Harla Journals

Harla Journal of Engineering and Technology

Journal home page: https://journals.ddu.edu.et/index.php/HJET

Harla journal of Engineering and Technology

Survey on IP Spoofing Detection and Prevention

[1]Teshome Mulugeta Ababu, [2]Abdulmejid Tuni Johar,

[12]*Computer Science Department, School of Computing, Dire Dawa University, Dire Dawa, Ethiopia*

teshome.mulugeta@ddu.edu.et, tuniabdulmejid@gmail.com

Abstract

The weakness of the network layer in the OSI model allows an intruder to modify the original IP address of the packet and replace it with a forged IP address of the sender to mask the authentic or genuine IP address of the packet that transmits over a network. IP spoofing is the process in which the attackers change the actual IP address of the packet and replace it with a fake IP address and masquerade or impersonate legitimate users over the internet. Then, the attacker collects confidential information they can use or sell. Hence, this paper provides a survey on different art techniques used to detect and prevent IP spoofing over the internet (IP). Spoofed packet detection is included routing methods and non-routing methods. Hop count filtering by building IP2HC and other techniques are there. As we observed in many papers, a hop count filter is the most used technique to detect and prevent IP spoofing packets. Still, it has limitations on different Operating systems with different TTL (Time to live). Generally, the detection and prevention of IP spoofing can be implemented through artificial neural networks. It is more sophisticated when we compare them with other techniques of detecting and preventing Spoofed packets.

Keywords: IP spoofing, IP spoofing detection, IP spoofing prevention

1. INTRODUCTION

In Today's world, security is a critical issue over the internet and the most challenging task to maintain. There are data theft, identity theft, data forged, and attacking infrastructure. As the internet is accelerated enormously, it is challenging to maintain computer and network security become it is a tedious activity [1]. Computers communicate over the internet through the exchange of network data packets. Each data packet has the destination IP address on a header and is transported over a network. The concept of IP spoofing is the act of falsifying the content of the source IP address where the packet is come from, usually with a random number if it is not on the same subnet to hide the real identity of the sender's or to launch distributed denial of services [2] [1].

According to [2], the most effective approach to detect and prevent IP spoofing is hop counting filtering methods by constricting H2PC. By spoofing the IP address the intruder attack DDOS, Smurf attack, NTP synchronization reflection, Distributed reflection DOS, DNS request reflection, TCP-

---

**Corresponding author: Teshome Mulugeta, teshome.mulugeta@ddu.edu.et*

DOI:

 Manuscript received October, 2022; revised November, 2022; accepted December, 2022.

SYN flooding attack [3] . Anti IP spoofing is extensively studied by different scholars for more than a decade. However, feasibility and integrated solution that cover intra-domain and inter-domain scope are still under the ways of research [4]. The most existing IP spoof detection and traceback heavily depend on an internet services provider that is not more flexible [1]. There are different ways to identify the spoofed IP address over the network a protocol from those methods host-based OS fingerprint which is applied by using passive and active methods. This approach is done by matching the filtered spoofed IP packet to the operating system of arriving packet from its database. This method is furthermore implemented in cloud computing. Using the mapping IP address and their hop count to the server can distinguish the legitimated and spoofed or unauthorized IP address client from legitimated one.

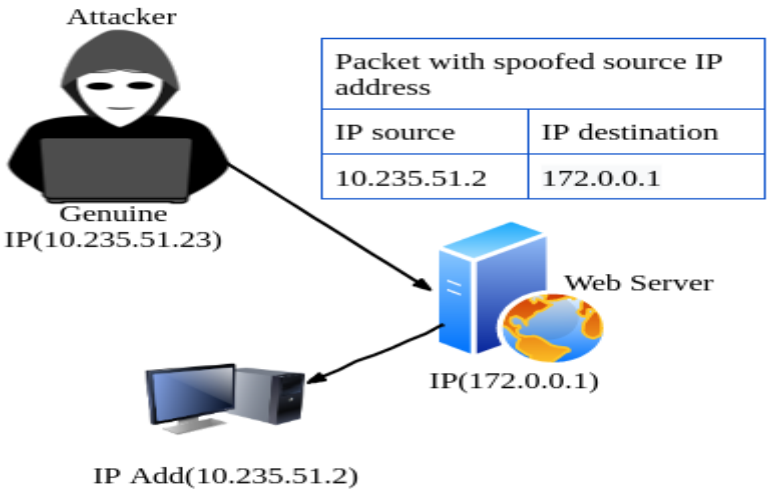

Fig. 1: Transmission of Spoofed IP packet (Spoofed on the same subnet) the basic architecture is inspired or benchmark architecture accepted from [5].

2. RELATED WORK

According to [6] there are various techniques are used to detect spoofed IP address such as penetration testing, using hop count, using packet filtering and other. Penetration test means test all possible vulnerability that intruders used to penetrate over the network.it is a systematic approach to check the vulnerability of the network. Hop count filtering is another techniques used by many researcher hope count filter algorithm receive IP destination IP address indirectly from TL (time to live) field rather than obtain directly destination IP address from the packet header. In this technique, each packet that arrives at the destination is monitored and compared hope count values with stored hope count values, if any miss-match occurs the packet is discarded automatically [6]. Most papers have used this approach to guess the attacker or intruder fooled packet. This prevention scheme is trying to improve the security schema of computers or networks [7]. Hop count the most techniques used to prevent IP spoofing in which the TTL (Time to Live) field determines the validity period of

the sent packet [2] but different operating systems use the different time to live data packet. IP spoofing prevention using reverse path forwarding to a Software-defined network is checked at the gateway is validated by verifying the existing route to the original IP address [8].

According to the survey on IP spoofing made by[9], there are three methods used to prevent IP spoofing attacks the first method is IP can be spoofed over the internet because authentication can just be made on the source IP address. There is other criteria in which authentication are independent of the source IP address. The second method of spoofing is occurring due to the design flow of UDP. However, TCP can provide an effective mechanism because it is establishing a connection linkage between sender and receiver by handshake mechanism. Finally, the third method proposed by this article is disabling the ping command. According to [1] the researcher develops an algorithm that track-back the location of an attacker and it uses K-means clustering for better file management. Similarly, the proposed system used a Support vector machine for classification. The passive approaches follow ISP can block attackers or any authorized body can take action over it.

3. MOTIVATION

Today as human when we are connected to the internet there is no hundred percent warrant that our computer, network, and the file is secure. We are not the first researcher to survey on IP spoofing detection and prevention; it is an open field of study that can be studied/surveyed by many scholars. Even though there are a few survey papers available in this area, it is not enough when we compare the risk of IP spoofing. This motivates this survey to be conducted. IP spoofing is a serious criminal activity except for legitimate/educational purposes. There are different techniques used to detect and prevent IP spoofing each technique has their advantage and disadvantages so comparing them, analyzing them, and suggesting the best techniques for our network is motivate the survey to be conducted by comparing many research papers with each other. This kind of survey is initiated us to know about IP spoofing and its consequence. Furthermore, this is motivating us what to do if we are a security consultant of some company.

4. IP SPOOFING DETECTION

IP Spoofing can be classified into full random IP spoofing addresses and Subnet spoofing [10]. Full Random IP spoofing address means that an attacker can modify the header of the packet with a random IP address this method does not produce a valid IP address it is the random IP address from 0.0.0.0-to-255.255.255.255 the weakness of this system is that it generates a non-routable IP address. The subnet spoofing in this spoofing the attacker has a hint about the IP address (on the same subnet) and he/she is trying the neighbor IP address [10].

4.1 Techniques of Detection and prevention of spoofed IP Packet

According to [11] the first technique is Hop count filtering. This technique compares the values obtained from constructed IP to Hop-count (IP2HCP) if there is a mismatch between them the packet is discarded automatically. The disadvantages of this technique are all operating systems have unique initial TTL (time to live). Another tool used to detect spoofed packets is traceroute. It is a network tool that is used to tells the hop number to original packet sources. One disadvantage of this tool is its Latency. Finally, the researcher recommends TCP because it is a connection-oriented protocol. This technique ensures efficient delivery of packets because it is providing acknowledgment between sender and receiver.

According to [1] the most existing methods of detecting spoofed IP address depends on Internet services provider. The disadvantages of this technique are it not flexible and robust to overcome this shortage the researcher introduces the concept of K-means clustering. According to [3] there are techniques and tools are used to detect spoofed IP addresses in a wireless network. Hybrid detection of IP spoofed nodes is efficient in this way the researcher use bat optimization it is inspired on BAT algorithm based on SI techniques. This algorithm is used to distinguish legitimated packets from un legitimated packets. The advantages of this algorithm are it very efficient for complex network analysis. But Disadvantage of this algorithm is implementing this algorithm is somewhat complicated.

According to [4] the researcher arise different techniques used to detecting spoofed IP packets the first methods used by the researcher is IP address source filtering this filtering can be implemented by three filtering ingress, egress, and rout based filtering which checks the packet legitimacy in router ingress, egress, and internal modules. The second approach is IP source encryption. In this approach, the sender replaces the source IP address of the packet with an encrypted one and it is decrypted by the legitimated user only even if it is theft. The third approach is SDN – based on Source IP address validation this approach is used to validate the source IP address before processing any request. And the fourth approach is protocol and host stack redesign in this approaches new protocol is installed and named with Host identity Protocol in the middle of IP and TCP.

According [1] [12] [6] [13] and other researcher conclude that there are different techniques used to prevent IP spoofed packet from those of them the following are the basic

1 Implementing filtering in both in and outbound traffic.

2 By configuring switch and router if the switch and router support the validity of an incoming packet.

3 By using authentication based on a key exchange between machines on a network.

4 Enable encryption session on a router so that trusted host outside of a network is securely communicated.

5 By using an access control list to deny private IP addresses on your downstream interface.

The other techniques used to prevent Spoofed IP packet is by using network analysis tools such as

- ✓ Trace out and other commercial applications are there [3]

Table 1. **Comparison of previous work on Detection and prevention Spoofed IP address**

Reference	Year of publication	Title of Study	Spoofed IP Packet Detection and Prevention approaches	Proposed algorithm/ mechanism
[1]	2019	A two-way approach for detection and prevention of IP spoofing attacks	Detect by matching the IP address of the current host by matching the IP address of the dynamic list generated by API. Prevention: File encryption	k-means for file clustering SVM-for classifying detail fetched by API
[2]	2018	An Improved Strategy for Detection and Prevention IP Spoofing Attack,	The detection and prevention approach proposed by the paper is Hop count filtering methods.	Hop-count inspection algorithm with IP2HC
[11]	2018	IP Spoofing Detection for Preventing DDoS Attack in Fog Computing	Detection Approaches: HCF(hope count filter) Prevention approaches: Establishing TCP connection-oriented protocol that has provides acknowledgment for sender so the attacker never acknowledges.	TCP-connection oriented protocol with Operating system fingerprinting
[14]	2008	Controlling IP Spoofing Through Inter-Domain Packet Filters	Detection and prevention approach: inter-domain packet filtering. this does not need global routing information	IDPF Mechanism
[15]	2007	Defense Against Spoofed IP Traffic Using Hop-Count Filtering	Detection and prevention: By comparing Mapping IP address and their Hop count, the server infers hop count information from the TTL (Time to Live) field of the IP header.	HCF by this mechanism 90 % of the spoofed IP packet is discarded.
[13]	2019	Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in ANN	Detection and prevention approach: 5-node architecture network is used to detect man in the middle of the network.	An artificial neural network algorithm is used to detect and prevent spoofed IP addresses. The algorithm accuracy is 88.235%

[3]	2019	Detection of Spoofed IP nodes using BAT Algorithm and Extreme Learning Machine	Detection and prevention approaches: the hybrid of • Bat optimization approaches • Behavior of bat • ELM approaches	BAT based ELM algorithm with 100 % accuracy of detecting spoofed IP address ELM
[12]	2019	Proposed Methods of IP Spoof	Detection approach: Routing and non-route approaches. Routing methods mean that it is perfume ingress filtering on the packet that is protecting from outside attack. Non-routing methods: using network monitoring software Prevention Approaches: compression ✓ Lossy compression ✓ Lossless compression Encryption: by encrypting the source IP address of the packet.	Algorithm used by researcher have the following steps Split packet header with data >>apply GRS compression>>apply cryptography>>transmit >>decryption>>decompression >>plain text received

5. CONCLUSION

Cybercrime is the most serious issue in today's world. It can be implemented in various ways, from spoofing or fooling the IP address of the genuine packet. IP spoofing is the mechanism in which an intruder or attacker modifies the legitimated IP address of the sender packet with the forged IP address to obtain un legitimated confidential and sensitive information without authorization. IP spoofing has different categories, such as blind spoofing, which means that the attacker fools the IP address of the packet with a random IP address; non-blind spoofing is spoofing in which the attacker is on the same subnet, denial of services. This attack occurs when the attacker sends a successive request to the server that seems legitimate uses and finally makes the server busy to stop serving other clients and become a denial service. The other categories of IP spoof attack are the man in the middle. These kinds of attackers are targeted to reveal target information. Different approaches are used to detect and prevent IP spoofing, as described in the above table.

Similarly, additional open-source and commercial tools are used to detect and avoid IP spoofs, as we observed from the different research papers. Most research illustrates that Internet service providers are still used to detect and prevent spoofed IP packets but arecould be better at tracking back the attacker. Later different tools are developed to detect, control, and track back the IP address of the attacker. Most research papers illustrate that IP spoof detection and prevention can be implemented on three levels: route, host, and flow. As we observed in this literature, more than three

papers used hop count filters to detect and prevent spoofed packets over the networks. In general, the ways of science in IP spoof detection and prevention are improved, as illustrated in this survey.

6. REFERENCES

[1] K. Vijayakumar, A. Rai, G. S. Kumar, T. S. Angel, and N. Snehalatha, "A two-way approach for detection and prevention of IP spoofing attacks," in *AIP Conference Proceedings*, 2020, vol. 2277, no. 1, p. 020002.

[2] H. B. Said and T. A. Khaleel, "An Improved Strategy for Detection and Prevention IP Spoofing Attack," *International Journal of Computer Applications*, vol. 975, p. 8887, 2018.

[3] S. Banu. A, and P. Ganapathi, "Detection of Spoofed IP nodes using BAT Algorithm and Extreme Learning Machine," vol. 9, no. 2, Dec. 2019, [Online]. Available: https://www.ijeat.org/wp-content/uploads/papers/v9i2/B2962129219.pdf

[4] C. Zhang *et al.*, "Towards a SDN-based integrated architecture for mitigating IP spoofing attack," *IEEE Access*, vol. 6, pp. 22764–22777, 2017.

[5] N. Vlajic, M. Chrowdhury, and M. Litoiu, "IP Spoofing In and Out of the Public Cloud:From Policy to Practice," vol. 8, no. 4, Nov. 2019, [Online]. Available: https://www.mdpi.com/2073-431X/8/4/81

[6] A. M. Jacob and S. Saritha, "Survey on Various IP Spoofing Detection Techniques".

[7] Y. Chen, S. Das, P. Dhar, A. El-Saddik, and A. Nayak, "Detecting and Preventing IP-spoofed Distributed DoS Attacks.," *Int. J. Netw. Secur.*, vol. 7, no. 1, pp. 69–80, 2008.

[8] S. Rajashree, K. S. Soman, and P. G. Shah, "Security with ip address assignment and spoofing for smart iot devices," in *2018 international conference on advances in computing, communications and informatics (ICACCI)*, 2018, pp. 1914–1918.

[9] S. Dubey and S. Gupta, "A Survey on Various IP Spoofing Attacks Techniques".

[10] R. Singh, K. Thakur, G. Singh, and S. Gupta, "Prevention of IP spoofing attack in cyber using artificial Bee colony and artificial neural network," in *Proceedings of the Third International Conference on Advanced Informatics for Computing Research*, 2019, pp. 1–10.

[11] A. E. Agoni and M. Dlodlo, "Ip spoofing detection for preventing ddos attack in fog computing," in *2018 Global Wireless Summit (GWS)*, 2018, pp. 43–46.

[12] S. Rashid and S. P. Paul, "Proposed methods of IP spoofing detection & prevention," *International Journal of Science and Research*, vol. 2, no. 8, pp. 438–444, 2013.

[13] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, vol. 2019, 2019.

[14] Z. Duan, X. Yuan, and J. Chandrashekar, "Controlling IP spoofing through interdomain packet filters," *IEEE transactions on Dependable and Secure computing*, vol. 5, no. 1, pp. 22–36, 2008.

[15] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," *IEEE/ACM Transactions on networking*, vol. 15, no. 1, pp. 40–53, 2007.