International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Real Time Feature Impact Optimization (RFIO) Based Deep Neural Network Model for Improved 5G-IoT Security

**G. Ramasubramanian[1], S. Rajaprakash[2]**

**Submitted**: 05/11/2023 **Revised**: 24/12/2023 **Accepted**: 06/01/2024

**Abstract**: The problem of data security in 5G-IoT network has been well studied. The support of rapid communication provided by the network has been used by various sectors. The security threat has been identified in the same frequency as it supports the communication. Towards handling such intrusion threats, there exist numerous techniques which address specific problem and consider only limited factors of communication. This inclined their performance against security towards different threats. To address this issue, an efficient Real-time Feature Impact Optimization (RFIO) based DNN model (RFIO-DNN) is presented in this article. The method uses multiple standard data sets for the evaluation of the methods in restricting different threats. To start with, the data sets are merged and normalized to a single entity using Feature Level Fuzzy Normalizer. Second the method applies Feature Impact Optimization (RFIO) algorithm towards feature selection. Using the features selected, the method trains the deep neural network. At the test phase, the neurons of the network compute Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW). Using these values, the output layer neuron computes Multi Constraint Trust Weight (MCTW) according to the IoT devices present in the transmission route. Incoming data are classified with MCTW towards intrusion detection.

***Keyword:*** *5G-IoT Networks, wireless networks, Intrusion attack, Intrusion detection, RFIO, RFIO-DNN.*

## 1. Introduction

The recent trends in communication sector have been used by various domains of business world. The increased use of internet technology requires high speed communication at all times. The entry of 5G-IoT network supports the high speed communication. The 5G-IoT network has number of IoT nodes which is capable of transmitting data through the frequency and supports data communication in the network. Unlike other generation networks, the IoT devices can be act as a router which supports the higher speed communication. In this model, the IoT devices receives the data packets belongs to other nodes and act as a forwarder. This increases the data rate of the network to improve the transmission speed and increases the QoS performance.

Like any network, 5G-IoT network has different threats towards the data transmission. The intrusion attack is the most dominant network threat, which allows the malicious node to perform any malicious activity. By learning the data transmission in the network,, the IoT devices would perform any kind of intrusion attack.

For example, when the data transmitted in the network is about an fund transfer then it would learn the data which contains information about the account details and security passwords, then the malicious node would malformed the data and perform different threats. Similarly, in case of intrusion attack, adversary can intrude and analyze complete data transmission and access various services to collect the data to perform any threat in future.

Towards detecting intrusion attack, various IDS are described in literature. The most approaches consider only limited features and limited records in analyzing the trust of users. But, they produce poor performance in intrusion detection, which challenges entire functioning. However, the performance of IDS can be improved by considering more number of features and factors. Also, the performance is greatly depending on the volume of data set being used. The most data sets contain only specific features but by combining multiple data sets, the volume as well as feature size can be improved. On the other side, the general methods are not capable of handling huge volume of data, so that, deep learning methods can be used in this case. The Decision Tree, Support vector machine, Naïve Bayes Classifier, KNN and other are capable of handling limited features and records. By considering deep learning models, the performance of classification can be improved. The deep learning algorithms would handle huge volume of data toward the problem of intrusion detection.

With the consideration to improve the performance in IDS in 5G-IoT networks, an efficient Real-Time Feature Impact Optimization (RFIO) Based Deep Neural Network Model is presented in this article. This approach intended to club multiple data sets like NSL-KDD, UNSW-NB15 and

[1]*Research Scholar, Faculty of Arts and Science Vinayaka Missions Research Foundation, Salem, Tamil nadu State-636308 Emil:rram2005@hotmail.com*
[2]*Professor,Department of Computer Science and Engineering,Aarupadaiveedu Institute of Technology, Vinayaka Missions Research Foundation,Paiyanoor, Chengalpattu District. Tamil Nadu State-613104.Emil: srajaprakash_04@yahoo.com*

AWID are considered for the analysis. The method applies the normalization technique and RFIO feature selection scheme to extract the features. Further, the method trains the network and performs classification by computing MCTW measure towards intrusion detection.

## 2. Related Work

There are number of approaches described in literature to handle the intrusion detection problem in 5G-IoT networks. This section briefs set of methods related to the problem.

A light weight secure routing (LSR) is presented in [1], which uses ant colony optimization to measure direct and indirect trust values towards secure routing in WSN. An cluster based scheme is presented in [2], towards secure routing in 5G networks, which choose a cluster head according to the genetic algorithm and BAT algorithm. An energy efficient data aggregation method (EEDAM) is presented in [3], which reduces energy by performing data aggregation at cluster level and chooses IoT with least delay with blockchain security. A hierarchical trust management scheme (TSW) is presented in [4], which support cooperative decision making strategy in various nodes by computing trust values towards secure routing. A blockchain based model is presented in [5], which applies machine learning classifier like histogram gradient boost (HGB) towards classifying the malicious node.

Time Interval Conditional Entropy- Based Intrusion Detection System (TCE-IDS) is presented in [6], which measure the conditional entropy towards detecting intrusion attack in Automotive Controller Area Networks.

A two-stage network traffic anomaly detection model is presented in [7], which performs dimensionality reduction of edges in 5G network and applies deep neural network classifier to detect the threat.

A Layer wise Graph Theory Based Intrusion Detection System (LGTBIDS) is presented in [8], which analyze the layers and identifies the vulnerable nodes according to the energy efficiency. The attacked nodes are re-authenticated with the system.

A traffic load learning framework is presented in [9], to perform intrusion attack. The method monitors the traffic and estimates the possible load, and identifies the intrusion attack.

A Convolutional Neural Network (CNN) with Gated Recurrent Unit (GRU) model (CNN-GRU) is presented in [10], which detect the cyber threat using the image data.

A 5G-IoT node authentication scheme is presented in [11], which increases the unique radio frequency (RF) fingerprinting data to train the Deep learning model to detect legitimate and non-legitimate IoT nodes.

A Few-shot Latent Dirichlet Generative Learning (FLAG) based semantic-aware traffic detection is presented in [12], which augment the trained data and uses Fuzziness Recycle Method (FRM) with long short-term memory (LSTM) to perform classification.

A Wasserstein Distance-based Combined Generative Adversarial Network (WCGAN) is presented in [13], which updates the loss function and combines multiple generators towards intrusion detection.

A pattern-based feature selection a method is presented in [14], which uses machine learning (ML) based botnet detection system. The method generates dominant pattern feature values and identifies maximal frequent item sets. The method uses unsupervised learning to perform feature selection.

For a wireless Mobile Ad-Hoc network (MANET) to operate at high data rates, efficient packet access must be improved. Due to similar traits with trustworthy nodes in the sensing region, reducing the severity will be a challenging task because the deterioration is brought on by the discovery of malicious nodes [15].

IoT is one of the upcoming internet technologies that focuses on the delivery of services and adjusting the way that technologies are implemented across various communication networks [16].

## 3.Real-time Feature Impact Optimization (RFIO) Based DNN model (RFIO-DNN):

The RFIO-DNN model reads the data sets and merges the data set. The merged data set is normalized using Feature Level Fuzzy Normalizer. Further, Feature Impact Optimization (RFIO) algorithm is applied to select specific features from the data set. Then, the features and values of the records is extracted and converted into feature vector. Extracted feature vector set has been used to train DNN. At the test phase, the neurons of network compute Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW). Using these values, the output layer neuron computes Multi Constraint Trust Weight (MCTW) according to the IoT devices present in the transmission route. Using MCTW, the incoming data are classified.

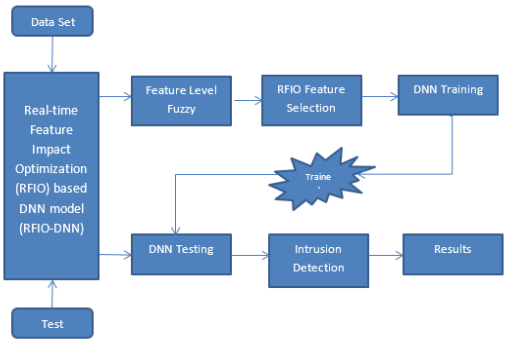


**Fig 1**: Working Diagram of Proposed RFIO-DNN Model

The working model of proposed RFIO-DNN scheme is presented in Figure 1, where the functional aspects of each stage have been briefed in this section.

### 3.1 Feature Level Fuzzy Normalizer

The feature level fuzzy normalizer reads the multiple data sets initially. Set of features available in the data set are identified. Also, class based tuples are collected. Using the range_min and range_max values, the method generates number of ensemble for each tuple according to different features of various data set. The method generates k number of ensemble with exact values of all features of the tuples of different data records. Further, the method generates N mutations according to the range min and range max values of the data set.

**Algorithm:**

Given: Data sets Ds

Obtain: Preprocessed data set Pds

Start

Read Ds.

Initialize feature set Fs = $\left(\sum_{i=1}^{Size(Ds)} \sum_{j=1}^{size(Ds(i))} Features \in Ds(i)(j)\right) \cup Fs$

For each data set D

Find class data Cd = $\sum_{i=1}^{size(D)} D(i).class == c$

For each feature f

Compute Range _Min = $\sum_{i=1}^{size(cd)} Min(Cd(i))$

Compute Range_Max = $\sum_{i=1}^{size(cd)} Max(Cd(i))$

End

For each other data set Od

Find Class C's Tuple set Ts = $\sum_{i=1}^{Size(Od)} Od(i).class == C$

Find features set Fs = $\left(\sum_{j=1}^{size(Ts)} Features \in Ts(i)\right) \cup Fs$

For each record r of Cd

Add features of Fs with r

R = $\left(\left(\sum Features \in r\right) \cup \sum Features(Fs)\right.$

For each feature f belongs to Fs in R

R(Fs(f))= Random(Fs(f).range_min, Fs(f).range>max)

End

End

End

End

Stop

The feature level normalizer algorithm finds the features of other data sets and computes Range_min and Range_max values. According to the range values, the method generates number of records and appends the features of other data set and initializes them with different random values between the ranges computed. The preprocessed set is used to perform intrusion detection.

The above algorithm computes feature impact frequency for variety of features on the different data set. As per frequency values, a subset of features are identified to perform intrusion detection.

### 3.3 DNN Training

The method trains the deep neural network with number of intermediate layers. The number of intermediate layer is decided according to the number of classes and number of trust values measured. Accordingly, the model trained with six layers with four intermediate layers. The first intermediate layers involve in computing Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW) for the binary class with 1, where the second two intermediate layers are designed to compute Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW) values for the binary class 0. The output layer returns two set of Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW) values which has been used to compute MCTW value to perform intrusion detection.

### 3.4 DNN Testing

The test sample given has been taken for DNN testing. With the tuple given, the method extracts the features and generates the feature vector. Generated feature vector has been passed to the network trained. The first intermediate layers involve in computing Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW) for the binary class with 1, where the second two intermediate layers are designed to compute Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW) values for the binary class 0. Obtained result on the output layer has been used to compute MCTW value. Estimated value has been used to perform intrusion detection.

**Algorithm:**

Given: DNN, Test Sample Ts

Obtain: Class C

Start

Read DNN and Ts.

Feature vector fv = $\sum Features \in Ts$

Pass Fv to DNN.

At first intermediate layer

Each neuron computes Feature Level Trust Flt for genuine class.

$$\text{FLT (gc)} = \frac{\sum_{sizei=1}^{size(Cs)} \left( \frac{\sum_{j=1}^{size(Fv)} Count(Dst(Fv(j),Cs(i)(j)) < Th)}{size(Fv)} \right)}{Size(Cs)}$$

At second intermediate layer.

Each neuron computes Tltw value for genuine class. Compute Transmission Level Trust Weight Tltw.

$$\text{Tltw (gc)} = \frac{\sum_{size(i=1)}^{size(Cs)} Count(Cs(i).state == Genuine)}{Size(Cs)}$$

Third intermediate layer computes FLT for malicious class.

$$\text{FLT (mc)} = \frac{\sum_{sizei=1}^{size(Cs)} \left( \frac{\sum_{j=1}^{size(Fv)} Count(Dst(Fv(j),Cs(i)(j)) < Th)}{size(Fv)} \right)}{Size(Cs)}$$

Fourth intermediate layer computes Tltw value for malicious class.

$$\text{Tltw (Mc)} = \frac{\sum_{size(i=1)}^{size(Cs)} Count(Cs(i).state == Genuine)}{Size(Cs)}$$

Output layer returns Flt(gc)Tltw(gc),Flt(mc) and Tltw(mc).

Compute MLTW value for genuine class

MLTW(gc) = FLT(gc)×TLTW(gc).

Compute MLTW value for malicious class

MLTW(mc) = FLT (gc)×TLTW(gc).

Class C= choose the class value with maximum MLTW value

Stop

The DNN testing algorithm computes MLTW value for various classes and based on that the method identifies the class of data.

## 4. Results and Discussion

The proposed model is implemented using matlab and performance is measured using different data sets. The performance evaluation is carried out by using NSL-KDD, UNSW-NB15 and AWID data sets.

**Classification Accuracy**:

The performance of the method is measured for its classification accuracy. It has bee measured as follows:

$$\text{Classification Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

**Precision**:

The precision represent the positive rate produced by the method in classification. It has been measured as follows:

$$PR = \frac{TP}{TP+FP}$$

**Recall:**

Recall is the measure which represents the true positive rate produced by the method. It has been measured as follows:

$$TPR = \frac{TP}{TP+FN}$$

**False Positive Rate**:

FPR is the measure which represents the ratio of false classification produced by the method. It has been measured as follows:

$$FPR = \frac{FP}{FP+TN}$$

According to the above factors, the methods are measured for their performance and presented in this section.

**Table 1:** Analysis on various metrics

| Methods | TPR (%) | FPR (%) | Precision (%) | Accuracy (%) |
|---|---|---|---|---|
| **LGTBIDS** | 89 | 5 | 81.65 | 93.80 |
| **TCE-IDS** | 75 | 8.75 | 68.18 | 88 |
| **FLAG** | 68 | 11.75 | 59.13 | 84.20 |
| **CNN-GRU** | 80 | 6.25 | 76.19 | 91 |
| **RNN-LSTM** | 99 | 2.3 | 98.9 | 99 |
| **RFIO-DNN** | 99.2 | 1.4 | 99.4 | 99.6 |

The performance of the method is evaluated on different metrics and displayed in Table 1. The proposed RFIO-DNN method introduces higher performance in all the factors.

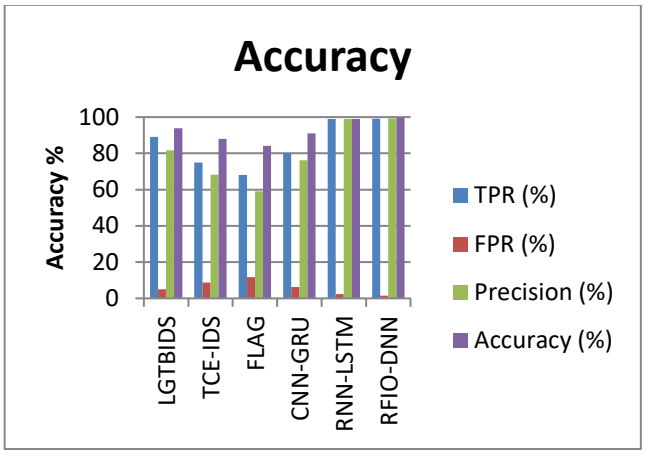


**Fig 2.**Performance Analysis

Analysis of various metrics is performed and compared in Figure 2. The proposed, RFIO-DNN algorithm has produced higher performance in all the factors. The method used NSL-KDD and UNSW-NB 15 data sets. Both were merged and normalized to frame the data set and features are extracted to train the model. Accordingly, the method are measured for their performance and presented in the above Figure 2. In all the case, the RFIO-DNN algorithm has produced higher performance than others.

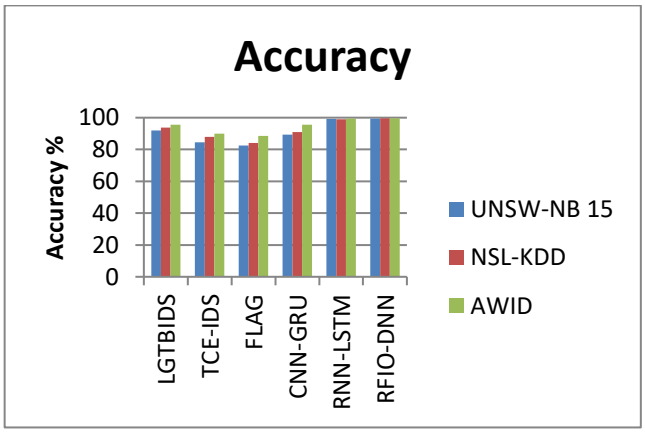


**Fig 3:** Analysis on Accuracy

The performance in classification accuracy is measured for different data sets and presented in Figure 3. The proposed RFIO-DNN algorithm has produced higher accuracy in classification than other methods.

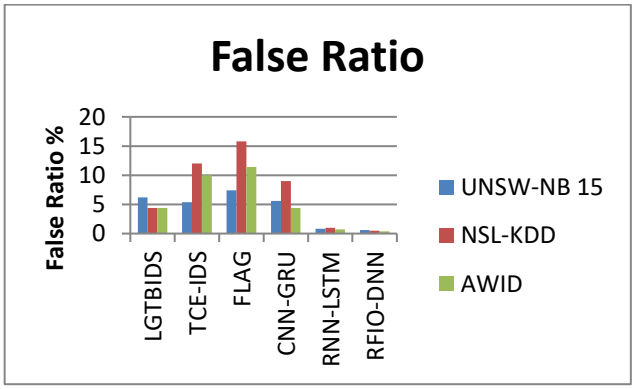


**Fig 4:** Analysis on false ratio

The ratio of false classification produced by different methods are measured and presented in Figure 4. The proposed RFIO-DNN algorithm has produced less false classification than others.

## 5.Summary

This paper presented a novel real-time feature impact optimization based DNN model (RFIO-DNN) towards intrusion detection in 5G networks. The method uses various data sets and merge them towards normalization using Feature Level Fuzzy Normalizer. Further, Feature Impact Optimization (RFIO) algorithm is applied to select specific features from the data set. Then, the features and values of the records is extracted and converted into feature vector. Extracted feature vector set has been used to train the deep neural network. At the test phase, the neurons of the network compute Feature Level Trust (FLT) and Transmission Level Trust Weight (TLTW). Using these values, the output layer neuron computes Multi Constraint Trust Weight (MCTW) according to the IoT devices present in the transmission route. Using the value of MCTW, the method classifies the incoming data as well as node to perform intrusion detection.

## References

[1] A. Pathak, I. Al-Anbagi and H. J. Hamilton, "An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23826-23840, 1 Dec.1, 2022, doi: 10.1109/JIOT.2022.3189832.

[2] S. Verma, S. Zeadally, S. Kaur and A. K. Sharma, "Intelligent and Secure Clustering in Wireless Sensor Network (WSN)-Based Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 13473-13481, Aug. 2022, doi: 10.1109/TITS.2021.3124730.

[3] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," in IEEE Access, vol. 10, pp. 11404-11419, 2022, doi: 10.1109/ACCESS.2022.3146295.

[4] M. Bin-Yahya, O. Alhussein and X. Shen, "Securing Software-Defined WSNs Communication via Trust Management," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22230-22245, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3102578.

[5] M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran and N. Javaid, "Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs," in IEEE Access, vol. 11, pp. 6106-6121, 2023, doi: 10.1109/ACCESS.2023.3236983.

[6] Z. Yu, Y. Liu, G. Xie, R. Li, S. Liu and L. T. Yang, "TCE-IDS: Time Interval Conditional Entropy- Based Intrusion Detection System for Automotive Controller

Area Networks," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1185-1195, Feb. 2023, doi: 10.1109/TII.2022.3202539.

[7] K. Sood, M. R. Nosouhi, D. D. N. Nguyen, F. Jiang, M. Chowdhury and R. Doss, "Intrusion Detection Scheme With Dimensionality Reduction in Next Generation Networks," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 965-979, 2023, doi: 10.1109/TIFS.2022.3233777.

[8] M. Shafi, R. K. Jha and S. Jain, "LGTBIDS: Layer-Wise Graph Theory-Based Intrusion Detection System in Beyond 5G," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 658-671, March 2023, doi: 10.1109/TNSM.2022.3197921.

[9] Z. Zhao, Q. Du and H. Song, "Traffic Load Learning Towards Early Detection of Intrusion in Industrial mMTC Networks," in IEEE Transactions on Industrial Informatics, vol. 19, no. 7, pp. 8441-8451, July 2023, doi: 10.1109/TII.2022.3218722.

[10] H. Whitworth, S. Al-Rubaye, A. Tsourdos and J. Jiggins, "5G Aviation Networks Using Novel AI Approach for DDoS Detection," in IEEE Access, vol. 11, pp. 77518-77542, 2023, doi: 10.1109/ACCESS.2023.3296311.

[11] D. D. N. Nguyen, K. Sood, Y. Xiang, L. Gao, L. Chi and S. Yu, "Toward IoT Node Authentication Mechanism in Next Generation Networks," in IEEE Internet of Things Journal, vol. 10, no. 15, pp. 13333-13341, 1 Aug.1, 2023, doi: 10.1109/JIOT.2023.3262822.

[12] T. Ye, G. Li, I. Ahmad, C. Zhang, X. Lin and J. Li, "FLAG: Few-Shot Latent Dirichlet Generative Learning for Semantic-Aware Traffic Detection," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 73-88, March 2022, doi: 10.1109/TNSM.2021.3131266.

[13] Y. He, M. Kong, C. Du, D. Yao and M. Yu, "Communication Security Analysis of Intelligent Transportation System Using 5G Internet of Things From the Perspective of Big Data," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2199-2207, Feb. 2023, doi: 10.1109/TITS.2022.3141788.

[14] M. Lefoane, I. Ghafir, S. Kabir and I. -U. Awan, "Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 921-929, Jan. 2023, doi: 10.1109/TII.2022.3192044.

[15] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420, DOI: 10.1080/19361610.2021.2002118

[16] Satyanarayana, P., Diwakar, G., Subbayamma, B. V., Phani Sai Kumar, N. V., Arun, M., & Gopalakrishnan, S. (2023). Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications. Computer Communications, 198, 262–281. https://doi.org/10.1016/j.comcom.2022.12.006