دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۱ (۷۵-۸۲)
https://monadi.isc.org.ir

ارائه‌شده در هجدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه اصفهان، ۱۰ و ۱۱ شهریور ۱۴۰۰

ارائه یک روش مسیریابی قابل اعتماد مبتنی بر RPL در اینترنت اشیا★

رضا خاتونی* و محمد قاسمی گل

گروه مهندسی کامپیوتر، دانشگاه بیرجند، بیرجند، ایران

اطلاعات مقاله

کلمات کلیدی:
اینترنت اشیا
شبکه‌های کم‌توان و پراتلاف
پروتکل مسیریابی RPL
مسیریابی قابل اعتماد.

dor: 20.1001.1.24763047.1401.11.1.9.6

نوع مقاله: پژوهشی

چکیده

امروزه برقراری یک مسیر ارتباطی قابل اعتماد بین دستگاه‌های موجود در شبکه‌های کم‌توان و پراتلاف (LLNs) به چالشی بزرگ تبدیل شده است. پروتکل مسیریابی شبکه‌های کم‌توان و پراتلاف (RPL) به عنوان یک پروتکل مسیریابی استاندارد در شبکه‌های LLN مورد استفاده قرار می‌گیرد. پروتکل RPL که در لایه شبکه قرار دارد، از تابع هدف برای انتخاب مسیر بهینه استفاده می‌کند. با توجه به اینکه در فرآیند مسیریابی ممکن است حملات مختلفی ایجاد شود، از این رو لزوم توجه به مسیریابی مطمئن و مورد اعتماد به یکی از مسائل به‌روز و مهم پژوهشی تبدیل شده است. به همین علت، در این پژوهش یک روش مسیریابی قابل اعتماد مبتنی بر RPL برای اینترنت اشیا ارائه شده است. مزایای روش پیشنهادی در مقایسه با سایر روش‌های مقایسه شده در این است که از یک سو با وجود حملات مشهوری چون حمله رتبه و Sybil، نرخ بسته‌های از دست رفته کاهش یافته است و از سوی دیگر میزان پایداری یک گره نسبت به تغییرات رتبه بیشتر شده است. در نهایت، برای ارزیابی روش پیشنهادی از شبیه‌ساز Cooja استفاده شده است.

۱ مقدمه

امروزه گسترش روزافزون شبکه‌های حسگر بی‌سیم و شبکه‌های اینترنت اشیا به راحتی قابل درک است. دلیل اصلی این گسترش را می‌توان در توسعه فناوری‌ها و زیرساخت‌های ارتباطی جستجو کرد. چرا که روز به روز دستگاه‌ها و سیستم‌های متعددی با اتصال به اینترنت به این شبکه‌ی عظیم می‌پیوندند. واژه اینترنت اشیا نخستین بار توسط کوین اشتون در سال ۱۹۹۹ به کار برده شد. در واقع اینترنت اشیا را می‌توان یکی از مهم‌ترین عوامل تاثیرگذار بر زندگی مردم دانست چرا که زندگی بشر را با استفاده از فناوری‌های روز دچار تحولی شگرف کرد.

با پیشرفت روزافزون میکروکنترولرها و تکنولوژی میکروالکترونیک تجهیزاتی که اشیای هوشمند نامیده می‌شوند زمینه ظهور پیدا کرده‌اند. یک شی هوشمند یک دستگاه کوچک میکروالکترونیکی است که شامل قطعه ارتباطی (معمولا رادیویی کم‌توان)، ریزپردازنده‌ای کوچک و یک حسگر یا عملگر هست. در کاربردهای مختلف از تعداد وسیعی از اشیای هوشمند استفاده می‌گردد و این اشیا شبکه‌هایی تشکیل می‌دهند که به دلیل ویژگی‌های خاص اشیای هوشمند شبکه‌های کم‌توان و پراتلاف [1] نامیده می‌شوند. در این گونه شبکه‌ها از رادیوهای ارتباطی کم‌توان و با نرخ ارسال محدود استفاده می‌شود. تلاش‌های بسیاری در زمینه قدرتمندسازی تجهیزات شبکه‌های کم‌توان و پراتلاف از لحاظ سخت‌افزاری صورت گرفته است و همچنین ساده‌سازی پروتکل‌های موجود، تدوین وطراحی پروتکل‌های جدید مخصوص اینگونه تجهیزات، قدرت اتصال آن‌ها به اینترنت را فراهم آورده است. کارگروه مهندسی اینترنت [2]، برای اینکه

★از کمیته علمی هجدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: rezakhatooni@birjand.ac.ir (رضا خاتونی)، ghasemigol@birjand.ac.ir (محمد قاسمی گل)

[1] low-power and lossy networks [2] internet engineering task force

پروتکل‌های مسیریابی موجود در شبکه‌های کم‌توان و پراتلاف نمی‌توانستند امنیت ارتباطات بین دستگاه‌های با منابع محدود را به خوبی برقرار کند، پروتکل مسیریابی IPv6 را برای شبکه‌های کم‌توان و پراتلاف (RPL) [۱] معرفی کرد. تکنولوژی RPL در جهت برآوردهای نیازهای حوزه وسیعی از کاربردهای LLN از قبیل اتوماسیون ساختمان، شبکه‌های حسگر شهری و شبکه‌های هوشمند برق در نظر گرفته شده است.

به طور کلی، شبکه‌های کم‌توان و پراتلاف (LLNs) که تشکیل شده‌اند از دستگاه‌هایی با توان پردازشی، حافظه و انرژی محدود، نقش مهم و اساسی در شبکه‌های اینترنت اشیا ایفا می‌کنند. به علاوه، پروتکل RPL که توسط کارگروه مهندسی اینترنت معرفی شده است، یک مورد مناسب و رایج برای مسیریابی در دستگاه‌های با منابع محدود است که در لایه شبکه کار می‌کند. نحوه‌ی کار پروتکل RPL بدین صورت است که مسیرها را به سرعت می‌سازد و در عین حال اطلاعات مسیر را نیز به طور موثر بین سایر گره‌ها در شبکه اینترنت اشیا توزیع می‌کند. پروتکل RPL برای نشان دادن ساختار شبکه و نحوه قرارگیری گره‌های حسگر از توپولوژی شبیه درخت بهره می‌برد که گراف بدون دور جهت‌دار (DAG) نامیده می‌شود. همچنین اطلاعات مربوط به توپولوژی RPL نیز در ساختاری شبیه درخت به نام گراف بدون دور جهت‌دار مقصدگرا (DODAG) نگهداری می‌شود. به طور کلی، مجموعه مسیرهایی که بسته‌های داده را از گره‌های فرستنده به گره سینک منتقل می‌کنند، DODAG را تشکیل می‌دهند. RPL این DODAG را با استفاده از تابع هدف ایجاد می‌کند. به طور کلی، توابع هدف معیارهای مسیریابی را بهینه یا محدود می‌کنند تا بدین طریق نقش خود را در انتخاب بهترین مسیر به درستی ایفا کنند. هر DODAG توسط ۴ عامل شناسه منحصربه فرد DODAG، شماره نسخه DODAG، شناسه منحصر به فرد نمونه RPL و رتبه (Rank) مشخص می‌شود [۲]. پروتکل RPL در شبکه‌های کم‌توان و پراتلاف، مسیرها را با استفاده از دو تابع هدف یعنی MRHOF و تابع هدف OF0 ایجاد می‌کند. MRHOF [۳] برای پیدا کردن مسیری با کمترین هزینه در شبکه طراحی شده است. همچنین، تابع هدف (OF0) برای پیداکردن نزدیک‌ترین مسیر به ریشه ارائه شده است.

نوآوری‌های مقاله شامل موارد زیر است:

(۱) در این مقاله، روشی جدید مبتنی بر اعتماد روی پروتکل مسیریابی RPL ارائه شده است تا این پروتکل را در مقابل حملات رتبه و Sybil مقاوم سازد.

(۲) در این مقاله، روش پیشنهادی با شبیه‌سازی با دو روش موجود برای ایمن‌سازی RPL یعنی پروتکل RPL استاندارد و Sec-Trust RPL مقایسه شده است.

مطالب این مقاله در قالب پنج بخش آورده شده است. بخش ۲ دربرگیرنده پژوهش‌های مرتبط با موضوع پیشنهادی و معرفی روش پیشنهادی است. در بخش ۳ نتایج به دست آمده از شبیه‌سازی ارزیابی شده است. بخش ۴ یا بخش نهایی نیز به نتیجه‌گیری اختصاص یافته است.

۲ مطالب اصلی

تحقیقاتی که تا کنون بر روی شبکه‌های حسگر بی‌سیم انجام شده اکثرا روی مصرف انرژی و روش‌های مسیریابی مانند پروتکل مسیریابی برای شبکه‌های کم‌توان (PRL) تمرکز دارند. چانگ [۱] و همکارانش، یک مکانیزم مسیریابی انرژی محور مبتنی بر معیارهای تعداد انتقالات مورد انتظار (ETX) و انرژی باقی‌مانده برای بهبود پروتکل مسیریابی PRL مطرح کرده‌اند. این مکانیزم باعث افزایش طول عمر شبکه شده است. همچنین مصرف انرژی گره‌های شبکه را نیز به تعادل رسانده است [۴].

ماچادو [۲] و همکارانش، یک پروتکل مسیریابی مبتنی بر کیفیت انرژی و پیوند [۳] برای برنامه‌های اینترنت اشیا ارائه داده‌اند. برای افزایش قابلیت اطمینان و بهره‌وری انرژی، REL براساس مکانیزم تخمینی، کیفیت لینک انتها به انتها [۴]، انرژی باقیمانده و تعداد گام‌ها مسیرها را انتخاب می‌کند. علاوه بر این، REL یک مکانیزم محرک رویداد را پیشنهاد می‌دهد تا تعادل بار را فراهم کند و از کاهش سریع انرژی گره‌ها یا شبکه جلوگیری کند. نتایج نشان می‌دهد که REL طول عمر شبکه و خدمات در دسترس را به خوبی کیفیت سرویس برنامه‌های اینترنت اشیا افزایش می‌دهد [۵].

جدجک [۵] و همکارانش، طرح امنیتی جدیدی برای اینترنت اشیا و RPL پیشنهاد داده‌اند که طرح اعتماد RPL مبتنی بر معیار [۶] نامیده می‌شود. MRTS مسئله اعتماد را در طول ساخت مسیر از هر گره به مسیریاب مرزی [۷] مورد بررسی قرار می‌دهد. برای حل این مساله، پیام DIO از طریق معرفی یک معیار جدید مبتنی بر اعتماد به نام گسترش اعتماد گره RPL [۸] و یک تابع هدف جدید به نام تابع هدف اعتماد [۹] گسترش پیدا کرده است. در واقع، ERNT مقدار اعتماد را برای هر گره درون شبکه نشان می‌دهد و TOF نشان می‌دهد چگونه ERNT به هزینه مسیر نگاشته شده است. در MRTS تمام گره‌ها برای محاسبه ERNT با در نظر گرفتن رفتار گره‌ها از جمله خودخواهی، انرژی و صداقت همکاری می‌کنند [۶].

دیمن [۱۰] و همکارانش، الگوریتم جستجوی جاذبه کسری چند هدفه [۱۱] به منظور ایجاد یک مسیریابی کارآمد در اینترنت اشیا پیشنهاد کرده‌اند. هدف اصلی الگوریتم MOFGSA افزایش طول عمر گره‌های شبکه است. الگوریتم پیشنهادی برای افزایش طول عمر گره از معیارهای طول عمر پیوند، تأخیر، انرژی و مسافت پیموده شده استفاده کرده است. در ابتدا انرژی هر گره تخمین زده می‌شود؛ اینکار به منظور ایجاد یک مسیریابی موثر نیاز است تا از تحویل بسته‌ها اطمینان حاصل شود. الگوریتم پیشنهاد شده FGSA تئوری کسری و الگوریتم جستجوی گرانشی را با هم ترکیب کرده است؛ به این منظور که به طور مرتب، سرخوشه را تعیین کند [۷].

آیررور [۱۲] و همکارانش، پروتکل مسیریابی RPL آگاه به اعتماد

[1]Chang [2]Machado [3]routing by energy and Link quality [4]end-to-end [5]Djedjig [6]metric-based RPL trustworthiness scheme [7]border router [8]extended RPL node trustworthiness [9]trust objective function [10]Dhumane [11]multi-objective fractional gravitational search algorithm [12]Airehrour

و ایمن [۱] را برای اینترنت اشیا پیشنهاد کرده‌اند. پروتکل مسیریابی SecTrust-RPL علاوه بر این که حملات مسیریابی را تشخیص می‌دهد، کارایی شبکه را نیز به طور قابل قبولی افزایش می‌دهد. در نهایت با استفاده از شبیه‌ساز Cooja کارایی پروتکل مطرح شده با فرض وجود حملات مختلف مسیریابی مانند حمله رتبه [۲] با پروتکل RPL استاندارد مقایسه شده است [۸].

سنان [۳] و همکارانش، برای انتخاب والدین بهینه و کارآمد [۴] در RPL از الگوریتم بهینه‌سازی کرم شب‌تاب برای افزایش طول عمر شبکه اینترنت اشیا استفاده کرده است. در EEOPS-RPL، هر گره در شبکه به عنوان کرم شب‌تاب در نظر گرفته شده است. به همین دلیل برای هر کرم شب‌تاب، مکان فعلی کرم شب‌تاب، جاذبه کرم شب‌تاب، تابع تصادفی، سرعت و بهترین مقادیر سراسری در شبکه محاسبه می‌شود. انرژی باقیمانده و تعداد انتقالات مورد انتظار از پارامترهای جذابیت هستند و فاصله یک پارامتر حرکتی برای انتخاب والد بهینه در DODAG است [۹].

پوشپالاتا [۵] و همکارانش، با هدف بررسی دقیق رفتار تعداد انتقالات مورد انتظار (ETX) در RPL که وظیفه انتخاب مسیر را در مسیرهای طولانی دارد، یک روش مسیریابی انرژی محور مبتنی بر RPL برای ارائه مسیرهای پایدار پیشنهاد داده‌اند. روش L-RPL با بررسی دقیق مقدار ETX، به یک گره کمک می‌کند تا مقاوم‌ترین مسیر را انتخاب کند. خروجی این روش قابلیت اطمینان داده‌ها را بهبود می‌بخشد و سربار کنترل را کاهش می‌دهد [۱۰].

سباستین [۶] و همکارانش، برای بهینه‌سازی تعادل بار مسیرها در RPL، پروتکل مسیریابی مبتنی بر معیار تعادل بار را به نام lbRPL پیشنهاد داده‌اند. در پروتکل پیشنهادی، یک معیار مسیریابی جدید برای RPL به نام شاخص تعادل بار (LBI) معرفی شده است. LBI شامل معیارهای ETX، تعداد والدین [۷] و انرژی باقی‌مانده [۸] برای تصمیم‌گیری مسیریابی است. نتایج شبیه‌سازی نشان داده است که lbRPL باعث بهبود عملکرد شبکه، پایداری و بهبود طول عمر شبکه برای RPL شده است [۱۱].

به طور کلی در اکثر روش‌های ارائه شده، مسیریابی فقط بر اساس یک معیار انجام شده است که عیب این روش این است که اگر به طور مثال RPL فقط براساس معیار قابلیت اطمینان مسیریابی را انجام دهد، گره‌ها انرژی زیادی را از دست می‌دهند یا اگر RPL تنها معیار انرژی را در نظر بگیرد، گره‌ها نرخ بسته‌های از دست رفته زیادی خواهند داشت. همچنین، بخش دیگری از روش‌های اشاره شده، مسیریابی را بر اساس چند معیار انجام داده‌اند که اکثرا حملات مسیریابی را در نظر نگرفته‌اند. همین امر موجب می‌شود که نتایج شبیه‌سازی خیلی به واقعیت نزدیک نباشد. در بخش بعدی درباره روش پیشنهادی توضیح داده شده است.

[1]Secure-Trust-RPL [2]rank attack [3]Sennan [4]energy efficient optimal parent selection [5]Pushpalatha [6]Sebastian [7]parent count [8]remaining parent energy

۱.۲ مفاهیم اولیه

معیار اعتماد: این معیار میزان اعتماد یک گره را مشخص می‌کند؛ بدین صورت که رفتار یک گره را در حالی که یک ارتباط مستقیم یا غیرمستقیم با همسایگان خود دارد، در طول یک دوره زمانی بررسی می‌کنیم.

حمله رتبه: در این نوع حمله، گره مخرب رتبه‌ای پایین‌تر از رتبه واقعی خود را در شبکه همه‌پخشی می‌کند. همین امر موجب ترغیب گره‌های همسایه به گره مخرب و مسیر معرفی‌شده توسط آن می‌شود. در واقع گره مخرب با این کار این گونه القا می‌کند که مسیر بهتری را دارد به همسایگانش نشان می‌دهد تا از این طریق بسته‌های خود را ارسال کنند.

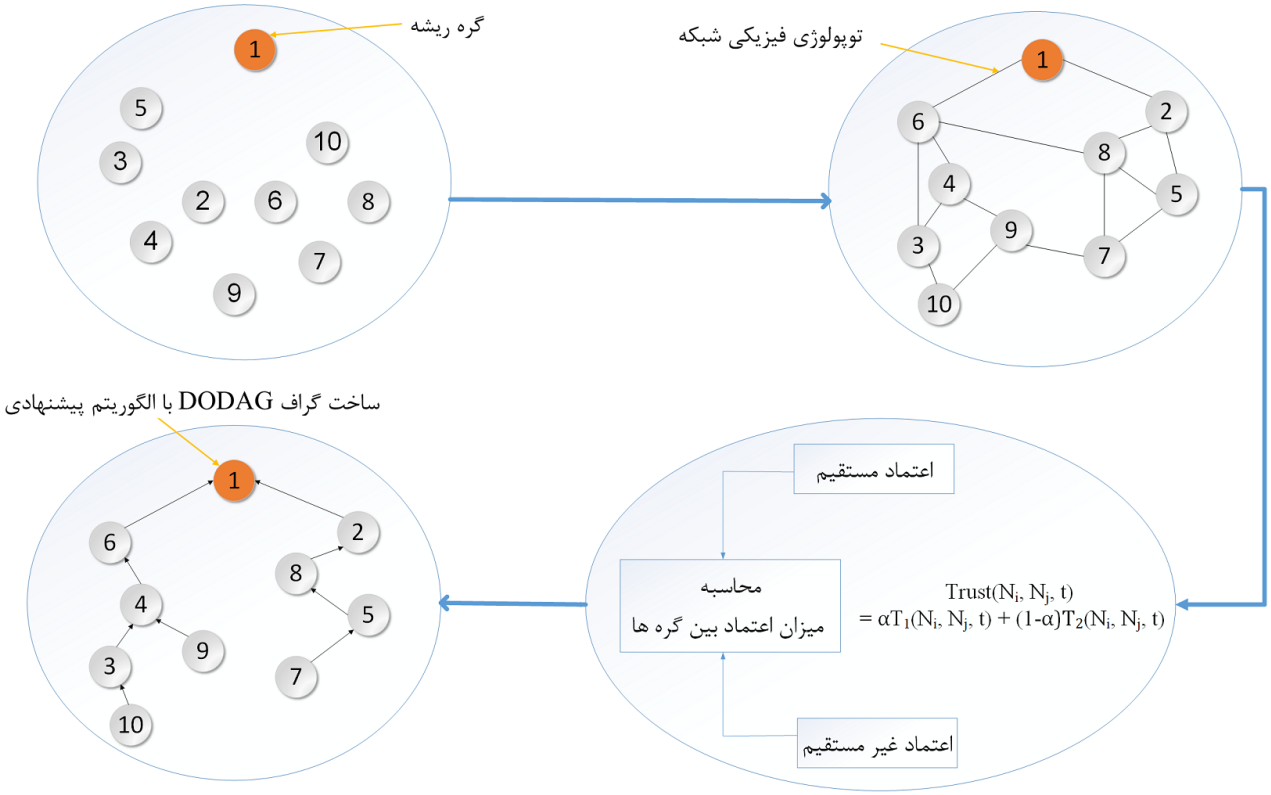
حمله Sybil: در این نوع حمله، لایه شبکه به دفعات مورد تهاجم قرار می‌گیرد. گره مخربی که این نوع حمله را انجام می‌دهد، می‌تواند به عنوان چندین موجودیت درآید. در واقع گره مخرب با استفاده از هویت گره‌های موجود در شبکه، هویت خود را جعل می‌کند و به این ترتیب اقدام به تغییر ماهیت خود می‌کند.

۲.۲ طرح مساله

همان طور که در بخش‌های قبل ذکر شد، مهم‌ترین و اساسی‌ترین چالش پروتکل RPL انتخاب مسیر بهینه در شبکه‌های کم‌توان و پراتلاف می‌باشد. این پروتکل به طور پیش‌فرض برای مسیریابی از دو تابع هدف OF0 و MRHOF استفاده می‌کند. توابع هدف براساس معیارهای مختلفی همچون معیار رتبه، فرآیند مسیریابی را انجام می‌دهند. وجه تمایز مسیریابی‌های مختلف را معیارهای انتخاب شده در توابع هدفشان، مشخص می‌کند. در همه روش‌هایی که در بخش گذشته مورد بررسی قرار گرفت، هدف محققان یافتن معیارهای مؤثر برای مسیریابی بهینه بوده است. با این حال، انتخاب معیار(های) مناسب از میان انبوهی از معیارهای مسیریابی هنوز به عنوان یک چالش مطرح است. در این راستا، در این تحقیق سعی بر آن است که با انتخاب مجموعه‌ای از ویژگی‌های مناسب و جامع، روشی مؤثر و کارا جهت انتخاب مسیر بهینه ارائه شود.

۳.۲ روش پیشنهادی

روش پیشنهادی از معیار اعتماد که یک معیار جامع است برای به دست آوردن اطلاعات و انجام تجزیه و تحلیل اطلاعات استفاده می‌کند. بدین صورت که در ابتدا لیست گره‌های موجود در شبکه و ارتباطات آن‌ها را به عنوان ورودی روش پیشنهادی درنظر گرفته شده است. سپس، میزان اعتمادی که بین یک گره به همسایه‌اش وجود دارد، محاسبه می‌شود. در نهایت براساس میزان اعتمادی که بین گره‌های موجود در شبکه وجود دارد، مسیریابی انجام می‌شود. میزان اعتماد یک گره به گره‌های همسایه‌اش را می‌توان از طریق بسته‌هایی که بین گره‌ها در شبکه تبادل می‌شود، محاسبه کرد. بر همین اساس از نتیجه تقسیم تعداد بسته‌های ارسال شده به بسته‌های دریافت شده می‌توان میزان اعتماد بین گره‌ها را به دست آورد. اعتماد مستقیم در واقع اعتمادی است که از طریق ارتباط



شکل ۱. شمای کلی روش پیشنهادی

مستقیمی که بین یک گره با همسایه‌اش وجود دارد، به دست می‌آید. همچنین، اعتماد توصیه‌شده (اعتماد غیرمستقیم) در واقع اعتمادی است که از ارتباط مستقیم گره ثالث معتبر با یکی از گره‌های کاندید به دست می‌آید. در نهایت برای به دست آوردن اعتماد کلی و بهینه این دو اعتماد را با هم ترکیب شده‌اند.

بر این اساس در این مقاله یک الگوریتم مسیریابی قابل اعتماد مبتنی بر RPL در اینترنت اشیا ارائه شده است. خروجی الگوریتم پیشنهادی، لیست مرتبی از مسیرهای انتخاب شده بر حسب میزان اعتماد می‌باشد. روش پیشنهادی با کمک شبیه‌ساز Cooja در هنگام وجود حملات مشهوری مانند حمله رتبه و حمله Sybil ارزیابی شده است. شکل ۲، کلیات روش پیشنهادی را نشان می‌دهد.

در روش پیشنهادی از اعتماد مستقیم و غیر مستقیم برای محاسبه قابلیت اطمینان گره‌ها در مسیریابی استفاده شده است. بدین ترتیب که در ابتدا برای محاسبه اعتماد گره‌ای که تا به حال برایش بسته‌ای ارسال نشده است از میزان اعتماد مستقیم بین گره‌های همسایه آن گره کمک گرفته شده و میانگین آنها به عنوان اعتماد اولیه برای آن گره در نظر گرفته می‌شود. سپس با گذشت زمان که بسته‌های بیشتری ارسال شده است ضریب اهمیت اعتماد توصیه شده همسایه‌ها کم و ضریب اهمیت (تاثیر) اعتماد مستقیم گره ارسال‌کننده افزایش داده می‌شود. به عبارت دیگر، در ارتباطی که بین دو گره i و j برای ارسال بسته‌ها برقرار می‌شود، گره i که می‌خواهد بسته‌هایش را به گره j بفرستد سه سابقه از این ارتباط را برای خود ذخیره می‌کند که شامل موارد زیر است:

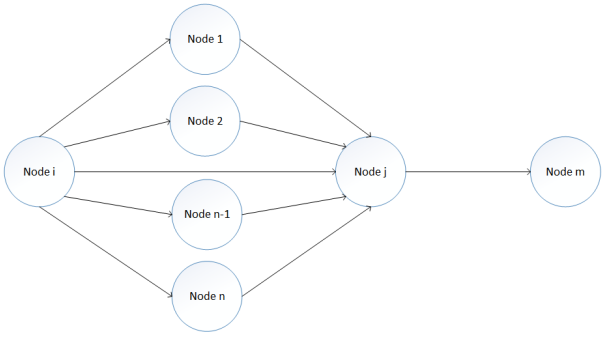
- $PS(N_i, N_j)_t$: تعداد بسته‌هایی که گره i برای گره j ارسال کرده است.
- $PF(N_i, N_j)_t$: تعداد بسته‌هایی که گره j از گره i دریافت کرده و سپس بازارسال کرده است.
- t: زمانی است که ارزیابی گره j انجام می‌شود.

در اینجا میزان اعتماد مستقیم با نماد T_1 مشخص شده است. در واقع، اعتماد مستقیم بیانگر اعتمادی است که گره j مستقیما از گره i به دست آورده است. همچنین، میزان اعتماد غیرمستقیم با نماد T_2 مشخص شده است. در واقع اعتماد غیرمستقیم بیانگر میزان اعتمادی است که گره j از طریق سایر همسایگانش به جز گره i به دست آورده است. در نهایت، میزان اعتماد به صورت زیر محاسبه می‌شود:

$$Trust(N_i, N_j, t) = \alpha T_1(N_i, N_j, t) + (1-\alpha) T_2(N_i, N_j, t) \quad (1)$$

$$T_1(N_i, N_j, t) = PF(N_i, N_j)_t \Big/ \left[(\beta)\,(PS(N_i, N_j)_t) + (1-\beta) \frac{\sum_{N_{ne} \in \text{Neighbour}(N_i, N_j)} PS(N_i, N_{ne})_t}{|N_{ne}|} \right] \quad (2)$$

$$T_2(N_i, N_j, t) =$$



شکل ۲. توصیف رابطه مستقیم و غیرمستقیم

الگوریتم ۱ Reliable-RPL

Input: $N = \{N_1, N_2, \ldots, N_L\}, \text{Parent}(N_k) = \{P_{k1}, P_{k2}, \ldots, P_{kM}\}, \ \forall k \in N$

Output: $DODAG$

$0 \leq \alpha \leq 1$

for each $N_k \in N$ **do**

  for each $P_{kl} \in \text{Parent}(N_k)$ **do**

    $\text{Trust}(N_k, P_{kl}, t) = \alpha T_1(N_k, P_{kl}, t) + (1 - \alpha) T_2(N_k, P_{kl}, t)$

  end for

  $\text{Trust}(N_k, \text{Parent}(N_k), t) = [\text{Trust}(N_k, P_{k1}, t), \text{Trust}(N_k, P_{k2}, t), \ldots]$

end for

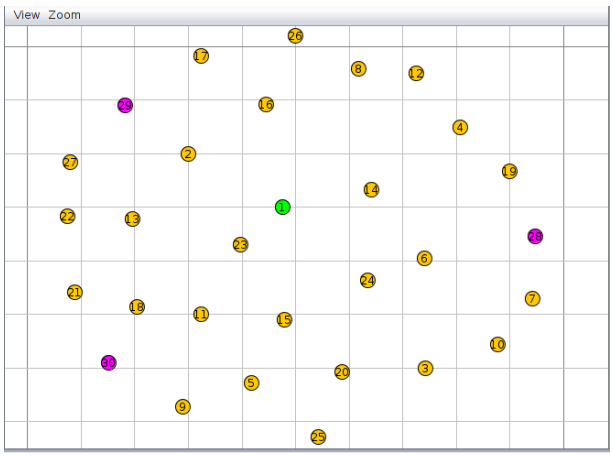
$\overrightarrow{\text{Parent}(\text{N}_\text{K})} = \text{sort}(\text{Parent}(N_k), \text{Trust}(N_k, \text{Parent}(N_k), t))$

Build $DODAG$ based on maximum trust

$$\left[\sum_{\substack{N_{ne} \in \text{Neighbour}(N_i, N_j), \\ N_{ne} \neq N_i}} PF(N_{ne}, N_j)_t \right] \Big/ |N_{ne}| \quad (۳)$$

شکل (۲) رابطه مستقیم و غیرمستقیمی که بین گره‌های i و j وجود دارد را نشان می‌دهد. در رابطه‌ی مستقیم، گره i به طور مستقیم با یک پیوند ارتباطی به گره j متصل شده است. در رابطه‌ی غیرمستقیم بین گره i و j ممکن است یک یا چند گره (n تا گره) وجود داشته باشد. بنابراین، گره i می‌تواند با استفاده از میزان اعتمادی که سایر همسایگان به گره j داشتند، میزان اعتماد غیرمستقیم بین خود با گره j را محاسبه کند. درنهایت، میزان اعتماد بر اساس رابطه‌ی مستقیم و غیرمستقیم برآورد می‌شود.

در الگوریتم پیشنهادی، مجموعه گره‌ها با نماد N و والدین آن‌ها با نماد $\text{Parent}(N_k)$ به عنوان ورودی در نظر گرفته شده‌اند. $\overrightarrow{\text{Parent}(\text{N}_\text{K})}$ لیست والدین هر گره است که براساس معیار اعتماد مرتب شده‌اند. رفتار یک گره در حالی که ارتباط مستقیم یا غیرمستقیم با سایر گره‌های همسایه



شکل ۳. شبکه RPL با ۳۰ گره شامل ۳ گره حمله کننده در شبیه‌ساز COOJA

خود دارد در یک زمان مشخص بررسی می‌شود. در واقع پس از اجرای الگوریتم والدین هر گره بر اساس معیار اعتماد امتیازبندی شده‌اند. ساخت گراف $DODAG$ و مسیریابی می‌تواند بر این اساس انجام شود.

۳ نتایج شبیه‌سازی

در این بخش نتایج به دست آمده از شبیه‌سازی بررسی، تجزیه و تحلیل می‌شود. روش پیشنهادی با روش‌های SecTrust و MRHOF مقایسه شده است. در سناریوی آزمایش، شبکه‌ای با ۳۰ گره شامل ۲۶ گره ارسال‌کننده و ۳ گره مخرب و یک گره ریشه در محیطی با ابعاد ۷۰ * ۷۰ مترمربع گسترده شده‌اند. گره‌های حمله‌کننده در گوشه‌های شبکه قرار داده شده‌اند. به این دلیل که، یک سناریوی واقعی را نشان دهد که در آن حمله‌کننده می‌تواند از راه دور به این حسگرهای قدرتمند دسترسی پیدا کند و به داخل شبکه نفوذ کند. هر گره بسته‌هایی را به سمت گره ریشه ارسال می‌کنند. مدت زمان شبیه‌سازی برابر با ۳۶۰۰ ثانیه معادل ۱ ساعت می‌باشد. در این سناریو دو حمله Rank و Sybil نیز پیاده‌سازی شده است.

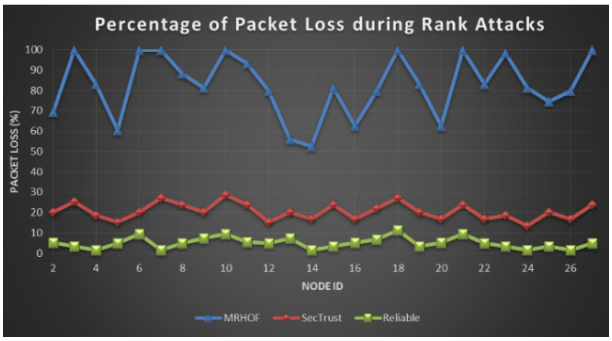
توپولوژی شبکه و نحوه‌ی استقرار گره‌ها در شبیه‌ساز cooja در شکل ۳ نشان داده شده است. جدول ۱ نیز جزئیات بیشتری از تنظیمات شبیه‌سازی ارائه کرده است.

گره‌های موجود در این شبکه، بسته‌هایی را هر یک دقیقه یک بار و بعد از یک تاخیر زمانی اولیه ۵ ثانیه‌ای به گره سرور یا گیرنده ارسال می‌کنند. گره sink یا سرور با رنگ سبز و گره‌های ارسال‌کننده با رنگ نارنجی و گره‌های حمله‌کننده با رنگ بنفش نشان داده شده‌اند.

برد رادیویی و برد تداخلی برای همه دستگاه‌ها به ترتیب ۵۰ متر و ۵۵ متر تنظیم شده است. در شکل ۴ یک مقایسه بین نرخ بسته‌های از دست رفته Reliable-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های از دست رفته MRHOF-RPL در بازه ۵۲ تا ۱۰۰ درصد است، در حالی که این بازه برای SecTrust-RPL بین ۱۳ تا ۲۸ درصد است و برای Reliable-RPL بین ۱ تا ۱۱ درصد است. در نتیجه، پروتکل Reliable-RPL در مقایسه با دو پروتکل دیگر در مقابل

جدول ۱. تنظیمات و پارامترهای شبیه‌سازی شبکه

پارامترها	مقدار
Simulation tool	Contiki/Cooja 3.0
Simulation coverage area	70 m * 70 m
Total number of nodes	30
Malicious nodes	3 (Nodes 28, 29, and 30)
Malicious to legitimate node ratio	1:10
TX range	50 m
Interference range	55 m
Start delay	5 s
Simulation time	60 min
Link failure model	UDGM with distance

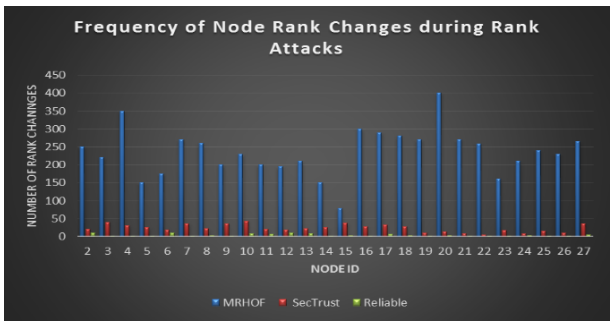


شکل ۴. مقایسه نرخ بسته‌های از دست رفته بین Reliable-RPL، SecTrust-RPL و MRHOF-RPL

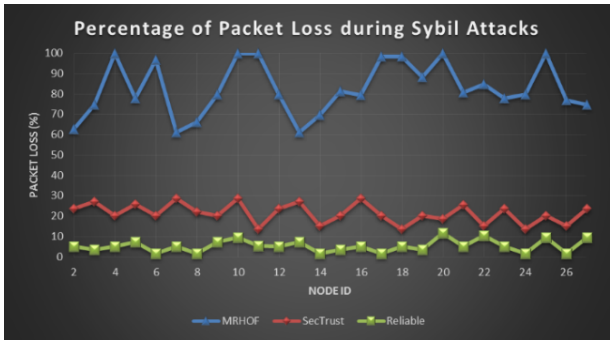
حملات Rank عملکرد بهتری را نشان می‌دهد. به این دلیل که میانگین نرخ بسته‌های از دست رفته کمتری نسبت به دو پروتکل دیگر را ارائه کرده است.

شکل ۵ مقایسه فرکانس تغییرات درجه گره بین MRHOF-RPL، SecTrust-RPL و Reliable-RPL را نشان می‌دهد. آسیب‌پذیری MRHOF-RPL نسبت به تغییرات رتبه گره در برابر حملات Rank نسبت به SecTrust-RPL و Reliable-RPL بسیار بیشتر است. به علاوه، همان طور که از روی شکل ۵ مشخص است آسیب‌پذیری SecTrust-RPL در مقایسه با Reliable–RPL بسیار بیشتر است. از طرف دیگر، Reliable-RPL به طور مداوم در طول دوره شبیه‌سازی تغییرات درجه گره را در حد پایین حفظ می‌کند.

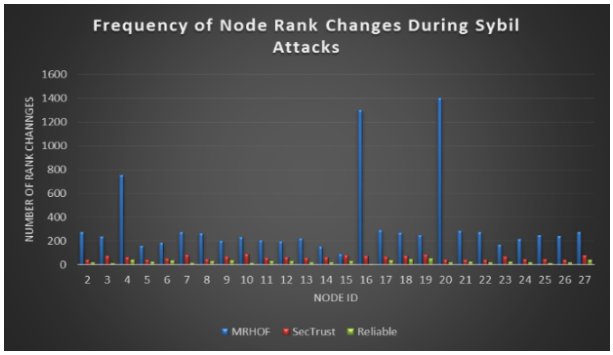
در شکل ۶ یک مقایسه بین نرخ بسته‌های از دست رفته Reliable-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های از دست رفته MRHOF-RPL در بازه ۶۱ تا ۱۰۰ درصد است، درحالی که این بازه برای SecTrust-RPL بین ۱۱ تا ۲۸ درصد است و برای Reliable-RPL بین ۱ تا ۱۱ درصد است. در نتیجه، پروتکل Reliable-RPL در مقایسه با دو پروتکل دیگر در مقابل حملات Sybil عملکرد بهتری را نشان می‌دهد. به این دلیل که میانگین نرخ بسته‌های



شکل ۵. مقایسه فرکانس تغییرات رتبه گره بین Reliable-RPL، SecTrust-RPL و MRHOF-RPL



شکل ۶. مقایسه نرخ بسته‌های از دست رفته بین Reliable-RPL، SecTrust-RPL و MRHOF-RPL



شکل ۷. مقایسه فرکانس تغییرات رتبه گره بین Reliable-RPL، SecTrust-RPL و MRHOF-RPL

از دست رفته کمتری نسبت به دو پروتکل دیگر را ارائه کرده است.

شکل ۷ مقایسه فرکانس تغییرات درجه گره بین MRHOF-RPL، SecTrust-RPL و Reliable-RPL را نشان می‌دهد. آسیب‌پذیری MRHOF-RPL به تغییرات رتبه گره در برابر حملات Sybil نسبت به SecTrust-RPL و Reliable-RPL بسیار بیشتر است. به علاوه همان طور که از روی شکل زیر مشخص است آسیب‌پذیری SecTrust-RPL در مقایسه با Reliable-RPL بسیار بیشتر است. از طرف دیگر، Reliable-RPL به طور مداوم در طول دوره شبیه‌سازی تغییرات درجه گره را در حد پایین حفظ می‌کند.

هدف از اجرای سناریوی پیشنهادی، مقایسه‌ی روش Reliable-RPL با روش‌های SecTrust-RPL و MRHOF-RPL است، که نتایج شبیه‌سازی

بیانگر کارایی بیشتر روش پیشنهادی در مقایسه با دو روش دیگر هم از نظر نرخ بسته‌های از دست رفته و هم از نظر میزان پایداری گره‌ها را نشان می‌دهد.

۴ نتیجه‌گیری

ظهور اینترنت اشیا و پیشرفت آن در سال‌های آینده انقلاب قرن فعلی خواهد بود. در اینترنت اشیا تمامی اشیای هوشمند از قبیل تجهیزات تعبیه‌شده، گوشی‌های هوشمند، حسگر و ... با استفاده از فضای آدرس‌دهی وسیع IPv6 به اینترنت متصل خواهند بود. خانه و ساختمان‌های هوشمند، شبکه برق هوشمند، اتوماسیون شهری و خیلی از کاربردهای دیگر به وقوع خواهند پیوست. شبکه‌های کم‌توان و پراتلاف متشکل از تجهیزات تعبیه‌شده و حسگر نیز بخشی از اینترنت اشیا خواهند بود. در بعضی از کاربردها این شبکه‌ها بسیار عظیم خواهند بود. پروتکل RPL به منظور استفاده در این گونه شبکه‌ها طراحی گردیده است. در این پژوهش، یک روش مسیریابی قابل اعتماد مبتنی بر RPL در حوزه اینترنت اشیا ارائه شده است. در روش پیشنهادی از معیار اعتماد برای مسیریابی استفاده شده است. بهره‌گیری از این معیار باعث افزایش کارایی شبکه شده است. همچنین نتایج به دست آمده از شبیه‌سازی نیز سودمندی روش ارائه داده شده را تایید می‌کند. روش پیشنهادی در این پژوهش با دیگر روش‌های ارائه‌شده مقایسه شد و نتایج نشان می‌دهند که روش پیشنهادی به دلیل انتخاب مسیر بهینه‌تر، نسبت به سایر روش‌ها عملکرد بهتری دارد.

مراجع

[1] Amol V Dhumane and Rajesh S Prasad. Multi-objective fractional gravitational search algorithm for energy efficient routing in iot. *Wireless networks*, 25(1):399–413, 2019.

[2] David Airehrour, Jairo A Gutierrez, and Sayan Kumar Ray. Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things. *Future Generation Computer Systems*, 93:860–876, 2019.

[3] Sankar Sennan, Ramasubbareddy Somula, Ashish K Luhach, Ganesh Gopal Deverajan, Waleed Alnumay, NZ Jhanjhi, Uttam Ghosh, and Pradip Sharma. Energy efficient optimal parent selection based routing protocol for internet of things using firefly optimization algorithm. *Transactions on Emerging Telecommunications Technologies*, 32(8):e4171, 2021.

[4] Mullur Pushpalatha, T Anusha, T Rama Rao, and Revathi Venkataraman. L-rpl: Rpl powered by laplacian energy for stable path selection during link failures in an internet of things network. *Computer Networks*, 184:107697, 2021.

[5] Alphonse Sebastian and S Sivagurunathan. Load balancing metric based routing protocol for low power and lossy networks (lbrpl). *Int. J. Eng. Technol*, 7(2.22):39, 2018.

[6] Zach Shelby and Carsten Bormann. *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011.

[7] Omprakash Gnawali and Philip Levis. The minimum rank with hysteresis objective function. Technical report, 2012.

[8] Pascal Thubert. Objective function zero for the routing protocol for low-power and lossy networks (rpl). Technical report, 2012.

[9] Lin-Huang Chang, Tsung-Han Lee, Shu-Jan Chen, and Cheng-Yen Liao. Energy-efficient oriented routing algorithm in wireless sensor networks. In *2013 IEEE International Conference on Systems, Man, and Cybernetics*, pages 3813–3818. IEEE, 2013.

[10] Kássio Machado, Denis Rosário, Eduardo Cerqueira, Antonio AF Loureiro, Augusto Neto, and José Neuman De Souza. A routing protocol based on energy and link quality for internet of things applications. *sensors*, 13(2):1942–1964, 2013.

[11] Nabil Djedjig, Djamel Tandjaoui, Faiza Medjek, and Imed Romdhani. New trust metric for the rpl routing protocol. In *2017 8th International Conference on Information and Communication Systems (ICICS)*, pages 328–335. IEEE, 2017.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 19, Number 3 (pp. 75–82)
https://monadi.isc.org.ir

Presented at the ISCISC 2021 in University of Isfahan, Isfahan, Iran

Providing an RPL-based Reliable Routing Method in the Internet of Things★

Reza Khatouni * and Mohammad Ghasemi Gol

Department of Computer Engineering, Birjand University, Birjand, Iran

ARTICLE INFO.

Keywords:
internet of things
low power and lossy networks
RPL routing protocol
reliable routing

dor: 20.1001.1.24763047.1401.11.1.9.6

Type: research paper

ABSTRACT

Today, establishing a reliable communication path between devices in low power and lossy networks (LLNs) has become a big challenge. Routing protocol for low power and lossy networks (RPL) is used as a standard routing protocol in LLN networks. The RPL protocol, located at the network layer, uses the objective function to select the optimal path. Due to the fact that various attacks may be created in the routing process, hence the need to pay attention to reliable and trusted routing has become one of the most important and up-to-date research issues. For this reason, in this research, a reliable routing method based on RPL for the Internet of Things is presented. The advantages of the proposed method compared to other methods are that, on the one hand, the rate of lost packets has decreased, and on the other hand, the stability of a node is higher in relation to rank changes. Finally, Cooja simulator has been used to evaluate the proposed method.

★ The ISCISC 2021 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: rezakhatooni@birjand.ac.ir (Reza Khatouni), ghasemigol@birjand.ac.ir (Mohammad Ghasemi Gol)