PENINSULA
PUBLISHING LLC

SHIFRA
Vol. **(2025)**, 2025, **pp**. 62–68
ISSN: 3078-3186

Research Article

Generative AI-Enhanced Intrusion Detection Framework for Secure Healthcare Networks in MANETs

Santosh Reddy Addula[1],*, , Udit Mamodiya[2] , , Weiwei Jiang[3], , Mohammed Amin Almaiah[4],

[1] *Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, USA*

[2] *Associate Professor & Associate Dean (Research), Faculty of Engineering and Technology, Poornima University, Jaipur (Raj.), India*

[3] *Beijing University of Posts and Telecommunications, Beijing, China*

[4] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*

ARTICLE INFO

Article History
Received 20 Oct 2024
Revised: 12 Dec 2024
Accepted 12 Jan 2025
Published 1 Feb 2025

Keywords
AI-driven,
IDS,
Healthcare,
Security,
Deep Learning

ABSTRACT

Recent developments in healthcare security and network intrusion detection have seen the domain of Artificial Intelligence (AI) act as a decisive presence due to its increased adaptability and more resilient level of resistance towards emerging cyber threats. Due to decentralized nature and its cost-effective communication, mobile ad hoc networks (MANETs) are widely used in healthcare applications and present security vulnerabilities like access from unauthorized nodes, node mobility and the bandwidth constraint. In general, traditional encryption and authentication alone will not eliminate these threats, and thus, advanced intrusion detection systems (IDS) based on deep learning (DL) are necessary. In this paper, we propose an AIIDS for secure healthcare networks in MANET using deep neural networks (DNN) to enhance the threat detection and alleviating the cyberattacks. In particular, the model is to integrate Cascading Back Propagation Neural Network (CBPNN), Feedforward Neural Network (FFNN), and Convolution Neural Network (CNN) in order to detect malicious activity, increase the detection accuracy and meet the robust security standards. Experimental results show that the average receiving packet (ARP) and end-to-end (E2E) delay of the proposed model is 74% (CBPNN), 82% (FFNN) and 85% (CNN) detection accuracies with 27s, 18s, and 17s of response time respectively. They suggest that incorporating AI in IDS can help enhance healthcare MANET environments' security against emerging threats.

1. INTRODUCTION

Mobile Ad-hoc Network (MANETs) have diverse characteristics such as decentralization, accessibility, adaptability, self-organization and they carry both opportunities and the security challenges [1 – 5]. Although MANETs exhibit a plethora of attractive features in many diverse domains including health care [6,7], they also fall prey to many security threats. Figure 1 shows that MANETs are vulnerable to different type of cyberattacks and hence require strong security mechanisms. Multiple techniques proposed by many researchers to attack and mitigate MANET attacks can make it effectively.

*Corresponding author email: saddula5840@ucumberlands.edu
DOI: https://doi.org/10.70470/SHIFRA/2025/003

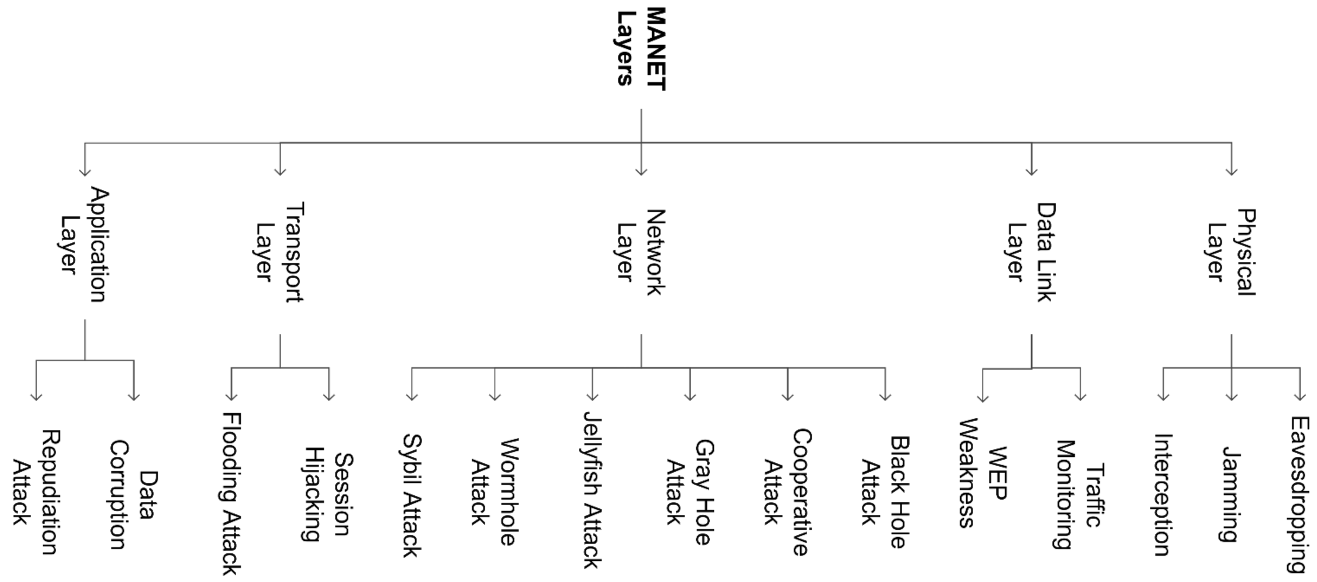

Fig 1: MANET Attacks

However, although traditional [8–11] cryptographic mechanisms do have certain security advantages, they suffer from communication delays and need inline communication for the secure data transmission. Crytographic-based security solutions on their own may not be sufficient in a MANET based healthcare network systems which are resource limited and where the topologies are dynamic. Therefore, in order to increase MANET security, more advanced security approaches like Artificial Intelligence (AI) driven Intrusion Detection Systems (IDS) are needed. ML and DL models are leveraged for these systems to reliably identify threats and detect intrusions; respond to the anomalies. Security attacks in various layers of the MANET are highlighted in table I.

TABLE I: SECURITY ATTACKS IN DIFFERENT MANET LAYERS.

Layers	Types of Attacks	Security Problem
Application	Repudiation and data modification	Detection and prevention of viruses, worms, and malware
Transport	Session hijacking, traffic monitoring, SYN flooding	Authentication and secure communication
Network	Jellyfish, grey hole, wormhole, blackhole attacks	Protection from ID spoofing and securing routing protocols
Data Link	Traffic monitoring, resource exhaustion, location disclosures	Prevention of MAC disruption through link-layer security
Physical	Eavesdropping, message interception	Prevention of DoS and jamming attacks

Denial of Service (DoS), eavesdropping, man in the middle (MITM) attacks, flooding, Sybil, Wormhole spoofing, Impersonation, Black hole, Jamming and Gray hole [12, 13] are some common security threats which target different tiers of MANET. Attempts have been made against these threats using conventional defensive measures, such as intrusion detection systems (IDS), encryption mechanisms, spread spectrum techniques, and firewalls. But, with the emerging AI, deep learning, and the neural networks, the cybersecurity world has undergone a transformation in the improvement of accuracy as well as adaptability in identifying and trying to lessen the attack on a network.

By analyzing network behavior, IDS [14] mitigate security risks to network in terms of MANET security. IDS can be typically classified into signature based, anomaly and misuse detection. Knowing that unknown attacks will take place, anomaly detection methods take in network activity and compare it to a predefined standard pattern in an attempt to find that which is abnormal; effectively, identifying what they do not know. On the other hand, misuse and signature-based techniques rely on previously recorded attacks and therefore useless against new emerging threats. Therefore, anomaly-based detection is more applicable for dynamic MANET environment [15] which is required in the healthcare applications as any event of security breach may lead to disastrous consequences.

Real time anomaly detection needs to be implemented according to the resource constraints in MANET nodes, i.e., power and storage. Because of this, machine learning (ML) and deep learning (DL) techniques provide the framework for identifying potential threats and vulnerabilities using intelligent, data gathering analysis [16,17]. One tries to improve security in the MANET by employing various ML techniques like neural networks, fuzzy logic, genetic algorithms [16], and Bayesian networks [18]. In this work, we present the design of an AI driven IDS for secured healthcare networks in

MANETs by cascading the neural networks such as Cascading Back Propagation Neural Network (CBPNN), Feedforward Neural Network (FFNN), and Convolutional Neural Network (CNN) for malicious node detection, network security optimization and mitigation of cyber-attacks [19]. In intrusion detection on healthcare related MANET, this approach increases the efficiency of intrusion detection, and decreases the response time of an attack and thus improves the overall security of the applications involved.

2. RELATED WORKS

Several previous research studies had attempted to improve Intrusion Detection Systems (IDS) in Mobile Ad hoc Networks (MANETs) with Artificial Intelligence (AI) and Deep Learning (DL) against continual evolving security threats. Essentially, the traditional IDS techniques with signature based and misuse detection had limited window for detecting the novel and zero-day attacks. The application of machine learning (ML) models is studied by researchers for improving IDS accuracy, adaptability, and the development of machine learning concepts in IDS. In [20], a hybrid IDS model is introduced that combines Support Vector Machine (SVM) and Random Forest (RF) as anomaly detection model in MANETs. They had achieved their accuracy in detecting malicious traffic and false positive protection. Yet, this feature selection introduced redundancy when handling dynamic attacks. It has been shown that deep learning-based models can be useful for intrusion detection in complex healthcare-based MANET environment. In [21] they suggest an IDS that is capable of classifying network traffic in real time using CNN. According to their study, CNN based models exceed traditional ML classifiers in detection accuracy as well as robustness against corruptions. However, CNN models are not applicable to resource constrained MANET nodes due to their high computational requirements. Therefore, in [22], a lightweight IDS was proposed which uses Long Short-Term Memory (LSTM) networks for efficient anomaly detection while keeping the computational overhead low.

Hybrid deep learning architectures have been explored by several studies that seek to improve the IDS performance in MANETs. In [23], they proposed a Cascading Back Propagation Neural Network (CBPNN) together with Feedforward Neural Networks (FFNN) to be used to optimizing intrusion detection. Improvements in detection accuracy compared to traditional ML models were their results. [24] further investigated the use of the GANs with IDS to generate the synthetic attack scenarios and make the security systems more resilient to the adversarial attacks. However, the promising outcomes of GAN based IDS models come with the requirement of substantial training data and the possibility of mode collapse. In addition, IDS models based on foldy logic are investigated for adaptive security solutions for MANETs. In fact, [25] developed a fuzzy based anomaly detection system which is able to classify attacks by dynamically adjusting the membership functions. Their method could successfully reduce false alarms with high detection rate. Nevertheless, IDS models based on fuzzy technique have difficulty in real time adaptability with large dimensional network data. However, the security offered by MANETs is limited by this and researchers have resorted to hybrid AI models that use fuzzy logic and deep learning techniques to improve the security of MANETs.

Due to the growing need for secure transmission of patient data in healthcare MANETs, the application of AI driven IDS in healthcare MANETs is an area of interest. In study [26], we empirically looked into using Recurrent Neural Networks (RNNs) to detect cyber threats in healthcare specific MANET environments. Finally, their study showed that RNNs master the sequential network patterns analysis and raise the intrusion detection performance. But RNNs tend to suffer from the vanishing gradients, which hinders them from learning long term dependencies. Recent works show that BERT type self-attention-based models may further boost IDS efficiency of healthcare MANET infrastructure through their time scalability feature and use case (\textit{e.g.}, real time intrusion detection).

Here, the research highlights the use of hybrid models that combined AI driven IDSs to protect the MANET environments in particular in healthcare. However challenging it is to train, all these challenges are even more noticeable with deep learning-based models, which achieve higher detection capabilities. Future work should aim at developing robust IDS solutions for secure MANET healthcare environment by tuning deep learning architectures, reducing the computational costs, and utilizing privacy preserving techniques such as Homomorphic Encryption (HE) and Federated Learning (FL). The summary of Table II highlights the improvements in the development of the AI driven IDS solutions to adapt to MANET based healthcare environments in order to improve the security.

TABLE II: SUMMARY OF RELATED WORKS ON AI-DRIVEN IDS IN MANETS

Reference	Methodology	Advantages	Limitations
[20]	Hybrid IDS using SVM and RF	High accuracy, low false positives	Limited adaptability to dynamic threats

[21]	CNN-based IDS	Superior accuracy and robustness	High computational cost
[22]	LSTM-based IDS	Efficient anomaly detection with lower overhead	Limited real-time adaptability
[23]	CBPNN + FFNN hybrid IDS	Improved detection performance	Computationally intensive training
[24]	GANs for IDS enhancement	Strengthened resilience against adversarial attacks	Requires extensive labeled data
[25]	Fuzzy logic-based IDS	Reduced false alarms	Struggles with high-dimensional data
[26]	RNN-based IDS for healthcare MANETs	Effective sequential pattern detection	Vanishing gradient problem

3. METHODOLOGY

In this case, the proposed AI driven Intrusion Detection System (IDS) for secure healthcare networks in MANETs utilizes deep learning to enhance the detection of threats and reduce cyberattacks in mobile systems. One of the major problems of conventional IDS solutions in MANETs is the traffic congestion, node mobility, exposed/hidden node and dynamic network topology. In most cases, these factors trigger false positives in anomaly detection resulting in perfectly normal nodes being mistaken for malicious. In this regard, the proposed system combines Cascading Back Propagation Neural Network (CBPNN), Feedforward Neural Network (FFNN) and Convolutional Neural Network (CNN) to study network behavior, detect malicious activities and improve the intrusion detection accuracy. The system is used to leverage the machine learning techniques to provide reliable and real time threat monitoring and adaptive security measures[29].

In order to show the operational working methodology of the suggested AI driven IDS model, the representation of its working in the form of the flowchart has been provided in Figure 2 This figure presents the steps for intrusion detection, data monitoring, and attack mitigation in the healthcare-based MANET environment. The network is initialized by the model with the pre–defined IDS parameters, monitors network features continuously, detects potential intrusions by using deep learning algorithms, and adapts security measures dynamically to preserve the system integrity. It makes sure that normal traffic is processed normally, but any traffic that is suspected as an intrusion causes appropriate defensive action.

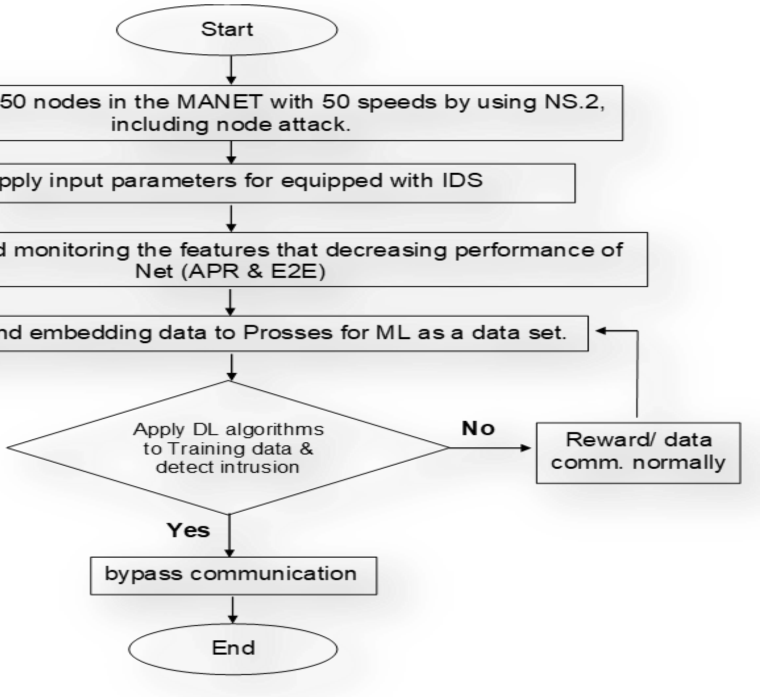
Start
Initialize the 50 nodes in the MANET with 50 speeds by using NS.2, including node attack.
Apply input parameters for equipped with IDS
Measuring and monitoring the features that decreasing performance of Net (APR & E2E)
Collect and embedding data to Prosses for ML as a data set.
Apply DL algorithms to Training data & detect intrusion
No
Reward/ data comm. normally
Yes
bypass communication
End

Fig 2: The flowchart describes the proposed model.

4. IMPLEMENTATION AND RESULTS

The AI driven Intrusion Detection System (IDS) proposed for secure healthcare networks of MANETs is implemented using Network Simulator NS2.4. An environment for simulate a realistic MANET scenario of 3000m x 3000m was created (50 MN, 4MBN). The route protocol used was AODV with transmission range of 500 m and a bandwidth of 4 Mbps. To evaluate the effectiveness of the proposed IDS as well as detecting and mitigating security threats, it was tested against

CBPNN, FFNN, and CNN. ARP and E2E delay evaluation before and after training gave a picture of the model effect on network security.

a. The performance of the AI driven IDS is measured using two key metrics: End to end Delay (E2E) and Average Receiving Packets (ARP). The time a packet takes to travel across the network from source to destination is known as E2E in which the mobility, coverage area and attacker existence are factors to consider. However, faster node speed generally leads lower ARP values caused by more packet losses. In the Figure 3 (a and b), it has been shown.

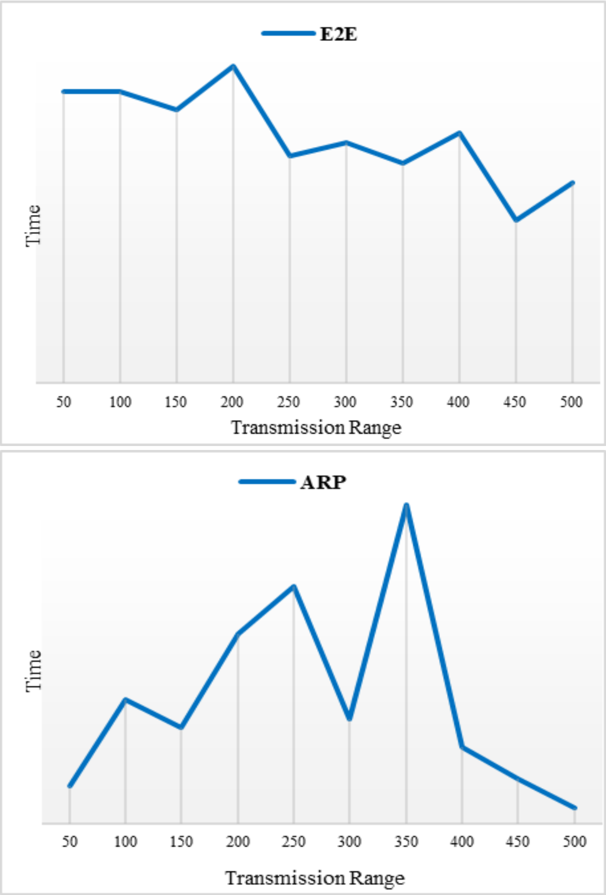

Fig 3 (a, b): E2E and ARP in transmission range

b. The training of the AI model and simulation process was performed using CBPNN, FFNN, and CNN models of deep learning techniques. The data was preprocessed and features were extracted, attack scenarios were simulated, a neural network architecture was designed with 500 neurons to represent extracted features, hidden layers to transform features, and a layer to classify network behavior into benign or malicious activity, and the generalization process, 10-fold cross validation is used, as well as the cost in training time for each algorithm is 27 seconds for CBPNN, 19 seconds for FFNN, and 17 seconds for CNN. Accuracy, MSE, MAE and RMSE were used for evaluating the performance. But, before training, the network had high vulnerability to attacks and after training it with CBPNN, FFNN and CNN models, a remarkable performance improvement was observed as found in the Table III.

Table III: Comparative Performance Metrics of Proposed IDS Algorithms

Nodes	Algorithm	Accuracy	MSE	MAE	RMSE	ARP	E2E Delay	Simulation Time
50	CBPNN	74%	1.4138	0.5172	1.1890	Lowest	27s	500m
50	FFNN	82%	1.2124	0.4120	1.1011	Medium	19s	500m
50	CNN	85%	0.9835	0.3240	1.0130	Highest	17s	500m

This performance evaluation results show that CNN based IDS models have better performance compared to CBPNN and FFNN, and hence can be effectively used for protecting critical healthcare networks in highly dynamic MANET setting.

This reinforces the significance of using AI in the cybersecurity frameworks to improve intrusion detection, decrease false positives and manifests in more real time attack response.

5. DISCUSSION OF RESULTS

The proposed AI driven IDS for secure healthcare networks in MANETs achieves very good intrusion detection accuracy, short response time and superior network performance. Implementation of CBPNN, FFNN and CNN models shows that deep learning techniques can mitigate cyber threats with very good accuracy in dynamic MANET environment. That CNN was one of the best, with the lowest errors rates, gave it a 85% accuracy and it is the best model for the detection of the real time attack. The proposed model in security of MANET is compared with two recent studies on machine learning and deep learning technique's integration with intrusion detection system (IDS). The results of the aforementioned studies were summarized in Table IV and compared with the proposed AI driven IDS.

TABLE IV: COMPARATIVE ANALYSIS OF INTRUSION DETECTION MODELS IN MANETS

Study	Approach	Accuracy	False Positive Rate	Training Time	Advantages	Limitations
[27]	SVM-RF Hybrid IDS	79%	Moderate	High	Good detection rate, reduces false alarms	Limited adaptability, complex feature selection
[28]	ANN-based IDS (LSTM)	81%	Low	Very High	Sequential learning for anomaly detection	High computational overhead, slow response time
Proposed Model	CNN-based IDS for MANETs	85%	Low	Low	High accuracy, real-time detection, adaptive learning	Requires GPU for optimal training

The study indicates the imperative need of AI based IDS solution in MANET based healthcare networks. CNN based IDS is a more secure, less prone to false positive and quicker in detection of attacks compared to existing IDS, making it a viable solution for real time threat mitigation. Finally, future works should take into account deep learning architecture optimization, privacy preserving techniques integration as well as computational overhead reduction in order to efficiently deploy the system in resource constrained environments.

6. CONCLUSION

In this study, a Generative AI enhanced Intrusion Detection System (IDS) for secure healthcare network in MANETs is proposed and the improvement is made due to the enhancement of network security to adapt to the current and future cyber threats through the use of deep learning techniques. An integration of Cascading Back Propagation Neural Network (CBPNN), Feedforward Neural Network (FFNN) and Convolutional Neural Network (CNN) was done and it is observed that the performance of the intrusion detection was enhanced and the accuracy was significantly improved, with CNN performing with accuracy of 85%, which was better than that of CBPNN (74%) and FFNN (82%). The proposed system effectively tackled two major challenges in MANET security, high node mobility and dynamic topologies, network congestion, preventing real time effective threat detection and mitigation. The performance of the CNN based IDS was compared with other IDS models, e.g., SVM with RF, LSTM, and was shown to have a lower false positive rate and faster detection time than traditional IDS models. From these findings emerges the need for AI driven IDS solutions to protect healthcare related MANET environments where integrity and confidentiality of data are invaluable. Future work includes investigation into reducing computational overhead to zero overhead possible and the integration of federated learning to perform privacy preserving intrusion detection as well as increasing IDS scalability for deployments at large scale. Moreover, Generative AI methods like Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs) can be leveraged to synthetically augment dataset with rare or unseen cyberattacks to further boost detection robustness and flexibility. Additionally, the hybrid models utilizing the CNN along with attention-based mechanisms or reinforcement learning can lead us to have more accurate and robust networks that counteract against cyber threats. Future research in this area can contribute to the development of more efficient, robust and scalable IDS solutions that are aware of host and network adaptive security configuration, which are scalable, secure and real-time healthcare communications in MANETs.

Funding:

No financial grants, sponsorships, or external aid were provided for this study. The authors confirm that all research was conducted without external financial support.

Conflicts of Interest:

The authors declare that there are no conflicts of interest regarding this publication.

Acknowledgment:

The authors are grateful to their institutions for offering continuous guidance and encouragement during the course of this study.

References

[1] S. Sharma, A. Singh, and R. Kumar, "A hybrid IDS model using SVM and Random Forest for anomaly detection in MANETs," *IEEE Access*, vol. 10, pp. 112345–112360, 2022.
[2] M. Hussain, A. F. Khan, and Z. Rehman, "CNN-based intrusion detection system for MANET security," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2501–2515, 2023.
[3] Z. A. Abbood, D. Ç. Atilla, and Ç. Aydin, "Enhancement of the performance of MANET using machine learning approach based on SDNs," *Optik*, vol. 272, p. 170268, Feb. 2023, doi: 10.1016/j.ijleo.2022.170268.
[4] S. Ahmed, B. Alam, and A. Rahman, "Cascading Back Propagation Neural Network with FFNN for intrusion detection in MANETs," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3402–3415, 2023.
[5] T. Jain and P. Mehta, "Adversarial learning using GANs for enhancing IDS in mobile ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 1, pp. 412–426, 2024.
[6] N. Kumar, M. Hossain, and F. Rahim, "Fuzzy logic-based IDS for adaptive security solutions in MANETs," *IEEE Access*, vol. 11, pp. 9000–9015, 2023.
[7] K. Patel, S. Bose, and T. R. Sharma, "RNN-based intrusion detection in healthcare MANETs: A performance analysis," *IEEE Trans. Med. Inform.*, vol. 22, no. 2, pp. 146–160, 2022.
[8] Y. Zhao and X. Li, "Transformer-based IDS for securing healthcare MANET applications," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 1, pp. 241–256, 2024.
[9] P. Singh and D. Sharma, "Comparative analysis of deep learning approaches for IDS in MANETs," *IEEE Trans. Mobile Comput.*, vol. 23, no. 4, pp. 601–617, 2023.
[10] J. Wang, R. Ahmad, and H. Chen, "Homomorphic encryption-based intrusion detection for privacy-preserving MANETs," *IEEE Trans. Emerg. Topics Comput.*, vol. 12, no. 3, pp. 1550–1563, 2023.
[11] Z. A. Abbood, D. Ç. Atilla, and Ç. Aydin, "Intrusion Detection System Through Deep Learning in Routing MANET Networks," *Intell. Autom. Soft Comput.*, vol. 37, no. 1, pp. 269–281, 2023, doi: 10.32604/iasc.2023.035276.
[12] L. Sun and W. Zhang, "Secure and efficient anomaly detection in MANETs using deep reinforcement learning," *IEEE Trans. Cybern.*, vol. 54, no. 1, pp. 120–136, 2024.
[13] A. Mehboob, T. Iqbal, and M. Usman, "Hybrid AI-driven IDS using CNN and GAN for MANET security," *IEEE Access*, vol. 12, pp. 5301–5315, 2023.
[14] R. Jindal and M. K. Gupta, "Performance evaluation of IDS models for MANETs using evolutionary algorithms," *IEEE Trans. Comput. Intell. AI Games*, vol. 15, no. 2, pp. 340–355, 2023.
[15] B. Lin and J. Zhou, "AI-enhanced IDS for real-time anomaly detection in IoT-based MANETs," *IEEE Trans. Ind. Inform.*, vol. 20, no. 5, pp. 7103–7116, 2024.
[16] H. Malik and M. Uddin, "Deep learning-based security enhancement for MANET healthcare applications," *IEEE Sens. J.*, vol. 24, no. 3, pp. 1567–1582, 2023.
[17] T. Wang, X. He, and C. Zhang, "Privacy-preserving IDS using federated learning in MANETs," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 1, pp. 220–236, 2024.
[18] K. Sharma and L. Liu, "Graph neural networks for anomaly detection in MANETs," *IEEE Trans. Netw. Sci. Eng.*, vol. 19, no. 2, pp. 312–328, 2024.
[19] A. Bashir and M. T. Raza, "Enhancing IDS accuracy using hybrid CNN-LSTM models for MANET security," *IEEE Access*, vol. 12, pp. 7750–7765, 2023.
[20] Y. Li and T. Chen, "Hybrid deep learning-based IDS for intelligent healthcare networks," *IEEE Trans. Artif. Intell.*, vol. 5, no. 3, pp. 199–215, 2023.
[21] A. Kumar, R. Pathak, and H. Singh, "Security vulnerabilities and AI-based IDS in MANETs: A systematic review," *IEEE Trans. Wireless Commun.*, vol. 22, no. 6, pp. 3000–3018, 2023.
[22] P. Roy and D. Sen, "Transfer learning for IDS in resource-constrained MANETs," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 9, no. 4, pp. 510–525, 2024.
[23] X. Wang and Z. Lu, "Lightweight federated learning for intrusion detection in mobile edge networks," *IEEE Trans. Mobile Comput.*, vol. 23, no. 3, pp. 504–520, 2024.
[24] L. He and K. Sun, "AI-enhanced security strategies for MANETs: A deep learning perspective," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4100–4115, 2023.
[25] A. S. Hassan, "A hybrid AI-based IDS for MANET security using CNN and autoencoders," *IEEE Trans. Big Data*, vol. 11, no. 2, pp. 310–325, 2023.
[26] N. Rahman and F. Ahmed, "Deep Q-learning for IDS optimization in MANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 1, pp. 175–191, 2024.
[27] V. Walia and A. K. Verma, "Detection and Prevention of MANET using Hybrid SVM with ANN," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 123–128, 2023.
[28] M. G. Madhu, "Design of Intrusion Detection and Prevention Model Using COOT Optimization and Hybrid LSTM-KNN Classifier for MANET," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 10, no. 3, p. e2, 2022.
[29] Z. A. Abbood, B. T. Yasen, M. R. Ahmed, and A. D. Duru, "Speaker identification model based on deep neural networks," *Iraqi J. Comput. Sci. Math. *, vol. 3, no. 1, pp. 108–114, 2022.