ICWR2022
May 11-12, 2022; Tehran, Iran
8th International Conference on Web Research

A Novel and Secure Energy-aware Routing Protocol for IoT based on Cryptography

Zohre Shoaei*[1], Rasool Esmaeilyfard[2]

[1] PhD student, Faculty of Computer Engineering and Information Technology, Shiraz University of Technology, Fars, Iran
z.shoaei@sutech.ac.ir

[2] Assistant Professor, Faculty of Computer Engineering and Information Technology, Shiraz University of Technology, Fars, Iran
esmaeily@sutech.ac.ir

Abstract

The Internet of Things (IoT) has introduced new advances in sensors, Internet technologies, and communication protocols. Sensors in the IoT network have the important task of collecting information from the environment in which they are located. These sensors face important limitations such as limited energy resources, data storage, transmission, and processing power. In addition to the inherent limitations of the network's sensor nodes, they are vulnerable to a variety of security threats due to the presence of invasive and malicious nodes. In previous research, less attention has been paid to the issue of energy conservation and secure routing. Accordingly, in this paper, an energy-aware and secure protocol for routing data in the Internet of Things is presented. This protocol detects and prevents data compromise by simultaneously using the heuristic and Elliptic-curve Diffie–Hellman (ECDH) cryptographic method. The evaluation shows the proper performance of the proposed protocol compared to competing protocols. The results showed that the protocol managed to improve the metrics for the number of lost packets by 13.44%, the throughput by 86.55%, and the power consumption by 0.022% for 250 nodes.

Keywords: Internet of Things, Energy-Aware Routing, Secure Routing, Heuristic Algorithms, Elliptic-curve Diffie–Hellman Cryptography.

ICWR2022
May 11-12, 2022; Tehran, Iran
8th International Conference on Web Research

یک پروتکل جدید و ایمن مسیریابی آگاه از انرژی برای اینترنت اشیا مبتنی بر رمزنگاری

زهره شعاعی*[۱]، رسول اسماعیلی‌فرد[۲]

[۱] دانشجوی دکتری، دانشکده مهندسی کامپیوتر و فناوری اطلاعات ، دانشگاه صنعتی شیراز، فارس ، ایران
z.shoaei@sutech.ac.ir

[۲] استادیار ، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شیراز، فارس، ایران
esmaeily@sutech.ac.ir

چکیده

اینترنت اشیاء پیشرفت‌های جدیدی را در حسگرها، فناوری‌های اینترنتی و پروتکل‌های ارتباطی ایجاد کرده است. حسگرها در شبکه اینترنت اشیا وظیفه مهم جمع‌آوری اطلاعات از محیطی که در آن قرار دارند را برعهده دارند. این حسگرها با محدودیت‌های مهمی نظیر منابع محدود انرژی، ذخیره داده، انتقال و قدرت پردازش روبرو هستند. علاوه بر محدودیت‌های ذاتی در گره‌های حسگری این شبکه، آنها در برابر انواع تهدیدات امنیتی به دلیل وجود گره‌های مهاجم و مخرب، آسیب‌پذیر هستند. در تحقیقات گذشته به موضوع حفظ همزمان انرژی و مسیریابی امن کمتر توجه شده است. بر این اساس در این مقاله، یک پروتکل آگاه از انرژی و امن برای مسیریابی داده‌ها در شبکه اینترنت اشیا ارائه شده است. این پروتکل با بکارگیری همزمان روش اکتشافی و رمزنگاری منحنی بیضوی دیفی هلمن به خطر افتادن داده را تشخیص می‌دهد و از آن جلوگیری می‌کند. ارزیابی انجام گرفته نشان از عملکرد مناسب پروتکل پیشنهادی نسبت به پروتکل های رقیب دارد. نتایج نشان داد که پروتکل موفق شده است معیارهای تعداد بسته‌های از دست رفته را به میزان ۱۳,٤٤ درصد، توان عملیاتی را به میزان ۸٦,٥٥ درصد و تحلیل و میزان مصرف انرژی را ۰,۰۲۲ درصد برای ۲۵۰ نود بهبود دهد.

کلمات کلیدی

اینترنت اشیا، مسیریابی انرژی آگاه، مسیریابی امن، الگوریتم‌های اکتشافی، رمزنگاری منحنی بیضوی دیفی هلمن

۱- مقدمه

پیشرفت فن‌آوری‌های اطلاعات و ارتباطات نشان می‌دهد که عصر دیگری از فراگیری هوشمندسازی در زمینه برنامه‌های کاربردی اینترنت اشیا در حال شکل‌گیری است. شبکه‌های اینترنت اشیا از سنسورهای کوچک تشکیل شده‌اند که برای مشاهده و ثبت شرایط فیزیکی با اشیا تعامل دارند[۱]. گره‌های سنسور مستقل هستند و توپولوژی ارتباطی بین خود را به صورت موقت ایجاد می‌کنند.

در برنامه‌های اینترنت اشیا، سنسورها داده‌های حس شده را برای سایر عملیات به ایستگاه مرکزی ارسال می‌کند. این امر از طریق پروتکل‌های مسیریابی کارآمد برای بهبود انتقال داده‌ها همراه با مقیاس‌پذیری و بهره‌وری انرژی حاصل می‌شود، که در نتیجه امکان اجرا و توسعه شبکه تقویت می‌شود [۲]. با این حال، محدودیت‌های اصلی گره‌های حسگر منابع محدود آنها برای

مدیریت انرژی، ذخیره داده، انتقال و قدرت پردازش است. با وجود تحقیقات صورت گرفته در این نوع شبکه‌ها، گره‌های حسگر به تعداد زیاد و اندازه‌ی کوچک، هنوز هم برای تامین انرژی خود، وابسته به باتری‌های با توان اندک هستند. همچنین بخاطر به کارگیری این نوع شبکه‌ها در محیط‌های بزرگ و وسیع، امکان شارژ مداوم یا تعویض سنسورها به راحتی امکان پذیر نیست[۳, ۴]. به دلیل توسعه‌ی سریع سیستم‌های اینترنت اشیا ، اطلاعات و تهدیدات متعدد شبکه‌ای وجود دارد که مانع رشد آن می‌شود [۵].

بنابراین یکی از مسائل مهم در بسیاری از برنامه‌ها بهبود بهره‌وری انرژی برای شبکه‌های اینترنت اشیا با تحویل امن و به موقع داده‌ها است. زیرساخت اینترنت اشیا اغلب مبتنی بر استفاده از زیرساخت شبکه اینترنت است و در این میان به دلیل به منظور کاهش مصرف انرژی و مسیریابی در این شبکه ها پروتکل هایی نظیر RPL بصورت گسترده مورد استفاده قرار می‌گیرند. این پروتکل با انتقال چند هاپه داده‌ها به سمت ایستگاه مرکزی داده‌ها را مسیریابی می‌کند. در این میان، راه‌حل‌های متفاوتی توسط محققان برای دسته‌بندی گره‌های حسگر، افزایش طول عمر شبکه و پوشش شبکه‌ای در محدوده‌های مختلف پیشنهاد شده است. به عنوان نمونه، Sankar و همکاران [۶] با خوشه بندی مبتنی بر درخت طول عمر شبکه را افزایش داده و از ارسال ترافیک تکراری بین گره‌های شبکه جلوگیری کرده است. افزایش طول عمر شبکه، به دو معیار کلیدی معیار کاهش مصرف انرژی و توزیع صحیح مصرف انرژی بین گره‌های حسگر وابسته است[۷]. در حوزه‌ی بهینه‌سازی مصرف انرژی در این نوع شبکه‌ها، پروتکل‌های مسیریابی کارآیی شبکه را تا حد زیادی تحت تأثیر قرار می‌دهند. اما صرفا مصرف انرژی کافی نیست و در بسیاری از حوزه‌ها و کاربردهای اینترنت اشیاء نیاز به ارسال سریع و همچنین امن داده‌ها وجود دارد. در این حالت کمینه کردن تاخیر که وابسته به مسیر مناسب است یک فاکتور بسیار مهم خواهد بود. فاکتور مهم دوم، ارسال و مسیریابی امن داده‌ها به منظور جلوگیری از حملات مخرب توسط مهاجمین خواهد بود.

با در نظر گرفتن این شرایط این مقاله به ارائه پروتکلی جدید می‌پردازد که بطور همزمان مسیریابی سریع و آگاه از انرژی برای افزایش طول عمر شبکه همراه با رمزنگاری داده‌ها با حداقل سربار و ایمن سازی عملیات مسیریابی با وجود گره‌های مخرب و مهاجم را مد نظر قرار می دهد. در این مقاله از الگوریتم رمزنگاری منحنی بیضوی دیفی هلمن (ECDH)[۲] بدین منظور استفاده شده است.

مهمترین نوآوری های این مقاله به شرح زیر هستند:

- این مقاله یک پروتکل مسیریابی انرژی آگاه امن برای افزایش طول عمر شبکه های اینترنت اشیا ارائه می‌دهد که به طور موثر شبکه را مدیریت می‌کند.
- در پروتکل پیشنهادی به‌منظور مقابله با محدودیت حافظه در سنسورهای شبکه‌های اینترنت اشیا از الگوریتم جستجوی پرتو استفاده شده است.
- پروتکل مسیریابی پیشنهادی برای انتقال امن داده‌ها در شبکه‌های اینترنت اشیا از روش رمزنگاری منحنی بیضوی دیفی هلمن استفاده می‌کند.
- ثبات و حفظ مسیر در پروتکل پیشنهادی با استفاده از محاسبه نسبت ترافیک برای لینک مورد نظر حفظ شده است.
- ارزیابی از عملکرد پروتکل پیشنهادی بر اساس معیارهای مختلف انجام شده است.

ادامه‌ی این مقاله به شرح زیر سازمان‌دهی شده است:

بخش ۲ پیشینه‌ی تحقیق را مرور می‌کند. بخش ۳ جزئیات پروتکل پیشنهادی را ارائه می‌دهد. نتایج شبیه‌سازی و ارزیابی عملکرد مقایسه‌ای مبتنی بر شبیه سازی در بخش ۴ مورد بحث قرار گرفته است و در آخر به بحث و نتیجه‌گیری و ارائه زمینه های پیشنهادی برای تحقیقات آینده پرداخته شده است.

۲- پیشینه تحقیق

در این بخش به بررسی پژوهش‌های پیشین در حوزه ارائه پروتکل‌های امن و آگاه از انرژی می‌پردازیم. بخش زیادی از پژوهش های گذشته به موضوع ارائه الگوریتم‌های انرژی اگاه برای مسیریابی در حوزه اینترنت اشیا پرداخته‌اند.

به عنوان مثال، Mir و همکاران [۸]، یک رویکرد انرژی آگاه کارآمد برای مسیریابی در اینترنت اشیا پیشنهاد شده است که در آن تمرکز بر برنامه زمانبندی خواب–بیداری گره‌ها است. آنها از یک الگوریتم بهینه‌سازی جدید به نام الگوریتم بهینه‌سازی ملخ فازی استفاده کردند. الگوریتم پیشنهادی احتمال شکست در مقابل حملات و تهدیدات امنیتی را دارد. اما پروتکل پیشنهادی نمی‌تواند با تهدیدات شبکه مقابله کند و امنیت بالایی ندارد.

Bouaziz و همکاران [۹]، پروتکلی به نام EMA-RPL ارائه دادند که برخلاف RPL که اساساً برای دستگاه‌های استاتیک طراحی شده است، باعث می‌شود اتصال گره‌های متحرک بهتر حفظ شود و انرژی ذخیره شود. EMA-RPL بر مشکلات ناشی از تحرک گره ها غلبه کرده و آنها را کاهش می دهد. مجدداً بحث امنیت نیز در این پروتکل مورد توجه قرار نگرفته است.

Djedjig و همکاران [۱۰]، برای رسیدگی به فقدان مکانیسم‌های امنیتی قوی در RPL، یک طرح ارزش اعتماد RPL مبتنی بر متریک MRTS را طراحی کردند که ارزیابی اعتماد را برای ساخت توپولوژی مسیریابی امن معرفی می‌کند. شبیه سازی های گسترده نشان می دهد که MRTS از نظر نسبت تحویل بسته، مصرف انرژی، تغییرات رتبه گره‌ها و توان عملیاتی کارآمد است اما از متریک‌های مهم ارزیابی دیگری که امنیت پروتکل را با درصد بالایی تضمین کند استفاده نشده است.

Praveen و همکاران [۱۱]، یک پروتکل مسیریابی و تخصیص منابع آگاه از تراکم انرژی (ECRR) برای شبکه اینترنت اشیا بر اساس تکنیک‌های بهینه‌سازی ترکیبی را پیشنهاد دادند. این پروتکل نیز با وجود کاهش و بهبود مصرف انرژی، در برابر تهدیدات امنیتی مقاوم نبوده و ممکن است در صورت حملات و گره‌های مخرب عملکرد شبکه تحت تاثیر قرار گیرد.

Vijayalakshmiو همکاران [۱۲]، یک روش خوشه‌بندی سلسله مراتبی پیشرفته برای شبکه‌های حسگر تلفن همراه با استفاده از سیستم‌های استنتاج فازی پیشنهاد شد.آزمایشات مبتنی بر شبیه‌سازی نشان داد که راه حل پیشنهادی عملکرد شبکه را در طول عمر و انحراف خوشه نسبت به سایر کارها بهبود بخشیده است.

در پژوهش دیگری، Gaber و همکاران [۱۳]، یک روش خوشه‌بندی سلسله مراتبی پیشرفته برای شبکه‌های حسگر تلفن همراه با استفاده از سیستم‌های استنتاج فازی پیشنهاد شد که هدف آن کاهش مصرف انرژی و کاهش تلفات بسته بین گره‌های حسگر تلفن همراه است. ، نتایج نشان می‌دهد که گره‌ها در صورت وجود مخرب در برابر تهدیدات امنیتی آسیب‌پذیر هستند.

Salameh و همکارانش [۱۴]، یک پروتکل مسیریابی RPL امن در اینترنت اشیاء برای ایمن سازی ارتباطات از رتبه و حملات Sybil پیشنهاد کردند. اگرچه ، پروتکل پیشنهادی عملکرد مسیریابی را در برابر تهدیدهای شبکه بهبود می بخشد ، اما تصمیم مسیریابی مطلوب نیست و عملکرد تحویل داده را کاهش می‌دهد.

Binu و همکاران [۱۵]، یک استراتژی جدید مسیریابی انرژی آگاه با استفاده از روش‌های اکتشافی پیشنهاد کردند که هدف آن کاهش بار مصرف انرژی و نسبت از دست رفتن بسته است. راه حل پیشنهادی هیچ طرح امنیتی برای مقابله با تهدیدات مخرب را ندارد.

Edla و همکاران [۱۶]، یک پروتکل امنیتی جدید با استفاده از الگوریتم‌های مشارکتی ارائه دادند که هدف آن بهبود عملکرد و قابلیت ارتجاعی و اطمینان داده‌ها در برابر حملات سایبری است. نتایج نشان داد که روش ارائه شده امنیت شبکه را بهبود می‌بخشد، اما با تعداد کمی از گره‌های حسگر مناسب است و عملکرد مسیریابی نادیده گرفته می‌شود.

در پژوهشی Lee و همکاران [۱۷] مسیریابی امن را در شبکه‌های اینترنت اشیا تحت حمله‌ی Jamming (مسدود کردن) پیشنهاد کردند، که هدف آن بهبود عملکرد ارائه داده‌ها و ایمن‌سازی مسیر مسیریابی از مبدا به مقصد است. با این حال، تصمیم مسیریابی با در نظر گرفتن پارامترهای مهم شبکه مطلوب نیست. علاوه بر این ، عملکرد راه حل پیشنهادی فقط بر اساس نسبت تحویل بسته مورد تجزیه و تحلیل قرار می گیرد و سایر معیارهای شبکه را نادیده می‌گیرد.

در این میان برخی از پژوهش ها شبکه‌های حسگر بیسیم که زادگاه اینترنت اشیا است را مورد توجه قرار داده اند و مطالعاتی را در این زمینه انجام داده اند. به عنوان مثال، Haseeb و همکاران [۱۸]، یک پروتکل مسیریابی امن و آگاه از انرژی برای شبکه‌های حسگر بی‌سیم ارائه داده اند که هدف آن بهینه‌سازی استراتژی مسیریابی با تصمیم‌گیری هوشمند در برابر گره‌های مخرب است. این پروتکل که SEHR نام دارد، بر عوامل حیاتی مانند مصرف انرژی ، تحویل امن داده‌ها و نگهداری مسیر متمرکز است. این کار از طریق اعمال محدودیت‌های اساسی برای دستیابی به انتقال قابل اعتماد انجام می گیرد. اما علیرغم امن بودن آن، از محدودیت‌های اساسی این مقاله استفاده از روش رمزنگاری CTR است. CTR یک روش بلاکی است و یک بلاک افزونه همراه خودش ایجاد می‌کند. این بلاک افزونه قطعا باید ارسال شود که باعث می‌شود حجمی از صف ایجاد شده را اشغال کند. ما در این مقاله از روش رمزنگاری منحنی بیضوی دیفی هلمن استفاده کرده ایم و این مشکل در این پژوهش وجود ندارد.

در مطالعات گذشته تمرکز تمرکز بر بهینه سازی سربارها بوده است و حتی در مواردی که از روش های ایمن استفاده شده است این روش ها سربار بالایی ایجاد کرده اند. در این مقاله سعی بر این است تا با استفاده از روش رمزنگاری منحنی بیضوی دیفی هلمن و ویژگی کوتاه بودن طول کلید و تبادل سریعتر کلید انتخاب مسیر دقیق تر و با سربار کمتری انجام گیرد.

۳- پروتکل پیشنهادی

در این بخش پروتکل پیشنهادی ارائه خواهد شد و شرح پروتکل پیشنهادی و مراحل آن ارائه می شود. پروتکل پیشنهادی برای دستگاه‌های با محدودیت کم توسعه یافته است تا نتایج شبکه را برای مصرف انرژی کارآمد داده‌ها و امنیت آن بهبود بخشد. در این راستا، فرضیات زیر مورد نظر قرار گرفته اند:

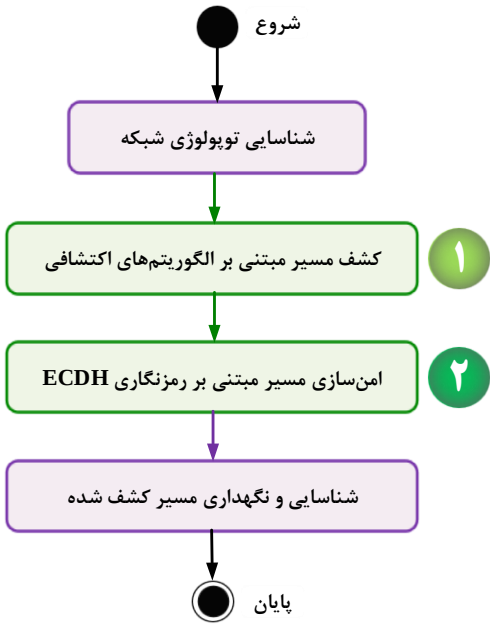
- همه گره‌ها از نظر منابع محدود هستند ، به استثنای ایستگاه مرکزی
- گره‌ها پس از توزیع در منطقه شبکه به اندازه ابعاد شبکه ثابت می مانند.
- گره‌ها مجهز به سیستم GPS هستند.
- همه گره‌ها همگام هستند تا بتوانند بطور همزمان فعال شوند و داده‌ها را حس کنند و انتقال دهند.
- یک گره مخرب یک پاسخ اشتباه برای انتخاب مسیر مرحله بعدی ارسال می‌کند.

جدول (۱) فهرستی از نمادهای استفاده شده در پروتکل پیشنهادی را نشان می دهد.

مراحل کلی پروتکل پیشنهادی در شکل (۱) نمایش داده شده است. در این پروتکل پس از شکل گیری توپولوژی شبکه، تعداد گره‌ها و لینک‌ها و سایر پارامترهای شبکه شناسایی می شود. فرض بر این است که در این توپولوژی تعدادی از گره‌ها به عنوان گره مخرب عمل می کنند. در ادامه دو مرحله اصلی کشف مسیر و امن‌سازی مسیر انجام می گیرد.

جدول (۱): نمادها

نمادها	تعریف
G(N,L)	گرافی با N نود و L یال
$\mathbf{h_{BS}}$	تعداد گام‌ها تا ایستگاه مرکزی
$\mathbf{e_i}$	انرژی باقیمانده در نود i
$\mathbf{dl_i}$	درجه یکپارچگی پیوند برای نود i
$\|$	الحاق
h(f)	تابع هش
M(c)	کد پیام
$\mathbf{energy_{thres}}$	آستانه‌ی انرژی
$\mathbf{P_1}$	بسته‌ی کاوشگر
$\mathbf{n_1}, \mathbf{n_2}$	گره‌های متصل
RREQ	درخواست مسیر
$W(\mathbf{f_n})$	مجموع وزنی
W(beam width)	عرض پرتو
p	تعریف عدد اول فیلد محدود F_p
a,b	پارامترهای تعیین کننده منحنی y^2
G	نقطه مولد
d	کلید خصوصی
Q	کلید عمومی



شکل (۱): روند پروتکل پیشنهادی

در مرحله‌ی اول، از الگوریتم اکتشافی برای بهینه‌سازی تصمیم‌گیری برای مسیریابی مطمئن داده‌ها استفاده می شود. الگوریتم اکتشافی نیز از پارامترهای شبکه و یکپارچه سازی پیوندها برای انتخاب هوشمند مسیر بعدی و کاهش حافظه مصرفی گره‌ها استفاده می‌کند. در مرحله‌ی دوم با هدف ایجاد مسیریابی امن داده‌ها، رمزنگاری منحنی بیضوی دیفی هلمن ECDH انجام می‌شود. در آخر مسیر کشف شده نگهداری می‌شود. در ادامه جزئیات هر یک از مراحل شرح داده شده است.

۳-۱-شناسایی توپولوژی شبکه

ابتدا گره‌های سنسور شبکه اینترنت اشیا در یک گراف غیرجهت‌دار G قرار می گیرند. در گراف $G(N;L)$، N تعداد گره‌ها را نشان می‌دهد و L پیوند بهینه شده بین دو گره‌ی متصل شده n_1و n_2 است. در ابتدای کار، مسیر بین همسایگان بر مبنای فاکتور فاصله محاسبه می‌شود.

در مرحله اول، از تابع اکتشافی برای محاسبه مقدار وزنی برای یافتن گره مطلوب به عنوان مرحله بعدی استفاده می شود. تابع اکتشافی تصمیم مسیریابی را به سمت گره مقصد هدایت می‌کند. در پروتکل پیشنهادی، تابع اکتشافی یک مسیر آموزش دیده را برای پیش‌بینی مطلوب‌ترین همسایه ای که به یک هدف منجر می‌شود، ارائه می‌دهد. برای شروع مرحله کشف مسیر، گره ورودی مسیر خود را به سمت ایستگاه مرکزی در یک جدول محلی بررسی می‌کند. اگر مسیری را پیدا کرد که استانداردهای تعداد گام به ایستگاه مرکزی h_{BS} را داشت، مجموع انرژی (e_i) و درجه کیفیت لینک (dl_i) را محاسبه می‌کند، گره مبدا آن را به عنوان مرحله بعدی انتخاب می کند و بسته‌های داده را مستقیماً به آن ارسال می‌کند.

با این حال ، ممکن است یک مسیر معتبر با توجه به نیازهای مسیریابی در جدول محلی گره منبع وجود نداشته باشد. در چنین شرایطی ، از همه همسایگان خواسته می‌شود که در فرایند انتخاب گام بعدی شرکت کنند.

درجه یکپارچگی لینک از تابع رمزنگاری هش استفاده می‌کند تا اطمینان حاصل شود که بیت‌های داده‌ی منتقل شده به دلیل آسیب دیدن لینک‌ها تغییر کرده‌اند یا خیر. پس گره i یک بسته کاوشگر از k بیت تولید می‌کند و باید آن را به گره j ارسال کند. ابتدا گره i ، بسته کاوشگر P_1 را به تابع هش منتقل می‌کند تا کد پیام آن M (c) مشخص شود. سپس، کد پیام بدست آمده با بسته کاوشگر واقعی به عنوان $P_1 + M(c)$ ادغام شده و به گره j ارسال می شود. با دریافت بسته P_1 به‌همراه کد پیام M (c) ، گره j کد پیام بسته دریافتی P_1 را مجدداً محاسبه می‌کند. اگر کد پیام محاسبه شده همان کد پیام دریافتی باشد ، j یکپارچگی پیام کاوش دریافتی را اعلام می‌کند. علاوه بر این ، بر اساس مقدار هش محاسبه شده در یک گره j ؛ پروتکل پیشنهادی آستانه لینک مشخص شده را کم یا زیاد می‌کند.

مقدار آستانه پایین با ۰ و مقدار آستانه بالا ۱ نشان داده می‌شود. آستانه بالا نشان می‌دهد که لینک مشخص شده قابل اطمینان تر است و ممکن است به کمترین میزان خطا عمل کند. همچنین، مجموع انرژی باقیمانده e_i در دو مرحله محاسبه می‌شود. ابتدا ، هر گره به طور مداوم سطح باقیمانده e_1 را زیر نظر دارد و میزان انرژی باقی مانده در اطراف منطقه e_{loc} خود را با توجه به ne، $\sum_{n=0}^{N} me_n - ce_n$همسایه ، me_n حداکثر انرژی و ce_n انرژی مصرفی همسایه است.

بر این اساس ، گره با انرژی باقیمانده بیشتر اولویت بالاتری دارد. در پایان ، گره به جدول محلی خود نگاه می‌کند و مقدار شمارنده را که تعداد گام به سمت BS را نشان می‌دهد ، بررسی می‌کند. هرچه مقدار کمتری را مشخص کند، گره به BS نزدیکتر است و برای انتقال داده نیاز به کمترین هزینه ارتباطی دارد. سرانجام، تمام مقادیر محاسبه شده انرژی باقیمانده، تعداد گام و یکپارچگی پیوندها در یک جنبه وزنی خلاصه می‌شود تا تابع ابتکاری $h(f)$ همانند فرمول (۱) تعیین شود.

$$h(f) = \alpha * (e_i + e_{loc}) + \beta * {}^{1}/_{h_{BS}} + \gamma * dl_i \qquad (۱)$$

در فرمول (۱) ، β ،α، γ ضرایب وزنی هستند و تأثیر قابل توجهی بر تابع اکتشافی دارند. پس از محاسبه $h(f)$، هر گره اطلاعات همسایه‌ی خود را با گره مبدا برای پیش‌بینی تصمیم بهینه برای رسیدن به سمت BS به اشتراک می گذارد.

گره همسایه با بالاترین $h(f)$ نشان دهنده رتبه قوی‌تری برای انتخاب مرحله بعدی است. بر این اساس ، گره مبدا بسته RREQ [۳] را به همسایه انتخاب شده به عنوان مرحله بعدی برای ارسال داده انتقال می‌دهد.

پس از آن، پروتکل پیشنهادی از الگوریتم اکتشافی پرتو، که یک جستجوی آگاهانه است، و روش رمزنگاری منحنی بیضوی دیفی هلمن استفاده می‌کند که جزئیات آنها در بخش‌های بعدی بیان شده است.

۳-۲- مسیریابی مطمئن داده‌ها با استفاده از الگوریتم اکتشافی

پروتکل پیشنهادی از الگوریتم پرتو [۱۸, ۱۹]، که یک روش مبتنی بر جستجوی آگاهانه است ، استفاده می‌کند و گراف متصل شده را در یک مجموعه جزئی ، کاوش می‌کند. پروتکل پیشنهادی جداول گره‌ها را بهینه می

کند ، به این معنا که استفاده از حافظه را برای ذخیره گره‌های غیر منتخب در هر مرحله در تعیین مرحله بعدی محدود می‌کند.

در این کار، الگوریتم اکتشافی پرتو استراتژی را برای انتخاب گره مطلوب به عنوان مرحله بعدی بر اساس بیشترین وزن از بین همه کاندیداهای ممکن، بهینه می‌کند. چنین مکانیزمی احتمالاً محاسبه و پیچیدگی زمانی گره-های حسگر را کاهش می‌دهد. پروتکل پیشنهادی یک عدد w از پیش تعیین شده را ذخیره می‌کند که عرض پرتو نامیده می شود و حالات مطلوب در هر سطح را نشان می دهد. عملکرد الگوریتم بستگی به مقدار عرض تیر دارد ، با حفظ حداقل مقدار آن پیچیدگی فضا و زمان گره‌های حسگر را بهبود می بخشد.

از آنجا که گره‌های حسگر محدودیت دارند ، بنابراین ، بر اساس عرض پرتو ، فقط گره‌های w با اعمال تابع اکتشافی $h(f)$ و نادیده گرفتن سایر گره‌ها در گراف گسترش می‌یابند. بر این اساس ، این روند تا زمانی ادامه می-یابد که یک مسیر بهینه با بالاترین مقدار $h(f)$ کاوش نشود ، در حالی که مصرف انرژی و هزینه ارتباطات در سنسور کاهش می یابد.

$h(f_0),h(f_1),...,h(f_n)$ بالاترین مقادیر وزنی با استفاده از الگوریتم اکتشافی پرتو هستند، سپس مجموع وزنی آنها $W(f_n)$ را می‌توان طبق فرمول (۲) نشان داد.

$$W(f_n) = h(f_0) + h(f_1) + ... + h(f_n) \qquad (۲)$$

بنابراین به‌طور کلی طبق شبه کد الگوریتم (۱) می‌توان گفت: الگوریتم پرتو برای صرفه‌جویی در مصرف حافظه یک تابع h برای تخمین هزینه‌ی رسیدن به راس موردنظر (گره مقصد) از راس داده شده (گره مبدا) در نظر می‌گیرد. همچنین از پارامتر عرض بیم استفاده می‌کند که نشان‌دهنده‌ی تعداد راس‌هایی است که در هر مرحله از الگوریتم جستجوی اول سطح ذخیره شده‌است؛ بنابراین الگوریتم پرتو فقط راس‌های با بهترین مقدار در هر مرحله از جستجو را ذخیره می‌کند و از اتلاف حافظه قبل از رسیدن به هدف جلوگیری می‌کند.

۳-۳-مسیریابی امن با استفاده از الگوریتم رمزنگاری منحنی بیضوی

پروتکل رمزنگاری ECDH یا رمزنگاری منحنی بیضوی دیفی هلمن، رمزنگاری به روش کلید عمومی است که بر اساس ساختاری جبری از منحنی‌های بیضوی بر روی میدان‌های متناهی طراحی شده‌است.

این رمزنگاری در مقایسه با بقیه رمزنگاری‌های مبتنی بر میدان‌های گالوا برای ایجاد امنیت یکسان، به کلید کوچکتری نیاز دارد. این روش معمولاً هنگام اتصال به سایت‌هایی نظیر مایکروسافت لایو، گوگل و فیس‌بوک استفاده می‌شود. این روش به دلایل احراز هویت سریع و آسان، تبادل کلید سریع و اندازه کلید کوچک بهینه گزینه مناسبی برای این نوع شبکه می باشد[۲۰] [۲۱]. علاوه بر ویژگی های ذکر شده، روش رمزنگاری ECDH دارای استقرار کلیدی قوی و سطح ایمنی بالا می باشد و طبق بررسی و

الگوریتم(۱): شبه کد الگوریتم جستجوی پرتو

Start with *k* randomly generated states
Loop:
All the successors of all k states are generated
if anyone is a goal state **then** stop
else select the k best successors from the complete list of successors and repeat.

مقایسات با سایر الگوریتم های رمزنگاری، این روش از کارایی و ایمنی نسبتا بالاتری نسبت به سایر روش‌ها دارا می باشد.در واقع این روش یک روش ریاضی کلید عمومی می‌باشد که بر روی دشواری حل لگاریتم گسسته استوار است. به منظور فراهم کردن نیازهای رمزنگاری امروز، منحنی بیضی یک صفحه منحنی است تا اینکه بر روی یک میدان محدود باشد که شامل نقطه هایی است که فرمول (۳) را برآورده می‌کند:

$$y^2 = x^3 + ax + b \qquad (۳)$$

همراه یک نقطه مشخص در بینهایت ∞. رابطه‌ی (۱)، نشان دهنده‌ی رابطه‌ی اصلی برای تشکیل یک منحنی بیضوی است. در این رابطه x و y مختصات در صفحه‌ی دوبعدی هستند. علاوه بر آنها، a و b ضرایب متغیر و pپیمانه مورد استفاده می‌باشد. بدین صورت که تمامی اعداد باید در بازه‌ی $(-p,p)$قرار بگیرند و تمامی نقاط بر روی نمودار قرار بگیرند و شروط فرمول (۴) تضمین می‌کند که هیچ نقطه‌ی عطفی وجود نداشته باشد.

$$a,b \in F_p \ , \ 4ax^3 + 27\,b^2 \neq 0 \qquad (۴)$$

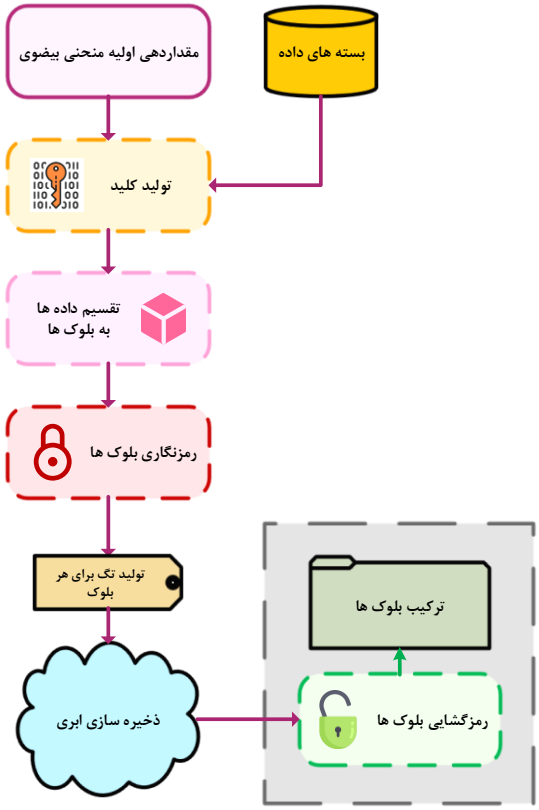
رمزنگاری ECDH به دلیل اینکه اندازه‌ی کلید آن کوتاه است و تبادل کلید سریعی دارد و مقدار بافر کمتری را برای هر بسته لازم دارد. به‌طور کلی هر بسته هم در مقصد و هم در مبدا داخل یک بافر قرار می‌گیرد و اگر این بافر پر شود، بسته‌های بعدی از دست می‌روند یا به اصطلاح Drop می‌شوند. بنابراین هر الگوریتمی که سریع‌تر عمل کند، قطعا از آن صف زودتر خارج می‌شود و برای شبکه بهتر خواهد بود. روند رمزنگاری استفاده شده به روش ECDH در شکل (۲) نمایش داده شده است.

به‌طور کلی در این روش رمزنگاری هنگامیکه A می‌خواهد یک کلید مشترک با B از طریق یک کانال ناامن ارائه دهد، ابتدا پارامترهای محدوده‌ی رمزنگاری منحنی بیضوی یعنی ECC(p,k,G,n) مورد توافق قرار می‌گیرند.

همچنین ، هر طرف باید دارای یک جفت کلید متناسب با اجرای رمزنگاری منحنی بیضوی باشد که شامل یک کلید خصوصی d و یک کلید عمومی به عنوان نقطه منحنی بیضوی Q است.

- تولید کلید خصوصی d: کلید خصوصی d یک عدد صحیح تصادفی در بازه صفر و یک است.
- تولید کلید عمومی Q: کلید عمومی توسط فرمول (۵) تولید می-شود:

$$Q=Dg \qquad (۵)$$



شکل (۲): روند رمزنگاری منحنی بیضوی دیفی هلمن (ECDH)

هر دو طرف باید قبل از اجرای پروتکل، کلید عمومی یکدیگر را بدانند. A رمز مشترک را به شرح فرمول (۶) محاسبه می‌کند:

$$S=d_A Q_B \qquad (۶)$$

B رمز مشترک را به صورت فرمول (۷) محاسبه می‌کند:

$$S=d_B Q_A \qquad (۷)$$

رمز مشترک محاسبه شده توسط هر دو طرف طبق فرمول (۸) برابر است با:

$$d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A \qquad (۸)$$

هیچ طرف دیگری بجز A و B نمی‌تواند راز مشترک را محاسبه کند. بنابراین کلید خصوصی ایمن نگه داشته می‌شود و فقط در گیرنده‌ی نهایی که ایستگاه مرکزی هست محاسبه می‌شود. همچنین، بدون اطلاع از هر دو کلید خصوصی ، پیام را نمی‌توان رمزگشایی کرد. شبکه کد مراحل رمزنگاری ECDH در الگوریتم (۲) نشان داده شده است.

۳-٤-نگهداری مسیر

برای دستیابی به مرحله‌ی نگهداری مسیر، اگر گره‌های انتخابی در گام بعدی سطح انرژی خود را به آستانه انرژی مشخص شده کاهش دهند، مسیرهای

الگوریتم (۲): شبکه کد پروتکل رمزنگاری ECDH

Input:

Elliptic curve domain parameters (p, k, G, n), Cipher Text (C_1,C_2) and Public Key Q_A

Output:

Computed private key and encrypted Message M
Compute Shared Secret ($S = d_B Q_A$)
Compute Private Key (d_A= S /Q_B)
Decrypt Cipher text using Private Key d_A (C_1,C_2) -> M)

جایگزین مشخص می‌شوند. چنین مکانیزمی احتمال شکست مسیر و انتقال مجدد داده‌ها را کاهش می‌دهد.

هرگاه گره کم مصرف انرژی در مرحله مسیریابی شناسایی شود، از انتقال داده خارج می‌شود و مسیریاب پیام خطا را به گره مبدا ارسال می‌کند. گره مبدا تابع اکتشافی را برای تعیین گره با بیشترین وزن اجرا می‌کند و بر این اساس ، گام بعدی برای مسیر یابی مجدد داده‌ها انتخاب می‌شود. آستانه انرژی در نگهداری مسیر به طور قابل توجهی نقص مسیر و تأخیر شبکه را کاهش می‌دهد.

علاوه بر این، گره‌های گام‌های بعدی که در همسایگی ایستگاه مرکزی واقع شده‌اند باید بسته‌های داده بیشتری منتقل کنند. چنین گره‌هایی بیش از حد بارگیری می‌شوند و منجر به مصرف بالای منابع انرژی در مسیریابی داده-ها می‌شوند، که منجر به افزایش نسبت از دست دادن بسته و قطع اتصال شبکه می‌شود. بنابراین ، پروتکل پیشنهادی نسبت ترافیک T_r بین BS و گره‌های گام بعدی را ارزیابی می‌کند: b_d پهنای باند لینک بین گره گام بعدی یعنی از i به BS است ، P_t تعداد بسته‌های منتقل شده در لینک i به BS را نشان می‌دهد و B_t حداکثر پهنای باند است، بنابراین نسبت ترافیک T_r مطابق فرمول (۹) محاسبه می‌شود.

$$B_t \;/)\; b_d - P_t = (T_{r(i\,.\,BS)} \qquad (۹)$$

اگر نسبت ترافیک بین گام بعدی i و BS از حد آستانه فراتر رود، از ارسال داده خارج می‌شود و یک بسته تایید ACK را برای انتخاب یک فرستنده مناسب به گام بعدی منتقل می‌کند. در نتیجه ، گره مبدا بسته ۳RREQ را به همسایگان ارسال می‌کند تا وزن آنها محاسبه شود و بر این اساس ، گام بعدی بر اساس تابع اکتشافی h (f) انتخاب می‌شود. این مکانیزم حفاظت و ثبات مسیر را به مدت قابل توجهی افزایش می‌دهد.

٤- ارزیابی کارایی

جهت پیاده‌سازی و ارزیابی پروتکل پیشنهادی و مقایسه عملکرد آن از نرم‌افزار شبیه‌ساز NS-2 ورژن ۳۵ استفاده شد. عملکرد الگوریتم پیشنهادی بر اساس پارامترهای ارائه شده در ادامه مورد ارزیابی قرار گرفته است.

٤-۱-پارامترهای سناریوهای شبیه‌سازی

جدول (۲) پارامترهای کاربردی و نحوه مقداردهی آن‌ها را ارائه می‌دهد. پارامترهای شبیه‌سازی و نحوه‌ی تنظیمات آن‌ها از عامل‌های اساسی بوده که

جدول (۲):پارامترها و تنظیمات آن‌ها جهت پیکربندی سناریوهای شبیه‌سازی

پارامتر	مقادیر
ابعاد شبیه‌سازی	۱۰۰ متر *۱۰۰ متر
نودهای حسگر	۵۰-۲۵۰
نرخ تولید داده	۵-۲۵ ثانیه
نودهای مخرب	۱۰-۱۵
اندازه بسته (k)	۳۲ بیتی
سطح انرژی	۲ ژول (J)
تعداد ایستگاه مرکزی (چاهک)	۱
موقعیت ایستگاه مرکزی	(۱۵۰و۱۰۰)
پیام کنترلی	۲۰ بیتی
رنج انتقال	۲۰m
نوع ترافیک	CBR (نرخ بیت ثابت)
نوع صف	DropTail(FiFo)
زمان شبیه سازی	۱۰۰ ثانیه

به واسطه‌ی آن‌ها شبکه و جزئیات وابسته به آن قابلیت تنظیم و پیکربندی دارد. بر همین اساس و در راستای مقداردهی صحیح پارامترهای مدل‌سازی شده، سعی شده تا ویژگی‌ها، ضرورت‌ها و ماهیت شبکه اینترنت اشیا در مقداردهی پارامترهای کاربردی حفظ، و متناسب با ماهیت واقعی شبکه تنظیمات انجام شود. افزون بر این در تعریف و تنظیم پارامترها از مقالات و تحقیقات معتبر گذشته الگو گرفته شده تا راهنمایی مؤثر برای تنظیمات صحیح‌تر سناریوهای شبیه‌سازی باشند. قابل توجه است که مدل‌سازی و تعریف پارامترهای شبیه‌سازی و پیاده‌سازی سناریوهای مورد نظر، برای هر دو مکانیزم تحت آزمایش یکسان در نظر گرفته شده تا ارزیابی‌ها در یک شرایط یکسان انجام شود.

٤-۲-ارزیابی نتایج شبیه‌سازی

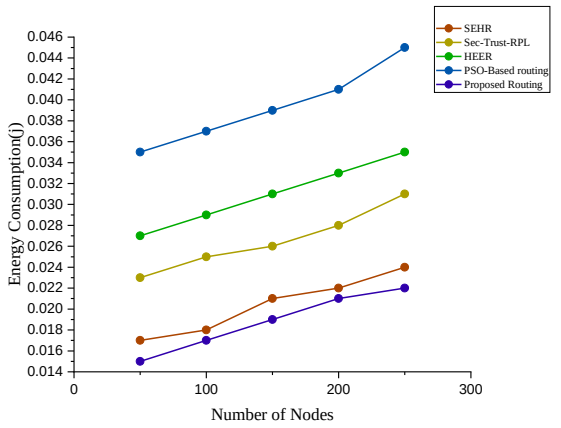
جهت ارزیابی و تحلیل عملکرد مکانیزم‌ها در آزمایشات مورد نظر از میزان انرژی مصرفی، توان عملیاتی، و تعداد بسته‌های از دست رفته استفاده شده است. نتایج این معیارها با روش های SEHR [۱۸]، PSO [۱۶]، SecTrust-RPL [۱۴] و روش مسیریابی مبتنی بر هیورستیک (HEER) [۱۵] مورد مقایسه قرار گرفته است. این معیارها، معیارهای ارزش‌سنجی عملکرد پروتکل پیشنهادی در قیاس با مکانیزم‌های تحت مقایسه می‌باشند.

٤-۲-۱-میزان مصرف انرژی

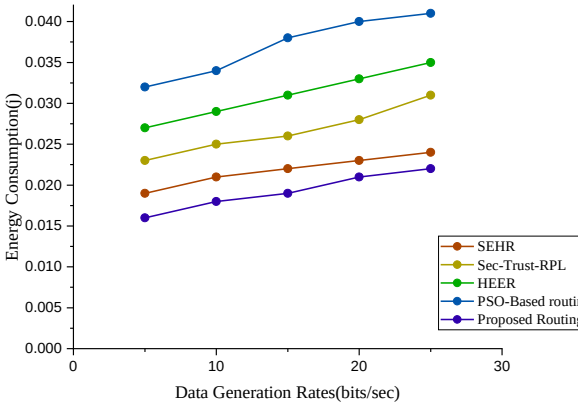
پروتکل پیشنهادی بر مبنای تحلیل انرژی و بهینه‌سازی تبادلات تا حد امکان سعی بر استفاده از گره‌هایی با کارایی بالاتر و مسیرهای میانی بهینه‌تر را دارد. این عملکرد منجر بهینه‌سازی مؤثر انرژی در روش پیشنهادی گردیده است. نمودارهای ارائه شده در شکل (۳) و (۴) نتایج مرتبط با انرژی مصرفی در پروتکل پیشنهادی در مقایسه با روش‌های دیگر را ارائه و نمایش می‌دهند.

٤-۲-۲-تعداد بسته‌های از دست رفته

شکل (۵) و شکل (۶) رفتار پروتکل پیشنهادی را از نظر تعداد متفاوت گره‌ها و نرخ تولید داده برای تعداد بسته‌های از دست رفته نشان می‌دهد. نتایج نشان



شکل(۳): نتایج شبیه‌سازی مصرف انرژی شبکه و تعداد نودها در پروتکل پیشنهادی



شکل (٤): نتایج شبیه‌سازی مصرف انرژی شبکه و نرخ تولید داده در پروتکل پیشنهادی در مقایسه با روش‌های دیگر

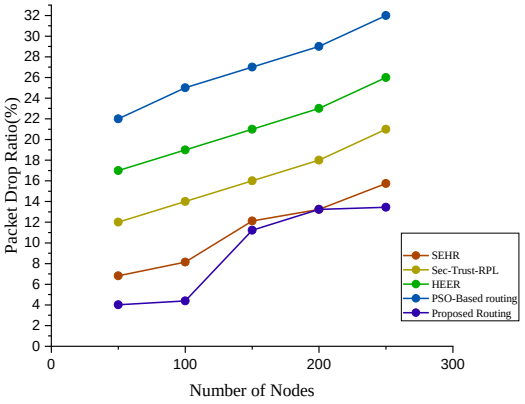
می دهد که پروتکل پیشنهادی نسبت افت بسته‌ها را به طور متوسط در هر دو سناریوی شبکه کاهش می‌دهد.

بر خلاف سایر راه حل ها ، پروتکل پیشنهادی با استفاده از الگوریتم ابتکاری پرتو ، تابع وزنی بر اساس انرژی باقی مانده، شمارش پرش به ایستگاه مرکزی و عوامل یکپارچگی طراحی شده است. چنین استراتژی انتخاب بیشتر گره های کارآمد و قابل اعتماد برای مسیریابی داده ها را ارائه می‌دهد. علاوه بر این، ترکیب رمزگذاری داده‌های مبتنی بر رمزنگاری منحنی بیضوی با عملکرد ساده و تصادفی آن نیز سطح اطمینان شبکه را افزایش می دهد و از دست رفتن بسته‌ها دشوار است.

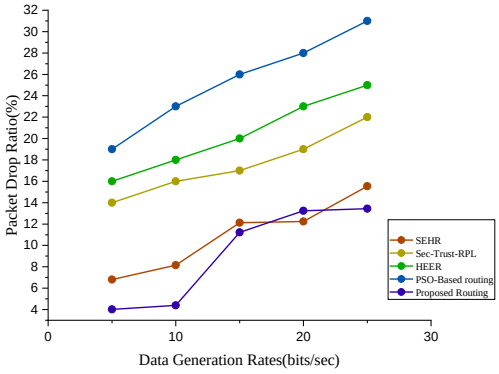
٤-۲-۳-توان عملیاتی

شکل (۷) و (۸) توان عملیاتی شبکه را بر حسب تعداد گره‌های مختلف و نرخ تولید داده متفاوت نشان می‌دهد. نتایج نشان داد که پروتکل پیشنهادی به طور متوسط توان شبکه را در مقایسه با کارهای موجود بهبود می‌بخشد.

این به دلیل مسیریابی قوی است که در طراحی پروتکل پیشنهادی با کمترین هزینه سربار در گره‌های حسگر دخیل است. علاوه بر این ، استفاده از حالت رمزنگاری برای امنیت داده‌ها ، پروتکل پیشنهادی شانس ایجاد گره‌های مخرب را برای کاهش عملکرد تحویل داده بین گره‌های حسگر و ایستگاه مرکزی کاهش می‌دهد.



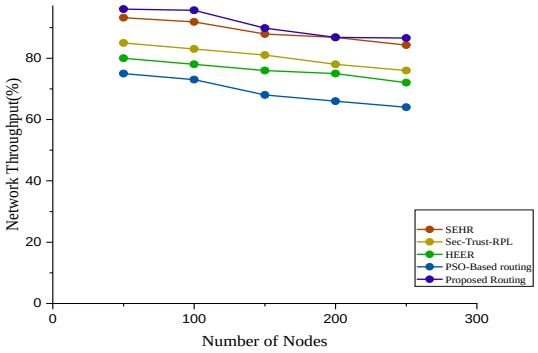
شکل (۵): نتایج شبیه‌سازی تعداد بسته‌های از دست رفته و تعداد نودها در پروتکل پیشنهادی در مقایسه با سایر روش‌ها



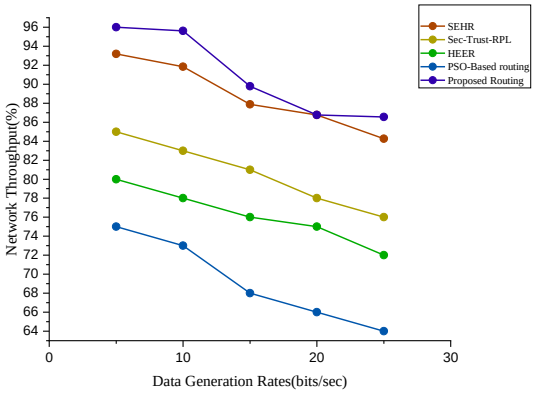
شکل (٦): نتایج شبیه‌سازی تعداد بسته‌های از دست رفته و نرخ تولید داده در پروتکل پیشنهادی در مقایسه با سایر روش‌ها

۵-نتیجه‌گیری

افزایش طول عمر شبکه و ذخیره‌ی انرژی در شبکه‌های اینترنت اشیا، نقش حیاتی را در بهبود بازدهی و افزایش کارایی شبکه ایفا می‌نماید. در این مقاله به بررسی یکی از مباحث مهم و حیاتی شبکه‌های اینترنت اشیا، تحت عنوان افزایش طول عمر شبکه و بحث امنیت مسیریابی پرداخته شد و مکانیزمی برای بهبود این معیارها معرفی گردید. این مقاله یک پروتکل مسیریابی امن و آگاه از انرژی با استفاده از الگوریتم اکتشافی پرتو و رمزنگاری منحنی بیضوی برای شبکه‌های اینترنت اشیا ارائه داد که هدف آن بهینه‌سازی استراتژی مسیریابی با تصمیم‌گیری هوشمند در برابر گره‌های مخرب است. این پروتکل عملکرد اکتشافی مبتنی بر هوش مصنوعی را ارائه کرد که از انرژی باقیمانده، تعداد گام تا ایستگاه مرکزی و عوامل یکپارچگی برای بهبود عملکرد شبکه از نظر مسیریابی داده‌ها و انتقال قابل اعتماد و امن استفاده می‌کند. پروتکل پیشنهادی امنیت داده‌ها را بر اساس الگوریتم رمزنگاری منحنی بیضوی دیفی هلمن فراهم می‌کند که دارای طول و تبادل کلید کوتاه‌تر و سریع‌تر می‌باشد. نتایج شبیه سازی پروتکل پیشنهادی نشان داد بهبود معیارهای مهم شبکه-های اینترنت اشیا از قبیل میزان انرژی مصرفی، نرخ تعداد بسته‌های از دست رفته، توان عملیاتی از توانمندی‌های روش پیشنهادی است و این روش عملکرد خوبی را در این زمینه ها از خود به نمایش گذاشته است. در آینده،



شکل (۷): نتایج شبیه‌سازی توان شبکه و تعداد گره‌ها در پروتکل پیشنهادی در مقایسه با سایر روش‌ها



شکل (۸): نتایج شبیه‌سازی توان شبکه و نرخ تولید داده در پروتکل پیشنهادی در مقایسه با سایر روش‌ها

هدف ما بهبود پروتکل ارائه شده با استفاده از تکنیک‌های سبک مبتنی بر یادگیری ماشین و یادگیری عمیق است تا شبکه را با قابلیت تحمل خطا هوشمندتر کنیم. همچنین، کارایی انرژی و عملکرد مسیریابی امن را با استفاده از سایر الگوریتم‌های رمزنگاری و مدل‌های مختلف بررسی می‌کنیم.

منابع

[1] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review," Ad Hoc Networks, vol. 101, p. 102096, 2020/0 4/15/ 2020, doi: https://doi.org /10.1016/ j.adhoc. 2020.102096.

[2] J. Marietta and B. C. Mohan, "A Review on Routing in Internet of Things," Wireless Personal Communications, vol. 111, no. 1, pp. 209-233, Mar 2020, doi: 10.1007 /s11277-019-06853-6.

[3] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," Computers & Industrial Engineering, vol. 155, p. 107174, 2021/05/01/ 2021, doi: https://doi.org/10 .1016/j.cie.2021.107174.

[4]]B. K. Pattanayak, D. Nohur, S. K. Cowlessur, and R. K. Mohanty, "An IoT-Based System Architecture for Environmental Monitoring," in Progress in Advanced Computing and Intelligent Engineering, Singapore, C. R.

13, no. 6, pp. 1853-1871, 2020/11/01 2020, doi: 10.1 007/s12083-020-00939-w.

[16] D. R. Edla, M. C. Kongara, and R. Cheruku, "A PSO Based Routing with Novel Fitness Function for Improving Lifetime of WSNs," Wireless Personal Communications, vol. 104, no. 1, pp. 73-89, 2019/01/01 2019, doi: 10.1007 /s11277-018-6009-6.

[17] J. Lee and C. Teng, "An Enhanced Hierarchical Clustering Approach for Mobile Sensor Networks Using Fuzzy Inference Systems," IEEE Internet of Things Journal, vol. 4, no. 4, pp. 1095-1103, 2017, doi: 10.1109 /J IOT .2017.2711248.

[18] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network," IEEE Access, vol. 8, pp. 163962-163974, 2020, doi: 10.1109/ ACCESS .2020.3022285.

[19] Y. Zuo, Y. Wu, G. Min, and L. Cui, "Learning-based network path planning for traffic e ngine ering," Future Generation Computer Systems, vol. 92, pp. 59-67, 2019/03/01/ 2 019

[20] M. Safieh, "Elliptic Curve Cryptography," in Algorithms and Architectures for Cryptography and Source Coding in Non-Volatile Flash Memories, M. Safieh Ed. Wiesbaden: Springer Fachmedien Wiesbaden, 2021, pp. 5-23.

[21] E. K. Subramanian and L. Tamilselvan, "Elliptic curve Diffie–Hellman cryptosystem in big data cloud security," Cluster Computing, vol. 23, no. 4, pp. 3057-3067, 2020/12/01 2020, doi: 10.1007/s10586-020-03069-3.

زیرنویس‌ها

1 Secure Energy-aware heuristic-based routing
2 Elliptic-curve Diffie–Hellman
3 Frequent Route REQuest

Panigrahi, B. Pati, B. K. Pattanayak, S. Amic, and K.-C. Li, Eds., 2021// 2021: Springer Singapore, pp. 507-514 .

[5] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes," Computer Communications, vol. 160, pp. 475-493, 2020/07/01/ 2020, doi: https://doi.org/10.1016/j.comcom.2020.06.030.

[6] S. Sankar, S. Ramasubbareddy, A. K. Luhach, A. Nayyar, and B. Qureshi, "CT-RPL: Cluster Tree Based Routing Protocol to Maximize the Lifetime of Internet of Things," Sensors, vol. 20, no. 20, Oct 2020, Art no. 5858, doi: 10 .3390/s20205858.

[7] K. Jaiswal and V. Anand, "EOMR: An Energy-Efficient Optimal Multi-path Routing Protocol to Improve QoS in Wireless Sensor Network for IoT Applications," Wireless Personal Com mun ications, vol. 111, no. 4, pp. 2493-2515, 2020/04/01 2020, doi: 10.1007/s 11277-019-07000-x.

[8] M. Mir, M. Yaghoobi, and M. Khairabadi, "A new approach to energy-aware routing in the Internet of Things using improved Grasshopper Metaheuristic Algorithm with Chaos theory and Fuzzy Logic," Multimedia Tools and Applications, 2022/01/08 2022, doi: 10. 1007/s11042-021-11841-9.

[9] M. Bouaziz, A. Rachedi, A. Belghith, M. Berbineau, and S. Al-Ahmadi, "EMA-RPL: Energy and mobility aware routing for the Internet of Mobile Things," Future Generation Computer Systems, vol. 97, pp. 247-258, 2019/08/01/ 2019,

[10] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," Journal of Information Security and Applications, vol. 52, p. 102467, 2020/06/01/ 2020, doi: https: //doi.org/ 10. 1016/j.jisa.2020.102467.

[11] K. V. Praveen and P. M. J. Prathap, "Energy Efficient Congestion Aware Resource Allocation and Routing Protocol for IoT Network using Hybrid Optimization Techniques," Wireless Personal Communications, vol. 117, no. 2, pp. 1187-1207, 2021/03/01 2021, doi: 10.1007 /s11277-020-07917-8.

[12] K. Vijayalakshmi and P. Anandan, "A multi objective Tabu particle swarm optimization for effective cluster head selection in WSN," Cluster Computing, vol. 22, no. 5, pp. 12275-12282, 2019/09/01 2019, doi: 10.1007/s10586-017-1608-7.

[13] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in WSN-based intelligent transportation systems," Computer Networks, vol. 146, pp. 151-158, 2018/12/09/ 2018, doi: https:// doi.org/ 10.1016/j.comnet.2018.09.015.

[14] H. B. Salameh, R. Derbas, M. Aloqaily, and A. Boukerche, "Secure Routing in Multi-hop IoT-based Cognitive Radio Networks under Jamming Attacks," presented at the Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Miami Beach, FL, USA, 2019.

[15] G. S. Binu and B. Shajimohan, "A novel heuristic based energy efficient routing strategy in wireless sensor network," Peer-to-Peer Networking and Applications, vol.