ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Defense against DDoS Attacks Using IP Address Spoofing

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

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

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

ABSTRACT: Distributed Denial of Service (DDoS) attacks is launched by large number of compromised host to interrupt the services of the legitimate users. It is most challenging to defense against such attacks because most of the attacker use source IP address spoofing in order to hide their identity and such attack packets appear to the target server as if they came from a legitimate client. In this paper, defense mechanism is presented that classify packets as legitimate or attack using cryptographic technique and filter the attack packets. Once the packets are classified attack packets are dropped at the border router of the target network before reaching the victim. The mechanism is easy to implement without requiring restrictions or additional changes to internet routing protocols. The efficiency of algorithm in identifying spoof attack packets is evaluated by simulation experiments in NS3.

KEYWORDS: DDoS attacks, spoofing, detection, defense, cryptography, filtering.

I. INTRODUCTION

Distributed Denial of Service (DDoS) is the launched by large number of distributed attackers in a co-ordinated manner to interrupt the services of the legitimate clients and excessively consume the target resources that prevents the server from responding to legitimate clients. The attack tools are evolving continuously, but there are not enough effective defense mechanisms against such attacks. Defense mechanism must b able to classify each packet that is travelling across the router as legitimate or attack and packets identified as the attack packets must not be forwarded to the target. This can prevent the DDoS attack and save valuable target resources.

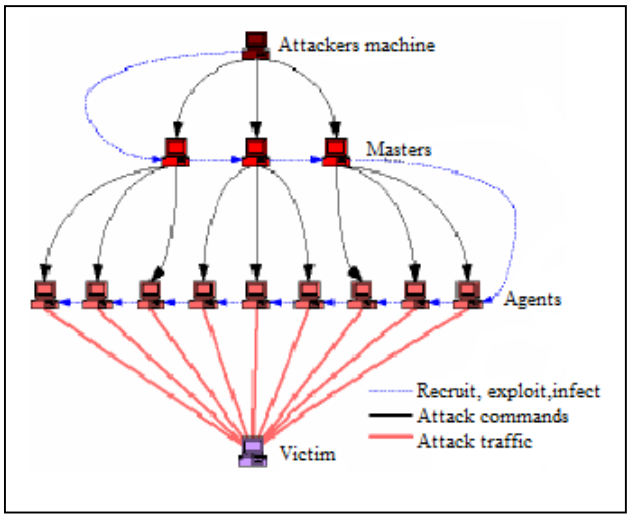

Fig. 1: DDoS attack model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

DDoS attacks with source IP address spoofing is of two types. First is direct attack in which the attackers send malformed packets with fake source IP address and second is reflector attack in which attacker send large number of attack packets through large number of compromised hosts in the network. Network resources are thus wasted in processing such attack packets causing denial of service to legitimate clients.

While forwarding packets towards destination only destination address is often used and source address is never verified. Attackers take advantage of this fact for launching attack using spoofing of source IP address in order to hide their identity and avoiding the possibility of getting caught. 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. that are useful in controlling the spoofed attack packets but complete prevention of spoofed IP address attack is still a challenging problem.

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 server. The rest of this paper is organized as follows. In Section II, recent proposed work for defending against DDoS attacks is presented in brief. In Section III, defense mechanism that uses Cryptographic technique is presented. In Section IV Pseudo Code for algorithm is mentioned and Section V contains simulation results followed by conclusion in Section VI.

II. RELATED WORK

In this section, review of existing literature on defense mechanisms against Distributed Denial of Service attacks is presented.

S. Yu, et al. [1], proposed a dynamic resource allocation technique for protecting individual customers of cloud during DDoS attack ensuring quality of service during attack. The cloud environment is capable of controlling the resource allocation because it has large number of resources to allocate to individual user. The resource allocation strategy used in clouds plays vital role in mitigating the impact of attack by giving access to resources. In cloud environment the success of attack or defense depends upon who is holding more resources, attacker or cloud user. The dynamic extra resource allocation prevents starvation, thus defending against DDoS attack. They also presented queue based model of resource allocation under various attack scenarios. They used real world data set available on DDoS attack for analysis of resource allocation. In normal scenario, the virtual server in cloud has intrusion prevention system (IPS) for security purpose and queue that maintains the list of incoming packets. During attack situation, large number of packets passes through the queue as botnets are used for launching DDoS attacks there arise a need of duplicating the resources to increase the intrusion prevention systems. This is made possible by dynamic resource allocation. They evaluated the performance of developed model through simulations in normal and attack situations and using Amazon EC2 cloud for obtaining results.

B. Liu, et al. [2], proposed mutual egress filtering for providing protection against IP spoofing based flooding attacks using real internet dataset for obtaining simulation results. Access control list of autonomous systems (AS) is used which contains list of rules for applying ingress/egress filtering. 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.

In [4], A. Compagno, et al. presented defense against inertest flooding distributed denial of service attacks in Named Data networking. Interest flooding requires limited resources to launch attack. Pending interest table is maintained at routers for avoiding duplicate interests. Poseidon framework is introduced for detection and mitigation of inertest

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

flooding attacks. The evaluation of the framework over network simulation environment using NS3 showed that it is possible to utilize up to 80% available bandwidth during attack using this framework.

J. Francois, et al. [5], proposed collaborative architecture, FireCol which is composed of Intrusion prevention Systems at the Internet Service Providers level. It uses the rings of intrusion prevention systems around a host as single prevention system is not sufficient to defend flooding based DDoS attacks. The attacks are detected by observing the detection window for finding out the deviation of traffic from normal traffic pattern. Based on the percentage of deviation, the attacks are classified as low or high potential attack. FireCol system has some rules defined for subscribers that match a pattern of IP addresses. The packet processor in the system examines the incoming traffic and update counter and frequencies whenever a rule is matched. Metrics manager calculate entropies and relative entropies. Selection manager checks whether the traffic distribution was within the profile. A score is assigned to each selected rules based on entropies and frequencies. Lastly, collaboration manager confirms flooding attack if the traffic generated is higher than customer's capacity. False positive rate is low for this mechanism and also it is robust, computational and communication overhead is less. The results have been verified using real world datasets of normal and attack traffic pattern.

F. Soldo, et al. [6], 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. [7], 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.

S. Khanna, et al. [8], presented an adaptive selective verification method for preventing DDoS attacks. It involves server initiated selective random sampling for incoming packet and classification of packets as attack or legitimate. In this method bandwidth is used as currency and each client wanting to access server resources has to spend bandwidth for obtaining server state. Protection level employed by the clients dynamically adjusts to the level of attack. In this method client C sends request to server for which it gets acknowledgement from the server. Time-out window of duration T is used by clients based on the worst-case round trip time between client and server. During attack client does not receive acknowledgement for its request. Replication protocol is used by clients in this situation. Replication rate is proportional to current attack rate. On the server side randomized sampling is used to select a random sample of sequentially arriving packets. This prevents the timing attacks. The simulation carried on network simulator NS2 illustrates the effectiveness of developed mechanism at variable attack rates.

L. Kavisankar, et al. [9] 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 [10], 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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 [11] 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. [12], 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. [13] 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. [14] 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 [15], 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. [16], 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. [17] 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. [18] 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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 [19], 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 [20] 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. [21] 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. [22] 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.

A. Yaar, et al [23] 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.

T. K.T. Law, et al. [24], 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.

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.

III. DEFENSE ALGORITHM

Both communicating ends must be authenticated and verified by their identity for secure communication for preventing attacks with source IP address spoofing that causes denial of service to legitimate users. Hash based cryptographic technique is used for providing authentication to the packets transmitted from clients to the server. Certain fields in the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

IP header of packet are extracted and encrypted by using hash mechanism. Secret key required for the encryption process is obtained from certain packet field values. 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, i.e. ECN bits are used in the process of secret key generation. Different combination of these two bits results in generation of different key. Secret key is generated from exclusive OR of source address and flag field in the IP header of packet ff the two bits are 11. And secret key is generated from exclusive OR of source address and identification field of IP header of packet if the two bits are 10. The process of secret key generation is shown in figure 2. HMAC is used for encryption of source address with the secret key generated. The generated result is stored in first 32 bits of option field of IP header of packet being transmitted.

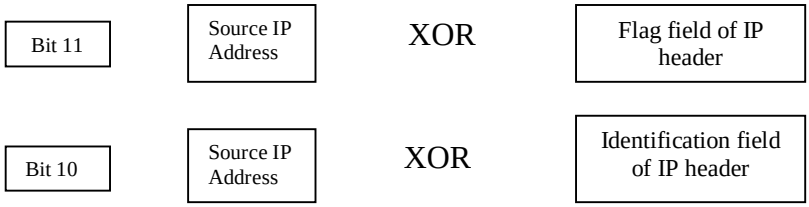

Fig. 2: Secret key generation.

Border router of client attaches this secure information to all the forwarded packets towards server which is verified by border router of receiving network. Based on this verification packets are classified as attack packets or normal packets. Router near the client network 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 network receives the packets, extract the IP header for received packet and obtain the first 32 bit of option field from that IP header. Secret key is generated based on the combination of bits in ECN field. The source address of the incoming packet is encrypted using this key. The hash value obtained is compared with the value obtained from the first 32 bits in the option field of received packet. 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.

IV. PSEUDO CODE

If new node N then
Generate hash H_i= {src_ip|| node id|| session-key}
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

V. SIMULATION RESULTS

Simulation environment is created using NS3 network simulator for testing the developed defense mechanism. DDoS attack is launched using IP address spoofing. Each normal packet contains appended secret information that provides authentication. This secret information is verified at the border router of target network. Attacker's packets are separated from normal packets 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.

The graph in figure 3 shows that as the attack packets are increasing with time, at the same time all attack packets are verified and dropped at the router. During simulation experiment 1130 normal TCP packets were sent to the server and attacker network sent 2289 TCP attack packets containing spoofing of source IP address in 20 ms. The algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

efficiently classified all the normal and attack packets and DDoS attack was prevented by dropping the packets at border router before reaching the target.

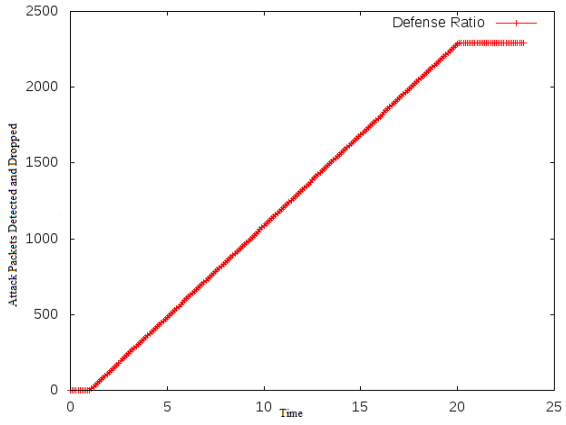

Fig. 3: Total attack packets detected and dropped

The graph in figure 4 shows attack packets reaching the target server before applying defense are large in number and attack packets reaching the target server after applying defense mechanism are almost zero, while normal packets reaching the target server before and after applying defense are same (indicated by overlapping of red and green lines respectively) indicating that normal traffic is forwarded unaffected by the defense mechanism.

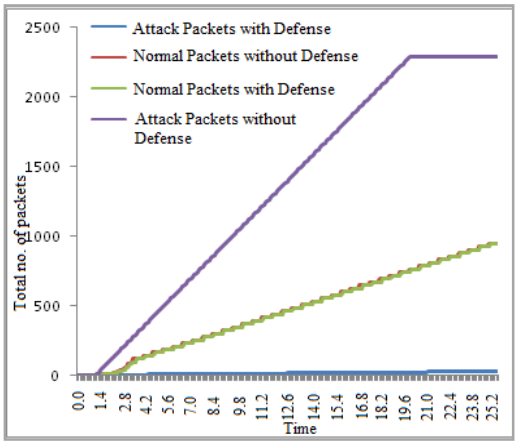

Fig. 4: Total packets transmitted with and without defense

VI. CONCLUSION

In this paper, we have presented a lightweight cryptographic technique for defending against spoofing attacks that requires no additional overhead on the routers and no changes in the internet routing protocols. By providing authentication to each packet at the client side and verifying the packet identity at the routers near the target server can efficiently identify the attack packets with fake source IP address. Attack packets are separated from normal packets and dropped before reaching the target server while normal packets are forwarded unaffected thus allowing the legitimate clients to access the server resources. The simulation results illustrated efficiency of defense mechanism against DDoS attack with 99.9% accuracy, 0% false positives and quick response time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

REFERENCES

[1] S. Yu, Y. Tian, S. Guo, D. Wu, "Can We Beat DDoS Attacks in Clouds?", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2245-2254, 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, 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, 2014.
[4] A. Compagno, M. Conti, P. Gasti, G. Tsudik, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", IEEE 38th Conference on Local Computer Networks, pp. 630-638, 2013.
[5] J. Francois, I. Aib, R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1828-1841, 2012.
[6] 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, 2012.
[7] 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, 2012.
[8] S. Khanna, S. S. Venkatesh, O. Fatemieh, F. Khan, C. A. Gunter, "Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks", IEEE/ACM Transactions on Networking, vol. 20, no.3, pp. 715-728, 2011.
[9] 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, 2011.
[10] J. Mirkovic, E. Kissel, "Comparative Evaluation of Spoofing Defenses", IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 218-232, 2011.
[11] 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, 2010.
[12] 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, 2010.
[13] 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, 2010.
[14] 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, 2009.
[15] 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, 2009.
[16] 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, 2009.
[17] 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, 2009.
[18] 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, 2008.
[19] 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, 2008.
[20] 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, 2008.
[21] 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, 2007.
[22] 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, 2007.
[23] 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, 2006.
[24] 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, 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, 2005.