Optimizing Cybersecurity Threat Detection: An Integrated Approach Using Particle Swarm Optimization and Generative Adversarial Networks

Bhagya Lakshmi[1], Dr. M. Vargheese[2]

[1]*Master of Engineering in Computer Science and Engineering Psn College of Engineering and Technology (Autonomous) Melathediyoor,Tirunelveli 627152*

[2] *M.Tech., Ph.D Professor and Head, Department of Computer Science and Engineering PSN College of Engineering and Technology, Tirunelveli – 627152*

Abstract*—This project presents an innovative security framework for Mobile Ad hoc Networks (MANETs), utilizing a Particle Swarm Optimization (PSO) algorithm combined with a Generative Adversarial Network (GAN) to improve the performance of Intrusion Detection Systems (IDS). Due to their dynamic and decentralized nature, MANETs are highly vulnerable to a range of security threats, including unauthorized data access, routing attacks, and denial-of-service attacks. To mitigate these risks, the proposed framework employs PSO, a bio-inspired optimization algorithm that mimics the social behavior of bird flocking and fish schooling. PSO is used to enhance the feature selection process, ensuring that the most relevant features for intrusion detection are identified and prioritized through global best optimization. The second component, GAN, incorporates deep learning techniques with supervised classification to accurately identify and classify network intrusions based on the selected features. By training on labeled datasets such as NSL-KDD, UNSW-NB15, and D820S, GAN effectively distinguishes between normal and malicious traffic, ensuring reliable detection. The combination of PSO and GAN not only strengthens the feature extraction and selection process but also improves the overall detection capability. This hybrid approach is highly adaptable, capable of handling the evolving and complex nature of attacks in MANETs. Experimental results demonstrate the framework's superior performance in terms of detection accuracy, false alarm rates, and computational efficiency, providing a robust solution for addressing the security challenges inherent in MANET environments. This project is implemented using NS-2 simulation.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) represent a dynamic and decentralized form of wireless networking where nodes communicate with each other without relying on any fixed infrastructure or centralized administration. These networks are self-organizing, flexible, and capable of rapid deployment, making them ideal for military operations, disaster recovery, and remote area communications. However, the open and dynamic nature of MANETs also exposes them to a wide range of security vulnerabilities. Among these, the wormhole attack is one of the most severe and challenging to detect. In a wormhole attack, malicious nodes create a low-latency link, or "tunnel," between two distant locations in the network, replaying packets to distort routing paths. This manipulation misleads routing protocols into selecting malicious routes, thereby allowing attackers to eavesdrop, drop, or alter data packets, ultimately degrading network performance and reliability.

Detecting wormhole attacks in MANETs is a complex task due to the absence of centralized monitoring and the dynamic topology caused by node mobility. Traditional cryptographic techniques alone are often insufficient, as wormholes be established without compromising encryption or authentication. Therefore, advanced detection mechanisms such as packet timing analysis, neighbor verification, geographic leashes, hop-count monitoring, and trust-based models—have been proposed to identify abnormal routing behaviors caused by wormholes.

The effectiveness of these detection strategies largely depends on balancing security accuracy with computational and energy efficiency, as MANET nodes are resource-constrained. Hence, research continues to focus on developing lightweight, adaptive, and intelligent detection algorithms that accurately identify and mitigate wormhole attacks without compromising the scalability or performance of MANETs. This study aims to explore and analyze such techniques to enhance the overall security framework of MANETs.

Wormhole attacks pose a significant threat to the integrity and trustworthiness of Mobile Ad Hoc Networks because they disrupt routing protocols such as AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and OLSR (Optimized Link State Routing). In such an attack, two or more colluding malicious nodes create a tunnel between distant parts of the network. When a packet is captured at one end of the tunnel, it is transmitted to the other end and replayed into the network, creating the illusion that nodes far apart are immediate neighbors. This false perception results in incorrect routing information, allowing attackers to attract data traffic through malicious routes. Consequently, this lead to packet loss, increased delays, and even complete network partitioning. The impact is particularly critical in time-sensitive applications, where reliable communication is essential for mission success.

Due to the stealthy nature of wormhole attacks, detecting them requires more than conventional intrusion detection methods. Researchers have proposed various solutions, including location-based techniques, which rely on GPS coordinates to verify the legitimacy of routing paths; temporal leashes, which restrict packet transmission times; and trust-based frameworks, where nodes assign reputation scores based on observed behavior. Another promising approach involves machine learning and artificial intelligence, where algorithms learn to distinguish normal routing behavior from attack patterns using data-driven models. However, these methods must be designed carefully to handle MANET constraints, such as limited bandwidth, battery power, and high mobility.

In modern network security research, hybrid models combining cryptographic verification, statistical analysis, and behavioral monitoring have shown potential for detecting wormhole attacks effectively. The integration of blockchain-based trust management systems and fuzzy logic-based anomaly detection further enhances resilience against routing manipulation. Ultimately, the goal of wormhole detection mechanisms is not only to identify and isolate malicious nodes but also to maintain the overall network's efficiency, scalability, and robustness. As MANETs continue to play an important role in emerging technologies like IoT, vehicular networks, and tactical communications, strengthening their defense against wormhole attacks remains a vital research priority to ensure secure and reliable data transmission.

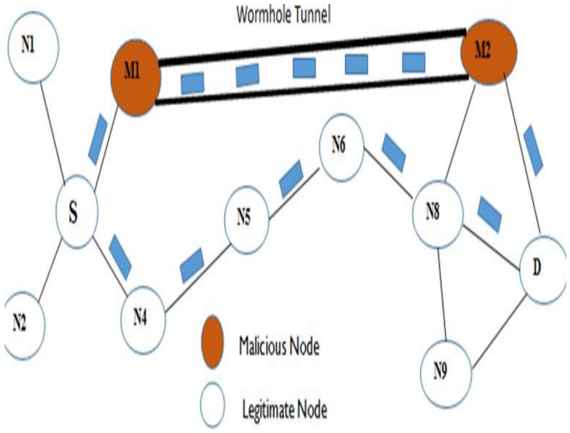


Figure 1.1 Wormhole Attacks in Manets

1.1 Introduction To Manets

Mobile Ad Hoc Networks (MANETs) are decentralized wireless systems where mobile nodes communicate directly without any fixed infrastructure or central authority. Each node acts as both a transmitter and a router, forwarding data to other nodes dynamically. This flexibility makes MANETs ideal for applications like military operations, emergency rescue, and remote area communication. However, their open and dynamic nature introduces several security challenges. Since nodes freely join or leave the network, malicious users easily exploit routing protocols to launch attacks. The absence of centralized monitoring and dynamic topology makes detecting such attacks extremely difficult. Common threats include blackhole, Sybil, and wormhole attacks, which disrupt data routing and reduce network performance. Additionally, resource constraints like limited bandwidth, energy, and processing power restrict the use of complex encryption mechanisms. Therefore, ensuring secure and reliable communication in MANETs requires lightweight, adaptive, and intelligent detection mechanisms that maintain performance while preventing unauthorized access.

Overview of Mobile Ad Hoc Networks (MANETs)

Mobile Ad Hoc Networks (MANETs) are self-configuring, infrastructure- less wireless networks composed of mobile nodes that communicate with each other using radio signals. Unlike traditional networks, MANETs do not rely on routers, access points, or centralized control systems; instead, every node acts as both a host and a router. This decentralized nature enables quick and flexible network formation, especially in scenarios such as military communications, disaster relief, vehicular networks, and remote sensing. MANETs are highly adaptive, allowing nodes to join, leave, or move freely within the network without disrupting overall communication. However, the dynamic topology also introduces frequent route changes and variable link quality. Since nodes depend on each other for data forwarding, maintaining efficient routing becomes a core challenge. Popular routing protocols like AODV, DSR, and OLSR help establish reliable paths, but their performance degrade under high mobility conditions. Additionally, limited bandwidth, energy constraints, and signal interference make MANETs vulnerable to both performance degradation and malicious attacks. Thus, while MANETs offer flexibility and scalability, they also present significant technical and security challenges that must be addressed to ensure safe communication.

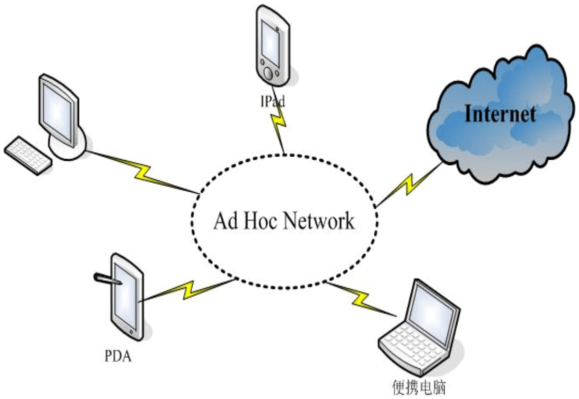


Figure: 1.2 Structure of Ad hoc network

Security Challenges in MANETs

Security is one of the most critical issues in MANETs because of their open medium, decentralized control, and frequent topology changes. Unlike wired networks, where access points be protected physically, MANET nodes communicate wirelessly, making them prone to eavesdropping, data tampering, and impersonation attacks. The absence of a centralized authority makes authentication and key management complex, leaving the network exposed to internal and external threats. Common attacks in MANETs include blackhole, grayhole, Sybil, and particularly wormhole attacks, which disrupt routing by tunneling packets through malicious nodes. These attacks degrade network throughput, cause data loss, and compromise confidentiality. Furthermore, MANETs are resource-constrained nodes have limited power, computation, and storage capacity so implementing strong cryptographic security drain their resources quickly. Security solutions for MANETs must therefore be lightweight, adaptive, and distributed. Achieving this balance between strong security and efficient communication remains one of the most demanding research areas in MANET development.

1.2 Overview Of Wormhole Attacks

Wormhole attacks are one of the most severe and deceptive security threats in Mobile Ad Hoc Networks (MANETs). In this attack, two or more malicious nodes establish a private, high-speed communication link known as a “wormhole tunnel.” Through this tunnel, packets captured at one end are transmitted and replayed at the other end, creating the illusion that two distant nodes are direct neighbors. This misleads the routing protocol into selecting routes that pass through the malicious nodes, giving attackers control over a significant portion of network traffic. Once in control, they drop, delay, or modify packets, leading to degraded performance or complete communication failure. Unlike other attacks, wormholes be launched without compromising cryptographic keys, making them difficult to detect using standard security mechanisms. These attacks severely disrupt routing algorithms such as AODV and DSR by creating false shortest paths, increasing routing overhead, and enabling data interception. Hence, understanding the nature and types of wormhole attacks is essential for designing effective detection and prevention strategies in MANETs.

Working Mechanism of Wormhole Attacks

The wormhole attack operates by capturing data packets from one network location and replaying them at another through a fast link between malicious nodes. For instance, two colluding nodes say Node A and Node Bare placed in different regions of the network. When Node A receives a route request, it forwards it instantly to Node B through the wormhole tunnel, bypassing the normal multi- hop route. Node B then rebroadcasts the packet, making nodes near it believe that they are directly connected to Node A. This false neighbor relationship tricks routing protocols into selecting the wormhole link as the shortest path. As a result, legitimate nodes unknowingly send data through the attackers, who monitor, drop, or manipulate packets. The attack does not require packet modification, cryptographic key knowledge, or high processing power, which makes it stealthy and hard to detect. The wormhole link be established using wired connections, directional antennas, or high-power wireless channels, depending on the attacker's capability.

Types of Wormhole Attacks

Wormhole attacks be classified into three main types open, closed, and half- open based on how visible the malicious nodes are during the attack. In an open wormhole attack, the attacker's identity is revealed in the routing path, allowing other nodes to see them as part of the route, even though they manipulate packet transmission. In a closed wormhole attack, the malicious nodes remain completely hidden by tunneling packets without appearing in the routing tables, making detection extremely difficult. The half-open wormhole attack is a hybrid form where only one of the malicious nodes participates openly in routing, while the other stays concealed. Each type of attack affects the network differently, but all share the same goal disrupting routing integrity and misleading nodes about their actual topology. Understanding these variations helps researchers develop targeted detection strategies, such as hop-count analysis, timing constraints, and neighbor verification techniques, to safeguard MANETs from these stealthy threats.

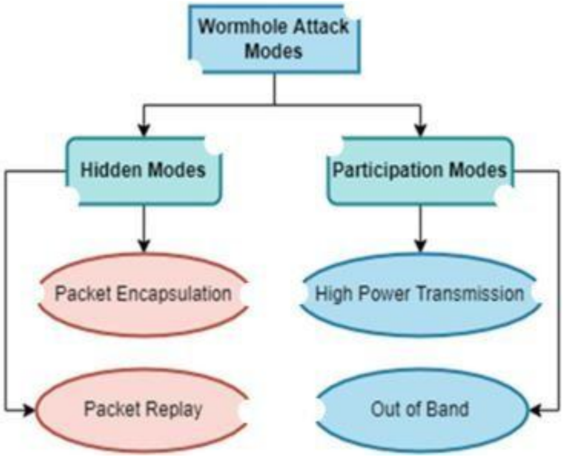


Figure 1.3 Wormhole Attack Modes

1.3 Classification Of Wormhole Detection Techniques

Detecting wormhole attacks in MANETs is a challenging task due to their stealthy behavior and the absence of centralized monitoring systems. Since wormhole links be established without altering packet contents, traditional security methods like encryption or authentication are often ineffective. Therefore, researchers have developed several detection approaches based on timing, location, hop-count, and trust models to identify abnormal routing behaviors. These methods analyze factors such as packet transmission delay, node distance, or route metrics to detect inconsistencies caused by wormhole tunnels. Each detection technique offers its own advantages and limitations depending on network size, node mobility, and energy constraints. The goal is to ensure that detection accuracy is maximized while maintaining network efficiency and minimizing computational overhead. The following subtopics describe three widely used detection approaches that play a key role in defending MANETs against wormhole attacks.

Time-Based Detection Techniques

Time-based methods rely on measuring the time taken for packets to travel between nodes. In normal conditions, packet propagation time depends on the number of hops and the distance between nodes. However, in the presence of a wormhole attack, the packet appears to travel an abnormally short distance within an unrealistically short time, indicating the presence of a tunnel. Techniques like Round Trip Time (RTT) analysis and Temporal Leashes are used to monitor these anomalies. In temporal leash-based detection, each packet includes a timestamp, and if the receiving node detects a delay beyond a set threshold, it suspects a wormhole link. Time-based techniques are effective because wormholes often distort transmission delays; however, their accuracy be affected by synchronization errors or variable propagation speeds in dynamic MANET environments. Therefore, they often require precise clock synchronization among nodes for reliable performance.

Location and Distance-Based Detection Techniques

Location-based detection techniques use the physical positions of nodes to detect suspiciously short routes caused by wormhole tunnels. Each node determines its geographical location using GPS or other localization methods and shares it with neighboring nodes. Based on this information, the geographical leash approach calculates the maximum allowed communication range. If two nodes claim to be direct neighbors but are physically located beyond the radio transmission range, a wormhole is likely present. Distance-based methods also employ signal strength or time-of-flight measurements to estimate node proximity. These techniques are powerful because wormhole attacks often create false neighbor relationships between distant nodes. However, they require additional hardware like GPS modules and not perform well indoors or in environments with high signal interference. Despite these limitations, location-based systems remain one of the most effective strategies for detecting wormhole attacks in geographically constrained MANETs.

Satellite 3
Satellite 1
Satellite 2

Figure: 1.4 Location and Distance-Based Detection Techniques

Hop-Count and Trust-Based Detection Techniques

Hop-count and trust-based methods analyze routing information and node behavior to identify potential wormhole links. In hop-count-based detection, nodes compare the number of hops in a routing path against the expected distance. If the hop count is unusually small for distant nodes, it indicates a wormhole tunnel. On the other hand, trust-based detection assigns trust values to nodes based on their behavior such as packet forwarding rate, response time, and historical reliability. Nodes with low trust values are considered suspicious and isolated from the routing process. These techniques provide dynamic and adaptive detection by continuously monitoring the network. Although hop-count and trust-based methods are lightweight and energy-efficient, they face challenges in highly mobile networks where trust evaluation needs frequent updates. Combining hop- count analysis with trust metrics provides a more robust solution, effectively balancing accuracy, scalability, and computational cost in wormhole detection.

1.4 Impact Of Wormhole Attacks on Routing Protocols

Wormhole attacks have a devastating impact on routing protocols in Mobile Ad Hoc Networks (MANETs) because they directly manipulate the path selection mechanism. Routing in MANETs relies on trust among neighboring nodes and on dynamic route discovery processes like those in AODV, DSR, and OLSR. When a wormhole tunnel is established between two distant nodes, it creates a false perception of a shorter or more efficient path. As a result, most network traffic is rerouted through the malicious nodes. This manipulation leads to packet loss, increased delays, and misrouting of data. It also causes routing table inconsistencies, high overhead, and degradation of network throughput. Since the attackers drop, delay, or modify packets, the overall network reliability and performance are severely affected. Understanding how wormholes exploit routing mechanisms is essential for designing secure, attack-resistant protocols.

Effect on AODV Protocol

The AODV protocol operates by establishing routes on demand using route request (RREQ) and route reply (RREP) messages. In a wormhole scenario, malicious nodes capture the RREQ messages and quickly tunnel them to distant parts of the network, bypassing intermediate hops. This makes the wormhole path appear as the shortest route, tricking legitimate nodes into using it. Once data transmission begins, attackers drop or alter packets, leading to significant packet loss and communication breakdowns. Additionally, because the wormhole link is perceived as a low-latency path, AODV continuously prefers it, even when legitimate routes exist. This behavior not only reduces throughput but also causes routing loops and false route entries. Detecting such manipulations is difficult since the malicious nodes do not modify the RREQ packets. Hence, wormholes severely degrade AODV's reliability and performance, making it one of the most affected protocols in MANETs.

Impact on DSR Protocol

In DSR, every node maintains a route cache containing paths to various destinations. When a node wants to send data, it checks its cache before initiating a route discovery. During a wormhole attack, the malicious nodes tunnel RREQ packets to distant locations, causing the destination to receive them much earlier than normal. This makes the wormhole route appear shorter, and it gets stored in multiple route caches across the network. As a result, data packets are often transmitted through the malicious path, allowing attackers to intercept or drop them. Since DSR relies on stored routes, even after the attack ends, nodes continue using compromised paths from their caches, prolonging the damage. The attack also increases control message overhead due to frequent route rediscovery when data transmission fails. Thus, wormholes not only reduce DSR efficiency but also corrupt the route learning process, undermining the protocol's trust and adaptability.

Consequences on OLSR (Optimized Link State Routing) Protocol

OLSR is a proactive routing protocol where each node periodically exchanges topology information with its neighbors to maintain an updated routing table. Wormhole attacks distort these updates by creating false neighbor relationships. When malicious nodes form a tunnel, distant nodes appear as direct neighbors, leading OLSR to generate incorrect topology maps. This misrepresentation of network structure results in routing errors, loops, and unnecessary retransmissions. Because OLSR frequently exchanges control messages, the attack spread false information quickly across the network. Moreover, the protocol's multipoint relay (MPR) selection process, which optimizes broadcast transmission, also be manipulated by wormholes to gain more control over the routing process. This increases communication latency and bandwidth consumption, while reducing delivery ratio and network stability. In essence, the wormhole attack corrupts the proactive nature of OLSR, compromising both routing accuracy and overall network performance.

1.5 Existing Detection and Prevention Mechanisms

Over the years, numerous detection and prevention mechanisms have been developed to counter wormhole attacks in Mobile Ad Hoc Networks (MANETs). These mechanisms are designed to identify abnormal routing behaviors, detect fake neighbor relationships, and prevent attackers from manipulating network paths. Since wormhole attacks are difficult to detect using traditional cryptographic approaches, researchers have introduced a combination of techniques such as time-based, location-based, hop-count, and trust-driven models. Some methods use packet leash concepts to limit packet travel distance, while others rely on neighbor verification or signal strength analysis. Cryptographic approaches focus on securing packet exchanges, whereas topology- based methods analyze inconsistencies in routing structures. However, each mechanism comes with trade-offs in energy efficiency, computational cost, and detection accuracy. The following subtopics discuss three key categories of existing solutions widely adopted in MANET security research.

Cryptographic and Authentication-Based Methods

Cryptographic mechanisms aim to secure routing communication by ensuring that only authorized nodes exchange valid routing messages. Techniques such as digital signatures, hash chains, and message authentication codes (MACs) are employed to prevent packet alteration and unauthorized transmission. Protocols like Ariadne and SEAD (Secure Efficient Ad hoc Distance vector) integrate cryptographic tools to enhance routing integrity. By authenticating each node and verifying message authenticity, attackers find it harder to inject false routing data or manipulate route discovery. However, while cryptography enhances security, it cannot fully prevent wormhole attacks since malicious nodes tunnel packets without modification. Moreover, cryptographic operations are computationally expensive and drain limited node energy. Hence, although cryptographic-based mechanisms strengthen security against some attacks, they are not sufficient alone to counter wormholes effectively. These methods are often used in combination with other lightweight detection schemes to achieve a balanced and efficient security solution in MANETs.

Packet Leash and Neighbor Verification Techniques

Packet leash methods, first introduced by Hu, Perrig, and Johnson, are among the most effective wormhole detection techniques. A packet leash adds extra information such as time or geographic position into each transmitted packet to restrict its maximum travel distance. There are two primary types: temporal leashes and geographical leashes. Temporal leashes use strict time limits to ensure that packets cannot travel farther than the expected transmission range, while geographical leashes use location data to verify whether nodes claiming to be neighbors are within communication distance. Additionally, neighbor verification protocols confirm the authenticity of adjacent nodes using mutual communication or signal strength analysis. These techniques successfully identify false neighbor relationships caused by wormholes. However, they require accurate time synchronization or GPS-based positioning, which be challenging in high-mobility or resource-constrained environments. Despite these limitations, packet leash and neighbor verification remain foundational tools for detecting and mitigating wormhole attacks in MANETs.

Topology and Statistical-Based Detection Mechanisms

Topology-based detection approaches analyze structural patterns and routing inconsistencies within the network to identify wormholes. By comparing routing metrics such as hop count, link delay, and connectivity degree, these methods detect unusual patterns that indicate the presence of a tunnel. For instance, a wormhole often results in an abnormally high number of connections between nodes that are physically distant, which be detected through graph-based analysis. Similarly, statistical detection methods use data such as packet arrival time, routing frequency, or neighbor count variations to distinguish normal behavior from attacks. These methods are lightweight and require minimal additional hardware, making them suitable for energy-limited MANET nodes. However, they generate false alarms under conditions of high mobility or fluctuating signal strength. To improve accuracy, modern implementations combine topology-based monitoring with machine learning or trust models to dynamically adapt to changing network conditions while maintaining effective wormhole detection.

1.6 Machine Learning and Intelligent Detection Approaches

With the growing complexity of network attacks, traditional rule-based and cryptographic methods often fail to detect advanced wormhole activities in MANETs. To overcome these limitations, researchers have begun integrating machine learning (ML) and artificial intelligence (AI) techniques into wormhole detection systems. These intelligent models analyze large sets of network data, recognize hidden attack patterns, and make adaptive decisions based on real-time observations. ML algorithms learn from normal and abnormal routing behaviors, enabling the system to detect wormholes dynamically even under changing network conditions. Techniques such as supervised learning, unsupervised clustering, and deep learning models are increasingly applied for automated intrusion detection. Unlike static threshold-based systems, intelligent models update themselves continuously, improving detection accuracy and reducing false positives. The following subtopics discuss the primary categories of ML-based approaches for wormhole detection in MANETs.

Supervised Machine Learning Models

Supervised learning approaches rely on labeled datasets, where normal and malicious behaviors are clearly defined for training. Algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forests, and Naïve Bayes classifiers are commonly used to detect wormhole attacks. These models analyze features such as hop count, packet delay, link quality, and signal strength to distinguish between legitimate and malicious routes. During the training phase, the classifier learns the patterns associated with wormhole activities, such as unrealistically short path lengths or high link reliability between distant nodes. Once trained, the model predicts whether a new routing pattern indicates a possible wormhole. Supervised models are highly accurate when trained on comprehensive datasets; however, their performance degrade in dynamic networks with unseen attack patterns. Therefore, continuous retraining and feature updating are essential to ensure the system adapts effectively to evolving network conditions and attack strategies.

Unsupervised and Clustering-Based Detection Methods

Unsupervised learning approaches are effective when labeled data are unavailable. These methods identify anomalies by grouping similar network behaviors and flagging outliers as potential attacks. Techniques like K-Means clustering, DBSCAN, and Self-Organizing Maps (SOM) are popular for detecting wormhole attacks without prior knowledge of attack signatures. By analyzing parameters such as node density, transmission delay, or signal distance, unsupervised algorithms automatically detect irregular connections that indicate tunneling behavior. One of their key advantages is adaptability—since they do not depend on pre-labeled data, they function effectively in real-time, self-organizing MANETs. However, unsupervised techniques sometimes produce false positives, especially when legitimate network variations resemble attack behaviors. Combining clustering with statistical filtering or fuzzy logic help refine results and enhance detection precision. Overall, these methods provide a flexible and efficient solution for detecting hidden or unknown wormhole activities in dynamic environments.

Deep Learning and Hybrid Intelligent Systems

Deep learning (DL) and hybrid intelligent systems represent the most advanced direction in wormhole attack detection research. Deep Neural Networks (DNN), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN) are capable of learning highly complex temporal and spatial patterns from network data. For example, an LSTM-based model analyzes time-series routing data to detect sudden latency reductions caused by wormholes, while CNNs capture topological features from connectivity matrices. Moreover, hybrid frameworks combining ML with fuzzy logic, genetic algorithms, or swarm intelligence enhance decision-making accuracy and robustness. These models dynamically adapt to environmental changes and handle large-scale MANETs with high node mobility. The integration of AI-based optimization further improves feature selection and reduces computational costs. Though deep learning requires more processing power, its capability to achieve real-time detection with minimal human intervention makes it a powerful tool for intelligent MANET security systems.

1.7 Future Research Directions and Challenges

The detection and prevention of wormhole attacks in MANETs remain an active research area, given the evolving complexity of attack mechanisms and the dynamic nature of mobile ad hoc networks. As technology advances, attackers develop more sophisticated techniques to exploit routing protocols, making it essential for researchers to explore adaptive and intelligent defense mechanisms. Future research should focus on developing hybrid detection systems that combine machine learning, cryptographic techniques, and trust-based mechanisms to improve accuracy and reduce false positives. Moreover, lightweight solutions that consume minimal power and bandwidth are needed for mobile environments with limited resources. The integration of blockchain technology and AI-based trust models provide new avenues for secure routing and authentication in MANETs.

However, scalability, mobility handling, and real-time detection remain challenging factors. Continuous evaluation of proposed models in real-world and large-scale simulations is crucial to ensure practical applicability and robustness against evolving threats.

Artificial Intelligence and Machine Learning in Wormhole Detection

Machine learning (ML) and artificial intelligence (AI) are emerging as powerful tools for detecting complex network attacks like wormholes in MANETs. By analyzing network traffic patterns and identifying deviations from normal behavior, AI-based systems detect anomalies with high precision. Techniques such as deep learning, reinforcement learning, and ensemble methods be used to create adaptive detection frameworks capable of learning from evolving attack scenarios. Unlike traditional methods, ML models generalize across diverse network conditions and topologies, making them highly efficient for mobile environments. Additionally, unsupervised learning approaches be applied where labeled data is unavailable, enhancing flexibility in unknown scenarios. Researchers are also focusing on integrating explainable AI (XAI) to make detection decisions transparent and interpretable. However, challenges such as data scarcity, high computational cost, and overfitting must be addressed for real-world adoption.

Blockchain-Based Secure Routing Mechanisms

Blockchain technology offers a decentralized and tamper-proof framework that significantly enhance the security of MANETs. By storing routing information in immutable ledgers, blockchain ensures data integrity and prevents malicious alterations during communication. In the context of wormhole detection, blockchain be employed to verify the authenticity of nodes and their routing activities through consensus algorithms. This eliminates the need for centralized control, which is often a target of attacks. Furthermore, smart contracts automate security policies, enabling real-time validation of routes and transactions. However, integrating blockchain in MANETs introduces computational and energy overheads, which be challenging for mobile devices. Ongoing research aims to design lightweight blockchain frameworks and consensus mechanisms optimized for mobile and dynamic networks. Despite these limitations, blockchain remains a promising direction for enhancing trust and transparency in ad hoc communications.

Lightweight Cryptographic Solutions and Energy Efficiency

Energy efficiency is a critical concern in MANETs, where nodes rely on limited battery power and computational capacity. Implementing cryptographic mechanisms for security often introduces additional overhead, leading to faster energy depletion. Therefore, future research must focus on designing lightweight cryptographic algorithms that balance security and energy consumption. Techniques such as elliptic curve cryptography (ECC) and symmetric key encryption offer strong protection with reduced computational requirements. Additionally, adaptive cryptographic frameworks that adjust security levels based on network context and node energy status enhance sustainability. Energy-aware routing combined with secure key distribution further minimize resource utilization while maintaining defense against wormhole attacks. The ultimate goal is to create an integrated system that ensures confidentiality, integrity, and availability without compromising the operational lifespan of the network.

1.8 Objectives

- To develop efficient detection techniques that accurately identify wormhole attacks in MANETs under diverse mobility patterns and dynamic network topologies, ensuring reliability in various real-time environments.
- To enhance overall network security and reliability by preventing unauthorized tunneling of data and malicious link formation that disrupt communication paths and degrade performance.
- To minimize computational, bandwidth, and energy overheads in the detection process, thereby creating lightweight mechanisms suitable for resource-constrained mobile nodes in MANETs.
- To improve the integrity of routing protocols by integrating wormhole detection systems seamlessly with existing protocols such as AODV, DSR, and OLSR for secure route discovery and maintenance.
- To enable real-time monitoring, detection, and prevention of wormhole attacks through adaptive and automated systems capable of handling fast-changing MANET environments effectively.

1.9 Advantages

- Wormhole detection enhances the overall network security by preventing attackers from creating false routes and manipulating data transmission within the MANET.
- It improves data reliability and communication integrity, ensuring that messages are delivered through legitimate nodes without interception or

alteration.

- The detection system helps in maintaining network performance by reducing packet loss, routing delays, and congestion caused by malicious tunnels.
- Implementing wormhole detection techniques increases the trust and stability of MANETs, making them more suitable for critical applications like military, disaster recovery, and emergency communications.

1.10 Applications

- Military communication systems
- Disaster recovery networks
- Emergency rescue operations
- Vehicular ad hoc networks
- Remote sensing systems

1.11 Thesis Organization

- Chapter 2: Literature Survey
- Chapter 3: Current System
- Chapter 4: Proposed system
- Chapter 5: Results and Discussions
- Chapter 6: Conclusions and future scope
- Chapter 7: Reference

II. LITERATURE SURVEY

Mobile Ad-hoc Networks (MANETs) represent a paradigm shift in wireless communication, forming self-configuring, infrastructure-less networks of mobile devices connected via wireless links. This decentralized architecture grants MANETs unparalleled flexibility and rapid deploy ability, making them indispensable for critical applications such as military battlefields, disaster relief operations, and emergency communications. However, the very features that make MANETs attractive their dynamic topology, absence of a central authority, and reliance on multi-hop routing also render them profoundly vulnerable to a wide spectrum of security threats. Among these, the wormhole attack is considered one of the most severe and challenging to defend against. In a wormhole attack, a malicious actor tunnels network packets received at one point in the network to another distant point, replaying them there. This creates a virtual, high-speed link the "wormhole" that disrupt routing protocols by creating the illusion that two distant nodes are neighbors. The consequences are dire: traffic is lured through the wormhole path where it be eavesdropped upon, selectively dropped, or analyzed to launch further sophisticated attacks, effectively compromising the network's confidentiality, integrity, and availability.

The insidious nature of the wormhole attack lies in its ability to function without compromising cryptographic keys or node identities, making it difficult to detect using conventional authentication mechanisms. Early research into wormhole mitigation primarily focused on specialized hardware, such as directional antennas, tightly synchronized clocks, or GPS receivers for location verification. While effective in theory, these approaches often proved impractical for genuine MANET scenarios, which are characterized by resource-constrained nodes and a need for lightweight, scalable solutions. Consequently, the research community has witnessed a significant pivot towards software-based, protocol- level detection techniques. These methods be broadly categorized into statistical, topological, and trust-based approaches. Statistical methods, such as monitoring packet delivery ratios (PDR) and round-trip times (RTT), aim to identify the anomalous latency and throughput characteristics induced by the wormhole tunnel. Topological approaches analyze the network's graph structure to detect the unnatural network distortions caused by the wormhole link, often by examining neighborhood lists or using specialized packets like "boomerang" packets to probe for inconsistencies.

More recently, the escalating arms race between network attackers and defenders has catalyzed the adoption of sophisticated artificial intelligence (AI) and machine learning (ML) paradigms. The dynamic and non-linear nature of MANETs generates vast amounts of data, which traditional algorithms struggle to analyze in real-time. Machine learning models, particularly deep learning with Long Short-Term Memory (LSTM) networks, are increasingly being deployed to identify complex, multi-faceted attack patterns, including wormholes, by learning from historical network traffic data. Furthermore, the emergence of bio-inspired optimization algorithms like Particle Swarm Optimization (PSO) has provided powerful tools for optimizing detection parameters and minimizing false positives. The frontier of research continues to expand, exploring revolutionary concepts such as digital twin technology to create virtual replicas of the network for safe attack analysis and game theory to model the strategic interactions between malicious and legitimate nodes. Quantum-inspired computing models are also being investigated for their potential to perform resilient pathway discovery at unprecedented speeds. This literature survey aims to provide a comprehensive and critical analysis of the evolution of wormhole attack detection mechanisms in MANETs. It will trace the trajectory from foundational hardware-dependent solutions to contemporary intelligent, adaptive systems, evaluating their respective strengths, limitations, and applicability, thereby offering a clear panorama of the state-of-the-art and illuminating promising pathways for future research.

Mukul Shukla *et al* [2021] proposed “A Trust-Based Approach to Mitigate Wormhole Attacks in Mobile Adhoc Networks,” which introduces a trust evaluation mechanism to enhance security in MANETs. The approach assigns trust values to nodes based on key parameters such as packet receiving time and data rate to detect malicious behavior caused by wormhole links. Nodes with low trust scores are isolated to prevent disruption in routing. Simulation results reveal that the proposed trust-based scheme significantly improves Packet Delivery Ratio (PDR) and throughput while maintaining low end-to-end delay, even under attack conditions. The study demonstrates that integrating trust-based metrics effectively strengthens network resilience and ensures stable communication in dynamic and infrastructure-less MANET environments.

Joonsu Ryu *et al* [2024] proposed a trust-based and multiple verification mechanism to enhance wormhole attack detection in Mobile Ad Hoc Networks (MANETs). The approach employs a dynamic trust evaluation system that assigns and updates credit values for each node based on behavioral analysis during routing. Nodes exhibiting suspicious behavior experience reduced trust levels, and those falling below a specific threshold are identified as malicious. Reinforcement learning is integrated to continuously refine the trust system, improving detection accuracy over time. Simulation results indicate that the method significantly reduces data transmission through malicious routes, enhances overall routing reliability, and strengthens the resilience of MANETs against wormhole attacks.

Tahboush and Agoyi *et al* [2021] address the significant security threat of wormhole attacks in Mobile Ad-hoc Networks (MANETs), where malicious nodes tunnel network packets to undermine routing protocols. The authors identify that existing detection solutions often suffer from drawbacks such as dependency on special hardware, high delivery delays, low throughput, and high energy consumption. To overcome these limitations, they propose a Hybrid Wormhole Attack Detection (HWAD) algorithm. The HWAD algorithm is designed to detect both in-band wormholes by analyzing Round Trip Time (RTT) and Packet Delivery Ratio (PDR), and out-of-band wormholes by assessing the transmission range between nodes. A key efficiency feature of HWAD is that it reduces delay and energy consumption by avoiding universal node detection. The algorithm, which requires no special hardware, was simulated using NS-2 with the AODV routing protocol. Performance evaluation based on throughput, end-to-end delay, PDR, and energy consumption demonstrated that the proposed HWAD approach outperformed other comparable algorithms in wormhole detection.

Rathore and Sarkar et al [2024] propose a comprehensive security framework to defend Wireless Sensor Networks (WSNs) against wormhole attacks. The authors develop a multi-layered algorithm that integrates key distribution, packet timestamping, location-based detection using RSSI, and wormhole detection via probe packets. A central feature of their approach is the use of the Twofish algorithm for both establishing a shared key and encrypting data packets. In the event a wormhole is detected, the proposed method isolates the compromised network segment to prevent further damage. The efficacy of this integrated system was validated through NS-2 simulations, with results demonstrating that the approach significantly enhances the security and reliability of WSNs.

Rajalakshmi *et al* [2023] address the challenge of securing Mobile Ad-hoc Networks (MANETs) against multiple routing attacks, including Black Hole, Gray Hole, and Worm Hole attacks. The authors note that traditional Intrusion Detection Systems (IDS) and protection methods are insufficient for the dynamic topology of MANETs. To overcome this, they propose a hybrid Black Hole, Gray Hole, Neuro-Fuzzy (BGNF) based Intrusion Detection System. This system is enhanced with Particle Swarm Optimization (PSO) to optimize detection, minimize false alarms, and reduce data loss. The proposed approach provides a comprehensive solution that not only detects but also prevents the generation of these security attacks in a self-sustaining manner.

Bhawsar *et al* [2020] propose a trust-based routing system to counter wormhole attacks in MANETs. Acknowledging the difficulty of preventing such attacks due to the network's lack of fixed infrastructure, their method integrates attack detection directly into the AODV routing protocol. The core of their approach involves trust calculation and multiple path selection to identify the most secure route. When a node is detected as a wormhole, the system dynamically selects an alternative path from the available options. This mechanism significantly improves network performance, with reported results showing a 71.25% improvement in Packet Delivery Ratio (PDR), a throughput increase of 74.09 kbps, and a reduction in end-to-end delay of 57.92 ms for a 125-node network.

Rajkumar *et al* [2024] propose a novel security framework to mitigate wormhole attacks in MANETs. The core of their approach involves selecting an admin node from a pool of trusted nodes. This admin node periodically sends a boomerang packet a packet destined to return to itself throughout the network. By analyzing the state of the returning boomerang packet, the admin node determines if the packet traversed a wormhole link. If an attack is detected, immediate preventive measures are taken. The authors conducted exhaustive experiments in the NS-3.26 simulator, demonstrating that their strategy achieves a high detection accuracy of 97%. Furthermore, the method results in a lower packet loss rate compared to other state-of-the-art solutions, attributed to its early and accurate detection capability.

Kumar *et al* [2022] propose a Cluster-Based Algorithm (CBA) to detect hybrid wormhole attacks in MANETs. The authors note that existing solutions often result in high delivery delays, poor packet delivery ratios, and excessive energy consumption. Their CBA model uses a combination of sequence number analysis and Round-Trip Time (RTT) to detect both in-band and out-of-band wormhole connections. A key feature is the use of predicted RTT thresholds to distinguish between attack routes and non-attack routes. The proposed algorithm was implemented and tested in the NS-2 simulator. Performance evaluation demonstrated that the CBA model successfully reduced the total energy consumption by 20% compared to the traditional AODV routing protocol, while also improving throughput.

Chourasia and Tokekar *et al* [2024] propose a novel security framework that leverages Reinforcement Learning (RL) to mitigate multiple routing attacks—namely wormhole, blackhole, and grayhole—in MANETs. The authors utilize a flexible actor-critic architecture to implement the RL model, enabling the system to learn and adapt to complex attack patterns that are difficult to detect with traditional methods. The primary objective is to identify these intricate threats and enhance network security by detecting and blocking malicious nodes. Simulation results confirm that the proposed RL-based policy efficiently mitigates the combined threat of wormhole, blackhole, and grayhole attacks, demonstrating the potential of machine learning for proactive security in dynamic ad-hoc environments.

Praveenkumar *et al* [2024] propose a novel resource allocation strategy to mitigate wormhole attacks in MANETs. The core of their approach is the application of Cox Regression techniques to calculate regression coefficients that model the association between mobile nodes. This model is used to identify optimal paths for routing based on key metrics like residual energy, delay, and bandwidth. By proactively selecting robust paths, the method aims to disrupt the deceptive shortcuts created by wormhole attacks. The proposed strategy enhances network security and performance, leading to improvements in the packet delivery rate, reduced latency, and an extended network lifetime for data transmission.

Nausheen and Upadhyay *et al* [2023] address the critical security challenges in MANETs, which are exacerbated by inherent flaws such as the lack of authorization, infrastructure, and dynamic node mobility. The authors emphasize that multiple concurrent attacks have a more severe impact on network performance and power efficiency than single attacks. In response to the rising demand for robust security where fully secure protocols remain elusive, this study introduces a novel approach designed to simultaneously detect a combination of routing threats, specifically blackhole, grayhole, and wormhole attacks. The proposed method aims to enhance the overall security effectiveness in the complex and vulnerable MANET environment.

Alenezi *et al* [2021] propose a novel countermeasure, SWANS, to address the challenge of wormhole attacks in Software-Defined MANETs. The authors highlight that existing security measures for wired Software-Defined Networks (SDNs) are unsuitable for the dynamic MANET environment. The SWANS approach leverages the centralized view of an SDN controller to analyze the similarity of neighbor counts across nodes. This method effectively detects wormholes without relying on location information and avoids significant communication overhead. Furthermore, SWANS is designed to counter false positives and negatives caused by vulnerabilities in the Link Layer Discovery Protocol (LLDP). Extensive simulations confirm that SWANS efficiently and accurately detect various intelligent wormhole attacks while maintaining low false-positive and false-negative rates.

Gotti *et al* [2023] address the security vulnerabilities of MANETs by developing an Intrusion Detection System (IDS) to combat blackhole attacks. Their methodology involves simulating a 25-node network with both TCP and UDP connections and extracting various network characteristics from the generated trace files. The core of their approach lies in the application of multiple machine learning algorithms to analyze these characteristics and identify the presence of a malicious blackhole node. This data-driven technique presents a novel method for building an efficient IDS capable of detecting intruders that exploit the infrastructure-less nature of MANETs.

Aravind and Poongodi *et al* [2025] introduce a novel algorithm named Quantum Resilient Pathway Discovery for Attack Mitigation (QR-PDAM) to address security threats like wormhole attacks in MANETs. The proposed framework leverages quantum-inspired methods for zone discovery and resilient path exploration to dynamically identify optimal and secure communication pathways. This approach is designed to be highly adaptive to the network's changing topology, thereby avoiding vulnerabilities and ensuring robust security alongside energy efficiency. Performance evaluation demonstrates that QR- PDAM significantly outperforms conventional schemes like SAODV and THR across key metrics, including reduced energy consumption, lower latency, higher packet delivery ratio, and improved throughput. The authors conclude that QR- PDAM is a superior candidate for mission-critical applications in dynamic and adversarial network environments.

Raj and Durga *et al* [2025] propose a hardware-accelerated Intrusion Detection and Prevention System (IDPS) to counter cyber threats in MANETs. Their system employs two AI models Random Forest (RF) and a Convolutional Neural Network (CNN) to identify network attacks and anomalies. Experimental results indicate that the CNN model outperformed RF in terms of accuracy and precision for detecting malicious traffic. The proposed IDPS demonstrated a high efficacy with an 83% network attack detection rate and a 91% anomaly identification rate. The authors conclude that hardware-driven AI processing is essential for real-time MANET security, as it significantly reduces latency and improves detection accuracy, thereby facilitating secure communication for mission-critical applications.

Jebakumar Immanuel *et al* [2022] focus on developing a secure routing protocol to counter malicious attacks in the dynamic MANET environment. They introduce a Protected AODV (PAODV) protocol, which integrates a dynamic anomaly detection scheme into the standard AODV routing protocol. The core objective of PAODV is to identify false alarm nodes within the network and establish a reliable communication path from source to destination. Simulation results demonstrate that the proposed PAODV protocol improves the detection rate while simultaneously minimizing packet drop rate and delay compared to existing techniques, thereby enhancing both the security and performance of data dissemination.

Messabih *et al* [2025] propose a novel security mechanism named Digital Twin-Based Stackelberg Game for AODV (DTSGAODV) to counter sophisticated attacks in MANETs. The proposed framework operates across two layers: a physical layer that gathers real-time network data, and a digital layer that uses this information to model the network. The digital twin leverages a Stackelberg game theory model to strategically select optimal reference nodes, enabling the construction of secure routes between sources and destinations without modifying the underlying AODV protocol. When evaluated under selfish attacks, the DTSGAODV mechanism demonstrated superior performance by achieving the highest packet delivery ratio and a minimal attack success rate compared to the standard AODV protocol, proving its efficacy in enhancing security without disrupting established network operations.

Nara *et al* [2025] conduct a comprehensive study focused on enhancing security and network lifetime in MANETs through advanced clustering and routing techniques. The research addresses threats like wormhole, gray-hole, and blackhole attacks by employing a trust-based optimization method. This methodology leverages fuzzy-based algorithms and optimization techniques such as Particle Swarm Optimization (PSO) and the Crow Search Algorithm to improve cluster head selection and identify optimal routing paths. The performance of the proposed secure clustering and routing models was evaluated in MATLAB, with key metrics including end-to-end delay, latency, throughput, and Packet Delivery Rate (PDR) used to assess their effectiveness in preventing network security breaches.

Suryadevara et al [2025] propose a novel transfer learning model utilizing Long Short-Term Memory (LSTM) networks to detect a wide range of anomalies including DoS, DDoS, Sybil, Sinkhole, Wormhole, and Blackhole attacks in data streaming environments such as VANETs. The research addresses the challenge of high false positive rates in existing methods by leveraging LSTM's inherent features, like the forget gate, to manage continuous data flow and eliminate redundant information. This integrated approach, which encompasses preprocessing, feature extraction, and classification, ensures high- quality data analysis. Simulation results implemented in Python demonstrate that the model achieves higher accuracy, lower latency, and increased throughput, making it a suitable and effective solution for real-time applications in IoT and cybersecurity.

Marah Knaj *et al* [2023] proposed "Detecting and Mitigating Wormhole Attack Effect in MANETs Based on Hop Count Technique," which focuses on enhancing the security of Mobile Ad Hoc Networks (MANETs) by identifying and mitigating wormhole attacks. The authors analyze the impact of single and multiple tunnel wormhole scenarios on network performance metrics such as Average Throughput, Packet Delivery Ratio (PDR), and End-to-End Delay. A hop count–based detection technique is implemented to recognize abnormal routing paths caused by malicious tunnels. Simulation experiments conducted using NS-
2.35 demonstrate that the proposed approach effectively mitigates the wormhole attack's impact while maintaining higher throughput and packet delivery ratio.

III. EXISTING SYSTEM

The existing an innovative hybrid security framework for Mobile Ad Hoc Networks (MANETs) by integrating the Invasive Weed Optimization Algorithm (IWOA) with a Generative Adversarial Network (GAN) to enhance the performance of Intrusion Detection Systems (IDS). MANETs are self-configuring, decentralized networks consisting of mobile nodes that communicate wirelessly without any fixed infrastructure. Due to their dynamic topology, open communication medium, and lack of centralized control, MANETs are highly vulnerable to various security threats such as unauthorized access, routing attacks, blackhole attacks, wormhole attacks, Sybil attacks, and denial-of-service (DoS) attempts. These vulnerabilities can severely degrade the performance, reliability, and security of the network, making the development of an effective and intelligent intrusion detection mechanism essential.

The existing hybrid framework leverages the strength of the Invasive Weed Optimization Algorithm (IWOA) to improve the feature selection process. IWOA is a nature-inspired metaheuristic optimization algorithm that mimics the colonization and reproduction behavior of weeds in nature. In this context, IWOA is employed to identify, select, and prioritize the most significant and relevant features from the network dataset, which are crucial for accurate classification of normal and malicious activities. The algorithm ensures that redundant or irrelevant features are minimized, thereby reducing the computational complexity and improving the detection efficiency of the system. By optimizing the feature subset, IWOA contributes to higher classification accuracy and a lower false alarm rate, which are vital for maintaining reliable intrusion detection in real-time network environments. The GAN component provides a deep learning-based classification mechanism using a generator and discriminator. The discriminator classifies network traffic as normal or malicious, while the generator creates synthetic samples to improve detection capability. This adversarial process helps the model learn complex and evolving intrusion patterns. Combined with IWOA, the framework ensures optimal feature selection, improving classification accuracy and reducing false positives. The hybrid IWOA-GAN system is efficient, adaptive, and suitable for dynamic MANET environments. The system is implemented and tested using NS-2 simulations, showing better performance in detection accuracy, false alarm rate, and computational efficiency compared to traditional methods.

3.1 Existing Block Diagram

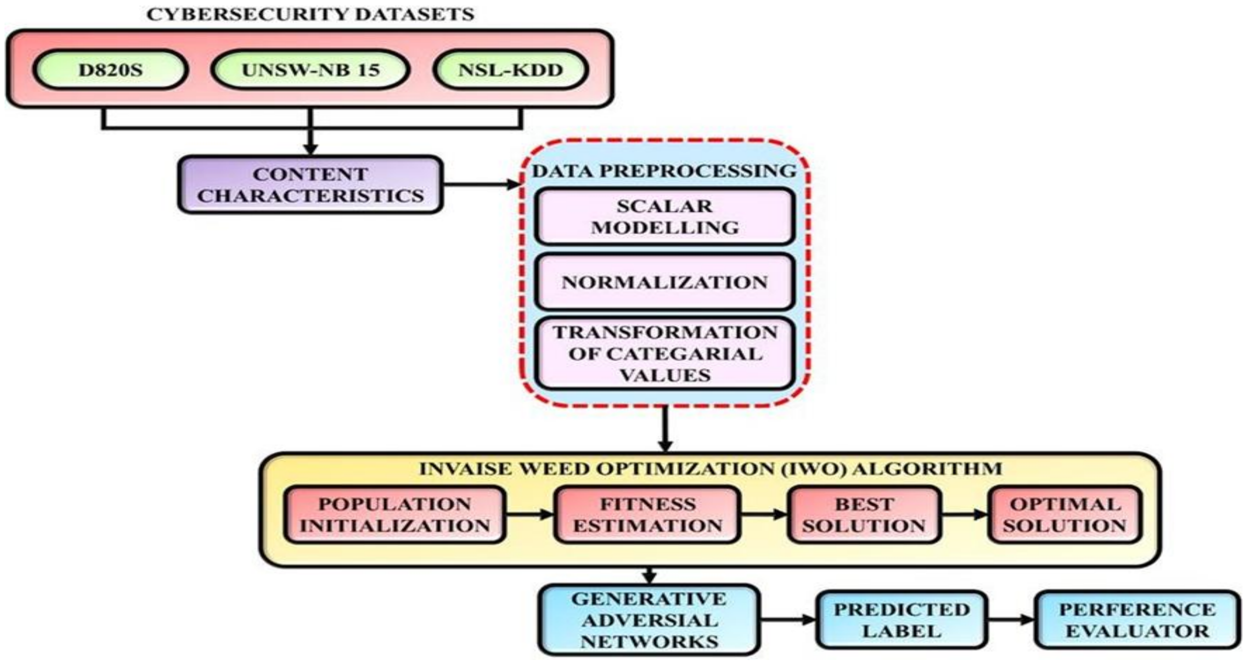


Figure 3.1 Block Diagram of Existing System

Cybersecurity Datasets

The diagram presents a hybrid intrusion detection framework combining IWO and GAN for cybersecurity. It starts with datasets like DDoS, UNSW-NB15, and NSL-KDD, from which important network features are extracted. These features undergo preprocessing, including scaling, normalization, and categorical conversion to prepare the data for learning. The processed data is then optimized using the Invasive Weed Optimization (IWO) algorithm, which selects the most relevant features based on performance. These optimal features are fed into a Generative Adversarial Network (GAN), where the discriminator classifies traffic as normal or malicious. Finally, the system evaluates performance using metrics like precision, recall, and detection accuracy, ensuring effective and robust intrusion detection.

Content Characteristics

Content characteristics are the key features extracted from cybersecurity datasets like DDoS, UNSW-NB15, and NSL-KDD that describe network behavior. These include attributes such as IP addresses, ports, protocols (TCP/UDP/ICMP), packet size, duration, and data transfer details. They help identify relevant information for intrusion detection, such as connection patterns, traffic behavior, and suspicious activities like failed logins or unusual access. By selecting important features, the system can distinguish between normal and malicious traffic. These characteristics are then preprocessed and converted into numerical form for machine learning models, enabling accurate detection and classification of cyber-attacks.

Data Preprocessing

Data preprocessing is an essential step in machine learning and cybersecurity frameworks to ensure clean, consistent, and usable data. It includes three main processes: scalar modeling, normalization, and categorical transformation. Scalar modeling standardizes numerical features so all attributes contribute equally. Normalization scales values (typically between 0 and 1) to improve model performance and convergence. Categorical transformation converts non-numeric data into numerical form using encoding techniques. Overall, preprocessing improves data quality and enhances model accuracy for effective training and classification.

Invasive Weed Optimization (IWO)

Invasive Weed Optimization (IWO) is a population-based metaheuristic algorithm inspired by the natural growth and colonization process of weeds in an ecosystem. It imitates how weeds spread, reproduce, and compete for survival in a given environment, gradually converging toward optimal solutions. The algorithm begins with the random initialization of a population of seeds, each representing a potential solution to the problem. In the context of intrusion detection, each seed corresponds to a subset of selected network features. These seeds are evaluated using a fitness function that measures their effectiveness in improving detection accuracy and minimizing false alarms.

Seeds with higher fitness produce more offspring, which are dispersed randomly within the search space to explore new regions and maintain diversity. Over time, as generations evolve, weaker solutions are eliminated and only the fittest individuals survive. The dispersion rate gradually decreases, allowing the algorithm to fine-tune around promising areas and avoid premature convergence. Generative Adversarial Network

A Generative Adversarial Network, commonly known as GAN, is a deep learning framework that consists of two competing neural networks called the generator and the discriminator. These two networks work in opposition to each other in a process known as adversarial learning. The generator's role is to create synthetic data samples that closely resemble real data, while the discriminator's task is to distinguish between genuine and generated data. During training, the generator continuously improves its ability to produce realistic outputs, and the discriminator becomes more skilled at detecting fake samples.

Predicted Labels

Predicted labels refer to the final output generated by a machine learning or deep learning model after it processes the input data. In an intrusion detection system, the model analyzes network traffic features and classifies each data instance as either normal or malicious. This classification result is called the predicted label. These predicted labels are then compared with the actual labels from the dataset to evaluate the model's accuracy, precision, recall, and other performance metrics. In the IWOA-GAN framework, predicted labels help measure how effectively the model can detect attacks and differentiate between safe and harmful network activities. Preference Evaluator

A preference evaluator is the final assessment stage in the IWOA- GAN intrusion detection framework, used to measure how well the model performs after classification. Once the Generative Adversarial Network

(GAN) produces predicted labels for the network traffic data, the preference evaluator compares these predictions with the actual labels from the dataset to evaluate the system's overall performance.

3.2 Drawbacks Of Existing System

- The integration of IWOA and GAN increases computational complexity significantly, leading to higher processing time, increased resource consumption, and difficulty in deploying the system in real-time environments.
- GAN training is often unstable and requires careful parameter tuning, which may lead to issues like mode collapse, reducing the reliability

and consistency of intrusion detection performance.

- The overall system performance heavily depends on the quality, size, and diversity of the training dataset, making it less effective when handling unseen or imbalanced network attack patterns.
- Implementing the hybrid model in resource-constrained MANET nodes is challenging due to limited memory, processing power, and energy availability, affecting real-time intrusion detection capabilities.
- The use of NS-2 simulation may not accurately represent real-world MANET conditions, limiting the practical applicability and reliability of the intrusion detection framework in real deployments.

3.3 Conclusion

In conclusion, the hybrid IWOA-GAN framework provides an effective and intelligent intrusion detection solution for MANETs. By combining optimal feature selection with advanced deep learning classification, the system achieves high detection accuracy, reduced false alarms, and improved adaptability to dynamic network conditions. Despite challenges like computational cost and training complexity, the framework demonstrates strong potential for enhancing MANET security and serves as a promising foundation for future research in secure wireless communication systems.

IV. PROPOSED SYSTEM

This project presents an innovative and intelligent security framework for Mobile Ad hoc Networks (MANETs) by integrating Particle Swarm Optimization (PSO) with a Generative Adversarial Network (GAN) to enhance the performance of Intrusion Detection Systems (IDS). MANETs are decentralized and self- configuring wireless networks where mobile nodes communicate without fixed infrastructure. Although this flexibility supports applications such as military communication, disaster recovery, and remote sensing, it also makes MANETs highly vulnerable to security threats. Common attacks include unauthorized access, packet dropping, blackhole and wormhole attacks, Sybil attacks, and denial-of-service (DoS) attacks. The absence of centralized control and dynamic topology further increases these vulnerabilities, making efficient IDS solutions essential.

To overcome these challenges, the proposed framework employs PSO as a feature selection and optimization technique. PSO is inspired by the social behavior of bird flocking, where each particle represents a potential solution. These particles iteratively update their positions based on personal best and global best values to identify the optimal subset of features. This process reduces dimensionality, removes redundant data, and improves detection efficiency while minimizing computational cost.

The optimized features are subsequently fed into a GAN-based classification module, which plays a crucial role in enhancing cybersecurity threat detection. A Generative Adversarial Network (GAN) consists of two primary components: a generator and a discriminator. The generator is responsible for producing synthetic network traffic samples that closely resemble real data, while the discriminator evaluates these samples and classifies them as either normal or malicious. Through this adversarial learning process, both components continuously compete and improve, enabling the discriminator to become highly effective in identifying even complex and previously unseen cyber-attacks.

This adversarial mechanism significantly enhances the model’s ability to generalize across diverse and evolving threat patterns, which is essential in dynamic and decentralized environments such as Mobile Ad Hoc Networks (MANETs). By leveraging the feature optimization capability of Particle Swarm Optimization (PSO) and the powerful pattern recognition ability of GANs, the proposed framework ensures robust and intelligent threat detection.

The system is trained and validated using well-known benchmark datasets, including NSL-KDD, UNSW-NB15, and D820S, which provide a wide range of normal and attack traffic scenarios. To further evaluate real-world applicability, simulations are conducted using the NS-2 network simulator under varying network conditions, such as changes in node density, mobility, and traffic load.

Comprehensive performance evaluation is carried out using multiple metrics, including accuracy, precision, recall, F1-score, false alarm rate, and computational efficiency. These metrics ensure a balanced assessment of both detection capability and system performance. Experimental results clearly indicate that the proposed PSO-GAN framework outperforms traditional machine learning and standalone deep learning approaches. It achieves higher detection accuracy, significantly reduces false positives, and demonstrates strong adaptability to changing network behaviors.

Overall, this integrated PSO-GAN approach provides a scalable, efficient, and intelligent solution for optimizing cybersecurity threat detection, making it highly suitable for securing dynamic and resource-constrained MANET environments against sophisticated and emerging cyber threats.

4.1 Proposed Block Diagram

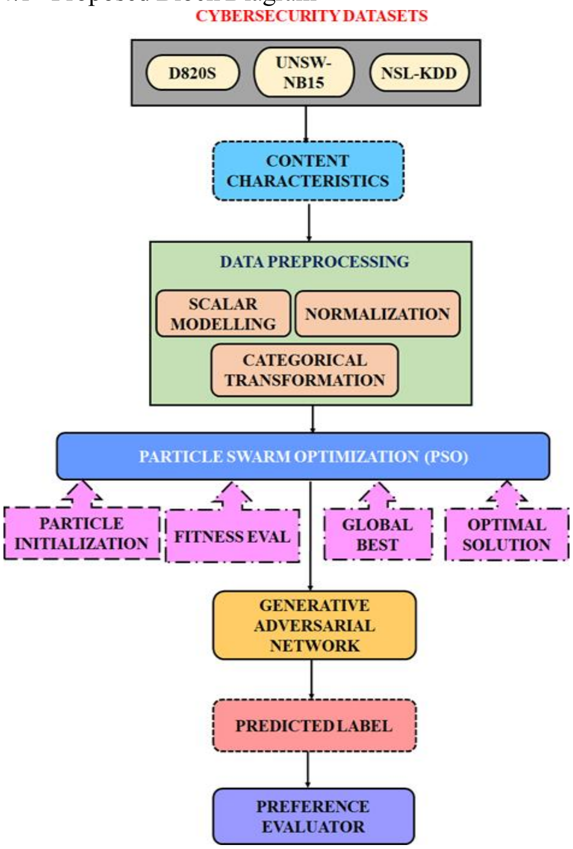


Figure 4.1 Block Diagram of proposed System

4.2 Cybersecurity Datasets

The given diagram illustrates a hybrid intrusion detection framework integrating the Invasive Weed Optimization (IWO) algorithm and Generative Adversarial Networks (GAN) for cybersecurity applications. The process begins with cybersecurity datasets such as DDoS, UNSW-NB15, and NSL-KDD, which contain network traffic data with labeled attack and normal instances. From these datasets, content characteristics are extracted to identify essential network parameters like packet type, protocol, connection duration, and source–destination details. The next step is data preprocessing, which involves scalar modelling, normalization, and transformation of categorical values. Scalar modelling converts numerical data into standardized formats, normalization scales all features into a uniform range to improve algorithm convergence, and categorical transformation converts non-numeric data into machine-readable form.

After preprocessing, the refined data is passed to the Invasive Weed Optimization algorithm. In this stage, population initialization creates a set of random candidate solutions, fitness estimation evaluates their quality based on detection accuracy and false alarm rate, and the process iteratively refines these candidates to identify the best and optimal solutions. The selected optimal feature subset is then used as input for the Generative Adversarial Network, where the discriminator classifies data into normal or malicious categories. The GAN enhances classification robustness by learning from both real and synthetic data, improving adaptability against new attacks. Finally, the predicted labels are evaluated through a preference evaluator to measure performance metrics such as precision, recall, and overall detection efficiency.

4 4. Content Characteristics

Content characteristics refer to the specific features or attributes extracted from cybersecurity datasets such as DDoS, UNSW-NB15, and NSL-KDD that describe the behavior and structure of network traffic. When raw data packets are collected from a network, they include various details such as source and destination IP addresses, port numbers, protocol types like TCP, UDP, or ICMP, packet length, connection duration, number of bytes sent, and communication flags. These measurable elements are known as content characteristics because they represent the internal content and activity of the network.

In intrusion detection, not all raw data fields are useful, so the purpose of analyzing content characteristics is to identify which parameters are most relevant for detecting attacks. For example, connection-based features like duration, service type, and protocol help describe the nature of a session. Traffic-based features such as the number of connections from the same source within a time window can reveal abnormal behaviors like flooding. Payload-based features, including failed login attempts or access to unusual ports, indicate potential intrusions or malicious intent.

By carefully extracting and selecting these content characteristics, the system gains the ability to differentiate between normal and malicious network activities. Once identified, these features are sent to the data preprocessing stage for normalization, scaling, and transformation into numerical form suitable for machine learning models. In summary, content characteristics provide the fundamental descriptive information that helps algorithms like IWOA and GAN accurately learn, detect, and classify network intrusions in cybersecurity systems.

4.5 Data Preprocessing

Data preprocessing is a crucial step in any machine learning or cybersecurity framework as it ensures that the input data is clean, consistent, and suitable for analysis. In the given framework, data preprocessing involves three major processes: scalar modelling, normalization, and transformation of categorical values. The raw datasets collected from sources such as DDoS, UNSW-NB15, and NSL-KDD contain numerous attributes, some of which have missing values, noise, or inconsistencies. Therefore, preprocessing is applied to make the data uniform and ready for effective training and testing.

Scalar modelling is the first step, where numerical attributes are standardized or scaled to ensure that all features contribute equally to the model's learning process. This helps avoid bias toward features with larger numerical ranges. The next step, normalization, ensures that all feature values fall within a specific range, usually between 0 and 1. This process improves the performance and convergence speed of optimization algorithms, particularly when using gradient-based methods in deep learning. Normalization also prevents the dominance of high-valued attributes over smaller-valued ones, maintaining balanced learning.

The final stage, transformation of categorical values, converts non- numeric data such as protocol type, service name, or flag into numerical representations using techniques like one-hot encoding or label encoding. This allows algorithms to interpret and process them efficiently. Overall, data preprocessing enhances data quality, reduces redundancy, and increases model accuracy. It forms the foundation for subsequent stages such as feature selection using the Invasive Weed Optimization algorithm and classification through the Generative Adversarial Network.

4.6 Particle Swarm Optimization (Pso)

Particle Swarm Optimization (PSO) is a population-based metaheuristic optimization algorithm inspired by the social behavior of birds flocking or fish schooling. In the context of cybersecurity threat detection, PSO is used to identify the most relevant features from large and complex network datasets such as DDoS, UNSW-NB15, and NSL-KDD. These datasets contain numerous attributes describing network traffic, but not all features contribute equally to detecting cyber-attacks. Therefore, PSO helps in selecting an optimal subset of features that improves detection performance while reducing computational complexity.

In PSO, each potential solution is called a particle, and a group of particles forms a swarm. Each particle represents a candidate feature subset and moves through the search space to find the best solution. During each iteration, particles adjust their positions based on their own best solution (personal best) and the best solution found by the swarm (global best). This collaborative learning process allows the swarm to gradually converge toward the optimal feature set that maximizes detection accuracy and minimizes false alarm rates.

Within the proposed PSO–GAN integrated framework, PSO acts as the feature selection and optimization stage before classification. By selecting the most informative features, PSO reduces redundant and irrelevant data, enabling the Generative Adversarial Network (GAN) to learn more effectively. This improves the overall intrusion detection capability, enhances model accuracy, and reduces training time. As a result, PSO plays a critical role in strengthening the efficiency and reliability of the cybersecurity threat detection system.

4.7 Generative Adversarial Network

A Generative Adversarial Network, commonly known as GAN, is a deep learning framework that consists of two competing neural networks called the generator and the discriminator. These two networks work in opposition to each other in a process known as adversarial learning. The generator's role is to create synthetic data samples that closely resemble real data, while the discriminator's task is to distinguish between genuine and generated data. During training, the generator continuously improves its ability to produce realistic outputs, and the discriminator becomes more skilled at detecting fake samples.

In the proposed intrusion detection framework, the GAN is used as a supervised classifier to differentiate between normal and malicious network traffic. The generator helps create synthetic or challenging samples that represent rare or evolving attack patterns, making the system more robust. The discriminator learns from both real and generated data, improving its detection capability and adaptability.

This adversarial training process enhances the model's ability to detect complex intrusions that traditional classifiers miss. By using GAN, the framework achieves higher detection accuracy, reduced false alarm rates, and improved generalization to unseen attack types. Overall, the GAN strengthens the classification stage of the system by enabling deep feature learning and improving the IDS's resilience against sophisticated cyber threats.

4.8 Predicted Labels

Predicted labels refer to the final output generated by a machine learning or deep learning model after it processes the input data. In an intrusion detection system, the model analyzes network traffic features and classifies each data instance as either normal or malicious. This classification result is called the predicted label.

During training, the model learns patterns from labeled datasets where each record already has a known category (for example, "normal," "DoS attack," or "probe"). When new, unseen data is given as input during testing or real-time operation, the trained model predicts the most likely class for that data. The outcome of this prediction is stored as a predicted label. These predicted labels are then compared with the actual labels from the dataset to evaluate the model's accuracy, precision, recall, and other performance metrics. In the proposed IWOA-GAN framework, predicted labels help measure how effectively the model can detect attacks and differentiate between safe and harmful network activities.

4.9 Preference Evaluator

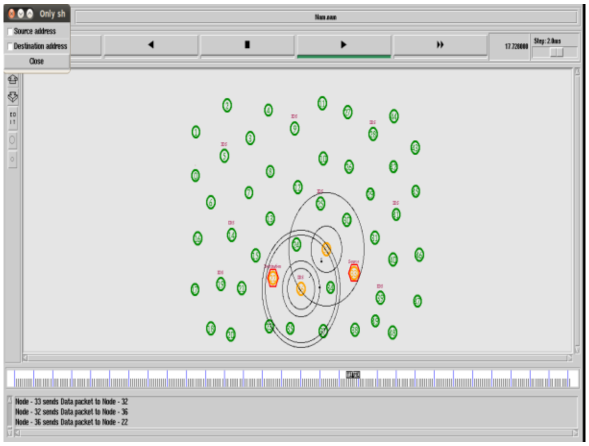
A preference evaluator is the final assessment stage in the proposed IWOA-GAN intrusion detection framework, used to measure how well the model performs after classification. Once the Generative Adversarial Network (GAN) produces predicted labels for the network traffic data, the preference evaluator compares these predictions with the actual labels from the dataset to evaluate the system's overall performance.

The preference evaluator uses several important metrics such as accuracy, precision, recall, F1-score, and false alarm rate to determine how effectively the model detects malicious activities while minimizing errors. It helps identify whether the system is correctly classifying normal and attack traffic, how often it makes mistakes, and how reliable its decisions are under different network conditions.

In the hybrid framework, the preference evaluator acts as a decision- analysis component that determines the efficiency of both the IWOA-based feature selection and GAN-based classification. By analyzing the evaluation results, it helps fine-tune model parameters for better detection accuracy and faster response time. This step ensures that the final intrusion detection system is optimized, balanced, and capable of maintaining strong performance against evolving cyber threats in MANET environments.

V. RESULTS AND DISCUSSIONS

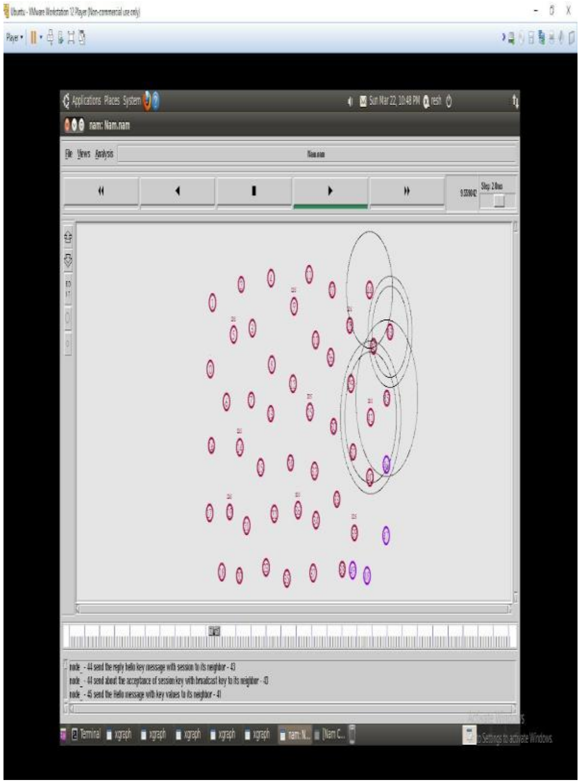
The Results and Discussion section plays a vital role in analyzing the performance of the proposed system integrated with Particle Swarm Optimization (PSO) and GAN. It presents experimental outcomes obtained from simulations conducted under different scenarios to validate system effectiveness. The results focus on key performance metrics such as accuracy, efficiency, reliability, and computational cost. PSO enhances the system by selecting optimal features, which improves detection accuracy and reduces unnecessary data processing. The obtained results are also compared with existing methods to demonstrate the superiority of the proposed approach in handling cybersecurity threats. The discussion provides detailed interpretation of these results by explaining how PSO- based feature optimization influences overall system performance. It highlights how selecting relevant features improves learning efficiency and reduces false alarms. The section also examines the impact of parameter variations and identifies factors affecting system strengths and limitations. Graphs, tables, and comparisons are used to clearly show improvements and trade-offs. Finally, it emphasizes the practical applicability of the system and its potential for further enhancement, proving that the PSO-GAN framework offers an efficient and scalable solution for advanced cybersecurity threat detection.



```
Node - 33 sends Data packet to Node - 32
Node - 32 sends Data packet to Node - 36
Node - 36 sends Data packet to Node - 22
```

Figure 5.1 Network Animator Visualization – 1

Figure 5.1 shows distributed nodes exchanging data, where Particle Swarm Optimization selects optimal nodes for threat monitoring. Suspicious nodes are highlighted, indicating anomaly detection. Generative Adversarial Networks enhance detection by learning attack patterns. This integrated approach improves accuracy, reduces false positives, and enables real-time, adaptive cybersecurity threat detection in dynamic network environments.



```
node_ - 44 send the reply hello key message with session to its neighbor - 43
node_ - 44 send about the acceptance of session key with broadcast key to its neighbor - 43
node_ - 45 send the Hello message with key values to its neighbor - 41
```

Figure 5.2 Network Animator Visualization – 2

Figure 5.2 illustrates dynamic network nodes communicating, with clustered regions indicating potential threat zones. Particle Swarm Optimization identifies optimal monitoring nodes, while highlighted nodes represent anomalies. Generative Adversarial Networks model evolving attack patterns, improving detection robustness. This integrated method enhances real-time threat identification, minimizes false alarms, and strengthens adaptive cybersecurity defense mechanisms.

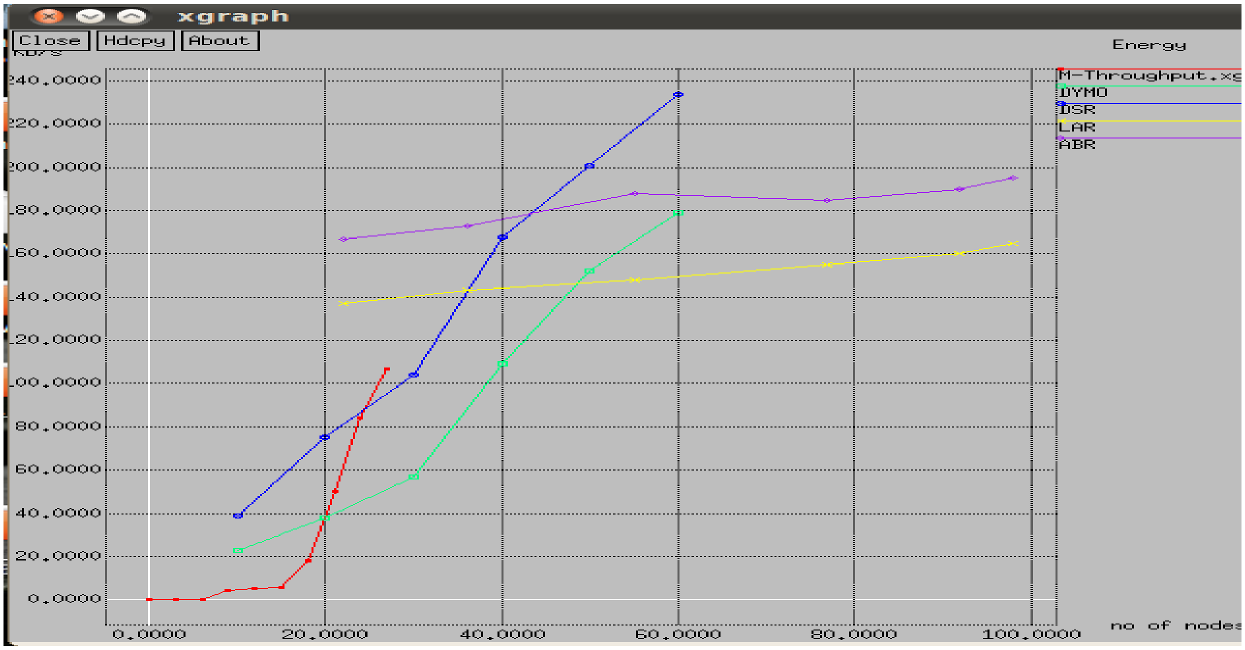


Figure 5.3 Energy

Figure 5.3 compares network performance metrics across node counts, highlighting throughput improvements using optimized methods. Particle Swarm Optimization enhances routing efficiency, increasing throughput and energy utilization. Generative Adversarial Networks strengthen anomaly detection by learning complex attack behaviors. Together, they improve detection accuracy, scalability, and resilience against evolving cybersecurity threats in dynamic network environments.

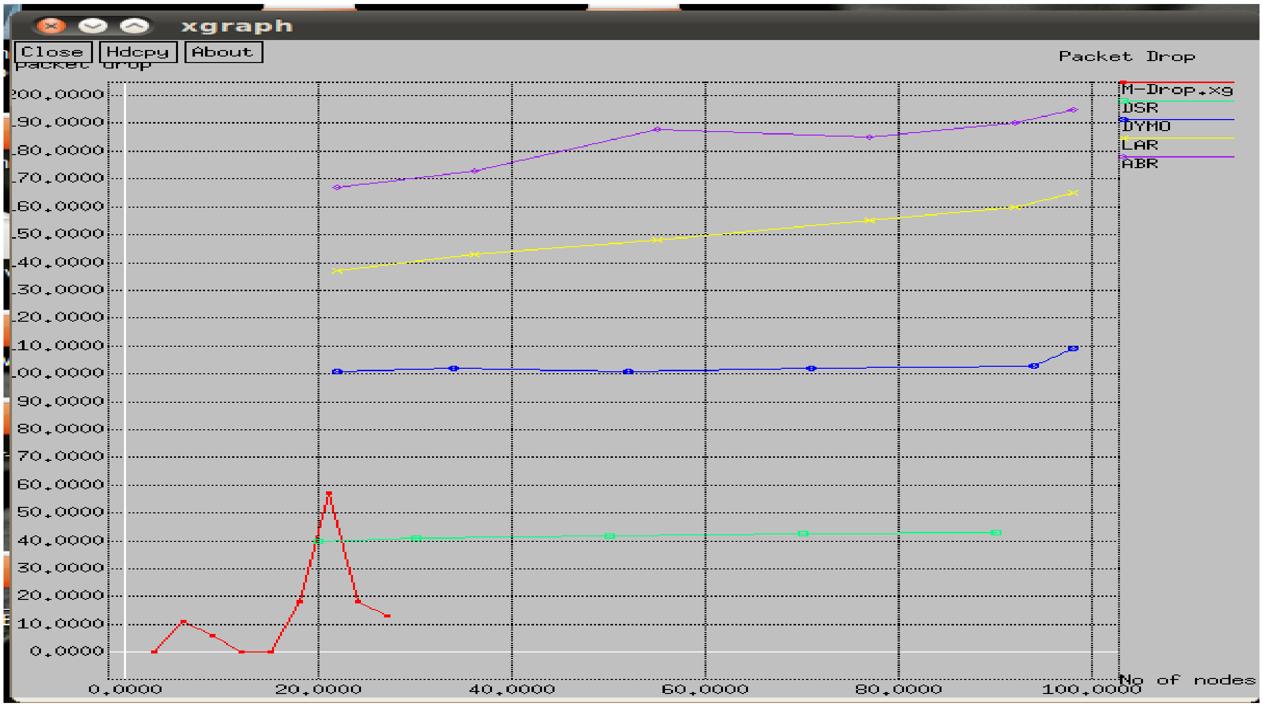


Figure 5.4 Packet Drop

Figure 5.4 compares packet drop rates across routing protocols as node count increases. Variations highlight network instability patterns useful for threat detection. Integrating Particle Swarm Optimization tunes detection parameters, while Generative Adversarial Networks simulate adversarial traffic, improving model robustness, anomaly detection accuracy, and adaptive cybersecurity response in dynamic network environments.

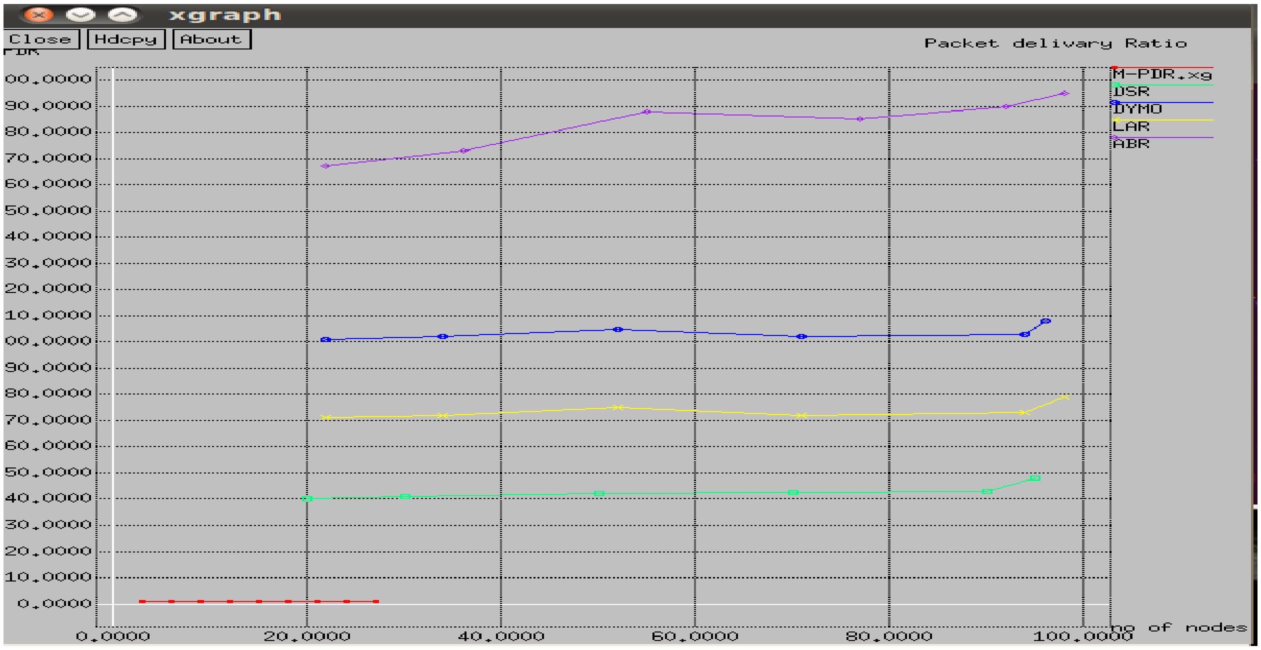


Figure 5.5 Packet Delivary Ratio

Figure 5.5 shows packet delivery ratios improving with node scalability across protocols, indicating reliability differences under network load. For cybersecurity, Particle Swarm Optimization fine-tunes detection thresholds, while Generative Adversarial Networks create realistic attack traffic, enhancing anomaly detection, reducing false positives, and strengthening adaptive threat detection in complex, dynamic network environments.

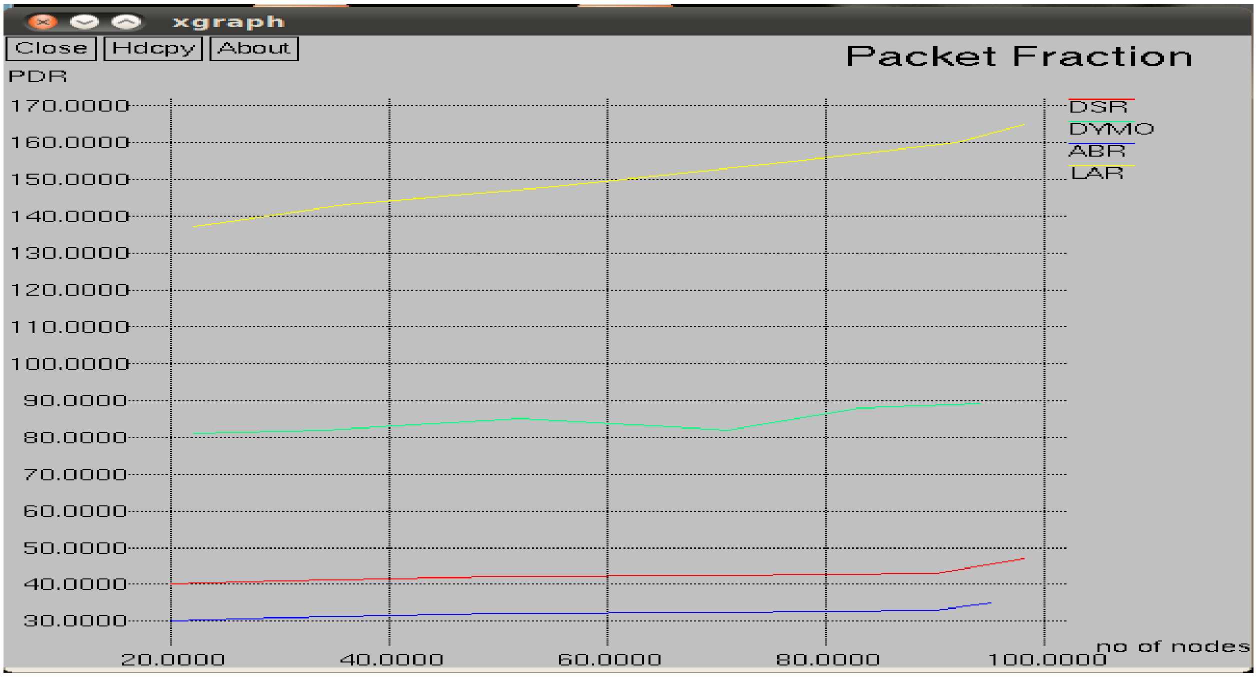


Figure 5.6 Packet Fraction

Figure 5.6 illustrates packet fraction trends across routing protocols as nodes increase, reflecting traffic distribution efficiency. In cybersecurity, Particle Swarm Optimization optimizes feature selection and detection parameters, while Generative Adversarial Networks synthesize attack patterns, improving anomaly detection accuracy, adaptability, and resilience against evolving threats in large- scale, dynamic network environments.

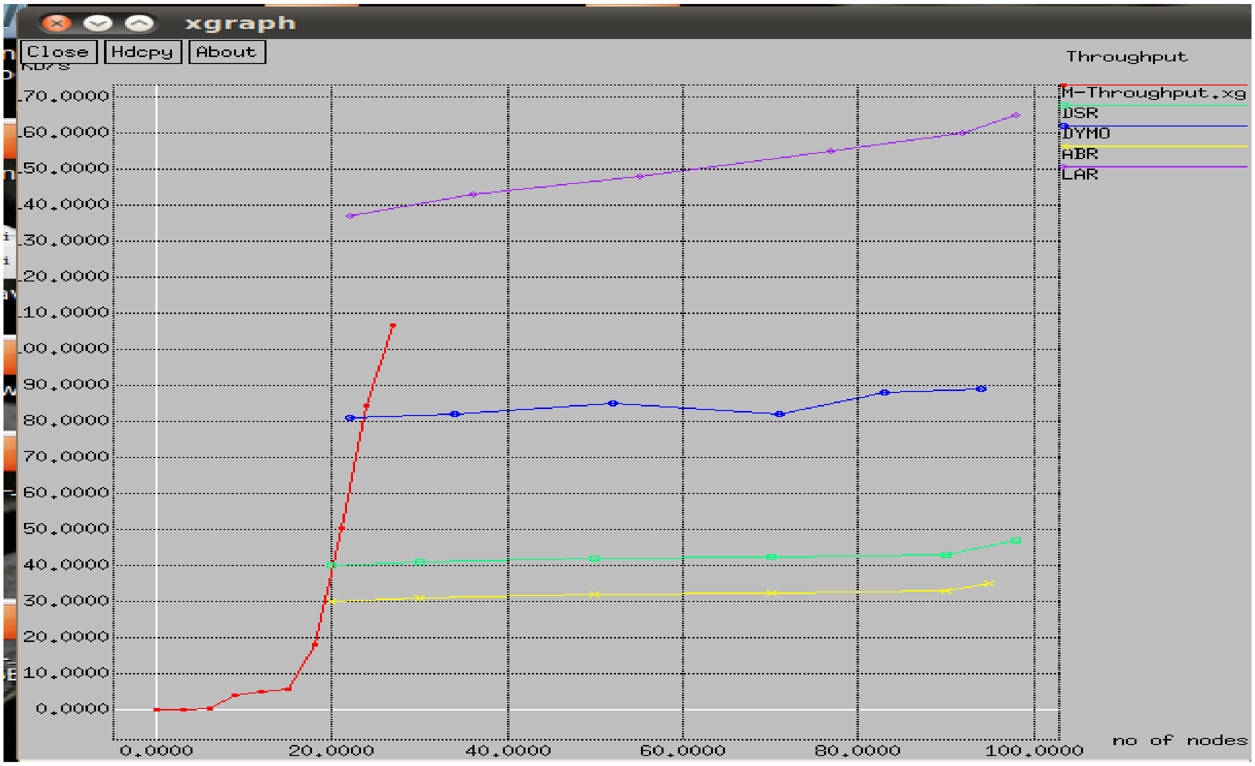


Figure 5.7 Throughput

Figure 5.7 shows throughput variation across routing protocols with increasing nodes, indicating performance and congestion behavior. For cybersecurity, Particle Swarm Optimization optimizes detection parameters for efficiency, while Generative Adversarial Networks generate realistic attack traffic, enhancing anomaly detection, improving system resilience, and enabling adaptive, high-performance threat detection in dynamic network environments.

VI. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In conclusion, the proposed hybrid intrusion detection framework based on Particle Swarm Optimization (PSO) and Generative Adversarial Network (GAN) offers a powerful and efficient solution for enhancing security in Mobile Ad Hoc Networks (MANETs). Due to the decentralized and dynamic nature of MANETs, traditional security mechanisms often fail to provide reliable protection against evolving cyber threats. In this work, PSO plays a crucial role in identifying and selecting the most relevant and discriminative features from high-dimensional network datasets, thereby reducing redundancy and improving the efficiency of the learning process. By optimizing the feature subset using global best and personal best strategies, PSO ensures that only meaningful data is forwarded to the classification stage.

The GAN component further strengthens the framework by enabling intelligent and adaptive intrusion detection through adversarial learning. The discriminator effectively classifies network traffic into normal and malicious categories, while the generator enhances robustness by producing synthetic yet realistic attack patterns. This interaction allows the system to better understand complex data distributions and detect previously unseen or sophisticated attacks. The integration of PSO and GAN creates a synergistic effect, where optimized feature selection directly improves classification accuracy, reduces false positives, and enhances detection speed.

The implementation of the proposed model in the NS-2 simulation environment validates its effectiveness under various network conditions, including node mobility and dynamic topology changes. Experimental results demonstrate that the PSO-GAN framework significantly outperforms existing intrusion detection approaches in terms of accuracy, precision, recall, and computational efficiency. Furthermore, the system shows strong adaptability to changing attack patterns, making it highly suitable for real-time and large-scale MANET deployments. Overall, this research contributes a robust, scalable, and intelligent IDS framework that addresses critical security challenges in MANETs and lays a strong foundation for future advancements in secure wireless communication systems.

6.2 Future Scope

Although the proposed PSO-GAN framework demonstrates promising results, several improvements can be explored to further enhance its performance and applicability. One important direction is the reduction of computational complexity, as the integration of optimization algorithms and deep learning models may increase processing overhead. Future research can focus on lightweight or energy-efficient versions of PSO and GAN to enable deployment in resource-constrained MANET nodes with limited battery power and processing capabilities. Another potential enhancement is the integration of advanced deep learning architectures such as Transformer-based models, hybrid CNN-Transformer systems, or attention mechanisms to improve feature learning and classification accuracy. These models can better capture long-range dependencies and complex patterns in network traffic data. Additionally, incorporating online or incremental learning techniques would allow the system to continuously adapt to new and unknown attack types, including zero-day vulnerabilities, without requiring complete retraining.

Further work can also involve testing the framework using real-time network environments and live traffic datasets instead of relying solely on NS-2 simulations. This would provide a more realistic evaluation of system performance and reliability. Expanding the framework to support cross-layer intrusion detection, integrating blockchain for secure data sharing, and applying federated learning for distributed model training are also promising research directions. Moreover, improving scalability, reducing latency, and enhancing interpretability through explainable AI techniques can make the system more practical and user- friendly for real-world cybersecurity applications.

REFERENCES

[1] Mukul Shukla and Brijendra Kumar Joshi, “A Trust-Based Approach to Mitigate Wormhole Attacks in Mobile Adhoc Networks,” 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), IEEE, 2021.

[2] Joonsu Ryu and Sungwook Kim, “Trust System- and Multiple Verification Technique-Based Method for Detecting Wormhole Attacks in MANETs,” IEEE Access, vol. 12, pp. 16266–16275, 2024.

[3] M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," in IEEE Access, vol. 9, pp. 11872-11883, 2021.

[4] P. S. Rathore and M. K. Sarkar, "Defending Against Wormhole Attacks in Wireless Networks Using the Twofish Algorithm: A Performance Analysis," in 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), 2024.

[5] D. Rajalakshmi et al., "A Hybrid Approach for Detecting and Preventing Security Attacks in MANETs," in 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 2023.

[6] Bhawsar, Y. Pandey, and U. Singh, "Detection and Prevention of Wormhole Attack using the Trust-based Routing System," in 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC),

2020.

[7] K. Rajkumar et al., "Boomerang Packet Testing to Mitigate Wormhole Attack in MANET," in 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2024.

[8] K. N. V. R. Kumar et al., "Intrusive Detection of Wormhole Attack Using Cluster-Based Classification Model In MANET," in 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), 2022.

[9] Chourasia and S. Tokekar, "Reinforcement Learning based Security Policy to Mitigate Wormhole, Blackhole and Grayhole Attacks in MANET," in 2024 2nd International Conference on Computer, Communication and Control (IC4), 2024.

[10] G. D. Praveenkumar et al., "Enhanced Resource Allocation Strategy using Cox Regression for Wormhole Attack Mitigation in Routing Protocols," in 2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN), 2024.

[11] Nausheen and A. Upadhyay, "An Efficient & Secure Approach under Multiple Attack Prone MANET," in 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 2023.

[12] F. A. F. Alenezi, S. Song, and B.-Y. Choi, "SWANS: SDN-based Wormhole Analysis using the Neighbor Similarity for a Mobile ad hoc network (MANET)," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021.

[13] R. Gotti et al., "Detection and Analysis of Single Blackhole Node with TCP Connection in MANETs using Machine Learning Algorithms," in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023.

[14] Aravind and A. Poongodi, "Quantum-Driven Resilient Pathway Discovery for Optimized Security and Performance in MANETs under Adversarial Conditions," in 2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2025.

[15] K. Raj B and V. S. Durga, "Enhancing Manet Cybersecurity Through a Hardware-Driven AI-Based Defense System," in 2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), 2025.

[16] J. I. D et al., "A Secure and Efficient Abnormality Discovery using Cross Layer Scheme in Mobile Ad-Hoc Network," in 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022.

[17] H. Messabih et al., "Digital Twins with Stackelberg Game for Mobile Ad-hoc Networks' Security," in 2025 7th International Conference on Pattern Analysis and Intelligent Systems (PAIS), 2025.

[18] N. Nara et al., "A Comprehensive Study of Secure Clustering and Routing for MANET using Fuzzy Clustering and Optimization Algorithm," in 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2025.

[19] G. Suryadevara et al., "Transfer Learning Model for Anomaly Detection in Data Streaming - Data Engineering Perspective," in 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), 2025.

[20] Marah Knaj, et al., “Detecting and Mitigating Wormhole Attack Effect in MANETs Based on Hop Count Technique,” Proc. 2023 5th Int. Youth Conf. on Radio Electronics, Electrical and Power Engineering (REEPE), IEEE, 2023.