Improving Accuracy of Rule Based Collaborative Intrusion Detection System – Security and Performance Trade off in Manet

Radha Narayanan[1], Deepa Venkatraman[2]*

[1]Professor, School of Computer Science and Applications, Reva University, Bangalore
[2]Assistant Professor Department of Information Technology, PSGR Krishnammal College for Women, Coimbatore, Email:deepa@psgrkcw.ac.in
*Corresponding Author

Received: 10.07.2024 Revised: 13.08.2024 Accepted: 11.09.2024

ABSTRACT
The Intrusion Detection System (IDS) is essential for network security, but its complex environment can result in high false detection rates due to the large number of normal samples. To tackle this issue, an Enhanced Generative Adversarial Network with Bidirectional Long Short-Term Memory and Cross-correlated Convolutional Neural Network (EGAN-BiLSTM-CCNN) has been developed in MANET. This model was deployed in Cluster Heads (CHs) for IDS based on the local information of nodes but faces challenges in capturing global information. Integration issues across diverse clusters hinder its ability to detect coordinated attacks. This study introduces a novel Transfer Learning (TL) mechanism coupled with the EGAN-BiLSTM-CCNN model for IDS. The main objective of this model is to utilize both local and global information of the network based on the TL to enhance the performance of collaborative IDS. First, a cluster-based MANET simulation is established to simulate various attacks such as flooding, black holes, gray holes, and forging attacks. Then, network parameters related to these attacks are collected for each node within clusters and transmitted to respective CHs. CHs share local information to attain a global perspective. By leveraging local and global information, a common latent subspace for various attacks and an optimized representation are discovered based on the TL process, thus generating a training dataset. This dataset is used to train the EGAN-BiLSTM-CCNN model deployed within each CH for intrusion detection, achieving a balance between security and performance in MANETs.

Keywords: MANET, Network IDS, EGAN-BiLSTM-CCNN, Network attacks, Transfer learning.

1. INTRODUCTION

MANETs enable mobile nodes to create networks without a fixed infrastructure or centralized control, adapting to specific requirements dynamically. Each node uses its wireless transmitter and receiver to communicate with others within its radio range. If a node requests to forward a packet beyond its radio range, it utilizes multi-hop communication, requiring each node to function as both a host and a router. The network's topology can change significantly as nodes enter, leave, or move within the network. MANETs are now utilized in various applications, including military, civilian, and commercial ones [1]. However, their increasing use has raised security concerns, as most routing protocols assume all nodes are friendly, leaving the network vulnerable to compromise [2]. MANETs are susceptible to both passive and active attacks, such as eavesdropping and packet injection [3]. Various proactive schemes, such as cryptography and authentication, have been implemented [4], but they are not always effective. An IDS can help detect attacks as they enter the network, preventing damage to the system or data [5].

IDS involve monitoring activities in a computer or network system, which collects and analyzes activity information to identify security violations. However, current intrusion detection techniques for wired networks are not suitable for wireless networks like MANETs [6].

Therefore, modifications or new techniques are needed to make intrusion detection effective in MANETs.The use of Artificial Intelligence (AI) in IDS has led to a focus on AI-based detection methods in research [7-9]. Challenges in designing and implementing IDS include handling large-scale, high-dimensional data, imbalanced data, and difficulty in extracting features from network traffic data [10]. To address these issues, a network intrusion detection algorithm [11] was developed using a combination of hybrid sampling and a deep hierarchical network. This approach established a balanced dataset, allowing the model to fully learn minority sample features and significantly reduce training time. Additionally, the

algorithm employed a Convolutional Neural Network (CNN) for spatial feature extraction and BiLSTM for temporal feature extraction, creating a deep hierarchical network model. However, the complexity of network traffic data makes it challenging to extract features. Inaccurate retrieval of features will result in low accuracy. As a result, a new model for network IDS was proposed. First, an EGAN was adopted [12] to increase the minority sample, creating a balanced dataset that allows the network to fully capture the characteristics of minority samples when significantly reducing the learning period. Next, an improved deep correlated hierarchical network was created utilizing the BiLSTM to capture temporal characteristics and the CCNN to capture spatial traits. The softmax was later utilized to categorize intrusion information.

1.1 Problem description

The implementation of EGAN-BiLSTM-CCNN in CHs of MANET clusters is beneficial for detecting and classifying collaborative network attacks locally. This is achieved by collecting node parameters, such as local context information within each cluster, during various types of attacks. However, a significant limitation is that the model's effectiveness in capturing global information across the entire MANET may be compromised. The hierarchical nature of the network implies that the CHs in different clusters act as intermediaries for information exchange. The BiLSTM-CCNN model might face challenges in seamlessly integrating global information from diverse clusters, impacting its ability to detect coordinated attacks that span multiple clusters.

Additionally, the scalability of the proposed model across large and dynamic MANETs raises concerns. The model's performance may degrade when deployed in larger networks, and adapting to dynamic network conditions may pose challenges, potentially leading to increased false positives or negatives. Addressing these limitations will be instrumental in advancing the proposed IDS model's capability to effectively utilize both local and global information within MANET clusters, thereby improving its overall accuracy and adaptability in real-world network environments.

1.2 Major contributions of the paper

Hence, this manuscript develops the TL-EGAN-BiLSTM-CCNN model for IDS in MANETs. The key contributions include:

- First, a cluster-based MANET is established to simulate various types of attacks, including flooding, black hole, gray hole, and forging attacks.
- Next, network parameters related to the different attacks for each node within each cluster are gathered and transmitted to their respective CHs. The local information stored in each CH is then shared with every other CH to obtain a global perspective.
- By leveraging both local and global information, the TL process is utilized to identify a common latent subspace for various attacks, as network attacks exhibit similar characteristics, and aids in developing an optimized representation that is invariant to changes in attack behaviors. As a result, a training dataset is generated.
- The EGAN-BiLSTM-CCNN model within each CH is deployed using the obtained training dataset to detect and classify network intrusions.
- By leveraging both local and global information of the network, a balance between security and performance in MANETs is achieved. This equilibrium ensures that security measures do not excessively compromise the network's performance, and vice versa.
- Finally, extensive simulations demonstrate that the TL-EGAN-BiLSTM-CCNN yields superior network performance compared to existing IDSs.

1.3 Outline of the paper

The following manuscript is structured as follows: Section 2 covers the related works. Section 3 discusses the TL-EGAN-BiLSTM-CCNN. Section 4 presents the experimental outcomes. Section 5 concludes the study.

1.4 Literature survey

Several relevant works in the field of IDSs based on the AI approaches are listed below:

In [13], a Double-Layered Hybrid Approach (DLHA) was presented for IDS using a hybrid naive Bayes and Support Vector Machine (SVM). First, general features of various attacks were extracted by Principal Component Analysis (PCA). Then, the naive Bayes was used to identify DoS and Probe attacks, while the SVM was used to separate R2L and U2R from regular cases. However, the accuracy was not effective for detecting unknown collaborative attacks.In [14], a tree-based stacking model was introduced for IDS that takes into account the ranking of features based on their scores and uses these features to build a stacking

model. However, the model primarily focused on intrusion detection as a binary classification problem, leading to low accuracy in classifying collaborative attacks. In [15], a hybrid deep learning framework was presented by combining CNN and LSTM for IDS. However, the detection accuracy was impacted by the data imbalance problem.

In [16], a new IDS was introduced, which integrates Q-learning with a deep Feed-Forward Neural Network (FFNN) to detect network intrusions. However, the accuracy of the model was still very low. In [17], a Deep Learning-based Network IDS (DLNIDS) was developed that incorporates an attention strategy and BiLSTM. The system initially extracts sequence features of data traffic using CNN and reallocates the weights of all channels utilizing the attention strategy. The BiLSTM was then employed to learn these features for intrusion detection. To address data imbalance, Adaptive Synthetic Sampling (ADASYN) was used to increase the minority class samples, and an adapted stacked autoencoder was used for reducing data dimensions. But the accuracy was low and it was unable to detect collaborative attacks.

In [18], a hybrid Recurrent Neural Network (RNN) and correlation-based feature optimization were introduced for IDS. Initially, data pre-processing was employed to remove data redundancy and select the most suitable feature set. Subsequently, the chosen features were classified by the hybrid RNN, including LSTM and Gated Recurrent Unit (GRU), to distinguish between benign activity and various network attacks. However, the recalland precision were ineffective in classifying collaborative attacks.

In [19], a new and reliable ensemble machine-learning framework was developed for detecting network intrusions. This model includes a pre-processing based on the SMOTE, regularization, and tag encoding. XGBoost was then used to select the best features, which were then input into various classifiers for detecting network intrusions. On the other hand, the accuracy was low since it did not learn the relationship among different features.

In [20], a Whale Optimization Algorithm (WOA)-based Deep Neural Network (DNN) was developed to optimize the dataset and categorize intrusions in MANET. But the accuracy was low because of inadequate features. In [21], an IDS was developed using the FFNN, Cascading Back Propagation Neural Network (CBPNN), and Convolutional Neural Network (CNN) for MANET to identify complex patterns and malicious nodes. On the other hand, the precision was ineffective due to the lack of global features.

In [22], a new deep learning-based IDS was presented for IoT devices. A four-layer deep fully connected network structure was used to identify malicious traffic that could potentially launch attacks on connected IoT devices. However, the accuracy was less for detecting collaborative attacks sinceit includes only specific types of attacks. In [23], a hierarchical LSTM-based IDS was developed to effectively manage an entire packet and classify network intrusions. However, they found that the classification accuracy decreased as the volume of traffic to be processed increased.

1.5 Research gap

Despite advancements in IDS for MANETs, there is a research gap in incorporating both local and global information of MANET nodes for enhanced intrusion detection capabilities. Existing works focus on developing IDS models using deep learning techniques for MANETs to identify complex patterns and malicious nodes, but often lack comprehensive consideration of both local and global context information. Local information is crucial for identifying node-specific anomalies and attacks, while global information provides a broader context for detecting coordinated attacks and anomalies at the network level. The research community has not extensively explored IDS models that effectively integrate both local and global information, limiting the ability to detect sophisticated attacks involving collaboration among multiple nodes. Addressing this research gap is essential for developing more robust and adaptive IDS solutions capable of providing a holistic view of the MANET environment, improving detection accuracy and responsiveness to emerging threats in dynamic and resource-constrained network settings.

2. METHODS

This section explains the TL-EGAN-BiLSTM-CCNN. A detailed pipeline of this study is illustrated in Fig. 1.

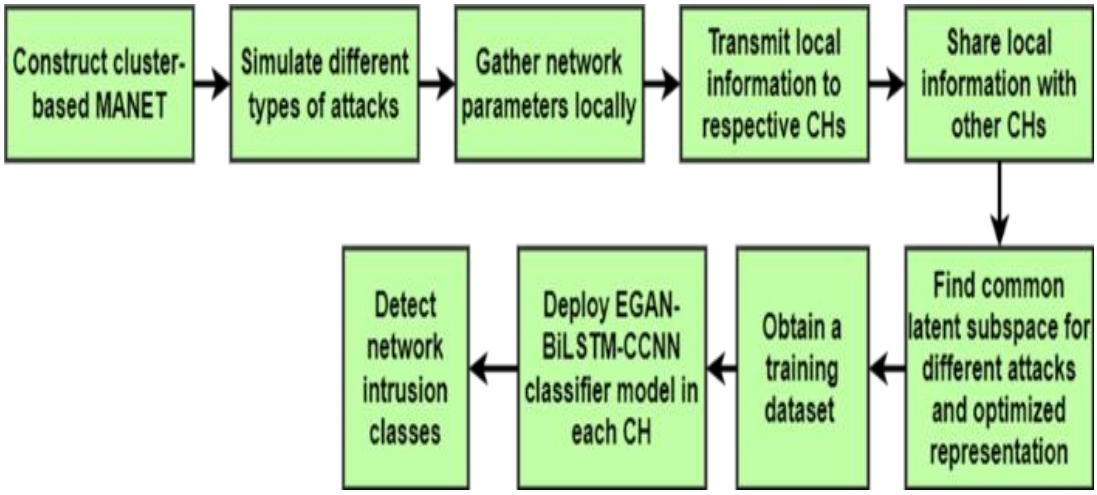

Figure 1. Pipeline of the proposed study

Figure 2. Threat model for MANET in this study

2.1 Threat model

The threat model for MANETs identifies the potential security risks and vulnerabilities that arise from the dynamic and self-organizing nature of these networks. This study examines four different types of network attacks, as shown in Fig. 2.

1. Flooding attack: This is a malicious activity in which an adversary floods the network with an excessive volume of packets or requests. The main goal of this attack is to overwhelm the target network's resources, causing disruption and degradation of service. This study focuses on the Route Request (RREQ) flooding attack, in which an intruder node continuously floods the RREQs for non-existent node IDs. Regular nodes unwittingly forward these RREQs in an attempt to discover a route to malicious nodes.
2. Black hole attack: This is a malicious activity, in which a node selectively drops or absorbs data packets, creating a "black hole" in the network. In this type of attack, a compromised or malicious node falsely advertises itself as having the shortest route to the destination, luring traffic towards it. However, instead of forwarding the received packets, the malicious node intentionally drops them, leading to data loss and communication disruptions. Black hole attacks take advantage of the dynamic and decentralized nature of MANETs, where nodes work together to relay information without depending on a fixed infrastructure.
3. Gray hole attack: This is a form of malicious activity in which a compromised node selectively drops or modifies certain data packets while allowing others to pass through. Unlike a black hole attack, where all packets are dropped, a gray hole attacker exhibits more sophisticated behavior by manipulating or dropping some packets while allowing others to pass through. This selective forwarding makes gray hole attacks more difficult to detect than straightforward packet dropping attacks.
4. Forging (spoofing) attack: It is a type of cyberattack where an adversary attempts to deceive a system or network by using falsified information to gain unauthorized access or manipulate the system's

behavior. This study focuses on identity spoofing attacks, in which attackers forge the identity of a legitimate node to gain unauthorized access to the network.

2.2 Gathering local and global information

In MANETs, gathering information involves collecting data at the individual node level (local information) and aggregating relevant features at the cluster level (global information). Nodes within a cluster exchange information locally, and CHs exchange summarized data with neighboring CHs to maintain a balance between local and global perspectives.

- Local information: Each node in the MANET collects and maintains local information related to its own state, behavior, and communication patterns. Local information (x_i) for node i in any cluster can include features such as node ID, energy level, connectivity status, traffic load, and other relevant parameters (e.g., bandwidth, hop count, round trip time, amount of packets dropped, amount of packets received, and total number of packets in transmission). Nodes transmit this information to their corresponding CHs.
- Global information: CHs aggregate local information from their member nodes to create a global view of the cluster. This aggregated data may include average energy levels, traffic patterns, or summaries of local intrusion detection results. CHs communicate with each other to exchange summarized global information, enabling a network-wide perspective and coordinated responses to network events.

The IDS continually updates local and global information as network conditions change. This dynamic updating ensures that the IDS can adapt to evolving security threats and network dynamics.

2.3 Transfer learning strategy for generating optimized representation

This study models the IDS as a multi-label classification dilemma, which is to categorize all network data as normal and different types of attacks. Consider the local information examples $X_l = \{x_i\}$, where $x_i \in \mathbb{R}^m$ represents the local features of nodes in the MANET, and $LS = \{y_i\}$ denotes the corresponding labels.

Additionally, consider a global information $X_g = \{u_i\}$, where $u_i \in \mathbb{R}^n$ are network-wide features in the MANET, and the associated labels are denoted by $GS = \{z_i\}$. The local and global information are learned from various distributions, $P(X_l) \neq P(X_g)$, where $P(X_g)$ is indefinite and the sizes of x_i and u_i are varied ($m \neq n$). The objective is precisely estimate the tags Z (attack types) on the global information X_g based on the local information X_l in the MANET for IDS.

The TL strategy identifies common traits in network attacks and uses them to find a common latent subspace. It then maps local and global information to create new feature representations that can be used for classification. The model utilizes both local and global information from various attacks to explore a common latent space. This space preserves the original data structure while ensuring that discriminative examples remain far apart.

2.3.1 Optimization

For local information data X_l and global information data X_g, the objective is to find the optimal subspaces V_l and V_g. The optimization objective is given in Eq. (1):

$$\min_{V_l,V_g} f(V_l, X_l) + f(V_g, X_g) + \beta D(V_l, V_g) \quad (1)$$

In Eq. (1), $f(V_l, X_l)$ denotes a bias function that estimates the variance between the actual local information and its projection onto V_l, $f(V_g, X_g)$ denotes a distortion function that evaluates the difference between the actual global information and its projection onto V_g, $D(V_l, V_g)$ is the difference between the projected data of the local and global information, and β is the tradeoff variable that regulates the similarity between both local and global information. So, the first two elements of Eq. (1) guarantee that the projected data preserve the actual data patterns as much as possible.The $D(V_l, V_g)$ is defined in terms of $f(*,*)$ in Eq. (2):

$$D(V_l, V_g) = \|V_l - V_g\|^2 \quad (2)$$

A linear transformation is applied to find the projected space. The $f(*,*)$ is defined by Eq. (3).

$$f(V_l, X_l) = \|X_l - V_l P_l\|^2;\ f(V_g, X_g) = \|X_g - V_g P_g\|^2 \quad (3)$$

Here, V_l and V_g are attained by a linear conversions with linear mapping matrices, represented by $P_l \in \mathbb{R}^{k\times m}$ and $P_g \in \mathbb{R}^{k\times n}$ to the local and global information, correspondingly. $\|X\|^2$ defines the Frobenius norm. Alternatively, $P_l^{X_g} \in \mathbb{R}^{m\times k}$ and $P_g^{X_g} \in \mathbb{R}^{n\times k}$ project the local information X_l and X_g into a k-dimensional latent subspace, where the estimated information is analogous (i.e., $f(V_l, X_l) = \left\|X_l P_l^{X_g} - V_l\right\|^2$). This results in a trivial solution $P_l = 0, V_l = 0$. Therefore, Eq. (3) is applied. It is observed as a

matrix factorization dilemma, commonly known as a powerful technique to capture latent subspaces when maintaining the actual data patterns.

Substituting Eq. (3) and Eq. (2) into Eq. (1), the following objective Eq. (4) is obtained:

$$\min G(V_l, V_g, P_l, P_g) = \min \left(\|X_l - V_l P_l\|^2 + \|X_g - V_g P_g\|^2 + \beta \|V_l - V_g\|^2 \right) \quad (4)$$

A gradient approach is utilized to obtain the global minimum by iteratively setting 3 of the matrices and solving the residual until convergence.

2.3.2 Clustering-based transfer learning

It relies on the configuration of a hyperparameter, specifically the significance of the local and global information (β). Inappropriate selection of parameters could result in less effective outcomes. The rank of the class for X_l and X_g might impact the outcomes of $D(V_l, V_g)$. In reality, our knowledge of the new attack in X_g may be limited, therefore the conversion procedure in (4) can be ambiguous.

To solve this issue, the clustering-based TL is introduced that automatically determines the significance of the local and global information before applying the projection. Initially, the instances for the global information data, considering that the local information already exhibits five natural clusters (classes: normal, flooding attack, black hole attack, gray hole attack, and forging attack). The similarity of each cluster is computed, and a mapping is established for each cluster in the global information to the local information. Instances are sorted according to their cluster labels, ensuring that the rows in matrices representing the global (X_g) and local (X_l) information shared an identical class rank. Subsequently, objective (4) is solved for the ranked X_g and X_l information.

Fig. 3 illustrates the clustering-based TL process, with the entire process detailed in Algorithm 1. K-means is selected for clustering and the Euclidean distance is utilized for similarity calculation.

Algorithm 1: Clustering-based TL

Input: Local (X_l) and global (X_g) information

Output: Optimal latent subspace and representations

1. **Initialize**c clusters for X_l and X_g, $c = 5$;
2. $C_{X_g} = \text{kmeans}(X_g, c)$; $//C_{X_g}$: the cluster tag for all instances in X_g
3. $C_{X_l} = Y_{X_l}$; $//C_{X_l}$: the cluster tag for all instances in X_l, Y_{X_l}: the class tag for X_l
4. **if**(the dimensions of $X_g \neq X_l$)
5. $X_g = \text{pca}(X_g)$; $X_l = \text{pca}(X_l)$;
6. Calculate the Euclidean distance between centers of all clusters in X_g and X_l;
7. **for**(each cluster in X_g)
8. Select an analogous cluster from C_{X_l}, which has the minimum Euclidean distance to create a comparable cluster pair, and allocate a similar tag to all comparable pairs of clusters;
9. **end for**
10. Sort the matrices $[X_g, C_{X_g}]$ and $[X_l, C_{X_l}]$ in the order of C_{X_g} and C_{X_l}, to obtain the updated global and local information, respectively;
11. **end if**
12. **Return** the optimal latent subspace

This algorithm has a time complexity of $O(N^2)$ and a space complexity of $O(N)$, where N is the number of data instances in the given datasets.

2.4 Training EGAN-BiLSTM-CNN model for IDS

After creating the new training dataset with optimized representations, the EGAN-BiLSTM-CCNN model is implemented in each CH. The training dataset, which is derived from the optimized latent subspace using the clustering-based TL mechanism, is used as input for training the EGAN-BiLSTM-CCNN model.

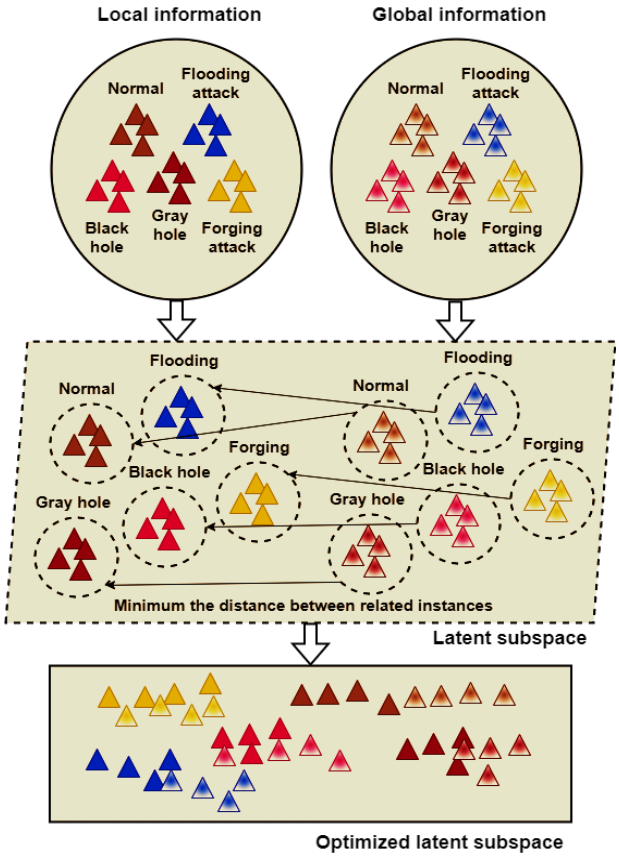

Figure 3. Clustering-based TL process

This model learns to differentiate between normal network behavior and various types of network attacks by utilizing the optimized latent representations. Once trained, the EGAN-BiLSTM-CCNN model can detect intrusions within each CH based on the learned features and patterns from training. CHs communicate and share relevant information, contributing to a collaborative IDS. Information exchange among CHs allows for a network-wide perspective and improves the detection of collaborative attacks across multiple clusters.

Therefore, the IDS in MANETs strike a balance between security and network performance by detecting various network attacks using the EGAN-BiLSTM-CCNN model within each CH and leveraging the optimized latent space for training.

3. RESULTS AND DISCUSSION

This section assesses the efficiency of the TL-EGAN-BiLSTM-CCNN model and compares it with existing IDS models, including EGAN-BiLSTM-CCNN [12], CNN-LSTM [15], hybrid RNN [18], and CNN [21]. The threat models are simulated in Network Simulator (NS2.35) to create a dataset for Python, which supports the IDS. The simulations are carried out on a system with an Intel ® Core TM i5-4210 CPU @ 2.80 GHz platform. Table 1 presents the parameters and their values utilized for simulating both existing and proposed IDS models to measure performance.

Nodes are randomly selected to send and receive data. The path for data transmission is determined based on the minimum distance between nodes. After forming the network and calculating the clusters, CHs, and nodes trust each other. The value function of CHs and members is then calculated.

Malicious nodes are also placed within the clusters. To simulate a flooding attack, malicious nodes transmit forged RREQ packets every 100ms, attacking multiple paths within the network layer. A selective packet-dropping attack is also simulated, in which malicious nodes drop every RERR packet, causing authentic nodes to transfer packets over failed paths. Feature vectors are selected after simulating these attacks, which will be used in classification to signify system activity and differentiate between typical and atypical activities. Training datasets for all sampling periods (5, 10, 15, 30 s) are generated by running simulations with UDP, nodes speed of 10m/s, and different quantities of malevolent nodes (5, 15, 25) for different network mobility. The sender and receiver nodes are chosen randomly and the path between them is calculated.

Table 1. Simulation parameters

Parameters	Value
Simulation tool	NS2.35
Simulation region	1000×1000 m^2
No. of nodes	200
Attack types	RREQ flooding, black hole, gray hole, and identity spoofing
Transmission range	1000 m
Routing protocol	Adhoc On-demand Distance Vector (AODV)
Traffic model	Constant Bit Rate (CBR)
Mobility type	Random waypoint
Antenna type	Omni directional
Channel type	Wireless
Transport layer protocol	UDP
Node speed	10 m/s
Simulation time	100 sec

The derived datasets include both local and global information like bandwidth, remaining energy, traffic, hop count, round trip time, amount of packets dropped, amount of packets received, and total number of packets in communication. These parameters are collected from each simulation and grouped into a training dataset for each sampler intermission. The same procedure is followed for creating test datasets. These datasets are then used in the TL-EGAN-BiLSTM-CCNN and other IDS models to find malicious nodes in the network.

3.1 Performance evaluation measures

1. Accuracy: It is the ratio of correctly recognized instances to the entire dataset, and calculated by Eq. (5).

$$\text{Accuracy} = \frac{\text{True Positive (TP)}+\text{True Negative (TN)}}{\text{TP}+\text{TN}+\text{False Positive (FP)}+\text{False Negative (FN)}} \quad (5)$$

In Eq. (5), TP measures the total attack instances properly categorized as an intrusion, TN refers to the total normal instances correctly categorized as normal, FP measures the total normal instances improperly categorized as an intrusion, and FN measures the total attack instances incorrectly categorized as normal.

2. Precision: It is calculated by Eq. (6).

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \quad (6)$$

3. Recall: It is calculated by Eq. (7).

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (7)$$

4. F-score: It is computed by Eq. (8).

$$\text{F}-\text{score} = \frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \quad (8)$$

Fig. 4 presents a comparison of different IDS models during training. It can be observed that the accuracy of TL-EGAN-BiLSTM-CCNN is significantly higher than the CNN, CNN-LSTM, hybrid RNN, and EGAN-BiLSTM-CCNN, with increases of 15.2%, 10.8%, 6.4%, and 2.7% respectively. Similarly, the precision, recall, and f-score of TL-EGAN-BiLSTM-CCNN are also notably higher compared to the other models. This performance improvement is attributed to the model's ability to consider both local and global information of network properties for detecting various types of intrusions in MANETs. TL-EGAN-BiLSTM-CCNN appears to leverage these combined features more effectively than other models.

Fig. 5 illustrates a comparison of different IDS models during testing. The accuracy of TL-EGAN-BiLSTM-CCNN has improved by 13.4%, 10.4%, 6.1%, and 2.7% compared to the CNN, CNN-LSTM, hybrid RNN, and EGAN-BiLSTM-CCNN, respectively. The precision has also increased by 13.8%, 11.3%, 5.8%, and 2.7% compared to the CNN, CNN-LSTM, hybrid RNN, and EGAN-BiLSTM-CCNN, respectively. Additionally, the recall is 13.4%, 10.9%, 6%, and 2.7% higher than the CNN, CNN-LSTM, hybrid RNN, and EGAN-BiLSTM-CCNN, respectively. Furthermore, the f-score has increased by 13.6%, 11.1%, 5.9%, and 2.7% compared to the CNN, CNN-LSTM, hybrid RNN, and EGAN-BiLSTM-CCNN, respectively. These improvements are achieved by considering both local and global information on network properties for detecting various types of intrusions in MANETs.

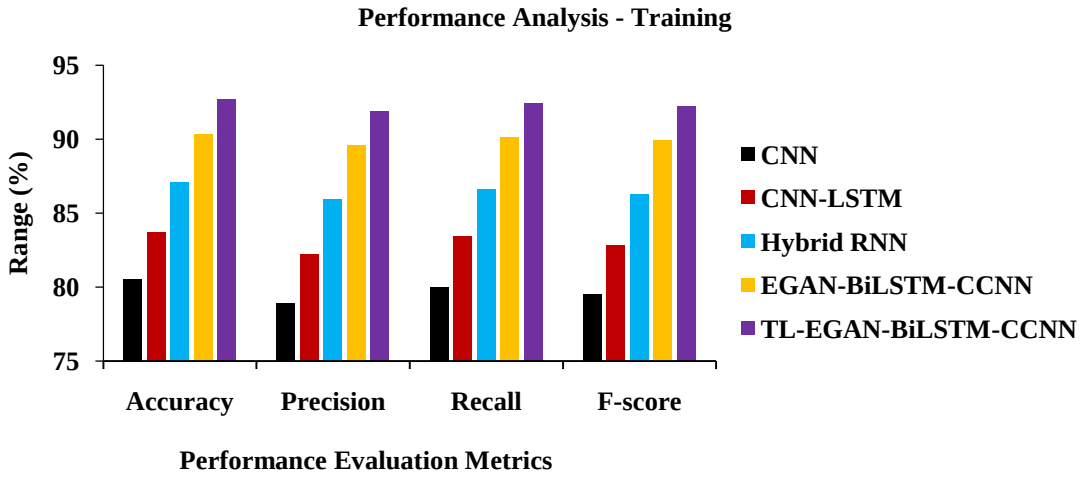

Figure 4. Performance of different IDS models during training

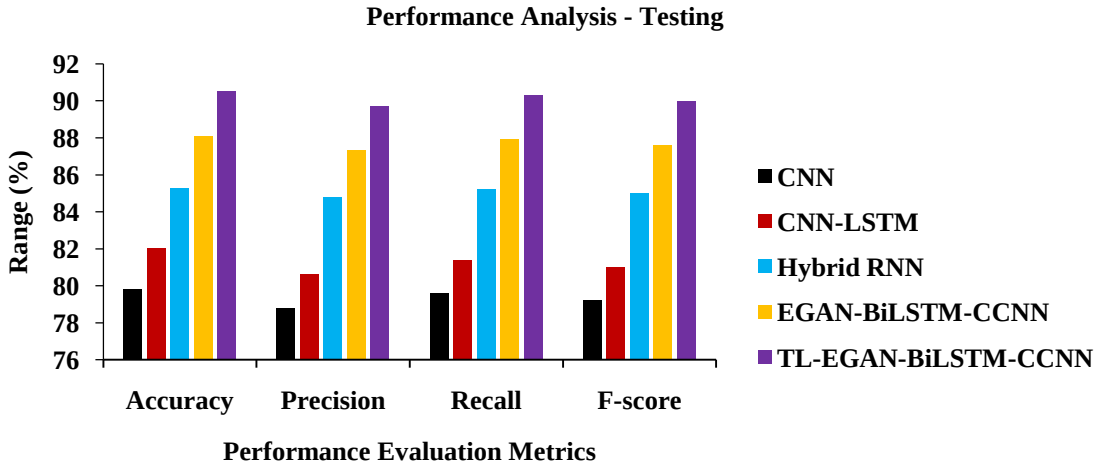

Figure 5. Performance of different IDS models during testing

4. CONCLUSION

This study introduces the TL-EGAN-BiLSTM-CCNN model, which combines local and global information on network parameters to address various threats and provide a robust solution for collaborative IDS. The improved performance and security demonstrated in the study highlight the potential of this approach for real-world applications in dynamic and challenging network environments. The model's capability to handle diverse threats, such as flooding, black holes, gray holes, and forging attacks, is showcased, and extensive simulations validate its effectiveness. The results indicate that the TL-EGAN-BiLSTM-CCNN model reached an accuracy of 92.7% and 90.5% for training and testing, respectively, outperforming existing IDS models. Overall, the proposed model has the potential to enhance the security posture of MANETs in dynamic and challenging environments.

Acknowledgements

The authors would like to express their sincere gratitude to the family and friends for their invaluable support and guidance throughout this research. We are particularly grateful to our colleagues and peers for their constructive feedback and encouragement.

REFERENCES

[1] M. Singh, N. K. Jhajj, and A. Goraya, "IoT-Enabled Wireless Mobile Ad-Hoc Networks: Introduction, Challenges, Applications: Review Chapter," Internet of Things, pp. 121-134, 2022.

[2] N. Sivapriya and R. Mohandas, "Analysis on Essential Challenges and Attacks on MANET Security Appraisal," Journal of Algebraic Statistics, vol. 13, no. 3, pp. 2578-2589, 2022.

[3] S. V. Simpson and G. Nagarajan, "Security Challenges and Attacks in MANET-IoT Systems," Enterprise Digital Transformation, pp. 159-201, 2022.
[4] G. Vidhya Lakshmi and P. Vaishnavi, "An Efficient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution," Wireless Personal Communications, vol. 124, no. 1, pp. 333-348, 2022.
[5] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, "Intrusion Detection and Prevention System for an IoT Environment," Digital Communications and Networks, vol. 8, no. 4, pp. 540-551, 2022.
[6] S. Pamarthi and R. Narmadha, "Literature Review on Network Security in Wireless Mobile Ad-hoc Network for IoT Applications: Network Attacks and Detection Mechanisms," International Journal of Intelligent Unmanned Systems, vol. 10, no. 4, pp. 482-506, 2022.
[7] M. S. Habeeb and T. R. Babu, "Network Intrusion Detection System: A Survey on Artificial Intelligence-Based Techniques," Expert Systems, vol. 39, no. 9, p. e13066, 2022.
[8] C. E. Singh and S. M. C. Vigila, "An Investigation of Machine Learning-Based Intrusion Detection System in Mobile Ad Hoc Network," International Journal of Intelligent Engineering Informatics, vol. 11, no. 1, pp. 54-70, 2023.
[9] T. Sowmya and E. M. Anita, "A Comprehensive Review of AI Based Intrusion Detection System," Measurement: Sensors, vol. 28, p. 100827, 2023.
[10] T. Yi, X. Chen, Y. Zhu, W. Ge, and Z. Han, "Review on the Application of Deep Learning in Network Attack Detection," Journal of Network and Computer Applications, vol. 212, p. 103580, 2023.
[11] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network," IEEE Access, vol. 8, pp. 32464-32476, 2020.
[12] D. Venkatraman and R. Narayanan, "Integrated Framework for Intrusion Detection through Adversarial Sampling and Enhanced Deep Correlated Hierarchical Network," Revue d'IntelligenceArtificielle, vol. 36, no. 4, pp. 597-605, 2022.
[13] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," IEEE Access, vol. 9, pp. 138432-138450, 2021.
[14] M. Rashid, J. Kamruzzaman, T. Imam, S. Wibowo, and S. Gordon, "A Tree-Based Stacking Ensemble Technique with Feature Selection for Network Intrusion Detection," Applied Intelligence, vol. 52, no. 9, pp. 9768-9781, 2022.
[15] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," IEEE Access, vol. 10, pp. 99837-99849, 2022.
[16] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep Q-learning Based Reinforcement Learning Approach for Network Intrusion Detection," Computers, vol. 11, no. 3, p. 41, 2022.
[17] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, "A Deep Learning Model for Network Intrusion Detection with Imbalanced Data," Electronics, vol. 11, no. 6, p. 898, 2022.
[18] S. Gautam, A. Henry, M. Zuhair, M. Rashid, A. R. Javed, and P. K. R. Maddikunta, "A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization," Electronics, vol. 11, no. 21, p. 3529, 2022.
[19] M. A. Talukder et al., "A Dependable Hybrid Machine Learning Model for Network Intrusion Detection," Journal of Information Security and Applications, vol. 72, p. 103405, 2023.
[20] C. E. Singh and S. M. Celestin Vigila, "WOA-DNN for Intelligent Intrusion Detection and Classification in MANET Services," Intelligent Automation & Soft Computing, vol. 35, no. 2, pp. 1737-1751, 2023.
[21] Z. A. Abbood, D. Ç. Atilla, and Ç. Aydın, "Intrusion Detection System through Deep Learning in Routing MANET Networks," Intelligent Automation & Soft Computing, vol. 37, no. 1, pp. 269-281, 2023.
[22] A. Awajan, "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks," Computers, vol. 12, no. 2, p. 34, 2023.
[23] J. Han and W. Pak, "Hierarchical LSTM-Based Network Intrusion Detection System Using Hybrid Classification," Applied Sciences, vol. 13, no. 5, p. 3089, 2023.