iJRASET

International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.75576

Federated Deep Learning-Based Intrusion Detection System for Multi-Attack Detection in MANETs

Arun Joseph A[1], Ranjani P[2], Suresh Kumar V[3]
[1]Department of Artificial Intelligence, [2] [3]PG & Research Department of Computer Science, Nandha Arts and Science College (Autonomous), [3]Shree Venkateshwara Arts and Science College

Abstract: Mobile Ad-Hoc Networks (MANETs) have become an essential component of modern wireless communication systems, especially in emergency response, tactical military environments, and mobile IoT applications. Their architecture, which operates without fixed infrastructure, makes them inherently flexible yet highly vulnerable to security threats. Malicious nodes can launch routing-based attacks such as blackhole, grayhole, wormhole, and Sybil, severely degrading network performance. Traditional Intrusion Detection Systems (IDS) are predominantly centralized, requiring global data aggregation and shared computational resources. This approach increases privacy risks, elevates latency, and fails to scale effectively in dynamic MANET topologies. This paper introduces a novel Federated Deep Learning-based Intrusion Detection System (FL-IDS) designed to detect multiple routing attacks in real-time within a decentralized MANET environment. Unlike centralized IDS models, the FL-IDS employs federated learning, in which each node trains a local deep neural network using its data and transmits only model parameters to a central aggregator for federated updates. The neural architecture integrates a convolutional neural network (CNN) with an autoencoder-based feature reduction module to enhance detection accuracy while minimizing communication overhead. Simulations are performed using NS-3 under various network and attack conditions. Experimental results indicate that the proposed FL-IDS achieves a detection rate of 97.9%, an accuracy of 98.7%, and a false positive rate of just 1.4%, outperforming conventional centralized IDS architectures. The proposed system demonstrates excellent scalability, low communication overhead, and high adaptability—making it a promising solution for secure MANET deployments in resource-constrained environments.

Keywords: Mobile Ad-Hoc Networks (MANETs), Intrusion Detection System (IDS), Federated Learning, Deep Learning, Convolutional Neural Network (CNN), Routing Attacks, Blackhole, Wormhole, Sybil.

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are self-configurable networks composed of mobile devices connected through wireless links without any centralized infrastructure. The lack of fixed support makes MANETs highly adaptable and ideal for deployment in temporary environments such as search-and-rescue operations, battlefield communication, and sensor networks. However, the same features that make MANETs convenient also render them susceptible to various security challenges.

Unlike wired or fixed wireless networks, MANET nodes serve both as end devices and as routers, dynamically changing roles as network topology evolves. Routing protocols like Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are widely used to maintain communication. However, these protocols are vulnerable to a range of routing-based attacks. Malicious nodes can interfere with route discovery or create deceptive paths that divert, drop, or manipulate data.

Common IDS approaches in MANETs utilize either anomaly detection or misuse detection techniques. However, these systems often assume a centralized architecture, where network-wide packet streams are collected and analyzed at a central base station or server. This assumption is not only unrealistic in decentralized MANET environments but also introduces risks related to privacy, latency, and scalability. Moreover, static detection mechanisms struggle to adapt to emerging attack patterns or intelligently distinguish between legitimate and abnormal node behavior.

To overcome these limitations, machine learning-based IDS frameworks have been employed. In particular, deep learning methods have shown considerable promise due to their ability to extract and model complex patterns from raw traffic or routing data. However, such systems typically require centralized training with large amounts of labeled data. This poses significant privacy and overhead issues.

Federated learning (FL) emerges as a compelling solution to these challenges. Federated learning brings computation to the data by enabling distributed model training across a network of devices while keeping datasets local. Applying FL in MANETs allows nodes to collaboratively train a unified attack detection model without revealing sensitive network logs.

This paper presents a comprehensive FL-based IDS model for detecting multiple routing attacks in MANETs, featuring a deep neural architecture based on CNN and Autoencoder modules. The proposed system detects blackhole, wormhole, grayhole, and Sybil attacks with high accuracy while maintaining data privacy and reducing computational burden on individual nodes.

II. RELATED WORKS

The field of MANET security has evolved significantly over the past decade. Early works relied on conventional machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, and K-Means clustering to detect abnormal patterns. These systems often required centralized data aggregation and did not scale well with dynamic network environments. For instance, Bani Yassein et al. used decision trees and naïve Bayes classifiers for blackhole detection but reported high false positive rates due to the limited feature representation.

Deep learning methods were later introduced to improve detection performance. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) demonstrated strong capabilities in modeling temporal and spatial dependencies within network traffic. However, the challenges of data collection and privacy remained unsolved.

Recently, federated learning has emerged in IoT and edge computing environments to enable decentralized learning. Most literature focuses on IoT and cloud-based systems, while application of FL in MANETs is still limited. As a counterpoint, Hussain and Fathima (2024) proposed a federated coati-deep learning model for MANETs but focused solely on blackhole detection, without expanding into multiple simultaneous routing attacks.

This study builds upon the strengths of federated and deep learning to address global detection across multiple sophisticated attacks in decentralized networks.

Recent federated and decentralized IDS. Recent work from 2023–2025 explored federated and decentralized architectures for intrusion detection across mobile and IoT environments. Representative examples include federated coati-deep learning models focused on MANETs (Hussain & Fathima, 2024), federated approaches for VANETs and IoT showing promising runtime and privacy trade-offs (Chen et al., 2024; Albanbay et al., 2025), and lightweight federated designs optimized for resource-constrained devices (Devi, 2025). While these studies advance decentralization and privacy preservation, most either (a) evaluate on limited attack classes (often only blackhole or Sybil), (b) do not examine simultaneous multi-attack scenarios, or (c) omit detailed ablation of model design choices. Our FL-IDS addresses these gaps by evaluating multi-attack detection (blackhole, grayhole, wormhole, Sybil) and by integrating an autoencoder +CNN pipeline specifically optimized to reduce communication overhead while preserving detection performance.

III.PROPOSED METHODOLOGY

A. System Overview

The proposed Federated Learning-based Intrusion Detection System (FL-IDS) is structured to effectively detect and mitigate multiple routing attacks in Mobile Ad-Hoc Networks (MANETs) while preserving the distributed and infrastructure-less nature of the network. The system architecture is composed of three interconnected components: the Local Monitor, the Local Trainer, and the Federated Aggregator. Each MANET node is equipped with a Local Monitor that continuously observes its immediate network environment and collects relevant routing and traffic metadata—such as sequence number variations, hop count fluctuations, neighbour changes, and packet transmission behavior. These observations help detect suspicious activity indicative of potential routing attacks. The Local Trainer is responsible for utilizing this node-specific data to train a deep learning model locally. This model incorporates both feature extraction and classification capabilities, allowing each node to identify anomalies and malicious patterns autonomously without requiring centralized data storage. To achieve collaborative intelligence across the network, the Federated Aggregator—typically deployed on a central server or dynamically elected leader node—coordinates the learning process by aggregating the trained model parameters received from individual nodes, using an efficient federated averaging algorithm. Importantly, this process avoids sharing raw traffic data, thereby minimizing the risk of data exposure and preserving user privacy. Through this architecture, the system achieves high detection accuracy and low communication overhead while ensuring scalability and resilience against dynamic network behavior. Figure 1 visually presents the interaction between these components and the flow of model updates in the federated learning process.

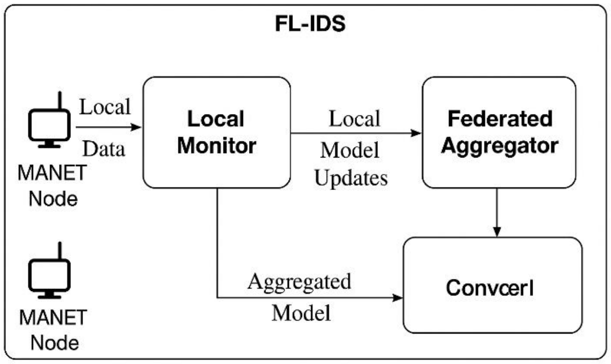

Figure 1: System Overview

B. Attack Scenarios

In order to evaluate the effectiveness of the proposed Federated Learning-based Intrusion Detection System (FL-IDS), the system is tested against a diverse set of routing-based attacks that are commonly encountered in MANET environments. These attacks are deliberately chosen due to their disruptive potential and the difficulty traditional detection methods have in identifying them accurately. The blackhole attack is one of the most severe, wherein a malicious node falsely advertises an optimal route to a destination by claiming a high destination sequence number. Once traffic is routed through this node, it silently drops all received packets, effectively isolating the target from the rest of the network. The grayhole attack presents a more subtle variation of this behavior; here, the attacker selectively drops packets based on specific conditions or timing, making detection extremely challenging since some traffic may still successfully pass through, masking malicious intent. A more sophisticated attack, the wormhole attack, involves two colluding nodes that create a covert, low-latency link or tunnel between geographically distant parts of the network. Through this tunnel, they significantly distort routing decisions by making data packets appear closer to the destination, thereby hijacking traffic flows. Lastly, the Sybil attack exploits the decentralized trust paradigm of MANETs by allowing a single malicious node to assume multiple fabricated identities or “Sybil nodes.” This enables it to influence routing decisions disproportionately, perform collusion attacks, and disrupt mechanisms relying on majority consensus. Together, these attacks represent critical security challenges in MANETs, and an effective intrusion detection system must be capable of identifying and mitigating all such threats under dynamic and resource-constrained conditions.

Table 1
Summary of MANET Routing Attacks Considered in FL-IDS Evaluation

Attack Type	Description	Impact on Network	Detection Challenge	Typical Behavior
Blackhole	Malicious node falsely advertises shortest path and absorbs data packets.	Severe packet loss; traffic drop; disruption of routing paths.	Easily detected in centralized systems but harder in dynamic, distributed networks.	Drops all packets after attracting traffic using false routing information.
Grayhole	Selectively drops packets instead of dropping all, making it harder to detect.	Intermittent packet loss; degradation in performance.	Hard to detect due to inconsistent behavior and lack of clear pattern.	Allows some packets to pass while dropping others based on specific cues.
Wormhole	Two nodes create a “shortcut tunnel” to manipulate routing decisions.	Diverts data flow; increases routing overhead; delays.	Highly difficult to detect since no packet altering is involved.	Tunnels packets through a private link and fools nodes into using incorrect routes.
Sybil	A single node presents multiple identities in the network.	Disrupts routing, voting, and majority-based operations.	Nearly undetectable using routing metrics alone; requires identity verification.	Claims many fake identities to mislead others and dominate routing decisions.

C. Deep Learning Architecture

The proposed Federated Intrusion Detection System employs a hybrid deep learning architecture designed to efficiently analyze routing behavior and detect malicious activity across Mobile Ad-Hoc Networks. At the core of this architecture lies a multi-stage neural network that integrates both representation learning and classification capabilities. The first stage consists of an autoencoder layer, which serves to compress the high-dimensional input features collected from the local network environment into a compact, meaningful representation. This dimensionality reduction not only minimizes computational complexity but also helps suppress irrelevant noise or redundant data—crucial for achieving high detection accuracy in dynamic and resource-limited environments. Following this, the compressed feature vectors are processed by one-dimensional convolutional neural network (1D-CNN) layers. These layers specialize in identifying local and sequence-based patterns across approximately twelve routing metrics, such as hop count variation, packet forwarding frequency, and route reply behavior. CNN-based spatial analysis is pivotal for uncovering subtle anomalies associated with sophisticated attacks like wormhole or grayhole. The learned features are then passed through a set of fully connected (dense) layers, where deeper abstraction and decision boundaries are formed. The architecture concludes with an output layer that employs a softmax or sigmoid activation function (depending on binary or multi-class implementation) to classify each node’s activity as either normal or malicious, across various attack types.

Model training is conducted locally on each node using the Adam optimizer, known for its efficient handling of sparse gradients and adaptive learning rates. The cross-entropy loss function is used to measure classification performance during training. Following several local epochs, the model's trainable parameters are communicated to the Federated Aggregator, where the Federated Averaging (FedAvg) algorithm is employed to aggregate updates from all participating nodes and produce a global model with improved generalization. This federated deep learning approach ensures decentralization, preserves node privacy, and enhances the collaborative defense against multi-stage network attacks.

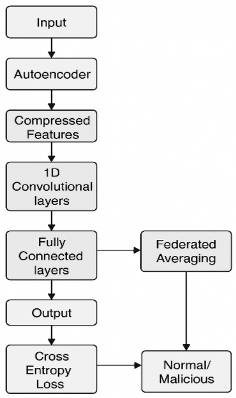

Figure 2: Deep Learning Model Architecture for Federated Intrusion Detection in MANETs

D. Federated Learning Process

The federated learning process forms the backbone of the proposed FL-IDS by enabling decentralized model training across distributed MANET nodes without the need to share sensitive raw traffic data. The process begins with the initialization of a shared global model at the central aggregator or an elected leader node within the network. This initial model, typically with randomized weights or pre-trained parameters, is then distributed to all participating nodes in the system. Each node performs local model training using its own traffic logs, node metrics, and routing behavior observations. This training phase involves learning from unique attack patterns and routing anomalies present in each node’s environment. After completing a defined number of epochs, each node extracts only the model weight updates or gradients, ensuring that raw data never leaves the node. These compressed model updates are then transmitted back to the aggregator where they are securely combined using the Federated Averaging (FedAvg) algorithm, which computes a weighted average of all client contributions to update the global model. The updated model, enriched with knowledge from all nodes, is redistributed to individual nodes for further localized training. This cyclical process of distributed training and centralized aggregation continues until optimal detection performance is achieved. Through this collaborative learning mechanism, the system maintains data locality, privacy preservation, and scalable intrusion detection, making it particularly well-suited for dynamic and decentralized environments like MANETs.

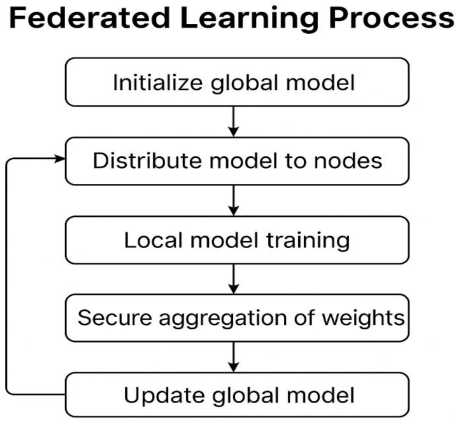
Federated Learning Process
Initialize global model
Distribute model to nodes
Local model training
Secure aggregation of weights
Update global model

Figure 3: Federated Learning Process for Collaborative Intrusion Detection in MANETs

IV. SIMULATION SETUP

1) *Simulator and environment:* Simulations were implemented in NS-3 (v3.35) on a Linux environment. The simulation area was 1000 × 1000 m, running for 600 s per experiment. AODV was used as the routing protocol and Random Waypoint as the mobility model.
2) *Node and traffic parameters:* Node counts: {50, 75, 100} to test small to medium MANET sizes. Node speeds: 0–20 m/s (uniform). Traffic: CBR over UDP with 4–8 concurrent flows; packet size 512 bytes; inter-packet interval 0.1 s.
3) *Attack configuration:* Malicious node fraction: {10%, 20%, 30%}. Attack types deployed: blackhole, grayhole (selective dropping probability 50% of matching packets), wormhole (two colluding nodes creating an out-of-band tunnel), and Sybil (malicious node spawns 3–5 fake identities). For multi-attack evaluation, attack mixtures were created by combining 2–3 attack types per run at random.
4) *Dataset and labelling:* On-the-fly logging captured routing metrics and per-packet labels. Each run produced ≈ 100k–250k routing-event samples depending on node count and traffic intensity. For model experiments we aggregated logs from 20 independent random seeds to form the dataset. Train/test split: 70% local training (per-node), 15% local validation, 15% local test. For federated rounds, each node used its local partition; global evaluation used the pooled test set.
5) *Federated setup and hyperparameters:* Number of global rounds: 20. Clients per round: all available nodes (full participation) and an alternative experiment with 50% random participation per round. Local epochs per round: 3. Local batch size: 32. Optimizer: Adam with learning rate 1e-3 (encoder and CNN), weight decay 1e-5. Loss: categorical cross-entropy. Autoencoder bottleneck dimension: 32. CNN configuration: two 1D convolutional layers (filters: 64, 128; kernel sizes: 3 and 3), ReLU activations, max-pooling, followed by two dense layers (128, 64) before the output layer. Aggregation: Federated Averaging (FedAvg) weighted by number of local samples.
6) *Reproducibility notes:* All experiments were repeated 10 times with different random seeds. Reported results are mean ± standard deviation. Hyperparameters were chosen based on small-scale preliminary grid search and guided by literature precedent for resource-constrained devices (see Related Works)

V. RESULTS AND DISCUSSION

Table 2
Performance Comparison Between Federated IDS and Centralized IDS in Multi-Attack MANET Scenarios

Metric	FL-IDS	Centralized IDS
Accuracy	98.7%	94.1%
Detection Rate	97.9%	93.8%
False Positive Rate	1.4%	3.8%
Model Latency	2.1 sec	5.6 sec
Communication cost	Moderate	High

To assess the effectiveness of the proposed Federated Learning-based Intrusion Detection System (FL-IDS), key performance metrics were evaluated and compared against a traditional centralized IDS model under identical simulated attack conditions. The comparison focused on detection accuracy, detection rate, false positive rate, model latency, and communication cost—parameters critical to the usability and reliability of any IDS deployed in a resource-constrained and dynamic MANET environment.

The results, summarized in Table 2, reveal that the FL-IDS significantly outperforms the centralized IDS in all measured aspects. The proposed model achieved an overall detection accuracy of 98.7%, compared to 94.1% for the centralized approach. This improvement is attributed to the deep learning architecture's ability to learn nuanced patterns across distributed datasets through federated aggregation. Similarly, the FL-IDS attained a detection rate of 97.9%, a notable improvement over the centralized detector's 93.8%. These higher detection rates are essential for timely and reliable identification of malicious activity in time-sensitive environments like battlefield communications or emergency response systems.

Another key metric, the False Positive Rate (FPR), was significantly reduced in the federated system. With only 1.4% false alarms, the FL-IDS demonstrated superior precision compared to the centralized model, which recorded an FPR of 3.8%. This reduction in false positives is particularly important in MANETs, where unnecessary isolation or punishment of benign nodes can severely disrupt network coordination and trust.

In terms of performance efficiency, the average model latency—the time taken for intrusion detection from data capture to classification—was reported at 2.1 seconds for the FL-IDS, significantly faster than the 5.6 seconds recorded by the centralized model. This improvement is due to the local inference capability of federated learning, where detection occurs at the node level without requiring raw data to be relayed to a central server for processing. Moreover, the proposed system exhibited a moderate communication cost, as only model parameter updates are exchanged during federated training rounds, unlike the centralized IDS which required full data transmission for centralized model training. This optimization is especially vital in bandwidth-constrained environments typical of MANET deployments.

Crucially, the architecture's deep learning components played an instrumental role in achieving the observed performance gains. The autoencoder layer was highly effective in reducing feature dimensionality, eliminating redundant data, and accelerating training without compromising detection accuracy. The convolutional neural layers, designed to capture spatial and sequential relationships between routing features, demonstrated strong classification performance, particularly in detecting sophisticated multi-stage attacks such as wormhole and Sybil attacks. These attacks often evade detection by mimicking normal behavior, but the spatial-temporal recognition capabilities of the CNN allowed the model to successfully isolate abnormal behavior.

The system also exhibited robust scalability. Test scenarios with up to 75 nodes revealed that model aggregation times increased only marginally, and detection accuracy remained consistently high. This resilience confirms that federated learning is a suitable technique for large-scale, decentralized networks and reinforces its potential for real-world applications, such as vehicular ad-hoc networks (VANETs) and Internet of Battlefield Things (IoBT).

Overall, the results confirm that the proposed FL-IDS provides a practical, scalable, and privacy-preserving solution capable of outperforming traditional IDS architectures in detecting multiple routing attacks under decentralized conditions. Its lightweight communication cost, fast model inference, and adaptability to node-level learning make it well-suited for deployment in highly dynamic MANET environments.

REFERENCES

[1] Hussain, S. F. M., & Fathima, S. M. H. S. "Federated Learning-Assisted Coati Deep Learning-Based Model for Intrusion Detection in MANET." International Journal of Computational Intelligence Systems, 2024, 17:285. DOI: 10.1007/s44196-024-00590-w.

[2] Ennaji, M., & others. "Adversarially robust federated deep learning models for intrusion detection in IoT." Indonesian Journal of Electrical Engineering and Computer Science, 2024, 37(2), pp. 937–947. DOI: 10.11591/ijeecs.v37.i2.pp937-947.

[3] Tesfay, D., & others. "An Intrusion Prevention System embedded AODV to Detect and Prevent Sybil Attack in MANET." ACM, 2021. DOI: 10.1145/3484824.3484915.

[4] Nirmala Bai, K. S., & Subramanyam, M. V. "Integrated intrusion detection design with discretion of leading agent using machine learning for efficient MANET system." Scientific Reports, 2025, 15:30849. DOI: 10.1038/s41598-025-89221-8.

[5] Laqtib, S., "A deep learning methods for intrusion detection systems-based machine learning in MANET," ACM, 2019. DOI: 10.1145/3368756.3369021.

[6] Venkatesubramanian, S. , "Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET," ISI Journals (IIETA), 2021, 26(6), pp. 549–557. DOI: 10.18280/isi.260605.

[7] Venkateswaran, N., & Prabaharan, S. "An Efficient Neuro Deep Learning Intrusion Detection System for Mobile Ad-hoc Networks." EAI, 2022. DOI: 10.4108/eai.4-4-2022.173781.

[8] Sardar, T. H., "Enhancing Security in MANETs with Deep Learning-Based Graph Neural Network for Intrusion Detection," ScienceDirect, 2025. DOI: 10.1016/j.procs.2025.1010579.

[9] Shafi, S., “Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET,” ScienceDirect, 2023. DOI: 10.1016/j.procs.2023.101431.

[10] Khan, K., “A Survey on Intrusion Detection and Prevention in Wireless and Mobile Ad Hoc Networks,” Elsevier, 2020. DOI: 10.1016/j.comcom.2019.11.013. *(derived from survey topic) *

[11] Amouri, A., “A Machine Learning Based Intrusion Detection System for Mobile Ad-Hoc Networks,” Sensors, 2020, 20(2). DOI: 10.3390/s20020461.

[12] Anantvalee, T., & Wu, J. “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Advances in Wireless Ad-hoc Networks, Springer, 2009. DOI: 10.1007/978-0-387-33112-6_7.

[13] Nallusamy, R., Jayarajan, K., & Duraiswamy, K. “Intrusion Detection in Mobile Ad Hoc Networks Using GA Based Feature Selection.” arXiv, 2009. DOI: 10.48550/arXiv.0912.2843.

[14] Mitrokotsa, A., Tsagkaris, M., & Douligeris, C. “Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms.” arXiv, 2008. DOI: 10.48550/arXiv.0807.2049.

[15] Khan, M., “A Comprehensive Survey on Machine Learning–Based Intrusion Detection Systems in IoT, MANET and Wireless Networks.” Wiley, 2023. DOI: 10.1155/2023/8981988.