Covenant Journal of Informatics & Communication Technology. Vol. 8 No. 2, December, 2020
ISSN: *print* 2354 – 3566 *electronics* 2354 – 3507 DOI:

An Open Access Journal Available Online

Multi-layer Perceptron Model for Mitigating Distributed Denial of Service Flood Attack in Internet Kiosk Based Electronic Voting

Jiro Aphia Almustapha, Olayemi Mikail Olaniyi, Ibrahim Mohammed Abdullahi, Juliana Ndunagu, Francis Bukie Osang

Department of Computer Science, Federal Polytechnic, Bida-Niger State, Nigeria
Department of Computer Engineering, Federal University of Technology, Minna-Niger State, Nigeria
Department of Computer Science, National Open University, Abuja, Nigeria
aphijee@gmail.com, mikail.olaniyi@fut.minna.edu.ng, amibrahim@futminna.edu.ng, jndunagu@noun.edu.ng

Received: 16.07.2020 Accepted: 27.11.2020
Date of Publication: December, 2020

Abstract— Distributed Denial-of-Service (DDoS) flood attack targeting an Internet Kiosk voting environment can deprive voters from casting their ballots in a timely manner. The goal of the DDoS flood attack is to make voting server unavailable to voters during election process. In this paper, we present a Multilayer Perceptron (MLP) algorithm to mitigate DDoS flood attack in an e-voting environment and prevent such attack from disrupting availability of the vulnerable voting server. The developed intelligent DDoS flood mitigation model based on MLP Technique was simulated in MATLAB R2017a. The mitigation model was evaluated using server utilization performance metrics in e-voting. The results after the introduction of the developed mitigation model into the DDoS attack model reduced the server utilization from 1 to 0.4 indicating normal traffic. MLP showed an accuracy of 95% in mitigating DDoS flood attacks providing availability of voting server resources for convenient and timely casting of ballots as well as provide for credible delivery of electronic democratic decision making.

Keywords/Index Terms— Distributed Denial-of-Service (DDoS), Flood Attacks, Internet Kiosk Voting System, Multilayer Perceptron and Simulink Blocks.

1. Introduction

The Internet Kiosk Voting has the potential to provide convenient voting process. Although, Internet Kiosk voting has the advantage for conducting transparent election, it is highly susceptible to varieties of attacks if not properly secured Musial-Karg *et al.,* 2017. These attacks could breach security and lead to e-voting systems being unreliable during an election and thus questioning required confidences and trust of electronic democratic decision making. E-government is an evolving approach to e-governance that Nigeria is currently adopting as identified in Jonathan *et al.,* 2014 and Edikan *et al.,* 2019. An e-government's e-voting system should provide secure, reliable e-voting systems during the election process, and voters' should be able to cast votes in a timely manner.

Distribute Denial of Service (DDoS) flood attacks which include User Datagram Protocol (UDP), Smurf, Hyper Text Transfer Protocol (HTTP) flood and SQL Injection DDoS (SIDDoS) involves sending large number of packets to the victim server with the aim of slowing down the network Alkasassbeh *et al.,* 2016.

The goal of a DDoS flood attack on an Internet Kiosk Voting scenario is to create packet traffic congestion by consuming server resources, such as memory and storage space which in turn causes the e-voting experience to be slow or unresponsive during the voting process Al-Ameen and Talab *et al.,* 2013. By implication, the availability of the e-voting server is affected and this may lead to unsuccessful casting of electronic ballots. According to Musial-Karg *et al.,* 2015, voting system availability, confidentiality and integrity are security issues that must be addressed in the e-voting systems. An e-voting system's server is available when there is no delay while voters are accessing the voting website during the voting process.

In this paper, we present a Feed Forward Artificial Neural Network algorithm called Multilayer Perceptron (MLP) model capable of detecting DDoS flood attack from legitimate traffic is presented. The model has the advantage of recognizing and preventing DDoS flood attacks and forward traffic quickly and efficiently, which in turn improves the Internet Kiosk Voting system's performance in terms of voting server utilization and load response time.

This paper is organized into sections with Section I including a brief explanation of e-voting as it relates to DDoS environment and providing a rationale for the selection of this research area. Section II contains definition of main terms and contains theoretical frameworks that have been previously introduced to the research area on DDoS attacks on Internet Kiosk voting. Section III explains the research process and design and choice of data collection and tools used in this research, while Section IV presents Results and Discussion, and Section V concludes and summarizes the achievement of our research aim and objectives as well as acknowledging the limitations of this study and highlighting future studies in this same research area.

2. Literature Review

An overview of the techniques used in securing e-voting systems are explained with the help of previous related researches starting with the research work presented in Patil *et al.,* 2015 explaining how an e-voting system using Dactylogram, biometric-security system with a one-time password generating systems as well as Face detection system for verifying voters' image can be used to secure vital related information during the process of voting. In comparison with other biometrics system, using the dactylogram and face recognition have distinct compensations. Face images can be captured by maintaining certain distance without touching the person being identified, and the identification does not require communication with the voter. Face recognition serves the crime deterrent purpose because face images that have been captured and stored can be useful in identifying persons involved later. It therefore supports the required confidence and trust required of electronic decision making process through voting.

In Paul *et al.,* 2012, an online voting authentication technique was proposed, which provided biometrics as well as password security to voter accounts. This system improves the security of online voting as unauthorised users have to discover the secret key, pin number, fingerprint and facial image before attempting to break into the voting system. SHA 256 used for hashing is replaced with MD5 in order to improve the speed

Voters are first identified by their facial image by using Principal Component Analysis (PCA). Second step is the fingerprint recognition and lastly steganographic method is used to merge the secret key and pin number with the cover image which results in a fingerprint image. This system greatly provides secure election procedure by preventing hackers from finding secret key, pin number, fingerprint and facial image. Message-Digest Algorithm 5 (MD5) is used for hashing to improve speed of processing in e-voting system.

Similarly, Olaniyi *et al.,* 2013 proposed a Stegano-cryptographic model for securing votes cast in Electronic Kiosks placed at designated poll sites. The model provides accurate comparison of voters' fingerprint with database template and accurate remote response to visual response on the grid in mobile voting as well as verification of voters ID. Frequency domain video steganographic technique, which produces stego-video provides confidentiality of submitted votes to application server for decryption by the administrator. Memory resources and multiple computational requirements of RSA were taken into consideration by limiting RSA cryptosystem ONLY for e-voting process. The proposed concurrent, multilayer (stegano-cryptographic) and multimedia e-voting model resulted in high imperceptibility index, high robustness to attacks and high payload capacity in image and video when compared with models in Katiyar *et al.,* 2011 and Okediran *et al.,* 2011, which tackled security requirements in piece-meal.

2.1 Categories of Machine Learning Techniques used for Mitigating DDoS Flood Attacks

According to Odusami *et al.,* 2020, machine learning gave the highest proportion of 36% for detecting DDoS attacks as compared to web user features at 8% and request stream during absolute time interval at 12%. Other works using machine learning to detect DDoS attacks especially in e-voting include Syed *et al.,* 2018, with their proposed hybrid e-voting systems employed to use fingerprint and face recognition for voters' identification and documented a result of 91% accuracy in identifying voters based on face recognition to curb the multiple vote problems. Their research did not address voting server availability during election process as when compared with our proposed simulated model. Research works have been conducted in the areas of cryptography and biometrics to address the security issues of system confidentiality and system integrity. In addition, research works involved in the development and implementation of

DDoS detection models based on Artificial Neural Network and packet filtering techniques have been proposed and these research works addressing availability in network systems especially in e-voting is limited to DDoS attack identification.

DDoS detection approaches can be categorized into supervised, semi-supervised and unsupervised machine learning algorithms. In supervised detection DDoS detection approaches can be categorized into supervised, semi-supervised and unsupervised machine learning algorithms. In supervised detection approach, a trained dataset comprising of input data and output classes is used to extract the hidden functions and predict the class of incoming packet instances Aggarwal et al., 2015. Examples include classification techniques, such as Random Forest, Naive Bayes and Multilayer Perceptron (MLP) algorithms as shown in Almustapha et al., 2019 were the result showed an improvement in the accuracy, precision and recall when 9 attributes were used for classification to achieve an accuracy of 98.56%, 96.89% and 98.65% for Random Forest, Naïve Bayes and MLP concluding that MLP had a better value of 98.7 compared to 98.6 and 97.3 for Naïve Bayes and Random Forest respectively. In Alkasassbeh et al., 2016, a network simulator (NS2) was used to record different types of DDoS attacks, namely Smurf, UDP-Flood, HTTP-Flood and SIDDOS that target the Application and Network layers. Three machine learning algorithms (MLP, Random Forest, and Naïve Bayes) were applied on the collected dataset to classify the DDoS attacks with MLP classifier achieving the highest accuracy rate of 98.63%.

Aljumah et al., 2017 proposed a DDoS detection system using artificial neural network to identify attack on data traffic from authentic data traffic and the research was evaluated based on the basis of precision, recall and accuracy performance metrics to achieve a 98.0% accuracy provided by applying back propagation learning algorithm and sigmoid invoking function.

In Abayomi-Zannu et al., 2019, their proposed m-voting system made use of block chain technology and Multi-Factor Authentication for securing user’s votes as well as ensuring the authentication of legitimate voters.

Furthermore, Odusami et al., 2019 proposed a Long Short Term Memory (LSTM) algorithm were the Tensor Flow Backend will be used to code the algorithm to detect Layer 7 DDoS attack. A summary of related works on E-voting in terms of their security goals is shown in Table 1.

2.2 Review of Related Works Using Machine Learning to Secure E-Voting

In recent years, machine learning techniques have been applied in conventional network environments, cloud environments and software-defined network architecture to classify DDoS attack traffic from legitimate traffic. In this regard, a trained neural network model was deployed and

tested in a network environment and the model was able to detect Transmission Control Protocol (TCP) attack, User Datagram Protocol (UDP) Flood attack and Ping Flood attack Cheng *et al.,* 2018. Supervised learning algorithms perform well in classifying DDoS attacks from normal traffic and such algorithms can easily be updated with new data using back propagation technique. These algorithms require the availability of huge volumes of labelled network traffic dataset to learn from effectively.

Table I. Summary of Related Works on E-Voting

S/No	***Author(s)***	***Title of Publication***	***Year of Publication***	***Technique***	***Function of the Technique***	***AIC (Availability, Integrity and Confidentiality) Triad***		
						A	***I***	***C***
1.	Katiyar, S. *et al.*	Online Voting System Powered by Biometric Security Using Steganography	2011	Biometric scheme using Cryptography and Steganography as well as password security to voters' account	This technique merges secret key with the cover image on the basis of key image to providing secure authentication of voters	X	√	X
2.	Paul, L. & Anilkumar, M. N.	Authentication for Online Voting using Steganogarphy and Biometrics	2012	Online Voting Authentication Model using Biometric and Steganographic Method	Provide a more secure e-voting system	X	√	X
3.	Olaniyi, O. *et al.*	Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions	2013	Multifactor Authentication and Cryptographic Hash Function methods.	Prevent hacking of votes	X	√	X
4.	Patil, R. *et al.*	A Secure E-Voting System Using Face Recognition and Dactylogram	2015	Proposed a Secure E-voting System using Face Recognition and Dactylogram Method	Provide a more secure e-voting system	X	√	X

5.	Alkasassbeh, M. *et al.*	Detecting Distributed Denial of Services Attacks Using Data Mining Techniques.	2016	Proposed system for collecting new dataset made up of different types of DDoS attacks and normal data traffic	A record of the dataset could be used to train Artificial Neural Network to detect DDoS attacks	X	X	X
6.	She, C. *et al.*	Detection of Application Layer DDoS by Clustering Algorithm	2016	A detection mechanism was proposed using Affinity Propagation (AP) clustering algorithm	Identify Application Layer DDoS attacks and prevent them using Internet Protocol (IP) blacklisting	X	X	X
7.	Aljumah *et al.*	Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks	2017	An Artificial Neural Network DDoS Detection System for flagging off malicious data traffic from the genuine traffic was proposed	The trained solution was used to identify TCP and UDP attacks from authentic data traffic	√	√	X
8.	Cheng, J. *et al.*	Adaptive DDoS Attack Detection Method Based on Multiple-Kernel Learning	2018	Simple Multiple-Kernel Learning (SMKL) Model	Classifier for identifying early DDoS attack in a cloud environment	X	X	X
9.	Abayomi-Zannu, T. P. *et al.*	A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication	2019	M-Voting System harmonized mobile devices with the use of Blockchain Technology, Multi-Factor Authentication to secure votes	The framework was used to secure votes cast and authenticate voters	X	√	X
10.	Almustapha, A. *et al.*	Detection and Analysis of DDoS Attacks in Internet Kiosk Voting Using Machine Learning Algorithms	2019	Proposed DDoS mitigation model for detecting DDoS Flood attack traffic from legitimate data traffic	The trained Multilayer Perceptron Model was used to identify and block DDoS attacks from reaching voting server while allowing legitimate data traffic	√	√	√

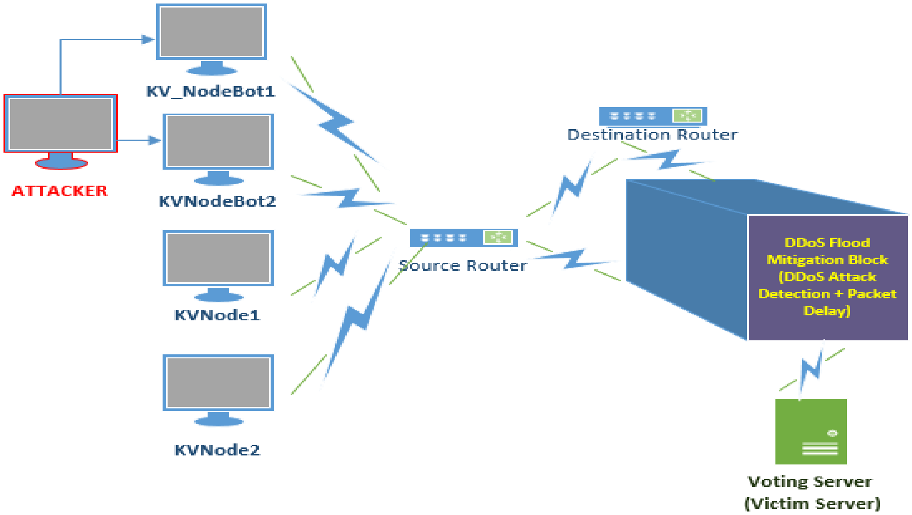

KV_NodeBot1
ATTACKER
KVNodeBot2
KVNode1
KVNode2
Source Router
Destination Router
DDoS Flood Mitigation Block (DDoS Attack Detection + Packet Delay)
Voting Server (Victim Server)

Figure 1. Architecture of the Proposed DDoS Mitigation Model

In She *et al.*, 2016, a detection mechanism based on Affinity Propagation algorithm was proposed and the normal users' behaviour models were built to detect application layer DDoS attacks and blacklist abnormal user Internet Protocol (IP) addresses.

In summary, machine learning algorithms were studied in this work with the goal of providing better results in terms of accurately recognizing and preventing DDoS attacks early enough to reduce massive damages to e-voting networks in terms of either cost of network infrastructure or manipulation of votes and election results.

Furthermore, the goal of this research is to bridge that gap between classifying DDoS attack in network environment with the prevention of such attacks from reaching vulnerable servers in an e-voting environment using machine learning algorithms, such as MLP to develop intelligent models for mitigating DDoS flood attacks in Internet Kiosk Voting systems.

3. Research methodology

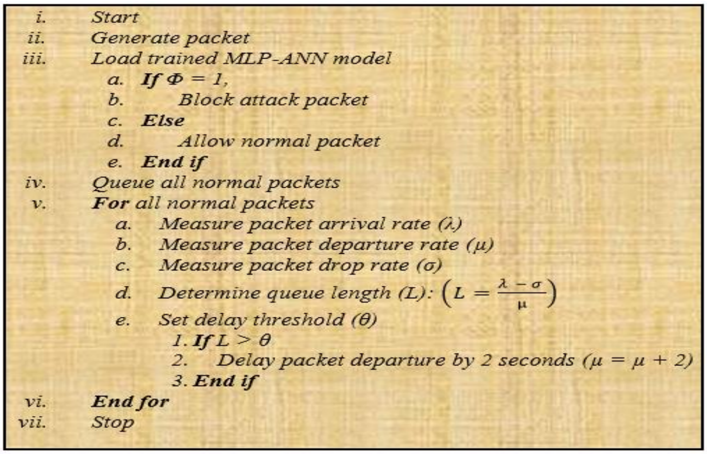
From the proposed model architecture in Figure 1, there are four voting points with the attacker controlling two of the voting clients and the last two voting points are accessible by legitimate voters. The votes from each voting point are sent to the server, however, during DDoS attack, the attacker makes the voters become bots or zombies and flood the server rendering it unavailable to legitimate voting clients. The DDoS flood mitigation model, which comprises a packet storage and delay model, detects DDoS attacks and slows

The DDoS flood mitigation model, which comprises a packet storage and delay model, detects DDoS attacks and slows down normal packet arrival to the server to prevent voting server unavailability.

In Almustapha *et al.*, 2018, a baseline information on the recent efficient techniques against DDoS attacks was reported. Furthermore, adopting MLP technique for detecting DDoS flood attacks in Internet Kiosk voting was as a result of the research conducted in Almustapha *et al.*, 2019, which investigated and tested Random Forest, Naive Bayes and MLP classifiers on a sample of the KDD Cup99 dataset to arrive at a result of 98.65% for MLP and concluding that MLP was the best for classifying DDoS flood attacks from normal voting traffic.

3.1 DDoS Flood Attack Mitigation Model

The DDoS flood attack mitigation model comprises of the MLP model for detection of DDoS attacks and a First-In-First-Out (FIFO) queue for packet storage. The queue stores packets that are detected as normal by the MLP-ANN model since normal packets can also cause a server unavailability if their rate shows the DDoS Flood Attack Mitigation Pseudocode where i^{th} packet in queue is represented as P_i: {i = 1:L}, and L is the of arrival to the server is high, hence, the packet departure time delay was introduced to prevent denial of service. A two seconds time delay was set for the considered case. Figure 2 queue length. Also, the MLP-ANN output (Φ) is set as 1 for an attack packet and 0 for a Normal Packet.



```
i.    Start
ii.   Generate packet
iii.  Load trained MLP-ANN model
        a. If $\Phi = 1$,
        b.     Block attack packet
        c. Else
        d.     Allow normal packet
        e. End if
iv.   Queue all normal packets
v.    For all normal packets
          a.  Measure packet arrival rate ($\lambda$)
          b.  Measure packet departure rate ($\mu$)
          c.  Measure packet drop rate ($\sigma$)
          d.  Determine queue length (L): $\left(L = \frac{\lambda - \sigma}{\mu}\right)$
          e.  Set delay threshold ($\theta$)
                1. If $L > \theta$
                2.    Delay packet departure by 2 seconds ($\mu = \mu + 2$)
                3. End if
vi.   End for
vii.  Stop
```

Figure 2. DDoS Flood Attack Mitigation Pseudocode

3.2Simulating Incoming Voting Traffic Scenarios using SimEvents

MATLAB R2017a was one of the tools used in this research on a ZINOX laptop having a 2.4GHz processor and 4GB RAM. Seed initialize technique was use to initialize different seeds for all generated packets with the value of each seed having a 5 digit odd number for the different random blocks within the model. The DDoS Flood Mitigation System was modelled using MATLAB R2017a, which included SimEvents for building the three model scenarios with the help of Random Number Generators and Simulink for time-based simulations. The three traffic scenarios simulated are described as follows:

3.2.1 Normal Traffic Scenario

In Figure 3, this scenario depicts two (2) voting clients called KV_Node1 and KV_Node2 respectively belonging to a Voting Kiosk with each block generating incoming packets based on exponential intergeneration times with uniform distribution. Means are set as 150 for both V_Node1 and V_Node2 clients. The source and destination router route the generated packets to the Voting server while each FIFO (First-in-First-Out) queue storage temporary stores the incoming packets and have a predefined queue size of 25.

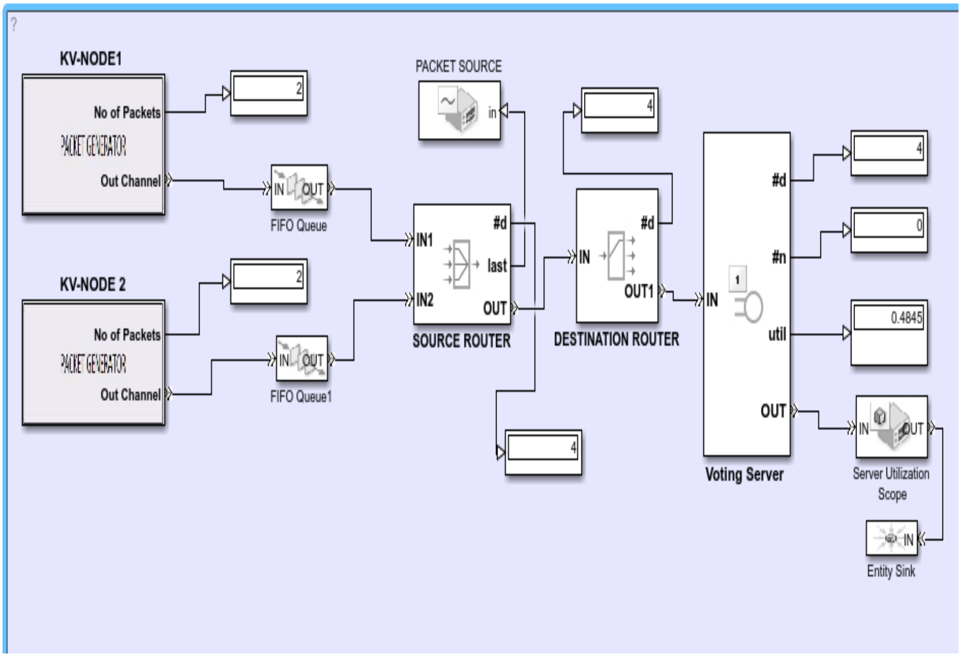


Figure 3. Normal Traffic Model Setup

3.2.2 DDoS Flood Attack Traffic Scenario

In this scenario as shown in Figure 4, the normal traffic state was disrupted by a group of nodes comprising of an attacker controlling computer bots called KVNodeBot1 and KVNodeBot2 with the aim of sending attack packets to the victim server (voting server). The DDoS attack causes the server to become overwhelmed resulting in slow network and inability of voters to cast their votes via e-voting applications located on the client computers.

Attack Replicator block works by accepting attack packets from KV_NodeBot1 and KV_NodeBot2 and the attack block is controlled by the Step Block, which activates Enabled gates based on its switching on (1) and off (0) signals. When step block has 1 as final parameter value, it causes Enabled Gates 1, 2 and 3 to be activated, which allow legitimate packets from KV_Node1 and KV_Node2 to be routed to voting server.

The Attack Replicator block is activated when step block is 0 allowing attack packets to be redirected to server. KV_NodeBot1 and KV_NodeBot2 imitate real life situation where the attacker controls the computers in order to send attack packets that exhaust the resources of the Voting Server.

3.2.3DDoS Flood Mitigation Traffic Scenario

In this scenario as shown in Figure 4, a Packet delay mitigation technique is applied to the simulated network. The developed model will have the advantage of detecting and blocking DDoS Flood attack traffic, divert, filter and forward normal packets quickly and efficiently to the voting server. The mitigation block works by first detecting attack packets and then applying an increase in time delay for packets leaving the mitigator block so as to control the amount of traffic reaching the voting server at a given time.

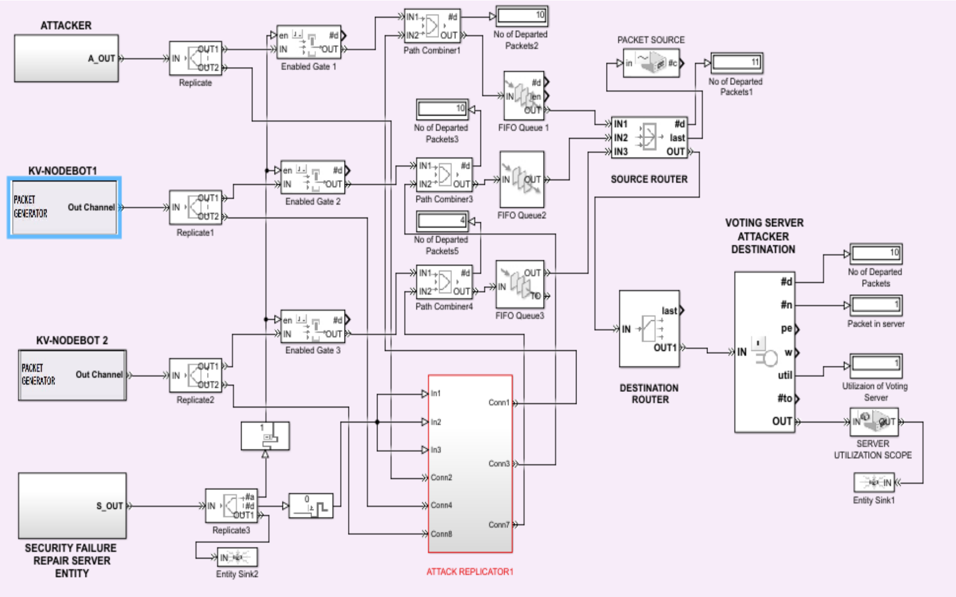


Figure 4. DDoS Flood Attack Traffic Model Setup

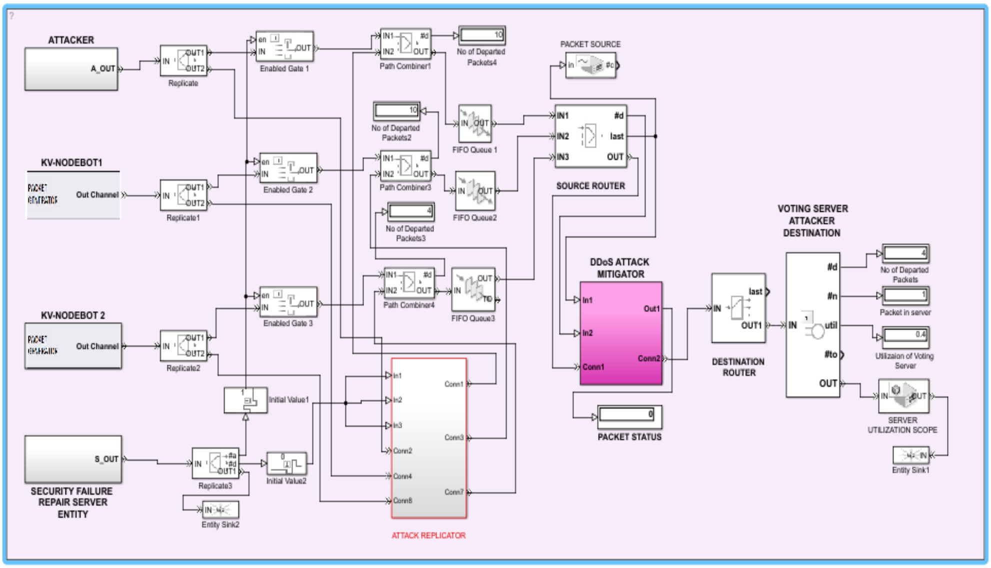


Figure 5. DDoS Mitigation Traffic Model Setup

The main aim of this research is to compare the Availability and Utilization of the Voting Server under situations that include normal traffic, DDoS attack traffic and when an Intelligent DDoS Flood Mitigation System is applied in Internet Kiosk Voting Scenario.

4. MODEL SIMULATION RESULT

The Instantaneous scope was used to connect signals in order to view and analyze simulation results for each model scenario. The service time of the voting server was set at 1 second for all voting scenarios.

4.1Performance Metrics for Evaluation of Developed Model

The server utilization is the proportion of available time that the voting server is in operation and the server utilization monitor uses the observation function, which returns the value 1 for voting server under attack and the value of 0 for inactive server. This performance metrics measures how busy or idle the voting server operates under normal conditions, under DDoS flood attack and when the mitigation model is used to prevent the server from being busy, and it is denoted as:

$$\text{Server Utilization} = \left(\frac{\text{amount of time server is busy}}{\text{simulation time}}\right) * 100 \quad (3)$$

4.2Normal Scenario Results

Figure 6 shows the Instantaneous Scope for Normal traffic signal. This scope shows the availability of Voting Server. The lines on the graph represent time zones during which the server is available or not. For instance, between times 0-1, 2 – 6 and 6-9, the voting server is available.

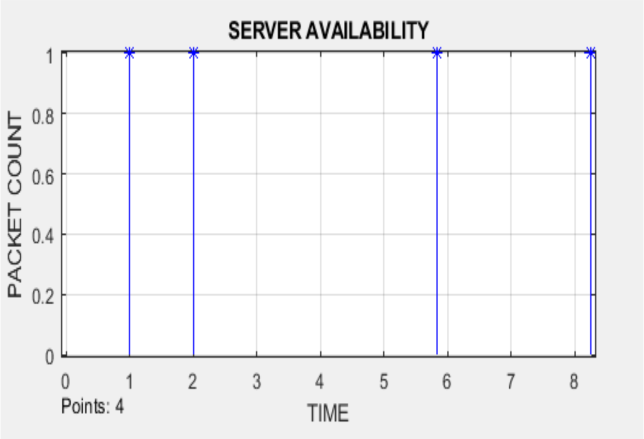


Figure 6. Server Utilization Plot for Normal Traffic

4.3DDoS Flood Attack Scenario Results

In Figure 7, Instantaneous Scope shows unavailability of servers as attack packets are generated from KV_NodeBot1 and KV_NodeBot2. Signal Scope shows great activity from both nodes as the block generates attack packets.

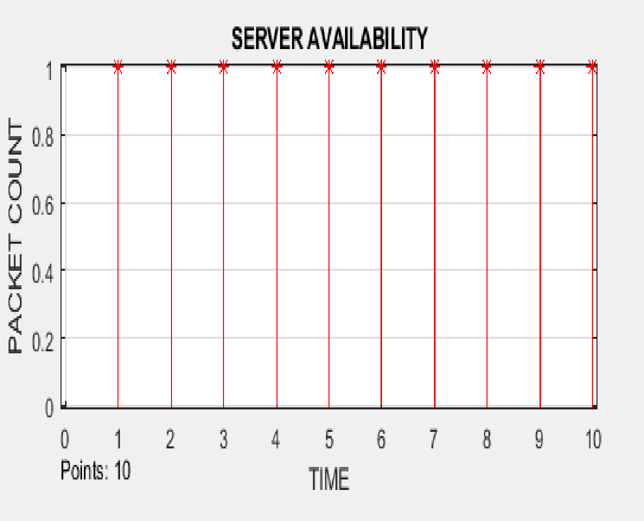


Figure 7. Server Utilization Plot for DDoS Attack Traffic

4.3 Proposed Mitigation Model Results

Figure 8 shows the Instantaneous Scope for mitigation traffic signal. This scope shows the availability of Voting Server from 0-3, 3-5, 5-7 and 7-9 respectively. The lines on the graph represent time zones during which the server is available.

4.4Simulation Result Summary

From Figure 9, when the voting server is under DDoS attack, the utilization of the server is 1 which is equal to the expected output of 1 for DDoS Flood attack packets. When the Mitigation model is introduced in an attack scenario, the Utilization of Voting Server reduces to 0.4 indicating server utilization.

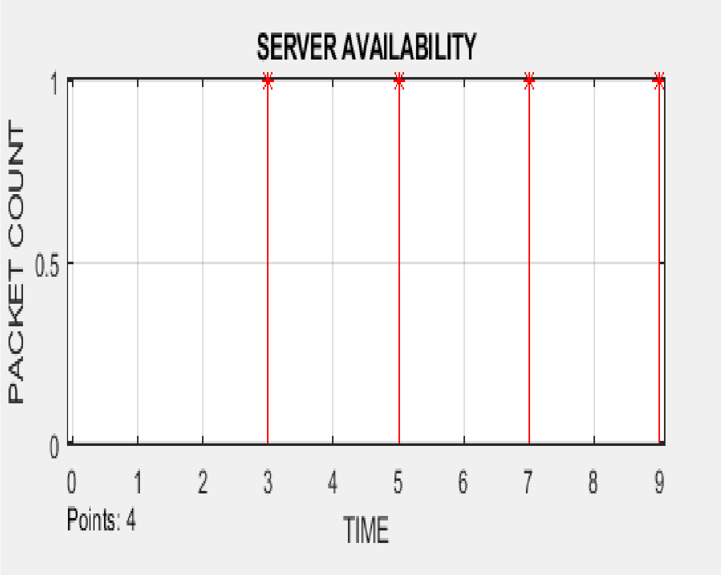


Figure 8. Server Utilization Plot for Mitigation Traffic Scenario

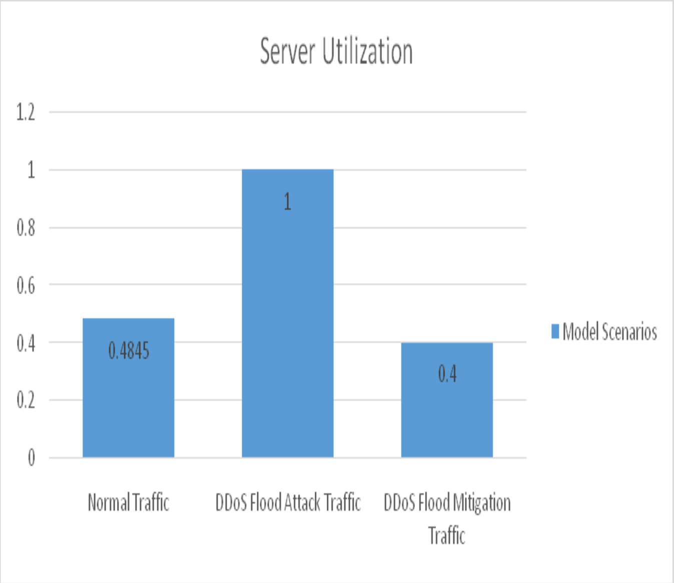


Figure 9. Result Summary for Voting Server Utilization

Figure 10 shows the bar chart for packet delivered under normal, attack and mitigation scenarios. The chart shows that during attack, the highest packets were delivered which comprises of mostly attack packets while normal packets were denied reaching the server.

Figure 11 shows the bar chart for packet blocked under normal, attack and mitigation scenarios. The chart shows that during mitigation, the 19 out of the 20 attack packets were blocked from reaching the server. This shows that the proposed mitigation model is effective in blocking DDoS attack.

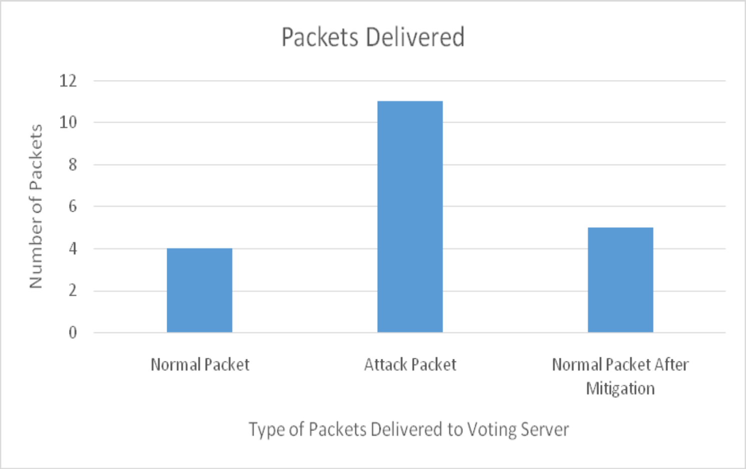


Figure 10. Result Summary for Packets Delivered

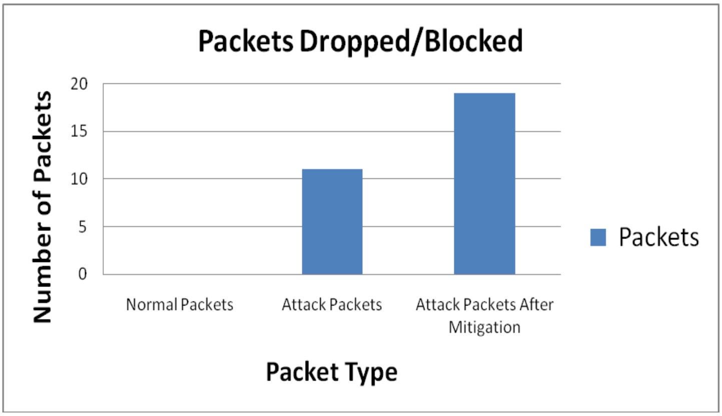


Figure 11. Result Summary for Packets Dropped/Blocked

5. Conclusion

The DDoS Flood attack mitigation model was developed using MLP Neural Network Technique and simulated using MATLAB SimEvents tool. A result of 95% accuracy was achieved for effectively preventing DDoS attack flood packets from reaching the Voting server.

Although, the proposed mitigation model in this research does not provide 100% protection from DDoS flood attacks in Internet Kiosk Voting network based on the results obtained, it is important that the e-voting system is protected from DDoS flood attacks to ensure voters' trust and ease of casting ballots during election. Future research could be carried out on the proposed mitigation model by implementing it in real-time e-voting environment as well as the use of machine learning models, such as Support Vector Machine algorithms for further investigation.

References

Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F., & Misra, S. (2020). Implementing a Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria. In *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)* (pp. 857-872). Springer, Singapore.

Agrawal, S., & Gupta, A. (2015). Survey on Data Mining and IP Traceback Technique in DDoS Attack. *International Journal of Engineering and Computer* Science, 4(6), 12595–12598.

Aljumah, A. (2017). Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks. *International Journal of Adavanced Computer Science and Applications (IJACSA),* 8(8), pp. 315-317.

Alkasassbeh, M., Al-Naymat, G., Hassana, A. & Almseidin, M. (2016). Detecting Distributed Denial of Services Attacks Using Data Mining Techniques. *International Journal of Advanced Computer Science and Applications,* doi: 10.14569/IJACSA.2016.070159, 7(4),pp. 438-439.

Almustapha A. J., Olaniyi O. M., Abdullahi I. M., & Ndunagu O. Detection and Analysis of DDoS Attacks in Internet Kiosk Voting Using Machine Learning Algorithms. *Proceedings of the 3rd International Conference on Applied Information Technology, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria*, pp. 133-140, October, 2019.

Almustapha A. J., Olaniyi O. M., Abdullahi I. M., & Abdulsalam Y. S. Towards the use of BPANN Technique for Mitigating Layer 4 DDoS Attack in Electronic Voting. *Proceedings of the 12th International Multi-Conference on ICT Applications, Obafemi Awolowo University, Ile-Ife, Osun State, Nigeria, November 2018*.

Cheng, C., Zhang, C., Tang, X., Sheng, V., Dong, Z. & Li J. (2018). Adaptive DDoS Attack Detection Method Based on Multiple-Kernel Learning. *Hindawi Security and Communication Networks*. doi:10.1155/2018/5198685.

Edikan, E., Misra, S., Ahuja, R., Sisa, F. P., & Oluranti, J. (2019). Data Acquisition for Effective E-Governance: Nigeria, a Case Study. In *International Conference on Recent Developments in Science, Engineering and Technology* (pp. 397-411). Springer, Singapore.

Jonathan, O., Ayo, C. K., & Misra, S. (2014). A Comparative study of e-Government successful implementation between Nigeria and Republic of Korea. In *Asia-Pacific World Congress on Computer Science and Engineering* (pp. 1-7). IEEE.

Katiyar, S., Meka, K. R., Barbuiya, F. A., & Nandi, S. (2011) Online Voting System Powered by Biometric Security Using Steganography. *Proceedings of the Second International Conference on Emerging Applications of*

Information Technology, (pp. 288 - 291), IEEE.

Musial-Karg, M. (2017). Challenges of I-Voting – Practices, Rules and Perspectives. Adam Mickiewicz University in Poznań, doi:10.14746/pp2017.22.4.6, pp.76-77.

Musial-Karg, M. (2015). Implementation of Electronic Voting and the Matter of Security, doi:10.1515/curie-2015-0022, 22(1), pp. 125-130.

Odusami, M., Misra, S., Abayomi-Alli, O., Abayomi-Alli, A., & Fernandez-Sanz, L. (2019). A Survey and meta-analysis of application-layer distributed denial-of-service attack. *International Journal of Communication Systems, 33*(18), e4603.

Odusami, M., Misra, S., Adetiba, E., Abayomi-Alli, O., Damasevicius, R., & Ahuja, R. (2019). An Improved Model for Alleviating Layer Seven Distributed Denial-of-Service Intrusion onWebserver. In *Journal of Physics: Conference Series* (Vol. 1235, No. 1, p. 012020). IOP Publishing.

Okediran, O. O., Omidiora, E.O., Olabisi, S. O., Ganiyu, R. A., & Alo, O. O. (2011). A Framework for a Multifaceted Electronic Voting System. *International Journal of Applied Sciences, USA*, 1(4), pp. 135-142.

Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Okediran, O. O. (2013). A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System. *Covenant Journal of Informatics and Communication Technology (CJICT),* 1(2), pp. 5-11.

Patil, R. H., Tarte, B. B., Wadekar, S. S., Zurunge, B. S., & Phursule, R. (2015). A Secure E-Voting System Using Face Recognition and Dactylogram. *International Engineering Research Journal*, 1(8), 620-623.

Paul, L. & Anilkumar, M. N. (2012). Authentication for Online Voting using Steganography and Biometrics. *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET),* 1(10), 27-31.

She, C., Wen, W., Lin, Z., & Zheng, K. (2016). Detection of Application-Layer DDoS by Clustering Algorithm. *2nd International Conference Artificial Intelligence and Industrial Engineering (AIIE2016)*. Published by Atlantis Press-Advances in Intelligent Systems Research, 133.

Syed, N. S., Aamir, Z. S., & Shabbar, N. (2018). A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition. *Mehran University Research Journal Engineering and Technology,* 37(1), 1-6.