Artificial Neural Network Model for Decreased Rank Attack Detection in RPL Based on IoT Networks

Musa Osman[1], Jingsha He[1], Fawaz Mahiuob Mohammed Mokbal[1,2], and Nafei Zhu[1]
(Corresponding author: Nafei Zhu)
Faculty of Information Technology, Beijing University of Technology[1]
Beijing 100124, China
Faculty of Engineering and Information Technology, Taiz University[2]
Taiz, Republic of Yemen
Email:znf@bjut.edu.cn
(Received March 26, 2020; Revised and Accepted Nov. 10, 2020; First Online Apr. 17, 2021)

Abstract

Internet of Things (IoT) cyber-attacks are growing day by day because of the constrained nature of the IoT devices and the lack of effective security countermeasures. These attacks have small variants in their behavior and properties, implying that the traditional solutions cannot detect the small mutant variations. Therefore, a robust detection method becomes necessary. One of the common attacks is routing protocol for low power and lossy network attacks, which has not been well investigated in the literature. In this paper, we propose an artificial neural network (ANN) model for detecting decreased rank attacks, which includes three phases: Data pre-processing, Feature extraction using random forest classifier, and an artificial neural network model for the detection. The proposed model has been tested in multi and binary detection scenarios using the IRAD dataset. The results obtained are promising with accuracy, precision, false-positive rate, and AUC-ROC scores of 97.14%, 97.03%, 0.36%, and 98%, respectively. The proposed approach is efficient and outperforms previous methods of precision, recall, and F-score metrics.

Keywords: 6LoWPAN; Attacks; Detection Technique; IoT; RPL; Security

1 Introduction

Internet of Things (IoT) is a system of interconnected devices, machines and related software services. The core elements of IoT are the sensors and actuators, which are used to collect and actuate data. These devices use many communication techniques such as Bluetooth, WiFi, LoRa, IEEE802.15.4, *etc.* Many technologies are classified under IoT such as smart homes, smart cities, smart healthcare, *etc.* Moreover, IoT is expected to be the next generation of worldwide network, where a large number of things are expected to be part of the Internet [9, 22, 23].

To make the things a part of the Internet, a routing protocol for low power and lossy network (RPL) has been developed by IETF [5] to perform routing over IPv6 over Low-power wireless personal area network (6LoWPAN). Furthermore, RPL forms the topology in a mathematical graph model which is known as a directed acyclic graph (DAG) without directed cycles. In a DAG, all nodes are connected in a way that the traffic is routed through the nodes via one or more routes and there is no cyclic round within the DAG. In the DAG, there are one or more destination oriented directed acyclic graph (DODAG) in which there will be one node named the sink node or the border router (6BR) [6]. Moreover, within the DAG, several instances may also exist and each instance may have one or more DODAG. Figure 1 shows the RPL network with one instance and two DODAG in each instance. Besides, RPL DODAG is constructed by four control messages, DODAG Information Solicitation (DIS), DODAG Information objects (DIO), Destination Advertisement Objects (DAO), and DODAG acknowledges (DAO ACK).

The DIO message is advertised by a root node or a node in a DODAG which contains such information as RPL instance ID, DODAGs ID, DODAGs version number, RPL mode of operation, the rank of sending node, and the objective function used, and other control information. If the sender is a root, then the DIO contains information to create the DODAG. If the sender is not a root node, it means that this node wants to join the DODAG [17]. When a node wishes to join a DODAG and, for a while, doesn't receive any DIO message, it starts to broadcast DIS messages looking for an existing DODAG. While DIO

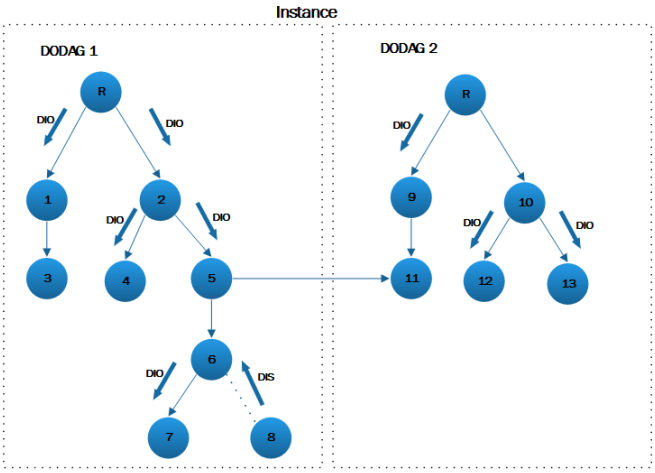

Figure 1: RPL network (one instance two DODAG)

and DIS are used to maintain the upward path towards the root node, DAO is used to construct the downward path from the root to the leaf nodes or children [6, 21].

The RPL protocol is vulnerable to different types of attacks, some of which are originated from wireless sensor networks (WSN) and traditional networks [10, 11]. Moreover, RPL has its specific vulnerabilities [6]. Consequently, these attacks require robust and versatile techniques to protect valuable resources and data. Rank attack is one type of RPL attacks in which the malicious node advertises a false rank which will be the best parent for the benign nodes. Literatures [7, 17] investigated the rank attack as three types of attacks: Decreased rank attack (DR) in which the malicious node advertises a rank that is lower than the other nodes, which will make it the best parent node [12], resulting in attracting a large part of the traffic, increased rank attack (IR) in which the node that in reality is close to the root node advertises a higher rank, forcing nodes to choose other parents [7], and worst parent attack in which the malicious node advertises its correct rank but selects the worst parent for itself. Attacks against routing protocol in IoT need more attention from research to better protect IoT networks and devices from such attacks. Some research showed that lightweight solutions are the best solutions. From our point of view, machine learning techniques provide a viable approach for detecting these attacks because IoT devices generate a tremendous amount of data, rendering a robust detection mechanism a necessity. In this paper, a robust artificial neural network-based multilayer perceptron (MLP) model is proposed to detect RPL attacks such as decreased rank attack, along with feature selection using the random forest (RF) classifier [2]. IRAD dataset is used as a benchmark [23] for training and validation of the proposed model.

The proposed model has successfully surpassed several tests on the held-out testing dataset and achieved promising results with accuracy, precision, detection probabilities, false-positive rate, false-negative rate, and area under the ROC curve (AUC) scores of 97.01%, 97.03%, 97.01%, 4.6%, 1.6% and 98%, respectively.

The rest of this paper is organized as follows. Section 2 reviews some related work. Section 3 describes the proposed method. Section 4 presents the experimental results and Section 5 shows the conclusion and future work.

2 Related Work

Attacks against IoT devices have increased significantly, affecting the availability of both traditional networks and IoT devices. Recent research on RPL attacks has been focused on the detection and mitigation of different types of attacks. Furkan *et al.* [23] prepared a real IoT dataset using the COOJA simulator called the IoT Routing Attack Dataset (IRAD) which contains three types of attacks: Version number attacks (VN), decreased rank attacks (DR) and hello flood attacks (HF). They employed artificial neural networks model for classification to obtain good accuracies like 94.9% in the DR model, 99.5% in the HF model and 95.2% in the VN model. Another dataset was generated by Verma *et al.* [20] for IoT and was named RPL-NIDDS17 which is specially developed for IoT routing attacks. It contains seven types of routing attacks such as clone ID, hello flooding, local repair, selective forwarding, sinkhole, blackhole and sybil in the IoT field comprised of 20 features and 2 labeling attributes. The authors used five deep learning techniques to evaluate the complexity of this dataset, such as naive Bayes (NB), decision tree (DT), logistic regression (LR), expectation-maximization (EM) clustering and artificial neural networks (ANN), and achieved accuracies of 80.71%, 94.07%, 79.79%, 77.17% and 93.99%, respectively. Ahmet *et al.* [1] proposed a lightweight technique to mitigate the effect of version number attacks in RPL by using two techniques. One is the elimination of any version number updates (VN) coming from leaf nodes and the other, called a shield, makes the node change the VN depending on its neighbors with a better rank. It was claimed that the delay caused by the attacker can be shortened up to 87% and the average power consumption can be reduced up to 63%. In addition, the control message overhead can be lowered up to 71% and the data packets delivery ratio can be increased up to 86%. Mayzaud *et al.* [13] investigated the effect of VN attacks in a network with 20 nodes. In the work, the authors claimed that the control overhead can be increased by up to 18 times.

The authors also reported that the delivery ratio of packets was reduced by 30% and the location of the attacker could affect the consistency of the network. If the attacker is close the root, the effect of the attack is less than if it is far away from the root. Nikravan *et al.* [15] first analyzed the RPL routing protocol and proposed a lightweight technique to mitigate VN attacks. The technique relies on using the identity based offline/online signature (IBOOS) scheme which is divided into two phases,

Table 1: Sample of the dataset features and instances

No	Time	Source	Destination	Length	Info	Trans Rate(per 1000 ms)	Reception Rate(per 1000 ms)	TR/ RR	Sources Count Per Sec	Destination Count Per Sec
1	00.00	1	9999	64	2	0.039	0.195	0.2	39	195
2	0.003289	1	9999	64	2	0.039	0.195	0.2	39	195
3	0.006555	1	9999	64	2	0.039	0.195	0.2	39	195
4	0.009851	1	9999	64	2	0.039	0.195	0.2	39	195
5	0.013153	1	9999	64	2	0.039	0.195	0.2	39	195
6	0.016411	1	9999	64	2	0.039	0.195	0.2	39	195

i.e., the online phase where most of the heavy computational operations are performed and the online phase where it performs a lightweight scheme. Snehal *et al.* [3] designed an IDS for detecting wormhole attack using received signal strength indicator (RSSI) which is converted to distance and by using Euclidean distance method so as to compare the distance between a node and its neighbors. If the distance is more than the transmission range of the node, it is identified as an attacker node. The proposed IDS has good results in a small number of nodes. The detection of rank attack has also been investigated by Usman *et al.* [18] through using a root-based statistical intrusion detection system to detect rank attacks by applying statistical algorithms to comparing the rank of the nodes.

Under normal conditions, the number of nodes is small and there is no mobility and the model can achieve high accuracy. However, when the number of nodes increases, the accuracy decreases. Kfoury *et al.* [8] proposed an IDS using a self-organizing map to detect three types of RPL attacks: Hello flood, sinkhole and version number attacks. However, there is no clear implementation of this IDS method and the power consumption is not clear from the study. Dvir *et al.* [4] proposed an IDS based on cryptographic techniques to avoid false rank and claimed that these techniques had high computational overhead which would affect the IoT device's power consumption. Besides, it is also vulnerable to other attacks such as those discussed in paper [16].

3 Proposed Methodology

The proposed model named multi-layer RPL attack detection (MLRPL) is composed of three modules that work together to perform the detection of RPL attacks. The first module is data pre-processing, the second is feature selection and the third is the artificial neural network for attack detection.

3.1 Dataset

The dataset used to evaluate the MLRPL model is the IRAD dataset [23] which consists of three types of attacks: VN attack, DR attack and HF attack. Each attack appears in a separate CSV file consisting of 18 features with 1048575 samples in total (579944 malicious and 468630 benign). The label feature is binary (0 is benign and 1 is decreased rank attack). Table 1 shows the sample records of the IRAD DR attack dataset. Then the dataset of the decreased rank attack and the version number attack is combined in one dataset named RPL attack dataset for categorical classification. The new dataset consists of 2997150 records and 18 features. The label feature is categorical (0 means benign, 1 means DR attack and 2 means VN attack) encoded using a one-hot encoder. Table 2 shows a subdivision of the RPL dataset.

Table 2: Subdivision of the RPL attacks dataset

Category	Malicious	Benign	Total
DR attack	468631	579944	1048575
VN attack	503326	545249	1048575
Total	971957	1125193	2097150

3.2 Features Selection

To improve the performance of the model, feature selection is used to extract the most important features from the dataset. The feature selection process contributes most in the prediction of the model, moreover, it reduces the training and validation time and increases the performance of the model. In general, pre-processing is performed applying the dataset before running the artificial neural networks model. To identify features of high importance, information gain is used to evaluate the gain for each variable and a random forest (RF) classifier is trained on the entire dataset. By using entropy shown in Equation (1) as a measure of information gain while splitting samples at each node of a tree, we assumed that features with low entropy were strong signals for identifying the most relevant features, which is summarized in Table 3.

$$\begin{cases} E_s = & \frac{n_l}{n} E_l + \frac{n_r}{n} E_r \\ E_l = & -\sum_{i \in c} p_{il} \log p_{il} \\ E_r = & -\sum_{i \in c} p_{ir} \log p_{ir} \end{cases} \quad (1)$$

where p_{ir} is the proportion of samples of the left split, p_{ir} is the proportion of samples of the right split, n_i is the number of samples in the left split, and N represents the total number of samples.

Table 3: The important features selected from the dataset

No.	Selected Feature	Score
8	DIO	0.04499746
7	DAO	0.05063975
6	Transmission Rate (per 1000 ms)	0.07437906
5	TR / RR	0.07781687
4	Trans Total Duration Per Sec	0.09315402
3	Trans Average Per Sec	0.09966616
2	Rcv Total Duration Per Sec	0.17506193
1	Rcv Average Per Sec	0.188617
0	Rcv Total Duration Per Sec	0.17506193

Before fitting the random forest, the dataset was preprocessed. Firstly, we manually dropped features that did not affect an artificial neural network model such as Source, Destination, *etc.* Then, we checked out the missing values and split the dataset into training and test set (70% for training and 30% for the test). Subsequently, feature scaling was performed so that they could be compared based on common grounds. Thereafter, the preprocessed data is fitted into the Random Forest (RF) Classifier for selecting the most important features. As the result, the best 10 features were selected based on the importance score as shown in Table 3. Figure 2 depicts the selected features and their scores. Furthermore, RPL protocol depends on three types of control message which are DIO, DAO and DIS. So, DIS was included in the selected feature set despite its low score rate of 0.00648158.

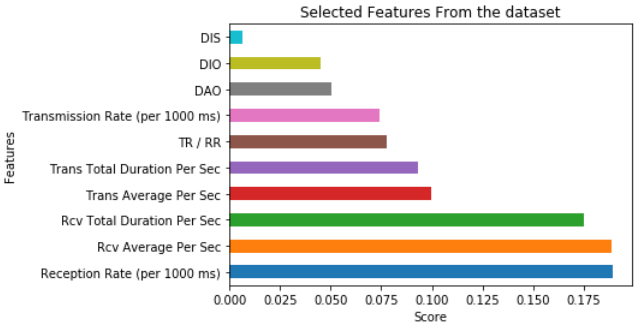

Figure 2: The selected feature and score

3.3 The ANN Model

Artificial neural network (ANN) attempts to mimic the human brains. ANN consists of a set of units named as neurons that are interconnected together to form layers [14]. ANN consists of an input layer, one or more hidden layers and an output layer. Each layer consists of several neurons. The model has one input layer which receives the data as a vector of features (xi) and produces the result as a vector of (yi) which is $y_i \in \{0, 1\}$ where 0 means benign and 1 means malicious. The output of each previous layer and the bias b value is computed by a nonlinear activation function f, which takes a weighting w_n from the previous layer as an input for the next layer and the calculation follows Equation (2).

$$a_n = f\left(\sum_{i=0}^{n} w_i x_i + b\right) \tag{2}$$

The neurons at the hidden layer(s) has activation functions, i.e., RelU and Tanh. The output layer neurons have the f_z activation function, i.e., sigmoid. The output of the sigmoid function is a binary output which is 0 or 1 calculated using Equation (3).

$$sigmoid = \frac{1}{(1+e^x)} \tag{3}$$

The main model which is used to detect the anomaly in the IoT network is based on artificial neural network (ANN) named as a multilayer perception technique for detecting RPL attacks (MLRPL) with input layer consisting of 20 neurons and three hidden layers. The first hidden layer has 50 neurons, the second hidden layer has 150 neurons and the third layer has 20 neurons. All these layers use rectified linear function (ReLU) as the activation function, and the output layer uses logistic function (Sigmoid) as the activation function in binary classification case and the Softmax function for categorical classification. For the loss function, mean square error (MSE) is used which is the sum of squared distances between the target variable and predicted values. Moreover, stochastic gradient descent (SGD) optimizer is used for optimizing the loss function with suitable properties. Table 4 shows the performance of the MLRPL model in the case of the three optimizers (SGD, Adam, and Adadelta optimizer). From the results, it can be concluded that SGD is the best optimizer in the RPL attack dataset as it can be inferred from the values of the metrics. To train the MLRPL model, grid search is used for tuning the best parameters, and 64 is the batch size whereas 700 is the best number of epochs.

4 Results and Discussions

4.1 Performance Evaluation Metrics

The performance of the proposed model was evaluated using various measurement metrics such as accuracy, detection rate (DR), precision and F1 score. Accuracy is a ratio of a number of correct predictions to the total number of samples and it is counted for both training and validation datasets. DR is the ratio of intrusions detected by the model. Another estimator is the precision which is the ratio between the correct positive results (TP) to all positive results predicated by the model. An additional estimator is the recall which is correct positive results to all samples that are supposed to be identified as positive.

Another measure of the quality of the model is the F1-score which is a consistent mean between precision and recall [14, 19]. The formulas are defined as follows:

$$
\begin{aligned}
Accuracy &= \frac{(TP+TN)}{(TP+TN+FP+FN)} \\
DR &= \frac{TP}{(TP+FN)} \\
Precision &= \frac{TP}{(TN+FP)} \\
F1-score &= \frac{2TP}{2(TP+FP+FN)} \\
AreaUndertheCurve &= \frac{1}{2}\left(\frac{TP}{(TP+FN)}+\frac{TN}{(TN+FP)}\right)
\end{aligned}
$$

where TN is true negative which denotes that a benign case was correctly labeled as benign, FP is false positive which points that a benign case was incorrectly labeled as an attack. As for the performance metrics, FN is false negative which indicates that an attack is incorrectly identified as benign, TP is true positive that indicates that an attack is correctly identified as an attack.

4.2 Experiment Results

The artificial neural network model was trained and tested using the method proposed in both cases for the multi and binary detection problems, respectively. The results are shown in the following.

4.2.1 Binary Classification Results

As a result of our proposed model, in the case of decreased rank attack dataset, for the binary classification case, the training and testing accuracy obtained is 97.14% and 97.01%, respectively, as shown in Figure 3. Furthermore, Figure 4 shows the loss function performance over time. Figure 5 shows the results of the confusion matrix while the receiver operating characteristic (ROC) is shown in Figure 6. The results are summarized in Table 4, showing that excellent precision can be obtained.

4.2.2 Multi-classification Results

In the case of the multi-classification problem, we used the same model (MLRPL) with the same parameters with Softmax as the activation function and the categorical cross-entropy as the loss function. Table 6 shows the classification results obtained, where 0 is benign, 1 is DR attack and 2 is VN attack. Furthermore, Figure 7 shows the training and testing accuracy for the model in which the accuracy obtained is 96.59% for the training phase and 96.39% for the testing phase. In Figure 8 the loss function in training and testing is shown. Based on these results it can be concluded that MLRPL can achieve high accuracy in both training and testing for DR attacks and VN attacks. The precision of MLRPL in detecting DR attacks is also high in the case of multi-classification as

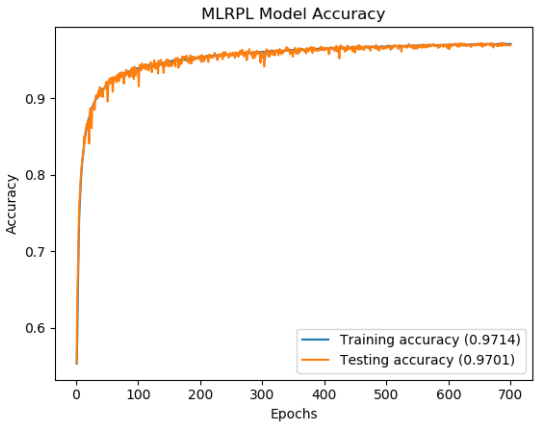

Figure 3: Model accuracy (training and testing)

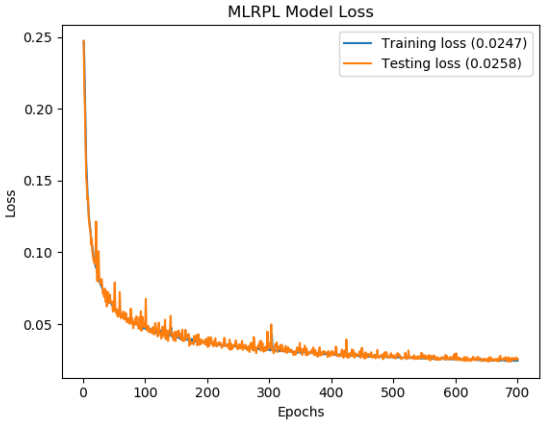

Figure 4: Model log loss values over time

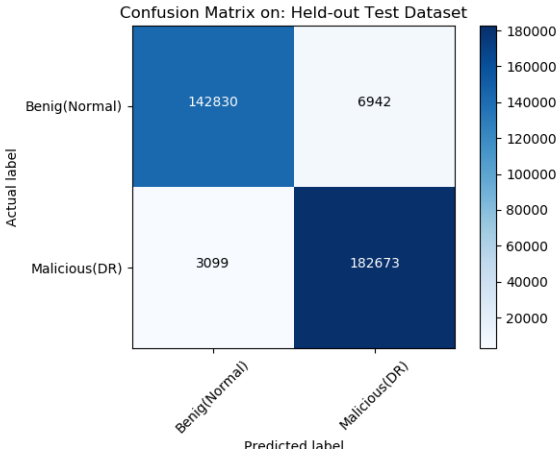

Figure 5: Confusion matrix on test dataset

Table 4: Classification report

	Precision	Recall	F1-score	Support
0	0.9788	0.9536	0.9660	149772
1	0.9634	0.9833	0.9733	185772
Avg./Total	0.9703	0.9701	0.9700	335544

Table 5: Result comparison MLRPL with other classifiers

Optimizer	**Benign**			**Malicious**		
	Precision	Recall	f1-score	Precision	Recall	F1-score
MLRPL	0.9788	0.9536	0.9660	0.9672	0.9882	0.9776
KNN	0.91	0.90	0.91	0.92	0.93	0.92
SVM	0.95	0.92	0.93	0.93	0.96	0.94
Random forest	0.96	0.95	0.95	0.96	0.97	0.96

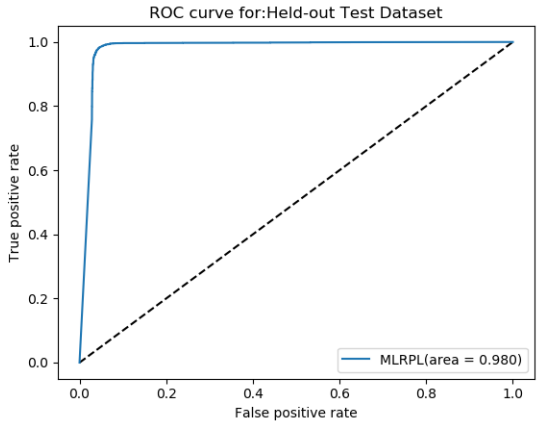

Figure 6: Receiver operating characteristic

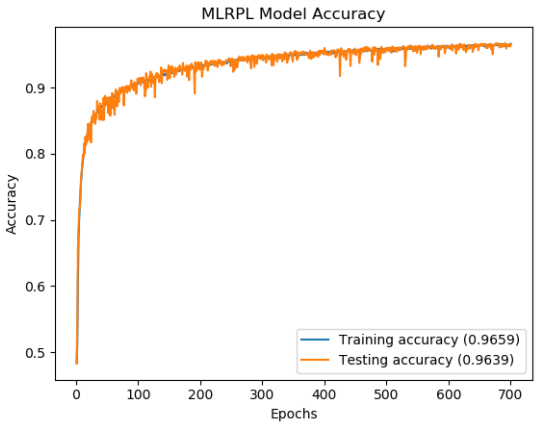

Figure 7: Model accuracy (training and testing)

in the binary classification. Table 6 shows the comprehensive multi-classification results generated based on the confusion matrix. Also, we performed a new experiment using the same dataset with different machine learning algorithms such as KNN, SVM and RF Classifier. Table 5 shows the classification results.

Table 6: Multi-classification report

	Precision	Recall	F1-score	Support
0	0.95608	0.9702	0.9630	334163
1	0.9651	0.9629	0.9640	191685
2	0.9792	0.9525	0.9657	166212
Avg./Total	0.9641	0.9639	0.9639	692060

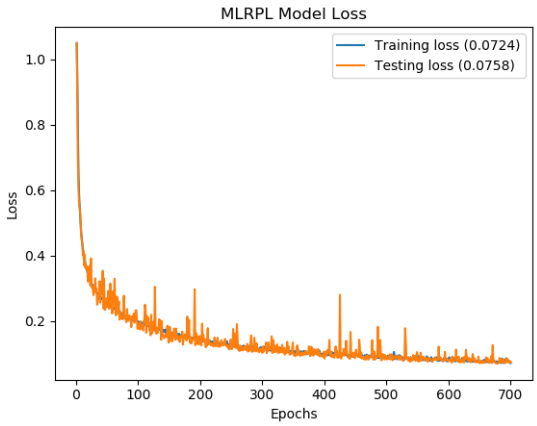

Figure 8: Log loss values over time

4.3 Comparison with Related Methods

To evaluate the proposed scheme, the MLRPL model is compared to some related methods. The comparison is

Table 7: Comparison of related work

Models	Precision	Recall	F1-score	Accuracy
MLRPL (binary)	97.14%	97.88%	95.36%	97.01%
Furkan *et al.* [23]	94.9%	95%	96%	94%
Abhishek *et al.* [20]	93.99	-	-	-

applied to proposed work by Furkan *et al.* [23] and by A. Verma *et al.* [20] which were discussed in the related work. Table 7 are the comparison results which show that the MLRPL model is better in the case of accuracy, precision, and F1-score. Moreover, the MLRPL model is also more efficient in the form of training time (number of epochs) and the complexity of the model (number of neurons and the number of layers).

5 Conclusion

In this paper, we proposed a machine learning model for detecting decreased rank attacks. The proposed model consists of three steps, namely data collection, feature extraction using random forest classifier and classification. Experiment results revealed that the proposed approach can achieve better results than other related methods. The results obtained from the MLRPL model indicate the fact that accuracy can be further improved. We believe that artificial neural network techniques provide the best direction for detecting and preventing routing attacks for both traditional networks and IoT networks. However, it is worth mentioning that better accuracy can be further achieved by conducting more experiments. It is clear that securing IoT is still in its infancy and, therefore, more solutions and additional research can be pursued to develop more effective solutions to secure IoT data and the networks.

Acknowledgment

The work in this paper has been supported by National Key Research and Development Program of China under grant 2019QY(Y)0601. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Aris, S. B. Ö. Yalçın, and S. F. Oktuğ, "New lightweight mitigation techniques for RPL version number attacks," *Ad Hoc Networks*, vol. 85, pp. 81–91, 2019.

[2] T. T. Gao, H. Li, and S. L. Yin, "Adaptive convolutional neural network-based information fusion for facial expression recognition," *International Journal of Electronics and Information Engineering*, vol. 13, no. 1, pp. 17-23, 2021.

[3] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based internet of things," *Procedia Manufacturing*, vol. 32, pp. 840–847, 2019.

[4] A. Dvir, T. Holczer, and L. Buttyan, "Vera-version number and rank authentication in RPL," in *IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 709–714, Oct. 2011.

[5] O. Gaddour and A. Koubaa, "RPL in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012.

[6] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[7] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based internet of things: Survey," in *International Conference on Emerging Trends & Innovation in ICT (ICEI'17)*, pp. 33–39, Feb. 2017.

[8] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A self organizing map intrusion detection system for RPL protocol attacks," *International Journal of Interdisciplinary Telecommunications and Networking (IJITN'19)*, vol. 11, no. 1, pp. 30–43, 2019.

[9] A. Kumari, V. Kumar, M. YahyaAbbasi, and M. Alam, "The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," in *International conference on advances in computing, Communication Control and Networking (ICACCCN'18)*, pp. 321–325, Oct. 2018.

[10] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[11] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[12] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459-473, 2016.

[13] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schonwalder, "A study of RPL dodag version attacks," in *IFIP International Conference on Au-*

tonomous Infrastructure, Management and Security, pp. 92–104, 2014.

[14] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, F. Akhtar, and W. Xiaoxi, "MLPXSS: An integrated xss-based attack detection scheme in web applications using multilayer perceptron technique," *IEEE Access*, vol. 7, pp. 100567–100580, 2019.

[15] M. Nikravan, A. Movaghar, and M. Hosseinzadeh, "A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks," *Wireless Personal Communications*, vol. 99, no. 2, pp. 1035–1059, 2018.

[16] H. Perrey, M. Landsmann, O. Ugus, T. Schmidt, and M. Wahlisch, "Trail: Topology authentication in RPL," in *Proceedings of International Conference on Embedded Wireless Systems and Networks*, pp. 59-64, 2013.

[17] A. Raoof, A. Matrawy, and C. H. Lung, "Routing attacks and mitigation methods for RPL-based internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2018.

[18] U. Shafique, A. Khan, A. Rehman, F. Bashir, and M. Alam, "Detection of rank attack in routing protocol for low power and lossy networks," *Annals of Telecommunications*, vol. 73, no. 7-8, pp. 429–438, 2018.

[19] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *International Conference on Wireless Networks and Mobile Communications (WINCOM'16)*, pp. 258–263, Oct. 2016.

[20] A. Verma and V. Ranga, "Evaluation of network intrusion detection systems for RPL based 6lowpan networks in IoT," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1571–1594, 2019.

[21] A. Verma and V. Ranga, "Mitigation of dis flooding attacks in RPL-based 6lowpan networks," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, pp. e3802, 2020.

[22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[23] F. Y. Yavuz, D. Unal, and E. Gul, "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.

Biography

Musa Osman is a PhD student at Beijing University of Technology (BJUT), China. He received his BSc in computer science at University of Gazira, Sudan, and MSc in Information System at Osmania University,India. His main research interests are security issues in the Internet Of Things mostly based on RPL protocol, Machine Learning, and Artificial Neural Network.

Jingsha He received his bachelor's degree in computer science from Xi'an Jiaotong University in China and his Master's and Ph.D. degrees in computer engineering from the University of Maryland at College Park in US. He is currently a professor in the Faculty of Information Technology at Beijing University of Technology (BJUT) in Beijing, China. Prior to joining BJUT in August 2003, Prof. He worked for several multi-national companies in the US, including IBM Corp., MCI Communications Corp. and Fujitsu Laboratories, during which he published more than 10 papers and received 12 US patents. Since joining BJUT in August 2003, Prof. He has published over 270 papers in scholarly journals and international conferences, received 66 patents and 33 software copyrights in China and finished 9 books. He has been the principal investigators of more than 30 research projects. Prof. He's research interests include information security, wireless networks and digital forensics.

Fawaz Mokbal received his BS degree in Computer Science from Thamar University, Yemen, and MS degree in Information Technology from the University of Agriculture, Pakistan. He is currently pursuing Ph.D. studies in Computer Science and Technology with Beijing University of Technology, China. He has won numerous international and university awards and he is the author and reviewer with various SCI, EI, and Scopus indexed journals. His area of interest includes Machine Learning, Artificial Neural Networks, Web Application Security, and Security issues in IoT.

Nafei Zhu received her B.S. and M.S. degrees from Central South University, China in 2003 and 2006, respectively, and her Ph.D. degree in computer science and technology from Beijing University of Technology, China in 2012. From 2015 to 2017, she was a postdoc as well as an assistant researcher in the Trusted Computing and Information Assurance Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences in China. She is now on the faculty of Information Technology in Beijing University of Technology. Dr. Zhu has published over 20 research papers in scholarly journals and international conferences (16 of which have been indexed by SCI/EI/ISTP). Her research interests include information security and privacy, wireless communications and network measurement.