A New Mechanism For Approach of IP Spoofers: Passive IP Traceback Using Backscatter Messages

Dharam Pavithra[1], B. Narasimha Swamy[2] , Dr.A. Sudhir Babu[3]
[1]M.Tech (CSE), [2]Sr.Assistant Professor, [3]Professor
Department of CSE, Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, A.P., India.

Abstract - IP Spoofing has been a long vulnerability that the attackers may use fabricated source IP address to cover their real regions. Different techniques have been recommended in order to catch spoofers. There has not been a general mechanism, at the Internet level in any event because of the overhead of implementation. To catch the spoofers, different IP traceback systems have been proposed. However, because of the difficulties of arrangement, there has been not a generally received IP traceback arrangement, in any event at the Internet level. This paper proposes passive IP traceback (PIT) that side steps the sending challenges of IP traceback strategies. PIT examines Internet Control Message Protocol blunder messages (named way backscatter) activated by mocking movement, and tracks the spoofers in light of open accessible data (e.g., topology). This paper shows got regions of spoofers through applying PIT in transit backscatter data set. The outcomes can assist further with uncovering IP spoofing, which has been examined for long however never surely known. In spite of the fact that PIT can't work in all the spoofing attacks, it might be the most valuable instrument to follow spoofers before an Internet-level traceback framework has been sent in genuine.

Keywords — Denial-of-service, IP Traceback, PIT.

1. INTRODUCTION

IP spoofing is the creation of IP packets using somebody else’s IP source addresses. This technique is used for obvious reasons and is employed in several of the attacks [1]. A common misconception is that IP spoofing can be used to hide our IP address while surfing the Internet, chatting online, sending e-mail, and so on. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. There are several approaches of IP Spofing like:

- Man–in-the-middle: packet sniffs on link between the two endpoints, and can pretend to be one end of the connection.
- Routing re-direct : redirects routing information form the original host to the hacker’s host (a variation on the man-in the-middle attack)
- Source routing: redirects individual packets by the hacker’s host
- Blind spoofing: predicts responses from a host, allowing commands to be sent, but does not get immediate feedback
- Flooding; SYN flood fills up the receive queue from random source addresses; smurf/fraggle spoofs victims address, causing everyone to respond to the victim [2][3].

Though there has been a popular conventional wisdom that IPspofing can be controlled by certain mechanisms like monitoring packets using network monitoring software. A filtering router could also be installed. On the upstream interface source address originating outside of the IP valid range will be blocked from sending spoofed information. In certain cases, it might be possible for the attacker to see or redirect the response to his own machine [4]. The most usual case is when the attacker is spoofing an address on the same LAN or WAN. Hence the attackers have an unauthorized access over computers. To capture the origins of IP spoofing traffic is of great importance. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks. In this paper, we will examine the an alternative approach to solving IP spoofing using the technique called Passive IP traceback(PIT) [5]. The working of Passive IP traceback (PIT) and how it can detect for and defend against IP spoofing is shown [6].

2. PERFORMANCE EVOLUTATION

Due to its stateless nature, the Internet Protocol (IP) requires forwarding devices to only know each packet's next hop to correctly route any IP datagram towards its final destination. Thus, since identification of the source solely relies on information provided by the sender, IP makes it extremely difficult to correctly identify the real origin of any flow if the sender wishes to remain unknown. This peculiarity is often exploited during malicious Denial of Service (DoS) attacks to hide the source, so that the attack itself cannot be easily disabled. It is expected that if attack sources could be identified the incidence of “anonymous” DoS attacks would decrease significantly since the attackers, that are currently shielding behind IP source spoofing techniques, could be located, stopped and eventually be prosecuted. Using IP traceback, sources of Internet traffic, and attack traffic in particular, can be identified from the network traffic they generate. One technique for realizing IP traceback for flooding style DDoS attacks is Probabilistic Packet Marking (PPM), in which network routers embed their own identities in packets randomly selected from all the network traffic that the routers process. In the event of an attack, the router identity markings present in the attack packets can be used to reconstruct the attack graph – the paths taken by attack traffic – and establish its sources. The technique of probabilistically marking packets for IP traceback is the basis of many other schemes hereafter referred to as PPM-based schemes. It is important to point out that PPM-based schemes are not the only proposed approaches to IP traceback.

Alternatives include packet logging, specialized routing, Internet control message protocol (ICMP) traceback[7], deterministic packet marking and hybrid approaches which combine different traceback techniques, or combine traceback with anomaly detection. However, the results also show that networks within a super family exhibit notably similar performances which indicates a link between their underlying structure and their IP traceback performance. The convergence time is used as a measure of scheme performance.

Though PIT is used to perform IP traceback, it is very different from existing IP traceback mechanisms. PIT is inspired by a number of IP spoofing observation activities.

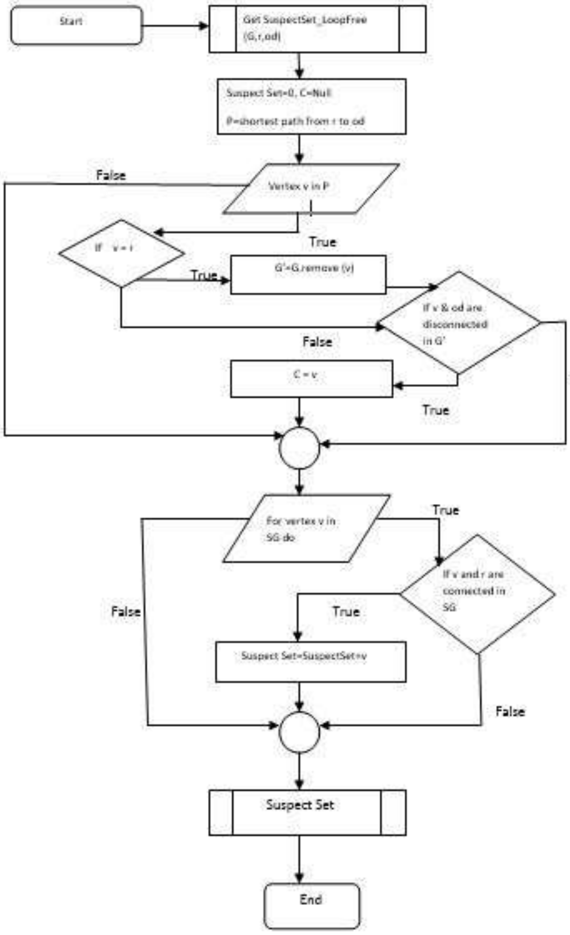
The victims can find the locations of the spoofers directly from the attacking traffic. Not all the packets reach their destinations. A network device may fail to forward a packet due to various reasons. Under certain conditions, it may generate an ICMP error message, i.e., path backscatter messages [8]. The path backscatter messages will be sent to the source IP address indicated in the original packet. If the source address is forged, the messages will be sent to the node who actually owns the address. This means the victims of reflection based attacks, and the hosts whose addresses are used by spoofers, are possibly to collect such messages [9].

3. RELATED WORK

Basic Tracking Mechanism Whenever a path backscatter message whose source is router r (named reflector) and the original destination is od is captured, the most direct inference is that the packet from attacker to od should bypass r. Use a very simple mechanism in spoofing origin tracking. The network is abstracted as a graph G(V, E), where V is the set of all the network nodes and E is the set of all the links.

A network node can be a router or an AS, depending on the tracking scenario. From each path backscatter message, the node r, r ∈ V which generates the packet and the original destination od, od ∈ V of the spoofing packet can be got. Denote the location of the spoofer, i.e., the nearest router or the origin AS, by a, a ∈ V[10]. We make use of path information to help track the location of the spoofer. Use path (v, u) to denote the sequence of nodes on one of the path from v to u, and use PAT H(v, u) to denote the set of all the paths from v to u. Use ϕ(r, od) to denote the set of nodes from each of which a packet to od can bypass r, i.e ∈ ∈ PATH(v,od) ϕ(r, od) actually determines the minimal set which must contain the spoofer. We name the result set of ϕ(r, od) by suspect set. If the topology and routes of the network are known, this mechanism can be used to effectively determine the suspect set. For example, an ISP can make this model to locate spoofers in its managed network. However, for most cases, the one who performs tracing does not know the routing choices of the other networks, which are non-public information. Moreover, the topologies of most of the ASes are unknown to the public.

Passive IP Traceback (PIT), PIT is actually composed by a set of mechanisms. generally the routing information is hard to achieve. IP traceback, it is very different from existing IP traceback mechanisms. PIT is inspired by a number of IP spoofing observation activities. Thus, the related work is composed by two parts. The first briefly introduces existing IP traceback mechanisms, and the second introduces the IP spoofing observations.

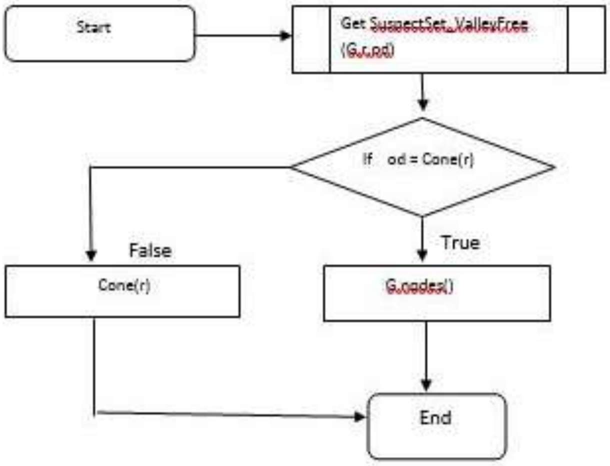


Algorithm1: The algorithm to determine the suspect set based on loop-free assumption.

The following algorithm 1 can be proofed to illustrate the correctness of the algorithm.

Theorem 1: From the second vertex along path(r, od), remove the first articulation point c whose removal will break r and od. Denote the subgraph containing r by SG(r). If and only if v is in SG(r), there exists a loop-free path from v to od containing r. Apparently, to determine a suspect set whose size is no larger than N requires the vertex number connected with r is no more than N in G − CutEdge(r, od). Especially, if the size of suspect set is 1) the degree of r must be one, and od must not be r. 2) Tracking on Valley-Free Assumption: Based on the valley-free assumption, a vertex v is in the path (r, od) if and only if there is at least one valley-free path from v to od passing r. Denote a valley-free path from v to u by v f path(v, u), which is a sequence of verticals along the path. Then the suspect set is ϕ (r, od) = {v|∃v f path(v, od),r ∈ v f path(v, od)}. The valley-free assumption can be only used in AS-level topology. Considering the scale of AS-level Internet topology, for a path backscatter message (r, od), it is very costly to find all the ASes that has a valley-free path to od through r. At first we introduce the concept of customer cone [11], which means "AS A, plus A's customers, plus its customers' customers, and so on". The customer cone of AS v is denoted by Cone(v). Then we can proof the following theorem:

Theorem 2: When od ∈/ Cone(r), if and only if v ∈ Cone(r), there is a valley-free path from v to od passing r.



Algorithm 2: The algorithm to determine suspect set based on valley-free assumption.

Based on this algorithm 2, when od ∈/ Cone(r), the suspect set is just Cone(r). When od ∈ Cone(r), because any valley-free path followed by a downhill path is still a valley-free path, the suspect set is the whole node set (Note that loop-free is not considered here). Thus, the algorithm is as specified in Fig. 7. Fig. 8 illustrate the suspect set tracked based on the valleyfree assumption. To determine a suspect set whose size is not larger than N requires the customer cone size of r is no larger than N. Especially, if the size of suspect set is 1, the r should be a stub AS.

IP Traceback: describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or "spoofed", source addresses. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Moreover, this traceback can be performed "post-mortem" – after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology.

Attacker: there are two types of attacker is present one is who is spoofing the IP address. Active attacker is one who is injecting malicious data to the corresponding node and also passive attacker will change the destination IP of the particular node. After attacking a node we can view attacked nodes inside router.

Service provider: the service provider will browse the data file, initialize the router nodes, for security purpose service provider encrypts the data file and then sends to the particular receivers (A, B, C, D…). Service provider will send their data file to router and router will select smallest distance path and send to particular receiver.

IDS Manager: the IDS Manager detects introducer and stores the introducer details. In a router any type of attacker (All Spoofers like source, destination, DOS Attacker) is found then details will send to IDS manager. And IDS Manager will detect the attacker type (Active attacker or passive attacker), and response will send to the router. And also inside the IDS Manager we can view the attacker details with their tags such as attacker type, attacked node name, time and date.

Receiver (End User): the receiver can receive the data file from the router. Service provider will send data file to router and router will accept the data and send to particular receiver (A, B, C, D, E and F). The receivers receive the file in decrypted format by without changing the File Contents. Users may receive particular data files within the network only

Router: The Router manages a multiple nodes to provide data storage service. In router number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and routing path details. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then flow will be send to IDS manager and router will connect to another node and send to particular receiver.

4. RESULTS & PERFORMANCE METRICS

We build a prototype of PIT as backscatter nodes in the network. A Java based application for implementation of PIT using and customizes it to incorporate backstatter node identification and algorithms described. This mainly includes user interface for changing the reader commands to allow backscatter nodes to run the algorithm as shown in Figure 1-4. Instead, we collect the traces from the receiver and process them offline.

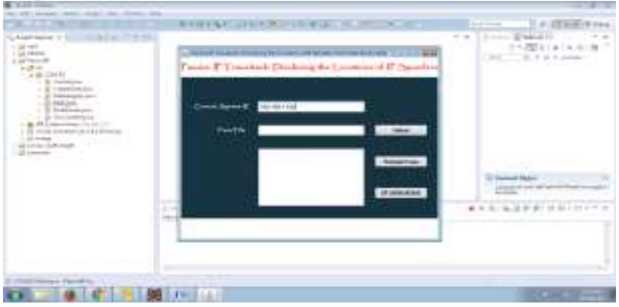


Figure 1: interface for choosing a file to send.

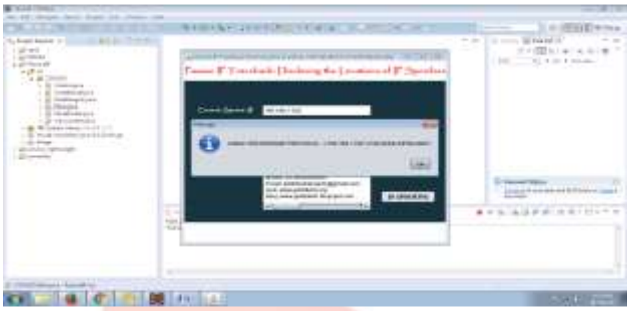


Figure 2: intiating the all nodes for sending the data.

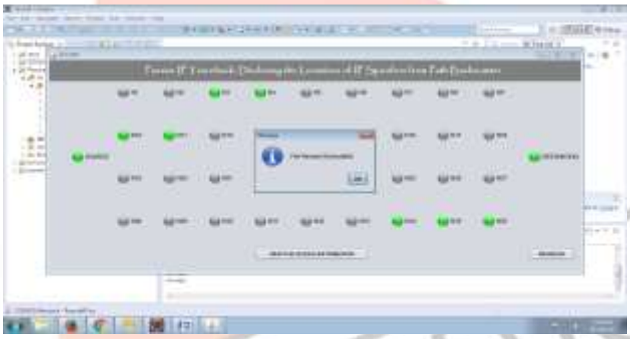


Figure 3: successful sending the data from the source to destination.

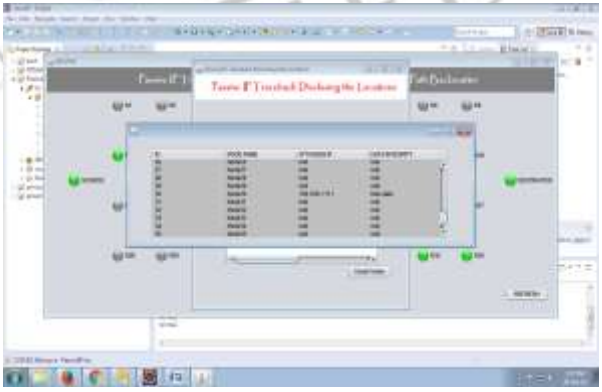


Figure 4: one of the attacks on the router.

PIT is very different from any existing IP traceback mechanism. The main difference is the generation of path backscatter message is not of a certain probability. Thus, we separate the evaluation into 3 parts: the first is the statistical results on path backscatter messages; the second is the evaluation on the traceback mechanisms presented in section. Detecting IP spoofers by using PIT (passive IP Traceback) can be evaluated through graph.

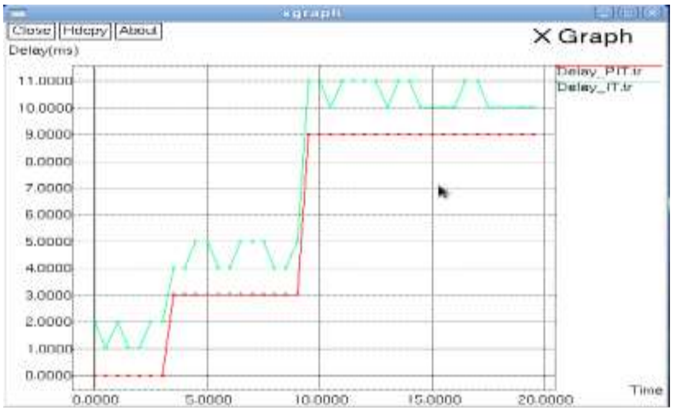


Figure 5: End -To –End Delay

The Red line in the above shows proposed system and green line is for existing system. Figure 5 shows the end to end delay for both existing and proposed system. Delay after applying PIT is less in proposed system as compared to existing system.

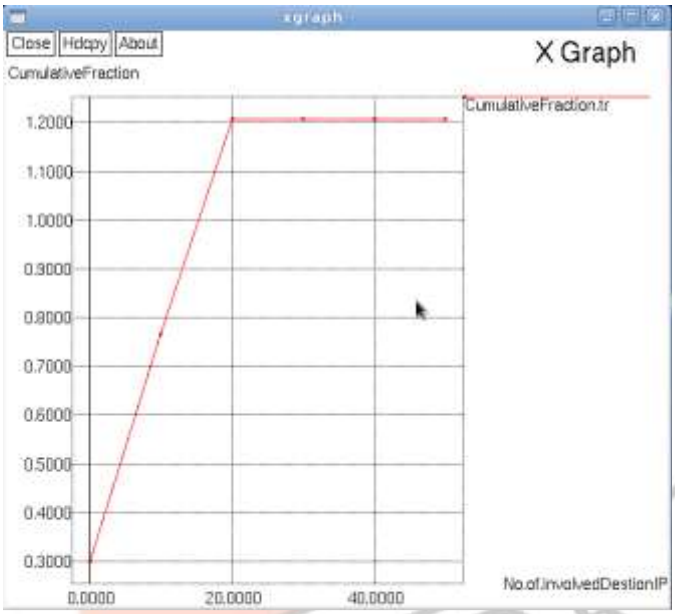


Figure 6: Cumulative Fraction

Figure 6 above shows overall performance in terms of cumulative fraction of packets sent from source to destination of the proposed system.

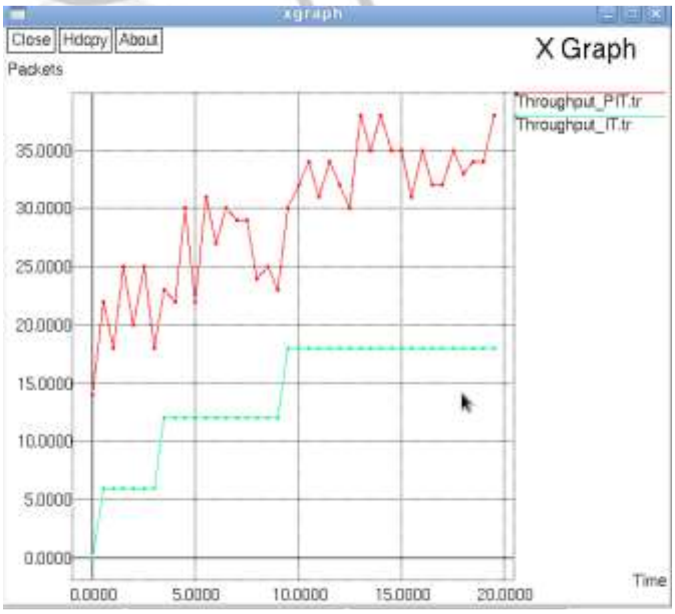


Figure 7: Throughput

Figure 7 shows throughput for existing and proposed system. Throughput is more in proposed system than in existing system.

Figure 8 shows number of bytes received in proposed system is more than the existing system. In above graph the No. of bytes received is more in proposed system this is achieved by PIT (Passive IP Traceback).

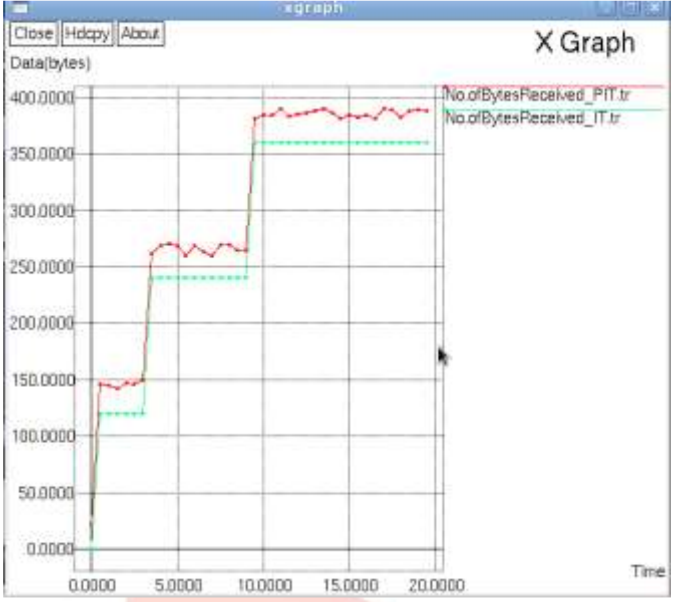


Figure 8: Number Of Bytes Received

5. CONCLUSION

Here the attempt is try to find the locations of spoofers based on investigating the path backscatter messages. In this paper, the Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. The proposed ICMP based passive IP traceback (PIT) system is offered the results to scatter the mist on the locations of spoofers based on investigating the path backscatter messages. Passive IP Traceback (PIT) tracks spoofers based on path backscatter messages and public available information. Specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. An effective algorithm is used to apply PIT in large scale networks and proofed their correctness. The proposed system showed the captured locations of spoofers through applying PIT on the path backscatter dataset. In future work we can extend this to include more power full cryptographic technique.

6. References

[1]. Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE , Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter . NO. 3, MARCH 2015.
[2]. Seung Jae Won, Naveen Garg,"Harden the TCP/IP stack", Accessed October 15,2009..
[3] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity,"ACM Trans, Computer Systems,vol. 24, no. 2, May 2006
[4]. Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, Mar. 1995
[5]. S. M. Bellovin, "Security problems in the TCP/IP protocol suite,"ACM SIGCOMM Comput. Commun.Rev., vol. 19, no. 2, pp. 32–48,Apr. 1989.
[6] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput.Commun. Rev., vol.31, no. 4, pp.3–14, Aug. 2001
[7] S. M. Bellovin, "ICMP traceback messages," Internet Draft: draft-bellovin-itrace-00.txt, Mar, 2000.
[8] Houle, K.J., Weaver, G.M.: Trends in Denial of Service Attack Technology, CERT Coordination Center(October2001), http://www.cert.org/archive/pdf/DoS_trends.pdf.
[9]. Postel, J.: Internet Protocol, Request for Comments 0791, Internet Engineering Task Force (1981)
[10]. M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.
[11]. X. Dimitropoulos et al., "AS relationships: Inference and validation,"ACM SIGCOMM Comput. Commun. Rev., vol. 37, no. 1, pp. 29–40,Jan. 2007.