IST-Africa 2018 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2018
ISBN: 978-1-905824-60-1

Preventing Utilization of Shared Network Resources by Detecting IP Spoofing Attacks through Validation of source IP Address

Hussein LEMA, Fatuma SIMBA, Abdulla ALLY
College of ICT (CoICT), University of Dar-es-Salaam, P.O. Box 33335, Dar es Salaam, Tanzania
Tel: +255 678362122, +255 754034375, +255 713475497, Email:
hussul2005@yahoo.co.uk, fatmasimba@gmail.com, abdul.informatics@gmail.com.

Abstract: Network intruders may spoof IP packets by modifying headers of the IP packets in order to fool people to believe that the transmissions are originating from trusted source. Consequently, various defencing mechanisms have been developed to identify and prevent IP spoofing attacks. However, most of them were implemented on either hosts or routers levels which utilizes a lot of shared resources on the networks during the attacking process. On the contrary, this paper proposes an algorithm for validating source IP address by using Layer Three Switches (L3S) in a Local Area Network (LAN), which means that the IP spoofing attacks will be identified and prevented without utilizing shared network resources. The study employed Mininet network emulator, POX controller, L3S, packets analyzer, and packet constructor to design and develop the algorithm. Results have shown that the algorithm was capable of detecting and preventing IP spoofed packets on LAN before L3S forward them to a target, and eventually an attacker was identified by using his/her MAC address.

Keywords: Media Access Control (MAC), POX controller, Mininet, Layer Three Switch (L3S), spoofing packet

1. Introduction

Internet Protocol (IP) address is the major identification for source and destination hosts on the Internet. However, network intruders may create IP packets with a fake IP address to hide their identity or impersonate others, presenting a false truth in a credible way. Attackers often make use of IP spoofing techniques to perform malicious activities, such as Blind Spoofing[1], Man-in-the-Middle Attack[2], and Denial of Service Attack[3]. IP Spoofing is generally used to maintain anonymity and cause despoliation on the Internet. Attackers can modify headers of the IP packets to fool people believe that the transmissions are originating from the trusted source. As such, attackers utilize victim's shared resources, such as bandwidth, in order to reduce the performance of activities made by a victim or prevent a victim to gain an access to the Internet. Since attackers are mostly interested with consuming shared resources, they do not worry about properly completing transactions; rather they wish to flood the victim with many packets as possible in a short time. In order to continue the attack without being identified, they spoof their source IP addresses to make it difficult to trace them or to stop them from their attacks.

Internet originality did not consider validation of source IP address [4]. Consequently, various mechanisms have been developed to prevent IP spoofing attack [5]. One of the most prominent technique is the Ingress [6] and Egress [7] filtering. They are running on a router at the border of a network. Ingress and Egress filtering use routers to investigate the addresses of packets flowing in and out of the network edge. A packet originating from the edge network is suspected as a spoofing packet if the source IP address does not belong to

the edge network (Egress mechanism). Likewise, regarding a packet coming from outside the edge network, if the source address belongs to an edge network (Ingress mechanism), the packet is suspected as a spoofing packet. The edge routers are simply able to filter out any packet that identified as a spoofing packet. Another method similar to ingress/egress filtering is Reverse Path Forwarding (RPF) [8], whereby routers running RPF attempt to filter packets depending on where a packet is coming from with a given source IP address. While Ingress/Egress filtering considers two directions, which is the direction moving either into an edge network or out of an edge network. RPF attempts to deal with traffic passing through a given router from any direction to any direction. It uses the forwarding table information at the router to detect whether the packets are IP spoofing packets or not. It is believed that any direction, or interface, a packet with destination address, say address *"a"*, should be forwarded to; in the same direction a packet with source address *"a"* should arrive.

Another ways of defending against IP spoofing packets are the use of TCP-specific probe and cryptographic solutions [9]. TCP-specific probe use TCP handshake that is enough to prevent attackers from spoofing TCP packets since attackers may be able to predict TCP sequence numbers. Most of the operating systems use a random sequence number selection to generate a sequence number. The pseudo-random number generators may not use sequence numbers which are random enough to prevent an attacker from predicting them [10]. TCP-specific probes cleverly create TCP acknowledgment messages to add another layer of protection. Since the sender of IP spoofing packets is often unable to see any replies, a recipient host can send acknowledgments that should change the TCP window size or cause packet retransmission, and then observe whether the supposed source responds correctly or not. If the supposed source does not change the window size or does not retransmit the packet, the recipient host considers sender spoofs the packet's source IP address. 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 be able to rewrite or read a packet successfully or making a connection to the one of the hosts who uses IPSec because he/she has no key for decrypting the message.

Despite numerous techniques, IP spoofing attack still remains an open problem [11]. Yet, most of the existing defense mechanisms for identification and prevention of an IP spoofing packets were implemented on either hosts or routers levels [5] which utilizes a lot of resources on the networks. This means that attackers whose target is the utilization of resources will definitely succeed. Moreover, since the owner of a computer has a full control on system files, it is possible for intruder to change configuration of the source IP validation in order to make an attack. Also, validation of source IP address on the host level is a threat to networks in the sense that, an attacker can disable this validation by using whichever means to continue the attacking. Therefore, validation at the host level is not a good solution to an IP spoofing attack. Likewise, when the validation is made on the receiver side, it will be too late to make an action to protect a victim from attacking. Other host-based methods require too much overhead that may impact router's performance [5].

To solve IP spoofing problem effectively, it is recommended to use Local Area Network (LAN) as a place for validating source IP address in order to reduce utilization of network resources. This is because resources used on LAN are fewer compared to number of resources that could be affected if validation was to be done at a Wide Area Network (WAN) level. Furthermore, it is easier to locate an attacker by using MAC address in a LAN. It appears that the existing Internet architecture can hardly solve an IP spoofing attack due to absence of explicit notion of packet-level authenticity[12]. However, through the use of OpenFlow protocols, the evolution of Internet architecture can be made easier

[13]. This technology provides an interface to control flow level traffic on router/switch that supports OpenFlow protocol by POX controller, which implements the controller for OpenFlow switches and routers. Its architecture provides necessary components and interfaces to make extensions easy to implement new innovation on internet. Such architecture shifts the complexity of adopting a new protocol from the router/switch to the controller, and makes it easier to take an evolution. With the adoption of OpenFlow in router/switch, evolutions based on OpenFlow can be adopted much easier.

This paper proposes an algorithm to validate source IP address using OpenFlow technology on Layer Three Switch (L3S) in a LAN. The algorithm identifies and prevents IP spoofing packets with minimum utilization of shared resources and locates an attacker by using MAC address. Implementing this algorithm will enable systems administrators to monitor users for efficient utilization of resources.

2. Objectives

The general objective of this study was to design and develop an algorithm for detecting and preventing IP spoofing attacks through validation of source IP address closer to the attacker, hence prevent utilization of shared network resources. Specific objectives were:

1. To establish protocol, technologies and location of IP spoofing identification that can support validation of source IP address.
2. To design and implement an algorithm for source IP address validation. The algorithm must detect IP spoofed packets before L3S forward the packets to a target.
3. To evaluate the effectiveness of the proposed algorithm.

3. Methodology

The methodology used in this study is Design Science Research Methodology (DSRM) as shown in Figure 1. DSRM focuses on the development and performance of (designed) artefacts with the explicit intention of improving the functional performance of the artefact. It is typically applied to categories of artefacts including (but not limited to) algorithms, human/computer interfaces, design methodologies (including process models) and programming languages [14].

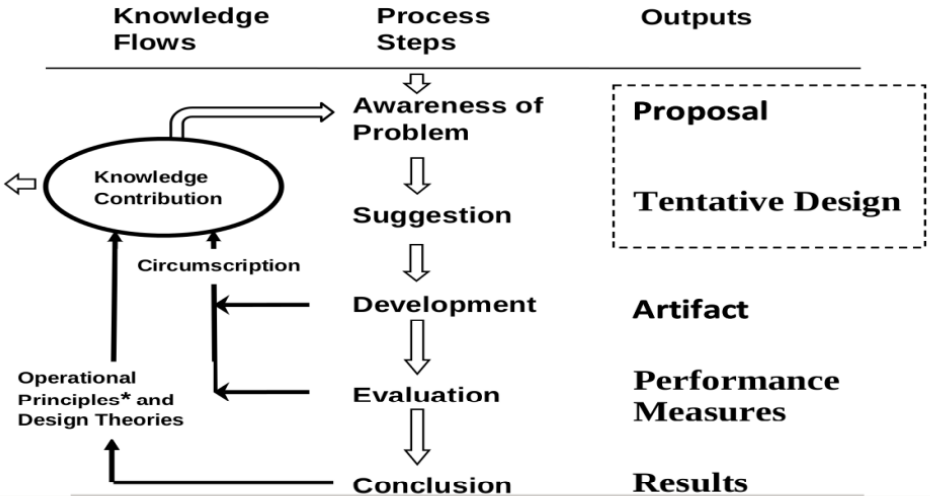

Figure 1: Design Science Research Methodology steps[14].

4. Technology Used

A network with Ethernet technology for LAN and Layer-2 addresses (MAC addresses) used to support communication between networks devices were considered in this study. OpenFlow

technology was also used. The OpenFlow technology used a device called controller to handle or control flow of packets in the Internet. Other technologies/tools used include the following:-

- Scapy and Hping3: These are packets sniffer and constructors that were used to construct IP spoofing packet and test the security of a network. Scapy was used to create packet with an IP spoofing address while Hping3 was used as a ping command with more options including modify fields and/or contents like inserting IP spoofing address to a packet.
- Iptables program: It was used to set a default source IP address in a Network Address Translators (NAT), which was used by a sender on a Linux operating system. Therefore, it helps to create IP spoofing packets by setting fake IP address on NAT. After running the Iptable command in Linux operating system, any packet sent by such node contains fake/spoof source IP address.
- Tcpdump: A packet analyser; it was used to capture packets, to monitor, intercept, and decode data packets as they are transmitted across networks.
- Mininet network emulator: This software was used to create a virtual network topology that can run kernel, switch and application code on a single machine. It was designed to interact with other software such as POX controller, scapy, and Hping3 and perform different commands on networks.
- POX Controller: It was used to implement the algorithm. In addition, data collected on it was used to determine either a spoofed packets are detected or not. POX controller integrated with Mininet emulator was used to control flow of packets and make decisions on behalf of a switch.
- Virtual Machine: This is a software which was used to simulate more than one machine on a single personal computer. It was used to create and demonstrate four hosts on a topology designed for this study.
- Openvswitch: Openvswitch was integrated to the mininet emulator in order to come up with switches which were controlled by POX controller.

5. Developments

The developed algorithm was implemented on POX controller for emulation process and topology were created by Mininet with four host, two L3S and one controller. Each L3S was connected with two hosts as shown in Figure 2.

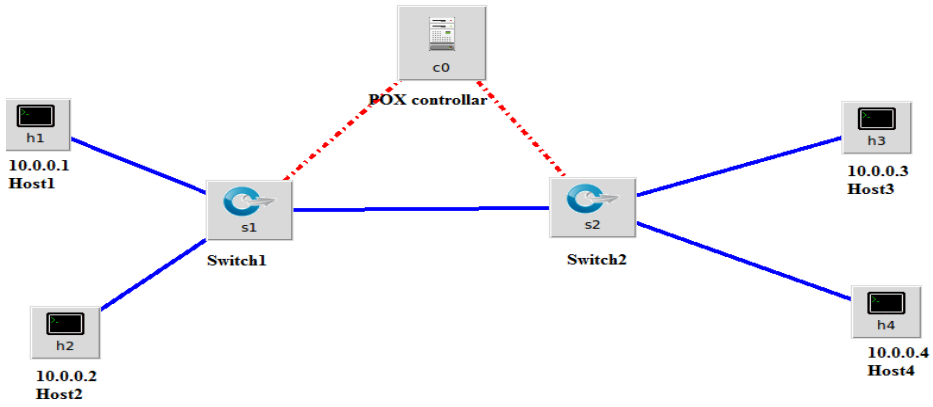

Figure 2: Virtual network topology used to test IP spoofing attack

The proposed algorithm for validating source IP address is illustrated in Figure 3. Note that, the record stored on ARP table was used to make comparison with IP packets.

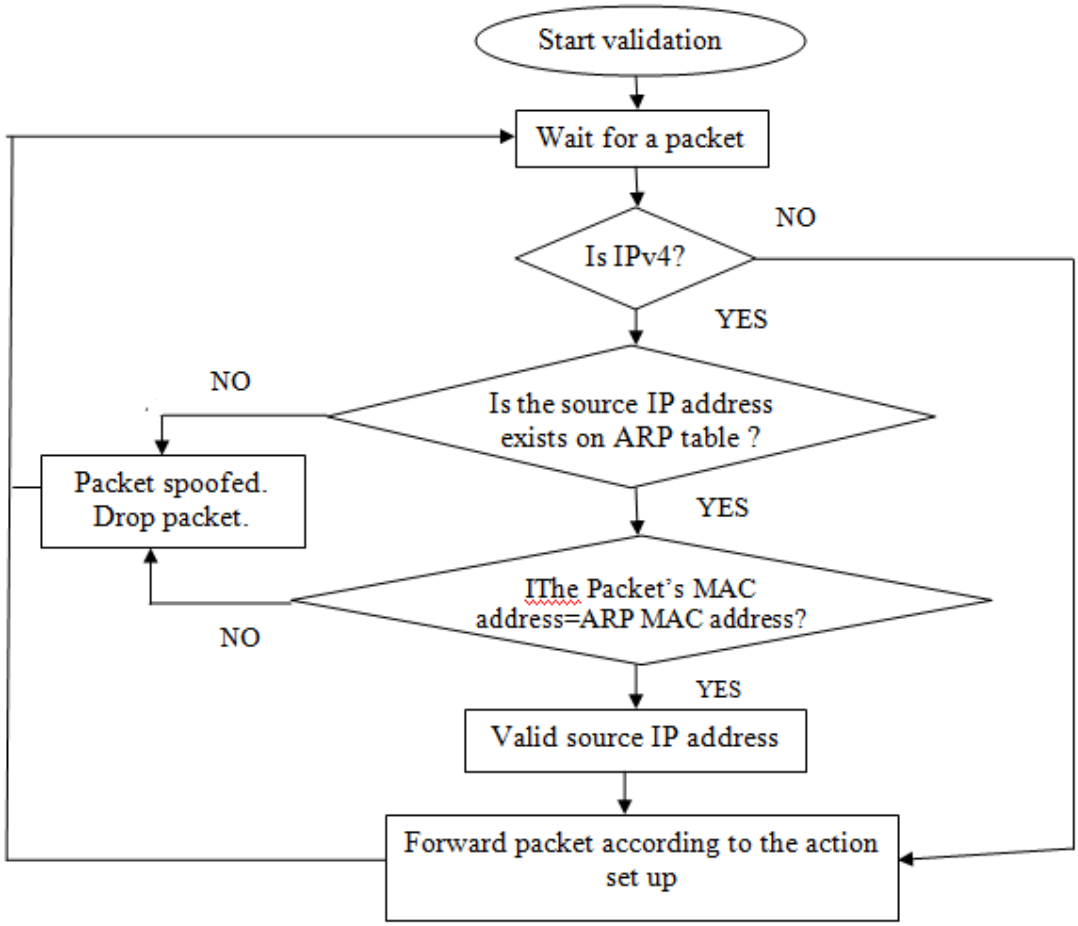

Figure 3: Flowchart of algorithm for source IP address validation

6. Results

Herein, we present results that were collected in terms of log file on POX controller and tcpdump program on Hosts where Host1 acted as an attacker and Host3 as a victim.

6.1 Log Files on POX Controller

The findings indicated that the algorithm has succeeded to identify IP spoofing packets sent from Host 1 to Host 3 through LAN in POX controller. For example, source IP address 192.168.1.150 was suspected as a spoofed IP packet with a MAC address b6:94:09:e2:04:94 as demonstrated in Figure 4 (Part One). Source IP address 100.100.100.100 with a MAC address b6:94:09:e2:04:94 was also detected as spoofed IP address (Figure 4 (Part Two). Since the algorithm was implemented on LAN, the utilization of shared resources among users is minimized. On the other hand, when ARP cache/table in the L3S is not updated, valid IP address can also be detected as spoofed packet. However, this problem occurs rarely and can be eliminated once the ARP is updated.

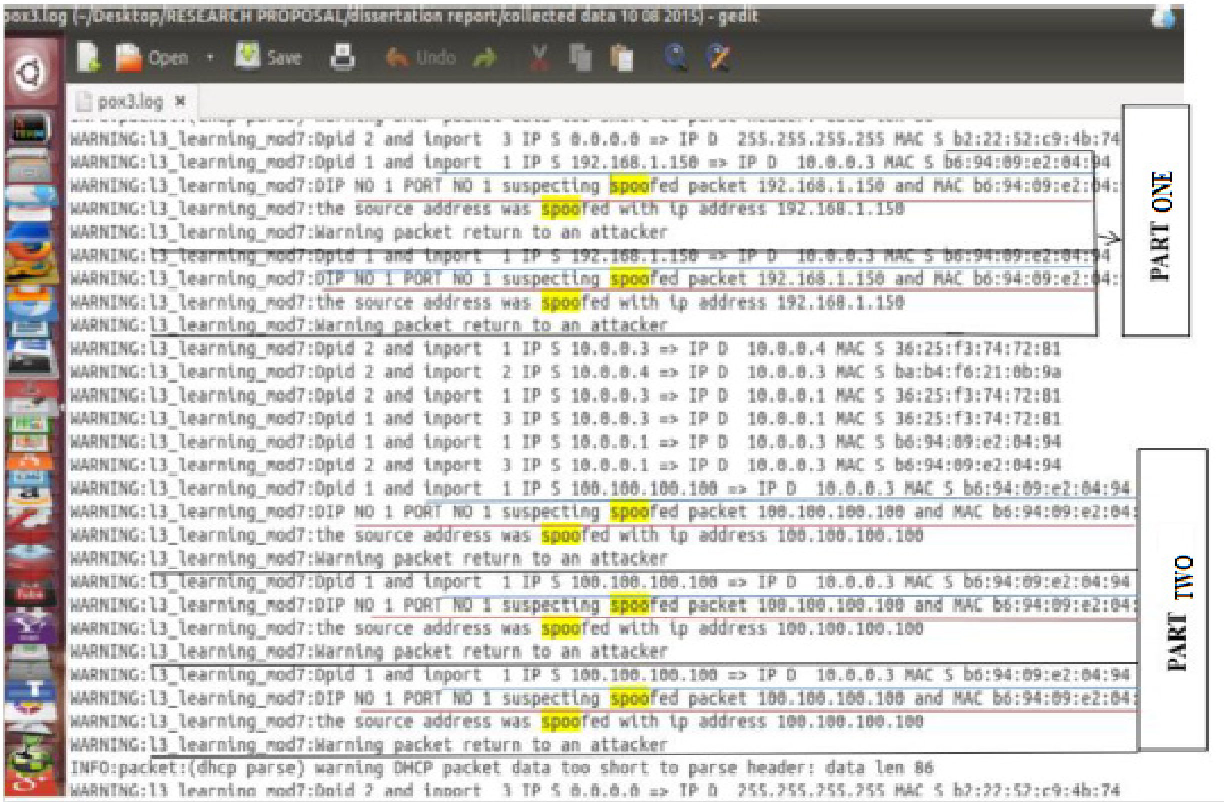

Figure 4: Results from the POX Controller

6.2 tcpdump Program on Hosts

It can be seen that an attacker (Host1) sent spoofed packet with an IP address 100.100.100.100 (Host 1 address is 10.0.0.1) to Host3 (10.0.0.3) as reply packets without having request packets from Host3, as illustrated in Figure 5. However, the victim (Host 3) in Figure 6 didn't show any received packet with that IP address. That means the spoofed packet did not reach the indented victim/target, and only packets with correct IP address were captured. This implies that the switch through POX controller detected all spoofed packets and did not allow them to reach to the victim by dropping the suspected packets.

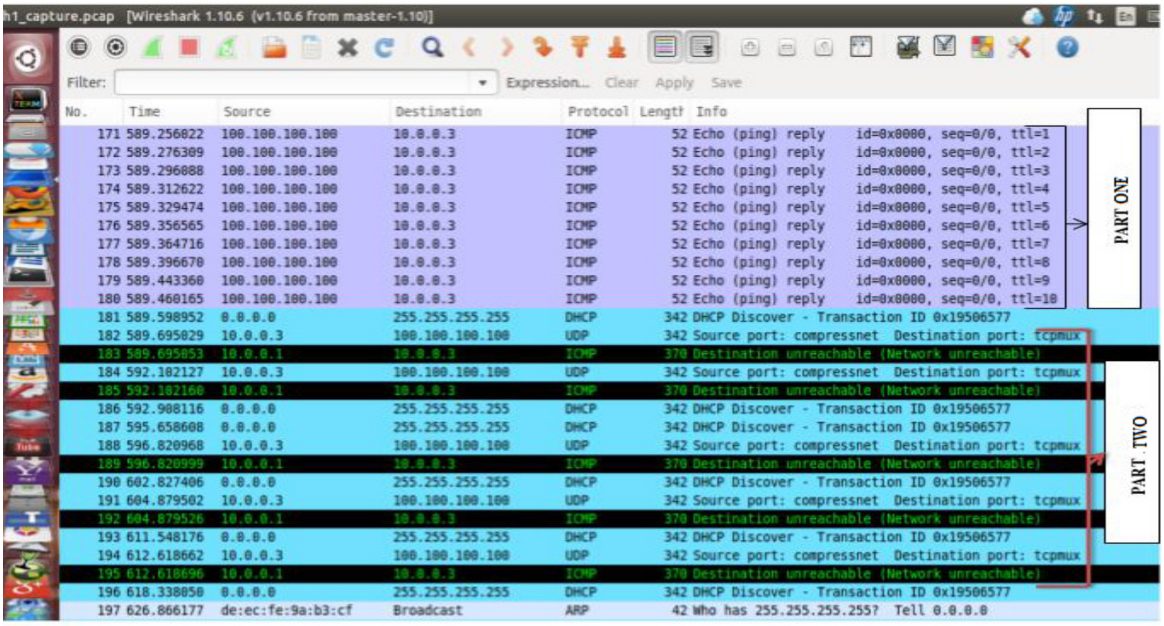

Figure 5: Results from/to the Host1 (Attacker)

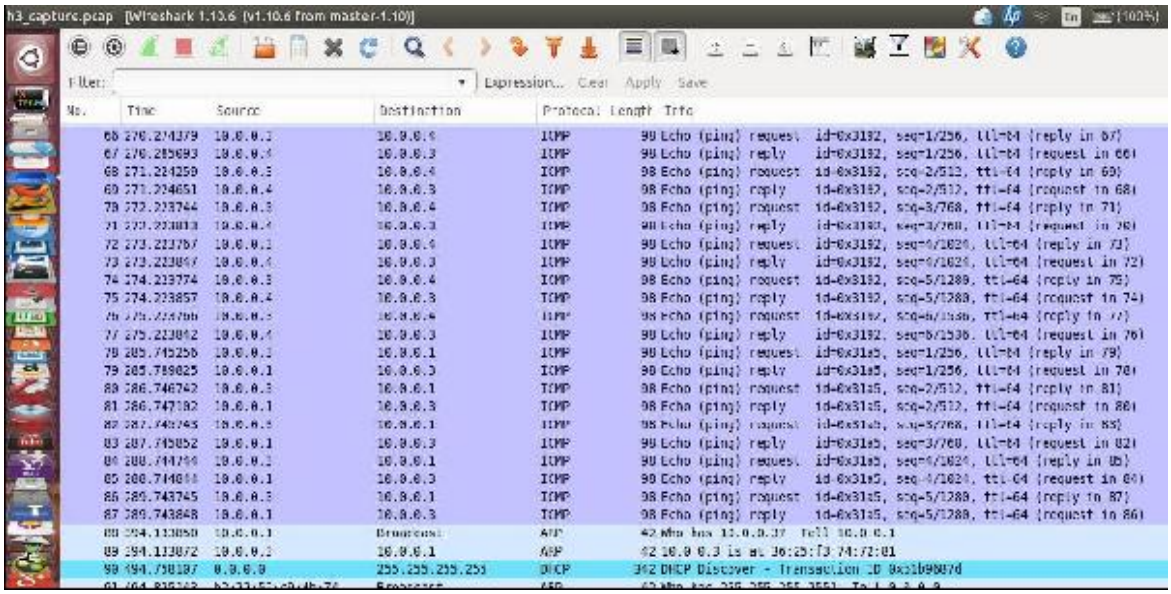

Figure 6: Results from/to the Host3 (Victim)

7. Business Benefits

The proposed algorithm if implemented will prevent misuse of shared network resources by IP spoofing attacks, as a result there will be a good network performance, hence business benefits. Users of the network will be assured of network services i.e. availability and integrity. When users are satisfied, more people can be attracted to use networks hence more business benefits.

8. Conclusion

While the existing defence mechanisms relied on hosts and routers levels in Wide Area Networks, this study implemented a defence mechanism on Local Area Networks (LAN) using Layer Three Switches (L3S). By using OpenFlow technology, OpenFlow protocol and python programming language, the algorithm was designed and implemented. The results have shown that the proposed algorithm was capable of detecting and preventing IP spoofed packets on LAN before L3S forward them to a target, and eventually an attacker was identified by using his/her MAC address.

During IP spoofing attacking process, attackers usually target to utilize shared network resources. The implemented mechanism reduces utilization of shared resources as the detection takes place in a LAN and all spoofed packets are detected using their MAC addresses, which are in turn used to identify the real location of an attacker. Moreover, the algorithm can prevent a victim from receiving any spoofed packets. Future work entails exploring the actions to be taken for the identified attacker to stop his/her IP spoofing attacking activities.

References

[1] M. Tanase, "IP Spoofing: An Introduction," 10 Mar 2003. [Online]. Available: https://www.symantec.com/connect/articles/ip-spoofing-introduction. [Accessed Jan. 18, 2018].

[2] C. Chambers, J. Dolske, and J. Iyer, "TCP / IP Security," *Control*, Columbus, Ohio 43210, pp. 1–22, 06-Dec-2011. [Online]. Available: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html.[Accessed Dec, 29, 2017].

[3] Q. Gu and S. Marcos, "Denial of Service Attacks," . In *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*; Bidgolli, H., Ed.; John Wiley & Sons: Hoboken, NJ, USA, 2007.

[4] T. Ehrenkranz, "Ensuring A Valid Source And Destination For Internet Traffic,", Doctor of

Philosophy Thesis,University of Oregon, 2012.
[5] T. Ehrenkranz and J. Li, "On the state of IP spoofing defense," *ACM Trans. Internet Technol.*, vol. 9, no. 2, pp. 1–29, 2009.
[6] 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.
[7] T. Killalea, "RFC 3013: Recommended Internet Service Provider Security Services and Procedures." 2000.
[8] P. S. F. Baker, "Ingress Filtering for Multihomed Networks," *RFC 3704*, pp. 1–16, 2004.
[9] Y. Kong, J. Seberry, J. R. Getta, and P. Yu, "A Cryptographic Solution for General Access Control," in *Science*, no. September 2005, 2005, pp. 461–473.
[10] M. Zalewski, "Strange Attractors and TCP / IP Sequence Number Analysis," Bind View Technical Report, April 2001. [Online]. Available: http://www.bindview.com/Services/ Razor/Papers/ 2001 /tcpseq.cfm. [Accessed Jan. 18, 2018].
[11] P. Vixie, "Addressing the challenge of IP spoofing," no. September, pp. 1–17, 2015. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf. [Accessed Mar. 12, 2018].
[12] BEVERLY, R., BERGER, A., HYUN, Y., AND CLAFFY, K. Understanding the Efficacy of Deployed Internet Source Address Validation Filtering. In Internet Measurement Conference (IMC), 2009.
[13] N. Mckeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, and S. Louis, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, p. 69, 2008.
[14] V. Vaishnavi and B. Kuechler Vaishnavi, V., Kuechler, W., and Petter, S. (Eds.) (2004/17). "Design Science Research in Information Systems,". [Online]. Available: http://www.desrist.org/desrist /content/design-science-research-in-information-systems.pdf. [Accessed Mar. 12, 2018].