I. J. Computer Network and Information Security, 2013, 5, 47-54
Published Online April 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.05.06

Defending of IP Spoofing by Ingress Filter in Extended-Inter Domain Packet Key Marking System

G.Velmayil, Dr. S.Pannirselvam,
Dept. of Computer Science, Department of Computer Science
Quaid-E-Milleth Govt. college for Women (A), Erode Arts & Science College (A) Tamilnadu, India.
velmayil@yahoo.com, pannirselvam08@gmail.com

Abstract — The significance of the DDoS problem and the increased occurrence and strength of attacks has led to the dawn of numerous prevention mechanisms. IP spoofing is most frequently used in denial-of-service attacks. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. IP spoofing is one of the basic weaknesses in the Internet Protocol to launch the DDOS attack. Each prevention mechanism has some unique advantages and disadvantages over the others. The existing methods become ineffective due to a large number of filters required and they lack in information about where to place the filter. We propose Ingress filter in Extended Inter Domain Packet Key marking system .This paper comprises of two functional blocks namely, Key marking system and filtering blocks. In the marking block, each source is labeled with a key. The key is changed continuously for a certain period of time to provide secured system and is validated at border routers. In the filtering block, spoofed packets are filtered at the border router using Ingress filter to filter beyond periphery routers. The filter placement algorithm clearly put forwards the conditions under which the filter can operate accurately. The accuracy of the proposed systems is validated using Network Simulator (NS-2).

Index Terms— DDOS, IP spoofing, BGP, Ingress Filtering

I. INTRODUCTION

Distributed Denial of Service attacks have become a weapon of ideological attacks, causing damages in the millions of dollars to commercial, government and personal sites. A human attacker typically stages a DDoS attack using several compromised machines called zombies. The actual number of zombies on the Internet at any given time is not known, but it is estimated to be in the thousands [1]. To keep management simple, groups of zombies are typically organized in attack troops that the attacker can then repeatedly use to flood a target. In DDoS attack, goal of the attacker is to tie up chosen key resources at the victim, usually by sending a high volume of seemingly legitimate traffic requesting some services from the victim. It reveals big loopholes not only in specific applications, but also in the entire TCP/IP protocol suite. DoS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. The TCP/IP protocol suit is widely used in the Internet, vulnerable to a variety of attacks including IP spoofing [2]. IP spoofing is an emerging threat to the Internet systems. IP packets are sent through forged source address and the attackers make use of this for a number of purposes [3]. An attacker uses a large number of zombies to increase the power of the attack and to make difficult of defending mechanism. The master attacker sends commands to the previously compromised zombies, ordering them to attack the victims. The master attacker uses the reflectors to attack the victim [4]. This research work investigates the defense mechanisms against IP Spoofing. To filter out the spoofed packets, we propose the Ingress filter in Extended Inter Domain Packet Key marking system with two blocks. This system allows the border router to validate the correctness of the source IP address. The major advantage of this approach is the Internet systems are compatible with the marking system and even in the partial deployment, it offers much gain to its users.

Problem definition

DDoS attack is the most dangerous threat to the Internet and it uses IP spoofing as its attacking tool. An attacker imposes a large volume of network traffic towards the Internet server to degrade its performance. The source broadcast the IP packet to the target using source and target IP address and there is no assurance for the correctness of these IP addresses. There are several filter based designs that eliminate DDoS attacks but they use a large number of filters and fail to block the spoofed packets perfectly. In this paper, we provide better solution to detect and remove the IP spoofed packets. This paper is proposed with two functional blocks to detect and filter the IP spoofed packet. The key marking system identifies the spoofed packets efficiently. The filter deployment scheme proposed here is ingress filtering Park and Lee show [5] that filtering

based on routing information available to routers by ingress filtering can be very effective against spoofed traffic in Internet-like topologies if deployed by as few as 20% of ISPs that resolves the filter placement issues. While the filtering method with this key marking system discussed is effective by 80% and this does absolutely nothing to protect against flooding attacks but overcomes to filter beyond periphery routers.

Paper organization

This paper is structured as follows: Section II deals with the previous work and section III discusses a brief overview of the proposed solution. Section IV provides detailed description of proposed filter placement algorithm. Finally, section V concludes the paper.

II. PREVIOUS WORK

DDoS shield protects the attack on the application layer resource ,unremitting values provided to all clients while the DDoS resilient scheduler exploit these values to decide when a user send request for scheduling [6]. Distributed change point Detection (DCD) is a new method to detect DDoS attacks at the traffic flow level using Change Aggregation Trees (CAT) [7]. TCP SYN packets from a random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services such as e-mail, file transfer, or WWW to legitimate users. There is no easy way to trace the originator of the attack because the IP address of the source is forged [8]. Ingress Filtering is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge. Route based filtering, proposed by Park and Lee [9], extends ingress filtering and uses the route information to filter out spoofed IP packets. It is based on the principle that for each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated. The basic idea behind DCD is to detect sudden traffic oscillations before they occur across inter domain network. The ISP domain server collects the traffic information from the routers and uses this information to construct the CAT. The route based filter (RBF) identifies and removes the IP spoofed packets using the previous hop between source and destination [10]. IDPF is similar to RBF but IDPF uses a group of feasible previous hops instead of using a single previous hop [11].

Statistical monitoring examines the data packet to identify the normal and abnormal activities using optimal routing policies. This kind of statistical based filtering discard the packets with abnormal activities and forward the packet with normal activities [12]. Hop Count Filtering (HCF) is associated with hop count information between the source and the destination. HCF constructs a perfect IP-to-hop-count (IP2HC) mapping table and initialization and insertion of IP address into this mapping table requires equivalent pollution-proof method. Hop count value is not directly specified in the mapping table but the inspection algorithm and validation algorithm is associated with this mapping table [13]. ANTID filters the attack packets when the DDOS attack take place. In this scheme, a unique path fingerprint describing the route it has crossed [14]. Another mechanism that provides protection against large bandwidth consumption is revealed in [15]. This method involves both local and global mechanism for controlling such DDoS attacks.

MOVE detects DDoS attacks, but it does not depend on infrastructure support [16] and filtering schemes. MOVE allots a new region to valid users in the overlay networks. Path identifier [17] marks each packet with a path fingerprint and thus allows the victim to have knowledge of packet's path over the internet on per packet fashion without considering the source IP address. Packet can also be marked on the TTL basis called TPM [18] in which all packets are marked with probability i.e. inversely proportional to the distance covered. D-WARD [19] is the source to the end solution for the DDoS attack. This solution provides better spoofing detection with the traffic profiling mechanism. Spoof Prevention Method (SPM) depends on packet marking to check the validity of the packet close to the destination [20].

III. PROPOSED SYSTEM

3.1 Overview of the Ex-IDPF

This paper proposes an Ingress Filter in Extended-Inter Domain Packet Key Marking System. This work is the extension of IDPF [12] [21]. There are two main functional blocks namely, marking block and filtering block. In the Key marking system, the security keys are placed at the border routers at the source AS and then it is verified at each border routers before entering into the network. This method is much secured as the security key is changed continuously for every 2-3 hours [21]. BGP exchanges the routing information between the ASes. The filtering block works correctly only when it does not discard any packets with valid source address prohibits an attacker from using "invalid" source addresses which reside outside of this prefix range.

3.2 Key marking system

It is necessary to detect the spoofed packet prior to filtering it. Spoofed Packets [22] are detected using the key marking system. The security key is placed in the identification field of IP header as shown in the figure 1. The security key corresponds to a pair of source AS and target AS. The border routers verify the security key on the source packet that matches with the security key of the target packet to detect the spoofed packet. Each outgoing packet from the source network AS is labeled with the security key Ks(S, T) of 16 bits related to the source and the target AS. The security keys are placed at

the border routers at the source AS and then it is verified at each border routers before entering into the network. This method is much secured as the security key is changed continuously for every 2-3 hours. The verification is done only at the border router.

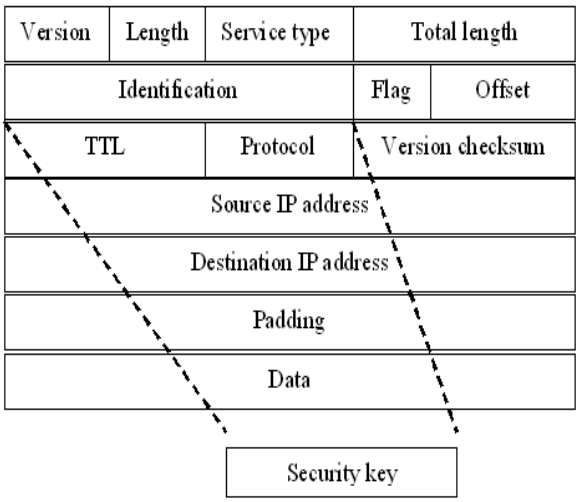


Figure 1: IP header with a security key

3.3 Table Construction

Before executing, it is necessary to initialize or fill the path history table and to keep on revising the data in the table.

3.3.1 Populating PH Table

The initial step to populate the PH table is that the Internet Service Provider (ISP) should have knowledge of the path of its customers to attain IP address and a feasible route. At the beginning stage, the knowledge gaining period must be longer to assure better filtering precision and this period is based on the level of server's day to day traffic. It keeps on adding the upcoming latest entries to the PH table on the basis of unnoticed genuine IP address request.

3.3.2 Updating Feasible Path

The path history record must be updated as every packet keeps on changing its path. There may be some temporary shortcomings in computing the accurate feasible path due to insecure routing, repositioning of networks and network connectivity failures. The table update function mainly engages in two steps: the first step is to create a content page with the available source IP address and then, it has to keep on changing the content page for every new feasible path.

3.4 Labeling Packets with Security Key

The intermediate routers that perform the labeling process retain a key validation table. The router labels the security key and each server in an AS system passes the key details to other routers which is updated in BGP. The main functions of AS server are as follows: (a) select the security key for marking; (b) distribute these keys to routers in AS; (c) declare the keys to other AS that participate in labeling process; (d) update the entries in the BGP routers. The border routers have the mapping information very prepared as they exploit it for a given network information that maintains the net traffic across various ASes.

The border routers validate the security key. Each router adds the security key in the IP header and passes through various routers to reach the target. These keys are selected at a random manner and then distributed to every other AS servers. It is important to note that, at the instant of security key substitution, every router holds two security keys: old/previous and new. As a result, each router contains the key validation table with two keys corresponding to the source address.

3. 5 Filtering section

The ingress filtering is constructed using only the updated information in the BGP routers [11]. Let P(s, t) represent the packet with source address "s" and with the target address "t". Consider the source node "A" that transmits packet P(s, t) to the target node "B" only when N (A, B) belongs to the feasible route R_f(s, t). If this condition is not satisfied, the node "B" is supposed to drop the packet. The packet P(s, t) is transmitted successfully when the node N (A, B) belongs to the short and best route R (s, t). Otherwise, the target node drops all other packets that do not satisfy the above criteria. The filtering block filters the spoofed packet using the path history and feasible route tables. The PH table contains the updated information about the path that each node follows to reach the target. The FR table contains the entire possible route. An input traffic filter on the ingress (input) which provides connectivity to the attacker's network, restricts traffic to allow only traffic originating from source addresses within the prefix, and prohibits an attacker from using "invalid" source addresses which reside outside of this prefix range. And finally, it uses this information to choose the shortest and best route.

3.5.1 Ingress filtering

The Ingress filtering method discussed in this document does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules. An additional benefit of implementing this type of filtering is that it enables the originator to be easily traced to its true source, since the attacker would have to use a valid, and legitimately reachable, source address. Is a welcome and necessary part of the solution to the problem? Ingress filtering will take time to be implemented pervasively and be fully effective, but the extensions to the operating systems can be implemented quickly. This combination should prove effective against source address spoofing [22].

3.5.2 Working of Ingress filtering

The ingress filter would check:

IF packet's source address from within the prefix range THEN
Forward as appropriate
Else IF packet's source address is outside the prefix range THEN
Deny packet
End if.

3.5.3 Identifying spoofed packets

The spoofed packets are identified at the border routers through a key validation table. The key is a random number selection of 16 bits that label all the traffic among source and target AS. There are eight possible combinations to decide whether a packet is spoofed or not which is given in the following table. These combinations clearly put forward the condition under which a packet must be marked as a spoofed and Ingress filter filters those spoofed packets out.

It is much difficult to filter the packet when it has a valid key and reaches the filtering section; the ingress filter verifies whether it is originating from the source address within the prefix through non feasible route. If the packet has come from source addresses outside the prefix, then the packet is spoofed packet. Therefore, discards such packets. When the packet reaches the filtering section with an invalid key and valid FR, discards the packet. During the key replacement, each packet contains two keys such as an old key and a new key. At the filtering section, the packet must have the key that matches with either of these keys. If not so then even if the packet has arrived from source address within the prefix range, discards the packets.

If both the key and the FR are invalid, the filtering section can discard the packet. At the filtering section, even if the packet has arrived from source address within the prefix range, discards the packets. When the key does not obey the marking scheme and reaches the destination in not feasible route, it is marked as the spoofed packet and filtered out.

If the packet reaches the filtering section with a valid key and valid FR, it is considered as the genuine packet. At the filtering section, it is verified that the packet has arrived from source address within the prefix range, the packet is not discarded and the packet with a valid FR and key and is forwarded to the destination. Same way If the packet reaches the filtering section with a valid key and invalid FR the packet has arrived from source address within the prefix range , then also it is considered as the genuine packet since the origin and key is valid and path has a deviation in the traffic.

Table 1: Truth table to represent the condition under which the packet is allowed

Key Validity	Feasible Path	Source address within prefix range	State in which packet is allowed
F	F	F	
F	F	T	
F	T	F	
F	T	T	
T	F	F	
T	F	T	Allow packet
T	T	F	
T	T	T	Allow packet

Algorithm for the working principle of the proposed system

Step 1: Source node generates packet, P.
Step 2: The source node labels P with a security key of 16 bit address in the identification field of IP header. The 16 bit address represents the source and destination AS.
Step 3: P reaches BGP of another AS.
Step 4: Current BGP exchanges its routing details with previous BGP from which it received P.
Step 5: Different packets from different ASes entering BGP are made stored in a queue and the border router processor process these packets.
Step6: A border router processor maintains its own routing table and a collection of routing tables from neighboring ASes.
Step7: In addition, it maintain PH and FR table. The path history (PH) table contains the updated information about the path of each node taken to reach the target. The feasible route (FR) table contains the entire possible route.
Step 8: Ex-IDPF is deployed at BGP and it is designed with marking and filtering block.
Step 9: In the marking block, the key is validated using key validation table.
Step 10: The key is changes for every 2-3 hours.
Step 11: At the time of key substitution period, each router holds two security keys, old and new keys.
Step12: For any incoming packets, the marking block verifies whether the labeled key is equivalent to either old or new key using key validation table.
Step13: If it is equivalent to old or new key, the marking block marks the packet as "genuine" or "spoofed" otherwise.
Step14: Ingress filter implemented here verifies the presence source addresses which reside inside of the prefix range or not.
Step15: The filtering block checks the validity of the packet under which it falls.
Step 16: Filtering block refers to the PH and FR table and the result of marking block.
Step 17: Filtering block first verifies the packets if the key is either new or old and the feasible path of the packet is valid and source address within the prefix range.
Step 18: Filtering block then verifies the feasible path of the packets validity.
Step 19: The genuine packets are then queued out to the corresponding destination.
Step20: It drops the packets in all the other combination of values.

3.5.4 Filter Placement Algorithm- Effectiveness measurement

The filter placement algorithm overcomes the drawbacks using the information implied in BGP updates to construct the filters. The FR table describes the shortest and best route to reach a particular destination. This algorithm is mainly used to place the filter in (or among) AS using the information in FR table as well as restricts traffic to allow only traffic originating from source addresses within the prefix by verifying through ingress filters. Filters should discard the packets with an invalid source IP address and it should permit packets with valid source IP address and address from valid origin to the destination point. For a given set of K deployment points, there exist several (s, t, AS_{num}) combinations. Let's' and 't' corresponds to the source and target IP address while AS_{num} corresponds to the AS number. Let us consider an empty set of optimal deployment points, U and also an empty set of already filtered (s, t, AS_{num}) group V. If spoofed packet is detected, AS filtering groups that is not present in the set V is added to U and subsequently, corresponding routers updates the set V. In the proposed system, filter placement scheme chooses a set of n parts (samples) along with the (s, t, AS_{num}) group. In the chosen group ingress filters verifies the origin prefixes so that the ingress filters overcomes the drawback restricted to the origin to chosen group. The proposed algorithms estimate the K number of appropriate filter placement points that includes the group of (s, t, AS_{num}).

IV. IMPLEMENTATION

4.1 Experimental setup

We executed the proposed solution in NS-2 simulator to observe the validation of the spoof defense mechanism. Let us implement the performance of the proposed system among 6000 ASes The path history table is maintained and updated in border routers. The key is also validated in border routers and they need to carry out at least one lookup operation. During the lookup operation, each packet is validated using the key validation table. The security key is a 16 bit random number and it includes the source and target AS. The filters are deployed according to the deployment scheme. During the security key replacement, each packet header holds both old and new keys. The time estimated for detection of one spoofed packet is less than 6 ns. The estimated time taken to verify the packet within the range is 1ns. The estimated time per packet is 7ns. Ingress filters with the Key Marking System overcomes the restriction to the size of the networks.

Table 2 presents the simulation parameter of the proposed system.

Table 2: Simulation Parameter

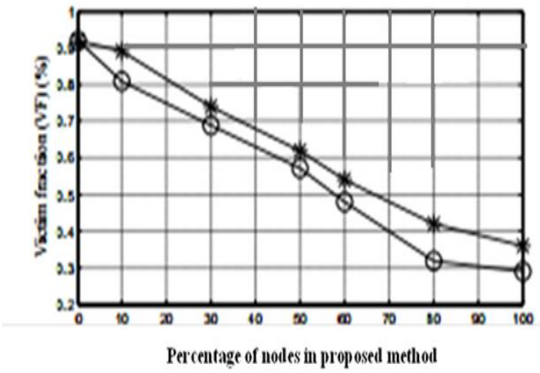
Parameter	Values
Number of ASes	6000
Number of users per AS	200
Per packet estimation time	7ns
Number of feasible routers	30-40
Number of feasible path	400
Key replacement	For every 2-3 hours
Size of security key	16 bit
Simulation run time	1000sec

4.2 Performance evaluation

The performance level of Ex-IDPF is measured using three performance metrics: Victim Fraction (VF), Attack Fraction (AF), and Victim Trace Fraction (VTF).

Victim Fraction:

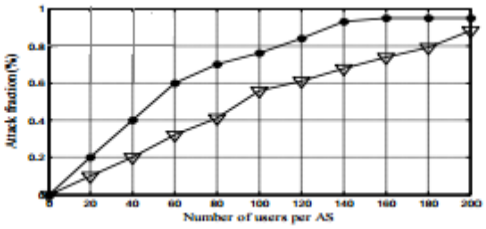
Victim fraction is the number of nodes that an attacker could attack and spoofs the IP address of almost n nodes. Graph 1 represents the victim fraction of nodes that participates in the proposed system with non participants.



Graph 1: Victim fraction

Attack Fraction:

Attack fraction is the percentage of nodes among which the zombies cannot attempt any IP spoofing attacks over other nodes.

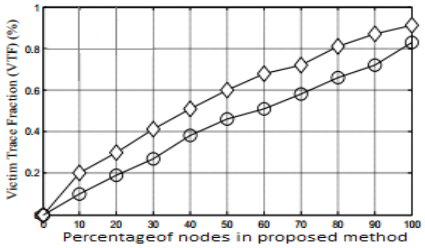


Graph 2: Attack fraction

The relationship between the number of users per AS and attack fraction is presented in graph 2. From the above graph, it is clear that the efficacy of the proposed is up to 93.3%.

Victim Trace Fraction:

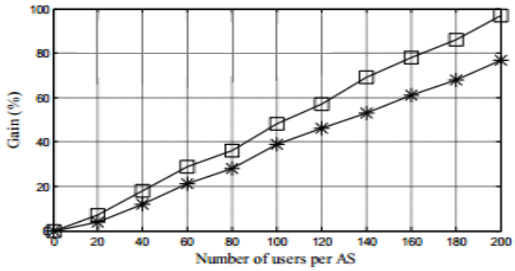
The victim trace fraction represents the percentage of nodes that are capable to identify the spoofed packets and locate the origin of the spoofing process. Graph 4 indicates the victim trace fraction of the proposed system and existing system.



Graph 3: Victim trace fraction

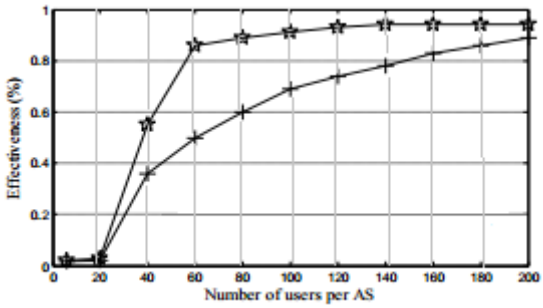
Gain:

This parameter deals with the gain that detection method (marking) offer to its users. The users with marking scheme achieve more gain than the others. A sample of 200 users per AS is considered. The user with the security key achieves almost 97.01% of gain and hence this method is considered as a beneficial method. The gain of users per AS with a security key and without a marking block is shown in the graph 5.



Graph 4: Gain of marking block

Effectiveness of Ingress Filter with and without a key marking system:



Graph 4: Effectiveness of Ingress Filter with and without marking block

4.3 Comparison of success of the proposed method with existing systems

Table 2 represents the comparison of the proposed and existing scheme [21]. Three best existing defense schemes such as RBF, IDPF and HCF are compared to the proposed system. The percentage of packet estimation of proposed method is much less than the IDPF and comparatively less than RBF and HCF. The existing IDPF does not use any marking scheme so it has low storage value. The victim fraction is much less for the proposed system and it is high for RBF. The proposed system protects about 93.3% of the target from the attacker. The proposed system can trace the location of the true origin of attack about 94.33%.

Table 3: Parameter metrics comparison with existing schemes

Factor	RBF	IDPF	HCF	Proposed Filtering Method
Per packet estimation time	8 ns	22 μs	8 ns	7ns
Gain (%)	63	57	96.2	96.50
Victim Fraction (%)	92.8	80.03	74.1	65
Attack Fraction (%)	81.21	86.32	90	93.3
Victim Trace Fraction (%)	80.05	83.6	90.4	94.33

V. CONCLUSION

In this paper, Detection and Removal of IP Spoofing by Ingress Filter in Extended-Inter Domain Packet Key Marking System proposed actively controls the IP spoofing based DDOS attacks in an effective manner. The construction depends on BGP updates and this filter framework perfectly works without discarding any packets with valid source IP address. This paper presents filter placement algorithm that explains the AS relationship from BGP updation. BGP provides a guarantee for correctness of source AS using functional blocks. It is easy to deploy an input traffic filter on the ingress (input) to the attacker's network, restricts traffic to allow only traffic originating from source addresses within the prefix, and prohibits an attacker from using "invalid" source addresses which reside outside of this prefix range. Filters are based on the filter deployment scheme over the AS based Internet Architecture. It facilitates to localize the origin/source of the attack regardless of the size of networks. Ingress filters without the Key Marking System is restricted to the size of the networks.

Our simulation result proves that 40 optimal filter deployment points on various ASes provide better and effective solution against DDoS attacks. The performance remains better with even if more than 40 filters are deployed. The Proposed system is 90% efficient in detecting and Removing Spoofed packets.

REFERENCES

[1] David Moore, Geoffrey Voelker, and Stefan Savage "Inferring Internet denial of service activity" in Proceedings of the USENIX Security Symposium, Washington, DC, USA, USENIX August 2001

[2] S.M. Bellovin. “Security Problems in the TCP/IP Protocol Suite” Computer Communication Review, Volume 19, Issue- 2, pp. 32-48, 1989.
[3] L. Todd Heberlein, Matt Bishop. "Attack Class: Address Spoofing", Proceedings of the 19th National Information Systems Security Conference, pp: 371-377, 1996.
[4] V. Paxson.,“ An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, ACM SIGCOMM Computer Communications Review, Volume 31, Isssue 3, pp 38-47, 2001.
[5] Kihong Park and Heejo Lee. “On the effectiveness of Route based packet filtering for distributed DoS attack prevention in power-law internets”. In Proceedings of the ACM , SIGCOMM, August 2001.
[6] Supranamaya Ranjan, Ram Swaminathan , Mustafa Uysal,Antonio Nucci, and Edward Knightly. “DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks”, IEEE/ACM Transactions on Networking, Volume 17, Issue 1, pp 26-39, 2009.
[7] Yu Chen, Kai Hwang and Wei-Shinn Ku. “Collaborative Detection of DDoS Attacks over Multiple Network Domains” IEEE Transactions on Parallel and Distributed Systems, Volume 18, Issue 12, pp 1649-1662, 2007.
[8] Noureldien A. Noureldien , Izzeldin M. Osman, “A Method for Defeating DoS/DDoS TCP SYN flooding Attack”, The SYNDEF College of Technological Sciences Sudan University of Science and Technology, Research gate.
[9] K. Park, and H. Lee, “On the effectiveness of router- based packet filtering for distributed DoS attack prevention in power-law Internets," Proceedings of the ACM SIGCOMM Conference, 2001, pp. 15-26, 2001.
[10] Jelena Mirkovic , Nikola Jevtic and Peter Reiher. “A Practical IP Spoofing Defense through Route based Filtering ” .University of Delaware, CIS department, Technical Report, CIS-TR, 2006.
[11][21] Zhenhai Duan, Xin Yuan and Jaideep Chandrasekhar. “Controlling IP Spoofing through Inter domain Packet Filters” IEEE Transactions on Dependable and Secure Computing, Volume 5, Number 1 , 2008.
[12] Qiming Li, Ee-Chien Chang, Mun Choon Chan. “On the Effectiveness of DDOS Attacks on Statistical Filtering”, proceedings of IEEE INFOCOM, pp 1373-1383, 2005.
[13] Haining Wang, Cheng Jin , and Kang G. Shin . “ Defense against Spoofed IP Traffic Using Hop-Count Filtering“, IEEE /ACM Transactions on Networking, Volume 15, Issue 1, pp 40-53, 2007.
[14] Fu-Yuan Lee and Shiuhpyng Shieh. “Defending against spoofed DDoS attacks with path fingerprint”, International Journal on Computers and Security, Volume 24, Issue 7, pp 571- 586, 2005.
[15] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis Vern Paxson, and Scott Shenker. “Controlling High Bandwidth Aggregates in the Network” ACM SIGCOMM Computer Communication Review, Volume 12, Issue 3, pp 62-73, 2002.
[16] Stavrou, A., Keromytis, A.D., Nieh, J., Misra, V., Rubenstein, D.. “MOVE: An End-to-End Solution to Network Denial of Service”, In Proceedings of the Network and Distributed System Security Symposium, 2005.
17] Abraham Yaar Adrian Perrig and Dawn Song. “Pi: A Path Identification Mechanism to Defend against DDoS Attacks” Proceeding of Symposium on Security and Privacy, 2003.
[18] Vamsi Paruchuri, Arjan Durresi and Sriram Chellappan. “TTL based Packet Marking for IP Trace back” IEEE Conference on Global Telecommunications, 2008.
[19] Jelena Mirkovic and Peter Reiher. “D-WARD: A Source-End Defense against Flooding Denial-of-Service Attacks” IEEE Transactions on Dependable and Secure Computing, Volume 2, Issue 3, pp 216- 232, 2005.
[20] Anat Bremler-Barr Hanoch Levy. “Spoofing Prevention Method ” 24th IEEE Proceedings of Annual Joint Conference of the Computer and Communications Societies, pp 536-547, 2005.
[21] G.Velmayil and Dr. S.Pannirselvam. “ Detection and Removal of IP Spoofing Through Extended-Inter Domain Packet Filter Architecture.” International Journal of Computer Applications, July 2012.
[22] P. Ferguson D.Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing” . January 1998.

Authors profile

G. Velmayil is an Assistant Professor in Department of Computer Science, Quaid-E-Millath Govt. College for Women (Autonomous), Madras University, Chennai, Tamil Nadu, India. She has obtained her Masters degree in Computer Applications and M.Phil degree in Computer Science from Bharathidasan University having 16 years of teaching experience. She has organized various workshops, seminars and conferences. She is currently pursuing her Ph.D in the field of Computer Networks. Her research interest includes DDoS attacks, IP Spoofing and Network Security.

Dr. S. Pannirselvam was born on June 23rd 1961. He is working as Associate Professor and Head of the Department of Computer Science in Erode Arts College (Autonomous), Erode, Tamilnadu, India. He was awarded the degree of Doctor of Philosophy in 2009. On Completion of his M.Sc., Program he served as Lecturer in Erode Arts College, (Autonomous), Erode. Further he

was promoted as Associate professor cum Head of the Department of Computer Science. He has supervised several MCA project works and more than 40 M.Phil Thesis works. His other interests include, Data Mining, Network Security and Mobile Computing. He has presented more than 15 papers in National and International level conferences. He has published more than 5 papers in International journals. He has organized various workshops, seminars and conferences. He has given his valuable contribution to the Bharathiar University, Tamilnadu, India as Senate and Syndicate Member. He served as a Member of various Syndicate sub-committees like Affiliation Committee, Audit and Accounts Committee, Conduct of Examinations in School of Distance Education of Bharathiar University, Coimbatore. He has also served as a member of board of studies in various Universities, Autonomous Colleges and deemed Universities in Tamilnadu. He served as a review committee member for various International conferences held in India.

