International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

DDoS Attack Defense against Source IP Address Spoofing Attacks

Archana S. Pimpalkar[1], Prof. A. R. Bhagat Patil[2]

[1, 2]Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India

Abstract: ***Distributed Denial of Service (DDoS) attacks is the most challenging problems for network security. The attacker uses large number of compromised hosts to launch attack on victim. Various DDoS defense mechanisms aim at detecting and preventing the attack traffic. Source IP address spoofing is one of the most common ways of launching Distributed Denial of Service attacks. In these types of attacks, attack packet's true origin is difficult to identify. Thus, it is very challenging to detect attack packets and handle defense mechanisms against such attacks. In this paper, defense mechanism uses cryptographic technique for identifying attack packets with source IP address spoofing and dropping those attack packets. This mechanism does not require restrictions or changes to internet routing protocols and is easy to deploy. The algorithm is efficient in identifying spoof attack packets and its effectiveness is evaluated by simulation experiments in NS3.***

Keywords: DDoS attacks, spoofing, detection, defense, cryptography, packet filtering

1. Introduction

Distributed Denial of Service (DDoS) is the coordinated attempt to compromise the availability of network resources or servers as shown in figure 1. These attacks cause financial losses by interrupting legitimate access to servers and online services. To mitigate the impact of these attacks strong defense mechanisms are needed that can detect and prevent ongoing attacks. Many defense mechanisms have been proposed and deployed at various locations in current internet. The effectiveness of these mechanisms depends on the performance trade-offs and cost incurred in deployment.

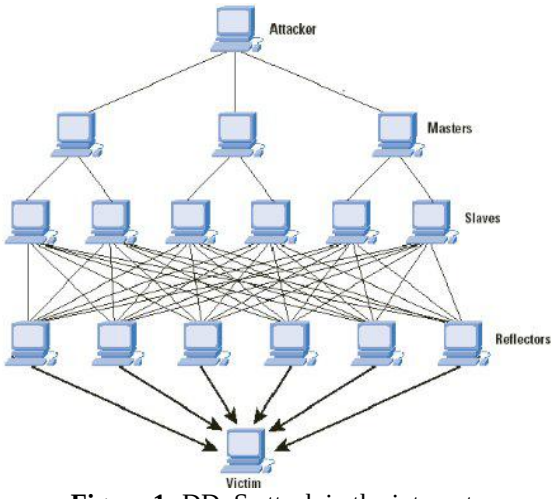

Figure 1: DDoS attack in the internet

In DDoS attacks attack packets are sent to server that consumes all the server resources in processing the received packets which causes denial of service for its intended legitimate clients. DDoS attacks with source IP address spoofing is of two types, namely, reflector attack and direct attack. In reflector attack, attacker uses spoof source IP address hence the response from the receiver of packet or the server to whom request is made goes to some other client on the internet who is not the intended receiver of the response packet. This consumes the network resources as well as the resources of that client thus wasting valuable resources and causing denial of service for the legitimate users. In direct attack the attacker uses spoofing of source IP address in which it may keep same source and destination IP address in the packet sent to server, hence the server continuously send reply and request to itself causing server machine to crash.

In normal packet forwarding approach only destination address in the packets is used and source IP address is not checked most of the times. This makes it easy to use source IP address spoofing for launching DDoS attack. Many defense mechanisms have been proposed against source IP address spoofing such as ingress filtering, hop count based packet filtering, source address validity enforcement, etc. These mechanisms are useful in controlling the spoofed attack packets but it does not completely prevent the spoofed IP address attack.

In this paper, defense mechanism uses cryptographic technique for identifying attack packets with spoof source IP address and dropping the attack packets at the edge router of target victim server. The rest of this paper is organized as follows. In Section 2, recent proposed work for defending against DDoS attacks with source IP address spoofing is presented in brief. In Section 3, defense mechanism that uses Cryptographic technique is presented. In Section 4 Pseudo Code for algorithm is mentioned and Section 5 contains simulation results followed by conclusion in Section 6.

2. Related Work

In this section, review of existing literature on defense against Distributed Denial of Service attacks with source IP address spoofing is presented.

V. A. Foroushani, et al. [1], proposed defense against DDoS attacks containing attack packets with spoofed IP addresses called Traceback based defense against DDoS flooding attacks. The mechanism is implemented closed to attack source, rate-limiting amount of traffic forwarded towards victim. The performance evaluation of the mechanism using real world CAIDA DDoS attack datasets illustrated increase

in throughput of legitimate traffic imposing less overhead on participating routers.

B. Liu, et al. [2], proposed mutual egress filtering for providing protection against IP spoofing based flooding attacks. They have used real internet dataset for obtaining simulation results. The mechanism uses the access control list of autonomous systems (AS) that contains list of rules for applying ingress/egress filtering and unicast reverse path forwarding. This method protects the systems which deploy the mechanism while preventing non-deployers from freely using it. On-demand filtering is provided and the global registry is maintained that contains peering relationships and policies of deplorers. False positive rate reduces by using mutual egress filtering.

In [3], R. Maheshwari, et al. implemented distributed probabilistic hop count filtering based on round trip time. The mechanism was deployed in intermediate network system for maximizing detection rate of attack traffic and minimizing the computation time for filtering attack packets. The simulation results using Matlab 7 showed up to 99% detection of malicious packets. It is advantageous for solving problems of host resources exhaustion and network bandwidth congestion.

F. Soldo, et al. [4], proposed a method for blocking the attack traffic using source based filtering. The access control list maintained at router uses some predefined rules for blocking the IP addresses or prefixes of predefined type, but accessing this access control list is expensive as it is stored in ternary content addressable memory and consumes more space and power. Hence, they suggested aggregation method that uses filtering of source prefixes rather than IP addresses. This method has some drawbacks that it sometimes filters legitimate traffic. To overcome this problem, they formulated the filtering as optimization problem for blocking the attackers with minimum damage and limited filters. They developed cost efficient algorithm and evaluated the simulation results using logs from Dshield.org. The results were beneficial compared to non-optimized filter selection.

K. Verma, et al. [5], proposed method to detect and defend UDP flood attacks under different IP spoofing techniques in VANET. Detection method IPCHOCKREFERENCE used storage efficient data structure and bloom filter for detecting abnormal changes in traffic. It involves random and nonparametric tests for classifying detected events into random spoofing, subnet spoofing or fixed spoofing types by analysing a hash table for the source IP characteristics with less computational requirements. The evaluation on NS2.34 network simulator illustrated accurate detection with low cost.

L. Kavisankar, et al. [6] proposed a technique for preventing spoofing attacks. TCP probing for reply argument packet is used to intelligently append TCP acknowledgement messages. The receiver of TCP SYN sends acknowledgement that change window size or cause packet retransmission. If the supposed source does not behave as intended, it is considered as attack. Overhead and computational cost is involved in receiving and analysing response from client.

In [7], J. Mirkovic, et al. presented comparison between defense mechanisms that filter spoofed attack traffic based on some performance metrics. The available defenses are either deployed at end network or require collaboration of core router for filtering or packet marking. Each defense is evaluated in its controlled environment; hence, they performed a comparative analysis to find out the performance of each mechanism in general network setting with no topology changes. Their work focused on answering some questions that evaluate the performance of these defenses, for example, whether end network deployment can be made efficient using the support of core routers, the required optimal deployment location for core routers, etc. They evaluated the defenses individually and comparatively in common network settings and their results indicate that three defenses, namely hop count filtering, route based packet filtering and PiIp can bring significant reduction in spoofing attacks on Internet users.

Y. Ma [8] proposed defense method based on co-operation of trusted adjacent nodes. This method contains three modules. First module is IP authentication that verifies IP address. If IP address is verified then node is called trusted node and is considered as host reachable in second module i.e. trace-route module and. Third module is filtering in which the hosts identified as not reachable are considered as attackers and their packets are blocked while access to destination node is granted for trusted nodes. The developed mechanism was evaluated in Visual C++ simulation environment that used node information table for storing information of trusted nodes and route information table that maintain routing information of hosts.

P. Du, et al. [9], proposed probing mechanism called Bypass Check for authenticating clients of TCP or UDP services. Detection method employed for detecting abrupt changes in sequential packet symmetry (ratio of transmitted to received traffic) used cumulative sum (CUSUM) technique. Suspicious flows are tested using preferential dropping tests for blocking unresponsive flows. The mechanism was developed on Linux using Click modular router and evaluated on PlanetLab.

B. KrishnaKumar, et al. [10] proposed a hop count based packet processing approach for identifying attackers using spoofed source IP address. In this method the packets from the systems at the same hop count passing through the same router are marked with the same identification number which is the combination of 32 bits IP address of the router path and the encrypted value of the hop count. This value is matched with already stored value at receiving router. Thus, attack packets are identified early and spoofing threats are reduced.

G. Jin, et al. [11] proposed a packet marking scheme called hash based path identification for defending against DDoS attack with spoofing of IP addresses. 16-bit IP Identification field in each packet is used to generate unique identifier corresponding to a path through which packet traverses. Hashing of last 16 bits is performed by routers along the path enabling the victim to differentiate between legitimate and attack packets. HPi2HC filter is presented providing filtering capabilities to victim to drop malicious packets.

In [12], M. Nagaratna, et al. presented a defense mechanism against source IP address spoofing that uses cryptographic technique for classifying attack and legitimate packet and then drop the attack packet. Results illustrated high speed filtering of spoof packets and enhancement in packet transmission.

Y. Xiang, et al. [13], proposed a new IP traceback method called flexible deterministic packet marking for defending against the attack sources. They used two characteristics, namely, flexible mark length strategy and flexible flow based marking scheme for making the method compatible to different network environment and for marking packets according to load of participating router. When a packet enters in a protected network, it is marked by the ingress edge routers. Packet marking consumes memory and CPU time of involved router. Hence to overcome this problem of overload, they suggested flow-based marking scheme. The flow based marking maintains separate state for each flow with the goal of reducing complexity and increasing efficiency. This method isolates those flows that consume more bandwidth and are likely to contain DDoS attack packets. Such packets are marked with certain probability of attack. The data structures used are a dynamic flow table and a FIFO queue. They evaluated the mechanism in real as well as simulation environment. SSFNet simulator was used which is a collection of Java components for network simulation.

B. R. Swain, et al. [14] presented a DDoS mitigation method based on hop count value implemented on server side in wireless environment. A probabilistic approach is developed to count the number of malicious packets. Based on this counts malicious packets are filtered allowing legitimate packets. For calculating hop count time-to-live field in packet is used that cannot be altered by attacker. This method dropped 80 to 85% of attack packets reducing computational time and memory during packet processing.

I. B. Mopari, et al. [15] presented a defense mechanism against DDoS attacks involving spoofing in which spoof attack packets are identified on the basis of hop count that packet traverses before reaching the destination. The method contains two states, namely learning state and filtering state. In learning state attackers are identified while in filtering state attack packets are dropped. This reduces delay in critical path of packet processing. After detecting attacker in learning state, the mechanism switches to filtering state dropping the attack packets. This method is time efficient and reduces CPU memory utilization.

In [16], Y. Shen, et al. presented signature and verification based IP spoofing prevention method for inter-AS and intra-AS levels. In the Intra-AS level, the end host tags a one-time key into each outgoing packet and the gateway at the AS border verifies the key. In Inter-AS level, the gateway at the AS border tags a periodically changed key into the leaving packet and the gateway at border of the destination AS verifies and removes the key.

Z. Duan, et al [17] presented route based packet filtering scheme called inter-domain packet filter deployed at network border routers that identify attacker on the basis of Border Gateway Protocol updates before entering the network system. This method ensures that packet with valid source address are not dropped and when it is not possible to completely stop attack, the packets are forwarded to relatively less number of autonomous systems. Inter-domain packet filters can be deployed independently in the autonomous systems.

S. Malliga, et al. [18] presented deterministic packet marking scheme called modulo technique for interface marking that allows single packet traceback. ID field of IP packet is used for packet marking. Router marks the packet using its interface number rather than IP address associated with it thereby reducing time and contents required for marking. Performance is evaluated using parameters such as convergence time, storage and communication overhead.

C. Chae, et al. [19] proposed IP traceback method which contains agent system that report any abnormal traffic phenomenon, create iTrace message and send it to server system. Destination system detects attack by analyzing iTrace message and collect relevant information which is used for IP traceback. The method is scalable and requires no structural changes to existing network.

H. Wang, et al. [20], presented hop count based packet filtering approach for filtering out the packets with spoofed source IP address near victim servers. Attacker can use IP address of target machine as source IP address. All the acknowledgement and responses intended for sender goes to IP address given by the attacker which consumes all the resources of this machine causing denial of service for intended user. Attacker can launch attack by inserting wrong information in any field of IP header, but cannot deny the hop-count which is calculated from the difference of final and initial time-to-live field in the IP header. The proposed defense mechanism uses this hop count values for validating any packet. Each packet is assigned a packet-id which is calculated by combining the IP address of router path and hop-count. This packet-id is encrypted using a shared secret key. Each router maintains IP-to-hop-count mapping table for each arriving packet. When any new packet arrives at a router, it checks the validity of packet-id and hop-count by comparing with the respective values stored in mapping table. If the packet is not valid, the router creates an attack graph for finding source of attack and filtering out the attack source. This protects the server and also prevents it from becoming an agent for denial of service attack.

A. Yaar, et al [21] presented defense against spoofing DDoS attack using packet marking and filtering. Two marking schemes are used namely stack based marking and write ahead marking for improving performance of Pi marking scheme. Optimal threshold strategy is used for flooding based spoof source IP address attacks. Stack marking is based on TTL field for identifying path from source to destination and in write ahead marking routers mark for its next hop router. The results showed that method is efficient even when only 20% routers are involved in marking process.

B. Al-Duwairi, et al. [22], proposed a hybrid traceback technique that combines the advantages of packet marking and packet logging. In packet marking some path information is inserted by the routers through which they pass for

blocking packets with spoofed source address and in packet logging some information is maintained at the routers in the form of packet digest. Packet marking requires large sequences of packets for finding attack source and packet logging consumes extra resources at the router. Hence, for obtaining traceback results using less number of packets they combined the features of both schemes and presented two schemes called Distributed Link-List Traceback (DLLT) and Probabilistic Pipelined Packet Marking (PPPM). Distributed linked list enables invoking the packet information maintained at router and pipelining enables forwarding of information at one router to other in the intermediate network. They used some new metrics for performance evaluation including path coverage ratio, attack source localization distance, number of attackers' ratio and detection ratio. The experimental results prove the success of these schemes against spoofed attacks, requiring less storage overhead at the routers.

T. K.T. Law, et al. [23], proposed probabilistic packet marking algorithm for attack source traceback. This algorithm creates attack graph at victim site from which intensity of normal traffic can be obtained. The network domains with most of the attack traffic can be predicted from this graph. Their algorithm works for finding the minimum time required for finding the attack location accurately with the available traffic traces. Their experimental evaluation of the developed algorithm applied to general network topology at various packet arrival rates and under different attack patterns gives the minimum time required to find attack source efficiently so that they can be blocked as early as possible for minimizing the damage.

J. Mirkovic, et al. [24], proposed D-WARD, a source end based defense system for differentiating legitimate traffic from attack traffic and filtering the outgoing traffic. Although a source based defense is alone not sufficient, but it gives better results in combination with intermediate network based and destination based mechanisms. Source end defense provides protection against IP spoofing by applying egress filtering. They evaluated the developed mechanism against TCP SYN, UDP and ICMP flood attack in testbed and real environment in LASR lab at UCLA. Their results showed that the developed system adapt to network changes and provide variable responses. They evaluated it for single source as well as for distributed environment.

Y. Xiang, et al. [25] proposed a defense technique of large scale IP traceback called flexible deterministic packet marking. Packet flow is marked at router interface close to source that passes unchanged through all routers. Scalable marking is provided based on the deployed network protocols within protected network. Dynamic flow table is used to store flow records which is hashing of source and destination IP addresses. Flows that consume unfair share of bandwidth are identified and packets in these flows are dropped. The simulations were performed using SSFNet network simulator by embedding three new Java packages into it namely, Encoding sub-system, Reconstruction sub-system and Flow-based Marking sub-system.

3. Defense Algorithm Using Cryptographic Technique

Source address spoofing is done by anonymous users; hence both communicating ends must be authenticated and verified by their identity for secure communication. Sending spoofed packets disrupts the services to legitimate users. Thus, preventing spoofed packets automatically prevents Distributed Denial of Service attacks. For providing authentication to the packets transmitted from clients to the server, hash based cryptographic technique is used. Certain identification fields in the IP header of packet are extracted and encrypted by using hash mechanism. Secret key required for the encryption process is obtained from the packet credentials. In the 8 bit Type-of-Service field of IP header the first 6 bits are for Differentiated Service Field (DSF) and the last two bits stands for Explicit Congestion Notification (ECN). These last two bits are used in the process of secret key generation. Different key is generated for different combination of these two bits. If the two bits are 11, then secret key is generated from exclusive OR of source address and flag field in the IP header of packet. And if the two bits are 10, then secret key is generated from exclusive OR of source address and identification field of IP header of packet. Encryption of source address is performed with the secret key generated using HMAC. The generated result is appended with packet header in option field. First 32 bits of option field of IP header represent the encrypted information.

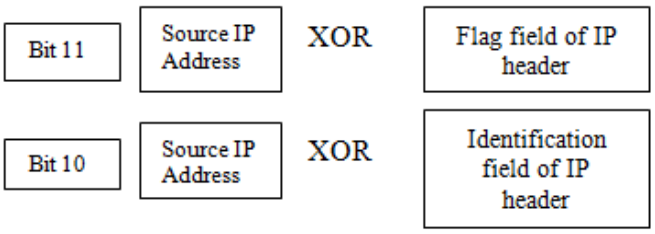

Figure 2: Secret key generation.

Border routers of client and server are responsible for establishing shared secure channel for communication. Border router of client attaches secure information to all the forwarded packets towards server. The border routers of server verify this secure information. All the legitimate packets are forwarded to the server; and the attack packets are identified and dropped before reaching the target victim server. Router near the client generates the secret key and encrypts the source address using this secret key. The encrypted information is stored in the first 32 bits of option field of IP header. Router near the server receives the packets, extract the IP header for received packet and obtain the first 32 bit of option field from that IP header. It observes the last two bits of the Type-of-Service field and accordingly generates the secret key. The source address of the incoming packet is encrypted using this key and this hash value is compared with the value obtained from the first 32 bits in the option field. If both the values matches, then packet is considered as legitimate packet and forwarded to the server; otherwise the packet is considered as attack packet with spoof source IP address and dropped at the router.

4. Pseudo Code

If new node N then
  Generate hash H_i = {src_ip|| node id || sessionkey}
  Forward H_i to N
  N appends H_i with packet and forwards
  Extract H_i at border router
  If H_i = Calculated H_i
      Remove H_i from packet
      Process packet marking
  Else
      Discard packet

5. Simulation Results

The developed defense mechanism has been tested in simulation environment created by using NS3 Network Simulator. DDoS attack is created from distributed attackers using IP address spoofing. Each normal packet contains appended information that provides authentication. This authentication is verified at the edge router of victim network. Attacker's packets are identified and dropped at the router before reaching the target server. The results obtained from simulation showed that the attack packets are identified efficiently with 0% false positives.

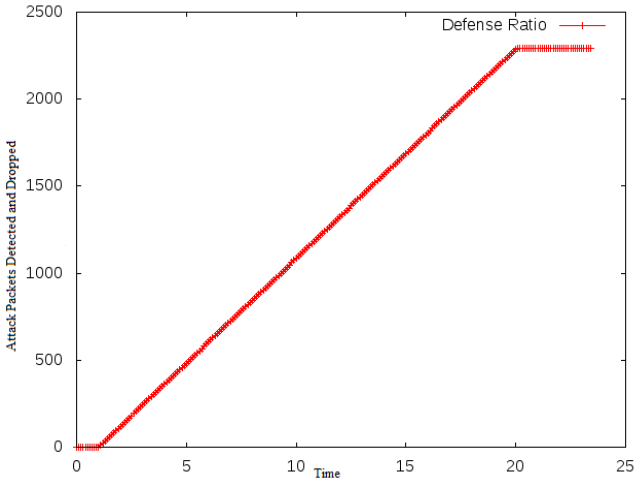

Figure 3: Total attack packets detected and dropped

The graph in figure 3 illustrate that as the attack packets are increasing with time, all attack packets are verified and dropped at the router. For example, during simulation experiment attacker network sent 2287 TCP attack packets for 20 ms. All the attack packets were identified at 20.1 ms and dropped thus preventing DDoS attack to the victim.

The graph in figure 4 illustrates that large number of attack packets are reaching the server before applying defense and attack packets reaching the target server are almost zero after applying defense mechanism. Also normal packets reaching the target server before and after applying defense are same (indicated by overlapping of red and green lines respectively) which indicates that the defense mechanism does not affect the normal traffic.

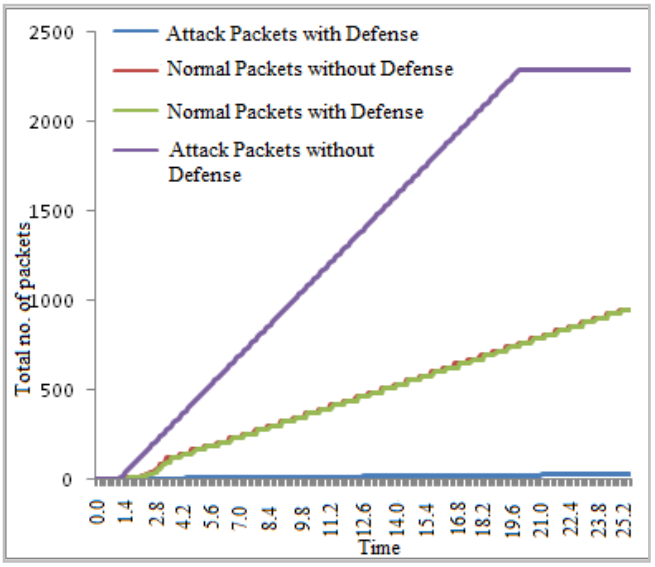

Figure 4: Total packets transmitted with and without defense

6. Conclusion

In this paper, we have presented an overview of DDoS defense schemes against source IP address spoofing developed so far and lightweight cryptographic technique for defending against spoofing attacks that requires no additional overhead on the routers and no changes in the internet routing protocols. It is very challenging to defend against spoofing address attacks as packet origin is not known. By providing authentication to each packet at the client side and verifying the packet identity at the routers near the server can efficiently identify the attack packets with fake source IP address. Such packets are dropped before reaching the target server thus allowing the legitimate clients to access the server resources. The simulation results illustrated efficient defense against DDoS attack having 99.9% accuracy with 0% false positives and quick response time.

References

[1] V. A. Foroushani, A. N. Zincir-Heywood, "TDFA: Traceback-based Defense against DDoS Flooding Attacks", *IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 597-604, May 2014.
[2] B. Liu, J. Bi, A. V. Vasilakos, "Toward Incentivizing Anti-Spoofing Deployment", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 436-450, March 2014.
[3] R. Maheshwari, C. R. Krishna, M. S. Brahma, "Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique", *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 206-209, Feb. 2014.
[4] F. Soldo, K. Argyraki, A. Markopoulou, "Optimal Source-Based Filtering of Malicious Traffic", *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 381-395, April 2012.
[5] K. Verma, H. Hasbullah, A. Kumar, "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET", *IEEE*

3rd International Advance Computing Conference (IACC), pp. 550-555, Feb. 2012.
[6] L. Kavisankar, C. Chellappan, "A Mitigation model for TCP SYN flooding with IP Spoofing", *IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 251-256, June 2011.
[7] J. Mirkovic, E. Kissel, "Comparative Evaluation of Spoofing Defenses", *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 218-232, March-April 2011.
[8] Y. Ma, "An Effective Method for Defense against IP Spoofing Attack", *IEEE International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, pp. 1-4, Sept. 2010.
[9] P. Du, A. Nakao, "Mantlet Trilogy: DDoS Defense Deployable with Innovative Anti-Spoofing, Attack Detection and Mitigation", *19th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1-7, Aug. 2010.
[10] B. KrishnaKumar, P. K. Kumar, R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks", *IEEE International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 271-273, March 2010.
[11] G. Jin, F. Zhang, Y. Li, H. Zhang, J. Qian, "A Hash-based Path Identification Scheme for DDoS Attacks Defense", *IEEE 9th International Conference on Computer and Information Technology*, pp. 219-224, Oct. 2009.
[12] M. Nagaratna, V. K. Prasad, S. T. Kumar, "Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking based Detection and Filtering (EMDAF)", *IEEE International Conference on Advances in Recent Technologies in Communication and Computing*, pp. 753-755, Oct. 2009.
[13] Y. Xiang, W. Zhou, M. Guo, "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 4, pp. 567-580, April 2009.
[14] B. R. Swain, B. Sahoo, "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method", *IEEE International Advance Computing Conference (IACC)*, March pp. 1170-1172, March 2009.
[15] I. B. Mopari, S. G. Pukale, M. L. Dhore, "Detection and Defense Against DDoS Attack with IP Spoofing", *International Conference on Computing, Communication and Networking (ICCCN)*, pp. 1-5, Dec. 2008.
[16] Y. Shen, J. Bi, J. Wu, Q. Liu, "A Two-Level Source Address Spoofing Prevention based on Automatic Signature and Verification Mechanism", *IEEE Symposium on Computers and Communications*, pp. 392-397, July 2008.
[17] Z. Duan, X. Yuan, J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters", *IEEE Transactions on Dependable And Secure Computing*, vol. 5, no. 1, pp. 22-36, Jan-Mar. 2008.
[18] S. Malliga, A. Tamilarasi, "A defensive mechanism to defend against DoS/DDoS attacks by IP traceback with DPM", *IEEE International Conference on Computational Intelligence and Multimedia Applications*, pp. 115-119, Dec. 2007.
[19] C. Chae, S-H. Lee, J-S. Lee, J-K. Lee, "A Study of Defense DDoS Attacks using IP Traceback", *IEEE International Conference on Intelligent Pervasive Computing*, pp. 402-408, Oct. 2007.
[20] H. Wang, C. Jin, K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 40-53, Feb. 2007.
[21] A. Yaar, A. Perrig, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense", *IEEE Journal on Selected Areas In Communications*, vol. 24, no. 10, pp. 1853-1863, Oct. 2006.
[22] B. Al-Duwairi, M. Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback", *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 5, pp. 403-418, May 2006.
[23] T. K.T. Law, J. C.S. Lui, D.K.Y. Yau, "You Can Run, But You Can't Hide: An Effective Statistical Methodology to Trace Back DDoS Attackers", *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 9, pp. 799-813, Sept. 2005.
[24] J. Mirkovic, P. Reiher, "D-WARD: A Source-End Defense against Flooding Denial-of-Service Attacks", *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 216-232, July-Sept. 2005.
[25] Y. Xiang, W. Zhou, "A Defense System Against DDoS Attacks by Large-Scale IP Traceback", *IEEE 3rd International Conference on Information Technology and Applications (ICITA)*, pp. 431-436, July 2005