# Detection and prevention of Sybil attacks in Optimized Link State Routing protocol for Mobile Ad-Hoc Networks

[1]Cecilia Agunbiade, [2]Funmilola Ipeayeda, [3]Adeleye Falohun, [4]Oladayo Olakanmi and [5]John Ogunyode
[1234]Computer Science department, Ajayi Crowther University Oyo, Oyo state, Nigeria.
[5]Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria.
zion278agunbiade@gmail.com|fw.ipeayeda@acu.edu.ng |asfalohun@lautech.edu.ng |dayoolakanmi@gmail.com
|almightyjasio@gmail.com

Received: 14-JAN-2026; Reviewed: 30-MARCH-2026; Accepted: 01-AUGUST-2026
https://dx.doi.org/10.46792/fuoyejet.v11i3.1515

**ORIGINAL RESEARCH**

**Abstract**— Mobile Ad Hoc Networks (MANETs) are decentralized and infrastructure-less wireless networks characterized by dynamic topology and limited resources, making them highly susceptible to security threats such as Sybil attacks. The Optimized Link State Routing (OLSR) protocol, widely used for its proactive routing and Multi-Point Relay (MPR) efficiency, is particularly vulnerable to such attacks, where malicious nodes assume multiple identities to disrupt routing operations. This study proposes an enhanced OLSR protocol integrated with an Improved Grey Wolf Optimizer (IGWO) for effective detection and mitigation of Sybil attacks. In the proposed model, the IGWO algorithm is applied to optimize route selection and detect malicious nodes by modeling network nodes as search agents and evaluating their trustworthiness based on routing behavior, neighborhood consistency, and message exchange patterns. Specifically, HELLO and Topology Control (TC) messages are analyzed to identify anomalies associated with Sybil identities, while the IGWO dynamically selects optimal routing paths by prioritizing trustworthy nodes. The model was implemented and simulated in MATLAB under varying node mobility and packet sizes. Performance evaluation was conducted using packet delivery ratio (PDR), throughput, and end-to-end delay. Simulation results show that the proposed IGWO-OLSR protocol significantly outperforms the conventional OLSR protocol, achieving higher throughput (up to 20,570 Kbps), improved packet delivery ratio (up to 0.967), and reduced end-to-end delay, particularly under high mobility conditions. These results demonstrate that the integration of the Grey Wolf Optimizer enhances routing efficiency, improves detection of Sybil attacks, and strengthens overall network security. The proposed approach provides a robust and adaptive framework for securing routing protocols in dynamic MANET environments.

**Keywords**— Mobile Ad hoc Networks, Sybil attack detection, Optimized Link State Routing, Optimization Techniques, Improved Grey Wolf Optimizer.

## 1 INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are decentralized and infrastructure-less wireless networks in which nodes function as both data sources and routers. Their flexibility and self-organizing nature make them highly suitable for critical applications such as military communication, disaster recovery, vehicular networks, and sensor-based systems (Abolhasan et al., 2009). However, because MANETs rely heavily on cooperation among nodes and lack centralized control, they are highly vulnerable to security threats that can severely affect network reliability and performance.

One of the most critical and widely studied security threats in MANETs is the Sybil attack, in which a malicious node assumes multiple false identities within the network. These fake identities allow the attacker to manipulate routing decisions, distort topology information, and undermine trust mechanisms (Douceur, 2002). As a result, key performance metrics such as packet delivery ratio, throughput, accuracy, and end-to-end delay are significantly degraded, threatening the overall integrity and functionality of the network.The Optimized Link State Routing (OLSR) protocol is a proactive routing protocol widely used in MANETs due to its efficiency in reducing routing overhead through the use of Multi-Point Relays (MPRs) (Clausen and Jacquet, 2003). However, OLSR is particularly susceptible to Sybil attacks because malicious nodes can exploit the MPR selection mechanism by assuming multiple identities. This allows attackers to influence routing decisions, inject false topology information, and disrupt network communication (Huhtonen, 2022).

Existing solutions for mitigating Sybil attacks in OLSR primarily rely on cryptographic techniques, fixed threshold mechanisms, and resource-testing approaches. While cryptographic methods provide strong identity verification, they introduce significant computational and communication overhead, making them unsuitable for resource-constrained MANET environments. Similarly, threshold-based approaches lack adaptability and may fail under highly dynamic network conditions, while resource-testing techniques are often inefficient against intelligent or coordinated attackers. These limitations highlight the need for a lightweight, adaptive, and intelligent detection mechanism capable of operating effectively in dynamic MANET environments.

To address these challenges, this study proposes an enhanced OLSR protocol integrated with an Improved

Corresponding Author: zion278agunbiade@gmail.com; (+234)8036284310
**Section B-** ELECTRICAL/COMPUTER ENGINEERING and RELATED SCIENCES
**Can be cited as:**
Agunbiade C. B., Ipeayeda F. W., Falohun A. S., Olakanmi O. O. and Ogunyode J. O. (2026). Detection and prevention of Sybil attacks in Optimized Link State Routing protocol for Mobile Ad-Hoc Networks. FUOYE Journal of Engineering and Technology (FUOYE**JET**), **11(3), 373-378.** https://dx.doi.org/10.46792/fuoyejet.v11i3.1515

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

Grey Wolf Optimizer (GWO) for Sybil attack detection. GWO is a bio-inspired metaheuristic algorithm that mimics the leadership hierarchy and hunting behavior of grey wolves, enabling adaptive optimization and efficient decision-making (Mirjalili et al., 2014). By embedding the improved GWO into OLSR, the proposed approach enhances detection accuracy, reduces false classifications, and improves overall network security and routing stability in MANET environments. This work contributes to the advancement of secure routing solutions in MANETs and provides a foundation for future research on intelligent intrusion detection in wireless ad hoc networks.

## 2 LITERATURE REVIEW

### 2.1 An Overview of Wireless Networking

Wireless networking enables communication without physical connections and forms the foundation of technologies such as Wi-Fi, Bluetooth, and cellular systems. In the context of Mobile Ad Hoc Networks (MANETs), wireless communication allows nodes to dynamically self-organize without centralized infrastructure. Variants such as Vehicular Ad Hoc Networks (VANETs) and Flying Ad Hoc Networks (FANETs) extend these capabilities to transportation and aerial systems. However, the decentralized nature of these networks introduces significant security challenges, particularly in routing and identity management (Yen and Chou, 2021; Akyildiz et al., 2020). Wireless networks use radio frequency signals to provide flexibility, mobility, and scalability, making them suitable for both structured infrastructure-based networks and decentralized infrastructure-less networks. In particular, wireless ad hoc networks operate without centralized control, allowing nodes to self-organize and act as both hosts and routers, which is especially valuable in dynamic and emergency scenarios (Wagner, 2021). Ongoing developments in emerging technologies such as 5G, mesh networking, and satellite communications continue to expand the capabilities and impact of wireless networking, reinforcing its role as a critical enabler of global connectivity and modern digital systems (Siau and Shen, 2020).

### 2.2 Overview of Mobile Ad Hoc Network (MANETs)

Mobile Ad Hoc Networks (MANETs) are decentralized wireless networks where nodes act as both hosts and routers, communicating without fixed infrastructure. Their dynamic topology, scalability, and quick deployment make them ideal for military operations, disaster recovery, vehicular networks, and sensor systems (Conti and Giordano, 2014; Sarkar et al., 2013). MANETs rely on multi-hop routing, which extends network connectivity but also introduces challenges such as increased routing complexity, energy consumption, and vulnerability to security attacks. Protocols like OLSR provide low-latency routes but are vulnerable to attacks. While flexible and cost-effective, MANETs require robust routing and security mechanisms for reliable operation.

### 2.3 Classification of Attacks in Mobile Ad Hoc Network (MANETs)

Attacks on Mobile Ad Hoc Networks (MANETs) target either the data being transmitted or the network's control mechanisms. Data attacks include eavesdropping, packet dropping, jamming, and energy depletion, which disrupt communication or drain node resources (Aljohani, 2021). Control attacks, such as Sybil, DoS, location tracking, and hello flood attacks, manipulate routing, trust, or network management to degrade performance (Newsome et al., 2004). Conventional detection methods often fail to effectively mitigate these attacks due to the dynamic topology and decentralized structure of MANETs, which limit the effectiveness of static or centralized security mechanisms.

### 2.4 Overview of Routing Protocols for MANETs

Routing protocols in Mobile Ad Hoc Networks (MANETs) are designed to ensure efficient communication despite frequent topology changes and limited resources. They are generally classified into proactive, reactive, and hybrid protocols. Proactive protocols, such as Optimized Link State Routing (OLSR) and Destination-Sequenced Distance Vector (DSDV), maintain up-to-date routing tables, enabling immediate packet delivery but at the cost of high overhead and energy consumption (Perkins and Bhagwat, 1994). Reactive protocols, such as Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), establish routes on demand, reducing overhead and saving energy, though route discovery may introduce delays (Johnson and Maltz, 1996). Hybrid protocols, exemplified by the Zone Routing Protocol (ZRP), combine proactive and reactive strategies, dividing the network into zones to balance efficiency, scalability, and adaptability (Haas et al., 2002). Together, these protocols address the challenges of dynamic and infrastructure-less MANETs, with each type offering trade-offs between speed, resource use, and network overhead.

### 2.5 Optimized Link State Routing Protocol

The Optimized Link State Routing (OLSR) protocol is a proactive, table-driven routing protocol designed for mobile ad hoc networks, where nodes act as both hosts and routers. OLSR reduces control message overhead by selecting a subset of neighbors, called Multi-Point Relays (MPRs), to forward topology information, enabling efficient multi-hop communication and fast route convergence (Zhang, 2019). Its benefits include scalability, loop-free routing, adaptability to changing network conditions, and support for Quality-of-Service requirements (Wang, 2021). However, OLSR is vulnerable to security threats such as spoofing, denial-of-service, routing table poisoning, eavesdropping, resource exhaustion, and Sybil attacks, which exploit its reliance on neighbor information to manipulate network topology

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://.doi.org/10.46792/fuoyejet.v11i3.1515 engineering.fuoye.edu.ng/journal

and routing decisions (Qayyum, 2019). Despite these risks, OLSR remains widely used for its efficiency and reliability in dynamic, infrastructure-less network environments.

### 2.6 Sybil Attacks and classification

In Mobile Ad Hoc Networks (MANETs), Sybil attacks represent a serious threat to network integrity, where a malicious node assumes multiple fake identities to disrupt communication, consume resources, and spread false routing information (Xiaohui, 2020). These attacks can be classified as single Sybil attacks, involving one malicious node intercepting or dropping packets, or cooperative Sybil attacks, where multiple nodes coordinate to amplify the impact and evade detection (Neeraj, 2021). In protocols like OLSR, Sybil nodes manipulate routing by broadcasting false link-state information, creating routing loops, isolating nodes, or degrading overall performance, thereby undermining trust and network reliability. Detecting such attacks requires behavioral monitoring, routing pattern analysis, and cryptographic safeguards to protect the integrity and stability of MANET communication.

### 2.7 Optimization Techniques and the Grey Wolf Optimizer (GWO)

Optimization techniques like Genetic Algorithms, Particle Swarm Optimization, and Simulated Annealing efficiently solve complex problems across engineering and computer science (Vecchi, 2022). The Grey Wolf Optimizer (GWO), inspired by grey wolf hunting behavior, offers simplicity, scalability, and robustness, with improved variants enhancing convergence and accuracy (Mirjalili et al., 2014). While widely used in engineering and feature selection, GWO also shows promise in securing and optimizing routing in Mobile Ad Hoc Networks (MANETs). Integrating GWO with protocols like OLSR can improve routing efficiency, resilience, and protection against attacks such as Sybil attacks in dynamic, infrastructure-less networks (Mahdy et al., 2021).

### 2.8 Review of Sybil Attack Detection Techniques in MANETs

Several techniques have been proposed to detect Sybil attacks in MANETs. Trust-based approaches evaluate node behavior to identify malicious activities; however, they often suffer from high false positive rates in highly dynamic MANET environments. Cryptographic techniques provide strong identity verification but introduce significant computational overhead, making them unsuitable for resource-constrained MANETs. Machine learning-based approaches improve detection accuracy but require large training datasets and may not adapt effectively to rapidly changing network conditions. In OLSR-based networks, most detection mechanisms rely on monitoring HELLO and Topology Control (TC) messages to identify inconsistencies in node behavior. While these methods can detect abnormal routing patterns, they often lack adaptability and fail to optimize routing performance simultaneously. Therefore, there is a need for an intelligent and adaptive approach that integrates optimization techniques with routing protocols to enhance both security and performance. This gap motivates the integration of the Grey Wolf Optimizer in this study.

## 3 METHODOLOGY

### 3.1 Research Approach

The research implements and evaluates the Optimized Link State Routing (OLSR) protocol enhanced with the Grey Wolf Optimizer (GWO) at the data link layer using MATLAB on a Windows 11 platform. The GWO algorithm was adapted to detect Sybil attacks and integrated into OLSR to create a modified protocol capable of mitigating such threats. Two simulations were conducted for performance comparison: one with conventional OLSR and another with the GWO-enhanced OLSR. Using 50 randomly generated mobile nodes, the simulations were executed in MATLAB, and the modified protocol was evaluated based on packet delivery ratio, throughput, and end-to-end delay. The simulations were conducted within a 1000 m × 1000 m network area using 50 mobile nodes. Node mobility followed the Random Waypoint Mobility Model with node speeds ranging from 2 m/s to 20 m/s. The simulation time was set to 100 seconds, and each node had a transmission range of 250 m. Constant Bit Rate (CBR) traffic was used with packet sizes varying from 512 bytes to 8192 bytes. The IEEE 802.11 MAC protocol was adopted. To evaluate security performance, both single and cooperative Sybil attack scenarios were introduced into the network.

### 3.2 Design of Grey Wolf Optimizer based Optimized Link State Routing (OLSR) Protocol

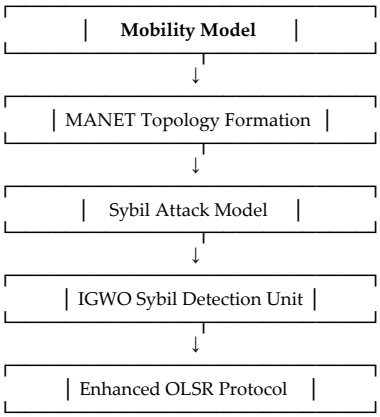


Fig. 1. System Architecture of the Implemented IGWO-OLSR Routing Protocol

The implemented technique enhances the Optimized Link State Routing (OLSR) protocol in MANETs by integrating a modified Grey Wolf Optimizer (GWO) to detect and mitigate Sybil attacks. The system first models network topology and simulates potential Sybil attacks, after which the improved GWO algorithm identifies key nodes, alpha, beta, delta, and omega, based on their positions relative to the attacker. Nodes are grouped into sub-packs

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

to collaboratively encircle and monitor malicious activity, with parameters dynamically updated to adapt to network conditions. This adaptive mechanism allows the algorithm to efficiently explore and exploit routing paths, optimize communication, and enhance network stability and resilience. The overall framework, illustrated in Figure 1, demonstrates how the IGWO-OLSR protocol proactively secures routing while maintaining efficient data transmission in dynamic and infrastructure-less MANET environments.

### 3.3 Modified OLSR protocol

The modified OLSR protocol integrates the Grey Wolf Optimizer (GWO) through a trust-based routing optimization mechanism. In this approach, each network node is treated as a search agent within the GWO framework. A fitness function is defined based on node behavior, including packet forwarding reliability, neighbor consistency, and validity of HELLO and Topology Control (TC) messages. During optimization, nodes are ranked into alpha, beta, delta, and omega categories according to their fitness values. Nodes with higher trust values (alpha, beta, and delta) are preferred for routing decisions, particularly in the selection of Multi-Point Relays (MPRs), while nodes exhibiting suspicious behavior are classified as omega and excluded from routing activities. The GWO algorithm iteratively updates node trust values and routing decisions, enabling the detection and isolation of Sybil nodes. This integration ensures that the optimization process directly influences OLSR routing operations, thereby improving network security, stability, and performance.

### 3.4 Implementation of the designed Routing Protocol

The OLSR routing protocol was implemented in MATLAB with a modified Grey Wolf Optimizer to optimize its parameters. The network topology, node positions, and protocol settings were defined, and the GWO iteratively adjusted routing decisions until a stopping criterion was met. The optimized protocol was then simulated to evaluate its performance and effectiveness in improving MANET routing.

### 3.5 Performance Evaluation

During the evaluation, several key metrics were taken into account, including the packet delivery ratio, end-to-end delay, and throughput. This is to determine how well the Grey Wolf-OLSR method performed in comparison to the standard protocols. These performance metrics are calculated using the following formulas:

**Packet delivery ratio (PDR):** The Packet Delivery Ratio (PDR) is a metric that provides valuable insights into the efficacy of a network protocol in delivering packets reliably to their destinations. It quantifies the ratio of the number of successfully delivered packets to the total number of packets generated. It is calculated using:

$$PDR = \frac{Total\ Number\ of\ packet\ received}{Total\ Number\ of\ packets\ sent} \times 100\% \quad (1)$$

**End-to-end delay:** End-to-End Delay is a crucial metric used to measure the time it takes for a packet to travel from the source node to the destination node. It serves as an important indicator of the overall delay experienced by packets in a network. A lower End-to-End Delay indicates better performance, reflecting faster packet delivery, and a higher level of efficiency in the network. It is calculated using:

$$End\ to\ End\ Delay = \frac{\sum Packets\ Arrival\ Time - Transmission\ Time}{\sum Connections} \quad (2)$$

**Throughput:** Throughput is a term used to describe the amount of data that is transmitted successfully across a network within a given period of time. It is calculated by dividing the total amount of data that was successfully transmitted by the total time it took to transmit it.

$$Throughput = \frac{\sum Received\ Packets}{Time} \quad (3)$$

## 4 RESULTS AND DISCUSSION

### 4.1 Presentation of Results

The modified OLSR protocol was assessed using Packet Delivery Ratio (PDR), Throughput, and End-to-End Delay, and compared to the standard OLSR protocol to gauge its effectiveness in mitigating Sybil attacks in a Mobile Ad Hoc Network (MANET). The packet size varied from 512 bytes to 8192 bytes. The simulation's graphical user interface is depicted in Figure 2, while Figure 3 showcases the network topology with 50 nodes initialized in random positions. Graphical representations of the results are also included to illustrate performance trends across varying node speeds. These plots provide a clearer comparison between the standard OLSR and the proposed IGWO-OLSR protocol.

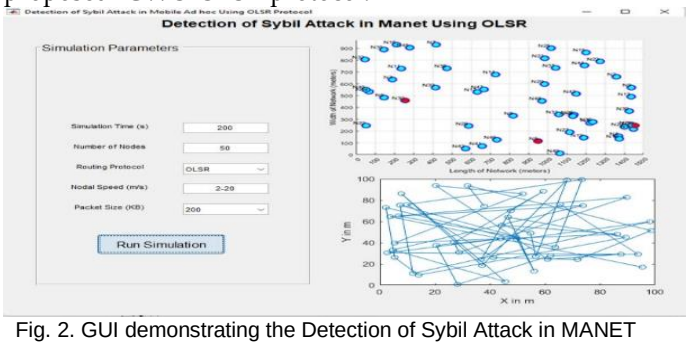


Fig. 2. GUI demonstrating the Detection of Sybil Attack in MANET using OLSR

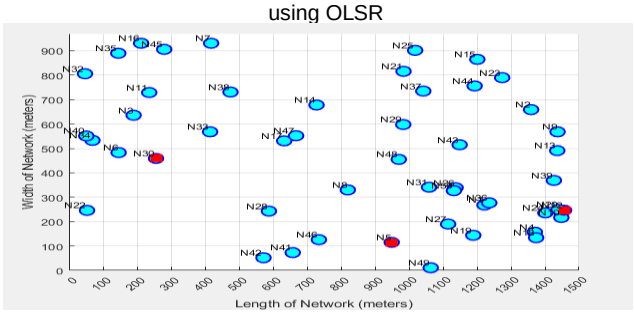


Fig. 3. showcases the network topology with 50 nodes initialized in random positions

### 4.2 Throughput Results

The throughput results in Table 1 clearly indicate that the Improved GWO-OLSR protocol consistently outperforms the standard OLSR under all tested network conditions.

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://.doi.org/10.46792/fuoyejet.v11i3.1515 engineering.fuoye.edu.ng/journal

At low mobility and small packet sizes, GWO-OLSR already achieves noticeably higher throughput, and this advantage is maintained as nodal speed and packet size increase. As the network becomes more dynamic, the performance gap between the two protocols widens, showing the improved protocol's ability to efficiently handle higher mobility and larger data transmissions. This enhanced performance can be attributed to the Grey Wolf Optimizer's effective route optimization, which reduces packet loss and routing overhead. Overall, the results confirm that GWO-OLSR offers better scalability and data transmission efficiency, making it more suitable for high-speed and data-intensive MANET environments. The graphical results, as shown in Figure 4, further reveal that throughput increases steadily with node speed for both protocols; however, the IGWO-OLSR protocol exhibits a steeper growth rate. This indicates its superior adaptability to dynamic network conditions, as it maintains efficient route selection even under high mobility.

Table 1. Results for the throughput comparison

| Nodal Speed (m/s) | Packet Size (bytes) | OLSR (%) | Improved GWO-OLSR (%) |
|---|---|---|---|
| **2** | 512 | 0.862 | 0.897 |
| **5** | 1024 | 0.884 | 0.911 |
| **10** | 2048 | 0.906 | 0.925 |
| **15** | 4096 | 0.928 | 0.939 |
| **20** | 8192 | 0.936 | 0.967 |

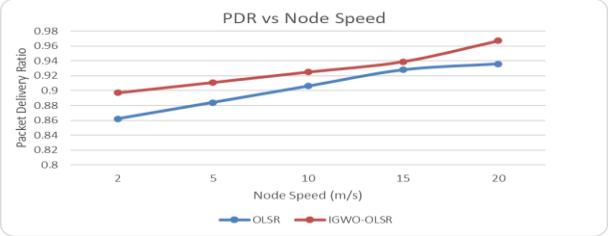


Fig. 4. Throughput vs Node Speed for OLSR and IGWO-OLSR

### 4.3 Packet Delivery Ratio (PDR) Analysis of OLSR and Improved GWO-OLSR Protocols

The Packet Delivery Ratio (PDR) results in Table 2 show that the Improved GWO-OLSR protocol consistently outperforms the standard OLSR across all tested nodal speeds and packet sizes. While both protocols demonstrate improved PDR as network conditions scale, GWO-OLSR maintains a clear advantage, delivering a higher percentage of packets at each stage. This performance gap becomes more noticeable at higher node speeds and larger packet sizes, where network dynamics are more challenging. The improved protocol's ability to optimize routing decisions and suppress the impact of disruptive behaviors enables more reliable packet delivery, confirming its effectiveness and suitability for highly dynamic MANET environments. From the graphical analysis as shown in Figure 5, it is evident that while both protocols improve in packet delivery ratio as network conditions scale, IGWO-OLSR consistently maintains a higher curve. This demonstrates its ability to sustain reliable communication by effectively mitigating the impact of Sybil attacks, especially at higher node speeds.

Table 2. Packet Delivery Ratio (PDR)

| Nodal speed (m/s) | Packet Size (bytes) | OLSR | Improved GWO-OLSR |
|---|---|---|---|
| **2** | 512 | 3000 | 4500 |
| **5** | 1024 | 6000 | 6600 |
| **10** | 2048 | 10500 | 11500 |
| **15** | 4096 | 13500 | 15060 |
| **20** | 8192 | 18000 | 20570 |

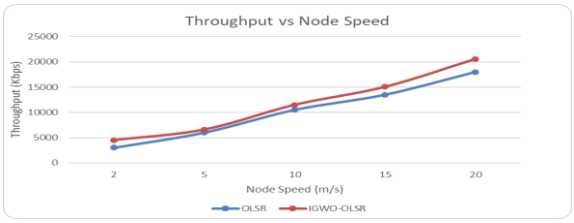


Fig. 5. Packet Delivery Ratio vs Node Speed for OLSR and IGWO-OLSR

### 4.4 End-to-End Delay Analysis of OLSR and Improved GWO-OLSR Protocols

The end-to-end delay results, summarized in Table 3, clearly show that the Improved GWO-OLSR protocol consistently outperforms the standard OLSR across all tested network conditions. At low node speeds and smaller packet sizes, both protocols exhibit comparable delays, with GWO-OLSR showing a slight improvement. However, as node mobility and packet size increase, the performance gap becomes more evident. While the delay in standard OLSR rises sharply due to increased congestion and inefficient routing, GWO-OLSR maintains significantly lower delays by selecting more stable and secure routes. Even at the highest speed and largest packet size, GWO-OLSR effectively controls transmission delay, demonstrating its robustness and efficiency in handling dynamic and high-traffic MANET environments. The delay graph as shown in Figure 6, shows a sharp increase for the standard OLSR as node speed rises, whereas IGWO-OLSR maintains a relatively gradual increase. This confirms that the proposed method successfully minimizes routing instability and congestion, resulting in faster packet delivery even in highly dynamic scenarios.

Table 3. End-to-End delay

| Nodal Speed (m/s) | Packet Size (bytes) | OLSR | Improved GWO-OLSR |
|---|---|---|---|
| **2** | 512 | 1.160 | 1.130 |
| **5** | 1024 | 5.884 | 1.611 |
| **10** | 2048 | 5.906 | 1.925 |
| **15** | 4096 | 5.928 | 2.939 |
| **20** | 8192 | 6.936 | 2.967 |

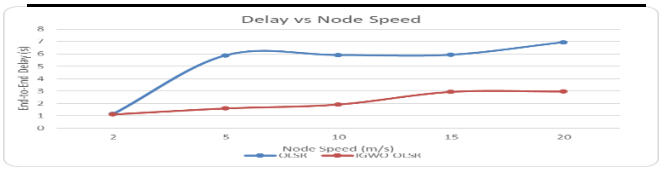


Fig. 6. End-to-End Delay vs Node Speed for OLSR and IGWO-OLSR

### 4.5 Discussion of Results

The comparative results demonstrate that the Improved GWO-OLSR consistently outperforms the standard OLSR protocol in the presence of Sybil attacks across varying node speeds and traffic conditions, as shown in Table 4.

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

Table 4. Summary of the results for all the performance metrics

| Result for Throughput (Kbs) | | | |
|---|---|---|---|
| **Nodal Speed (m/s)** | **Packet Size (bytes)** | **OLSR** | **Improved GWO-OLSR** |
| **2** | 512 | 3000 | 4500 |
| **5** | 1024 | 6000 | 6600 |
| **10** | 2048 | 10500 | 11500 |
| **15** | 4096 | 13500 | 15060 |
| **20** | 8192 | 18000 | 20570 |
| **Packet Delivery Ratio (PDR)** | | | |
| **Nodal Speed (m/s)** | **Packet Size (bytes)** | **OLSR (%)** | **Improved GWO-OLSR (%)** |
| **2** | 512 | 0.862 | 0.897 |
| **5** | 1024 | 0.884 | 0.911 |
| **10** | 2048 | 0.906 | 0.925 |
| **15** | 4096 | 0.928 | 0.939 |
| **20** | 8192 | 0.936 | 0.967 |
| **End to End delay Table** | | | |
| **Nodal Speed (m/s)** | **Packet Size (bytes)** | **OLSR** | **Improved GWO-OLSR** |
| **2** | 512 | 1.160 | 1.130 |
| **5** | 1024 | 5.884 | 1.611 |
| **10** | 2048 | 5.906 | 1.925 |
| **15** | 4096 | 5.928 | 2.939 |
| **20** | 8192 | 6.936 | 2.967 |

The enhanced protocol achieves higher throughput, improved packet delivery ratio, and lower end-to-end delay, indicating more reliable and efficient data transmission in dynamic network environments. These gains are mainly attributed to the Grey Wolf Optimizer's ability to detect and isolate Sybil nodes, thereby preventing false routing information, reducing packet losses, minimizing route rediscovery, and avoiding congestion. Overall, the results confirm that integrating GWO into OLSR significantly strengthens routing stability, security, and performance, making the proposed approach more suitable for MANETs operating under adversarial and highly mobile conditions. Furthermore, the results obtained in this study are consistent with previous research that applied optimization techniques such as Particle Swarm Optimization and Genetic Algorithms to MANET routing protocols. While these approaches improve packet delivery ratio and throughput, they often increase computational complexity. In comparison, the IGWO-OLSR protocol achieves competitive or superior performance with lower delay and better adaptability to dynamic network conditions, highlighting the effectiveness of the Grey Wolf Optimizer as a lightweight and efficient solution for enhancing routing security and performance in MANETs.

## 5 CONCLUSION AND FUTURE WORK

This study addressed the security challenges of Mobile Ad Hoc Networks (MANETs), particularly Sybil attacks, by developing and implementing an IGWO-OLSR model that integrates the Grey Wolf Optimizer with the Optimized Link State Routing protocol. The results demonstrate that the IGWO-OLSR approach significantly improves packet delivery ratio, throughput, and end-to-end delay compared to the standard OLSR, thereby enhancing routing efficiency, network stability, and security in dynamic environments. Future work can extend this approach to other routing protocols and incorporate additional security mechanisms to further improve the robustness and scalability of MANETs.

## REFERENCES


Abolhasan, M., Wysocki, T., and Dutkiewicz, E. (2009). A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, 2(1), 1–22.

Akyildiz, I. F., Wang, X., and Wang, W. (2020). Next-generation routing protocols for wireless ad hoc networks. *IEEE Communications Magazine*, 58(2), 110-119.

Aljohani, A. J. (2021). A comprehensive survey on security attacks and countermeasures in mobile ad hoc networks. *IEEE Access*, 9, 156878–156901. https://doi.org/10.1109/ACCESS.2021.3129635

Clausen, T., and Jacquet, P. (2003). Optimized Link State Routing Protocol (OLSR). *RFC 3626*. IETF.

Conti, M., and Giordano, S. (2014). Mobile ad hoc networking: Milestones, challenges, and new research directions. *IEEE Communications Magazine*, 52(1), 85–96.

Douceur, J. R. (2002). The Sybil attack. *In Proceedings of the 1st International Workshop on Peer-to-Peer Systems*, 251–260.

Haas, Z. J., Pearlman, M. R., and Samar, P. (2002). The zone routing protocol (ZRP) for ad hoc networks. *Internet Draft.*

Huhtonen, T. (2022). Security threats and trust management in mobile ad hoc networks. *Journal of Network and Computer Applications*, 198, 103274. https://doi.org/10.1016/j.jnca.2021.103274

Johnson, D. B., and Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, 353–367.

Mahdy, A.M.S.; Lotfy, K.; Hassan, W.; El-Bary, A.A. (2021). Analytical solution of magneto-photo thermal theory during variable thermal conductivity of a semiconductor material due to pulse heat flux and volumetric heat source. *Waves Random Complex Media,* 31, 2040–2057.

Mirjalili, S., Mirjalili, S. M., and Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, 69, 46–61.

Neeraj, K. (2021). Cooperative Sybil attacks in OLSR: Threats and countermeasures. *Journal of Network Security and Applications*, 31(3), 112-125.

Newsome, J., Shi, E., Song, D., and Perrig, A. (2004). The Sybil attack in sensor networks: Analysis and defenses. *In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, 259–268.

Qayyum, A. (2019). Security challenges in OLSR protocol: A survey. *Journal of Network and Computer Applications*, 22(1), 85-95.

Sarkar, S. K., Basavaraju, T. G., and Puttamadappa, C. (2013). *Ad hoc mobile wireless networks: Principles, protocols, and applications*. Auerbach Publications.

Siau, J., and Shen, C. (2020). Performance optimization techniques for ad hoc networks. *Journal of Computer Networks*, 25(6), 152-165.

Vecchi, M. P. (2022). Simulated annealing and modern optimization techniques. *Springer*.

Wagner, D. (2021). Wireless ad hoc and sensor networks: Principles, architectures, and applications. *Springer Nature*.

Wang, P. (2021). Scalability and performance optimization in OLSR networks. *Ad Hoc and Sensor Wireless Networks*, 25(2), 89-101.

Xiaohui, L. (2020). Sybil attack mitigation techniques in MANETs. *International Journal of Computer Networks and Communications*, 30(5), 78-90.

Yen, C., and Chou, T. (2021). Adaptive routing algorithms in dynamic mobile networks. *International Journal of Computer Science and Applications,* 19(1), 92-105.

Zhang, L. (2019). Optimized Link State Routing for wireless ad hoc networks. *International Journal of Network Protocols*, 15(4), 102-115.


© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)