Checksum Based Centralized Management Framework for Internal Intrusion Detection and Prevention

Ankitha K
Department of CSE
Sahyadri College of Engineering & Management

A P Manu
Department of ISE
Sahyadri College of Engineering & Management

***Abstract*—With the wide usage of internet in many fields, networks are more exposed to attacks such as distributed denial of service (DDoS) attack, IP Spoofing, worm/virus, and so on [2]. Therefore, awareness of net attacks is vital. Intrusion Detection and Prevention Systems (IDPS) are security systems that are used to detect and prevent security threats in the network. IP spoofing is one of the attacks in the network. It is a technique used to gain unauthorized access to computers, whereby the interloper sends messages to a system with associate IP address indicating that the message is returning from a trustworthy host. In proposed system an effective method for defense against IP spoofing is used, which is based on checksum and the cooperation with centralized checksum verification server. The protocol is designed at application layer to detect and prevents the intruder who is spoofing an IP address of another system. The expected result is to demonstrate the method that can effectively and steadily detects and prevents the IP spoofing attack, there by verifying checksum and block.**

Keywords—Checksum, Router, IP Spoofing

I. INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. IP spoofing is one of the most significant threats to the security of the Internet. Spoofing is a technique used to gain unauthorized access to computers, wherever by the aggressor sends messages to a client with an IP address indicating that the message is returning from a trusty host. IP spoofing poses an increasingly grave threat to the Internet [1]. In spoofing, associate aggressor will hide its actual identity and use others identity to send data, rendering source-based packet filtering less effective. The vulnerability and security deficiency of the TCP/IP suite brings the initiating information processing spoofing attacks on simply; nevertheless it's extraordinarily laborious to defend against them.

There are a few variations on the types of attacks that using IP spoofing. Spoofing is classified as following [12]:

1. Non-blind spoofing
   This attack takes place once the wrongdoer is on a similar subnet because the target that would see sequence and acknowledgement of packets.
2. Blind spoofing
   This attack might occur from outside wherever sequence and acknowledgement numbers area unit unreached.
3. Man in the Middle Attack
   Packet sniffs on link between the two endpoints, and might fake to be one finish of the affiliation.
4. Denial of Service Attack
   Attackers are involved with overwhelming information measure and resources by flooding the target with as several packets as potential in an exceedingly short quantity of your time.

In normal data forwarding traffic (figure1), the source sends the data to destination through intermediates with its own IP address.

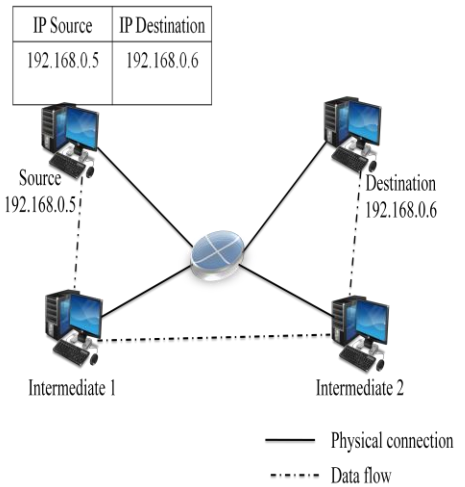

Figure 1 Normal network traffic

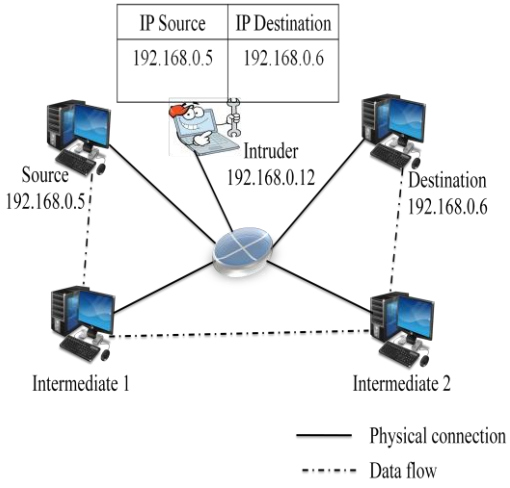

Figure 2 IP spoofing

The figure 1 shows a normal traffic between source (192.168.0.5) and destination (192.168.0.6) through intermediate1 and Intermediate 2. When intruder inject data with spoofed source addresses into the intranet, intermediate nodes forward those data to the destination just like any other data—often without checking whether the data is from trustworthy or not. These spoofing consume network information measure on the way to their destinations, and they usually a part of some malicious activity, like a Denial of Service (DoS) attack, man within the middle attack, Blind spoofing etc. The figure 2 shows network traffic with IP spoofing. The IP address of an intruder is 192.168.0.12. Intruder spoof the IP address of source (192.168.0.5) and send the data to destination (192.168.0.6) with an IP of 192.168.0.5. Destination receives the data with sender IP address as 192.168.0.5, but data is actually sent by the intruder (192.168.0.12).

IP Networks are vulnerable to source address spoofing, by using a raw socket to fill arbitrary source IP addresses into packet headers [12]. IP spoofing attack consists of following steps [2]:

- Selecting a target host (or victim),
- Identify the host that has a trust relationship with a target host,
- The trusted host is then disabled and the target's TCP sequence numbers are sampled,
- The trusted host is then impersonated, the sequence numbers forged,
- A connection attempt is made to a service that only requires address-based authentication (no user id or password).

Thus, the mechanism is to present a schema to detect and prevent the internal intruder using checksum. The proposed system seeks to assist organizations in understanding Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) and also provides the facility to detect the malicious nodes or systems.

The proposed system uses predefined path for packet transmission. A protocol is designed at application layer, where it inserts a checksum to each forwarding data at every system. The destination system is intimated by the centralized checksum verifier about the received message status i.e. whether the received message is from trust worthy or not.

IP spoofing is the creation of data using somebody else's IP source addresses and sending to the destination. IP spoofing accompanies many security attacks, such as flooding, Denial of Service (DoS) and vulnerability scanning, and hinders the design of simple, cost-effective defenses. Finding an IP spoofing attack is a difficult task. The aim is to design a framework to detect internal intrusion and develop a prevention system in the Local Area Network (LAN) using centralized checksum based mechanism.

II. RELATED WORK

V.K Soundar Rajam and S. Mercy Shalinie proposed a scientific trace back mechanism for the outsized scale distributed on-line system [1]. The projected system relies on replication and tolerates capricious failures of servers. The service supported security considerations of server is enforced by science trace back system supported settled packet marking theme. Packet marking approaches generally acquire bit overhead at the routers while exchange some packets to the victim which has to use a marked information at the IP header to reconstruct the attack source IP. Consume more resources, such as memory of routers.

Yunji Ma have proposed a methodology for defense against informatics spoofing attack that is predicated on trace route and also cooperates with trusted adjacent nodes [2]. In this method, only trace the route information by software method to find intruder. Preventing IP spoofing attacks based on trusted network. By the mutual cooperation among trusted adjacent nodes and traceroute, 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.

Manusankar *et al.* proposed a tendency to create use of Associate in nursing improved EADS (Exception Agent Detection System) for creating the header info secures [3]. Packet filtering is one defense against information science spoofing attacks. The entrance way to a network sometimes performs ingress filtering, that is obstructing of packets from outside the network with a supply address within the network. This prevents an outdoor spoofing the address of an enclosed machine. Ideally the entrance way would conjointly perform egress filtering on outgoing packets that is obstructing of packets from within the network with a supply address that's not within. While filtering the packet extra care to be taken so that packets with valid supply addresses should not be discarded. In this paper, there so no procedure or trace back mechanism to take action on the

intruder. Filtering spoofing packets at the edge of network which involves high deployment and maintenance cost.

Bingyang Liu *et al.* proposed a deployable approach for inter-AS anti-spoofing (DIA) [4]. This proposed DIA, embodying all three properties of AS i.e. incremental deployability, high deployment incentives and low deployment cost. The DIA method uses pseudo random number function instead of UMAC, which makes the deployment cost hard to evaluate. There is more memory overhead for maintaining mapping table.

Belenky and N. Ansari proposed a Deterministic Packet Marking (DPM) scheme. In this method Incoming packets are marked; outgoing packets are not marked [5]. The trace back method will be performed post-mortem that permits for tracing the attacks which will not are detected at first. The involvement of the web service suppliers (ISP) is extremely restricted, and changes to the infrastructure and operation needed to deploy DPM are tokenism. DPM performs the trace back while not revealing the interior topology of the provider's network that may be a fascinating quality of a trace back theme. Deterministic Packet Marking is another variation, where a router marks every packet that enters in to a network so there is computational overhead. Consume more resources, such as memory of routing routers.

S. Rubin *et* al. proposed a common signature-based NIDS is to remodel associate attack instance that the NIDS acknowledges into another instance that it misses [6]. For instance, to avoid matching the attack payload to a NIDS signature, attackers split the payload into many transmission control protocol packets or hide it between benign messages. Here attack mechanisms have relied on ambiguities in TCP to develop evasion techniques using overlapping IP fragments, TTL manipulation, and other transformations. In signature based IDPS, the new signature intruder is not recognized, because the signature of the intruder may not be present in the list of predefined signature.

L. Tan and T. Sherwood proposed a string matching architecture for intrusion detection and prevention [7]. Network intrusion detection and bar systems have emerged jointly of the foremost effective ways in which of providing security to those connected to the network, and at the guts of virtually each trendy intrusion detection system could be a string matching rule. String matching is one among the foremost essential parts as a result of it permits for the system to create choices primarily based not simply on the headers, however the particular content flowing through the network. Sadly, checking each computer memory unit of each packet to examine if it matches one among a group of 10 thousand strings becomes a computationally intensive task as network speeds grow into the tens, and eventually lots of, of gigabits/second. to stay up with these speeds a specialized device is needed, one which will maintain tight bounds on worst case performance, which will be updated with new rules while not interrupting operation, and one that's economical enough that it might be enclosed on chip with existing network chips or perhaps into wireless devices.

Kruegel *et al.* [8] proposed achieving high speed intrusion detection by distributing the load across several sensors, using a scatterer to distribute the load and slicers and reassembles' to provide stateful detection. Still other approaches seek to provide better performance by splitting up (and possibly replicating) a sensor onto multiple cores or processors. These approaches show that allocating additional hardware will higher shield large networks with large amounts of traffic; however they're not a cost effective manner of addressing algorithmic quality attacks.

The NIDS cannot invariably confirm what traffic reaches a given host or however that host can interpret the traffic, and attackers might exploit this ambiguity to avoid detection or cause dishonest alarms. U. Shankar and V. Paxson [9] have proposed an active mapping method to actively test each host and derive the policy. Several factors can complicate the mapping in practice. For example, associating an IP address to a host is not one-to one with the use of NAT and DHCP. The active testing may be imprecise due to packet filtering by firewalls or unexpected packet drops on an intermediate router when the traffic volume through it is high. There is more memory overhead for maintaining mapping table.

S.Savage *et al.* [10] described a way for tracing anonymous packet flooding attacks within the web back toward their sender. This work is motivated by the exaggerated frequency and class of denial-of-service attacks and by the issue in tracing packets with incorrect, or "spoofed," sender addresses. 'Probabilistic packet marking within the network' this approach permits a victim to spot the network path(s) traversed by attack traffic while not requiring interactive operational support from Internet Service providers (ISPs). Moreover, this trace back may be performed "post mortem"-after associate attack has completed. Each router deploys a special tracing equipment to store the IP or MAC of forward router.

An advanced method named IDPF (Inter Domain Packet Filtering) has been brought in by Zhenhai Duan *et al* [11]. It is constructed from the information implicit in Border Gateway Protocol (BGP) route updates and is deployed in network border routers; however, this method does not have the strength to handle subnet spoofing address.

III. DESIGN METHODOLOGY

The data travels from source to destination through intermediate systems where every system is connected via router and monitored by a centralized checksum verifier (figure 3). The centralized checksum verifier intimates the destination whether the packet is spoofed or not. Suppose an intruder forge the identity of source and sends the packet to the destination as if it as a source, this spoofed packet is identified by the centralized checksum verifier by

comparing the inserted checksums for each forwarded data. In proposed system the protocol is designed at application layer, which inserts a checksum to each forwarding data. The checksum is inserted to data at source and the inserted checksum is replaced with new checksum at every intermediate system, but each inserted checksum is appended at centralized checksum verifier/centralized server. Centralized checksum verifier is used to verify the each inserted checksum of length six to detect and prevent the intruder. The verified information is provided to the destination. The designed protocol block the intruder further sending spoofed data.

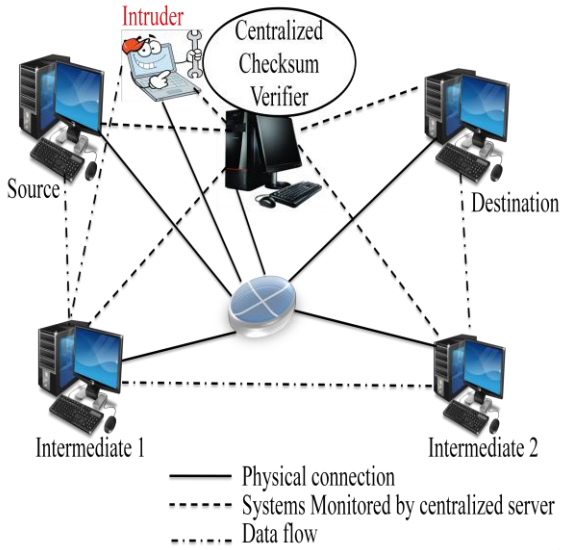

Figure 3 System Architecture

In figure 3, a checksum with the length of six is inserted to data at source end, this checksum is replaced with new checksum of same length at intermediate1, again this checksum is replaced with new checksum of same length at intermediate 2, finally the data is received by the destination with the intimation of intruder by a centralized checksum verifier.

IV. RESULT ANALYSIS

An advanced method named IDPF (Inter Domain Packet Filtering) [11] is constructed from the information implicit in Border Gateway Protocol (BGP) route updates and is deployed in network border routers; however, this method does not have the strength to handle subnet spoofing address.

Each intrusion has its own signature, in signature-based IDPS [6] the signature of each intrusion is compared with predefined signature. In such cases intrusion with the signature which does not match predefined signature is not identified.

The placement of checksum based centralized management framework plays a key role in controlling spoofing-based attacks. The intrusion detection and prevention system is deployed at centralized system. A six bit of checksum is inserted to every forwarding packet but Instead of appending the checksum to data, checksum is replaced with new checksum at every system, these checksums are compared at centralized system to detect intruder. The intruder is blacklisted to prevent the attack. So the obtained result is to provide software to detect internal intrusion and then develop a mechanism to prevent the intruder in LAN.

V. CONCLUSION

The main objective of the proposed system is to identify and prevent the intruder of TCP/IP protocol. The protocol is designed at application layer which inserts the checksum to each forwarding data from source to destination through intermediate system. Every system in the network is monitored by a centralized checksum verifier but no other systems have control over it. The each inserted checksum is verified at centralized checksum verifier to detect and prevent the intruder; destination is intimated by this verifier about intruder. If the IP address is spoofed then the intruder is detected with its original IP address so receiver can take action against it and the intruder is blocked further sending the data and also inserted checksum is replaced with new checksum at each system, because of these the proposed system is efficient scheme to detect and prevent intruder. The proposed system detects and prevents the internal intruder and managed by centralized system. Using distributed system, we can detect and prevent intruder in different domains.

REFERENCES

[1] V.K Soundar Rajam, Dr. S. Mercy Shalinie, "A novel traceback algorithm for DDoS attack with marking scheme for online system", Recent Trends in Information Technology (ICRTIT), April 2012.
[2] Yunji Ma, "An Effective Method for Defense against IP Spoofing Attack in Wireless Communications Networking and Mobile Computing (WiCOM)", Sept. 2010.
[3] Manusankar. C, Karthik. S, Rajendran. T, "Intrusion Detection System with packet filtering for IP Spoofing", Communication and Computational Intelligence (INCOCCI), Dec. 2010.
[4] Bingyang Liu, Jun Bi, Yu Zhu, "A deployable approach for inter-AS anti-spoofing", Network Protocols (ICNP), Oct. 2011.
[5] Belenky and N. Ansari, "Tracing multiple attackers with deterministic packet marking (DPM)", in 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM'03), pp. 49-52, Aug. 2003.
[6] S. Rubin, S. Jha, and B. P. Miller, "Automatic generation and analysis of NIDS attacks", In ACSAC '04, pages 28–38, Washington, DC, USA, Dec. 2004. IEEE Computer Society.
[7] L. Tan and T. Sherwood, "A high throughput string matching architecture for intrusion detection and prevention", In International Symposium on Computer Architecture ISCA, June 2005.
[8] C. Kruegel, F. Valeur, G. Vigna, and R. Kemmerer, "Stateful Intrusion Detection for High-Speed Networks", In Proceedings of the IEEE Symposium on Security and Privacy, pages 285–293, Oakland, CA, May 2002. IEEE Press.

[9] U. Shankar and V. Paxson, "Active mapping: resisting NIDS evasion without altering traffic", In IEEE Symposium on Security and Privacy, pages 44–61, May 2003.

[10] S.Savage, D.Wetherall, Anna Karlin and Tom Anderson, "Network support for IP Traceback", IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001.

[11] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters", IEEE Trans. On Dependable and Secure Computing, Vol. 5, No. 1, March, pp.22-36, 2008.

[12] Michael E.Whitman, Herbert J.Mattord, "Principles of Information Security", 4th edition, CENGAGE learning, 2012