I. J. Computer Network and Information Security, 2017, 12, 29-35
Published Online December 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.12.04

Distributed Denial of Service Detection using Multi Layered Feed Forward Artificial Neural Network

Ismaila Idris, Obi Blessing Fabian, Shafi'i M. Abdulhamid
Department of Cyber Security, Federal University of Technology, Minna, Nigeria.
E-mail: ismi.idris@futminna.edu.ng, obiblessing33@gmail.com, shafii.abdulhamid@futminna.edu.ng

Morufu Olalere and Baba Meshach
Department of Cyber Security, Federal University of Technology, Minna, Nigeria
E-mail: lerejide@futminna.edu.ng, babameshach01@futminna.edu.ng

Received: 20 June 2017; Accepted: 10 August 2017; Published: 08 December 2017

***Abstract*—**One of the dangers faced by various organizations and institutions operating in the cyberspace is Distributed Denial of Service (DDoS) attacks; it is carried out through the internet. It resultant consequences are that it slow down internet services, makes it unavailable, and sometime destroy the systems. Most of the services it affects are online applications and procedures, system and network performance, emails and other system resources. The aim of this work is to detect and classify DDoS attack traffics and normal traffics using multi layered feed forward (FFANN) technique as a tool to develop model. The input parameters used for training the model are: service count, duration, protocol bit, destination byte, and source byte, while the output parameters are DDoS attack traffic or normal traffic. KDD99 dataset was used for the experiment. After the experiment the following results were gotten, 100% precision, 100% specificity rate, 100% classified rate, 99.97% sensitivity. The detection rate is 99.98%, error rate is 0.0179%, and inconclusive rate is 0%. The results above showed that the accuracy rate of the model in detecting DDoS attack is high when compared with that of the related works which recorded detection accuracy as 98%, sensitivity 96%, specificity 100% and precision 100%.

***Index Terms*—**DDoS attacks, DDoS detectors, Artificial Neural Network, Feed Forward Artificial Neural Network.

I. Introduction

Distributed Denial-of-Service (DDoS) attack is a serious situation facing the world at large. This is perpetuated when large amount of internet packets are sent from numerous systems that have been infected (usually called salves/zombies) to a victim's network, consuming it resources (bandwidth), slowing down network and performance of the system, causing services to be unavailable and most times destroys the system. These activities make it difficult for legitimate users to use the targeted system. DDoS attack is one of the attacks that cause menace to the stability of the Internet, affecting services like online applications and procedures, system and network performance, emails and other system resources. Fig. 1. Shows example of a DDoS attack, it explains how the attack is carried out.

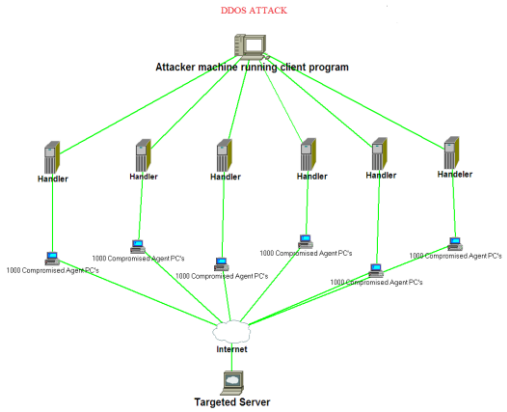

Fig.1. An Example of DDoS Attack

Many researchers have worked on DDoS attacks using different techniques, algorithm and datasets to give solution to the problem. There are many reasons why some people engage in DDoS attacks these includes; financial benefit, political tussle and fun for hackers as the case may be.

The aim of this paper is to detect DDoS attacks using multi layered feed forward FFANN technique and its main contributions are to enhanced the multi-layer Feed-Eorward ANN (FFANN) model to detect DDoS attacks and evaluate the performance of the developed model.

The remaining sections of the paper are organized as follows: section II presents related literatures in DDoS and ANN classification. Section III details the concept of ANN optimization as utilized in the methodology. Section IV chronicles the results obtained in the

experimental simulation and section V describes the summary, conclusion and future recommendations.

II. Related Works

Many research works has been done on DDoS attacks and in these works several algorithms, models and techniques are proposed and used the researchers to detect the attacks in simulated or real time environment. In [1] ANN was used to detect DDoS attacks the result obtained was compared with another result gotten from Bayesian, entropy and decision tree. The researchers were able to detect users' requests, how users access resources, and the way they communicate with data. The samples of their observation were sent into the detection mechanism to test for abnormalities in their request. The writers in [2] used a technique in neural network called Learning Vector Quantization (LVQ) to identify attacks. LVQ model was able recognized pattern, compress data and classify data with multiple classes. The datasets with qualitative variables was used for the experiment, since all the variable are not numerical in nature, it was normalized so that the neural network can learn it. [3] formulated model for Probabilistic Neural Network Based Attack Traffic Classification which detected a range of DDoS attacks and flash events. Their work centered on classifying Distributed Denial of Service attacks and Flash Events using Radial Basis Function Neural Network (RBFNN), Bayes inferences and Bayes decision rule as their tool for classification. It worked well because it was able to classify and make a distinction between DDoS attack traffic and normal traffic. [4] used entropy variation and neural network to discover the relationships that exist between compromised systems in the network and to identify the total number of compromised systems involved in the attack. The model predicts the class of an attack using a feed-forward neural network. The authors [5] used entropy variation and packet marking mechanisms to identify the source of the packet considering the router each packet passed through. [6] Worked on detection and prevention of DDoS attack using Energy Weight Monitoring System (EWMS) as the tool and model. The technique was able to save the power of nodes in a network and avoid transmission of packets unnecessarily. The authors in [7] formulated a model that uses three layers to verify and validate traffic and users into a network, although it time consuming when distinguishing genuine and illegal users. The algorithm allows only genuine user to have access to the server. Puzzle, mac filtration and cryptography based are the three layers used. [8] Reviewed various researches on DDoS attacks in cloud computing, intrusion detection, prevention, and mitigation. They proposed a mechanism that detects DDoS attack in the cloud. In [9] in other to ensure fairness between participants in multi-party, simulated a denial of service attack against two fair multi-party computation.

[10] proposed a model that uses Artificial Neural Network and Snort – Al to detect both known and unknown DDoS attacks in real time environment. The result gotten was compared with these related works Chi – square, snort, Support Vector Machine, Probability Neural Network, k – PCA, BP, and PSO. [11] formulated a model called GMDH, this model provides security access which makes it easy to detect DDoS attack. Their work was classified using three ranking systems which are: GMDH, gain ratio and technique information, the result gotten by the model shows that it has high attack detection rate. The writers [12] attempt to solve the anomalies in internet and web services, observed the behaviour of some frame works containing well-known web services to determine the presence and effect of DDoS attacks on the web services, normal services of a computer and when the system is idle. The security testing tool used is called WSF Aggressor. In a paper written by [13] fuzzy logic estimator was used to develop a model that will detect DDoS attacks on online environment. The model successfully detected abnormal IPs before the victim services will be used up completely as a result of the attack. The authors [14, 18] reviewed various researches that have been carried out on IP trace back and they provided broad analysis of different IP trace back approaches. They explained many research questions of the papers they have reviewed so that the current trends in would be clearly understood. [15, 17] formulated an attack called puppet attack, the attack was developed to cause denial of service in AMI network. The writers then proposed a model that could effectively detect and prevent the attack. [16] reviewed 96 research publications done from 2009 to 2015 on DDoS attack and defense approaches in cloud computing. They presented taxonomy of the theoretical structure for DDoS mitigation in the cloud based on change point detection.

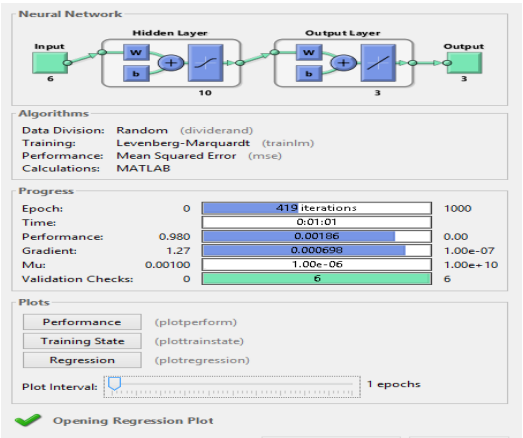

Fig.2. Structure of ANN Model

III. Artificial Neural Network Concepts

Artificial Neural Network (ANN) consists of neurons which are also called processing elements. It takes inputs from dataset that have been preprocessed and normalized, passed it to the hidden layers for processing and gives output [10, 19]. ANNs is used by most researchers to develop systems that will provide solution to problems, it

has the structure of human brain and is applied in many research areas like science, medicine computing among others. The input nodes are linked to the neurons in the hidden layer, the hidden layer is also linked to the neurons in the output layer. The weight coefficient and bias is used to compute the threshold value. The threshold value defines the significance and accuracy rate of the neural network. The value of the weighted coefficient and bias is modified while training the model as shown in Fig. 2.

A. The Architecture of our Neural network Model

ANN is an efficient mechanism for detecting DDoS attack. For this work multilayer feed-forward network will be used because it can make prediction as well as classification. The DDoS detection model was built using Neural Network which has three layers that are logically arranged. The model consist of six input layers which are Destination byte, source byte, Duration, service count protocol bit 1and protocol bit 2, ten hidden layers which consist of activation function and transfer function then three output layers which are represented as OBT1, OBT2 and OBT3.

B. DDoS Attack Detection Framework

The DDoS attack detection framework shows the chain of activities that takes place in the detection system ranging from input of dataset, preprocessing and filtering of the dataset to get just the normal flow and DDoS attack traffic and the transformation of connection records. The framework of the DDoS attack detection is shown in Fig. 3.

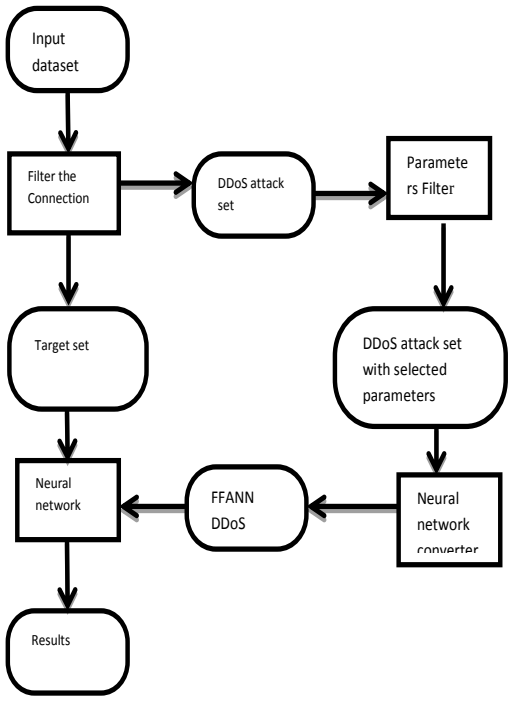

Fig.3. DDoS Attack Detection Framework

C. Dataset

The datasets used for training and testing the model is the KDD99 DDoS attack set. it was separated into two part in the ratio of 70:30. For training the model 70% of the dataset was used and 30% was used for testing. These dataset was preprocessed, normalized and filtered into of instances.

D. ANN Performance Metrics

Specificity: this is the portion of the test set that is predicted as correct. It is also referred as True Negative Rate (TNR).

TNR is the amount of samples that are properly rejected from the class [20, 21, 22].

$$\text{TNR} = \frac{TN}{TN+FP} \quad (1)$$

Sensitivity: this is the detection or the portion of the test set that the model predicts correctly. It is also referred to as True Positive Rate (TPR). It is denoted as

$$\text{TPR} = \frac{TP}{TP+FN} \quad (2)$$

False Positive Rate: it is also known as the false alarm rate, it is the portion of the test set that the model predicts falsely as positive when it was actually negative. It is denoted as

$$\text{FPR} = 1 - \text{Specificity} = \frac{FP}{TN+FP} \quad (3)$$

False Negative Rate: it is the portion of the test set that the model predicts falsely as negative when it is actually positive. It is denoted as

$$\text{FPR} = 1 - \text{Sensitivity} = \frac{FN}{TP+FN} \quad (4)$$

Accuracy: this is the portion of the test set that the model predicts correctly. It is denoted as

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

Precision: it is the portion of the test set that the model predicts incorrectly. It is denoted as

$$\text{Precision} = \frac{TP}{TP+FP} \quad (6)$$

IV. RESULTS

ANN structural model: figure 1 depicts the architecture structure of the model. The model has six input nodes, ten hidden layers three output layers and three output nodes. It also contains the activation function, number of epoch, algorithm and all one need to know about the model. An epoch is the number of iteration done in complete training set. At the end of the iteration the weights of the neurons are adjusted to reduce mean squared error in all the Epoch.

To get a result with high accuracy rate the model needs

to be trained for some number of time, in the model training phase to get the least mean square error and better performance model for the work, 419 iterations (epoch) was done with 310 iterations in the testing phase.

At the end of the training phase 419 epochs was recorded but the preeminent validation performance was 0.0016862 at epoch 413. In Fig. 4 the graph of Mean Squared Error (MSE) against Epochs was presented.

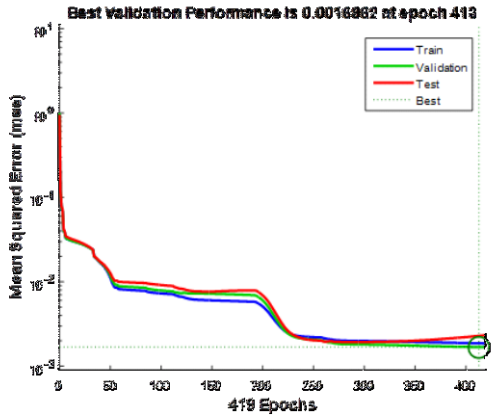

Fig.4. Performance State

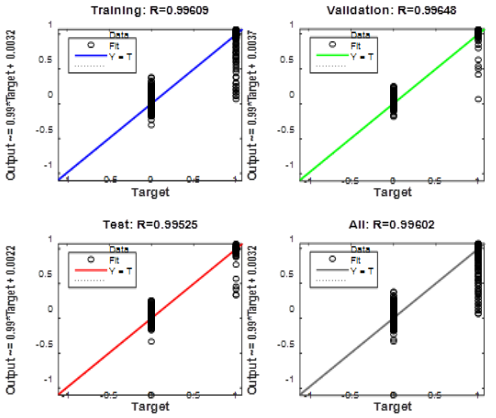

Fig.5. Regression State of the Training Phase

Figure 5 presents the regression state of the training phase as, the training set: R= 0.99609, test set: R = 0.99525, validation: R = 0.99648 and the overall: R= 0.99602. This shows that our result is accurate because in regression the more closer a value is to 1 the more accurate it is. Following this statement the result gotten from this state is accurate because it is closer to 1.

Figure 6 presents graph of the threshold value of the model against accuracy value, after training the model a graph plotted through it was over fitted, because huge instances was used to train the data. At the beginning of model training the system is learning the data in the set while at the end of the training phase the system would have finished learning the set and will be resting to get an accurate result, 0.2 and 0.8 are the points that was considered for plotting the graph.

Figure 7 shows the standard deviation of the model against threshold value. This helps in getting a reliable threshold value and standard deviation that will be minimal.

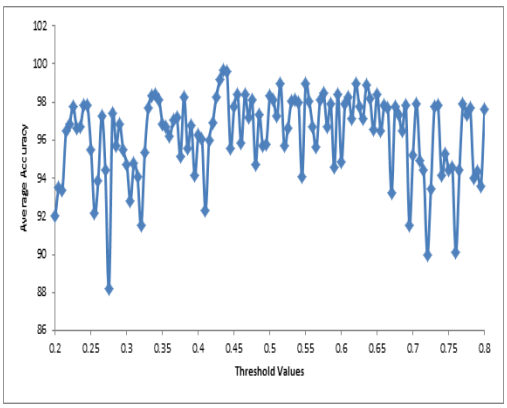

Fig.6. Over Fitted Graph for Threshold Value and Average Accuracy

Figure 7 depicts the generalized training set which is properly fitted and understandable. To make the graph clearer points 0.4 – 0.6 was used. After training model three values were close to each other they are 99.15668203 = 0.43, 99.68202765 = 0.435 and 99.59907834 = 0.4 but most accurate threshold value was 0.435 which is the value for global maximum and global minimum deviation.

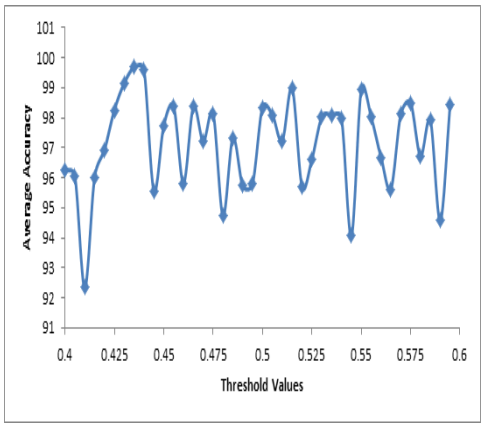

Fig.7. Generalized /Fitted Graph for Threshold Value and Average Accuracy

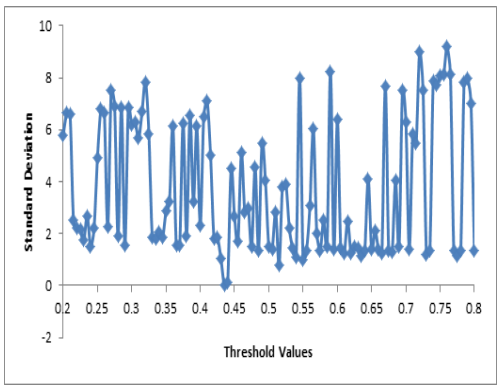

Fig.8. Graph for Standard Deviation

A. Testing Dataset Performance

Fig. 9 presents the ANN Structural Model and Parameters used in the testing phase.

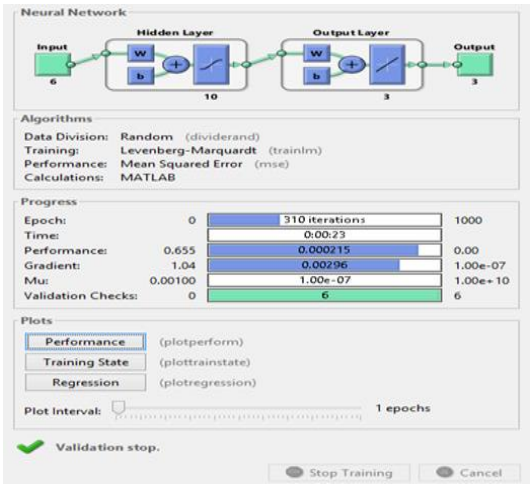

Fig.9. ANN Structure for the Testing Phase

Fig. 10 presents the graph of the mean squared error in the testing phase and it was observed that the number of (epochs) was 310 and at 304th iteration the best validation performance was gotten which is 0.00013525 and the least mean squared error was gotten at this point.

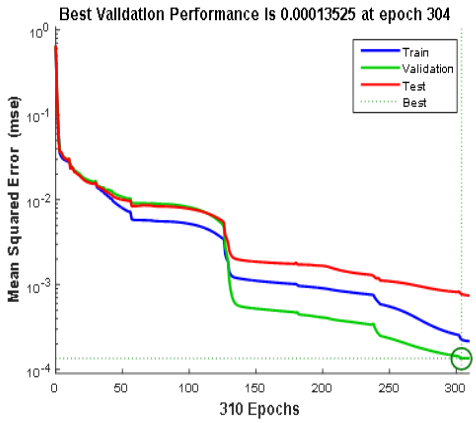

Fig.10. Mean Squared Error for the Testing Phase

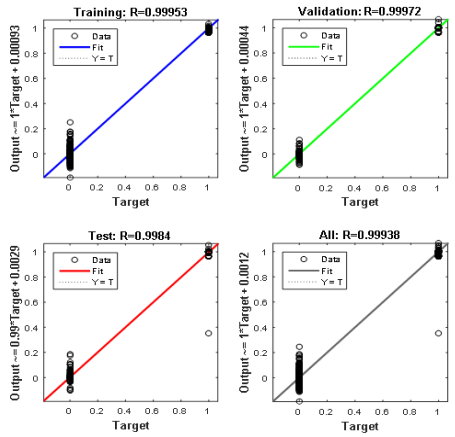

Fig.11. Regression State for the Testing Phase

Figure 11 presents the regression state of the testing phase it was observed the result produce by the regression state of the testing phase is more accurate than that of the training phase. Which implies that the model developed was able to detect DoS attacks accurately.

In the testing phase the same threshold value used during the train was used too. To get the best accuracy value the model was trained twenty (20) times, the best ten (10) values was selected and their average was computed. In Table 1 the accuracy values of the ten (10) testing phase that was used to compute the average accuracy is shown.

Table 1. Accuracy (Value) of the Testing Phase

S/N	Accuracy
1	99.99
2	99.9462
3	97.7945
4	100
5	100
6	97.4718
7	99.7848
8	94.9435
9	99.9462
10	97.5256
Average Accuracy	98.7413

B. Model Performance and Evaluation Analysis

Table 2 shows the performance and evaluation analysis of our model.

Table 2. Performance and Evaluation Analysis of Our Model

Parameter tested for	Result Accuracy
Correct Rate	99.98%
Error Rate	0.017931%
Inconclusive Rate	0%
Classified Rate	100%
Sensitivity	99.97%
Specificity	100%
Precision	100%

After the experimental analysis of the model was carried out the results obtained was compared with the results obtained by the baseline literatures. The comparison will be shown in Table 3.

Table 3. Comparison between Our Methods and Other Related Works

Method	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)
Our model	99.98	99.97	100	100
Saied A et al	98	96	100	100
Snort	93	90	97	96
PNN	92: 97	NA	NA	NA
BP	90	NA	NA	NA
Chi – square	94	92	NA	NA

The work has the following contribution to knowledge, after carrying out the simulated experiment, from the results shown in Table 2, it was observed that the model outperformed the other models in the baseline works with high detection accuracy, precision specificity and sensitivity, as shown in Table 3.

When the model was tested and evaluated the following was recorded, both real and malicious traffic was found in the dataset and the model detected the DDoS attacks during the training and testing phase. The result from our experiment indicated that inconclusive rate was 0% which is also the rate of false positive and 0.003% was the false negative rate recorded.

V. Conclusion and Recommendations

This research work studied the problems caused by Distributed Denial of Service attacks and its negative impacts in every aspect of the society, and proposed a model that will detect DDoS attacks. The performance of the model was evaluated based on these performance metric; sensitivity precision, accuracy and specificity. Related works were reviewed, the model was built using Multi – layered feed – forward Artificial Neural Network (FFANN). The dataset used was preprocessed and used to train the model, analyzes the results of the experiment was discussed and recommendations were given for further work.

Supervised learning method was used to developed a model that was able to detect DDoS attacks in the following protocol layer of the network TCP, UDP and ICMP using six input features differentiate normal traffic from DDoS attacks. Source byte Destination byte, service count, Duration, and protocol bit are used as input features. KDD99 dataset was to train the model using multi layered feed forward ANN. Dataset preprocessing was the first step taking, after that it was divided into two parts in the ratio of 70:30. 70% of the data was used for training while the other 30% was used for testing. The results obtained from the model were evaluated using the performance metrics and then compared with that of the baseline literatures. The model performs better with accuracy rate of 99.98%, sensitivity rate 99.97%, 100% specificity, 100% precision, and 0.0179% error rate.

In other to get a more accurate model the following suggestions are recommended, more instances should be used to train the dataset, parametric evaluation of this model should be done more work should be carried out on prevention and mitigation techniques for the DDoS attacks the model has detected.

Acknowledgements

The authors would like to acknowledge and appreciate the Department of Cyber Security, Federal University of Technology, Minna, Nigeria for their support.

References

[1] Jie-Hao C.; Feng-Jiao C., Z. (2012). "DDoS defense system with test and neural network,."in: Proceedings of the IEEE International Conference on Granular Computing (GrC), Hangzhou, China pp.38 - 43.

[2] Li J.; Liu Y.; Gu L. (2010). "DDoS attack detection based on neural network,." in: Proceedings of the 2nd International Symposium on Aware Computing (ISAC), Tainan: pp. 196–199.

[3] Akilandeswari V.; Shalinie S.M. (2012). "Probabilistic neural network based attack traffic classification." in: Proceedings of the Fourth International Conference on Advanced Computing (ICoAC), Chennai: pp. 1- 8.

[4] Gupta B.B., Misra M., (2011). "ANN based scheme to predict number of zombies in a DDoS attack." international Journal on network security 13(3):pp. 216–225.

[5] Yu S., R.Doss and W.Jia, (2011). "Traceback of DDoS attacks using entropy variations.", IEEE Trans. Parallel Distrib. Syst 22(3): pp. 412–425.

[6] Gaikwad, A. P. (2015). "Comparative analysis of the Prevention Techniques of Denial of Service Attacks in wireless Sensor Network." International Conference on Intelligent Computing, Communication & Convergence 48 pp.387 – 393.

[7] Prakasha, A. Sri M. S., T .Sai Bhargava and N. Bhalajia (2016). "Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture." 4th International Conference on Recent Trends in Computer Science & Engineering 87: pp. 27 – 280.

[8] Andrew M., Carlin H. O. A. (2015). "Defence for Distributed Denial of Service Attacks in Cloud Computing." The International Conference on Advanced Wireless, Information, and Communication Technologies 73: pp. 490 – 497.

[9] Beekman, G. J. (2016). "A Denial of Service attack against fair computations using Bitcoin deposits." pp.144–146.

[10] Alan Saied, R. Tomasz Radzik O. (2016). "Detection of known and unknown DDoS attacks using Artificial Neural Networks." pp.385–393.

[11] Zubair A.Baig, S. M. S., and Abdul Rahman Shaheen (2013)."GMDH - based networks for intelligent intrusion detection." pp. 1731–1740.

[12] Rui Andr é Oliveira, N. L. M. V. (2015). "Assessing the security of web service frameworks agains Denial of Service attacks." pp. 109: 18–31.

[13] Stavros N. Shiaeles, V. K., Alexandros S. Karakos, Basil K. Papadopoulos (2012). "Real time DDoS detection using fuzzy estimators." 31

[14] Karanpreet Singh, P. S. (2016). "A systematic review of IP trace back schemes for denial of service attacks." computers & s e c u r i t y 56:pp. 111–139.

[15] Ping Yi, T. Z., Qingquan Zhang, Yue Wua and Li Pan (2016). "Puppet attack: A denial of service attack in advanced metering infrastructure network." pp.325–332.

[16] Opeyemi Osanaiye, K. (2016). "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework." 67:pp. 147–165.

[17] Alomari, E. B. Ga. S. K. (2012). "Botnet-based distributed denial of service (DDoS) attacks on webservers." classification and art Int. J. Comput. Appl. 47(9): pp.24–32.

[18] Munivara K. Prasad, A. (2014). "DoS and DDoS Attacks: Defense, Detection and Trace back Mechanisms -A Survey." Global Journal of Computer Science and Technology: E Network, Web & Security 14(7).

[19] Abdulhamid S. M., Abd Latiff M. S., H. Chiroma, O. Osho, G. Abdul-Salaam, A. I. Abubakar, and T. Herawan

(2017), "A Review on Mobile SMS Spam Filtering Techniques", IEEE Access, DOI: 10.1109/ACCESS.2017.2666785.
[20] Gupta, R., & Shukla, P. K. (2015). Performance Analysis of Anti-Phishing Tools and Study of Classification Data Mining Algorithms for a Novel Anti-Phishing System. *International Journal of Computer Network and Information Security (IJCNIS)*, *7*(12), 70.
[21] Adebayo, O. S., Ugiomoh, D. O., & AbdulMalik, M. D. (2013). The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity. *International Journal of Computer Network and Information Security*, *5*(5), 9.
[22] Yasin, Adwan F. "Spam Reduction by using E-mail History and Authentication (SREHA)." *International Journal of Computer Network and Information Security* 8, no. 7 (2016): 17.

Authors' Profiles

Dr. Ismaila Idris is with the Deparment of Cyber Security Science. He obtain his Bachelor degree with Federal University of Technology, Minna. M.Sc. with university of Ilorin and PhD degree with University of Teknologi Malaysia. His research interest are Information Security, Data Mining, Machine Learning, Evolutionary Algorithm.

Obi Blessing Fabian is a Masters student in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. She obtained her Bachelor degree in Computer Science in the same University with Second Class Upper. She did her National Youth Service Corp (NYSC) in Niger State School of Health Technology as a lecturer, currently she is working as a teacher in NECO Staff School Minna, Niger State Nigeria. Obi obtained her First School Living Certificate from Aliyu Mustapha Academy Yola, Adamawa State, Nigeria in the year 1999, Senior School Certificate and West Africa Senior School Certificate from Federal Government Girls' College Yola, Adamawa state Nigeria.

Shafi'i Muhammad ABDULHAMID received his PhD in Computer Science from Universiti Teknologi Malaysia (UTM), MSc in Computer Science from Bayero University Kano (BUK), Nigeria and a Bachelor of Technology in Mathematics/Computer Science from the Federal University of Technology Minna, Nigeria. His current research interests are in Cyber Security, Cloud computing, Soft Computing and BigData. He has published many academic papers in reputable International journals, conference proceedings and book chapters. He has been appointed as an Editorial board member for UPI JCSIT and IJTRD. He has also been appointed as a reviewer of several ISI and Scopus indexed International journals such as JNCA Elsevier, ASOC Elsevier, EIJ Elsevier, JKSU-CIS Elsevier, NCAA Springer, BJST Springer, IJNS, IJST, IJCT, JITE:Research, JITE:IIP, JAIT, IJAER and JCEIT SciTechnol. He is a member of IEEE, International Association of Computer Science and Information Technology (IACSIT), Computer Professionals Registration Council of Nigeria (CPN), International Association of Engineers (IAENG), The Internet Society (ISOC), Cyber Security Experts Association of Nigeria (CSEAN) and Nigerian Computer Society (NCS). Presently he is a lecturer at the Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.

Morufu Olalere is a lecturer in the Department of Cyber Security Science, Federal University of Technology Minna, Niger State, Nigeria. He graduated in 2005 from the Department of Industrial Mathematics and Computer Science of the Federal University of Technology Akure, Nigeria with Bachelor of Technology in Industrial Mathematics. He bagged MSc. in Computer science from the University of Ilorin, Kwara State, Nigeria in 2011. He completed his PhD in Security in computing in 2016 from the Faculty of Computer Science and Information Technology of the University Putra Malaysia, Selangor, Malaysia. He has a number of professional certifications including OCH, CWSA and CWSP. He is a member of the following professional bodies; The Computer Professionals Registration Council of Nigeria (CPN), The Nigeria Computer Society (NCS), The Institute of Electrical and Electronics Engineers (IEEE) Computer Society, and The Association for Information Systems (AIS). His current research interests include: Access control, Biometrics, Information Security, and Network Security.

Baba Meshach is a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He obtained her Bachelor degree in Electrical Computer Engineering in Federal University of Technology, Minna, Nigeria.
Email: babameshach01@futminna.edu.ng

How to cite this paper: Ismaila Idris, Obi Blessing Fabian, Shafi'i M. Abdulhamid, Morufu Olalere, Baba Meshach,"Distributed Denial of Service Detection using Multi Layered Feed Forward Artificial Neural Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.12, pp.29-35, 2017.DOI: 10.5815/ijcnis.2017.12.04

