Robust IP Spoof Control Mechanism Through Packet Filters

S. Sri Harsha Naresh Reddy[1], S. Tulsi Prasad[2]

[1]M.Tech (CSE), Dept. of Computer Science & Engineering, Chaitanya Engineering College Visakhapatnam, A.P., India.

[2]Assoc.Professor, Dept. of Computer Science & Engineering, Chaitanya Engineering College Visakhapatnam, A.P., India.

Abstract - **A new approach for detecting spoofed IP level, called IP Spoofing Detection Approach (ISDA), is proposed. The purpose of this approach is maximally to keep effective parts and remove forged parts of Source IP addresses under flooding attacks and dynamically configure flow aggregation scheme for flow-based network Intrusion detection to build the most effective intrusion detection approach. With the wide usage of internet in many fields, networks are being exposed to many security threats, such as distributed denial of service (DDoS) attack, worm/virus, and so on. So prevention failure of network security leads to the revealing of information or interruption of network services, thereby results in the enormous economic loss. In this paper, we propose an effective method for defense against IP spoofing attack, which is based on trace route and the cooperation with trusted adjacent nodes. IP Spoofing is a problem without an easy solution, since it's inherent to the design of the TCP/IP suite. Understanding how and why spoofing attacks are used, combined with a few simple prevention methods, can help protect your network from these malicious cloaking and cracking techniques.. Intrusion Detection System (IDS) has been used to secure these environments for sharing their data over network and host based IDS approaches. The rapid improvements of intrusions in internet and other networks are the main factors responsible for the propagation of different threats and vulnerabilities in the computing environment. Now a days the Ids makes use of the signature based detection approach which detects the actions based on analyzing the patterns such as text, password, time etc. We present the results of the experiment, compare the method with others. The result demonstrates that the method can effectively and steadily detect the IP spoofing attack, thereby blocks it.**

Keywords **– ISDA, DDoS, IP Spoofing, TCP/IP, IDS.**

I. 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. The first one is an

anomaly based detection approach that 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. The Second one is signature based detection approach, which is used to detect unclear and ambiguous actions by analyzing and describing the action patterns such as (time, text, password etc).

The below figure shows the online environment workflow for our improved EADS. The sharing of data over these environments actually represents the technique used by IDS for securing IP datagram while transferring data from one environment to another. As we know that many architectures and protocols for LAN and Host based IDS were designed without considering the possibility of other threats attack. Currently, the existing mechanisms of defence against such attacks in host network are not so effective to analyze and detect the unknown attacks because of the differences in their characteristics.

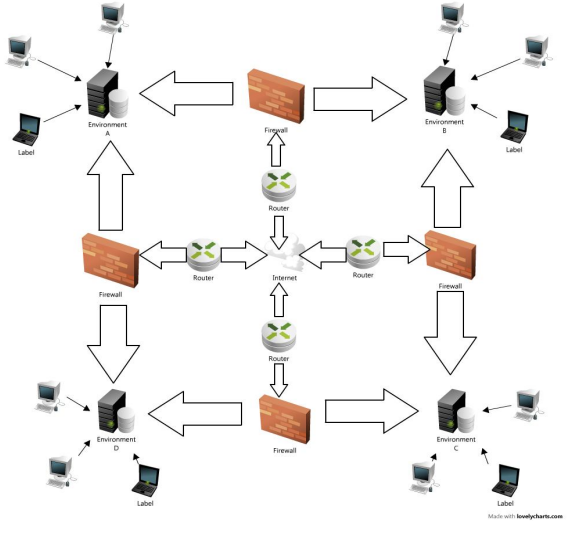

Figure 1. Online environment workflow

These environments need to have secure systems to detect and eliminate the external and internal attacks from other attackers over LAN and Host based IDS. As we know that the environments are constantly changing introduces some new threats and unknown attacks so the intrusion detection system has been made use of to secure and support these environments for sharing their data over networks. Together with that the IP spoofing over online environments presents different patterns and follows the exceptional behaviors based on attacker's techniques which are a major concern with the deployment of new technique for detecting and eliminating the unknown threats attacks during the time of data sharing. The major disadvantages that have been detected in using the commonly used the signature based detection approach are the basic difficulties in updating in formations needed, the second one is with the maintenance of the IDS that is necessarily correlated with detecting of and analyzing the security holes or vulnerabilities, the attack knowledge is operating environment dependent, and the lack of information on user privileges, unable to detect unknown novel attacks and attack signature structure. Together with these there is a lack of detecting and describing the new IP spoofing patterns based on signature detection approach, such as random spoofing or by spoofing a set of addresses consistently or spoofing a small address based on the attackers moves from set to another and etc. So, we proposed an improvement in the current detection techniques for IP spoofing over online environments based on signature detection approach. Actually this paper proposes an enhancement in the current detection approach in terms of exception agent or the virtual agent system to examine and analyze the network traffic packets over multiple online environments by adding a behavioral detection also. In addition, this paper will follow the classification of intrusion detection system and implementation of the new scanning technique rather that the content scanning and the context scanning.

II. 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 can not control hop count. But for maintaining IP2HC mapping table, more memory overhead is needed.

III. PROPOSED METHOD FOR DEFENSE AGAINST IP SPOOFING ATTACK

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.

A. Network Architecture with Trusted Nodes

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.

B. The process 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- hand shakes [9], 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.

C. The Model of Traceroute

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 can not detect IP spoofing attack by traceroute 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 traceroute 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 traceroute result is "host unreachable", otherwise, in normal access status, source node is reachable. We describe the process of traceroute as Fig. 4.

D. Proposed System Model

Based on the network architecture with trusted adjacent nodes information and the model of traceroute, we propose the system model. Fig. 5 shows its architecture and we describe the model as follows in detail.

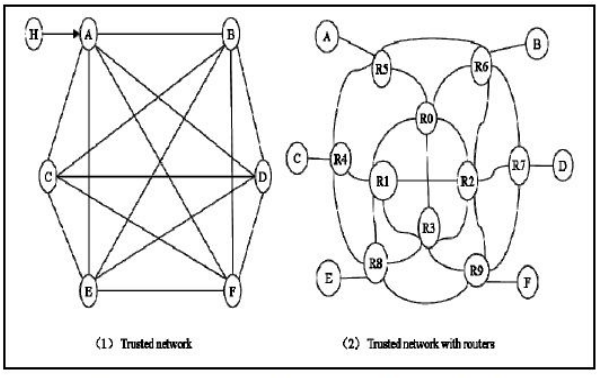

Figure 1. Network architecture with trusted nodes

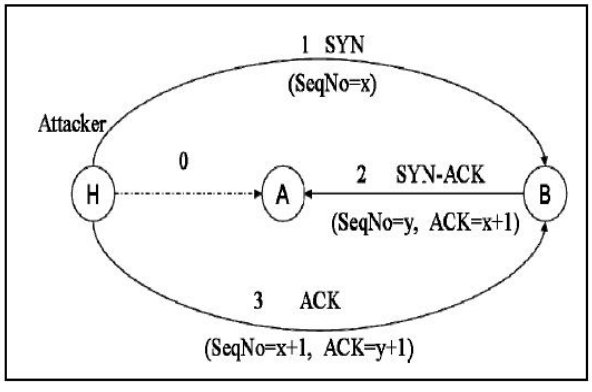

Figure 2. The process of IP spoofing attack

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
Analyze_packets(p,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

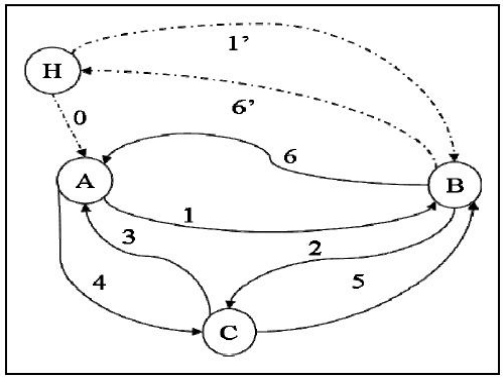

Figure 3. The model of traceroute

1. Source node A sends normal access request to target node B, or attacker H sends request to victim node B by disguising IP address of A;
2. After node B receives the request, node B sends traceroute request to detection node C;
3. Node C traces the route information from node C to node A;
4. Node C gets traceroute result (reachable or unreachable);
5. Node C informs the traceroute result to node B;
6. If (host reachable) node B accepts the access of node A, else node B blocks the attacker;
7. If (IP spoofing) node B sends alarm information.

Fig.4. The process of traceroute.

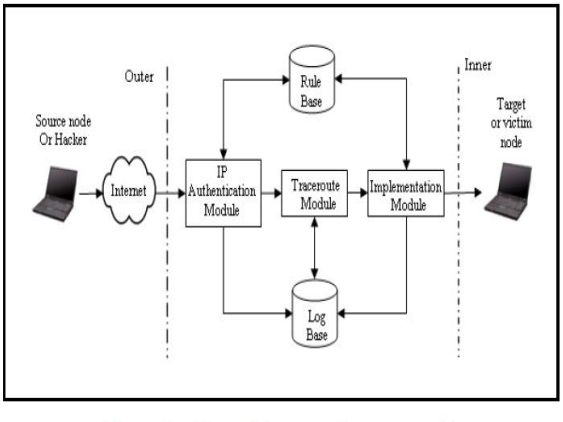

Figure 5. The architecture of system model

1) IP Authentication Module

Based on trusted network architecture, only the trusted nodes can be accessed each other. This module is used to judge whether source host is a trusted node. The information of IP authentication includes node name, node IP address, hop count from itself to target node. When a node requests access, the information is compared with that of rule base. Only when the user pass the IP authentication, it is considered as an trusted node, Otherwise the user is considered as an node from outer site, then the other authentication method will be used.

2) Trace route Module

In this module, we implement the trace route from detection node to source node. If source host is trusted node, the result information of trace route is "host reachable", otherwise, when IP spoofing attack occurs, the result information is "host unreachable". At the same time, the rule base and log base will be updated dynamically. The result of trace route is sent to the implementation module.

3) Implementation Module

Implementation module receives the result from the above two modules, and implement it. If IP authentication is illegal or IP spoofing attack occurs, the node is blocked. Otherwise, source node is permitted to access destination node. In order to further describe the method, the system flow chart of IP spoofing prevention method is shown as Fig. 6.

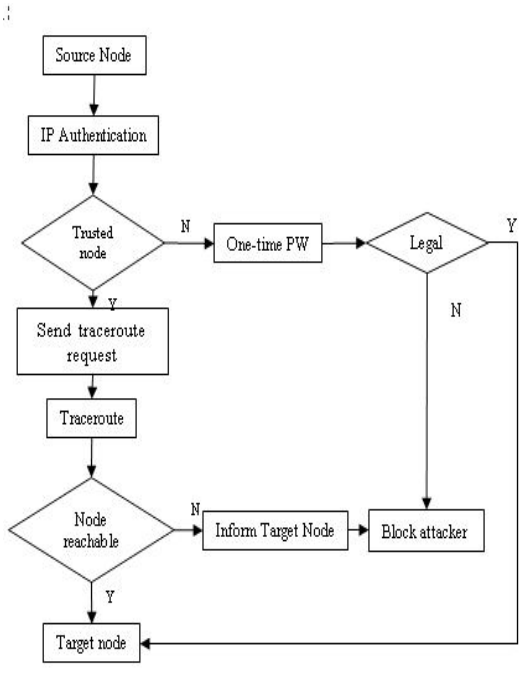

Figure 6. Flow chart of prevention system

IV. SIMULATION AND RESULT ANALYSIS

We simulate the experiment by using winsock programming. We implement the detection of IP spoofing attack by mutual cooperation with trusted computers. The database used in this experiment includes two data tables (Access Rule Base), which are shown as the follow:

- Node Information Table (node name, node IP, hop count), which is used for storing the information of trusted nodes.
- Route Information Table (node IP, SeqNo, HopIP), which is used for storing the trace-route information hop-by-hop from detection host to source host.

We first implement the testing in external network, which includes the status of normal access and IP spoofing attack. According to the model of traceroute, we trace the route information in hop-by-hop from detection node to source node or controlled node. Fig. 7 and Fig. 8 show the traceroute information in the status of normal access and abnormal access respectively. Here, IP address of detection node is 211.35.79.254 and that of source node is 210.125.186.29. The geographical positions of detection node and source host are in Seoul, and Jinju, Korea respectively. From Fig. 8, we find that hop count of traceroute is 14, the result of detection is unreachable when IP spoofing attack occurs. Moreover, we compare our proposed method with the method of TNA, which is shown as table 1. From this table, the trace time of our

proposed method is less than that of TNA. Additionally, table 2 shows the evaluation with other methods.

V. CONCLUSION AND FUTURE WORK

In this thesis, we propose an effective method for defense against IP spoofing attack in the network structure with trusted nodes. By trace route and the cooperation with the trusted nodes, we implement the detection and prevention of IP spoofing attacks. The experiment result demonstrates that the method can effectively and steadily detect the IP spoofing attack, thereby block it. Above all, the scheme is only implemented by software method, does not depend on some additional hardware. Secondly, we propose a cooperation model of trace route with the help of trusted adjacent node. Thirdly, rule base can be updated dynamically. In the future work, we consider how to further analyze the method of trace route and how to analyze packet information better.

NodeIP	SeqNo	HopIP
210.125.186.29	1	211.35.79.254
210.125.186.29	2	99.99.99.99
210.125.186.29	3	202.136.122.13
210.125.186.29	4	211.35.65.231
210.125.186.29	5	124.139.129.85
210.125.186.29	6	219.253.5.81
210.125.186.29	7	219.253.1.13
210.125.186.29	8	219.253.1.42
210.125.186.29	9	59.18.54.69
210.125.186.29	10	118.38.152.109
210.125.186.29	11	118.38.152.110
210.125.186.29	12	222.97.21.222
210.125.186.29	13	121.156.18.130
210.125.186.29	14	210.125.186.29
Reports: Traced host of 210.125.186.29 reachable.		

Figure 7. Normal trace route

NodeIP	SeqNo	HopIP
210.125.186.29	1	211.35.79.254
210.125.186.29	2	99.99.99.99
210.125.186.29	3	202.136.122.21
210.125.186.29	4	211.35.65.231
210.125.186.29	5	124.139.129.85
210.125.186.29	6	219.253.5.81
210.125.186.29	7	219.253.1.13
210.125.186.29	8	219.253.1.42
210.125.186.29	9	59.18.54.69
210.125.186.29	10	118.38.152.109
210.125.186.29	11	118.38.152.110
210.125.186.29	12	222.97.21.222
210.125.186.29	13	121.156.18.130
**** Reports: Traced host of 210.125.186.29 unreachable.		

Figure 8. Abnormal trace route

REFERENCES

[1] 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.

[2] S. H. Lee, H. J. Kim, J. C. Na, and J. S. Jang, "Abnormal traffic detection and its implementation," The 7th International Conference on Advanced Communication Technology, vol. 1, pp. 246–250, 2005.

[3] A. Soule, K. Salamatian, and N. Taft, "Combining Filtering and Statistical Methods for Anomaly Detection," Internet Measurement Conference 2005, Research, pp. 331–344, 2005.

[4] A. 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.

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

[6] 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.

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

[8] I. 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.

[9] L. Garber, "Denial-of-service attacks rip the Internet," IEEE Computer, vol. 33, pp. 12–17, April 2000.