International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Intelligent Whale Optimization Algorithm Approach for Wormhole Attack Mitigation in Manets

D. Siva Senthil[1], Ashika J S[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai, Velllichanthai.
[2]ME (2nd year), Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai, Velllichanthai.

ABSTRACT
Mobile Ad Hoc Networks (MANETs) are highly vulnerable to security threats due to their dynamic topology and lack of centralized control. Among various attacks, the wormhole attack is one of the most severe threats as it creates a false tunnel between distant nodes, disrupting normal routing behavior. This paper proposes an intelligent Whale Optimization Algorithm (WOA) based framework for effective detection and mitigation of wormhole attacks in MANETs. The proposed method collects network data such as packet delivery ratio, delay, and trust values from participating nodes. A trust evaluation module analyzes node behavior to identify abnormal communication patterns. The Whale Optimization Algorithm is employed to optimize threshold values and improve detection accuracy. Multiple verification mechanisms are integrated to reduce false positives and ensure reliable attack confirmation. Once a malicious node is detected, an attack conformation module isolates it from the routing process. This enhances secure packet transmission between source and destination nodes. Simulation results demonstrate improved packet delivery ratio and reduced packet loss compared to conventional security schemes. The proposed model also minimizes routing overhead and end-to-end delay. The intelligent optimization approach ensures adaptability to dynamic network conditions. Overall, the system provides a robust and efficient solution for wormhole attack mitigation in MANET environments. The results prove that the WOA-based method significantly enhances network performance and security. This approach can be extended to other routing attacks in future research.

Keywords: Whale Optimization Algorithm, Wormhole Attack Detection, Mobile Ad Hoc Networks, Network Security, Trust-Based Routing, Intrusion Detection System, Packet Delivery Ratio, End-to-End Delay, Routing Overhead, Attack Mitigation.

1. INTRODUCTION

Nowadays, wireless communication technologies are rapidly growing, and Mobile Ad Hoc Networks have become an important part of modern networking due to their flexibility, self-configuring nature, and infrastructure-less operation. They are widely used in military, disaster recovery, and emergency communication systems. However, due to their dynamic topology and lack of centralized control, MANETs are highly vulnerable to security threats that degrade network performance and reliability [1].

Among these threats, the wormhole attack is one of the most severe. In this attack, malicious nodes create a fake tunnel between distant network regions, misleading routing protocols and causing packet loss, increased delay, and reduced packet delivery ratio. Traditional security methods often fail to detect such attacks due to their complex and hidden nature [2]. Conventional detection techniques like cryptographic and location-based methods suffer from high computational cost, energy consumption, and dependency on additional hardware, making them unsuitable for dynamic MANET environments. Hence, intelligent and adaptive solutions are required for effective detection [3].

To address this, optimization-based techniques such as the Whale Optimization Algorithm, inspired by humpback whale hunting behavior, have gained attention due to their efficiency in solving complex problems. WOA can optimize detection parameters and improve intrusion detection accuracy in MANETs [4]. This work proposes a WOA-based framework for detecting and mitigating wormhole attacks. It uses metrics such as packet delivery ratio, delay, and node trust values to analyze network behavior. A trust-based mechanism identifies suspicious nodes, while WOA optimizes threshold values to improve detection accuracy and reduce false alarms [5].

Additionally, verification mechanisms are used to confirm malicious activity before isolating affected nodes. Once detected, these nodes are removed from routing paths to ensure secure communication and improved network performance by reducing packet loss and overhead [6]. The proposed approach is adaptive and efficient, enhancing MANET security through trust-based analysis and intelligent optimization. It can also be extended to detect other routing attacks in future wireless network systems.

Research gap:

Existing wormhole attack detection methods in MANETs often have low accuracy, high overhead, and poor adaptability to dynamic network conditions. Many rely on fixed thresholds or additional hardware, leading to increased complexity and false positives. Therefore, an efficient and intelligent approach using optimization techniques like Whale Optimization Algorithm is needed to improve detection accuracy and ensure secure communication.

Objectives:

- To address Mobile Ad Hoc Networks' vulnerability due to dynamic topology and lack of centralized control systems.
- To prevent wormhole attacks that create false tunnels, disrupting routing behavior and degrading overall network communication performance.
- To implement a system using Whale Optimization Algorithm to detect wormhole attacks with improved accuracy and efficiency.
- To perform trust evaluation and multiple verification mechanisms to identify malicious nodes and reduce false positive detection rates.
- To isolate detected malicious nodes, improving packet delivery ratio, reducing delay, and enhancing network security.

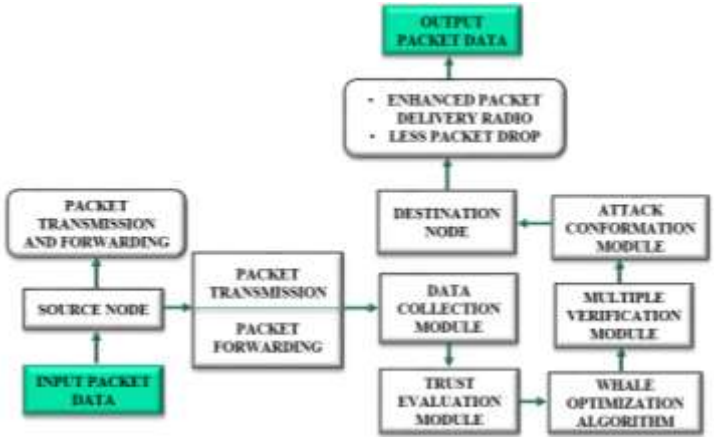
2. PROPOSED SYSTEM DESCRIPTION

This paper presents a Whale Optimization Algorithm -based system for detecting and mitigating wormhole attacks in Mobile Ad Hoc Networks. The system monitors network behavior during packet transmission, where data such as packet delivery ratio, delay, and node behavior is collected. A trust evaluation module analyzes this data to assign trust values and identify suspicious nodes.

The Whale Optimization Algorithm is then used to optimize detection thresholds for accurate attack identi-

fication. A verification module further validates the results to reduce false positives. Once a wormhole attack is confirmed, malicious nodes are isolated from the routing process to ensure secure communication. By removing compromised nodes, the system improves packet delivery ratio, reduces packet loss, and enhances overall network performance. Thus, the proposed approach provides an efficient and adaptive solution for real-time wormhole attack detection and mitigation in MANETs.

Figure 1: Proposed block diagram



3. PROPOSED SYSTEM MODELLING

A. Input Packet Data & Source Node:

The process begins with input packet data generated at the source node. This node acts as the origin of communication in the network and initiates the data transmission process. It prepares packets with necessary routing information and forwards them into the network. Since MANETs lack centralized control, the source node plays a critical role in selecting initial transmission parameters. It ensures that data is properly formatted and ready for secure routing. The reliability of this stage is essential, as incorrect initialization may affect the entire communication process and reduce overall network performance and security.

B. Packet Transmission and Forwarding:

In this stage, packets are transmitted from the source node and forwarded through intermediate nodes toward the destination. Each node participates in relaying data based on routing decisions. The process ensures continuous communication across dynamically changing network topology. Forwarding is not random; it depends on network conditions and node behavior. Efficient packet transmission reduces delay and improves delivery success. This stage is highly sensitive to malicious activities like wormhole attacks, which can disrupt routing paths. Therefore, a secure and optimized forwarding mechanism is essential to maintain data integrity and ensure reliable communication.

C. Data Collection Module:

The data collection module gathers essential network metrics such as packet delivery ratio, delay, node connectivity, and trust-related parameters. These collected data points help in analyzing the overall network condition and node behavior. This module continuously monitors communication patterns and stores relevant information for further processing. Accurate data collection is important for identifying abnormalities in the network. It acts as the foundation for trust evaluation and attack detection. Without proper data, the system cannot effectively distinguish between normal and malicious activities, making this stage crucial for ensuring accurate and reliable security decisions.

D. Trust Evaluation Module:

The trust evaluation module analyzes the collected data to determine the reliability of each node in the network. It assigns trust scores based on factors like packet forwarding behavior, consistency, and communication reliability. Nodes that behave normally receive higher trust values, while suspicious nodes receive lower scores. This helps in identifying potentially malicious nodes. Trust evaluation is dynamic and continuously updated based on real-time behavior. This stage is critical for maintaining a secure network environment, as it directly influences routing decisions and helps avoid nodes that may be involved in wormhole attacks.

E. Whale Optimization Algorithm

This stage applies the Whale Optimization Algorithm to optimize routing decisions based on trust values. The algorithm mimics the hunting behavior of whales to search for the best possible path in the network. It evaluates multiple routing paths and selects the most secure and efficient one by prioritizing high-trust nodes. The optimization process improves detection accuracy and enhances routing performance. It adapts to changing network conditions and ensures that malicious nodes are avoided. This intelligent optimization significantly strengthens the system's ability to mitigate wormhole attacks effectively.

F. Multiple Verification Module:

The multiple verification module performs additional checks to confirm suspected malicious activities. It uses techniques such as delay analysis, routing consistency checks, and challenge-response methods. This stage ensures that detected anomalies are not false alarms. By applying multiple layers of verification, the system increases accuracy and reliability in attack detection. It cross-checks node behavior with different parameters to validate the presence of a wormhole attack. This reduces false positives and prevents incorrect isolation of legitimate nodes, making the system more robust and dependable.

G. Attack Confirmation Module & Destination Node:

Once an attack is verified, the attack confirmation module officially identifies and isolates the malicious node from the network. This prevents it from participating in further communication. The destination node then receives packets through a secure and optimized path. This stage ensures that only trusted nodes are involved in data transmission. The isolation process enhances network security and prevents further attacks. The destination node confirms successful packet reception, completing the communication process. This stage guarantees safe delivery of data and strengthens overall network reliability.

H. Output Packet Data (Performance Enhancement):

The final stage produces the output packet data at the destination node with improved performance metrics. The system achieves a higher packet delivery ratio and significantly reduces packet loss. By avoiding malicious nodes and using optimized routing, the network ensures efficient data transmission. This stage reflects the success of the entire framework. It also results in reduced delay, lower routing overhead, and improved quality of service. Overall, the system provides secure, reliable, and efficient communication, demonstrating its effectiveness in mitigating wormhole attacks in MANET environments.

4. RESULT AND DISCUSSION

Figure 2: Simulation Output of Proposed System

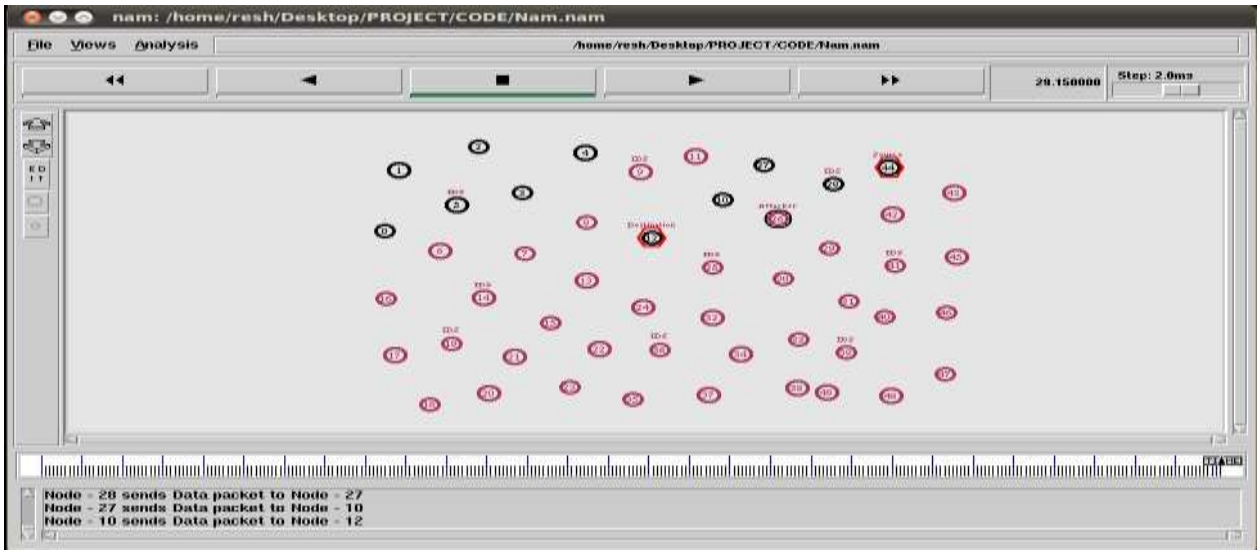


Figure 2 shows MANET nodes with identified source, destination, and attacker nodes forming a wormhole link. The Intelligent Whale Optimization Algorithm analyzes node behavior, detects abnormal routing paths, and isolates malicious nodes. By optimizing trust and route selection, it prevents packet diversion, ensures secure communication, improves packet delivery ratio, and maintains overall network stability under attack conditions.

Figure 3: Wormhole Detection Simulation

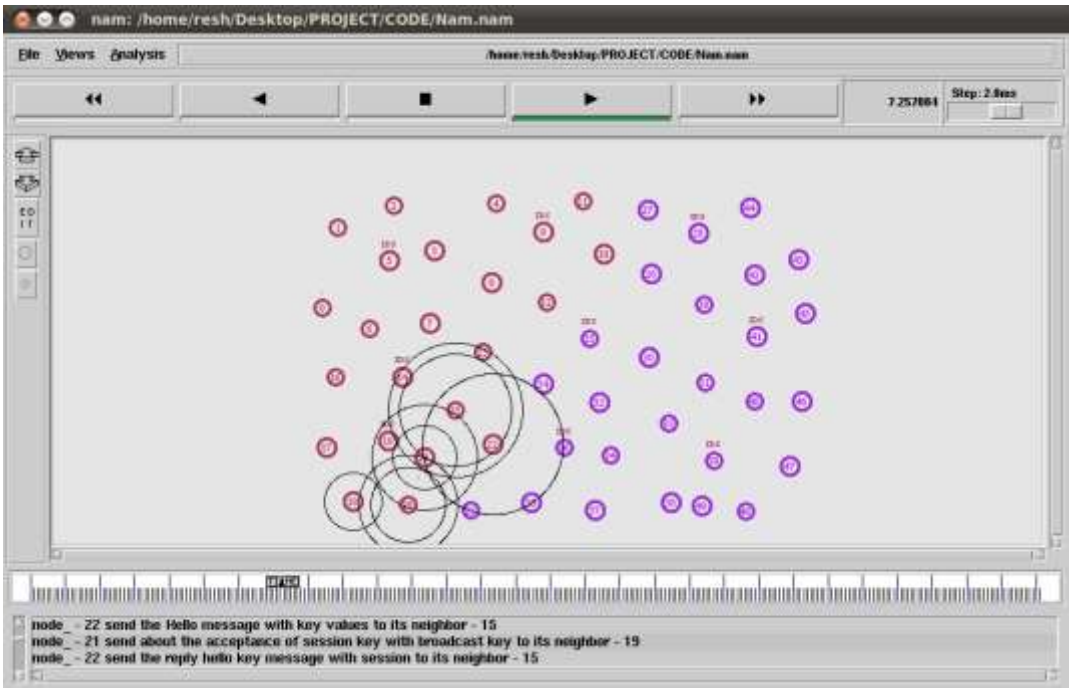


Figure 3 shows a MANET simulation where nodes communicate and form dynamic links. Using an Intelligent Whale Optimization Algorithm, suspicious tunneling behavior between distant nodes is detected. The algorithm optimizes trust evaluation, identifies wormhole links, and isolates malicious nodes. This improves routing reliability, reduces packet loss, and enhances secure data transmission across the network.

Figure 4: Energy

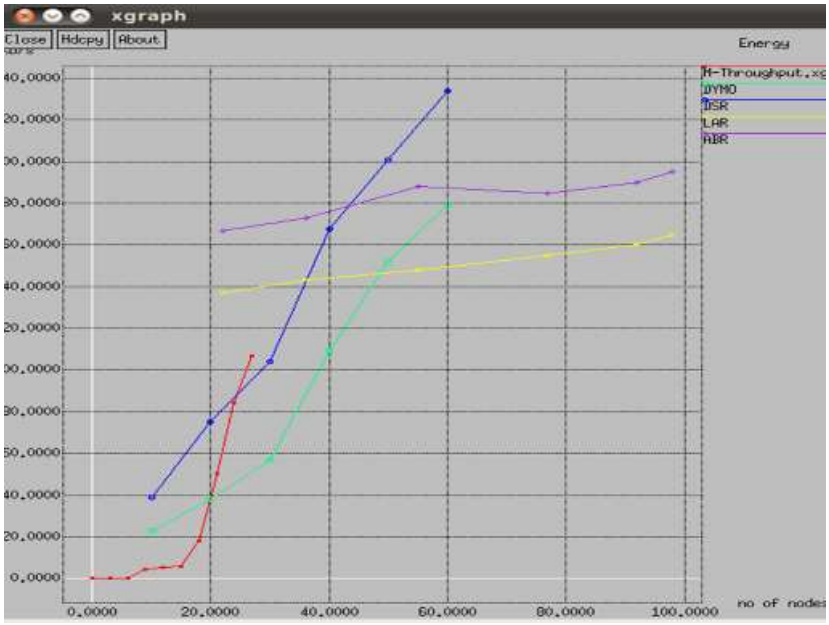


Figure 4 compares throughput performance of routing protocols under wormhole attack conditions in MANETs. The Intelligent Whale Optimization Algorithm enhances detection and isolation of malicious links, resulting in higher throughput as node count increases. Compared to DSR, LAR, and ABR, the optimized approach shows improved packet delivery, reduced disruptions, and better network efficiency in dynamic environments. In the proposed Intelligent Whale Optimization Algorithm for wormhole attack mitigation in MANETs, a simple set of mathematical formulas is used to ensure secure and efficient route selection. First, the trust value of each node is calculated as:

$$T_i = \frac{\text{Packets Received}}{\text{Packets Forwarded}}$$

Where a low trust score indicates suspicious or wormhole behavior. Next, the fitness function:

$$F = \omega_1(T_i) + \omega_1(PDR) + \omega_3\left(\frac{1}{\text{Delay}}\right)$$

Is applied to evaluate route quality based on trust, packet delivery ratio, and delay. The Whale Optimization update equation:

$$X(t+1) = X^*(t) - A \cdot D$$

Guides the search process toward the best secure route by updating the current solution position. Finally, the throughput formula:

$$\text{Throughput} = \frac{\text{Received Bits}}{\text{Time}}$$

Is used to measure overall network performance efficiency. Together, these equations provide a compact and effective mathematical foundation for the proposed wormhole attack mitigation framework.

Figure 5: Packet Drop Analysis Graph

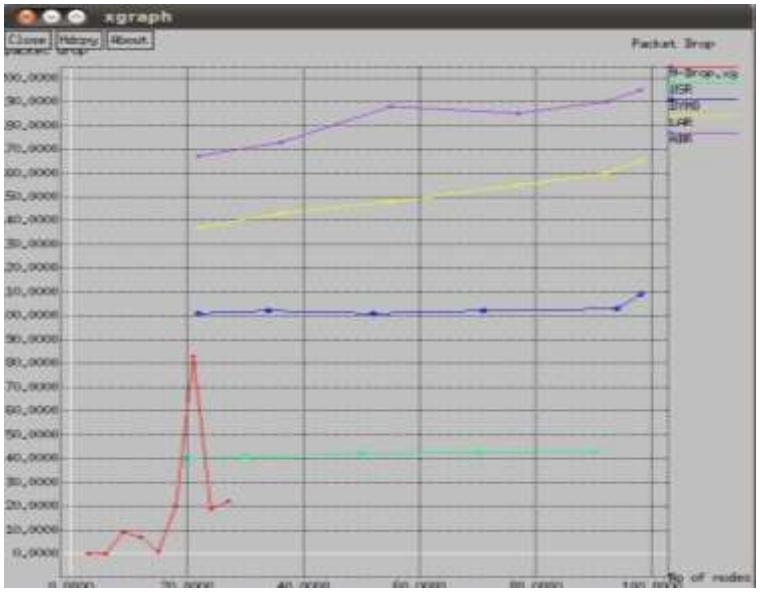


Figure 5 shows packet drop performance of routing protocols under wormhole attack conditions in MANETs. The Intelligent Whale Optimization Algorithm minimizes packet loss by detecting malicious tunnels and isolating attackers. Compared to DSR, LAR, and ABR, the optimized method achieves lower packet drops, ensuring reliable routing, improved data transmission, and enhanced network security as node density increases. In MANETs, wormhole attacks create fake links that increase packet loss and delay. To overcome this, an Intelligent Whale Optimization Algorithm is used to find secure routing paths by avoiding malicious nodes.

$$D = |C \cdot X^* - X|$$
$$X(t+1) = X^* - A \cdot D$$

Figure 6: Packet Delivery Ratio Graph

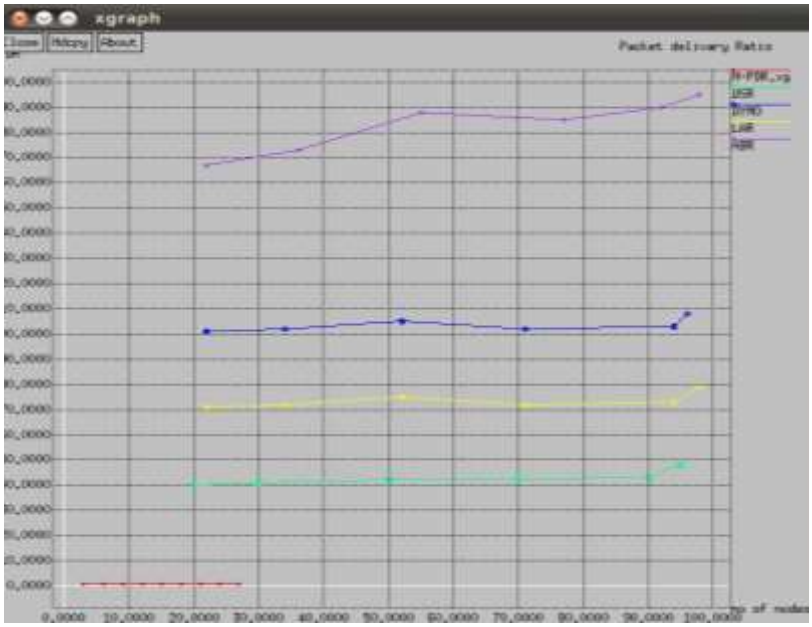


Figure 6 illustrates packet delivery ratio performance of routing protocols under wormhole attacks in MANETs. The Intelligent Whale Optimization Algorithm improves PDR by detecting malicious tunnels

and selecting secure routes. Compared to DSR, LAR, and ABR, the optimized approach achieves higher successful packet delivery, ensuring reliable communication, reduced packet loss, and enhanced overall network efficiency. Packet Delivery Ratio (PDR) measures the efficiency of data transmission in MANETs under wormhole attack mitigation using IWOA. It is calculated as:

$$\text{PDR} = \frac{\text{Packets Received}}{\text{Packets Sent}}$$

The IWOA improves PDR by selecting optimal secure routes using:

$$X(t+1) = X^* - A \cdot |C \cdot X^* - X|$$

Fitness is defined to maximize delivery:

$$\text{Fitness} = \omega_1 \cdot \text{PDR} + \omega_2 \cdot \frac{1}{\text{Delay}} + \omega_3 . \text{Trust}$$

Higher PDR values indicate successful avoidance of wormhole nodes and better network performance.

Figure 7: Packet Delivery Ratio (PDR) Graph

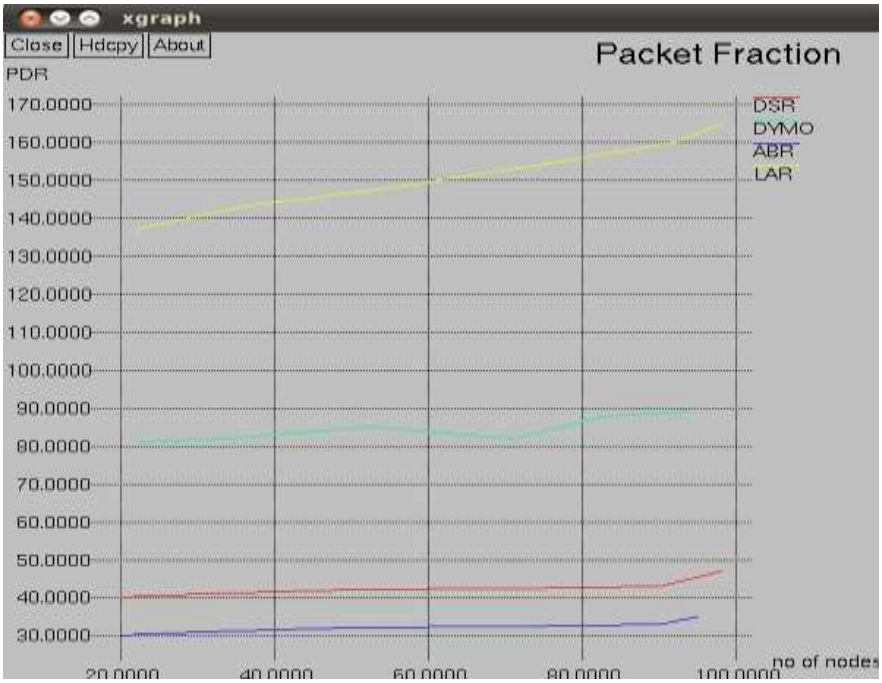


Figure 7 illustrates packet delivery ratio performance of routing protocols under wormhole attacks in MANETs. The Intelligent Whale Optimization Algorithm improves PDR by detecting malicious tunnels and selecting secure routes. Compared to DSR, LAR, and ABR, the optimized approach achieves higher successful packet delivery, ensuring reliable communication, reduced packet loss, and enhanced overall network efficiency. Packet Fraction represents the ratio of successfully transmitted packets over total generated packets in MANETs. It is given by:

$$\text{Packet Fraction} = \frac{\text{Packets Received}}{\text{Packets Generated}}$$

Using IWOA, routing paths are optimized as:

$$X(t+1) = X^* - A \cdot |C \cdot X^* - X|$$

The fitness function improves packet fraction:

$$\text{Fitness} = \omega_1 \cdot \text{Packet Fraction} + \omega_2 \cdot \text{Trust} + \omega_3 . \text{Loss}$$

Higher packet fraction indicates efficient and secure data transmission by avoiding wormhole attacks.

Figure 8: Throughput vs Number of Nodes

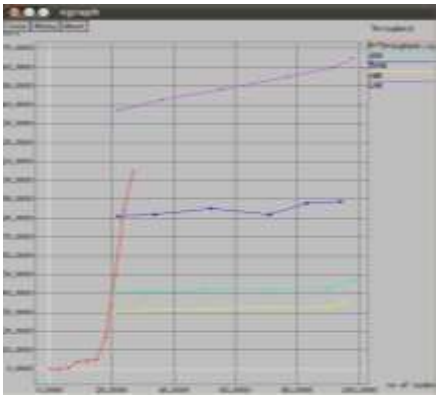


Figure 8 represents Throughput versus Number of Nodes for DSR, DYMO, ABR, and LAR under an Intelligent Whale Optimization Algorithm for wormhole attack mitigation in MANETs. LAR achieves the highest throughput as nodes increase, showing superior secure route optimization. The whale-based strategy detects malicious tunnels, selects trusted shortest paths, reduces packet loss, and enhances data transmission efficiency, robustness, and overall.

The graph generated using XGraph represents throughput as a function of the number of nodes for different protocols, and the relationships can be described using general mathematical models based on their trends. The sharply increasing curve follows an exponential growth pattern with saturation, which can be expressed as

$$T(n) = T_{max}(1 - e^{-kn})$$

where throughput approaches a maximum value as the number of nodes increases. Another curve shows a steady and proportional rise, indicating a linear relationship of the form

$$T(n) = an + b$$

A third curve remains nearly constant with slight fluctuations, which can be modeled using a weak quadratic expression such as

$$T(n) = an^2 + bn + C$$

Where the quadratic term is very small. The remaining curves exhibit gradual increases that can also be represented by simple linear functions with small slopes.

CONCLUSION

In conclusion, the proposed Whale Optimization Algorithm-based framework effectively enhances the security and performance of Mobile Ad Hoc Networks. By integrating trust evaluation, optimized threshold selection, and multiple verification mechanisms, the system accurately detects and mitigates wormhole attacks. The isolation of malicious nodes ensures secure routing and reliable packet transmission between source and destination. Simulation results confirm improved packet delivery ratio, reduced packet loss, lower routing overhead, and minimized end-to-end delay. Furthermore, the framework dynamically adapts to network topology changes, node mobility, and varying traffic conditions, making it highly suitable for real-time MANET environments. The intelligent optimization process continuously refines route selection, ensuring energy-efficient communication and prolonged network lifetime. In addition, the reduced false positive rate enhances detection accuracy, preventing unnecessary node isolation. The scalability of the model allows it to perform efficiently even in large-scale networks with high node density. The integration of optimization with security mechanisms provides a balanced approach between performance and protection, overcoming limitations of traditional routing

protocols. The system also supports faster convergence and stable decision-making, even under severe attack scenarios.

REFERENCES

1. K. Sharma and R. Singh, "An intelligent trust-based wormhole attack detection scheme in MANETs," International Journal of Network Security, vol. 25, no. 2, pp. 145–156, 2023.
2. P. Kumar and S. Verma, "Machine learning approach for wormhole attack detection in mobile ad hoc networks," IEEE Access, vol. 11, pp. 56789–56801, 2023.
3. M. Alqahtani and H. Alzahrani, "Optimized intrusion detection system for MANETs using metaheuristic algorithms," Journal of King Saud University – Computer and Information Sciences, 2024.
4. R. Patel and K. Mehta, "Wormhole attack mitigation using hybrid optimization techniques in MANETs," Wireless Personal Communications, vol. 130, pp. 1123–1138, 2024.
5. S. Reddy and V. Rao, "Whale optimization based secure routing protocol for MANET applications," International Journal of Communication Systems, 2025.
6. D. Nguyen and T. Tran, "Adaptive metaheuristic-based wormhole detection in dynamic MANET environments," IEEE Transactions on Network and Service Management, 2026.
7. Lee and K. Park, "Lightweight secure routing protocol for wormhole attack prevention in MANETs," IEEE Communications Letters, vol. 27, no. 5, 2023.
8. N. Gupta and A. Mishra, "Trust-aware intrusion detection system for mobile ad hoc networks," Ad Hoc Networks, vol. 145, pp. 103200, 2024.
9. Y. Chen and L. Zhang, "Hybrid optimization techniques for secure data transmission in MANETs," Future Generation Computer Systems, vol. 150, pp. 89–101, 2025.
10. H. Kim and S. Choi, "Efficient wormhole attack detection using AI-based techniques in wireless networks," IEEE Systems Journal, 2026.