JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in e-ISSN: 3009-075X
AAN PUBLISHING

Volume 2 Issue 5

Article Number: 230100

Evaluating the Advantages and Challenges of Mobile Ad-Hoc Networks

Priya Poonia*and Laxmi Narayan Balai

Department of Electronics and Communication Engineering, Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India 301022

Abstract

Mobile Ad-Hoc Networks (MANETs) are decentralized assemblies of mobile nodes, including smartphones, laptops, iPads, and PDAs, that operate autonomously, contrasting with conventional wireless networks. These networks dynamically adapt their topology and routing tables as nodes join or leave, ensuring a seamless data packet transmission. This article aims to provide a comprehensive overview of MANETs, elucidating their advantages, challenges, and diverse applications. Unlike traditional networks that require a centralized administrator, MANETs enable mobile nodes to exchange data packets solely through wireless links. However, the volatile topologies and limited resources challenge establishing a power-efficient and secure routing system. This study introduces a reliable routing mechanism considering network power consumption and node reputation. Utilizing a Krill Herd-based Grasshopper Optimization Algorithm (KH-GOA), in conjunction with a reputation model, the proposed system establishes a trustworthy route between the origin and destination nodes. The reputation model considers node mobility, actual capabilities, historical performance, and peer reviews. Upon evaluating these reputation metrics, the KH-GOA method is employed, amalgamating the Krill Herd (KH) and Grasshopper Optimization Algorithm (GOA) techniques. The proposed KH-GOA-based routing protocol considers multi-objective criteria like reputation, power efficiency, distance, and latency for optimal route selection.

Keywords: Mobile Ad-Hoc Networks (MANETs); Routing Protocols; Krill Herd-Based Grasshopper Optimization Algorithm (KH-GOA); Network Topology; Data Packet Transmission

1 Introduction

Mobile Ad-Hoc Networks (MANETs) represent a critical component of the wireless networking ecosystem, enabling direct communication between mobile devices without the need for fixed infrastructure [1, 2]. As depicted in Figure 1, MANETs are a subset of ad-hoc networks that are especially relevant in scenarios where rapid deployment and dynamic reconfiguration are necessary [3, 4]. The dynamic nature of MANETs introduces complex routing challenges, addressed in this study through the evaluation of established protocols like DSR, TORA, and OLSR, as well as a proposed hybrid protocol, KH-GOA. This research fills a critical gap by providing an extensive comparative analysis of these protocols, revealing insights into their performance across various network densities—a key consideration for the deployment of MANETs in fields ranging from emergency response to military operations [5][6][7][8]. Preliminary findings indicate that the KH-GOA protocol may offer advancements in terms of energy efficiency and resilience to security threats, promising to enhance the robustness of MANETs significantly. This contribution is poised to influence future developments in ubiquitous computing, where reliable and efficient wireless communication is paramount [9][10][11][12][13][14].

*Corresponding author: priyapoonia94@gmail.com;

Received: 01 September 2023; **Revised:** 19 October 2023; **Accepted**: 31 October 2023; **Published:** 31 October 2023

DOI: 10.57159/gadl.jcmm.2.5.230100.

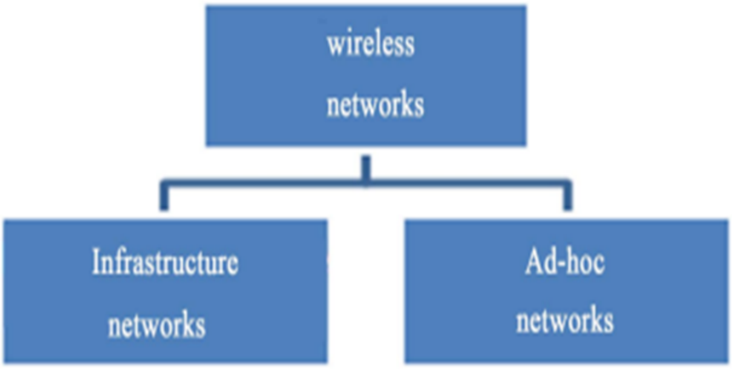


Figure 1: Classification of wireless networks into infrastructure and ad-hoc networks.

2 Methods

The aim of this research was to evaluate the efficacy of a novel hybrid routing protocol—referred to as KH-GOA—in Mobile Ad-Hoc Networks (MANETs), and to compare its performance against established protocols such as Dynamic Source Routing (DSR) [15, 16], Temporally Ordered Routing Algorithm (TORA) [17], and Optimized Link State Routing (OLSR) [18]. The performance metrics focused on in the study were not limited to traditional metrics such as WLAN delay, throughput, and network load, but also included advanced parameters like energy consumption, packet delivery, and end-to-end delay.

- Dynamic Source Routing (DSR)
- Temporally Ordered Routing Algorithm (TORA)
- Optimized Link State Routing (OLSR)
- Krill Herd based Grasshopper Optimization Algorithm (KH-GOA)

The evaluation was conducted using a MATLAB-based MANET simulation environment that allowed for the dynamic movement of nodes, reflecting the ever-changing topology of a real-world MANET. Node densities of 25, 50, and 75 were tested to assess scalability and performance under varied conditions.

Critical to the assessment of the hybrid KH-GOA protocol's performance were several key metrics:

- Energy Consumption: To evaluate the protocol's resource efficiency.
- Packet Delivery Ratio: To determine the reliability of the network communication.
- Throughput: To assess the data transmission capability.
- End-to-End Delay: To measure the latency from source to destination.
- Routing Overhead: To examine the additional protocol processing required for maintaining routes.

The simulations were particularly attuned to the behavior of malicious nodes, specifically black hole nodes, to determine the impact on network performance and the robustness of the routing protocol. The detection rate of such nodes was a crucial metric, showcasing the protocol's capacity for maintaining network security and integrity.

3 Results and Discussion

The statistical analysis conducted contradicts the prevailing notion that current strategies are more energy-intensive. Instead, the data indicates that the proposed KH-GOA method outperforms existing mechanisms, demonstrating its proficiency in efficiently managing the deployment of services. A critical evaluation in the presence of a flooding attack has been carried out, focusing on latency, detection rate, throughput, and energy consumption. Figure 2 offers a visual representation of the node distribution within a simulated network environment. The network spans a square region with dimensions of 100 meters on each side. Nodes are scattered throughout this area, indicating a non-uniform distribution which is characteristic of a realistic MANET environment. Notably, the nodes are labeled from 1 to 28, providing a clear reference for individual node analysis.

The simulation, as constructed, highlights the decentralized nature of MANETs and the necessity for nodes to operate without centralized control. The cyan node, labeled as node 27, is identified as a malicious entity introducing a false routing path. The spatial distribution suggests potential clusters where packet exchange might be more efficient and areas where connectivity may be sparse, necessitating multi-hop routing to achieve network-wide communication. Figure 2 thus, substantiates the dynamic topology that is a fundamental aspect of MANETs, and serves as a foundation for understanding the network behavior under various routing protocols and security threats.

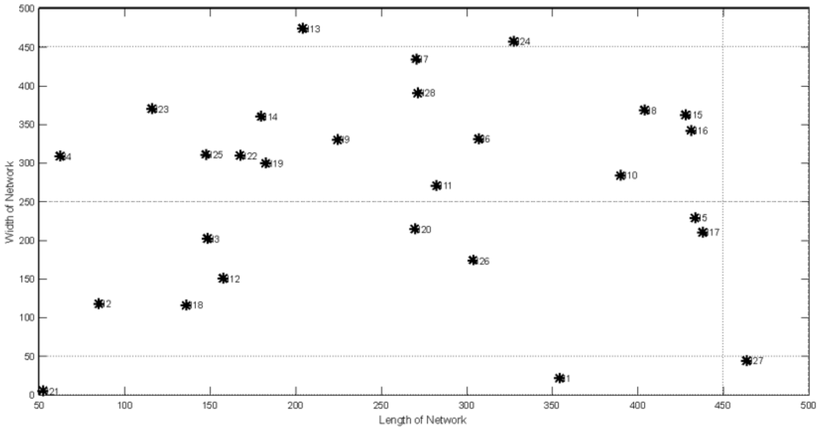


Figure 2: Node distribution in a 100m x 100m MANET simulation.

Figure 3 provides a detailed visualization of the network with an emphasis on the identification of a black hole node within a MANET. The network layout is consistent with the previous figure, maintaining a 100-meter square area. However, this figure uniquely identifies the black hole node, labeled 'BN' and depicted with a square, which is instrumental in simulating security attacks within the network. The positioning of 'BN' in relation to other nodes is crucial, as it represents the node's reachability and potential impact on the network's routing mechanisms. The dispersion of nodes illustrates the challenge in maintaining secure communications over a decentralized network, where any node could potentially become malicious. The simulation underscores the importance of robust security protocols that can detect and isolate such threats to preserve the integrity of data transmission within the network. This visualization is key to understanding how the proposed KH-GOA routing protocol adapts to dynamic conditions and mitigates security risks.

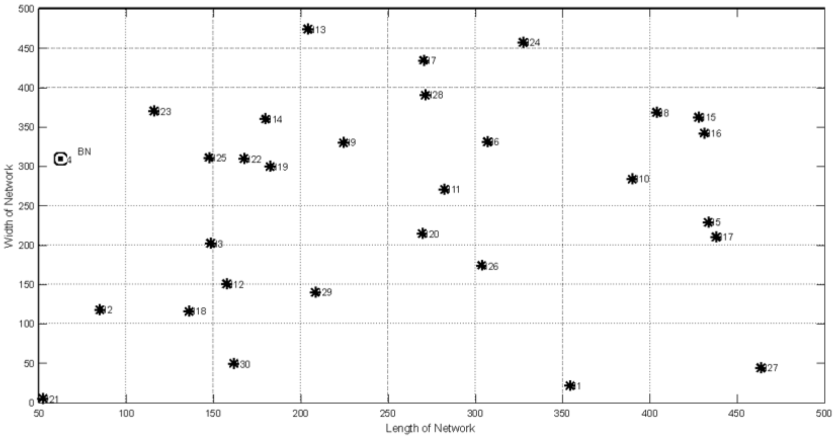


Figure 3: Visualization of the MANET with a focus on the malicious black hole node (BN).

Figure 4 expands the simulation scope, portraying a network extending 1000 meters in both length and width. The greater scale of the network showcases a more complex distribution of nodes, which simulates a more realistic and challenging MANET environment for routing and security protocols. Notably, certain nodes are circled, which may represent nodes of interest, possibly due to their strategic positioning or role within the network. The larger network space depicted here can be indicative of the increased complexity in maintaining efficient routing and communication protocols. Such a simulation is essential for stress-testing the proposed KH-GOA protocol against more demanding scenarios that reflect real-world applications. It provides a visual tool for identifying potential network vulnerabilities and the effectiveness of the protocol in managing a larger set of mobile nodes. Figure 5 offers a vivid illustration of the routing paths within the simulated MANET, highlighting the central node with red dashed lines radiating outward to other nodes. This central node, possibly a designated data packet distributor or a significant relay within the network, is shown to have direct routes to every other node within the network. The visual representation of these paths is crucial for understanding the underlying routing structure that supports data packet transmission across the network.

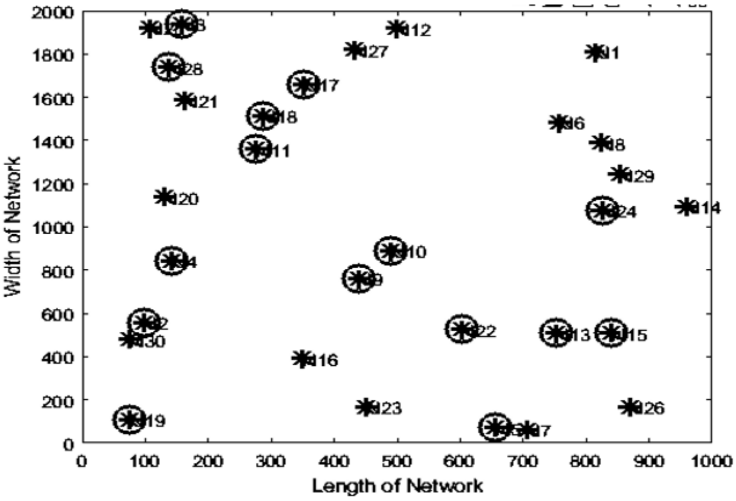


Figure 4: Expanded simulation of the MANET over a 1000m x 1000m area with strategic node placements highlighted.

The extensive connectivity from the central node underscores the importance of strategic node placement and the routing protocol's ability to dynamically adjust to the ever-changing topology of a MANET. Figure 5 is thus instrumental in visualizing the proposed KH-GOA protocol's efficiency in establishing and maintaining a robust communication framework, even in a large-scale and dense network environment.

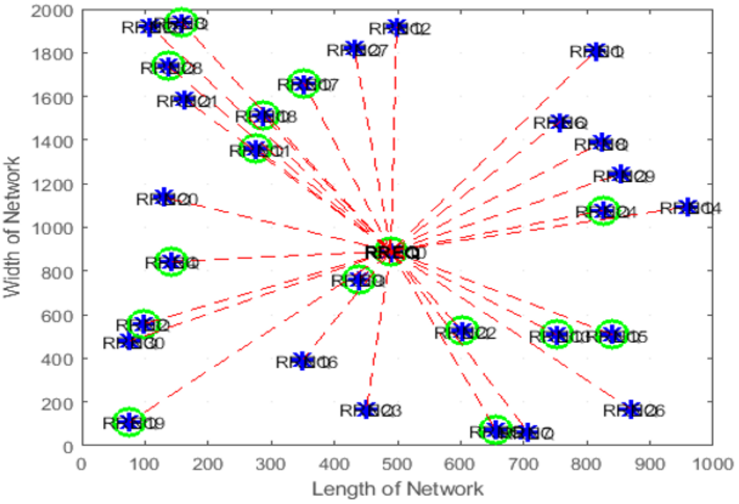
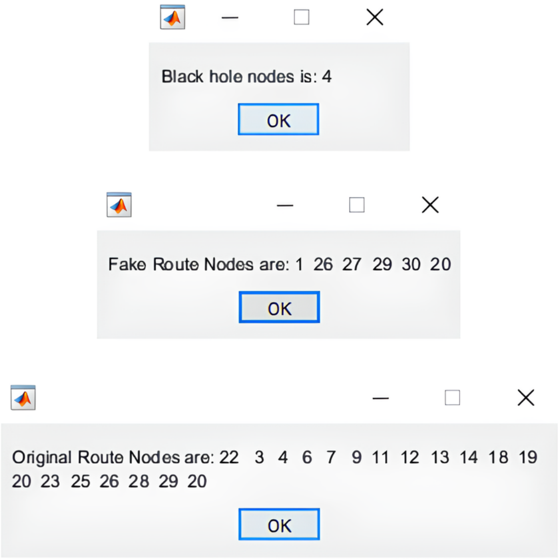


Figure 5: The routing paths in the MANET with a central node's connectivity to other nodes depicted by red dashed lines.

Figure 6 captures a critical component of the network simulation: the security alert dialogues. These dialogues are indicative of the simulation's ability to identify and categorize nodes based on their behavior and status within the network. The first dialogue box identifies a black hole node, which is crucial for security protocols to recognize and mitigate against potential threats. The second box lists nodes involved in a fake route, an essential feature for understanding the impact of malicious activities. Finally, the third box confirms the original route nodes, signifying the network's resilience and the ability of the routing protocol to restore the intended routing paths post-attack. These alerts provide a clear and user-friendly interface for monitoring the network's health and security, demonstrating the practicality of the proposed KH-GOA protocol in real-time threat detection and network recovery.

Figures 7a and 7b illustrate two key performance metrics of the hybrid routing protocol in a simulated MANET environment: energy consumption and packet delivery ratio. The energy consumption graph (Figure 7a) exhibits a nonlinear increase with the addition of routing nodes, showing an initial steep climb followed by a plateau. This suggests that the protocol maintains energy efficiency up to a moderate network size, beyond which the incremental energy cost per node decreases. Such a trend demonstrates the scalability of the protocol without significant energy penalties, reinforcing the protocol's applicability for large-scale networks where energy conservation is essential. Conversely, the packet delivery ratio graph (Figure 7b) demonstrates a significant improvement in efficiency as the network density increases, approaching the ideal delivery ratio of 1. This indicates that the protocol's packet delivery effectiveness scales well with network size, maintaining high reliability despite increased complexity. The ability to uphold a high packet delivery ratio is critical for effective communication in dynamic MANETs.

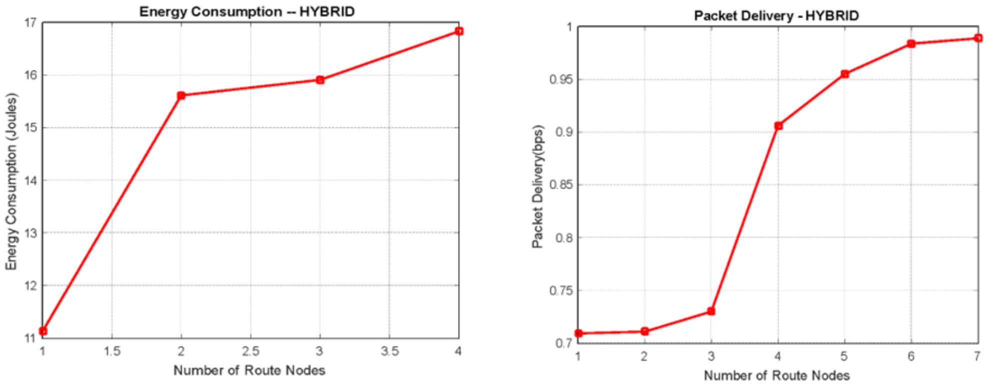


Black hole nodes is: 4

Fake Route Nodes are: 1 26 27 29 30 20

Original Route Nodes are: 22 3 4 6 7 9 11 12 13 14 18 19 20 23 25 26 28 29 20

Figure 6: Security alert dialogues from the simulation indicating black hole nodes, fake route nodes, and original route nodes.

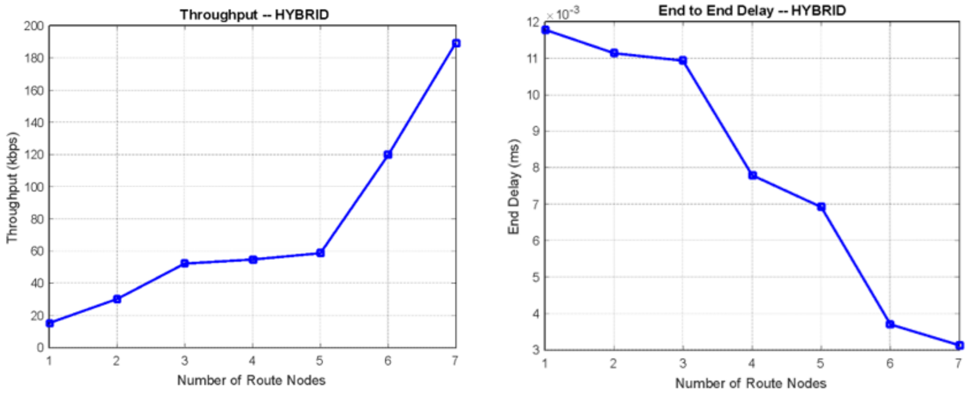


(a) Energy consumption as a function of routing nodes.

(b) Packet delivery ratio with increasing routing nodes.

Figure 7: Comparative performance metrics of the hybrid routing protocol.

The performance of the hybrid routing protocol within the simulated MANET is assessed through key metrics: network throughput and end-to-end delay, as illustrated in Figures 8a and 8b. The throughput graph shows a notable increase with more routing nodes, suggesting effective data transmission scaling. Concurrently, the end-to-end delay graph indicates latency minimization as the number of nodes increases, a testament to the protocol's efficiency.



(a) Network throughput in relation to the number of routing nodes.

(b) End-to-end delay as a function of the number of routing nodes.

Figure 8: Comparative analysis of network throughput and end-to-end delay in a hybrid routing protocol environment.

4 Conclusion

This study conducted an extensive evaluation of a novel hybrid routing protocol, KH-GOA, within the context of Mobile Ad-Hoc Networks (MANETs), comparing its performance with traditional routing protocols such as DSR, TORA, and OLSR. The results from the MATLAB-based simulations revealed that the KH-GOA protocol exhibited superior performance across various metrics. Notably, it demonstrated the lowest latency in data transmission, an optimized packet delivery ratio, and high throughput, even with increasing node densities. These attributes underscore its potential for application in dynamic and scalable network environments. Furthermore, the KH-GOA protocol showed remarkable energy efficiency, which is critical for the longevity and sustainability of MANETs. Its ability to maintain robust communication in the presence of malicious nodes, particularly black hole nodes, was also confirmed, highlighting its effectiveness in ensuring network security. In conclusion, the proposed KH-GOA routing protocol provides a promising solution to the challenges faced by MANETs, balancing efficiency, security, and performance. The findings suggest that it is well-suited for future wireless networks that require adaptive, scalable, and resilient routing mechanisms.

Declaration of Competing Interests

The authors declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any grants from governmental, private, or nonprofit funding bodies.

Author Contribution

Priya Poonia: Conceptualization, Writing – Original Draft Preparation ; **Laxmi Narayan Balai**: Methodology, Data Curation, Investigation, Validation, Writing - Reviewing and Editing.

References

[1] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, "Moving ad hoc networks—a comparative study," *Sustainability*, vol. 13, no. 11, p. 6187, 2021.

[2] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, eds., *Mobile ad hoc networking: cutting edge directions*. John Wiley & Sons, 2013.

[3] R. Ramdhany, P. Grace, G. Coulson, and D. Hutchison, "Manetkit: supporting the dynamic deployment and reconfiguration of ad-hoc routing protocols," in *Middleware 2009: ACM/IFIP/USENIX, 10th International Middleware Conference*, vol. 10, (Urbana, IL, USA), pp. 1–20, Springer Berlin Heidelberg, 2009.

[4] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad hoc networks*, vol. 1, no. 1, pp. 13–64, 2003.

[5] L. Raja and S. Santhosh Baboo, "An overview of manet: Applications, attacks and challenges," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 1, pp. 408–417, 2014.

[6] M. Chitkara and M. W. Ahmad, "Review on manet: characteristics, challenges, imperatives and routing protocols," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 2, pp. 432–437, 2014.

[7] S. Mohammad, M. Alsanabani, and T. Alahdal, "Comparison study of routing protocols in manet," *International Journal of Ad Hoc, Vehicular and Sensor Networks*, vol. 1, no. 1, pp. 1–9, 2014.

[8] A. Odeh, E. AbdelFattah, and M. Alshowkan, "Performance evaluation of aodv and dsr routing protocols in manet networks," *International Journal of Distributed and Parallel Systems*, vol. 3, no. 4, p. 13, 2012.

[9] S. M. Badhusha and K. Duraiswamy, "Energy efficient improved bandwidth video streaming through reliable multipath propagation in manets," *International Journal of Applied Engineering Research*, vol. 10, no. 13, 2015.

[10] G. S. Mamatha and D. S. Sharma, "Analyzing the manet variations, challenges, capacity and protocol issues," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 1, no. 1, pp. 14–21, 2010.

[11] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management*, vol. [volume missing], no. 2011, pp. 32–37, 2011.

[12] M. U. Aftab, A. Nisar, D. Asif, A. Ashraf, and B. Gill, "Rbac architecture design issues in institutions collaborative environment," *arXiv preprint arXiv:1310.5962*, 2013.

[13] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, and M. Irfan, "Attributed role based access control model," in *2015 Conference on Information Assurance and Cyber Security (CIACS)*, pp. 83–89, IEEE, 2015.

[14] R. Agrawal, N. Faujdar, C. A. T. Romero, O. Sharma, G. M. Abdulsahib, O. I. Khalaf, R. F. Mansoor, and O. A. Ghoneim, "Classification and comparison of ad hoc networks: A review," *Egyptian Informatics Journal*, 2022.

[15] Y. Cheng, E. K. Cetinkaya, and J. P. Sterbenz, "Dynamic source routing (dsr) protocol implementation in ns-3," in *Proceedings of the 5th international ICST conference on simulation tools and techniques*, pp. 367–374, 2012.

[16] S. A. Almazok and B. Bilgehan, "A novel dynamic source routing (dsr) protocol based on minimum execution time scheduling and moth flame optimization (met-mfo)," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, pp. 1–26, 2020.

[17] V. D. Park and M. S. Corson, "A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing," in *Proceedings Third IEEE Symposium on Computers and Communications. ISCC'98*, pp. 592–598, IEEE, 1998.

[18] T. Clausen and P. Jacquet, "Optimized link state routing protocol (olsr)," RFC RFC 3626, RFC Editor, 2003.