# Deep Learning Based Network Intrusion Detection for Industrial Internet of Things

Fabliha Bushra Islam, Rubina Akter, Dong-Seong Kim and Jae-Min Lee
Networked Systems Lab., IT Convergence Engineering
Kumoh National Institute of Technology
Gumi, Gyeongbuk 39177, Korea
Email:{fablihabushra,rubina2836,dskim,ljmpaul}@kumoh.ac.kr

***Abstract*— This paper represents a deep learning model dependent on anomaly detection techniques for malicious discovery in network traffic configuration assembled from TCP/IP packets. Four Artificial Neural Network (ANN) model variations were compared using a public dataset called NSL-KDD. The ANN was implemented using R-programming, where in, input layer, hidden layer and output layer were manipulated to select the best model with optimal performance in terms of reduced Mean Absolute Percentage Error (MAPE). The experimental results illustrate that model 1 outperformed other ANN models with an accuracy of 96.74%. The conclusion of this paper is that ANN model offers a good performance for malicious detection. However, caution should be on design of ANN models as we observed that layer numbers have impact on their accuracy. This proposed ANN model can be effective for Industrial IoT networks, and smart factories management to restrain future malicious attacks.**

***Index Terms*— Artificial Neural Network (ANN), Industrial Internet of Things (IoT), Mean Absolute Percentage Error (MAPE), R-programming.**

## I. INTRODUCTION

Internet of things (IoT) has enforced a significant role in modernization, leads to the rapid growth of development in wireless and communication sectors. It introduces an emerging solution where several embedded devices also known as things are connected to the Internet in a way that using these interfaces, people can easily communicate with others and things. With these tremendous recognition, these frameworks are proclaimed and enormously applied in various sectors such as smart home, smart factories, manufacturing, and industrial schemes [1]. A developing class of IoT empowered modern creation structures is known as the Industrial IoT (IIoT) that, when received effectively, gives extensive viability and economic advantages to system establishment, practicality, dependability, adaptability, and interoperability [2]. However, IoT engaged mechanization systems have uncovered industrial and habitation environments to innumerable new dangers [3]. Malicious activities originate hideous situations both in security and wireless communication interruption. Attackers can easily thieve or erase information from computers as well as network structures shortly which promoting to involve in cyber war. There are several attacks mentioned such as port-scan, network scanning, address-sweep, Man-in-the-Middle (MitM), port-sweep, vulnerability scanning, data theft and botnet attacks. On May 2020, Taiwan state-owned petroleum company CPC Corporation and Formosa Petrochemical Corporation (FPCC), have both been experienced cyber-attacks by ransomware. Swvl, a transport booking application, situated in Cairo, has been confronted security issues by unauthorized access to its IT foundation in July 2020. These examples signify the vulnerabilities of network security consequences. Due to large Diversity of IoT devices and unsecured Machine-to-Machine (M2M), Machine-to-People (M2P) connections, a large number of information get affected and stolen by hackers which violates the privacy and usage of device safely.

To detect malicious activities and achieving reliability in network traffic, Intrusion Detection System (IDS) is viewed as powerful or precise in recognizing interruptions when it simultaneously accomplishes high detection accuracy and low false positive rates [4]. Anomaly detection systems (ADS) has brought a new revolution in research world. Deep Learning approach can easily contemplate anomalous behaviour of network packets both for labeled and unlabeled data. Some of renowned algorithms include Random Forest (RF), Support Vector Machine (SVM), K-Nearest-Neighbors (KNN), Fuzzy interpolation, Multi-Layered Perceptions (MLP), Artificial neural network (ANN), and other machine learning algorithms have been utilized for detection of malicious discovery [3],[5]. A set of algorithms that make artificial intelligence something new through preparing is called ANN. It is similar to the human brain system and imitates the learning arrangement of the human mind. Today ANN is applying for detecting unauthorized activities in network traffic. In [6], authors proposed ANN based threat discovery to solve the verification issues using UNSW-15 dataset in IoT condition and accomplished 84 percent detection accuracy. Taher et al. [7] represented two ANN models utilizing NSL-KDD dataset to discover identification accuracy of 94.02% and 83.68%, respectively.

In this paper, we apply an ANN model to track out malicious event and system performance for higher detection accuracy. The significant contributions of this paper are summarized as follow:

- An effective anomaly detection technique for network intrusion detection using ANN in an R-programming environment.

• A consecutive training and attack prediction process is conducted to learn network behaviour and analyzing malicious occurrence, utilizing dataset NSL-KDD [8].

The rest of the paper is detailed as: following this Section I, a system model of the proposed idea requirements is described in Section II, where we focus on IIoT scenario with brief identification and describe the technique of detecting malicious activity applying ANN. Results and discussions of the findings are presented Section III and paper is concluded in Section IV.

## II. System Model

In IIoT environments, a number of gadgets can be connected. For instance, cell phones, smart light, vehicles, surveillance cameras, TV, PC, and different gadgets can be associated in smart factories scenarios. In Fig. 1, we illustrate a IIoT environment to engage ANN models analyzing malicious affected network traffic. The information from these IoT devices passes through gateways such as base stations or routers following TCP/IP protocols. In case of mixing with malicious activities, network traffic got interrupted with malware or ransomware, a possibility of stealing and erasing significant information by attackers. We apply four ANN models for identifying interruption.

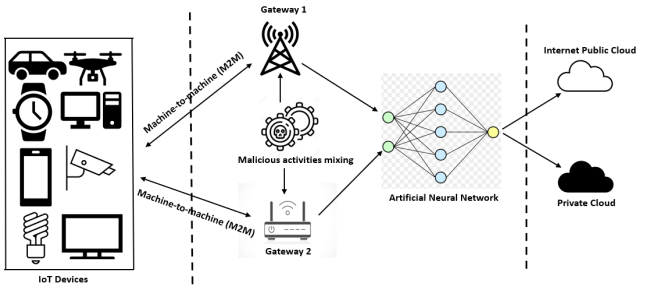


Fig. 1. Applying ANN models in network traffic to analyze intrusion in IIoT scenarios

ANN is a machine learning approach utilized for classification as well as regression. It comprises of three layers namely input, hidden, and output layer. The data passed from IoT gateways is called an input layer as signals to the hidden layer. The hidden layer applies the activation function with the assistance of input signal. The activation function changes over the input signal to an output signal. In Fig. 2, we display our proposed ANN2 model.

The configuration or parameters of the four ANN models for analyzing network traffic, the model's layers are shown in Table I.

TABLE I
ANN MODELS FOR ANALYZING NETWORK TRAFFIC

| Model No. | Input Layer | Hidden Layer | Output Layer |
|---|---|---|---|
| ANN1 | 10 | Input Layer*2 | 5 |
| ANN2 | 5 | 10 | 10 |
| ANN3 | 5 | 15 | 5 |
| ANN4 | 20 | 25 | 10 |

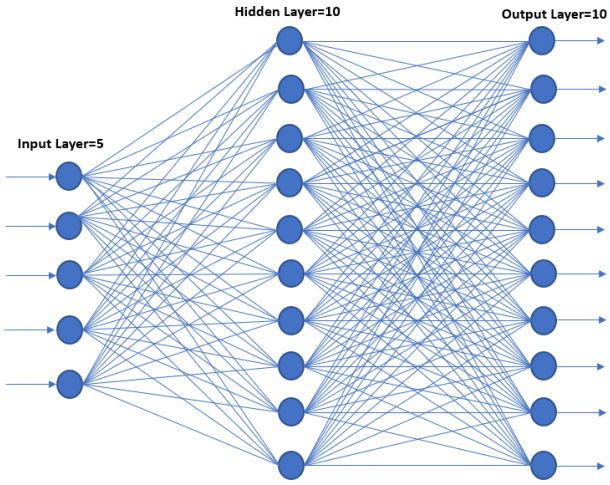


Fig. 2. The architecture of ANN2 model

This paper used the NSL-KDD dataset, an improved form of the KDD CUP 99 which tackled the problems of KDD CUP 99 by eliminating its excess records and choosing quantities from it with respect to their rates. There are five classes, to be specific, Probing, DoS, User to Root (U2R), Remote to Local (R2L), and Normal. This dataset comprised of four sub data sets:

- KDDTest+,
- KDDTest-21,
- KDDTrain+,
- 20Percent KDDTrain+.

A gradual chart of number of attack records is showed for NSL-KDD dataset.

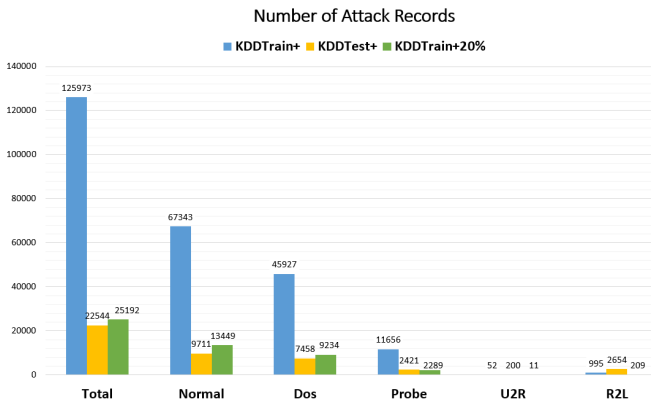


Fig. 3. Attacks visualization in NSL-kDD.

In the performance evaluation, we obtain small training set and apply in the proposed four models to observe the Mean Absolute Percentage Error (MAPE) and find detection accuracy.

## III. Performance Evaluation

The MAPE is a proportion of predicting accuracy of a determining strategy and a loss function for model evaluation, regression problems in machine learning. It estimates

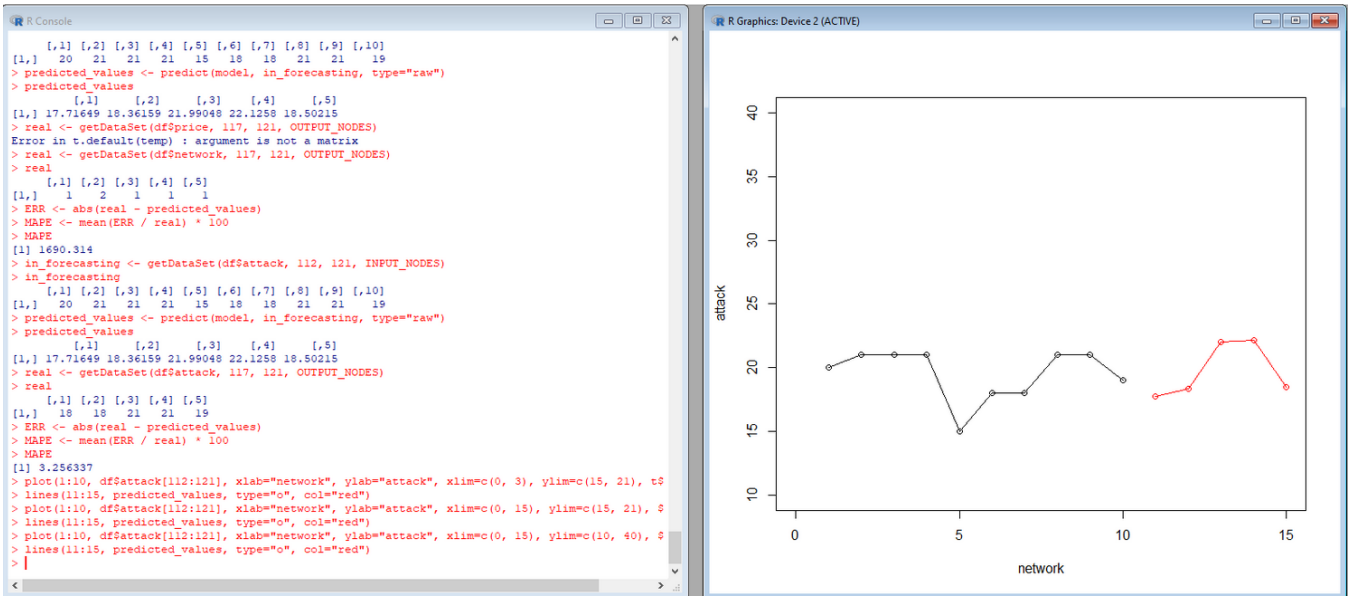


Fig. 4. The MAPE value of NSL-KDD dataset for ANN1 model.

exactness and the size of error in percentage terms. It is defined as:

$$MAPE = \frac{1}{m}\sum_{i=1}^{m}\frac{|Real_i - Predict_i|}{Real_i} * 100\% \quad (1)$$

Where, $Real_i$ the actual value and $Predict_i$ is the forecasting value.

As ANN has been proven to be very compelling at predicting. We propose to achieve MAPE for these four models employing ANN and represent accuracy. The accuracy from MAPE is:

$$Accuracy = max(0, 1 - MAPE) \quad (2)$$

We evaluated dataset in terms of our proposed ANN models in R programing. We observed the MAPE results and found detection accuracy for each model.

The accuracy rates show different results for these models. It depends on the number of layers used in input, hidden and output. Table II illustrates MAPE values and accuracy for comparison in terms of layer numbers.

TABLE II
MAPE AND ACCURACY RESULTS FOR FOUR ANN MODELS.

| Model No. | MAPE | Accuracy |
|---|---|---|
| ANN1 | 3.256337 | 96.743663 |
| ANN2 | 8.75654 | 91.243346 |
| ANN3 | 6.983475 | 93.016525 |
| ANN4 | 16.85773 | 83.14227 |

For the first model ANN1, the input layer number is greater than output and for hidden layer, we utilized two times number of Input layer and we get 96.74% accuracy of detecting intrusion, shown in Fig. 4. In case of ANN2, the accuracy rate is lower than ANN1, 91.24%, where number of Input, hidden and output layers are 5, 10 and 10, respectively. By increasing hidden layer to 15 and decreasing input layer to 5, we improved accuracy 93.02% percent for ANN3 model. However, we experienced accuracy reduction of 83.14% in ANN4, by increasing all the layer numbers 20 for input, 25 for hidden and 10 for output, separately. The effect of layer numbers can influence the accuracy level. In [9], authors showed by increasing the size of the batch, the performance of Convolutional Neural Network is going to be deduced.

## IV. CONCLUSION

In this paper, we introduced a deep learning approach in R programming environment to discover malicious interruption in the network traffic by evaluating ANN in a public dataset. We acquired detection accuracy by solving MAPE. We approached four ANN models to compare accuracy rate for detection and observed the first model accomplished the most noteworthy every one of them. This proposal can be useful for choosing model layers efficiently as well as can be effective for intrusion recognition in IIoT scenarios, smart factories, and smart city paradigm.

## ACKNOWLEDGMENT

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2018R1A6A1A03024003).

## REFERENCES

[1] C. I. Nwakanma, W. Nwadiugwu, J. M. Lee and D. S. Kim, “Real-Time Validation Scheme using Blockchain Technology for Industrial IoT,” in Proceedings of *2019 Korean Institute of Communications and Information Sciences Summer Conference, Jeju Island*, Korea pp. 379-382, June 19-21, 2019.

[2] N. B. Long, H. Tran-Dang and D. Kim, "Energy-Aware Real-Time Routing for Large-Scale Industrial Internet of Things," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2190-2199, June 2018.

[3] ] I. Hafeez, M. Antikainen, A. Y. Ding and S. Tarkoma, "IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge," in *IEEE Transactions on Network and Service Management,* vol. 17, no. 1, pp. 45-59, March 2020.

[4] M. A. Hawawreh, N. Moustafa and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models", in *Journal of Information Security and Applications,* vol. 41, pp. 1-11, August 2018.

[5] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," in *IEEE Access,* vol. 7, pp. 38597-38607, 2019.

[6] S. Hanif, T. Ilyas and M. Zeeshan, "Intrusion Detection In IoT Using Artificial Neural Networks On UNSW-15 Dataset," in Proceeding of *2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT),* Charlotte, NC, USA, 2019, pp. 152-156, 2019.

[7] K. A. Taher, B. Mohammed Yasin Jisan and M. M. Rahman, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection," in Procceding of *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST),* Dhaka, Bangladesh, pp. 643-646, 2019

[8] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications,* Ottawa, ON, pp. 1-6, 2009.

[9] I. Kandel, M. Castelli, "The effect of batch size on the generalizability of the convolutional neural networks on a histopathology dataset," in *ICT Express,* in Press, Corrected Proof, Available online May 2020.