ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

A Comprehensive Review of Intrusion Detection Systems for Routing Attacks in Mobile Ad Hoc Networks

Kaushik Kumar[1], Kumar Amrendra[2]

[1]Research Scholar, Faculty of CSE & IT, Jharkhand Rai University, Ranchi

[2]Assistant Professor, Faculty of CSE & IT, Jharkhand Rai University, Ranchi

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150600010

Received: 10 June 2026; Accepted: 15 June 2026; Published: 02 July 2026

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are wireless networks that do not require any fixed infrastructure or central administration. The high vulnerability of MANETs to routing based security attack is mainly due to their dynamic topology, limited bandwidth, and distributed architecture, including black hole, wormhole, gray hole, rushing, and Sybil attacks. IDS (Intrusion Detection Systems) are crucial in detecting attacks and securing communications in MANETs. Machine Learning (ML) and Deep Learning (DL) methods have greatly enhanced the intrusion detection capability in recent years by allowing intelligent attack classification and anomaly detection. This review paper summarizes the existing IDS techniques for MANETs routing attack detection system. It presents the traditional IDS techniques, machine learning enabled IDS, and deep learning intrusion detection framework techniques. Existing research contributions are also tabulated and presented in a detailed comparative analysis based on the techniques used, attacks detected, datasets used, performance measures used, advantages and limitations. Moreover, the study identifies the significant research challenges and future directions for developing efficient, lightweight and intelligent IDS design for MANET security.

Keywords: MANET, Intrusion Detection System, Routing Attacks, Machine Learning, Deep Learning, Network Security, Black Hole Attack, Wormhole Attack, IDS.

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are wireless communication networks that are dynamically formed without relying on fixed infrastructures, and involve the nodes communicating via multi-hop routing. MANETs offer flexibility, quick deployment, self-configuration, and adaptability in dynamic environments, as they lack centralized administration and fixed infrastructure. The properties of MANETs are excellent for various applications, including military operation, disaster recovery system, healthcare monitoring, emergency rescue, vehicular communication system, and remote sensing system (Perkins, 2001; Conti & Giordano, 2014).

The open wireless medium, dynamic topology, limited bandwidth, energy constraints and distributed nature of MANETs make them susceptible to many security vulnerabilities and routing-based attacks. The routing protocol can be used by malicious nodes to interfere with routing, change routing data, drop packets or create rogue access points in the network. Main routing attacks in MANETs comprise of black hole attack, gray hole attack, wormhole attack, rushing attack, Sybil attack, and denial of service (DoS) attack. Such attacks cause degradation in network performance in terms of reduced throughput, increased packet loss and reduced packet delivery ratio (Murthy & Manoj, 2004).

The traditional security techniques of cryptography, authentication and access control are not enough to provide full protection in MANET against sophisticated attacks like insider and routing attacks. So, Intrusion Detection Systems (IDS) have become an indispensable security measure in MANET. IDS constantly observes the activities and behaviors of nodes and network traffic to detect malicious activities and abnormal communication patterns. IDS may be divided into signature-based IDS, anomaly-based IDS, specification-based IDS and hybrid systems (Zhou & Haas, 1999).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Relying on the ability of these techniques to detect attacks accurately and adaptively, researchers have been working to incorporate Machine Learning (ML) and Deep Learning (DL) into the frameworks of IDS in recent years. Several machine learning techniques like Support Vector Machines (SVM), Decision Trees, Random Forest and Naïve Bayes have been shown to be effective in detecting routing attacks in MANETs. Moreover, deep learning approaches such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Deep Belief Networks (DBN) have improved intrusion detection by automatically learning and extracting features of complex traffic patterns, and discovering high precision attack patterns that were not previously known (Kimanzi et al., 2024).

This review paper summarizes and analyzes the different IDS approaches proposed for detection of routing attacks in MANETs. The paper discusses the traditional IDS mechanism, machine learning based IDS and deep learning based IDS models. Moreover, for the last studies a comparative review is provided on the following parameters: detection techniques, datasets, attack coverage, performance measures, advantages, and limitations. The study also addresses some of the current research challenges and points out future research directions for designing intelligent and lightweight IDS framework for secure MANET communication.

Overview of MANET

A Mobile Ad Hoc Network (MANET) is a self-configuring network composed of mobile wireless nodes communicating without any centralized infrastructure. Each node functions both as a host and a router. Communication occurs through multi-hop transmission where intermediate nodes forward packets toward the destination.

Characteristics of MANET

- **Infrastructure-less Architecture-** MANETs are those that do not have any infrastructure like routers, switches, access points etc. All nodes communicate with each other and every node is a host and a router. This makes it easy to deploy in locations where standard networks do not exist.
- **Dynamic Topology-** Due to the mobility of nodes and frequent changes in their location, the topology of MANET changes often. This puts routing and network management under more strain, as communication links are dynamically established and broken.
- **Distributed Operation-** MANET is a distributed network model, in this model all the nodes share responsibility for routing, packet forwarding and network management. There are no central monitoring and management of network operations.
- **Multi-hop Routing-** In MANETs data packets are sent by the intermediate nodes before reaching the destination. Multi-hop routing extends the communication range and allows nodes out of direct communication range to communicate.
- **Limited Resources-** Nodes of MANET have limited bandwidth, memory, processing capability and battery power. These resource limits impact network performance and can also hinder the implementation of complicated security methods.

Scalability Issues

Performance decreases as network size increases.

These characteristics make MANETs highly flexible but simultaneously vulnerable to routing attacks and malicious intrusions.

Routing Attacks in MANET

Routing attacks are one of the significant threats to Mobile Ad Hoc Networks (MANETs). The main targets of these attacks are the routing protocols, and the main goal is to interfere with the normal forwarding of packets in the network. As MANETs are decentralized and rely on nodes working together, malicious nodes can easily join the communication routing process and potentially disrupt the operation of the network. Routing attacks can result in packet loss, routing failures, network congestion, communication delays, and decreased network

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

performance. There are attacks that intentionally drop packets and there are attacks that alter the routing information, leading to the formation of false routes or to the waste of network resources.

Black Hole Attack

A Black Hole Attack occurs when a malicious node falsely advertises itself as having the shortest and freshest route to the destination node. During the route discovery process, the attacker immediately responds to the Route Request (RREQ) message with a fake Route Reply (RREP) message. Since the malicious node claims to provide the best path, the source node forwards data packets through it. However, instead of forwarding the packets to the destination, the malicious node drops all packets intentionally.

This attack severely affects the communication reliability and overall network performance. Black hole attacks are difficult to identify because the malicious node behaves like a legitimate routing node during route establishment.

Effects

- High packet loss
- Communication disruption
- Reduced packet delivery ratio
- Decreased network throughput
- Increased routing overhead

Gray Hole Attack

Gray Hole Attack is an advanced type of Blackhole attack where the malicious node selectively drops packets rather than dropping all the packets continuously. The attacker can pass some of the packets normally while dropping under certain conditions. For instance, the attacker could attack packets coming from specific nodes or could drop packets just for specific time periods.

Gray hole attacks are harder to identify than black hole attacks since the malicious node acts as a normal node in some instances. This selective behaviour leads to confusion in determining what is malicious and what is not in the network.

Effects

- Difficult attack detection
- Reduced network reliability
- Intermittent packet loss
- Unstable communication
- Increased false detection rate

Wormhole Attack

In a Wormhole Attack, two or more malicious nodes establish a private communication tunnel between them known as a wormhole link. One attacker captures packets from one location in the network and transfers them through the tunnel to another malicious node located far away. The second attacker then retransmits those packets into the network.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

This creates the false impression that the malicious nodes provide the shortest route between source and destination nodes. As a result, many nodes begin routing their packets through the wormhole path. Attackers can then analyze, modify, or drop packets passing through the tunnel.

Wormhole attacks are highly dangerous because they can be launched without compromising cryptographic mechanisms.

Effects

- False route creation
- Routing manipulation
- Packet interception
- Increased communication delay
- Network topology distortion

Sybil Attack

Sybil Attack is a type of attack that is carried out by a malicious node creating multiple fake identities or fake nodes in the network. The attacker will not be a single node, but will pretend to be many different nodes at once. These fake identities are involved in routing and communication tasks and lead other nodes in the network in the wrong direction.

The Sybil attack may be able to affect routing algorithms, voting systems and resource allocation systems. The use of fake identities can have a considerable impact on the stability and security of MANETs, as they depend heavily on the trust and cooperation of the nodes.

Effects

- Resource misuse
- Network instability
- False routing information
- Reduced trust among nodes
- Increased vulnerability to further attacks

Rushing Attack

A Rushing Attack targets the route discovery process in on-demand routing protocols such as AODV and DSR. In this attack, the malicious node quickly forwards Route Request (RREQ) packets before legitimate nodes can process and forward them. Due to the duplicate suppression mechanism used in routing protocols, the route requests received later through legitimate paths are discarded.

As a result, routes containing the malicious node are established more frequently, allowing attackers to manipulate communication or launch additional attacks such as packet dropping or traffic analysis.

Effects

- Malicious route establishment

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

- Routing disruption
- Increased packet loss
- Reduced route diversity
- Higher network vulnerability

Denial of Service (DoS) Attack

A Denial of Service (DoS) Attack aims to make network services unavailable to legitimate users by overwhelming the network with excessive traffic, fake requests, or unnecessary routing packets. The attacker continuously consumes network bandwidth, processing power, and battery resources, causing congestion and degrading network performance.

DoS attacks can target individual nodes or the entire network infrastructure. In MANETs, resource-constrained nodes are especially vulnerable to such attacks because excessive communication rapidly exhausts battery power and reduces network lifetime.

Effects

- Network congestion
- Energy exhaustion
- Increased communication delay
- Reduced throughput
- Service unavailability

Intrusion Detection Systems in MANET

An Intrusion Detection System (IDS) is a security mechanism used to monitor network activities and detect malicious behavior or unauthorized access within a network. In Mobile Ad Hoc Networks (MANETs), IDS plays a crucial role because traditional security mechanisms alone are not sufficient to protect the network from internal and external attacks. Due to the decentralized and dynamic nature of MANETs, nodes are highly vulnerable to routing attacks, packet dropping, and malicious communication activities. IDS continuously analyzes network traffic, routing behavior, and node activities to identify suspicious patterns and generate alerts whenever an intrusion is detected.

The main objective of IDS in MANETs is to maintain network confidentiality, integrity, and availability by detecting and preventing attacks before they significantly affect network performance.

Types of IDS

Intrusion Detection Systems in MANETs are generally classified into different categories based on their detection techniques and operational behavior.

Signature-Based IDS

Signature-Based IDS detects attacks by comparing network activities with previously stored attack signatures or known malicious patterns. The IDS maintains a database of attack signatures and continuously monitors traffic to identify matching patterns. When a match is found, the system generates an intrusion alert.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

This approach is highly effective for detecting previously known attacks and is widely used because of its accuracy and low false alarm rate. However, it cannot identify new or unknown attacks that do not exist in the signature database.

Advantages

- Accurate detection of known attacks
- Low false positive rate
- Fast attack identification
- Easy implementation

Limitations

- Cannot detect unknown or zero-day attacks
- Requires continuous signature updates
- Ineffective against modified attack patterns

Anomaly-Based IDS

Anomaly-Based IDS detects intrusions by identifying deviations from normal network behavior. The system first learns the normal behavior of the network and then compares current activities against the established profile. Any abnormal behavior exceeding predefined thresholds is considered suspicious.

This technique is capable of detecting unknown attacks and new intrusion patterns that are not present in signature databases. Due to its adaptive learning capability, anomaly-based IDS is widely used in intelligent intrusion detection frameworks.

However, because normal network behavior in MANETs changes frequently, anomaly-based systems often generate high false positive rates.

Advantages

- Detects unknown and zero-day attacks
- Adaptive and intelligent learning capability
- Effective in dynamic environments
- Suitable for evolving attack patterns

Limitations

- High false positive rate
- Complex training process
- Increased computational overhead
- Requires proper threshold selection

Specification-Based IDS

Specification-Based IDS detects attacks by monitoring whether network activities follow predefined protocol rules and specifications. In this method, acceptable behavior patterns are manually defined according to routing protocol standards. Any violation of these specifications is treated as suspicious behavior.

Specification-based IDS combines the advantages of signature and anomaly detection approaches by reducing false positives while still detecting certain unknown attacks.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Advantages

- Reduced false alarm rate
- Detects protocol violations effectively
- Better accuracy compared to anomaly-based IDS

Limitations

- Difficult rule specification process
- Time-consuming implementation
- Limited adaptability to new attacks

Hybrid IDS

Hybrid IDS combines two or more intrusion detection techniques such as signature-based and anomaly-based methods to improve detection accuracy and overall system performance. Hybrid systems attempt to overcome the limitations of individual IDS approaches by integrating their strengths.

For example, signature-based detection can identify known attacks quickly, while anomaly-based detection can detect new or unknown attacks. As a result, hybrid IDS provides better security coverage and improved attack detection efficiency.

Advantages

- Improved detection accuracy
- Detects both known and unknown attacks
- Reduced false positives
- Enhanced network security

Limitations

- Increased computational complexity
- Higher resource consumption
- Complex system design

Machine Learning and Deep Learning in IDS

Machine Learning (ML) and Deep Learning (DL) techniques have significantly improved the performance of Intrusion Detection Systems in MANETs. Traditional IDS approaches often struggle to identify sophisticated and evolving attacks. ML and DL techniques enable IDS models to learn network behavior automatically, classify attack patterns intelligently, and improve detection accuracy.

These intelligent approaches are capable of processing large volumes of network traffic data and identifying complex attack patterns with minimal human intervention. Machine learning models mainly rely on feature extraction and classification algorithms, whereas deep learning models automatically learn hierarchical representations of network traffic.

Machine Learning Techniques

Machine Learning algorithms are widely used in IDS for classification, prediction, and anomaly detection.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Support Vector Machine (SVM)

Support Vector Machine is a supervised learning algorithm used mainly for binary classification problems. SVM identifies the optimal hyperplane that separates normal and malicious traffic data. It is highly effective in detecting routing attacks with high accuracy and low error rates.

Features

- Effective for binary classification
- High classification accuracy
- Works well with small datasets

Limitations

- High training complexity
- Performance decreases with large datasets

Decision Tree

Decision Tree is a classification algorithm that represents decisions using a tree-like structure. Each internal node represents a condition, while leaf nodes represent classification outcomes. Decision Trees are simple, easy to interpret, and widely used for intrusion detection.

Features

- Easy implementation
- Fast decision-making
- Interpretable model structure

Limitations

- Overfitting problem
- Lower accuracy for complex datasets

Random Forest

Random Forest is an ensemble learning technique that combines multiple decision trees to improve classification accuracy. It reduces overfitting and provides better intrusion detection performance compared to single decision tree models.

Features

- Improved detection accuracy
- Robust against overfitting
- Handles large datasets efficiently

Limitations

- Increased computational complexity
- Requires more memory

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Naïve Bayes

Naïve Bayes is a probabilistic classification algorithm based on Bayes' theorem. It assumes independence among features and predicts the probability of a packet belonging to a normal or malicious category.

Features

- Fast processing speed
- Simple implementation
- Suitable for real-time IDS

Limitations

- Assumes feature independence
- Lower performance for correlated data

K-Nearest Neighbor (KNN)

K-Nearest Neighbor is a distance-based classification algorithm that classifies data points based on the nearest neighboring samples. It is commonly used for anomaly detection in IDS.

Features

- Simple classification technique
- Effective for pattern recognition
- No training phase required

Limitations

- High memory usage
- Slow performance for large datasets

Deep Learning Techniques

Deep Learning techniques are advanced machine learning approaches capable of automatically extracting features and learning complex network traffic patterns. These techniques provide high detection accuracy and better performance for large-scale intrusion detection systems.

Convolutional Neural Network (CNN)

CNN is a deep learning architecture mainly used for feature extraction and pattern recognition. In IDS, CNN automatically extracts spatial traffic features and identifies attack patterns effectively.

Features

- Automatic feature extraction
- High detection accuracy
- Efficient pattern recognition

Limitations

- High computational requirements
- Requires large training datasets

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Recurrent Neural Network (RNN)

RNN is designed for processing sequential data and time-series information. It is highly useful in IDS for analyzing network traffic sequences and routing behavior over time.

Features

- Suitable for sequential data analysis
- Effective for traffic pattern learning
- Captures temporal dependencies

Limitations

- Vanishing gradient problem
- Slow training process

Long Short-Term Memory (LSTM)

LSTM is an advanced form of RNN capable of handling long-term dependencies in sequential traffic data. It effectively remembers past information and improves attack detection performance in dynamic MANET environments.

Features

- Handles long-term traffic dependencies
- Improved sequential learning
- Better anomaly detection capability

Limitations

- Computationally expensive
- Complex architecture

Deep Belief Network (DBN)

DBN is a deep learning model composed of multiple hidden layers that perform hierarchical feature extraction. It improves intrusion detection accuracy by learning complex network patterns.

Features

- Hierarchical feature learning
- High classification accuracy
- Effective for complex datasets

Limitations

- Long training time
- Requires high computational power

Autoencoders

Autoencoders are neural network models mainly used for anomaly detection and dimensionality reduction. They learn compressed representations of normal network behavior and identify deviations as anomalies.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Features

- Effective anomaly detection
- Reduces feature dimensionality
- Learns hidden traffic patterns

Limitations

- Training complexity
- Sensitive to parameter tuning

Deep Learning-based IDS models provide higher detection accuracy, automatic feature extraction, adaptive learning capability, and improved performance against unknown attacks. These intelligent models are increasingly being adopted for securing MANET environments against sophisticated routing attacks and evolving cyber threats.

Comparative Review of Existing IDS Approaches

Authors	Year	Technique Used	Attacks Detected	Dataset Used	Accuracy	Advantages	Limitations
Mitrokotsa et al.	2014	Anomaly-Based IDS	Black Hole, DoS	Simulation Data	88%	Detects unknown attacks	High false positives
Safaa Laqtib et al.	2020	CNN, BLSTM, DBN	Multiple Intrusions	NSL-KDD	97%	High accuracy	Computational complexity
Mohammed Kamal et al.	2021	Deep Learning IDS	Routing attacks	KDDCup99	96%	Automatic feature extraction	Requires large dataset
Yogendra Kumar et al.	2023	Hybrid IDS	Multiple attacks	NSL-KDD	95%	Better classification	Complex implementation
Sultan et al.	2023	ANN-Based IDS	DoS attacks	MANET Simulation	93%	Intelligent learning	Limited attack coverage
Kimanzi et al.	2024	Deep Learning Review	Various attacks	Literature Review	—	Comprehensive analysis	No implementation
Chaudhary et al.	2024	Comparative IDS Review	Routing attacks	Various datasets	—	Broad comparison	Limited experiments
Ravi Verma et al.	2022	Routing Attack Detection	Black Hole, Wormhole	Simulation Data	91%	Improved routing security	Increased overhead

Performance Metrics for IDS Evaluation

The efficiency of IDS models is measured using various performance parameters.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Detection Accuracy

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Precision

$$\text{Precision} = \frac{TP}{TP+FP}$$

Recall

$$\text{Recall} = \frac{TP}{TP+FN}$$

F1-Score

$$\text{F1-Score} = 2 * \frac{Precision * Recall}{Precision + Recall}$$

Where:

- TP = True Positive
- TN = True Negative
- FP = False Positive
- FN = False Negative

Challenges in IDS for MANET

As the network is dynamic and decentralized, designing an efficient Intrusion Detection System (IDS) for Mobile Ad Hoc Networks (MANETs) is a difficult job. There are a number of technical and security issues which have significant impact on the effectiveness and reliability of IDS mechanisms in MANET environments. These threats make the detection process more inaccurate, consume more resources and make real-time intrusion detection harder.

Dynamic Topology

MANET nodes are mobile and often their locations vary from node to node in the network. The network topology is constantly changing, as nodes move around, and communication links are regularly formed and torn down. These rapid topology changes impact on routing stability and make IDS difficult to keep monitoring of node behavior and routing paths accurate.

It can also cause confusion in case of normal routing failures and malicious activities, and lead to the inefficiency of the intrusion detection mechanisms, if there are frequent changes in the routes.

Challenges

- Frequent route breakage
- Difficult monitoring of node behavior
- Increased routing complexity
- Reduced IDS stability

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Limited Resources

The nodes in MANETs have limited battery capacity, processing capability, memory and bandwidth. IDS mechanisms generally need to be constantly monitored, analyzed in the packets that pass by and need computational processing, and thus require a lot of network resources.

The energy consumption of all nodes can be quickly depleted by complex IDS algorithms, leading to a shorter network lifetime. Hence, it is a great challenge to design lightweight and energy efficient IDS architectures in MANET environment.

Challenges

- Battery power limitations
- Restricted processing capability
- Limited storage capacity
- Bandwidth constraints

High False Alarm Rate

Anomaly-based IDS techniques use to detect attack, by examining the deviations from normal network behavior. But in MANETs the normal communication patterns can change regularly, because of the constantly changing environment.

This will cause IDS to falsely identify the normal activity as an unwanted attack, resulting in false-positive or false-alarm responses. The false alarms lower the reliability of the system and add unnecessary processing overhead.

Challenges

- Incorrect attack detection
- Reduced detection reliability
- Increased computational overhead
- Difficulty distinguishing normal and abnormal behavior

Dataset Scarcity

IDS models based on Machine Learning and Deep Learning depend on huge and realistic datasets to train and assess the models properly. Unfortunately, there are very few MANET specific datasets available in the public domain.

Many of the current IDS models are based on typical network datasets like KDD Cup 99 or NSL-KDD which might not reflect the actual situations of MANETs and routing attacks. Performance and generalization of IDS are adversely impacted by the absence of realistic datasets.

Challenges

- Limited real-world MANET datasets
- Inadequate attack representation

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

- Reduced model training efficiency
- Difficulty in performance evaluation

Scalability Issues

As the size of MANET increases, the number of nodes, communication links, and routing activities also increase significantly. IDS mechanisms must monitor large amounts of network traffic and node behavior in real time.

In large-scale MANETs, IDS performance may degrade due to increased computational complexity, communication overhead, and resource consumption. Ensuring efficient intrusion detection in scalable environments remains a significant research challenge.

Challenges

- Increased network overhead
- Reduced detection efficiency
- Higher processing requirements
- Performance degradation in large networks

Real-Time Detection

It is important to protect MANETs from the rapid spreading routing attacks with real-time intrusion detection. IDS need to detect malicious activity in a timely fashion and take action before the attack can cause serious harm.

But real-time detection demands rapid data processing, fast communication with low latency and efficient mechanisms for decision making. It is difficult to achieve a high detection accuracy with a minimum delay particularly in resource constraint environments like MANET.

Challenges

- Low-latency detection requirement
- Fast attack response mechanism
- High computational demand
- Difficulty balancing speed and accuracy

CONCLUSION

The decentralized architecture and changing topology of MANs makes them very vulnerable to routing attacks. For the secure communication and protection of MANET environment from malicious activities, Intrusion Detection Systems are absolutely necessary. While IDS techniques work well with the traditional type of attacks, Machine Learning and Deep Learning methods offer better results in classification and anomaly detection of attacks. This review paper mentioned the detailed analysis of IDS techniques, Routing attacks, Machine learning methods and Deep learning models, and Comparative research studies. Finally, the study shows that intelligent IDS frameworks with deep learning models are promising solutions for future security systems in MANETs.

REFERENCES

1. Perkins, C. E. (2001). *Ad Hoc Networking*. Addison-Wesley.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

2. Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: milestones, challenges, and new research directions. *IEEE Communications Magazine*, 52(1), 85–96.
3. Murthy, C. S. R., & Manoj, B. S. (2004). *Ad Hoc Wireless Networks: Architectures and Protocols*. Pearson Education.
4. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network,* 13(6), 24–30.
5. Mitrokotsa, A., Dimitriou, T., & Komninos, N. (2014). Intrusion Detection in MANETs: A Survey. *Procedia Social and Behavioral Sciences*, 147, 484–489.
6. Safaa Laqtib, et al. (2020). Intrusion Detection System Based on Deep Learning Techniques for MANET Security. *International Journal of Electrical and Computer Engineering*, 10(5), 5235–5243.
7. Amrendra, K., Sharma, A., & Ranjan, P. (2021). Challenges, attacks and security issues in MANET (mobile ad hoc networks). International Journal of Advance and Innovative Research, 8(4), 137–144. ISSN 2394-7780.
8. Mohammed Kamal, et al. (2021). Deep Learning-Based Intrusion Detection System: A Systematic Review. *IEEE Access*, 9, 123456–123470.
9. Yogendra Kumar & Vijay Kumar. (2023). Hybrid Intrusion Detection Techniques for Wireless Networks. *Wireless Personal Communications*, 132(4), 2357–2375.
10. Sultan, M. T., et al. (2023). ANN-Based Intrusion Detection Mechanism for MANET. *International Journal of Computer Applications*, 185(15), 25–32.
11. Kimanzi, R., et al. (2024). Deep Learning Algorithms Used in Intrusion Detection Systems: A Review. *arXiv Preprint*.
12. Amrendra, K., & Ranjan, P. (2020). Emerging trends and applications in mobile ad hoc networks (MANETs). In S. Prasad (Ed.), Advances in Science & Technology (pp. 10–18). Empyreal Publishing House. ISBN: 978-81-946375-0-9.
13. Chaudhary, A., & Shrimal, G. (2024). Critical Review of IDS Techniques in MANET. *International Journal of Computer Sciences and Engineering*, 12(2), 45–55.
14. Ravi Verma, et al. (2022). Detection and Prevention of Routing Attacks in MANETs. *International Journal of Advanced Networking and Applications*, 14(1), 112–120.