International Journal of Real-Time Applications and Computing Systems (IJORTACS)

Volume 2, Issue II, February 2023, **No. 38, pp. 390-402**

Submitted 25/3/2023; Final peer review 24/4/2023

Online Publication 4/5/2023

Available Online at http://www.ijortacs.com

DETECTION AND ISOLATION OF BLACK-HOLE IN WIRELESS BROADBAND ECOSYSTEM USING ARTIFICIAL INTELLIGENCE

[1]Ogbuanya I.M., [2]Eke James

[1,2] Department of Electrical and Electronic Engineering; Faculty of Engineering; Enugu State University of Science and Technology, Enugu State, Nigeria.

Corresponding Author Email: [1]Ifeyinwamargaret2@gmail.com

ABSTRACT

This paper presents the detection and isolation of black-hole in wireless broadband ecosystem using artificial intelligence technique. Literatures were and it was observed that solution for real time isolation of black-hole which satisfied user experience has not been achieved. The methods utilized to solve the problem are data collection, feature extraction, artificial neural network methods, training and the threat detection and isolation system. The system design used neural network and data of black-hole to generate a black-hole detection model. The model was implemented with Simulink, tested and validated with tenfold cross validation approach. The result showed that with the neural network-based security algorithm, the average throughput achieved is 89.45% which is good when compared to the Nigerian Communication Commission Standard for 4G network analysis.

Keywords: Black-Hole; Broadband; Neural Network Artificial Intelligence; Network Analysis

1 INTRODUCTION

In this 21st century the rise of information communication has grown exponentially and as a result has contributed to the advancement in the present-day telecommunication industry. This has presented huge benefits such as the limitless ability to send, receive, store and retrieve information in real time using the necessary hardware and software components. One of such ecosystems is the wireless broadband network.

Wireless local area network (WLAN) has gain momentum all over the world, thanks to IEEE 802.11 wireless standard; the technology has been transformed to open solutions with both flexibility, quality of service and wireless services for communication systems. The IEEE 802.11 wireless standard provides security access to network infrastructures. The increase of WLAN applications have provided the demand for optimization of the wireless

network both in terms of service and security., both for home users and in office places (Kiran and Sandeep, 2017).

Over the years, there have been many methodologies employed for the protection of wireless network includes a wifi protected network (WPN) architecture, data encryption, decryption, password protections among others. However, most of these methods have their limitations and are more effective for data offline. In order to secure the network services, there is an increasing need to improve authentications, thus eliminating wireless security threat by augmenting the network with security system that would provide data confidentiality, and protection. The multiple organizations need adequate data security for communications between various organizations like the banks, schools, offices and industries. However, these domains have overtime been attacked with middle attack type, IP spoofing, worm-hole, grey-hole among others as presented in (Subramanian, 2019).

Today the current trend is the black-hole which is an advanced form of distributive denial of service attack. Majority of these attacks have been combated in (Gen 2008; Subramanian 2019; Cryptoclarity, 2009) among others, however the black-hole is still a major concern for wireless network. A black-hole is a DoS attack in which a malicious node falsely claims that it has the shortest path to the destination node. This attack is carried out by an attacker sending fake routing information (Mills, 2009).

To solve black-hole, various techniques like the generic algorithm, encryption algorithm and machine learning clustering algorithms have been revealed, however due to the adaptive intelligence of machine learning, the performance exceeds other techniques, but despite the success it has certain issues that must be fixed.

Machine learning techniques are set of algorithms which can make correct predictions based on learned input data. The algorithms are presented in Kiran and Sandeep (2017) and from the study it was observed that the artificial neural network (ANN) performs best when compared to the rest. This neural network has been used in many works to protect mobile ad hoc network, heterogeneous networks, wireless mobile access network against black-hole and achieved great success. This will be sued in this research to protect the case study wireless broadband ecosystem using artificial neural network technique.

2. LITERATURE REVIEW

Mohammed et al. (2020) researched on the use of Machine learning (ML) and Deep learning (DL) methods for Internet of Things (IoT) Security. The major purpose of this work is to give a clearer and descriptive review of Machine Learning methods and newer advances in Deep Learning methods that will be useful in developing enhanced security methods for Internet of things (IoT) Systems. This technique will be used to develop a faster and more accurate system that can be reliable in protecting and securing the network of IoT systems. However, the opportunities and challenges presented in this work will be helpful for future research directions in future works.

Sabah and Liang (2018) researched on Generation of black-hole Dataset for Effective IDS Development and Evaluation, and presented how black -hole is attacked via multiple agents to a single victim. The goal of this work is to simulate a wireless network environment using OMNET++ simulation tool, feeding it with different black-hole types. The results of the number of algorithms and applications presented in this work can be used for developing effective algorithm techniques and procedures to prevent black-holes in future research works.

Vikrant et al. (2013) researched on Intrusion Detection System for WLAN, which presented ways which can be applied to counter different kinds of attacks on the WLAN environment with the use of Intrusion Detection System (IDS) techniques. IDS is a security layer over the WLAN environment that can be used to detect any ongoing intrusion in the network with the application of Artificial Neural Networks and a fuzzy clustering. However, the ANN method used for this study was not specified but the use of RNN has been proved to be effective for such systems.

According to Poulmanogo et al., (2019), their research work on Securing Fog-to-Things Environment Using Intrusion Detection System Based on Ensemble Learning, uses NSL-KDD in combination with multiple learners to build and ensemble learners for intrusion detection systems development, which will help to increase the accuracy of the intrusion detection task. It also uses two levels of the fog-of-things architecture to perform anomaly detection and attack classification level which identifies the presence of an attack in the WLAN environment. The architecture and algorithm implemented in this system is huge and complex to understand and adopt

to. Therefore, a less complex system should be adopted to n future works.

Yang (2018) researched on WLAN Intrusion Detection Using Artificial Bee Colony-BP Network Algorithm, which uses bee colony-BP neural network algorithm to detect the complicated aggressive behaviors, by applying it to the detection module. The artificial bee colony-BP neural network algorithm is used in the detection module, so as to detect the complicated aggressive behaviors. The accuracy of this technique used in this research is 91.25%. Hence an improvement in this study will be helpful.

3 METHODOLOGIES

The physical design methodology was used to develop the new system and then designed using structural and mathematical method. The system design presented the models used for the development and evaluation of the new security system. The modeling considering the packet transmitted on the network, the throughput rate of delivery, latency, data collection, feature extraction, artificial neural network, training and development of the intelligent security model.

3.1 Packet Rate Model

This model was used to measure the amount of packet data transmitted from each of the communicating nodes within the network. This was measured using the data rate model in equation 1;

$$R_{u,t= \alpha W \log 2(1+SINR_.)} \quad 1$$

Where α is the fraction of bandwidth employed for the packet data transmission, W is the bandwidth, SINR is signal to noise to interference at user u and time slot of t. The model was initiated after the UE transmission control protocol was activated for communication.

3.2 Throughput Model

This is the measure of the amount of data delivered on the network. Usually, when data are transmitted not all are delivered to the destination end due to issues of loss, however when the amount of data delivered are less than 75% and latency lass then 150ms for http data according to the Nigerian Communication Commission (NCC). The throughput model was presented in equation 2;

$$TP = \frac{I}{T_t(P_x) - T_f(P_x)} \quad 2$$

Where I is the among of packet transmitted within the network (ie between the communicating nodes), $T_t(P_x)$ and $T_f(P_x)$ presented the first and last data sent per given time unit between the two communicating nodes with the security protocol (P_x).

3.3 Latency Model

This parameter was used to measure the amount of delay on the wireless network when inflicted with black-hole. This is the measure of the time it takes for the data transmitted to get to the destination and it was achieved using the model in equation 3;

$$\text{Latency} = \frac{\sum iA_{th}(packetarrivali - packetstarti)}{n} \quad 3$$

Where Packet arrival is the time when packet "i" reaches the destination and Packet Starti is the time when packet "i" leaves the source. "n" is the total number of packets. Where A_{th} is average throughput, N is the number of users in the cell at a given time.

The next method is the data collection used for the development of the new system. Data was collected of back-hole from Afrihub center, Enugu Nigeria containing 5 major attributes as presented in the table 1;

Table 1: Data description of black-hole

S/N	Attributes	Data description
1	Target IP address or range	IP address or range of addresses that the attacker wants to target.
2	Traffic redirection technique	Specific method used to redirect traffic to the blackhole, which can involve modifying routing tables, using DNS poisoning, or other techniques.
3	Type of traffic affected	Specific type of traffic that is being redirected to the blackhole, such as HTTP, FTP, or other protocols
4	Duration of the attack	The amount of time the attack will last before the attacker stops redirecting traffic to the blackhole
5	Goals of the attack	Specific objective of the attack, such as causing a denial of service, stealing sensitive information, or other malicious purposes.

The table 1 presented the data description of the blackhole attributes.

3.4. Feature extraction model

The feature extraction model used for the conversion of the data into a compact feature vector is presented as (Rathore et al., 2021; Hasan et al., 2021);

$$F = (N, P, T, B, S, L, R, M) \quad 4$$

Where:

- N represents the number of network connections made during the attack
- P represents the type of protocol used in the attack (e.g. TCP, UDP, ICMP)
- T represents the time duration of the attack
- B represents the size of the data packets exchanged during the attack
- S represents the severity of the attack based on the impact on the targeted system or network
- L represents the level of sophistication of the attack
- R represents the degree of resource consumption by the attack

- M represents the motivation or intent of the attacker

3.5 Model of the neural network

The neural network is the machine learning algorithm used to train the data extracted. He neural network type used for the work is the Feed Forward Neural Network (FFNN). This FFNN is a simple but very effective neural network model which can solve pattern recognition problems like the issues of cyber threat as identified in the study. To develop the neural network, the number of neurons was specified, the number of hidden layers determined, learning rate, training algorithm, activation functions among other parameters to achieve the machine learning algorithm to detect black -hole on the wireless ecosystem. The model of the neural network configuration was presented in figure 1;

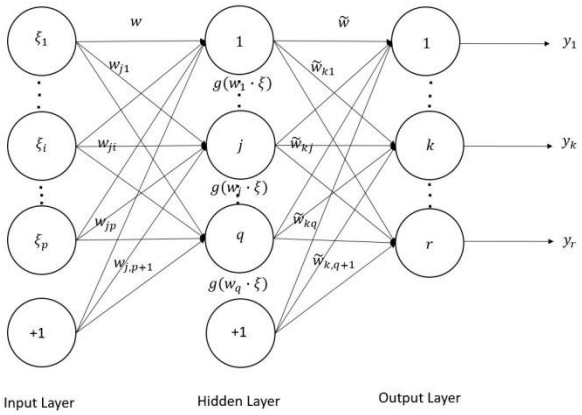

Figure 1: A model of the neural network

The model of the neural network was developed considering the number of classes in the dataset and then attributes for each class. Where ξ is the neuron, p is the number of neurons, w_{ij} is the weight, j,q are the layers, g is the activation function, r, k ae outputs (y).

This was used to decide the number of input features which is 5 and then number of hidden layers which is 40. The need to decide the type of packet if black-hole or normal packet presented the probability function used as the activation function which is the tansig function and then output been a statistical values of packet vectors are feed for training as in the section 3.5.1; other parameters used for the configuration of the neural network like the number of epoch, the training rate, delay input and output among others are all presented in the table 1;

3.5.1 The Training Algorithm

Start

1. ***Identify black-hole feature extraction data of packet***
2. ***Select the feature attributes as vectors***
3. ***Initialize weight and bias function of the neural network***
4. ***Generate epoch parameters***
5. ***Adjust weight and bias of the neurons to learn the attributes parameters***
6. ***Set epoch interval (n) = 100***
7. ***Check performance learning performance at n +1***
8. ***If***
9. ***learning is good for validation, mean square error and regression= true***
10. ***Then***
11. ***stop training***
12. ***Generate reference black-hole model***
13. ***Else***
14. ***Return***
15. ***Retrain***
16. ***End***

The neural network training algorithm presented how the neural network used the back-propagation algorithm for the training of the neurons when loaded with the features of the blackhole to generate the threat detection model.

3.5.2 Back-propagation algorithm

1. ***Initialize the weights and biases of the neural network randomly.***
2. ***Feed an input through the neural network and compute the output.***
3. ***Compute the error between the output and the target output.***
4. ***Backpropagate the error through the network using the chain rule to compute the gradient of the loss function with respect to the weights and biases.***
5. ***Update the weights and biases using the gradient descent algorithm.***
6. ***Repeat steps 2-5 for a certain number of epochs or until the error is below a certain threshold.***

The pseudo code presented the training algorithm which was used to train the neural network. The figure 2 presented flow chart of the neural network training process for the detection of blackhole on the network.

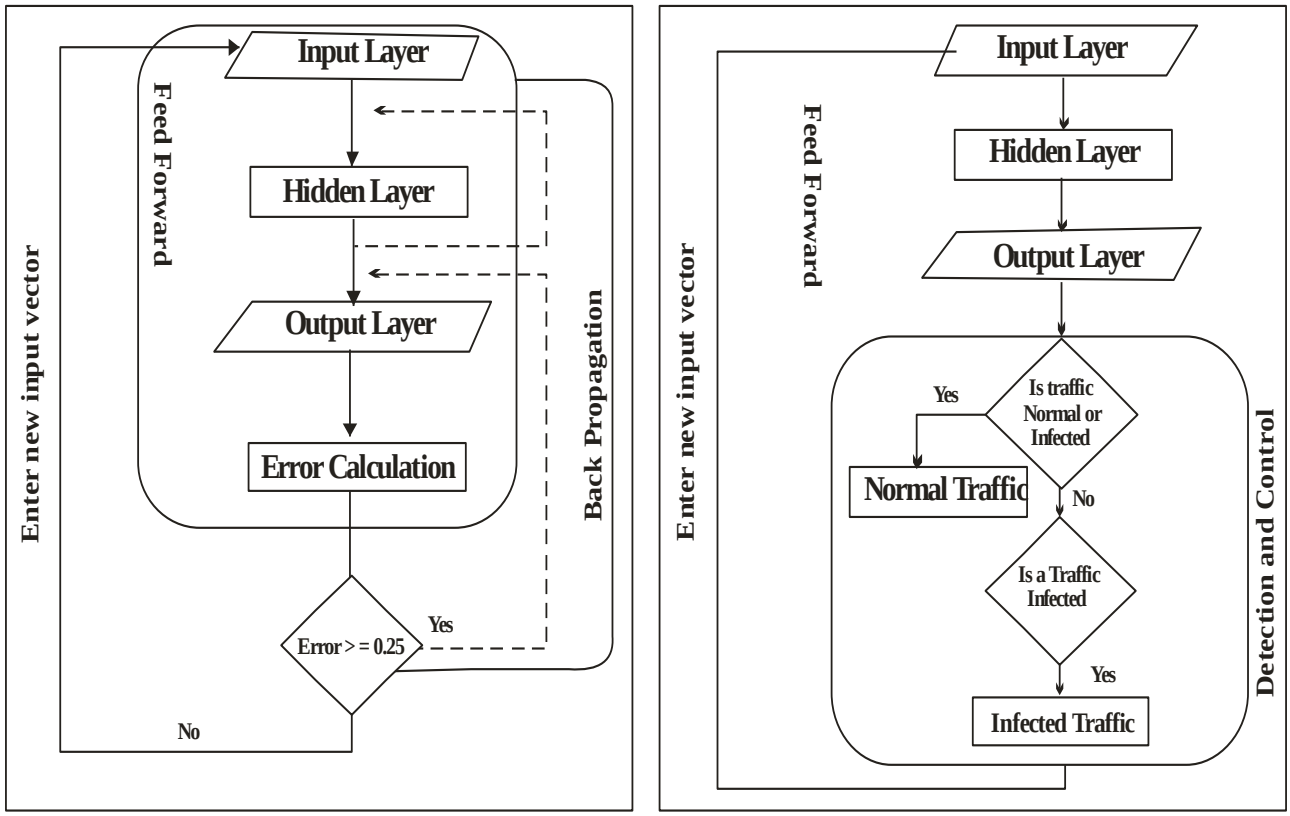

Figure 2: The training and evaluation process

4. SYSTEM IMPLEMENTATION

The system was implemented with statistics and machine learning toolbox, neural network toolbox, communication toolbox and Simulink. The neural network toolbox was configured using the neural network model developed. The communication toolbox was used to deploy the algorithm in the wireless network. The statistics and machine learning toolbox were used for the data extraction process. The model of the wireless network developed with the improved security algorithm is presented in figure 3;

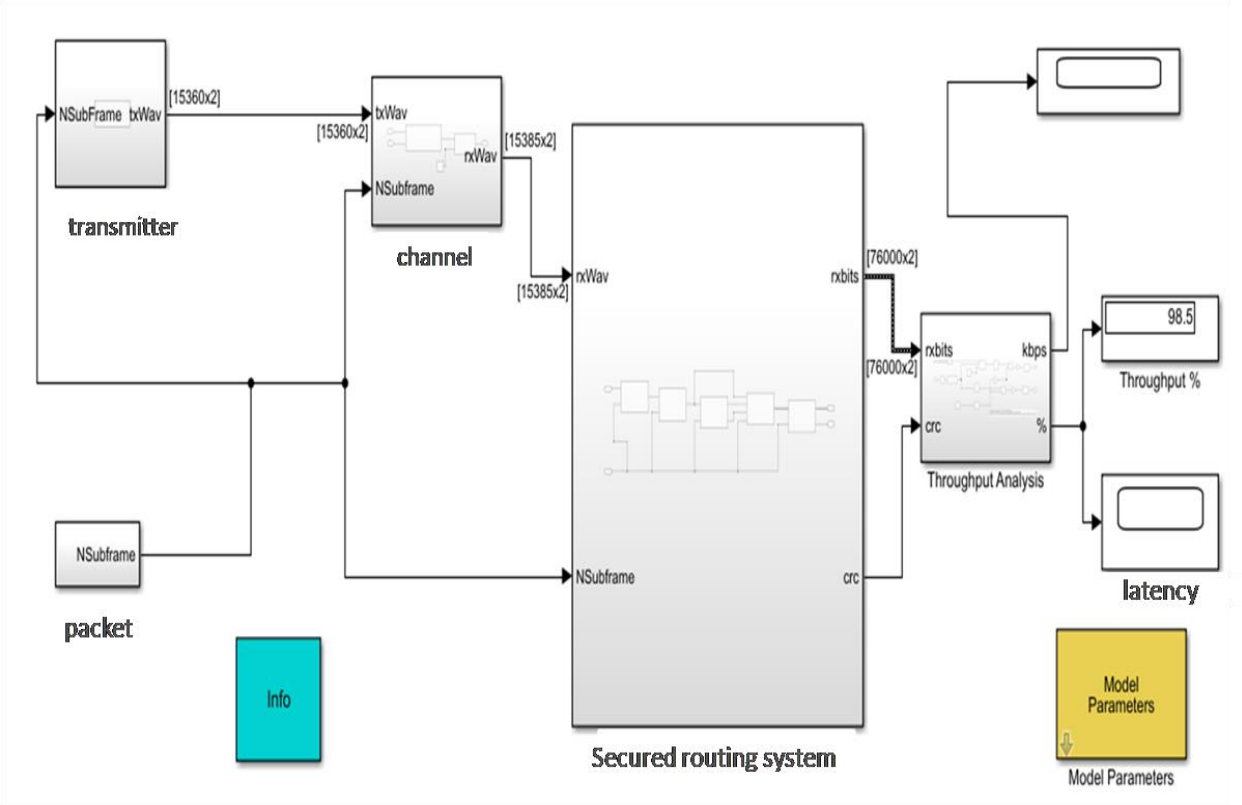

Figure 3: The model of the Wireless Network

The figure 3 presented the Simulink model of the improved wireless network developed with the black-hole detection algorithm. The simulaiton parameters used for the testing are four nodes for normal communication; two blackhole nodes, traffic amount is 6; packet per seconds is 60 and total time of simulation is 180ms.

5. RESULT

This section presented the performance of the training algorithm. The aim is to evaluate the reliability of the black-hole reference model generated and be sure that it

will completely protect the wireless network from attacker. The result was measured using Mean Square Error (MSE) analyzer and regression tools embedded in the neural network tool as presented in the figure 4;

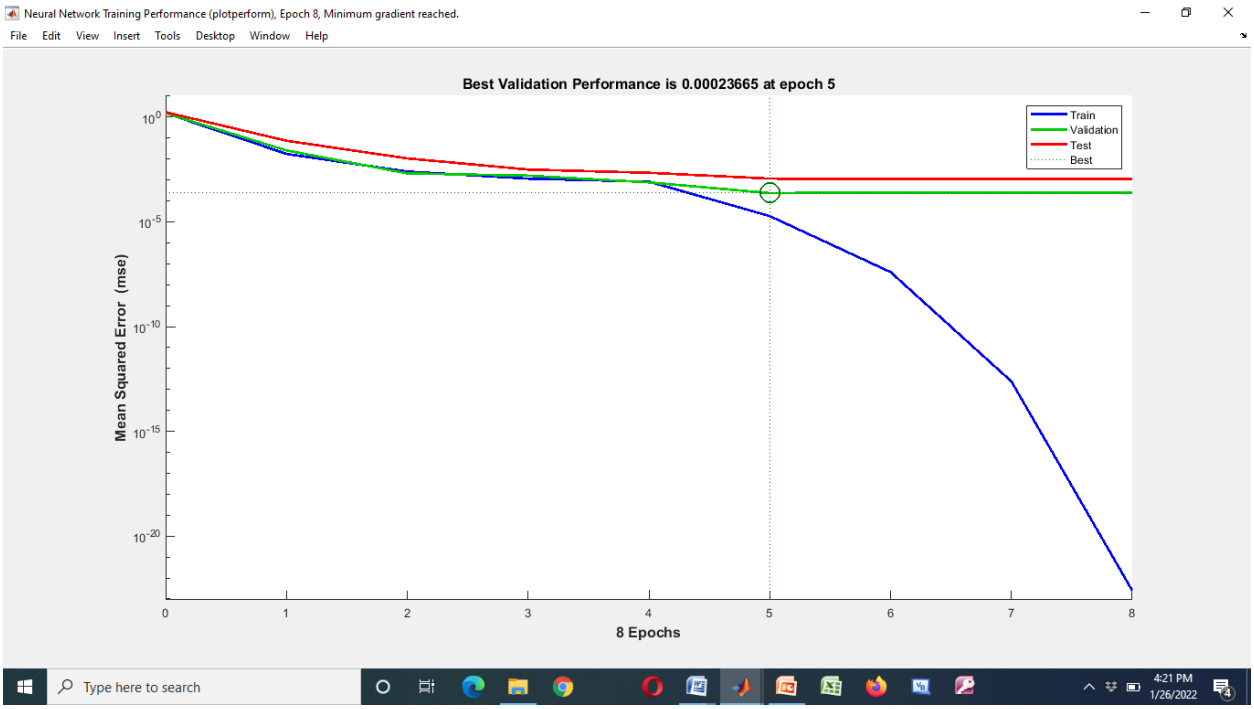

Figure 4: The MSE result of the algorithm

The figure 4 presented the MSE performance of the algorithm developed. The aim of this tool is to achieve a MSE value equal or approximately zero. The result in the figure 6 showed that neural network evaluated the performance of the algorithm in 8 epoch steps and achieved the best result at epoch 5 with a MSE value of 0.00023665Mu which is very good as it is approximately zero.

The next result presented the regression performance of the system using the regression tool in the neural network. The aim is to achieve an ideal regression value of 1 or approximately 1 which implied reliability of the algorithm to correctly classify and detect black-hole attack. The result was presented in the figure 5;

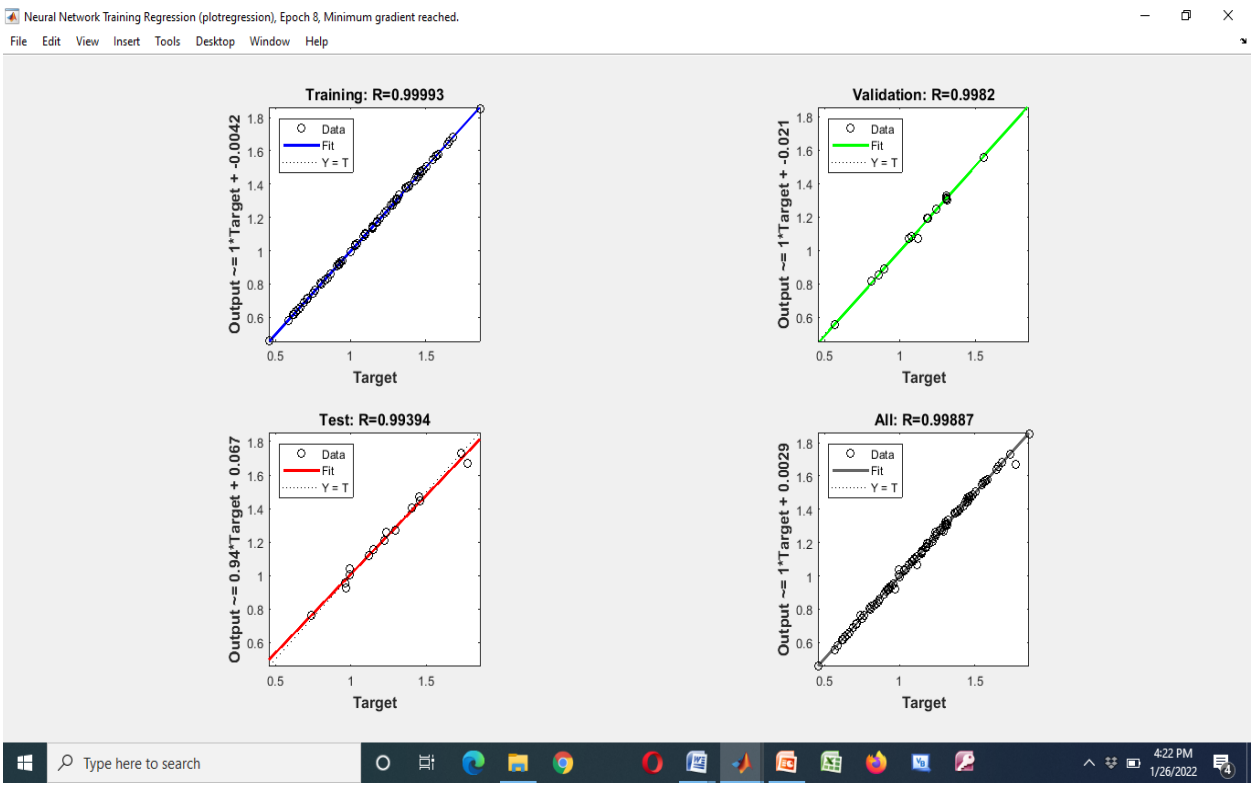

Figure 5: The Regression result

The figure 5 presented the performance of the algorithm when measured with regression analyzer. The result showed that the average regression performance of the algorithm is 0.99887 which is very good as it is approximately the ideal values expected.

5.1.The Simulation Result

The previous section has evaluated the performance of the neural network and shown that the training performance was good, indicating that it has accurately learned the black-hole data and will provide a reliable security function on the wireless network. This was integrated on the testbed network via and simulated. The result of the throughput and latency performance is presented in figure 6;

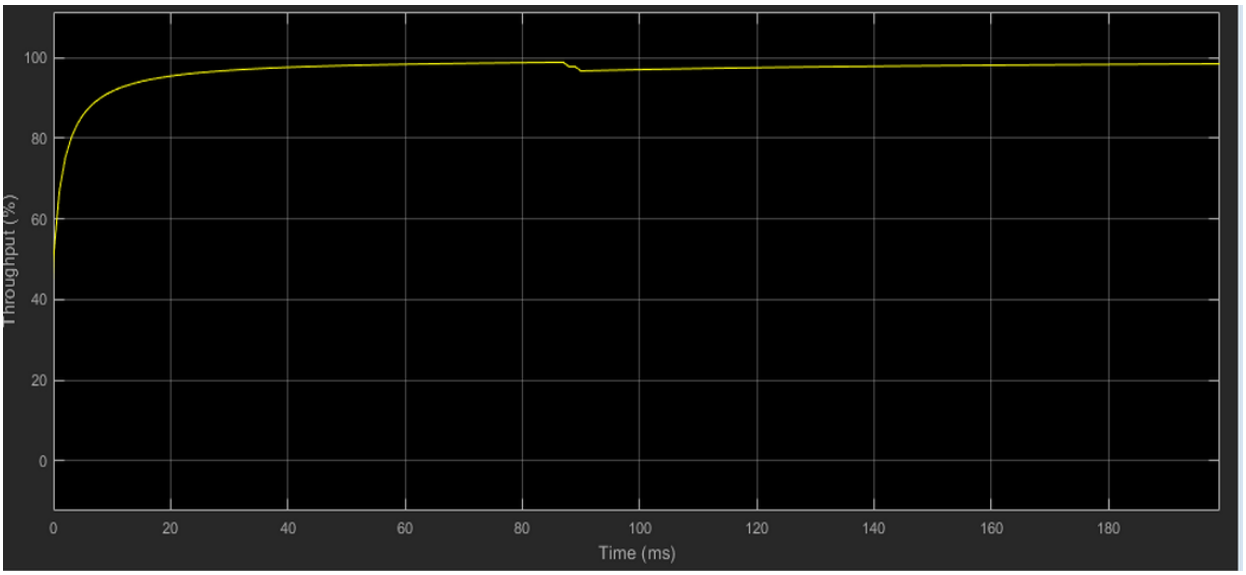

Figure 6: Throughput result

The figure 6 presented the throughput performance of the 4G network when simulated and from the result it was observed that the average throughput on the network is 89.4% which according to the NCC standard is very good for a network quality of service. The latency of the network is also measured and the result is presented in figure 7;

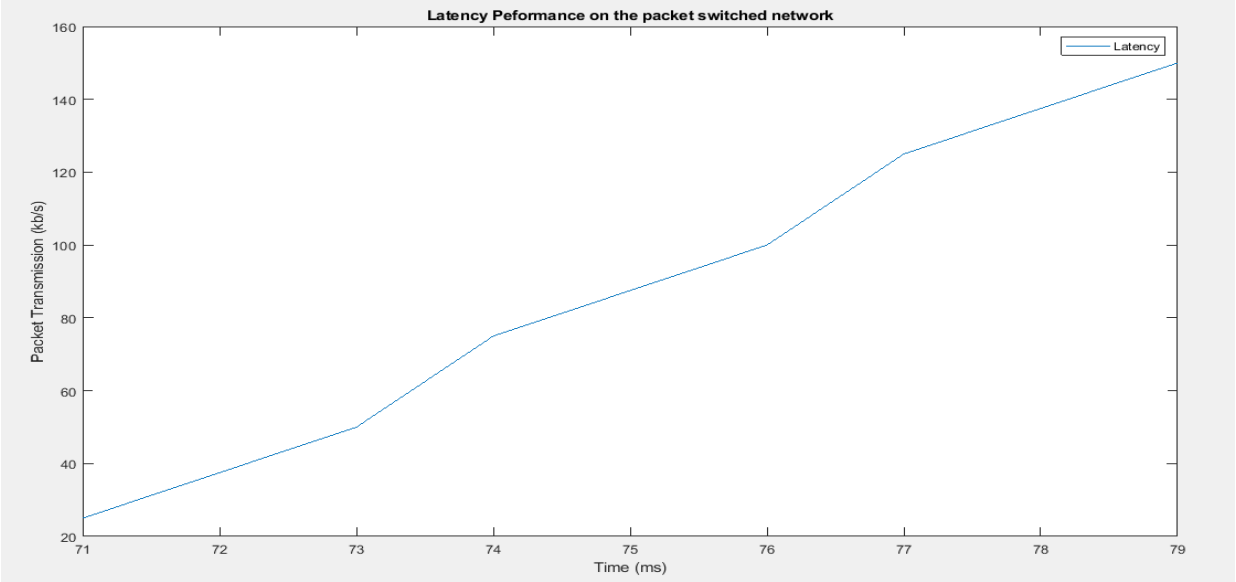

Figure 7: Latency performance

The result of the latency performance is presented in the figure 9 shows the latency performance of the 4G network and it was observed that the average latency is 76.37ms which according to the ITU and NCC

standard is good. However, the reason for this latency value is due to the training of the data by the neuro security algorithm developed which took some time to train and check for block-hole before throughput to the cloud if no threat was detected.

6. CONCLUSION AND RECOMMENDATION

This study has successfully developed an intelligent security algorithm to protect wireless network against black-hole. This was achieved after series of literatures was reviewed and research gap established. This study collected data of the block-hole from Afrihub network center and train a neural network model to generate a black-hole detection algorithm. The algorithm was implemented with Simulink and tested. The result showed that with the neural network-based security algorithm, the average throughput achieved is 89.45%. The latency achieved with neural network is 76.37ms.

6.1 Recommendation

a) The study recommends that the algorithm be deployed on other forms of wireless network to protect the network against black-hole

b) The training data can be improved and then train with deep learning to achieve better result

c) The latency achieved on the network can be improved using optimal routing scheme

d) The throughput on the network can be improved using congestion management schemes

7. REFERENCES

Cryptoclarity (2009). Encrypted storage and key management for the WLAN. Retrieved from

Gens, F. (2008). Defining "WLAN services" and “WLAN”. Retrieved from http://blogs.idc.com/ie/?p=190

Hasan T, Uddin A., and Alam S., "A Novel Feature Extraction Technique for Detection of Blackhole Attack in Mobile Ad-hoc Networks," in Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 6025-6037, 2021.

Kiran, Sandeep Sharma (2017). Enhance Data Security In WLAN Using Machine Learning And Hybrid Cryptography Techniques. International Journal of Advanced Research in Computer Science. DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5042 Volume 8, No. 9, November-December 2017. ISSN No. 0976-5697,

Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani. (2019) A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. NPRP grant #8-408-2-172 from the Qatar National

Research Fund (a member of Qatar Foundation

Poulmanogo Illy, Georges Kaddoum, Christian Miranda Moreira, Kuljeet Kaur, and Sahil Garg (2019). Securing Fog-to-Things Environment Using Intrusion Detection System Based on Ensemble Learning. IEEE Wireless Communications and Networking Conference, 15- 18 April 2019, Marrakesh, Morocco. arXiv:1901.10933v1 [cs.CR] 30 Jan 2019.

Rathore, S., Singh, K., and Singh, K."A Survey on Recent Advancements in Detection and Prevention Techniques for Blackhole Attack in Wireless Sensor Networks," in Wireless Personal Communications, vol. 116, no. 4, pp. 2219-2242, 2021.

Sabah Alzahrani, Liang Hong, (2018). Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation. Journal of Information Security, 2018, 9, 225-241 http://www.scirp.org/journal/jis ISSN Online: 2153-1242 ISSN Print: 2153-1234. https://doi.org/10.4236/jis.2018.94016

Subramanian K. (2009). Recession is good for WLAN – Microsoft Agrees. Retrieved from http://www.WLANave.com/link/recession-is-good-for-WLAN-computing-microsoft-agrees

Vikrant G. Deshmukh, Atul G. Borkut, Nikhil A. Agam, (2014). Intrusion Detection System for WLAN. International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4

Yang Hui (2018). WLAN Intrusion Detection Using Artificial Bee Colony-BP Network Algorithm. Journal of DigitalInformation Management.http://www.scirp.org/journal/jisISSN Online: 2153-1242 ISSN Print: 2153-1234. https://doi.org/10.4236/jis.2018.94234