International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(2): 144-151
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

Preventing IP Spoofing Attacks in a Shared Resources Network

Mr. Hussein Sudi Lema[1] and Dr. Fatuma Simba[2]
University of Dar-es-Salaam, College of Information and Communication Technologies.
[1]lema.hussein@udsm.ac.tz and [2]fatmasimba@udsm.ac.tz

ABSTRACT

Network intruders may spoof IP packets by modifying headers of the IP packets to fool people believe that the transmissions are originating from the trusted source. Consequently, various defence mechanisms have been developed to identify and prevent IP spoofing attack. However, the existing prevention mechanisms are implemented on either destination hosts or routers levels. At these levels facilitate utilization of shared resources on the networks during the attacking process even if there is a mechanism on those levels. To the best of our knowledge, there is no research work reported on how an IP spoofing attacker can be prevented from attacker's LAN before utilizing shared network resources. Therefore, this paper proposes an algorithm for providing an attacker a warning due to his/her attacking activities. The study employed Mininet network emulator, POX controller, Layer 3 switches (L3S), packets analyzer, and packet constructor to design and develop a prototype of the algorithm in a Local Area Network (LAN) environment. Results show that the developed algorithm is capable of returning packets to an attacker as a warning mechanism in a LAN level. The warning packets utilize attacker's network resources/keep the attackers network busy, hence stops IP spoofing attacks. Therefore the attacker is as well get affected by his/her attacking activities.

KEYWORDS

IP Spoofing, POX controller, mininet network emulator, Layer 3 Switch (L3S), Local Area Network (LAN), Software Defined Networking (SDN).

1 INTRODUCTION

Network is one of the biggest components on Information and Communication Technology (ICT). However, despite the benefits gained from the network; its usage poses many challenges such as receiving wrong information and network security flaws [1]. Among the major security flaw is IP spoofing attack. IP spoofing packet is an IP packet which is sent by a sender with forged source IP addresses [11]. The purpose of IP spoofing is to gain access to unauthorized data or information or to hide an attacker identification and utilize a victim shared resources. According to Tanase [12], IP spoofing is one of the most common forms of online hidings. In IP spoofing attack, an attacker gains access to unauthorized information or data from a computer or a network of a victim and malicious messages appear as if they are coming from a trusted machine. Attacks that use IP Spoofing techniques are dangerous because it is difficult to identify location of an attacker. Such attacks include Man in the Middle[13] whereby an attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Another attack is Connecting Hijacking[3] whereby an attacker steals the session of one of the two communicating hosts and drops one of the communicating partner. Denial of Service Attack (DoS)[15] is also an IP spoofing attack in which its target is to utilize shared resource of a victim in order to reduce the victim's performance or prevent a victim from gaining access to the Internet.

The main scenario that facilitates IP spoofing attack is the weaknesses of TCP/IP protocol that allows editing of an IP packet by modifying source IP address and other fields in a packet during packet routing. Routers responsibility is to route or forward IP packets without validating source IP address. Instead, they use only destination IP address to forward packets to the intended host. In addition, during the process of connecting two hosts, a three ways handshaking is used, this same technique can be used by an attacker to prevent a victim to get connection to his/her trusted host. The attacker can fake as a trusted host, hence prevent legitimate communication.

Researchers have implemented different defense mechanisms to detect, prevent and locate IP spoofing attackers on routers. Due to high responsibility of the routers, adding an extra task to detect, prevent and locate IP spoofing attackers reduce performance (add overhead on the operation) of the routers. However, most of the existing mechanisms were implemented at either hosts level (application layer) or routers (network layer). Through this implementation, an attacker can utilize shared network resources on his/her way to the victim before being detected.

Furthermore, tools that were developed to test vulnerability of network components can be used by attackers to make an IP spoofing attack. These tools have a capability to spoof source IP address and they can scan a specific port to check if it is active/open or not. Hence, simplify an attacking process. They include nmap, scapy, and hping3 tools.

Research studies on IP spoofing attack suggest different mechanisms to identify, prevent and locate possible location of an attacker. Some of the mechanisms suggested are Hop-Count Filtering (HCF) [4], Source Address Validity Protocol [5], Spoofing Prevention Method [6] and Ingress [7] and Egress [8] Filtering. However, all these mechanisms do not punish or provide a warning to an attacker and some of the assumptions made in some mechanisms are not realistic. For example, Hop-Count Filtering assume all packets must path on the one route while in real situation, packets of one message can use different paths to the destination. Furthermore, most of the defense mechanisms against IP spoofing are implemented on the router in Wide Area Network (WAN) and host (affected host in the destination network)[9]. This situation allows an attacker to utilize shared resources of the network, even though he/she did not access any information from the intended victim. Therefore, an attacker denies a victim to access information from other legitimate users by utilizing her/his network resources. Lack of any mechanisms to provide a warning to an attacker is also another problem that gives attackers a confidence to continue their attacking activities as there is no effect of any sort is imposed on them. If a warning mechanism is introduced, it can make an attacker stay alert and consequently may stop his/her attacking activities. Among the major challenges to prevent IP spoofing attacks is to locate the correct position of attackers. This is because, attackers use fake IP identification to make communication. Furthermore, Most of the existing mechanisms were implemented at either hosts level (application layer) or routers (network layer). Through this implementation, an attacker could utilize more shared network resources. There is a mechanism developed to identify an IP spoofing attacker using MAC address on LAN level by using Layer 3 switches with POX controller. This mechanism prevent utilization of shared network resources of a victim [16]. This mechanism after detecting an attacker, drop the packets without doing any action for an attacker as a punishment.

Therefore, this study extend the work in [16] by designing and developing an algorithm for locating an IP spoofing attacker and send warning packets to an attacker which will alert an attacker for his/her attacking activities. The warning packets are considered as a punishment to an attacker as it will affect an attacker by utilizing his/her own shared resources and prevent him/her from making more attacks. When the attacker is punished, most likely he/she will stop the attacking activities, hence improve network performance and prevent IP spoofing attacks.

2 DEFENSE MECHANISMS AGAINST IP SPOOFING ATTACKS

There are difference types of defense mechanisms used for IP spoofing packets identification, prevention and locating an attacker. These mechanisms are basically categorized into three types namely, Host based, Router based and Switch based defense methods/mechanisms [16]. To the best of our knowledge, there are no existing mechanisms, which provide a warning to an attacker once IP spoofing attack is detected.

2.1 Host-Based Defense Mechanism

There are two types of host-based defense mechanisms, which are active and passive Defense mechanisms. The active mechanisms need the end-host to perform a pro-active action or active probing. Active host-based mechanisms include cryptographic solutions [17], active probing solutions [18] and IP puzzles [19]. In cryptographic solutions, such as IPSec require a handshaking operation to set up secret keys between two hosts to communicate with an encrypted or signed message. Encryption of a message ensures that only trusted hosts access encrypted message by that secret keys. An attacker cannot rewrite or read a packet or make a connection to any of the hosts which uses IPSec because he/she has no key for decrypting the message.

Passive mechanisms on the other hand, rely only on the information which a host collect locally without probing the supposed source of a packet [9]. In passive host-based defense mechanisms, the decision is made on whether a packet is spoofing or not by passively observing incoming traffic. An examples of passive host-based IP spoofing defense mechanisms is the Hop-Count Filtering (HCF). According to Jin, Wang & Shin [4], Hop-Count Filtering (HCF) system counts and records number of hops from one host to another during a normal time. By measuring the number of hop during normal times, HCF builds a mapping of IP addresses to hop counts. Then, if an IP spoofing attacker sends a spoofing packet to the victim, there is a high possibility for the hop-count of the packet failing to match with the expected hop-count of valid packets from the spoofed source IP address. However, this mechanism has a weakness since legitimate hop-counts can change due to routing changes. In this situation, all packets that do not match the expected ho count are automatically filtered, even if they are legitimate packets.

2.2 Router-Based Defense Mechanism

An example of router-based IP spoofing defense mechanisms are Ingress [7] and Egress [8] filtering, which are the methods that use routers to investigate addresses of packets flowing in and out of network edge and then filter illegal packets.

2.3 Switch-based Defense Mechanism.

This type of mechanism is implemented on LAN by using Layer 3 switches, Address Resolution Protocol (ARP)_and OpenFlow protocol[16]. In this case, an attacker can be identified his/her location by using MAC address on LAN. This mechanism detect IP spoofing attack by comparing source IP address on packet with that of the ARP table. If source IP address does not match, the packet is spoofed. If source IP addresses are the same, authentication will be verified by comparing source MAC address on packet with that of the ARP table. All these validation are done on POX controller by using OpenFlow protocol.

3 METHODOLOGY

This paper use Design Science Research Methodology (DSRM). The DSRM is suitable in developing artifacts such as algorithms or human/computer interfaces [22]. There are five steps in DSRM, problem awareness, suggestion, development, evaluation and conclusion, to be followed during designing, implementing and testing an algorithm or an interface as shown in Figure 1.

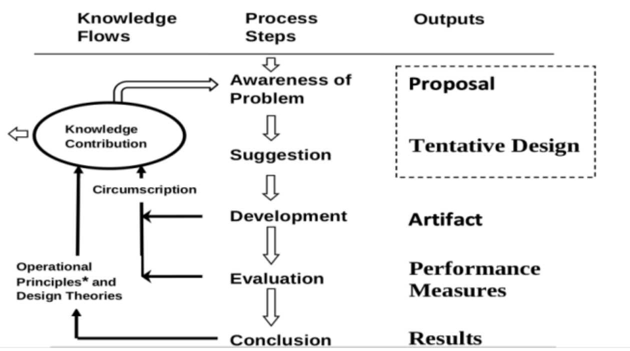

Fig 1:Design Science Research Methodology steps [22]

First step is the awareness of problem during a proposal phase; this is used to investigate in more detail the causes, sources, and level of the problem. This study realised reasons for IP spoofing attack continue to a problem on today’s communication networks, despite several defense mechanisms.

The second step is the suggestion step which is also used during the proposal phase. It is used to determine the possible solution of the existing problem. This study suggested the possible

solutions to the problem and chose the most efficient solution on source IP address validation and warning provision to an attacker. Moreover, the best position, technology, and area to implement algorithms were also suggested.
Development is the third step in DSRM, which is used for designing and implementing an artifact for the suggested solution. During the development phase, an algorithm was designed and implemented for source IP address validation and warning provision to an attacker.
Evaluation is the forth step used in DSRM to test the results of the developed artifact. This study used captured packets from packet analyzer (tcpdump command) to evaluate the results of algorithms. The measurements of performance on this study are; detection of IP spoofing packets by using source IP addresses validation, the conversion of the addresses (MAC and IP address. i.e source to destination and destination to source address) of the detection packets and the effect to an attacker after receiving warning packets(Converted packets their address).
The final step is conclusion; this is used to conclude based on the results obtained during evaluation step. This study made conclusions on the basis of the results obtained during evaluation step.

3.1 Design of an Algorithm for Warning Provision to an IP Spoofing Attacker

The five steps of DSRM were followed in developing an algorithm for warning provision to an IP spoofing attacker as shown in Figure 2.

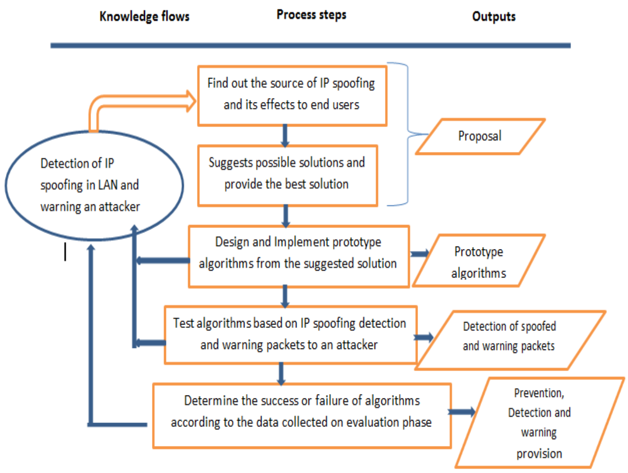

Fig. 2. Steps used to develop prototype of an algorithm to provide a warning to an IP spoofing attacker

Flowchart in figure 3 show how the developed prototype of an algorithm for source IP address validation and sending warning packets to an IP spoofing attacker designed.

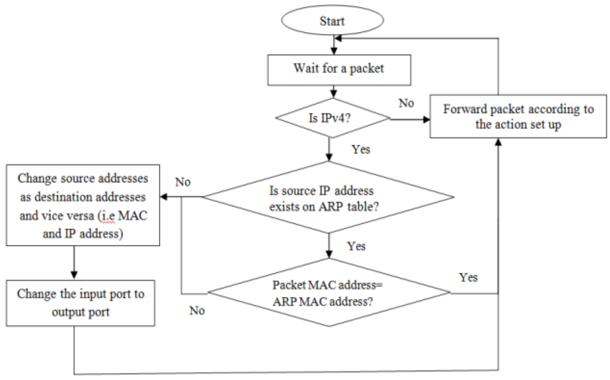

Fig. 3. Flowchart of an algorithm for source IP address validation and warning provision to an IP spoofing attacker

3.2 Implementation of an Algorithm for Warning Provision

Mininet is a *network emulator* which creates a network of virtual hosts, switches, controllers, and links[23]. Mininet hosts run standard Linux operating system, and its switches support OpenFlow for highly flexible custom routing and Software-Defined Networking (SDN). Mininet emulator was used to implement a virtual network topology by using python programming language and Linux operating system. The implemented network topology had four hosts (four virtual machines): host1, host2, host3 and host4, two layer three switches (L3S) and one POX controller as shown on Figure 4. Host1 acts as an attacker and host3 acts as a victim. Controller is used to capture all packets with an IPv4 and analyses whether, it is IP spoofing packets or not. If it is an IP spoofing packet, the algorithm for warning provision to an attack is executed.

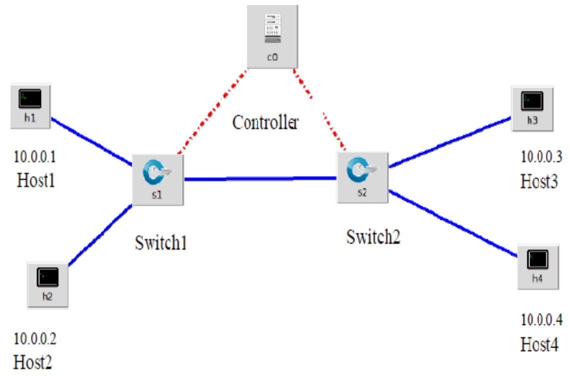

Fig. 4. Virtual network topology used to send warning to an attacker

POX controller is a Python based open source OpenFlow/ SDN Controller[24]. POX is used for faster development and prototyping of new network applications. POX controller was installed with the mininet and virtual machine. POX controller was used to develop algorithm that controls flow of packets by validating source IP addresses and returning back warning packets. POX controller was used to create a warning packet by exchanging source IP address and MAC address as destination addresses and vice versa. Additionally, the input port changed to an output port on which a switch can send the packet back to an attacker. The warning packet created utilizes shared resources of an attacker, hence an attacker suffer for his/her attacking activities. In general, since the packets are still on a LAN, the exchange of address will assists to send the packet back to the attacker by using his/her MAC address.

Virtual machine is a software computer that, like a physical computer, runs an operating system and applications[25]. Every virtual machine has virtual devices that provide the same functionality as physical hardware and have additional benefits in terms of portability, manageability, and security. Virtual machine was used to create hosts within the topology created by mininet emulator. Openvswitch is a virtual switch used to create the two layer 3 virtual switches to connect hosts and POX controller. Scapy and Hping3 are packet manipulation tools that facilitate forging, dissecting, emitting or sniffing network packets [27]. They were used to construct IP spoofing packets. Packet analyzers used by the study are wireshark and tcpdump. Tcpdump is a common packet analyzer that runs under the command line. It allows users to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached[28]. Tcpdump was used to capture packet information as a data collection tool. Wireshark like tcpdump can be used to capture packets information. But on this paper it was used to demonstrate/display data collected on tcpdump only. Log file also was used to capture information/data on POX controller to find errors and other important information about failure or success of algorithms.

4 RESULTS AND DISCUSSION

To test the developed algorithm, IP packets were sent from Host1 (as an attacker) to other hosts without IP spoofing packets and later with spoofed packets to Host3 as a victim. Host1 uses iptables command, scapy and hping3 tools to spoof IP addresses.

4.1 Results from the POX Controller

The log file captures results from POX controller, which collects information from the prototype implemented algorithm. The data collected on log file helps to know whether an algorithm detects a spoofed packet or not. In addition, they show whether warning packet codes are executed or not. POX controller results are shown in Figure 5 and Figure 6. Part One on figure 5 shows a communication with a valid IP address and figure 6 demonstrate communication with IP spoofing attack. In part one of figures 5, the results shows that before an attacker spoofs his/her IP packets, there are requests and replies of packets, which show that there is a good communication to all hosts. Host1 makes a request to Host3 and Host3 returns a reply to Host1.

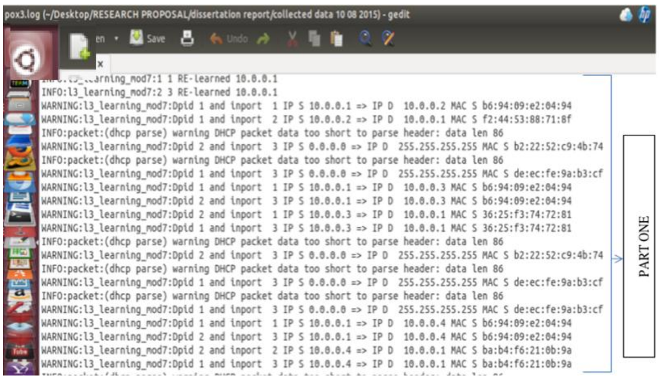

Fig. 5. Results from the POX Controller showing communication with valid IP address before IP spoofing attack

But in part two in Figure 6, Host1 with MAC address b6:94:09:e2:04:94 spoofs IP packet with IP address 192.168.1.150 made by the hping3 tool. After Host1 spoof IP packet, the log file reported that source IP address suspected as spoofed IP packet with no reply packet from destination IP address. In addition, part three in Figure 6, Host1 again spoof IP packet with IP address 100.100.100.100. The spoofed packets are detected and the warning message is executed.

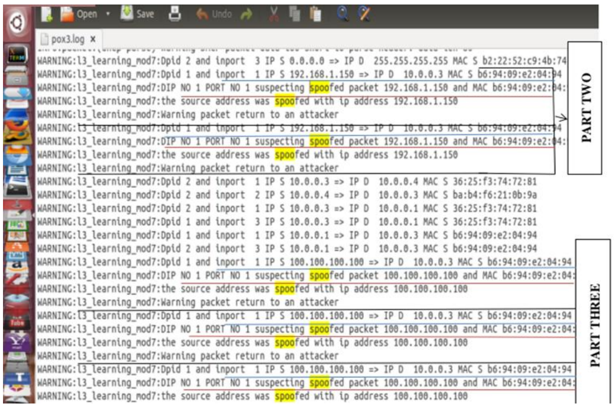

Fig. 6. Results from the POX Controller showing IP spoofing packets and warning packets after IP spoofing attack

Results on POX controller show that the developed algorithm creates a warning packet for every detected spoofing packet sent by an attacker. Warning packets keep a switch and an attacker busy, which is the purpose of this study. This means that an attacker utilizes his/her own resources and works as if he/she is attacking himself/herself.
In general, the algorithm succeeded to create a warning packet and sent it to an attacker after detecting IP spoofing packet by using algorithm for validating source IP address in a LAN. The warning packets sent to an attacker uses the attacker's resources as a negative effect due to his/her attacks. Practically, the attacker experienced adverse effect on getting access for legitimate communication for sometimes. This is because; the warning packets sent to the attacker utilize his/her shared resources. The duration an attacker stay without getting access to communication depends on a number of packets an attacker sent to a victim.

4.2 Results from Host (Virtual Machine)

Results captured by issuing ping command from host 1 to other hosts are divided in three parts; part one is before an attacker spoofs his/her IP address, Part two is after an attacker spoofs his/her IP address and the part three concerns other hosts who communicate with each other before and after an attacker spoof his IP address.
In Figure 7, part one, host 1 has no problems of communication to all other hosts (host 2 (h2), host 3 (h3) and host 4(h4)) because an attacker (host1) did not spoof an IP address. The results show packet loss of 0% and all transmitted packets are received by a target hosts, hence an evidence of successful communication.
But in part two, after an attacker (host1) spoofs an IP packet by using hping3 tool with IP address 192.168.1.150, results show a packet loss of 100% and none of the packets are received to a victim host 3 (h3), communication fails by reporting "destination host unreachable".
Hping3 command works like a ping command but allows inserting fake IP address.

Fig 7. Part one shows results before an attack (packets lost is 0%) and in part two show results after an attack (the packet lost is 100%)

5 CONCLUSION AND RECOMMENDATIONS

This paper succeeded to demonstrate implementation of an algorithm to detect IP spoofing packets, locate an attacker by using MAC address and then send warning packets on LAN level. The identified spoofed packet provides MAC address of an attacker as a correct identifier after spoofing an IP address. For every IP spoofing packet detected, a warning packet is created and sent back to an attacker by using MAC address. The warning packets utilizes the attacker's own shared resources such as a local switch, hence prevented an attacker to continue with his/her attacking activities and his/her legitimate communication. It is recommended that algorithms to detect and prevent IP spoofing be implemented at the LAN level in order to prevent misuse of shared network resources and to correctly locate the attackers by using MAC address. Once an IP spoofing attack is detected and the attacker is located, a punishment must be implemented in order to prevent further attacks. SDN can facilitate implementation of such algorithms on existing networks as demonstrated in this paper.

REFERENCES

[1] Kleindorfer, P. R. and Wind, J., eds. Network challenge: the strategy, profit, and risk in an interlinked world. Pennsylvania, US: Wharton School Publishing. 2010.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, February 2004, Vol.11, No. 1.

[3] C. Chambers, J. Dolske, and J. Iyer, TCP/IP Security:[Online]. Available: http://www .linuxsecurity.com/ resource_files/documentation/ tcpip-security.html, 2019

[4] C. Jin, H. Wang, and K. G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic," *Proc. 10th ACM Conf. Comput. Commun. Secur. - CCS '03*, p. 30, 2003.

[5] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "SAVE: Source address validity enforcement protocol," in *Proceedings - IEEE INFOCOM*, 2002, vol. 3, pp. 1557–1566.

[6] A. Bremler-Barr and H. Levy, "Spoofing prevention method," *Proc. IEEE 24th Annu. Jt. Conf. IEEE Comput. Commun. Soc.*, vol. 1, no. April 2005, pp. 536–547, 2014.

[7] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," *Rfc 2827*, no. 2827. p. 10, 2000.

[8] T. Killalea, "RFC 3013: Recommended Internet Service Provider Security Services and Procedures." 2000.

[9] T. Ehrenkranz and J. Li, "On the state of IP spoofing defense. ACM Trans. Internet Technol. 9, 2, Article 6 ," 2009.

[10] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network of networks," *Phys. Rev. Lett.*, vol. 107, no. 19, 2011.

[11] S. J. Templeton and K. E. Levitt, "Detecting spoofed packets," *Proc. DARPA Inf. Surviv. Conf. Expo.*, vol. 1, 2003.

[12] Matthew Tanase, "IP Spoofing Defense : An Introduction," vol. 1674, Accessed: Feb.16, 2019. [Online].Available: https://www.symantec.com/ connect/articles/ip-spoofing-introduction, 2003.

[13] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-Middle in Tunneled Authentication Protocols IETF Drafts for Tunneled Authentication Protocols," pp. 1–15, 2002.

[15] Q. Gu and S. Marcos, "Denial of Service Attacks Department of Computer Science Texas State University – San Marcos School of Information Sciences and Technology Pennsylvania State University Denial of Service Attacks Outline," pp. 1–28.

[16] H. Lema, F. Simba, and A. Ally, "Preventing Utilization of Shared Network Resources by Detecting IP Spoofing Attacks through Validation of source IP Address," pp. 1–8, IEEE 2018 IST-Africa Week Conference (IST-Africa). Gaborone, Botswana, 2018

[17] Kong Y., Seberry J., Getta J.R., Yu P., "A

Cryptographic Solution for General Access Control". In: Zhou J., Lopez J., Deng R.H., Bao F. (eds) Information Security. ISC 2005. Lecture Notes in Computer Sciene, vol 3650. Springer, Berlin, Heidelberg, 2005.

[18] M. Brodie, I. Rish, S. Ma, G, Grabarnik, N. Odintsova, Active probing, Technical Report IBM, 2002.

[19] W. Feng, E. Kaiser, and A. Luu, “Design and implementation of network puzzles,” *Proc. IEEE 24th Annu. Jt. Conf. IEEE Comput. Commun. Soc.*, vol. 4, 2005.

[20] C. Jin, H. Wang, and K. G. Shin, “Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic,” *Proc. 10th ACM Conf. Comput. Commun. Secur. - CCS ’03*, 2003.

[21] P. S. F. Baker, “Ingress Filtering for Multihomed Networks,” *RFC 3704*, pp. 1–16, 2004.

[22] V. Vaishnavi and B. Kuechler, “Design Science Research in Information Systems Overview of Design Science Research,” *Ais*, p. 45, 2012.

[23] M. Team, “Mininet Overview - Mininet,” [Online]. Available: http://mininet.org/overview/, 2018.

[24] S Kaur, J Singh andN S Ghumman, “Network Programmability Using POX Controller,” [Online] Available at:http://sbsstc.ac.in/icccs2014/Papers/ Paper28. pdf, 2014.

[25] James, E.S. & Ravi, N., "The architecture of virtual machines.", IEEE Computer. 38. 32-38, 2005.

[26] L. Torvalds, "*OpenvSwitch software*." Linux Foundation Collaborative Project, 2016.

[27] P. Biondi and the Scapy community, "*Scapy documentation",2018.* [Online]. Available: https:// media.readthedocs.org/pdf/scapy/latest/scapy.pdf.

[28] P. Asrodia, H. Patel, "Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis", in IJEECE, 2012, paper 2277-2626, p. 55-58