RESEARCH PAPER

ON
Preventing IP Spoofing Attacks in a Shared Resource Network

PRINCE RIXON HADLIN

Keraleeya Samajam's Model College, Dombivali East, Mumbai, Maharashtra, India

1.ABSTRACT

Network theif may spoof IP packets by modifying the headers of the IP packets to fool people believe that the transmissions are originating from the trusted source. Therefore, various defence operation have been developed to identify and prevent IP spoofing attack. However, the existing prevention operation or mechanisms are implemented on either destination hosts or routers levels. At these levels simply 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 none of the 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 of Mininet network emulator, POX controller, 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 or operation in a LAN level. The warning packets utilize attacker's network resources or keep the attackers network busy, hence stops IP spoofing attacks. Therefore the attacker is as well get affected by his or her attacking activities.

Keywords: IP Spoofing, mini-net network emulator, Layer 3 Switch , Local Area Network (LAN), Software Defined Networking (SDN).

2. INTRODUCTION

Network is one of the biggest components on Information and Communication Technology (ICT). However, despite the benefits gained from the networks, it's an usage pose more challenges such as receiving incorrect information and network security flaws.. Among the major security flaw is IP spoofing attack.

IP spoofing packet is an IP packet that is despatched through a sender with cast supply IP addresses. The motive of IP spoofing is to advantage get admission to to unauthorized facts or records or to cover an attacker identity and make use of a sufferer shared resources. According to Tanase, 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 community of a sufferer and malicious messages seem like they're coming from a depended on machine. Attacks that use IP Spoofing strategies are risky due to the fact it's miles tough to become aware of area of an attacker. Such attacks include Man in the Middle whereby anattacker secretly relays and possibly. Alters the communique among events who agree with they're without delay speaking with every other. Another attack is Connecting

Hijacking 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) 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 primary situation that helps IP spoofing assault is the weaknesses of TCP/IP protocol that lets in 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 excessive obligation of the routers, including an additional challenge to detect, prevent and discover IP spoofing attackers lessen performance (upload overhead at the operation) of the routers. However, maximum of the present mechanisms have been applied at both hosts level (utility layer) or routers (community layer).

Through this implementation, an attacker can make use of shared community assets on his/her manner to the sufferer earlier than being detected.

Furthermore, equipment that have been advanced to check vulnerability of community additives may be utilized 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 tools.

Some of the mechanisms suggested are Hop-Count Filtering (HCF) ,Source Address Validity Protocol, Spoofing Prevention Method and Ingress and Egress Filtering. However, some of these mechanisms do now no longer punish or offer a caution to an attacker and a number of the assumptions made in a few mechanisms aren't 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, maximum of the protection mechanisms in opposition to IP spoofing are applied on the router in Wide Area Network (WAN) and host (affected host in the destination network). This situation allows an attacker to utilize shared resources of the network, even though he/she didn't 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 offer a caution to an attacker is likewise every other trouble that offers 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 may stop his/her attacking activities. Among the main demanding situations to save you IP spoofing assaults is to find the ideal function of attackers. This is because, attackers use faux IP identity 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 should make use of greater shared community resources. There is a mechanism advanced to discover an IP spoofing attacker the use of MAC deal with on LAN stage via way of means of the use of Layer three switches with POX controller. This mechanism save you usage of shared community sources of a victim . 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 by designing and developing an algorithm for locating an IP Spoofing attacker and ship caution packets to an attacker to be able to alert an attacker for his/her attacking activities. The caution packets are taken into consideration as a punishment to an attacker because it will affect An attacker via way of means of utilizing his/her personal shared assets and save you him/her from making greater 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 AGAINSTIP SPOOFING ATTACKS

There are difference types of defense mechanisms used for IP spoofing packets identification, prevention and locating an attacker. These mechanisms are essentially categorized into 3 kinds namely, Host primarily based totally, Router primarily based totally and Switch primarily based totally protection methods/mechanisms. To the first-rate of our knowledge, there aren't anyt any present mechanisms, which offer a caution to an attacker as soon as IP spoofing assault 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 lively mechanisms want the end-host to carry out a pro-lively motion or lively probing.

Active host-primarily based totally mechanisms consist of cryptographic answers, lively probing answers and IP puzzles. Active host-primarily based totally mechanisms consist of cryptographic answers, lively probing answers and IP puzzles. 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 guarantees that simplest relied on hosts get right of entry to encrypted message through that mystery 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 themessage.

Passive mechanisms on the opposite hand, depend simplest at the facts which a bunch accumulate domestically with out probing the meant supply of a packet. 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, Hop-Count Filtering (HCF) gadget counts and information range of hops from one host to any other in the course of a everyday 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 may be a excessive opportunity for The hop-depend of the packet failing to fit with the anticipated hop-depend of legitimate packets from the spoofed supply IP address. However, this mechanism has a weak spot for the reason that valid hop-counts can extrade because of routing changes. In this situation, all packets that don't in shape the anticipated ho remember are mechanically filtered, even supposing they're valid packets.

2.2 Router-Based Defense Mechanism

An example of router-based IP spoofing defense mechanisms are Ingress and Egress filtering, which are the strategies that use routers to research addresses of packets flowing inside and outside of community area after which clear out out 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. In this case, an attacker can be identified his/her location by using MAC address on LAN. This mechanism detect IP spoofing attack bycomparing source IP address on packet with that of the ARP table. If source IP address does not match, the packet is spoofed. If supply IP addresses are the same, authentication may be established via way of means of evaluating supply MAC cope with on packet with that of the ARP table. All these validation are done on POX controller by using OpenFlow protocol.

3. METHODOLOGY

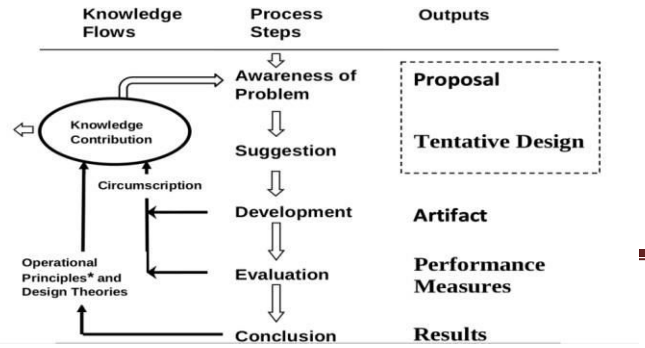
This paper use Design Science Research Methodology (DSRM). The DSRM is suitable in developing artifacts such as algorithms or human/computer interfaces.
There are five steps in DSRM, trouble awareness, suggestion, development, assessment and conclusion, to be followed during designing, implementing and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

Fig 1:Design Science Research Methodology

First step is the awareness of problem during a inspiration phase; that is used to analyze in extra element the causes, sources, and degree of the problem. This study realized reasons for IP spoofing attack continue to a problem on today’s communication networks, despite severaldefense mechanisms.

The second step is the concept step which is likewise used in the course of the thought 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 performanceon 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 provisionto an IP spoofing attacker as shown in Figure 2.

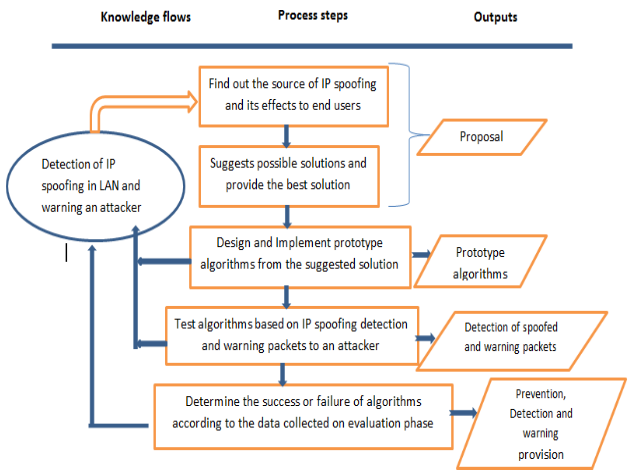

Knowledge flows
Process steps
Outputs
Find out the source of IP spoofing and its effects to end users
Suggests possible solutions and provide the best solution
Proposal
Detection of IP spoofing in LAN and warning an attacker
Design and Implement prototype algorithms from the suggested solution
Prototype algorithms
Test algorithms based on IP spoofing detection and warning packets to an attacker
Detection of spoofed and warning packets
Determine the success or failure of algorithms according to the data collected on evaluation phase
Prevention, Detection and warning provision

Fig. 2. Steps used to develop prototype of an algorithm toprovide 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. 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. Theimplemented 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.

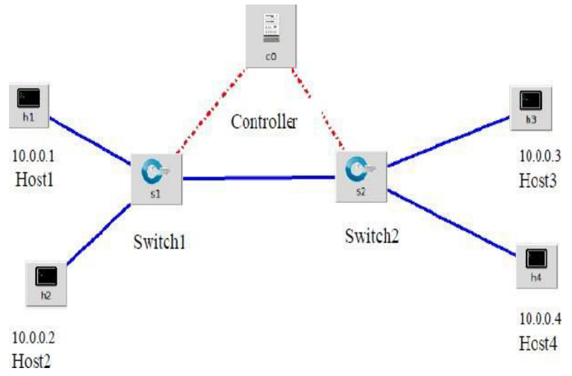
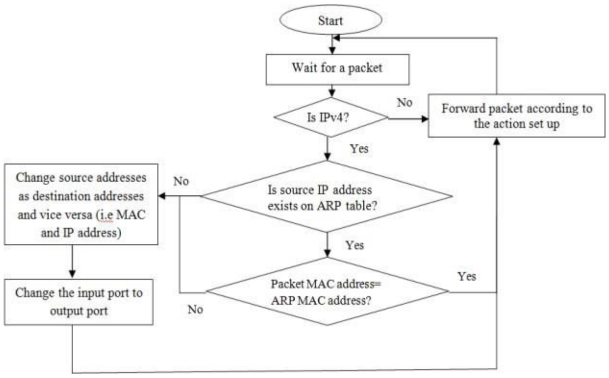


Fig. 4. Virtual network topology used to send warning toan attacker

POX controller is a Python based open source OpenFlow/ SDN Controller. 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


Start
Wait for a packet
Is IPv4?
No
Forward packet according to the action set up
Yes
Change source addresses as destination addresses and vice versa (i.e MAC and IP address)
No
Is source IP address exists on ARP table?
Yes
Change the input port to output port
Packet MAC address= ARP MAC address?
No
Yes

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.

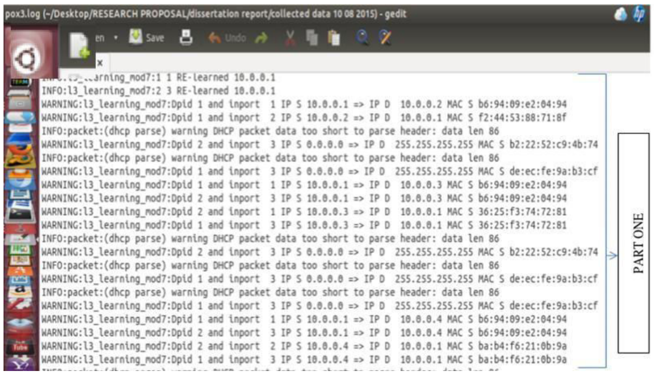
Virtual machine is a software computer that, like a physical computer, runs an operating system and applications. Every virtual machine has virtual devices that provide the same functionality as physical hardware and have additional benefits in terms of portability, manageability, and security. Virtual 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 are packet manipulation tools that facilitate forging, dissecting, emitting or sniffing network packets. 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 commandline. 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. 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 wasused 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 Host 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 resultsare shown in Figure 5 and Figure 6. Part One on figure 5 shows a communication with a valid IP address and figure 6 demonstrate communicationwith 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.

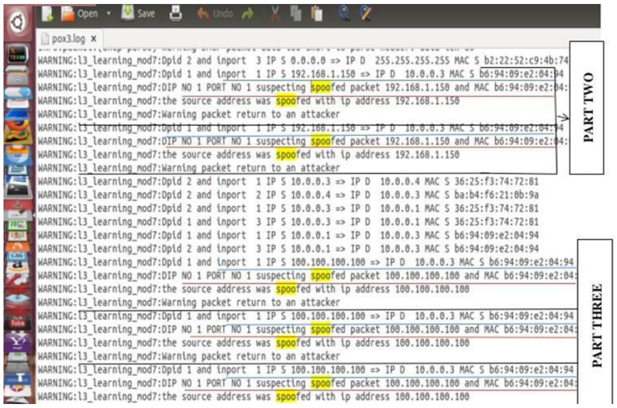


pox3.log (~/Desktop/RESEARCH PROPOSAL/dissertation report/collected data 10 08 2015) - gedit

```
INFO:l3_learning_mod7:1 1 RE-learned 10.0.0.1
INFO:l3_learning_mod7:2 3 RE-learned 10.0.0.1
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 10.0.0.1 => IP D  10.0.0.2 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 1 and inport  2 IP S 10.0.0.2 => IP D  10.0.0.1 MAC S f2:44:53:88:71:8f
INFO:packet:(dhcp parse) warning DHCP packet data too short to parse header: data len 86
WARNING:l3_learning_mod7:Dpid 2 and inport  3 IP S 0.0.0.0 => IP D  255.255.255.255 MAC S b2:22:52:c9:4b:74
INFO:packet:(dhcp parse) warning DHCP packet data too short to parse header: data len 86
WARNING:l3_learning_mod7:Dpid 1 and inport  3 IP S 0.0.0.0 => IP D  255.255.255.255 MAC S de:ec:fe:9a:b3:cf
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 10.0.0.1 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 2 and inport  3 IP S 10.0.0.1 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 2 and inport  1 IP S 10.0.0.3 => IP D  10.0.0.1 MAC S 36:25:f3:74:72:81
WARNING:l3_learning_mod7:Dpid 1 and inport  3 IP S 10.0.0.3 => IP D  10.0.0.1 MAC S 36:25:f3:74:72:81
INFO:packet:(dhcp parse) warning DHCP packet data too short to parse header: data len 86
WARNING:l3_learning_mod7:Dpid 2 and inport  3 IP S 0.0.0.0 => IP D  255.255.255.255 MAC S b2:22:52:c9:4b:74
INFO:packet:(dhcp parse) warning DHCP packet data too short to parse header: data len 86
WARNING:l3_learning_mod7:Dpid 1 and inport  3 IP S 0.0.0.0 => IP D  255.255.255.255 MAC S de:ec:fe:9a:b3:cf
INFO:packet:(dhcp parse) warning DHCP packet data too short to parse header: data len 86
WARNING:l3_learning_mod7:Dpid 1 and inport  3 IP S 0.0.0.0 => IP D  255.255.255.255 MAC S de:ec:fe:9a:b3:cf
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 10.0.0.1 => IP D  10.0.0.4 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 2 and inport  3 IP S 10.0.0.1 => IP D  10.0.0.4 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 2 and inport  2 IP S 10.0.0.4 => IP D  10.0.0.1 MAC S ba:b4:f6:21:0b:9a
WARNING:l3_learning_mod7:Dpid 1 and inport  3 IP S 10.0.0.4 => IP D  10.0.0.1 MAC S ba:b4:f6:21:0b:9a
```

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.



```
WARNING:l3_learning_mod7:Dpid 2 and inport  3 IP S 0.0.0.0 => IP D  255.255.255.255 MAC S b2:22:52:c9:4b:74
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 192.168.1.150 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:DIP NO 1 PORT NO 1 suspecting spoofed packet 192.168.1.150 and MAC b6:94:09:e2:04:
WARNING:l3_learning_mod7:the source address was spoofed with ip address 192.168.1.150
WARNING:l3_learning_mod7:Warning packet return to an attacker
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 192.168.1.150 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:DIP NO 1 PORT NO 1 suspecting spoofed packet 192.168.1.150 and MAC b6:94:09:e2:04:
WARNING:l3_learning_mod7:the source address was spoofed with ip address 192.168.1.150
WARNING:l3_learning_mod7:Warning packet return to an attacker
WARNING:l3_learning_mod7:Dpid 2 and inport  1 IP S 10.0.0.3 => IP D  10.0.0.4 MAC S 36:25:f3:74:72:81
WARNING:l3_learning_mod7:Dpid 2 and inport  2 IP S 10.0.0.4 => IP D  10.0.0.3 MAC S ba:b4:f6:21:0b:9a
WARNING:l3_learning_mod7:Dpid 2 and inport  1 IP S 10.0.0.3 => IP D  10.0.0.1 MAC S 36:25:f3:74:72:81
WARNING:l3_learning_mod7:Dpid 1 and inport  3 IP S 10.0.0.3 => IP D  10.0.0.1 MAC S 36:25:f3:74:72:81
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 10.0.0.1 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 2 and inport  3 IP S 10.0.0.1 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 100.100.100.100 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:DIP NO 1 PORT NO 1 suspecting spoofed packet 100.100.100.100 and MAC b6:94:09:e2:04:
WARNING:l3_learning_mod7:the source address was spoofed with ip address 100.100.100.100
WARNING:l3_learning_mod7:Warning packet return to an attacker
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 100.100.100.100 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:DIP NO 1 PORT NO 1 suspecting spoofed packet 100.100.100.100 and MAC b6:94:09:e2:04:
WARNING:l3_learning_mod7:the source address was spoofed with ip address 100.100.100.100
WARNING:l3_learning_mod7:Warning packet return to an attacker
WARNING:l3_learning_mod7:Dpid 1 and inport  1 IP S 100.100.100.100 => IP D  10.0.0.3 MAC S b6:94:09:e2:04:94
WARNING:l3_learning_mod7:DIP NO 1 PORT NO 1 suspecting spoofed packet 100.100.100.100 and MAC b6:94:09:e2:04:
WARNING:l3_learning_mod7:the source address was spoofed with ip address 100.100.100.100
```

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

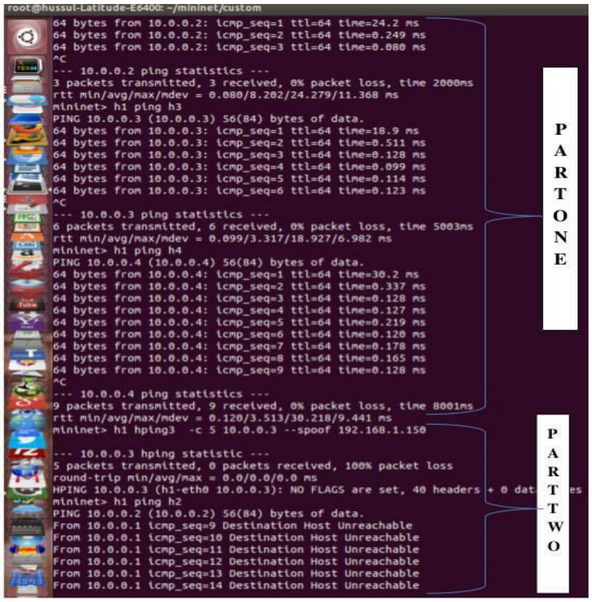
Results on POX controller show that the developed algorithm creates a warning packet for every detected spoofing packet sent by an attacker. Warning packets keep a switch and an attacker busy, which is the purpose of this study. This means that an attacker utilizes his/her own resources and works as 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 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.



```
root@hussul-Latitude-E6400: ~/mininet/custom
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=24.2 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.249 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.080 ms
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.080/8.202/24.279/11.368 ms
mininet> h1 ping h3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=18.9 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.511 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.128 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=0.099 ms
64 bytes from 10.0.0.3: icmp_seq=5 ttl=64 time=0.114 ms
64 bytes from 10.0.0.3: icmp_seq=6 ttl=64 time=0.123 ms
^C
--- 10.0.0.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5003ms
rtt min/avg/max/mdev = 0.099/3.317/18.927/6.982 ms
mininet> h1 ping h4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=30.2 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.337 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=0.128 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=0.127 ms
64 bytes from 10.0.0.4: icmp_seq=5 ttl=64 time=0.219 ms
64 bytes from 10.0.0.4: icmp_seq=6 ttl=64 time=0.120 ms
64 bytes from 10.0.0.4: icmp_seq=7 ttl=64 time=0.178 ms
64 bytes from 10.0.0.4: icmp_seq=8 ttl=64 time=0.165 ms
64 bytes from 10.0.0.4: icmp_seq=9 ttl=64 time=0.128 ms
^C
--- 10.0.0.4 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8001ms
rtt min/avg/max/mdev = 0.120/3.513/30.218/9.441 ms
mininet> h1 hping3  -c 5 10.0.0.3 --spoof 192.168.1.150

--- 10.0.0.3 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 10.0.0.3 (h1-eth0 10.0.0.3): NO FLAGS are set, 40 headers + 0 dat   es
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=9 Destination Host Unreachable
From 10.0.0.1 icmp_seq=10 Destination Host Unreachable
From 10.0.0.1 icmp_seq=11 Destination Host Unreachable
From 10.0.0.1 icmp_seq=12 Destination Host Unreachable
From 10.0.0.1 icmp_seq=13 Destination Host Unreachable
From 10.0.0.1 icmp_seq=14 Destination Host Unreachable
```

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

5.CONCLUSION AND RECOMMENDATION

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, M. 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.