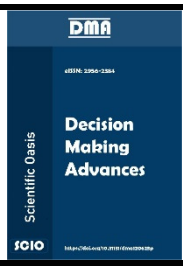
SCIENTIFIC OASIS

Decision Making Advances

Journal homepage: www.dma-journal.org
ISSN: 2956-2384



Deep Learning Models for Intrusion Detection Systems in MANETs: A Comparative Analysis

S. Saravanan[1], Showkat A. Dar[2], Aafaq A. Rather[3], Danish Qayoom[3], Irfan Ali[4,*]

[1] Department of IT, Karpagam College of Engineering, Myleripalayam, Coimbatore, Tamil Nadu, India
[2] Department of Computer Science and Engineering, GITAM University Bangalore Campus, India
[3] Symbiosis Statistical Institute, Symbiosis International (Deemed University), Pune-411004, India
[4] Department of Statistics and Operations Research, Aligarh Muslim University, Aligarh-202002, India

ARTICLE INFO

Article history:
Received 4 June 2024
Received in revised form 7 October 2024
Accepted 29 November 2024
Available online 9 October 2024

Keywords:
Intermediate nodes; Deep learning; Multipath routing data; Networks.

ABSTRACT

MANETs are dynamic, collaborative networks that maintain reliable connections in a self-organized manner. The intermediate nodes aim to forward the data packets between the source and destination nodes. However, most nodes are prone to attack, where intruders tend to attack these nodes and invade the data. With such consideration, the multipath routing in MANETs requires a serious intrusion detection system to detect the attacks in the network. In this paper, we develop a deep learning algorithm named graph neural network (GNN) to detect the possible intrusions of attacks in the nodes. GNN is trained with the possible datasets, and that is tested onto the network. The simulation shows a better resilience to the network against attacks than the other methods.

1. Introduction

A mobile ad hoc network (MANET) describes a group of wireless devices connected for a limited period of communication [1]. These networks do not have a leadership or infrastructure that is centralized anywhere. MANETs have several advantages over networks that do not have a permanent architecture. Some of these advantages include the ability to create an ad hoc network with mobile devices regardless of location, the simplicity with which additional nodes can be added to the network, and the decreased overhead costs associated with managing the network [2, 3].

In recent years, there has been an increase in the development of MANETs. This trend can be attributed to the relatively cheap cost of wireless networking hardware and its flexibility in terms of location and timing [4]. MANET consists of many distinct components, each of which can communicate with the other components through wireless communications. When the two terminals are within range, they can easily exchange data [5].

* *Corresponding author.*
E-mail address: irfii.st@amu.ac.in

https://doi.org/10.31181/dma31202556

It is not tethered to any location; a mobile computing device can move freely throughout the territory covered by wireless links. This makes it possible to cover a more incredible amount of ground. As a result of the reduction in the range of cellular mobile computing devices, it is now possible to construct applications using MANETs. In the past, accomplishing this was impossible. The applications and their capacity to auto-configure themselves are directly responsible for the increase in prevalence that these applications have witnessed. It is now feasible to perform computations of network processes wirelessly [6].

MANETs are in a category of their own regarding the infrastructure of the networks they use. There are now more opportunities for expanding ad hoc networks because of the incorporation of increasingly sophisticated computing and transmission methods [7]. There are no firewalls or other data security measures; ad hoc networks, typically the environments in which these applications are executed, pose a security risk. Even though many software and hardware architectures have been developed specifically for certain objectives, these challenges are still present. These networks are susceptible to various attacks, including those carried out by opportunistic nodes and those carried out by malicious nodes [8].

The wireless network may suffer no ill effects depending on the attack's motivation. A distinguishing characteristic of attacks motivated solely by self-interest is the unwillingness of individual nodes to coordinate their data transmission across the network by working together with one another. It is necessary to retransmit data within the system because the nodes have refused to cooperate [9]. This results in an increase in the quantity of electricity consumed by each node because of the necessity of retransmitting the data.

Malicious attacks suggest any behavior that deviates from the protocol that has been established. Malicious attacks can come in many forms. When it comes to malicious intrusions, the infected node itself is the one acting maliciously and causing harm to other nodes in the network [10].

The challenges lie in developing an intrusion detection system (IDS) and setting up nodes to safeguard the network in real time from all these threats. The high amounts of node movement, interference, and path loss that MANETs experience cause them to have a continuously changing topology. This is one of the distinguishing characteristics of MANETs [11]. Without a dynamic transportation mechanism, they are incapable of functioning appropriately. If there is not a single node in the network that disrupts the efficient operation of the routing protocol and if the nodes are unable to defend against attacks or malicious nodes, then MANET will have successfully implemented many IDS that are dependent on routing protocols.

In this research, we construct an algorithm based on deep learning to determine whether individual nodes are the target of potential attacks. Before the graph neural network (GNN) algorithm can be evaluated on the network, it must first be trained on the network by utilizing the various accessible datasets to be used on the network.

2. Related Works

Since mobile nodes are a network component, malevolent nodes have already established a foothold inside. MANET has become an appealing target for cybercriminals because of the security vulnerabilities that have been discovered. Many studies have been conducted to investigate the viability of implementing MANET intrusion detection systems, with a primary emphasis on utilizing machine learning and deep learning methodologies. This article has only covered a small fraction of those strategies up to this point. There are many more that could be used.

Thirumalairaj and Jeyakarthic [12] introduced a cuckoo search tuning technique designed specifically for deep neural networks (DNN) use. Within this DNN architecture, several auto-encoder

layers are chained together to form an SM classification layer, and the HCSTS technique that is described here is used to fine-tune the settings for those auto-encoder layers. In other words, an SM classification layer is formed by chaining together a few auto-encoder layers. Once the model had been trained, using the challenging dataset to determine the presence of intrusions was possible; this was the area in which the recommended approach performed exceptionally well.

The grasshopper optimization method was used as the foundation for the support vector machine (SVM) that Rao *et al.* [13] developed. This was done to increase the accuracy of the vulnerability scanning that was performed using the SVM. This article presents GOA-SVM and applies SVM to this task. Specifically, the article focuses on improving the accuracy of invasion diagnosis. The findings of the experiments provide conclusive evidence that the innovative approach is superior to the methods that were used previously.

This type of attack, which uses the identities of legitimate nodes as a cover, can potentially find the node trust that creates confusion. An adaptive network-based fuzzy inference system (ANFIS) was developed by Ye *et al.* [14]. The experiments' findings showed that the recommended method made it easier to monitor each node in parallel by reducing the amount of effort required to do so.

The network uses a security protocol that validates performance measures end-to-end, utilizing a key to authenticate its nodes [15]. In addition, the network operates a device that generates symmetric keys. The implementation of a security procedure is what allows this to be possible. A significant amount of time to think about and discuss the various security concerns related to finding a secure routing route that utilizes the least amount of energy to transmit data. Active and passive attacks are the two primary types of risk that MANETs present, and they are known by those respective names. Other kinds of holes have also been involved. Developing defense mechanisms such as these is impossible without a comprehensive understanding of the attacks.

Xu *et al.* [16] developed a policy enforcement model where the destination node was the location where the checks were performed. If the prerequisites for the routing and confidence tiers were met, then information could be transmitted from one node to another. If a server cannot acknowledge these levels, it will not be permitted to join the network. This is because they were designed to make the network safer by ensuring only authorized devices could access the data.

Sadeghi and Yahya [17] examined the consequences of black hole attacks and flooding strikes on AODV. Both types of attacks were described. Some of the measures that were used in the assessment of effectiveness include the ratio of packets delivered, typical delays from end to end, and regularised routing. Other measures included the ratio of packets delivered.

Prakash & Swaroop [18] discussed how the impact of multiple attacks could contribute to high overhead routing and, as a result, poor network performance throughput. Specifically, this was done in the context of a network. They were able to investigate how the synthetic network would perform when subjected to the DSR protocol by increasing the number of black holes in the network. This allowed them to analyze how the network would behave when subjected to the protocol. This allowed them to observe the network's response. The findings indicated that there was a negative correlation between the nodes in the network that had the potential to be categorized as black holes and the efficiency of the network.

The literature review brought to light several errors, one of which is that the network structure of most of the presently available models is overly simplistic and devoid of any significance (Table 1). This was one of the shortcomings brought to light by the study. An additional limitation is that the degree of precision of some already-existing models is inferior to that of other models.

Table 1
Comparison methods of the existing systems

Authors	Methods	Merits	Demerits
Thirumalairaj and Jeyakarthic [12]	Cuckoo search optimization	Reduce hardware expenses and improve time savings	It does not require a high detection rate and minimum false rate
Rao et al. [13]	Bloom filter algorithm	It reduced the probability of false and missed detection	It does not improve the level of security required to protect sensitive data from being accessed by unauthorized parties
Ye *et al.* [14]	Adaptive network-based fuzzy inference system	Identities of legitimate nodes	The potential to find the node trust that creates confusion
Hu *et al.* [15]	Ad-hoc network	Prevents denial of service, a highly efficient symmetric cryptographic primitive	The routing problem in a non-adversarial setting, assuming a trusted environment
Xu et al. [16]	Trusted ad-hoc network	It improves the security analysis	The lack of infrastructure and trusted entities
Sadeghi & Yahya [17]	Proactive routing protocol and reactive routing protocol	It improves the throughput, end-to-end delay, and network load	They are vulnerable and defenseless to different security attacks
Prakash & Swaroop [18]	Zone routing protocol	It increases the detection and avoidance of blackhole attacks in MANETs	MANET is less protected, and, as a consequence, the system has malicious nodes

The findings of this study apply to the field of IDS. This study is more helpful in detecting the attacks. Nowadays, the MANET is a decentralized wireless network. It does not rely on a managed infrastructure access point or a pre-existing infrastructure like routers do in wired networks. The existing techniques have the following drawbacks: high intrusion detection and false detection rates, a lack of infrastructure for trusted entries, a routing problem, unauthorized parties, and certain malevolent nodes with less security. To address these challenges, we create a deep learning technique called GNN to detect potential intrusions of assaults in nodes. Finally, the proposed method outperforms the current packet delivery ratio (PDR) rate and delay approaches. Another implication of this research is that it is helpful for researchers who are doing research in the field of deep learning and IDS. This research provides knowledge of transfer learning in deep learning models. The primary goal of this effort is to create an effective intrusion detection system that detects intrusion signatures in network data in real time. The objectives of this study are summarized as follows:

i. To investigate and evaluate existing network intrusion detection solutions utilizing machine learning algorithms.
ii. To determine the best ways to detect recent threats in IDS.
iii. To use deep learning approaches, as well as create and develop enhanced and new IDS models.
iv. Examine the various intrusion detection systems used in MANETs.
v. To perform real-time intrusion detection to prevent loss to the greatest extent possible.

3. Proposed Method

The architecture of the MANET-IDS was designed to recognize intrusions and halt them before they could cause any damage. The IDS model integrates various components, such as threshold

valves, mobile nodes, a trained data collection system, a packet analyzer, and an attack categorization system.

The capacity of a node in a MANET to move in any direction while still transmitting data results in increased network traffic. This increases the likelihood that an unauthorized user will attempt to disrupt the network. The IDS model shown in Figure 1 provides detection and prevention strategies that can reduce the impact of network attacks. These strategies can be found in the figure.

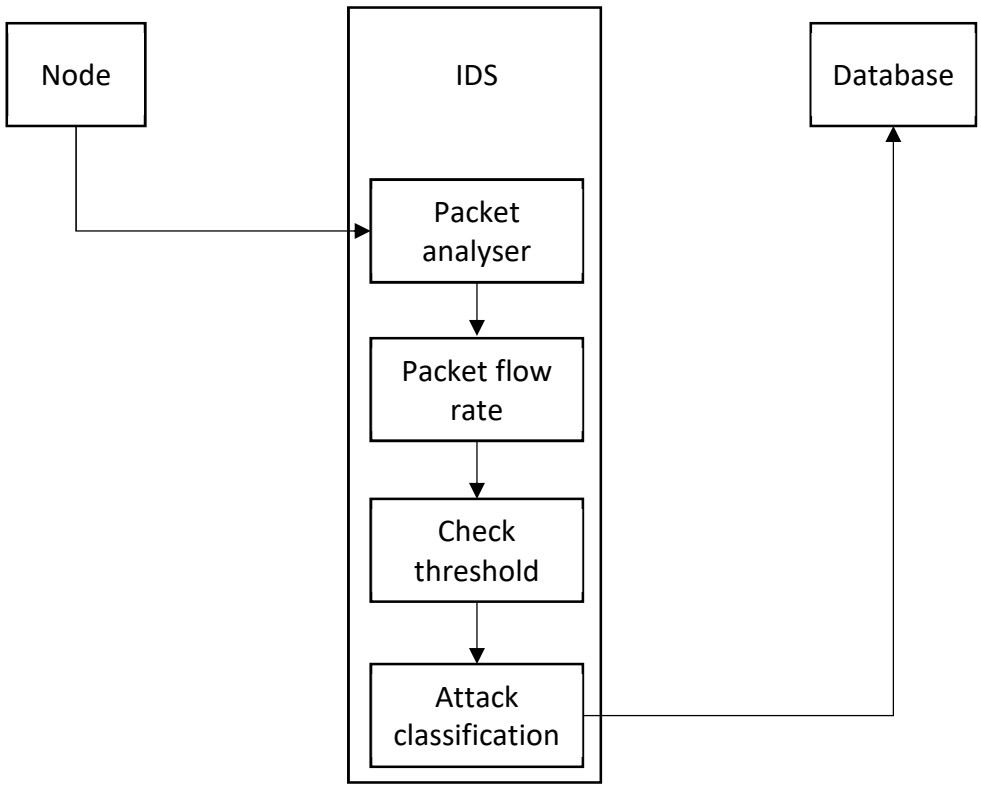


Fig. 1. Proposed framework

The IDS contributions significantly aid the detection and avoidance of prospective hazards in both areas. The packets that are used to make up the monitoring system evaluate the infrastructure of the network based on data such as the time at which the packets arrive, the total number of packets, the height of each packet, and the number of packets that are used to make up each cycle.

The threshold valves are utilized to classify potential attacks on the network, and with the assistance of the trained dataset, the degree of uncertainty associated with the valves is determined. The intrusion prevention engine will trigger an alarm to notify the appropriate parties if an attack is identified.

3.1 Graph Neural Network

Traditional convolutional neural networks (CNNs) are dependent on data that is organized in matrices that are derived from Euclidean geometry. On the other hand, non-Euclidean data structures are significantly more common in the actual world. In such circumstances, the significance of non-Euclidean data structures such as graphs can substantially increase.

A graph can symbolize non-Euclidean data because it comprises a collection of nodes (vertices), edges (links), and node features. The mathematical definition of a graph is represented by the

equation $X : G(V, E, X)$. It comprises these three components: a graph can represent data that does not conform to the Euclidean geometry model.

When two nodes in a network interact, a new edge is generated to describe the nature of the connection between the nodes. This edge is used to characterize the nature of the interaction between the two nodes. Each node and line in the graph can have distinct attributes and associated characteristics.

An adjacency matrix A is a square matrix that illustrates the connectivity between elements, also known as an adjacency matrix. The connectedness of the nodes in question determines whether this matrix is assigned the number 1 (connected) or the number 0 (not linked), respectively. A network can be either undirected or directed; it is also possible to be either weighted or unweighted; it is also possible for a network to be either homogeneous or heterogeneous; and it is also likely to be either stagnant or dynamic.

A graph is said to be undirected when the relationship between any two vertices in the graph is symmetric, such as in the expression $A_{ij} \neq A_{ji}$. On the other hand, we say that a graph is directed when there is an unequal relationship between the vertices in the graph. When the relationship between two nodes is unequal, a graph is said to be directed. Edges in a weighted graph are not limited to simply being 1s and 0s; they can also have numerical values allocated to them. The edges of a weighted graph do not need to consist solely of 1s and 0s; rather, the edges of such a graph can also have numerical numbers associated with them.

However, in a homogeneous graph, each node symbolizes an instance of the same type, and each edge captures a relation between instances of the same kind. This contrasts with the situation in a heterogeneous graph, in which the nodes and edges can each be of a different type. However, in a homogeneous graph, each node symbolizes an instance of the same kind, and each edge captures a relation between instances of the same type. Graphs can be homogeneous or heterogeneous.

The process of handling nodes and edges of various types and the properties associated with each is greatly simplified with a user-friendly graphical user interface provided by a heterogeneous graph. In contrast to static graphs, which do not undergo any modifications to their input characteristics or structure over time, dynamic graphs are those that do. Static graphs do not experience any shifts in their input characteristics or structure. One type of graph is called a multi-graph, and it is distinguished from other kinds of graphs because every node in the graph is connected to every other node in the graph more than once. Figure 2 represents the block diagram of DL for IDS in MANET.

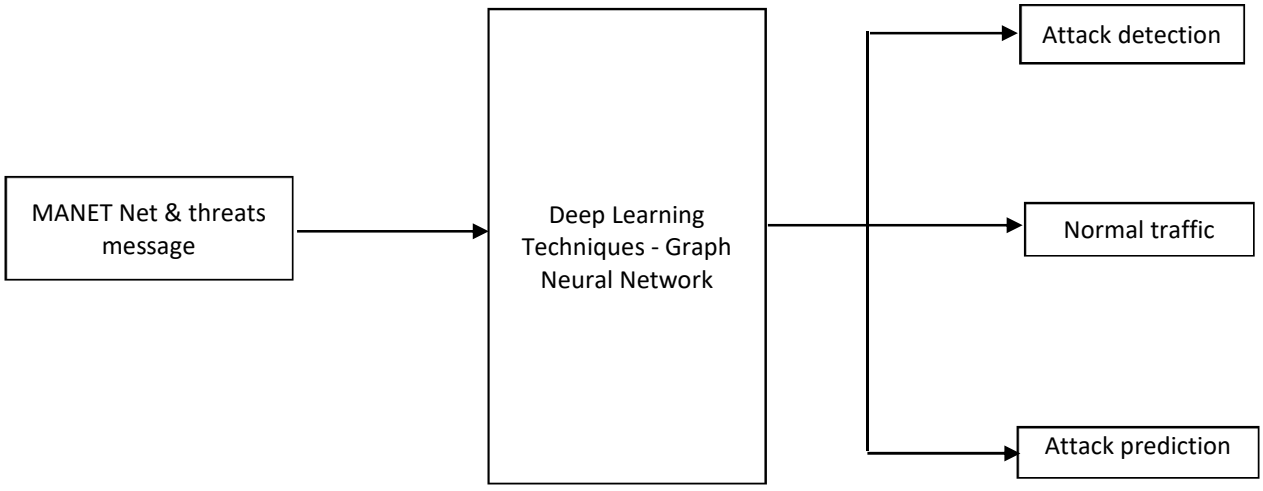


Fig. 2. Block diagram of DL for IDS in MANET

GNNs typically use a message-passing technique, in which nodes update their representations by combining the messages from the representations of their immediate neighbors with their ego representations. This is done by combining the representations of their immediate neighbors. The following is the process that is used to bring about a change to the lth layer of the GNN for each node $v \in V$:

$$m_v(l) = \text{aggregate}(l)\left(\left\{h(l-1)\, u : u \in N(v)\right\}\right), \tag{1}$$

$$h_v(l) = \text{update}(l)\left(h(l-1), m_v(l)\right), \tag{2}$$

where $m_v(l)$ represent a message vector, $h_v(l)$ is a representation vector, v is a node, l is a layer, $\text{aggregate}(.)$ is an aggregation function, and $\text{update}(.)$ is an update function.

The learned node representations at each layer of an L-layer GNN can be described as:

$$H(l) = h_h(l) v_i, \tag{3}$$

where $v = (1, 2, ..., V)$ and $l = (1, 2, ..., L)$. This is based on the presumption that X is the input to the first layer $H(0) = X$. While carrying out a node classification, the final node $H(l)$ is given as input to a classifier. This allows for the generation of class predictions during the process.

3.2 Heterophily/Homophily

There are two ways to determine the heterophily and homophily of a graph: the node homophily and the edge homophily: $G = (V, E)$. One method to measure the homophily (H_{node}) of a collection of nodes is to determine the average percentage of the node neighbors that belong to the same class [19]:

$$H_{node} = \frac{1}{|V|} \sum_{v \in V} \frac{\left|u \in N(v) : y_v = y_u\right|}{N(v)}. \tag{4}$$

The homophily hedge maintains a tally of the number of edges linking locations that share a particular attribute. The range of values between 0 and 1 can be found in the spectra of both the (H_{node}) and the (H_{edge}).

3.3 Non-local Neighbor Extension

The node messages in a neighborhood get aggregated using homophilic graphs, which use the principle of uniform message passing. A neighborhood is typically the set of all neighbors situated one hop away from a node in the graph. Nodes of the same class exhibit significant structural similarity in these networks.

Considering these considerations, modern heterophilic GNNs primarily use two strategies to attempt to move from local to non-local. These strategies are high-order neighbor mixing and potential neighbor discovery. The capability of heterophilic GNNs to symbolize data can be

substantially improved by encapsulating the essential characteristics of nodes in distant but informative locations.

3.4 High-order Neighbor Mixing

Heterophilic GNNs can integrate latent information from neighbors of varying distances, with the node with latent representations from its one-hop and *k*-hop neighbors [20]. There is a formal way to characterize the *k*-hop neighbor set, and it goes as follows:

$$\boldsymbol{N_k(v)=\{u:d(v,u)=k\}.} \tag{5}$$

This can be determined by calculating the shortest distance between any two nodes, indicated by $d(u,v)$.

3.5 Neighbor Discovery

Potential neighbor discovery methods are the neighbors and construct neighbors through heterophily exploration. This is developed compared to neighbor mixing methods that exploit the structural information within graphs. $N_p(v)=\{u:s(v,u)<\tau\}$ is the name given to the new collection of potential neighbors that these methods produce for the node v [21]. The metric function $s(u,v)$ measures the u and v node distance in a latent space and acts as a threshold for limiting the neighbors.

4. Results and Discussions

This section tests the proposed method under a simulation condition, as in Table 2. The proposed method is computed in an NS2 simulation tool that runs on an Intel i7 core processor with 16GB RAM [22]. The proposed method is compared with the existing methods in terms of packet delivery rate and delay rate.

Table 2
Practical simulation parameters

Parameters	Value
Area	750x750m
Movable nodes	75
Transmission range	250 m
MAC layer	IEEE-802.11B
Initial energy	100J
Routing protocol	AODV
Link bandwidth	1.8Mbps
Mobility model	Random waypoint
Traffic model	CBR
Data rate	1024 bytes

The research collected a total of 2000 samples, some of which are safe and some of which could be hazardous (normal 1781 and malicious 119). It will compile the data and assign up to eight variables designated to each record to identify it. This enormous dataset was collected in the context of a completely unstructured ad hoc network to determine whether wormhole attacks had been carried out.

4.1 *Packet Delivery Ratio*

PDR indicates the number of data packets that were dropped during transmission. PDR is an important measure for determining the effectiveness of a network [23]. The number of packets delivered to the constant bit rate (CBR) sink at the destination is the basis for this metric, which calculates the percentage of packet transfers that have occurred [24].

A simulation that considers the inherent routing method of the network can showcase the distinguishing characteristics of the various performance levels. Figures 3-6 displays the outcomes of an investigation conducted to determine the percentage of successfully delivered packets and the end-to-end delay when there were no attacks on the network. These findings are described for a range of node speeds from 0 to 10ms.

When there are no attacks and for various node speeds measured in metres per second, Figure 3 presents a breakdown of the PDR in the absence of an onslaught as a function of the node speed. In a scenario where there are no attacks on the GNN protocol, PDR remains stable. When there are no attacks taking place in a network that includes packets of varying sizes, Figure 3 demonstrates that the GNN protocol PDR functions better than the DSR protocol [25], the AODV protocol [26], and the DSDV protocol [27].

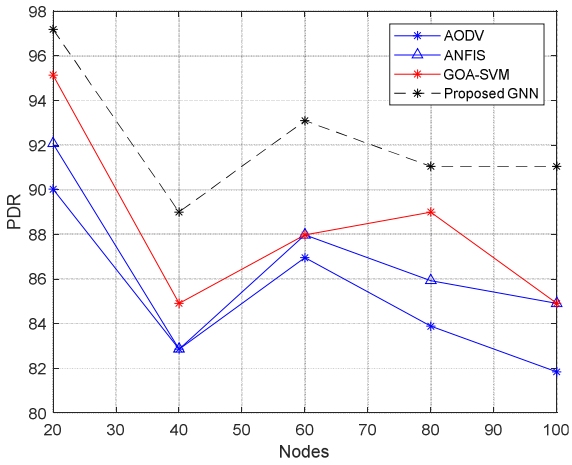


Fig. 3. PDR without attacks (training)

In a scenario where there are attacks on the GNN protocol, PDR decreases (Figure 4).

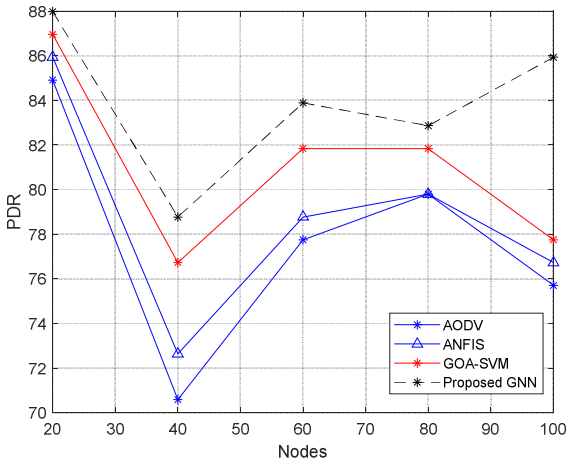


Fig. 4. PDR with attacks (training)

As in Figure 4, the DSR, AODV, and DSDV protocols are all effective at warding off attacks on a network. However, the PDR protocol that GNN developed emerged as the victor in this competition.

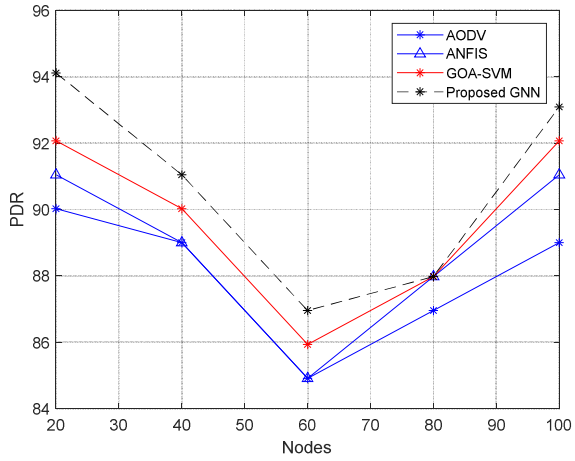


Fig. 5. PDR without attacks (testing)

Compared to PDRs of various other routing algorithms, PDR of the GNN algorithm is significantly higher than those of those other routing algorithms. When PDR for the GNN procedure is investigated both with and without attacks, it is discovered that the latter has a lower value. This is the conclusion reached after comparing the two scenarios.

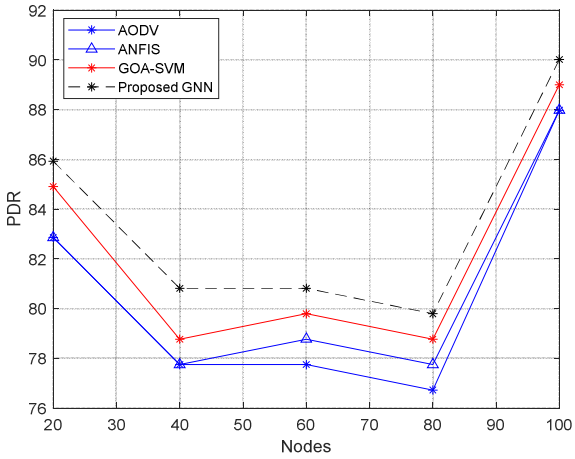


Fig. 6. PDR with attacks (testing)

4.2. End-to-end delay

Delays in communication are measured end to end, meaning they are measured from the beginning of transmission at the source node to the conclusion of packet distribution at the destination node. This is known as the end-to-end method. The end-to-end technique is the name given to this approach. Various factors may have brought on the slowdown, including but not limited to packet buffering, interface data queuing, route finding, network latency, transmission delay, propagation delay, and delay in transmission.

Latency is such an important predictor of the efficiency of a network that it is one of the most important metrics that needs to be monitored. The research investigates the end-to-end delay with and without the presence of attacks and with and without modifying the speed of individual nodes or the size of individual packets.

Figures 7-10 display the results of an investigation into end-to-end delay, which includes a comparison of the performance of individual nodes to the latency. The end-to-end delay that is caused by the GNN protocol will be affected by packet size if there are no attacks on the network, but not nearly as much as you might expect it will be affected by packet size.

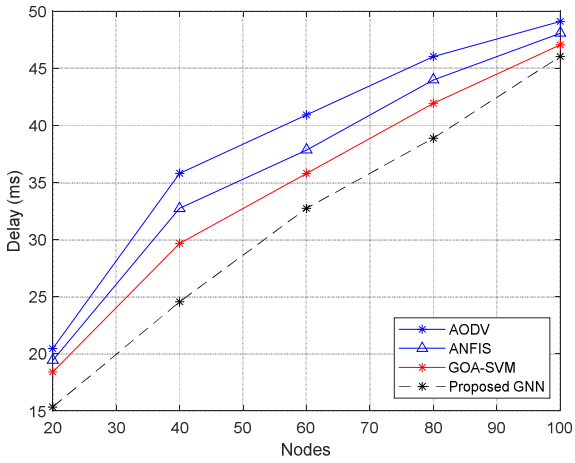


Fig. 7. E2E delay without attacks (training)

The E2E delay grows at a rate proportional to the speed at which the nodes are moving; GNN protocols bring this delay to a number significantly lower than that of any other routing protocol currently being used. Even when attacks are present, the end-to-end latency of the GNN protocol is less than if attacks were not present [28]. This is the case even though the GNN protocol is designed to prevent attacks.

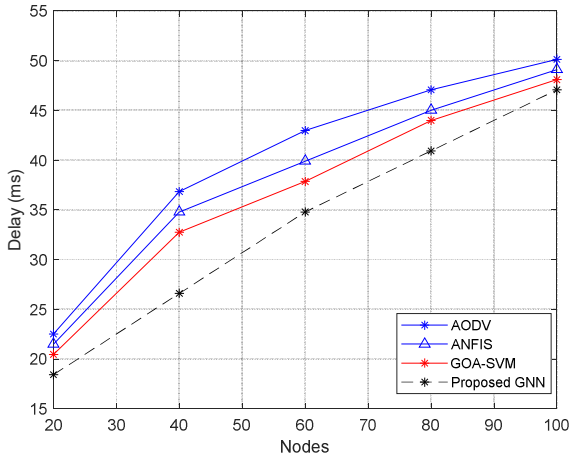


Fig. 8. E2E delay with attacks (training)

The end-to-end delay of the GNN protocol is affected by breaches in a manner that is not as substantial as it would be in the absence of breaches. The results of an investigation into the packet delivery ratio and the end-to-end delay when there are no attacks on the network.

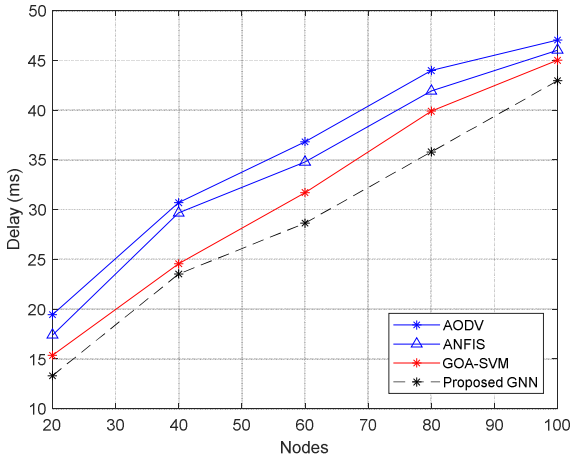


Fig. 9. E2E delay without attacks (testing)

Compared to both established protocols with and without attacks, Figures 6-9 demonstrate that the GNN protocol results in a significant reduction in the amount of end-to-end delay experienced. When the GNN algorithm is implemented, this outcome is achieved. The performance metrics of the GNN protocol are superior and acceptable when compared to those of the existing AODV [29], ANFIS [30], and GOA-SVM [14] protocols in terms of high PDR and low end-to-end delay. This is because the GNN protocol has a higher PDR than the other two protocols.

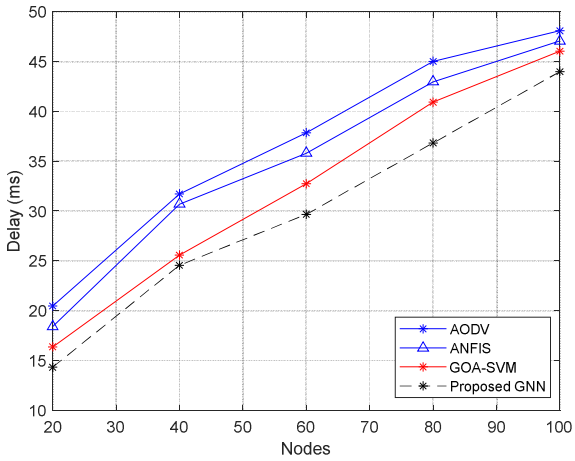


Fig. 10. E2E Delay with attacks (testing)

5. Limitations and Future Enhancement

The proposed research's major limitation is that traditional intrusion detection and prevention techniques such as firewalls, access control mechanisms, and encryption have various limitations in securing networks and systems from ever-more sophisticated attacks such as service denial. Furthermore, most systems based on such techniques have large false positive and false negative detection rates and a lack of ongoing adaptation to changing harmful behavior.

To guard against malicious behavior, secure MANET routing, and deal with the limits of cryptographic systems IDSs, wireless ad-hoc networks have been successfully utilized to detect assaults in MANETs. They can provide an appropriate second line of defense to identify malicious traffic and misbehaving nodes in wireless environments.

Deep learning thus facilitates data summary and visualization, intending to make it easier for safety specialists to identify system flaws and shortcomings. Several deep learning methods have been applied to the problem of intrusion detection to improve detection rates and flexibility. The following concepts can be used to broaden the scope of this research in the future:

i. The design is easily adaptable to various unattended regions and the detection of new MANET assaults.
ii. The presented models can be enhanced by employing a hybridized learning model and lowering the dataset's dimensions using dimensionality approaches.
iii. The presented models can be extended to be used on advanced network platforms such as IoT, vehicular networks, SDN, smart cities applications, etc.
iv. The feature matching and detection algorithms can be enhanced by testing the model with additional mobility models and creating new assault models.
v. The research can be redefined by using additional methods of deep learning based on artificial intelligence and agent-based intelligent systems, such as deep reinforcement learning, deep CNN, GRU, adversarial deep neural networks and so on.

6. Conclusions

In this research, we constructed an algorithm based on deep learning to determine whether individual nodes are the target of potential attacks. Before the deep learning algorithm can be evaluated on the network, it must first be trained on the network by utilizing the various accessible datasets. Data that is put to good use in the model training process can originate from multiple sources, including situations that occur in the real world and evaluations of classifications. It is possible to model the data from the experiments as a function of a target value.

A total of 2000 samples were utilized, each serving as an illustration of both secure and harmful examples, rendering them both benign and malicious. The results showed that the proposed method achieved a higher rate of PDR and reduced delay than the other existing methods.

Conflicts of Interest

The authors declare no potential conflicts of interest in relation to this study.

References

[1] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors, 22*(6), 2087. https://doi.org/10.3390/s22062087.

[2] Quy, V. K., Nam, V. H., Linh, D. M., Ban, N. T., & Han, N. D. (2021). A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. *Wireless Personal Communications, 120*(1), 49-62. https://doi.org/10.1007/s11277-021-08433-z.

[3] Ercan, S., Ayaida, M., & Messai, N. (2021). Misbehavior detection for position falsification attacks in VANETs using machine learning. *IEEE Access, 10*, 1893-1904. https://doi.org/10.1109/ACCESS.2021.3136706.

[4] Sivaram, M., Yuvaraj, D., Mohammed, A. S., Manikandan, V., Porkodi, V., & Yuvaraj, N. (2019). Improved enhanced DBTMA with contention-aware admission control to improve the network performance in MANETS. *CMC-Computers Materials & Continua, 60*(2), 435-454. https://doi.org/10.32604/cmc.2019.06295.

[5] ALRikabi, H. T., & Hazim, H. T. (2022). Secure Chaos of 5G Wireless Communication System Based on IOT Applications. International *Journal of Online & Biomedical Engineering, 18*(12), 89-105. https://doi.org/10.3991/ijoe.v18i12.33817.

[6] Tadic, B., Rohde, M., Randall, D., & Wulf, V. (2023). Design Evolution of a Tool for Privacy and Security Protection for Activists Online: Cyberactivist. *International Journal of Human–Computer Interaction, 39*(1), 249-271. https://doi.org/10.1080/10447318.2022.2041894.

[7] Amponis, G., Lagkas, T., Zevgara, M., Katsikas, G., Xirofotos, T., Moscholios, I., &Sarigiannidis, P. (2022). Drones in B5G/6G networks as flying base stations. *Drones, 6*(2), 39. https://doi.org/10.3390/drones6020039.

[8] Hajiee, M., Fartash, M., & OsatiEraghi, N. (2021). An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique. *Neural Processing Letters, 53*(4), 2829-2852. https://doi.org/10.1007/s11063-021-10525-7.

[9] Yue, K., Zhang, Y., Chen, Y., Li, Y., Zhao, L., Rong, C., & Chen, L. (2021). A survey of decentralizing applications via blockchain: The 5G and beyond perspective. *IEEE Communications Surveys & Tutorials, 23*(4), 2191-2217. https://doi.org/10.1109/COMST.2021.3115797.

[10] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity, 4*, 1-27. https://doi.org/10.1186/s42400-021-00077-7.

[11] Tilwari, V., Maheswar, R., Jayarajan, P., Sundararajan, T. V. P., Hindia, M. N., Dimyati, K., et al. (2020). MCLMR: A multicriteria based multipath routing in the mobile ad hoc networks. *Wireless Personal Communications, 112*, 2461-2483. https://doi.org/10.1007/s11277-020-07159-8.

[12] Thirumalairaj, A., & Jeyakarthic, M. (2020). Hybrid Cuckoo Search Optimization based Tuning Scheme for Deep Neural Network for Intrusion Detection Systems in Cloud Environment. *Journal of Research on the Lepidoptera, 51*(2), 209-224. https://doi.org/10.36872/LEPI/V51I2/301089.

[13] Rao, P. V., Murthy, K. S., Krishnan, V. G., Divya, V., & Sathyamoorthy, K. (2022). Detection Of Sybil Attack In MANET Environment Using ANFIS With Bloom Filter Algorithm. *Indian Journal of Computer Science and Engineering (IJCSE), 13*(1), 82-92. https://doi.org/10.21817/indjcse/2022/v13i1/221301058.

[14] Ye, Z., Sun, Y., Sun, S., Zhan, S., Yu, H., & Yao, Q. (2019). Research on network intrusion detection based on support vector machine optimized with grasshopper optimization algorithm. In *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (IDAACS), pp. 378-383, IEEE. https://doi.org/10.1109/IDAACS.2019.8924234.

[15] Hu, Y. C., Perrig, A., & Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking*, pp. 12-23. https://doi.org/10.1145/570645.570648.

[16] Xu, G., Borcea, C., & Iftode, L. (2010). A policy enforcing mechanism for trusted ad hoc networks. *IEEE Transactions on Dependable and Secure Computing, 8*(3), 321-336. https://doi.org/10.1109/TDSC.2010.11.

[17] Sadeghi, M., & Yahya, S. (2012). Analysis of Wormhole attack on MANETs using different MANET routing protocols. In *2012 Fourth International Conference on Ubiquitous and Future Networks* (ICUFN), pp. 301-305, IEEE. https://doi.org/10.1109/ICUFN.2012.6261716.

[18] Prakash, S., & Swaroop, A. (2016, April). A brief survey of blackhole detection and avoidance for ZRP protocol in MANETs. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 651-654). IEEE.

[19] Qian, C., Zhang, Y., & Ren, S. (2019). Evolution of a self-organizing manufacturing network with homophily and heterophily. *Procedia CIRP, 83*, 800-804. https://doi.org/10.1016/j.procir.2019.04.333.

[20] Abu-El-Haija, S., Perozzi, B., Kapoor, A., Alipourfard, N., Lerman, K., Harutyunyan, H., et al. (2019). Mixhop: Higher-order graph convolutional architectures via sparsified neighborhood mixing. In *International Conference on Machine Learning*, pp. 21-29, PMLR.

[21] Yan, Z., Li, H., Nakazato, H., Park, Y. J., & Lee, J. H. (2019). DNS based Neighbor Discovery in ITS. In *2019 IEEE International Conference on Consumer Electronics* (ICCE), IEEE. https://doi.org/10.1109/ICCE.2019.8662016.

[22] Al-Baz, A., & El-Sayed, A. (2018). A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks. *International Journal of Communication Systems, 31*(1), e3407. https://doi.org/10.1002/dac.3407.

[23] Draz, U., Ali, T., Yasin, S., & Shaf, A. (2018). Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment. In *2018 International Conference on Computing, Mathematics and Engineering Technologies* (iCoMET), pp. 1-7, IEEE. https://doi.org/10.1109/ICOMET.2018.8346385.

[24] Gupta, S. K., Alsamhi, S. H., & Saket, R. K. (2016). Comparative performance analysis of AODV for CBR & VBR traffic under influence of ART & DPC. In *2016 11th International Conference on Industrial and Information Systems* (ICIIS), pp. 112-117, IEEE. https://doi.org/10.1109/ICIINFS.2016.8262917.

[25] Zarzoor, A. R. (2021). Enhancing dynamic source routing (DSR) protocol performance based on link quality metrics. In *2021 International Seminar on Application for Technology of Information and Communication* (iSemantic), pp. 17-21, IEEE. https://doi.org/10.1109/iSemantic52711.2021.9573233.

[26] Jhajj, H., Datla, R., & Wang, N. (2019). Design and implementation of an efficient multipath AODV routing algorithm for MANETs. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference* (CCWC), pp. 527-531, IEEE. https://doi.org/10.1109/CCWC.2019.8666607.

[27] Fengjie, Y., Hui, Y., & Ying, Z. (2018). Research on DSDV routing protocol based on wireless Mesh network. In *2018 Chinese Control and Decision Conference* (CCDC), pp. 4292-4297, IEEE. https://doi.org/10.1109/CCDC.2018.8407870.

[28] Casares-Giner, V., Inés Navas, T., Smith Flórez, D., & Vargas Hernández, T. R. (2019). End to end delay and energy consumption in a two tier cluster hierarchical wireless sensor networks. *Information, 10*(4), 135. https://doi.org/10.3390/info10040135.

[29] Volkov, A. S., Muratchaev, S. S., & Kulpina, Y. A. (2019). Developing simulation model of two-rank MANET Network. *TRUDI MAI, 109*, 13 https://doi.org/10.34759/trd-2019-109-13.

[30] Ali, M., Parwanti, A., & Firdaus, A. A. (2020). Optimization of water level control systems using anfis and fuzzy-pid model. In *2020 Third International Conference on Vocational Education and Electrical Engineering* (ICVEE), IEEE. https://doi.org/10.1109/ICVEE50212.2020.9243229.