International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - I ISSN (Online): 2454- 1966

Research Manuscript Title

An Improved Mechanism based on BGP for Detecting and Preventing IP Spoofing

S.Swarna Latha, J.Bhavithra, M.E,

PG Scholar, Assistant Professor,

Dept. of Computer Science and Engineering

Dr.MCET, Pollachi, TamilNadu, India.

E-mail: swarnalathascb@gmail.com, bavi@drmcet.ac.in

March – 2016

www.istpublications.com

International Journal of Future Innovative Science and Engineering Research (IJFISER), Volume - 2, Issue – I,
ISSN (Online): 2454- 1966 www.istpublications.com.

An Improved Mechanism based on BGP for Detecting and Preventing IP Spoofing

S.Swarna Latha, , J.Bhavithra, M.E,

PG Scholar, Assistant Professor,
Dept. of Computer Science and Engineering
Dr.MCET, Pollachi, TamilNadu, India.
E-mail: swarnalathascb@gmail.com, bavi@drmcet.ac.in

ABSTRACT

In computer networking, the term IP address spoofing indicates the process of modifying the packet's header with a forged source IP address for the purpose of concealing their real location. To screen the origin of a network level attack in today's best effort, IP traceback is an important mechanism. IP traceback defend against IP spoofing attacks. Passive IP Traceback (PIT) is one of the promising approaches to realize IP Traceback. It improves the efficiency and accuracy of IP Traceback and it provides incentives for ISPs to deploy traceback in networks. Therefore PIT approach improves the performance and probability of IP traceback. IP Traceback is a technique used for tracking the path of IP datagram back towards the origin. PIT analyzes the Internet Control Message Protocol (ICMP) error message called Path Backscatter, generated by spoofing traffic. Simultaneously it tracks the spoofers based on public available information (e.g., Topology) and capture the location of spoofers thereby improving the efficiency. We must also note that PIT cannot handle all sorts of spoofing attacks and all spoofers. The proposed system combines PIT with BASE (BGP based Anti-Spoofing Extension) which is an anti-spoofing protocol intended to achieve the incremental deployment properties which are necessary in today's Internet environment. BASE is used for preventing spoofers and can be adopted easily and deployed in real networks. In spoofers identification process, a value called "Marking" is calculated for these packets that use BGP update messages. It is distributed to routers where the value is checked against values in filter table. This method is called Packet Marking and Filtering in BASE. This method will detect more number of packets and, will minimize the computation overhead on the router.

***Index Terms*— IP spoofing, PIT, BASE Mechanism**

I. INTRODUCTION

The growth of internet in these days is enormous and securing the internet is a challenging task. Current major environments like our Society, Government and the Economy is progressively dependent on the internet. Hence, securing the internet is really important and therefore internet security comes into existence. One of the most difficult challenges in internet is IP spoofing, which is more important in Distributed Denial of Service (DDoS) attacks. A DDoS attack is the most pressing security attacks on the internet [1]. In DDoS attacks, the intruder initiates the attacks from different corners of the internet and the attack flows can be switched off by configuring IP source based filters if one can discover the malicious clients. Though, attack flows can use forged source addresses to hide attacker's real location, or to use the flaw of the target system, or even to gain the ability of initiating reflection based attack, it leads to failure in source based filtering.

IP spoofing is a serious security problem on the internet which makes use of the forged source IP address to promote the attacks in order to mislead the receiver of the true packet origin [2]. Preventing the IP spoofers from attacking the network is a tedious task. Various attacks such as SYN flooding [3], Smurf [4], and DNS amplification [5] rely on IP spoofing. Among these attacks, DNS amplification attack is the main attack that severely degrades the service of the TLD (Top Level Domain) name server for a long period.

IP Traceback [6] is a major technique used in the network to identify the real location of spoofers without relying on the source IP address field of the packet header, and it is the most important method to find the real attack sources. One of the novel methods in IP Traceback mechanism is the Passive IP Traceback (PIT) which analyses the Path Backscatter message. Path Backscatter message is an ICMP error message that is generated by the routers when it fails to forward an IP spoofing packet due to several reasons, e.g., TTL exceed and finally the generated
message is send to the spoofed origin. Though the PIT method finds the location of the spoofers, it doesn't work in all attacks and cannot capture all the spoofers in the network.

To overcome this drawback, an anti-spoofing mechanism called BGP based Anti-Spoofing Extension (BASE) is used. BASE mechanism involves a spoofer identification process which includes Packet Marking and Filtering. This method can discover more number of spoofing packets and it also reduces the overhead on the router. The BASE protocol needs to satisfy three properties that are initial benefits for the early adopters, incremental benefits for the early majority, and efficiency under partial deployment. BASE shows desirable IP spoofing prevention capabilities under partial deployment.

The rest of the paper is organized as follows. Section 2 Related works has been discussed. Section 3 Existing system has been discussed. In section 4 proposed systems has been discussed. In section 5 we gave the result and in section 6 the conclusion is discussed.

II. RELATED WORK

Other than IP traceback, another way of identifying attack packets is to have an ability to differentiate between attack packets and legitimate packets and filter those attacked ones. The reason for selecting IP Traceback is, it not only identifies the attack packets but also the location of spoofers. IP Spoofing defense mechanism is of two types named Host-based solutions and Router-based solutions [7]. Host-based solution is untouched as BASE is a Router-based solution. The Router-based solution is classified majorly into 2 types namely distributed methods of spoofing defense and filtering. BASE falls under distributed methods of spoofing defense and a short discussion on those existing distributed methods is followed.

In distributed methods of spoofing defense, routers cooperate to discover information for distinguishing valid and spoofing packets. The information might be related to the key value which the valid packets will carry or to the incoming direction for the packets from a given source. This method is classified into five main categories: Spoofing Prevention Method, Passport, Distributed Packet Filtering, Source Address Validity Enforcement and Inter-Domain Packet Filters [7].

A router implementing Spoofing Prevention Method (SPM) [7], authenticates a packet by examining the secret key embedded into the packet. A source Autonomous System (AS) s, chooses upon a key calculated for every (s,d) pair, where d is a destination AS. When a packet reaches the destination d, the router ensures the

secret key. A packet with the key is valid, and the packet without the key is spoofed. If the AS does not follow SPM method, there won't be any key associated with the packets. Hence router cannot recognize the spoofed and non-spoofed packets.

Passport system [8] is a cryptography based authentication technique which verifies the source address at the destination. Passport has a habit of solving the source address spoofing which happens in the Inter-domain network environment. Packet passport technique requires light weight MAC computation. Source node includes the computed MAC value into the Option field of IP header. The border router at AS will check the MAC value from each packet. At the border router, the calculated MAC is compared to MAC value computed at the router.

If the values are alike then the packet is forwarded to next router. If values are unlike then the packet is marked as Spoofed packet and is discarded. Packet passport system validates only the domain origin of the packet and not the host origin of the packet. It works only with the Inter Autonomous System.

Distributed Packet Filtering or DPF [9] have routers throughout the network. It maintains the incoming direction knowledge (knowledge of the interface from which a packet travels from a given source to a given destination). When a packet with a spoofed source address arrives at an incorrect interface, the router can detect this and filter the packet.

Source Address Validity Enforcement protocol (SAVE), runs on individual routers and build incoming table. Incoming table contains entries of IP Address with corresponding packet interface. Each router will have two tables specifically forwarding and incoming tables. Forwarding table will hold the information regarding the outgoing packet's IP address with its interface and incoming table has incoming packet's IP address with its interface. Each router allows mapping incoming interface to IP Address with the existing one to check whether it comes from a legal interface or not. If the interface is valid, then the packet is transmitted or else it is discarded [10].

Inter-Domain Packet Filters (IDPF) attempts to deliver an execution of the DPF principles. Learning from BGP updates, and assuming that BGP routers follow a specific set of distributing rules, routers running IDPF can discover AS relationship information and then use this information to build packet filtering rules [11]. In general, ASes can be in a provider-customer, peer-peer, or sibling-sibling relationship. These relationships put limits on which AS paths are possible, and which are not possible. Packets which arrive from neighbors along an infeasible path can be filtered out. The routers know the real valid incoming direction of packets but routers running IDPF only know possible incoming directions, not real incoming directions. With this delimited knowledge, IDPF is not as effective as an accurate DPF implementation; attackers are able to positively spoof more source address spaces. Also, with IDPF's dependency on AS relationship information gathered from BGP updates, it is delimited to function in conjunction with BGP.

III. EXISTING SYSTEM

Spoofers launch attacks with forged source IP address and this has been documented as a serious security problem on the internet commonly called IP Spoofing. To capture the origins of IP spoofing traffic on the internet is thorny. Passive IP Traceback (PIT) mechanism is resulted in search

of identifying the origin of spoofing traffic. PIT examines the Internet Control Message Protocol (ICMP) error message called Path Backscatter, produced by spoofing traffic.

A. Path Backscatter

During transmission, there is no guarantee that all the packets reach their destinations. If the spoofer use single source address and transmit the packet to multiple destinations then this attack is called Single Source, Multiple Destinations Reflection attack. To burden the router, spoofers try to send packets continuously with minimum Time To Live (TTL) value. Routers may fail to forward an IP spoofing packet further whose TTL value is zero. Under those conditions, router may generate an Internet Control Message Protocol (ICMP) error message called path backscatter message. Path backscatter message is generated based on the idea that the routers can be close to the spoofers. Hence the path backscatter messages may possibly disclose the locations of the spoofers. This means the victims of reflection based attacks, and the hosts whose addresses are used by spoofers, are probably to collect such messages. The path backscatter message analysis is described below in Fig 1.

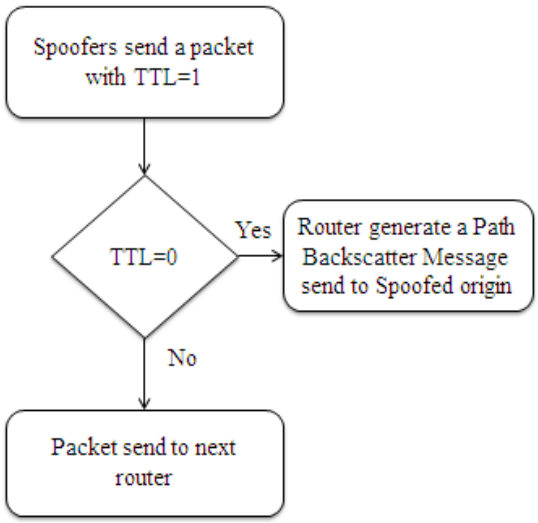

Fig 1- Path Backscatter Analysis

Time exceeded message or Path backscatter message is produced when the gateway router handling the packet, discovers the Time To Live field (this field is in the IP header of all packets) equals zero or something else. If the value is zero, then the packet will be discarded else the packet will be transmitted to the next router. The similar gateway may also inform the source host via the time exceeded message.

B. Passive IP Traceback

PIT – An IP Traceback method for analyzing the path backscatter messages. PIT is composed by a set of mechanisms among which tracking without routing information is selected. Tracking without Routing Information make use of two assumptions namely Loop-Free Assumption and Valley-Free Assumption. Valley-Free Assumption is used for finding the location of spoofers in a network and it also states that there must be no valley in the AS level paths. This assumption is the most common model of AS level routing. A gateway router

will definitely have many AS connected to it and hence the process of identifying spoofers becomes tedious. A set called Suspect set is generated which hold certain AS. The scale of AS-level Internet topology, for a path backscatter message (r,od*)*, is very costly to find all the ASes that has a valley-free path to original destination through reflector. The suspect set is created with the help of a concept called customer cone. To introduce the concept of customer cone, it is defined as the customer cone of an AS A as the AS A itself plus all the ASs that it can reach for free [13]. The customer cone of AS n is denoted by Cone (n).

```
1. Function GETSUSPECTSET_VALLEYFREE(G,r,od)
2.     If od ∈ Cone(r) then
3.             return G.nodes()
4.      else
5.             return Cone(r)
6.     end if
7. End function
```

Fig 2- The algorithm to determine suspect set based on valley-free assumption. (Source: ref [22])

When od ∉ Cone(r), the suspect set is just Cone(r). When od ∈ Cone(r), the suspect set is the entire node set and is described in Fig 2. A suspect set whose size is not greater than N requires the customer cone size of r is no larger than N. Mostly, if the size of suspicious set is 1, then r should be a stub AS. Likewise, based on the valley free assumption, the probability of finding the accurate location of the attacker from a path backscatter message *(*r, od*)* is based on three conditions:

1) VF-C1: the size of Cone (a) is 1;

2) VF-C2: od is not a;

3) VF-C3: r is *a*.

IV. PROPOSED SYSTEM

This section propose a mechanism called ‘‘BGP-based Anti-Spoofing Extension’’ (BASE), which contains the features of Path Identification (Pi) [5] and Distributed packet Filtering (DPF) [6]. BASE (BGP based Anti-Spoofing Extension) which an anti-spoofing protocol is intended to achieve the incremental deployment properties which are necessary in today’s Internet environment. BASE is used for preventing spoofers and can be adopted easily and deployed in real networks. In spoofers identification process, a value called “Marking” is calculated for these packets that use BGP update messages. It is distributed to routers where the value is checked

against values in filter table. This method is called Packet Marking and Filtering in BASE. This method will detect more number of packets and, will minimize the computation overhead on the router.

A. Distribution of marking values

BASE mechanism allocates valid marking values via BGP update messages. BGP (Border Gateway Protocol) is a standard inter-AS routing protocol in the Internet. BGP obtains subnet reachability information from neighbouring ASes and broadcasts it to other BGP-enabled routers, so that all the ASes will know about the subnets. The marking values are calculated by a one-way hash chain, i.e., m_i = MAC (k_i,m_{i-1}), where i denotes the index of a filter node (from i = 1 to all filter nodes), and k_i is the secret key and m_0 is the prefix of the source AS. The figured marking value for each node is spread to next nodes as described in Fig.3.The marking values are distributed using BGP informs and kept in the Filtering Tables of BASE applications.

MAC and one-way hash chains are used for creating a cryptographically unique value for a filter node Message Authentication Code (MAC). Cryptographic methods improve the strength of packet marking under the attacker's fake of marking values as well as source addresses. Since spoofing the marking field reduces the effectiveness of packet marking, a cryptographic Message Authentication Code (MAC) is used to guard the integrity of marking values.

Marking value Procedure

1. m_o = the prefix of the source AS
2. FOR each BASE filter v_i from i=1 to all filter nodes
3. m_i = MAC(k_i,m_{i-1})
4. Forward m_i to next BASE filter nodes by using the Optional transitive attributes
5. ENDFOR

Fig 3- Distribution algorithm of marking values

(Source: ref [23])

BASE routers need not necessarily share common keys, but each router only has a local symmetric AS key. That AS key is at least 128 bits long, which ensures very strong security even if the attacker learns a lot of marking values. A smaller MAC does not make it easier to disrupt the AS key, in fact, it makes it harder because fewer MAC bits are available to prove the correctness of a predicted key in a brute force attack. Sharing keys within an AS is simple – no sophisticated key management system is necessary.

B. Packet Marking and Filtering

During spoofing attack, an attacker sends spoofed packets to the destination node to hide the identity of the attacker. A victim has the ability to recognize a spoofing attack. At the victim side the spoofed packets are identified by TCP-specific probing and SYN cookies. In TCP-specific probing, a victim replies with a crafted TCP ACK such as varying TCP window size. Since the sender cannot see the crafted ACK, the victim can detect spoofed packets by perceiving the sender's responses that should meet changed TCP window size. Once the attack is known, the victim can apply BASE to protect itself from the attack. A controller in a victim network sends invocation messages to SDN controllers, and controllers receive the invocation message initiate packet marking and filtering for the consistent addresses is described in Fig 5.

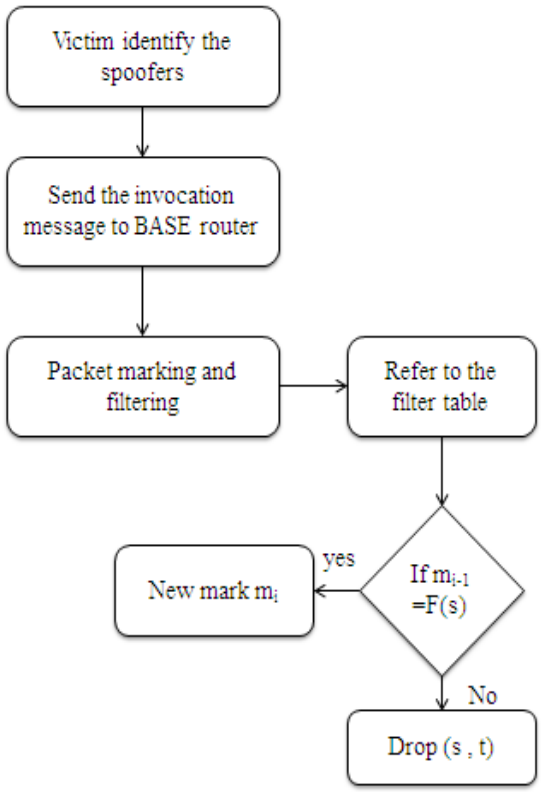

Fig 4-Packet Marking and Filtering

Each node will have BASE filters and the role of a BASE filter is described in Fig 4. Each BASE filter has a Filtering Table F. If F can store only one marking value in each record, then it is called as ''one mark'' and if multiple marking values are stored, then it is called as ''multiple marks.'' By default, BASE is ''multiple marks.'' In this case, it can store all likely marking values in the Filtering Table. In the distribution phase, when a BASE filter collects a marking value, it stored in its Filtering Table F. In the marking and filtering phase, when a BASE filter receives a packet (s,t), the filter forwards the packet to R(t) with a new mark mi only if $m_{i-1} \sum F(s)$otherwise it drops(s,t).

Packet Marking and Filtering Procedure

1. FOR each BASE filter v_i from i=1 to all filter nodes
2. IF m_{i-1} ε F(s) // F is a Filtering Table
3. forwards (s,t) to R(t) with a new mark mi
4. ELSE
5. drops (s,t)
6. ENDIF
7. ENDFOR

Fig 5- Packet Marking and Filtering algorithm in a node (source: ref [23])

SYSTEM ANALYSIS

The main motive of this system is to identify the IP spoofing attack using BASE mechanism in distributed network and differences between the various types of attack along with the reasons behind those attacks. In the distribution phase, BASE requires a small computation for creating marking values. The marking values can be computed even before they are distributed through BGP update messages. This process occurs rarely, only when a BGP path changes or a new BASE-enabled node is deployed. Also, if some nodes sometimes need to inform their key values, then the marking values also need to be updated. Using PIT, the location of the spoofers is identified and it is analyzed that the spoofers are caught correctly to a great extent. Thus IP spoofing attack might be attained with improved performance result. Using a graph called X-graph, the overload of the router is evaluated and detection accuracy and shown in fig 6 and 7.

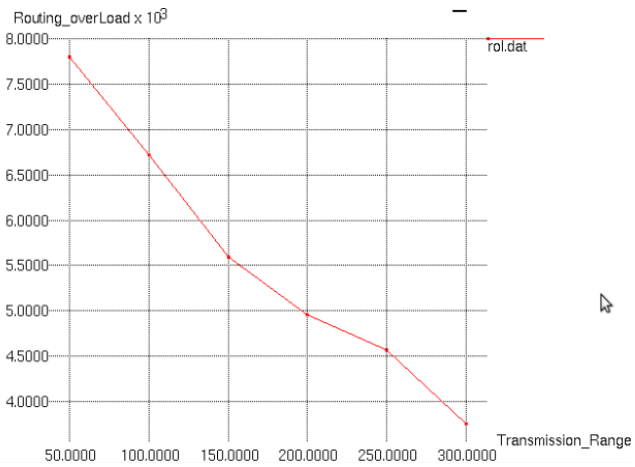

Fig 6- Router Overload

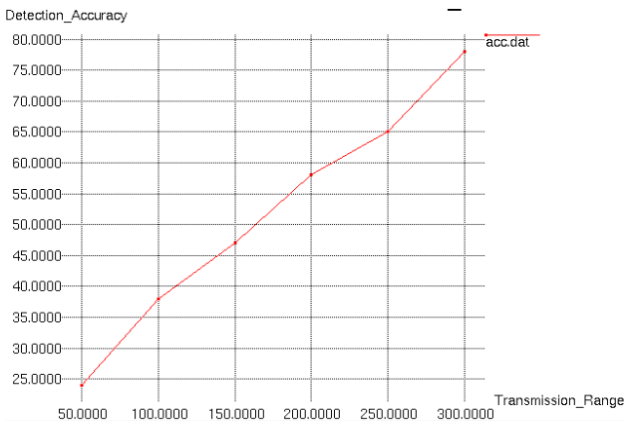

Fig 7 – Detection Accuracy

BASE is to be evaluated further to prevent IP spoofing attack and efficiency of the system is to be examined.

VI. CONCLUSION

The existing system tries to dissolve the fog on the locations of spoofers based on investigating Path Backscatter messages. Passive IP Traceback (PIT) is used to track spoofers based on the path backscatter messages and public available information. In proposed system, BASE mechanism is applied to satisfy the incremental deployment properties that are vital for current Internet environments. The protecting power is greater as BASE filters are distributed gradually. This is due to its ability to stop the spoofing to a large percentage of the IP address space when it has only been deployed to handle relatively a small percentage of that space. AS's routing policies can prevent the BGP update messages from broadcasting to neighboring AS, and also malicious BASE speakers at negotiated routers can pass attack packets and drop legitimate packets. Additionally, the result of real world routing rules on distribution of BASE control data needs further examination. Despite this, BASE offers a capable new way in IP spoofing prevention.

VII. REFERENCES

[1] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao, (2007), "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computing Surveys, Vol. 39, No. 1,pp. 20-29.

[2] Sharmin Rashid, Subhar Prosun Paul, (2013), "Proposed Methods of IP Spoofing Detection & Prevention", International Journal of Science and Research', ISSN: 2319-7064.

[3] CERT, "TCP SYN Flooding and IP Spoofing Attacks", http://www.cert.org/advisories/CA-1996-21.html.

[4] CERT, "Smurf IP Denial-of-Service Attacks", http://www.cert.org/advisories/CA-1998-01.html.

[5] R.Vaughn, and G. Evron, "DNS Amplification Attacks",http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.

[6] S.Savaga, D.Wetherall, A.R.Karlin, and T.anderson, (2000), "Practical network support for IP traceback", ACM SIGCOMM, pp.295-306.

[7] Ehrenkranz, Jun Li, (2009), "On the State of IP Spoofing Defence", ACM Vol 9, No.2.

[8] Sonal Patel, Vikas Jha, (2015), "Various Anti IP Spoofing Techniques", Journal of Engineering computers & applied sciences (JECAS) Vol 4, No.1.

[9] Birger Toedtmann and Erwin P.Rathgeb, (2006), "Anticipatory Distributed Packet Filter Configuration for Carrier-Grade IP-Networks", International federation for Information Processing, Vol.11, No.32, pp.928-41.

[10] Robert Beverly, Arthur Berger, Young Hyun, (2009), "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering", ACM 978-1-60558-770-7/09/11.

[11] Zhenhai Duan, Xin Yuan, and Jaideep Chandrasekhar, (2006), "Controlling IP Spoofing Through Inter-Domain Packet Filters", IEEE INFOCOM.

[12] Guang Yao, Jun Bi, Zijian Zhou, (2010), "Passive IP Traceback: Capturing the Origin of Anonymous Traffic through Network Telescope", ACM 978-1-4503-0201-2/10/08.

[13] Xenofontas Dimitropouls, Dmitri Krioukov, Marina Fomenkov, Bradley Huffaker, (2000), "AS Relationships: Inference and Validation", ACM 568-3-5504-1321-5/9/5.

[14] A. Yaar, A. Perrig, D. Song, (2003), "Pi: a path identification mechanism to defend against DDoS attacks", IEEE Symposium on Security and Privacy.

[15] K. Park, H. Lee, (2001), "On the effectiveness of router-based packet filtering for distributed DoS attack prevention in power-law Internets", Proceedings of ACM SIGCOMM.

[16] Bingyang Liu, Jun Bi and Yu Zhu, (2011), "A Deployable Approach for Inter-AS Anti-Spoofing", IEEE International Conference on Network Protocols, 978-1-4577-1393/11/26.00.

[17] Malliga, S. and Tamilarasi, A. (2010), "A hybrid scheme using packet marking and logging for IP traceback", International Journal of Internet Protocol Technology, vol. 5, no. 1-2, pp. 81–91.

[18] Sonal Patel, Vikas Jha, (2015), "Various Anti IP Spoofing Techniques", Journal of Engineering

computers & applied sciences (JECAS) Vol 4, No.1.

[19] Gong, c. and sarac, K., (2005), "IP traceback based on packet marking and logging", IEEE International conference on Communications, Seoul, Korea.

[20] Bradley Huffaker, Matthew Luckie, Among Dhamdhere, (2013), "AS Relationship, Customer cones, and Validation", ACM 978-1-4503-1953-9/13/10./15.00.

[21] X. Liu, X.Yang, D.Wetherall, and, T. Anderson, (2006), "Efficient and Secure source Authentication with Packet Passport", Proc. Second Usenix workshop Steps to Reducing Unwanted Traffic on the Internet.

[22] Guang Yao, Jun Bi, Athanasios V.Vasilakos, (2015), "Passive IP Traceback: Disclosing the Location of IP Spoofers from Path Backscatter", IEEE Transaction on Information forensics and security, Vol., 10, No.3.

[23] Jonghoon kwon, Dongwon seo, Minjin kwon, Heejo Lee, Adrian Perrig, Hyogon Kim, (2015), "An incrementally deployable anti-spoofing mechanism for software defined network's", Elsevier-0140-36644.

[24] Heejo Lee, Minjin kwon, Geoffrey Hasker, Adrian Perrig, (2007), "BASE: An Incrementally Deployable Mechanism for viable IP spoofing Prevention", ACM Vol 1-59593-544-6/0/0003.