Detection of Distributed Denial of Service Attacks in a VOIP Network using Machine Learning Technology and OPNET Modeler

[1]Ayodele S. Oluwole, [2]Henry E. Akhionbare, [3]Olaitan Akinsanmi
[1]Department of Electrical and Electronics Engineering, Federal University, Oye Ekiti, Ekiti State, Nigeria
[2]Department of Electrical and Electronics Engineering, Federal University, Oye Ekiti, Ekiti State, Nigeria
[3]Department of Electrical and Electronics Engineering, Federal University, Oye Ekiti, Ekiti State, Nigeria
ayodele.oluwole@fuoye.edu.ng|efosahenry@yahoo.com|olaitan.akinsanmi@fuoye.edu.ng

Received: 10-JUNE-2026; Reviewed: 22-JUNE-2026; Accepted: 30-JUNE-2026
https://dx.doi.org/10.46792/fuoyejet.v11i1.1602

ORIGINAL RESEARCH

Abstract—Voice Over Internet Protocol (VoIP) in contrast to the Public Switched Telephone Network (PSTN) and cellular networks is emerging as an alternative to the conventional public telephony networks, as a result, it becomes an attractive target to be abused and exploited by malicious attackers because it lacks defence against the growing security threats especially the Distributed Denial of Service (DDoS). In an attempt to prevent Denial of service, DDoS detection in a VoIP network using machine learning technology was proposed. In this work, attacks in VoIP network was formulated as a classification problem and Wireshark was used to capture, enhance the extract features of the Session Initiation Protocol (SIP) messages. A detailed simulation approach for generating VoIP traffic successfully to obtain a dataset using the OPNET network simulator was used, the approach predicts the best and satisfying quality of service requirements of the network services and provide adequate capacity for future growth. This is achieved by carrying out a number of simulations on a segmented network, which provided graphical results used in the study of VoIP traffic. These results will benefit network planners in the successful implementation of VOIP services and also provide correct dataset that will be used by the ML technology. The simulation results will then be verified by comparing with the result obtained by Diogo & Rodolfo, (2022).

Keywords— DDoS, OPNET, SIP, UML, UDP, VoIP.

1 INTRODUCTION

Voice over Internet Protocol (VoIP), in contrast to the Public Switched Telephone Network (PSTN) and cellular networks, adds a third dimension to voice communication. VoIP allows you to make a call to any PSTN or mobile phone anytime anywhere in the world. Although some services require a computer or a specific VoIP phone to operate, others enable a caller to use a regular phone with an adaptor. The conversion of the present circuit switched PSTN to a Public Switched Network (PSN) is expected to be possible with VoIP. Advanced functionalities have begun to emerge as VoIP has gained wide acceptance by most telecommunication provider Kumar, V and Roy, O (2021).

IP telephone service providers are moving fast from low-scale toll bypass deployments to large-scale competitive carrier deployment, thus it gives an opportunity to enterprise networks a choice of supporting less expensive single network solution rather than using multiple separate networks. The broadband-based residential customers also switch to IP telephony due to its convenience and cost effectiveness. In contrast to a traditional telephone system where the end devices are dumb, the VoIP architecture pushes intelligence towards the end devices such as PCs, IP phones and enables many new services. Furthermore, VoIP allows for the creation of customized solutions by allowing for the addition of personalized and value-added services Werapun W. (2021). The confluence of the voice and digital worlds, as well as the number of VoIP subscribers hiting a critical mass brings with it not just opportunities but security risks and issues as well [4]. Some security isssues in VoIP system and the possible mitigation mechanism are shown in Table 1 below.

Table 1. Security issues in VoIP system [4]

Types of Security Issue	Problems	Possible Solutions
Vulnerabilities for Attackers	Physical connection and gain access to network	User authorization implementation properly
Eavesdropping	Privacy Loss	Encrypting the data
Rogue Set	Threat to confidentiality	Network lock down mechanism
Spoofing attack	Unauthorized access	Firewall configuration
Denial of Services (DOS) attacks	False SIP invite messages and memory exhaustion	Packet source IP address on sending replies
VoIP Media DOS attack	Non availability of transmission	Firewall at hardware and software level
Flooding Based DOS attack	Consumption of memory and processing resource	**Designing of AI based mitigation scheme**

Corresponding Author: ayodele.oluwole@fuoye.edu.ng
Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Oluwole A. S., Akhionbare H. E., Akinsanmi O. (2026). Detection of Distributed Denial of Service Attacks in a VOIP Network using Machine Learning Technology and OPNET Modeler. FUOYE Journal of Engineering and Technology (FUOYE**JET), 11(2), 280-286.** https://dx.doi.org/10.46792fuoyejet.v11i2.1602

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

1.1 VoIP Technology

Voice over Internet Protocol (VoIP) is a recent technology used to transfer media and voice over Internet Protocol (IP). The voice transfer is demonstrated in Figure 1, Tas, I.M. & Baktir, S. (2023).

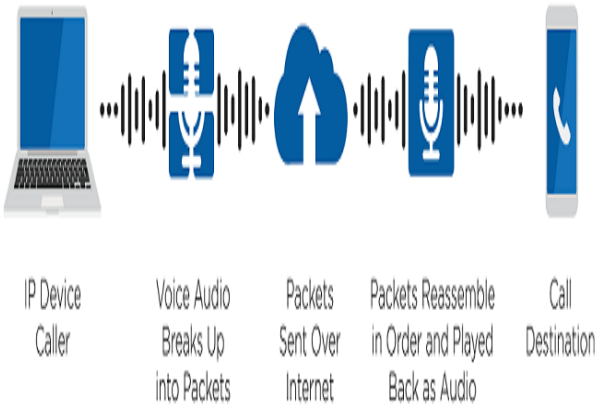

Fig. 1. VoIP Communication

Many organizations moved to VoIP services instead of the traditional telephone systems because of its low cost and variety of introduced services. The Session Initiation Protocol (SIP) is the most used protocol for signalling functions in VoIP networks. It has simple implantation but suffers from less protection against attacks especially Distributed Denial of Service attacks, Tas, I.M. & Baktir, S. (2023).DDoS attacks are the most common means of cyber attacks against VoIP infrastructure, and its detection is the first step in combating them. The current DDoS AI based detection systems mainly uses the improvement of supervised machine learning methods to improve classification performance, Alazab A. et al (2012). However, most classifiers are trained with statistical flow features as input, ignoring unknown pattern of attacks. This one-sidedness affects the detection accuracy and cannot provide a basis for the distribution of attack sources. This work covers VoIP network monitoring, improving threat detection accuracy and detection time of DDoS attacks using unsupervised machine learning algorithm to account for the unknown threat pattern in addition to the known pattern. Experimental test bed was setup using Opnet modeller 14.5 which contain all required VoIP components for simulation to measure the performance of the system and provide means of validation. In Addition, the work was implemented as a module of inline-based IDPS and functions with VoIP packets that are transmitted to and from a live VoIP network. The organization of the paper is as follows: introduction and problem statement has been presented in section one. The remaining sections are structured as follows: Detailed methods as well as review of similar works is presented in section two. Section three is devoted for implementation and evaluaton. Simulation results will be highlighted in section four. Finally, conclusion and future work makes up section five. The list of cited references is provided at the end of this report.

2 METHOD

2.1 Existing Detection Systems

Diogo and Rodolfo, (2022) investigates the detection of abnormal sequences of signaling packets purposely generated to perpetuate signaling-based attacks in computer networks. The problem is studied for the Session Initiation Protocol (SIP) using a dataset of signaling packets exchanged by multiple end-users. A sequence of SIP messages never observed before can indicate possible exploitation of a vulnerability and its detection or prediction is of high importance to avoid security attacks due to unknown abnormal SIP dialogs. They start by briefly characterizing the adopted dataset and introduces multiple definitions to detail how the deep learning-based approach is adopted to detect possible attacks. The proposed solution is based on a convolutional neural network capable of exploring the definition of an orthogonal space representing the SIP dialogs. The space is then used to train the neural network model to classify the type of SIP dialog according to a sequence of SIP packets prior observed. The classifier of unknown SIP dialogs relies on the statistical properties of the supervised learning of known SIP dialogs. Experimental results are presented to assess the solution in terms of SIP dialogs prediction, unknown SIP dialogs detection, and computational performance, demonstrating the usefulness of the proposed methodology to rapidly detect signaling-based attacks. The work achieved higher performance independently of the detection model. The experimental assessment and the results achieved accurate detection probability of 8.5 – 9.5 and this shows the effectiveness of the proposed methodology to improve the security of SIP-based services but computation time was a bit high to about 48s due to the model computational complexity. The DDoS attack is a serious cyber security attack that attempts to disrupt the availability of security principles in a network and information systems [3]. It is therefore critical to detect DDoS attacks quickly and accurately while using as less computing power as possible in order to minimize damage and cost efficiency. This research proposes a fast and high-accuracy detection approach by using an unsupervised machine learning algorithm. Due to the distributive nature of DDoS attacks, attack traffic stem from multiple sources and the aggregate of this traffic which results in a huge volume leads to the exhaustion of the victim's network infrastructure, C. Shorten and T. M. Khoshgoftaar(2019). This indicates that the generated network traffic at the source is usually small compared to the traffic received at the victim's network, Almuairfi S. J. and Alenezi M., (2020).

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://.doi.org/10.46792/fuoyejet.v11i2.1602 engineering.fuoye.edu.ng/journal

Currently, many DDoS detection systems have focused more on obtaining more effective computational costs of detection systems i.e. processing power requirements and memory consumptions, programmability of systems due to the ever changing attack landscape and flexibility in deployments to support the different needs of networks, Alazab A. et al (2012). However, less attention has been given to the accuracy, reduction of false alarm rates and simplification of detection systems.

2.2 Proposed System

A Distributed Network Intrusion Detection and Prevention System (NIDPS) consists of multiple Intrusion Detection Systems (IDS) over a large network, Amaizu, G.C. (2021), all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data, Kurt, B. (2018). To achieve the aim of this work, the traffic and attacks will be modelled in such a way that it will be near live situation using bandwidth and memory as additional parameters to the SIP feature parameters because this are two most targeted parameters by most attackers in the recent time.

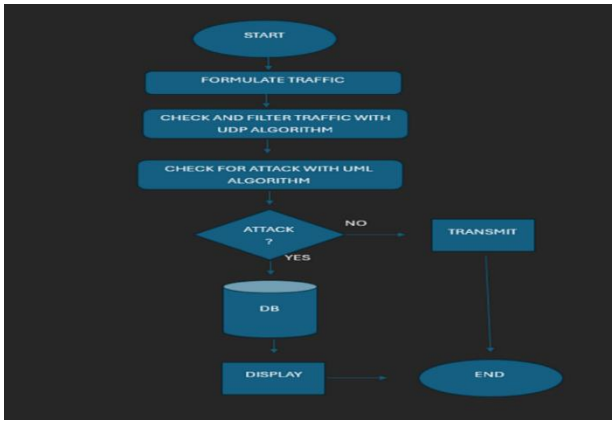

Fig. 2. shows the proposed methodology flow.

2.3 Artificial Intelligence (AI) Method for DDoS Attacks Detection

DDoS is one of the most common attacks on the web today, Luh R. (2020). Hence, a quick detection system can enable automatic blocking or notification of an attack. Figure 2 shows existing DDoS anomaly detection flow Based on the work of Diogo & Rodolfo, (2022).

The AI method is based on three major modules:

1) pre-processing data incoming to the server,
2) Classification/Clustering, and
3) decision-making.

The 3 modules formed the basis of the proposed system as shown in figure 4.

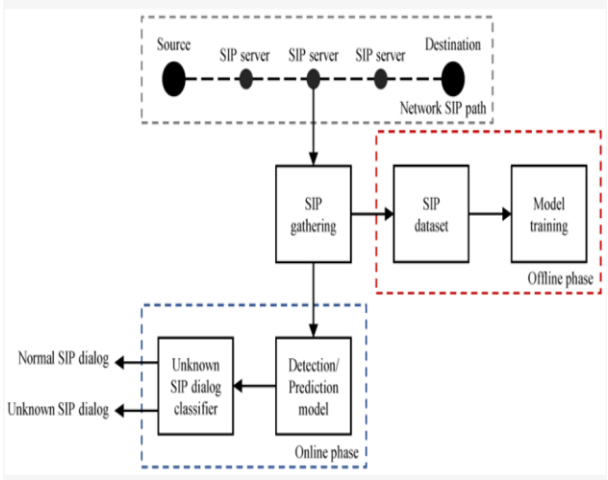

Fig. 3. Existing System Model

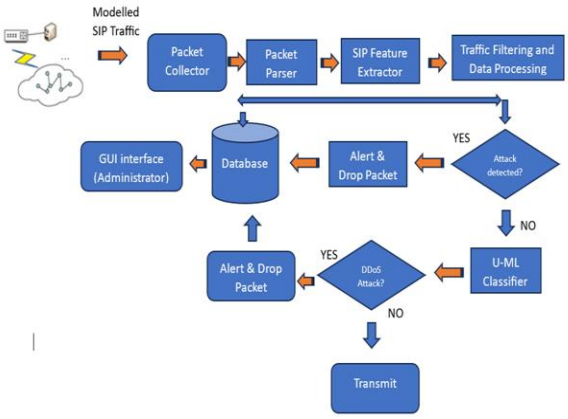

Fig. 4. Proposed System Model

The model gets the probability from the implemented AI method which is Unsupervised machine Learning and analyzes/aggregates them for making a final decision about the attack. The idea is based on the analysis of the SIP and TCP/UDP information reaching the target server and a quick and effective decision method makes an inference Almuairfi S J and Alenezi M., (2020). Figure 3 shows proposed model used in this research. The detail model description in the sub sections below.

2.3.1 Traffic modelling Module

An android based mobile app slow droid was used to sends a SIP server numerous SIP request messages within a short time, and deliberately varying the resources required to process each message using the Slow Droid installed devices which makes it possible to provide normal VoIP traffic and an attack traffic. While modelling the traffic in this work, the probability either bandwidth or buffer size depletion on the victim server was considered in addition to the basic resources. This probability is computed by:

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://.doi.org/10.46792/fuoyejet.v11i2.1602 engineering.fuoye.edu.ng/journal

The total probability depletion of resources at the victim end is given by [7].

$$Total_{Attack} = 1 - (1 - p^{\beta})(1 - p^{m}) \quad (1)$$

The probability of bandwidth (p^{β}) depletion is given by:

$$p^{\beta} = \frac{\frac{a^{c}}{c!}}{\sum_{i=0}^{c} \frac{a^{i}}{i!}} \quad (2)$$

$$a = \frac{(\beta_A + \beta_N)}{\beta_{Total}} = \frac{\left(\frac{\delta_{\beta A}}{\tau_{\beta A}} + \frac{\delta_{\beta N}}{\tau_{\beta N}}\right)}{\beta_{TOTAL}} \quad (3)$$

where:
β = Bandwidth
A = Attack
N = Normal

The probability of memory (p^{M}) or buffer exhaustion is given by:

$$p^{M} = \frac{\frac{\gamma^{M_{TOTAL}}}{M_{TOTAL}}}{\sum_{i=0}^{M_{TOTAL}} \frac{\gamma^{i}}{i!}} \quad (4)$$

Where:

$$\gamma = M_A + M_N = \frac{\delta_{MA}}{\tau_{MA}} + \frac{\delta_{MN}}{\tau_{MN}} \quad (5)$$

Therefore,

$$M_A = \frac{\delta_{MA}}{\tau_{MA}} \; and \; M_N = \frac{\delta_{MN}}{\tau_{MN}}$$

Based on above, certain probability of attack was attached to each traffic generated randomly in addition to the SIP characteristics of the traffic, and this then fed into the collection module, Diogo P. and Rodolfo O., (2022) as depicted in the flow shown in Figure 3.

2.3.2 Traffic Collection Module

The collection module mainly composes of three parts: Packet collector, Packet Parser and SIP feature extractor.

Packet collector: Modelled traffic from the threat modelling module was captured using Wireshark, the traffic packet collection tool. Wireshark is a user level packet capture interface that provides a convenient application framework for low level network monitoring, Golait D and Hubballi N., (2016). It provides users with a unified and easy to use packet capture API.

1) Packet Parser: A custom Wireshark dissector was written and used to parse out the captured data fields and rebuild the data stream so the file's binary data could be transformed and have a more meaningful view. The batch data processing method was used in packet parser, the parsing was done as the traffic data is collected. A series of fixed time windows was used to periodically segment the real-time collected traffic packets to generate many small datasets, the packets in the same dataset are parsed in batches to enable easy extraction of SIP attributes. The captured change in time Δt time interval from the packet stream was put together to form the dataset and the attributes or features was then extracted from the dataset. The cleaned parsed data then fed into feature extractor. A similar pattern has been proven to be effective in terms of cost saving, Fenil E. and Mohan Kumar P., (2020).

2) SIP Feature Extractor: A T-shark command was also applied to the parsed data from (ii). At first, it collects every parsed IP packets from the network, and inspects application headers of the dataset, it then distinguish SIP packets from the other types of IP packets and gathers SIP attributes (e.g. callID, caller/callee URI, SIP method type etc.) to obtain its features or fields. The output is then presented in a CSV file. The generated feature information can then be sent to VoIP Traffic Monitoring and Detecting module for initial filtering using the UDP based protocol, Kurt, B. et al (2018).

2.3.3 Traffic Monitoring and Detecting Module

The monitoring and detection module consist mainly of three parts:

1) Traffic Filtering and Data Processor
2) U-ML Clustering
3) Admin Graphical User Interface

1) **Traffic Filtering and Data Processor**: It is very difficult to detect distributed attacks based on SIP message behaviour only. But packets that have same Synchronizing Source Collision Resolution identifier (SSRC) means they are sent from same host. Therefore, if the number of source IPs of the packets that has same SSRC within a dataset is more than one, then it can be suspected to be a distributed attack. SSRC is a 32-bit number that uniquely identifies a single source of a packet stream, This was applied to further handle the traffic features extracted from the Collector module and
2) **U-ML Clustering** - The processed data was submitted into the unsupervised machine learning classifier for the detection of DDoS attacks. If it is detected as a DDoS attack, the traffic attribute of the attack will be saved for model update and evidence collection. At the same time, an alarm will be issued to notify the network administrator on the GUI.
3) **Admin GUI** – This display the output of activity and analysis that occurred for easy understanding and action for the system administrator.

3 IMPLEMENTATION AND EVALUATION

3.1 Network Design

OPNET modeller 16.1 is the software tool used for designing the networks and implementing them. This tool is very user friendly and easily understandable for everyone. Numerous advantages of this tool make this more popular when compared to the other network simulation tool like NS1, NS2, OMNET, etc. Structure of OPNET simulation tool is divided into three main classifications or domains: network domain, node domain and process domain. Basic computing languages like C and C++ are used for building the components of OPNET, so these codes can be changed according to requirements and it is possible to build

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://.doi.org/10.46792/fuoyejet.v11i2.1602 engineering.fuoye.edu.ng/journal

customized components based on the requirements. These network simulation tools are very useful for the researchers and network developers for developing the new network and also to test the network that are going to be built in the real world. Network administrators can use this to find the problems in the network and ascertain the best way it can be rectified before going into it real time. The following sub-section gives the detailed explanation of the experiemnt scenario, the configurations and the implementation process. Results collected from these scenario is then analysed in the next section.

3.2 Requirements and Components

General requirements for this implementation are OPNET 16.1 modeller, Slow Droid Android installed devices and a PC. OPNET 16.1 modeller can't be installed in our personal computer, so the lab resources of ITSKY Solution Limited are used. All the components required for the implementations and design processes are available in the object palette of OPNET modeller. There is vast availability of objects in object palette, which resembles the real time components and performs the same functionality as the real time components. General components required here are application definition node, profile definition node, IP QoS node, subnets, end users, connecting links, routers, and servers. For any network application definition, profile definition and IP QoS nodes are the configurations nodes. Applications and profile definition nodes are configured according to requirements, whereas the IP QoS node is self configured. The required components are dragged and dropped into the work space. After the required objects are dragged into the workspace, they are the configured. The Configuration of components are done carefully and correctly, or else the functionality of the network changes.

3.3 Experiement Scenario

A prototype of the detection system as depicted on the system model was developed as shown in Figure 4. The design has several servers and each server work on an Intel Xeon CPU E5-2690 CPU with 64 GB memory and are running Ubuntu 14.04. Two different kinds of DDoS attacks (SSH brute-force and ICMP flooding attacks) where formulated from the andorid devices simulating the legitimate users and attacks.

3.4 Data Collection, and Processing

In the experiment, Traffic packages going out of the attackers devices was collected for 1 hours. Two kinds of attacks are programmed to randomly start and end in addition to the legitimate traffic, some of which start simultaneously. The main goal is detecting attacks, no matter which category an attack falls into. The data are collected using wireshark and processed to extract the features as shown in Figure 6 and Figure 7.

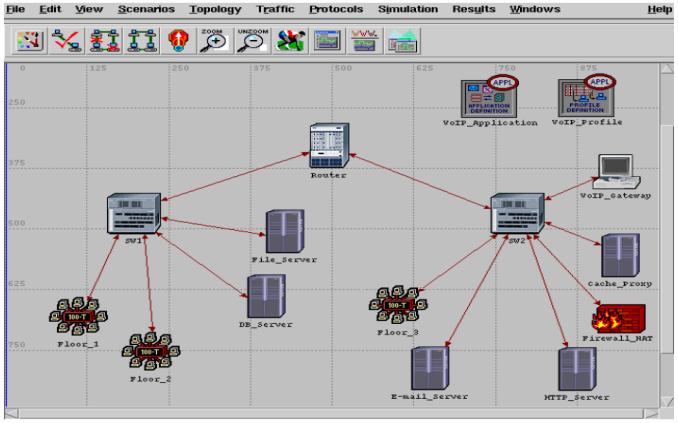

Fig. 5. Network Simulation

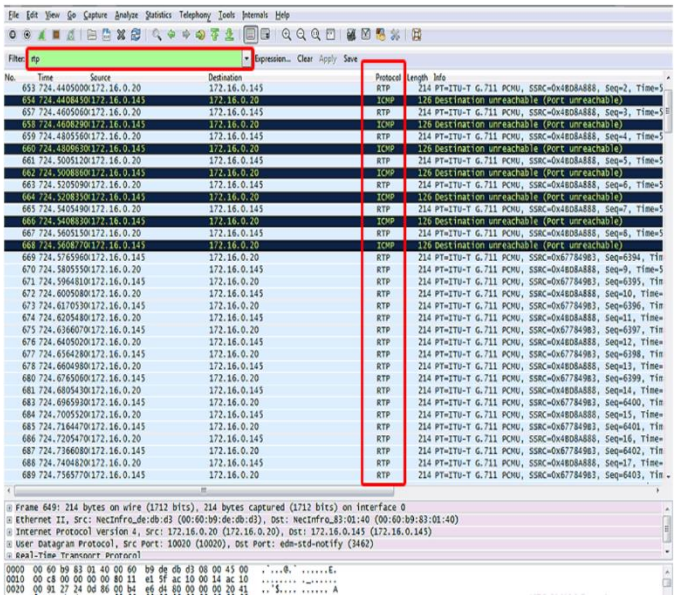

Fig. 6. RTP Traffic Capture

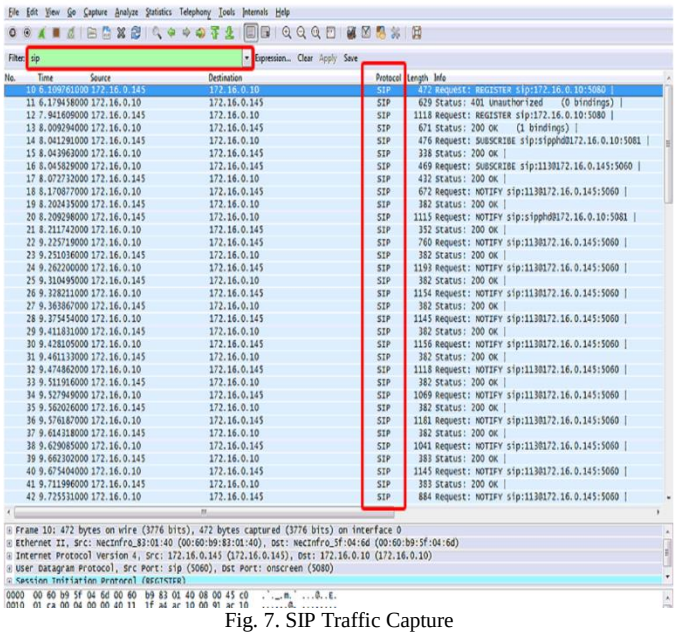

Fig. 7. SIP Traffic Capture

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://.doi.org/10.46792/fuoyejet.v11i2.1602 engineering.fuoye.edu.ng/journal

4 SIMULATION RESULTS

Before the simulation started, OPNET was configured to obtain graphed results for numerous network components which include VoIP traffic, router, switches, and links for voice traffic. Graphed results for some of the most important components were generated. The OPNET simulation was configured for 1 hour. The recognition of traffic by default in OPNET started at 40 seconds from the start time of the simulation run. The VoIP traffic from slow droid started at 1 second at which a total of 3 VoIP bi-directional calls were initially added. Then, every 2 seconds 3 VoIP calls are added. The Simulation stops at 1 hour as configured in which a total of 6115 calls got generated. Since the simulation stops at 1 hour, the last 3 calls to be added were at 59 minutes and 58 seconds Figure 7 shows the VoIP traffic that was sent, received, and dropped. Figure 8 shows the VoIP traffic and the corresponding end-to-end delay as VoIP calls are added every two seconds. This delay does not exceed 70ms earlier. The delay stays less than 70ms until a simulation time of about 5 minutes at which the delay increases sharply to 1 second 500 milliseconds and maintain it for the simulation period. One can then find out the number of VoIP calls that the network can support to satisfy the 70ms time constraint. Therefore, one can conclude that, based on these simulation results, the number of voice calls to be supported by the network is bounded more by the network bandwidth than the delay. Hence, the number of the VoIP calls that the network can support based on simulation is 3300 calls.

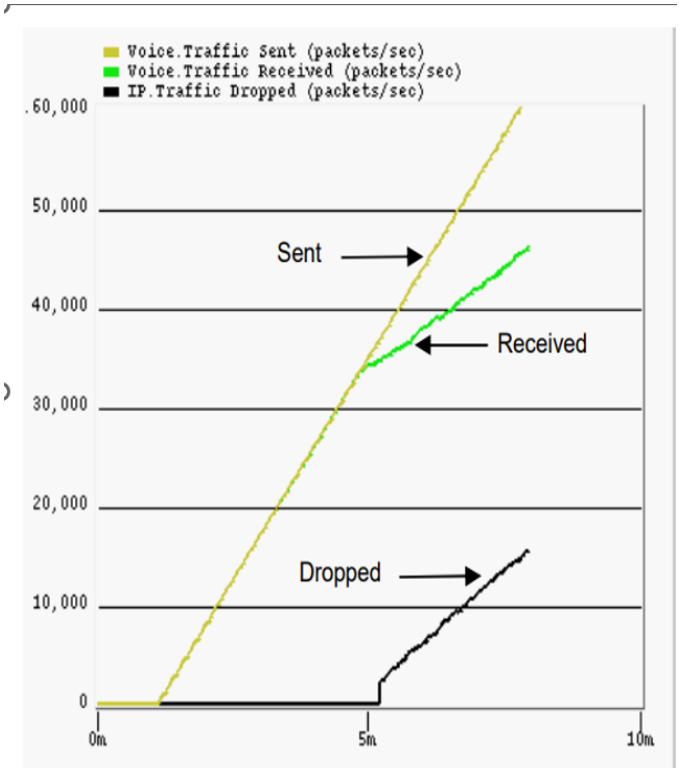

Fig. 8. VoIP traffic sent, received and dropped

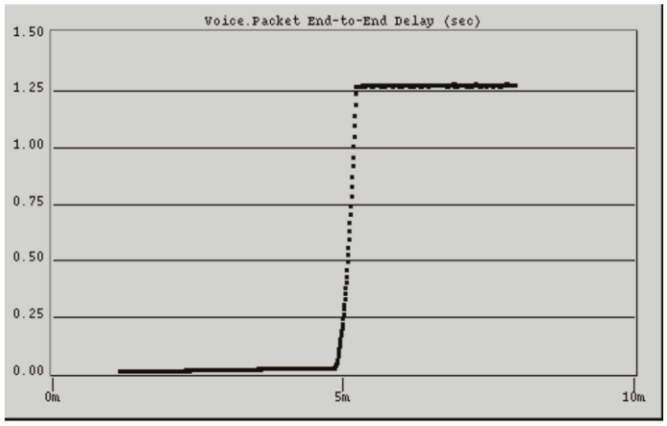

Fig. 9. VoIP traffic end-to-end delay

4.1 Model Result

The initial procedure in the proposed model is to reduce the dimensionality of the generated data by doing feature selection and data filtering using UDP based algorithm. This is to obtain a reliable dataset to be used for the experiments. It is interesting to note that the quality of dataset used has aid in achieving the best value of accuracy on the models as 99.03% for UML and 94.5% for DL respectively, as shown in Figure 10 below.

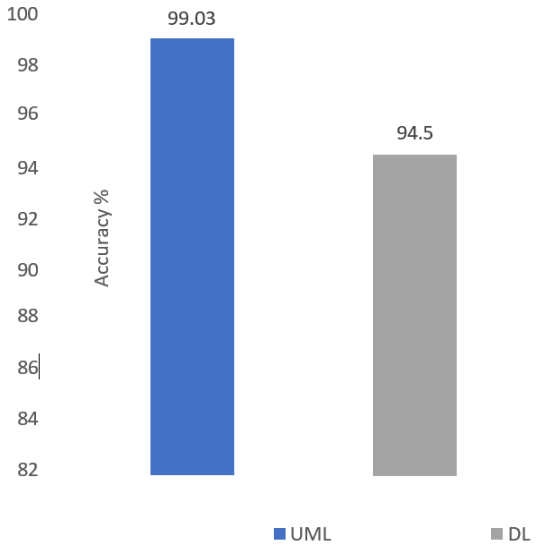

Fig. 10. Comparison of accuracy of proposed UML and DL models.

5 CONCLUSION AND RECOMMENDATION

In this paper, a DDoS attack detection system based on machine learning to prevent attacks on the source side in VoIP network was proposed. We formulated VoIP traffic as a classification problem, extract the features of SIP messages and launch real attacks in lab settings using slow droid for evaluation. Our proposed system is able to produce a dataset with high accuracy (99.03%) based on low voice traffic

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

dropped rate and this will enable achievement of low false positives (< 0.07%) based on high voice traffic received rate. The Proposed method generated a dataset that can effectively differentiates DDoS attacks and legitimate burst traffic when used with Unsupervised Machine Learning algorithm, this is a future work.

ACKNOWLEDGEMENT

This research does not receive any grant or funding from any research funding agencies in the public, private, commercial or NGO.

REFERENCES

Kumar, V and Roy, O (2021). Reliability and Security Analysis of VoIP Communication Systems. 10.1007/978-981-15-6014-9_84.

Werapun W. (2021) Solution Analysis For Sip Security Threats Ieee International Conference On Multimedia Computing And Systems 174- 180.

Tas, I.M. & Baktir, S. (2023) "A Novel Approach for Efficient Mitigation against the SIP-Based DRDoS Attack". Appl. Sci. 2023, 13, 1864. https://doi.org/10.3390/app13031864.

C. Shorten and T. M. Khoshgoftaar, "A survey on Image Data Augmentation for Deep Learning," *J. Big Data*, vol. 6, no. 1, 2019, doi: 1.1186/s40537-019-0197-0.

Alazab A., Hobbs M., Abawajy J., and Alazab M., (2012) "Using Feature Selection For Intrusion Detection System," In 2012 International Symposium On Communications and Information Technologies (Iscit), IEEE, 2012, Pp. 296–301.

Almuairfi S J and Alenezi M., (2020) "Anonymous Authentication for Privacy Preserving Of Multimedia Data In The Cloud" Handbook Of Research On Multimedia Cyber Security (Igi Global) 48-72

Amaizu, G.C., Nwakanma, C.I., Bhardwaj, S., Lee, J.M., Kim, D.S. (2021). Composite And Efficient DDos Attack Detection Framework For B5g Networks. Computer Networks, 188: 107871.Https://Doi.Org/10.1016/J.Comnet.2021.107871

Diogo P. & Rodolfo O., (2022) "Detection of Abnormal SIP Signaling Patterns: A Deep Learning Comparison" Computers 2022, 11(2), 27; https://doi.org/10.3390/computers11020027 Received: 29 October 2021 / Revised: 13 February 2022 / Accepted: 15 February 2022 / Published: 17 February 2022

Fenil E. and Mohan Kumar P., (2020) "Survey On DDoS Defense Mechanisms," Concurrency and Computation: Practice and Experience, Vol. 32, No. 4, E5114, 2020.

Golait D and Hubballi N., (2016) "Detecting Anomalous Behavior In Voip Systems: A Discreteevent System Modeling" IEEE Transactions On Information Forensics And Security 12(3) 730-745

Korstanje J., (2021) "The F1 score," Towards Data Science, 31 August 2021. [Online]. Available: https://towardsdatascience.com/the-f1-score-bec2bbc38aa6. [Accessed March 2022].

Kurt, B.; Yildiz, C.; Ceritli, T.Y.; Sankur, B.; and Cemgil, A.T. (2018). "A Bayesian change point model for detecting SIP-based DDoS attacks". Digital Signal Process. 2018, 77, 48–62.

Luh R, Temper M, Tjoa S, Schrittwieser S and Janicke H., (2020) "Penquest: A Gamified Attacker/Defender Meta Model For Cyber Security Assessment And Education" Journal Of Computer Virology And Hacking Techniques 16(1) 19-61.

Moubayed, A., Aqeeli, E., Shami, A. (2020). Ensemble-Based Feature Selection and Classification Model For Dns Typo-Squatting Detection. Ieee Canadian Conference On Electrical and Computer Engineering (CCECE), Pp. 1-6. Https://Doi.Org/10.1109/Ccece47787.2020.9255697

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)