ISSN: 2584-0495 Vol. 1, Issue 2, pp. 99- 112

International Journal of Microsystems and IoT

ISSN: (Print) (Online) Journal homepage: https://www.ijmit.org

Development of a Novel Methods for Detecting & Preventing the Spoofed attack Packets

N. D. Patel, B.M. Mehtre, R. Wankar, and R. Priyadarshi

Cite as: N. D. Patel, B.M. Mehtre, R. Wankar, & R. Priyadarshi. (2023). Development of a Novel Methods for Detecting & Preventing the Spoofed attack Packets. International Journal of Microsystems and IoT, 1(2), 99-112. https://doi.org/10.5281/zenodo.8289269

Published online: 24 Jul 2023.

DOI: https://doi.org/10.5281/zenodo.8289269

International Journal of Microsystems and IoT
Vol. 1, Issue 2, pp. 99-112; DOI: https://doi.org/10.5281/zenodo.8289269

Development of a Novel Methods for Detecting & Preventing the Spoofed attack Packets

N. D. Patel[1], B.M. Mehtre[2], R. Wankar[3], and R. Priyadarshi[4]
[1] School of Computing Science and Engineering(SCSE), VIT Bhopal University, Kothrikalan, Sehore MP.
[2]Centre of Excellence in Cyber Security, Institute for Development & Research in Banking Technology (IDRBT).
[3]School of Computer & Information Sciences (SCIS), University of Hyderabad (UoH), India.
[4]Faculty of Engineering Technology, ITER, Siksha 'O' Anusandhan deemed to be University, Bhubaneswar, India.

ABSTRACT

IP-Spoofing is an attack that forges the source "IP- Address" to mislead the receiver about the sender, making it difficult to trace back. Existing IP-Spoofing prevention methods like Ingress/Egress filtering, and Reverse Path Forwarding have the following limitations: they filter only the IP Packets of the local network, limited logging capabilities, and work only for specific types of TCP/IP protocol attacks. This paper introduces BGP- ASE, an effective method called Border Gateway Protocol Anti-Spoofing Extension, designed to combat IP spoofing by successfully intercepting and preventing the transmission of fraudulent packets. The proposed mechanism is tested using emulation network environments consisting of Mininet, OpenFlow Switch, and POX Controller. The usage of random filter placement improves the performance for dropping attack packets ratio. BGP-ASE is more potent than Ingress/Egress and RPF filtering in dropping attack packets. In the BGP-ASE mechanism, only 30% of transit Autonomous Systems can filter greater than 90% of the malicious packets. BGP-ASE also has the following desirable properties - Initial-Benefits for early users, Incremental-Benefits for subsequent users, and effectiveness in partial deployment.

KEYWORDS

Border-Gateway Protocol (BGP); Ingress Filtering; IP-Spoofing; Reverse-Path Forwarding; Security; Spoofed Attack.

1. INTRODUCTION

Internet Protocol (IP) is a TCP/IP suite protocol responsible for exchanging information on the Internet, using a data unit called IP Packet for transmitting information from the source host to the target host. Each IP Packet has a header that contains various fields, including source address, target address, fragmentation, and sequence number fields. Each domain has some designated functions. While the source and target fields provide an addressing mechanism, the fragmentation field permits the fragmentation of IP Packets and their reassembly. This scheme provides excellent results; however, malicious users have developed several techniques that enable spoofing of IP Packets source addresses [1].

"IP-Address" Spoofing is a network layer security threat that can be carried out through various techniques. This type of spoofing poses a significant threat because it forges IP Packets that can be used for different malicious purposes. Such as unauthorized access to the victim's system. The weaknesses of existing studies, a new search can determine whether the packet of the corresponding "IP-Address" has passed the expected path by Marking the packets passing through the Router [2].The main challenge in Spoofed packet detection is source IP-Address verification, traffic volume and speed, distributed attacks, IP fragmentation, and Distinguishing legitimate use cases of IP spoofing from malicious activities.

IP-Spoofing is an attack that exploits the security vulnerability of IP itself and accesses it by tricking one's own "IP-Address" [3]. If an unauthorized person changes their "IP-Address" to the "IP-Address" of a host in a trust relationship, as shown in Figure 1, a service that authenticates with an "IP-Address" such as "rlogin and rsh" (remote login services provided by Linux) is quite large. In other words, it refers to an intrusive form in which an attacker attempts access by altering the source "IP-Address" of a packet, like a Bit sent by a trusted person.

IP-Spoofing takes advantage of the fact that users connected to the Internet can freely manipulate IP Packets and transmit packets. Hand signal, when a packet determines a packet, the destination host has no way to know where the packet came from because it only has the "IP-Address" written on the packet and determines the sending host. Epps et al. [4] defined the structure of IP Packets that come and go when inter-networking between two computers is performed. In general, to communicate between hosts using the TCP protocol, three steps are required for the three-way handshake, TCP/IP creates a connection through three steps, such as a request for response/permit response number as shown in Figure 1. To communicate with other hosts, the source sends a TCP SYN packet [5]. The evil of this packet is synchronizing sequence numbers.

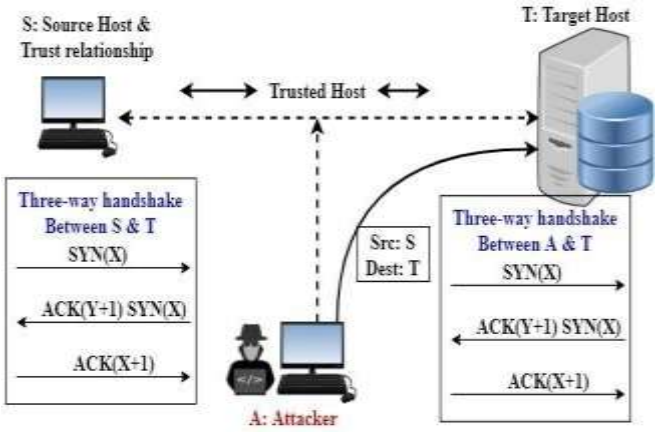

Fig. 1 Packet Transmission using IP-Spoofing Technique.

The destination host notifies that it has received an SYN packet and responds with an SYN/ACK packet. Finally, the source host sends an ACK packet, indicating that both hosts are ready to commence data exchange once this process is complete. However, during this process, the attacker can mistakenly identify the target host as being connected to another regular host by employing a spoofed source "IP-Address" and a guessed TCP sequence number. Given that such attacks are prevalent on the open Internet, it becomes crucial to promptly implement an effective solution to mitigate potential damages caused by IP-Spoofing attacks [6].

Ingress/Egress filtering [7] and RPF (Reverse-path forwarding) [8] is a procedure used in the network to locate the spoofer's actual location without depending on the packet header's source "IP-Address" field. It is the primary technique to find the real attack sources. When it fails to forward an IP-Spoofing packet for various excuses, e.g., Time-to-Live (TTL) exceeds, the created message is eventually sent to the spoofed source. It doesn't operate in all attacks and cannot identify all the spoofers in the network environments. An Anti-Spoofing mechanism called BGP-ASE: Border Gateway Protocol-Anti Spoofing Extension' is developed to overcome this flaw. It involves an attacker identification process that includes packet Marking & Filtering.

1.1 Contribution Highlights of The Paper

The BGP-ASE extension contributes to the improvement of Border Gateway Protocol (BGP) security by effectively detecting and mitigating IP spoofing attacks, enhancing the overall resilience and reliability of the BGP routing protocol.

1.2 Outline of The Paper

The rest of the paper is ordered as follows: In section 2, we describe the related work on the IP Packet Header Structure, TCP Protocol 3 Way handshaking Process, IP-Spoofing background, Router-based basic Filtering mechanisms, and Limitations on Existing IP-Spoofing Detection Techniques. In Section 3, we proposed a Router-based BGP-ASE mechanism. In Section 4, we present the IP-Spoofing detection method using BGP-ASE. In Section 5, we created and tested an IP- Spoofing detection experiment in an emulation environment. Section 6 presents the Results and Discussion. Section 7 gives the conclusions and future work.

1.3 Practical Implications of the Study

This study introduces a novel approach known as BGP- ASE (Border Gateway Protocol Anti-Spoofing Extension) to address the limitations of existing methodologies, including Ingress/Egress filtering, and Reverse Path Forwarding. The primary objective of this method is to improve the prevention of IP-spoofing. This indicates that organizations and network administrators now possess a more effective approach for addressing IP spoofing attacks, hence enhancing the overall security of their networks.

Enhanced traceability is achieved by BGP-ASE by its effective interception and prevention of fraudulent packets, leading to the maintenance of a higher level of traceability compared to conventional methods. Accurate determination of the source of an attack has significant significance within the realm of investigations and forensic analysis after security breaches [9].

The BGP-ASE methodology provides a more comprehensive level of security in comparison to previous methodologies, which often focus just on packets inside the local network. The Border Gateway Protocol - Autonomous System External (BGP-ASE) operates effectively throughout several network domains, hence offering comprehensive protection against IP spoofing attacks. The significance of this broadened reach becomes particularly evident in scenarios when attacks may originate from many sources outside the boundaries of the local network [10].

The study highlights the limitations of existing methodologies with regards to their logging functionalities. The use of Border Gateway Protocol Autonomous System External (BGP-ASE) assists organizations in acquiring benefits via improved logging and monitoring techniques, hence enabling more efficient examination of network traffic patterns and detection of potential security issues [11].

The degree of interoperability with various TCP/IP protocols differs with prior methodologies. Nevertheless, BGP-ASE offers a more versatile approach that effectively mitigates a wider range of attack vectors. The ability to adapt ensures that organizations are well-prepared to efficiently counter evolving attack strategies.

The use of random filter placement is acknowledged as a tactic to enhance the efficacy of mitigating the proportion of lost attack packets [12]. The findings of this study hold

promise in offering network administrators useful insights for optimizing the configuration of BGP-ASE, hence leading to enhanced results.

The findings of the research about the effectiveness of Border Gateway Protocol - Autonomous System Extension (BGP-ASE) in different deployment scenarios provide valuable insights. Organizations have the capacity to strategically determine the implementation of BGP-ASE inside certain transit Autonomous Systems, considering their network architecture and unique requirements. There is a potential for significant improvements in the filtering of attack packets.

The potential for deploying BGP-ASE in a phased manner is supported by the concept of Initial-Benefits and Incremental- Benefits, which refer to the benefits that early adopters and subsequent users, respectively, may enjoy [13]. This technique facilitates a step-by-step implementation of BGP-ASE. This has significant importance for organizations that may have worries over the financial ramifications and efforts associated [14] with executing a thorough deployment.

According to the study findings, it is indicated that organizations have the potential to attain significant enhancements in the effectiveness of attack packet filtering with the partial deployment of BGP-ASE. This discovery has the potential to motivate businesses to choose a gradual deployment approach [15]. The assertion acknowledges the challenges that come when rapidly and totally adopting a certain strategy or concept and posits that substantial improvements may still be achieved incrementally.

In summary, the use of BGP-ASE as a preventive strategy against IP spoofing has noteworthy practical implications within the domain of network security. The solution being suggested demonstrates a high level of sophistication in its approach, successfully addressing the limitations seen in existing methodology [16]. Furthermore, it enhances security measures and provides flexible deployment strategies that can be tailored to various corporate situations.

1.4 Limitation of the Study

It is possible that the proposed BGP-ASE method will not perform as intended if emulation networks are used.

The effectiveness of the method against new forms of attack may have been compromised since the research did not test for all possible IP spoofing attacks. Border Gateway Protocol Autonomous System Extension (BGP-ASE) implementation in dynamic network circumstances may not ensure consistent behavior across Autonomous Systems (AS), which might reduce the mechanism's efficiency. The study might go further into the complexities associated with deploying BGP-ASE across a spectrum of network architectures, considering the many potential roadblocks and conflicts that could develop. Further research on the potential performance and resource implications of BGP-ASE is required. Current estimates may be too low. While the study's findings show that BGP-ASE is superior to existing methods, a more in-depth comparative study would help accurately weigh its benefits and drawbacks.

Research beyond the scope of this research is needed to learn more about BGP-ASE's long-term viability and adapt- ability in complex network settings. The possible obstacles that businesses may face during the deployment of BGP-ASE are underexplored. These difficulties may include opposition from stakeholders, knowledge gaps among employees, and the need to comply with regulatory standards. It is unclear how well the study's findings would apply to actual network deployments in the absence of practical implementation insights from real- world enterprises. To properly interpret the study's findings and provide recommendations for future practical implementations of the proposed BGP-ASE mechanism, it is crucial to acknowledge and account for these constraints.

2. RELATED WORK

Samadi et al. proposed "A wrapper-based feature selection for improving performance of intrusion detection systems", It addresses the challenge of selecting the most relevant features from a large set of available features to improve the detection accuracy and efficiency of the IDS [17]. Seyfollahi et al. proposed MFO-RPL optimizes the energy consumption of IoT devices by selecting the most energy-efficient routes for data transmission. This helps prolong the network lifetime and maximize the operational time of battery powered IoT devices [18].

2.1 IP-Spoofing Attacks

In the Internet Protocol, IP Packets are routed from the source host to the destination host through one or more intermediate networking devices such as switches and routers. Routing decisions are made by the intermediate routing devices, which are based on the "IP-Address" of the packets (either source "IP-Address" or the target IP address) contained in the IP Packets' headers [19]. Anyone who can access the network layer could spoof the address of IP Packets. There are two main types of IP-Spoofing.

2.1.1 Non-Blind IP-Spoofing Attack

It occurs in a state where the packets exchanged between hosts can be seen. An attack can be easily performed since the sequence number can be known [20].

2.1.2 Blind IP-Spoofing Attack

The attack is brutal because the attack's success or failure depends on how accurately the sequence number is estimated. After all, the packets exchanged between hosts

cannot be seen. However, most operating systems generate sequence numbers under two simple rules [21].

IP-Spoofing is used to gain unauthorized access to a host by changing the IP Packet's source address to conceal the dispatcher's identity. In the Internet routing operation, only the destination" IP-Address" to which the packet is transmitted is used, and the source address is ignored. Therefore, the public grid can transmit (Send) packets that can damage the system and disguise the source address for them so that the user cannot know the source of these malicious packets [11]. Asgharzadeh et al. proposed the IDS focuses on detecting anomalies and unusual patterns of behavior in IoT devices and networks. By leveraging the power of CNN, it can effectively learn and identify abnormal activities, such as malicious attacks or unauthorized access attempts. [12].

While spoofing doesn't always compromise your system, it does tell you that intrusions into your system can occur. This address could be addressed outside the network used to hide the intruder's identity or a trusted internal address with privileged access. Also, IP-Spoofing is one of the characteristics of an attack that generates a large amount of traffic. Many of the packets are introduced by altering the source IP address, and Denial of Service (DoS) attacks such as SMURF, MITM, DDoS, and Tribe Flood Network (TFN) are representative of spoofing [22].

2.2 Router-based Basic Filtering mechanisms

Router-based mechanisms are mainly filtering methods that range from basic filtering to distributed filtering. The Router- based mechanisms can be effectively used to defend IP- Spoofing, but they are challenging to deploy due to deployment, coordination, and overhead issues [23]. The primary filtering mechanisms are widely employed methods for filtering IP Packets from attacks at the IP level. A primary filtering mechanism can identify spoofed packets if they are deployed fully and efficiently on the network.

2.2.1 Ingress/Egress Filtering

Ingress and egress filtering mechanisms are considered acceptable and commonly used mechanisms to run on border router protocol. The ingress filtering mechanism is used for the incoming filtering of IP Packets, while the egress filtering mechanism is used to filter outgoing IP Packets [7]. The ingress filtering checks the incoming packets, and if an IP Packet does not belong to the intended (core) network, it is treated as spoofed [24]. Ingress filters can filter the IP Packets if they are used at all the routers on the web network. The coordination of the intermediate routers is necessary for the filtering purpose.

2.2.2 Reverse Path Filtering

The second kind of primary filtering mechanism like Ingress filtering is reverse path for- warding (RPF) [8]. In this type of filtering mechanism, routers filter IP Packets based on the source address. Ingress/Egress filters consider incoming direction by ingress filter and outgoing approach by egress filter [25]. On the other hand, reverse path filters deal with IP Packets passing through any router on the network from any direction and use "Routing Table" information.

2.3 Practical Protocol Characteristics

Therefore, as the protocol has the following three characteristics, it can have the appearance of a practical protocol that can be applied in real life [13].

2.3.1 Practical Prototype (Initial benefit)

A practical (experimental) protocol should give the initial user an advantage in using the protocol. Two users who use the protocol before other users have the benefit of using the protocol to play the role of motivating other users to use the protocol. Therefore, granting the benefits of using the protocol to the initial user serves as an excuse to persuade other users to use it [26].

2.3.2 Benefits that gradually increase as the number of users increases (Incremental Benefit)

Based on the benefits given to early users of the protocol, as more and more users use the protocol, the more the number of users who purchase the protocol, the more the protocol's benefits should be.

2.3.3 Efficiency in Partial Deployment:

Although most users do not use the protocol, if more than a certain level of users use the protocol, there should be sound effects. Since most users need a lot of time to use the protocol, it should exhibit sufficient effective performance even if 30-50% of routers are used [27].

2.4 Limitations on Existing IP-Spoofing Detection Techniques

However, the existing spoofing detection techniques are widely used in real life because they do not satisfy these three characteristics. It is impossible, and Ingress/Egress filtering prevents external attackers from tricking themselves into being the host. In other words, it filters out incoming and outgoing calls from the outside [14]. Unicast RPF (Reverse Path For- warding) checks whether a Reverse Path Route to the source "IP-Address" is written on the packet on the packet's input interface when a packet comes into the Router [28]. If the source "IP-Address" written in the packet is spoofed, there is no reverse path to the source "IP-Address" on the input interface. In other words, the Router passes packets with reverse paths, and drops spoofed packets that do not. This technique also does not directly benefit you using it. In addition, it has a disadvantage that it is difficult to

distribute a lot [29].

3. PROPOSED ROUTER BASED BGP-ASE MECHANISM

As an abbreviation of Border Gateway Protocol Anti Spoofing Extension (BGP-ASE), it is a distributed filtering router-based mechanism. In the distributed Defence mechanism, the cooperation of organizations responsible for man- aging routers is necessary to distinguish between valid and spoofed IP Packets. BGP-ASE needs to get the correct incoming direction of IP Packets for a particular source [15].

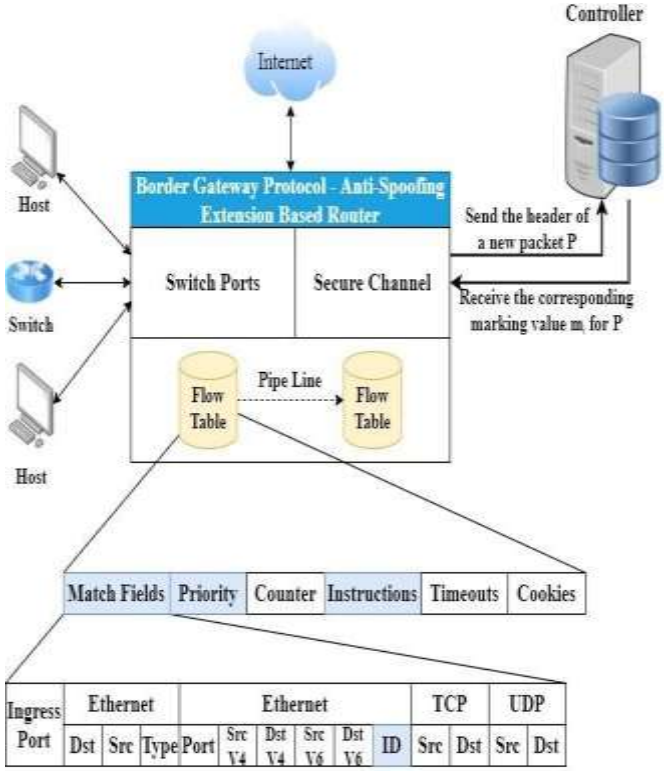

Fig. 2 A Scenario of BGP-ASE Router (Storing the Marking Value).

The BGP-ASE Router needs to update its "Marking Values" from the controller's "Filtering Table". Figure 2 shows how the BGP-ASE Router works on the Open-Flow. Open-Flow has three main modules, "Switch-Ports", "Secure-Channels", and "Flow-Tables". The "Switch-Ports" connection to additional switches/hosts for the network-packet passing. The confidential channels are for interface with the "POX-Controller," and the "Flow-Tables" hold each run flow instruction and related specification for all "Flow-Entry". We added one value that stores the Marking Values in ID. Once a BGP-ASE router gets a network packet from "Switch-Ports", it differentiates the network-packet details upon every "Flow-Entry" included on the "Flow-Table" utilizing the "Match-Fields". If the network- packet peers with any entries, the BGP-ASE Router forwards a "Network-Packet-In-Msg" to the Controller through a "Secure Channel". The BGP-ASE module on the controller gets the Network-Packet-In-Msg and finds particular "Marking-Values" on the "Filtering-Table" and updates the "Flow-Table" on the BGP-ASE Router (see the Listing 1).

Listing 1 (figure 2a): A Pseudo-Code of BGP-ASE module for Table- Entries updates, during a packet appears in the controller [16], and the BGP-ASE module replies with the identical New Marking Value.

```
Def  handle Packet In Msg (self, event):
1. dp id =event.connection.dp id
2. packet = event.parsed
3. dst addr = packet.next.dst ip
4. src addr = packet.next.src ip
5.prev-mark = packet.next.id
6. IF dst addr in self.arpTable[dp id]
7. IF prevmark in self.filterTab[dp id][srcaddr]
8.prt=self.arpTable[dp id][dst addr).port
9. MAC = self.arp Table[dp id][dst addr].MAC
10. nextmark =self.filter
 Table[dp id][p mark].n mark
11. action = [ ] //"action.actions = a.a"
12. a.a(of.ofp action dl.addr.set.dst(MAC))
13.a.a(of.ofpaction new id.set id(next-mark)
14. a.a(of.ofp action output(por =port))
15. match= ofp match.from packet(packet,in port)
16. msg=of.ofp flow mod(command=of.OFPFC MODIFY,
 idleTimeout = FLOW IDLE TIMEOUT,
 hard Timeout = of.OFP FLOW PERMANENT,
 bufferid=event.ofp.bufferid,
 actions = actions,
 match = of.ofp match.from packet
 (packet,in port))
17. event.connection.send(msg.pack())
18. ENDIF
19. ENDIF
END of code
```

Fig. 2(a) A Pseudo-Code of BGP-ASE module

The proposed BGP-ASE framework fulfills all three protocol characteristics, namely Initial Benefits for early users, Incremental Benefits for subsequent users, and effectiveness under partial deployment. On the other hand, the existing mechanism fails to meet all these protocol characteristics. If an attacker were to send a considerable volume of spoofed packets to a single destination simultaneously, it could potentially overload the destination network. To mitigate this risk, BGP-ASE proactively blocks such packets before they reach the destination network, thereby preventing any potential overload [30].

In other words, when a spoofed packet originates from the attacker's host and encounters a router using the BGP-ASE mechanism on the path to the destination host, the Router checks whether the packet has the correct Marking Value. The packet is passed to the next Router only if it has the correct Marking Value. Otherwise, the packet is dropped from the Router. Here, the Marking Value contains the path that the packet has come through, and the value is marked on

the packet's header (16-bit identifier [4]). When distributing the Marking Values used when transmitting packets between the BGP-ASE filters in advance, the Marking Values are distributed using BGP, an inter-AS routing protocol used as a standard of today's Internet [31]. This BGP-ASE mechanism consists of 4 steps, as shown in Figure 3.

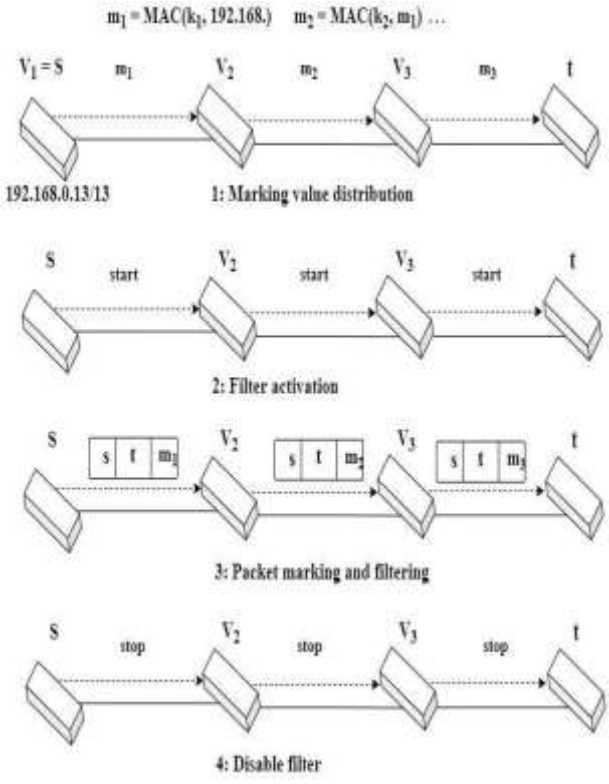

Fig. 3 BGP-ASE mechanism Steps.

3.1 Marking Value Transfer

This step is to transfer the Marking Value to BGP-ASE filters while calculating it. BGP message is When passing through the filter, and each filter creates its Marking Value (mi) using the Marking (mi 1) written on the packet received from the previous Router, and it is secret key (ki).

That is, the Marking Value at the first Router has a value of mi.

= MAC (ki, mi 1). Each BGP-ASE filter interferes with the received Marking Value and its Marking Value in its filter table [17]. Passing the Marking Value to the BGP-ASE filters occurs

only once unless the BGP path changes. Algorithm 1 shows the calculated distribution Marking Value for a particular Node to the Next-Nodes [32].

Algorithm 1: Distribution Algorithm of Marking Value

1: m0 = the source host AS

2: for every BGP-ASE router filter Vi from i=1 to all "Filter-

Nodes" do

3: if mi = MAC(ki, mi 1) then

4: Forwards mi to the following BGP-ASE Filter-

Nodes by adopting the BGP optional transitive attributes.

3.2 Filter Activation

The BGP-ASE mechanism does not always work but only works when the destination host thinks a spoofed packet is received and activates the BGP-ASE filter. The message that triggers the BGP-ASE filter is delivered to all BGP-ASE filters using BGP. When each of the BGP-ASE filters receives the filter activation message, the padding to the address can pass through the BGP-ASE filters only when they have a specified Marking Value [33].

3.3 Packet Marking and Filtering

In the filtering phase, each BGP-ASE Marking Value is marked on the packet's header for packets going out of the network. Packets entering the BGP-ASE filter are dropped if they do not have the correct Marking Value. Each BGP-ASE Node has extra attributes for "Packet Marking" & "Filtering" [18]. This Node is considered as a BGP-ASE filter Node (has a "Filtering Table") and shown in Algorithm 2. Where Source is s, and Destination is t, and F is a Filtering − Table.

Algorithm 2: Packet Marking and Filtering Algorithm

1: procedure PATH(s, t)

2: P(s,t) = v1, v2, vn

3: where, v1 = s and vn = t

4: for each BGP-ASE filter Vi from i=1 to all "Filter-

Nodes" do

5: if mi 1 F(s) then

6: Forward(s,t) to R(t) with a Nezt Mark mi;

7: else

8: drops(s,t) ⊳ Packet Marking Value(s,t)

3.4 Filter Deactivation

When the destination host controls no more risk of spoofed packets, the BGP-ASE filter is deactivated. This message also used BGP for all BGP-ASE filters and delivered [34].

4. IP-SPOOFING DETECTION METHOD

USING BGP-ASE

As explained in Packet Marking and Filtering, if the Marking Value marked on the packet has the same value as the distributed Marking Value using BGP [15]. Then the packet is transmitted to the next Router, but if it has a different value, the packet is spoofed, and it is dropped. As shown in Figure 4, each BGP-ASE filter has a "Filtering Table" and a "Routing Table". Entries in the "Filtering Table" and "Routing Table" are updated when a BGP message is delivered to all routers. In this state, when the destination router t detects a spoofed packet and enables the BGP-ASE filter, after that, when the source s wants to send a packet, it must send by putting the Marking Value in the header part of the packet [22]. At this time, the Marking Value of the packet is generated and delivered from an authoritative source. It is passed to each Router and added to the "Filtering Table".

It will have the same value as the saved Marking Value. In Figure 4, Router v4 sets the Marking Value to either m2 or m3. If so, it is recognized as a packet that has passed a standard. path. After that, it calculates its private key on the Marking Value after making m4 and checking whether the m4 Marking Value instead of the received m2 or m3 Marking Value is the same as the Marking Value written in the Premark value. corresponding to the packet's IP address. If it is the same, then it corresponds to the destination "IP-Address" in the "Routing Table", and loss is marked on and forwarded to the next Router, v5. For each BGP-ASE filter, the received packet's Marked Value Sends the packet to the Next-Node.

In this case, the Marking Value corresponds to the source "IP-Address" of the "Filtering Table". After calculating the next mark value, it is marked and delivered. Suppose the Marking Value recorded (listed) in the "Filtering Table" does not match the Marking Value recorded in the packet. In that case, this packet is transferred from the host with the corresponding source "IP-Address" to a packet that does not go through a normal route, mainly dropped [23]. In BGP-ASE, not all routers use the BGP-ASE mechanism. If it works well without any problems, Figure 5 shows the appearance when the BGP- ASE mechanism is partially deployed. The colored routers use the BGP-ASE mechanism, and the uncolored routers do not use the BGP-ASE mechanism. The BGP-ASE filter sends and receives messages to and from the next BGP-ASE filter, regardless of whether routers that do not use the BGP-ASE mechanism are mixed in the middle. Even in this case, as shown in Figure 5, router V is a standard packet only when it has a Marking Value of m1. Still, suppose an attacker sends a packet marked with mz. In that case, it is filtered by the BGP-ASE filter V. In addition, as shown in Figure 5, when an attacker sends a packet to a router that does not use the BGP-ASE mechanism, the packet marked as spoofed in the BGP-ASE filter first encountered in the routing path to the destination, it is considered a packet and is therefore dropped. Therefore, BGP-ASE utilizes a spoofed source "IP-Address" by the attacker. When a packet is transmitted, the source "IP-Address" follows a route distinct from the usual routing path. The BGP-ASE filter identifies packets with a non-standard Marking Value. Additionally, as each Router employs its private key to generate the Marking Value, the attacker cannot determine the expected Marking Value for the corresponding source "IP-Address". Consequently, when a spoofed packet is transmitted, it arrives with a Marking Value that differs from the "Filtering Table" Value stored in each Router. The BGP-ASE filter detects this discrepancy and considers it a spoofed packet, causing it to be discarded before reaching the destination network.

5. IP-SPOOFING DETECTION EXPERIMENT (EMULATION ENVIRONMENT)

To measure the IP-Spoofing detection efficiency of the BGP-ASE mechanism and compare it with other IP-Spoofing detection mechanisms, the Autonomous System (AS) experiments were performed using the Mininet network emulator [19]. We performed the emulation using Mininet, "Open-Flow Switch" [20], and "POX-Controller" [21]. Mininet is an open-source and virtual-network-based emulator and gives a flexible simulation platform. It creates a virtual host network (simple host, attacker host), Switch, Legacy Switch, Legacy Router, Net Link, and Controller. Together, Mininet, OpenFlow Switch, and POX Controller form a powerful combination for developing and evaluating SDN applications. Mininet enables the creation of virtual network environments, OpenFlow switches provide programmable network infrastructure, and the POX Controller allows for centralized control and management of the network. These tools facilitate experimentation, prototyping, and research in the field of software-defined networking [24].

OpenFlow Switch is called a legacy switch, a virtual switch that allows data packets to be sent to networks. OpenFlow switches provide features such as flow-based forwarding, flow table management, and support for network virtualization. POX-Controller is a Python-Based open-source network controller for running OpenFlow/Network experiments [35].

Figure 6 shows an emulation test setup including 3 BGP-ASE enabled ASes (AS1 3) and one legacy AS (AS4). Each BGP-ASE enabled AS has a Controller (C1 3) and OpenFlow Switches (S1 7) that are functioning as the border gateway to create Net Link between AS. And Source host H1, target host H3, and malicious host H2, H4 located sequentially at AS1, AS3, AS2, AS4.

To experiment with Spoofed-Packet Filtering, we exhibited

an ARP attack scenario. In this scenario the attacker (H2, H4) located at AS2 and AS4 sequentially and launched" ICMP Packets" to destination host H3. Write down "IP-Address" of the "ICMP Packets" that were modified to the "IP-Address" of H1 applying "Python-SCAPY Library". If the malicious IP-based network-packets are filtered prior to gaining H3, it is considered i.e., the BGP-ASE endeavor's effective. Wechecked packet transmission status by using Wireshark (see Figure 7). H1 accomplished sending the "ICMP Packets" to H3 lacking a bit of network-packet dropping, although H2 and H4 were unsuccessful in doing the communication due to the unreachable state.

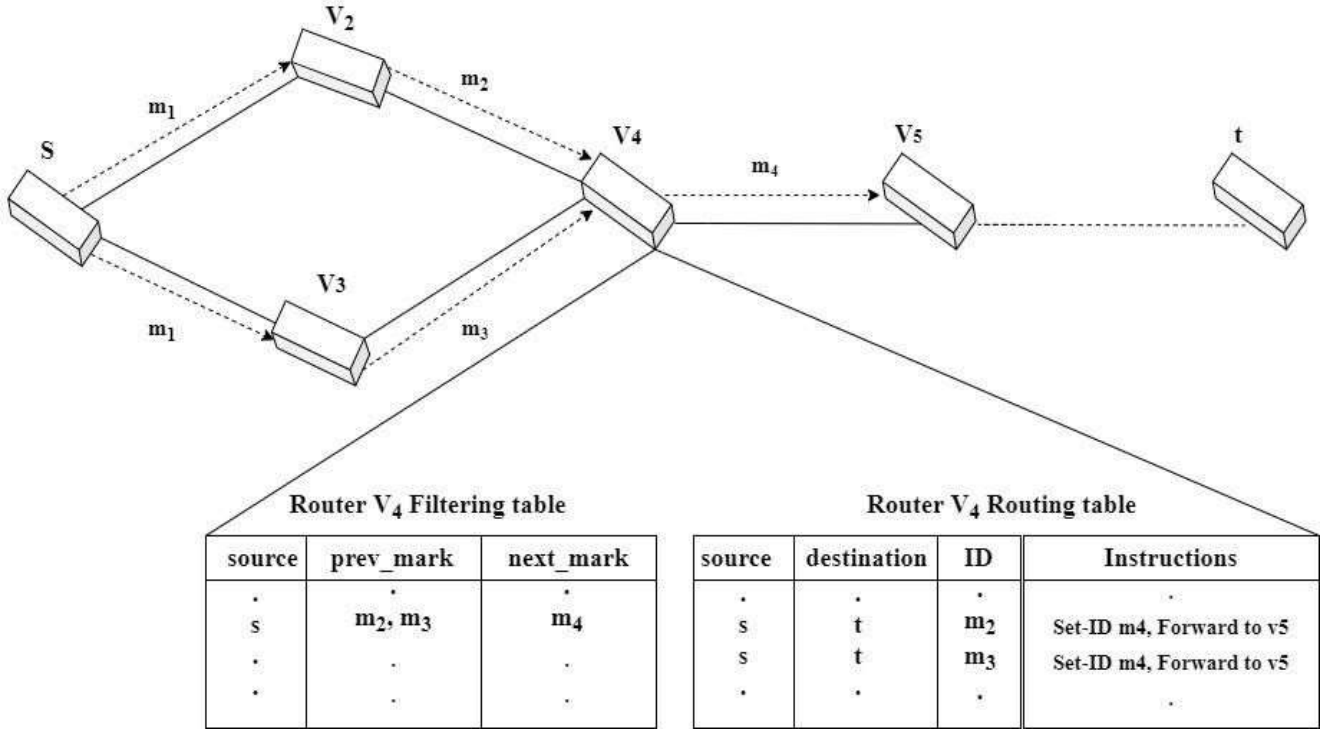

Fig. 4 Filtering Table & Routing Table in Router V_4

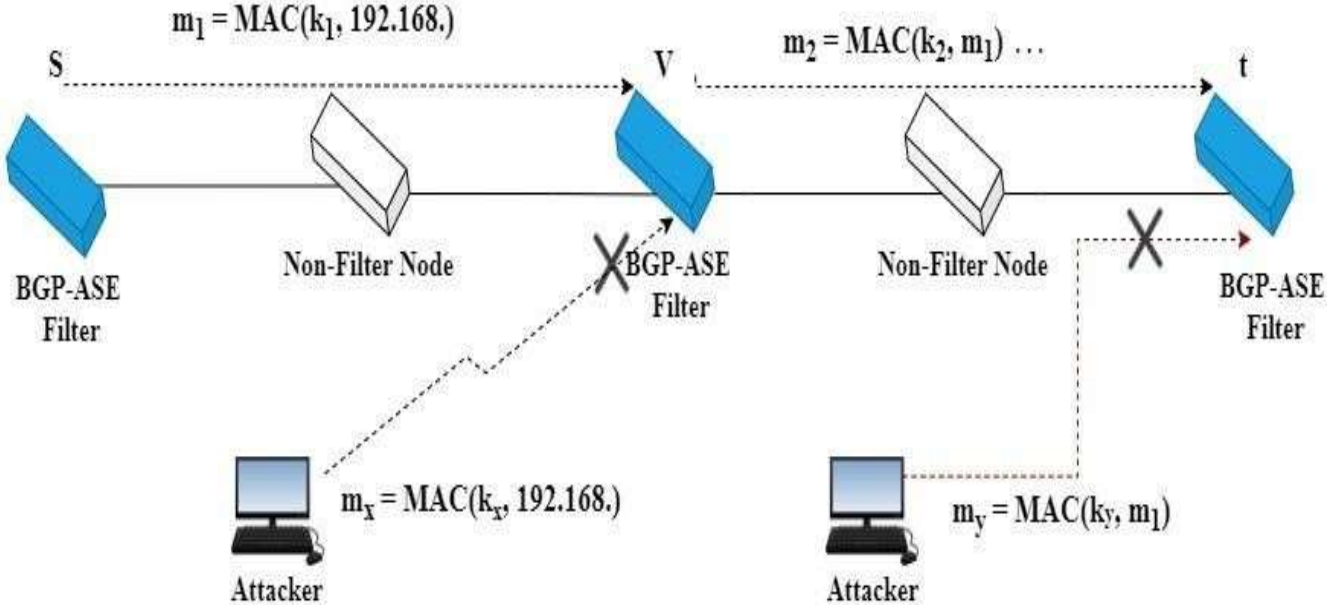

Fig. 5 BGP-ASE Filter Operation Under Partial Deployment

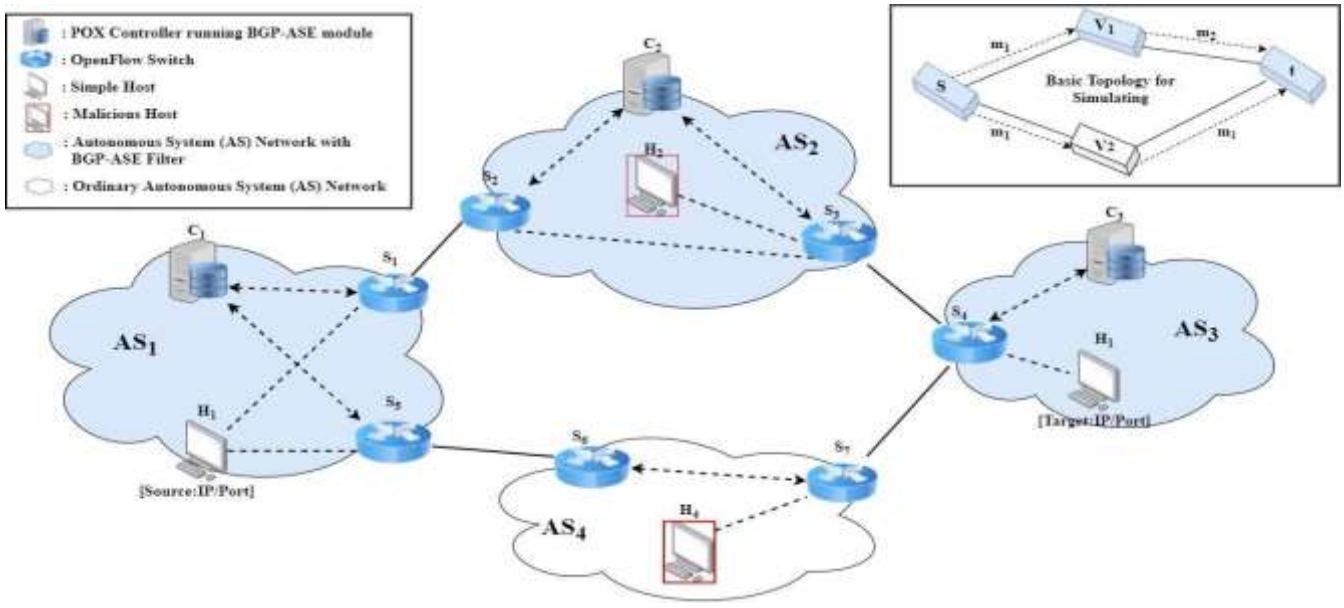

Fig. 6 Test Emulation Network Environments

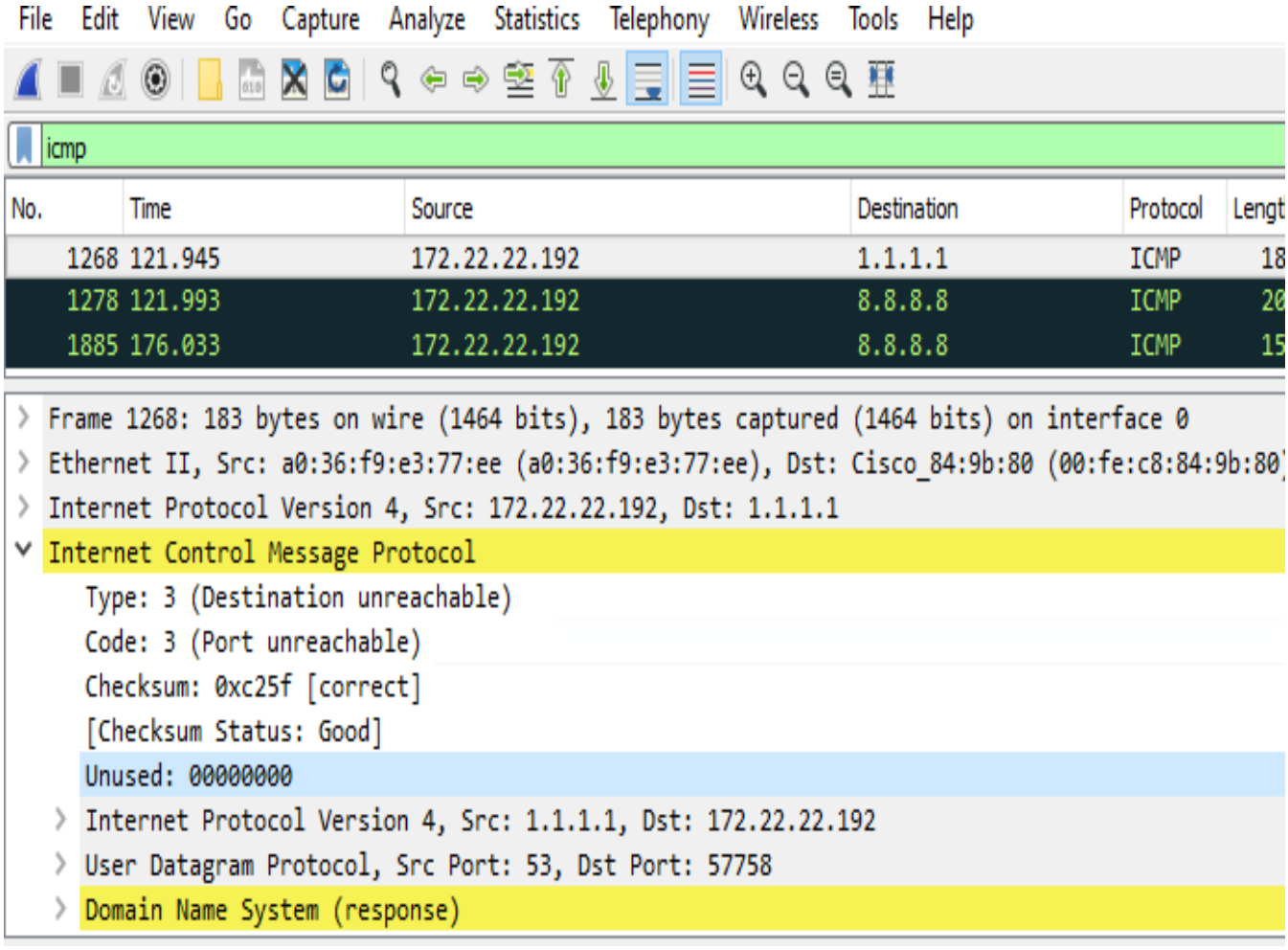

Fig. 7 Packet Transmission Status after BGP-ASE Filtering

Table.1 Output Readings Tabulated by Varying the Packet Drop-in Attack Mode

Time	Attack	Filtering Mechanism Comparisons		
(m/sec)	Packet Drop	Ingress Egress [22]	RPF [23]	Proposed (BGP-ASE)
0-20	Packet Drop(*10^4)	0.97*	1.23*	3.34*
20-40	#NAME?	1.32*	0.94*	3.12*
40-60	- Packet Delivered ”Packets are transmitted at 2 Mbps = 54000 bits”	0.23*	1.42*	2.28*
60-80		0.84*	1.13*	4.54*
80-100		1.34*	0.84*	2.68*
Randomly Deployment on Nodes		40 - 50%	50 - 60%	25 - 30%
Overall Attack Packet Dropping Ratio		50%	60%	90%

located at AS2 and AS4 sequentially and launched ”ICMP Packets” to destination host H3. Write down ”IP-Address” of the ”ICMP Packets” that were modified to the ”IP-Address” of H1 applying ”Python-SCAPY Library”. If the malicious IP-based network-packets are filtered prior to gaining H3, it is considered i.e the BGP-ASE endeavors effective. Wechecked packet transmission status by using Wireshark (see Figure 7). H1 accomplished sending the ”ICMP Packets” to H3 lacking a bit of network-packet dropping, although H2 and H4 were unsuccessful in doing the communication due to the unreachable state [36-40].

6. RESULTS AND DISCUSSION

To compare the filtering performance of spoofed packets, we experimented with not only BGP-ASE but also ingress filtering and RPF mechanisms. Table I shows that BGP- ASE is more powerful than others in dropping attack packets among three mechanisms. Using this mechanism on only 30% of transit Autonomous Systems (ASes) can filter over 90% of the malicious packets. It shows the filtering performance of the mechanism with a different base.It has a much better understanding of detecting spoofed packets than other systems. Figure 8 exhibits the filtering mechanisms fulfillment for dropping attack packets by applying “Random Filter Placement”. The attack packet must wait for the link to transmit 4.5 ∗ 1, 500bytes = 54, 000bits since these bits are transmitted at 2 MBPS. Wireshark shows the packet transmission status. Besides, the BGP-ASE mechanism satisfies the three characteristics of the practical protocol described earlier. The first characteristic was that the filtering effect should also be given

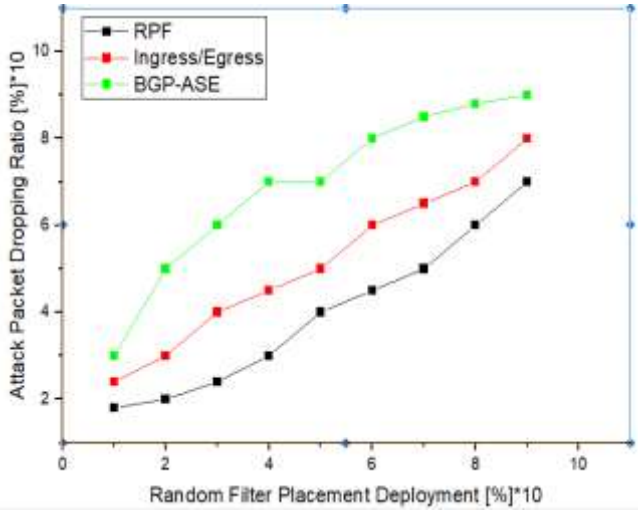

Fig. 8 Comparisons of Deployment and Attack Packet Drop- ping Ratio

The second characteristic is the gradually improving filter. Many As routers use the BGP-ASE mechanism, the filtering process increases slowly. And as a third characteristic, even if not all routers use the BGP-ASE mechanism, the mechanism works well, and excellent performance is gathered. Therefore, the BGP-ASE mechanism satisfies the characteristics of three practical protocols and outperforms other IP-Spoofing detection mechanisms.

7. CONCLUSIONS AND FUTURE WORK

We looked at the many different types of IP-Spoofing assaults, as well as the dangers they provide and the assistance they get, throughout this paper. These assaults have the goal of keeping the location of the perpetrator a secret. IP-Spoofing is conceivable due to weaknesses in the design and execution of TCP/IP; as a result, it is difficult to construct a full protection mechanism without first adopting a new protocol. However, it is possible to improve the speed of the network by screening bogus packets before they reach the target host. This would be a step in the right direction. It is possible to achieve this goal by implementing countermeasures in the router that take advantage of the BGP-ASE mechanism. The system can effectively withstand huge spoofing packets while just taking a moderate amount of work to install, since it is equipped with the necessary computing power. Because it fits all three of the essential conditions of a practical protocol, the BGP-ASE mechanism, when used on genuine AS routers, offers an extra layer of Defence against spoofing attacks. This Defence is made possible by the fact that it is a practical protocol. BGP-ASE not only delivers advantages to customers, but it also surpasses existing anti- spoofing algorithms that are already in circulation. In the not-too-distant future, there are plans to review the efficiency of the Router's filtering capabilities and to put a greater focus on dynamic network-packet marking.

REFERENCES

1. S. J. Templeton and K. E. Levitt (2003), Detecting spoofed packets, in Proc. DARPA Information Survivability Conference and Exposition, Washington, DC, USA, 164-175. https://doi.org/10.1109/DISCEX.2003.1194882 .

2. N. Tripathi, M. Swarnkar and N. Hubballi (2017), DNS spoofing in local networks made easy, in Proc. IEEE ANTS, Bhubaneswar, India, 1-6, https://doi.org/10.1109/ANTS.2017.8384122 .

3. C. Zhang et al. (2018), Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack, IEEE Access, 22764-22777(Vol. 6). https://doi.org/10.1109/ACCESS.2017.2785236 .

4. G. P. Epps and M. Laor (2004), Flexible engine and data struc ture for packet header processing, US Patent 6,721,316. https : / / patents . google . com / patent / US6721316B1/en.

5. A. Dua, V. Tyagi, N. Patel and B. Mehtre (2019), IISR: A Secure Router for IoT Networks, in Proc. 4th ISCON, Mathura, India, 636-643. https://doi.org/10.1109/ISCON47742.2019.9036313 .

6. Y. Gilad and A. Herzberg (2012), Lot: A Defense Against IP Spoofing and Flooding Attacks, ACM Trans. Inf. and Syst. Secur., 1–30(Vol. 15). https://doi.org/10.1145/2240276.2240277

7. P. Du and A. Nakao (2010), DDoS Defense Deployment with Network Egress and Ingress Filtering, in Proc. IEEE Int. Conf. Commun., Cape Town, South Africa, 1-6. https://doi.org/10.1109/ICC.2010.5502654 .

8. K. Benton, L. J. Camp, T. Kelley and M. Swany (2015), "Filtering IP source spoofing using feasible path reverse path forwarding with SDN, in Proc. IEEE Conf. CNS, Florence, Italy, 733-734. https://doi.org/10.1109/CNS.2015.7346909 .

9. M. S. Bonab, A. Ghaffari, F. S. Gharehchopogh, and P. Alemi (2020), A wrapper-based feature selection for improving performance of intrusion detection systems, Int. J. of Commun. Syst., e4434(Vol. 33). https://doi.org/10.1002/dac.4434

10. A. Seyfollahi, M. Moodi, and A. Ghaffari (2022), MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications, Computer Standards & Interfaces, (Vol. 82). https://doi.org/10.1016/j.csi.2022.103622 .

11. S. Rashid and S. P. Paul (2013), Proposed Methods of IP Spoofing Detection & Prevention, IJSR, 438–444(Vol. 2). https : / / www . ijsr . net / archive / v2i8 / MTIwMTMxMzA=.pdf .

12. H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. S. Gharehchopogh (2023), Anomaly-based intrusion detection system in the internet of things using a convolutional neural network and multi-objective enhanced capuchin search algorithm, J. Parallel Distrib. Comput., 1-21(Vol. 175). https://doi.org/10.1016/j.jpdc. 2022.12.009 .

13. N. D. Patel, B. M. Mehtre, and R. Wankar (2019), Things-to-Cloud (T2C): A Protocol-Based Nine-Layered Architecture, in ICICCT, Springer, 789–805. https://doi.org/ 10.1007/978-981-15-7345-368 .

14. J. Yu, E. Kim, H. Kim and J. Huh (2016), A Framework for Detecting MAC and IP Spoofing Attacks with Network Characteristics, in Proc. ICSSA, Saint Pölten, Austria, 49-53. https://doi.org/10.1109/ICSSA.2016.16

15. B. Field, J. V. Doorn, and J. Hall (2021), Content delivery network routing using border gateway protocol, US Patent App. 13/569,692. https://patents.google.com/patent/US11178244B2/en

16. S. Kaur, J. Singh, and N. S. Ghumman (2014), Network Programmability using POX Controller, in Proc. Int. Conf. Commun. Comput. Syst. IEEE, 134–138(Vol.

138).

17. K. Park and H. Lee (2001), On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets, ACM SIGCOMM computer communication review, 15–26(Vol. 31). DOI: https://doi.org/10.1145/383059.383061 .

18. A. Yaar, A. Perrig and D. Song (2006), StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense, IEEE J. Sel. Areas Commun., 1853-1863(Vol. 24). https://doi.org/10.1109/JSAC.2006.877138

19. R. L. S. de Oliveira, C. M. Schweitzer, A. A. Shinoda and Ligia Rodrigues Prete (2014), Using Mininet for emulation and prototyping Software-Defined Networks, in Proc. IEEE Colomb. Conf. Commun. Comput., Bogota, Colombia, 1-6. https://doi.org/10.1109/ColComCon.2014.6860404 .

20. S. Acharya and N. Pradhan (2017), DDos simulation and hybrid ddos defense mechanism, International Journal of Computer Applications, 20-24(Vol. 163). https://doi.org/10.5120/ijca2017913736 .

21. C. Zhang, F. Luo and G. Ranzi (2019), An Advanced Persistent Distributed Denial-of-Service Attack Model With Reverse-Path Forwarding-Based Defending Strategy, IEEE Access, 185590-185596(Vol. 7). https://doi.org/10.1109/ACCESS.2019.2959985 .

22. V. Parekh and S. M (2022), A Hybrid Approach to Protect Server from IP Spoofing Attack, in Proc. International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 1-9. https://doi.org/ 10.1109/ICSES55317.2022.9914164 .

23. S. M. Morsy and D. Nashat (2022), D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing, IEEE Access, 49142-49153(Vol. 10). https://doi.org/10.1109/ACCESS.2022.3172329

24. H. A. S. Adjei, M. T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah and E. S. A. Gyarteng (2021), SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection), in Proc. 23rd International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 187-193. https://doi.org/10.23919/ICACT51234.2021.9370460 .

25. S. Park, S. Kwon, Y. Park, D. Kim and I. You (2022), Session Management for Security Systems in 5G Standalone Network, IEEE Access, 73421-73436(Vol. 10). https://doi.org/10.1109/ACCESS.2022.3187053 .

26. H. Y. Ibrahim, P. M. Ismael, A. A. Albabawat and A. B. Al-Khalil (2020), A Secure Mechanism to Prevent ARP Spoofing and ARP Broadcasting in SDN, in Proc. International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 13-19. https://doi.org/10.1109/CSASE48920.2020.9142092 .

27. P. Roopchandka, S. Khanam, R. Dhan, K. Neelam, D. Prasad and V. Nath (2019), Design of Password Based Door Locking System, in Nath V., Mandal J. (eds) Proceedings of the Third International Conference on Microelectronics, Computing and Communication Systems, Lecture Notes in Electrical Engineering, Springer, Singapore, 605-612(Vol. 556). https://doi.org/10.1007/978-981-13-7091-5_50 .

28. A. Muthigi, A. Kumar, G. Bhagchandani, K. Muthigi, V. Nath (2023), Automated Cheque Processing Through Data Verification and Siamese Networks, in Microelectronics, Communication Systems, Machine Learning and Internet of Things. Lecture Notes in Electrical Engineering, vol 887, Springer, Singapore. https://doi.org/10.1007/978-981-19-1906-0_59

29. U. Anchalia, K. P. Reddy, A. Modi, K. Neelam, D. Prasad and V. Nath (2019), Study and Design of Biometric Security Systems: Fingerprint and Speech Technology, in Nath V., Mandal J. (eds) Proceedings of the Third International Conference on Microelectronics, Computing and Communication Systems, Lecture Notes in Electrical Engineering, Springer, Singapore, 577-584(Vol. 556). https://doi.org/10.1007/978-981-13-7091-5_47

30. V. Goel, H. Raj, K. Muthigi, S. S. Kumar, D. Prasad and V. Nath (2019), Development of Human Detection System for Security and Military Applications, in Nath V., Mandal J. (eds) Proceedings of the Third International Conference on Microelectronics, Computing and Communication Systems, Lecture Notes in Electrical Engineering, Springer, Singapore, 195-200 (Vol. 556). https://doi.org/10.1007/978-981-13-7091-5_18 .

31. S. S. Kumar, A. Khalkho, S. Agarwal, S. Prakash, D. Prasad, V. Nath (2019), Design of Smart Security Systems for Home Automation, in Nath V., Mandal J. (eds) Nanoelectronics, Circuits and Communication Systems. Lecture Notes in Electrical Engineering, 599-604(Vol. 511). pp. Springer, Singapore; https://doi.org/10.1007/978-981-13-0776-8_56

32. S. Sun, X. Fu, B. Luo and X. Du (2020), Detecting and Mitigating ARP Attacks in SDN-Based Cloud Environment, in Proc. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, Canada, pp. 659-664, https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162965 .

33. A. Nigam, S. Sharma, R. K. Patel and M. Agrawal

(2022), Man-In-The-Middle-Attack and Proposed Algorithm for Detection, in Proc. International Mobile and Embedded Technology Conference (MECON), Noida, India, pp. 83-88, https://doi.org/10.1109/MECON53876.2022.9752406 .

34. H. A. S. Adjei, T. Shunhua, G. K. Agordzo, Y. Li, G. Peprah and E. S. A. Gyarteng (2022), SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection), in Proc. 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon Do, Korea, Republic, pp. 187-193, doi: 10.23919/ICACT53585.2022.9728961.

35. I. M. Tas, B. G. Unsalver and S. Baktir (2020), A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism, IEEE Access, 112574-112584(Vol. 8). https://doi.org/10.1109/ACCESS.2020.3001688 .

36. T. S Reddy, K.A. M Junaid, Y. Sukhi and Y. Jeyashree and P. Kavitha and V. Nath (2023), Analysis and design of wind energy conversion with storage system. e-Prime - Advances in Electrical Engineering, Electronics and Energy 100206(Vol. 17). https://doi.org/10.1016/j.prime.2023.100206

37. D. Sharma, A. Rai, S. Debbarma, O. Prakash, M K Ojha and V. Nath (2023), Design and Optimization of 4-Bit Array Multiplier with Adiabatic Logic Using 65 nm CMOS Technologies, IETE Journal of Research, 1-14. https://doi.org/10.1080/03772063.2023.2204857

38. J. Tirkey, S. Dwivedi, S. K. Surshetty, T. S. Reddy, M. Kumar, and V. Nath. (2023), An Ultra Low Power CMOS Sigma Delta ADC Modulator for System-On-Chip (SoC) Micro-Electromechanical Systems (MEMS) Sensors for Aerospace Applications. International Journal of Microsystems and Iot, 26–34(Vol.1). https://doi.org/10.5281/zenodo.8186894

39. D. Sharma, N. Shylashree, R. Prasad, and V. Nath. (2023), Analysis of Programmable Gain Instrumentation Amplifier. International Journal of Microsystems and Iot, 41–47(Vol. 1). https://doi.org/10.5281/zenodo.8191366

40. N.Anjum, V. K. Singh Yadav, and V. Nath. (2023). Design and Analysis of a Low Power Current Starved VCO for ISM band Application. International Journal of Microsystems and IoT, 82–98. (Vol. 1) https://doi.org/10.5281/zenodo.8288193

AUTHORS

ND Patel received his B.Tech degree in Computer Science from Dr A.P.J. Abdul Kalam Technical University in 2012 and the MTech degree in Computer Science from the School of Computer and Information Sciences (SCIS), University of Hyderabad (UoH), India, in 2015. He is currently pursuing a PhD degree in Computer Science from the Centre of Excellence in Cyber Security (CoECS) at the Institute for Development and Research in Banking Technology (IDRBT) and the University of Hyderabad (UoH), India. His research interests include the area of Computer and Network Security, Attack Graph, Fog/Edge Computing, the Internet of Things, Cyber Security, and Digital Forensics.

Corresponding Author E-mail: narottamdaspatel@vitbhopal.ac.in

BM Mehtre is Professor and Head, Centre of Excellence in Cyber Security (CoECS) at IDRBT (Institute for Development and Research in Banking Technology) India. His areas of interest include Cyber Security, Digital Forensics, and Technologies for Cyber Defense. He received his BE (Electronics & Communication) from Gulbarga University in 1983, an MTech (Automation & Control), and PhD (Engineering) from the Indian Institute of Technology, Kharagpur, in 1985 and 1991, respectively. His seminal work on fingerprint identification led to the development of the first automated fingerprint identification system in India, which was later deployed in many state police departments in India and some countries outside India.

E-mail: bmmehtre@idrbt.ac.in

Rajeev Wankar is working as a Professor in the School of Computer and Information Sciences (SCIS) at the University of Hyderabad (UoH). He earned PhD in Computer Science from the School of Computer Sciences, Devi Ahilya University Indore. In 1998, the German Academic Exchange Service (DAAD) awarded him" Sandwich Model" fellowship. His research interests are in the areas of Cloud Computing and Grid Computing.

E-mail: wankarcs@uohyd.ernet.in

Rahul Priyadarshi received his B Tech degree in electronics and communication engineering from Amrita School of Engineering, Bangalore, India in 2013, MTech degree in communication system & network from National Institute of Technology Hamirpur, India in 2018 and PhD degree in Wireless Sensor Network from National Institute of Technology Patna, India in 2023. He is currently assistant professor at Siksha O Anushandhan University Bhubaneswar, India. His area of interest is wireless sensor network.

E-mail: rahulpriyadarshi@soa.ac.in