Development of Machine Learning Based Security Algorithm for 4G Network against Wormhole

Eze E.M.[1], Ituma C.[2], Asogwa T.C[3]., Ebere U.C.[4]
[123]*Enugu State University of Science and Technology*
[4]*Destinet Smart Technologies Ltd.*

Abstract: **This work development of machine learning based security algorithm for 4G network against wormhole. This was achieved using methods such as data collection, data extraction, training and classification process. The system design employed mathematical and structural method to develop the models of the wormhole and also the new security algorithm using artificial neural network. This was implemented with Simulink and neural network toolbox, before testing. The result showed that the algorithm was able to detect wormhole at a regression of 0.9978 and Mean square error of 2.05x10^-5. The security algorithm deployed on a 4G network and tested; the result showed that throughput percentage of 89.16% and latency of 76.325ms which according to International Telecommunication Union (ITU-U) and Nigerian Communication Commission standard (NCC) are good.**

Keywords**: Wormhole, 4G Networks, Security, Machine Learning, Neural Network**

I. INTRODUCITON

Over the years, the rapid growth in Internet of Things (IoTs) connectivity has equally presented the need for information technology (IT) companies to upgrade their capacity and network size so as to meet up with the demand for data and management of user equipments. To achieve this aim, the various IT companies have constantly upgrade their service equipments with the transformation of the broadband ecosystem from the original state of 3G to the presents day state of the art Long Term Evolution (LTE) network. The LTE is today know as 4G network with proposed solution to wireless broadband and heterogeneous network connectivity; providing increase bit rate of over 20Mbps and improved service quality (Payaswini et al., 2013). This advancement in the IT sector has lead to the rapid adoption of the technology; as today internet has become part of man with limitless applications. According to Contel (2020), security is ranked as both the primary benefit and biggest challenge for IT professionals. This is to say that despite the huge benefit the internet service offers, addressing the security concerns is the only way to take its full advantage. It is therefore imperative to carefully analyze these security issues and the conventional security approaches proposed and implemented in the past with a view to improve the performance using a better solution.

Over the past decades, these issues of information security in wireless network have been one of the most active research area, with (Kolias et al., 2016; Khosroshahy et al., 2013) identifying some of the attack trends as man in the middle, wormhole, botnet, denial of service, black hole, spoofing among other attack forms to mention a few. In these attack types mentioned, all take different forms and requires different approaches for mitigation, however the wormhole type is very dynamics and till date still remain the main attack tool for hackers to bring down network nodes. According to Nicklas (2017) wormhole attack is one of the serious security issues currently faced by wireless networks. The wormhole attack (WHA) creates an illusion of two nodes which can attract large amount of network traffic and as a result manipulates the network to launch series of attacks. To solve this problem various techniques have been proposed such as neighbor discovery algorithm, encryption algorithm and machine learning, but all have their limitations; however the use of machine learning provided the most reliable security solution for wormhole. Machine learning (ML) is intelligent system which has the ability learn from pattern recognition problems and make accurate decisions (Mehta, 2019). This involves many algorithms such as support vector machine, K-nearest neighbor, artificial neural network (ANN) among others, however the effectiveness of ANN in other fields when compared to other ML counterparts have made it special to solve this problem and will be used to train clusters of wormhole vector and then deploy on the 4G network for security.

II. LITERATURE REVIEW

Singh et al. (2016) proposed a research on Wireless Sensor Network (WSN) based on the concept of watchdog and Delphi schemes to guarantee that wormhole are detected in sensor networks. In this study, the dual wormhole detection mechanism was used for computing the probability of factor time delay and packet loss probability of the established path in order to find the probability value of wormhole presence. However, the security solution never considered the quality of service impact of the algorithm.

Sunneetha et al. (2019) presented a research on data security model using artificial neural network and database fragmentation in wireless sensor network. The research was implemented using dynamic hashing fragmented components and implemented for storing fragmented sensitive secret data. The proposed solution applied shows high data security confidentiality on WSN database, however quality of service was not considered.

Nabeel and Adil (2016) researched on identifying WSN security threats to strengthen wireless sensor network adoption framework. The work revealed that wireless sensor network give firms the chance to outsource their information technology (IT) process, thereby permitting business concentration to improve productivity and innovation in serving customers. Furthermore, it allows businesses to reduce the cost of IT infrastructure without losing attention on customer needs.

Nayak et al. (2013) proposed a study on Mobile Ad-hoc Network (MANET) based on the packet detection security against wormhole. In this technique, detection packet was used for detecting malicious node in network which consists of three fields such as processing bit, count to reach next hop and time stamp. Timestamp was used for strongly detection with conformance at wormhole attack. Here, detection packet can simply be added in the wide range of ad-hoc routing protocol for defense against wormhole attack. However quality of service impact of the algorithm was not considered.

Giannetsos and Dimitirou (2014) presented a study for the mitigation of wormhole in MANET using neighbor discovery algorithm. Initially, the problem of neighbor discovery at physical and routing layer was studied. Then, a Localized and Decentralized Algorithm for Countering (LDAC) protocol was proposed to detect wormholes in both static and mobile wireless networks by enabling nodes for verifying potential risk of attack. The performance however can be improved with machine learning technique.

III. METHODS

The methods used for the development of the new system are data collection, data extraction, artificial neural network, system identification, training and classification.

Data collection: This process involves the collection of wormhole data which was done by the researcher at the Institute of Electrical Electronics Engineering (IEEE) repository in Nivedhaet al. (2015), containing 512005 samples of wormhole and stored as the training dataset.

Data extraction: This process was used to extract the data collection into statistical features for training purposes. The feature extraction process was done using static and dynamic method static and dynamic analyses (Saxe and Berlin, 2015).

Artificial neural network: This is a machine learning algorithm which was sued for the training of the data extracted. The algorithm is a biological inspired system which has weights, bias and activation functions; with the ability to learn patterns and make correct classification decisions.

System identification: The process was used by the artificial neural network to identify the wormhole feature vectors extracted for training purpose.

Training: This process ensures the artificial neural network learns the wormhole patterns and generates the desired detection algorithm.

Classification: This process involves the use of the learned data by the neural network to make comparative decision and detect wormhole on the network. This was done collecting time series data from wireless network gateway and then train with the reference model for detection of wormhole.

The block diagram shows how the intelligent security system was analyzed using the various processed as shown in figure1;

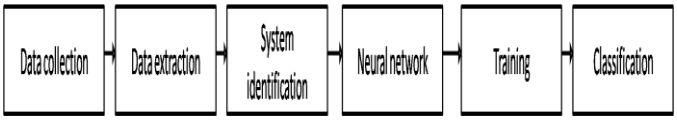

Figure 1: system block diagram

The system collected data of wormhole feature vectors and then extracts into an artificial neural network model developed are an intelligent security strategy. The ANN identified the features as a nonlinear auto regressive model and then trained using training algorithm for the classification of wormhole attack in the wireless network gateway and isolate.

IV. SYSTEM DESIGN

Development of the Wormhole Model

The wormhole was generated using modeling diagram. From the model the wormhole penetrated into the network using out of band tunnel through a wormhole link. This wormhole link can be of many forms such as optical fiber, Ethernet cable, or secured long range wireless link according to (Mohammed, 2016), but in this case is long range wireless link. During the attack process when the wormholes are initiated, packets are captured and rebroadcast through the link to other neighboring nodes as shown in the figure 2.

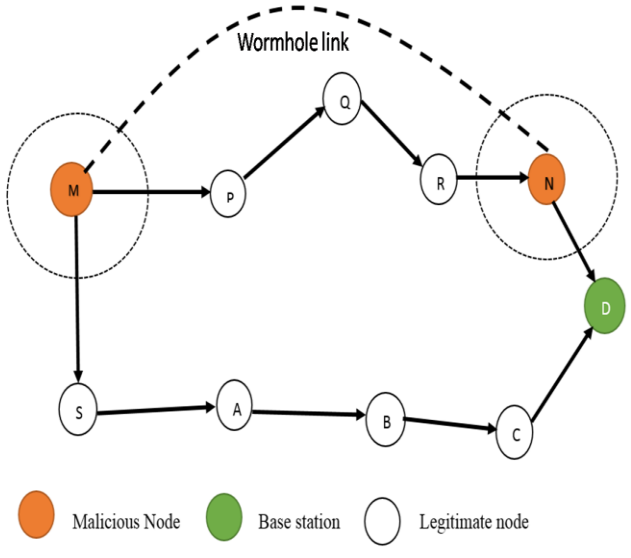

Figure 2: The Wormhole model

The model in figure 2 presented the two malicious nodes M and N on the 4G network, when node S which is a legitimate node broadcasted packet to the base station D, the node A received the packet to rebroadcast to other nodes until it gets to the base station. Simultaneously malicious node M received the packet and also uses the wormhole link to send to malicious node N which then transmits to the base station D. Now when the actual packet from the legitimate links and nodes A to B to C and getting to the base station D is rejected as the malicious nodes has first transmitted to the base station. This type of wormhole attack is called the out of band form and has to be mitigated as it affects quality of service in the 4G network. The data table showing the wormhole attributes is presented in table 1;

Table 1: Data table of the Wormhole

S/N	Feature names	Data Type
1	Duration	Continuous
2	Protocol	Discrete
3	Packet size	Continuous
4	Flag	Discrete
5	Header length	Continuous
6	Hop count	Continuous
7	Life time	Continuous
8	Message type	Continuous
9	Destination sequence number	Continuous
10	Stream index	Continuous
11	Land	Discrete
12	Message transfer mode	Discrete
13	Number of neighbors	Continuous
14	Highest data flow	Continuous
15	Average data flow	Continuous
16	Lowest data flow	Continuous
17	Average number of hop count	Continuous
18	Number of drop box	Continuous
19	Rate of drop box	Continuous
20	Label	Discrete

From the table 1; duration presents the time it takes the packet to travel from the sending node to the receiver node, while the data status is called the flag, the intermediary nodes between the transmitting node and receiving nodes are defined by the hop counts while the packet size defined the capacity of data rate transmitted; destination sequence number, steam index features and message sequence number are number identifications for the transmitting or receiving node as a given time. Land presents the binary behavior of the nodes. For more description of the wormhole attributes see (Prasad et al., 2019).

Development of the Machine learning based Wormhole Detection algorithm

The machine learning algorithm to be employed to mitigate this wormhole threat is the artificial neural network. Today machine learning has series of algorithm which are expertise in modeling a many nonlinear pattern recognition problems, however Artificial Neural Network (ANN) remain the best according to Mehta (2018) due to their adaptive nature and ability to precisely learn patterns of dataset and make accurate decision better than other machine learning algorithm. This ANN was modeled in figure 3 was the number of interconnected neurons presented in table 2, activation and trained with wormhole data in table 1 to generate a reference wormhole model with the help of a training algorithm as in the pseudo code below;

The Training Pseodocodia **(back propagation algorithm)**

Start

1. Identify network behavior as the table 1
2. Select the wormhole parameters to learn
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 wormhole parameters
6. Set epoch interval (n) = 100
7. Check performance learning performance at n +1
   If
8. learning is good for validation, mean square error and regression= ture
   Then
9. stop training
10. Generate reference wormhole model
11. Else
12. Return
13. Retrain
14. End

The activity diagram in the figure 3 was used to model the complete training of the neural network to generate the reference model with the back propagation algorithm. The model shows how the data flow from the wormhole training dataset was feed forward into the neural network model for identification using its weighs and bias function. The summation of the input was activated with tangent sigmoid function and then trained with back propagation algorithm to learn the wormhole data and generate a reference model for time series identification of wormhole threat.

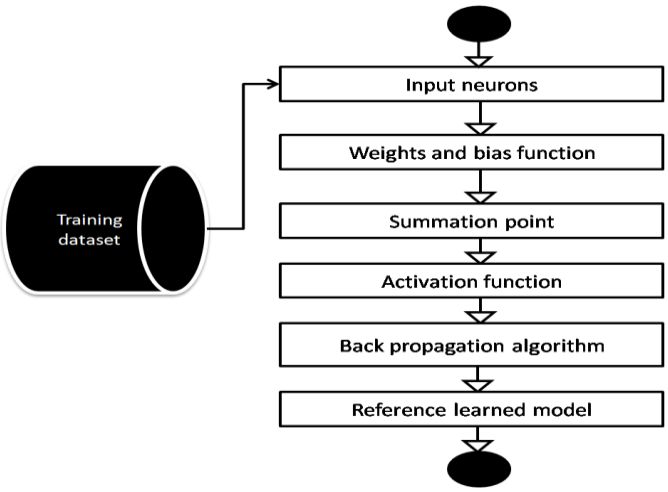

Figure 3: Activity model of the neural network training process

The model in figure 3 was sued to show how the neural network was designed to learn the wormhole data and generate the reference model for time series wormhole detection. The pseudo code of the algorithm is presented below;

Pseudopodia of the Neural Network Based Wormhole detection algorithm

Start

1. Load wormhole dataset
2. Identify network behaviors from the training data set
3. Configure neural network and training parameters
4. Train the neural network with back propagation algorithm
5. Check training performance until desired epoch is achieved
   If
6. Desired epoch is achieved = true
   Then
7. stop training
8. Else
9. Retrain until desired epoch is achieved
10. Stop
11. Generate a reference model
12. Classify data collected with reference model
    If
13. patter the same as reference model = true
14. Isolate from network and flag as wormhole
15. Else
16. Allow throughput
17. Return
18. **End**

The System Flow Chart

The system flow chart in figure 4 shows the logical data flow in the entire system architecture. The system showed how the already trained security algorithm with the wormhole dataset was used to protect the 4G network against time series wormhole threat. In the flow chart, when data from the other nodes are transmitted, the packets are extracted and then trained with the intelligent security algorithm developed to classify features of wormhole. If this condition is true, then wormhole is flagged as threat, else throughput is allowed to the packet.

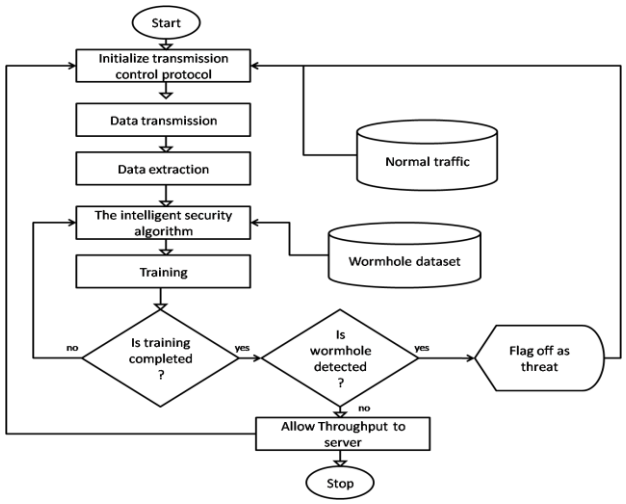

Figure 4: The system flow chart

V. IMPLEMENTATION

The system was implemented using the neural network toolbox, communication toolbox, long term evolution network toolbox, the modeling diagrams developed, algorithm and then simulink. The neural network tool was used to train the data to generate the wormhole detection algorithm develop as shown in the neural network toolbox. The neural network toolbox divided the data into training, test and validation set before training and then evaluated the performance using Mean square error (MSE), Regression, and confusion matrix. The training parameters are presented in the table 2;

Table 2: Training Parameters

Parameters	Values
Training epochs	20
Size of hidden layers	35
Training segments	30
No. delayed reference input	23
Maximum feature output	2
Maximum feature input	23
Number of non hidden layers	12
Maximum interval per sec	2
No. delayed output	1
No. delayed feature output	2
Minimum reference value	-0.7
Maximum reference value	0.7
Time	0.05sec

VI. RESULTS AND DISCUSSION

This section presented the performance of the neural network training process and also the performance intelligent secured 4G network. The neural network testing was done using the neural network performance evaluation tool to measure the neural network training, test and validation performance using Mean square error (MSE) and Regression analyzer. The regression is presented in figure 5;

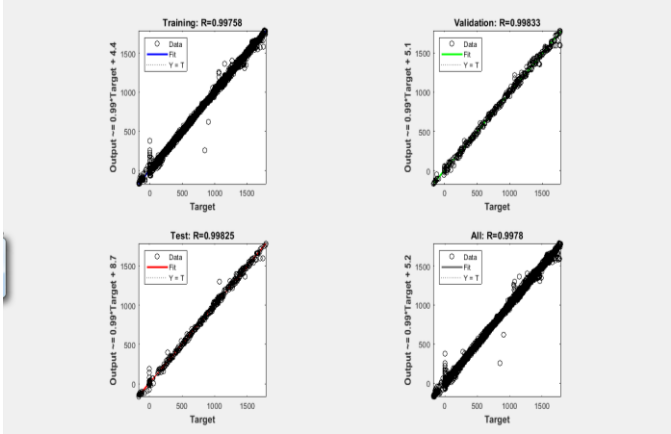

Figure 5: Regression performance of the neural network algorithm

The figure 5 presented the regression performance of the neuro security algorithm developed. The aim of this regression process is to achieve a regression value of equal or approximately 1 which indicated that the neural network correctly learn the wormhole behavior and also that the reference model is reliable. The regression result here was summarized using the mean score for the training, test and validation regression values respectively and then overall result achieved is R= 0.9978, indicating very good training process. To further justify the result a Mean Square Error (MSE) analyzer was used to measure the neural network performance and the result is presented in figure 6;

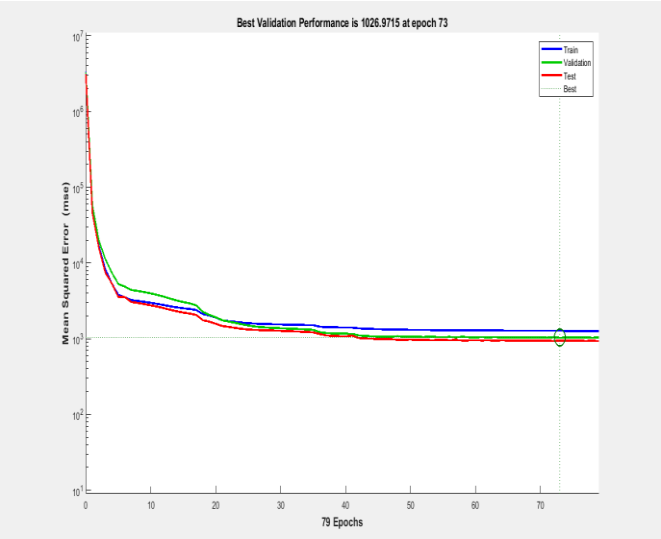

Figure 6: MSE performance

The reason for MSE is to measure the amount of error in the decision making of the security algorithm, although the aim is to achieve MSE of zero or approximately zero. From the result of the MSE analyzer in figure 6 it was observed first that the multi sets (training, test and validation) patterns correlated in the same direction, indicating that the training process experienced no overshoot which is a good signs. Secondly it was observed that the neural network achieved that best learning result at epoch 73, with a mean MSE for the multi set at 1023.9715e which is very good, indicating a negligible training error.

Performance Validation

The result achieved in the neural network training and also in the simulated 4G network was validated using the tenfold cross validation technique which evaluated the performance of the respective system in tenfold and then compute the average as the actual result. The validation performance of the neural network based wormhole detection algorithm and also the performance when simulated on the 4G network as presented in the table 3;

Table 3: Validation of the Results

S/N	MSE (Mu)	Regression
1	0.0000239715	0.9978
2	0.0000130254	0.9978
3	0.0000119755	0.9978
4	0.0000138758	0.9978
5	0.0000239333	0.9978
6	0.0000238215	0.9978
7	0.0000190752	0.9978
8	0.0000219753	0.9978
9	0.0000239714	0.9978
10	0.0000289705	0.9978
Average	0.00000020500	0.9978

The table 3 which showed the validation result presented the tenfold mean value for the key performance indicators for the 4G network. The average MSE result achieved is 2.05X 10^5Mu which is very good as it is approximately zero. The regression value achieved on the other hand is 0.9978 which is approximately 1 and hence very good too.

VII. CONTRIBUTION TO KNOWLEDGE

This study have produced a wormhole detection algorithm which is very reliable with regression value of 0.9978

VIII. CONCLUSION

This work has successfully developed and implemented an improved wormhole detection algorithm using machine learning technique. This new system was developed using artificial neural network to detect real time wormhole threat. This was done usinf artificial neural network and The work

designed various models which were used to implement the study, in line with Mathlab and other implementation toolbox. The average MSE result achieved is 2.05X 10^5Mu which is very good as it is approximately zero. The regression value achieved on the other hand is 0.9978 which is approximately 1 and hence very good too according to the work of Eliah and Ellen (2017) which identified MSE and R values close to the ideal as very good results.

REFERENCE

[1] Contel Bradford (2020)," 7 Most Famous Cloud Security Breaches"; Storage Craft Technology Corporation.

[2] Eliah K. and Ellen A (2017) "Neural Network Model for Predicting Student Achievement in blended courses at the University of Dar Es Salam" IJAIA; 8(2):23-35

[3] Giannetsos and T. Dimitriou (2014) "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks", J. Comput. Syst. Sci., vol. 80, no. 3, pp. 618-643.

[4] Khosroshahy M., DongyuQiu, and M.K. Mehmet Ali. (2013) "Botnets in 4G cellular networks: Platforms to launch ddos attacks against the air interface". In Mobile and Wireless Networking (MoWNeT), International Conference on Selected Topics in, pages 30–35

[5] Kolias C, G. Kambourakis, A. Stavrou, and S. Gritzalis (2016) " Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset". IEEE Communications Surveys Tutorials, 18(1):184–208,.

[6] Mehta A (2019) " Machine learning": https://www.digitalvidya.com/blog/types-of-neural-networks/ (Retrieved 9/7/2021).

[7] NabeelKhana, Adil Al-Yasiri (2016):The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies;(IoTNAT' 2016) Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework University of Salford, 43 CresentSalford, Manchester and M5 4WT, United Kingdom. Procedia Computer Science 94 (2016) 485 – 490 on Recent Advances in Information Technology (RAIT), 2012, pp. 131–136

[8] Nayak, A. Sahay and Y. Pandey (2013) "Detection and prevention of wormhole attacks in Manets using detection packet", Int. J. Sci. Eng. Res., vol. 4, no. 6, pp. 1216-1222.

[9] NicklasBeijar (2017), Zone Routing Protocol (ZRP), Helsinki University of Technology.

[10] Nivedha S.Hu C, A. Perrig, and D. B. Johnson (2015), "Wormhole attacks in wireless networks," IEEE Journal on Selected Areas in Communications., vol. 24, no. 2, pp. 370–380.

[11] Payaswini P, Manjaiah D.H (2013) "Challenges and issues in 4G – Networks Mobility Management" International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5; ISSN: 2231-2803 http://www.ijcttjournal.org Page 1247

[12] Singh, J. Singh and R. Singh (2016) "WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks", Mob. Inf. Syst.

[13] Suneetha D. Rathna Kishore, G.G.S.Pradeep (2019); Data Security Model Using Artificial Neural Networks and Database Fragmentation in Cloud Environment ; International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019 ,5972 Published By: Blue Eyes Intelligence Engineering & Sciences Publication

[14] Saxe J., Berlin K., (2015)" Deep neural network based malware detection using two dimensioninal binary program features; proceedings of the International Conference on Malicoius and Unwanted Software; Fajardo, Puerto Rico. 20-22