IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Security Mechanism to Mitigate Ddos Attack on Wireless Local Area Network (WLAN) Using MAC with SSID

Feven Teferi[1*], J. Sebastian Nixon[2]

[1,2]Dept. of IT, School of Informatics, Wolaita Sodo University, Ethiopia

[*]*Corresponding Author: feven.teferi@wsu.edu.et, Tel.: +251-910050963*

DOI: https://doi.org/10.26438/ijcse/v7i4.864869 | Available online at: www.ijcseonline.org

Accepted: 19/Apr/2019, Published: 30/Apr/2019

Abstract— In Wireless Local Area Networks (WLANs), the clients can speak each other by using the Access Point [AP] easily. Since it uses wireless medium for words there are lots of security challenges exists. WLANs provide speed equal to wired LANs and allow wireless devices to be mobile. Even though it is very useful, there are lots of security attacks specially it is vulnerable to distributed Denial of Service (DDOS) attacks, this leads to unavailability of a service or resource by how of either crashes a service or by flooding the network with unwanted traffic to slowing down the delivery of service to the client. A distributed denial of service attack is the one in which the attacker attacks the victim by many sources. In this paper, we deployed WLANs in infrastructure mode as the extension of wired local area network. It was done in experimental approach to detect and prevent DDoS attack by using Intrusion Detection and Prevention System (IDPS) and Machine Authentication Code(MAC) with Service Set Identifier (SSID) was studied and simulated utilizing OPNET 17.5 simulator. The IDPS on the server distinguishes legitimate users from the illegal user by the registered MAC. If the client is illegal, then it withdraws the user from the connection. And the access point will not show SSID. The SSID should be hidden by the Admin and will be given to only the registered users with MAC Address. Our Proposed solution can enhance the security of DDoS and can secure the WLAN from the Attackers.

Keywords— Distributed Denial of Service (DDOS), Intrusion Detection and Prevention System(IDPS), OPNET ,Service Set Identifier (SSID), Machine Authentication Code(MAC) and Wireless Local Area Networks (WLANs).

I. INTRODUCTION

The infrared or radio frequency technology is used in Wireless Local Area Network (WLAN) to exchange data. The first WLAN standard, 802.11 was introduced in 1997 using radio technology with 2.4 GHz frequency and 1 to 2 Mbps of maximum throughput [1][2].

WLANs are used in many fields like corporate, education, finance, healthcare, retail, manufacturing, and warehousing. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost-of-ownership, and scalability[3].

There are the two components in WLAN one is Access Point (AP) and the second is Network Interface Card (NIC). AP is used to connect the wireless devices or clients and the other side it equates with a wired backbone through a standard Ethernet cable using NIC [4].

In WLAN, every client needs proper authentications, privacy and protection against attacks [5]. Moreover, WLAN has limited physical security to prevent unauthorized access and security becomes more difficult. For example, the employees in the corporate environment have unrestricted access to the network. At the same time, outsiders who are share the same air medium should not be allowed to access network resources [6].

Due to more internet users, the illegal access of the internet resources and attacks also increased there are many types of attacks that will be discussed later. The Distributed Denial of Service (DDoS) attack is a big threat to the internet and its clients because the attackers can perform this attack easily if they get the vulnerability in the network. In the past fifteen years, DDoS attacks become more difficult to be mitigated [7].

Thus, security standard services such as confidentiality, integrity, availability, authentication, and access control are not achieved because the internet is exposed to brute force, dictionary, handshake, DoS and DDoS problems and other related attacks.

However, the main goal of this study is to describe different types of DDoS attacks and evaluates the flooding type of

DDoS attack using OPNET simulator which was chosen because of its high reliability to obtain accurate results and propose a solution to improve its security.

We organized this paper into five Sections: Section I contain the introduction to WLAN, various components of WLAN and some security issues. In Section II, we discussed about the related works already done in the Security of WLAN. Section III, Methodology in this, we explained about our experiment with attacks and without attack using the networking simulation tool OPNET. Section IV, Results and Discussions, in this section we discussed briefly about the results we obtained from the experiments and finally we explained about our proposed method that how it would be prevent/mitigate from DDoS attacks. Section V, Conclusion and Future Scope in this we concluded our proposed solution and given some suggestion for future research works in this field.

II. RELATED WORK

The DDOS attacks are known to disrupt services causing inconvenience to intended users. The effects of such attacks can be either temporary or permanent. Heavy processor and memory usage, slow service, more resource consumption of resources. etc are the example of temporary attacks and these make non-availability of resource or service temporarily. In the permanent attacks, the server or services may be crashed, routing information may be corrupted these attacks spoil the image of an organization. [7][8].

According to [9], The proposed solution was within the existing network create a network of virtualized honey pots with minimal cost and administration overheads. The existing network provides security for the following : ftp, mail, web and DNS that are offered to the outside world through a demilitarized zone (DMZ). DMZ consists of external firewall used to protect these servers from external attacks and internal firewall which is used to protect the internal network of the organization. This provides multiple layer protection to the internal network.

Beyond this, other security mechanisms like vulnerability scanners, host based intrusion detection systems, encryption, virtual private network (VPN) is used to strengthen the security. However, effective detection, deflection, and identification of attack sources is necessary [10]. This can be done using honey pots. Another proposed solution was the honey pots can be implemented in Virtual Machines (VM) [11]. These honey VM's will be expose some vulnerabilities to attackers to tempt them to attack and monitor them to secure the network. This ensures that the actual servers may not affect since the honey pots are mimic like a file server, mail server web server .etc and this forms a network of virtual honey pot servers [12].

If the honey VM is compromised, then, the backup Honey VM's will be taken charge. This ensures that intrusion detection and deflection will not be stopped when an existing honey pot is compromised by a DDoS attack. The following figure 1 illustrates the Honey Mesh security infrastructure.

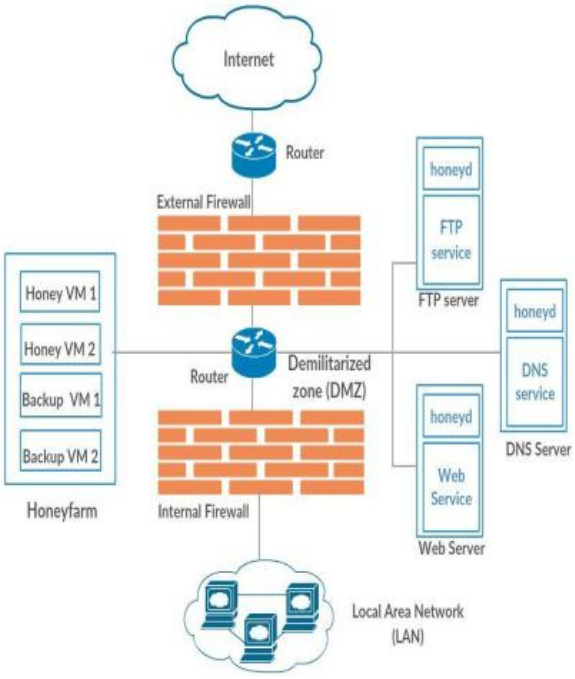

Figure 1 Honey mesh security infrastructures

The Protection against DDoS, attacks extremely depend on the type of attack and the structure of the network. The security protocols can be strengthen by Protocol reordering and Protocol enhancement methods to mitigate resource consumption attacks [13]. The Spoofed IP address attacks can be prevented by a proposed mechanism called Network ingress filtering in this, the router drop packets for illegitimate source IP addresses [14].

The ICMP trace back messages are used to identify the path taken by packets through the Internet. This requires a router to use a very low chance with which trace back messages are sent with the traffic. So, it is possible to find the route taken by the traffic during an attack. This enables localization of the aggressive host [15].

III. METHODOLOGY

A. Simulation of DDoS attack

We used the tool OPNET for different scenarios in our research that support providing reliable outcomes for this study. By using this, we performed DDoS attack.

Scenario 1: File server for normal users

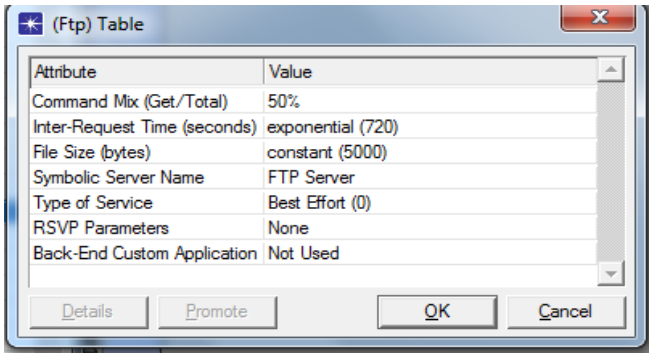

Figure 2. File Server Applications for Normal Users

The goal of the simulation is to have an insight into the detection scheme in addition to the impact of the attack on the WLAN. The Figure2 shows without attack and Fig. 3 shows the result of with an attack in terms of CPU usage, the server's response time and the traffic flow between the server and client for the above-mentioned scenarios. Figure 2 and Figure 3 illustrates the file server for normal client and a file server for abnormal client respectively.

Scenario 2: File server for abnormal users

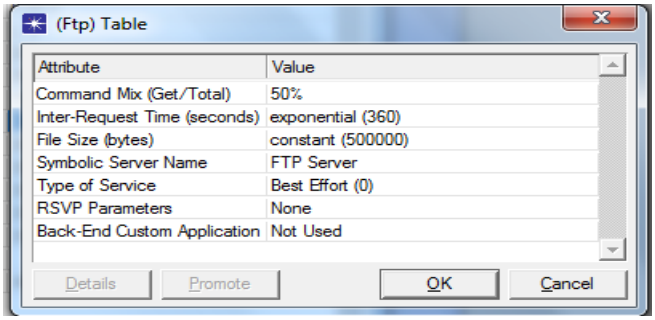

Figure 3. File Server for Abnormal Users

In this scenario first 10 seconds there was no attacks in 20th second the attacks was started with different loads by all the DDoS botnets. Figure 4 illustrates the complete topology including clients and the file server which is trying to attack by the botnets.

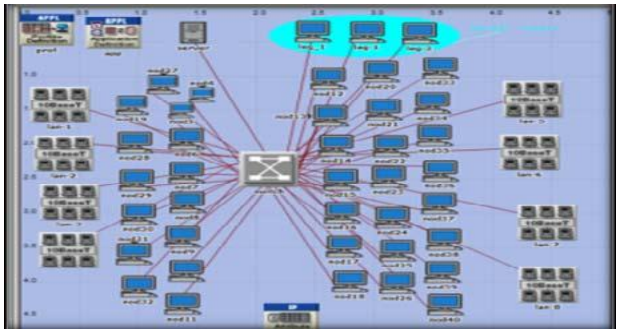

Figure 4.The Simulated Scenarios

B. DDoS attack scenario results

Two tests were done in traffic and network performance. The first test was performed without Attack by sending packets to three normal clients as in Figure 5, in which the rate of traffic sent from users is around 18000 Bytes/sec in a form of three shipments, each user generating traffic of 6000 Bytes/sec. All start at 10 sec for whole simulation time.

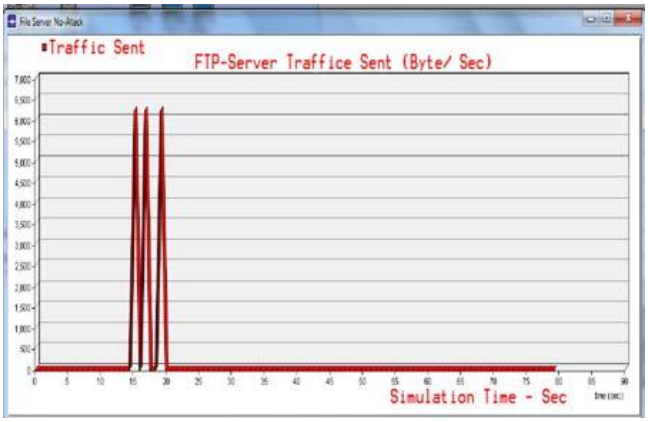

Figure 5 FTP-Server Sent Bytes/sec

Figure 5 shows the traffic of 750 Bytes/sec of a normal client and an attacked client with the traffic of 75 Bytes /sec, and it illustrates that how a DDos could affect the network performance and security.

Figure 6 shows the impact of DDoS attack on legitimate clients in which the red line shows 6000 Byte/sec of traffic received by the normal client and the blue line shows the amount of traffic received after attack that is 500 Byte/sec.

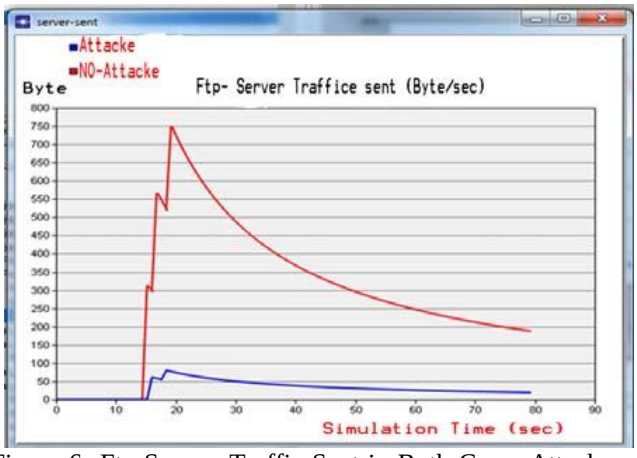

Figure 6 Ftp-Server, Traffic Sent in Both Cases Attack and No Attack

Figure 7 illustrates the effect of DDoS when users try to access the File Transfer Service on the internet.

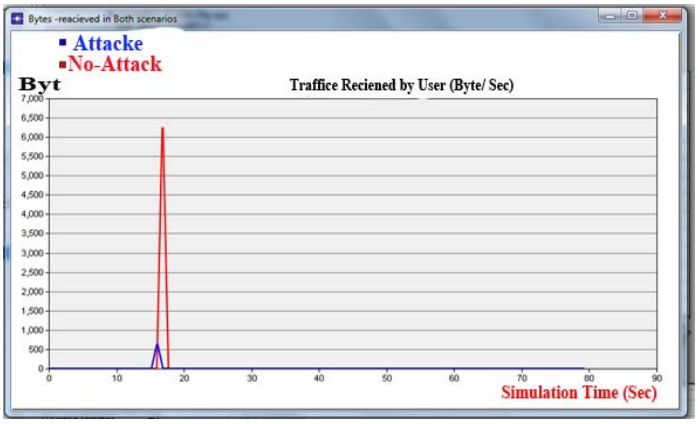

Figure 7.The Comparison of the Normal client and Attacked clients received traffic.

IV. RESULTS AND DISCUSSION

From Experiment 1:

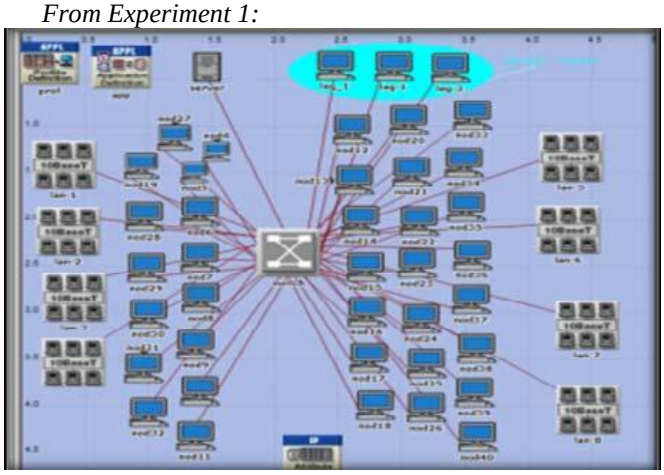

Figure 8. The Simulated Scenario

A. DDoS attack scenario results

To analyzing network performance and traffic, two scenarios were created and tested. The Figure 8 shows the file server traffic without attack while sending packets to three normal clients, rate of traffic around 18000, Bytes/sec is sent from users in a form of three shipments, each user generating traffic of 6000 Bytes/sec. All start at 10 sec for whole simulation time.

Figure 6 illustrates the traffic of normal clients 750 Bytes/sec, and the traffic of attacked clients 75 Bytes /sec. It clearly explains the effect of DDoS attack on the network Figure 9 shows the impact of DDoS attack on legitimate clients. The red and blue lines show the comparison of the received traffic by normal client [6000 Byte/sec], and the attacked client [500 Byte/sec] respectively.

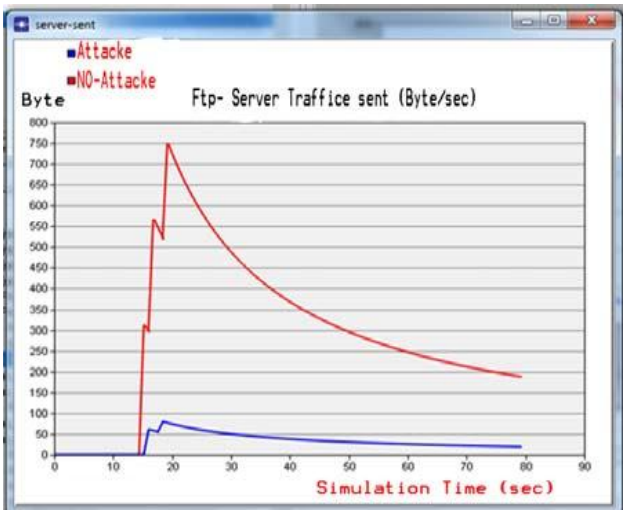

Figure **9** Ftp Server, Traffic Sent in Both Cases Attack and No Attack

B. Proposed Solution

This research proved that there were many loopholes in WLAN security. Therefore, the proposed solution is to improve WLAN security by using IDPS and SSID access control. This helps to discover the loophole in the WLAN by building a model as in the figure 10 below.

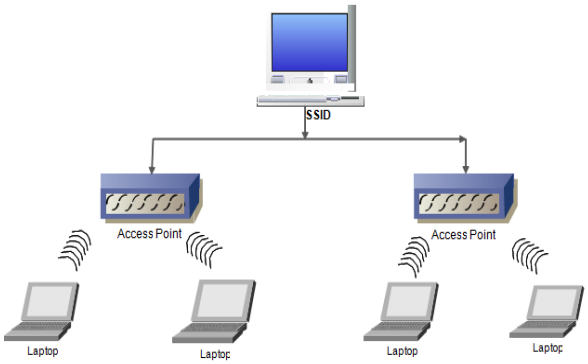

Figure 10. DDoS attack preventing method by SSID

The SSID is the 32 character's name used to connect with a AP in a WLAN. SSID and the password authentication mechanism prevent the unauthorized access of users or attacks to ensure the security of wireless local area network. We can use the SSID in 2 methods.

1. OPEN MODE:

In this the SSID is broadcast in the air, and the clients those who know the password can access the AP at the same time using sniffer tools like NetStumbler3 anyone can find such networks.

2. CLOSED MODE:
In this method, the SSID will be hidden and it will be assigned to the authorized clients by the admin so other users around the WLAN can't be know the SSID.

Any AP will not show SSID. The SSID should be hidden by Admin. The SSID will be given by the Admin only to the authorized clients. We can do it in AP setting itself. The admin will store the MAC address of the authorized clients in the access control database, so the system will only allow the authorized clients in the WLAN. Even the attacker knows the SSID also he can't access the AP since his MAC address is absent in the access control list.

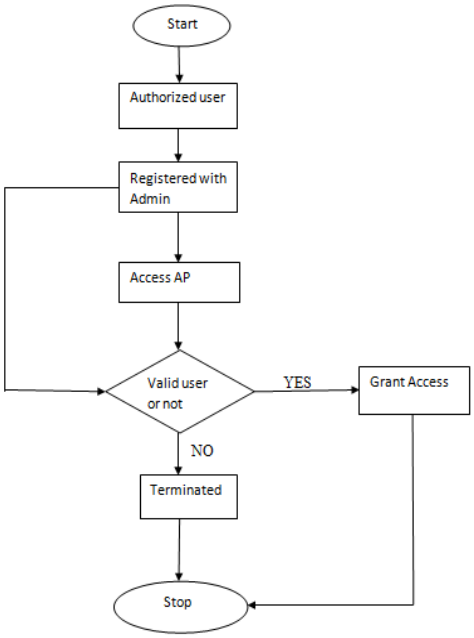

Figure 11 Flowchart of proposed solution

This flowchart explains the access control of the AP's SSID by MAC in a WLAN. By this method, the unauthorized clients can be terminated from the communication.

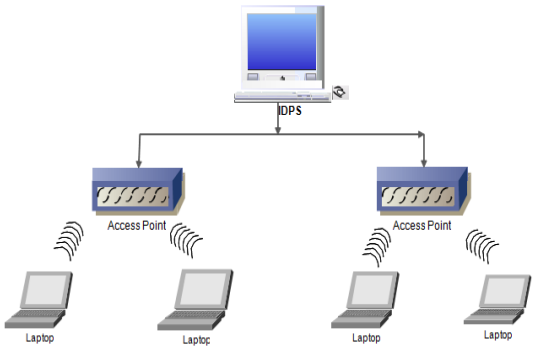

Figure 12. Detect DDoS attack using IDPS

In the figure 12 above, the IDPS on the server distinguish legitimate users from the illegal access. If the client is unauthorized, then it withdraws the user from the connection. Even if the legitimate user sent useless data also, it stops the communication. By installing IDPS in the main server that controls all the APs. If any clients produce unwanted traffic then the server will terminate the client to avoid traffic.

V. CONCLUSION AND FUTURE SCOPE

As WLAN have become more fruitful and complex security vulnerabilities and issues must be met with well thought-out solutions to maintain security. Although the security concerns of WLAN cannot be eliminated by a single absolute security technology, we can moderate them by a proper management and integration of standards, technologies, policies and service environments. In other words, enough security knowledge, proper implementation and continued maintenance is the need of hours for preserving the security of wireless networks.

In this paper, we have done the experiment of DDoS attack using OPNET 17.5 simulator. The Detection and prevention are the good mechanism to secure the network. Since the hidden SSID is only known by the registered/Authorized clients by their MAC address, other unauthorized clients cannot access the network. Also, the IDPS terminate the clients which are making more traffic than the usual one it can avoid the DDoS Attacks even performed by the internal attackers. By this mechanism, we can mitigate/prevent our WLAN from DDoS Attacks. So, our Proposed mechanism can enhance the security of WLAN against DDoS Attack.
The following are some of the future works we suggested for the future researchers:

1. Involving dynamic IP addresses of the resources of packets and performing the required modification on the design of the proposed framework to embrace this change.

2. Including packet fragmentation. In this case, the TTL value will be affected. Therefore, the framework needs to deal with the ID field in order to trace the various fragmented packets of the sent request.

3. Selecting additional packets for further random verification in order to enhance the framework robustness.

4. Embracing the new trend, Bring Your Own Device (BYOD) into the scope of the proposed method to investigate its impacts in amplifying the DDoS attacks from the inner customer's network.

REFERENCES

[1] D. Tepsic, M. Veinović, and D. Uljarević, "Performance evaluation of WPA2 security protocol in modern wireless networks," in the *Proceedings of the2014 1st International Science Conference on Science, Sintaza,* pp. 600–605, 2014.

[2] C. Yang, J. Ma, and X. Dong, "A new evaluation model for security protocols," *Journal of Communication*, vol. 6, no. 6, pp. 485–494, 2011.

[3] D. Dhiman, "WLAN Security Issues and Solutions," *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, vol. 16, no. 1, pp. 67–75, 2014.

[4]. M. D. G. Waliullah, "Wireless LAN Security Threats & Vulnerabilities," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.

[5] Y. Xiao and X. J. Du, "Security mechanisms , attacks and security enhancements for the IEEE 802 . 11 WLANs Chaitanya, Bandela, Edilbert, Kamal Dass", International Journal of Wireless and Mobile Computing, vol. 1, pp. 276–288, 2006.

[6] A. B. M. M. and M. S. R. Md Waliullah, "An Experimental Study Analysis of Security Attacks at IEEE 802 . 11 Wireless Local Area Network", International Journal of Future Generation Communication and Networking Vol. 8, No. 1 (2015), pp. 9-18

[7] "Investigation Of The Impact Of Ddos Attack On Network", Journal University of Zakho, vol. 3, no. 2, pp. 275–280, 2015.

[8] W. Alosami, M. Alshamrani, and K. Al-Begain, "Simulation-Based Study of Distributed Denial of Service Attacks Counteract in the Cloud Services, WSEAS Transactions on Co Simulation-Based Study of Distributed Denial of Service Atta",The University of Nattingham,ePrints,vol. 4, no. 7, pp. 19–30, 2016.

[9] Hrishikesh Arun Deshpande, "HoneyMesh: Preventing Distributed Denial of Service Attacks using Virtualized Honeypots", International Journal of Engineering Research & Technology (IJERT),Vol. 4 ,Issue 08, pp. 263–267, 2015.

[10] Sunil Kumar, Kamalesh Dutta, "Securing Mobile Ad Hoc Networks: Challenges and Solutions", International Journal of Handheld Computing Research, Vol. 7, Issue 1, PP. 26-76,January 2016

[11] Manmohan Dagar, Rashmi Popli "Honeypots: Virtual Network Intrusion Monitoring System", International Journal of Science Research in Network Security and Communication(IJSRNSC), Vol.6,Issue 2, April 2018..

[12] A.Prathap and R.Sailaja, "Detection and Prevention of Denial of Service Attacks Using Distributed Denial-of-Service Detection Mechanism", International Journal of Computer Science and Information Technologies (IJCSIT), vol. 3, no. 6, pp. 5434–5438, 2012.

[13] Usha G, Goudar R H., "ICMPv6 : A Mechanism to Detect and Prevent DDoS Attack", International Journal of Science Technology & Engineering (IJSTE), Vol. 2 ,Issue 12, pp. 420–423, 2016.

[14] S. Behal and K. Kumar, "Trends in Validation of DDoS Research," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 7–15, 2016.

[15] R. Niranchana, N. Gayathri Devi, H. Santhi, and P. Gayathri, "Securing internet by eliminating DDOS attacks," *IOP Comference Series. Materials Science and Engineering*, vol. 263, no. 4, 2017.

Authors Profile

Mrs. Fevan Tafari pursed Master of Information Technology ,Wolaita Sodo University, Ethiopia in 2018. She is working as a Lecturer in Department of Computer Science, School of Informatics, Wolaita Sodo University, Ethiopia. Her main research works focused on WLAN, WSN, Network Security, and Machine Learning.

Dr.J. Sebastian Nixon working as a Professor in Department of Computer Science and Information Technology, School of Informatics, Wolaita Sodo University, Ethiopia. He has secured Professional Certifications from both CISCO and Microsoft Technologies-CCNA & MCSE. His research areas of interests are Information & Network Security, Cyber Scurity, IoT, Machine Learning and Robotics. He is published notable number of research papers in international journals. He is a life member of several academic and professional bodies.

