UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

A Survey of Defence Mechanisms against IP Spoofing

Sarita Sahni[1], Pankaj Jagtap[2]

M. Tech Student, SCSIT, DAVV, Indore, India[1]

Lecturer, SCSIT, DAVV, Indore, India[2]

Abstract: IP address spoofing is a serious threat to the legitimate use of the Internet. Many Preventive mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. Attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper a study of methods for detection of IP address spoofing is undertaken. It compares various host based methods such as IPSec, the OS Fingerprinting, TCP probing, SYN Cookies and IP puzzles with router based methods such as ingress and egress filtering, Reverse Path Forwarding (RPF), Router based Filtering (RBF), Spoofing Prevention Method (SPM), Distributed Packet Filtering (DPF), Inter Domain Packet Filtering (IDPF), SAVE, BASE, Hop Count Filtering (HCF), Pi and StackPi on the bases of their performances and effectiveness.

Keywords: Reverse Path Forwarding (RPF); Router Based Filtering (RBF); Spoofing Prevention Method (SPM); Distributed Packet Filtering (DPF); Inter Domain Packet Filtering (IDPF); Path Identification; Stack Path Identification.

INTRODUCTION

The Internet Protocol or IP is used for sending and receiving data over the Internet and computers that are connected to a network. Each packet has header that contain some field like fragmentation, sequence number field, flag including source and destination address.

The source address is normally the address that the packet was sent from. By forging the source address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packet will send response back to the forged address,

In IP spoofing, an attacker gain unauthorized access to computer or network by making it appear that a Malicious message has come from a trusted machine by spoofing the ip address of that machine.

A.IP ADDRESS SPOOFING

IP address spoofing denotes the action of generating IP packets with fake source IP addresses in order to impersonate other systems or to protect the identity of the sender. Spoofing can also refer to forging or using fake headers on emails or Netnews to – again – protect the identity of the sender and to mislead the receiver or the network as to the origin and validity of sent data.

The Internet Protocol or IP is the fundamental protocol for sending/receiving data over computer network and the Internet. With the Internet protocol, each packet sent or received contains information relevant to the operation such as the source and the destination of the packet. With IP address spoofing, the information placed on the source field is not the actual source of the packet. By using a different address in the source field of the packet, the actual sender can make it look like the packet was sent by another computer and thus the response of the target computer will be sent to the fake address specified in the packet – unless the attacker wants to redirect the response to his own computer.
Internet protocol (IP) is a network protocol operating at layer 3 (network) of the OSI model. It is a connectionless model, meaning there is no information regarding transaction state, which is used to route packets on a network. Additionally, there is no method in place to ensure that a packet is properly delivered to the destination.

Using one of several tools, an attacker can easily modify these addresses – specifically the “source address” field. It's important to note that each datagram is sent independent of all others due to the stateless nature of IP and this is the main reason behind ip spoofing. The enhancement in internet protocol from IPv4 to IPv6 has reduced many flaws by addition of features such as IPSec. Ip address spoofing can be classified as a) non-blind spoofing b) blind spoofing c) man in the middle attack d) denial of service attack.

DOI10.17148/IARJSET.2017.4704

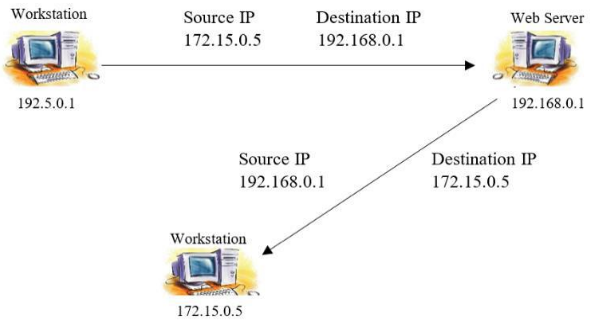

Figure1 Spoofed source address

B. NON-BLIND SPOOFING

This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets. The threat of this type of spoofing is session hijacking and an attacker could bypass any authentication measures taken place to build the connection. This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine.

C. BLIND SPOOFING

It refers to a type of attack using Internet Protocol (IP) spoofing, and may take place outside where sequence and acknowledgment numbers are unreachable. In this situation, an attacker can send several packets to the target computer in order to locate sequence numbers. If the sequence number became vulnerable, data could be sent to the target.
Today, most OSs implement random sequence number generation, making it difficult to predict them accurately. If, however, the sequence number was compromised, data could be sent to the target.

D. MAN IN THE MIDDLE ATTACK

This is also called connection hijacking. In these attacks, a malicious party intercepts a legitimate communication between two hosts to controls the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge. In this way, an attacker can fool a target into disclosing confidential information by spoofing the identity of the original sender or receiver. Connection hijacking exploits a “desynchronized state” in TCP communication. When the sequence number in a received packet is not the same as the expected sequence number, the connection is called “desynchronized.” Depending on the actual value of the received sequence number, the TCP layer may either discard or buffer the packet. When two hosts are desynchronized enough, they will discard/ignore packets from each other. An attacker can then inject forged packets with the correct sequence numbers and potentially modify or add messages to the communication. This requires the attacker to be located on the communication path between the two hosts in order to replicate packets being sent. The key to this attack is creating the desynchronized state.

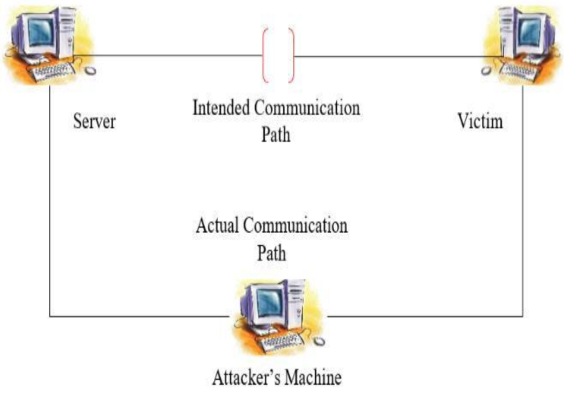

Figure2. Man in the middle attack

E. DENIAL OF SERVICE ATTACK

IP spoofing is almost always used in denial of service attacks (DoS), in which attackers are concerned with consuming bandwidth and resources by flooding the target with as many packets as possible in a short amount of time. To effectively conducting the attack, attackers spoof source IP addresses to make tracing and stopping the DoS as difficult

DOI10.17148/IARJSET.2017.4704

as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic; it is very challenging to quickly block the traffic.
DoS attacks do not result in the theft or loss of information or other assets but can a considerable amount of time and money is lost to recover the victim machine. Broadly, DoS attacks are either flood attacks or crashing attacks. Flood attacks occur when the system receives excessive traffic than its buffer can handle causing it to slow down and eventually stop offering services. Common flooding attacks include buffer overflow attacks, ICMP flood and SYN flood. Other DoS attacks exploit vulnerabilities that cause the target system or service to crash.
Distributed Denial of Service (DDoS) attack is an advanced DoS attack in which the target is attacked from multiple locations at once.

2. CATEGORIES OF ADDRESS SPOOFING DEFENCES MECHANISMS

Spoofing defence solutions can essentially be broken down into three main categories which are shown in Figure 3

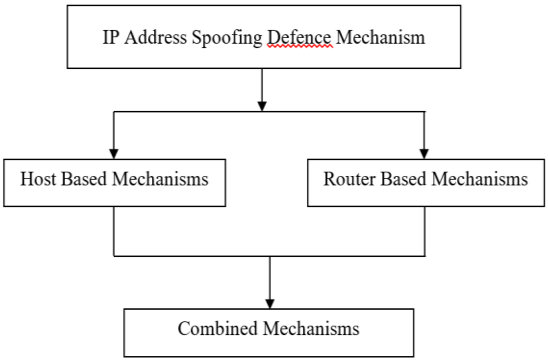

Figure3 Types of IP address spoofing mechanism

Host based mechanisms: As the name implies, the solution is centered on end hosts where an end host identifies the spoofed IP packets. The solution of this type does not depend on the functionalities of router. They are easily deployable and do not need any modification in network infrastructure. However, this type incurs delay in detecting spoofed packet, as the packet has to reach the end host.
Router based mechanism: The Router based mechanisms are implemented on the intermediate routers in the existing infrastructure of the internet. These mechanisms are very complicated in terms of their deployment; however, they show good response by detecting and stopping the spoofed IP packets very quickly before reaching the victim machine.
Combined or Hybrid Mechanisms: it is combination of host and router based mechanism. This mechanism is implemented host as well as router. Their response is far better than router based mechanism but their implementation is very difficult to achieve.

A.HOST BASED DEFFENCE MECHANISM

It can be classified in two categories, active and passive mechanism. Following figure shows the various host based ip address spoofing defence mechanism.

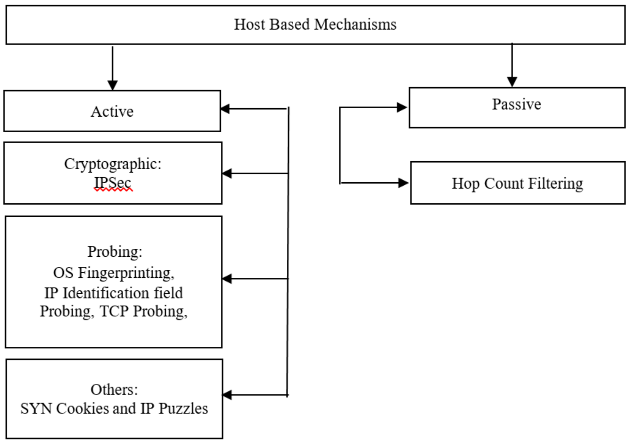

Figure4. Host based IP address spoofing defence

DOI10.17148/IARJSET.2017.4704

IPSec

In computing, Internet Protocol Security (IPSec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys for use during the session. IPSec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host) Internet Protocol security (IPSec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPSec supports network-level peer authentication, data-origin authentication, data integrity, and data confidentiality (encryption), and replay protection.

The main objective of IPSec is to achieve confidentiality, integrity, and privacy and to prevent data from spoofing. Its use is optional in ipv4 and also it faces deployment problem on incompatible operating system.

OPERATING SYSTEM FINFERPRINTING

OS fingerprinting is the process of determining the operating system used by a host on a network. Probing tools such as NEMSIS, NMAP etc can be used to determine the operating system of a node.

NMAP OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then NMAP listens for responses. Dozens of attributes in those responses are analyzed and combined to generate a fingerprint. Every probe packet is tracked and resent at least once if there is no response. All of the packets are IPv4 with a random IP ID value. Probes to an open TCP port are skipped if no such port has been found. For closed TCP or UDP ports, NMAP will first check if such a port has been found. If not, NMAP will just pick a port at random and hope for the best.

IP IDENTIFICATION PROBING

When a sending host finds a suspicious IP packet, it can send packets to a supported source to observe response of its identification field. Further, different packets may have sent different IP identification field e.g. some hosts may choose random identification number while other hosts may use ascending or descending order for each packet. Suppose some hosts increment the identification field of each packet then identification field in these probing responses must approach the identification field number of suspicious packets. Otherwise, the suspicious packet is spoofed. However, it is a very complicated procedure and has many complexities involved in its implementation. It may identify spoofed packets only if spoofed source does not use any sophisticated method for packet identification number.

TCP PROBING

Since packet numbering can be easily modified through TCP sequence numbers, therefore, simple TCP handshaking is not a secure procedure. Some OS's use random sequence number generated by some pseudo-random number generation algorithms. However, the algorithm used for pseudo-random number generation may not be truly random in nature. TCP specific probes add an acknowledgement message as another layer for protection. In TCP specific probing, an attacker who sends spoofed packets is unable to receive the replies and instead a receiving host sends acknowledgement with a request to change the TCP window size or packet retransmission request before proceeding further. The receiving host observes the response received from the supposed source. If the supposed source does not change window size or does not retransmit the packets, then recipient host treats the packets as spoofed. TCP Probing can identify early, easily and reliably because attacker is unable to receive TCP control messages and cannot correct them.

SYN PROBING

The SYN cookies technique causes absolutely zero state to be generated by a received SYN. Instead, the most basic data comprising the connection state is compressed into the bits of the sequence number used in the SYN-ACK. Since for a legitimate connection, an ACK segment will be received that echoes this sequence number (actually the sequence number plus one), the basic TCB data can be regenerated and a full TCB can safely be instantiated by decompressing the Acknowledgement field. This decompression can be effective even under heavy attack because there is no storage load whatsoever on the listener, only a computational load to encode data into the SYN-ACK sequence numbers. The downside is that not all TCB data can fit into the 32-bit Sequence Number field, so some TCP options required for high performance might be disabled. Another problem is that SYN-ACKs are not retransmitted (because retransmission would require state), altering the TCP synchronization procedures from RFC 793

IP PUZZLE

The client puzzle approach means that before engaging in any resource consuming operations, the server first generates a puzzle and sends its description to the client that is requesting service from the server. The client has to solve the puzzle and send the result back to the server. The server continues with processing the request of the client, only if the

DOI10.17148/IARJSET.2017.4704

client's response to the puzzle is correct. This is summarized in the following abstract protocol, where C and S denote the client and the server, respectively:

Step 1 C →S: sending service request
Step 2 S: generation of a puzzle
Step 3 S →C: sending description of the puzzle
Step 4 C: solving the puzzle
Step 5 C →S: sending solution to the puzzle
Step 6 S: verification of the solution if the solution is correct:
Step 7 S: continue processing service request

HOP COUNT FILTERING

One of the passive host based method is hop count filter. Hop count is a rough measure of distance between two hosts. A hop count of n means that n gateways separate the source host from the destination host
This hop-count information can be inferred from the Time-to-Live (TTL) value in the IP header. Based on this observation, a novel filtering technique for Internet servers to block spoofed IP packets. By clustering address prefixes based on hop-counts, Hop-Count Filtering (HCF) builds an accurate IP to hop-count (IP2HC) mapping table to detect and discard spoofed IP packets. Through analysis using network measurement data, HCF can identify and then discard close to 90% of spoofed IP packets with little collateral damage.

ROUTER BASED MECHANISM

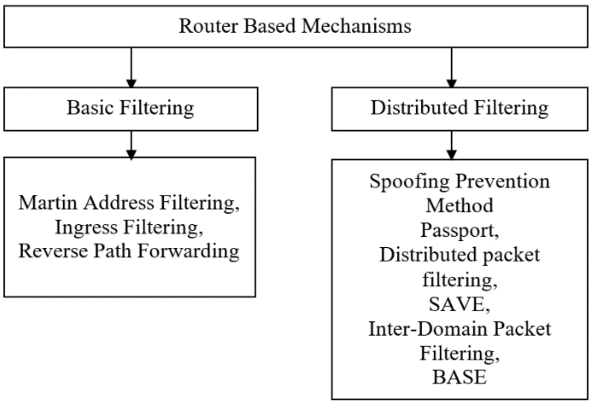
Router Based Mechanisms
Basic Filtering
Distributed Filtering
Martin Address Filtering, Ingress Filtering, Reverse Path Forwarding
Spoofing Prevention Method Passport, Distributed packet filtering, SAVE, Inter-Domain Packet Filtering, BASE

Figure5. Classification of router based mechanism

Router based defence mechanism are installed inside IP routers and hence trace the source of attack and block the corresponding traffic originating from that source
Router based mechanism are of two types, basic filtering and distributed filtering. Above figure shows classification of router based filtering mechanism

MARTIN ADDRESS FILTERING

Martin address filtering is one of the simplest and earliest methods to detect spoofing. It simply checks IP field and looks for invalid address such as non-Unicast, loopback or any other spoofed address. However, it can only detect and defend simple and common types of attacks.

INGRESS EGRESS FILTERING

Ingress and egress filtering are used to filter large classes of networks that should not been seen at different parts of the network. Ingress filtering is used to eliminate routing of spoofed packets by discarding any packet that are coming from the outside (Internet) to the inside of the network. Egress filtering prevents the private network from being the source of forged communication used in DoS attacks Ingress and Egress filters must be placed on the edge router of the network in order to filter any packets going in and out the private network.

REVERSE PATH FORWARDING

Reverse path forwarding (RPF) is a technique used in modern routers for the purposes of ensuring loop-free forwarding of multicast packets in multicast routing and to help prevent IP address spoofing .

DOI10.17148/IARJSET.2017.4704

When a multicast packet enters a router's interface, it will look up the list of networks that are reachable via that interface i.e., it checks the reverse path of the packet. If the router finds a matching routing entry for the source IP address of the multicast packet, the RPF check passes and the packet is forwarded to all other interfaces that are participating in multicast for that multicast group. [10] If the RPF check fails, the packet will be dropped. As a result, the forwarding of the packet is decided based upon the reverse path of the packet rather than the forward path. RPF routers only forward packets that come into the interface that also holds the routing entry for the source of the packet, thus breaking any loop.

SPOOFING PREVENTION METHOD (SPM)

SPM prevention method validates methods using embedded secret key. Before transmitting an IP packet a source node embeds a secret key(s, d). For each packet that arrives at its destination network, routers in the destination network check the source network and verify key. The packet which contains the valid secret key is considered as a valid packet while the packet without secret key or invalid secret key are spoofed packet.

The important characteristic of the SPM method is that packets that come from an ASes deployed with SPM are marked and are authenticated. Hence, if an ISP detects an attack on itself or on one of its customers, it protects itself from spoofed packets by allowing in only packets that originate from SPM member.

DISTRIBUTED PACKET FILTERING

Route-based distributed packet filtering (DPF) uses routing information to determine if a packet arriving at a router—e.g., border router at an AS—is valid with respect to its inscribed source/destination addresses, DPF passes all the IP packet with correct source address while the ip packets with incorrect address are rejected. If a set of routers in a network has complete knowledge of incoming directions, then the chances of successful IP spoofing can be considerably reduced. DPF assumes that routers have prior knowledge of incoming direction. The main problem of DPF is its actual method of learning the incoming direction information for routers.

SOURCE ADDRESS VALIDITY ENFORCEMENT (SAVE)

The SAVE operates in a manner similar to DPF where the routers filter IP packets on the basis of incoming direction, however, unlike DPF, in this mechanism SAVE provides routers with valid incoming direction. SAVE is run by routers in parallel with the routing protocol in which one or more routers are in charge of a given source address space that send the SAVE updates corresponding to each forwarding table entry. The SAVE updates and normal traffic from a source address space travel through the same path. When intermediate routers receive the updates, it records the incoming interface of updates as a valid incoming direction of corresponding source address space. Updates are also sent periodically whenever any router change occurs. SAVE also contributes in the form of incoming tree; in which each router maintain its own incoming tree that keeps track of the topological relations of upstream source address spaces. If one routing change affects the incoming direction of many spaces, then routers can update the information for every affected space automatically. A sub network can easily deploy SAVE across its routers but for a large network its deployment is very difficult. SAVE considers its full deployment on routers which is not feasible. It can identify all spoofing packets when destination and attacker are on the different networks.

INTERDOMAIN PACKET FILTER (IDPF)

An inter domain packet filter (IDPF) architecture minimize the level of IP spoofing on the Internet. A key feature of this scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers. Each node only propagates and selects to neighbor based on two set of routing policies. They are import policy and export policy. The IDPFs uses a feasible path from source to the destination node, and a packet can reach to the destination through one of its upstream neighbor. Even with the partial deployment on the internet IDPF can significantly limit the spoofing capability of attackers. [3]

BGP ANTI-SPOOFING EXTENSION (BASE)

BASE contains the features of path identification and distributed filtering (DPF). It is path based packet filtering mechanism which relies on BGP. BASE filters packet based on their path tags. Packet is tagged by a hashed marking value of their BGP path that is distributed using BGP updates. Every packet from the same source address will have the same tag regarding the path they traverse and interface they arrive from. When a packet arrives at a BASE deployed router, the router will tag outgoing packet and drop incoming packet without proper tag.

C. COMBINATION BASED DEFENCE MECHANISM

Combination based mechanism based on both routers as well as hosts. Above fig shows various combinational IP spoofing defence mechanisms

DOI10.17148/IARJSET.2017.4704

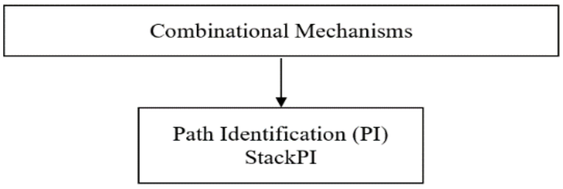

Figure6. Combinational IP spoofing defence mechanism

PATH IDENTIFICATION (PI)

Path Identification (PI) was basically designed to defend DoS attacks but it shows some defence against IP address spoofing as well. PI reuses fragmentation field of IP packets which identifies the path undertaken by the packets. For each path/router through which a packet travels, a bit is set in its fragmentation field. Thus, a packet at the destination will contain a unique marking of the path it has taken. The destination end host does not know which path the packet has travelled through; however, if multiple packets have same markings, it is considered that these packets have travelled through the same path. When an end host identifies an attack packet, then the host is able to filter out subsequent packets using the markings through the path identifier field. Since routes are dynamic, therefore, the markings cannot be unique for attack as well as normal packets. Some of the legitimate packets may be lost if PI drops packets with attack path marking. To minimize such false positives, it is recommended to drop packets only when the host is under attack [9]

STACK PATH IDENTIFICATION

Stack pi is an improved and enhanced version of pi mechanism. It is an incremental deployment of pi mechanism. It is composed of two parts marking scheme and filtering scheme. The marking scheme defines how StackPi enabled routers mark all the packets that they forward. Each router treats the IP Identification field as though it were a stack. Upon receipt of a packet, a router shifts the IP Identification field (hereon referred to as the marking field) of the packet's header to the left by n bits, and writes a precalculated set of n bits (represented by the marking m) into the least significant bits that were cleared by the shifting. This is the equivalent of pushing a marking onto the stack. Every following router in the path does the same until the packet reaches its destination. Because of the finite size of the marking field, after [16/n] routers have pushed their markings onto the marking field, additional markings simply cause the oldest markings (the ones pushed first onto the stack) to be lost. The packet's StackPi mark is merely the concatenation of all the markings in the marking field when the packet arrives at its destination

The filtering scheme defines how end hosts utilize the packet markings to most efficiently defend against DDoS and IP spoofing attacks.

3. PERFORMANCE COMPARISION

Route-based and host-based are two different approaches taken by researchers to thwart DDoS attacks. The former installs the defence mechanism inside IP routers and hence trace the source of attack and block the corresponding traffic originating from that source. However, the drawback of this approach is that it requires coordination among different routers and networks, and also a widespread deployment to reach the proximity of the attacker. The host-based approach can be deployed immediately. Also, a much stronger incentive is required to deploy the defense mechanism at the end system compared to that of network service provider.

One of the earliest and simplest basic router based method is Martin filtering. To filter spoofed source address of packet, it simply cheeks IP field and looks for invalid address like non-Unicast, loopback or any other spoofed address. However, from its design, it can detect and defend simple and common type of attacks only otherwise it is ineffective. Ingress and egress filtering methods are considered to be among the best solutions as they run on boarder router protocol. It can filter almost any type of spoofed packets if deployed on all networks. It limits the attackers to their local networks only. However, it requires full deployment. Reverse path forwarding (RPF) functions similar to ingress and egress but the only difference is, RPF needs forwarding table information at routers and it is based on routing symmetry of the internet, which is not always possible.

Hop count filtering scans the incoming IP packet without using any cryptographic technique. The basic idea behind the scheme is to use the packet information – the route that packet travels along with the TTL field. The TTL field of the packet is used to determine if the packet has travelled the right number of hops before reaching the destination. In IP spoofing the attacker can falsify the IP address of the source but he cannot ideally alter the number of hops the packet would travel to the destination.

It is observed that none of the compared method except DPF and IDPF provides excellent performance in all compared parameters.

The second type of router-based methods is distributed defence method. In this method, routers co-operate on the key, which only valid packets carry, or to the incoming direction for packets from a given source. Spoofing prevention method (SPM) which validates packets based by checking their secret key, which is embedded into the packets are deployed on the border routers. The packets containing the secret key are passed and others are treated as spoofed.
SAVE and DPF operate in a similar way in which packets are filtered on the basis on their incoming detection. SAVE helps routers to learn the incoming direction knowledge. However, SAVE creates an incoming tree, which keeps track of topological relationship of source address. Whenever any router changes happen, the incoming direction is affected and other participating routers are updated on the incoming tree. However, SAVE assumes its full deployment, which is infeasible and shows inefficiency. BASE completely relies on BGP and functions similar to SAVE, which sends updates to the routers to learn the correct incoming direction of packets. BASE is path based filtering mechanism and updates must travel the same path as the BGP update. However, BGP updates do not always travel the same path. BASE also uses control message means BASE routers are only able to respond to the spoofed IP packets after receiving packets.
The combinational defence methods for IP Spoofing use both routers as well as hosts based methods, these are generally packet-marking solutions the disadvantage of combinational methods is that no action can be taken upon the attacking packets until they reach their destination or victim at the edge of the network.

4. CONCLUSION

In this paper we studied various mechanisms to fight against IP Spoofing based attacks. We saw that IDPF can significantly limit the spoofing capability of an attacker compared to other defence mechanisms. They also help localize the actual origin of an attack packet to be within a small number of candidate networks. In addition, IDPFs also provide adequate local incentives for network operators to deploy them. Hence we conclude, that compared to all other defence mechanisms IDPF has significant capacity to block the IP Spoofing attack with minimum false positive rate and also traceback the attack path effectively.

REFERENCES

[1] C.Jin, H.Wang, K. G. Shin,"Hop-count filtering: An effective defense against spoofed DDoS traffic", In Proc. of the 10t ACM conference on Computer and communications security,2003
[2] K. Park, H.Lee,"On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets", In Proc. of ACM SIGCOMM, 2006.
[3] Z.Duan, X.Yuan, J. Chandrashekar,"Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates", IEEE Transactions On Dependable And Secure
[4] CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, November 29, 2000, URL: http://www.cert.org/advisories/CA-1996-21.html.
[5] Computer Incident Advisory Committee (CIAC) (1995). Advisory Notice F-08 Internet Spoofing and Hijacked Session Attacks. url: http://ciac.llnl.gov/ciac/bulletins/f-08/shtml
[6] Definition of man-in-the-middle, Webpage 2002-03-26, retrieved 2002-09
[7] Mattias Eriksson, "An Example of a Man-in-the-middle Attack against Server Authenticated SSL-sessions", Simovits Consulting Wenner-Gren Center, 6 Stockholm, Sweden.
[8] S. Kent and K. Seo, "Security architecture for the Internet Protocol," RFC 4301, IETF, 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4301.txt.
[9] V.Shyamaladevi and Dr.R.S.D. WahidaBanu Detection of Spoofing Attacks Using Intrusive Filters for DDoS. available online: http://paper.ijcsns.org
[10] Yogen K. Dalal and Robert M. Metcalfe Xerox Corporation and Stanford University "reverse path forwarding of Broadcast packet". Online available : http://www.mathcs.emory.edu/~cheung/Courses/455/Syllabus/6-mcast