Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 11, Number 3, Autumn, pp. 31-47
Received: 09/03/2021, Revised: 09/27/2022, Accepted: 11/08/2022

A New RPL-based multi-objective routing method in the Internet of Things

Reza Khatooni[1], Mohammad GhasemiGol[2*]
1- Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, Iran
2*- Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, Iran
[1]rezakhatooni@birjand.ac.ir, [2*]ghasemigol@birjand.ac.ir

Corresponding author's address: Mohammad GhasemiGol, Faculty of Electrical and Computer Engineering, University of Birjand, Birjand, Iran.

Abstract- The Routing Protocol for Low-Power and Lossy Networks (RPL) is defined as a standard routing protocol for the Internet of Things (IETF) based on the definitions of the Internet Engineering Task Force (IETF). This protocol uses the objective function to select the optimum path. Generally, Routing depends on a variety of factors. Thus, it is desirable to use more objective functions to select the best path in the routing process. Therefore, in this paper, an RPL-based Multi-objective routing method is proposed for the Internet of Things. In the proposed method, in addition to the metric of trust, other comprehensive metrics have been used. Despite popular attacks such as rank and Sybil attacks, packet loss rates have decreased and the stability of a node has increased in relation to the rank changes. The advantages of the proposed method are that, despite the rank and Sybil attacks, the average rate of lost packets in different scenarios is between 5 and 13%, while in MRHOF-RPL and SecTrust- RPL is between 62% to 89% and 26% to 37% respectively. On the other hand, the degree of stability of a node compared to the rank changes of the proposed method has increased between 2 and 8 times compared to the mentioned methods. Finally, the Cooja simulator is used to evaluate the proposed method.

Keywords- Internet of things, Low-power and Lossy Network, RPL routing protocol, Multi-objective routing

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۱، شماره ۳، پاییز ۱۴۰۱ ، صفحه ۳۱-۴۷
دریافت: ۱۴۰۰/۰۶/۱۲، بازنگری: ۱۴۰۱/۰۷/۰۵، پذیرش: ۱۴۰۱/۰۸/۱۷

ارائه یک روش مسیریابی چند هدفه مبتنی بر RPL در اینترنت اشیا

رضا خاتونی[۱]، محمد قاسمی گل*[۲]
۱- دانشکده مهندسی برق و کامپیوتر، دانشگاه بیرجند، بیرجند، ایران.
*۲- دانشکده مهندسی برق و کامپیوتر، دانشگاه بیرجند، بیرجند، ایران.
[1]rezakhatooni@birjand.ac.ir, [2*]ghasemigol@birjand.ac.ir

* نشانی نویسنده مسئول: محمد قاسمی گل، بیرجند، بلوار دانشگاه، دانشگاه بیرجند، دانشکده مهندسی برق و کامپیوتر.

چکیده- پروتکل مسیریابی برای شبکه‌های کم‌توان و پراتلاف (RPL) براساس تعاریف کارگروه مهندسی اینترنت (IETF) به عنوان یک پروتکل مسیریابی استاندارد در حوزه اینترنت اشیا معرفی شده است. این پروتکل از توابع هدف مختلفی برای انتخاب مسیر بهینه استفاده می‌کند. به طور کلی مسیریابی به عوامل متعددی بستگی دارد. بنابراین مطلوب است که برای انتخاب بهترین مسیر در فرآیند مسیریابی از توابع هدف بیشتری استفاده شود. به همین علت در این پژوهش یک روش مسیریابی چند هدفه مبتنی بر RPL برای اینترنت اشیا ارائه شده است. در روش پیشنهادی علاوه بر معیار اعتماد از معیارهای جامع دیگری نیز استفاده شده است. مزیت معیارهای پیشنهادی در این است که از یک سو با وجود حملات مشهوری چون حمله رتبه و Sybil نرخ بسته‌های پراتلاف کاهش یافته است و از سوی دیگر میزان پایداری یک گره نسبت به تغییرات رتبه بیشتر می‌شود. مزایای روش پیشنهادی در این است که از یک سو با وجود حملات رتبه و Sybil، میانگین نرخ بسته‌های از دست رفته‌ی آن در سناریوهای مختلف بین ۵ تا ۱۳ درصد است، در حالی که در روش های MRHOF-RPL و SecTrust-RPL به ترتیب بین ۶۲ تا ۸۹ درصد و ۲۶ تا ۳۷ درصد است. از سوی دیگر میزان پایداری یک گره نسبت به تغییرات رتبه‌ی روش پیشنهادی در مقایسه با روش های ذکر شده بین ۲ تا ۸ برابر بیشتر شده است. در این مقاله جهت ارزیابی روش پیشنهادی از شبیه ساز Cooja استفاده شده است.

واژه‌های کلیدی: اینترنت اشیا، شبکه‌های کم‌توان و پراتلاف، پروتکل مسیریابی RPL، مسیریابی چند هدفه

۱- مقدمه

امروزه گسترش روزافزون شبکه‌های حسگر بی‌سیم و شبکه‌های اینترنت اشیا به راحتی قابل درک و مشاهده است. دلیل اصلی این رشد و نمو را نیز می‌توان در توسعه فناوری‌ها و زیرساخت‌های ارتباطی جستجو کرد. چرا که روزبه‌روز 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 [۱]. 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. از این رو از اینترنت اشیا و سرویس‌های مبتنی بر آن را پس از انقلاب‌های صنعتی پیشین که بر اثر مکانیکی شدن، الکتریسیته و فناوری اطلاعات[۱] به وجود آمدند، به عنوان انقلاب صنعتی چهارم یاد می‌کنند [۲].

علاوه بر این، تا پیش از ظهور اینترنت اشیا، یک شبکه همگن که صرفا شامل کامپیوترهای متصل به اینترنت بوده است، مفهوم شبکه جهانی را بیان می‌کرده است ولی بعد از پیدایش اینترنت اشیا مفهوم شبکه جهانی گسترش پیدا کرده و دربرگیرنده شبکه‌ای از تجهیزات ناهمگن شده است [۳].

اینترنت اشیا در واقع شبکه‌ای است از دستگاه‌های فیزیکی

غیرمتصل که هر کدام در درون خود تراشه‌ای هوشمند را جاسازی کرده‌اند که از این طریق بتوانند اطلاعات را جمع آوری و تبادل کنند. در واقع تکنولوژی اینترنت اشیا از دو تکنولوژی شبکه‌های حسگر بی‌سیم و MANETها (شبکه‌های متحرک Ad hoc) برگرفته شده است [۴]. MANET به مجموعه‌ای از گره‌ها گفته می‌شود که بدون استفاده از هیچ زیرساختی همچون نقاط دسترسی یا ایستگاه-های پایه با هم ارتباط برقرار می‌کنند. به دلیل اینکه گره‌ها در این نوع شبکه‌ها به هیچ زیرساخت ثابتی برای ارتباط با یکدیگر نیاز ندارند، به آن‌ها شبکه‌های خودسازمانده نیز می‌گویند [۵].

گره‌های متحرک در این شبکه‌ها اغلب با محاسبه مسیرها و ایجاد جدول‌های مسیریابی، نقش مسیریاب را برای سایر گره‌ها ایفا می-کنند. بعلاوه، مجموعه عظیم از گره‌های حسگر توزیع شده، متصل به هم و خودسازمنده که توانایی انجام پردازش سیگنال، محاسبات و ارتباطات را دارند، شبکه حسگر بی سیم را تشکیل می‌دهند.

گره‌های حسگر در شبکه حسگر بی سیم داده‌هایشان را به یک گره مرکزی مانند گره سینک انتقال می‌دهند. نکته مهم این است که خیلی زود شبکه‌های حسگر بی سیم و MANETها توسعه پیدا کردند و منجر به توسعه برنامه‌های کاربردی در زمینه کشاورزی، ساخت‌وساز و سیستم‌های بهداشت و درمان شده‌اند. در واقع اینترنت اشیا گرفته شده و عصاره ادغام همین دو تکنولوژی است. این موضوع نیز شایان ذکر است که دستگاه‌های اینترنت اشیا و برنامه‌های کاربردی، آسیب پذیری بالایی دارند، به این دلیل که پیوسته در معرض تهدید و حمله توسط گره‌های مخرب قرار دارند.

بحث دیگری که می‌توان به آن اشاره کرد و مورد بررسی قرار داد، موضوع مسیریابی در شبکه‌های اینترنت اشیا است. واضح است که با گسترش اینترنت اشیا، مشکلات و چالش‌های این حوزه به خصوص در بحث مسیریابی بیشتر می‌شود، به این دلیل که حسگرها و محرک‌هایی که در اینترنت اشیا به کار گرفته شده‌اند، داده‌های خود را در بستر اینترنت رد و بدل می‌کنند. لذا برقراری یک مسیر ارتباطی ایمن ما بین این دستگاه‌ها به چالشی بزرگ تبدیل شده است. بعلاوه، شبکه‌های کم‌توان و پراتلاف (LLNs) که تشکیل شده-اند از دستگاه‌هایی با توان پردازشی، حافظه و انرژی محدود، نقش مهم و اساسی در شبکه‌های اینترنت اشیا ایفا می‌کنند.

کارگروه مهندسی اینترنت، به دلیل اینکه 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) [۶] معرفی کرد. این پروتکل که یک مورد مناسب و رایج برای مسیریابی در دستگاه‌های با منابع محدود است، 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 جهت دار (DAG) نامیده می‌شود. همچنین اطلاعات مربوط به توپولوژی RPL نیز در ساختاری شبیه درخت به نام گراف بدون دور جهت دار مقصدگرا (DODAG) نگهداری می‌شود.

به طورکلی، مجموعه مسیرهایی‌که بسته‌های داده را از گره‌های فرستنده به گره سینک منتقل می‌کنند، DODAG را تشکیل می-دهند. RPL این DODAG را با استفاده از تابع هدف ایجاد می‌کند. به طورکلی، توابع هدف معیارهای مسیریابی را بهینه یا محدود می-کنند 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 منحصربه فرد نمونه RPL و رتبه (Rank) مشخص می‌شود [۷]. پروتکل RPL در شبکه‌های کم توان و پراتلاف، مسیرها را با استفاده از دو تابع هدف یعنی MRHOF و تابع هدف OF0 ایجاد می‌کند. MRHOF [۸] طراحی شده است برای پیدا کردن مسیری با کمترین هزینه در شبکه و تابع هدف (OF0) [۹] برای پیداکردن نزدیکترین مسیر به ریشه ارائه شده است. به دو دلیل در این مقاله یک روش مسیریابی چندهدفه مبتنی بر RPL در حوزه اینترنت اشیا را پیشنهاد شده است:

- مسیریابی تک هدفه یا تک معیاره، چندان با واقعیت مطابق نخواهد بود. به این دلیل که تنها از یک بعد، مسیریابی را درنظر می‌گیرد. از این رو یک روش مسیریابی چندهدفه مطرح شده که به مسیریابی از جهات مختلف توجه کرده و همچنین در آن روش جدیدی برای محاسبه اعتماد یک گره نیز ارائه شده است.
- در روش پیشنهادی به صورت همزمان دو نوع حمله نیز پایش و اعمال شده‌اند تا بدین طریق شبیه سازی و نتایج روش پیشنهاد شده مطابق با واقعیت و مورد اعتماد باشد.

نوآوری‌های مقاله شامل موارد زیر است:

۱- در این مقاله، الگوریتم جدیدی برای محاسبه میزان اعتماد مبتنی بر توصیه همسایگان ارائه شده است.

۲- در الگوریتم پیشنهادی معیارهای شاخص تعادل بار شامل ETX، تعداد والدین (PC) و معیار انرژی باقیمانده والدین (PPE) و معیار های Trust و Rank در انتخاب مسیر بهینه مورد استفاده قرار گرفته است.

۳- نتایج شبیه سازی روش ارائه شده نشان دهنده‌ی کاهش میانگین نرخ بسته‌های از دست رفته‌ی در سناریوهای مختلف بین ۵ تا ۱۳ درصد است، در حالی که در روش های MRHOF-RPL و SecTrust-RPL به ترتیب بین ۶۲ تا ۸۹ درصد و ۲۶ تا ۳۷ درصد است. همچنین میزان پایداری یک گره نسبت به تغییرات رتبه‌ی روش پیشنهادی در مقایسه با روش های ذکر شده بین ۲ تا ۸ برابر بیشتر شده است.

۴- در این مقاله، کارایی روش پیشنهادی با پروتکل RPL استاندارد و یکی از مقالات جدید این حوزه مقایسه شده است.

مطالب این مقاله در قالب چهار بخش آورده شده است. بخش دوم دربرگیرنده پژوهش‌های مرتبط با موضوع پیشنهادی ومعرفی روش پیشنهادی است. در بخش سوم نتایج به دست آمده از شبیه سازی ارزیابی شده است. بخش چهارم یا بخش نهایی نیز به نتیجه‌گیری اختصاص یافته است.

۲- پیشینه تحقیق

تحقیقاتی که تاکنون بر روی شبکه‌های حسگر بی‌سیم انجام شده اکثرا روی مصرف انرژی و روش‌های مسیریابی مانند پروتکل مسیریابی برای شبکه‌های کم‌توان (PRL) تمرکز دارند. اکثر پروتکل‌های مسیریابی نیز براساس یک معیار عمل می‌کنند. به همین دلیل اگر PRL تنها معیار قابلیت اطمینان را درنظر بگیرد گره‌ها انرژی زیادی را هدر می‌دهند همچنین اگر PRL فقط معیار انرژی را درنظر بگیرد گره‌ها نرخ بسته‌های پراتلاف زیادی خواهند داشت. چانگ[۲] و همکارانش، یک مکانیزم مسیریابی انرژی محور مبتنی بر معیارهای تعداد انتقالات موردانتظار(ETX) و انرژی باقی مانده برای بهبود پروتکل مسیریابی PRL مطرح کرده‌اند. این مکانیزم طول عمر شبکه را افزایش می‌دهد و مصرف انرژی گره‌های شبکه را به تعادل می‌رساند [۱۰].

ماچادو[۳] و همکارانش، یک پروتکل مسیریابی مبتنی بر کیفیت انرژی و پیوند[۴] برای برنامه‌های اینترنت اشیا ارائه داده‌اند. برای افزایش قابلیت اطمینان و بهره وری انرژی، REL براساس مکانیزم تخمینی، کیفیت لینک انتها به انتها[۵]، انرژی باقیمانده و تعداد گام‌ها انتخاب می‌کند، 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 می-دهد که REL طول عمر شبکه و خدمات در دسترس را به خوبی کیفیت سرویس برنامه‌های اینترنت اشیا افزایش می دهد [۱۱].

عمر سعید[۶]، برای انتخاب بهترین مسیر برای انتقال داده‌ها در سیستم اینترنت اشیا یک الگوریتم مسیریابی بهینه شده را پیشنهاد داده است. الگوریتم برای به دست آوردن بهترین مسیر از ایده‌های کلنی مورچه در سیستم اینترنت اشیا استفاده می‌کند. الگوریتم پیشنهادی محیط اینترنت اشیا را به مناطق مختلفی بر اساس انواع شبکه تقسیم بندی می‌کند. همچنین، این الگوریتم مناسب ترین کلونی مورچه را برای هر ناحیه از شبکه به کار می‌برد. بعلاوه، این الگوریتم مشکلات مسیریابی که ممکن است در مورد سیستم‌های اینترنت اشیا در مناطق تقسیم شده نیز بوجود آید را نیز در نظر می‌گیرد. نتایج شبیه سازی کارایی الگوریتم مسیریابی پیشنهاد شده را از لحاظ تاخیر، تلفات بسته، مصرف پهنای باند، توان مصرفی، سربار بیت‌های کنترل و نسبت مصرف انرژی نشان می‌دهد [۱۲].

اوتفی[۷] و همکارانش، یک پروتکل مسیریابی اینترنت اشیا انطباقی هرس شده(PAIR) ارائه داده‌اند که به صورت گزینشی، مسیرهایی را برای ارتباط برقرار کردن بین گره‌های اینترنت اشیا ایجاد می‌کند. از آنجایی که گره‌ها در اینترنت اشیا متعلق به صاحبان مختلفی هستند، یک مدل قیمت گذاری برای تبادل هزینه‌ها توسط گره‌های میانی ارائه شده است. در پروتکل مسیریابی انطباقی (PAIR)، پیام-های درخواست هرس کردن در میان گره‌های اینترنت اشیا پخش می‌شود تا مبدا و مقصد بتوانند از مسیر سودمندتری بر اساس معیارهای هزینه قابل تنظیم استفاده کنند [۱۳].

گوا[۸] و همکارانش، مدل‌های محاسبه‌ی اعتماد برای سیستم‌های اینترنت اشیا را بر اساس پنج بعد، کلاس بندی کرده‌اند: ترکیب اعتماد[۹]، انتشار اعتماد[۱۰]، تجمیع اعتماد[۱۱]، به‌روزرسانی اعتماد[۱۲] و ایجاد اعتماد[۱۳]. بعلاوه، مزایا و معایب هر بعد نیز به طور مختصر بیان شده‌اند. چندین هدف تحقیقاتی برای محاسبه اعتماد در سیستم-های اینترنت اشیا سرویس‌گرا وجود دارد. هدف اول این است که روش‌های تجمیع اعتماد بر اساس نظریه اعتقاد یا تحلیل رگرسیون بررسی شود. هدف دوم، بررسی معیارهای اعتماد اجتماعی نوآورانه است. هدف سوم، ایجاد یک مدل محاسبه‌ی اعتماد است که بتواند در برابر تمام حملات دفاع کند. هدف چهارم، بررسی استفاده موثرتر از روش‌های اعتماد سازی از جمله مجموع وزن پویا. هدف پنجم، طراحی یک روش محاسبه اعتماد است که مقیاس پذیر باشد. هدف ششم و نهایی این پژوهش، ادغام سرویس ابری با سرویس مدیریت اعتماد است [۱۴].

کیم[۱۴] و همکارانش، نشان دادند که اکثر بسته‌ها به خاطر ترافیک سنگین از بین می‌روند و باعث ایجاد مشکل جدی تعادل بار در RPL می‌شوند. برای غلبه بر این مشکل، استفاده از RPL مبتنی بر صف ساده و مؤثر[۱۵] پیشنهاد شده است که تعادل بار و عملکرد تحویل بسته‌های انتها به انتها را به شدت در مقایسه با RPL استاندارد بهبود می‌بخشد. QU-RPL برای هر گره طراحی شده تا گره والدش را به کمک صفی که از گره‌های همسایه‌اش دراختیار دارد، تعیین کند و فاصله‌شان را نیز تا مسیریاب مرزی[۱۶] بعدی مشخص کنند. همچنین، آن‌ها نشان دادند که QU-RPL باعث کاهش ۸۴ درصدی تلفات در صف می‌شود و ضریب تحویل بسته را تا ۱۴۷ درصد نسبت به RPL استاندارد بهبود می‌بخشد [۱۵].

شن[۱۷] و همکارانش، یک پروتکل مسیریابی انرژی محور[۱۸] جدید برای مدیریت انرژی شبکه‌های حسگر بی‌سیم به کمک اینترنت اشیا ارائه داده‌اند. به‌واسطه‌ی این پروتکل مسئله شکل گیری خوشه‌ها حل می‌شود. EECRP شامل سه بخش کلیدی است: یک تکنیک جدید برای ساخت خوشه توزیع شده، یکسری الگوریتم‌هایی برای انطباق خوشه‌ها و چرخش سر خوشه[۱۹] و یک مکانیزم جدید برای کاهش مصرف انرژی برای ارتباطات از راه دور [۱۶].

جدجک[۲۰] و همکارانش، طرح امنیتی جدیدی برای اینترنت اشیا و RPL پیشنهاد داده‌اند که طرح اعتماد RPL مبتنی بر معیار[۲۱] نامیده می‌شود. MRTS مسئله اعتماد را در طول ساخت مسیر از هر گره به مسیریاب مرزی مورد بررسی قرار می‌دهد. برای حل این مساله، پیام DIO[۲۲] از طریق معرفی یک معیار جدید مبتنی بر اعتماد به نام گسترش اعتماد گره RPL[۲۳] و یک تابع هدف جدید به نام تابع هدف اعتماد[۲۴] گسترش پیدا کرده است. DIO یک پیام کنترلی است که شامل اطلاعاتی مانند شناسه هویت و مرتبه‌ی یک گره 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 [۱۷].

گلیسا[۲۵] و همکارانش، یک پروتکل مسیریابی امن مبتنی بر RPL[۲۶] ارائه داده‌اند. هدف اصلی SRPL جلوگیری از تغییر مقادیر پیام‌های کنترلی مانند جلوگیری از تغییر و دستکاری رتبه یک گره، توسط گره‌های مخرب است که ممکن است با ایجاد یک توپولوژی جعلی باعث تخریب شبکه شود. به همین دلیل در این روش، مفهوم آستانه رتبه و روش احراز هویت زنجیره‌ای مخلوط برای مقابله با حملات داخلی مانند گودال[۲۷]، سیاه چاله[۲۸]، حمله‌های ارسال انتخابی[۲۹] و غیره معرفی شده‌اند. نتایج شبیه‌سازی نشان می‌دهد که SRPL در برابر این نوع حملات مقاوم است [۱۸].

دیمن[۳۰] و همکارانش، الگوریتم جستجوی جاذبه کسری چند هدفه[۳۱] 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 را 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 [۱۹].

کمبل[۳۲] و همکارانش، حملاتی که علیه پروتکل RPL وجود دارد را در سه دسته طبقه بندی کرده‌اند. دسته‌ی اول، حملاتی که علیه منابع انجام می‌شوند و طول عمر شبکه را به واسطه‌ی تولید پیام‌های کنترلی جعلی و یا ایجاد حلقه‌ها[۳۳] کاهش می‌دهند. دسته‌ی دوم، حملات علیه توپولوژی‌اند که باعث می‌شوند که شبکه به سمت پیکربندی غیر بهینه یا گره‌های ایزوله سوق داده شود. دسته‌ی آخر، حملات علیه ترافیک شبکه‌اند که بواسطه‌ی آن به یک گره مخرب اجازه تحلیل بخش بزرگی از شبکه داده می‌شود. همچنین آن‌ها، در مورد تکنیک‌هایی برای حفاظت از توپولوژی RPL بحث کرده‌اند. بنابراین در شبکه‌های اینترنت اشیا، مسیریابی امن نقش مهمی را در عملکرد بی‌نظیر و ایمن شبکه ایفا می‌کند [۲۰].

آیرور[۳۴] و همکارانش، پروتکل مسیریابی RPL آگاه به اعتماد و ایمن[۳۵] را برای اینترنت اشیا پیشنهاد کرده‌اند. این پروتکل علاوه بر اینکه حملات مسیریابی را تشخیص می‌دهد، کارایی شبکه را نیز به طور قابل قبولی افزایش می‌دهد. در نهایت با استفاده از شبیه ساز Cooja کارایی پروتکل مطرح شده با فرض وجود حملات مختلف مسیریابی مانند حمله رتبه[۳۶] با پروتکل RPL استاندارد مقایسه شده است [۲۱].

مدجک[۳۷] و همکارانش، از شبیه‌ساز Cooja - Contiki برای ارزیابی اثرات حمله DIS بر روی شبکه‌های PRL استاتیک و دینامیک استفاده کرده‌اند. علاوه بر این، یک رویکرد جدید به نام - RPL MRC را برای بهبود تاب آوری RPL در برابر DIS Multicast پیشنهاد و پیاده‌سازی شده است. هدف MRC - RPL کاهش پاسخ به پیام‌های DIS Multicast است. نتایج شبیه‌سازی نشان می‌دهد که چگونه حمله می‌تواند با افزایش قابل‌توجه سربار بسته‌های کنترل

و مصرف توان به عملکرد شبکه آسیب برساند. از سوی دیگر، مکانیزم پیشنهادیMRC - RPL ، افزایش قابل‌توجهی را در کاهش سربار کنترل و مصرف توان برای سناریوهای مختلف نشان می‌دهد [۲۲].

احمد زرزور[۳۸] و همکاران، برای غلبه بر این چالش‌ها، تکنیک جدیدی به نام MHOF در این مقاله پیشنهاد داده‌اند تا مسیر ایده‌آل بین فرزند و گره ریشه انتخاب شود. این تکنیک از سه لایه تشکیل شده است: لایه انتخاب والد که در آن والد بر اساس سه پارامتر (ETX، RSSI و انرژی باقیمانده گره ها) انتخاب می شود، لایه انتخاب مسیر که در آن بهترین مسیر با توجه به حداقل (مقدار ETX متوسط) انتخاب می شود.) و حداکثر (میانگین مقدار انرژی باقیمانده) همه گره ها در مسیر انتخاب شده. آخرین لایه کوچک سازی گره فرزند است که برای حل مشکل انرژی گره تراکم با استفاده از دو پارامتر (مرجع RSSI و مقدار آستانه) استفاده می شود. روش پیشنهادی با استفاده از نرم افزار شبیه ساز کوجا پیاده سازی و ارزیابی شده است [۲۳].

هزاریکا[۳۹] و همکارانش، توابع هدف چندگانه با در نظر گرفتن یک شبکه محدود با ماهیت ناهمگن، شبیه به شبکه هوشمند در هر دو بار ترافیک کم و بالا طراحی کرده‌اند. معیارهای چند هدفه انرژی، کیفیت پیوند، تاخیر و تعداد پرش را به عنوان پارامترهایی برای محاسبه معیارها در نظر می گیرند. شبیه‌سازی‌ها نشان داده‌اند که تابع(های) چند هدفه پیشنهادی باعث افزایش طول عمر شبکه، توان عملیاتی و همچنین کاهش تلفات بسته در شبکه شده است [۲۴].

گوپتا[۴۰] و همکارانش، یک الگوریتم تعمیم‌یافته برای MRHOF همراه با ارزیابی هزینه مسیریابی پیشنهاد داده‌اند که فرآیند کامل انتخاب والدین را تعریف می‌کند. علاوه بر این، تجزیه و تحلیل مقایسه‌ای از تابع هدف‌های مختلفی RPL برای شناسایی تابع هدف مناسب برای عملکرد RPL افزایش یافته انجام شده است. پارامترهای ارزیابی عملکرد به PDR، مصرف انرژی، تعداد پرش، میانگین ETX، متریک Rt و زمان بین بسته‌ها، برای اندازه شبکه و کیفیت لینک مختلف گسترش یافته‌اند. نتایج با استفاده از شبیه ساز کوجا به دست آمده است. RPL با معیار ترکیبی ۲۴٪ PDR بالاتر، ۲۸٪ مصرف انرژی کمتر و ۳۹٪ زمان بین بسته کمتری در مقایسه با RPL با معیار واحد ارائه داده است [۲۵].

۲-۱- چالش‌های تحقیق

در جدول ۱ روش‌های پیشنهادی و ویژگی‌های آن‌ها با هم مقایسه شده است. به طور کلی در روش‌های ارائه شده، یک بخش مسیریابی را فقط بر اساس یک معیار انجام می‌دهند که عیب این روش این است که اگر بطور مثال RPL فقط 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 پراتلاف زیادی خواهند داشت. از این رو بخش دیگری از روش‌های اشاره شده، مسیریابی را بر اساس چند معیار انجام داده‌اند که این روش نیز معایب خاص خود را دارد اما نسبت به روش تک معیاره عملکرد بهتری دارد ولی چرا که اگر RPL در مسیریابی معیارهای ETX و انرژی باقی مانده را در نظر گیرد باعث بهبود پروتکل مسیریابی RPL می‌شود از این جهت که طول عمر شبکه را افزایش می‌دهد و مصرف انرژی گره‌های شبکه را به تعادل می‌رساند.

اما چالشی که اکثر روش‌های بررسی شده دارند این است که حملات موجود در مسیریابی ها را در روش خود اعمال نکردند از این رو نتایج خیلی با واقعیت سازگار نخواهند بود. روش‌هایی که مسیریابی را چند هدفه و با توجه به حمله‌های انجام می‌دهند بخش آخری است که در این پژوهش آورده شده است. روش پیشنهادی نیز در این بخش قرار می‌گیردکه کارایی به مراتب بالاتری نسبت به سایر روش‌ها دارد و نسبت به روش‌های موجود در نیز مقایسه شده که خروجی و عملکرد شبکه را به شدت بالا برده است. در بخش بعدی درباره روش پیشنهادی بیشتر توضیح داده شده است.

۳- روش پیشنهادی

همان‌طور که در بخش‌های قبل ذکر شد، مهم‌ترین و اساسی‌ترین چالش پروتکل RPL انتخاب مسیر بهینه در شبکه‌های کم‌توان و پراتلاف است. این پروتکل به طور پیش‌فرض برای مسیریابی از دو تابع هدف OF0 و MRHOF استفاده می‌کند. توابع هدف براساس معیارهایی 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 فصل گذشته مورد بررسی قرار گرفت، هدف محققان یافتن معیارهای مؤثر برای مسیریابی بهینه بوده است. با این حال، انتخاب معیار(ها) مناسب از میان انبوهی از معیارهای مسیریابی هنوز به‌عنوان 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. روش پیشنهادی از معیارهای مختلف و جامع برای به‌دست آوردن اطلاعات و انجام تجزیه و تحلیل اطلاعات استفاده می‌کند. بدین صورت که در ابتدا، لیست گره‌های موجود در شبکه‌ی اینترنت اشیا و ارتباطات آن‌ها را به عنوان ورودی روش پیشنهادی درنظر می‌گیریم. سپس، اعتماد مستقیم را محاسبه می‌کنیم که در واقع اعتمادی است که از طریق ارتباط مستقیمی که بین یک گره به همسایه‌اش وجود دارد،

جدول ۱: مقایسه روش‌های پیشینه تحقیق

نام روش	سال انتشار	ویژگی های مورد استفاده	روش پیشنهادی
REL [۱۱]	۲۰۱۳	کیفیت پیوند- انرژی باقی مانده- تعداد گام	یک پروتکل مسیریابی مبتنی برکیفیت انرژی و کیفیت پیوند برای برنامه های اینترنت اشیا ارائه داده اند.
SOA [۲۶]	۲۰۱۶	اعتماد	یک پروتکل مدیریت اعتماد مقیاس‌پذیر و سازگار را برای پشتیبانی از سیستم‌های اینترنت اشیا مبتنی بر معماری خدمات‌گرا طراحی کرده‌اند.
MRTS [۱۷]	۲۰۱۷	اعتماد	طرح امنیتی جدیدی برای اینترنت اشیا و RPL پیشنهاد داده‌اند که طرح اعتماد RPL مبتنی بر معیار نامیده‌اند. طرح پیشنهای، همواره اعتماد مسیر بین هر گره موردنظر به روتر مرزی را مورد بررسی قرار می‌دهد.
SecTrust-RPL [۲۱]	۲۰۱۸	اعتماد- ETX- رتبه	یک پروتکل مسیریابی قابل اعتماد مبتنی بر RPL را برای ایمن سازی شبکه های اینترنت اشیا از حملات مسیریابی ارائه کرده‌اند.
MOFGSA [۱۹]	۲۰۱۹	طول عمر پیوند- تاخیر زمانی- انرژی – فاصله	یک الگوریتم چندهدفه برای ارائه یک مسیریابی کارآمد در اینترنت اشیا ارائه شده است.
EEOPS-RPL [۲۷]	۲۰۲۰	فاصله- انرژی باقی مانده- ETX	یک پروتکل مسیریابی انرژی محور مبتنی بر RPL را برای انتخاب والد بهینه ارائه کرده اند که موجب افزایش طول عمر شبکه می شود.
L-RPL [۲۸]	۲۰۲۰	ETX	یک روش مسیریابی انرژی محور مبتنی بر RPL برای ارائه مسیرهای پایدار پیشنهاد شده است. این روش با بررسی دقیق مقدار ETX، به یک گره کمک می کند تا مقاوم ترین مسیر را انتخاب کند. خروجی این روش قابلیت اطمینان داده ها را بهبود می بخشد و سربار کنترل را کاهش می دهد.
lbRPL [۱۵]	۲۰۱۸	تعداد والدین- مقدار انرژی باقی مانده- ETX	یک پروتکل مسیریابی مبتنی بر RPL برای ایجاد تعادل بار در شبکه ارائه شده است. این پروتکل باعث پایداری و بهبود طول عمر شبکه می شود.

به‌دست می‌آید. همچنین، اعتماد توصیه‌شده (اعتماد غیرمستقیم) که در واقع اعتمادی است که از ارتباط مستقیم شخص ثالث معتبری با یکی از گره‌های کاندید به دست می‌آید، محاسبه شده است و درنهایت برای به‌دست اوردن اعتماد کلی و بهینه این دو اعتماد با هم ترکیب شده‌اند. در ادامه، معیار ETX را که بیانگر تعداد انتقالاتی است که انتظار می‌رود در یک پیوند ارتباطی بین دو گره وجود داشته باشد تا انتقال یک بسته از مبدا به مقصد به درستی صورت بپذیرد را محاسبه می‌کنیم. زیرا که معیار ETX کوتاه‌ترین مسیر از یک گره به ریشه DODAG را محاسبه می‌کند. در ادامه تعداد والدین[۴۱] گره‌ها تا ریشه محاسبه شده است. پس از محاسبه تعداد والدین هر گره، نوبت به محاسبه گره‌هایی با بیشترین انرژی باقی مانده[۴۲] می‌رسد. در نهایت رتبه هر گره را محاسبه شده است. در واقع، معیارهای ETX، PC، PPE، رتبه و اعتماد به منظور اجرای روش پیشنهادی بکار گرفته شده‌اند. معیارهای ذکر شده در ادامه تعریف شده‌اند.

۳-۱- معیارهای مسیریابی مورد استفاده

معیار ETX: برآورد می‌کند تعداد انتقالاتی که یک گره باید در طول مسیر برای ارسال یک بسته انجام دهد تا فرآیند ارسال یک بسته در مسیر انتخابی از مبدا به مقصد با موفقیت انجام شود. معیار ETX کوتاه‌ترین مسیر از یک گره به ریشه DODAG را محاسبه می‌کند به عبارت دیگر نشان دهنده مسیری با کمترین مقدار ETX از مبدا تعریف شده به ریشه DODAG است [۲۶]. ETX یک مسیر با ۲ پیوند و نسبت تحویل ۱۰۰٪ ۲ است، در حالی که ETX یک مسیر با ۲ پیوند و نسبت تحویل ۲۵٪ ۸ است. در نتیجه هر چه مقدار ETX کمتر باشد، منجر به انتخاب مسیر بهتر می‌شود.

معیار PC: این معیار، تعداد والدین تا ریشه DAG را به ازای تمام والدین ارجح هر گره محاسبه می‌کند. این محاسبه قبل از انتخاب والد انجام می‌شود و خروجی آن مسیری است که PC کمتری داشته باشد. به عبارت دیگر در شبکه مبتنی بر RPL، گره جدید با انتخاب والدی که رتبه پایین را در پیام DIO خود پخش می‌کند، به DAG می‌پیوندد. رتبه پایین نشان می‌دهد که والدین به گره ریشه نزدیکتر هستند. مسیری که تعداد والدین کمتری دارد (PC) یک قدم نزدیکتر در ایجاد تعادل در شبکه خواهد بود. همچنین مسیرهای با تعداد والد بیشتر حذف خواهند شد. بنابراین با استفاده از PC می‌توان تعادل بار را در RPL ایجاد کرد.

معیار PPE: در شبکه‌های کم‌توان و پراتلاف میزان مصرف انرژی بسیار مهم و حیاتی هست. به همین دلیل، همواره سعی محققان بر ارائه روش‌ها و الگوریتم‌های جدید با مصرف حداقل انرژی بوده است. انرژی تجهیزات شبکه‌های کم‌توان و پراتلاف بسیار محدود بوده و گرایش‌ها به سمت کمینه کردن فعالیت‌های اجزای اینگونه شبکه‌ها بوده است. رادیو اصلی‌ترین جزء مصرف کننده انرژی است. همچنین، الگوریتم‌ها سعی در خاموش نگهداشتن رادیو تا حد امکان دارند. در این پژوهش میزان مصرف شده هر گره بنا به مدت زمان فعالیت پردازشگر و رادیوی آن در حالات مختلف محاسبه شده است.

معیار رتبه: هر گره رتبه خود را براساس تابع هدف و رتبه والدین انتخاب شده، محاسبه می‌کند. هر بار که یک گره رتبه یا والد ارجح خود را به روزرسانی می‌کند، به همه گره‌ها یک پیام DIO ارسال می‌شود. برای جلوگیری از تشکیل حلقه‌ها، RPL از قانون رتبه بندی استفاده می‌کند که به موجب آن یک گره همیشه باید رتبه کمتری نسبت به والدین خود داشته باشد. این معیار رتبه هر گره را با توجه به موقعیتش در درخت DODAG مشخص می‌کند. مزیت معیار رتبه این است که از به وجود آمدن حلقه‌ها (loop) در مسیریابی جلوگیری می‌کند و مسیریابی را بهینه می‌کند.

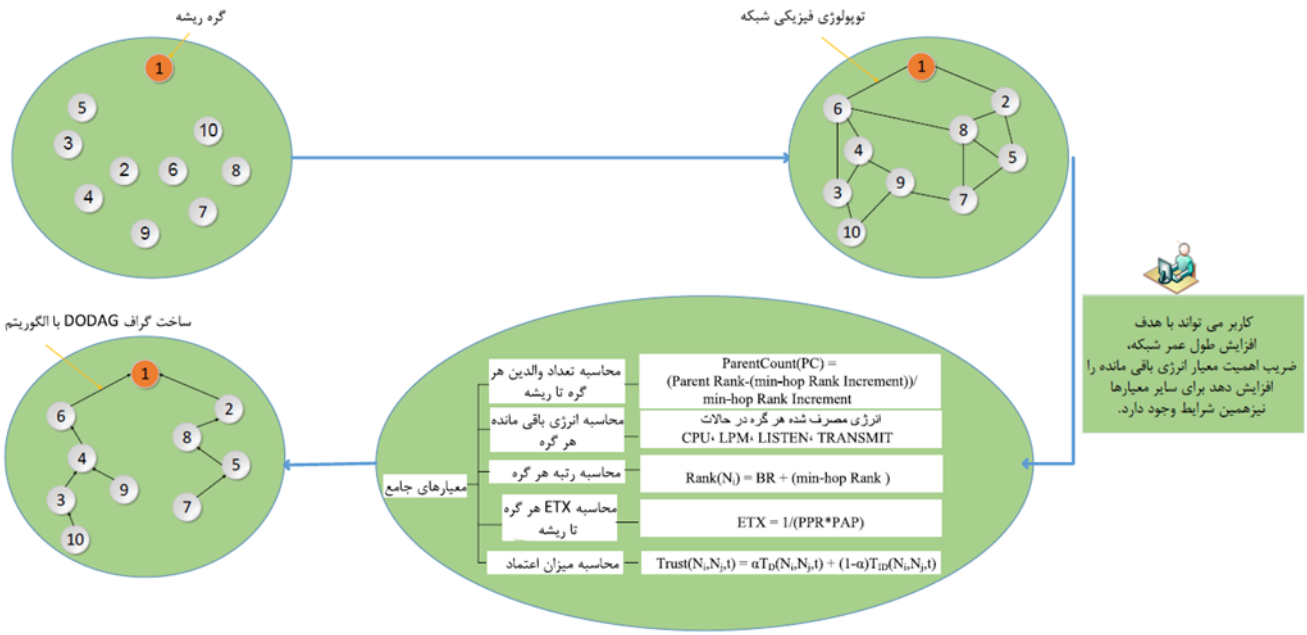
معیار اعتماد: این معیار میزان اعتماد یک گره را مشخص می‌کند بدین صورت که رفتار یک گره را در حالی که یک ارتباط مستقیم یا غیرمستقیم با همسایگان خود دارد در طول یک دوره زمانی بررسی می‌کند و میزان بسته‌های موفقیت آمیزی که آن گره می‌تواند بین گره‌های همسایه خود (کیفیت خدماتی) ارائه کند ارزیابی و محاسبه می‌کند.

در ادامه، کاربر می‌تواند ضریب اهمیت هر کدام از معیارها را مشخص کند، درنهایت یک الگوریتم مسیریابی چندهدفه مبتنی بر RPL مبتنی بر کیفیت سرویس درخواستی کاربر ارائه داده شده است. خروجی الگوریتم پیشنهادی، لیست مرتبی از مسیرهای انتخاب شده بر حسب معیارهای مختلف به کاربر موردنظر می‌دهد. برای شبیه‌سازی روش پیشنهادی از شبیه ساز Cooja استفاده می‌کنیم و در نهایت نیز روش مسیریابی چندهدفه پیشنهادی را با روش‌های موجود در این زمینه مقایسه می‌کنیم. شکل ۱، کلیات روش پیشنهادی را نشان می‌دهد.

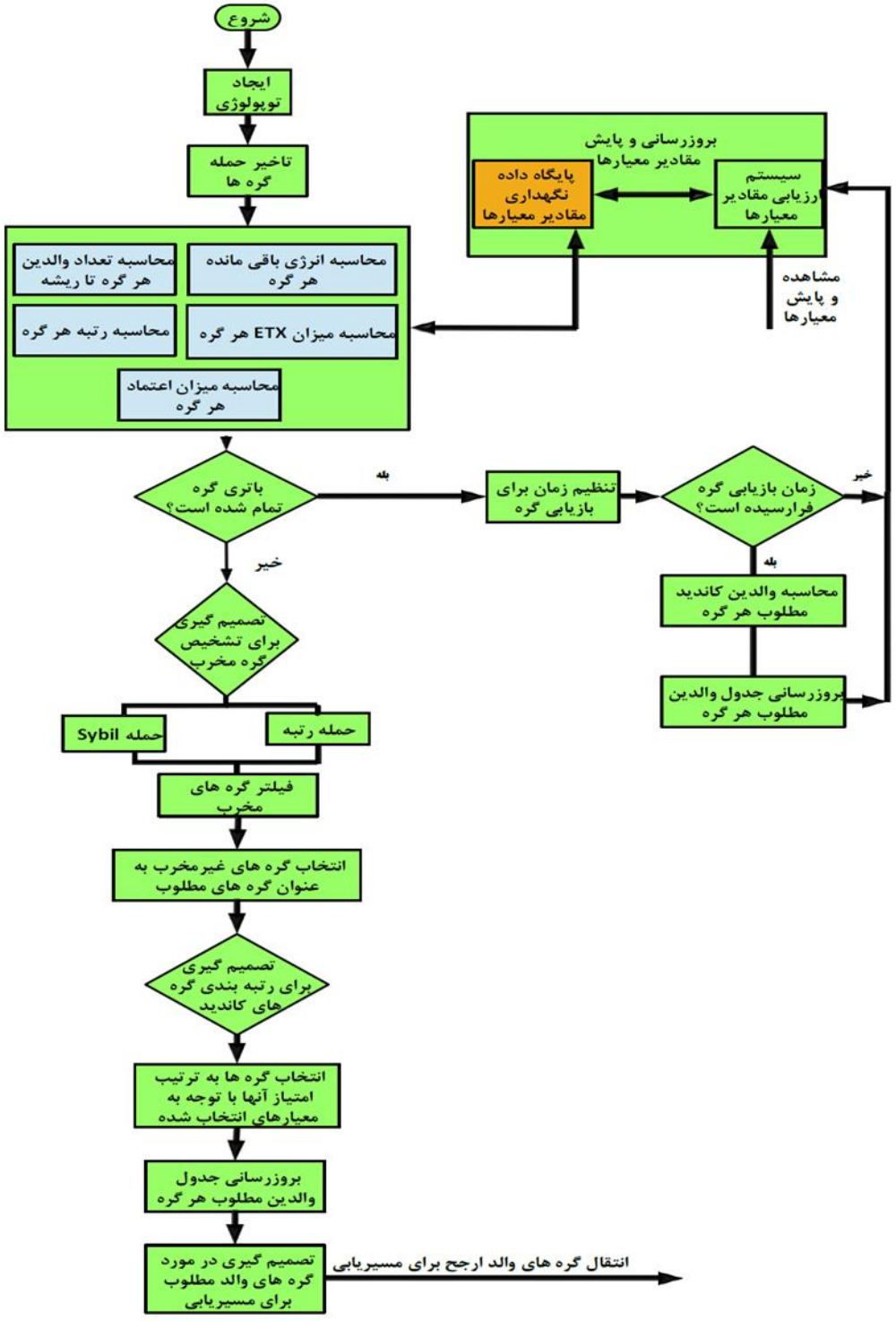
جزئیات چارچوب مسیریابی چندهدفه پیشنهادی در فلوچارت شکل ۲ ارائه شده است. در سیستم مسیریابی چندهدفه پیشنهادی، معیارهای جامع را در حالی که می‌توانیم وزن‌های مختلفی به آنها اختصاص دهیم، مشاهده می‌کنید. این سیستم به خوبی در حین انجام حملات گره های مخرب نیز مسیریابی را به بهترین شکل ممکن انجام می‌دهد.

۳-۲- روش مسیریابی چندهدفه پیشنهادی

در این بخش راهکاری برای رفع چالش‌های فراوان حوزه مسیریابی پیشنهاد شده است. از آن جا که مسیریابی به عوامل گوناگونی بستگی دارد. به همین دلیل در این پژوهش روش جدیدی برای مسیریابی در حوزه اینترنت اشیا مطرح شده است.



شکل ۱: کلیات روش پیشنهادی



شکل ۲: فلوچارت سیستم مسیریابی چندهدفه پیشنهادی

در این روش برای مسیریابی در شبکه‌های اینترنت اشیا از پروتکل مسیریابی RPL مبتنی بر معیار اعتماد و چند معیار جامع دیگر استفاده شده است. مزایای معیارها ذکر شده در این است که از یک سو سرعت تشخیص گره‌های حمله را افزایش داده است و از سوی دیگر دقت در تشخیص حمله را نیز بیشتر کرده است.

ورودی روش پیشنهادی، k تا والد برای هر گره به صورت غیرمرتب است و خروجی آن لیست مرتبی از والدین هر گره است که براساس معیارهای ذکر شده به دست می‌آید.

نحوه‌ی کار شبیه ساز Contiki به این صورت است که والدین ارجح هر گره را محاسبه می‌کند. در الگوریتم پیشنهادی، والدین هر گره براساس معیارهای جامع محاسبه و در نهایت طبق امتیازشان مرتب می‌شوند. در ابتدا، موقعیت والدین هر گره براساس معیارهای اعتماد، رتبه، مقدار انرژی باقی مانده، تعداد والدین هر گره، میزان etx یک تعیین می‌شود. سپس بین تمام همسایه‌های آن گره مقایسه انجام می‌شود و بر همین اساس والدینشان امتیازدهی می‌شوند. طبق این روش هر والدی که در فرآیند مقایسه، امتیاز بیشتری بگیرد، موقعیت‌اش یکی اضافه می‌شود. الگوریتم مذکور، امتیاز گره p1 رو با امتیاز گره p2 مقایسه میکنه. این کار برای همه گره ها به صورت دو تا دو تا انجام می‌شود. درنهایت، والدین هر گره برحسب امتیازشان مرتب می شوند. بعلاوه، بهترین اون‌ها برحسب امتیاز به عنوان والد ارجح انتخاب می‌شود. به عنوان مثال، اگر اعتماد گره‌ای که باید بررسی بشود بیشتر از نود همسایه بود، موقعیت‌اش رو یکی اضافه می‌شود. سپس، برای همه گره های همسایه این گره، این مقایسه انجام می‌شود تا رتبه اش بین همه گره ها به دست بیاید. پس طبق روش پیشنهادی، برحسب امتیازدهی گره ها مقایسه انجام می‌شود. در نتیجه روش مسیریابی ذکر شده، بسته رو دچار بن بست نمی کند.

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 گرهی که تا بحال 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 شده است. سپس با گذشت زمان که بسته‌های بیشتری ارسال شده است ضریب اهمیت اعتماد توصیه شده همسایه‌ها کم و ضریب اهمیت (تاثیر) اعتماد مستقیم گره ارسال کننده افزایش داده شده است.

به عبارت دیگر، در ارتباطی که بین دو گره i و j برای ارسال بسته‌ها برقرار می‌شود، نود 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 مدت زمانی که ارزیابی گره j انجام می‌شود

در روش پیشنهادی، برای محاسبه میزان اعتماد یک گره که تاکنون بسته‌ای برایش ارسال نشده از اعتماد مستقیم و غیر مستقیم استفاده شده است. به این دلیل که، با ترکیب اعتماد مستقیم و غیر مستقیم، میزان اعتماد یک گره با دقت بیشتری قابل محاسبه است. از این رو در روش پیشنهادی، میزان اعتماد مستقیمی که بین گره N_i و N_j وجود دارد با نماد $T_D(N_i, N_j, t)$ مشخص شده است. مقدار اعتماد مستقیم یک گره طبق معادله (۲) محاسبه می‌شود. در واقع، اعتماد مستقیم بیانگر اعتمادی است که گره j مستقیما از گره i به دست آورده است.

همچنین، میزان اعتماد توصیه شده (غیرمستقیم) که بین گره N_i و N_j وجود دارد با نماد $T_R(N_i, N_j, t)$ مشخص شده است. مقدار اعتماد توصیه شده یک گره همانطور که در معادله (۳) نشان داده شده، محاسبه می‌شود. در واقع اعتماد توصیه شده بیانگر میزان اعتمادی است که گره j از طریق سایر همسایگانش به جز گره i به دست آورده است. درنهایت، میزان اعتماد به صورت زیر محاسبه می‌شود:

$$Trust(N_i, N_j, t) = \alpha T_D(N_i, N_j, t) + (1-\alpha) T_{ID}(N_i, N_j, t) \quad (۱)$$

$$T_D(N_i, N_j, t) = \frac{PF(N_i, N_j)_t}{(\beta)(PS(N_i, N_j)_t) + (1-\beta)\frac{\sum_{N_{ne} \in Neighbour(N_i, N_j)} PS(N_i, N_{ne})_t}{|N_{ne}|}} \quad (۲)$$

$$T_R(N_i, N_j, t) = \frac{\sum_{N_{ne} \in Neighbour(N_i, N_j), N_{ne} \neq N_i} PF(N_{ne}, N_j)_t}{|N_{ne}|} \quad (۳)$$

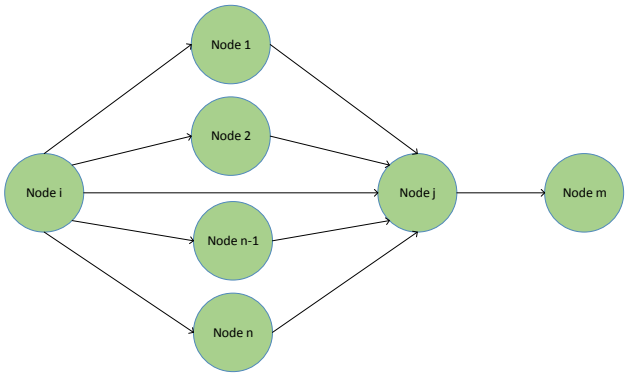
شکل ۲ رابطه‌ی مستقیم و غیرمستقیمی که بین گره‌های i و j وجود دارد را نشان می‌دهد. در رابطه‌ی مستقیم، گره i به طور مستقیم با یک پیوند[۴۳] ارتباطی به گره j متصل شده است. در واقع گره i با استفاده از این پیوند ارتباطی، میزان اعتمادی که بین خود و گره j دارد را محاسبه می‌کند.

همچنین، 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 و گره j را محاسبه کند. در واقع گره i با استفاده از میزان اعتماد غیرمستقیم یا به اصطلاح اعتماد توصیه شده گره‌های همسایه، اعتماد گره j را ارزیابی می‌کند.

از این رو، گره i با استفاده از تجمیع میزان اعتماد مستقیم و غیر

مستقیم که به دست می‌آورد، این امکان را برای خود فراهم می‌کند تا اعتماد گره j را دقیق‌تر مورد ارزیابی قرار دهد. در ادامه، گره i در مورد اعتماد بودن گره j برای ارسال بسته‌هایش تصمیم گیری می‌کند.

درنهایت، میزان اعتماد به دست آمده از رابطه‌ی مستقیم و غیرمستقیم را با هم ترکیب شده و به این ترتیب، میزان اعتماد بین دو گره محاسبه شده است.



شکل ۲: توصیف رابطه مستقیم و غیرمستقیم

Algorithm - MultiObjective-RPL

Input: N = {N1, N2, …, NL},
Parent(N_k) = {Pk1, Pk2, …, PkM}, $\forall k \epsilon N$
Output: DODAG
$0 \leq \alpha \leq 1$
BR = Base Rank
MHR = Min-Hop Rank increment
PPR = Probability that a Packet is Received by the neighbor
PAP = Probability that the Acknowledgement Packet is successfully received
PPE = Remaining Parent Energy
PC = Parent Count
PR = Parent Rank
ETX = Expected transmission
For each $N_k \in$ N
  For each $P_{kl} \in$ Parent(N_k)
    $Trust(N_k, P_{kl}, t) = \alpha T_D(N_k, P_{kl}, t) + (1-\alpha) T_R(N_k, P_{kl}, t)$
    $Rank(N_k, P_{kl}, t) =$ BR(P_{kl}, t) + MHR(P_{kl}, t)
    $PC(N_k, \text{Parent}(N_k), t) = PR(P_{kl}, t) - \text{MHR}(P_{kl}, t)/MHR(P_{kl}, t)$
    $ETX(N_k, P_{kl}, t) = 1/(\text{PPR}(P_{kl}, t) * \text{PAP}(P_{kl}, t))$
    $PPE(N_k, P_{kl}, t) = \text{PPE}(P_{kl}, t)$
    $\varphi(N_k, \text{Parent}(N_k), t) = [\varphi(N_k, P_{k1}, t), \varphi(N_k, P_{k2}, t), \dots]$
    $\forall \varphi = \{Trust, Rank, PPE, PC, ETX\}$
$\overrightarrow{\text{Parent}(N_K)_{Trust}} = sort(\text{Parent}(N_k), Trust(N_k, \text{Parent}(N_k), t))$
$\overrightarrow{\text{Parent}(N_K)_{Rank}} = sort(\text{Parent}(N_k), Rank(N_k, \text{Parent}(N_k), t))$
$\overrightarrow{\text{Parent}(N_K)_{PPE}} = sort(\text{Parent}(N_k), PPE(N_k, \text{Parent}(N_k), t))$
$\overrightarrow{\text{Parent}(N_K)_{PC}} = sort(\text{Parent}(N_k), PC(N_k, \text{Parent}(N_k), t))$
$\overrightarrow{\text{Parent}(N_K)_{ETX}} = sort(\text{Parent}(N_k), ETX(N_k, \text{Parent}(N_k), t))$
$Score\left(\overrightarrow{\text{Parent}(N_K)}, t\right) = \left(\sum_{h \epsilon \varphi} \left(\lambda_h . \overrightarrow{\text{Parent}(N_K)_h}\right)\right)$
  $\forall \varphi = \{Trust, Rank, Pe, Pc, ETX\}$
$\overrightarrow{\text{Parent}(N_K)} = sort\left(Score\left(\overrightarrow{\text{Parent}(N_K)}, t\right)\right)$
Build DODAG based on maximum $Score$

در الگوریتم پیشنهادی، مجموعه گره‌ها با نماد N و والدین آن‌ها با نماد Parent(N_k) به عنوان ورودی درنظرگرفته شده‌اند. $\overrightarrow{Parent(N_K)}$ لیست والدین هر گره است که براساس ترکیبی از معیارهای اعتماد، رتبه، مقدار انرژی باقی مانده تا گره ریشه، تعداد والدین تا گره ریشه و مقدار ETX مرتب شده‌اند. در واقع پس از اجرای الگوریتم والدین هر گره براساس معیارهای ذکر شده رتبه‌بندی شده‌اند و ساخت گراف DODAG و مسیریابی بر این اساس انجام می‌شود.

۴- نتایج شبیه سازی

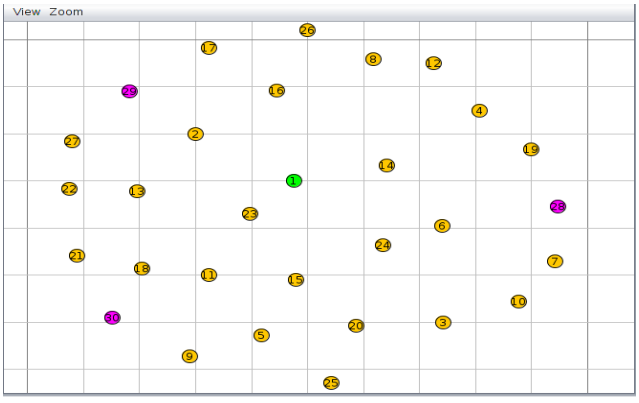
در بخش قبل روش مسیریابی چندهدفه مبتنی بر RPL در اینترنت اشیا ارائه گردید. در این بخش روش پیشنهادی تحلیل و ارزیابی شده است. بدین منظور شبیه سازی‌هایی در دو سناریوی مختلف با استفاده از شبیه‌ساز Contiki Cooja صورت گرفته است. برای ارزیابی عملکرد نیز روش پیشنهادی با سایر روش‌ها مقایسه شده است. روش پیشنهادی در سه سناریو مختلف با روش Sec-Trust و MRHOF مقایسه شده است. در هر سه سناریو، گره‌های حمله کننده در گوشه‌های شبکه قرار داده شده‌اند. به این دلیل که، یک سناریوی واقعی را نشان دهد که در آن حمله کننده می تواند از راه دور به این حسگرهای قدرتمند دسترسی پیدا کند و به داخل شبکه نفوذ کند. ضریب اهمیت همه معیارها در هر سه سناریو مقدار ۰.۲ درنظر گرفته شده است.

در سناریوی اول ۳۰ گره شامل ۲۶ گره ارسال کننده و ۳ گره مخرب و یک گره ریشه وجود دارند که بسته هایی را به سمت گره ریشه ارسال می‌کنند. در سناریوی دوم ۳۳ گره شامل ۲۶ گره ارسال کننده و ۶ گره مخرب و یک گره ریشه وجود دارند. در این سناریو تاثیر افزایش گره‌های مخرب بررسی می‌شود. در سناریوی سوم ۴۰ گره شامل ۳۶ گره ارسال کننده و ۳ گره مخرب و یک گره ریشه وجود دارند. در این سناریو تاثیر افزایش گره‌های نرمال بررسی می‌شود.

مدت زمان شبیه‌سازی برابر با ۳۶۰۰ ثانیه معادل ۱ ساعت هست. در هر سه سناریو دو حمله Rank و Sybil پیاده سازی شده است. در این بخش نتایج به دست آمده از شبیه‌سازی بررسی، تجزیه و تحلیل خواهد شد. سه سناریو با تعداد گره‌های مختلف و حملات مختلف شبیه‌سازی شده‌اند و نتایج حاصل از شبیه‌سازی براساس معیارهای اعتماد، رتبه، ETX، مقدار انرژی باقی مانده تا گره ریشه و تعداد والدین تا گره ریشه به دست آمده‌اند.

۴-۱- سناریوی اول

در سناریوی اول شبکه‌ای با ۳۰ عدد گره که در محیطی با ابعاد ۷۰*۷۰ مترمربع گسترده شده‌اند، به مدت زمان ۱ ساعت شبیه-سازی شده است. نتایج حاصل در قالب نمودارها و جداول در ادامه آورده و به طور کامل تفسیر شده‌اند. توپولوژی شبکه و نحوه‌ی استقرار گره‌ها در شبیه‌ساز Cooja در شکل ۳ نشان داده شده است. گره‌های فرستنده در این شبکه، بسته‌هایی را هر یک دقیقه یکبار 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 ارسال کننده با رنگ نارنجی و گره‌های حمله کننده با رنگ بنفش نشان داده شده-اند. گره sink بسته‌های ارسالی از تمام گره‌ها را دریافت می‌کند. در این شبیه سازی، حملات Sybil و rank نیز ارائه شده‌اند. همچنین در جدول ۲، تاخیر زمانی اولیه ۵ ثانیه برای همگرایی گره‌ها در شبکه RPL در نظر گرفته شده است. نسبت گره‌های نرمال به گره-های حمله کننده ۱ به ۱۰ درنظرگرفته شده است. جدول ۲ جزئیات بیشتری از تنظیمات شبیه‌سازی ارائه کرده است.



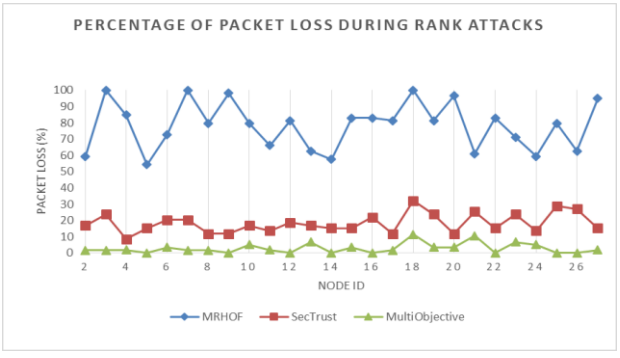
شکل ۳: شبکه RPL با ۳۰ گره شامل ۳ گره حمله کننده در شبیه ساز COOJA

جدول ۲: تنظیمات و پارامترهای شبیه سازی شبکه در سناریوی اول

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

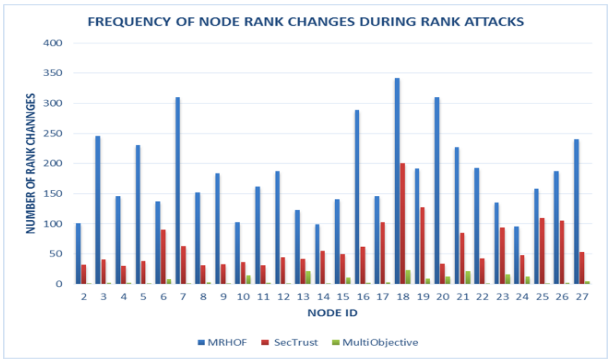
برد رادیویی و برد تداخلی برای همه دستگاه‌ها به ترتیب ۵۰ متر و ۵۵ متر تنظیم شده است. شبیه سازی با ۳۰ گره شامل ۳ گره حمله کننده برای ۶۰ دقیقه اجرا شده است. نتایج شبیه‌سازی در قسمت بعدی مورد بحث و بررسی قرار گرفته است.

شکل ۴ مقایسه‌ای را بین نرخ بسته‌های پراتلاف MultiObjective-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های پراتلاف MRHOF-RPL در بازه ۵۴ تا ۱۰۰ درصد است درحالی که این بازه برای SecTrust-RPL بین ۸ تا ۳۲ درصد است و برای MultiObjective-RPL بین ۰ تا ۱۱ درصد است. در نتیجه، پروتکل MultiObjective-RPL در مقایسه با دو پروتکل دیگر در مقابل حملات Rank عملکرد بهتری را نشان می‌دهد. به این دلیل که میانگین نرخ بسته‌های پراتلاف کمتری نسبت به دو پروتکل دیگر را ارائه کرده است.



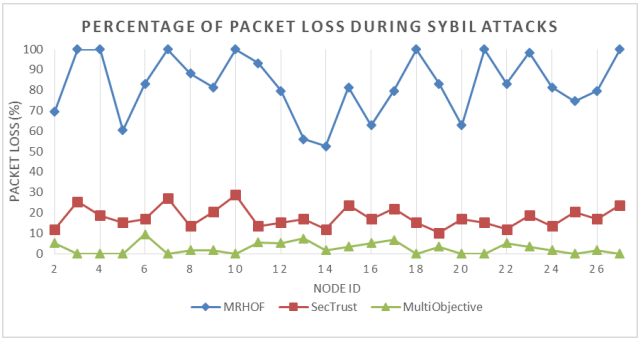
شکل ۴: مقایسه نرخ بسته‌های پراتلاف بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Rank

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



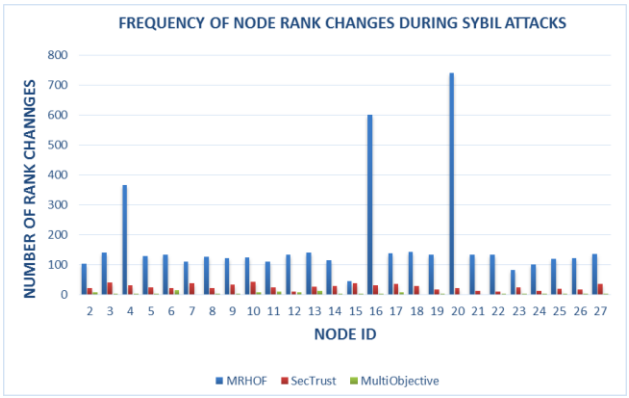
شکل ۵: مقایسه فرکانس تغییرات رتبه گره بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Rank

شکل ۶ مقایسه‌ای را بین نرخ بسته‌های پراتلاف MultiObjective-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های پراتلاف MRHOF-RPL در بازه ۵۲ تا ۱۰۰ درصد است درحالی که این بازه برای SecTrust-RPL بین ۱۰ تا ۲۷ درصد است و برای MultiObjective-RPL بین ۰ تا ۹ درصد است. در نتیجه، پروتکل MultiObjective-RPL در مقایسه با دو پروتکل دیگر در مقابل حملات Sybil عملکرد بهتری را نشان می‌دهد. به این دلیل که میانگین نرخ بسته‌های پراتلاف کمتری نسبت به دو پروتکل دیگر را ارائه کرده است.



شکل ۶: مقایسه نرخ بسته‌های پراتلاف بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Sybil

شکل ۷ مقایسه‌ی فرکانس تغییرات درجه گره بین MRHOF-RPL، SecTrust-RPL و MultiObjective-RPL را نشان می‌دهد. آسیب پذیری MRHOF-RPL به تغییرات رتبه گره در برابر حملات Sybil نسبت به SecTrust-RPL و MultiObjective-RPL بسیار بیشتر است. به‌علاوه همانطور که از روی شکل ۷ مشخص است آسیب پذیری SecTrust-RPL در مقایسه با MultiObjective-RPL بسیار بیشتر است. از طرف دیگر، MultiObjective-RPL به‌طور مداوم در طول دوره شبیه‌سازی تغییرات درجه گره را در حد پایین حفظ می‌کند.



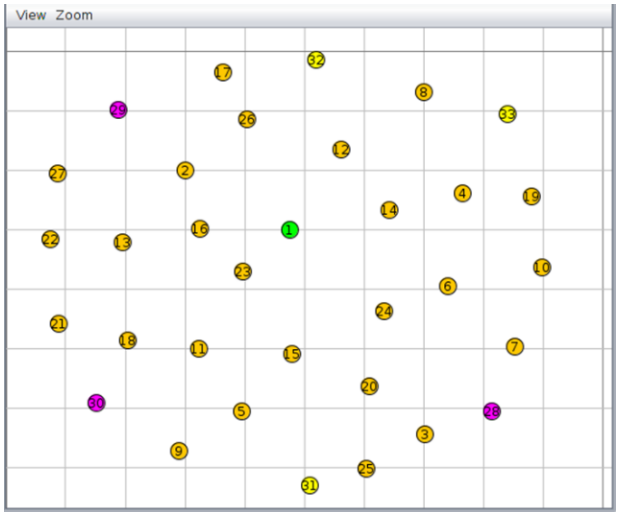
شکل ۷: مقایسه فرکانس تغییرات رتبه گره بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Sybil

هدف از اجرای سناریوی اول، مقایسه‌ی روش MultiObjective-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 پراتلاف و هم از نظر میزان پایداری گره‌ها را نشان می‌دهد.

۴-۲- سناریوی دوم

در سناریوی دوم شبکه‌ای با ۳۳ عدد گره که در محیطی با ابعاد ۷۰*۷۰ مترمربع گسترده شده‌اند. مدت زمان شبیه‌سازی ۱ ساعت درنظر گرفته شده است.

توپولوژی شبکه و نحوه‌ی استقرار گره‌ها در شبیه ساز Cooja در شکل ۸ نشان داده شده است. گره Sink یا سرور با رنگ سبز و گره‌های ارسال کننده با رنگ نارنجی و گره‌های حمله کننده با رنگ بنفش نشان داده شده‌اند. گره sink بسته‌های ارسالی از تمام گره‌ها را دریافت می‌کند. در این شبیه‌سازی، حملات Sybil و Rank نیز ارائه شده‌اند. در جدول ۳، تاخیر زمانی اولیه ۵ ثانیه برای همگرایی گره‌ها در شبکه RPL در نظر گرفته شده است. نسبت گره‌های نرمال به گره‌های حمله کننده ۲ به ۱۱ درنظرگرفته شده است. جدول جزئیات بیشتری از تنظیمات شبیه‌سازی ارائه کرده است.

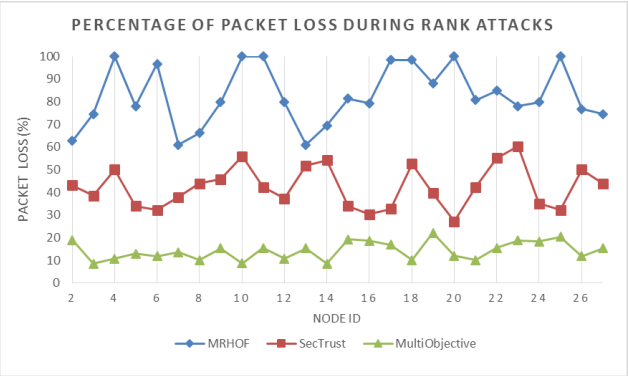


شکل ۸: شبکه RPL با ۳۳ گره شامل ۶ گره حمله کننده در شبیه ساز COOJA

برد رادیویی و برد تداخلی برای همه دستگاه‌ها به ترتیب ۵۰ متر و ۵۵ متر تنظیم شده است. شبیه‌سازی با ۳۳ گره شامل ۶ گره حمله کننده برای ۶۰ دقیقه اجرا شده است. در شکل ۹ یک مقایسه بین نرخ بسته‌های پراتلاف MultiObjective-RPL با SecTrust-RPL و MRHOF-RPL در مقابل حملات Rank ارائه شده است. نرخ بسته-های پراتلاف MRHOF-RPL بین ۶۱ تا ۱۰۰ درصد است، درحالی که این بازه برای SecTrust-RPL بین ۲۷ تا ۶۰ درصد است و برای MultiObjective-RPL بین ۸ تا ۲۰ درصد است. در واقع میانگین نرخ بسته‌های پراتلاف MultiObjective-RPL ۱۴ تا ۱۵ درصد است که این مقدار در مقایسه با دو پروتکل دیگر بسیار کمتر است.

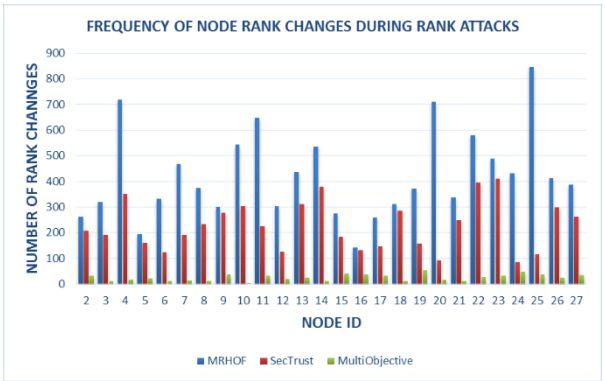
جدول ۳: تنظیمات و پارامترهای شبیه سازی شبکه در سناریوی دوم

پارامترها	مقدار
Simulation tool	Contiki/Cooja 3.0
Simulation coverage area	70 m * 70 m
Total number of nodes	33
Malicious nodes	6 (Nodes 28, 29, 30, 31, 32 and 33)
Malicious to legitimate node ratio	1 : 5.5
TX range	50 m
Interference range	55 m
Start delay	5 s
Simulation time	60 min
Link failure model	UDGM with distance



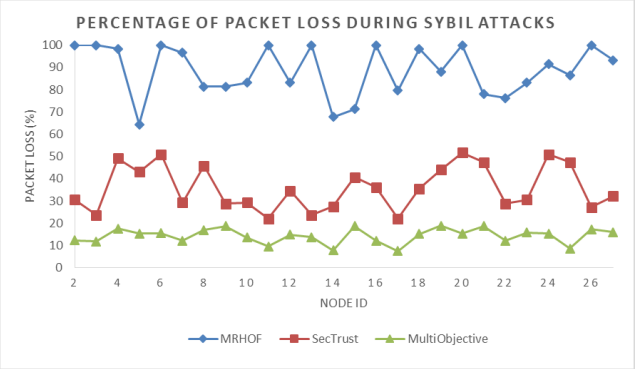
شکل ۹: مقایسه نرخ بسته‌های پراتلاف بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Rank

شکل ۱۰ مقایسه فرکانس تغییرات درجه گره بین MRHOF-RPL، SecTrust-RPL و MultiObjective-RPL را نشان می‌دهد. آسیب پذیری MRHOF-RPL به تغییرات رتبه گره در برابر حملات Rank نسبت به SecTrust-RPL و MultiObjective-RPL بسیار بیشتر است. بعلاوه همانطور که از روی شکل ۱۰ نیز مشخص است آسیب پذیری SecTrust-RPL نیز نسبت به MultiObjective–RPL به طور قابل توجهی بیشتر است. از طرف دیگر، MultiObjective - RPL به طور مداوم در طول مدت زمان شبیه سازی ۶۰ دقیقه‌ای تغییرات درجه گره را در حد پایین حفظ می‌کند.



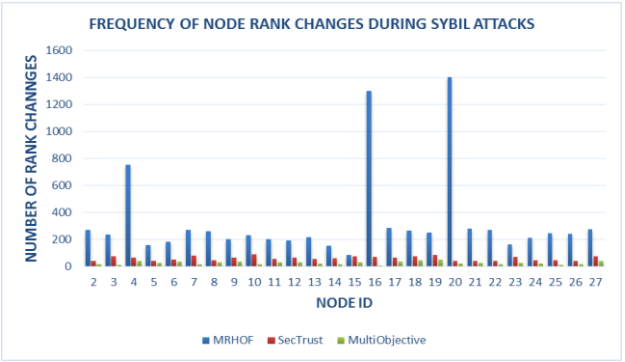
شکل ۱۰: مقایسه فرکانس تغییرات رتبه گره بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Rank

در شکل ۱۱ یک مقایسه بین نرخ بسته‌های پراتلاف MultiObjective-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های پراتلاف MRHOF-RPL در بازه ۶۴ تا ۱۰۰ درصد است درحالی که این بازه برای SecTrust-RPL بین ۲۲ تا ۵۱ درصد است و برای MultiObjective-RPL بین ۷ تا ۱۸ درصد است. در نتیجه، پروتکل MultiObjective-RPL در مقایسه با دو پروتکل دیگر در مقابل حملات Sybil عملکرد بهتری را نشان می-دهد. به این دلیل که میانگین نرخ بسته‌های پراتلاف کمتری نسبت به دو پروتکل دیگر را ارائه کرده است.



شکل ۱۱: مقایسه نرخ بسته‌های پراتلاف بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Sybil

شکل۱۲ مقایسه فرکانس تغییرات درجه گره بین MRHOF-RPL، SecTrust-RPL و MultiObjective-RPL را نشان می‌دهد. آسیب پذیری MRHOF-RPL به تغییرات رتبه گره در برابر حملات Sybil نسبت به SecTrust-RPL و MultiObjective-RPL بسیار بیشتر است. بعلاوه همانطور که از روی شکل ۱۲ مشخص است آسیب پذیری SecTrust-RPL در مقایسه با MultiObjective–RPL بسیار بیشتر است. از طرف دیگر، MultiObjective-RPL به طور مداوم در طول دوره شبیه‌سازی تغییرات درجه گره را در حد پایین حفظ می‌کند.

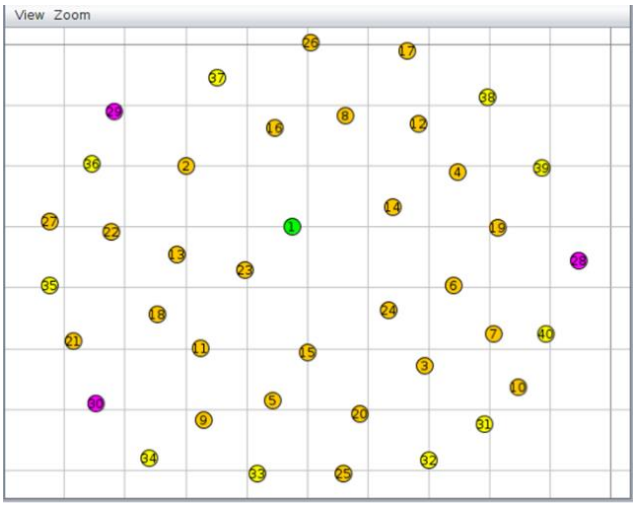


شکل ۱۲: مقایسه فرکانس تغییرات رتبه گره بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Sybil

هدف از اجرای سناریوی دوم، نشان دادن تاثیر افزایش تعداد گره‌های مخرب در عملکرد روش پیشنهادی با سایر روش‌های مقایسه شده است. نتایج شبیه‌سازی بیانگر کارایی بیشتر روش پیشنهادی در مقایسه با دو روش دیگر هم از نظر نرخ بسته‌های پراتلاف و هم از نظر میزان پایداری گره‌ها حتی با افزایش تعداد گره‌های مخرب در شبکه است.

۴-۳- سناریوی سوم

در سناریوی سوم شبکه‌ای با ۴۰ عدد گره که در محیطی با ابعاد ۷۰*۷۰ مترمربع گسترده شده‌اند، مدت زمان شبیه‌سازی ۱ ساعت در نظر گرفته شده است. توپولوژی شبکه و نحوه‌ی استقرار گره‌ها در شبیه ساز Cooja در شکل ۱۳ نشان داده شده است. گره Sink با رنگ سبز و گره‌های ارسال کننده با رنگ نارنجی و گره‌های حمله کننده با رنگ بنفش نشان داده شده‌اند. در این شبیه‌سازی، حملات Sybil و Rank نیز ارائه شده‌اند. در جدول ۴، تاخیر زمانی اولیه ۵ ثانیه برای همگرایی گره‌ها در شبکه RPL در نظر گرفته شده است. جدول ۴ جزئیات بیشتری از تنظیمات شبیه‌سازی ارائه کرده است.



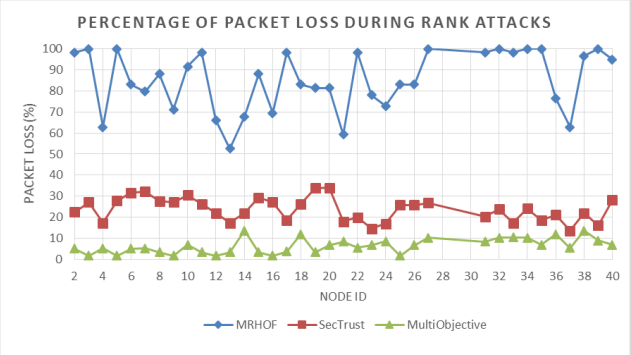
شکل ۱۳: شبکه RPL با ۴۰ گره شامل ۳ گره حمله کننده در شبیه ساز COOJA

جدول ۳: تنظیمات و پارامترهای شبیه سازی شبکه در سناریوی دوم

پارامترها	مقدار
Simulation tool	Contiki/Cooja 3.0
Simulation coverage area	70 m * 70 m
Total number of nodes	40
Malicious nodes	3 (Nodes 28, 29, and 30)
Malicious to legitimate node ratio	1.5 : 20
TX range	50 m
Interference range	55 m
Start delay	5 s
Simulation time	60 min
Link failure model	UDGM with distance

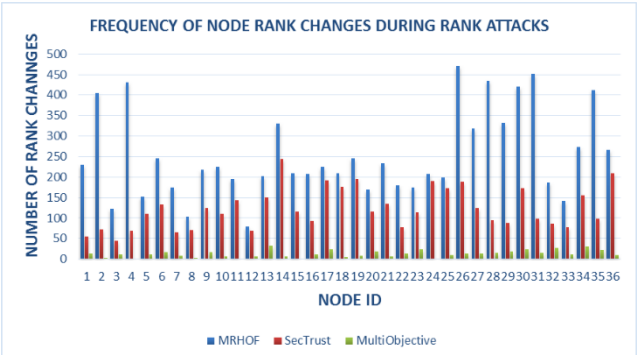
برد رادیویی و برد تداخلی برای همه دستگاه‌ها به ترتیب ۵۰ متر و ۵۵ متر تنظیم شده است. شبیه‌سازی با ۴۰ گره شامل ۳ گره حمله کننده برای ۶۰ دقیقه اجرا شده است. نتایج شبیه‌سازی در قسمت بعدی مورد بحث و بررسی قرار گرفته است.

در شکل ۱۴ مقایسه بین نرخ بسته‌های پراتلاف MultiObjective-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های پراتلاف MRHOF-RPL در بازه ۵۲ تا ۱۰۰ درصد است درحالی که این بازه برای SecTrust-RPL بین ۱۳ تا ۳۳ درصد است و برای MultiObjective-RPL بین ۱ تا ۱۳ درصد است. میانگین نرخ بسته‌های پراتلاف MultiObjective-RPL ۶ تا ۷ درصد است که این مقدار در مقایسه با دو پروتکل دیگر بسیار کمتر است. در نتیجه، پروتکل MultiObjective-RPL در مقایسه با دو پروتکل دیگر در مقابل حملات Rank عملکرد بهتری را نشان می‌دهد.



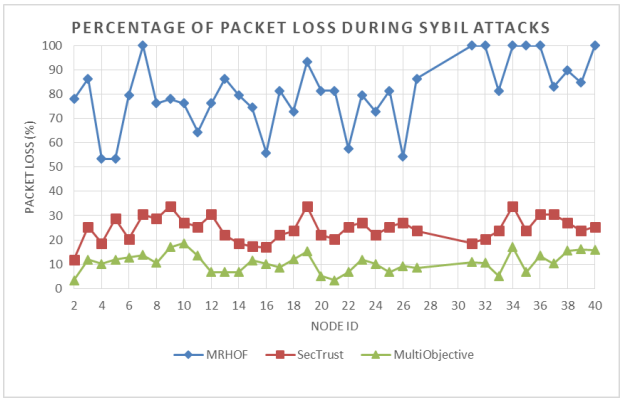
شکل ۱۴: مقایسه نرخ بسته‌های پراتلاف بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Rank

شکل ۱۵ مقایسه فرکانس تغییرات درجه گره بین MRHOF-RPL، SecTrust-RPL و MultiObjective-RPL را نشان می‌دهد. آسیب پذیری MRHOF-RPL به تغییرات رتبه گره در برابر حملات Rank نسبت به SecTrust-RPL و MultiObjective-RPL بسیار بیشتر است. بعلاوه همانطور که از روی شکل ۱۵ مشخص است آسیب پذیری SecTrust-RPL نیز در برابر حملات Rank نسبت به MultiObjective–RPL به طور قابل توجهی بیشتر است. از طرف دیگر، MultiObjective-RPL به طور مداوم در طول مدت زمان شبیه‌سازی ۶۰ دقیقه‌ای تغییرات درجه گره را در حد پایین حفظ می‌کند.



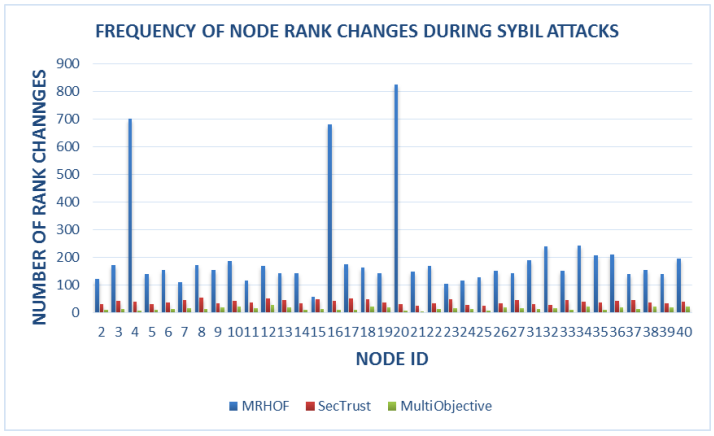
شکل ۱۵: مقایسه فرکانس تغییرات رتبه گره بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Rank

در شکل ۱۶ یک مقایسه بین نرخ بسته‌های پراتلاف MultiObjective-RPL با SecTrust-RPL و MRHOF-RPL ارائه شده است. نرخ بسته‌های پراتلاف MRHOF-RPL در بازه ۵۳ تا ۱۰۰ درصد است درحالی که این بازه برای SecTrust-RPL بین ۱۱ تا ۳۳ درصد است و برای MultiObjective-RPL بین ۳ تا ۱۸ درصد است. در نتیجه، پروتکل MultiObjective-RPL در مقایسه با دو پروتکل دیگر در مقابل حملات Sybil عملکرد بهتری را نشان می‌دهد. به این دلیل که میانگین نرخ‌های پراتلاف کمتری نسبت به دو پروتکل دیگر را ارائه کرده است.



شکل ۱۶: مقایسه نرخ بسته‌های پراتلاف بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Sybil

شکل ۱۷ مقایسه فرکانس تغییرات درجه گره بین MRHOF-RPL و SecTrust-RPL را نشان می‌دهد. MRHOF-RPL آسیب پذیری نسبت به SecTrust-RPL نسبت به تغییرات رتبه گره به طور قابل توجهی بالاتر نشان می‌دهد ، آسیب پذیری در برابر حملات Rank را نشان می‌دهد. از طرف دیگر ، SecTrust-RPL به طور مداوم در طول دوره شبیه‌سازی تغییرات درجه گره پایین را حفظ می‌کند.



شکل ۱۷: مقایسه فرکانس تغییرات رتبه گره بین MultiObjective-RPL، SecTrust-RPL و MRHOF-RPL تحت حملات Sybil

هدف از اجرای سناریوی سوم، نشان دادن تاثیر افزایش تعداد گره‌های نرمال در عملکرد روش MultiObjective-RPL در مقایسه با روش‌های SecTrust-RPL و MRHOF-RPL است. که نتایج شبیه‌سازی بیانگر بهبود کارایی روش پیشنهادی در مقایسه با دو روش دیگر هم از نظر نرخ بسته‌های پراتلاف و هم از نظر میزان پایداری گره‌ها حتی با وجود افزایش تعداد گره‌های نرمال در شبکه است.

۵- نتیجه گیری

این بخش به جمع‌بندی و نتیجه‌گیری پژوهش اختصاص داده شده است. ظهور اینترنت اشیا و پیشرفت آن در سال‌های آینده انقلاب قرن فعلی خواهد بود. در اینترنت اشیا تمامی اشیای هوشمند از قبیل تجهیزات تعبیه شده، گوشی‌های هوشمند، حسگر و ... با استفاده از فضای آدرس دهی 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 تعبیه شده 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 اینگونه شبکه‌ها طراحی گردیده است. تاکنون پژوهش‌های محدودی در رابطه با مسیریابی چندهدفه مبتنی بر RPL در حوزه اینترنت اشیا انجام شده است. به همین دلیل در این پژوهش، یک روش مسیریابی چندهدفه مبتنی بر RPL در حوزه اینترنت اشیا ارائه شده است. در روش پیشنهادی از معیارهای مختلفی برای مسیریابی استفاده شده است. بهره‌گیری از این معیارها باعث افزایش کارایی شبکه شده است. همچنین نتایج به دست آمده از شبیه‌سازی نیز سودمندی روش ارائه داده شده را تایید می‌کند. روش پیشنهادی با دیگر روش‌های ارائه شده مقایسه شد و نتایج نشان می‌دهند که روش پیشنهادی به دلیل انتخاب مسیر بهینه‌تر، نسبت به سایر روش‌ها عملکرد بهتری دارد.

مراجع

[1] Ashton, K., That ‘internet of things’ thing. RFID journal, 2009. 22(7): p. 97-114.

[2] Majid, M., et al., Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 2022. 22(6): p. 2087.

[3] Shelby, Z. and C. Bormann, 6LoWPAN: The wireless embedded Internet. Vol. 43. 2011: John Wiley & Sons.M.B.A. Haghighat, “Biometrics for Cybersecurity and Unconstrained Environments”, Ph.D. Thesis, University of Miami, USA, 2016.

[4] RFC791, I., Internet Protocol DARPA internet program protocol specification. 1981, September

[5] John, S.P. and P. Samuel, Self-organized key management with trusted certificate exchange in MANET. Ain Shams Engineering Journal, 2015. 6(1): p. 161-170.

[6] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC2460, December 1998.

[7] D. Harrington, R. Presuhn and B. Wijnen, “An Architecture for Describing SNMP Management Frameworks”, RFC2571, April 1999.

[8] Winter, T., et al., RPL: IPv6 routing protocol for low-power and lossy networks. 2012.

[9] Ko, J., et al., Connecting low-power and lossy networks to the internet. IEEE Communications Magazine, 2011. 49(4): p. 96-101.

[10] Chang, L.-H., et al. Energy-efficient oriented routing algorithm in wireless sensor networks. in Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on. 2013. IEEE.

[11] Machado, K., et al., A routing protocol based on energy and link quality for internet of things applications. sensors, 2013. 13(2): p. 1942-1964.

[12] Said, O., Analysis, design and simulation of Internet of Things routing algorithm based on ant colony optimization. International Journal of Communication Systems, 2017. 30(8): p.

[13] Oteafy, S.M., F.M. Al-Turjman, and H.S. Hassanein. Pruned adaptive routing in the heterogeneous Internet of Things. in Global Communications Conference (GLOBECOM), 2012 IEEE. 2012. IEEE.

[14] Guo, J. and R. Chen. A classification of trust computation models for service-oriented internet of things systems. in Services Computing (SCC), 2015 IEEE International Conference on. 2015. IEEE.

[15] Kim, H.-S., et al., Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks. IEEE Transactions on Mobile Computing, 2017. 16(4): p. 964-979

[16] Shen, J., et al., An Efficient Centroid-Based Routing Protocol for Energy Management in WSN-Assisted IoT. IEEE Access, 2017. 5: p. 18469-18479.

[17] Djedjig, N., et al. New trust metric for the RPL routing protocol. in 2017 8th International Conference on Information and Communication Systems (ICICS). 2017. IEEE.

[18] Glissa, G., A. Rachedi, and A. Meddeb. *A secure routing protocol based on RPL for Internet of Things*. in *Global Communications Conference (GLOBECOM), 2016 IEEE*. 2016. IEEE.

[19] Dhumane, A.V. and R.S. Prasad, *Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT*. Wireless networks, 2019. **25**(1): p. 399-413.

[20] Kamble, A., V.S. Malemath, and D. Patil. *Security attacks and secure routing protocols in RPL-based Internet of Things: Survey*. in *Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on*. 2017. IEEE.

[21] Airehrour, D., J.A. Gutierrez, and S.K. Ray, SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 2018

[22] Medjek, F., et al., *Multicast DIS attack mitigation in RPL-based IoT-LLNs*. Journal of Information Security and Applications, 2021. **61**: p. 102939.

[23] Zarzoor, A.R., Optimizing RPL performance based on the selection of best route between child and root node using E-MHOF method. International Journal of Electrical & Computer Engineering (2088-8708), 2021. 11(1).

[24] Hazarika, B., R. Matam, and S. Tripathy. Multiple RPL Objective Functions for Heterogeneous IoT Networks. in International Conference on Advanced Information Networking and Applications. 2021. Springer.

[25] Gupta, N., A. Pughat, and V. Sharma, A critical analysis of RPL objective functions in internet of things paradigm. Peer-to-Peer Networking and Applications, 2021. 14(4): p. 2187-2208.
[26] Chen R, Guo J, Bao F. Trust management for SOA-based IoT and its application to service composition. IEEE Transactions on Services Computing. 2014 Oct 30;9(3):482-95.
[27] Sennan, S., et al., Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. Transactions on Emerging Telecommunications Technologies, 2020: p. e4171.
[28] Pushpalatha, M., et al., L-RPL: RPL powered by laplacian energy for stable path selection during link failures in an Internet of Things network. Computer Networks, 2021. 184: p. 107697.

پاورقی‌ها:

[1] Information technology
[2] Chang
[3] Machado
[4] Routing by Energy and Link quality
[5] end-to-end
[6] Omar Said
[7] Oteafy
[8] Guo
[9] Trust composition
[10] Trust propagation
[11] Trust aggregation
[12] Trust update
[13] Trust formation
[14] Kim
[15] Queue utilization based RPL
[16] Border router
[17] Shen
[18] Energy-efficient centroid based routing protocol
[19] Cluster head
[20] Djedjig
[21] Metric-based RPL Trustworthiness Scheme
[22] DODAG Information Object
[23] Extended RPL Node Trustworthiness
[24] Trust Objective Function
[25] Glissa
[26] Secure routing protocol based on RPL
[27] Sinkhole
[28] Black hole
[29] Selective forwarding
[30] Dhumane
[31] Multi-objective Fractional Gravitational Search Algorithm
[32] Kamble
[33] Loops
[34] Airehrour
[35] Secure-Trust-RPL
[36] Rank Attack
[37] Medjek
[38] Zarzoor
[39] Hazarika
[40] Gupta
[41] Parent count
[42] Parent energy
[43] Link