Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.11, 2014

Denial of Service (DoS) in Internet Protocol (IP) Network and Information Centric Network (ICN): An Impediment to Network Quality of Service (QoS).

Elechi Onyekachi O.
Department of Computer Science, Ebonyi State University Abakaliki, P.M.B. 053, Ebonyi State, Nigeria.
kachyelechi@yahoo.com

Igwe Joseph S.
Department of Computer Science, Ebonyi State University Abakaliki, P.M.B. 053, Ebonyi State, Nigeria.
e-mail

Eze Elias C.*
Department of Computer Science, Ebonyi State University Abakaliki, P.M.B. 053, Ebonyi State, Nigeria.
*E-mail of the corresponding author: chinedum_ez@yahoo.co.uk

Abstract
This paper compares and analyses the Denial-of-Service attacks in the two different Network architectures. The two architectures are based on different routing approaches: Hop-by-Hop IP routing and source-routing using Bloom filters. In Hop-by-Hop IP routing, the packet header contains the address, and the route is decided node by node. Forwarding in this method requires a node to have a routing table which contains the port through which the packet should traverse depending on the address of the destination. Instead in source-routing, the forwarding identifier is encoded with the path a packet should take and it is placed in the packet header. The forwarding identifier in this approach does not require a forwarding table for look ups like the IP routing; it relies on Line Speed Publish/Subscribe (LIPSIN) forwarding solution that focuses on using named links not nodes or interfaces. The forwarding identifier encompasses a set of Link ID's which specifies the path to the recipient and they are encoded in a Bloom filter. The In-packet Bloom filters serve as both path selectors and as capabilities, and they are generated dynamically. However, this thesis is going to focus on the latter network technology by looking at both its benefits and drawbacks as well as analysing the possibilities of having a Denial of service attack.
Keywords: DoS, DDoS, TCP/IP Protocol Suite, ICMP flood, E-mail Bomb, Ping of Death, TCP and UDP

1. Introduction

DoS is an attempt to flood an online service or computer resource by an attacker(s), with unwanted traffic in order to prevent it from functioning efficiently or reliably (Yuval et al., 2010). A lot of sites were affected by such attacks and some believe that this DoS attacks can be minimized or completely eliminated by performing a change in packet forwarding logic in such a way that it will not affect Internet Protocol (IP) or other layers in TCP/IP (Transmission Control Protocol/Internet Protocol) protocol stack. DoS poses a lot of security threats, this made experts to categorize the attacks in certain stages (Mohammed & Martin, 2011). The first stage is the preventive stage which focuses mainly on trying to filter out as many unwanted packets as possible; it also reduces the problem of spoofed IP packet and putting deterrent warnings is also a` form of a preventive measure. The second stage is the detection stage which is concerned with discovering an attack and identifying it. The third one is defense which is also more like the first one; it is concerned with putting necessary security measures in place (Mohammed & Martin,2011).

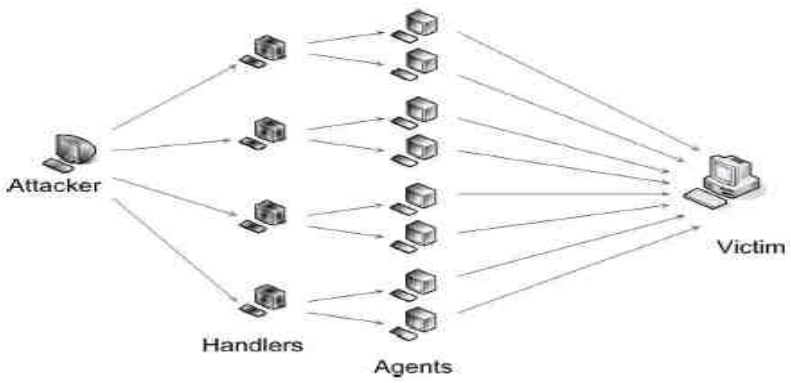

Fig. 1. DDoS: In a Distributed DoS attack the attacker compromises a first tier of vulnerable computers and through them orders a second tier of several more computers to simultaneously attack a specific target (Loukas & Okey, 2009).

The aim of this paper is to compare and analyze the Denial-of-Service attacks in the two different Network architectures. The two architectures are based on different routing approaches: Hop-by-Hop IP routing and source-routing using Bloom filters. In Hop-by-Hop IP routing, the packet header contains the address, and the route is decided node by node. Forwarding in this method requires a node to have a routing table which contains the port through which the packet should traverse depending on the address of the destination. Instead in source-routing, the forwarding identifier is encoded with the path a packet should take and it is placed in the packet header.

Denial of Service attack has become an issue of a concern mostly due to the speed, sophistication and distributed nature of the attack which makes it difficult to identify and mitigate. Also, DoS attacks can occur in any layer of the TCP/IP protocol suite, where each layer has its own distinct type of attack.

The problems caused as a result of DoS attacks is enormous in today's internet. Within the past few years, the Distributed DoS has been an increasing issue of a concern than mainly utilizes compromised machines from disparate locations to launch an attack on a single host. In 1999, an organization which overlooks the security of the internet famously known as Computer Emergency Response Team Coordination Centre (CERT/CC), created an ad-hoc team of security experts from different locations to provide a suitable solution for preventing DDoS. A year later, several sites most of business sites were attacked one after the other, such sites were eBay.com, yahoo.com, Amazon.com, Etrade.com, ZDNet.com and Buy.com (Sandstorm, 2001). And the nature of the attacks carried out was purely DDoS, because all the traffic generated was of malicious intent and they came from multiple locations at once. However, it can be seen that preventing DoS attacks has become an issue of great concern considering its speed, strength, sophistication and distributed nature. It is also very difficult or somewhat impossible for one to find a stable solution for DoS attack in the internet (Sandstorm, 2001).

If we look closely on the nature of DoS attacks, we will notice that all the attacks carried out are as a result of the knowledge of the destination address of the hosts. However, ICN network provides alternatives to the underlined forwarding mechanism that shifts the messaging paradigm to strictly publish/subscribe. This method makes information as the first class object and it is designed for efficient delivering of such information i.e. finding and forwarding information to hosts. In this architecture, the sender and the receiver are completely decoupled in both time and space thereby making the recipient as the initiator of the communication.

This project focuses on identifying the benefits of using ICN network as an alternative to forwarding mechanism in place of the traditional IP network. The ICN network uses an In-packet Bloom filter as the forwarding identifier, where a complete analysis of the false positive probability is carried out. The formulas used in the false positive analysis are, the classical formula, Bose formula and the experimental formula. However, this work does not involve the actual implementation of the Bloom filters on the router, but rather an explanation of the possibility is given.

2. Literature Review

During the Iranian presidential elections, reports showed that protestors lunched a Distributed Denial-of-Service attack (DDoS) on the official website of the Iranian government (Noah, 2009). Similarly, some social networking sites were also hit by a DDoS attack which made them incapacitated for some time. Again in 2010, a group famously known as "Anonymous" lunched a DDoS attack on several sites like MasterCard.com & Visa.com in showing solidarity on the popular Whistle blowing site known as wikileaks which is founded by Julian Assange (Addley & Halliday, 2010). These attacks were all deliberate action by hackers with the sole intention of redirecting heavy unwanted traffic to an intended site.

2.1 Denial-Of-Service Attack on IP Networks

The overall motive for carrying out a DoS attack varies from inconveniencing simple internet users to financial institutions such as banks, as well as intercepting credit card payment from their gateways. The most common method of DoS attack is by overwhelming the target with communication requests there by making it impossible for the target machine to respond to other legitimate request. Some of the major symptoms outlined by United States Computer Emergency Readiness Team (US-CERT) are:

- Denying access to web sites
- Slowing down overall Network Performance
- Rendering a particular web site unavailable
- Unusual amount of spam messages (e-mail bomb or e-bomb)

DoS can also be used to gain access to other peoples computers without their consent there by making the computers slaves to the attacker's machine. The attacker then instructs all slave computers to send simultaneous request to a particular destination. This type of DoS attack overloads the victim's computer and the network, it is popularly known as bandwidth attack. Some of the methods used by DoS attackers to flood services are:

- Exhaustion of computer resources
- Interruption of routing information
- Interruption of network-Host components
- Hindering communication between users and the intended victim to prevent them from communicating adequately.

According to (Tao et al., 2004), DoS attacks can be classified into those attacking stand-alone machines and those that attack network-connected host. DoS attacks can also be done by insiders (i.e. those that have knowledge about the organization), but this type of attack can be counter measured by putting adequate physical security on the servers and some of the network components.

i. **Standalone Attacks**: In this type of attack, the system resources (disk space & CPU time) are consumed by the perpetrators or programs (viruses). The popular standalone attack is known as Asymmetric attack. Examples are Smurf attack, SYN flood and sockstress. (Tao et al., 2004).

ii. **Network Host Attacks**: These are DoS attacks that are associated with Application Layer, Transport layer and Network layers. Some of the attacks are: Application-Level floods, nuke, Teardrop attack, ICMP flood, E-mail Bomb, Ping of Death, etc (Tao et al., 2004).
Other types of DoS attacks are, Permanent DoS (PDoS), Distributed DoS (DDoS) and Low-rate DoS attacks.

iii. **PDoS:** This is an attack that damages the entire system to a point of replacement or reinstallation; it is also known as plashing. It takes advantage of security flaws and remotely gains access to the management interface of the machine. The attacker normally replaces the victim's firmware with a corrupted or defected firmware image (John, 2009).

iv. **DDoS**: This occurs when multiple compromised systems are made to simultaneously target a system by flooding its bandwidth or resources. The attacker compromises a system mostly with a Trojan (virus), which at times comes with a zombie agent or allows the attacker to download one on the system there by making the system a slave to the attacker. The attacker then uses a client program mostly handlers to issue a command to the zombie agents. In DoS, an attack is made from a single host, while in DDoS the attacker uses multiple hosts to attack simultaneously against a host. Sometimes a machine may voluntarily be part of a DDoS attack.
The advantages of DDoS to an attacker are:
    - Difficult to turn off
    - Multiple machine means more traffic
    - Very hard to track down

v. **Low-Rate Dos**: This is a new type of DoS attack which is aimed at reducing TCP throughput by taking advantage of the TCP's transmission timeout. It is also called shrew attacks and eludes detection by the nature of its low-rate effect (Changwang et al., 2010).

2.2 Possible Denial-Of-Service Attacks In I.C.N. Using Source-Routing

i **Replay Attacks:** This happens when a legitimate traffic is used in an illegitimate way. For instance when a zfilter destined from a particular source to a destination is used to flood or provide traffic on that sink. (Rothernberg et al., 2009)

ii. **Computational Attack**: This is a situation where by the attacker makes some analysis about collected zfilter in order to discover some kind of correlation between them. The similarities in the bit pattern more likely represent a path to a particular destination. (Rothernberg et al., 2009)
An attacker can inject traffic in a delivery tree if he can identify a zfilter that passes from a source to the pre-defined route nodes.

2.3 Bloom Filters

A Bloom filter is defined as a set of data structures which is used to ascertain membership queries (Antognini, 2008), or simply it is used to test the membership of an element in a given set. The idea was first developed by Burton Howard Bloom in 1970 (Bloom, 1970), where he considered the following properties:

- False positives are liable to occur, but measures are put in place to control the frequency, while false negatives are impossible to come by.
- The amount of time required to ascertain the membership of an element at a particular node is always independent of the number of elements encoded in the set.
- Bloom filters require only a small amount of space to store its elements.

We know that in ICN, information objects are always considered as the first class abstraction: i.e. giving emphasis on the receiver's interest to ensure the reliability and efficiency in the distribution of the information (Kutscher et al, 2010). In this approach, the information is encoded in the forwarding identifier; this thesis will be focused on using Bloom filters as the forwarding mechanism, because it provides the flexible usage of source-routing-like services. The solution of source routing as proposed by LIPSIN (Jokela et al, 2009) ignores the naming of nodes or interfaces, instead only links are named which are separate in every direction. In addition, the forwarding identifier encompasses a set of link ID's which are encoded as Bloom filters (Bloom, 1970).
In source routing, all the routers (links) which a packet is expected to follow are predefined in the packet header and each forwarding node only contains information about directly connected links in its forwarding table. In essence, this makes the packets very large and the forwarding table to be very small (Trossend, 2009). Bloom filters gives basis for an efficient multicast routing in which all the recipient links are encoded in the packet header without having to replicate a packet at each transfer, it does have a very high degree of security by using a strong cryptographic algorithm when encoding the links. Bloom filters also have a way to reduce the rate of likeliness (false positives) generated in the set i.e. the probability of having a corresponding link in the set which is not previously defined in the Bloom filter (Rothernberg et al, 2009).

2.4 Forwarding With Bloom Link Identifiers

According to (Schnell et al, 2010), a bloom filter contains an array of m-bits (x1, x2,…, xm) with all bits set to zero, then there exist a k independent hash functions (h1,h2,…,hk) where k<<m and m can be very large. Then for a given element to be stored, a hash function will be applied and the result will determine where to place the value 1 at the m-bits. The fact that there are k hash functions makes it imperative to set 1 at all the k-bits positions in the bit array (Antognini, 2008). With the value of m-bits relatively large and k-bits been small makes the link ID's statistically unique. Normally, the link ID's serves 2 purposes: firstly, a Boolean OR is performed on the link ID's that constructs the delivery tree to the required destination, and secondly, upon arrival of a packet at a particular node, the node performs a Boolean AND on the packet from the list of links in its forwarding table.
If there exist multiple link ID's match, then the packet is forwarded as a multicast to all the corresponding links. The more the number of links included in the Bloom filter, the higher the probability of having false positives. Normally, false positives happen when an element does not belong to a set of links defined in the Bloom filter, but erroneously the link coincides when the Boolean AND is been performed. If the number of bits in the array increases then the probability of false positives decreases, at the same time, if the numbers of elements in the Bloom filter increases, then the probability of false positives increases as well. Another way to control the occurrence of false positives is the introduction of link ID Tag (LIT) mechanism, where by each outgoing link is been assigned a name, link name will have a distinct bit pattern which allows the Bloom filter selection on many criteria (Rothernber at al, 2009).
In source routing, the names of links are continuously changed but they are constantly connected to the upper layer protocols e.g. TCP and UDP, this way the upper layer protocols can distinguish between packets belonging to certain applications. This is done to ensure that only authorized packets are forwarded. When a subscriber requests for an application which is already published at the rendezvous system by the publisher, then the topology manager is responsible for creating a delivery tree to that subscriber. Normally, the topology system always knows which incoming or outgoing links to forward all packets to, and also to adjust whenever there are changes in the initial delivery tree. This approach makes forwarding of packets completely different from routing, and the forwarding trees which are inserted on packet headers are source dependent, i.e. different sources may use different Bloom filters to reach the same subscriber. As I already explained in chapter 2, zfilter will be used to refer to Bloom filters in packet headers throughout this thesis.
Bloom filters (zfilter) is developed with certain policy restrictions depending on the situation such restrictions are load balancing, avoiding congested paths, avoid certain links etc.

3. Preventing Denial of Service in ICN using Bloom Filter Packet Forwarding

As I discussed earlier, ICN is a content-driven networking and it is an emerging platform that intends to redefine communication, concentrating on content-centric access rather than hop-by-hop interaction as it is known today. The vast increase of contents generated by users and also due to the fact that most internet interactions are media content oriented which led scientist or researchers to develop a new model that regards contents as the intermediary that can be accessed in an independent location (Pavlou, 2011). This paradigm is based on the interest of the receiver as well as allowing an efficient in-network caching and multicast.

IP network uses source and destination addresses to forward packets, but in ICN we present a solution of routing packets which is Source-routing using in-packet Bloom filters as proposed by (Rothenberg et al, 2009). In IP network, routers serve as capabilities, but in source-routing, the packets serve as capabilities themselves. We then present the use of Bloom filters which is a data structure which verifies whether an element belongs to a given set or not. But it has limitations like huge processing time, heavy headers and false positives. False positives occur when an element is generated in a given set which has not been previously defined. However, the evaluation of false positives is given below, using the classical formula, experimental formula and Bose formula.

3.1 Experimental Formula

We were also able to create a formula with MATLAB that could be able to calculate the false positive probability of the Bloom filters. Firstly, We were able to generate links of all zeroes, and then we generated a random hash function which places 1 at the locations. Secondly, we encoded a number of links together by the process of ORing which in turn forms the Bloom filter. Thirdly, we forwarded the Bloom filter across the paths to evaluate the false positive probability (see appendix). However, a comparison of all the three formulas is given below with varying values of m, n and k respectively.

3.2 Evaluation of False Positive Probability

1. Using the classic formula, We were able to calculate the probability of having false positives under different values of m, n and k. the complete analysis is given below:
   a. If the number of bits (m) and the number of hash functions (k) are both fixed, while the number of nodes encoded in a packet header (n) varies; hence we set the values of the entries as, m=256, k=7, n=5:5:120,

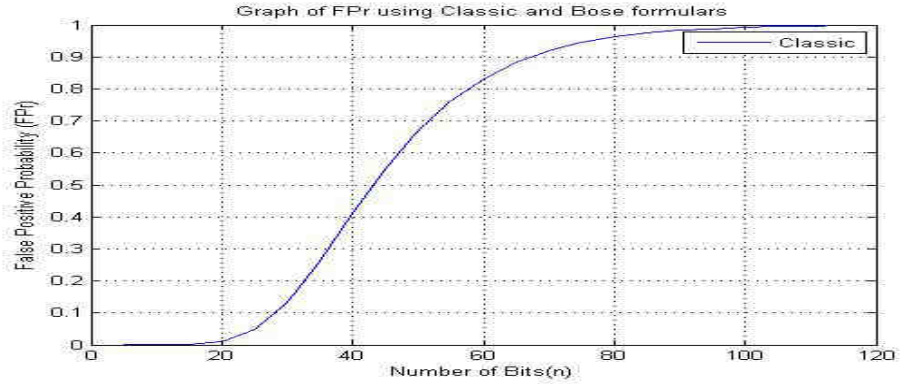

Figure 2: Number of encoded nodes increases in the Bloom filter

The above graph shows that, as the number of encoded nodes increases in the Bloom filter, so does the probability of having false positives irrespective of the higher values of m, and generally, any false positive that is less than 0.1 can be considered as acceptable, but if it is higher than 0.1 then it is considered unacceptable. However, it is mostly preferred not to have false positives at all, but we can obviously see that it is impossible to avoid it when we are dealing with Bloom filters.

   b. If the number of bits (m) and the number of nodes (n) are both fixed, while the number of harsh functions (k) remains constant. The values are given as, m=256, n=20 and k=1:7.

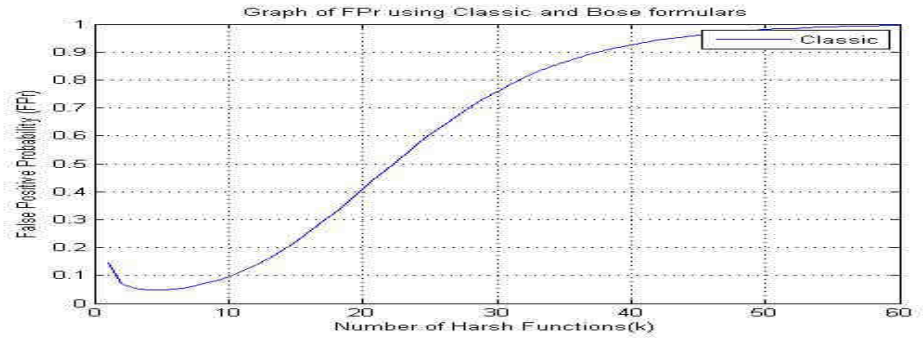

Figure 3: Number of harsh functions increases

This graph shows that, as the number of harsh functions increases, the probability of false positives decreases drastically which almost approaches zero.

c. If the number of nodes (n) and the number of harsh functions (k) are both fixed while the number of bits (m) varies, the entries are given as , m=100:15:250, n=20 and k=7.

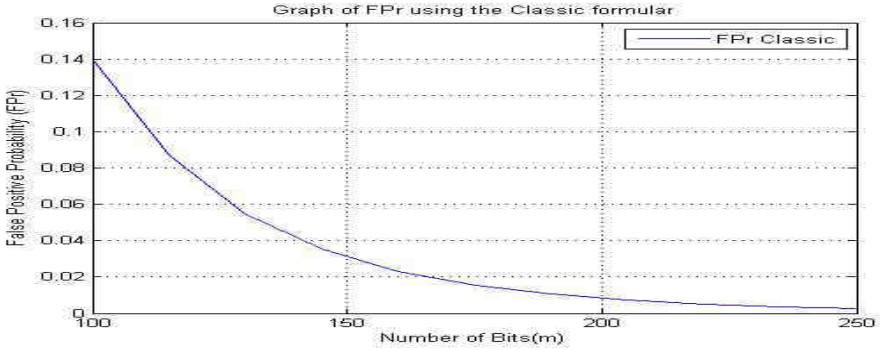

Figure 4: Probability of false positives

From the above graph, it can be seen that the probability of false positives reduces drastically as the number of bits increases. So the whole idea revolves around making the value of m very large to reduce the probability of false positives.

Generally from the above analysis, it can be seen that the number of nodes (n) is the only value that has significant impact on the false positive probability and as we try to encode a lot nodes in the Bloom filter header, we risk the probability of having false positives.

2. The second aspect is the combination of the 3 formulas which we have discussed earlier in this chapter, the experimental formula, the classical formula and the formula proposed by Bose et al (2011). The aim of this comparism is to find the difference, effectiveness or suitability among the 3 formulas. Also the comparism will be based on the fact that both the number of bits (m) and the number of nodes (k) are both kept constant, while the number of nodes (n) varies. The fact that the formula proposed by Bose et al (2011) has some limitations such as, the accommodation of only smaller values of m, n and k. furthermore, we used the smaller entries of m, n and k in order to compare the 3 formulas, as it can be seen below. Hence, we estimated the false positive probability when m=20, k=3 and n=2:2:16. The result is given below.

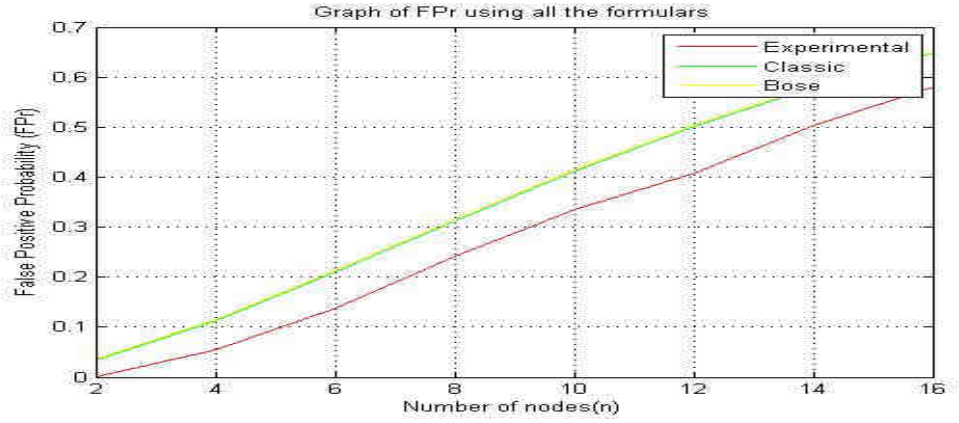

Figure 5: Classical formula and Experimental formula gragh

It can be seen from the result that both the classical formula and the formula proposed by Bose et al (2011) are very closely tied together while the experimented formula gives a more accurate result.

3. The third aspect of the combination is the comparism between the classic formula and the formula proposed by Bose et al (2011).
   a. The first entry is when the number of bits (m) and the harsh functions (k) are both kept constant while the number of nodes (n) varies.

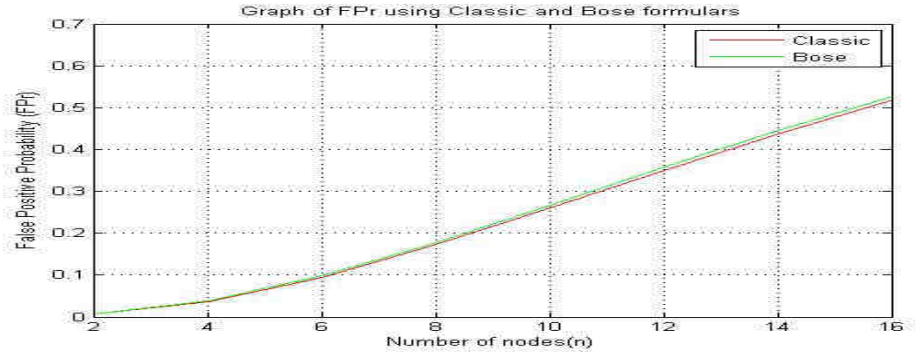

Figure 6: false positive probability graph

The graph shows that the false positive probability increases as the number of nodes increases.

   b. The second entry shows that m and n are both kept constant while k varies. The values are m=30, n=16 and k=1:5.

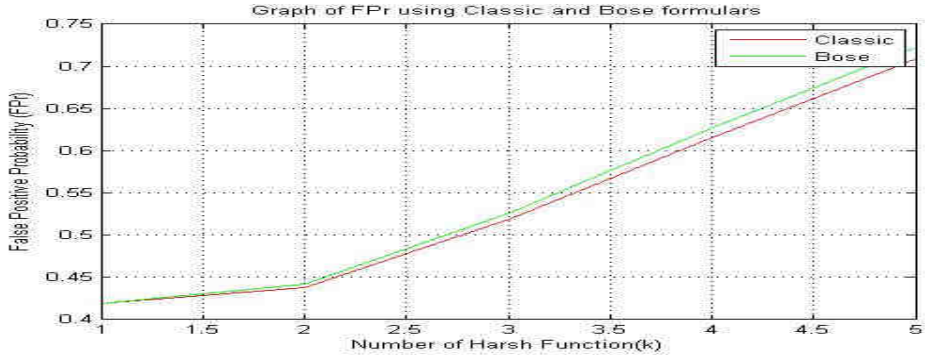

Figure 1: Hash function probability graph

The above graph does not give a very convincing solution because any false positive probability that exceeds 0.1 is unacceptable.

c. The third entry is when the number of nodes (n) and the harsh functions (k) are both kept constant while the number of bits varies. The values are given as n=16, k=3 and m=10:5:30;

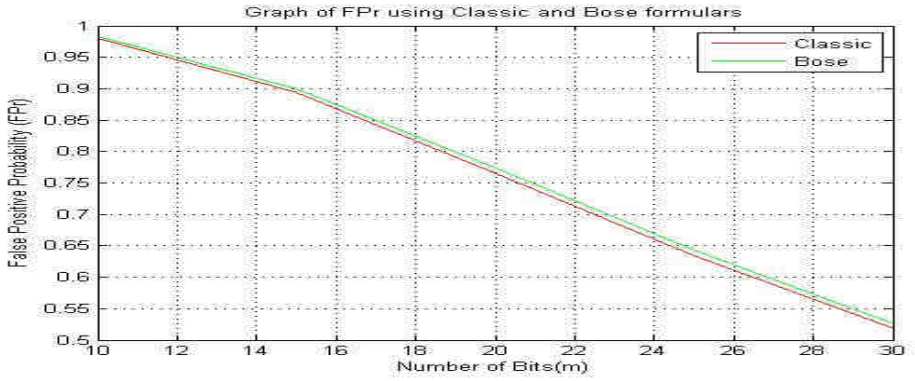

Figure 8: Bits and False Positive probability graph

It can be seen that as the number of bits increases, the probability of false positive decreases drastically

4. Preventing Denial of Service in IP Networks

It is in-fact difficult for someone to fully assure resistance against DoS attacks on one's computer. There are 2 fundamental issues in focus when it comes to denial of service; Protecting your underlined network against attackers, and Protecting machines from compromise (Because they can easily be used in a DDoS attack). Some of the widely known methods of preventing DoS attacks are:

i. Packet Filtering

The very first step taken against mitigating denial of service attack is to enable the ingress packet filtering which has been clearly described in request for Comment (RFC) 2267 which helps to block all unwanted packets coming from spoofed source address. However, this particular method has been confirmed to address the problem of prevention rather than reaction, but nevertheless, it reduces the possibility of using spoofed source address which in turn limits the success chances of the attacker. This method needs the underlined routers to have some knowledge of certain addresses in other to differentiate between the legitimate source address and spoofed ones, and also power to filter out unwanted packets (Alenzei & Reed, 2011). Furthermore, this method has 2 problems associated to it; the first problem involves the range at which the ingress filtering is set to be deployed, this presents issues like high overhead, also other programs require a spoofed address such as mobile IP (Perkins, 1998) and other satellite communications. While the second problem is when a legitimate machine has been compromised by zombie agent to mount an attack. This clearly shows that even if the filtering process is enabled, the attack is liable to be carried out (Alenzei & Reed, 2011)

ii. Intrusion Detection And Prevention Systems (IDPS):

This is a process of monitoring the entire network in order to detect anomalies that may serve as a potential security breach in an organization. In most cases, the intrusion detection system is a software which is specifically designed for such purposes. Some of the requirements needed in order for the IDPS to be effective and also to be deployed successfully include: understanding the network environment, the hosts connected to the network, understanding the arrangement of the physical and logical topologies, details about what is needs to be secured, understanding the various types of DoS and its level of severity etc. Some of the basic functions of the IDPS includes, recording information about anomalies and alerting the administrator about such anomalies, generating reports for future analysis, terminating unwanted connection, it also remove any trace of malicious code from an infected file etc (Gregory, 2011). Detection methods include, anomaly based detection; which tries to compare or sets boundaries between what is considered as normal and abnormal, it also uses mostly statistical measures and is very effective on new threats (Gregory, 2011). The second method is signature-based detection; which involves matching the pattern of the current threat with a previously known threat, the last method is stateful Protocol analysis; this method includes predefined actions on how a particular protocol is to be treated. It should also be able to trace network connections and other application protocols (Gregory, 2011). the types of IDPS include; host-based, which monitors a single host as well

as measuring traffic on that host, secondly we have the network based, which monitors network traffic for a precise network part, the third type is wireless, which monitors traffic on wireless networks, and finally Network analysis behavior, which monitors traffic variations as well as policy violations.

iii. Firewalls:

The main purpose of the firewall is to control the network traffic coming from and going to a secured network. It has the ability to allow or deny certain users access to certain services. At the same time it can enforce a level of authentication before permitting access. It is also used to monitor traffics coming in and going out of a particular network as well as providing a backbone for implementing IPSec tunnels. The types of firewall which can be used on IP Networks include:

iv. Stateful Packet Inspection:

A firewall is said to be a stateful firewall if it is able to record the state of all network connections flowing through it. Such connections mainly include TCP and UDP. It is solely designed with the ability to differentiate between legitimate packets in both TCP and UDP network connections, this way only legitimately active connections will be allowed to flow through the firewall, while all others will be rejected respectively. Normally, the stateful inspection relies on the 3-way handshake when it is been used by TCP, while in UDP it does not depend on the handshake. Also, when a user sends a request, it does that with the synchronization bit (SYN) already set in the header, and any packet received by a firewall which has SYN bit is seen as a new connection. Upon reception of the packet by the firewall, it examines the packet and verifies whether the service is permitted on the server or not, if so, it responds with a packet that has the SYN and ACK set. Then the user replies with a packet which sets ACK bit, which in turn establishes the connection. In essence, this firewall will now allow outgoing and incoming packets for the already established network, but will block all others there by making it extremely difficult for attackers to try and connect to the secured machine. This form of firewall supports wide range of protocols such as FTP, IRC and H.323 (which is used for videoconferencing and VOIP). FTP connections also go through the same process.

v. Application-Level Filters:

This method is used to securely deny P2P related network traffic, because packet filtering cannot guarantee such protection. It also seen as an enhancement on stateful packet inspection. It is used to specify the nature of protocol which is used on each port. For example, the application-level firewall is able to differentiate between HTTP traffic on web and HTTP traffic for file sharing, while a normal packet filtering firewall will consider all HTTP traffic the same. It also allows several application proxies on one firewall. It normally sits in the middle between a client and server, regulating and monitoring the movement of data across them. It can be transparent on the user or non-transparent, it all depends on implementation and address shielding not security. In general, application level proxies handle firewall implementation in one box, i.e. it allows clients to connect to it, it validates the request and it connects to the server. Therefore it also allows responses to come through it and can enforce policies and procedures.

vi. IP-Table Filters:

This is a Linux generated firewall, it checks and verifies packet through a particular network connection (coming to, from, or through) (Mirzaie, et al., 2010). The main components include tables, chains and rules.

a. **Rules**: this contains the criteria for the choice of packet as well as the necessary things to be done out on the packet.
b. **Chain:** this contains a set of rules which specifies the actions needed to be carried out on a packet. The 3 most commonly used chains are input, output and forward.
c. **Table:** this is formed with a collection of chains. It is also divided into filter, NAT & mangle where each has its outlined policy.
d. **Filter:** this usually allows or blocks packets; it uses 3 chains input, output and forward.
e. **Nat:** this is used to translate source or destination address coming in or going out of the network. It also has 3 chains pre-routing, post-routing and output.

f. **Mangle:** this feature is used to modify the packet header. For instance, it can be used to change the TTL field or TOS field. It also has some chains attached to it, pre-routing and post-routing (Mirzaie, et al., 2010)

5. Conclusions

The idea behind this project is to explain a proposed routing approach which is more likely to be highly resistant to DoS attack mainly DDoS. For any information to be sent over the internet, the sender has to get the forwarding identifier to the recipient. The interaction between an information producer and an information consumer in this paradigm is strictly based on publish/subscribe communication throughout the entire network. Publish/Subscribe communication paradigm is the form of messaging in which both the sender and the receiver are completely decoupled in both time and space where messages are not sent directly to the receiver, but rather messages are published or advertised in order for prospective subscribers to show interest. This form of decoupling allows for more improved scalability in the network topology as well as providing a DDoS resistant forwarding solution. It makes use of a recursive architecture that uses 3 elements, Rendezvous system, topology manager and physical layer.

With the Bloom filter is used, the packet is encoded in the forwarding identifier using Bloom filters as the forwarding mechanism because of its flexibility in using source routing like services. Forwarding packets in this approach ignores the naming of nodes or interfaces, instead only links are named and the forwarding identifier encompasses a set of link ID's which are encoded as Bloom filters. The key challenge in this approach is the issue of false positive, which is the probability of having a corresponding link in the set which is not previously defined in the Bloom filter. If there exists a false positive in a particular node, then the packet is forwarded as a multicast to all the corresponding links. The more the number of links included in the Bloom filter, the higher the probability of having false positives. The analysis of false positives has been clearly explained in chapter 4 of the thesis, where the outcomes are quite satisfactory. The anomalies foreseen in the implementation of Bloom filters are packet storms, forwarding loops, flow duplication, replay attacks, correlation attacks, injection attacks and target path attacks. While the security techniques in Bloom filters are limiting the fill factor, z-function formation, number of hash bits and link ID tags (LIT).

Other Dos mitigation techniques in IP networks are packet filtering, intrusion detection and prevention systems (IDPS), firewalls, stateful and stateless packet inspection, application-level filters, iptable filter, rate limit, disabling IP broadcast, enabling unicast path forwarding, etc. However, the most secure system is the system that feels insecure, and always tries to improve its security on a regular basis.

For the future work of this research, optimizing the number of hash functions, effectively and efficiently assigning more than one link ID's on every node, producing a fault tolerant Bloom filter and also creating a well-defined incentive that will lead to its adoption as well as its partial deployment remains a top research interest.

References

Addley, E., & Halliday, J. (2010, December 8). *Operation Payback Criples MasterCard Site in revenge for wikileaks Ban. The Guardian (London)* .

Alenzei, M., & Reed, M. J. (2011). IP Traceback Methodologies. *Computer Science and Electronic Engineering Conference (CEEC), 2011 3rd* , 98-102.

Antognini, C. (2008). Bloom Filters. *Bloom filters* .

Bloom, B. H. (1970). Space/Time trade-offs in hash coding with allowable errors. *communications of the ACM* .

Carrea, L., Almeida, R. C., & Guild, K. (2011). A Qualitative Method to Optimise False Positive Ocurrences for the In-Packet Cloom Filters Forwarding Mechanism. *Computer Science and Electronic Engineering (CEEC), 2011 3rd* , 121-126.

Changwang, Z., Jiaping, Y., Zhinping, C., & Weifeng, C. (2010). *RRED: Robust RED Algorithm to Counter Low-rate Denial-of-Service attacks. IEEE Communication Letters , 14, 489-491.*

Christain, E. R., Petri, J., Pekka, N., Mikko, S., & Jukka, Y. (2009). *Self-Routing Denial-of-Service Resistant Capabilities Using In-packet Bloom Filters. EC2ND '09 Proceedings of the 2009 European Conference on Computer Network Defense* .

Comer, D. E. (2006). *Internetworking with TCP/IPPrinciples, Protocols, and Architechture.* New jeysey: Pearson Prentice Hall.

David Dittrich, (1999). *The "stacheldraht" distributed denial of service attack tool. University of Washignton.*

Gregory, E. (2011). Week 11: Firewalls and Intrusion and Detection Systems (Online). *Available at: http://breo.beds.ac.uk* . Accessed 25-11-2011.

Jokela, P., Zahemszky, A., Esteve, C., Arianfar, S., & Nikander, P. (2009). LIPSIN: Line Speed Publish/Subscribe Inter-networking. *In Proceedings of ACM SIGCOMM '09, Bercelona, Spain* .

Katsaros, K., Stais, C., Xylomenos, G., & Polyzos, G. C. (2010). On the Incremental Deployment of Overlay Information Centric Network. *Future network and Mobile summit 2010 Conference proceedings* .

Kutcher, D., Ahlgren, B., Holgar, K., Ohlman, B., Oueslati, S., & Solis, I. (2011). *Infromation Centric Network. Toronto Canada* .

Kutscher, D., Ahlgrenz, B., Karl, H., Ohlman, B., Oueslatis, S., & Solise, I. (2010). Information Centric Networking. *Dagstuhl Seminar 10492* .

Loukas G. and Oke G. (2009): Protection against Denial of Service Attacks: A Survey. *Intelligent Systems and Networks Group, Imperial College London,* The Computer Journal Vol. 03 No. 7, 2009

Mirzaie, S., Elyato, A. k., & Sarram, M. A. (2010). Preventing os SYN Flood Attack with Iptables Firewall. *Communications Software and Networks 2010 ICSCN '10 Second Int' Conference* , 532-535.

Mohammed, A., & Martin, R. J. (2011*). IP Traceback Methodologies. 2011 3rd Computer Science and Electronic Engineering (CEEC)* , 1-3.

M, S., E, R. C., Aura, T., & Zahemszky, A. (2011). Forwarding Anomalies in Bloom Filter-based Multicast. *INFOCOM, 2011 Proceedings IEEE* , 2399-2407.

Noah, S. (2009, June 15*). Activist Lunch Hack attacks on Tehran Regime. Wired Magazine* .

Pavlou, G. (2011). Keynote2: Information-centric Networking: Overview, Current State and Key Challenges. *Computers and Communications (ISCC), 2011 IEEE Symposium* , 1.

Rothernberg, C. E., Jokela, P., Nikander, P., Sarela, M., & Ylitato, J. (2009). Self Roting Denial-of-Service Resistant Capabilities Using In-packet Bloom filters. *Ericson Research, Nomadic Lab, Finland*

Sarela, M., Rothenberg, C. E., Aura, ,. T., Zahemszky, A., Nikander, P., & Ott, J. (2011). BloomCast: Security in Bloom Filter Based Multicast. *INFOCOM, 2011 Proceedings IEEE* , 1-16.

Tao, P., Christopher, L., & Ramamohanarao, K. (2004). Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring. *In Proceedings of the Third International IFIP-TC6 Networking Conference (Networking 2004)*

Yuval, F., Uri, K., Yuval, E., Sholmi, D., & Chanan. (2010). *Google Android: A Comprehensive Security Assessment. IEEE Security and Privacy (IEEE) (In press) , doi:10.1109/MSP.2010.2.*

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar