SSRG International Journal of Recent Engineering Science
ISSN: 2349 – 7157 / https://doi.org/10.14445/23497157/IJRES-V10I2P103

Volume 10 Issue 2, 13-21, Mar-Apr 2023

Original Article

Securing IoT Networks: RPL Attack Detection with Deep Learning GRU Networks

Raveendranadh Bokka[1], Tamilselvan Sadasivam[2]

[1,2]*Department of ECE, Puducherry Technological University, Puducherry, India*

Received: 12 February 2023 Revised: 16 March 2023 Accepted: 28 March 2023 Published: 10 April 2023

Abstract - *The Internet of Things (IoT) can be defined as the internet-based connectivity of heterogeneous intelligent devices to control and run them. Smart gadgets and wireless networks are vulnerable to numerous routing attacks due to their open nature, worldwide connection, and resource constraints. The Routing Protocol for Low-Power Lossy Networks (RPL) is a prominent routing protocol used in IoT-based networks to design routing paths for resource-constrained devices. However, RPL's built-in security features do not prevent most routing attacks. Because IoT devices generate a vast quantity of data, we presented a Deep Learning-based GRU network in this study for detecting threats in RPL-based IoT networks. Our proposed data set contains traffic traces for normal scenarios and attack scenarios such as Sinkhole, Blackhole, Sybil, Selective Forwarding, DIS flooding, and DIO suppression with 21 features for 20 static nodes generated using the NetSim Standard version 12.1 software tool. The GRU model was trained and tested with 80% and 20% of the dataset. Metrics, including accuracy, precision, recall, f1-score, and AUC, are used to evaluate the model's performance. The model attained a testing accuracy of 95.51 percent, precision, recall, and f1-score values of 0.94, 0.81, and 0.87 for an attack class and 0.96, 0.99, and 0.97 for a normal class, respectively. The model's AUC value is 0.899, indicating that our suggested model can differentiate the attack and normal classes by almost 90%.*

Keywords - *Internet of Things (IoT), 6LoWPAN, RPL, Security, Attacks Detection, Deep Learning, GRU, NetSim.*

1. Introduction

The development of high-speed internet has connected billions of people worldwide [1]. In order to share data from sensors, actuators, processors, and transceivers, a network of intelligent devices with limited resources is known as the Internet of Things (IoT) [2]. A small Internet of Things network called IPv6 over a Low-power Wireless Personal Area Network (6LoWPAN) enables low-power devices to communicate using IPv6 [3]. One of the most critical duties is routing, requiring a power-efficient routing protocol. The Routing over Low Power and Lossy Networks protocol (RPL) [4] solves this problem. On its network layer, the Internet of Things employs the RPL protocol. However, the RPL protocol is susceptible to routing attacks related to the Internet of Things (IoT) [5]. Selective forwarding, version number attacks, sinkhole attacks, blackhole attacks, Sybil attacks, replay attacks, and Denial of Service (DoS) attacks are all common security threats in RPL. As a result, investigating the security implications of RPL security intrusion detection is crucial [3]. This paper focuses on the security of the RPL routing attacks, namely sinkhole attacks, Sybil attacks, selective forwarding attacks, DIO suppression attacks, and DIS flooding attacks. By threatening the Confidentiality, Integrity, and Availability (CIA) of linked nodes, these routing attacks have the biggest impact on the performance of RPL-based IoT networks. [6]. There is no inbuilt security mechanism in RPL protocol from the routing attacks. To prevent against external threats, techniques and algorithms like encryption and authentication are available. However, the attack may be insider or outsider, where the malicious node can mitigate like a normal node and degrade the network's performance [7]. So, there are no authentic methods to countermeasure these attacks.

Insider routing attacks cannot be found or detected using the current authentication and encryption techniques. Because of the enormous amount of data that IoT devices generate, deep learning (DL) techniques are an efficient solution for solving these issues. The DL models examine node behavior and then, using the new data, distinguish between normal and abnormal activity.

This research work's main objective is to propose a network-independent DL-based Gated Recurrent Unit (GRU) model to identify normal and abnormal (attack) behavior in RPL-based IoT networks. First, the normal and abnormal behavior of RPL nodes is simulated and created dataset using NetSim software. Then, the GRU model accesses created data to predict the normal and attack traffic. In the end, we examined the GRU model's performance in terms of accuracy, precision, recall, and f1-score values.

The remainder of the article is structured as follows. The works that have already been done to detect RPL attacks using deep learning techniques are described in Section II. A basic introduction to the RPL protocol, Deep Learning, and GRU networks is provided in section III. Section IV explains the proposed work, problem statement, dataset creation, implementation of GRU classifier, and performance metrics, followed by section V discusses the results. Finally, the research work's conclusion and future scope are presented in sections VI and VII, respectively.

2. Literature Review

In the study, the author Choukri et al. [7] proposed an Intrusion Detection System (IDS) that uses a Multi-Layer Perceptron (MLP) Neural Network to detect RPL rank attacks. The misbehaving of the RPL protocol for the rank attack was simulated using the Cooja simulator and created the dataset. The model's training accuracy was high, falling in at 94.57 %. In subsequent works, Osman et al. [8] proposed a Machine Learning Model Based on a Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks, the performance of the proposed model was evaluated using a variety of performance metrics, including accuracy, precision, F1-score, actual negative rate, and false-positive rate. The model achieved acceptable performance but had a slower execution time. In other related works, the authors [9] implemented to identify threats in IoT networks and categorize them into binary and multiclass models based on convolutional neural networks (CNN), and GRU was used. They validated the proposed models using the BOT-IoT dataset. The paper [10] proposed a GRU-based deep learning method to detect Hello Flooding (HF) attacks against the RPL protocol. In the Contiki operating system, they have run the Cooja simulator simulation, and data packets are produced for both normal and HF attack scenarios. For various numbers of normal and malicious nodes, GRU performance is compared.

Similarly, the authors in [33] proposed an ELNIDS for RPL networks that uses machine learning approaches to protect them from different routing attacks. All the suggested classifiers delivered an acceptable result. Yavuz et al. [12] developed a DL-based attack detection model for highly accurate and precise detection of IoT routing attacks such as decreased rank, hello-flood, and version number modification attacks. The longer training period is a disadvantage of the methodology. In [13], they proposed a machine learning-based IDS based on K-Means (KM), Decision Tree (DT), and Hybrid (KM-DT) for detecting warm-hole attacks in RPL routing. The drawback of the proposed method is achieved very low detection accuracies.

Table 1. lists recent deep learning advances for intrusion detection utilizing private and public datasets.

From the literature, most authors are considering only one or two attacks for detection using either DL or ML methods. Moreover, all the procedures specified in the papers achieved acceptable performance results. So, in this paper, we consider the five types of RPL routing attacks and the GRU network classifier detection method.

3. Overview

This section briefly overviews the RPL protocol standards and its operations. It also details the different deep-learning methods and discusses the structure and operation of the GRU cells.

3.1. RPL Protocol

The Routing Protocol for Low-Power Lossy Networks (RPL) is a widely used routing protocol in the Internet of Things networks composed of devices with limited resources [3]. RPL arranges nodes into Destination Oriented Directed Acyclic Graphs (DODAGs), where a node can join a single DODAG using RPL instances. The node's rank is determined by its position in the DODAG topology. As the distance between a node and its parent node in the DODAG topology increases, the node's rank value also increases [20]. RPL utilizes four categories of control messages for exchanging data between nodes, which are DODAG Information Object (DIO), DODAG Information Solicitation (DIS), Destination Advertisement Object (DAO), and Destination Advertisement Object Acknowledgment (DAO-ACK). These control messages facilitate the connection of all nodes to the current DODAG topology [21].

3.2. Deep Learning

Deep learning is a type of Machine Learning algorithm that involves learning abstract representations of data at a high level. It relies on Artificial Neural Networks (ANNs) with multiple hidden layers to perform complex computations and extract useful features from the input data [22].

Based on the literature, it has been observed that various deep-learning techniques are employed in different applications. Attack detection using deep learning techniques can be categorized into unsupervised, supervised, and hybrid methods. Unsupervised methods include Autoencoder (AE), Deep Belief Networks (DBN), and Generative Adversarial Networks (GAN). On the other hand, supervised methods include Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN). Furthermore, hybrid methods are a combination of two networks [23].

Deep learning models generally contain several hidden implementation layers between the input and output layers. RNN is one of the best deep-learning architectures [34]. The system's units are linked together by a loop and based on the logic of receiving raw input in a specific order. Unfortunately, Traditional recurrent neural networks experience issues with exploding and vanishing gradients [25].

Table 1. Some recent implementations in deep learning for intrusion detection

Reference	DL Model	Dataset	Classification	Performance Metrics
[14]	BiLSTM	NSLKDD	Binary	Accuracy
[15]	RNN	NSLKDD	Multiclass	Accuracy
[16]	GRU	Personal	Multiclass	Accuracy
[17]	GRU	Personal	Multiclass	F1 score
[18]	GRU	NSLKDD	Binary	Accuracy
[19]	LSTM	CIC-IDS2018	Multiclass	Accuracy
Our Study	GRU	Personal	Binary	Accuracy,Precision, Recall and F1-score

Long Short-Term Memory (LSTM), a form of RNN that can learn in long arrays, was used to solve the problem [10]. However, because LSTM cells have a complex structure and require more time to analyze than neural networks, the Gated Recurrent Unit (GRU) was developed. GRU stands out from LSTM [26] because of its quick training, streamlined structure, and easy analysis.

3.3. Gated Recurrent Unit (GRU)

The GRU is a more recent variation of Recurrent Neural Networks, which resembles the LSTM. Unlike the LSTM, the GRU does not use a cell state to transfer data, instead using the hidden state for this purpose. The GRU consists of two gates, as shown in Figure 1: the reset and update gates.

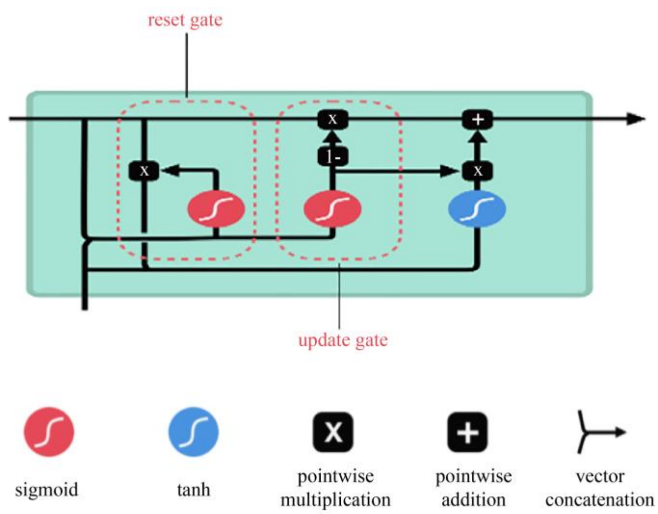

Fig. 1 GRU Memory Cell Structure [27]

Like the update gate in an LSTM, the forget and input gates serve a similar purpose. They decide which information to discard and which to retain. The reset gate, on the other hand, is used to determine how much past knowledge to forget [27].

The terms depicted in Figure 2 are defined as follows: For time step t, equation (1) is utilized to determine the update gate, z_t.

$$z_t = \sigma(W_z x_t + U_z h_{t-1}) \quad (1)$$

Where x_t is the input vector and h_{t-1}preserves the output of the previous timestamp $t-1$. When $x_t$and $h_{t-1}$are multiplied by their weights W_z and U_z, respectively. The multiplication results are summed, and then a sigmoid activation function σ is applied to match the results.
Reset gate r_t is used to decide how much of the fast information in the model is forgotten and determined by (2)

$$r_t = \sigma(W_r x_t + U_r h_{t-1}) \quad (2)$$

When $x_t$and $h_{t-1}$are multiplied by their weights W_z and U_z. The multiplication results are summed, and then a sigmoid activation function σ is applied.

Recent memory contents can be determined by analyzing the impact of the gates on the final output. To begin with, the reset gate is used to create unique memory content that stores crucial information from the past [28]. Equation (3) is used to compute it:

$$\tilde{h}_t = tanh(W x_t + r_t \odot U h_{t-1}) \quad (3)$$

Here, x_t and h_{t-1} is multiplied by its corresponding weights W and U, and the element−wise product between the reset gate r_t and Uh_{t-1}. The sum of the result is applied with the nonlinear activation function *tanh.*

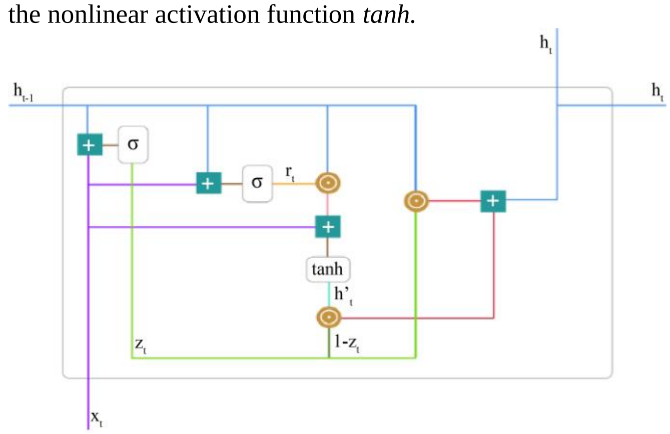

Fig. 2 GRU Memory cell detailed architecture [28]

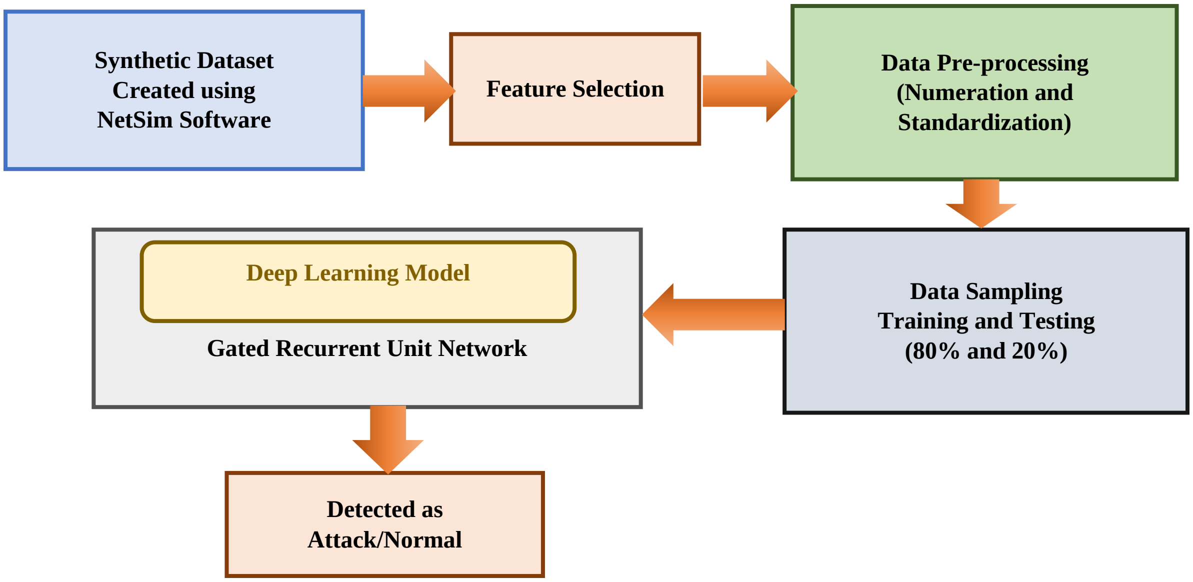

Fig. 3 Proposed Architecture for GRU-Based Attack Detection

The final memory at the current time step is h_t, which is a vector comprising the current unit's information and is fed into the model [10]. To achieve this, an update gate is required. Equation (4) is utilized to compute which information is to be retrieved from the current memory content $\tilde{h}_t$ and the previous steps h_{t-1} by the GRU network.

$$h_t = z_t \odot h_{t-1} + (1 - z_t) \odot \tilde{h}_t \quad (4)$$

Here, element-wise multiplication was done between $z_t$and h_{t-1}, and $to\ 1 - z_t\ and\ \tilde{h}_t$. Finally, the sum of the results is assigned to the h_t the current memory content.

4. Proposed Work

The RPL protocol is vulnerable to various insider and outsider attacks. Although several security measures exist to safeguard against outsider attacks, they are ineffective in the case of insider attacks [35]. Routing attacks, such as selective forwarding, sinkhole, DIO suppression, DIS flooding, and Sybil attacks, are major insider attacks that disrupt network topology and degrade the RPL protocol's performance. Unfortunately, there are no reliable approaches for detecting routing attacks in RPL-based IoT networks without increasing the overhead of the RPL protocol. As a solution, we proposed a network-independent intrusion detection system based on Deep Learning using GRU networks to identify various RPL routing attacks.

4.1. Proposed Architecture

Figure 3 details the proposed architecture for detecting routing attacks using a DL-based GRU network. It describes the different stages of implementation for attack detection using GRU networks. In the first stage, the synthetic dataset was generated using the NetSim v12.0 Software [30], which can simulate various networking environments, i.e., IoT, MANET, 5G, VANET, etc... The simulation and generation of the synthetic dataset are described in the next section, V(b).

In the next stage, the feature selection for selecting the best helpful feature from the simulated results and then the data preprocessing was made in Google Colab using Python programming with the help of Pandas and Numpy libraries. Next, the data preprocessing was done to enumerate categorical type features and standardize all the data into the same range. In the subsequent steps, the data sampling was done to split the total dataset into 80% of training and 20% of testing datasets for training and testing the DL model. In the final stage, the DL-based GRU network was implemented in Google Colab with the help of TensorFlow backend Keras libraries and trained using different model settings discussed in detail in section V(c). Finally, the trained model is tested using the test data and analyzed for the model's accuracy in detecting attacks or normal conditions.

4.2. Synthetic Dataset Generation

The RPL attacks synthetic dataset, which was simulated and built using the NetSim software, is discussed in this section. Table 2 provides information on the simulation parameter settings used to configure the IoT network scenario with sensor nodes, a 6LoWPAN gateway, a router, and a wired node, which were utilized to create the dataset. The simulation environment contains 20 IoT devices, including one parent node, seventeen sensing/child nodes, and two malicious nodes that build a single DODAG topology.

The created simulation scenario simulated five common attacks and a normal scenario, with two simulations for each attack and five for normal scenarios. The packet captures was then saved as distinct CSV files and labeled as either attack or normal instances before merging all the CSV files to obtain the final synthetic RPL attacks dataset.

Table 2. Simulation Parameter Details

Parameters	Description and Values
Simulator	NetSim Standard v12.0
Nodes Type	Sensing Nodes
No. of Nodes	20
Sink/Parent Nodes	1
Sensing/Child Nodes	17
Malicious Nodes	2
Routing Protocol	RPL
Nodes Positioning	Random

The created dataset comprises 21 features and two labeling attributes, namely, 'attack' and 'normal'. The final dataset consists of 95342 and 22168 instances for normal and attack classes, respectively, mentioned in Table 3.

Table 3. Dataset Description

Name of the Class	Number of Instances
Attack	22168
Normal	95342

Figure 4 illustrates the significance of each feature and its names in classification models. Among these features, *'packet-type', 'control_packet_type', 'source-id', 'destination-id', 'transmitter-id'*, and *'receiver_id'* are of nominal or text type. Since most machine learning and deep learning models only function with numeric data values. They are unable to understand text-based information [31]. Therefore, before putting the text data into the deep learning network, we converted them into numerical data.

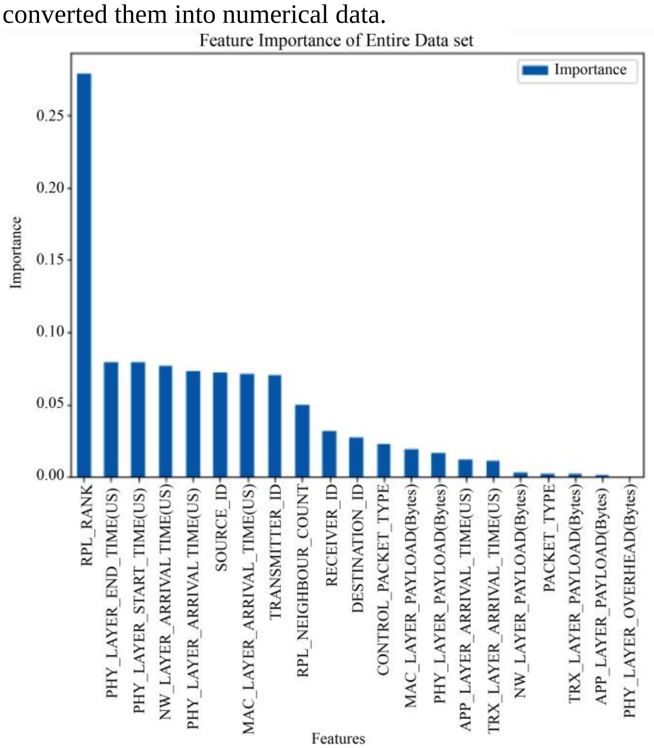

Fig. 4 Feature Importance in Entire Dataset

4.3. Implementation of GRU Network for RPL Attack Detection

Section IV(b) discussed that the Deep Learning-based GRU network for RPL attack detection implementation started after the data preprocessing. The network was created with an input layer size of 21 for accepting the 21 input features from the dataset. The detailed implementation setting of the GRU network for binary classification is mentioned in Table 4. In sequence with the input layer, there are four hidden layers with the size of 64,64,64 and 32 GRU cells. Each cell consists of a sigmoid and tanh activation function for generating output for the given input. Finally, the output layer with the size of one neuron with a sigmoid activation function is used to classify the output as either attack or normal, i.e., binary classification. The implemented model was trained for 80% of the training data for 100 epochs with a batch size of 64, an optimizer as 'Adam,' learning rate as '0.01', and a loss function as Binary cross-entropy.

Table 4. GRU Network Settings

Parameter	Value
Input Layer size	21
No. of Hidden Layers	4
Hidden Layer Sizes	64,64,64,32
Output Layer size	1
Optimizer	Adam
Batch size	64
Epochs	100
Learning Rate	0.01
Activation Functions	Sigmoid, Tanh
Loss Function	Binary cross entropy

3.4. Performance Metrics

The objective of this paper is to examine the effectiveness of the GRU classifier. The confusion matrix presented in Table 5 is utilized to evaluate the model's performance, which provides information on the relationship between the predicted and actual classes based on the test dataset. Correctly identifying attack data as an attack is classified as True Positive (TP), whereas if the model identifies an attack as normal, it is known as False Negative (FN). True Negative (TN) refers to when the model correctly detects no attack, and False Positive (FP) is when the model incorrectly detects an attack. These measures are utilized to assess the model's performance using various metrics such as Accuracy, Precision, Recall, AUC, and F1-score, which are calculated using equations 5, 6, 7, and 8.

Table 5. Confusion Matrix

			Predicted Class/Label	
			Attack	**Normal**
True Class/Label	**Attack**		TP	FN
	Normal	FP	TN	

Equation 5 defines *accuracy* as the proportion of correctly classified instances of both classes to the total number of instances. A higher value of this metric indicates superior model performance.

$$Accuracy = \frac{No\ of\ True\ Classes}{Total\ Number\ of\ classes} = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (5)$$

Precision, as shown in equation 6, refers to the proportion of true positive predictions to the total number of predicted positive instances.

$$Precision = \frac{True\ positive\ prediction}{Total\ predicted\ positive} = \frac{TP}{(TP+FP)} \quad (6)$$

Recall, as defined in equation 7, refers to the ratio of correctly classified instances to the total number of instances that should have been classified.

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

The *F1-score*, as shown in equation (8), is the harmonic mean of precision and recall. It is a crucial metric for evaluating the model's performance, particularly when dealing with imbalanced datasets [32].

$$F1 - Score = 2 * \frac{precison*recall}{precison+recall} \quad (8)$$

The *Area Under Curve (AUC)* is used to indicate the level of separability. A larger AUC implies the superior performance of the model, where it correctly identifies class 0 as 0 and class 1 as 1.

4. Results and Discussion

In this method, the GRU network is trained and tested using the network traffic data of 1,17,510 RPL routing attacks to identify two binary labeled classes, Attack and Normal. The complete dataset was divided into training and testing sets with 80% and 20%, respectively.

The accuracy and loss graphs of the model for training and testing data are shown in Figures 5 and 6. The absolute accuracy of the model for the training and testing dataset for 100 epochs is 95.49% and 95.51%, respectively. The testing and training accuracies are almost stable after 20 epochs. The final loss for the testing and training datasets is almost equal. At the initial stage, the loss is very high. The loss decreased for every epoch, and after 20 epochs, it became stable and reached 0.098 and 0.099 for the training and testing dataset, respectively.

After training the model with 80% of the dataset, the trained model was tested using the remaining 20%. It consists of 4414 instances of attacks and 19088 instances of normal data. After testing, the model performance was assessed using the confusion matrix generated using the predicted classes and actual classes of the test data shown in Figure 7. From the 4434 instances of attack, 3575 are predicted correctly as an attack, and 839 instances are predicted incorrectly as normal.

Fig. 5 Training and Testing Accuracy

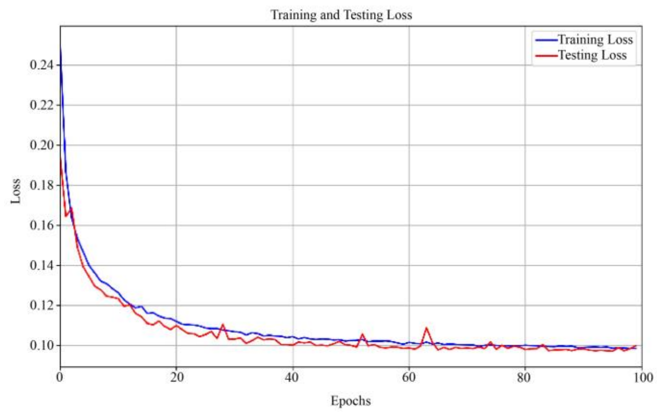

Fig. 6 Training and Testing Loss

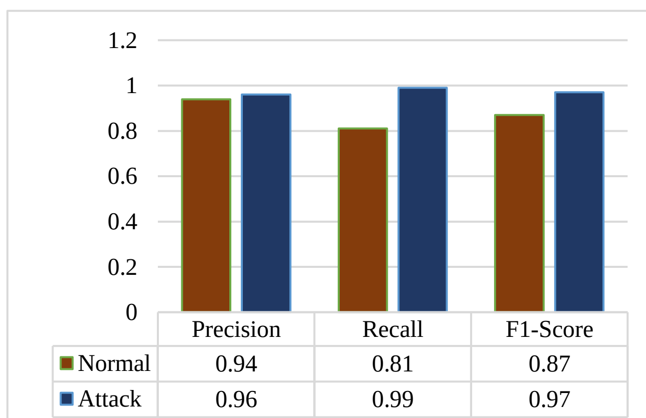

Fig. 7 Confusion Matrix

In another normal class, out of 19068 instances, 216 instances are misclassified as attacks, and the remaining 18872 instances are predicted correctly as normal. The final accuracy of the binary classification model was 95.511%. With the help of the confusion matrix, we calculated the metric False Positive Rate (FPR) as 1.13%, demonstrating that the model is better with a lower rate of false positives.

The precision, recall, and F1-score performance metrics were calculated and compared for binary classification of the normal and attack classes, as shown in Figure 8. The precision values obtained were 0.96 and 0.94 for the normal and attack classes, respectively. Similarly, the recall values were 0.81 for the attack class and 0.99 for the normal class. Additionally, the F1-score values were found to be 0.87 for the attack class and 0.97 for the normal class.

The ROC curve, displayed in Figure 9, illustrates the correlation between the True Positive Rate (TPR) and False Positive Rate (FPR). Its shape indicates that the model can accurately differentiate between TPR and FPR values, with an AUC value of 0.899. The ROC curve provides evidence that our model can effectively identify positive and negative classes.

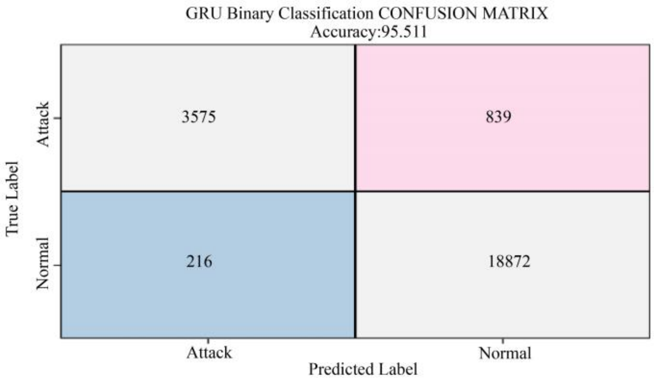

Fig. 8 Prediction Performance of GRU classifier

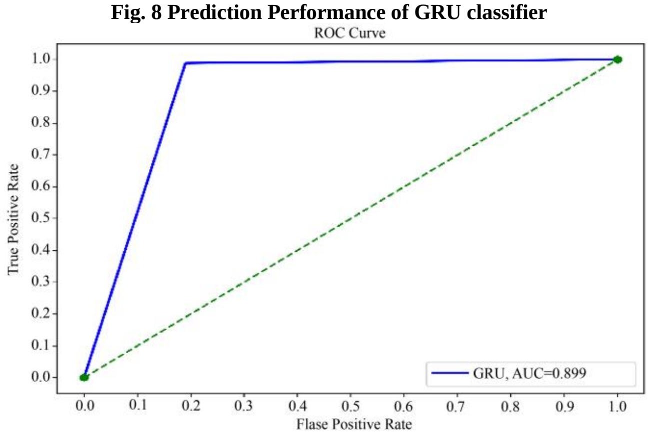

Fig. 9 ROC Curve

5. Conclusion

To detect attacks in RPL-based IoT networks, this research employed a GRU network based on Deep Learning techniques since IoT devices produce vast amounts of data. We utilized the NetSim Standard version 12.1 tool to produce a synthetic dataset consisting of traffic traces for normal and attack scenarios like Sinkhole, Blackhole, Sybil, Selective Forwarding, DIS flooding, and DIO suppression, featuring 21 attributes for 20 static nodes. We trained and tested the GRU model using 80% and 20% of the dataset, respectively, and evaluated its performance using metrics such as accuracy, precision, recall, f1-score, and AUC. The model achieved a testing accuracy of 95.51%, with precision, recall, and f1-score of 0.94, 0.81, and 0.87 for the attack class and 0.96, 0.99, and 0.97 for the normal class, respectively. The model's AUC value was 0.899, indicating an ability to distinguish the attack and normal classes with approximately 90% accuracy. The false positive rate was 1.13%, indicating a low rate of false positives. The proposed model was designed for binary classification only and exhibited better accuracy, recall, f1-score, and precision than existing models.

6. Future Scope

In our upcoming research, we aim to apply diverse deep learning techniques such as Convolutional Neural Networks, Recurrent Neural Networks (based on LSTM), and Hybrid and ensemble methods to identify RPL routing attacks in IoT networks. We will incorporate a range of optimization techniques to enhance these models' detection capabilities with respect to our synthetic dataset. Additionally, we will explore the utilization of GRU models to achieve multiclass categorization. Lastly, we plan to implement GRU models for multiclass classification.

Declarations

Ethical approval None of the authors of this article conducted any studies involving animals or human participants.

Availability of Data

The corresponding author possesses the datasets used in the study, but they are not publicly available.

References

[1] S. K. Fahmida Islam, Morium Akter, and Mohammad Shorif Uddin, "Design and Implementation of an Internet of things Based Low-cost Smart Weather Prediction System," *International Journal of Information Technology*, vol. 13, no. 5, 2021. [CrossRef] [Google Scholar] [Publisher link]

[2] Carlos D. Morales-Molina et al., "A Dense Neural Network Approach for Detecting Clone id Attacks on the RPL Protocol of the IoT," *Sensors*, vol. 21, no. 9, 2021. [CrossRef] [Google Scholar] [Publisher link]

[3] Sarumathi Murali, and Abbas Jamalipour, "A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2020. [CrossRef] [Google Scholar] [Publisher link]

[4] Etsuko Sugawara, and Hiroshi Nikaido, "Properties of AdeABC and AdeIJK Efflux Systems of Acinetobacter Baumannii Compared with Those of the AcrAB-TolC System of Escherichia Coli," *Antimicrobial Agents and Chemotherapy*, vol. 58, no. 12, pp. 7250–7257, 2014. [CrossRef] [Google Scholar] [Publisher link]

[5] Abhishek Verma, and Virender Ranga, "Analysis of Routing Attacks on RPL Based 6LoWPAN Networks," *International Journal of Grid and Distributed Computing*, vol. 11, no. 8, pp. 43–56, 2018. [CrossRef] [Google Scholar]

[6] Aryan Mohammadi Pasikhani et al., "Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review," *IEEE Sensors Journal*, vol. 21, no. 11, pp. 12940–12968, 2021. [CrossRef] [Google Scholar] [Publisher link]

[7] Wijdan Choukri, Hanane Lamaazi, and Nabil Benamar, "RPL Rank Attack Detection using Deep Learning," *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies*, 2020. [CrossRef] [Google Scholar] [Publisher link]

[8] Musa Osman et al., "ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks," *IEEE Access*, vol. 9, pp. 83654-83665, 2021. [CrossRef] [Google Scholar] [Publisher link]

[9] Imtiaz Ullah, Ayaz Ullah, and Mazhar Sajjad, "Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks," *IoT*, vol. 2, no. 3, pp. 428-448, 2021. [CrossRef] [Google Scholar] [Publisher link]

[10] Semih Cakir, Sinan Toklu, and Nesibe Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," *IEEE Access*, vol. 8, pp. 183678–183689, 2020. [CrossRef] [Google Scholar] [Publisher link]

[11] Anita Patrot, "Internet of Things (IoT) Security Issues and Challenges," *International Journal of Computer Trends and Technology*, vol. 70, no. 6, pp. 72-75, 2022. [CrossRef] [Publisher link]

[12] Furkan Yusuf Yavuz, Devrim Ünal, and Ensar Gül, "Deep Learning for Detection of Routing Attacks in the Internet of Things," *International Journal of Computational Intelligence Systems*, vol. 12, no. 1, pp. 39–58, 2018. [CrossRef] [Google Scholar] [Publisher link]

[13] Prachi Shukla, "ML-IDS: A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things," *2017 Intelligent Systems Conference*, 2018. [CrossRef] [Google Scholar] [Publisher link]

[14] Yakubu Imrana et al., "A Bidirectional LSTM Deep Learning Approach for Intrusion Detection," *Expert Systems with Applications*, vol. 185, p. 115524, 2021. [CrossRef] [Google Scholar] [Publisher link]

[15] Chuanlong Yin et al., "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017. [CrossRef] [Google Scholar] [Publisher link]

[16] Thien Nguyen et al., "DÏoT: A Federated Self-learning Anomaly Detection System for IoT," *2019 IEEE 39th International Conference on Distributed Computing Systems*, pp. 756–767, 2019. [CrossRef] [Google Scholar] [Publisher link]

[17] Fangyu Li et al.,"System Statistics Learning-Based IoT Security: Feasibility and Suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019. [CrossRef] [Google Scholar] [Publisher link]

[18] Zhida Li et al., "Machine Learning Techniques for Classifying Network Anomalies and Intrusions," *IEEE International Symposium on Circuits and Systems*, 2019. [CrossRef] [Google Scholar] [Publisher link]

[19] B.B. Borisenko et al., "Intrusion Detection using Multi-layer Perceptron and Neural Networks with Long Short-term Memory," *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications*, 2021. [CrossRef] [Google Scholar] [Publisher link]

[20] Anthea Mayzaud, Remi Badonnel, and Isabelle Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-based Networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472–486, 2017. [CrossRef] [Google Scholar] [Publisher link]

[21] Hanane Lamaazi, and Nabil Benamar, "OF-EC: A Novel Energy Consumption Aware Objective Function for RPL Based on Fuzzy Logic," *Journal of Network and Computer Applications*, vol. 117, pp. 42–58, 2018. [CrossRef] [Google Scholar] [Publisher link]

[22] Nadia Chaabouni et al., "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019. [CrossRef] [Google Scholar] [Publisher link]

[23] Yirui Wu, Dabao Wei, and Jun Feng, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey," *Security and Communication Networks*, 2020. [CrossRef] [Google Scholar] [Publisher link]

[24] A. Anandhavalli, and A. Bhuvaneswari, "IoT Based Wireless Sensor Networks – A Survey," *International Journal of Computer Trends and Technology*, vol. 65, no. 1, pp. 21-28, 2018. [CrossRef] [Publisher link]

[25] Devika Chhachhiya, Amita Sharma, and Manish Gupta, "Designing Optimal Architecture of Recurrent Neural Network (LSTM) with Particle Swarm Optimization Technique Specifically for Educational Dataset," *International Journal of Information Technology*, vol. 11, pp. 159–163, 2019. [CrossRef] [Google Scholar] [Publisher link]

[26] Rui Fu, Zuo Zhang, and Li Li, "Using LSTM and GRU Neural Network Methods for Traffic Flow Prediction," *2016 31st Youth Academic Annual Conference of Chinese Association of Automation*, 2017. [CrossRef] [Google Scholar] [Publisher link]

[27] Michael Phi, Illustrated Guide to LSTM's and GRU's: A Step by Step Explanation. [Online]. Available: https://towardsdatascience.com/illustrated-guide-to-lstms-and-gru-s-a-step-by-step-explanation-44e9eb85bf21

[28] Simeon Kostadinov, Understanding GRU Networks. [Online]. Available: https://towardsdatascience.com/understanding-gru-networks-2ef37df6c9be

[29] Amit Sagu, Nasib Singh Gill, and PreetiGulia, "Artificial Neural Network for the Internet of Things Security," *International Journal of Engineering Trends and Technology*, vol. 68, no. 11, pp. 129-136, 2020. [CrossRef] [Google Scholar] [Publisher link]

[30] Network Simulator, NetSim, Emulator, 5G, Military Communication, Vehicular networks. [Online]. Available: https://www.tetcos.com/

[31] Sohom Ghosh, "Identifying Click Baits using Various Machine Learning and Deep Learning Techniques," *International Journal of Information Technology*, vol. 13, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher link]

[32] Raveendranadh Bokka, and Tamilselvan Sadasivam, "Machine Learning Techniques to Detect Routing Attacks in RPL Based," *International Journal of Electrical Engineering and Technology (IJEET)*, vol. 12, no. 6, pp. 346–356, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Abhishek Verma, and Virender Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages*, 2019. [CrossRef] [Google Scholar] [Publisher link]

[34] Gauri Jain, Manisha Sharma, and Basant Agarwal, "Optimizing Semantic LSTM for Spam Detection," *International Journal of Information Technology*, vol. 11, pp. 239–250, 2019. [CrossRef] [Google Scholar] [Publisher link]

[35] Abhishek Verm, and Virender Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," *IEEE Sensors Journal*, vol. 20, no. 11, pp. 5666–5690, 2020. [CrossRef] [Google Scholar] [Publisher link]