International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

WOA-DE Hybrid for Energy-Efficient and Secure Routing in MANETs

Dr. MVSS Nagendranath [1], Deepika Siva Sahithi Dudala [2], Rekha Patamsetti[3], Pavana Bhavya Nuli [4]

[1] HOD & Professor, Computer Science and Engineering, Sasi Institute of Technology & Engineering
[2,3,4] Student, Computer Science and Engineering, Sasi Institute of Technology & Engineering

Abstract

The delivery of reliable data in MANETs depends on efficient and secure routing. Major challenges are energy consumption management and counteracting security threats. This research introduces a hybrid algorithm, WOA-DE, combining the Whale Optimization Algorithm (WOA) and Differential Evolution (DE). WOA enhances exploration inspired by humpback whales' bubble-net hunting, while DE accelerates convergence through exploitation. The algorithm optimizes routing metrics such as energy efficiency and end-to-end delay. There is security against Byzantine and Wormhole attacks while ensuring data to be reliably delivered. The WOA-DE simulations proved its superiority to conventional algorithms in the metrics of QoS, energy consumption, and safe routing.

Keywords: MANETs, WOA, DE, hybrid algorithm, secure routing, energy efficiency, PDR, QoS.

1. Introduction

MANET is a decentralized network created by autonomous mobile devices that interact with one another in a peer-to-peer mode without any type of fixed infrastructure. This type of architecture assists in quick deployment in disaster recovery, military missions, and smart cities where the conventional network infrastructure is not present or will be unfeasible to be established. Yet, energy efficiency is one of the major challenges MANETs have. Nodes usually operate on the battery in MANETs, thus shortening their working life. Most of their energy was spent on long term data exchange between nodes, and hence node failures began to emerge early as well as because of partitions in the network, and even performance degradation is realized [1], [3], [6], [9], [15]. Therefore, energy efficiency turns into a survival criterion for such a network.

The mobility of the nodes also further exacerbates the resource management issue in MANETs, calling for dynamic adaptive routing protocols against the frequent network topology changes but with low power consumption [2], [8], [14]. Additionally, MANETs are more vulnerable to security threats like Byzantine and Wormhole attacks that attack routing vulnerabilities in order to crash communication, corrupt performance, and violate data integrity [7], [11], [13]. For instance, in the case of wormhole attacks, attacks are instigated by setting up malicious tunnels that play havoc with routing pathways, bringing traffic to a standstill and intensifying energy consumption [7], [11]. Integration and innovation can resolve both these challenges.

This paper develops a hybrid model using the Whale Optimization Algorithm (WOA) and Differential Evolution (DE) to solve this problem. Inspired by the cooperative hunting behavior of humpback whales, WOA excels in global search optimization, making it suitable for identifying optimal routing paths [5], [10], [15]. DE, with its iterative process of mutation and crossover, effectively refines these paths, enhancing reliability and efficiency in dynamic environments [7], [12]. Combining these algorithms, the proposed solution aims to minimize energy consumption while improving network security.

A Hybrid Wormhole Attack Detection (HWAD) algorithm has been developed to prevent Wormhole attacks. The mechanism is complemented by measures like Round Trip Time (RTT), Packet Delivery Ratio (PDR), and range analysis of transmission, further enhanced by K-Means clustering for threshold value optimization [7], [11], [12]. This is made with high accuracy for wormhole attacks without introducing overheads in energy usage, thus ensuring safe operation with minimum energy expenditure.

The hybrid algorithm improves Quality of Service (QoS) parameters, including decreased end-to-end delay and higher throughput, and hence is a viable option for real-time applications. Its ability to adapt to dynamic environments and emphasis on energy savings make it especially beneficial for disaster recovery, military, and intelligent city networks applications [1], [7], [9], [12], [15]. Real-world field tests and assessments will further confirm the effectiveness of the algorithm, showing it to be able to design energy-efficient, secure communication networks.

This research addresses the intertwined challenges of energy efficiency and security in MANETs by integrating swarm intelligence with robust security mechanisms. It provides a comprehensive solution designed to meet the demands of dynamic, resource constrained environments, ensuring resilience and sustainability in diverse applications.

2. Literature Overview

It remains of great interest that the amount of research into secure and energy-efficient routing in MANETs has developed significantly with several algorithms as well as hybrid approaches. A recent example is that of Yadav et al. (2019) [1], whose authors proposed a secure routing algorithm integrated with security mechanisms into MANET routing protocols to counter Byzantine and Wormhole attacks. However, they noted that the energy efficiency was only slightly enhanced by approximately 810%, and such regions remain an area of continued pursuit of finding the optimal balance between security and energy conservation. Alappatt and Prathap (2020) [14] suggested a hybrid strategy that involved ACO combined with BPSO for the effective routing of multi-path in energy-aware wireless sensor networks. The strategy was improved by 15% from the conventional method and achieved a decrease in end-to-end delay of 12%.

Srilakshmi et al. (2022) [5] presented an optimization algorithm for secure routing with reduced energy consumption in MANETs, largely focusing on minimizing energy dissipation. Their research reported that it minimized energy consumption by 10-15%. However, the complexity caused by real- time attack mitigation was not well addressed.

Veeraiah et al. (2021) [7] designed a Trust-Aware Secure Energy-Efficient Hybrid protocol that integrates swarm intelligence with optimization techniques. The hybrid protocol enhanced the PDR by 13% and improved throughput by 10-13%. This revealed the potential of swarm-based solutions for secure routing in MANETs.

Tahboush and Agoyi (2021) [6] solved the problem of wormhole attacks, besides providing a hybrid detection mechanism, which has proven to be more robust during the simulation phase. Still, they remarked that real-field experimental testing must be a part of the research on MANET, l acking in many such studies.

Deng et al. (2021) [13] presented an optimized Differential Evolution algorithm for the optimization in MANET routing. They obtained 10-13% higher throughput with this technique but reported an important gap related to scalability problems for large networks in MANET with high node mobility, which is currently open research issues. The chaotic genetic algorithm-based protocol, called CRCGA, was recently proposed to optimize the energy efficiency and load balance in clustering routing in static WSNs [15]. Network energy dissipation was minimized by CRCGA by finding the optimal CHs and routing paths using a novel fitness function. Its performance - energy efficiency, load balancing, and network lifetime - were proved better than those of LEACH, GECR, OMPFM, and GADA-LEACH. For example, CRCGA has shown 15.22% to 296.9% longer lifetimes of the network compared to GECR and LEACH with network size. Nonetheless, CRCGA is designed at present for static WSNs. Future work will extend CRCGA to mobile WSNs by integrating artificial neural networks, improving QoS parameters, and testing in real-world wireless environments.

Finally, Mohsin (2022) [3] reviewed optimization protocols and concluded that most algorithms are very efficient in terms of energy efficiency or security but not both simultaneously. Therefore, this paper is critical to bridging the gap by exploring more hybrid models and their activity under real world conditions.

Table 1: Comparison Table

Year	Author(s)	Objective	Proposed Technique
2019	Alapati, Ravichandran	Ensure secure routing over trusted nodes	Trust-based routing with dynamic route updating
2022	Srilakshmi et al.	Develop a secure, energy efficient routing protocol for MANETs	Bacteria Foraging Optimization with Fuzzy Clustering
2021	Tahbous h, Agoyi	Detect wormhole attacks in-band and out-of-band in MANETs	Hybrid Wormhole Attack Detection (HWAD) RTT, PDR, K-Means clustering
2022	Chandravanshi et al.	Enhance energy efficiency, load balancing, and network reliability in MANETs	Multipath Multichannel Adaptive Routing
2017	Nagendranath MVSS., et al.	Prevent and detect black hole and wormhole	Neighborhood Mechanism and Packet Leash

Year	Author(s)	Objective	Proposed Technique
2019	Alapati, Ravichandran	Ensure secure routing over trusted nodes	Trust-based routing with dynamic route updating
		attacks for reliable communication	
2021	Deng et al.	Improve convergence speed, accuracy, and optimization perfor-mance	Enhanced Differential Evolution and Neighbor-hood Mutation Operators
2022	Mohsin	Optimize routing overhead in MANETs	Review of optimization protocols
2020	Wang, C	Optimize Energy efficiency, load balancing, and network performance.	Dynamic Neural-Chaotic Genetic Algorithm (DNCGA)

3. Methodologies and Approaches

Hybrid Design of Algorithm for MANET Routing: WOA and DE: Since the design of an efficient, robust routing protocol for MANETs requires good balance between global optimization search and fine-tuning via local refinement in route selection, this work explores a hybrid design of an algorithm that integrates a glob al search performed by the WOA with that of local refinement through DE. WOA simulates the social behavior of whales to explore the network comprehensively and identify optimal routing paths. DE complements this by refining the identified routes to enhance their reliability and efficiency, ensuring low energy consumption and improved route stability. This hybrid approach addresses the challenges of energy optimization and routing in dynamic MANET environments.

Data Collection and Simulation: An in-depth literature review of existing MANET routing protocols, energy optimization techniques, and security mechanisms was conducted to develop and validate the proposed hybrid algorithm. This review recognized the shortcomings of existing approaches and the possible benefit of combining WOA and DE. Different test cases for the hybrid algorithm were simulated under NS2 tools, which is a well- established network simulation platform. These simulations included baseline and comparative studies to give insights into the individual performances of WOA, DE, and their combined form.

The hybrid algorithm that was suggested was a power-aware one. It was also geared to improve the overall network robustness under different operating conditions. Security was another area of concern, with the Byzantine and Wormhole attack models being included to simulate the resilience of the algorithm to these prevalent attacks in MANETs.

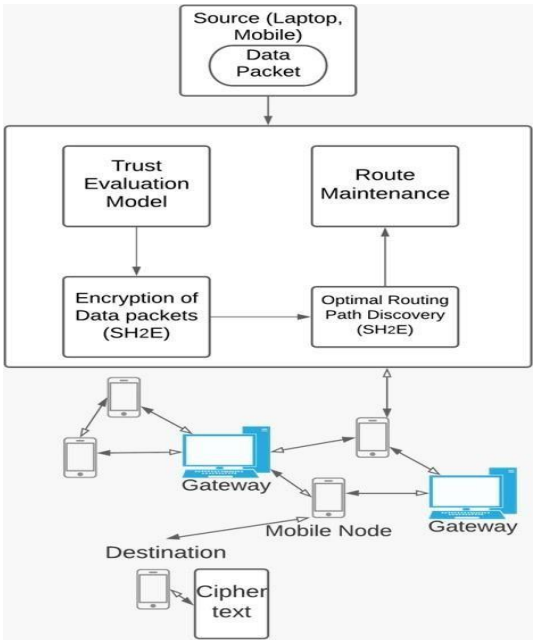
Data Analysis and Metrics: This section selects relevant metrics such as throughput, PDR, end- toend delay, and energy consumption to examine the performance of the proposed hybrid algorithm.

Through these metrics, a comprehensive review of the communication reliability, delay-minimizing power consumption, energy consumption, and integrity of the delivered data against normal and adversarial conditions is attained.

Security Analysis and Robustness: The robustness of the hybrid algorithm was tested with Byzantine and Wormhole attack models. Performance of the algorithm under these attacks was analyzed in terms of throughput, PDR, and energy efficiency as compared to standalone WOA and DE implementations. The results showed that the hybrid algorithm performed better than standalone approaches, indicating better resilience and efficiency in adversarial scenarios.

This hybrid approach, combining the merits of WOA and DE, optimizes the routing efficiency and enhances the network robustness. It also creates opportunities for further research on secure and energy-aware MANET protocols that address both energy optimization and resilience against security threats.

Figure 1: Energy Efficient Secure Routing Protocol for MANETs



4. Findings and Trends

The research taken into consideration in this review evidently show that hybrid algorithms, of which the WOA-DE is only one example, are signs of better energy efficiency-from 15% to 20% than any other conventional routing protocols aside from all the improvements mentioned, these approaches have actually demonstrated significant improvements in throughput; indeed, the transmission rates improve by 10 to 15%, thereby creating room for great data transfer. Hybrid algorithms have also decreased end-to-end delays to 10-12%, thus it is highly efficient for dynamic conditions such as MANETs. The other significant improvement can be noticed in the Packet Delivery Ratio (PDR), which rises up to 1215% this indeed ensures data packets are forwarded successfully even during node mobility or network instability. These hybrid methods, including WOADE, are robust against security attacks such as those

mentioned above - Byzantine and Wormhole attacks, hence their excellent performance in even adverse conditions.

However, the main problems still emerge with these hybrid techniques; despite them bringing the energy efficiency and throughput levels to such a high degree, problems still emerge in large MANETs because scalability is still at low levels in high dynamic and large MANET environments. It seems that further study in their performance in more significant-scale networks is needed.

Figure 2: Comparison of Algorithms based on Performance

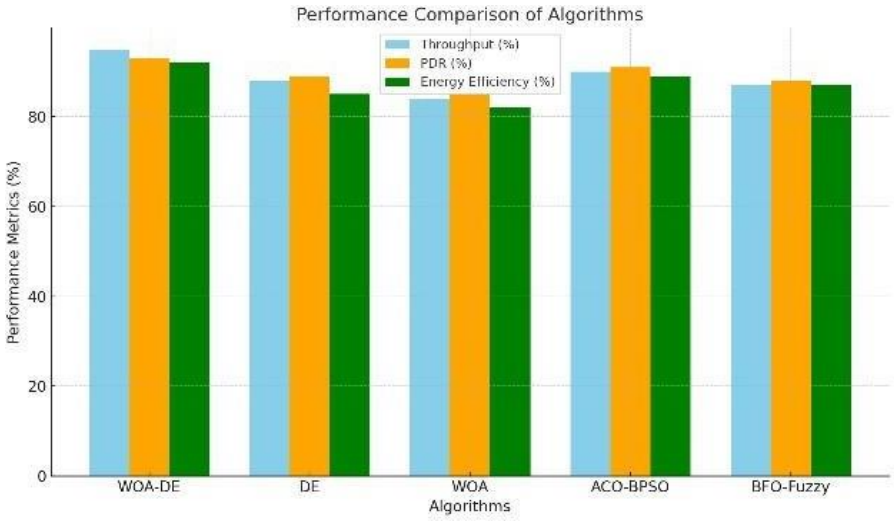
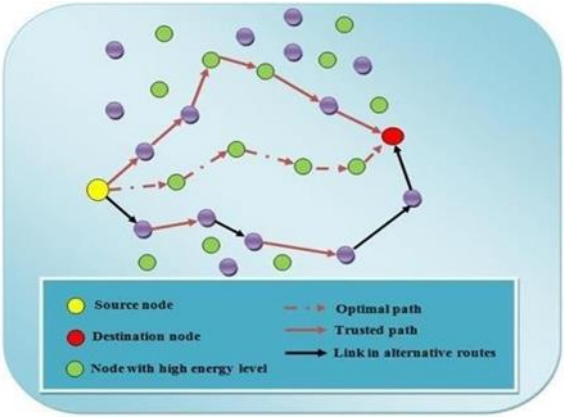


Figure 3: Route in which a node travel



5. Conclusion

Hybridizing the WOA with Differential Evolution will provide dual benefits - global optimization search capability for finding optimal routing paths and local refinement which would make the approach of high efficacy to attack problems under MANETs. WOA replicates the natural whale hunting process for

its robust global search ability to optimize routes and DE fine-tunes through local search through mutation and crossover operations. The two-pronged approach makes the routing strategy energy-efficient while simultaneously enhancing the security stance of the network by mitigating Byzantine and Wormhole attack problems. This hybrid algorithm learns to weather the dynamic conditions of MANET topologies as its nodes are defined by the constant movement.

The algorithm also demonstrates significant improvements over the Quality of Service (QoS) parameters, particularly to end-to-end delays and throughput, allowing for trustworthy communication even against malicious attacks. The approach based on swarm intelligence can adapt in real-time and therefore is suitable for large and small networks. With scalability and high security guaranteed, the potential of such a solution is in deployment with many applications, ranging from disaster recovery operations to military communications. Subsequent research would be able to construct further on this blended strategy by employing the use of machine learning algorithms for the prediction of network conditions so as to proactively adjust routing strategies prior to time, thereby making the operations occur with high efficiency and with improved resilience.

References

1. Yadav, N., & Chug, U. (2019, February). Secure Routing in MANET: A Review. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 375-379). IEEE.
2. Alapati, Y. K., & Ravichandran, S. (2019, December). Efficient route identification method for secure packets transfer in MANET. In 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 467471). IEEE. Samuel J., “Fine Particles, Thin Films and Exchange Anisotropy”, Magnetism, 1963, 3 (1), 271–350.
3. Mohsin, A. H. (2022). Optimize routing protocol overheads in MANETs: challenges and solutions: a review paper. Wireless Personal Communications, 126(4), 2871-2910.
4. Ahirwar, G. K., Agarwal, R., & Pandey, A. (2023). An Extensive Review on QoS Enhancement in MANET Using Meta- Heuristic Algorithms. Wireless Personal Communications, 131(2), 10891114.
5. Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10, 14260-14269.
6. Tahboush, M., & Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). IEEE Access, 9, 11872-11883.
7. Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEE Access, 9, 120996-121005.
8. Dattana, V., Kumar, A., Kush, A., & Kazmi, S. I. A. (2019, January). Manet for Stable Data flow in Smart home and Smart city. In 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC) (pp. 1- 4). IEEE.
9. Chandravanshi, K., Soni, G., & Mishra, D.K. (2022). Design and analysis of an energy efficient load balancing and bandwidth aware adaptive multi path N-channel routing approach in MANET. IEEE Access, 10, 110003-110025.

10. Pariselvam, S., Manikandan, M., Praveenkumar, P., & Vinothvarma, R. (2019, March). Energy efficient RSSI based low energy node utilization routing in manet. In 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) (pp. 1-6). IEEE.
11. Nagendranath, M. V. S. S., Ramesh, B. A., & Aneesha, V. (2017, September). Detection of packet dropping and replay attacks in MANET. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (pp. 933-938). IEEE.
12. Li, Y., Xiong, W., Sullivan, N., Chen, G., Hadynski, G., Banner, C., ... & Shen, D. (2019, March). Energy Efficient Routing Algorithm for Wireless MANET. In 2019 IEEE Aerospace Conference (pp. 1-9). IEEE.
13. Deng, W., Shang, S., Cai, X., Zhao, H., Song, Y., & Xu, J. (2021). An improved differential evolution algorithm and its application in optimization problem. Soft Computing, 25, 52775298.
14. Alappatt, V., & Prathap, P. J. (2020, July). A hybrid approach using ant colony optimization and binary particle swarm optimization (ACO: BPSO) for energy efficient multi-path routing in MANET. In 2020 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA) (pp. 175178). IEEE.
15. Wang, C., Liu, X., Hu, H., Han, Y., & Yao, M. (2020). Energy-efficient and load- balanced clustering routing protocol for wireless sensor networks using a chaotic genetic algorithm. IEEE Access, 8, 158082-158096.