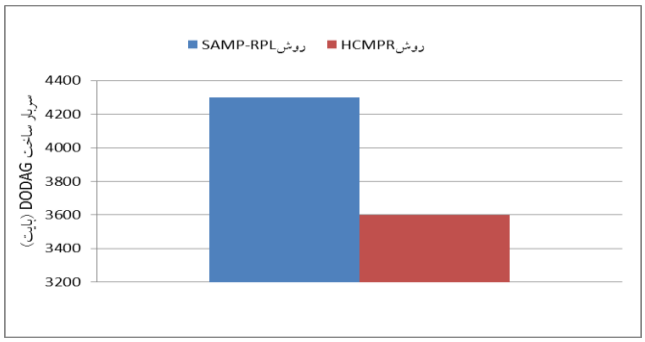
شکل۴ نتایج به دست آمده را برای هزینه‌های ساخت DODAG نشان می‌دهد. از آنجایی که فاز راه اندازیDODAG برای دو راه حل HCMPR و SAMP-RPL یکسان است. نتایج نشان می‌دهد که فرآیند تشکیلDODAG در روش HCMPR زمان همگرایی و تاخیر کمتری نسبت به روش SAMP-RPL دارد دارد. تاخیر بیشتر در روش SAMP-RPL ناشی از زمان مورد نیاز برای انجام اقدامات اولیه امنیتی اضافی در حین ساختن DODAG در SAMP-RPL است. روش HCMPR در حین مسیریابی اقدامات امنیتی ا انجام می‌دهد.



شکل۴: همگرایی برای ساخت DODAG

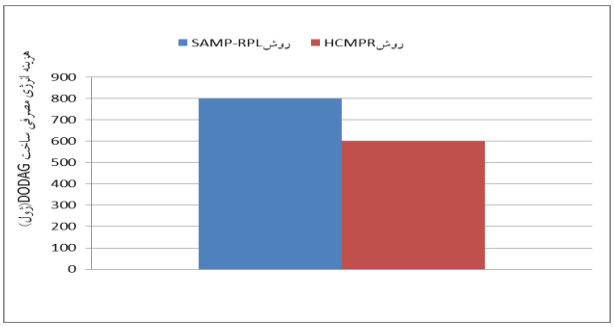
شکل۵ سربار ارتباطی برای ساخت DODAG را در روش HCMPR و روش SAMP-RPL نشان می‌دهد. سربار شبکه یکی دیگر از پارامترهای مهم ارزیابی است. تعداد بسته‌های تولید شده توسط تمام گره‌های شبکه را در طول زمان شبیه سازی در نظر می‌گیریم.

نتایج به‌دست‌آمده نشان داده شده در شکل ۵ به وضوح نشان می‌دهد که راه‌حل HCMPR نتایج سربار شبکه پایینی را به‌ویژه با راه‌حل‌های چند مسیری مبتنی بر جستجوی محلی تپه نوردی ارائه می‌کند. این امر با این واقعیت توجیه می‌شود که تکثیر بسته‌ها در راه حل مسیریابی چند مسیره تپه نوردی HCMPR در سطح گره‌های چند مسیره قدرتمند با احتمال موفقیت بالا شروع می‌شود، و از تکرار بسته‌ها از گره‌های مبدا انجام نمی‌شود بلکه از بین فرزندان شروع می‌شود. نتایج نشان می‌دهد که در روش HCMPR سربار ساخت درخت ۱۹.۵ درصد کاهش یافته است.



شکل۵: سربار ارتباطی برای ساخت DODAG

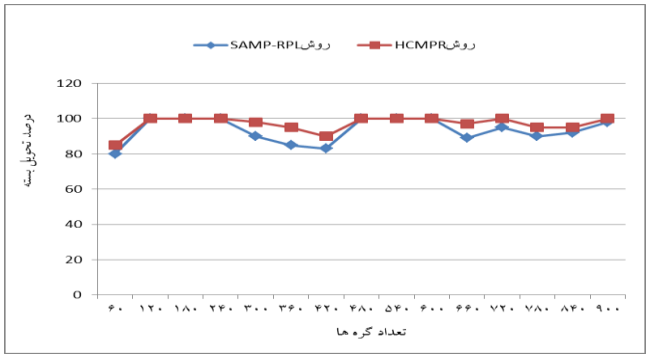
شکل۶ هزینه انرژی ارتباطی برای ساخت DODAG را در روش HCMPR و روش SAMP-RPL نشان می‌دهد. انرژی ارتباطی یکی دیگر از پارامترهای مهم ارزیابی است. تعداد بسته‌های تولید شده توسط تمام گره‌های شبکه را در طول زمان شبیه سازی در نظر می‌گیریم. نتایج به‌دست‌آمده به وضوح نشان می‌دهد که راه‌حل HCMPR نتایج انرژی ارتباطی پایینی را به‌ویژه با راه‌حل‌های چند مسیری مبتنی بر جستجوی محلی تپه نوردی ارائه می‌کند. جلوگیری از تکرار ارسال بسته‌ها از گره‌های مبدا باعث می‌شود که انرژی ارتباطی ساخت کاهش یابد. نتایج نشان می‌دهد که در روش HCMPR انرژی ارتباطی ساخت درخت ۳۳ درصد کاهش یافته است.



شکل۶: هزینه انرژی ارتباطی برای ساخت DODAG

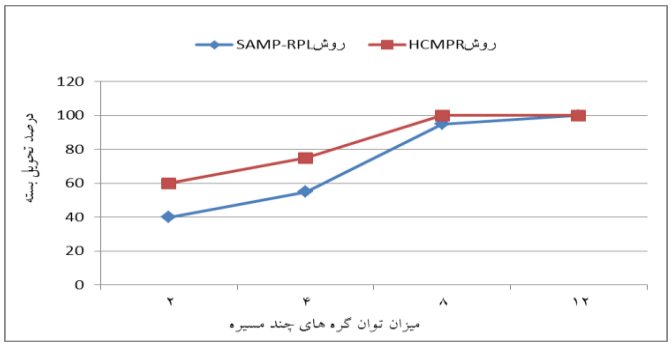
شکل ۷ نتایج ارزیابی را برای میانگین بسته تحویلی در طول زمان شبیه سازی برای ۶۰ تا ۹۰۰ گره نشان می‌دهد. نتایج به‌دست‌آمده نشان می‌دهد که راه‌حل HCMPR به طور قابل‌توجهی نسبت تحویل بسته و در نتیجه قابلیت اطمینان ارتباط در شبکه LLN را افزایش می‌دهد. استفاده از قابلیت اطمینان مسیر و جستجوی عمقی چندگانه با تپه نورد باعث انتخاب مسیرهایی با گره‌های سربار کم و قابلیت اطمینان بالا می‌شود که درصد تحویل بسته را افزایش می‌دهد. بطور کلی میانگین درصد تحویلی بسته ارسالی از مبدا به مقصد در روش HCMPR ۹۷ درصد است و در روش SAMP-RPL ۹۳.۵ درصد است که روش HCMPR ۳.۵ درصد بسته تحویلی

بیشتر بهبود می‌دهد. با درنظر گرفتن طول صف هر گره ارسال بسته به مسیرهای شلوغ انجام نمی‌شود و باعث کاهش ازدست دادن بسته می‌شود.



شکل۷: میانگین بسته تحویلی در طول زمان شبیه سازی

شکل ۸ نتایج ارزیابی را برای میانگین بسته تحویلی با مقادیر مختلف گره‌های چند مسیره باتوان بالا در طول زمان شبیه سازی برای ۲ تا ۱۲ توان گره نشان می‌دهد. نتایج به‌دست‌آمده نشان می‌دهد که راه‌حل HCMPR به طور قابل‌توجهی نسبت تحویل بسته در شبکه LLNرا افزایش می‌دهد. در واقع، فاکتور بسته تحویلی تحت تأثیر تعداد گره‌های چند مسیره قدرتمند مستقر در شبکه LLN است که با استفاده از قابلیت اطمینان مسیر و جستجوی عمقی چندگانه با تپه نورد باعث انتخاب مسیرهایی با گره‌های توانمند و قابلیت اطمینان بالا می‌شود که درصد تحویل بسته را افزایش می‌دهد.

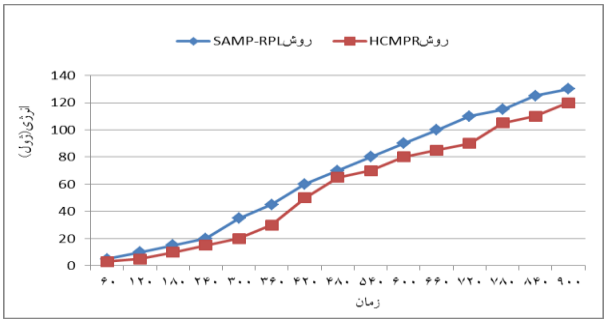


شکل۸: میانگین بسته تحویلی با مقادیر مختلف گره‌های چند مسیره باتوان بالا

نتایج به‌دست‌آمده نشان می‌دهد که هر چه تعداد گره‌های چند مسیره بیشتر باشد، بسته تحویلی بهتر است. با این وجود، استقرار تعداد بسیار مهمی از گره‌های چند مسیره گران خواهد بود. به همین دلیل قابلیت اطمینان هم از معیارهای انتخاب مسری ارسال بسته است.ظبطور کلی میانگین درصد تحویلی بسته ارسالی از مبدا به مقصد در روش HCMPR ۸۳.۷۵ درصد است و در روش SAMP-RPL ۷۲.۵ درصد است که روش HCMPR ۱۱.۲۵ درصد بسته تحویلی بیشتر بهبود می‌دهد. در نظر گرفتن قابلیت اطمینان مسیر با اعتماد بالا منجر به افزایش عملکرد روش HCMPR می‌شود.

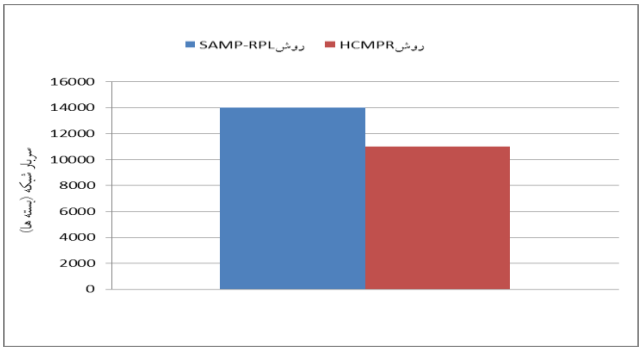
شکل ۹ نتایج ارزیابی را برای میانگین مصرف انرژی در طول زمان شبیه سازی برای ۶۰ تا ۹۰۰ گره نشان می‌دهد. نتایج به‌دست‌آمده نشان می‌دهد که راه‌حل HCMPR به طور قابل‌توجهی میانگین مصرف انرژی در طول زمان شبیه سازی را کاهش می‌دهد. برآورد هزینه انرژی یک عنصر کلیدی در ارزیابی راه حل‌هایی است که برای محیط‌های محدود تعیین می‌شوند. نتایج مربوط به مقادیر مصرف انرژی انباشته است. توجه داشته باشید که در راه حل HCMPR، انرژی مصرف شده توسط گره‌های چند مسیره توانند از محاسبه

مصرف انرژی کلی در شبکه مستثنی شده است. یعنی تنها گره‌های محدود معمولی در طول برآورد مصرف انرژی در نظر گرفته شدند. نتایج به‌دست‌آمده نشان می‌دهد که راه‌حل ما مصرف انرژی پایینی را ارائه می‌کند زیرا تا حد امکان وظایف مصرف انرژی را به گره‌های چند مسیره قدرتمند می‌سپارد. علاوه بر این، ماهیت تطبیقی سناریوی چند مسیری HCMPR که با روش ترکیبی جستجوی عمقی و تپه نوردی برای شروع مسیریابی چند مسیری در شبکه متکی است و به کاهش انرژی حاصله کمک زیادی کرده است.



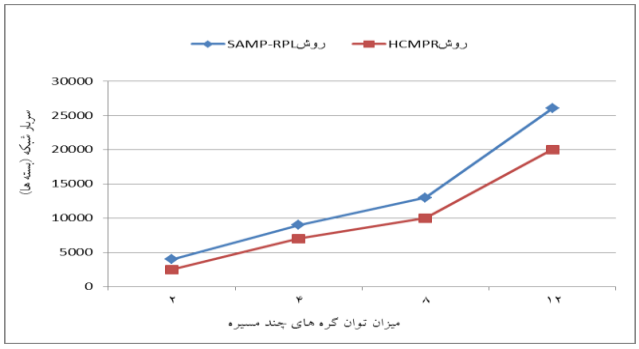
شکل۹: میانگین مصرف انرژی در طول زمان شبیه سازی

بطور کلی میانگین مصرف انرژی در روش HCMPR ۵۷.۲ ژول است و در روش SAMP-RPL ۶۷.۳۳ ژول است که روش HCMPR ۱۷.۷ درصد مصرف انرژی کاهش می‌یابد. عدم ارسال مجدد بسته از مبدا باعث کاهش سربار و درنتیجه کاهش مصرف انرژی می‌شود. شکل ۱۰ نتایج ارزیابی را برای ارزیابی کل هزینه‌های سربار ارتباطی در طول زمان شبیه سازی نشان می‌دهد. نتایج به‌دست‌آمده نشان می‌دهد که راه‌حل HCMPR به طور قابل‌توجهی میانگین سربار ارتباطی در طول زمان شبیه سازی را کاهش می‌دهد.



شکل۱۰: ارزیابی کل هزینه‌های سربار ارتباطی

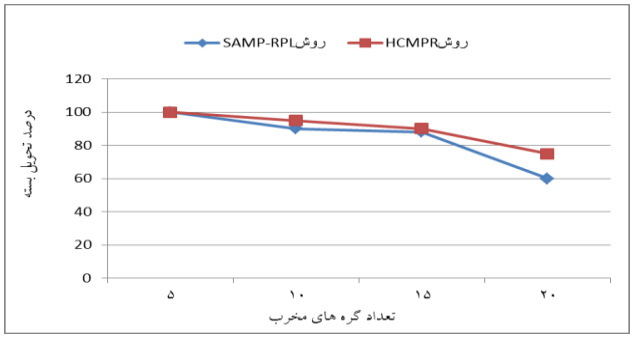
سربار شبکه یکی دیگر از پارامترهای مهم ارزیابی است. ما تعداد بسته‌های تولید شده توسط تمام گره‌های شبکه را در طول زمان شبیه سازی در نظر می‌گیریم. نتایج به‌دست‌آمده به وضوح نشان می‌دهد که راه‌حل HCMPR نتایج سربار شبکه پایینی را با راه‌حل چند مسیری مبتنی بر جستجوی عمقی چندگانه و تپه نوردی ارائه می‌کند. این امر با این واقعیت توجیه می‌شود که تکثیر بسته‌ها در راه حل مسیریابی چند مسیره HCMPR از سطح گره‌های فرزند شروع می‌شود و با در نظر گرفتن صف هر گره بسته ارسال می‌شود. سربار روش HCMPR ۲۷ درصد بهبود یافته است. شکل۱۱نتایج ارزیابی را برای ارزیابی سربار شبکه انباشته با افزایش مقادیر گره‌های چند مسیره در طول زمان شبیه سازی نشان می‌دهد. نتایج به‌دست‌آمده نشان می‌دهد که راه‌حل HCMPR به طور قابل‌توجهی میانگین سربار شبکه در طول زمان شبیه سازی را کاهش می‌دهد. از آنجایی که سربار شبکه با تعداد گره‌های چند مسیره رابطه مستقیم دارد، سربار شبکه انباشته شده را با افزایش مقادیر گره‌های چند مسیره ارزیابی کرده ایم. سربار روش HCMPR ۳۱ درصد کاهش یافته است.



شکل۱۱: سربار شبکه انباشته با افزایش مقادیر گره‌های چند مسیره

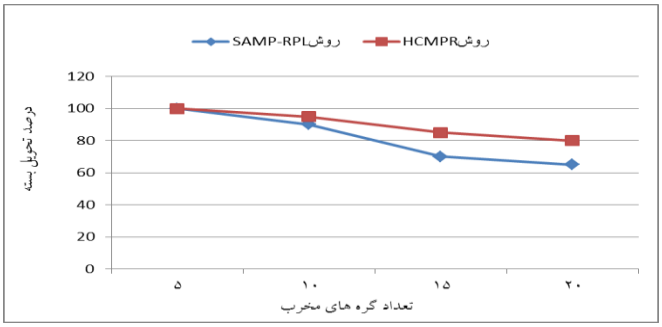
طرح‌های مسیریابی چند مسیری به دلیل مستعد بودن برای حملات سیبل شناخته می‌شوند که در آن مهاجم پیام‌های زیادی را با هویت جعلی ارسال می‌کند تا گره‌های اطراف باور کنندکه پیام‌ها از گره‌های مختلف منشأ می‌گیرند. به طور مشابه، در پروتکلRPL، یک گره مهاجم ممکن است بسیاری از پیام‌های DIO را با هویت‌های سرقت شده مختلف ارسال کند. در نتیجه چنین رفتار مخربی، گره‌های مشروع منبع فکر می‌کنند که گویی مسیرهای مجزای متعددی بین خود و ریشه ایجاد کرده‌اند، با این حال، این مسیرها به احتمال زیاد در یک یا چند گره مهاجم سیبل عبور می‌کنند. در روش HCMPR، هویت‌های گواهی شده مبتنی بر رتبه که با پیام‌های DIO ارتباط برقرار می‌کنند، مانع از سرقت هویت گره‌های دیگر توسط حملات سیبل می‌شود. در نتیجه، حمله سیبل به شبکه با روش HCMPR بسیار سخت است. از تعدادی گره‌های مخرب باحملا سیل، انتخابی رو به جلو و سیاه چاله استفاده شده است. در صورت حمله سیل، مهاجمان ترافیک پشت سر هم بسته‌های hello را به سمت ریشه ایجاد می‌کنند که ممکن است از ارسال بسته‌های قانونی توسط گره‌های میانی جلوگیری کند. گره‌های مخربی که حملات ارسال انتخابی را انجام می‌دهند، بسته‌های عبوری را به صورت انتخابی رها می‌کنند و در صورت حمله سیاه چاله، تمام بسته‌های دریافتی را رها می‌کنند.

شکل۱۲درصد تحویل بسته برای سناریوی حملات سیل را نشان می‌دهد. گره‌های مخرب بین ۵ تا ۲۰ گره تعیین می‌شود. نتایج نشان می‌دهد که روش HCMPR ۵.۵ درصد نرخ تحویل بسته را افزایش داده است.



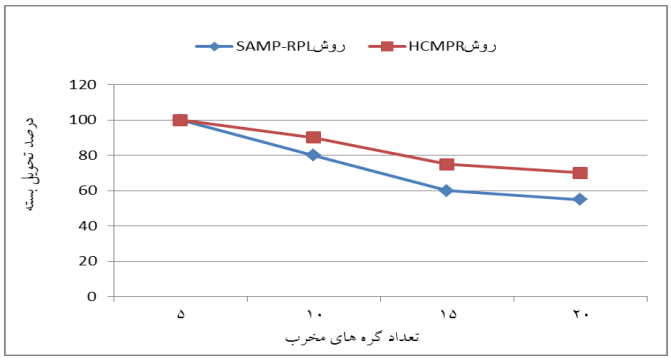
شکل۱۲:درصد تحویل بسته برای سناریوی حملات سیل

شکل۱۳درصد تحویل بسته برای سناریوی حملات ارسال انتخابی را نشان می‌دهد. گره‌های مخرب بین ۵ تا ۲۰ گره تعیین می‌شود. با افزایش تعداد گره‌های مخرب میزان بسته‌های تحویلی در روش HCMPR و روش SAMP-RPL کاهش می‌یابد. نتایج نشان می‌دهد که روش HCMPR میزان۹ درصد بسته بیشتری را نسبت به روش SAMP-RPL تحویل می‌دهد.



شکل۱۳: درصد تحویل بسته برای سناریوی حملات ارسال انتخابی

شکل۱۴درصد تحویل بسته برای سناریوی حملات سیاهچاله را نشان می‌دهد. گره‌های مخرب بین ۵ تا ۲۰ گره تعیین می‌شود. با افزایش تعداد گره‌های مخرب میزان بسته‌های تحویلی در روش HCMPR و روش SAMP-RPL کاهش می‌یابد. نتایج نشان می‌دهد که روش HCMPR میزان۱۰ درصد بسته بیشتری را نسبت به روش SAMP-RPL تحویل می‌دهد.



شکل۱۴: درصد تحویل بسته برای سناریوی حملات سیاهچاله

۵.بحث و نتیجه‌گیری

در این تحقیق الگوریتمی با عنوان ارائه یک الگوریتم چند مسیری مبتنی برروش ترکیبی جستجوی عمقی چندگانه و تپه نوردی برای بهبود قابلیت اطمینان و امنیت مسیرهای ارسال بسته در اینترنت اشیا ارائه شده است که هدف آن بهبود میزان سربار بسته ارسالی از مبدا به مقصد در شبکه، میزان سربار ارتباطی بین گره‌ها برای ارسال بسته، میزان درصد بسته تحویلی به مقصد، میزان انرژی مصرفی مبدا به مقصد و میزان نرخ ازدست دادن بسته است. نتایج حاصل از ارزیابی متغیرهای تحقیق این است که در روش HCMPR نسبت به روش پایه سربار ساخت درخت ۱۹.۵ درصد، انرژی ارتباطی ساخت درخت ۳۳ درصد و میانگین مصرف انرژی ۱۷.۷درصد کاهش یافته است. همچنین میانگین درصد تحویلی بسته ارسالی از مبدا به مقصد در طول زمان شبیه سازی ۳.۵ درصد، میانگین درصد تحویلی بسته ارسالی از مبدا به مقصد ۱۱.۲۵ درصد، سربار ارتباطی ۲۷ درصد، سربار انباشته شبکه ۳۱ درصد و نرخ تحویل بسته ۵.۵ درصد بهبود یافته است.

به عنوان کار آینده، ما قصد داریم امکان استفاده از گره‌های چندگانه مبتنی بر پهپاد را با راه حل خود بررسی کنیم و آن را در زمینه خاص تر مانند سناریوهای شهر هوشمند آزمایش کنیم .علاوه بر این، یک رویکرد یادگیری ماشین می‌تواند برای پیش بینی وقایع از دست دادن بسته اتخاذ شود .در حالت دوم، یک مطالعه کامل از هزینه‌های ناشی از آن و همچنین شرایط شبکه منجر به از بین رفتن بسته‌ها لازم خواهد بود.

۶.منابع

Reena Shinde, S.N. Shinde(۲۰۲٤) Hybrid Optimization Technique for Multipath Routing Mechanism in Internet of Things Lavasa, India Copyright © EAI DOI ۱۰,٤۱۰۸/eai.۲۳-۱۱-.۲۳٤۳۱۸٥

Niloofar Zahedy, Behrang Barekatain & Alfonso Ariza Quintana (۲۰۲٤) RI-RPL: a new high-quality RPL-based routing protocol using Q-learning algorithm Volume ۸۰, pages ۷٦۹۱–۷۷٤۹.

Jingxu Xiao, Chaowen Chang , Yingying Ma, Chenli Yang, Lu Yuan (۲۰۲٤) Secure multi-path routing for Internet of Things based on trust evaluation PMID: ۳۸٤٥٤۷۳۱ DOI: ۱۰,۳۹۳٤/mbe.۲۰۲٤۱٤۸

Abdelhamied A. Ateya, Sergey Bushelenkov, Ammar Muthanna, Alexander Paramonov, Andrey Koucheryavy, Samia Allaoua Chelloug , and Ahmed A. Abd El-Latif(۲۰۲۳) Multipath Routing Scheme for Optimum Data Transmission in Dense Internet of Things ۱۱, ٤۱٦۸. https://doi.org/۱۰,۳۳۹۰/ math۱۱۱۹٤۱٦۸

Yousefi HHN, Kavian Y, Mahmoudi A (۲۰۲۱) A Markov chain model for IEEE ۸۰۲,۱٥,٤ in time critical wireless sensor networks under periodic traffic with reneging packets. J Ambient Intell Human Comput. https:// doi. org/ ۱۰. ۱۰۰۷/ s۱۲٦٥۲- ۰۲۱- ۰۲۹۸٤-٦

Somia Sahraoui · Nabil Henni(۲۰۲۳) SAMP-RPL: secure and adaptive multipath RPL for enhanced security and reliability in heterogeneous IoT-connected low power and lossy Networks ۱٤, ٤۰۹–٤۲۹. https://doi.org/۱۰,۱۰۰۷/s۱۲٦٥۲-۰۲۱-۰۳۳۰۳-۹

Uma Meena, Promila Sharma (۲۰۲۲) Secret Dynamic Key Authentication and Decision Trust Secure Routing Framework for Internet of Things Based WSN Wireless Pers Commun ۱۲٥, ۱۷٥۳–۱۷۸۱ https://doi.org/۱۰,۱۰۰۷/s۱۱۲۷۷-۰۲۲-۰۹٦۳۲-y

K. Prathapchandran, T. Janani, M.Phil(۲۰۲۱)A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST doi.org/۱۰,۱۰۱٦/j.comnet.۱۰۸٤۱۳

Ali Seyfollahi, Meysam Moodi, Ali Ghaffari(۲۰۲۲) MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications ۱۰,۱۰۱٦/j.csi.۱۰۳٦۲۲ Elsevier B.V. All rights reserved.

Khatereh Ahmadi; Reza Javidan, (۲۰۲۲) Trust Based IOT Routing Attacks Detection Using Recurrent Neural Networks ۱۰,۱۱۰۹/SCIoT٥٦٥۸۳,۹۹٥۳۷۰۷ IEEE

Haitham Y. Adarbah; Mostafa Farhadi Moghadam; Rolou Lyn Rodriguez Maata; Amirhossein Mohajerzadeh; Ali H. Al-Badi, (۲۰۲۲) Security Challenges of Selective Forwarding Attack and Design a Secure ECDH-Based Authentication Protocol to Improve RPL Security۱۰,۱۱۰۹/ACCESS.۳۲۲۱٤۳٤ IEEE

Sridhar Manda, Charanjeet Singh(۲۰۲۳) CVFP: Energy and trust aware data routing protocol based on Competitive Verse Flower Pollination algorithm in IoT ۰۱٦۷-٤۰٤۸/© Elsevier Ltd. All rights reserved.

A. O. Bang, Udai Pratap Rao(۲۰۲۲) EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based internet of things Peer-to-Peer Netw. Appl. ۱٥, ٦٤۲–٦٦٥

Md. Mamunur Rashid, Joarder Kamruzzaman, Mohammad Mehedi Hassan,Tasadduq Imam, Santoso Wibowo, Steven Gordon, Giancarlo Fortino (۲۰۲۲)Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications ۰۱٦۷-٤۰٤۸/c Elsevier Ltd. All rights reserved.

F. Samie, L. Bauer, J. Henkel, IoT technologies for embedded computing, in: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis - CODES '۱٦, ۲۰۱٦, https://doi.org/۱۰,۱۱٤٥/۲۹٦۸٤٥٦,۲۹۷٤۰۰٤.

H. Suo, J. Wan, C. Zou, J. Liu, Security in the internet of things: a review, in: ۲۰۱۲ International Conference on Computer Science and Electronics Engineering, ۲۰۱۲, https://doi.org/۱۰,۱۱۰۹/iccsee.۲۰۱۲,۳۷۳.

Ajay Kumar, Ishan Budhiraja, Deepak Garg, Sahil Garg, Bong Jun Choi, Mubarak Alrashoud f (۲۰۲٥)Advanced network security with an integrated trust-based intrusion detection system for routing protocol https://doi.org/۱۰,۱۰۱٦/j.aej.۰۱,۰۸۷

D.K. Tosh, S. Shetty, P. Foytik, L. Njilla, C.A. Kamhoua, Blockchain-empowered secure Internet -of- Battlefield Things (IoBT) Architecture, in: MILCOM ۲۰۱۸ –۲۰۱۸ IEEE Military Communications Conference (MILCOM), ۲۰۱۸, https://doi.org/ ۱۰,۱۱۰۹/milcom.۲۰۱۸,۸٥۹۹۷٥۸.

multi-path algorithm based on the combined method of multi-depth search and hill climbing to improve the reliability and security of packet forwarding routes in the Internet of Things

Vazir Ahmad Tajik
Master student of Science in Artificial Intelligence Islamic Azad University Mashhad Department of Computer Engineering
Reza Sheibani
Member of the academic staff of Isalami Azad University, Mashhad branch

Abstract

Today, we can describe the Internet of Things as a pervasive and global network that provides a system for monitoring, controlling, processing and analyzing data generated by Internet of Things devices. Communication with IoT networks is not possible without the support of efficient infrastructure routing schemes. However, limitations related to low-power resources as well as the wireless and high-loss nature of IoT networks may severely affect the reliability of communication. As a result, routing efficiency can be affected. Additionally, exposure to internal and external cyber-attacks, especially those that threaten the availability of data and services, further complicates security missions and navigation in such a constrained context. In this thesis, an algorithm with the title of presenting a multi-path algorithm based on the combined method of multiple deep search and hill climbing to improve the reliability and security of packet sending paths in the Internet of Things is presented, which aims to improve the amount of packet overhead sent from the source to the destination in the network. , the amount of communication overhead between the nodes to send the packet, the percentage of the packet delivered to the destination, the amount of energy consumed from the source to the destination and the amount of packet loss rate. The evaluation results clearly show the effectiveness of the proposed solution to improve the reliability and security of communication, at a low cost.

Keywords: Multi path routing, Communication reliability, Network security, Internet of things, Multi depth search, Hill climbing