ارائه یک پروتکل مسیریابی امن در اینترنت اشیا برای مقابله و کشف حملات مسیریابی با مکانیسم مسیریابی بردار فاصله و اعتماد همسایگی

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

چکیده

اینترنت اشیا به شبکه‌ای متصل به هم مرتبط از دستگاه‌های هوشمند، حسگرها و رایانه‌های تعبیه‌شده اطلاق می‌شود که داده‌های ناهمگن را ذخیره پردازش می‌کنند. با افزایش مقیاس و پیچیدگی اینترنت اشیاء، نظارت بر امنیت اینترنت اشیاء دارای اهمیت و ضرورت خاصی می‌باشد. اینترنت اشیا با چالش‌های امنیتی بسیاری از جمله پیکربندی سیستم، ذخیره‌سازی و مدیریت امنیت اطلاعات، حفظ حریم خصوصی، کنترل دسترسی و احراز هویت مواجه است. در این مقاله یک الگوریتم مسیریابی امن در اینترنت اشیا ارائه می‌شود که با حملات سینک مقابله می‌کند. هدف اصلی از انجام تحقیق ارائه یک پروتکل مسیریابی امن در اینترنت اشیا برای مقابله و کشف حملات مسیریابی با مکانیسم مسیریابی بردار فاصله و اعتماد همسایگی می‌باشد. ابتدا میزان رتبه اعتماد هر گره براساس میانگین اعتماد همسایگان محاسبه می‌شود سپس ارسال بسته کشف گره همسایه مورد اعتماد با رتبه اعتماد بالا انجام می‌شود. در ادامه ارسال پیام کشف مسیرهای چندگانه از گره مبدا بر اساس جستجوی محلی با انتخاب K فرزند با بالاترین احتمال انتخاب رتبه اعتماد بالا و جستجوی K مسیر به سمت مقصد صورت می‌گیرد و در انتها کشف و حذف گره‌های مخرب از بسته‌های کشف مسیر توسط یک بسته کنترلی انجام می‌شود. بسته کنترلی با ارسال پیام به همه بسته‌ها، گره‌هایی که میزان اعتماد آن‌ها از میانگین اعتماد قابل قبول کمتر می‌باشند را به عنوان گره مخرب اعلام می‌کند. الگوریتم پیشنهادی با الگوریتم SOSRPL در محیط متلب شبیه سازی شدند. ارزیابی نتایج در سه سناریو به ترتیب ۱۰ درصد، ۲۰ درصد و ۳۰ درصد حمله سینک انجام شد. نتایج نشان می‌دهد که روش پیشنهادی کارایی بهتری در کاهش نرخ مثبت کاذب، منفی کاذب و نرخ بسته از دست رفته نسبت به روش SOSRPL دارد. همچنین روش پیشنهادی نرخ توان عملیاتی و نرخ بسته تحویلی بیشتری نسبت به روش SOSRPL دارد.

واژگان کلیدی:حملات مسیریابی-اینترنت اشیا- مدیریت داده- سیستم‌های هوشمند-سیستم‌های اعتماد-امنیت اطلاعات

۱.مقدمه

آغاز فناوری‌ها در اینترنت اشیا نشان‌دهنده سیگنال بعدی جامعه فراگیر اتباطات است (Kumar et al, ۲۰۲٤). شبکه‌های چندرسانه‌ای و پیوستگی مداوم آن‌ها با فناوری‌های یادگیری ماشین به طور کلی برای دریافت خدمات و برنامه‌های کاربردی هیجان‌انگیز برای مشاهده، لذت‌بخش، آموزش و عملکرد در خانه‌های هوشمند، شهرهای هوشمند، مناطق تپه‌ها (Sivakumar et al, ۲۰۲۳)، مراقبت‌های بهداشتی و حمل‌ونقل (Patel and Kumar, ۲۰۱۸) قابل پیش‌بینی هستند.

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. حجم عظیمی از داده‌های تولید شده توسط دستگاه‌های هوشمند هنگام انتقال و مسیریابی از طریق اینترنت چالش‌های متعددی را به همراه دارد .یکی از پروتکل‌های مسیریابی رایج در شبکه‌های اینترنت اشیا، RPL [۱](پروتکل مسیریابی برای شبکه‌های کم مصرف و با اتلاف) است، (Patel and Jinwala, ۲۰۲۲, Gong and Feng,۲۰۲۲). اما مستعد مسائل امنیتی و حملات است. 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 et al, ۲۰۲۲).

از آنجایی که وابستگی انسان‌ها به دستگاه‌ها روز به روز در حال افزایش است، از این رو، تقریباً در همه جنبه‌های زندگی روزمره خود توسط دستگاه‌ها احاطه شده است. همانطور که شبکه به بخشی جدایی ناپذیر از زندگی همه تبدیل می‌شود، فناوری‌های پیشرفته امنیت شبکه برای محافظت از داده‌ها در حال توسعه هستند(Choudhary and Kesswan, ۲۰۱۹). از طریق اینترنت اشیا، دامنه اینترنت با ادغام اشیای فیزیکی ایجاد می‌شود تا خود را به اشیای متقابل طبقه‌بندی کنند. یک شی فیزیکی می‌تواند با این ادراک مبتکرانه ایجاد شود تا خود را در دنیای دیجیتال نشان دهد. با افزایش اشیای مرتبط با اینترنت، نیاز به ساختارهای محافظت‌شده اهمیت زیادی داد، چون در معرض حملات متعدد قرار دارند. اینترنت اشیا به دلیل ویژگی‌های توزیع شده خود دارای نافرمانی مسیریابی خاصی هستند که به آن حمله حفره[۲] می‌گویند. در این حملات، یک گره مخرب اطلاعات واهی را در مورد مسیرها پخش می‌کند تا خود را به عنوان مسیری به سمت گره‌های خاص برای گره‌های همسایه تحمیل کند و در نتیجه ترافیک داده را جذب کند. مساله اساسی تحقیق مسیریابی امن در اینترنت اشیا برای مقابله و کشف حملات مسیریابی می‌باشد. در راستای این محدودیت‌ها یک پروتکل مسیریابی امن در اینترنت اشیا ارائه شد که برای مقابله و کشف حملات مسیریابی با مکانیسم مسیریابی بردار فاصله و اعتماد همسایگی استفاده می‌شود. هدف این تحقیق کاهش میزان منفی کاذب، کاهش میزان مثبت کاذب، افزایش میزان تشخیص حملات حفره سینک، افزایش توان عملیاتی و کاهش میزان بسته‌های حذف شده است (Zaminkar and Fotohi, ۲۰۲۰).

ابتدا میزان رتبه اعتماد هر گره براساس میانگین اعتماد همسایگان محاسبه می‌شود سپس ارسال بسته کشف گره همسایه مورد اعتماد با رتبه اعتماد بالا انجام می‌شود. در ادامه ارسال پیام کشف مسیرهای چندگانه از گره مبدا بر اساس جستجوی محلی با انتخاب K فرزند با بالاترین احتمال انتخاب رتبه اعتماد بالا و جستجوی K مسیر به سمت مقصد صورت می‌گیرد و در انتها کشف و حذف گره‌های مخرب از بسته‌های کشف مسیر توسط یک بسته کنترلی انجام می‌شود. بسته کنترلی با ارسال پیام به همه بسته‌ها، گره‌هایی که میزان اعتماد آن‌ها از میانگین اعتماد قابل قبول کمتر می‌باشند را به عنوان گره مخرب اعلام می‌کند. 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.

---

[۱] low-power and lossy networks

[۲] Sinkhole

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

اخیرا، انفجاری در تعداد دستگاه‌های اینترنت اشیا رخ داده است که منجر به عصر جدیدی از اتصالات و اشتراک‌گذاری داده‌های بی‌نظیر شده است(Burange et al, ۲۰۲٤). در قلمرو اینترنت اشیا، تضمین امنیت پیوندهای ارتباطی و ارزیابی ایمنی گره‌ها در این پیوندها همچنان یک چالش مهم است. تهدید مداوم پیوندهای غیرعادی، که دارای گره‌های مخرب هستند، خطراتی را برای انتقال داده بین گره‌های اینترنت اشیا و مراکز داده ایجاد می‌کند(Xiao et al, ۲۰۲٤).

در پژوهش(Mabodi et al, ۲۰۲۰)، یک روش کشف و پیشگیری از حمله حفره خاکستری از طریق اطلاع رسانی به سایر گره‌ها و مبتنی بر اعتماد چند سطحی مبتنی بر احراز هویت رمزنگاری در اینترنت اشیا پیشنهاد شده است. در این تحقیق متغیرهای نرخ مثبت کاذب، نرخ منفی کاذب و نرخ تشخیص مورد ارزیابی قرار می‌گیرند.

در پژوهش(Zaminkar and Fotohi, ۲۰۲۰) پروتکل مسیریابی امن اینترنت اشیاء در برابر حمله سینک با استفاده از رتبه گره مبتنی بر پروتکل RPL و مکانیسم رتبه‌بندی ارائه شده است. معیارهای ارزیابی نرخ تشخیص گره‌های مخرب، میزان منفی کاذب در شناسایی گره مخرب، میزان مثبت کاذب در شناسایی گره مخرب، نرخ بسته‌های ارسالی موفق و توان عملیاتی می‌باشد.

در پژوهش(KAVITHA et al,۲۰۲۲) یک الگوریتم مسیریابی امن در شبکه‌های مش اینترنت اشیا بر اساس تشابه اعتماد ارائه شده است. این الگوریتم محاسبه وزن پویا با استفاده از چندین تعامل، اعتماد کلی را محاسبه می‌کند.

در پژوهش(Ahmadi and Javidan, ۲۰۲۲) یک الگوریتم مسیریابی جهت 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 در صورت سناریوهای حمله RPL انجام شده است.

در پژوهش(Victor et at, ۲۰۲۲) یک الگوریتم مسیریابی کاهش حمله سینک در محیط اینترنت اشیاء مبتنی بر RPL با استفاده از تکنیک خوشه‌بندی KM[۱] بهینه شده ارائه شده است. این مقاله یک پروتکل مسیریابی ایمن برای شبکه‌های با توان کم و مبتنی بر خوشه‌بندی KM بهینه سازی شده ارائه می‌دهد. عملکرد الگوریتم بر روی معیارهای نسبت تحویل بسته، نرخ مثبت کاذب و نرخ منفی کاذب انجام شده است.

در پژوهش(Li et at, ۲۰۲۲) یک پروتکل جدید مسیریابی امن مبتنی بر کیفیت سرویس برای اینترنت اشیاء صنعتی به نام MCEAACO-QSRP[۲] ارائه شده است. به طور خاص، یک استراتژی بهینه‌سازی آشفته برای مقداردهی اولیه جمعیت طراحی شده است که تنوع جمعیت را افزایش می‌دهد و توانایی الگوریتم را برای پرش از بهینه محلی افزایش می‌دهد. علاوه بر این، استراتژی بهینه سازی تطبیقی برای تنظیم پویا روند الگوریتم طراحی شده است که به طور موثر سرعت همگرایی الگوریتم را بهبود می‌بخشد.

در پژوهش (Kumar et at, ۲۰۲۲) یک روش جداسازی حمله DDOS[۳] در اینترنت اشیا ارائه شده است. یک چشم انداز جدید در این کار تحقیقاتی، تکنیک احراز هویت متقابل است که گره‌های مخرب را از شبکه شناسایی و جدا می‌کند و در نتیجه تکنیک از سرگیری جلسه را برای به حداقل رساندن زمان اجرا بهبود می‌بخشد. تکنیک پیشنهادی پیاده سازی شده و همچنین از نظر پارامترهای خاصی با تکنیک موجود مقایسه شده است. این پارامترها عبارتند از: مصرف پهنای باند، سربار مسیریابی و نسبت تحویل بسته می‌باشد.

در پژوهش (Gangadharaiah and Bhajantri, ۲۰۲٤) الگوریتم انتشار و مسیریابی امن داده‌ها در اینترنت اشیا ارائه شده است. معماری پیشنهادی با اختصاص دادن این وظیفه به دروازه مقصد بدون به خطر انداختن محرمانگی و یکپارچگی داده‌ها در محیط

[۱] K means
[۲] multiobjective chaotic elite adaptive ant colony optimization
[۳] distributed denial of service

مسیریابی، رمزگذاری‌های متعدد را در این دستگاه‌های اینترنت اشیا با منابع محدود کاهش می‌دهد. الگوریتم پیشنهادی شامل یک طرح رمزگذاری مجدد پروکسی ترکیبی با زمان محدود است. این طرح از برچسب‌های محدود زمانی برای تعیین اعتبار بلوک‌های متن رمزی قابل استفاده مجدد استفاده می‌کند. این انتخاب طراحی منجر به زمان رمزگذاری و رمزگشایی سریعتر در مقایسه با الگوریتم‌های نامتقارن سنتی می‌شود. این تکنیک نوآورانه به طور موثر بار رمزگذاری چندگانه را بر روی گره‌های منبع اینترنت اشیاء با محدودیت انرژی کاهش می‌دهد و انتشار داده‌ها را برای مسیریابی ایمن در شبکه‌های نظیر به نظیر بهینه می‌کند. کارایی روش پیشنهادی در کاهش تأخیر، ترافیک شبکه، مصرف انرژی و همچنین زمان‌های رمزگذاری و رمزگشایی می‌باشد.

در پژوهش (Choukhairi et at, ۲۰۲٤) رویکرد اینترنت اشیا برای شناسایی و تجزیه و تحلیل ردیابی حمله فروچاله مبتنی بر روش آماری و پروتکلRPL ارائه شده است.

در پژوهش(Mona et at, ۲۰۲٤) الگوریتم جستجوی مبتنی بر ازدحام برای تشخیص موثر حمله فروچاله در اینترنت اشیا ائه شده است. در این مقاله، پیامدهای حمله فرورفتگی به اینترنت اشیا با جزئیات مورد بررسی و اثر حمله به دقت مورد تجزیه و تحلیل قرار گرفته است. علاوه بر این، یک روش کاهش منحصر به فرد را معرفی می‌کند که به طور ویژه برای مبارزه موثر با تهدیدهایی از این نوع ساخته شده است. این امر امکان ارزیابی توان عملیاتی شبکه و همچنین تاخیر کم و طول عمر بالای شبکه را فراهم کرده است.

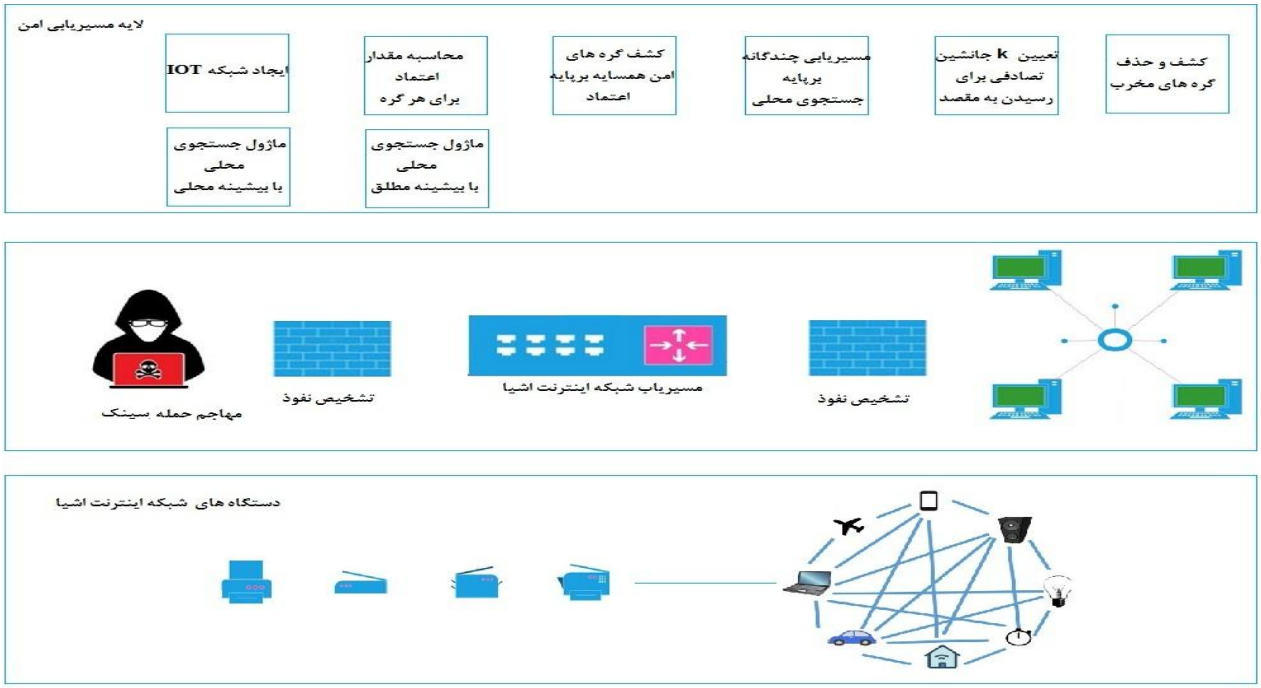
۳.روش تحقیق

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

۳-۱ مدل پیشنهادی تحقیق

در شکل۱ معماری پیشنهادی تحقیق است، تعداد n کاربر از طریق اینترنت و یک واسط نرم افزاری تحت وب به شبکه اینترنت اشیا متصل می‌شوند. شبکه اینترنت اشیا از تعدادی گره تشکیل می‌شود که گره‌ها در قالب گراف به یکدیگر متصل هستند. گره‌ها یا اشیاء در قالب قطعات کوچک، میکروکنترلرها، تراشه‌های الکترونیکی و مودم‌ها، در خانه و ابزارهای زندگی و محیط اطراف جاسازی شده‌اند. اشیا و وسایل محیط پیرامون به شبکه اینترنت متصل شده و توسط برنامه‌های کاربردی موجود در تلفن‌های هوشمند، تبلت، لپ تاپ و... قابل کنترل و مدیریت هستند. در لایه اول ابتدا یک شبکه اینترنت اشیا با N گره تصادفی در مکان‌های تصادفی ایجاد می‌شود. سپس برای هرگره یک مقدار اعتماد محاسبه می‌شود. ماژول مسیریابی چندگانه از گره مبدا به گره مقصد برپایه جستجوی محلی با کشف همسایه‌های امن انجام می‌شود. در صورت توقف جستجو در ماژول بیشینه محلی، k جانشین تصادفی برای ادامه جستجو انتخاب می‌شوند. با استفاده از ماژول جستجوی بیشینه مطلق مسیر رسیدن به مقصد شناسایی می‌شود.

در لایه بعدی همه مهاجم‌ها توسط یک لایه تشخیص نفوذ شناسایی می‌شوند و از لیست جدول مسیریابی حذف می‌شوند. در لایه بعدی دستگاه‌های اینترنت اشیا قرار دارند که در قالب یک گراف ایجاد شده اند.



شکل۱: معماری مدل پیشنهادی

۲-۳ روش پیشنهادی تحقیق

ابتدا به مفاهیم جستجوی محلی می‌پردازیم سپس روش پیشنهادی را بر مبنای جستجوی محلی بیان می‌کنیم. بهینه سازی به پیدا کردن مجموعه از ورودی‌ها برای یک تابع هدف گفته می‌شود که استفاده از آنها منجر به بیشینه یا کمینه شدن مقدار خروجی تابع هدف می‌شوند. ورودی‌ها می‌توانند پارامترها و وزن‌های دخیل باشند. بسیار متداول است که در مسائل، بهینه سازی در قالب دو عنوان محلی و سراسری توصیف کنند. در تحقیقات و الگوریتم‌های جستجویی که برای یافتن جواب بهینه ایجاد شده اند، دو شیوه متفاوت محلی و سراسری مطرح باشد.

بهینه سازی محلی: یک نقطه بهینه محلی یا بیشینه یا کمینه از تابع هدف است که در ناحیه محدود و مشخصی از ورودی پیدا شده و به دست آمده است. نوع تعریف یک تابع هدف، می‌تواند در فضای مسئله تعداد زیادی نقطه بهینه محلی داشته باشد؛ و حتی ممکن است تنها یک نقطه محلی بهینه در کل فضای مسئله ایجاد کند که در آن صورت همان نقطه بهینه عمومی است. در بهینه سازی محلی ما به دنبال نقطه‌ای هستیم که در واقع فقط به صورت محلی بهینه است، یعنی تابع هدف را فقط نسبت به نقاط نزدیک به خود کمینه یا بیشینه می‌کند اما لزوما جواب بهینه یا ماکزیمم مطلق نیست.

این نوع بهینه سازی تلاش می‌کند تا با شروع جستجو از نقطه ای، اولین نقطه بهینه‌ای را مکان یابی کند که تابع هدف را بیشینه یا کمینه می‌کند. الگوریتم‌های بهینه سازی محلی عموماً روی یک حالت منفرد به عنوان راه حل کاندید کار می‌کنند و تنها همان را در هر دوره تغییر می‌دهند؛ پس از اعمال هر تغییر کوچک روی راه حل کاندید، ارزیابی انجام می‌شود تا مشخص شود که بهبودی حاصل می‌شود و یا نه، و در صورت بهبود، آن را به عنوان کاندید جدید در نظر می‌گیرند. الگوریتم‌های جستجوی محلی هم می‌توانند نقطه بهینه سراسری را پیدا کنند، اگر نقطه بهینه محلی یکتا باشد و همان نقطه بهینه سراسری باشد یا اینکه مسیر و ناحیه جستجو شده شامل نقطه بهینه سراسری باشد و الگوریتم در همان نقطه توقف کند. این دو حالت، حالت‌های ایده آل و بهینه در استفاده از بهینه سازی محلی هستند.

بهینه سازی سراسری: بهینه ترین نقطه سراسری، نقطه‌ای است که در آن مقدار تابع هدف برای تمام فضای ورودی مسئله بهترین می‌شود. بهینه سازی سراسری یعنی الگوریتم برای پیدا کردن بهترین نقطه سراسری، مکانیزم‌هایی را به کار بگیرد تا بخش‌های بزرگتری از فضای مسئله را جستجو کند. یک تابع هدف در فضای ورودی‌های یک مسئله می‌تواند یکی یا بیشتر نقطه بهینه سراسری ایجاد کند. اگر نقاط بهینه سراسری در مسئله بیشتر از یکی باشد، آنگاه با یک مسئله چند نقطه روبرو هستیم که هر نقطه با ورودی‌های متفاوت به دست می‌آید اما ارزیابی و مقدار یکسانی را در تابع هدف ایجاد می‌کند. یک تابع هدف همیشه یک نقطه بهینه سراسری، همچنین می‌تواند نقاط بهینه محلی هم داشته باشد که در آنها مقدار تابع هدف به خوبی مقدار در بهینه سراسری نیست. وجود نقطه بهینه محلی در مسئله می‌تواند دشواری بهینه سازی سراسری را تعریف کند، چرا که پیدا کردن نقطه بهینه ملحی به نسبت آسان تر از پیدا کردن بهترین نقطه سراسری است. جستجوی سراسری هر دو به جستجو در فضای مسئله می‌پردازد تا نقطه بهینه سراسری را پیدا کند. الگوریتم جستجوی سراسری تمام یا بخش بسیار بزرگی از فضای ورودی‌های مسئله به تابع هدف را جستجو می‌کند تا بهترین نقطه را پیدا کند و می‌تواند به آن نزدیک شود یا دقیقاً خود آن را پیدا کند.

پروتکل مسیریابی مهمترین بخش برای ارسال بسته‌ها از یک گره به گره دیگر است و همچنین تکنیک خود را برای یافتن بهترین مسیر اتخاذ می‌کند. نوآوری روش تحقیق به اینصورت است که یک پروتکل مسیریابی چندگانه امن در شبکه اینترنت اشیا برای بهبود امنیت بسته‌های ارسالی به مقصد استفاده می‌کند. این پروتکل برای کشف مسیر امن از چند مسیر برای رسیدن به مقصد استفاده می‌کند که مراحل آن بصورت زیر است:

ابتدا یک بسته برای کشف همسایگان امن ارسال می‌کند. بعد از کشف همسایگان امن، بسته‌های با بالاترین رتبه انتخاب می‌شوند و با استفاده از روش جستجوی محلی بهینه بسته درخواست مسیر به همه گره‌های جانشین ارسال می‌شود. در هر مسیر گره‌های جانشین بهترین مسیرها را کشف می‌کنند و هر کدام از مقصد بسته پاسخ را برای گره مبدا ارسال می‌کنند. سپس از بین چندین مسیر کشف شده کوتاه ترین مسیر امن برای ارسال بسته انتخاب می‌شود. در هر مرحله بسته خرابی مسیر، خرابی در مسیر را کشف می‌کند و با ارسال بسته درخواست، مسیر بازسازی می‌شود در غیر اینصورت فرایند کشف مسیر مجددا انجام می‌شود.

فازهای روش پیشنهادی:

- محاسبه میزان رتبه اعتماد هر گره براساس میانگین اعتماد همسایگان
- ارسال بسته کشف گره همسایه مورد اعتماد با رتبه اعتماد بالا
- ارسال پیام کشف مسیرهای چندگانه از گره مبدا بر اساس جستجوی محلی با انتخاب K فرزند با بالاترین احتمال انتخاب رتبه اعتماد بالا و جستجوی K مسیر به سمت مقصد
- کشف و حذف گره‌های مخرب از بسته‌های کشف مسیر توسط یک بسته کنترلی. بسته کنترلی با ارسال پیام به همه بسته‌ها، گره‌هایی که میزان اعتماد آنها از میانگین اعتماد قابل قبول کمتر می‌باشند را به عنوان گره مخرب اعلام می‌کند.

۳-۲-۱ محاسبه رتبه اعتماد

در این بخش ابتدا مقدار اعتماد هر گره را محاسبه می‌کنیم سپس رتبه اعتماد محاسبه می‌شود. مقدار اعتماد هر گره از رابطه ۱ بدست می‌آید:

$$trust_{i,j} = \frac{m_{dlv}}{m_{sent}} \quad (۱)$$

بطوریکه که m_{dlv} تعداد بسته‌های گره i است که از طریق گره j تحویل داده می‌شود و m_{sent} تعداد کل بسته‌های ارسال شده توسط گره iبه گره j است.

میزان رتبه اعتماد هرگره براساس میانگین اعتماد همسایگان محاسبه می‌شود. ابتدا براساس پروتکل AOMDV، پیام‌های RREQ در شبکه پخش می‌شوند و جداول مسیریابی متعاقبا ایجاد می‌شوند. پس از ایجاد یک جدول مسیریابی، یک بسته سلام به گره‌های مجاور تک‌هاپ ارسال می‌شود. رتبه اعتماد هر گره از رابطه ۲ محاسبه می‌شود:

$$rank\_trust(n) = ParentRank\_trust(p) - NodeRank\_trust(n) \quad (۲)$$

برای شناسایی حملات حفره سینک، بررسی رتبه توسط گره i انجام می‌شود. هنگامی که حمله در شبکه صورت می‌گیرد، گره‌هایی که در واقع از یکدیگر دور هستند، همسایه می‌شوند و در نتیجه رتبه شبکه بصورت همسایگی ایجاد می‌شود.

۳-۲-۳ کشف مسیرهای چندگانه یا پیش مسیریابی

برای کشف مسیر از مسیریابی امن مبتنی بر پروتکل مسیریابی مبتنی برتقاضا بهبود یافته با استفاده از جستجوی محلی استفاده می‌کند. این پروتکل از چهار بسته کشف همسایه، بسته درخواست مسیر، بسته پاسخ و بسته کشف خرابی مسیر تشکیل شده است که در ادامه مراحل اجرای هر بسته تشریح خواهد شد:

ابتدا چند بسته کشف همسایگان از گره مبدا به همسایگان مستقیم ارسال می‌شود. برای هر گره میزان اعتماد خود آن و گره‌های همسایه را محاسبه نمود و به همراه فاصله گره تا همسایه در جدول مسیریابی ذخیره می‌شود. سپس بسته درخواست مسیر برای کشف چند مسیر یک پیام درخواست به تمام گره‌ها پخش می‌شود و یک مسیر امن مناسب تا مقصد جستجو می‌شود. برای جستجوی مسیرهای چندگانه با استفاده از الگوریتم جستجوی محلی چندین مسیر بهینه جستجو می‌شود. اگر در هر مسیر، تابع هدف به نتیجه رسید جستجوها متوقف می‌شوند و پیام پاسخ مسیر بهینه ارسال می‌شود. در هر مرحله جستجو از بین همسایگان گره‌ای که بالاترین میزان اعتماد دارد را بسط می‌دهیم. در صورتی که میزان اعتماد گره‌ها از گره والد کمتر باشند الگوریتم متوقف می‌شود. سپس از بین همسایگان k همسایه بصورت تصادفی انتخاب و بسط داده می‌شوند. به طوریکه احتمال انتخاب گره‌ها یک تابع افزایشی از تابع هدف باشد. در شکل ۲ شبه کد جستجو محلی مشاهده می‌شود.

```
Local_search()
begin
Start source node and extend successors node
if max_trust_succe(ni)>trust_ni
extend(max_trust_succe(ni));
else
Start with k randomly generated state
Loop:
All the successors of all k state are generated
```

```
If any one is a gol state then stop
Else select the k randomly best successors from the complete list of succesoors and repeat
end
```

شکل۲: شبه کد جستجو محلی

بسته پاسخ برای پاسخ به بهترین مسیر کشف شده از بین مسیرهای کشف شده مبدا به مقصد استفاده می‌شود. با استفاده از بسته خرابی مسیر درصورتیکه با ارسال پیام‌های فوق، خرابی در مسیر کشف شود و یا امنیت گره پایین باشد آنگاه گره فعلی با ارسال بسته درخواست مسیر بازسازی می‌شود در غیر اینصورت فرایند کشف مسیر مجددا انجام می‌شود.

۳-۲-۴ کشف و حذف گره‌های مخرب

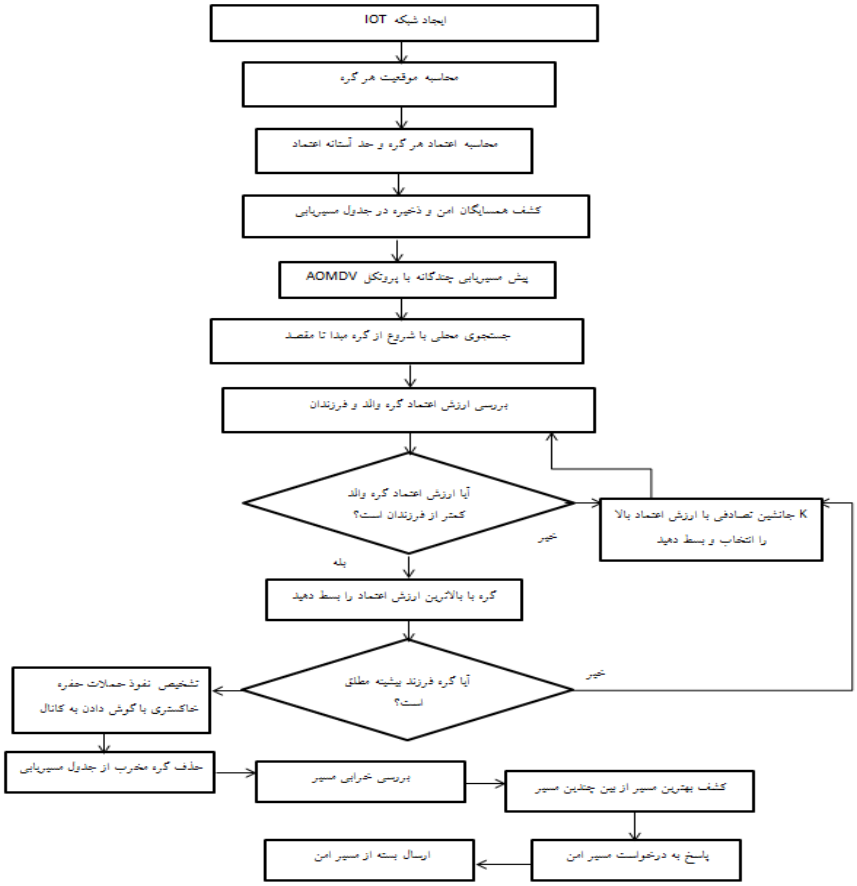
با عمل گوش دادن به گره مجاور، یک گره حفره سینک جستجو می‌شود. در اینجا، نرخ شنیدن در دوره N را به صورت رابطه ۳ تعریف می‌کنیم:

$$\text{listening(N)} = \left(\frac{\text{sum of forwarded packets}}{\text{sum of listened packets}}\right) \times 100 \quad (۳)$$

برای محاسبه نرخ گوش دادن، هر گره نرخ بسته‌های دریافتی و ارسال شده به بسته‌های شنیده شده را محاسبه می‌کند. اگر نرخ ارسال بسته یک گره کمتر از آستانه باشد، آن گره در مرحله بعد حفره سینک در نظر گرفته می‌شود. در نتیجه، بسته‌ها پس از شناسایی به گره‌های حفره سینک ارسال نمی شوند. در این مرحله، زمانی که یک گره به گره مجاور خود مشکوک می‌شود، شناسه گره مشکوک را به مبدا ارسال می‌کند. مقدار آستانه را ۰.۷ در نظر می‌گیریم. یعنی اگر بیش از ۳۰ درصد از بسته‌ها ارسال نشود، گره مشکوک است. سپس گره مبدأ از طریق مسیرهایی که دارای گره‌های مشکوک هستند، اقدام به یافتن مسیری به مقصد می‌کند.

۳-۳ فلوچارت روش پیشنهادی

در این بخش فلوچارت روش پیشنهادی ارائه می‌شود و بخش‌های مختلف آن مورد بررسی قرار می‌گیرد. شکل۳ فلوچارت روش پیشنهادی را نشان می‌دهد. در گام نخست یک شبکه اینترنت اشیا در قالب گراف با N گره ایجاد می‌شود. بعد از ایجاد شبکه، موقعیت گره‌ها در مکان هی تصادفی محاسبه می‌شود. برای هر گره میزان اعتماد محاسبه و سپس حد آستانه یا میانگین اعتماد همسایگان محاسبه می‌شود. سپس همسایگان امن شناسایی و کشف می‌شوند و در جدول مسیریابی ذخیره می‌شوند. در ادامه بعد از کشف همسایگان، با استفاده از پروتکل مسیریابی چندگانه AOMDV یک بسته درخواست مسیر ارسال می‌شود و اطلاعات همسایگان جمع آوری می‌شود. بسته‌های ارسالی از چندین مسیر به سمت مقصد ارسال می‌شوند و با جستجوی بهینه محلی محلی مبتنی بر اعتماد مسیرها جستجو می‌شوند. در هر مرحله اگر ارزش اعتماد گره والد از فرزندان کمتر باشد، از بین فرزندان گره با بالاترین ارزش اعتماد بسط داده می‌شود در غیر اینصورت K جانشین بصورت تصادفی با احتمال انتخاب گره‌های با ارزش اعتماد بالا انجام می‌شود. در ادامه بیشنه محلی و بیشینه مطلق جستجوی می‌شوند. در ادامه در هر مرحله با گوش داده به کانال گره‌های مخرب شناسایی و از جدول مسیریابی حذف می‌شوند. در انتها بسته پاسخ توسط گره مقصد از طریق مسیرهای کشف شده به سمت مبدا ارسال می‌شود. قبل از ارسال بسته پاسخ، توسط بسته خرابی مسیر، خرابی احتمالی مسیر کشف و بازسازی می‌شود و مسیریابی مجدد انجام می‌شود. و بسته از مسیر امن ارسال می‌شود.



شکل۳:فلوچارت روش پیشنهادی

۳-۴ شبه کد روش پیشنهادی

در این بخش شبکه کد روش پیشنهادی ارائه می‌شود و سپس به جزئیات آن می‌پردازیم. شکل۴ شبه کد مسیریابی امن روش پیشنهادی را نشان می‌دهد.

```
١.  Secure-routing()
٢.  Create iot network
٣.  Calculate trust for any node
٤.  Calculate threshold trust neighborhood
٥.  Send Hello message for Discovery neighborhood and save to routing table
٦.  Pre-roting with AOMDV protocol
٧.  Local Search from source node to destination node with call Local_search()
٨.  Intrusion detection malicious node
٩.  Delete malicious node from roting table
١٠. Send message RRER
١١. Send message RREP
١٢.  Send message secure_routing
١٣.  end
```

شکل۴: شبه کد مسیریابی امن روش پیشنهادی

در شکل۴ در سطر شماره ۱ تا ۳ شبکه اینترنت اشیا با N گره ایجاد می‌شود و مقدار اعتماد هر گره و مقدار حد آستانه اعتماد همسایگان محاسبه می‌شود. در سطر۴ پیام سلام برای کشف همسایگان ارسال می‌شود و در جدول سیریابی ذخیره می‌شود. در سطر ۵ پیش مسیریابی با پروتکل AOMDV انجام می‌شود. در سطر۶ عمل جستجوی مسیر امن از گره ابتدا تا گره مقصد با فراخوانی تابع جستجوی محلی بهینه شده انجام می‌شود. در ۷ و ۸ گره‌های مخرب شناسایی و سپس از جدول مسیریابی حذف می‌شوند. در سطر ۹ و ۱۰ پیام خرابی مسیر و پاسخ مسیر کشف شده به مبدا ارسال می‌شود. در سطر ۱۱ پیام از مسیر امن اسال می‌شود.

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 پیشنهادی، از روش پایه SOS-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 متلب ۲۰۱۹به عنوان ابزار شبیه‌سازی ارزیابی می‌شود و سپس نتایج مورد بحث قرار می‌گیرد. پارامترهای تنظیمات شبیه‌سازی و آزمایش به شرح جدول۱می‌باشد. در این جدول پارامترهای شبیه‌سازی در حالت اولیه آورده شده است.

جدول۱:تنظیمات اولیه شبیه سازی

پارامترها	مقادیر
MAC	۸۰۲.۱۱. b
تعداد گره	۵۰۰
سرعت	۱۵۰ متر بر ثانیه
اندازه بسته	۵۱۲بایت
ترافیک	CBR
زمان شبیه سازی	۲۰۰ ثانیه
درصد گره‌های آلوده	۱۰٪, ۲۰٪, ۳۰٪
نوع حمله	حملات سینک
نرخ انتقال	۲۰ مگابایت
انتخاب گره هدف	تصادفی

ابتدا یک شبکه اینترنت اشیا با تعداد ۵۰۰ گره ایجاد می‌شود. فاصله گره‌ها نسبت به یکدیگر بصورت تصادفی انتخاب می‌شود. سپس گره‌های آلوده بصورت تصادفی انتخاب می‌شود. لذا درهر بار شبیه‌سازی داده‌های شبیه‌سازی تغییر می‌کنند.

از سه سناریو برای شبیه سازی به شرح ذیل انجام می‌شود:

- در سناریوی اول نرخ گره‌های حملات سینک ۱۰درصد می‌باشد. توپولوژی فضای شبکه ۱۰۰×۱۰۰ متر می‌باشد. زمان شبیه‌سازی برای سناریوی اول ۱۰۰۰ ثانیه در نظر گرفته می‌شود.
- در سناریوی دوم نرخ گره‌های حملات سینک۲۰درصد می‌باشد. توپولوژی فضای شبکه ۱۰۰×۱۰۰ متر می‌باشد. زمان شبیه‌سازی برای سناریوی دوم ۱۰۰۰ ثانیه در نظر گرفته می‌شود.

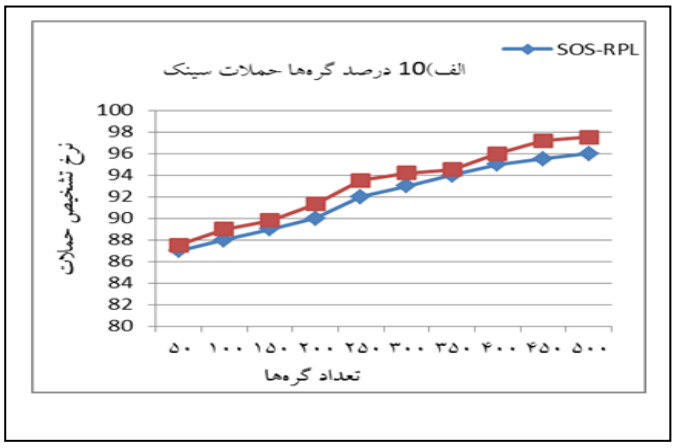
- در سناریوی سوم نرخ گره‌های حملات سینک۳۰درصد می‌باشد. توپولوژی فضای شبکه ۱۰۰×۱۰۰ متر می‌باشد. زمان شبیه‌سازی برای سناریوی سوم۱۰۰۰ ثانیه در نظر گرفته می‌شود.

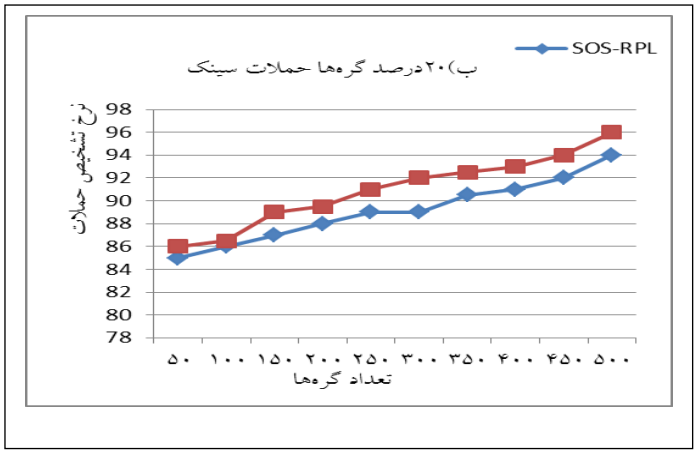
پارامترهای مورد ارزیابی شامل موارد ذیل می‌باشد:

- نرخ تشخیص حملات سینک برای تعداد مختلف گره‌ها
- نرخ منفی کاذب برای تعداد مختلف گره‌ها
- نرخ منفی کاذب برای تعداد مختلف گره‌ها
- نرخ بسته‌های تحویلی صحیح برای تعداد مختلف گره‌ها
- بیشترین توان عملیاتی برای تعداد مختلف گره‌ها

۴-۲ آزمایش و نتایج برای الگوریتم‌های پیشنهادی

طبق آزمایش‌های انجام شده برای روش پیشنهادی و روش SOS-RPL در شکل ۵ نرخ تشخیص حملات سینک برای تعداد گره‌های ۵۰ تا ۵۰۰ می‌باشد. بخش اول نرخ تشخیص مبتنی بر ۱۰ درصد گره‌های مخرب می‌باشد که برای روش پایه میانگین نرخ تشخیص خطا ۹۱.۹۵ و روش پیشنهادی ۹۳.۵ می‌باشد. با افزایش تعداد گره‌ها نرخ تشخیص حملات بیشتر می‌شود.

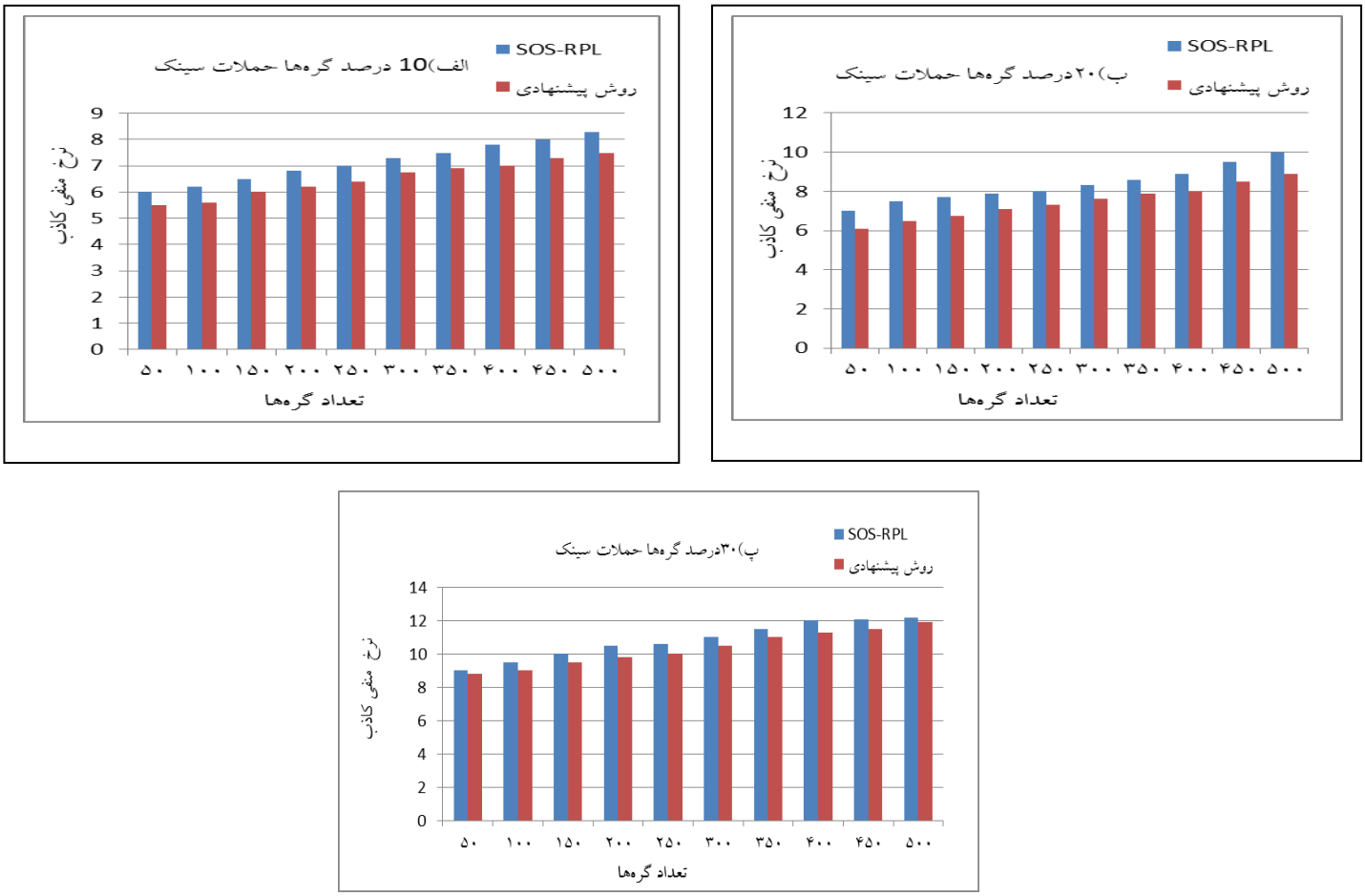




شکل۵: نرخ تشخیص حملات سینک برای تعداد گره‌های مختلف

با افزایش تعداد گره‌های مخرب به ۲۰ و ۳۰ درصد نرخ تشخیص حملات کاهش می‌یابد. برای ۲۰ درصد گره‌های مخرب نرخ تشخیص در روش پایه میانگین نرخ تشخیص خطا ۸۹.۱۵ و روش پیشنهادی ۹۰.۹۵ درصد می‌باشد. درصورتیکه ۳۰ درصد از گره‌ها مخرب باشند میانگین نرخ تشخیص خطا در روش پایه ۸۴.۵۵ و در روش پیشنهادی ۸۶.۴۱ می‌باشد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به روش پایه عملکرد بهتری دارد. روش پیشنهادی سعی می‌کند با اعتماد مستقیم و اعتماد غیرمستقیم گره‌هایی که میزان اعتماد آن‌ها از حد آستانه کمتر است را انتخاب نمی‌کند و به عنوان گره‌های مشکوک به حملات سینک شناسایی می‌کند. این عمل باعث می‌شود تا نرخ تشخیص حملات افزایش یابد.

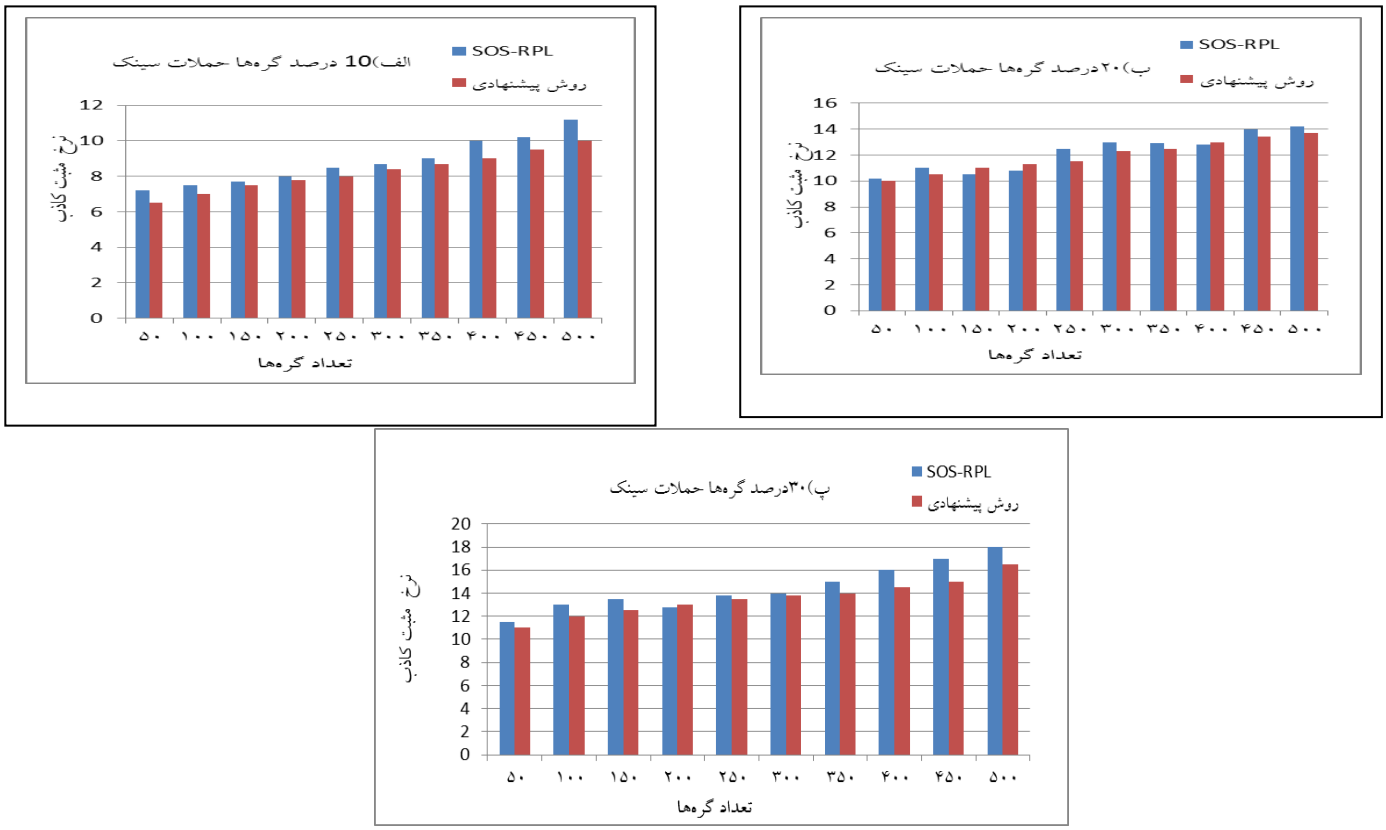
طبق آزمایش‌های انجام شده برای روش پیشنهادی و روش SOS-RPL در شکل ۶ نرخ منفی کاذب برای تعداد گره‌های ۵۰ تا ۵۰۰ می‌باشد. بخش الف نرخ منفی کاذب مبتنی بر ۱۰ درصد گره‌های مخرب می‌باشد. با افزایش تعداد گره‌ها نرخ منفی کاذب بیشتر می‌شود اما در روش پیشنهادی نرخ منفی کاذب نسبت به روش پایه کاهش دارد. با افزایش تعداد گره‌های مخرب به ۲۰ و ۳۰ درصد نرخ منفی کاذب نیز افزایش می‌یابد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به روش پایه عملکرد بهتری دارد. روش پیشنهادی مبتنی پروتکل مسیریابی مبتنی بر تقاضا سعی می‌کند گره‌های امن را از بین گره‌های همسایه کشف کند و گره‌های جعلی کمتر انتخاب می‌شوند.



شکل۶: نرخ منفی کاذب برای تعداد گره‌های مختلف

طبق آزمایش‌های انجام شده برای روش پیشنهادی و روش SOS-RPL در شکل۷ نرخ مثبت کاذب برای تعداد گره‌های ۵۰ تا ۵۰۰ می‌باشد. بخش الف نرخ مثبت کاذب مبتنی بر ۱۰ درصد گره‌های مخرب می‌باشد. با افزایش تعداد گره‌ها نرخ مثبت کاذب بیشتر می‌شود اما در روش پیشنهادی نرخ مثبت کاذب نسبت به روش پایه کاهش دارد.

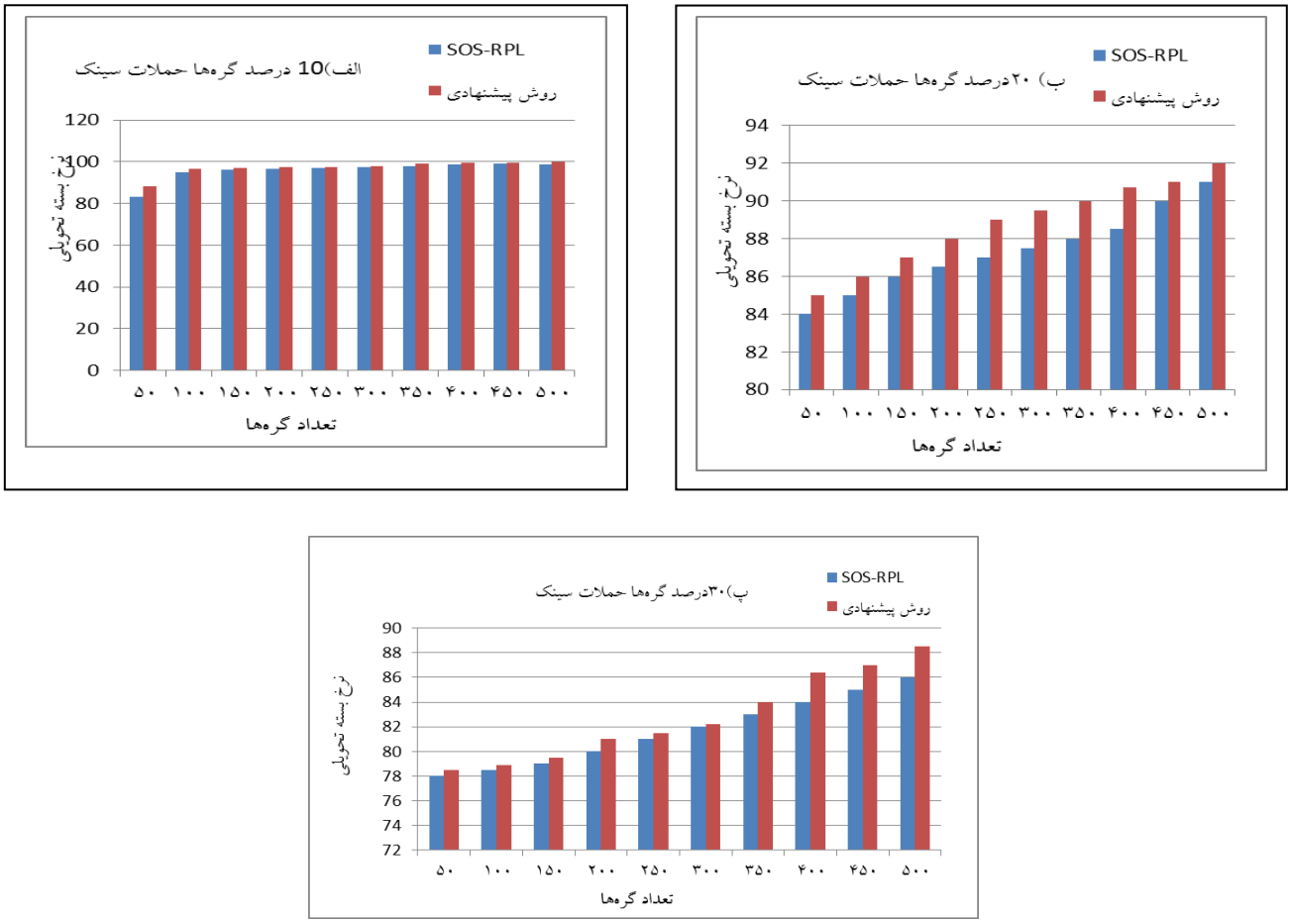
با افزایش تعداد گره‌های مخرب به ۲۰ و ۳۰ درصد نرخ مثبت کاذب نیز افزایش می‌یابد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به روش پایه عملکرد بهتری دارد. روش پیشنهادی مبتنی پروتکل مسیریابی مبتنی بر تقاضا سعی می‌کند گره‌های امن را از بین گره‌های همسایه مستقیم و همسایه‌های غیرمستقیم کشف کند و گره‌های جعلی کمتر انتخاب می‌شوند. لذا نرخ مثبت کاذب کاهش می‌یابد.



شکل۷: نرخ مثبت کاذب برای تعداد گره‌های مختلف

طبق آزمایش‌های انجام شده برای روش پیشنهادی و روش SOS-RPL در شکل۸ نرخ بسته تحویلی برای تعداد گره‌های ۵۰ تا ۵۰۰ می‌باشد. بخش الف نرخ بسته تحویلی مبتنی بر ۱۰ درصد گره‌های مخرب می‌باشد. در روش پیشنهادی درصد بسته تحویلی ۹۷.۳۹ و روش پایه ۹۵.۷۶ است. با افزایش تعداد گره‌ها نرخ بسته تحویلی بیشتر می‌شود اما در روش پیشنهادی نرخ بسته تحویلی نسبت به روش پایه افزایش بیشتری دارد. با افزایش تعداد گره‌های مخرب به ۲۰ و ۳۰ درصد نرخ بسته تحویلی کاهش می‌یابد. بطوری که نرخ بسته تحویلی در روش پایه ۸۷.۳۵ و در روش پیشنهادی ۸۸.۸۲ درصد برای سناریوی۲۰درصد گره مخرب می‌باشد. در زوش پیشنهادی نرخ بسته تحویلی ۸۳.۰۸ و روش پایه ۸۱.۵۵ برای سنایوی ۳۰ درصد گه مخرب می‌باشد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به روش پایه عملکرد بهتری دارد. در روش پیشنهادی هنگام مسیریابی بسته درخواست مسیر بهترین مسیر را شناسایی می‌کند و بسته

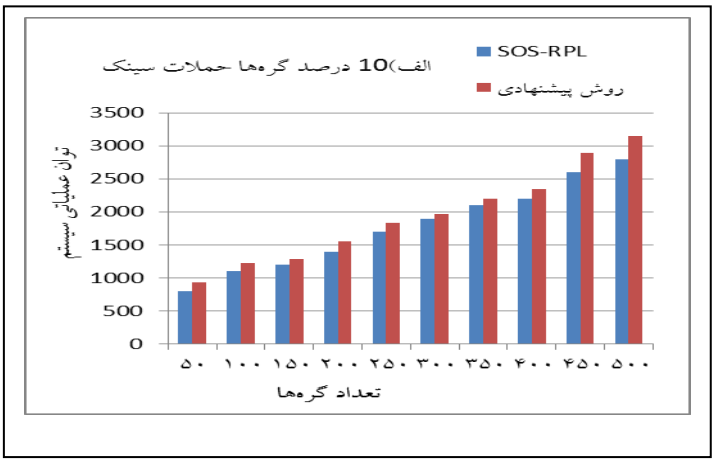
پاسخ مسیر، بهترین مسیر با گره‌هایی که رتبه اعتماد بالایی دارند را معرفی می‌کند. لذا نرخ بسته تحویلی به مقصد افزایش می‌یابد. همچنین در صورت خراب مسیر درخواست مسیر مجدد ارسال می‌شود و مسیر بازسازی می‌شود.

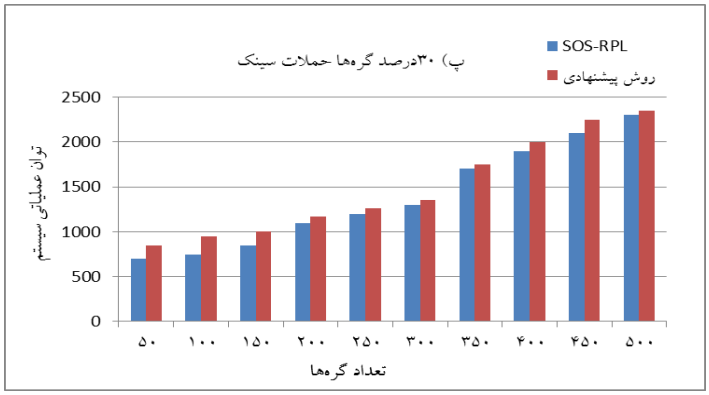


شکل۸: نرخ بسته تحویلی برای تعداد گره‌های مختلف

طبق آزمایش‌های انجام شده برای روش پیشنهادی و روش SOS-RPL در شکل۹ توان عملیاتی برای تعداد گره‌های ۵۰ تا ۵۰۰ می‌باشد. بخش الف توان عملیاتی مبتنی بر ۱۰ درصد گره‌های مخرب می‌باشد. با افزایش تعداد گره‌ها توان عملیاتی بیشتر می‌شود. میانگین توان عملیاتی برای سناریوی ۱۰ درصد گره آلوده، در روش پایه ۱۷۸۰ و در روش پیشنهادی ۱۹۳۸ است که در روش پیشنهادی ۱۵۸ واحد توان عملیاتی رشد داشته است. میانگین توان عملیاتی برای سناریوی ۲۰ درصد گره‌های آلوده، در روش پایه میانگین توان عملیاتی ۱۵۵۰ و در روش پیشنهادی ۱۶۶۳ می‌باشد. نتایج نشان می‌دهد که در روش پیشنهادی توان عملیاتی نسبت به روش پایه ۱۱۳ واحد افزایش دارد. و برای ۳۰ درصد گره آلوده، توان عملیاتی روش پایه ۱۳۹۰ و روش پیشنهادی ۱۴۹۳ است که روش پیشنهادی ۱۰۳ واحد توان بیشتری دارد.

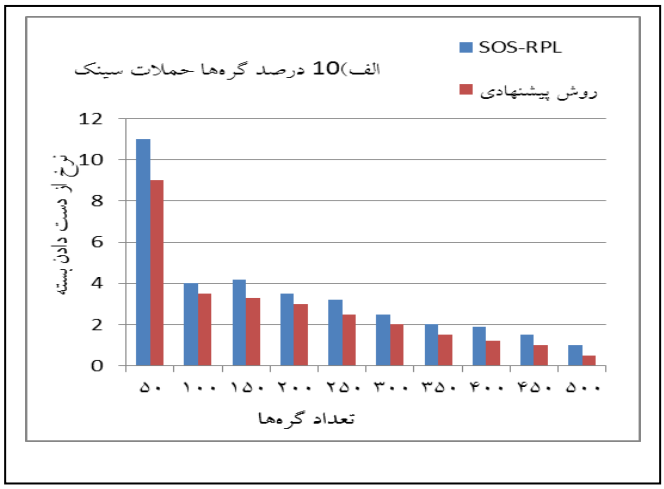
با افزایش تعداد گره‌های مخرب به ۲۰ و ۳۰ درصد توان عملیاتی کاهش می‌یابد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به روش پایه عملکرد بهتری دارد.

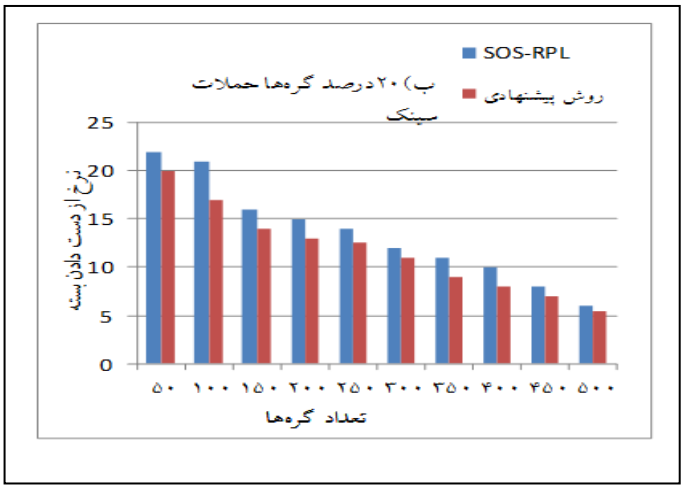


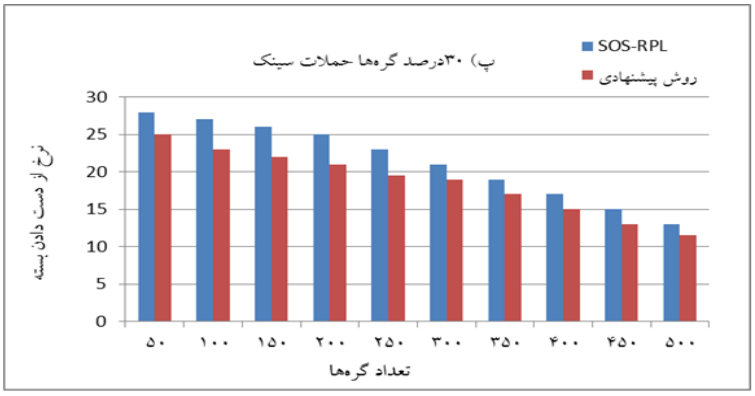


شکل۹: توان عملیاتی برای تعداد گره‌های مختلف

طبق آزمایش‌های انجام شده برای روش پیشنهادی و روش SOS-RPL در شکل ۱۰ نرخ از دست دادن بسته برای تعداد گره‌های ۵۰ تا ۵۰۰ می‌باشد.







شکل ۱۰: نرخ از دست دادن بسته برای تعداد گره‌های مختلف

بخش الف نرخ از دست دادن بسته مبتنی بر ۱۰ درصد گره‌های مخرب می‌باشد که این نرخ برای روش پایه ۳.۴۸ و روش پیشنهادی ۲.۷۵ است. با افزایش تعداد گره‌ها نرخ از دست دادن بسته کمتر می‌شود اما در روش پیشنهادی نرخ از دست دادن بسته نسبت به روش پایه کاهش دارد. با افزایش تعداد گره‌های مخرب به ۲۰ و ۳۰ نرخ از دست دادن بسته افزایش می‌یابد. نتایج نشان می‌دهد که روش پیشنهادی نسبت به روش پایه عملکرد بهتری دارد. در سناریوی ۲۰ درصد گره مخرب، نرخ از دست دادن بسته برای روش پیشنهادی ۱۱.۷ و روش پایه ۱۳.۵ است و در سناریوی ۳۰ درصد نرخ از دست دادن بسته برای روش پیشنهادی۲۱.۴ و روش پایه ۱۸.۶ است. روش پیشنهادی بعد از کشف همسایه‌های مورد اعتماد بسته‌ها را ارسال می‌کند و گره‌های همسایه با روش اعتماد غیرمستقیم گره‌های امن را انتخاب می‌کنند. هنگام کشف مسیر امن سعی می‌شود گره‌های مخرب کمتر انتخاب شوند در نتیجه میزان از دست دادن بسته‌ها کاهش می‌یابد. اما با افزایش گره‌های مخرب بسته‌های بیشتری ازدست داده می‌شوند. با این حال روش پیشنهادی نسبت به روش پایه بسته‌های کمتری را از دست می‌دهد.

۵.بحث و نتیجه‌گیری

در این تحقیق طراحی یک روش تشخیص حملات سینک در اینترنت اشیا مورد بررسی قرار گرفته است. روش پیشنهادی حملات را مبتنی پروتکل مسیریابی مبتنی بر تقاضا شناسایی می‌کند. راهکار پیشنهادی پروتکل مسیریابی مبتنی بر تقاضا ، اعتماد مستقیم و غیرمستقیم همسایگان را برای افزایش توان عملیاتی و کاهش نرخ از دست دادن بسته و افزایش نرخ تحویل بسته محاسبه می‌کند و احتمال انتخاب یک همسایه امن را برای ارسال بسته به گره‌های دیگر افزایش می‌یابد. برای برقراری اعتماد غیرمستقیم با گره‌های دیگر بر اساس اعتماد مستقیم باعث کاهش نرخ منفی کاذب و کاهش نرخ مثبت کاذب می‌شود. الگوریتم پیشنهادی با یکی از الگوریتم‌های شناخته شده به نام SOS-RPL مقایسه شد. ارزیابی نتایج در سه سناریو به ترتیب ۱۰ درصد، ۲۰ درصد و ۳۰ درصد حمله سینک انجام شد. نتایج نشان می‌دهد که روش پیشنهادی کارایی بهتری در کاهش نرخ مثبت کاذب، منفی کاذب و نرخ بسته از دست رفته نسبت به روش SOS-RPL دارد. همچنین روش پیشنهادی نرخ توان عملیاتی و نرخ بسته تحویلی بیشتری نسبت به روش SOS-RPL دارد.

برای کارهای آینده، استفاده از رایانش مه برای مدیریت اعتماد و بهبود مصرف انرژی در شبکه اینترنت اشیا توصیه می‌شود. همچنین یکی از روش‌های دیگری که می‌توان برای مسیریابی امن در اینترنت اشیاء استفاده نمود، استفاده از درخت تصمیم می‌باشد. با استفاده از این روش می‌توان حملات مسیریابی را شناسایی و مسیرهای معتبر را پیشنهاد داد. و بطور کلی برای تحقیقات آتی می‌توان از روش‌هایی مانند الگوریتم‌های هوشند مبتنی بر روش فازی و مبتنی بر یادگیری ماشین استفاده کرد.

۶.منابع

V. G. Sivakumar, V. V. Baskar, M. Vadivel, S. P. Vimal, and S. Murugan,(۲۰۲۳) “IoT and GIS integration for real-time monitoring of soil health and nutrient status,” in International Conference on Self Sustainable Artificial Intelligence Systems, ICSSAS ۲۰۲۳ - Proceedings, Oct. pp. ۱۲٦٥–۱۲۷۰, doi: ۱۰,۱۱۰۹/ICSSAS٥٧٩١٨,٢٠٢٣,١٠٣٣١٦٩٤.

N. R. Patel and S. Kumar, “Wireless sensor networks(۲۰۱۸)’ challenges and future prospects,” in Proceedings of the ۲۰۱۸ International Conference on System Modeling and Advancement in Research Trends, SMART ۲۰۱۸, Nov. ۲۰۱۸, pp. ٦۰–٦٥, doi: ۱۰,۱۱۰۹/SYSMART.٨٧٤٦٩٣٧

Mohanavel Jothish Kumar, Suman Mishra, Elangovan Guruva Reddy, Madasamy Rajmohan, Subbiah Murugan, Narayanasamy Aswin Vignesh(۲۰۲٤) Bayesian decision model based reliable route formation in internet of things Indonesian Journal of Electrical Engineering and Computer Science Vol. ۳٤, No. ۳, June ۲۰۲٤, pp. ۱٦٦٥~۱٦۷۳ ISSN: ۲٥۰۲-٤۷٥۲, DOI: ۱۰,۱۱٥۹۱/ijeecs.v۳٤.i۳.pp۱٦٦٥-۱٦۷۳

A. Patel and D. Jinwala(۲۰۲۲), "A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things", Int. J. Commun. Syst., vol. ۳٥.

X. Gong and T. Feng,(۲۰۲۲) "Lightweight anonymous authentication and key agreement protocol based on CoAP of Internet of Things", Sensors, vol. ۲۲, no. ۱۹, pp. ۷۱۹۱.

Haitham Y. Adarbah; Mostafa Farhadi Moghadam; Rolou Lyn Rodriguez Maata; Amirhossein Mohajerzadeh; Ali H. Al-Badi,(۲۰۲٤) Security Challenges of Selective Forwarding Attack and Design a Secure ECDH-Based Authentication Protocol to Improve RPL Security ۱۰,۱۱۰۹/ACCESS.۳۲۲۱٤۳٤

Kobra Mabodi, Mehdi Yusefi, Shahram Zandiyan, Leili Irankhah, Reza Fotohi, (۲۰۲۰) Multi level trust based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication © Springer Science+Business Media, LLC, part of Springer Nature

M Zaminkar · R Fotohi (۲۰۲۰) SoS RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism © Springer Science+Business Media, LLC, part of Springer Nature

Jingxu Xiao, Chaowen Chang, Yingying Ma, Chenli Yang and Lu Yuan(۲۰۲٤) Secure multi-path routing for Internet of Things based on trust evaluation licensee AIMS Press MBE, ۲۱(۲): ۳۳۳٥–۳۳٦۳. DOI: ۱۰,۳۹۳٤/mbe.۲۰۲٤۱٤۸

Anup W. Burange, Vaishali M. Deshmukh, Yugandhara A. Thakare , Nitin Arvind Shelke (۲۰۲٤) Safeguarding the Internet of Things: Elevating IoT routing security through trust management excellence doi.org/۱۰,۱۰۱٦/j.csi.۱۰۳۸۷۳

Choudhary S, Kesswani N. (۲۰۱۹) A survey: intrusion detection techniques for internet of things. Int J Inform Security Privacy (IJISP);۱۳(۱):۸٦–۱۰٥.

Upendra Kumar,Shreyshi Navaneet, Neeraj Kumar, Subhash Chandra Pandey(۲۰۲۰) Isolation of DDoS Attack in IoT: A New Perspective © Springer Science+Business Media, LLC, part of Springer Nature

Chaoqun Li; Yang Liu; Jing Xiao; Jie Zhou (۲۰۲۲) MCEAACO-QSRP: A Novel QoS-Secure Routing Protocol for Industrial Internet of Things ۱۰,۱۱۰۹/JIOT..۳۱٦۲۱۰٦

Martin Victor K, Immanuel Johnraja Jebadurai, Getzi Jeba Leelipushpam Paulraj, Jebaveerasingh Jebadurai (۲۰۲۲) Mitigating Sinkhole attack in RPL based Internet of Things Environment using Optimized K means Clustering technique ۹۷۸-۱-٦٦٥٤-۸۲۷۱-٤/۲۲ IEEE

Khatereh Ahmadi, Reza Javidan(۲۰۲۲) Trust Based IOT Routing Attacks Detection Using Recurrent Neural Networks ۹۷۸-۱-٦٦٥٤-۸۸۹۱-٤/۲۲ IEEE

ATHOTA KAVITHA, VIJENDER BUSI REDDY, NINNI SINGH, VINIT KUMAR GUNJAN, KURUVA LAKSHMANNA, ARFAT AHMAD KHAN, AND CHITAPONG WECHTAISONG(۲۰۲۲) Security in IoT Mesh Networks Based on Trust Similarity ۱۰,۱۱۰۹/ACCESS.۳۲۲۰٦۷۸ IEEE

S. Gangadharaiah, Lokesh B. Bhajantri (۲۰۲٤) Secure data dissemination and routing in Internet of Things
Int. j. inf. tecnol. https://doi.org/۱۰,۱۰۰۷/s٤۱۸۷۰-۰۲٤-۰۱۸٤۸-٤

Mouad Choukhairi, Sara Tahiri, Youssef Fakhri, Mohamed Amnai & Ali Choukri (۲۰۲٤) IoT Approach to Detect and Analyze Sinkhole Attack Traces in the RPL Protocol BDIoT. Lecture Notes in Networks and Systems, vol ۸۸۷. Springer, Cham. https://doi.org/۱۰,۱۰۰۷/۹۷۸-۳-۰۳۱-۷٤٤۹۱-٤_۲۷

Mona R, Manoranjitham R(۲۰۲٤), Swarm Based Searching Method for Effective Sinkhole Attack Detection in Internet of Things Swarm Based Searching Method for Effective Sinkhole Attack Detection in Internet of Things. ۱۰,۱۱۰۹/ICCSC٦۲۰٤۸,۱۰۸۳۰۳۳۱ IEEE

Providing a secure routing protocol in Internet of Things to counter and detect routing attacks with distance vector routing mechanism and neighborhood trust

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

The Internet of Things refers to an interconnected network of smart devices, sensors, and embedded computers that store and process heterogeneous data. With the increasing scale and complexity of the Internet of Things, monitoring the security of the Internet of Things is of particular importance and necessity. The Internet of Things faces many security challenges, including system configuration, information security storage and management, privacy, access control, and authentication. In this paper, a secure routing algorithm in the Internet of Things is presented that combats sink attacks. The main goal of the research is to present a secure routing protocol in the Internet of Things to combat and detect routing attacks with the distance vector routing mechanism and neighbor trust. First, the trust rating of each node is calculated based on the average trust of its neighbors, then a discovery packet is sent to the trusted neighbor node with a high trust rating. Next, the multiple path discovery message is sent from the source node based on local search by selecting K children with the highest probability of selecting a high trust rank and searching for K paths towards the destination, and finally, the detection and removal of malicious nodes from the path discovery packets is performed by a control packet. The control packet, by sending a message to all packets, declares nodes whose trust level is lower than the acceptable trust average as malicious nodes. The proposed algorithm was simulated with the SOSRPL algorithm in the MATLAB environment. The results were evaluated in three scenarios of ۱۰٪, ۲۰٪ and ۳۰٪ sink attack, respectively. The results show that the proposed method has better efficiency in reducing the false positive rate, false negative rate and packet loss rate than the SOSRPL method. The proposed method also has a higher throughput rate and packet delivery rate than the SOSRPL method.

Keywords: Attaks rout, iot, data management, Intelligent systems,Trust systems, Information securi**.**