A Survey on Network-Based DoS and DDoS Attack and Defense Mechanisms

Dr.N.Arumugam
Lecturer (SG), Dept of ECE, Nachimuthu Polytechnic College, Pollachi, Tamilnadu, India

Abstract- **Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. The phenomenal growth of the Internet owes much to the simplicity of its design principles, which allow to widely interconnecting heterogeneous systems. The design principles of Internet's do not provide any form of control for a server to dictate how much traffic it wants to receive and from whom. As a result, Internet hosts are vulnerable to network attacks like Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) attacks, whose economic and social impact has grown to considerable proportions. One of the major threats to the Internet is source IP address spoofing. In current Internet communication world, validity of the source of IP packet is an important issue. The problems of IP spoofing alarm legitimate users of the Internet. This paper review recent progress of IP spoofing detection and defenses by various researchers.**

Index Terms- Network Security, DoS attacks, DDoS attacks, IP Spoofing, Time-to-Live.

INTRODUCTION

In TCP/IP networks, packets sent from one host to another consist of an IP header that contains source IP address, destination IP address, source port and destination port. The source IP address identifies the sending host and destination IP address identifies the receiving host. The recipient host directs replies to the sender using this source IP address. However, the IP at the recipient has no means to validate the authenticity of the packet's source address. This vulnerability can be exploited by attackers to send packets with forged or spoofed source IP address. Sending IP packets with forged source addresses is known as packet spoofing or source IP spoofing.

IP Spoofing Techniques

When a client attempts to establish a TCP connection to a server, the client and the server exchange a set of sequence of messages. This connection technique is called TCP three way handshakes. To establish a TCP connection first, the client sends a SYN packet to the server requesting a new connection with initial sequence number (ISN). To acknowledge the receipt of this SYN packet, the server replies the client by sending it a SYN/ACK packet with an Acknowledgment (ACK) number of ISN+1. Finally, the client sends the server an ACK packet acknowledging the receipt of the SYN/ACK packet. If the server does not receive the final ACK packet, it will retransmit the SYN-ACK 5 times, doubling the time-out value after each retransmission. The initial time-out value is 3 seconds, so retries are attempted at 3, 6, 12, 24, and 48 seconds.

It is notable that in the above 3-way handshake process, the server will remain in half-open connection state before receiving final ACK packet. Since the server's backlog queue allocated for maintaining half-open connections is finite, so there is a limitation on the maximum number of half-open connections that can be maintained. The TCP SYN flooding attack works just by exploiting the above limitation of three way handshake. The attack begins when the master sends control packets to agents, ordering them to attack a given victim server. The agents then start at the same time to use one of the IP spoofing techniques to send a stream of flooding SYN packets with spoofed IP addresses to the victim's server. Since all previous spoofed IP addresses are inaccessible, so the victim's server cannot reach them. As a result, many half open connections will be created, leading to an exhaustion of server's backlog queue and thus the dropping of any new legitimate SYN packets (denial of service).

Detection and Defense Mechanism during the Packet Transmission

In general router-based and victim-based are two distinct approaches used by the research community to detect and prevent DDoS attacks. The victim-based method uses the cooperation between the victim and its upstream routers to locate attack sources and filter attack traffic close to its source. The router-based approach is a distributed defense architecture that can detect attack traffic close to its source. This method is based on a cooperative scheme in which routers can efficiently share evidence of attacks. The router-based approach makes improvements to the routing infrastructure, while the victim based approach enhances the resilience of Internet servers against attacks. Compared to the router-based approach, the victim-based approach has the advantage of being immediately deployable.

Ingress/ Egress filtering

Ingress filtering (RFC 2827) is based on the internal capability of an edge router or a gateway to identify internal IP addresses from external IP addresses. So if a router receives IP packets with external IP addresses on an internal filtering is to block such packets. Egress filtering is archetypal to ingress filtering. If a router or a gateway receives IP packets with an internal IP addresses on an external IP interface, then this is a spoofed packet and should be blocked [1].Ingress Filtering for Multihued Networks (RFC 2827) is designed to limit the impact of distributed denial of service attacks, by denying traffic with spoofed addresses access to the network, and to help ensure that traffic is traceable to its correct source network. As a side effect of protecting the Internet against such attacks, the network implementing the solution also protects itself from this and other attacks, such as spoofed management access to networking equipment [2].

Route-based filtering

Further extend the progress of filtering efficiency of spoofed packets implemented as Route-based filtering (RBF).RBF brings instant benefit to the deploying network, and that it can drastically reduce the amount of spoofed traffic in the Internet. The authors’ work was separated into two parts: populating incoming table entries and updating them when routing changes occur, and filtering spoofed packet using incoming table information and ingress filtering. The authors designed Clouseau system to handle the first part and RBF handles the second part. Clouseau system randomly drops TCP data packets that arrive at router and observe subsequence retransmission from the same source. RBF at the same time filters spoofed packets by comparing packet's incoming interface with the expected interface [3].

RBF works well for smaller networks, but for the complexity of the current architecture of the Internet, RBF will not scale. It will also be a problem for RBF to detect spoofed packets for a multihomed network and autonomous systems (AS). If the spoofed packet is sent and route from one network through another network, the packet will be detected as coming from another interface

Spoofing Prevention Method

Another new approach for filtering spoofed IP packets, called spoofing prevention method (SPM), is proposed and this method enables routers closer to the destination of a packet to verify the authenticity of the source address of the packet. This stands in contrast to standard ingress filtering which is effective mostly at routers next to the source and is ineffective otherwise. In the proposed method a unique temporal key is associated with each ordered pair of source destination networks (AS's, autonomous systems). Each packet leaving a source network S is tagged with the key K(S, D), associated with (S, D), where D is the destination network. Upon arrival at the destination network the key is verified and removed. Thus the method verifies the authenticity of packets carrying the address s which belongs to network S. An efficient implementation of the method, ensuring not to overload the routers, is presented. The major benefits of the method are the strong incentive it provides to network operators to implement it, and the fact that the method lends itself to stepwise deployment, since it benefits networks deploying the method even if it is implemented only on parts of the Internet. These two properties, not shared by alternative approaches, make it an attractive and viable solution to the packet spoofing problem [4].

IP source address spoofing is used by DDoS and DrDoS attacks in the Internet. This paper presents a signature-and-verification based IP spoofing prevention method, automatic peer-to-peer based anti-spoofing method (APPA). APPA has two levels: intra-AS (autonomous system) level and inter-AS level. 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. The most prominent characteristic of APPA is the automatically synchronizing state-machine, which is used to update keys automatically and effectively. The benefits of APPA are: (1) preventing IP address spoofing strictly, end systems capsulate even spoof addresses in the same AS or subnet, (2) providing very low running and management costs, (3) supporting anti-replay attacks and incremental deployment [5].

Automatic Peer-To-Peer Anti-Spoofing (APPA)

A signature-and-verification-based method, automatic peer-to-peer anti-spoofing (APPA), is proposed to prevent IP source address spoofing. In this method, signatures are tagged into the packets at the source peer, and verified and removed at the verification peer where packets with incorrect signatures are filtered. A unique state machine, which is used to generate signatures, is associated with each ordered pair of APPA peers. As the state machine automatically transits, the signature changes accordingly. KISS random number generator is used as the signature generating algorithm, which makes the state machine very small and fast and requires very low management costs. APPA has an intra-AS (autonomous system) level and an inter-AS level. In the intra-AS level, signatures are tagged into each departing packet at the host and verified at the gateway to achieve finer-grained anti-spoofing than ingress filtering. In the inter-AS level, signatures are tagged at the source AS border router and verified at the destination AS border router to achieve prefix-level anti-spoofing, and the automatic state machine enables the peers to change signatures without negotiation which makes APPA attack-resilient compared with the spoofing prevention method. The results show that the two levels are both incentive for deployment, and they make APPA an integrated anti-spoofing solution [6]. SPM and APPA have major advantage over RBF: SPM is an end-to-end protocol and requires lower deployment cost, while RBF can only work (efficiently) if all ASes implement RBF.Both SPM and APPA will work well if the edge router implements it. Spoofing detection will not work if either side of the source or the destination is not SPM or APPA router.

Route-Based Distributed Packet Filtering (DPF)

A novel approach to distributed DoS (DDoS) attack prevention is describe and evaluate as route-based distributed packet filtering (DPF) .DPF achieves proactiveness and scalability, and there is an intimate relationship between the electiveness of DPF at mitigating DDoS attack and power-law network topology. The salient features are two-fold. First, one is able to proactively filter out a significant fraction of spoofed packet flows and prevent attack packets from reaching their targets in the first place. The IP flows that cannot be proactively curtailed are extremely sparse so that their origin can be localized i.e., IP traceback to within a small, constant number of candidate sites. We show that the two proactive and reactive performance effects can be achieved by implementing route based filtering on less than 20% of Internet autonomous system (AS) sites. Second, we show that the two complementary performance measures are dependent on the properties of the underlying AS graph. In particular, we show that the power-law structure of Internet AS topology leads to connectivity properties which are crucial in facilitating the observed performance effects [7].

Inter-Domain Packet Filters (IDPF)

An inter-domain packet filters (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. A key feature of the scheme is that it does not require global routing information. In this paper we study the conditions under which the IDPF framework works correctly in that it does not discard packets with valid source addresses. Based on extensive simulation studies, we show that even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize the origin of an attack packet to a small number of candidate networks [8].

In the Internet there are a lot of distributed denials of service (DDoS) attacks. A lot of attacks aim to cause damage to network services applications. One of the efficient methods to protect regular traffic from the attacks called FSN method. FSN method is effective and practical and applicable to the real Internet environment. It uses topology information to detect the attacks and collects topology information using IGP routing protocol, so it is applicable to the environments including asymmetric paths and it doesn't require collected packets to construct neighbor information [9].Another detection method is proposed to detect the DDoS attack with the same concept using Open Shortest Path First (OSPF) [10].

Source Address Validation Enforcement (SAVE) protocol

SAVE is a new protocol proposed to provide information required to validate the source address of incoming packet. Each router that the packet traverse build correct incoming table with incoming interface. With this incoming table, each router can verify the packet and filter packets with mismatching source address. SAVE provides end-to-end anti spoofing mechanism. Each router sends updates to neighbor router from time to time to update each other's incoming table like BGP and Routing Information Protocol (RIP). SAVE update records the path the update had traversed and ensures that the update message traverses through the correct path [11].RBF limits the range of IP addresses for possible spoofing attacks but a spoofing attack is still possible. IDPF and SAVE further improve RBF by forwarding packets only if they came from the correct interface. Packet forwarding with source verification was proposed in [12] to address spoofing prevention via two approaches. In the first approach, definitive packet tagging, routers tag packet that originate from their domain. Along the path the packets traverse, the tag of packet will be verified. Once verified, the valid packet will be re-tagged with the tag of the forwarding router. This hop-wise tagging process will keep the number of tags each implementing router would has. Packet with insufficient tag or incorrectly tagged is dropped. The second approach, deductive packet tagging, routers can verify and tag packets from nearby domain.

BASE -BGP Anti-Spoofing Extension

BASE mechanism is an anti-spoofing protocol designed to fulfill the incremental deployment properties necessary for adoption in current internet environments [13]. BASE is similar to source verification method.

Packet Marking Approach

In the packet marking (Pi) approach a path fingerprint is embedded in each packet, enabling a victim to identify packets traversing the same paths through the Internet on a per packet basis, regardless of source IP address spoofing. Pi features many unique properties. It is a per-packet deterministic mechanism where each packet traveling along the same path carries the same identifier. This allows the victim to take a proactive role in defending against a DDoS attack by using the Pi mark to filter out packets matching the attacker’s identifiers on a per packet basis. The Pi scheme performs well under large-scale DDoS attacks consisting of thousands of attackers, and is effective even when only half the routers in the Internet participate in packet marking. Pi marking and filtering are both extremely light-weight and require negligible state [14].

Unicast Reverse Path forwarding (uRPF)

This approach requires that the traffic is forwarded only if the traffic carries at the same interface as the one that is used by the router to reach the source in the forwarding table. Although the mechanism is simple, the effectiveness of uRPF is limited. With current architecture of the Internet, many multihomed networks have different interfaces for incoming and outgoing traffics. Traffics might traverse different path and uRPF requires extra lookup at the router's forwarding table for each packet that arrive at the router. The efficiency of RPF depends on BGP routing information. RPF will drop valid packet if the router does not receive routing information BGP updates for the source prefix [15, 16].

Detection at Destination End

Hop Count Filter (HCF)

A novel filtering technique that is immediately deployable to weed out spoofed IP packets using hop count information. Since an attacker can forge any field in the IP header, he or she cannot falsify the number of hops an IP packet takes to reach its destination. This hop-count information can be inferred from the Time-to-Live (TTL) value in the IP header. Using a mapping between IP addresses and their hop-counts to an Internet server, the server can distinguish spoofed IP packets from legitimate ones [17]. The effectiveness of HCF lies on the hop-count values of the packet. HCF cannot detect spoofed and legitimate packets with same hop-count. Based on authors' work, they suggest that spoofed IP packets have mismatched IP address and hop-count (based on IP2HC). By performing a lookup in IP2HC map HCF is able to drop spoofed traffics. HCF is believed to work well as an attacker is not able to falsify the value of TTL, but intermediate attackers will be able to try to launch an attack from location with matching hop-count values. HCF causes delays to transmission. To overcome this problem, HCF operates under alert mode to detect spoofed traffic and action mode to drop packets when spoofed traffic is detected. Action mode will perform per-packet hop-count computation and compare with values in IP2HC. HCF is deployed at end host, hence easier to deploy compared to RBF.

A general purpose traceback mechanism based on probabilistic packet marking in the network is proposed [18].This approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). It is a technique for tracing anonymous packet flooding attacks in the Internet back towards their source.

Probabilistic Packet Marking (PPM)

PPM is a technique to mark packet with partial path information at routers. Each router marks their IP address onto the packet with the probability of P along the way the packet traversed. When DDOS attack is detected, the victim can reconstruct the whole path after collecting certain amount of packet by using the information of the mark, despite the source address in the IP header. PPM has very low overhead as it only mark by the probability of P, but it has a high computation overhead and this method is not effective. In [19] PPM was modified and reduces the computation overhead to an acceptable level. In [20] authors combine PPM and the concept of winding number. Their work shows that they are able to correctly trace the attacker's router IP address using integral equation.

IP Traceback with Deterministic Packet Marking (DPM)

DPM is a new approach for IP traceback which is scalable and simple to implement, and introduces no bandwidth and practically no processing overhead. It is backward compatible with equipment which does not implement it. The approach is capable of tracing back attacks, which are composed of just a few packets. In addition, a service provider can implement this scheme without revealing its internal network topology [21].

On Deterministic Packet Marking

It is an approach to IP Traceback based on marking all packets at ingress interfaces. DPM is scalable, simple to implement, and introduces no bandwidth and practically no processing overhead on the network equipment. It is capable of tracing thousands of simultaneous attackers during a DDoS attack. Given sufficient deployment on the Internet, DPM is capable of tracing back to the slaves responsible for DDoS attacks that involve reflectors. In DPM, most of the processing required for traceback is done at the victim. The traceback process can be performed post-mortem allowing for tracing the attacks that may not have been noticed initially, or the attacks which would deny service to the victim so that traceback is impossible in real time. The involvement of the Internet Service Providers (ISPs) is very limited, and changes to the infrastructure and operation required to deploy DPM are minimal. DPM is capable of performing the traceback without revealing topology of the providers' network, which is a desirable quality of a traceback method [22].

Flexible Deterministic Packet Marking (FDPM)

FDPM provides a defense system with the ability to find out the real sources of attacking packets that traverse through the network. FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate according to the load of the participating router by a flexible flow-based marking scheme [23].

StackPi- New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense

Earlier discussed path identification (Pi) DDoS defense scheme is a deterministic packet marking scheme that allows a DDoS victim to filter out attack packets on a per packet basis with high accuracy after only a few attack packets are receive. Enhancement of the idea called the StackPi marking, a new packet marking scheme based on Pi, and new filtering mechanisms. The StackPi marking scheme consists of two new marking methods that substantially improve Pi's incremental deployment performance: Stack-based marking and write-ahead marking. This scheme almost completely eliminates the effect of a few legacy routers on a path, and performs 2-4 times better than the original Pi scheme in a sparse deployment of Pi-enabled routers [24].

A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks

It is an attack mitigation scheme that adopts a divide-and-conquer strategy. Attack diagnosis (AD) combines the concepts of pushback and packet marking, and its architecture is in line with the ideal DDoS attack countermeasure paradigm - attack detection is performed near the victim host and packet filtering is executed close to the attack sources. AD is a reactive defense mechanism that is activated by a victim host after an attack is detected. By instructing its upstream routers to mark packets deterministically, the victim can trace back one attack source and command an AD-enabled router close to the source to filter the attack packets. This process isolates one attacker and throttles it, which is repeated until the attack is mitigated [25].

Traceback techniques

An ant-based traceback approach is proposed to identify the DoS attack origin. Instead of creating a new type or function or processing a high volume of fine-grained data used by previous research, the proposed traceback approach uses flow level information to identify the origin of a DoS attack [26].Another traceback method for detection of DDoS attacks is based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques [27].

Application of neural networks in DDoS detection

Artificial Neural Networks (ANNs) are famous learning models for their ability to cope with demands of a changing environment [28]. They are self-learning and self-organizing models which make them a suitable choice for processes which seek advantages like robustness, fault tolerance and parallelism. Moreover, due to self-learning characteristic, they are good enough to identify and resist unknown disturbances in a system. This property of neural networks has been utilized in DDoS attack detections in some research attempts, as they are capable of identifying unknown attack patterns that may exist in DDoS attacks. In [29], authors use Linear Vector Quantization (LVQ) model of ANN. In this model, input layers accept input vectors called neurons with specified weights which are adjustable according to ANN’s self-learning mechanism. The middle layers process the information and pass it on to output layers. In fact, input and middle layers exhibit same kind of functionality in all ANN models. However, the transfer function used for information processing at middle layers is unique for each kind of neural network and the appropriate result is consequently forwarded to output layers. In the case of LVQ model, the information in middle layers is processed in such a way that the winner neuron takes the entire output share and accordingly passes it on to output layers. It is similar to self-organizing maps and applied in techniques of pattern recognition, multi-layer classification and data compression. Under supervised learning, it knows the target output against different forms of various input patterns [30.]. After testing the system with LVQ model, authors use the same dataset with Backpropagation (BP) model of ANN (to be discussed ahead) for comparative study. On the basis of comparison results, they claim that LVQ is more accurate in determining DDoS attacks than BP. They show that LVQ is 99.723% accurate on average against tested dataset whereas the average accuracy of BP is 89.9259% for the same dataset. Accuracies are computed on the basis of percentages of obtained false positives and false negatives against each sample of testing data. There are 10 samples used to test the systems for each of the LVQ and BP models. In other research attempts found in [31] and [32], authors use BP model of neural networks to estimate the strength of DDoS attack in real time and predict the number of zombies respectively. Backpropagation neural network is a multilayer feed forward network with backpropagation (feedback) of an error function [33]. A simple feed forward neural network has only three layers i.e., input, output and middle layers. Input layer passes on certain weights to middle layer which processes them and sends calculated weights to the output. Each weight is revised according to gradient descent of the error through output layer, back propagated to hidden layer and then to the input layer. Again the information is fed forward and error is fed backward. In this way, weights are adjusted to reduce error and execute learning and training of the neural network. This process is continued until network's output error is brought down to an acceptable level or the preset time of learning is achieved [34]. In [31], authors train the BP neural network with a dataset of variations in traffic entropy as inputs and the corresponding actual DDoS strengths as outputs. 20 different samples in the dataset are used for training with 10 Mbps attack strength as the lowest and 100 Mbps being the highest in the dataset. The entropy variations are calculated as discussed before. Therefore, the scheme is based on an assumption that the attack traffic is seen different in the network from normal traffic. The model is tested with four random inputs of entropy variations for which calculated attack strengths are 20, 50, 70 and 95 Mbps. The BP neural network's output is seen promising with little errors. False positives and false negatives are also very less. Moreover, authors also test the system with variations in network size i.e., number of neurons in processing layer. They use two layer feed forward network with BP algorithm and find that with the increase in network size, errors are further reduced and more accuracy is achieved. However, in real cases, increasing the network size also increases both training time and implementation cost. In [32], authors train the BP neural network to predict number of zombies behind a DDoS attack. They train the system with a dataset of variations in traffic entropy as inputs and the corresponding actual number of zombies behind DDoS attack as outputs. The dataset is used for training from 10 to 100 zombies with an increment of 5. The attack strength is a constant rate of 25 Mbps. It effectively changes the attack rate per zombie in each data sample ranging from 0.25 to 2.5 Mbps. The model is tested with different random inputs of entropy variations and the BP neural network's output was seen promising with little errors. Moreover, they also test the system with variations in network size and find that with the increase in network size, errors are further reduced and more accuracy is achieved. In [35], authors test Time Delay Neural Network (TDNN) to produce early warning system against DDoS attacks. TDNN is a type of neural networks in which time delay factor is incorporated or hidden inside the representative signal. In their work, a Demilitarized Zone (DMZ) is created and TDNN is implemented in two-layer pattern. The node activity is monitored by neighboring nodes and attack information is passed on to the expert module for integrated analysis. The layered structure enables the system to take some appropriate actions as a proactive strategy against DDoS attacks such as initiating the deployed Intrusion Prevention System (IPS). Their detection results on deployed architecture show that proposed scheme is able to give 82.7% correct detection rate as compared to 46.3% with general Intrusion Detection System (IDS).Current evolutionary techniques to counter DDoS attacks indicates that application layer attacks are now getting more popular in attackers due to their unique properties of legitimate-like behavior. It is a fact that network layer attacks which contain packet manipulations are now relatively easier to detect with modern detection and mitigation tools.

CONCLUSION

This article reviewed a comprehensive survey of different types of IP spoofing techniques, DOS/DDOS attack detection and defense mechanisms that have been proposed by various researchers. From this study it is conclude that most of the researchers try to deploy defense mechanism during the packet transmission than at the destination. It is mandatory to fight these types of networks attacks is to increase the reliability of global network infrastructure. At the same time more reliable mechanisms are still needed to authenticate the source of Internet traffic. However, application layer DDoS defense needs more research for development of highly effective defense tools.

REFERENCES

[1] P.Ferguson, et al, "Network Ingress Filtering", RFC 2827, May 2000.

[2] F.Baker, et al, “Ingress Filtering for Multihomed Networks”, RFC 3704, March 2004.

[3] Jelena Mirkovic, et al, “A Practical IP Spoofing Defense Through Route-Based Filtering”, 2006.

[4] A. Bremler-Barr, et al, “Spoofing prevention method”, INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 536 - 547 vol. 1, 13-17 March 2005.

[5] Y.Shen, J. Bi, J. Wu, and Q. Liu, "A two-level source address spoofing prevention based on automatic signature and verification mechanism," in Proceedings - IEEE Symposium on Computers and Communications, Marrakech, 2008, pp. 392-397.

[6] J.Bi, B. Liu, J. Wu, and Y. Shen, "Preventing IP Source Address Spoofing: A Two-Level, State Machine-Based Method,” Tsinghua Science and Technology, vol. 14, pp. 413-422, 2009.

[7] Kihong Park,et al,“ On the Effectiveness of Route Based Packet Filtering for Distributed DoS Attack Prevention in Power Law Internets”, Network Systems Lab, Department of Computer Sciences, Purdue University, SIGCOMM’01, August 2731,2001, San Diego, California, USA.

[8] Z. Duan, X. Yuan, and J. Chandrasekhar, "Controlling IP spoofing through interdomain packet filters," IEEE Transactions on Dependable and Secure Computing, vol. 5, pp. 22-36, 2008.

[9] T. Ohtsuka, F. Nakamura, Y. Sekiya, and Y. Wakahara,"Proposal and efficient implementation of detecting and filtering method for IP spoofed packets," in ICICT 2007: Proceedings of International Conference on Information and Communication Technology, Dhaka, 2007, pp. 327-330.

[10] T. Otsuka, F. Nakamura, Y. Sekiya, and Y. Wakahara, "Realization of FSN method for detecting IP spoofed packets by making use of OSPF," IEICE technical report, 2007.

[11] J. Li, J. Mirkovic, T. Ehrenkranz, M. Wang, P. Reiher, and L. Zhang, "Learning the valid incoming direction of IP packets, “Computer Networks, vol. 52, pp. 399-417, 2008.

[12] C. A. Shue, M. Gupta, and M. P. Davy, "Packet forwarding with source verification," Computer Networks, vol. 52, pp.1567-1582, 2008.

[13] H. Lee, M. Kwon, G. Hasker, and A. Perrig, "BASE: An incrementally deployable mechanism for viable IP spoofing prevention," in Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ASIACCS '07, Singapore, 2007, pp. 20-31.

[14] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, 2003, pp. 93-107.

[15] “Unicast Reverse Path Forwarding Enhancements for the Internet Service Provider”, Cisco systems http://www.cisco.com/warp/public/732/Tech/security/docs/ur pf.pdf, 2005.

[16] “Unicast Reverse Path Forwarding”, Cisco Systems, http://www.cisco.com/en/US/docs/ios/11_1/feature/guide/uni_rpf.pdf, 2007.

[17] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," IEEE/ACM Transactions on Networking, vol. 15, pp. 40-53, 2007.

[18] Stefan Savage et al, “Practical Network Support for IP Traceback ,” Department of Computer Science and Engineering University of Washington,Seattle, WA, USA, SIGCOMM'00, Stockholm, Sweden.

[19] D. Q. Li, P. R. Su, and D. G. Feng, "Notes on packet marking for IP traceback," Ruan Jian Xue Bao/Journal of Software,vol. 15, pp. 250-258, 2004.

[20] M. M. Viana, R. Rios, R. M. De Castro Andrade, and J. N. De Souza, "An innovative approach to identify the IP address in denial-of-service (DoS) attacks based on Cauchy's integral theorem," International Journal of Network Management, vol. 19, pp. 339-354, 2009.

[21] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Communications Letters, vol. 7, pp. 162-164, 2003.

[22] Andrey Belenky, Nirwan Ansari, “On deterministic packet marking,” Elsevier, 2006.

[23] Y. Xiang, W. Zhou, and 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, pp. 567-580, May 2009.

[24] A. Yaar, A. Perrig, and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," IEEE Journal on Selected Areas in Communications, vol. 24, pp. 1853-1863, 2006.

[25] R. Chen, J. M. Park, and R. Marchany, "A divide-and-conquer strategy for thwarting distributed denial-of- service attacks," IEEE Transactions on Parallel and Distributed Systems, vol.18, pp. 577-588, May 2007.

[26] Gu Hsin Lai *, Chia-Mei Chen, Bing-Chiang Jeng, Willams Chao,“ Ant-based IP traceback,” Expert Systems with Applications , Elsevier 2008.

[27] Shui Yu, Member, IEEE,et al,“ Traceback of DDoS Attacks Using Entropy Variations,” IEEE Transactions on Parallel and Distributed Systems, VOL. 22, NO. 3, MARCH 2011.

[28] Liu, Y., Cukic, B., and Gururajan, S., ‘‘Validating neural network-based online adaptive systems: A case study,’’ Software Qual. J., 15: 309–326, 2007.

[29] Li, J., Liu, Y., and Gu, L., DDoS Attack Detection Based on Neural Network, Proceedings of IEEE 2nd International Symposium on Aware Computing (ISAC), 196–199 (2010).

[30] Biehl, M., Ghosh, A., and Hammer, B., ‘‘Dynamics and generalization ability of LVQ algorithms,’’ J. Mach. Learn Res., 8: 323–360,2007.

[31] Agarwal, P. K., Gupta, B. B., Jain, S., and Pattanshetti, M. K., Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme, Communications in Computer and Information Science (Springer), 157: 301–310,2011.

[32] Gupta, B. B., Joshi, R. C., Misra, M., Jain, A., Juyal, S., Prabhakar, R., and Singh, A. K., Predicting Number of Zombies in a DDoS Attack Using ANN Based Scheme, Communications in Computer and Information Science (Springer), 147: 117–122 2011.

[33] Xu, Z. H., Chen, W. B., Yang, W. F., and Liu, F., Fast Algorithm of Evolutional Learning Neural Network, Proceedings of IEEE International Conference on Intelligent Systems Design and Engineering Application (ISDEA), 262–265,2012.

[34] Zhao, Z., Xin, H., Ren, Y., and Guo, X., Application and Comparison of BP Neural Network Algorithm in MATLAB, DDoS Attack and Defense Strategies 197 Proceedings of IEEE International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 590– 593,2010.

[35] Chang-Lung, T., Chang, A. Y., and Ming-Szu, H., Early Warning System for DDoS Attacking Based on Multilayer Deployment of Time Delay Neural Network, Proceedings of IEEE 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 704–707 ,2010.