International Journal of Scientific Engineering and Science
Volume 1, Issue 2, pp. 5-8, 2017.

# A Survey on Internet Protocol Filtering Mechanisms

Sumeena P S[1], Alpha Vijayan[2], P P Joby[3]
[1]PG Scholar, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology
[2]Associate Professor, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology
[3]Professor and Dean, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology
Email address: [1]sumeenaraihan@gmail.com

***Abstract*—*Mechanism that decides which types of IP datagrams will be processed normally and which will be discarded is called IP filtering. Discarding datagrams means that the datagram is completely ignored and deleted, as if it had never been received. There are many criteria to determine which datagrams are to be filtered. IP filtering is a network layer facility which doesn't understand anything about the application using the network connection. It only knows about the connections themselves. if we want to deny users access to internal network on the default telnet port, but rely on IP filtering alone, it is not possible to stop them from using the telnet program with a port that allow to pass through firewall. By using proxy servers for each service, it is possible to solve this problem. The proxy servers can prevent abuses. If firewall supports a World Wide Web proxy, telnet connection will always be answered by the proxy and will allow only http requests to pass. A large number of proxy-server programs are there. Some are free software and many others are commercial products. Here we present a survey on IP filtering mechanisms.*

***Keywords*—** *IP filtering, routers, address, network traffic, protocols.*

## I. INTRODUCTION

IP filtering is mainly used for security purposes. It is done by allowing only the IP address of registered users. It can reduce the possibility of unauthorized users. IP filtering can provide protection to the operating systems. IP Sec identification is required to apply IP filtering to all traffic. IP filtering has the following characteristics. First is packet filtering and logging and the second is some filtering rules. In short IP filtering provides permission or denial of IP messages.

## II. IP FILTERING TECHNIQUES

IP filtering can provide primary means of protecting the personal computer and operating system. The commonly used IP filtering techniques are:

Inter domain packet filtering, Link Testing, Source filtering, Filtering using TCP timestamps, Logging, Hop count filtering, ICMP traceback, Adaptive Filtering, Bloom filtering, Packet Marking, History based filtering, , Ingress Filtering, Filtering for DDoS, Email filtering, Route filtering.

### *A. Interdomain Packet Filtering*

One of the most difficult security problems to address is the Distributed Denial of Service (DDoS) [1]. Backbone networks [2] are usually affected by DDoS attacks. Existing techniques does not concentrate on to mitigate the effect of an attack while it is raging on, but they focus on tracking the location of the attackers. Here is a novel technique for improving the overall throughput of the legitimate traffic. It can effectively filter out the majority of DDoS traffic. The scheme generalizes the IP traceback schemes to check whether a network edge is infected or not.

The scheme can remove the DDoS traffic while affecting legitimate traffic only slightly, by preferentially filtering out packets that are inscribed with the marks of "infected" edges. This technique can improve the throughput of legitimate traffic. The main disadvantage of this filtering is that there is an assumption that a set of routing policies are employed by the autonomous systems.

### *B. Link Testing*

Testing network links between routers to decide the source of attacker's traffic is the main functionality of link testing [3]. The technique starts from the router nearby to the victim. To decide which one carries the attackers traffic, link filtering interactively test its upstream link. It is done prior to the integration testing that is performed for the complete system and after the individual modules have been tested in isolation. There are two methods for link testing. They are: controlled flooding, Input debugging.

a) *Controlled flooding*

Creating a burst of network traffic from the victim's network to the incoming network segment is the controlled flooding [4]. It checks how the traffic intensity is attacked by this purposefully made to flood. It uses a map which is a known internet topology around the victim. These floods are targeted specifically at certain hosts that are coming from the victim's network.

The victim can trace the incoming network link on the upstream router because there is a change in frequency and intensity of the attacker. One level above on the router the process is repeated. It is a kind of DoS attack which can disturb the genuine traffic on the unsuspicious upstream router and network. This will make it inappropriate for anormous routine usage on the Internet. Advantages are it is well-suited with existing protocol and supports incremental application.

It is well-matched with existing routers and network infrastructure. Disadvantages of the mechanism include it works efficiently only if there is an accurate map of the network topology. For successful trace, the attack should last until the tracing is over. ISP cooperation is also required.

*b) Input debugging*

It is possible to decide the arriving network link on the router, if the router recognizes the attack signature [5]. Until

Volume 1, Issue 2, pp. 5-8, 2017.

the attacker is identified or the trace leaves present ISPs boundary, the ISP must then apply the same procedures to the upstream router joined to the network link. The administrator must contact the upstream ISP to carry on the tracing processes, if the process leaves the present ISP.

Link testing method can be done manually or using any tools that are developed by ISP. It is developed to trace attackers at their own network. It is well-suited with existing protocol. It has irrelevant network traffic overhead. It supports incremental application and it is well-matched with existing routers and network infrastructure.

Disadvantage of the system includes large management overhead in communication and organizing efforts across multiple network boundaries and ISP. It needs time and personnel information on both the victims and ISP side. For successful trace, the attack should last until the tracing is over. It is less appropriate for distributed DoS.

### C. Source Filtering

The features of open group, dynamic membership [6], IP style semantics are adopted by IP multicasting. An efficient group communication mechanism is the IP multicasting. Individual hosts are allowed to specify the reception of packets. Only from a list of source addresses, they may be sent to a multicast group or to explicitly identify a list of the sources whose data the hosts do not want to receive. This scheme provides support of source filtering for shared-tree based IP multicast routing [7]. It allows better bandwidth utility and scalability. The main disadvantage is that the source filtering mechanism has several implementation issues.

### D. Filtering Using TCP Timestamps

A flexible and light weight extension of the Linux net filter packet filter framework is proposed here. It helps to identify hosts completely independent of IP addresses. It takes the advantage of certain characteristics of TCP timestamps [8]. Here it is possible not only to count hosts behind a NAT gateway but also block TCP traffic from single hosts without blocking the gateway itself. This approach scales extremely. Therefore it is suitable for at least medium-scale networks of a few thousand hosts. Here there is an assumption that constant error occurs in the data. This assumption is the main disadvantage of the system.

### E. Logging

Storing the packets at the important routers all over the internet is the working behind logging method [3]. To extract the information about the source of the attackers, it uses data mining methods. Attack traffic can be accurately analyzed by this method. To store the packets, it needs high processing and storage overhead. It also has the legal and statistical problem to store and share the information among different ISP.

Alex Snoeren and colleagues [9] proposed Source Path Isolation Engine (SPIE). Tatsuya Baba and Shigeyuki Matsuda [10] proposed a different method for logging. For storing data in the router logging method uses sliding time window.

Advantages of the system are it is well-suited with existing protocol, irrelevant network traffic overhead, supports incremental application, well-matched with existing routers and network infrastructure, allows tracing even if attacks are stopped, can trace even a single packet.

Disadvantages of the system are resources required for processing and storage, there is legal and logistics issues for sharing information among different ISP, less appropriate for Distributed DoS.

### F. HOP Count Filtering

In flooding traffic to protect and prevent from DoS attack, reflectors should have the ability to filter spoofed IP packets near victim servers. The attacker cannot misrepresent the number of hops an IP packet takes to reach its destination, although an attacker can forge any field in the IP header [11]. An attacker cannot randomly spoof IP addresses while maintaining consistent hop-counts, since the hop count values are diverse. An Internet server can easily infer the hop-count information from the Time-to-Live (TTL) field of the IP header. The server can distinguish spoofed IP packets from legitimate ones, using a mapping between IP addresses and their hop-counts. Based on this observation, here introduces a novel filtering technique, called Hop Count Filtering (HCF) which can build an accurate IP-to-hop-count (IP2HC) mapping table to detect and discard spoofed IP packets.

The basic principles behind HCF are hop count computation, legitimate hop count value capturing and inspection and validation algorithm. As it does not require any support from the underlying network HCF is easy to deploy. HCF can identify spoofed IP packets, and then discard them with little collateral damage. The main issues are to install the HCF system at a victim site includes a systematic procedure for setting the parameters of HCF, such as the frequency of dynamic updates. Building and deploying HCF in various high-profile server sites is difficult. It is not effective in case of real spoofed DDoS traffic.

### G. ICMP Traceback

This method works by iTrace. The victim receives router generated messages in addition to information from the regular traffic in iTrace method. The router generated messages contain information that shows the source of the packet. In addition this message consists of the time the packet was sent and the identification of the packet. All the information to trace the path to its source is combined by network manager. The router will generate ICMP traceback [12] message for only one in 20,000 packets passing through that router to limit traffic.

Intension-driven ICMP traceback is the enhancement of ICMP traceback. The decision module will decide which type of packet can be used in the next iTrace generation module based on information in the routing table. The messaging function between the decision module and iTrace generation module is separated by this method. Based on the decision it will set a special bit in packet forwarding table. This bit can indicate the immediate packet corresponding to the particular

forwarding entry. It will be selected to generate iTrace message.

The advantages of the system are it is well-suited with existing protocol and supports incremental application. It is well-matched with existing routers and network. It allows tracing even if an attack is stopped and ISP coordination's are not required. Disadvantages are it creates additional network traffic and the attackers can use false ICMP traceback message into the packet stream to hide the attacker's original source.

### *H. Adaptive Filterin/G*

The IP pan-tilt-zoom (PTZ) camera is used for general object tracking [13]. This is an adaptive fuzzy filter. It is also a particle filter. Fuzzy membership functions are used to weight particle filter samples. The method is applicable to IP PTZ surveillance system for human tracking application. This method has a good tracking precision. This filtering technique cannot integrate zooming inside the tracking framework by evaluating the quality of samples at each frame.

### *I. Bloom Filtering*

It is initially proposed by Dhamapurikar et al [14]. The destination IP address of the packet is used for IP address lookup [15]. Each prefix length is associated with a W boom filter [16]. They are then grouped according to their prefix length. Then they are programmed into a bloom filter. These bloom filters are then queried well in parallel. The associated hash tables are then accessed serially from longest length. The main disadvantage is that this filtering has highly complex algorithm.

### *J. Packet Marking*

In addition to the packet forwarding, each router in the network puts a mark in the packet. This mark is a unique identifier representing the router. By observing the mark, the victim can find out all the internal hops for each packet. There are 2 types of packet marking, they are: Deterministic Packet marking (DPM) and Probabilistic Packet marking (PPM).

In DPM [17] each router marks all the packets passing through the router with a unique identifier. So the reconstruction of attack pattern at the victim is easy. But the routers are having additional overhead. If an attacker is controlling a trusted router then it can make any path up to that router unless an authentication mechanism is used. If authentication methods are added then it will add cost in terms of both processing time and space. Some of the packets will not be overwritten by the routers. So the attacker will write fake information knowing that these packets will confuse the victim. This method does not work for DoS because it needs large amount of packets to converge.

In PPM [18] DoS attack can be avoided if spoofed source IP address is traced back to its origin which allows assigning penalties to the wrong parties or separating the wrong host or network from the rest of the network.

Advantages are it can be installed incrementally, low cost, effective against Distributed DoS, does not require ISP cooperation, allows tracing even if the attack is stopped. Disadvantages are it needs change in the protocol, produce paths which are not attacking, victims receive a minimum number of packets, does not handle fragmentation.

### *K. History Based Filtering*

Since the operation of Voice over IP (VOIP) telephony relies on the underlying network it is vulnerable to many attacks. To defeat the DoS attacks by blocking the SIP packets from previously unseen sources a history based filtering mechanism is introduced here. To filter SIP packets from unknown source IP addresses during DoS attacks, a lightweight history-based filtering layer before the pre-processing module on the SIP server is placed [19].

This approach can block the attacking traffic during the DoS attack, while allowing the legitimate packets to pass the filter. Compared to an existing defense platform and the original SIP implementation, the proposed approach can improve the CPU utilization significantly during the DoS attacks.

### *L. Ingress Filtering*

Illuminating the capacity to forge source address is one way to overcome the problem of an unknown attacker [3]. It is a preventive method.

The routers should block all the packets that arrive with illegal source address [20]. The main requirement of this mechanism is that to distinguish between genuine and illegal address, a router with adequate power to inspect the source address of every packet and adequate knowledge.

Ingress filtering is most suitable in that network where traffic load is low and the address ownership is explicit like in customer network or at the boundary of Internet Service Provider (ISP).The routing of traffic that starts from a downstream network to recognized and advertised prefixes can be restricted by Ingress Filtering. The packets whose source address does not fit to one of the advertised networks must be dropped by the router.

The main advantage of this filtering is that it can support incremental applications. The disadvantage of the system is that the efficiency depends upon widespread, if not universal deployment. Even if ingress filtering were universally deployed at the customer to ISP level, the attackers can still forge address within the legal customer network.

### *M. Filtering for DDOS*

IP spoofing is commonly associated with DDoS attacks [21] [22] [23]. A new packet marking scheme is the stack path identification marking [24]. Write ahead marking and stack based marking are two new marking methods. Stack pi is a new filtering mechanism and also a new packet marking scheme. The effect of legacy routers are eliminated here. Here employs a new PiLP filter.

### *N. Email Filtering*

Removal of computer viruses and spam are possible with the help of email filtering [25]. Messages can be delivered to the user's mailbox with the help of this filtering. It is possible to edit messages using some email filters.

When a blacklisted IP address is transferred to a new network this filtering become problematic.

Volume 1, Issue 2, pp. 5-8, 2017.

### O. Route Filtering

This is the filtering applied at the routers [25]. This is done before the route is learned or the routes are announced. The filtering is done when a site is multihomed or to ensure that the use of private address does not leaked out.

## III. CONCLUSION

IP filtering is a network layer facility which doesn't understand anything about the application using the network connection. It only knows about the connections themselves. There are many filtering mechanisms available in IP filtering. These filtering mechanisms are mainly used for filtering the IP addresses. IP filtering is a network layer facility. IP filtering is mainly used for security purposes. IP filtering in addition to these functionalities can provide debugging and logging facilities. The IP filtering can reveal the IP address of users.

## REFERENCES


[1] Z. Duan, X. Yuan, and J. Chandrashekar. "Controlling IP spoofing through interdomain packet filters," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, issue 1, pp. 22-36, 2008.

[2] C. Labovitz, D. McPherson, and F. Jahanian, "Infrastructure Attack Detection and Mitigation," *Tutorial, Proc. ACM SIGCOMM*, Aug. 2005

[3] A. C Bhadran and M. Joy. "A survey on IP traceback mechanisms," *International Journal of Science and Research (IJSR)*, vol. 5, issue 8, August 2016.

[4] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," *in Proc. 2000 USENIX LISA Conf*., Dec. 2000, pp. 319-327

[5] R. Stone, "CenterTrack: An IP overlay network for tracking DoS Floods," *Proc. 9th Usenix Security Symp*., Usenix Assoc., 2000, pp. 199–212.

[6] K. C. Almeroth, "The evolution of multicast: From the Mbone to interdomain multicast to Internet2 deployment," *IEEE Network*, pp. 10–20, Jan./Feb. 2000.

[7] D.-N. Yang, W. Liao, and C.-J. Kao, "Source filtering in IP multicast routing," *IEEE Transactions on Broadcasting*, vol. 52, issue 4, pp. 529-542, 2006.

[8] P. D. Z. Varcheie, and G.-A. Bilodeau. "Adaptive fuzzy particle filter tracker for a PTZ camera in an IP surveillance system," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, issue 2, pp. 354-371, 2011.

[9] A. C. Snoeren, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Single-Packet IP traceback," *IEEE/ACM Trans. Networking*, vol. 10, no. 6, pp. 721–734, 2002.

[10] T. Baba and S. Matsuda, "Tracing network attacks to their sources," *IEEE Internet Computing*, vol. 6, no. 3, 2002, pp. 20–26.

[11] Wang, Haining, Cheng Jin, and Kang G. Shin, "Defense against spoofed IP traffic using hop-count filtering," *IEEE/ACM Transactions on Networking (ToN)*, vol. 15, issue 1, pp. 40-53, 2007.

[12] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, L. Zhang, "On design and evaluation of "Intention-Driven" ICMP traceback," *Proc. IEEE Int. Conf. Computer Comm. and Networks*, IEEE CS Press, pp. 159–165.30 IEEE, 2001.

[13] P. D. Z. Varcheie and G.-A. Bilodeau, "Adaptive fuzzy particle filter tracker for a PTZ camera in an IP surveillance system," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, issue 2, pp. 354-371, 2011.

[14] S. Dharmapurikar, P. Krishnamurthy, and D. Taylor, "Longest prefix matching using Bloom filters," *IEEE/ACM Trans. Netw*., vol. 14, no. 2, pp. 397–409, Feb. 2006.

[15] G. Varghese, Network Algorithmics, San Mateo, CA, USA: Morgan Kaufmann, 2005.

[16] J. H. Mun and H. Lim, "New approach for efficient ip address lookup using a bloom filter in trie-based algorithms," *IEEE Transactions on Computers*, vol. 65, issue 5, pp. 1558-1565, 2016.

[17] A. Belenky and N. Ansari, "IP Traceback with deterministic packet marking," *IEEE Comm. Letters*, vol. 7, no. 4, pp. 162-164, 2003.

[18] M. Adler, "Trade-Offs in probabilistic packet marking for IP traceback," *J. ACM*, vol. 52, no. 2, pp. 217-244, 2005.

[19] C. V. Zhou, C. Leckie, and K. Ramamohanarao, "Protecting SIP server from CPU-based DoS attacks using history-based IP filtering," *IEEE Communications Letters*, vol. 13, issue 10, pp. 800-802, 2009.

[20] E Ferguson and D. Senie, "Network ingress filtering: Defeating denial-of-service attacks which employ IP source address spoofing," RFC 2827, 2000R.

[21] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifyingdenial of service attacks," *in Proc. ACM SIGCOMM*, 2003, pp. 99–110.

[22] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denialof service attacks: The shrew vs. the mice and elephants," *in Proc. ACM SIGCOMM*, pp. 75–86, 2003.

[23] D. Moore, G. Voelker, and S. Savage, "Inferring internet denial of service activity," *ACM Trans. Comput. Syst*., vol. 24, no. 2, pp. 115–139, May 2006.

[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, issue 10, pp. 1853-1863, 2006.

[25] https://www.apnic.net/manageip/apnicservices/registrationservices/resource-quality-assurance/filtering.