Journal of Positive Sciences (JPS) **eISSN: 2582-9351, https://positive-sciences.com** **JPS. 2022 Sep; 2(5): 5-10**

Article info **Research Article**
Received on: 01.09.2022
Accepted on: 28.09.2022
Published on: 30.09.2022
doi: https://doi.org/10.52688/ASP54737

Denial of Service Attack Detection in Adhoc Wireless Network Using Transfer Learning Methods

Adel M. Salman [1, *]

[1] Baghdad College of Economic Sciences University, Baghdad, Iraq

[*] adelmsk63@baghdadcollege.edu.iq

ABSTRACT

Deep learning is designed for enhancement of security over the networks using software only. Deployment of Deep Learning technology implies implementation of software based network between two parties (or more) over the bigger physical network. Deep Learning technology can be realized in many applications such as internet (i.e. web applications), intranet (local/private network made between particular candidates for preforming a specific task where this network is separated from the public internet network). The development of internet and computer technologies have motivated the security engineers to design virtual network that can be operated over any physical network and can be used by any number of subscribers to protect the connection privacy. This paper is illustrating the Deep Learning technology enhancement overview and details. Big data can be collected from network monitoring system and hence can be used to train the transfer learning by recurrent neural network for attack detection. The recurrent neural network is reported higher accuracy of attack detection in adhoc in 111 seconds of training time with 98.2 percent of detection accuracy.

Keywords: Deep learning, ANN, deep learning, prediction, networks attacks

INTRODUCTION

As an example of Deep Learning is the banking applications. Since all the banking activates (at least those related to the bank clients) are made over the internet and folded under the so-called internet banking [1, 2]. The internet banking is susceptible for malicious activities since it is operating over a public network like internet. Banks have tried many (methods) to protect the online transactions [3]. Those methods are categorized into several groups and can be generalized according to their existence. Therefore, there are some security and precautions implemented at the end users handset to ensure that only the authorized person can access to the account, this implemented security features on the banking applications such as face recognition [4,5], finger impression, eye recognition, etc. As well as the network can be upgraded to accommodate a safe connection between the user (client) and the bank server. The network upgrading is the most important step to ensure safety of connection and prevent malicious activities. Banks are adopting a virtual network that encapsulate the active transaction. Deep Learning is established for tunneling the connections over the public network where no other candidate out of the DEEP LEARNING can participate in the connections without prior permission. This kind of protection has proven good performance in protecting connections over bigger networks including internet. Network includes various types of activities which may demand specific requirements of bandwidth and routing process. Some applications may demand high throughput and others may work in real-time bases where minimum delay should be there for packet transmission. Deep Learning should be made in (cooperation) with other network configurations concerned with time delay, throughput. Network security and network performance should be in the same level of interest for the network planners [6, 7].

Deep Learning is made to secure the connection between two terminals in by virtually separating that connection from the other connections in the network. Network may include too many request of connection as demonstrated in the preceding sections, the flood of requests might be sent from malicious node. Upon of receiving of the malicious request, the receiver might lose the data or suffer from long queuing time which may lead to receiver complete fail [8, 9].

***Corresponding author**
Adel M. Salman,
Baghdad College of Economic Sciences University, Baghdad, Iraq
e-mail: adelmsk63@baghdadcollege.edu.iq

OBJECTIVES

This work is focusing on monitoring data analyzing using ANN. However, this big data can be referred from the monitoring system and be used for training the classifier where attack can be automatically predicted.

a) Providing a solution for other network performance metrics such as throughput, time delay and packet loses in the presence of the Deep Learning. In other word, learn through the impacts of the Deep Learning on the other performance metrics apart from the security enhancement.

b) Implementation of the said network with number of host nodes using the network simulator version II software which can provide the real-life environments of computer network and host nodes. It also is capable to keep track of the network packets status in each seconds of the simulation time where, a complete idea of the network performance metrics can be derived.

c) Development of smart alternative of malware attacks detection program using the transfer learning by recurrent neural network which may be used to learn for various type of computers attacks behaviors so that it can prevent the attacks by detecting them in fast and reliable way. This can be done using the Matlab programming language.

LITERATURE SURVEY

Due to the DEEP LEARNING 's particular importance in preserving the privacy of data transmitted over public networks, extensive research has been done to improve its functionality. Secure Shell and Skype are the only two well-known service providers to have included Deep Learning technology into their infrastructures [7]. The major objective of this study is to choose the optimal protocol for various network activities because understanding protocols is crucial for accomplishing Deep Learning security goals. Conventional DEEP LEARNING s, on the other hand, have shown to be crucial for controlling internet network security and privacy. The effectiveness of conventional security has been reassessed in light of the increasing internet traffic brought on by the most recent data revolution. Because of the increasing network traffic and frequent payloads in network nodes, traditional security programmes are unable to keep up with the data threats.

More types of data, such as multimedia traffic, are now taken into consideration when constructing Deep Learning as a result of the variety of network traffic that is already available, such as internet protocol traffic and relay traffic [8]. The internet payload is significantly impacted by voice over IP. In this study, a Deep Learning 's performance was assessed while taking into account the significance of its capacity to handle various data types. According to the most recent survey, major retail companies globally are becoming more interested in Deep Learning s due to their simplicity of use, low cost, and high performance. While some of these applications require incredibly low latency in real-time data transmission, others require enormous capacity networks that can transmit high-quality data without packet loss. Network service providers need to use a new approach in order to satisfy these objectives over Deep Learning. According to this study, a central switch unit should incorporate a range of switch types with labels marking them for different types of traffic. Figure 1 depicts a network topology of this kind.

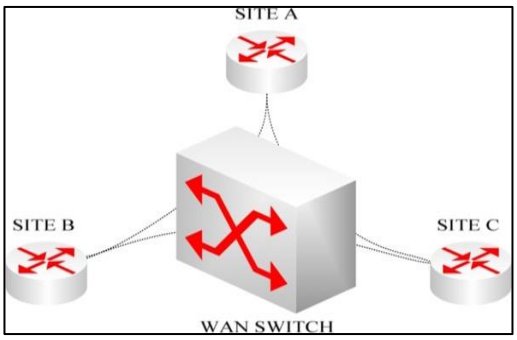

Figure 1: Wide area network topology for Deep Learning structure.

To maintain a high level of security over intranet networks like the college network, school network, and inter-building network, a novel study has been proposed [9, 10]. Recently, researchers tested the viability of incorporating the Deep Learning into the school's network architecture. In this study, Deep Learning s are built using a unique way as opposed to the conventional software defined Deep Learning method. The authors recommended integrating the Deep Learning into the school's network architecture using microcontroller chips. Since there is no chance that this link might be altered or disrupted by virus activity, it would allow secure data transmission between designated pairs only and a high level of security on intranet networks. Implementing such a network is slightly more expensive than using a standard software-defined Deep Learning.

*Corresponding author
Adel M. Salman,
Baghdad College of Economic Sciences University, Baghdad, Iraq
e-mail: adelmsk63@baghdadcollege.edu.iq

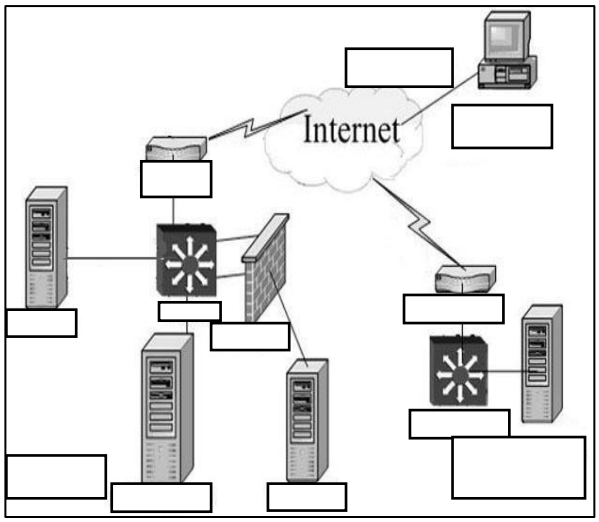

Figure 2: Intranet Deep Learning structure with hardware defined network using a microcontroller.

Hardware gateways are depicted in Figure 2 as an alternative to configuring the Deep Learning. The Deep Learning 's features can be implemented using specialised microcontrollers, which can then be incorporated into network architecture to provide dependable secure connections.

Due to their ambition to combine into a single organisation, universities and other educational institutions are having difficulty uniting their networks under a single, central network [11, 12]. This study highlights both the risk of security breaches and the difficulty of combining numerous networks at once. The authors recommended using IP Security protocol, one of the most dependable Deep Learning protocols, to ensure security during data transfer across the various blocks of the larger network. Without delay, the IP security protocol cannot function at high speeds. Figure 3 displays the suggested network's structure as it was used in this experiment. The trial was carried out on a campus where a network connecting many universities is intended.

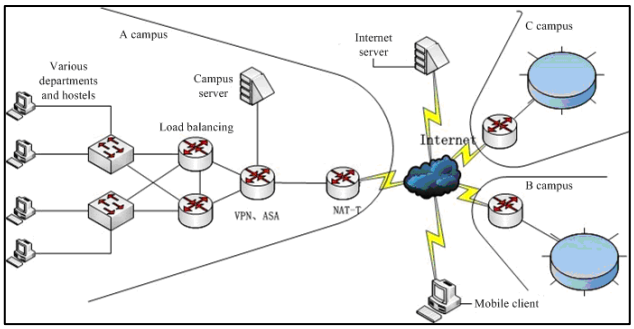

Figure 3: Interconnection of several colleges at one campus using the concept of Deep Learning.

METHODOLOGY

The influence Deep Learning on other network performance metrics should be studied for achieving robust network. Two models are implemented using the Network Simulator (Version 2) in order to understand the impact of Deep Learning on the network performance.

*Corresponding author
Adel M. Salman,
Baghdad College of Economic Sciences University, Baghdad, Iraq
e-mail: adelmsk63@baghdadcollege.edu.iq

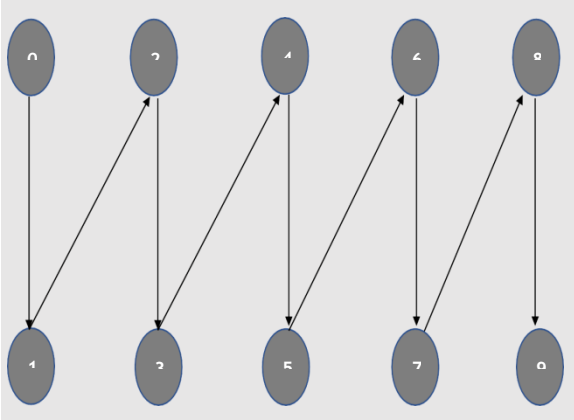

Figure 4: Nodes connected in Manhattan grid topology without Deep Learning

In the following models, network is implemented using ten nodes are distributed in form of Manhattan grid as shown in Figure 4. In each of the models mentioned below, network is examined by realizing performance metrics throughput and time delay, ultimately results from both proposed models are compared.

With same network topology illustrated in first model and demonstrated in Figure 4, new model is made by applying a Deep Learning over connection of pair (node 2 and node 3) in the network for each protocol (CBR, HTTP, and FTP).

Deep Learning is made to secure the connection between two terminals in by virtually separating that connection from the other connections in the network. Network may include too many request of connection as demonstrated in the preceding sections, the flood of requests might be sent from malicious node. Upon of receiving of the malicious request, the receiver might lose the data or suffer from long queuing time which may lead to receiver complete fail.

Virtual private connect doing nothing but securing particular connection on the network by applying tunnel on it where no other connection can sense that. Therefore, connection under Deep Learning might not be visible for other connections in the network. However, other connections can join the Deep Learning connect by pre-approval acquisition from the concern nodes. Network running with Deep Learning connect might not suffer from malicious activities in normal situations. Furthermore, the Deep Learning is also susceptible of malicious activities as the ability of software is developed and new methods are established for snooping on the networks.

In order to save the safeguard of the network against any malicious attack, a Recurrent neural network (RNN) shown in Figure 5 is utilized to develop a smart attack prevention paradigm. This paradigm may predict occurrence of attack depending of the attitude of each attack before it is actually take place and this is considered as a model of employing the RNN for predicting the malicious activities.

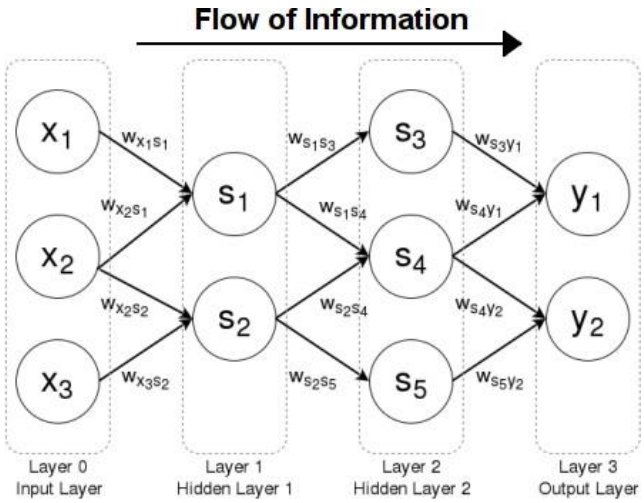

Figure 5: Structure of feed forward neural network

*Corresponding author
Adel M. Salman,
Baghdad College of Economic Sciences University, Baghdad, Iraq
e-mail: adelmsk63@baghdadcollege.edu.iq

OUTCOMES

Model with the configurations stated at Table 5 is implemented for adhoc network security enhancement. The detailed parameters are as below:

Parameter	Value
The count of Hidden layers	100
The count of Output layer	1
The count of Input layers	1
Algorithm of training	LM
Performance measure	MSE and Time
Targeted performance	1.088 e-100000

Therefore, the following results were obtained:

Algorithm	Time (seconds)	Accuracy
DNN	143	88.21
LSTM	132	78.0
CNN	187	88.15
RNN*	111	98.2

CONCLUSION

Computer networks such as internet are flooded with data from unlimited resources that aim to exchange data into global. This promotes security violence in the network epically after the wide deployment of smart software and computer applications. Hence, security is integral part for any organization or any individual who is willing to share data through network. Deep Learning technology is being analyzed in this paper and transfer learning by recurrent neural network is proposed to be integrated with the core Deep Learning in order to enhance the security performance. The recurrent neural network is reported higher accuracy of attack detection in adhoc in 111 seconds of training time with 98.2 percent of detection accuracy.

REFERENCES

[1] Feng Li, Hui Lu, Meiqian Hou, Kangle Cui, Mehdi Darbandi, Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality, Technology in Society, Volume 64, 2021
[2] F. Sellal, Anatomical and neurophysiological basis of face recognition, Revue Neurologique, 2021
[3] Marion Garaus, Udo Wagner, Ricarda C. Rainer, Emotional targeting using digital signage systems and facial recognition at the point-of-sale, Journal of Business Research, Volume 131, 2021
[4] André Perez, 4 - Transport Network MPLS-DEEP LEARNING Technology, Editor(s): André Perez, Implementing IP and Ethernet on the 4G Mobile Network, Elsevier, 2017
[5] A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016, pp. 84–90, 2016, doi: 10.1109/FiCloud.2016.20.
[6] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," J. Netw. Comput. Appl., vol. 84, pp. 25–37, 2017, doi: 10.1016/j.jnca.2017.02.009.
[7] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.
[8] Kamesh and N. Sakthi Priya, "A survey of cyber crimes Yanping," Secur. Commun. Networks, vol. 5, no. June, pp. 422–437, 2012, doi: 10.1002/sec.
[9] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv. Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013, doi: 10.1109/SURV.2012.121912.00006.
[10] A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," Int. J. Ad Hoc Ubiquitous Comput., vol. 9, no. 2, pp. 69–83, 2012, doi: 10.1504/IJAHUC.2012.045549.

*Corresponding author
Adel M. Salman,
Baghdad College of Economic Sciences University, Baghdad, Iraq
e-mail: adelmsk63@baghdadcollege.edu.iq

[11] Graham, R. Mirai and IoT Botnet Analysis. In Proceedings of the 2017 RSA Conference, San Francisco, CA, USA, 14–17 February 2017.
[12] L. Chen, "Scholarship at UWindsor Security Management for The Internet of Things By," p. 71, 2017, [Online]. Available: https://scholar.uwindsor.ca/etd/5932.

*Corresponding author
Adel M. Salman,
Baghdad College of Economic Sciences University, Baghdad, Iraq
e-mail: adelmsk63@baghdadcollege.edu.iq