A Novel Method Defense against IP Spoofing Using Packet Filtering and Marking

K. Durga Priyanka[1], Dr. N. Chandra Sekhar Reddy[2], B. Satish Babu[3]

[1]M. Tech CSE Department, Institute of Aeronautical Engineering, HYD-500043, Telangana, India

[2]Professor, CSE Department, Institute of Aeronautical Engineering, HYD-500043, Telangana, India

[3]Assistant Professor, CSE Department, Institute of Aeronautical Engineering, HYD-500043, Telangana, India

Abstract: ***With wide spread use of internet in various fields, networks are being exposed to many security vulnerabilities such as distributed denial of service (DDoS) attack, worm/virus, and so on. The prevention failure of network security leads to either revealing of sensitive information or interruption of network services, thereby results in the enormous economic loss. The distributed DoS attack will occurs at Network level by obtaining IP addresses. This kind of vulnerability is called as IP Spoofing. Intrusion Detection System (IDS) has been used to secure these environments for sharing their data over network and host based IDS approaches. This paper focus on the defense against IP spoofing attacks using Packet filtering methods and Packet Marking techniques. This scheme is defense against DDoS attacks and IP Spoofing attacks.***

Keywords: DDoS, IP Spoofing, TCP/IP, IDS

1. Introduction

The rapid improvements in the intrusion events for LAN as well as for the internet have compelled many organizations to implement security techniques against these threats. The Internet Protocol is actually responsible for providing stable services for the delivery of information across the internet. The information's presented by these IP packets will be based on the TCP/IP layers. The IP datagram will have a header which will have the source details for the network that is to be forwarded to the IP datagram destination. The details that are carried by IP header are time to live, source and destination addresses, types of service and others relevant information. The attackers usually make use of the information in the header to send and receive the information over the network. Intrusion Detection Systems can be considered as tools for managing the vulnerabilities and threats in the ever changing network environment. Here by the word threats we mean people or groups who have the potential capabilities so as to compromise some other computer systems [4]. These may be a discontented employee, an inquisitive teenager, or spy or hacker from an opponent company or any foreign government. Attacks on network computer system could be devastating, affect networks, and corporate establishments. It's requiring to provide and curb these attacks and Intrusion Detection System helps to identify the intrusions. By not using NIDS, to monitor any network activity will result in an irreparable damage to an organization's network. As we know intrusion attacks are said to as "those attacks in which an attacker enters your network to read, damage, and/or steal your data" [1].

These attacks can be sub divided into two categories: pre intrusion activities and the actual intrusions. In this paper, we propose an effective method for preventing IP spoofing attacks based on trusted network.

By the mutual cooperation among trusted adjacent nodes and trace route, our proposed method can detect and block the intruder from external network, which intrudes trusted network by IP spoofing attack. Additionally, for the case that only the local security system is run, because the trusted adjacent node monitors cooperatively the generating external attacks in the local node, the method can effectively reply IP spoofing attack.

Currently the IDS make use of two basic intrusion detection approaches.

a. Anomaly based Detection
b. Signature based Detection

In anomaly based detection approach, it is used to manipulate the relation between the current behavior of the TCP/IP and the profile. It also determines the difference between profiles and detects possible attack attempts. In signature based detection approach, it is used to detect unclear and ambiguous actions by analyzing and describing the action patterns such as time, text, password etc.

In this paper, we propose a technique which includes trace route model with trusted nodes and packets in StackPMi marked to identify the valid packets with their IP addresses. The rest of paper is organized as follows: section 2 reviews related work , section 3 describes network architecture model and section 4 discuss the proposed method with packet marking techniques and its analysis and finally concluded in section 5.

2. Related Work

Recently, the researchers conducted numerous studies in order to describe the basic architecture and the implementation of techniques for detecting and manipulating the general spoofing activities over network.

However, many researchers has [3] explained the Probabilistic Agent-Based Intrusion Detection (PAID) system. These systems were indented to perform specific intrusion detection task by use of cooperative agent architecture. PAID also helps to other agents to share the probability distribution of an event occurrence. A basic framework to investigate the cooperative and prospective adaptive defense mechanisms against the common Internet attacks was proposed in an earlier study. That suggested approach was based on the multi agent modeling and simulation. This framework basically represents the attack as interacting teams of intelligent agents that act under some adaptation criterion which creates some confusion for the administrator who is not that much experienced. This method also adjusts their behavior and configuration in compliance with the network conditions and attack (defenses) severity [6].

However, a study reported the design and evaluation of the Cousteau system, with the route-based filtering (RBF). This design was an effective one and provides practical defense against IP spoofing. Since RFB process critically customize on the accuracy of the IP layer information that used for spoofed packet detection. The inference process as described by them is "resilient to subversion by an attacker who is familiar with Clouseau" [8].

A study presented a model and architecture for enhancing the current signature detection approach based on intrusion. Spoofing the source IP address of packets on the internet is one of the major tools used by hackers to launch DDoS attacks. In such attacks, the attackers forge the source IP of packets that are used in the attack by using an arbitrary IP address which is selected either randomly or intentionally.

In the paper [4], they present a spoofing prevention method by which routers on destination networks can detect and filter out spoofed packets. Each packet leaving a source network is tagged with the key, once it arrives at destination network, the
routers verify the key to decide if the packet is discarded.

The authors [5] discuss attacks using spoofed packets and variety of methods for detecting spoofed packets. These include both host-based methods and the more commonly discussed routing-based methods. The scheme [6] provides more flexible features to trace the IP packets and can obtain better tracing capability and it only needs moderately a small number of packets to complete the trace back process and requires little computation work.

The paper [7] also proposes an IP trace back method (TNA) to identify the true IP address of a host originating attack packets by checking the source IP address filed of an IP packet. But special tracing equipment should be deployed at some point in the network. IP2HC scheme [8] proposes a detection method of the spoofed packets based on the hop count filtering. The legal packet can be find out by analyzing the number of hops that packet gone through before reaching at the destination because attacker cannot control hop count. But for maintaining IP2HC mapping table, more memory overhead is needed.

3. Network Architecture Model

In this section, we propose an effective method for defense against IP spoofing attack based on traceroute and the cooperation with trusted adjacent nodes. By this method, we can effectively detect and prevent IP spoofing attack.

3.1 Network Architecture with Trusted Nodes

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). We first propose the network architecture based on trusted adjacent nodes, which is shown as Fig. 1. In this network, each trusted node has access authority of others. Only these nodes can access each other, namely they are restricted access authority. We call these nodes as trusted nodes, where each trusted node has access information of the other trusted nodes, such as node name and IP address, hop count and trace route from itself to the other trusted nodes. In figure (1), six trusted nodes include node A, B, C, D, E and F. The network can is used for campus network or enterprise network and these nodes can be scattered in different geographical location. After the trusted node passes IP authentication, the node can access each other, which is denoted as: A={B, C, D, E, F}, B={A, C, D, E, F}, and so on. Figure (2) shows the detailed network structure with routers, Nodes of R1-R9 are the routers which connect with the trusted nodes.

Because we restrict the access authority, the user from outer can be identified by IP authentication. But if it intrudes the network by disguising IP address of a trusted node, it is difficult to be distinguished by IP authentication. In this paper, we are mainly focused on how to identify the attack by disguising the IP address of trusted node, namely IP spoofing attack.

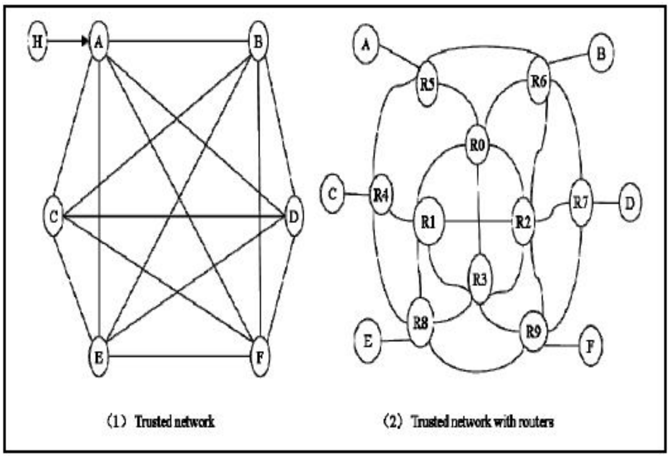

Figure 1: Network Architecture with Trusted Nodes

3.2 Scenario of IP Spoofing Attack

For explaining the proposed defense method well, we first introduce the process of IP spoofing attack. In Fig. 2, node A and node B are considered as trusted nodes. According to three-way- handshakes [10], if a hacker intrudes trusted node B by disguising IP address of another node A, it must firstly attack and control the node A, then blocks it from connecting with internet. Next, it sends a TCP SYN connection request to node B by disguising IP address of node A, after node B receives the request, node B sends a SYN-ACK to node A, but node A can not receive the message actually. Once the hacker gets the SeqNo (sequence number), it can send ACK to B again, the connection is established between the hacker and node B, IP spoofing attack comes true.

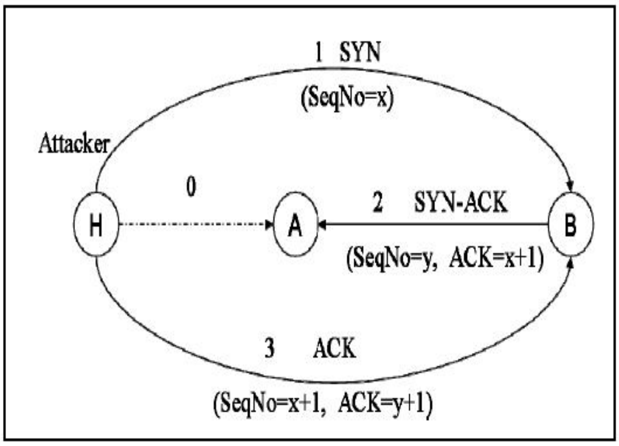

Figure 2: Scenario of IP Spoofing attack

3.3 Trace-route Model

According to the process of IP spoofing attack, we proposed the model of traceroute. As shown in Fig. 2, we suppose that node H is attacker, node A is source node and node B is victim/target node. When attacker H attacks node B by disguising the IP address of node A, on the third step of three-way handshake, attacker H will intercept the acknowledgement from victim node B to node A. So we cannot detect IP spoofing attack by trace-route from victim node B to source node A directly.

But in the network, these nodes can cooperate with each other. So the victim node gets help from other trusted nodes, IP spoofing detection can be implemented. Fig. 3 shows the model of trace-route model. Here, node C is a trusted adjacent node of node B, and we call node C as detection node. When source node A sends access request to target node B, we trace the route to node A with the help of detection node C. If the attacker H has controlled the node A, when we trace the route in hop-by-hop from IP address of node C to IP address of node A, the trace-route result is "host unreachable", otherwise, in normal access status, source node is reachable.

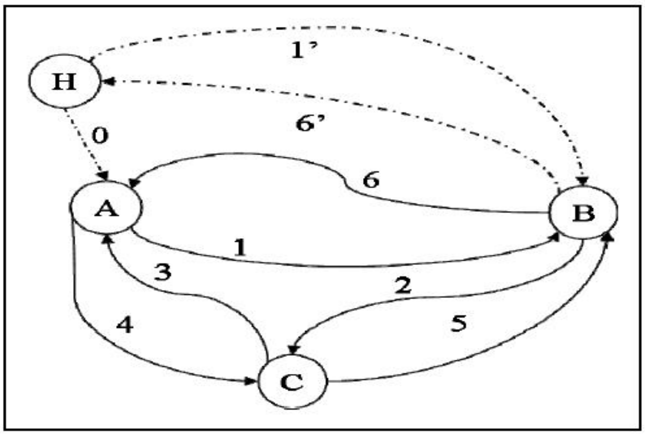

Figure 3: Trace route of Trusted Nodes in Network

4. Proposed Algorithm And Analysis

Based on the network architecture with trusted adjacent nodes information and the model of trace-route, we propose the system model. In this paper, we propose an spoof detection can be done with trusted nodes as well as the marking technique discussed in [9]. It prevents IP spoofing by marking the packets which are transferred over communication channel. The basic packet marking scheme is as shown in Figure 4,

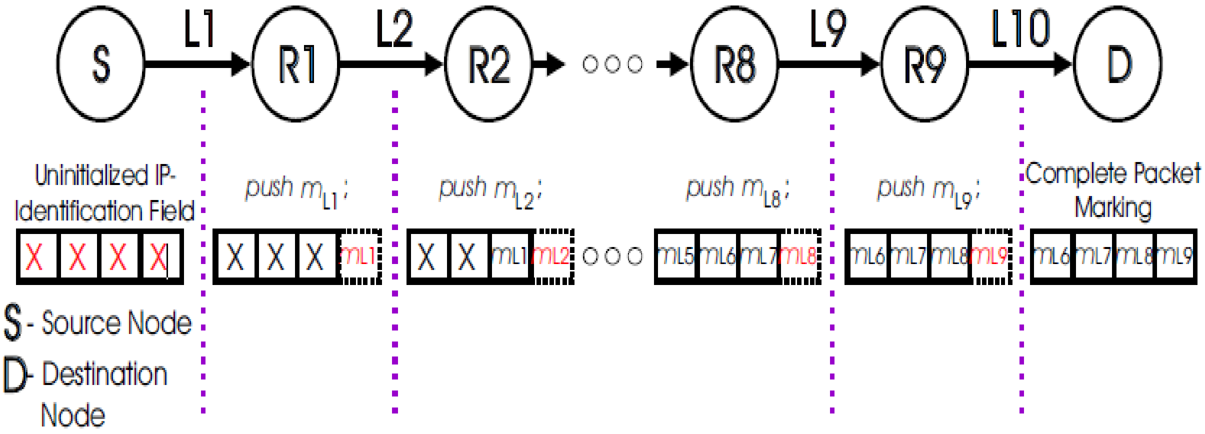

Figure 4: Basic Packet Marking scheme

Spoof detection is the main algorithm. In lines 2-5, the function variables are initialized with the set of routers that are currently connected to the judge router, the set of IP addresses assigned to each of the access routers and the set of probes that *JR* sent in previous monitoring times. In lines 6 - 9, *JR* receives packets for the monitoring period.

□*x* and the algorithm *analyze packets* is called to detect attacks related to scenario 2. The trust values for the access routers are calculated in lines 11 - 14. Lines 15 – 17 call the algorithm that performs detection and trust assessment related to the attacks in scenario 3.

Finally, lines 18 - 20 detect and calculate trust for scenario.

```
IR$_X$:=the set of the IP addresses assigned to access router x
PR:=the set of all the active probes
$Ar_i$ is the ith element in AR
While(Tx>0)
For each received packet p with mark
Analyze_packets(p ,p{i},p_Interface);
End for
End while
For each element $Ar_i$ in AR
If($Ar_i$. Packets>0)
    Calculate_trust($Ar_i$, $Ar_i$. Packets, $Ar_i$. Valid);
End for
For each interface $Ar_i$ in AR
Compare_packets($Ar_i$ );
End for
For each interface $Ar_i$ in AR
No_packet_received($Ar_i$ );
End for
     End Spoof_detection
```

4.1 Explanation of Algorithm

Because of the finite size of our marking field, a StackPi mark with n = 2 for each router will only capture information from the last 8 hops of a path. Since routers local to the victim do not usually add useful path information, but erase distinctive markings from routers further away; we propose that the local routers do not perform StackPi marking on packets destined for the victim. Figure 3 shows that on average, most path lengths are between 10 to 15 hops. Usually, local routers constitute 2 to 5 hops (from sample traceroutes we performed to large web-servers). So choosing n=2 for our marking scheme is likely to include the marks from routers close to the origin of the attacker network, provided that local routers do not mark.

4.2 Analysis

Another important issue is the interaction of StackPi with legacy routers that do not implement the marking scheme. Because only StackPMi enabled routers will mark bits into the marking field, any legacy routers.

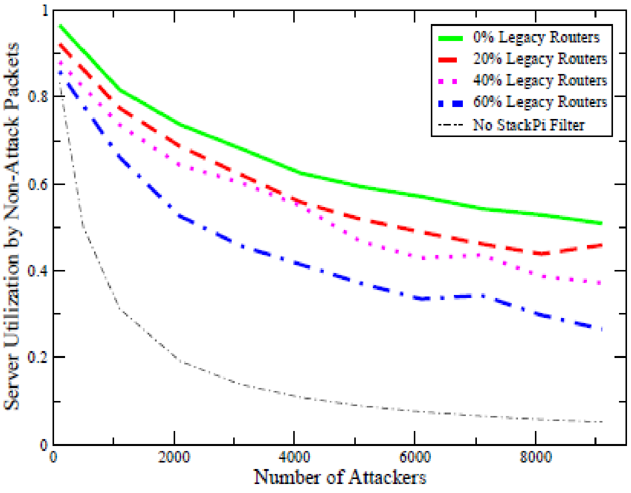

Figure 5: Server utilization by legitimate users under processing constraint and a varying percentage of legacy routers using the Internet

The metric that best quantifies the performance of the StackPMi-IP filter is the probability that a randomly selected attacker will be able to spoof an IP address that will be accepted by the victim. The figure 5 illustrates server utilization by legitimate users under processing constraint and a varying percentage of legacy routers using Internet map. The only way for this to happen, is for an attacker to spoof the IP address of an end-host that happens to have the same StackPMi mark as the attacker itself.

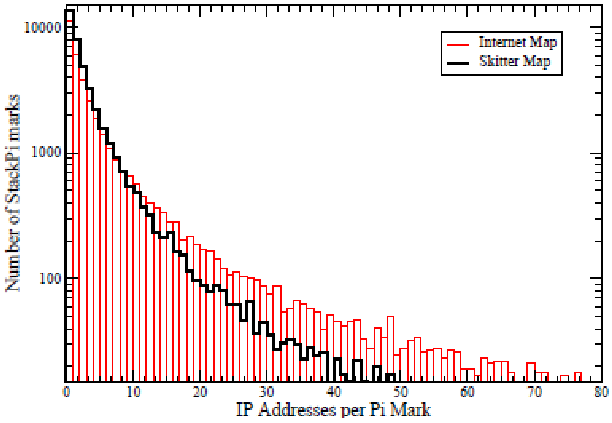

Figure 6: Histogram of the frequency of StackPi marks with a particular number of IP addresses that map to them.

This is hardest for the attacker when the IP addresses of end-hosts in the topology are distributed uniformly over the possible StackPi marks, because no StackPi mark has a large number of IP addresses that map to it and thus there are fewer IP addresses for that StackPi mark that will be accepted by the filter.

In this experiment, each end-host in the topology sends 10 packets with non-spoofed source IP addresses for the victim to bootstrap its filter. Figure 6 shows a histogram of the number of StackPMi markings with a particular number of unique IP addresses that map to them (note that the y-axis is logarithmic), after the initial 10 packets have been sent. The histogram shows us that the IP addresses are somewhat uniformly distributed over the possible StackPMi marks, with the large majority of StackPi marks having 1 to 4 unique IP addresses that map to them and very few StackPi marks with greater than 20 unique IP addresses that map to them.

5. Conclusion

In this paper, we present StackPi, a novel approach to defending against DDoS and IP spoofing attacks. The StackPi defense is split into two parts: StackPi marking and StackPi filtering. The StackPMi marking scheme defines how the routers along a packet’s path create a deterministic marking in the packet such that each packet traversing the same path has the same marking. StackPMi marking includes a write-ahead method whereby some legacy routers’ markings can be included in the StackPi mark. The StackPMi filter defines how an end-host utilizes the packet markings to filter out attack traffic.

6. Future Work

In the future work, There are many extensions to StackPi that have yet to be explored, such as variable bit marking and the application of machine learning techniques to StackPi filtering, that promise to make StackPi a critical deterrent to today’s most common Internet attacks. More Mechanisms to be need to be applied to the security aspects.

7. Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”.

References

[1] L. Garber, "Denial-of-service attacks rip the Internet," IEEE

[2] Computer, vol. 33, pp. 12–17, April 2000.

[3] T. Baba and S. Matsuda, "Tracing network attacks to their sources," IEEE Internet Computing, vol. 6, pp. 20–26, 2002.

[4] Adrian Perrig Dawn Song Abraham Yaar “StackPi: A New

[5] defense Mechanism against IP Spoofing and DDoS Attacks” published as TR-CS-CMU,2003.

[6] S. J. Templeton and K. E. Levitt, "Detecting spoofed packets," DARPA Information Survivability Conference and Exposition, vol. 1, pp. 164–175, April 2003

[7] Y. Xiang and W. L. Zhou, "Trace IP packets by flexible deterministic packet marking (FDPM)," Proceedings IEEE Workshop on IP Operations and Management, pp. 246–252, 2004.

[8] Bremler-Barr and H. Levy, "Spoofing prevention method," 24th Annual Jiont Conference of the IEEE Computer and Communications Societies, vol. 1, pp. 536–547, March 2005.

[9] K. Xu, Z. Zhang, and S. Bhattacharya. "Profiling Internet Backbone Traffic: Behavior Models and Applications," Proc. of ACM SIGCOMM, Philadelphia, PA, USA, pp. 169–180, August 2005.

[10] S. H. Lee, H. J. Kim, J. C. Na, and J. S. Jang, "Abnormal traffic

[11] detection and its implementation," The 7th International Conference on Advanced Communication Technology, vol. 1, pp. 246–250, 2005.

[12] Soule, K. Salamatian, and N. Taft, "Combining Filtering and

[13] Statistical Methods for Anomaly Detection," Internet Measurement Conference 2005, Research, pp. 331–344, 2005.

[14] B. Mopari, S. G. Pukale and M. L. Dhore, "Detection and defense against DDoS attack with IP spoofing," International Conference on Computing, Communication and Networking, 2008, pp. 1-5, Dec. 2008.