Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2023.035276
Article

Intrusion Detection System Through Deep Learning in Routing MANET Networks

Zainab Ali Abbood[1,2,*], Doğu Çağdaş Atilla[3,4] and Çağatay Aydin[5]

[1]Department Electrical and Computer Engineering, Altinbas University, Istanbul, Turkey
[2]Department Computer Technology Engineering, Al-Esraa University, Baghdad, Iraq
[3]Electric, Autonomous and Unmanned Vehicles Application and Research Centre, Altinbas University, Istanbul, Turkey
[4]Faculty of Engineering and Architecture, Altinbas University, Istanbul, Turkey
[5]Department Electrical and Electronics Engineering, Ege University, Izmir, Turkey
*Corresponding Author: Zainab Ali Abbood. Email: zainab.almamoori@org.altinbas.edu.tr
Received: 15 August 2022; Accepted: 04 November 2022

Abstract: Deep learning (DL) is a subdivision of machine learning (ML) that employs numerous algorithms, each of which provides various explanations of the data it consumes; mobile ad-hoc networks (MANET) are growing in prominence. For reasons including node mobility, due to MANET's potential to provide small-cost solutions for real-world contact challenges, decentralized management, and restricted bandwidth, MANETs are more vulnerable to security threats. When protecting MANETs from attack, encryption and authentication schemes have their limits. However, deep learning (DL) approaches in intrusion detection systems (IDS) can adapt to the changing environment of MANETs and allow a system to make intrusion decisions while learning about its mobility in the environment. IDSs are a secondary defiance system for mobile ad-hoc networks *vs.* attacks since they monitor network traffic and report anything unusual. Recently, many scientists have employed deep neural networks (DNNs) to address intrusion detection concerns. This paper used MANET to recognize complex patterns by focusing on security standards through efficiency determination and identifying malicious nodes, and mitigating network attacks using the three algorithms presented Cascading Back Propagation Neural Network (CBPNN), Feedforward-Neural-Network (FNN), and Cascading-Back-Propagation-Neural-Network (CBPNN) (FFNN). In addition to Convolutional-Neural-Network (CNN), these primary forms of deep neural network (DNN) building designs are widely used to improve the performance of intrusion detection systems (IDS) and the use of IDS in conjunction with machine learning (ML). Furthermore, machine learning (ML) techniques than their statistical and logical methods provide MANET network learning capabilities and encourage adaptation to different environments. Compared with another current model, The proposed model has better average receiving packet (ARP) and end-to-end (E2E) performance. The results have been obtained from CBP, FFNN and CNN 74%, 82% and 85%, respectively, by the time (27, 18, and 17 s).

Keywords: ARP; CBPNN; CNN; DNN; DL; E2E; FFNN; IDS; ML; MANET; security

1 Introduction

The different features of the MANETs network, including its decentralization, accessibility, adaptability, as well as ability to run itself, are both decent and evil [1–5]. While it attracted the attention of industries [6,7] for use in their activities, Fig. 1 shows several kinds of attacks since it is vulnerable. Many academics have proposed a range of safety techniques to distinguish and mitigate a consequence of MANET attacks.

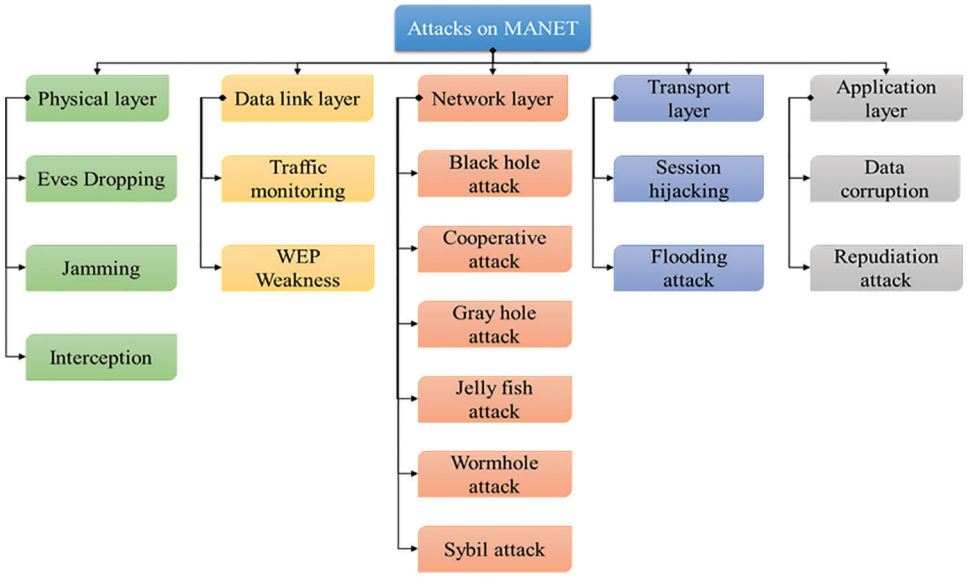

Figure 1: MANET attacks

Cryptographic mechanisms [8–11] offered definite benefits despite introducing a slight delay in communication as well as requiring a connection before keeping data transmission among the nodes, which is unworkable through MANET; therefore, techniques exist needed to enhance security in MANET as the nodes are vulnerable to a variety of attacks at various layers of MANET, Table 1 shown security attacks in different MANET Layers. DoS assaults, eavesdropping attacks, man-in-the-middle attacks, flooding attacks, Sybil attacks, wormhole spoofing attacks, impersonation attacks, black hole attacks, jamming attacks, and grey hole threats are all types of DoS attacks [12,13]. Among others are well-known and prevalent attacks that target certain levels. To some degree, intrusion detection systems, encryption techniques, spread spectrum analysis, and firewalls can identify several types of assaults. Still, the past decade has witnessed a paradigm change from cryptography to novel technologies such as artificial intelligence, machine learning, and genetic algorithms.

The intrusion Detection (IDS) technique [14] refers to a defensive strategy implemented in MANETs to investigate and analyze out-of-the-ordinary occurrences by employing a wide range of methods to spot irregularities or aberrations in behavior or behavior patterns. In general, there are three types of IDS: anomaly detection, misuse detection, and signature-based detection. A system based on anomaly detection can filter out anomalous outlier nodes by comparing them to conventional standard patterns. If an outlier is observed, a node is identified as an intruder. In contrast, abuse and signature-based detection rely only on previously stored signatures or designs. Therefore, they cannot be used to recognize novel attacks or assaults.

Table 1: Security attack in different MANET layers

Layers	Types of attacks	Security problem
Application	Repudiation and data modification.	Detection and prevention of viruses, worms and malicious.
Transport	Session and traffic monitoring and hijacking 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 consumption, location disclosures,	Prevention of MAC disruption through link layer-based security.
Physical	Eavesdropping, message interception.	Prevention of DOS and jamming of signals.

Consequently, anomaly-based detection surpasses the other two previous terms in its ability to deal with novel scenarios, such as those found in MANETs [15]. Which are known for their energy and the vulnerable environment in which nodes can attach and detach ad hoc, making them even more vulnerable to a variety of potential attacks. The primary objective is to identify malicious behavior before actual risk; thus, nodes in MANETs take the ability to filter illicit as well as illegal entries [16,17].

Since nodes are limited in resources such as power, storage, etc., implementing anomaly detection in real-time applications is a formidable barrier. Methods of machine learning assist in the identification of various and unique threats as well as system vulnerabilities. ML approaches may be configured using neural networks, fuzzy logic, genetic algorithms [16], or Bayesian networks [18]. These technologies have become a fantastic option for security analysts and researchers seeking an effective and optimized solution for enhancing security in MANET systems. This work provides a novel approach based on machine learning and a clustering method that can identify, avoid, forecast, and mitigate compromised nodes and safe routes [19].

2 Perspective on ML for IDS in MANET

The IDS's principal function is regularly monitoring network or isolated system traffic for signs of intrusion or other malicious activity. Since MANETs [20–22] use dynamically self-configuring mobile wireless nodes, IDS have protruded as a crucial part of nodes to furnish the network with robust security. Despite MANET's many advantages, such as high degrees of adaptability and scalability and a wide variety of successfully implemented applications, security-related restrictions are inevitably tightened by the networks' built-in weaknesses.

Extremely trustworthy and sturdy security procedures are required to utilize MANET safely and take advantage of its flexible and adaptable features. Avoiding an invasion is an excellent first defense against further attacks, but it cannot guarantee complete safety. Intrusion detection in MANET can be improved using the second line of protection based on classification algorithms that can tell the difference between typical activity and intrusion attempts. Unlike wired networks, in which all communication must pass through devices such as switches, routers, or gateways to implement, MANETs do not use such devices and allow any client to join [23]. Therefore, MANET cannot directly implement wired IDS approaches. Fig. 2. Shown ML for IDS in MANET.

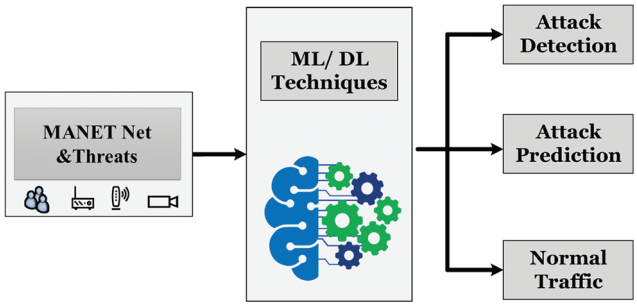

Figure 2: ML for IDS in MANET

2.1 Three Main Categories of (IDS) Applied to MANET[22]

2.1.1 IDS of Stand-Alone

a) The IDS system install on each node that makes up the MANET.
b) A lack of coordination among the individual nodes that make up the network.
c) A local or global reaction is created depending on whether or not there was an intrusion.
d) The IDS agent recognizes and gathers information on intrusions on a local level.
e) Only valuable for simple, single-layer networks; not appropriate for hierarchical or other types of networks.

2.1.2 IDS Hierarchical Structure

a) The network has been broken up into clusters, and intrusion detection systems (IDS) have been set up in the CH.
b) The cluster heads act as a Centre for data gathering and security monitoring.
c) The head of the cluster performs the functions of an IDS agent locally and globally. MANET network designs that are multi-layered and sophisticated can be accommodated.

2.1.3 IDS That Are Both Distributed as Well as Cooperative

a) Each node is equipped with an IDS agent responsible for collecting both local and global replies and working through other nodes in the event of hug detection or a broad seek. In the event of an intrusion, a local or worldwide agent will issue an alert.
b) Neighboring IDS agents will work together to detect a worldwide intrusion if the evidence is inconclusive.
c) IDS agents close to the target network collaborate for international intrusion detection if the evidence acquired is equivocal.
d) This approach is best suited for flat network systems, as it does not apply to multi-layer-based systems.

2.2 Use Machine Learning (ML) to Analyze MANET Data and Categories of ML

The application of machine learning (ML) facilitates improved data visualization for security analysts. The rate of intrusion detection and compliance in MANET are both enhanced by ML techniques. Additionally, it keeps track of recent happenings and compiles information regarding prospective dangers. The following list contains ML Categories [5]:

a) The Algorithms of Supervised Learning: Training takes place in a supervisor's presence and involves training data to arrive at an accurate or desirable conclusion. The supervised learning algorithm analyses the learning data, and an output is produced based on whether the data are discrete or

continuous. Some examples of classifiers include ANN, CBPNN, FFNN, CNN decision trees, Random Forest, linear, and ensemble classifiers.

b) The Algorithms of Unsupervised Learning: Training on data learning based on previous experience rather than predictions does not include goals or calculations based on such forecasts. It concerns the dilemma of unlabeled data stumbling upon a hidden structure in an environment with no precise aim. K-means clustering, hidden Markov models, genetic algorithms, and fuzzy logic algorithms are just a few examples.

c) The Algorithms of Reinforcement Learning: An agent is given the ability to learn in an interactive environment using replies based on trial and error, which are collected from the agent's actions and incidents using this method. A few instances of this include deep learning, SARSA, deep adversarial networks, A3C, and TD.

3 Methodology

The proposed model was implemented using machine learning in conjunction with a distributed intrusion detection system (IDS) and a deep learning model employing CBPNN, FFNN, and CNN algorithms to enhance the precision and performance of IDS in MANET. Due to traffic congestion, collision, and unavailability of a link resulting from exposed and hidden nodes, anomaly detection depends on learning during transmission. This will produce false alerts in the MANET context due to the wrong recognition of familiar as virulent node patterns. CBPNN, FFNN and CNN are implementing machine learning systems, respectively, to avoid the problem described above and manage the dynamic network architecture and mobility of nodes.

3.1 The Following Describes the Operational Methodology of the Proposed Model

a) MANETs are configured with prying nodes; an attacker and a packet dropper line generate erroneous data packets. The data transference is started by the source node, which also begins the procedure for pathfinding.

b) All nodes transmit data through the request forwarding (AODV) and receiving system. Targeted destination nodes generate route replies, and packets are forwarded via intermediate nodes till they reach a source node. The route is discovered, and source and intermediate nodes are responsible for data packet forwarding.

c) Monitoring the nodes with IDS keeps tracking routes and responses and performing physical layer eavesdropping to observe a reception and forwarding count packets of data. The wrong packets are created via the nodes test by calculating the E2E and ARP, initiating the detection procedure with CBPNN, FFNN and CNN algorithms based on DL.

d) The purpose of locating a malicious node is required to comprehend the effect of the attacker-victim link at the packet level. In essence, characteristics were observed: E2E and ARP. These characteristics are essential for any communication link and fluctuate based on any modifications to networks or nodes.

e) AI algorithms learn from data to detect attacks. AI has excelled at prevention. AI attack detection accuracy fluctuates due to attacker node behavior uncertainty. DL is used to recognize attacker node actions at every MANET node. Artificial neural networks (ANNs) can tackle challenging issues by investigating hidden relationships between input strings.

f) Supervised learning is started by providing input r and output T vectors. Changing the weight coefficients between layers reduces error. Error found by correlating resulting and target vectors. Random variable at s^{t0}, as presented in Eqs. (1) and (2). Where R is the output vector and b is model bias, Eq. (3), the net may adjust W coefficients to realize the better correlation between R

and T. Basically, learning is on the most negligible value existing in Eq. (4). *MSE* is training/learning performance statistic. Net is trained to guess the velocity that best recognizes attacker node activity, Eq. (5). for the definition of attack recognition accuracy.

$$R = net\ (r) \tag{1}$$

$$R = W \times r + b \tag{2}$$

$$e = R - T \tag{3}$$

$$MSE = \frac{\sum_{n=1}^{i} e(n)^2}{i} \tag{4}$$

$$Accuracy = \frac{CD}{TD} \times 100\% \tag{5}$$

g) Traffic congestion and malicious behavior can be distinguished using estimated values of link length factor, ARP, RMSE rate, MAE rate, and MSE rate, as well as the forwarding ratios of data and control messages and the dependability between original and fake packets.

h) Suppose a virulent node is revealed based on the trust factor and other input parameters. In that case, it is decided whether the packet must be delivered or a partition must be constructed to bypass the connection. Alterations are made to the connection path and a node drop, including an attack. In this manner, algorithms are implemented in the desired shape by continuously analyzing and predicting nodes depending on decisions. The main parts are shown in Table 2, and Table 3 represents our model's attacker node recognition performance; Fig. 3 shows a flowchart presenting the proposed model.

Table 2: Displays the simulation attributes and corresponding values

Attributes	Values
Number of nodes	50 nodes
Workspace arena	3000 m × 3000 m
Routing protocol	AODV
Transmission range	500 m
Simulation time	60 s
(Connection types) antenna	Omni directional
Transmission type	Cooperative
Packet size	1024 bytes
Bandwidth	4 Mbps
Nodes speed	50 km/h
Channel frequency	2.4 GHz
Mobility type	Random
Traffic sending rate	32 kbps

Table 3: ANN configuration

Particle	Details
hidden layers	2
Technique of training	SL/DL
No. of epochs	100
Max gradience	1 e (−30)
Training performing metric	MSE 1 e (−20)
ANN types (respectively)	CBPNN, FFNN, CNN
Validation data	K-fold cross-validation partition
Number of test sets	10 set

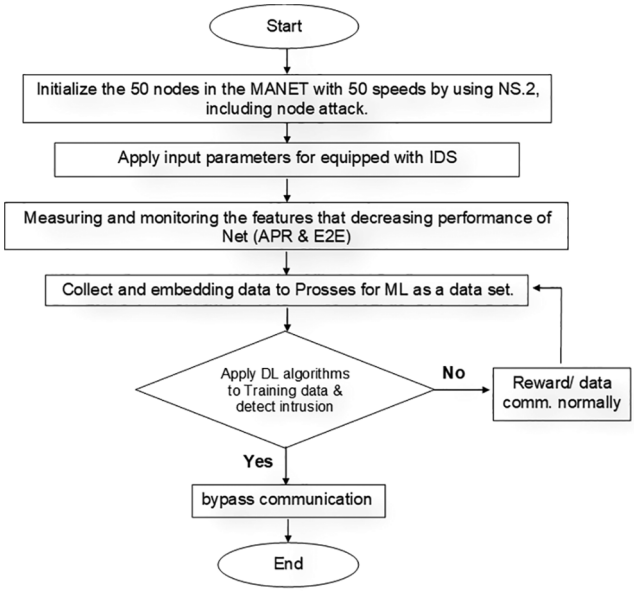

Figure 3: The flowchart describes the proposed model

4 Implementation of Model and Results

The proposed model is simulated using the network simulator (NS2.4). A 3000 m by 3000 m area is created for MANET experiments with support for four malicious nodes' wireless communications with a bandwidth of 4 Mbps. Node mobility is set at a random rate of 60 s, and the transmission range is approximately 500 m. The traffic type is (AODV) and the packet size (is 1024 bytes). The outcomes are calculated via analyzing them with existing detection approaches such as CBPNN, FFNN and CNN to authenticate the performance appraisal of the proposed method.

4.1 Metrics to Evaluate Detection of Malicious Nodes Before and After the Training

4.1.1 Results of Performance Network Under Attack Before the Training

a) End-to-End (E2E): Due to mobility and node coverage limits, victim-attacker connectivity varies across simulation time. Victim-attacker nodes aren't always connected. Also, node speed affects (E2E) Eq. (6). Where E2E: is end-to-end, T_a^{t+1}: time (seconds) of reception acknowledgement and

T_s^t: time (seconds) when the packet is sent. The faster the node speed, the longer and the more immediate nodes might return to the coverage point quicker than slow-moving nodes. Fig. 4 shows how node speed affects (E2E) time. Measured (E2E) under the effect of the attack before training the network, it reaches the lowest rate at 50 km/h speed.

$$E2E = T_a^t - T_s^t \tag{6}$$

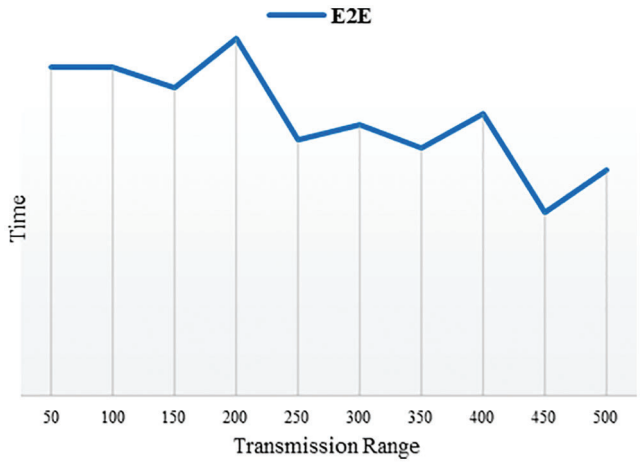

Figure 4: Description of the E2E under the effect of the attack reaches the lowest at 50 km/h speed

b) Average Received Packets (ARP): Packets from the target to the attacker node decrease when nodes move faster, indicating that the packet was unsuccessfully received via a station node, as shown in Fig. 5. And using Eq. (7). Where T_sim: simulation time (seconds) and x: received packet counter.

$$Rx_{mean} = \sum_{0}^{T_{sim}} x \tag{7}$$

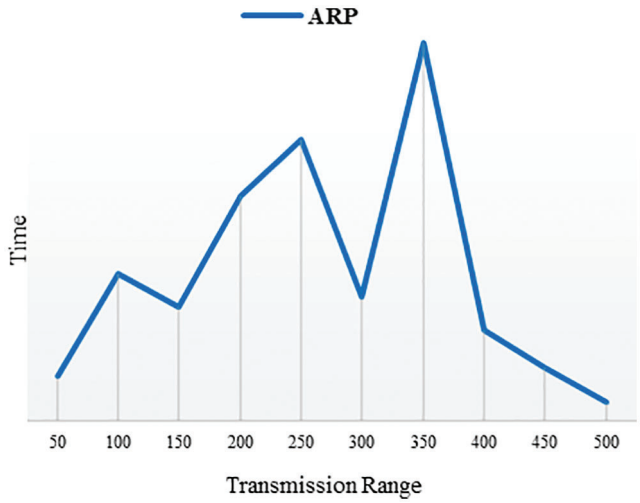

Figure 5: Description of the ARP under the effect of the attack reaches the lowest at 50 km/h

4.1.2 Process and Training Network Data

Data is processed by embedding data in machine learning algorithms with deep learning and then trained the network with a single input layer (500 neurons), two hidden layers (10 sets), and a single output layer. It is not actually "hidden" but just the appellation. The term "hidden" refers to any layer that is neither an input nor an output. In the first layer, all inputs are processed by each perceptron before a judgment is made. The results from these first-layer perceptions are used by the next-layer perceptions to make decisions.

Likewise, the output layer perceptron determines the outcome based on the outputs of the perceptions in the second hidden layer. The algorithms (CBPNN, FFNN, CNN) implemented by the proposed model achieved the algorithms (27, 19, 18 s) from 60 s, with 10-K fold cross-validation used to estimate the algorithms' performance. As shown in Fig. 6, ten values have been determined for each metric. Table 4 displays the results of validating the correctness of the metrics, including the number of observations, MSE, MAE, and RMSE. The CBPNN method produces less precise results, whereas the FFNN system algorithm produces results between CNN's and CBPNN's, while delivering the best result from CNN.

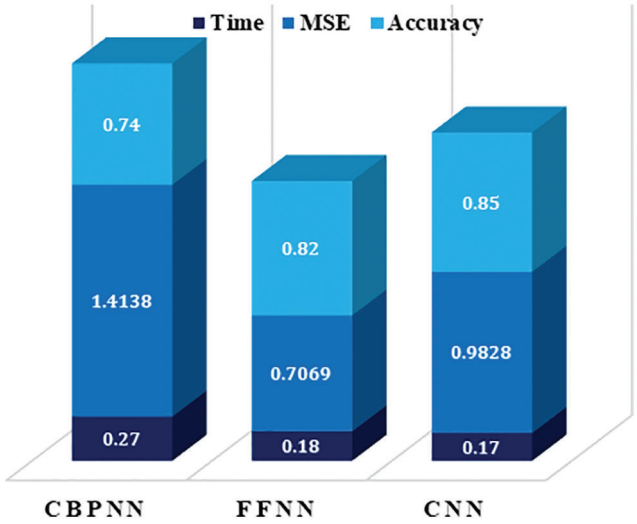

Figure 6: Compared between algorithms, performance based on (time, MSE, and accuracy)

Table 4: The performance of the algorithms depended on the metrics

Nodes	Algorithm	Accuracy	MSE	MAE	RMSE	ARP	E2E	Range	Time
50	CBPNN	74%	1.4138	0.5172	1.1890	Lowest	Lowest	500	27 s
50	FFNN	82%	0.7069	0.3276	0.8408	Good	Good	500	18 s
50	**CNN**	85%	**0.9828**	0.3276	**0.9913**	**Better**	**Better**	500	**17 s**

4.1.3 Results of Performance Network Under Attack After the Training

Fig. 7 depicts the comparison between (ARP and E2E) before and after training the network data into the proposed algorithms. Fig. 8 also illustrates the difference in the precision of the proposed algorithm after training on the data. The CBPNN algorithm displayed a lower level of accuracy, the FFNN algorithm showed a higher level of accuracy, and the CNN algorithm exhibited the highest level of accuracy and the quickest time to detect network intrusions.

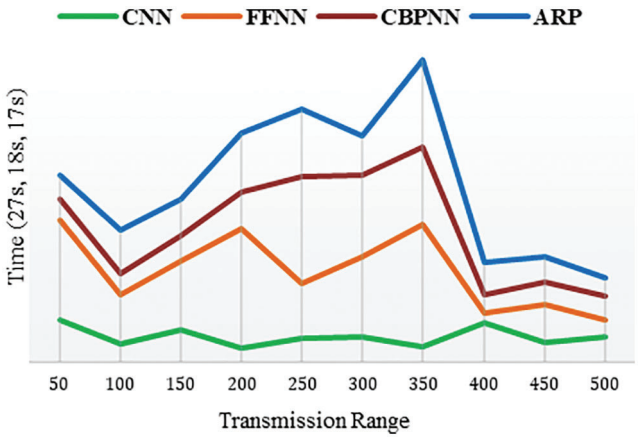

Figure 7: ARP comparison of the paradigm with previous ARP

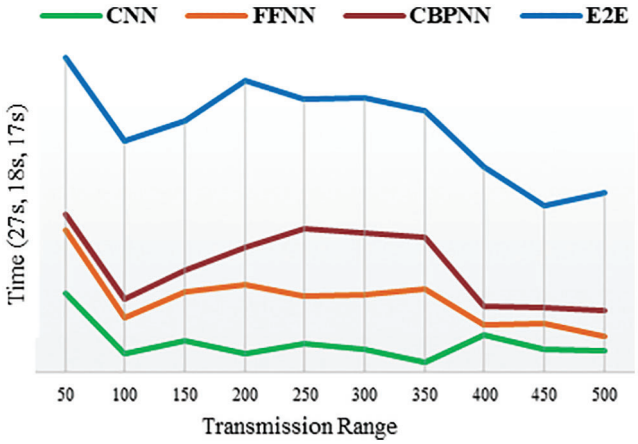

Figure 8: E2E comparison of the paradigm with the previous E2E

5 Discussing Results and Comparing with Traditional Studies

The remarkable technological advancements over the previous decade have enhanced every aspect of living. Additionally, there is the issue of illegal data, necessitating the installation of effective IDSs. The "curse of lower accuracy," however, has been demonstrated through previous studies to cause low detection rates, longer detection times, and lower accuracy when dealing with unbalanced network data. In order to evaluate the proposed model technique, we compare its outcomes to those of machine learning and deep learning. We also analyzed these instruments by analyzing their datasets, IDSs, assaults, algorithm kinds, and levels of precision. Not unexpectedly, CNN's classification accuracy of 85% was significantly higher than that of the original other studies, reaching 82%. See Table 5 for details.

On the other hand, Using ML enables the model to get the best detection and shortest time feasible. We evaluate the proposed model against the DBSCAN Classifier, the Convolutional Neural Network (CNN), and the Bagging (REP-Tree) Classifier, three widely used attribute selection methods. By analyzing the system's accuracy and detection speed, we may conclude how well it performs.

Table 5: Comparing the proposed algorithms with other studies

Authors	Type of data	ML algorithm	Acc %	Type of attack	Type of IDS	Time	Year
Gaikwad et al. [24]	NSL-KDD	Bagging (REP-tree) classifier	81%	R2L	HIDS	43 s	2015
Laqtib et al. [25]	NSL-KDD dataset	CNN	77%	DoS	CIDS	50 s	2019
Jaw et al. [26]	CIC-IDS2017	DBSCAN classifier	82%	Web attack	S-A IDS	78 s	2021
Proposed method*	Create MANET as datasets	CBPNN	74%	DoS	DCIDS	27 s	2022
Proposed method*	Create MANET as datasets	FFNN	82%	DoS	DCIDS	18 s	2022
Proposed method*	Create MANET as datasets	CNN	85%	DoS	DCIDS	17%	2022

As demonstrated in Fig. 9, the accuracy of our suggested model is 85%, which is greater than any of the other techniques evaluated in other studies. For an IDS task, malicious actions are anticipated to be right discovered, and benign actions are qualified not to be misplaced. Accordingly, higher detection accuracy and a faster time are intended in the proposed model.

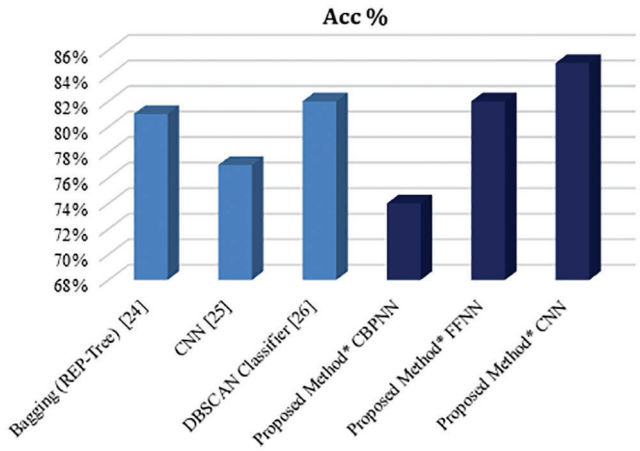

Figure 9: The accuracy of the proposed algorithms with other studies

6 Conclusion

As of late, there has been a lot of talk about using Deep Learning to detect intrusions. To protect highly mobile node networks from a wide variety of innovative assaults, in this paper, IDS with ML will examine the MANET data sample to detection of attacks. IDS that take DL methodology has advantages, including great precision and the ability to recognize or categorize assaults regardless of their surroundings. Consequently, it is essential to apply IDS while considering MANET scenarios strictly. This research delves into the specifics of deep learning-based intrusion detection techniques, which could prove helpful in situationally appropriate approaches in MANETs. Where unrestricted mobility of network nodes raises

major security problems because the paths set up for data transmission are not steady or dependable, which could be problematic for time-critical applications where privacy is paramount. Therefore, by sacrificing the Cooperative, proposing a secure and robust pattern for MANET environments is a significant problem. The suggested model uses machine learning to determine which neighbor node in a MANET is the most trustworthy and reliable for sending and receiving data by a decentralized and cooperative IDS. The fundamental objective of this influence, the selection of a dedicated node for transference, has been accomplished by detecting malicious nodes and their differentiation from ordinary nodes and establishing safe network architecture. In the future, the emphasis of research will shift from the discovery of alternative approaches to the selection of the decision threshold that the elucidation of the procedure for a technique that offers high learning performance, incorporates quality of service-based fundamentals in a more reliable such as reduced memory requirements, and enhanced scalability in large, complex MANET environments.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Alavizadeh, H. Alavizadeh and J. Jang-Jaccard, "Deep Q-learning based reinforcement learning approach for network intrusion detection," *Computers*, vol. 11, no. 3, pp. 1–19, 2022.

[2] S. Singh, D. Prasad, S. Rani, A. Singh, F. S. Alharithi *et al.,* "Wireless body area routing protocols impact analysis on entity mobility models with static sink node," *Applied Sciences*, vol. 12, no. 11, pp. 5655, 2022.

[3] D. M. Khan, T. Aslam, N. Akhtar, S. Qadri and N. A. Khan, "Black hole attack prevention in mobile ad-hoc network (Manet) using ant colony optimization technique," *Information Technology Control*, vol. 49, no. 3, pp. 308–319, 2020.

[4] S. Alampalayam, "Intrusion detection and response model for mobile ad hoc networks," Ph.D. dissertation, University of Louisville, 2007.

[5] Z. A. Abbood, D. Ç. Atilla, Ç. Aydin and M. S. Mahmoud, "A survey on intrusion detection system in ad hoc networks based on machine learning," in *Proc. 2021 Modern Trends in Information and Communication Technology Industry Conf. (MTICTI)*, Sana'a, Yemen, pp. 1–8, 2021.

[6] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with Naïve Bayes feature embedding," *Computer Security*, vol. 103, pp. 102158, 2021.

[7] S. Huang and K. Lei, "IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks," *Ad Hoc Networks*, vol. 105, pp. 102117, 2020.

[8] K. Wrona and P. Mähönen, "Stability and security in wireless cooperative networks," In: *The Wireless Networks, Principles and Applications*, 1st ed., vol. 1. Dordrecht, Netherlands: Springer, pp. 313–363, 2006.

[9] K. K. Karuna Khobragade, "Detection and prevention of blackhole attack in manet," *International Journal of Researches in Biosciences and Agriculture Technology*, vol. 1, no. 7, pp. 34–40, 2019.

[10] S. Kanthimathi and J. R. Prathuri, "Classification of misbehaving nodes in MANETS using machine learning techniques," in *Proc. Ethically Driven Innovation and Technology for Society (PhD EDITS)*, Bangalore, India, pp. 1–2, 2021.

[11] S. Sharma, S. Goswami and G. Thakur, "Intrusion detection using combination of GA based feature selection and random forest machine learning supervised approach," *Mathematical Statistician and Engineering Applications*, vol. 71, no. 3s, pp. 216–232, 2022.

[12] S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing blackhole attacks in MANETs using modified sequence number in AODV routing protocol," in *Proc. 48th Annual Conf. of the Industrial Electronics Society (IECON) 2022 Conf.*, Chiang Mai, Thailand, pp. 1–4, 2020.

[13] K. Thamizhmaran, "Efficient dynamic acknowledgement scheme for manet," *Journal of Advanced Research in Embedded System*, vol. 7, no. 3, pp. 1–6, 2021.

[14] M. Deepa and J. Dhilipan, "Intrusion detection for database security using a hidden Naïve Bayes binary classifier," *Journal of Soft Computing Paradigm*, vol. 4, no. 2, pp. 48–57, 2022.

[15] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020.

[16] Z. Abbood, M. Shuker, Ç. Aydin and D. Ç. Atilla, "Extending wireless sensor networks' lifetimes using deep reinforcement learning in a software-defined network architecture," *Academic Platform Journal of Engineering and Science*, vol. 9, no. 1, pp. 39–46, 2021.

[17] H. Elwahsh, M. Gamal, A. A. Salama and I. M. El-Henawy, "A novel approach for classifying MANETS attacks with a neutrosophic intelligent system based on genetic algorithm," *Security and Communication Networks*, vol. 2018, pp. 1–10, 2018.

[18] A. Chaudhary and G. Shrimal, "Intrusion detection system based on genetic algorithm for detection of distribution denial of service attacks in MANETs," in *Proc. Third Int. Conf. on Sustainable Computing*, Jaipur, India, pp. 370, 2019.

[19] C. Xu, J. Shen, X. Du and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018.

[20] A. Yang, Y. Zhuansun, C. Liu, J. Li and C. Zhang, "Design of intrusion detection system for internet of things based on improved bp neural network," *IEEE Access*, vol. 7, pp. 106043–106052, 2019.

[21] V. Amanoul, A. M. Abdulazeez, D. Q. Zeebare and F. Y. H. Ahmed, "Intrusion detection systems based on machine learning algorithms," in *Proc. 2021 IEEE Int. Conf. on Automatic Control & Intelligent Systems (I2CACIS)*, Malaysian, pp. 282–287, 2021.

[22] N. T. Luong, T. T. Vo and D. Hoang, "FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–17, 2019.

[23] P. Bharathi, M. Lakshmi, C. Madhumitha, J. Nasrinbanu and R. Nivetha, "A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks," *The SIJ Transactions on Computer Networks & Amp.; Commun. Eng.*, vol. 6, no. 2, pp. 01–05, 2018.

[24] D. P. Gaikwad and R. C. Thool, "Intrusion detection system using bagging with partial decision tree base classifier," *Procedia Computer Science*, vol. 49, no. 1, pp. 92–98, 2015.

[25] S. Laqtib, K. El Yassini and M. L. Hasnaoui, "A deep learning methods for intrusion detection systems based machine learning in MANET," in *Proc. 4th Int. Conf. on Smart City Applications (SCA)*, Casablanca Morocco, pp. 1–8, 2019.

[26] E. Jaw and X. Wang, "Feature selection and ensemble-based intrusion detection system: An efficient and comprehensive approach," *Symmetry (Basel)*, vol. 13, no. 10, pp. 1764, 2021.