JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH

E-ISSN: 2980-9231
https://sanad.iau.ir/journal/jce

https://doi.org/10.30495/jce.2025.1993480.1336

Vol. 14/ No. 56/2025

Research Article

Presenting an Attack-Resistant Communication Model for Secure Routing in Underwater Sensor Networks

Tayebeh Nourali Ahari [1] | Mehdi Sadeghzadeh [2]

[1]Department of Information Technology Management, SR.C., Islamic Azad University, Tehran, Iran.
tayebeh.ahari@srbiau.ac.ir

[2]Department of Computer Engineering, SR.C., Islamic Azad University, Tehran, Iran
mehdi.sadeghzadeh@iau.ac.ir

Correspondence
Mehdi Sadeghzadeh, Associate Professor of Computer Engineering, SR.C., Islamic Azad University, Tehran, Iran.
mehdi.sadeghzadeh@iau.ac.ir

Main Subjects:
Secure Routing in Underwater Sensor Networks
Paper History:
Received: 14 April 2024
Revised: 17 August 2024
Accepted: 18 August 2024

Abstract

Underwater communication networks face numerous challenges, including routing, signal interference, energy consumption, and security threats. Although routing protocols are optimized for resilience against common disturbances in underwater environments, they are not specifically designed to counter attacks or malicious neighbor nodes. Key security threat factors in underwater sensor networks include limited power sources, constrained communication media, and harsh underwater conditions. Therefore, this research aims to develop a secure communication model resistant to routing attacks in underwater sensor networks. Two communication link models were considered: Scenario 1 uses a basic distance-based model, while Scenario 2 employs a probabilistic channel gain model between node pairs. Simulation results encompass four stages: 1) secure neighbor discovery under wormhole attacks; 2) initial route discovery and selection of reliable nodes for data forwarding to the sink; 3) attack detection during data distribution based on node status information for identifying Sybil attacks; 4) alternative secure path discovery for detecting malicious nodes. The proposed scheme demonstrated higher success rates compared to the basic approach and lower mobility energy costs, achieving comparable success performance.

Keywords: Underwater Internet of Things, Safe Neighbor Discovery, Underwater Routing, Wormhole Attack.

Highlights

- Limitation of processing and communication capabilities in underwater Internet of Things.
- Simulation of guide signal transmission and neighbor table formation in two communication models.
- The proposed method demonstrated the highest network throughput compared to the basic method.

Citation: T. Nourali Ahari, and M. Sadeghzadeh, "Presenting an Attack-Resistant Communication Model for Secure Routing in Underwater Sensor Networks," *Journal of Southern Communication Engineering*, vol. 14, no. 56, pp. 58–74, 2025, doi:10.30495/jce.2025.1993480.1336 [in Persian].

1. Introduction

The introduction discusses the importance of neighbor discovery in underwater IoT networks and the risks posed if malicious nodes infiltrate the process. It proposes using physical layer authentication with trusted and sink nodes to ensure data security. This method leverages the unique characteristics of underwater acoustic channels for authentication. The approach is validated through simulations and marine experiments.

The paper also addresses privacy challenges in IoT networks, emphasizing the need for robust solutions. The article is structured as follows: Section 2 covers network modeling, Section 3 reviews the simulation steps, and Section 4 presents the results, with a concluding discussion in the final section.

2. Innovation and Contributions

This paper addresses key challenges in underwater IoT networks through a novel physical layer authentication method. Key innovations include:

- **Distributed authentication** using trusted nodes and sink nodes to enhance security.
- **Channel-based verification** leveraging spatial and temporal characteristics of underwater acoustic channels for reliable message authentication.
- **Comprehensive simulation** of the method in an underwater IoT voice communication network to assess wormhole attack impacts.
- **Experimental validation** through extensive numerical simulations and real-world marine tests.
- **Robust privacy solutions** for protecting location, device, and data privacy in distributed IoT environments.

These advancements strengthen data confidentiality, integrity, and availability in underwater IoT networks, enabling secure communication in challenging underwater conditions.

3. Materials and Methods

NS-2 is utilized for software simulation, capitalizing on its comprehensive library of network protocols. The simulation comprises four key stages:

1. Secure neighbor discovery under wormhole attack conditions
2. Initial path discovery to enhance packet delivery reliability
3. Attack detection during data distribution
4. Identification of alternative safe paths to detect malicious nodes

The neighbor discovery process involves broadcasting digitally signed request messages containing unique node identifiers.

4. Results and Discussion

The simulation results were obtained by averaging 40 runs for each output. Key findings include:

- **Packet Delivery Rate**: The proposed method maintains a high success ratio (above 93%) for networks of up to 400 nodes, outperforming the baseline method in both success rate and mobility energy cost.
- **Network Throughput**: Consistently higher throughput is achieved across all simulations, demonstrating superior performance to baseline methods even with increased hop counts.
- **End-to-End Delay**: While average delay generally decreases with additional nodes, a slight increase is observed at very high node densities. Overall, delays remain lower than in previous studies.
- **Energy Consumption**: The method exhibits improved energy efficiency, particularly in high-density networks, attributable to optimized path selection for data transmission.

These results demonstrate the effectiveness of the proposed approach in delivering reliable, efficient, and secure performance for underwater IoT networks.

5. Conclusion

This paper presents a simulation study of neighbor and path discovery mechanisms in underwater acoustic communication networks, specifically designed for IoT applications with constrained processing and communication capabilities. The investigation examines beacon signal transmission and neighbor table formation using two distinct communication models while evaluating the performance degradation caused by malicious nodes.

Key findings indicate that the presence of malicious nodes has a significant impact on network operations. Comparative analysis with prior studies reveals superior performance across multiple metrics:

- Throughput efficiency
- Reduced end-to-end delay
- Enhanced packet delivery rate (achieving 94%)
- Optimized energy consumption

The proposed method shows consistent improvement over existing approaches in all measured performance indicators, establishing its effectiveness for resource-constrained underwater IoT deployments.

6. Acknowledgement
There was no financial support for this article. But we are grateful for the valuable contributions made by the reviewers in shaping this paper into its final form.

Declaration of Competing Interest: The Authors do not have a conflict of interest. The authors approve the content of the paper.

Author Contributions:
Mehdi Sadeghzadeh: verified the analytical methods; **Tayebeh Nourali Ahari**: made the simulations and wrote the manuscript.

E-ISSN: 2980-9231
https://sanad.iau.ir/journal/jce

مهندسی مخابرات جنوب
دانشگاه آزاد اسلامی واحد بوشهر

https://doi.org/10.30495/jce.2025.1993480.1336

مقاله پژوهشی

ارائه یک مدل ارتباطی مقاوم در برابر حملات به‌منظور مسیریابی امن در شبکه‌های حسگر زیر آب

طیبه نورعلی آهاری[۱] | مهدی صادق زاده*[۲]

[۱] گروه مدیریت فناوری اطلاعات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
tayebeh.ahari@srbiau.ac.ir

[۲] گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
mehdi.sadeghzadeh@iau.ac.ir

نویسنده مسئول
*مهدی صادق زاده، دانشیار گروه علمی مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
mehdi.sadeghzadeh@iau.ac.ir

موضوع اصلی:
مسیر یابی امن در شبکه های حسگر زیر آب

تاریخچه مقاله:
تاریخ دریافت: ۲۶ فروردین ۱۴۰۳
تاریخ بازنگری: ۲۷ مرداد ۱۴۰۳
تاریخ پذیرش: ۲۸ مرداد ۱۴۰۳

چکیده:

شبکه‌های ارتباط زیرآب با چالش‌هایی مانند مسیریابی، تداخل سیگنال، مصرف انرژی و تهدیدات امنیتی مواجه هستند. اگر چه پروتکل‌های مسیریابی برای محیط‌های زیرآبی به‌منظور مقاومت در برابر اختلالات معمول بهینه شده‌اند، اما برای مقابله با حملات و رفتارهای مخرب گره‌های همسایه به‌طور خاص طراحی نشده‌اند. عوامل اصلی تهدیدات امنیتی در شبکه‌های حسگر زیرآب شامل منبع تغذیه محدود، رسانه‌های ارتباطی محدود و شرایط دشوار ارتباط زیرآب هستند. بنابراین هدف از این پژوهش ارائه مدل ارتباطی مقاوم در برابر حملات مسیریابی امن در شبکه‌های حسگر زیر آب است. بدین منظور دو مدل برای پیوندهای ارتباطی بین هر جفت گره در نظر گرفته شد. سناریو ۱، یک مدل پایه مبتنی بر فاصله است. در سناریوی دوم، از یک مدل احتمالی از بهره کانال بین هر جفت گره استفاده گردید. نتایج شبیه‌سازی شامل چهار مرحله: ۱) کشف همسایه امن تحت حملات کرم چاله ۲) فرآیند کشف مسیر اولیه و انتخاب گره های قابل اعتماد برای انتقال به سینک ۳) فرآیند تشخیص حمله در حین توزیع داده بر اساس اطلاعات وضعیت گره‌ها برای شناسایی حمله سیبل و ۴) کشف مسیر امن جایگزین برای شناسایی گره‌های مخرب می‌باشد، نشان داد که طرح پیشنهادی به نرخ موفقیت بهتری نسبت به طرح پایه دست یافته و با هزینه‌ی انرژی تحرک کمتری نسبت به روش پایه ، نسبت موفقیت قابل‌مقایسه‌ای را به دست آورده است.

کلید واژه‌ها: اینترنت اشیای زیر آب، کشف همسایه امن، مسیریابی زیر آب، حمله کرم چاله

تازه‌های تحقیق:

- محدودیت قابلیت‌های پردازش و ارتباطی در اینترنت اشیا زیر آب.
- شبیه‌سازی انتقال سیگنال راهنما و شکل‌گیری جدول همسایه در دو مدل ارتباطی.
- روش پیشنهادی بالاترین توان عملیاتی شبکه را در مقایسه با روش پایه نشان داد.

۱-مقدمه

اینترنت اشیا به‌عنوان جزئی از انقلاب صنعتی سوم که شی محاسباتی را برای ارسال و دریافت داده‌های فیزیکی از طریق اینترنت جاسازی می‌کند، مورد استقبال زیادی قرار گرفته است [۱]. اینترنت اشیا می‌تواند به‌صورت تلفیقی از یک شبکه ناهمگن در نظر گرفته شود که نه‌تنها چالش‌های امنیتی در شبکه‌های حسگر فعلی، ارتباطات مخابراتی تلفن همراه و اینترنت را در بردارد بلکه مسائلی همچون شبکه خصوصی، احراز هویت در شبکه ناهمگن، چالش‌های کنترل دسترسی و مسیریابی امن در بین دستگاه‌های ناهمگن را نشان می‌دهد [۲].

شبکه اینترنت اشیای زیر آب، متشکل از وسایل نقلیه خودران، حسگرهای از راه دور، رله‌های سطحی، و نظایر آن، به دلیل توانایی‌شان در پایش و بررسی مناطق اقیانوسی بزرگ، در سال‌های اخیر مورد توجه قرار گرفته است. شبکه‌های ارتباطی زیر آب با مجموعه چالش‌های متفاوتی نسبت به شبکه‌های ارتباطی زمینی، از جمله مسیریابی بسته، اختلال سیگنال، مصرف انرژی و حملات احتمالی در شبکه، مواجه است. از این‌رو در مطالعات متعددی به موضوع پروتکل‌های مسیریابی که شرایط منحصربه‌فرد تجربه‌شده در محیط زیر آب را کنترل می‌کنند[۳]، [۴]، پرداخته شده است. برای مثال، دنیل جی و همکارانش در مرکز امنیت ملی هیوم [۵] یک مدل شبیه‌سازی کشف همسایه و مسیر در شبکه ارتباطات صوتی زیر آب را ارائه کردند که در آن بر کاربرد اینترنت اشیای زیر آب که در آن توانمندی‌های پردازشی برای رمزگذاری/هویت‌سنجی و توانمندی‌های ارتباطی برای تصدیق یا بازانتقال را ارائه داده‌اند که ممکن است محدود باشند. آنها در مدل شبیه‌سازی‌شان تأثیر کانال زیر آب و رفتار گره مخرب بر کشف مبتنی بر سیگنال راهنما را اندازه‌گیری کردند. نتایج این بررسی نشان داد که گره مخرب می‌تواند با موفقیت بر عملکرد شبکه تأثیر بگذارد، با این حال، تأثیر کانال از اهمیت بیشتری برخوردار بود. بنابراین آنها نتیجه‌گیری کردند که، مسیریابی چندمسیره استراتژی کاهشی بالقوه‌ای هم برای شرایط کانال و هم برای حمله فروچاله خواهد بود.

قریشی[۱] و همکارانش [۶] پروتکل مسیریابی فرصت‌طلبانه اجتناب از حفره[۲] (OVAR) را برای شبکه‌های زیر آب مطرح می‌کند که به مسئله حفره‌هایی می‌پردازد که ممکن است طرح‌های مسیریابی رایج‌تر را مختل کنند. با اینکه پروتکل‌هایی همچون OVAR در مقابل اختلالات معمول تجربه‌شده در محیط زیر آب تاب‌آوری دارند، لزوماً برای کنترل حملات احتمالی و رفتار مخرب گره‌های همسایه طراحی نشده‌اند. آنها در مطالعه خود بر اهمیت قابلیت مقیاس‌پذیری در شبکه‌های زیر آبی با تعداد زیاد گره‌ها تأکید می‌کنند.

در بحث چالش‌های شبکه‌های حسگر بیسیم زیرآب می‌توان به این نکات اشاره کرد که در کانال‌های صوتی که پهنای باند کم و کیفیت لینک ضعیفی دارند، به دلیل محوشدگی و ویژگی‌های انعکاسی کانال صوتی، نرخ خطای بیت[۳] بالاست. با وجود این، ارتباطات صوتی بازه انتقال بهتری نسبت به فرکانس رادیویی/ القای مغناطیسی[۴] (MI) با پهنای باند بالاتر یا انتقال نوری زیر آب دارند [۷].

با توجه به سیار بودن حسگرها، عدم قطعیت افزوده در کشف و نگهداری همسایه‌ها را باید در نظر گرفت. گره‌ها در محیطی با عمق و با جریان‌های آبی متغیری قرار دارند که عدم قطعیت بیشتری در اتصال و مکان‌های آینده گره‌ایجاد می‌کنند.

شبکه‌های زیر آب در معرض انواع گوناگونی از حملات قرار دارند از این‌رو امنیت یکی مهم‌ترین نگرانی‌ها در شبکه‌های زیر آب وسایل نقلیه خودران و حسگرهاست [۸]، [۷]، از جمله حملات کرم‌چاله،حملات فروچاله[۵]، ارسال انتخابی[۶] و بسیاری موارد دیگر[۶]، [۹]، [۸]، [۱۰].برای مثال، در حملات کرم چاله، بسته‌های یک منطقه از شبکه از طریق لینک سریع و خارج از باند، به منطقه دیگری از شبکه منتقل شده و بازپخش می‌شوند، به‌طورکلی این حملات، با نامطمئن کردن اطلاعات مربوط به همسایه‌ها، پروتکل کشف مسیر شبکه را هدف قرار می‌دهند. فروچاله این کار را با همه‌پخشی[۷] شماره هاپ پایین یا اولویت مسیریابی بالا انجام می‌دهد و سپس همه بسته‌های دریافتی‌اش را حذف می‌کند. حمله کرم‌چاله دو گره دشمن را با کانال

---

[1] Ghoreishi
[2] opportunistic void avoidance routing
[3] bit error rate
[4] magnetic induction
[5] sinkhole attack
[6] selective forwarding
[7] broadcasting

ارتباطی سریع (مثلاً فرکانس رادیویی زمینی) به هم وصل می‌کند تا با استفاده از آن به‌سرعت اطلاعات سیگنال راهنما را ارسال کنند. آنها این اطلاعات را منتقل می‌کنند و شبکه نتیجه می‌گیرد که این دو گره به هم نزدیک‌اند، در نتیجه به تمام گره‌های مجاور اطلاعات مسیریابی نادرست می‌دهد. گره‌های مهاجم همچنین می‌توانند شبکه را متقاعد کنند که گره یکسانی در دو مکان متفاوت‌اند. در برخی مطالعات اخیر به این چالش‌ها پرداخته شده است. برای مثال؛ درگاهی و همکاران در مطالعه‌ای به بررسی چالش‌های امنیتی و حملات به شبکه‌های حسگر بیسیم زیر آب و همچنین راه‌حل‌های احتمالی کاهش این چالش احتمالی می‌پردازند [۱۱]. در برخی پژوهش‌ها نیز پروتکل‌های مسیریابی به‌طور خاص برای محیط‌های ارتباطی زیر آب طراحی شده‌اند [۵]، [۶]، [۱۲]-[۱۳]. به‌ویژه، محققان پروتکل‌هایی همانند OVAR [۶]، IVAR [۱۴]، و BEAR [۱۳] را ارائه کرده‌اند. پروتکل مسیریابی فرصت‌طلبانه اجتناب از حفره، یا OVAR، سعی می‌کند که توان عملیاتی را در محیط پراکنده و پراتلاف زیر آب، بالا ببرد و در عین حال در انرژی صرفه‌جویی کند [۶]. مسیریابی ٔ اجتناب از حفره[۱]، یا IVAR، مشابه پروتکل اجتناب از حفره‌ای است که سعی می‌کند از مشخص بودن مقصد برای داده‌ها به نفع خودش استفاده کند و از مکان مقصد و شماره هاپ گره‌های انتقال‌دهنده برای انتخاب انتقال بعدی بهره ببرد [۱۴]. طرح مسیریابی سازگار با انرژی متوازن[۲] (BEAR) به دنبال طولانی کردن طول عمر حسگرهای زیر آب از طریق ارزیابی طرح‌های مصرف انرژی کارآمد و مصرف انرژی متوازن است. پروتکل مسیریابی فشار به حفره (VAPR) از سونوبوی‌ها[۳] برای دور زدن مناطق حفره‌دار و انتقال داده به سینک استفاده می‌کند [۱۵]. در همین راستا ژانگ[۴] و همکارانش در مطالعه‌شان چند پروتکل کشف مسیر را ارائه کردند، آنها اذعان داشتند که مصرف بالای انرژی، ساختار پویا و تاخیر انتقال، نیازمند پروتکل‌های مسیریابی ویژه‌ای هستند، که عبارتند از:

- پروتکل‌های مبتنی بر انرژی: این پروتکل‌ها بر بهینه‌سازی مصرف انرژی در گره‌های حسگر زیرآبی تمرکز دارند.
- پروتکل‌های مبتنی بر داده: این پروتکل‌ها به رویکردهای مرتبط با داده برای انتقال کارآمد تمرکز دارند.
- پروتکل‌های مبتنی بر اطلاعات جغرافیایی: این پروتکل‌ها از اطلاعات مکانی برای تصمیم‌گیری‌های مسیریابی استفاده می‌کنند.

همچنین عواملی مانند تداخل نویز محیطی و تغییر فرکانس داپلر تأثیری بر کیفیت ارتباط گره‌های حسگر زیرآبی دارند [۱۶]. با اینکه رمزنگاری راه‌حل رایجی برای حفظ این فرایند از حملاتی چون فروچاله و کرم‌چاله است، ممکن است راه‌حلی به‌شدت پردازشی باشد که دستگاه‌های اینترنت اشیای زیر آب با توان محدود قادر به پشتیبانی از آن نباشند.

تخمین مسیر رسیدن[۵] (DoA) مفید است، چون با دانستن اینکه سیگنال از کجا می‌آید، الگوریتم‌های شکل‌دهی پرتو تطبیقی[۶] می‌توانند توان سیگنال‌های تداخلی را به حداقل برسانند. تخمین DoA معمولاً به آرایه‌ای از حسگرهای برداری یا آرایه‌ای از هیدروفون‌ها[۷] نیاز دارد که نیروهای آکوستیک صفحه‌ای[۸] را تشخیص می‌دهند و بعد اختلاف فاز سیگنال‌های دریافتی را برای تخمین جهت موردنظر تحلیل می‌کنند. اطلاعات DoA همچنین راهی برای شناسایی بالقوه گره‌هایی فراهم می‌کند که مطابق با مکان جغرافیایی‌شان رفتار نمی‌کنند (یا اطلاعات را گزارش نمی‌دهند).

با توجه به مطالبی که عنوان شد، و مطابق با نتایج مطالعات پیشین ایمن‌سازی به دلیل ویژگی‌ها و محدودیت‌های آنها آسان نیست و همچنین استقرار و نگهداری شبکه از سوی دیگر هزینه بالائی در برداشته و طرح‌ها از نظر مصرف انرژی بار سنگینی خواهند داشت.

همچنین با توجه به پیش‌بینی‌ناپذیر بودن محیط زیر آب، کشف همسایه نقش مهمی در تعیین مسیرهای دقیق انتقال بسته در شبکه زیر آب ایفا می‌کند. متأسفانه، اگر اقدامات احتیاطی درستی اتخاذ نشود، به‌راحتی می‌توان از کشف همسایه سوءاستفاده کرد. اگر گره مخرب بتواند به فرایند کشف همسایه نفوذ کند و به گره داخلی تبدیل شود، می‌تواند به داده‌های حساس گوش بدهد. برای جلوگیری از این اتفاق، گره‌ها باید با پروتکل‌هایی برنامه‌ریزی شوند که آنها را قادر به شناسایی گره‌هایی می‌کنند که، مثلاً براساس رفتار آموخته‌شده، عضو قانونی شبکه نیستند. در این مقاله، شبکه‌ای از دستگاه‌های اینترنت اشیای زیر آب را

[1] inherently void avoidance routing
[2] balanced energy adaptive routing
[3] sonobuoys
[4] R. Zhang
[5] DoA - Direction of arrival.
[6] adaptive beamforming algorithms
[7] hydrophones
[8] plane acoustics

شبیه‌سازی خواهیم کرد که در محیط ارتباطی صوتی فعالیت دارند و تأثیر حمله کرم چاله در چنین شبکه‌ای را بررسی می‌کنیم. از چارچوب شبیه‌سازی بهره می‌بریم تا امکان تصویرسازی فرایند کشف شبکه فراهم شود. از دیگر سو هدف این مقاله، بررسی آسیب‌پذیری طرح‌های مسیریابی زیر آب در مقابل رفتار مخرب در فرایند کشف مسیر شبکه می‌باشد. در واقع شبیه‌ساز شبکه ارتباطی زیر آب پویایی در این مطالعه ایجاد خواهد شد که روال سیگنال‌دهی را پیاده‌سازی کرده که می‌توان آن را اصلاح کرد تا طرح‌های مسیریابی پیشنهاد شده در منابع مطالعاتی را نشان دهد [۱۷].

رویکرد در نظر گرفته شده برای افزایش محرمانگی، یکپارچگی و در دسترس بودن داده‌ها احراز هویت لایه فیزیکی است که یک روش مشارکتی برای احراز هویت پیام‌ها در شبکه‌های صوتی زیر آب معرفی شده است .این شامل گره‌های قابل اعتماد و گره سینک است که برای تعیین اینکه آیا پیام دریافتی قانونی است یا از طرف یک مهاجم با یکدیگر همکاری می‌کنند .این روش از وابستگی مکانی و عدم تغییر زمانی ویژگی‌های کانال صوتی زیر آب برای محاسبه یک شاخص تصمیم برای احراز هویت استفاده می‌کند .گره‌های مورد اعتماد محاسبه را به‌صورت توزیع شده انجام می‌دهند، درحالی‌که گره سینک نظرات آنها را ترکیب می‌کند و بدون نیاز به ارائه بازخورد به گره‌های مورد اعتماد تصمیم نهایی را می‌گیرد .اثربخشی این رویکرد در شبیه‌سازی‌های عددی گسترده و آزمایش‌های دریایی در مطالعات دیگر تائید شده است. در محیط‌هایIoUT ، گره‌های حسگر به‌صورت پراکنده مستقر هستند، که مدیریت حریم خصوصی را بسیار دشوار می‌کند .بنابراین این محیط‌ها حساس و پیچیده در نظر گرفته می‌شوند .در زمینهIoUT ، اصطلاح "حریم خصوصی" معنای گسترده‌تری دارد و مکان، دستگاه و حریم خصوصی داده‌ها را پوشش می‌دهد . ازاین‌رو، راه‌حل‌های قوی برای حفظ حریم خصوصی در شبکه‌های IoUT ضروری است .رویکردهای FL به رفع نگرانی‌های مربوط به اعتماد کمک می‌کند .اما FL دارای محدودیت‌های حریم خصوصی خاصی است .پرداختن به مشکلات مربوط به حریم خصوصی در تنظیمات دارای حریم خصوصی یک چالش تحقیقاتی باز است. پیاده‌سازی پروتکل‌های سبک وزن و ایمن می‌تواند یک راه حل ممکن باشد [۱۸].

ساختار مقاله به این صورت است که سازمان‌دهی شده که در بخش ۲ به توضیح نحوه مدل‌سازی و شبیه‌سازی شبکه ارتباطی زیرآب، از جمله مدل لینک ارتباطی و مدل انرژی پرداخته خواهد شد. در بخش ۳ مراحل شبیه‌سازی به اجمال بررسی‌شده و در ادامه در بخش ۴ نتایج شبیه‌سازی ارائه می‌گردد، در نهایت در بخش نتیجه‌گیری به بحث و بررسی حول نتایج به دست آمده در شبیه‌سازی خواهیم پرداخت.

۲-مدل شبکه

داده‌ها و ویژگی‌های پژوهش پیش رو از داده‌های پژوهش‌های پیشین اقتباس شده است. در این بخش، نحوه مدل‌سازی و شبیه‌سازی شبکه ارتباطی زیر آب، از جمله مدل لینک زیر آب، روال سیگنال راهنما، کشف مسیر، و رفتار گره مخرب، را توضیح می‌دهیم.

۲-۱- مدل لینک ارتباطی

ما دو مدل برای لینک‌های ارتباطی بین هر جفت گره در نظر می‌گیریم.

اولی، سناریو ۱، یک مدل پایه مبتنی بر فاصله است. در این حالت، زمانی که فاصله بین آنها کمتر از حداکثر محدوده ارتباطی باشد، دو گره توسط یک پیوند ارتباطی معتبر به هم متصل می‌شوند. حداکثر محدوده ارتباطی یک پارامتر قابل تنظیم شبیه‌ساز است.

در حالت دوم، سناریو ۲، ما از یک مدل احتمالی از بهره کانال بین هر جفت گره استفاده می‌کنیم. به‌طور خاص، ما سود کانال در مقیاس بزرگ را با یک مؤلفه قطعی و یک مؤلفه تصادفی مدل می‌کنیم. جزء تصادفی با استفاده از فرآیند AR-۱ به‌عنوان یک فرآیند تصادفی عادی گزارشی مدل‌سازی می‌شود [۱۹]. سود کانال توسط فرمول زیر محاسبه می‌شود.

$$g(d.t) = \bar{g}(d) + g_{AR}(t)(dB) \quad (۱)$$

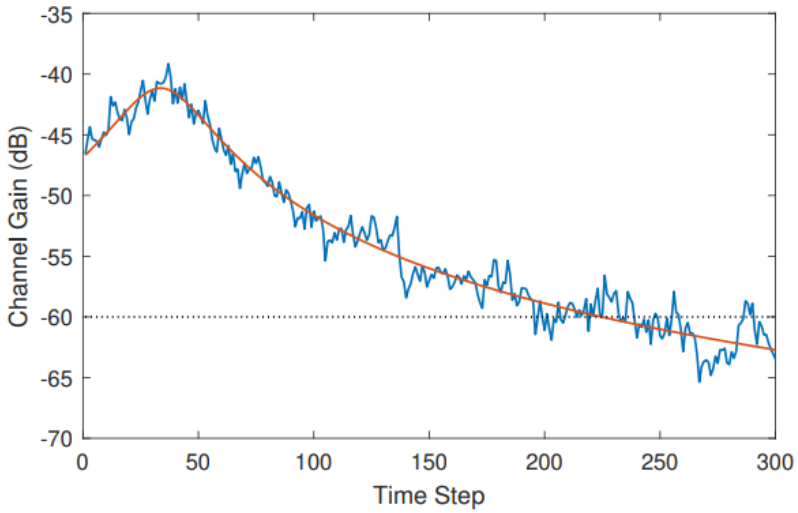
در اینجا، $\bar{g}(d)$ میانگین بهره لینک و $g_{AR}(t)$ فرایند تصادفی AR-1 (به دسی‌بل) است. میانگین بهره لینک به‌صورت قطعی براساس فاصله d بین گره‌ها و به شکل زیر محاسبه می‌شود:

$$\bar{g}(d) = g_0 - k_0 10\log 10 \quad (۲)$$

در اینجا، ثابت‌های g_0 و k_0 پارامترهای اتلاف انتشار بزرگ‌مقیاس هستند. مؤلفه بهره تصادفی به‌صورت فرایند تصادفی AR-1 و به شکل زیر مدل‌سازی می‌شود.

$$g_{AR}(t+\Delta) = \rho g_{AR}(t) + (1-\rho)\omega(t) \quad (۳)$$

در اینجا، Δ گام زمانی و ρ ضریب همبستگی در هر گام است که به اختلاف داپلر[1] f_0 براساس $\rho = (-2\pi f_0 \Delta)$ بستگی دارد، و $\omega(t)$ فرایند تصادفی گاوسی با میانگین صفر است. ما بر مقادیر تجربی ثابت‌های g_0 و k_0 تکیه می‌کنیم و f_0 از اندازه‌گیری‌های ثبت‌شده در آزمایش طوفان اقیانوس آرام (PS)[2] [۱۸] محاسبه می‌شود. یکی از مثال‌های عینی از بهره کانال در آزمایش PS در شکل ۱ نمایش داده شده است.



شکل ۱: خروجی شبیه‌سازی شده از بهره کانال برای سناریو ۲ (g۰ = -۳۹، K۰ = ۱.۸۹، f۰ = ۴۱۵، و Δ = ۳۰ ثانیه)

Figure 1 . Simulated output of channel gain for scenario 2 (g0 = -39, K0 = 1.89, f0 = 415, and Δ = 30 seconds)

۲-۲- مدل انرژی

مفروضات مربوط به اتلاف انرژی در حالت‌های ارسال و دریافت، مزیت‌های پروتکل‌های مختلف را تغییر خواهد داد. ما فرض می‌کنیم که اتلاف انرژی در اثر انتقال کانال وجود دارد. مدل انرژی برای گره‌های حسگر، هر گره دارای همان انرژی اولیه موجود برای ارسال یک پیام k-bit در فاصله R است، انرژی مصرف شده برای ارسال و دریافت پیام‌ها توسط رابطه زیر محاسبه می‌شود:

$$E_T X = E_{eleck} + E_{amp} k d^2 \quad (۴)$$

$$E_{RX} = E_{eleck} k \quad (۵)$$

انرژی مورد نیاز برای انتقال پیام E_{TX} است.

انرژی مورد نیاز برای دریافت پیام E_{RX} است.

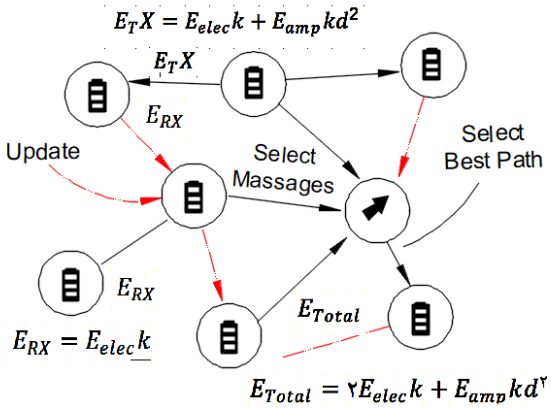
انرژی مورد نیاز برای مدار فرستنده گیرنده برای مقابله با یک بیت داده E_{elec} است.

انرژی مورد نیاز برای پردازش یک بیت داده به تقویت‌کننده فرستنده E_{amp} است.

d شعاع ارتباطی برابر گره‌ها است.

کانال رادیویی متقارن است به‌طوری‌که انرژی مورد نیاز برای انتقال یک پیام از گره A به گره B با انرژی مورد نیاز برای انتقال یک پیام از گره B به گره A برابر است.

[1] Doppler spread
[2] Pacific Storm



شکل ۲: مدل پیشنهادی انرژی
Figure 2. Energy Suggested Model

در این مدل انرژی، هر گره حسگر دارای منبع انرژی اولیه فرض می‌شود و هدف بهینه‌سازی عملکرد شبکه و در عین حال به حداقل رساندن مصرف انرژی برای افزایش طول عمر شبکه است. برای این مقادیر پارامتر، ارسال و دریافت پیام یک عملیات کم‌هزینه نیست. بنابراین پروتکل باید فواصل ارسال و همچنین تعداد عملیات ارسال و دریافت را برای هر پیام کاهش دهد. مسائلی که به آنها پرداخته می‌شود، محاسبه انرژی‌های ساخته شده با استفاده از مدل با توجه به فاصله بین گره‌ها و حذف گره‌های مرده از جدول همسایه است. در حین انتقال داده‌های جدید، اگر یک گره اطلاعاتی برای انتقال داشته باشد، گره در جدول مسیریابی خود بهترین همسایه را که نزدیک به سینک است بر اساس تعداد پرش و انرژی گره بررسی می‌کند. این کار با تعداد پرش شروع می‌شود و سپس انرژی بسته به اینکه گره بیش از یک گره در جدول همسایه خود با تعداد پرش یکسان داشته باشد و سپس انرژی باقیمانده را داشته باشد، انجام می‌شود. هنگامی‌که انرژی باقیمانده گره به زیر آستانه معینی می‌رسد، گره یک پیام به‌روزرسانی انرژی را به همسایگان خود ارسال می‌کند و آنها را از وضعیت انرژی خود مطلع می‌کند .هنگامی‌که گره‌ها پیام انرژی را دریافت می‌کنند، گره‌ای را که پیام را ارسال کرده است از جدول همسایه خود حذف می‌کنند.

۳- فازهای روش پیشنهادی (شبیه‌سازی)

برای شبیه‌سازی از نرم افزار NS2 استفاده شده است. NS2 به‌طور ساده یک ابزار شبیه‌سازی متن باز، مبتنی بر رویداد، وابسته به زمان و رخداد -گسسته است که در مطالعه طبیعت دینامیکی شبکه‌های ارتباطی مورد استفاده قرار می‌گیرد و از کتابخانه غنی از پروتکل‌های شبکه و آبجکت‌ها بهره می‌برد.

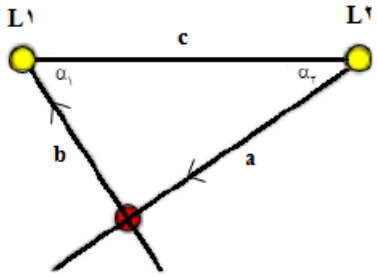
نوع ارسال بسته P2P بوده و ارسال و دریافت بسته به‌صورت همزمان نیز صورت می‌پذیرد. شبیه‌سازی از چهار مرحله تشکیل شده است: مرحله اول کشف همسایه امن تحت حملات کرم چاله در شبکه‌های حسگر زیر آب است. مرحله دوم فرآیند کشف مسیر اولیه است که گره ارسال قابل اعتماد بعدی را به گره سینک انتخاب می‌کند، بنابراین احتمال تحویل بسته به سمت سینک را افزایش می‌دهد و در نتیجه قابلیت اطمینان را افزایش می‌دهد. مرحله سوم فرآیند تشخیص حمله در حین توزیع داده است. این مرحله بر اساس اطلاعات وضعیت گره‌ها برای شناسایی حمله Sybil است. مرحله چهارم، کشف مسیر امن جایگزین برای شناسایی گره‌های مخرب است.

در شبکه‌های حسگر زیر آب که گره‌های حسگر ثابت و متحرک هستند، کشف همسایه یک نیاز اساسی است. در فرآیند کشف همسایه، هر گره همسایگان خود را کشف می‌کند و لیستی از همسایگان خود را ارائه می‌دهد. هنگامی‌که یک گره می‌خواهد گره‌های همسایه خود را پیدا کند، پیام درخواستی را در محدوده ارتباطی خود پخش می‌کند. هر پیام درخواستی شامل یک کلید خصوصی/کلید عمومی امضای دیجیتال، شماره شناسایی منحصر به فرد است. شماره شناسایی که در پیام درخواست تعبیه شده است پس از دریافت توسط گره مقصد در جدول ثبت می‌شود. با دریافت بسته‌های پخش، ابتدا گره گیرنده شماره شناسایی خود را در جدول جستجو می‌کند و در صورت وجود بسته دریافتی را حذف می‌کند. به‌این‌ترتیب از حملات مکرر جلوگیری می‌شود. اگر گره‌هایی که در محدوده ارتباطی گره بسته درخواست ارسال هستند موفق به تائید کلید عمومی/خصوصی در بسته

دریافت کننده شوند، تصمیم می‌گیرند گره‌های بسته‌ای را که دارای کلید عمومی/خصوصی معتبر هستند ارسال کنند و بسته پاسخ را به گره درخواست ارسال کنند. پیام پاسخ حاوی جهت سیگنال صوتی دریافتی و خود کلید عمومی و کلید خصوصی امضای دیجیتال است. برای یافتن جهت سیگنال صوتی، هر گره مجهز به آرایه هیدروفون است که می‌تواند جهت سیگنال صوتی ارسالی را تخمین بزند.

در صورت وجود تحرک گره در شبکه آکوستیک زیر آب، باید اثر آن بر روی گره‌ها بررسی شود. برای مدیریت گره‌های سیار، اثرات منفی این حرکات باید بر عملکرد پروتکل مسیریابی به حداقل برسد. مهم‌ترین روش کنترل تحرک، پیش‌بینی گره‌های متحرک است. در یک سناریوی واقعی، حرکات افقی در محدوده ۲-۳ متر بر ثانیه امکان‌پذیر نیست و فقط نوسانات جزئی وجود خواهد داشت، درحالی‌که به‌صورت عمودی، گره به‌طور مداوم با سرعت ۲-۳ متر بر ثانیه با جریان آب حرکت می‌کند. به‌عنوان مثال، گره x یک پیام درخواست ارسال می‌کند، گره y پیام را در L1 دریافت می‌کند، گره y بسته پاسخ را به گره x در L2 می‌فرستد. اکنون جهت سیگنال ارسالی از y به x تغییر کرده است. در چنین شرایطی، گره x پس از تائید امضای دیجیتال گره y، ابتدا بررسی می‌کند که معادله برقرار باشد.

با توجه به حرکت گره y از محل L1 به L2، یک مثلث بین گره x و گره y با رسم سیگنال‌های ارسالی و دریافتی همانطور که در شکل زیر نشان داده شده است ایجاد شد. a فاصله گره x تا گره y در L1 است. b فاصله گره x تا گره y در L2 است.



شکل ۳:تأثیر حرکت گره در فرآیند کشف همسایه (پیشنهادی)
Figure 3. The effect of node movement on neighbor discovery process

مسافت طی شده از محل گره قبلی تا مکان جدید C است.

$$\frac{a}{\sin a_1} = \frac{b}{\sin a_2} = 2R \quad (۶)$$

$$a^2 = b^2 + c^2 - 2bc \times \cos a_1 \quad (۷)$$

$$b^2 = a^2 + c^2 - 2ac \times \cos a_2 \quad (۸)$$

با به دست آوردن مقدار مساوی از معادله فوق می‌توان شعاع محیط مثلث را به دست آورد. اگر شعاع محیط مثلث بزرگتر از محدوده ارتباطی گره باشد، گره y از محدوده ارتباطی گره x خارج است و گره x گره y را به‌عنوان همسایه خود نمی‌پذیرد.

در صورت برقراری این رابطه، گره x مکان قبلی گره y را به‌روز می‌کند. جهت سیگنال صوتی از y تا x محاسبه می‌شود. گره y با دریافت بسته پاسخ از گره x، امضا را تائید می‌کند و سپس جهت دریافتی جدید سیگنال صوتی را از گره x محاسبه می‌کند و آن را در رابطه ۹ قرار می‌دهد.

$$\left|a_{yx} + a_{xy}\right| - \pi \le \partial \quad (۹)$$

δ خطاهای از پیش تعیین شده است. αxy زوایای جهت xy است. اگر ۱۸۰ درجه از مجموع سیگنال صوتی x به y کم شود و y به x کمتر از خطاهای از پیش تعیین شده باشد، گره y می‌تواند گره x را به‌عنوان همسایه واقعی بپذیرد و در لیست همسایگان خود قرار دهد و سپس بسته پاسخ را به گره x ارسال کند.

در بسته پاسخ، کلید عمومی گره x و y برای سیگنال صوتی قرار داده شده است. با دریافت بسته پاسخ توسط گره y، امضا تائید می‌شود. اگر امضا معتبر باشد، گره x تصمیم می‌گیرد که گره y دارای کلید عمومی/خصوصی معتبر باشد. سپس جهت سیگنال

صوتی y به x را محاسبه کرده و در رابطه قرار می‌دهد. در صورت برقراری رابطه فوق، گره x می‌تواند گره y را به‌عنوان یک همسایه واقعی بپذیرد و آن را در لیست همسایه خود قرار دهد.
پس از اینکه هر گره لیستی از همسایگان را ارائه کرد، فاصله فیزیکی واقعی بین دو گره محاسبه می‌شود تا روابط گره‌های همسایگی بررسی شود و کرم‌چاله شناسایی شود. اگر فاصله اندازه‌گیری شده بیشتر از محدوده گره‌های ارتباطی باشد، فرض می‌شود که گره‌ها از طریق کرم چاله به هم متصل شده‌اند. در SRAU، هر گره حسگر فاصله خود را با همسایگان محاسبه می‌کند. محاسبه گره مقصد با استفاده از انرژی سیگنال صوتی ارسالی توسط گره مبدأ و دریافت آن توسط گره مقصد انجام می‌شود. انرژی دریافتی به‌صورت معادله ۱۰ محاسبه می‌شود:

$$E_{recieve} = \frac{E_{send}}{4\,\pi R^2}\,\lambda \qquad (۱۰)$$

انرژی ارسال شده E_{send} است. R محدوده ارتباطی است و λ طول موج است. ما یک منطق فازی را در نظر می‌گیریم، بنابراین تابع ورودی فاصله و انرژی مصرفی گره است، تابع خروجی اعتبار سنجی گره است که جدول ۲ نشان‌دهنده آن هست.
در واقع هر گره همسایه‌هایی را که اعتبار پایینی دارند به‌عنوان حملات کرم چاله در نظر گرفته و از لیست همسایگان خود حذف می‌کند.

جدول ۱: پارامترهای شبیه‌سازی
Table 1. Simulation parameters

Parameter	Parameter Value
Network Dimensions	2000*2000
Number of nodes	40,50,70,100
Interface Queue Capacity	50 Packet
Interface Queue Type	DropTail
The initial energy of each node	50 Jol
Simulation Time	1500
Standard Type MAC	802.11

اطلاعات ورودی از مطالعات قبلی[۵] [۱۹] در جدول پارامترهای شبیه‌سازی ، محاسبه و بعد از استخراج خروجی‌ها، اطلاعات ورودی شامل تعداد گره و فضای شبیه‌سازی و زمان شبیه‌سازی، اطلاعات کیفیت سرویس از این ورودی‌ها استخراج می‌شود.
ازآنجاکه مسیریابی یک مسئله اساسی در شبکه است، الگوریتم مسیریابی باید گره ارسال بعدی را انتخاب کند که احتمال تحویل بسته را به سمت سینک افزایش می‌دهد و در نتیجه شاخص متریک قابلیت اطمینان که به لینک‌های شبکه مرتبط بوده و به‌صورت داینامیک محاسبه می‌شود را افزایش می‌دهد. هر گره یک جدول مسیریابی محلی دارد . هنگامی‌که هر گره حسگر یک بسته را ارسال می‌کند، یک شناسه منحصر به فرد به آن متصل می‌شود.
در فرآیند مسیریابی، ابتدا یک شاخص اتصال توسط گره سینک به هر گره اختصاص داده می‌شود. Sink node ابتدا یک بسته hello را پخش می‌کند تا ایندکس را به هر گره اختصاص دهد. به‌محض دریافت بسته‌های hello توسط گره‌های حسگر، یک شاخص اتصال و تعداد پرش از گره سینک تخصیص داده می‌شود. سپس با دریافت بسته‌های hello توسط گره‌ها، شاخص اتصال و تعداد پرش آنها به سمت سینک بازپخش می‌شود که ممکن است این بسته را توسط گره‌های همسایه خود نیز دریافت کنند. هنگامی‌که یک گره بسته‌ای را از گره همسایه دریافت می‌کند، ابتدا تعداد پرش گره‌های همسایه بررسی می‌شود. اگر تعداد پرش گره‌های همسایه کمتر یا مساوی از تعداد پرش آن باشد، شاخص اتصال آن یک واحد افزایش می‌یابد و شناسه، شاخص اتصال و تعداد پرش گره‌های همسایه را حفظ می‌کند. اکنون، هر گره یک بسته برای ارسال به گره سینک دارد و باید گره ارسال بعدی را انتخاب کند. ابتدا، آن گره لیست همسایه را بر اساس بالاترین شاخص اتصال در بین همسایگان خود که لیست همسایه آنها در مرحله قبل به دست آمده است مرتب می‌کند. اکنون، گره ارسال بعدی انتخاب شده بر اساس بالاترین شاخص اتصال، تعداد

پرش کوچکتر و انرژی باقی‌مانده بیشتر است. سپس، گره بسته درخواستی را به گره انتخابی بعدی ارسال می‌کند که حاوی موقعیت گره و مقصد نهایی است و منتظر بسته تائید می‌شود و بسته خود را با بسته تائید دریافتی ارسال می‌کند. عمر مسیریابی به زمان مهلت یا تائید دریافتی مربوطه بستگی دارد به‌طوری‌که هر گره با یک تایمر تنظیم می‌شود و منتظر بسته تائید است. اگر زمان منقضی شود یا بسته خراب دریافت کند، بخش دوباره ارسال می‌شود.

جدول ۲: تائید اعتبار
Table 2. Validation

Rate of validation	Energy consumption	distance
A lot	low	low
A lot	A lot	low
low	low	A lot
low	A lot	A lot

از شاخص اتصال متریک استفاده گردیده است که :

- متریک یک مقدار اختصاص داده شده به هر مسیر است.
- این مقدار تعیین می‌کند که مسیرهای بهینه برای ارسال بسته‌ها انتخاب می‌شوند.
- معمولاً متریک تعداد پرش‌ها (HOP) یا تعداد روترهایی است که باید برای رسیدن به شبکه مقصد از آن‌ها عبور کرد.
- اگر چندین مسیر وجود داشته باشد، معمولاً مسیری با کمترین متریک انتخاب می‌شود.
- مکانیزم جدول مسیریابی به این صورت است که وقتی بسته‌ای از مبدأ به مقصد ارسال می‌شود، روتر آن را باز می‌کند و اگر آدرس IP مقصد در جدول مسیریابی قرار داشت، بسته را به شبکه موردنظر هدایت می‌کند .در غیر این صورت، به بهترین مسیر برای رسیدن به مقصد هدایت می‌شود.
- این فرآیند باعث ارسال بهینه‌تر بسته‌ها در شبکه می‌شود.
- شماره شناسه:(Node ID)

این شماره به هر گره در شبکه اختصاص داده می‌شود که از آن برای شناسایی گره‌ها در جدول مسیریابی استفاده می‌شود.

- اتصال شاخص به سینک:(Connectivity to Sink)

این پارامتر نشان‌دهنده اتصال گره به سینک (گره مقصد) است. می‌تواند مقدار بولی (بله/خیر) داشته باشد.

- تعداد گام مانده به سینک:(Hops to Sink)

تعداد گام‌های باقی‌مانده تا رسیدن به سینک را نشان می‌دهد. این پارامتر می‌تواند عدد صحیح نامنفی باشد.

- انرژی:(Energy)

میزان انرژی باقی‌مانده در گره را نشان می‌دهد. معمولاً از واحدهای میلی‌ژول یا ژول استفاده می‌شود.

- طول عمر گره:(Node Lifetime)

مدت زمانی که گره قابل‌استفاده است را نشان می‌دهد. می‌تواند به واحدهای زمانی مانند ثانیه، دقیقه یا ساعت باشد.

- این پارامترها هنگام اجرا مقداردهی می‌شود:

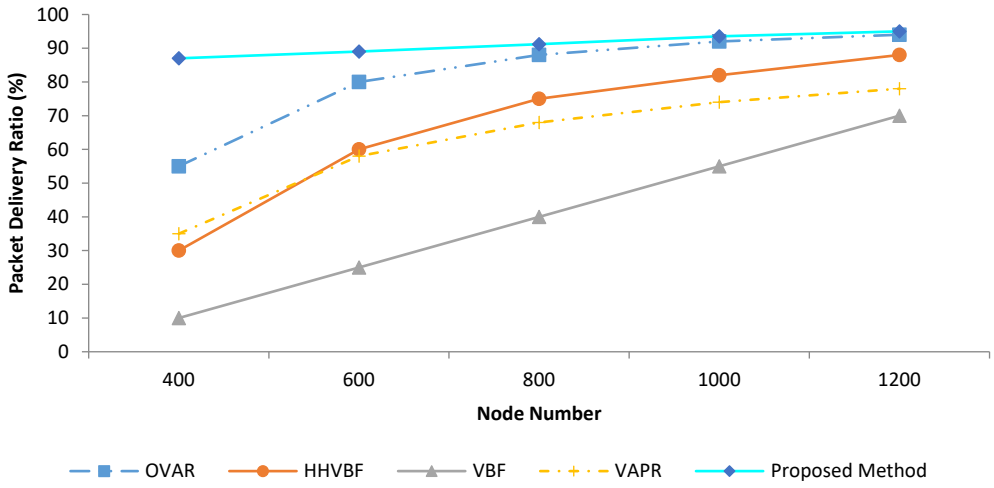
گره همسایه با دریافت هر قسمت، داده‌ها را بررسی می‌کند و قسمت در نظر گرفته شده را مجدداً به مقصد ارسال می‌کند. در طول انتشار داده‌ها، یک گره اغلب با گره‌های دیگر ارتباط برقرار می‌کند و هر گره هنگام ارسال و دریافت بسته‌ها انرژی مصرف می‌کند. سپس، انرژی گره باقی‌مانده کاهش می‌یابد. برخی ارزیابی‌ها برای شناسایی حمله Sybil در حین انتشار داده‌ها انجام می‌شود. حملات Sybil یک تهدید جدی در شبکه‌های حسگر زیر دریایی‌ها هستند. در چنین حملاتی، یک گره مخرب چندین هویت جعلی برای خود ایجاد می‌کند و گره‌های شبکه را گمراه می‌کند و انرژی گره‌های حسگر باقیمانده را کاهش می‌دهد. بنابراین طول عمر شبکه کاهش می‌یابد. برای یافتن گره مشکوک، داده‌های هر گره بررسی می‌شود.

در یک دوره زمانی مشخص، گره x شروع به ارسال بسته ها به گره y می‌کند. بسته‌های ارسال شده با Psend نمایش داده می‌شود.

گره y بسته ها را از گره x دریافت می‌کند. بسته‌های ارسال شده با Precieve نمایش داده می‌شود.
گره x پس از دریافت پاسخ از گره y، زمان اتصال را ثبت می‌کند. زمان پایان اتصال با Tend نمایش داده می‌شود.

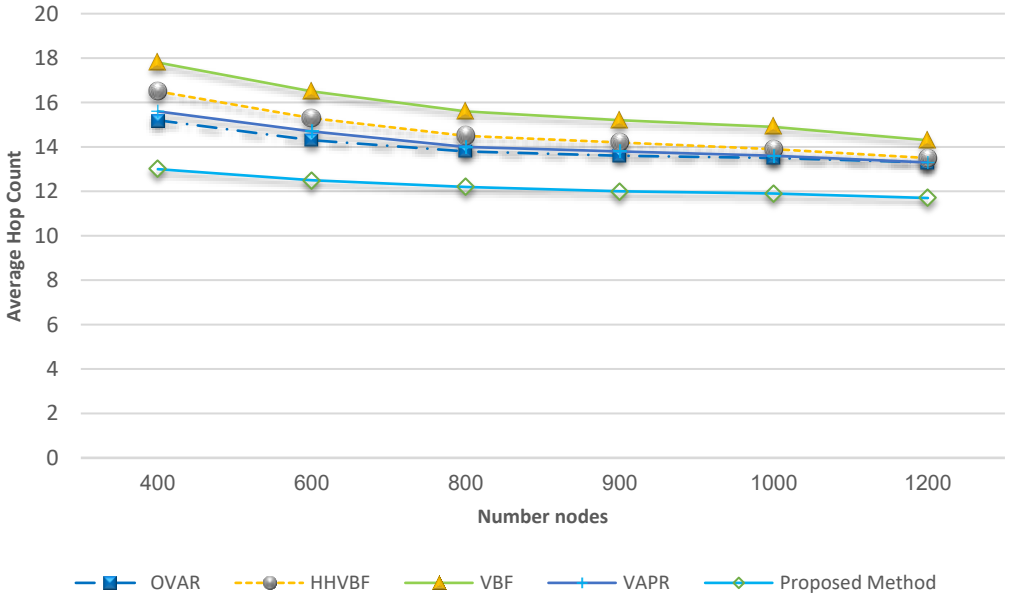
۴- نتایج شبیه‌سازی

برای هر خروجی ثبت شده در نمودار ۴۰ بار اجرا گرفته شده و میانگین آن به دست آمده است.



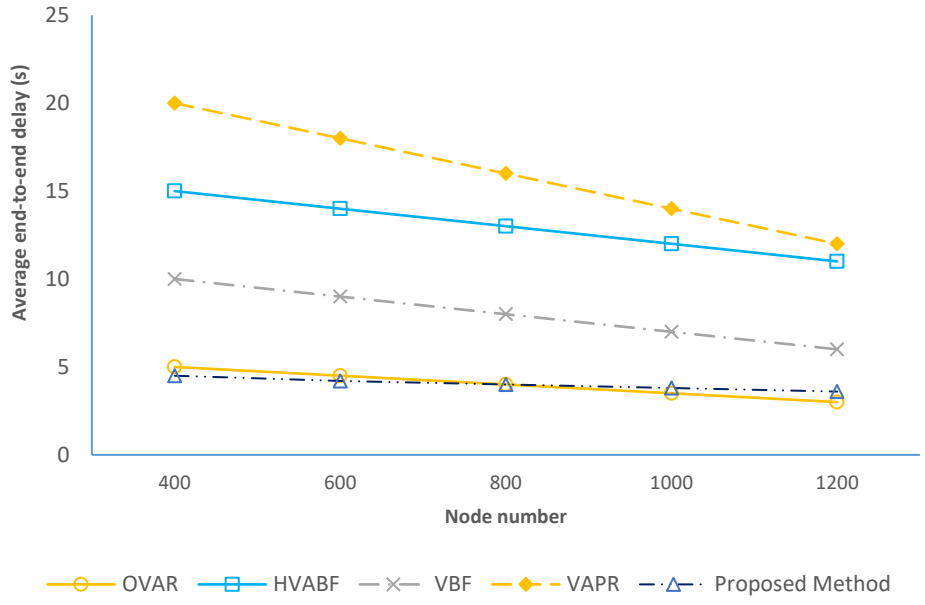
شکل ۴: مقایسه نمودار نرخ تحویل بسته شبکه نسبت به تعداد گره با مطالعات قبلی [۶]
Figure 4. Comparison of the graph of network packet delivery rate relative to the number of nodes with previous studies[6]

نرخ تحویل بسته، نسبت تعداد پیام‌های داده‌ای است که با موفقیت منتقل شده‌اند و توسط مقصد دریافت شده‌اند. متریک اول ما اندازه‌گیری نسبت موفقیت میانگین برای تعداد گره‌های مختلف متحرک می‌باشد. تمام پارامترهای شبیه‌سازی دیگر، مانند سناریوی شبیه‌سازی پیش فرض، مشخصات دهی شده‌اند. همانطور که در شکل ۴ نشان داده شده است میانگین نسبت موفقیت افزایش می‌یابد. نتیجه‌ی ما نشان می‌دهد که طرح پیشنهادی به نرخ موفقیت بهتری نسبت به طرح پایه[۶] دست یافته و با هزینه‌ی انرژی تحرک کمتری نسبت به روش پایه ، نسبت موفقیت قابل‌مقایسه‌ای را به دست آورده است.



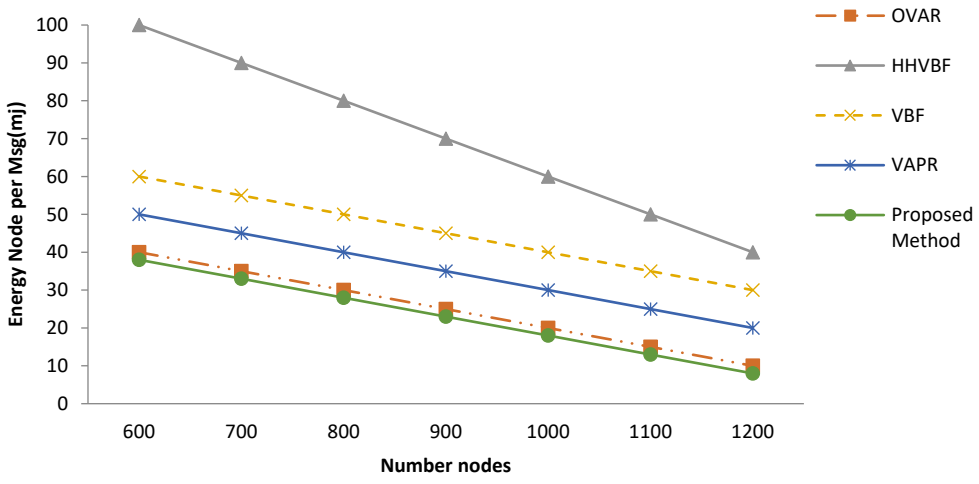
شکل ۵ : مقایسه نمودار توان عملیاتی شبکه نسبت به تعداد گره و تعداد پرش‌ها با مطالعات قبلی [۶]
Figure 5. Comparison of the graph of network throughput relative to the number of nodes and the number of nodes with previous studies[6]

ارتباط بین توان عملیاتی و تعداد پرش نود به این صورت است که با افزایش تعداد پرش‌ها، احتمال از دست رفتن داده‌ها و تأخیر در انتقال افزایش می‌یابد، که می‌تواند منجر به کاهش توان عملیاتی شود. به عبارت دیگر، هرچه تعداد پرش‌ها بیشتر باشد، احتمال بروز مشکلاتی مانند ازدحام و تأخیر بیشتر می‌شود، که این عوامل می‌توانند توان عملیاتی شبکه را کاهش دهد. شکل ۵ نشان می‌دهد که روش پیشنهادی نسبت به روش پایه دیگر [۶] دارای بیش‌ترین توان عملیاتی شبکه بوده است.



شکل ۶: مقایسه نمودار تاخیر انتها به انتها شبکه نسبت به تعداد گره با مطالعات قبلی [۶]

Figure 6. Comparison of the end-to-end delay chart of the network relative to the number of nodes with previous studies[6]



شکل ۷: مقایسه نمودار مصرف انرژی کل شبکه نسبت به تعداد گره با انرژی مصرفی هر گره با مطالعات قبلی [۶]

Figure 7. Comparing the graph of energy consumption of the entire network with the number of nodes and the energy consumption of each node with previous studies[6]

در نمودارشکل ۶، میانگین تأخیر انتها به انتها را به‌عنوان نموداری از تعداد گره‌های متحرک با سرعت متفاوت بررسی و با مطالعات قبل [۶] مقایسه نمودیم. این معیار میانگین زمان تأخیر گرفته شده از لحظه ایجاد بسته ها در مبدأ تا دریافت توسط سینک را برای همه بسته ها با موفقیت محاسبه می‌کند. تاخیر انتشار، تاخیر انتقال و زمان نگهداری بسته ها را برای محاسبه تاخیر انتها به انتها در نظر می‌گیریم. متوسط تأخیر انتها به انتها برای همه پروتکل‌ها با افزایش تعداد گره‌ها کاهش می‌یابد و به‌صورت کلی تاخیر نسبت به مطالعات قبلی کاهش یافته است. در این تحلیل، میانگین تاخیر به ازای هر گره در شبکه تأثیرگذار

است. اگر چه تغییر مسیر دینامیکی از یک فرستنده، مسیر مختلفی را به مقصدهای متحرک که با سرعت‌های مختلف حرکت می‌کنند، می‌فرستد.

در نمودار شکل ۷، میانگین مصرف انرژی بررسی شده است. تراکم گره، تأثیر کمی بر انرژی به ازای هر گره در روش پیشنهادی دارد، اگر چه همسایه‌های بیشتری، داده‌های یک فرستنده‌ی با تراکم بالا را استراق سمع می‌کنند. به این دلیل که شانس بیشتری وجود دارد که مسیرهای بهتر از نظر هزینه‌ی انرژی را می‌توان در یک شبکه‌ی با تراکم بالاتر یافت. روش پیشنهادی در شکل ۷، در مصرف انرژی کل، عملکرد بهتری رانسبت به مطالعات قبلی[۶] نشان می‌دهد. علت اینکه به مصرف انرژی کمتری دست یافته است این است که منبع می‌تواند رویداد انتقال را از مبدأها به مقصدهای با مسیرهای مناسب هدایت کند.

۵- نتیجه‌گیری

در مقاله حاضر، شبیه‌سازی کشف همسایه و مسیر در شبکه ارتباطات صوتی زیر آب را ارائه کردیم.کاربردی از اینترنت اشیای زیر آب را در نظر گرفتیم که در آن توانمندی‌های پردازشی برای رمزگذاری/هویت‌سنجی و توانمندی‌های ارتباطی برای تصدیق یا بازانتقال ممکن است محدود باشند. انتقال سیگنال‌های راهنما و تشکیل جداول همسایه را تحت دو مدل لینک ارتباطی شبیه‌سازی کردیم. رفتار گره مخرب بر کشف مبتنی بر سیگنال راهنما را اندازه‌گیری کردیم. نتایج ما نشان می‌دهد که گره مخرب می‌تواند با موفقیت بر عملکرد شبکه تأثیر بگذارد. نتایج مطابق جدول زیر با مطالعات قبلی مقایسه شده است و بیانگر موفقیت در توان عملیاتی، تاخیر انتها به انتها، نرخ تحویل بسته و تا حدودی مصرف انرژی است.

جدول۳: مقایسه نرخ تحویل بسته شبکه به تعداد گره در مطالعه جاری و مطالعات قبلی

Table 3. Comparing the network packet delivery rate to the number of nodes in the current study and previous studies

Porotocol	Ref	year	Packet delivery rate	Energy consumption of each node	End-to-end delay of the network(s)
VBF	[27]	2006	66	14	10/5
HHVBF	[26]	2007	90	20	-
FVBF	[25]	2018	72	7/5	6/4
EAVARP	[28]	2018	92	6	2/3
RDBF	[29]	2013	80	15	6
GEDAR	[30]	2016	82	15	5
SEECR	[31]	2020		33	23
GRMC-SM	[32]	2018	90	14	5/3
DMR	[33]	2019	35	7	-
SUGGESTED METHOD	-	-	94	8	3.2

مراجع

[1] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, p. 102022, 2020. doi: 10.1016/j.adhoc.2019.102022

[2] S. Nepali, "The Secure and Energy Efficient Data Routing in the IoT-based Network," 2020. doi: 10.1016/J.ADHOC.2019.102022

[3] J. Luo, Y. Chen, M. Wu, and Y. Yang, "A survey of routing protocols for underwater wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 23, no. 1, pp. 137-160, 2021. doi: 10.1109/COMST.2020.3048190

[4] S. M. Ghoreyshi, A. Shahrabi, and T. Boutaleb, "Void-handling techniques for routing protocols in underwater sensor networks: Survey and challenges," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 800-827, 2017. doi: 10.1109/COMST.2017.2657881.

[5] D. J. Jakubisin, C. McPeak, J. Sloop, and B. Davis, "Securing route discovery for the underwater Internet of Things," *OCEANS 2022, Hampton Roads*, pp. 1-10, Oct. 2022. doi: 10.1109/OCEANS47191.2022.9977183.

[6] S. M. Ghoreyshi, A. Shahrabi, and T. Boutaleb, "A novel cooperative opportunistic routing scheme for underwater sensor networks," *Sensors*, vol. 16, no. 3, p. 297, 2016. doi**:** 10.3390/s16030297

[7] H. Kaushal and G. Kaddoum, "Underwater optical wireless communication," *IEEE Access*, vol. 4, pp. 1518-1547, 2016. doi: 10.1109/ACCESS.2016.2552538

[8] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues, and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, 2018. doi: 10.3390/s18113907

[9] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54-60, 2015. doi: 10.1109/MCOM.2015.7180508

[10] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22-28, 2011. doi: 10.1109/MWC.2011.5714022

[11] A. G. Yisa, T. Dargahi, S. Belguith, and M. Hammoudeh, "Security challenges of internet of underwater things: A systematic literature review," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 3, p. e4203, 2021. doi: 10.1002/ETT.4203

[12] H. H. Rizvi, R. N. Enam, S. A. Khan, and J. Akram, "A survey on internet of underwater things: Perspective on protocol design for routing," *2020 Global Conf. on Wireless and Optical Technologies (GCWOT)*, pp. 1-8, Oct. 2020. doi: 10.1109/GCWOT49901.2020.9391628

[13] N. Javaid, S. Cheema, M. Akbar, N. Alrajeh, M. S. Alabed, and N. Guizani, "Balanced energy consumption-based adaptive routing for IoT enabling underwater WSNs," *IEEE Access*, vol. 5, pp. 10040-10051, 2017. doi: 10.1109/ACCESS.2017.2706741.

[14] S. M. Ghoreyshi, A. Shahrabi, and T. Boutaleb, "An inherently void avoidance routing protocol for underwater sensor networks," *2015 International Symposium on Wireless Communication Systems (ISWCS)*, pp. 361-365, Aug. 2015. doi: 10.1109/ISWCS.2015.7454364

[15] Y. Noh, U. Lee, P. Wang, B. S. C. Choi, and M. Gerla, "VAPR: Void-aware pressure routing for underwater sensor networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 895-908, 2012. doi: 10.1109/TMC.2012.53

[16] R. Zhang and Y. Zhang, "Wormhole-resilient secure neighbor discovery in underwater acoustic networks," *2010 Proceedings IEEE INFOCOM*, pp. 1-9, Mar. 2010. doi: 10.1109/INFCOM.2010.5462093

[17] F. Jan, N. Min-Allah, and D. Düştegör, "IoT-based smart water quality monitoring: Recent techniques, trends, and challenges for domestic applications," *Water*, vol. 13, no. 13, p. 1729, 2021. doi: 10.3390/w13131729

[18] N. Adam, M. Ali, F. Naeem, A. S. Ghazy, and G. Kaddoum, "A comprehensive survey of security schemes and privacy-preserving techniques for the internet of underwater things," *Communications*, vol. 1, no. 2, 2024. doi: 10.36227/TECHRXIV.171502698.82158311

[19] V. G. Menon and P. J. Prathap, "Comparative analysis of opportunistic routing protocols for underwater acoustic sensor networks," *2016 International Conference on Emerging Technological Trends (ICETT)*, pp. 1-5, Oct. 2016. doi: 10.1109/ICETT.2016.7873733

[20] M. T. Kheirabadi and M. M. Mohamad, "Greedy routing in underwater acoustic sensor networks: a survey," *Int. J. Distrib. Sens. Netw.*, vol. 9, no. 7, p. 701834, 2013. doi: 10.1155/2013/701834

[21] M. Chaudhary, N. Goyal, and A. Mushtaq, "Internet of underwater things: challenges, routing protocols, and ML algorithms," *Machine Learning Paradigm for Internet of Things Applications*, pp. 247-263, 2022. doi: 10.1002/9781119763499.CH13

[22] E. C. Liou, C. C. Kao, C. H. Chang, Y. S. Lin, and C. J. Huang, "Internet of underwater things: Challenges and routing protocols," *2018 IEEE International Conference on Applied System Invention (ICASI)*, pp. 1171-1174, Apr. 2018. doi: 10.1109/ICASI.2018.8394494

[23] S. M. Ghoreyshi, A. Shahrabi, and T. Boutaleb, "A stateless opportunistic routing protocol for underwater sensor networks," *Wireless Commun. Mob. Comput.*, vol. 2018, p. 8237351, 2018. doi: 10.1155/2018/8237351

[24] P. Qarabaqi and M. Stojanovic, "Modeling the large-scale transmission loss in underwater acoustic channels," *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 445-452, Sep. 2011. doi: 10.1109/ALLERTON.2011.6120201.

[25] R. Bu, S. Wang, and H. Wang, "Fuzzy logic vector-based forwarding routing protocol for underwater acoustic sensor networks," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 3, p. e3252, 2018. doi: 10.1002/ETT.3252.

[26] N. Nicolaou, A. See, P. Xie, J. H. Cui, and D. Maggiorini, "Improving the robustness of location-based routing for underwater sensor networks," *Oceans 2007-Europe*, pp. 1-6, Jun. 2007. doi: 10.1109/OCEANSE.2007.4302470.

[27] P. Xie, J. H. Cui, and L. Lao, "VBF: Vector-based forwarding protocol for underwater sensor networks," *NETWORKING 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems: 5th International IFIP-TC6 Networking Conference*, Coimbra, Portugal, May 15-19, 2006, Proc., vol. 5, pp. 1216-1221. Springer Berlin Heidelberg. doi: 10.1007/11753810_111

[28] Z. Wang, G. Han, H. Qin, S. Zhang, and Y. Sui, "An energy-aware and void-avoidable routing protocol for underwater sensor networks," *IEEE Access*, vol. 6, pp. 7792-7801, 2018. doi: 10.1109/ACCESS.2018.2805804

[29] Z. L. Li, N. M. Yao, and Q. Gao, "Relative distance-based forwarding protocol for underwater wireless sensor networks," *Applied Mechanics and Materials*, vol. 437, pp. 655-658, 2013. doi: 10.4028/WWW.SCIENTIFIC.NET/AMM.437.655

[30] R. W. Coutinho, A. Boukerche, L. F. Vieira, and A. A. Loureiro, "Geographic and opportunistic routing for underwater sensor networks," *IEEE Trans. Comput.*, vol. 65, no. 2, pp. 548-561, 2015. doi: 10.1109/TC.2015.2423677

[31] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, and M. N. K. Khattak, "SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 107419-107433, 2020. doi: 10.1109/ACCESS.2020.3000863

[32] F. Ahmed, Z. Wadud, N. Javaid, N. Alrajeh, M. S. Alabed, and U. Qasim, "Mobile sinks assisted geographic and opportunistic routing-based interference avoidance for underwater wireless sensor networks," *Sensors*, vol. 18, no. 4, p. 1062, 2018. doi: 10.3390/s18041062

[33] U. Ullah, A. Khan, S. M. Altowaijri, I. Ali, A. U. Rahman, V. V. Kumar, ... and H. Mahmood, "Cooperative and delay minimization routing schemes for dense underwater wireless sensor networks," *Symmetry*, vol. 11, no. 2, p. 195, 2019. doi: 10.3390/SYM11020195.