AN EFFICIENT MODEL FOR DETECTING AND IDENTIFYING CYBER ATTACKS IN WIRELESS NETWORKS

S. Gayathri[1], P. Abirami[2], K.Bakiyalakshmi[3]

[1]Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College Tamil Nadu, India
[2,3]Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India

---***---

Abstract - *All communications that occur within this technological era use various types of networks for transmission of messages. Numerous amount of information is being passed using the networks and it is very essential to protect these networks from cyber attacks. Nowadays many transactions are done using the wireless medium as the use of wired transmissions involves numerous expenditures in installation and maintenance. Use of wireless medium has given rise to many cyber attacks in the network which needs to be always monitored. Numerous researcher has been working on building a Network Intrusion Detection System (NIDS) in order to detect any cyber attacks in the network. In this paper, we have designed a model that is able to detect any malicious behaviors in the wireless network using deep learning approaches. The model is designed in such a way that it is able to do feature selection and classification for any given network. The dataset used for evaluating the parameters of the proposed NIDS was NSL KDD CUP. Some of the parameters used for finding the efficiency of the system was the detection rate, recall, precision.*

***Key Words*: Network, Security, Cyber Attacks, Deep Learning, NIDS, Feature Selection.**

1. INTRODUCTION

Nodes transmitting data in the form of signals between one another in a network without any wired connections are popularly called as Wireless Networks. These networks are majorly implemented in the real world to reduce the number of wires that connect the various nodes in the network. The node could be anything, an antenna or a base station that frequently communicates with other nodes in the network by sending or receiving signals. Broadcasting is one of the best characteristics of wireless networks where the data is echoed to the entire nodes in the network unless like in the traditional network where only the receiver will be able to receive the data. It consists of several applications and security is provided to all the applications that are used for communication with one another. There are various challenges and security attacks that encountered in a wireless network[1,2,3,4]. To avoid these numerous techniques and routing protocols[5,6,7] are designed for efficiently directing the packets from one node to another within the network. Numerous intrusion detection systems are also designed by various researchers to detect if there are any kind of cyber attacks or malicious activities that are occurring within the network.

The growth of Artificial Intelligence has given birth to many new technologies out of which the popular ones are being Machine Learning Approaches and Deep Learning Techniques. Use of ANNs is widely called as Deep Learning Approaches as the neural network learns each and every layer very deeply and uses the output of a layer as the input of the next layer. ANNs are information processing structures that can solve any problem through learned examples rather than pre-specified algorithms [8]. In this paper, we have proposed a framework for identifying and detecting various cyber attacks in a wireless network using machine learning techniques. The proposed system is evaluated on various parameters and is observed to perform better than the existing systems. The rest of the section is as follows: Section II consists of Literature Survey, section III consists of the methodology used in the paper and section III consists of various results obtained. The paper is concluded in the last by mentioning the relevant future works that could be applied or added to the proposed work.

2. RELATED WORKS

Wireless communication is one among the most vibrantly used communication technique[9] designed in such a way that it increases the reliability of the air interface[10]. Various researchers have developed numerous intrusion detection systems using various technologies. There are numerous attacks that occur in a network for which these NIDS are proposed [11]. Security is one of the important aspects that need to study in all the possible directions as the attack may be from anywhere [12]. Some attacks have been studied where the attacks try to attack the estimation and control systems where a number of sensors and actuators are deployed [13]. Detection of integrity attacks occurring in a network is identified by a model developed in [14]. The possible types of attacks in replay attacks are discussed in [15]. A topology was deployed for identifying all the possible attacks but it gained to provide the security to the network as discussed in [16] and [17]. In [18], Nathone Shone has developed an Intrusion Detection model that efficiently identifies all the malicious behavior of the network. The model is designed in such a way that the model makes use of Non - Symmetric Auto encoder. The system makes use of a Random forest in order to improve the total efficiency of the network. The system is inefficient in reducing the dimensionality of the data and was compared with Deep Belief Networks which yielded a better accuracy.

3. PROPOSED APPROACH

The system proposed in the following research paper makes use of deep learning techniques where it makes use of Random Forest Classifier. The network consists of various layers such as the input layer, the hidden layer, and the output layer. These layers are responsible for feature extraction. Features of the network are trained to the classifier of when a network is cyber attacked and when it is not. Based on the previous training given to the classifier, it is able to identify when a new behavior is observed in the network and alerts the system admin about the malicious behavior of the network. In Fig. 1 the architecture of the proposed methodology is given. We can see numerous layers that are responsible for feature extraction in the network. All the layers extract the features and further give the summation of the entire network to the classifier which then classifies the behavior of the network. The Random Classifier s used widely in order to make the weak learners as strong learners. The forest that is built consists of numerous weak learners tree. It is mainly used to increase the levels of bias in order to make few corrections and modifications to the network.

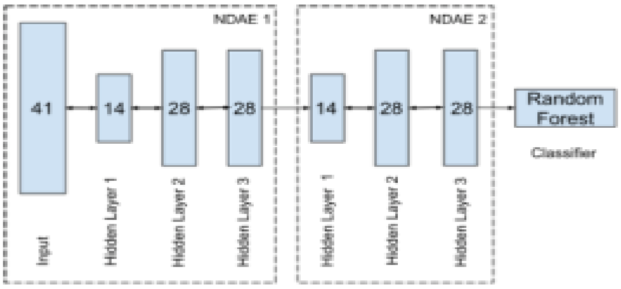


Fig. 1 Block Diagram of the Proposed System

The autoencoder is used in the proposed method. It is a neural network that follows unsupervised learning in nature. The neural network is used to learn all the available parameters of the network in order to build a required input of the system.

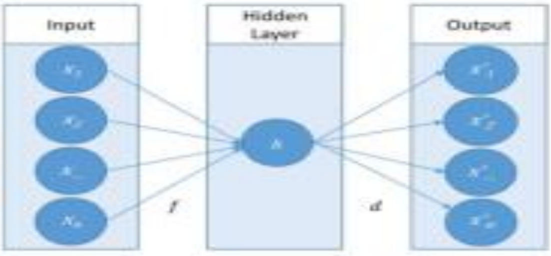
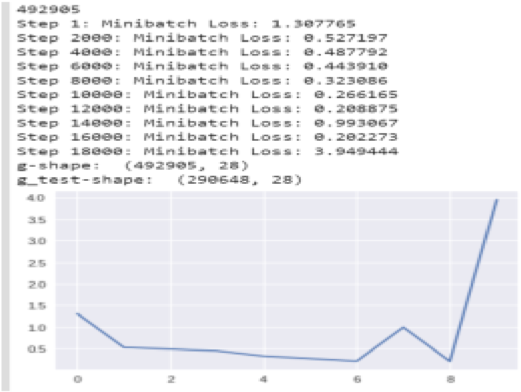


Fig. 2 Sample Auto Encoder

The entire generalization of the network is obtained using backpropagation algorithm. The autoencoder is combined with stack NDAE where each and every input vector is mapped step by step with its latent representations. The sigmoid activation function is also used for generalizing the system.

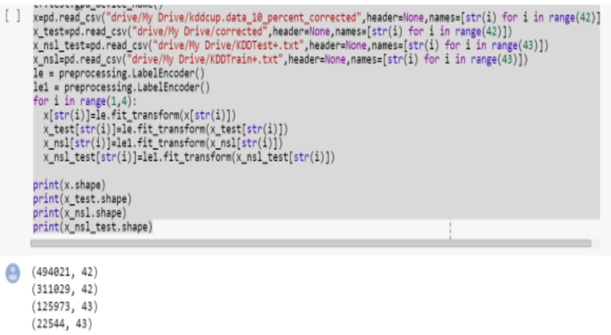
4. EXPERIMENTAL RESULTS

The experimental results were done on various datasets. Some of the prominently used datasets are KDD Cup '99 and NSL-KDD dataset. These datasets were used as they were proposed as one of the prominent datasets to be used as a benchmark in various literature. The experiment was performed in MAT Lab R2017b where a Random Forest classifier was used to train the network with all the behavior that could happen within the network. As the model was trained it was able to efficiently identify any malicious activities occurring within the network. Various parameters were used for evaluating the parameters of the model. In Fig. 3, the error loss of the autoencoder is depicted performed using NSL-KDD dataset.



```
492905
Step 1: Minibatch Loss: 1.307765
Step 2000: Minibatch Loss: 0.527197
Step 4000: Minibatch Loss: 0.487792
Step 6000: Minibatch Loss: 0.443910
Step 8000: Minibatch Loss: 0.323086
Step 10000: Minibatch Loss: 0.266165
Step 12000: Minibatch Loss: 0.208875
Step 14000: Minibatch Loss: 0.993067
Step 16000: Minibatch Loss: 0.202273
Step 18000: Minibatch Loss: 3.949444
g-shape:  (492905, 28)
g_test-shape:  (290648, 28)
```

Fig. 3 Error **loss of First Non-Symmetric Deep Auto Encoder (NSL -KDD)**



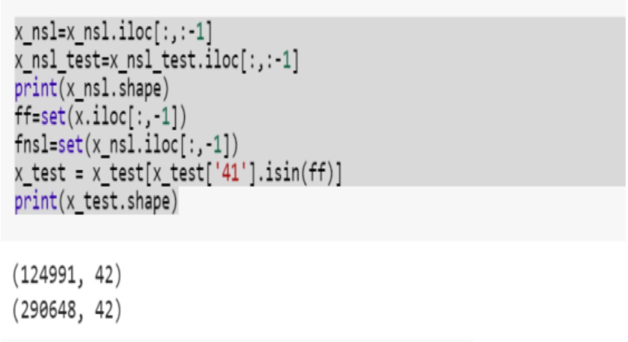
```
x=pd.read_csv("drive/My Drive/kddcup.data_10_percent_corrected",header=None,names=[str(i) for i in range(42)]
x_test=pd.read_csv("drive/My Drive/corrected",header=None,names=[str(i) for i in range(42)])
x_nsl_test=pd.read_csv("drive/My Drive/KDDTest+.txt",header=None,names=[str(i) for i in range(43)])
x_nsl=pd.read_csv("drive/My Drive/KDDTrain+.txt",header=None,names=[str(i) for i in range(43)])
le = preprocessing.LabelEncoder()
le1 = preprocessing.LabelEncoder()
for i in range(1,4):
  x[str(i)]=le.fit_transform(x[str(i)])
  x_test[str(i)]=le.fit_transform(x_test[str(i)])
  x_nsl[str(i)]=le1.fit_transform(x_nsl[str(i)])
  x_nsl_test[str(i)]=le1.fit_transform(x_nsl_test[str(i)])

print(x.shape)
print(x_test.shape)
print(x_nsl.shape)
print(x_nsl_test.shape)
```

```
(494021, 42)
(311029, 42)
(125973, 43)
(22544, 43)
```

Fig. 4 Input train and Test Dataset dimension

The train and test dataset are used to train the classifier and also to test it. Various dimensions need to be given in order to make the classifier to automatically select the features from the dataset.

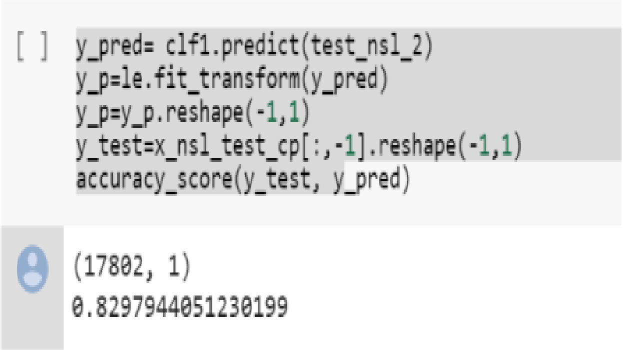


```
x_nsl=x_nsl.iloc[:,:-1]
x_nsl_test=x_nsl_test.iloc[:,:-1]
print(x_nsl.shape)
ff=set(x.iloc[:,-1])
fnsl=set(x_nsl.iloc[:,-1])
x_test = x_test[x_test['41'].isin(ff)]
print(x_test.shape)

(124991, 42)
(290648, 42)
```

Fig. 5 Identifying Class labels and removing Low-Frequency attacks.

The low-frequency attacks are identified and removed from the network as shown in Fig. 5. This is done by making the necessary class labels within the network that could help to identify the cyber attacks. The classification accuracy of the KDD CUP dataset obtained by using the deep learning technique is depicted in Fig. 4. The classification accuracy of about 82% is obtained where the system is able to correctly detect the malicious activities or cyber attacks in the system.



```
[ ]  y_pred= clf1.predict(test_nsl_2)
     y_p=le.fit_transform(y_pred)
     y_p=y_p.reshape(-1,1)
     y_test=x_nsl_test_cp[:,-1].reshape(-1,1)
     accuracy_score(y_test, y_pred)

     (17802, 1)
     0.8297944051230199
```

Fig. 4 Classification Accuracy of KDD CUP dataset

5. CONCLUSION

Communication is one of the most important aspects in this technical era. All the means of communications occur through some or the other networking devices that tend to form a network. The network could be either wired or wireless. As numerous amount of information is being transmitted via this network it needs to be protected against any kind of cyber attacks. In this paper, we have proposed an Intrusion Detection System that is able to efficiently identify the malicious behaviors of the network is present. The identification id sonde using deep learning techniques and by making use of the Random forest Classifier. The efficiency of the system is observed by making use of KDD CUP dataset. The system has produced an accuracy level of about 82% and is proved to be efficient when compared to other traditional systems..

REFERENCES

[1] G. Sabeena Gnanaselvi, T.V.Ananthan, "*An Analysis of Applications, Challenges and Security Attacks in MANET*", International Journal of Computer Sciences and Engineering, Vol.6, Issue.5, pp.941-947, 2018.

[2] Larsen, E., 2012. TCP in MANETs–challenges and Solutions. FFI-Rapport-2012/01514.

[3] Daly, E.M. and Haahr, M., 2010. The challenges of disconnected delay-tolerant MANETs. Ad Hoc Networks, 8(2), pp.241-250.

[4] Ding, S., 2008. A survey on integrating MANETs with the Internet: Challenges and designs. Computer Communications, 31(14), pp.3537-3551.

[5] Abolhasan, M., Wysocki, T. and Dutkiewicz, E., 2004. A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1), pp.1-22.

[6] Hong, X., Xu, K. and Gerla, M., 2002. Scalable routing protocols for mobile ad hoc networks. IEEE Network, 16(4), pp.11-21.

[7] Gupta, A.K., Sadawarti, H. and Verma, A.K., 2010. Performance analysis of AODV, DSR & TORA routing protocols. International Journal of Engineering and Technology, 2(2), p.226.

[8] Md. Badrul Alam Miah, Mohammad Abu Tousuf, Detection of Lung Cancer from CT Image Using Image Processing and Neural Network, IEEE, In Proceedings of 2nd Int'l Conference on Electrical Engineering and Information & Communication Technology, 2015.

[9] Tse, D. and Viswanath, P., 2005. Fundamentals of wireless communication. Cambridge university press.

[10] Akkaya, K. and Younis, M., 2005. A survey on routing protocols for wireless sensor networks. Ad hoc networks, 3(3), pp.325-349.

[11] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," Automatica, vol. 51, pp. 135–148, Jan. 2015.

[12] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Trans. Autom. Control, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[13] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," IEEE Trans. Control Syst. Technol., vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[14] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," IEEE Trans. Autom. Control, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[15] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay

attacks," IEEE Trans. Autom. Control, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[16] A. W. Al-Dabbagh and T. Chen, "Modelling and control of wireless networked control systems: A fixed structure approach," in Proc. IEEE Conf. Control Appl., Sydney, NSW, Australia, Sep. 2015, pp. 1051–1056.

[17] A. W. Al-Dabbagh and T. Chen, "Design considerations for wireless networked control systems," IEEE Trans. Ind. Electron., vol. 63, no. 9, pp. 5547–5557, Sep. 2016.

[18] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50.