Two level Authentication and Packet Marking Mechanism for Defending against DoS and DDoS Attacks

P.Ananthi
Assistant Professor,
Kongu Engineering College, India.

P.Balasubramanie
Professor,
Kongu Engineering College,India.

ABSTRACT
Denial of Service (DoS) attacks present a serious problem for Internet communications. IP source address spoofing is used by DoS and DDoS attacks on targeted victim. IP spoofing to forge the source IP address of the packet, and thereby hide the identity of source. This makes hard to detect and defend against such attack. This paper presents a token based authentication and Packet Marking mechanism (TAPM) for preventing IP spoofing. TAPM uses efficient public key cryptography to issue tokens and hash based cryptography for packet marking. It does not require changes or restrictions to the Internet routing protocol, is incrementally deployable, and offers protection from denial-of-service attacks based on IP spoofing. This paper presents efficient algorithm for token generation and evaluates its feasibility and correctness by simulation experiments.

Keywords
DDoS attacks, IP spoofing, packet marking, secret key .

1. INTRODUCTION
IP networks are vulnerable to source address spoofing. Source address spoofing of IP packets on the Internet is one of the major tools used by hackers for denial of service (DoS) attacks. Distributed denial-of-service (DDoS) attacks commonly devastate their victims by sending a vast amount of spoofed packets from multiple attack sites. A DDoS floods the connection of the victim network with a huge amount of packets that lead to a high rate of packet drops for legitimate users. As a consequence the victim spends its key resources processing the attack packets and cannot attend to its legitimate clients. The destination address based packet forwarding is one of the fundamental principles of current Internet [4]. In the forwarding process, the source IP address is not checked in most cases. This makes it very easy to spoof the source address of the IP packet [1]. Most attackers forge source IP addresses to evade responsibility for their malicious packets, and the defenders cannot easily trace the hosts from which these packets are sent, as in the case of DDoS attacks. Packet source IP address validation is challenging activity in dynamic Internet.

In the DDoS defense, many methods have been proposed to prevent IP address spoofing, such as Ingress Filtering [2], SPM[1], Hop-Count [19] and Passport [5]. However, such defense mechanisms have some incurred deficiencies, which lead to the fact that none of them has been widely deployed.

There are few and but not very effective mechanisms that network operators may use today to detect and filter out spoofed packets. The direct method of installing filters only at border routers is contributed inefficient by IP spoofing. The attacker chooses an IP address randomly as the source for different packets and thus makes the protection method infeasible. This paper presents a cryptographic token based authentication mechanism for IP source address spoofing prevention and marking packet using hash. The proposed mechanism concentrate on preventing source address spoofing in Intra -AS level and Inter-AS level.

2. RELATED WORKS
Many approaches against IP spoofing have been proposed by researchers recently. Some of the Inter-AS level methods are based on internet topology, such as uRPF, Ingress Filtering and IP traceback. Ingress filtering [2], SAVE [4], route- based filtering [7], and reverse path filtering [11] methods work on preventing source address spoofing. Ingress filtering aims to prevent IP spoofing by only allowing traffic to enter or leave the network if its source addresses are within the expected IP address range. This approach requires the knowledge about the IP address range of each router. In Internet, this knowledge is hard to obtain and can change over time. Both the Ingress Filtering and uRPF based method filter packets according to the reverse route table information. In network, Ingress filtering is deployed at edge of the network. For effective performance full scale deployment at both core and edge network is needed. Route based filtering, extends ingress filtering and uses the route information to filter out spoofed IP packets. For each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated. If an unexpected source address appears in an IP packet on a transmission channel, then it is identified that the source address has been spoofed, and hence the spoofed packet can be filtered. BGP routing information is used by RPF to filter traffic with spoofed source addresses. However, the filtering granularity of RPF is low[18].

Another mechanism works on detecting source address spoofing near the destination, such as Hop-count Filtering [19]. The routers near the destination can simply drop packets with spoofed source addresses. However, this type of approaches cannot identify the attacking source and can only protect the last-hop link. Others are marking and verification based methods like SPM, and Authentication Header [5]. In Hop-Count, the destination infers the final TTL value in the packets coming from each AS by a special algorithm. Packets with wrong TTL values will be filtered. This method is very easy to implement and works independently. Authentication Header is designed for the secure session between two end systems and could also be used for IP source address verification. The authentication header which is produced from heavy computation is tagged at the source and verified at

the destination. However, as a method for anti-spoofing, its cost is too heavy hence not DOS-resilient. If the attackers pretend to be the end system which is in a session with the victim and sends spoofed packets to the victim, the victim would perform heavy computation on each packet to verify its authenticity and exhaust its resource. SPM is an AS to AS solution, and a unique temporal key is associated with each ordered pair of source and destination networks for filtering. With these approaches the spoofed source address can only be validated at destination. SPM is a lightweight method, but its key-updating mechanism is not attack-resilient.

Passport [5] is a kind of signature-and-verification method, packet passports are cryptographically secure and un-forgeable. Source identifiers protected by packet passports can be directly used in filter expressions to block attack sources. The packet leaving an AS is tagged with several keys, and each router in the path verifies its corresponding key. But this method consists heavy overhead also cause a waste of network bandwidth.

In BASE (BGP antispoofing) mechanism [3], router marks packets with a unique key and uses the key as the incoming direction. Marking the packet with key as resisted to a physical interface is useful for incremental deployment when BASE routers are not physical neighbors. However, BGP updates not transmitted on the same path as normal traffic. When updates and normal traffic forwarded in various paths, routers will find the wrong marking and find legitimate packets as spoofing packets.

PPM method directly use IP packet to store path information which the packet is forwarded. Attack information is recorded after it occurred. IDS sensitivity, complexity of traceback algorithms and reactive solution are the disadvantages of this class of mechanism.

Most of the current methods can't stop spoofing on a fine granularity. Attackers could easily spoof IP address in the same domain. The method proposed in this paper could prevent spoofing strictly and support incremental deployment, and cost effective.

3. SECURITY REQUIREMENTS

3.1 Authentication

For secure communication, both ends should be authenticated and verified their identity. Source address spoofing is usually done by anonymous users. In inter AS communication each user requires strong authentication mechanism and user should be authenticated in the form of various credentials.

3.2 Confidentiality

During data transmission packets would be lost, modified or forwarded to bogus recipient. Packets sent by the origin should be received by the authorized destination. To stop information leakage fine grained protection needed in every level of transmission.

3.3 Integrity

Packets that are forwarded by the sender to another autonomous system must not be modifiable by any unauthorized user. This is assured through verification of packet identity, to avoid spoofing of source address.

3.4 Accessibility

Flooding of spoofed packet flow disrupting regular service of any system, it remains the unavailability of services to authorized users. Legitimate user can not forward or receive packets in time. Preventing spoofed packets automatically prevent service disruptions and denial of service attacks.

4. TOKEN BASED AUTHENTICATION MODEL

Token based mechanism possessed strong cryptographic technique for generating and issuing token in local and global communication. Public key cryptography is used for transferring of secret identification from the authority to the user within an autonomous system. User transfers data to the indented recipient with token. Access controller verifies the token attached with packet, it matches with predefined one then the packet is forwarded to recipient. Control the IP spoofing by verifying the authentication of incoming and outgoing packets. Two level authentication is obtained in node identification and token for communication. Mainly two design principles such as Intra AS level and Inter AS level are involved. In each level efficient and light weight cryptographic technique used for token generation and packet marking.

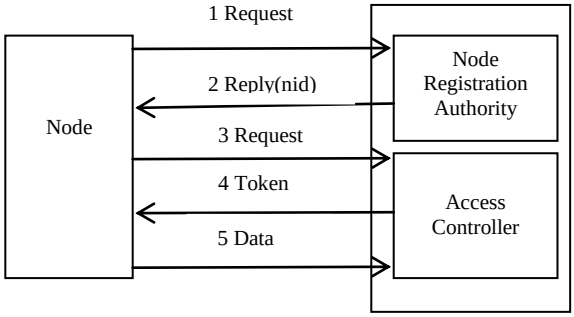

Fig 1: Node registration

4.1 Intra AS level Antispoofing

Each node has IP address and node identification. Node registration authority has maintain a pair of information about every node (IP,nid). In Intra AS level spoofing mechanism every node n enter into connection is first obtain node identification (nid) from Node Registration Authority (NRA). NRA maintains both IP and MAC address of each node and generate nid for these addresses. Node id is generated by exclusive OR of IP and MAC of requested node. Node id is forwarded to corresponding node. The packet destination indented to local node is directly forwarded through neighbor router. Router contains routing table entry with node identification. Router verifies the node id for each request and forwards the packet to indented destination.

4.1.1 Token generation and verification

Autonomous system contains group of nodes. In Internet scenario, node in autonomous system communicates any node within the AS or outside the AS. Edge router verifies the destination address of packet and forward to indented recipient. Routers are not able to distinguish legitimate and spoofed packet. This TAPM mechanism border router maintains the access list of node and verifies the token. Once the node id obtained by entrant node that will be updated with address list and access controller. Whenever the node communicates to outside AS, it communicates through access controller for issuing token. After received the request from node n, AC generates token in the form of MD5. The token would forward to node n using public key cryptography. For each communication token appended to every packet and

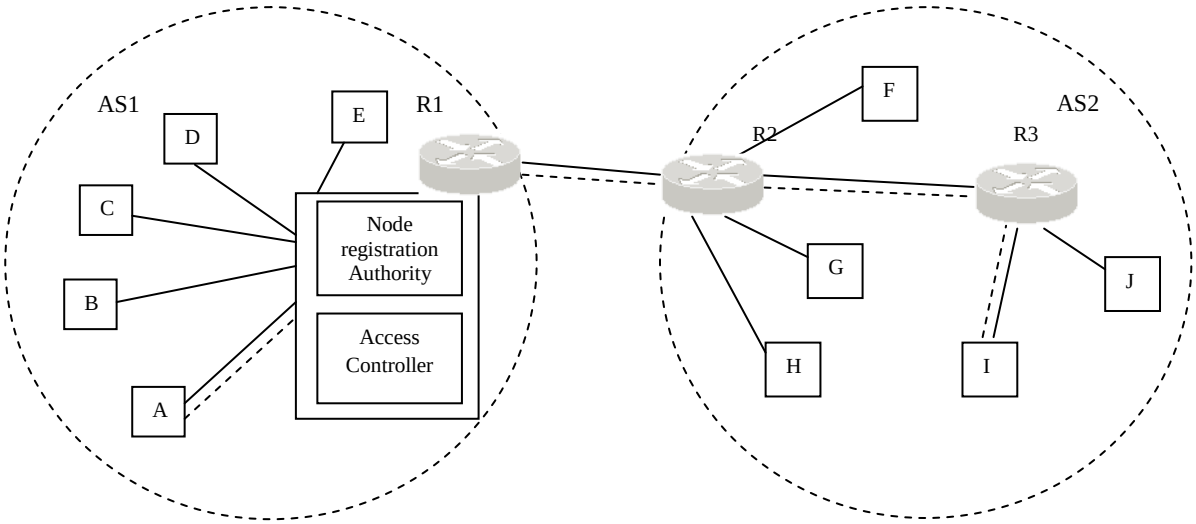

Fig 2: Inter AS level Packet forwarding

forwarded. Packet allowed forwarding outside only after verification of token. The autonomous system border router checks for the presence of the token. Any packet with the token is valid, and any packet without the token is spoofing. If the token is valid, then the token is removed from packet and the packet enters into border router for packet marking.

4.2 Inter AS level Packet marking

Efficient hash based packet marking scheme used for DDoS prevention. For Inter AS communication packet carries its secret. This reduces the overhead in incremental deployment. No prior establishment of secured channel between source and destination node for secret key transmission.

Table.1 Pseudo code for Token generation and Verification

If new node N then
  Register N with NRA
  NRA send nid_i to N
N send request to AC for token
  AC verifies nid of request
If $nid_i = AL\_nid_i$
  Generate token T_i={src_ip|| nid_i|| sessionkey}
  Forward T_i to N
For inter AS communication
N appends T_i with packet and forwards to AC
AC extract T_i
If $T_i = AL\_T_i$
  Remove Ti from packet
  Process packet marking
else
  Discard packet

NRA- Node Registration Authority
Nid (Node identification)= src_ip ⊕ MAC
AL- Access List
AC- Access controller

Certain identification fields in IP packet are extracted and encrypted by hash mechanism. Secret key is obtained from such packet credentials. In 8-bit differentiated Service field last two bits are served for key generation. If the two bits refer 11, secret key generated from exclusive OR of source address with flag field in the packet. If bits refer 10, secret key derived from exclusive OR of source address with identification field of IP header. Source address field is encrypted with secret key using HMAC and appended with packet header. Encrypted credential stored in option field. First 32 bits of option field hold encrypted information.

In figure 2 node A in AS1 communicates with node I in AS2. Router R1 and R2 are border routers of corresponding autonomous systems. Both routers shared secure channel for packet transmission. R1 attaches secure information with packet and R2 verifies that. Legitimate packets are forwarded to intended destination and spoofed packets are discarded.

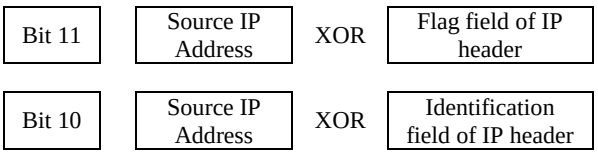

Fig 3: Secret key generation

Router R1 generates secret key and source IP is encrypted by that secret key. Encrypted information stored in first 32 bits of option field. Router R2 extracts the IP header field and obtains first 32 bits of option field. Identify the bit values of last 2 bits in service field and based on that generates secret key. Then incoming source IP is encrypted using this secret key. The computed hash value compare with option field value. If the hash value matches the packet allowed to inside the autonomous system and forward to indented destination.

5. RESULTS AND DISCUSSION

The proposed authentication and packet marking scheme is tested in NS2 simulator. Considering DDOS attack from various nodes to victim by IP spoofing, to detect attack traffic from flood of packets. Legitimate traffic is allowed into autonomous system and rests of them are discarded by verifying source validity at edge router. This scheme reduces internet protocol adaption for incremental deployment and produce reasonable false positive rate.

The graph in Figure 6 demonstrates the progression of decline in the performance of TAPM scheme when an increasing percentage of packets transfer through border router. The

simulation result clearly demonstrates that there is a significant impact on the performance of TAPM scheme. It's obvious that the mitigation of IP spoofing attacks should be addressed on this scheme is well.

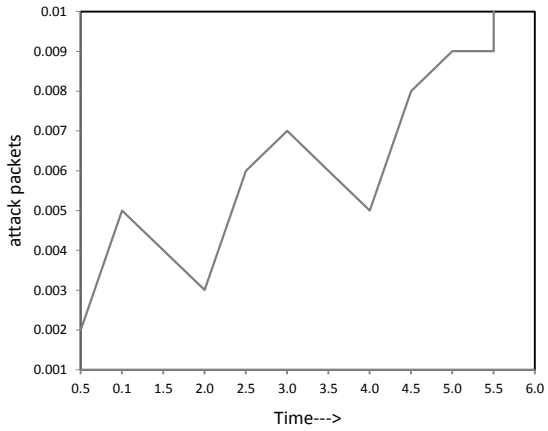

Fig 4: DDos attacks without defense

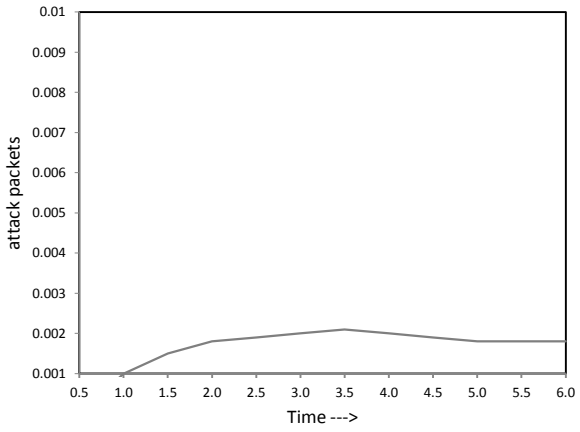

Fig 5: DDos attacks with defense

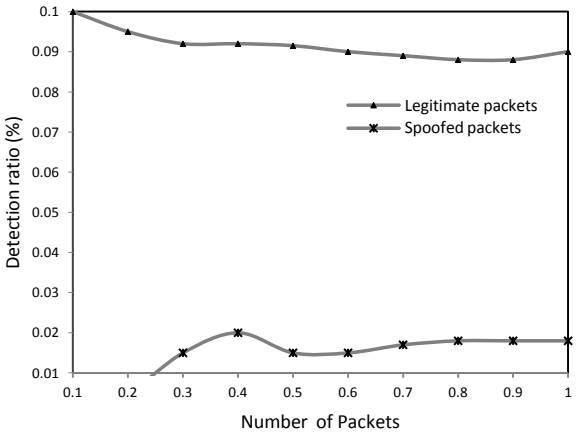

Fig 6: Detection rate of Legitimate Packets

6. CONCLUSION

In the present Internet infrastructure complete elimination of DOS/DDOS attacks are not possible. Differentiating legitimate and bogus packets are still a challenging work. This paper depicts the token based authentication and packet marking mechanism (TAPM) which mitigates the DDOS attack on victim by verifying all incoming and outgoing packets at border router of autonomous system in order to reduce IP address spoofing. TAPM prevents IP spoofing in Intra AS level and Inter AS level. In Intra AS level cryptographic token is generated for each node and verified for each packet transmission. This mechanism can be deployed and does not require any changes to Internet routing protocol. TAPM shows better effectiveness on DoS/DDOS defense in the form of antispoofing which can then easily be evaluated with regard to how completely it minimizes the attack impact. Future work remains to be done in tuning the parameters that define QoS requirements, testing the proposed metric in a variety of attack scenarios.

7. REFERENCES

[1] Bremler-Barr,A.and Levy, H.2005.Spoofing prevention method,Annual Joint Conference of the IEEE Computer and Communications Societies (InfoCom), 536-547.

[2] Ferguson,P.and Senie,D.2000.Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. ACM digital library.

[3] Lee, H., Kwon, M., Hasker,G., And Perrig, A. 2007. BASE:An incrementally deployable mechanism for viable IP spoofing prevention, ACM Symposium on Information, Computer, and Communication Security.

[4] Li,J., Mirkovic, J., Wang, M., Reiher, P. L., And Zhang, L. 2002. SAVE: Source address validity enforcement protocol,IEEEComputer and Communications Societies (InfoCom).1557–1566,DOI:10.1109 /INFCOM. 2002. 1019407 .

[5] Liu, X., Li, A., Yang, X., And Wetherall, D. 2008. Passport: Secure and adoptable source authentication, USENIX Symposium on Networked Systems Design and Implementation, 365-378.

[6] Mohammed A. Alhabeeb, Abdullah Almuhaideb, And Phu Dung Le 2010. Holistic Approach for Critical System Security: Flooding Prevention And Malicious Packet Stopping, Journal Of Telecommunications, Vol. 1(1).

[7] Zhenhai Duan, Xin Yuan, and Jaideep Chandrashekar 2008. ControllingIP Spooing Through Inter-Domain Packet Filter ,IEEE transaction on Dependable and Secure computing, Vol.5: 22-36 .

[8] Lee Soon, Mohamed Othman, Nur Izura Udzir 2009. IP Spoofing Defense: Current Issues, Trend and Challenges, MASAUM Journal Of Reviews and Surveys, Vol.1 (1).

[9] Junaid Israr, Mouhcine Guennoun, and Hussein T. Mouftah . 2009. Mitigating IP Spoofing by Validating BGP Routes Updates, IJCSNS International Journal of Computer Science and Network Security, Vol.9 (5).

[10] Junaid Israr, Mouhcine Guennoun, and Hussein T. Mouftah , 2009. Credible BGP – Extensions to BGP for Secure Networking, Fourth International Conference on Systems and Networks Communications DOI: http: //doi.ieee computer society.org /10.1109 /ICSNC .2009. 74.

[11] Mopari, I. B., Pukale, S. G. and Dhore , M. L., (2008). Detection and Defense Against DDoS Attack with IP Spoofing, International Conference on Computing, Communication and Networking (ICCCN 2008), 1-5.

[12] Soon Hin Khor and Akihiro Nakao 2008. Overfort: Combating DDoS with Peer-to-Peer DDoS Puzzle, IEEE

International Symposium on Parallel and Distributed Processing, 1-8.

[13] Lei Wang, Tianbing Xia, Jennifer Seberry , 2010. Inter-Domain Routing Validator Based Spoofing Defence System, Internaltional conference on Intelligence and Security Informatics,153-155.

[14] Turker Akyuz and Ibrahim Sogukpinar 2009. Packet Marking With Distance Based Probabilities for IP Traceback , First International Conference on Networks & Communications, ACM, 433-438.

[15] Markus Goldstein, Christoph Lampert, Matthias Reif, Armin Stahl and Thomas Breuel "BayesOptimal DDoS Mitigation by Adaptive History-Based IP Filtering" International conference on Networking, DOI: http:// doi. ieeecomputer society .org/ 10.1109 /ICN .2008.64.

[16] Christos Douligeris , Aikaterini Mitrokotsa 2004. DDoS attacks and defense mechanisms: classification and state - of -the-art, Computer Networks, Vol.44 (5): 643–666.

[17] Lersak Limwiwatkul and Arnon Rungsawangr, 2004. Distributed Denial of Service Detection using TCP/IP Headerand Traffic Measurement Analysis, International Symposium on Communications and Information Technologies, Vol 1.

[18] Gupta, B. B.,Joshi, R. C., and Manoj Misra 2010. Distributed Denial of Service Prevention Techniques, International Journal of Computer and Electrical Engineering, Vol. 2(2).

[19] Cheng Jin Haining Wang Kang G. Shin. 2003. Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic, ACM conference on Computer and communications security CCS'03, 30 – 41.

[20] Yao Chen, Shantanu Das, Pulak Dhar, Ab dulmotaleb El Saddik, and Amiya Nayak 2008. Detecting and Preventing IP-spoofed Distributed DoS Attacks, International Journal of Network Security, Vol.7(1): 69-80.

[21] Meiko Jensen, Nils Gruschka and Norbert Luttenberger 2008. The Impact of Flooding Attacks on Network-based Services, The Third International Conference on Availability, Reliability and Security, ACM, 509-513.

[22] Wang Xiao-jing Xiao You-lin 2009. IP Traceback based on Deterministic Packet Marking and Logging, International Conference on Scalable Computing and Communication, 178-182.

[23] Toby Ehrenkranz And Jun Li. 2009. On the State of IP Spoofing Defense, ACM Transactions on Internet Technology,Vol.9(2),DOI: 10.1145 /1516539. 1516541.

[24] Xin Liu and Xiaowei Yang David Wetherall and Thomas Anderson. 2006. Efficient and Secure Source Authentication with Packet Passports,USENIX,2nd workshop on steps to reducing unwanted traffic in Internet, Sruti.

[25] Ying Xu and Roch Gu ´erin. 2005. On the Robustness of Router-based Denial-of-Service (DoS) Defense Systems , ACM Vol. 35(3): 47-60.