Use of Information Centric Network (ICN) as a viable Alternative to Traditional IP Network in Forwarding Mechanism: A Practical Approach to Preventing DoS using Bloom Filter Packet Forwarding

Elechi Onyekachi O.[1*], Eze Elias C.[1] and Eze Joy C.[2]

1. Computer Science Department, Faculty of Physical Sciences, Ebonyi State University Abakaliki, PO box 053, Ebonyi State, Nigeria

2. Department of Industrial Mathematics and Applied Statistics, Faculty of Physical Sciences, Ebonyi State University Abakaliki. P.M.Box 053, Ebonyi State, Nigeria.

* E-mail of the corresponding author: kachyelechi@yahoo.com

Abstract

This paper 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 include 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. In the experimental program, we used MATLAB to generate a set of links and encode them as Bloom filters and used a function known as setdiff, which extracts the number of links to be tested from the actual links array.

Keywords: Information Centric Network (ICN), IP Network, DoS, DDoS, TCP/IP Protocol Suite.

1. Introduction

The internet connects lots of computers and serves many personal and professional needs of people across the world. However, this interconnectivity enables attackers to lunch Denial-of-Service (DoS) attacks on certain sites. These attacks (DoS) are an attempt to flood an online service or computer resource by 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)

Information Centric Network (ICN) is a clean slate design in the network. The architectural paradigm in ICN is no longer end-to-end communication as it is known today; instead it provides alternatives to nowadays communication which is believed to be more efficient and more reliable. The interaction between an information producer and an information consumer in this paradigm is strictly based on publish/subscribe communication primitive throughout the whole network (Kutcher et al., 2011). This gave rise to the proposal of Source-routing using Bloom filters (LIPSIN) (Jokela et al, 2009).

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).

2. Literature Review

In 2009 alone, there were several reports on DoS attacks which severely affected some sites and in some cases leading to the complete shutdown of the sites. During the Iranian 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 IP Networks

IP routing is the form of communication between computers on LANs, WANs and the internet. It removes the impediment of time and distance giving computers the ability to communicate almost anywhere, as well as allowing them to share digital data and applications. It achieves this by forwarding IP packet which consists of binary digits representing data, source address and destination address among other things, which can be routed through the network to the required destination. The routers which are responsible for routing such packets serves as both traffic directors as well as road maps to forward packets based on network address with effective routing protocols.

For an IP datagram to be forwarded on a network the data header must contain the following; Source address, destination address, MAC source address, MAC destination address and Ethernet type among others. The router extracts this information from the IP packet header, and uses the destination address to determine the next hop to which to route the datagram. The router then forwards the packet to the next hop, and then the next router performs the same operation until the packet reaches its final destination. These routers make efficient selection of paths by keeping information in the routing table or lookup table. Conceptually, a routing table maintains entries to a specific destination as well as next hop to that destination, the routing table is updated frequently especially in the event of changes in network topology or hardware failure. (Comer, 2006)

2.2 Denial-of-Service Attack on IP Networks

Denial-of-Service is an attempt to flood an online service or a computer resource by an unscrupulous individual or individuals with unwanted traffic in order to prevent it from functioning efficiently (Yuval et al., 2010). 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:

a) Denying access to web sites,
b) Slowing down overall Network Performance,
c) Rendering a particular web site unavailable and,
d) 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:

(i) Exhaustion of computer resources,
(ii) Interruption of routing information,
(iii) Interruption of network-Host components,

(iv) 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 phlashing. 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: (i) Difficult to turn off, (ii) Multiple machine means more traffic and, (iii) 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).

2.3 Information Centric Network

Information Centric Network (ICN) is a clean slate design in the network. The architectural paradigm in ICN is no longer end-to-end communication as it is known today; instead it provides alternatives to nowadays communication which is believed to be more efficient and more reliable. The interaction between an information producer and an information consumer in this paradigm is strictly based on publish/subscribe communication primitive throughout the whole network. The publish/subscribe system of data dissemination is mostly concerned with decoupling the data producers from consumers putting the consumer's interest ahead in forwarding information objects and its attributes. Based on this concept, (Rothernberg et al., 2009) felt the need to introduce a new forwarding scheme known as source-routing using Bloom filters.

Traditionally, the only method for forwarding packets in a network is Hop-by-hop where by the routers serve as Network capabilities i.e. checking if a packet has been requested by the receiver or not. Rothenberg et al., (2009) propose source-routing to be separate capabilities from forwarding identifiers and making the forwarding identifier serve as Network capability with the aim of producing a DDoS resistant forwarding service. 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 Inter-Networking (LIPSIN) forwarding solution which focuses on using named links not nodes or interfaces. The forwarding identifiers encompass a set of link ID's which specifies the path to the recipient, and they are encoded in a Bloom filter known as zfilter (Jokela et al., 2009). A Bloom filter is normally used to test whether a given element belongs to a set or not and the zfilter is an encoded path containing the names of links to the separate directions.

The zfilter contains some set of functions for making decisions such as the link ID tags, the information content of the packet, the interface information (incoming and outgoing) and a constantly changing secret. The link ID's to the destination are concatenated by a Boolean OR which is then passed to the source for forwarding. When a node receives a packet, it checks within the zfilter if a link ID for any of its outgoing ports is specified, if so, it forwards it to the link, if not, the packet is dropped. In the event of having false positives, there are many selection criteria's that can reduce the probability, for instance, false positives can be reduced by assigning tags to the links respectively. These tags will be given significant amount of bits to make them very large and make it difficult to guess or coincide. This approach addresses a lot of security threats and vulnerabilities by constantly changing the link names, but making sure that the upper layers are aware of the new links in place, as well as allowing only requested packets to be delivered. A node does not need to keep a forwarding lookup table; it just needs to determine the path a packet should take along an outgoing link.

3. Preventing DoS using Bloom Filter Packet Forwarding in ICN

As we 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 Classical Formula

The priori false positive rate can be estimated as thus: suppose we have a set A, which contains members' n, m and k, where n represents the number of nodes which is encoded in the Bloom filter header, K which represents the number of hash functions inserted in the entries and m which is the number of bits. The false positive rate can be estimated based on the formula given below, it is also assumed that the k hash functions are placed at random in the entries ranging from 1, ..., m. At the same time, false positive is said to occur if an element is erroneously generated that has not been previously stored in the Bloom filter and the probability of false positive is known as false positive rate.

$$F(n,m,k) = \left(1-\left(1-\frac{1}{m}\right)^{kn}\right)^{k} \approx \left(1-e^{-\frac{kn}{m}}\right)^{k} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.(1)$$

(Carrea *et al*, 2011)

However, it should be noted that the false positive probability depends on n the number of nodes encoded in the Bloom filter, m the number of bits and k which are the hash functions.

3.2 Bose Formula

This formula claims that the fpr been widely estimated in most books and journals within the past few years is inconclusive and imprecise. In addition, this formula gives some analysis of Bloom filters with some contributions attached; the formula gives the exact false positive rate but only uses lower entries for n, m and k, it shows that fpr is more like a strict lower bound and the formula will serve as an upper bound for all values of k ≥ 2. The formula is given below:

$$\left\{ {kn \atop i} \right\} = 1/i!\sum_{j=0}^{i}(-1)^{j}\binom{i}{j}j^{kn}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

This is known as the Stirling number. Also if everything is been put together, we put P as a function of m, n and k.

$$P(m,n,k) = \frac{1}{m^{k(n+1)}} \sum_{i=1}^{m} i^{k} i! \binom{m}{i} \left\{ {kn \atop i} \right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

3.3 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 (see appendix for the codes)

3.3 Evaluation of False Positive Probability

First and foremost, 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:

- 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.

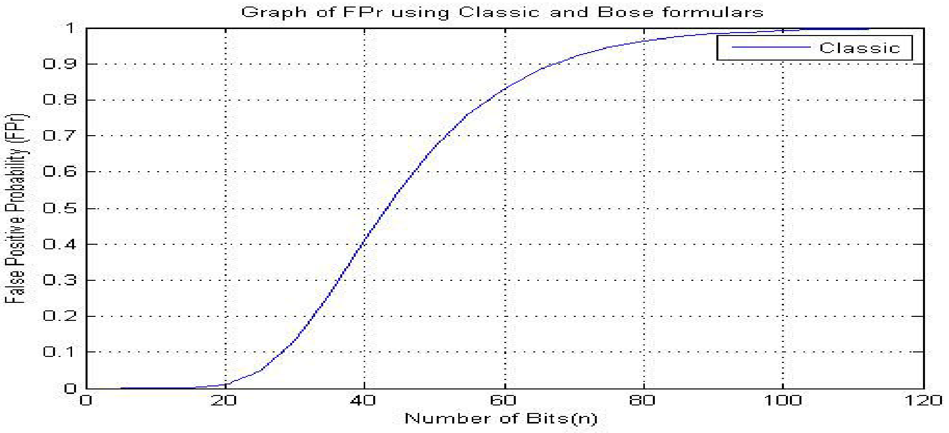

Figure 1. Number of encoded nodes increases in the Bloom filter

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.

- 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.

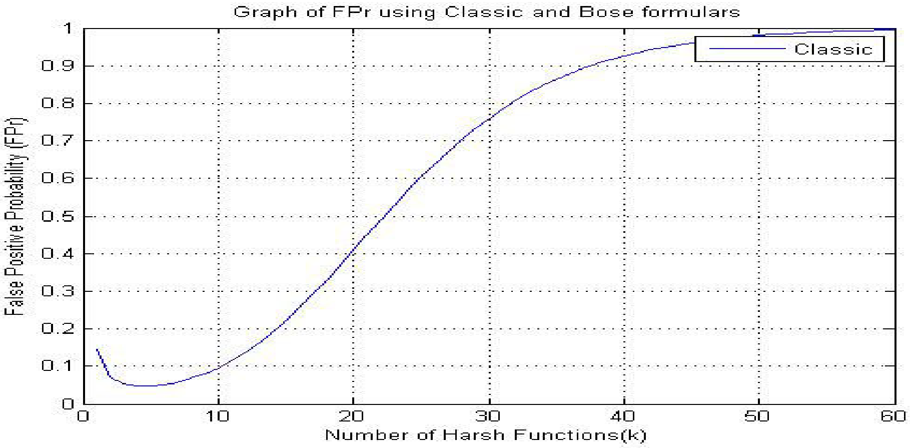

Figure 2. Number of harsh functions increases

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

- 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.

  From the graph below, 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.

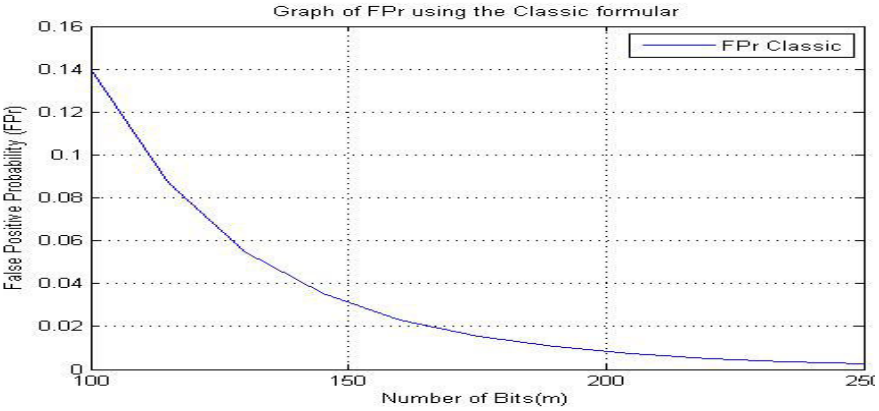

Figure 3. Probability of false positives

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.

The second aspect is the combination of the 3 formulas which we had discussed earlier in this chapter, the experimental formula, the classical formula and the formula proposed by Bose *et al* (2011). The aim of this comparison 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.

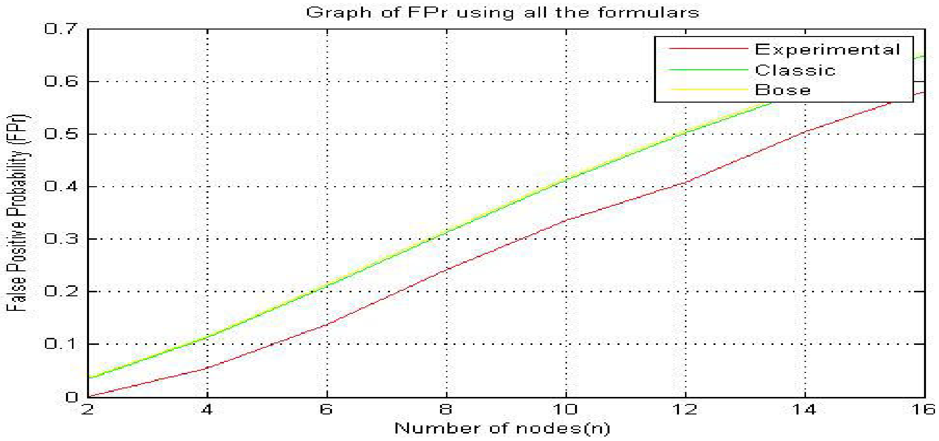

Figure 4. Classical formula and Experimental formula gragh

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.

The third aspect of the combination is the comparism between the classic formula and the formula proposed by Bose et al (2011).

- The first entry is when the number of bits (m) and the harsh functions (k) are both kept constant while th

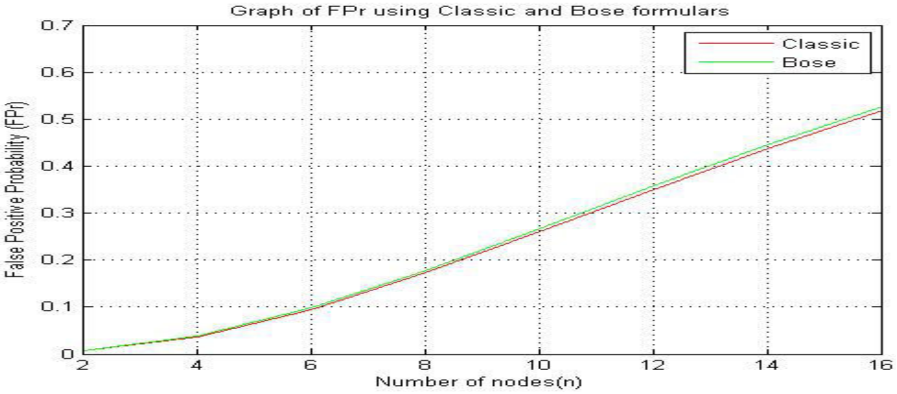

Figure 5. False positive probability graph

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

- 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.

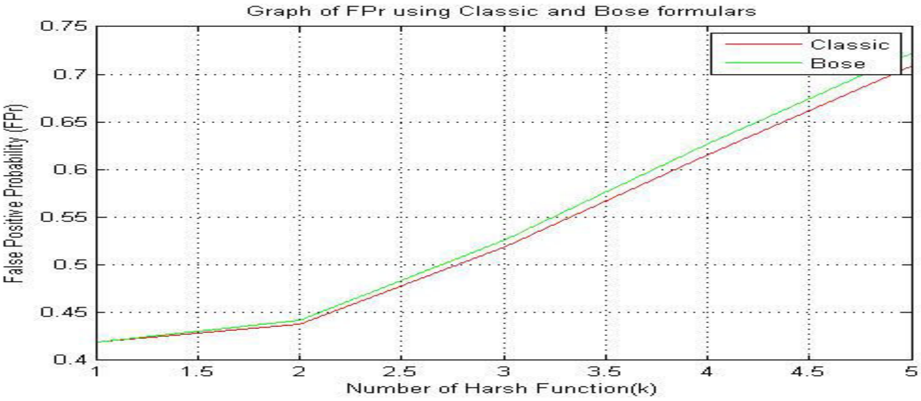

Figure 6. Hash function probability graph

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

- 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.

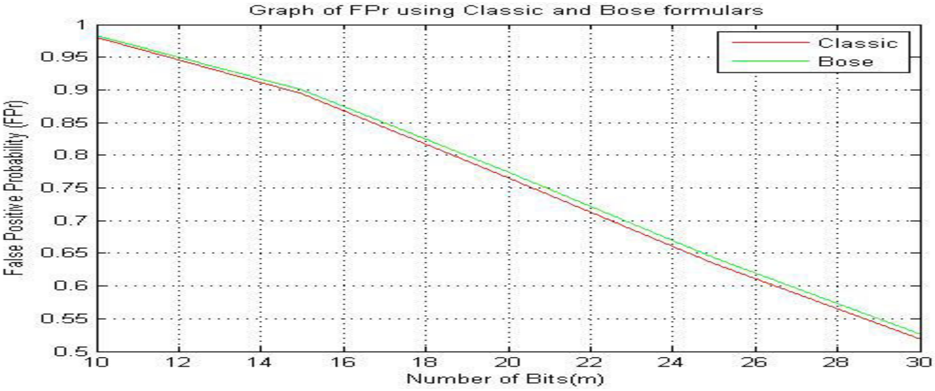

Figure 6. Bits and False Positive probability graph

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

4. Conclusion

ICN is a clean slate design in the network in which the underlying architectural paradigm is no longer end-to-end communication as it is known today; instead it provides alternatives to nowadays communication which is widely believed to be more efficient and more reliable. The interaction between an information producer and an information consumer in this paradigm is strictly based on publish/subscribe communication throughout the entire network.

We then propose a forwarding solution based on Bloom a filter which is used to test the membership of an element in a given set. 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 main 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.

The idea behind this research 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. 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 should be the focus.

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* .

Bradner, A. Mankin (1995). RFC 1752: The Recommendation for the IP Next Generation Protocol.

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.

Hain, Tony. A Pragmatic Report on IPV4 Address Space Consumption. Cisco Systems

John, L. (2009, 03 07). *Phlashing attack thrashes embeded sytems.* Retrieved 07 20, 2011, from The Register: http://www.theregister.co.uk

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* .

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

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.

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.

Perkins, C. (1998). Mobile Networking Trough Mobile IP. *Internet Computing, IEEE* , 58-68.

Prosenjit, B., Hua, G., Jason, M., Evangelos, K., Smid, M., Anil, M., et al. (2008). On The False-Positive Rate of Bloom Filters. *Informtion Processing Letters* , 1-6.

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*

Sandstorm, H. (2001). *A Survey of the Denial of Service problem.* Lulea Sweden: Department of Computer Science and Electrical Engineering, Lulea University of Technology.

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.

Schnell, R., Bachteler, T., & Reiheri, J. (2010). Private Record Linkage with Bloom Filters. *Proceedings of Statistics Canada Symposium* .

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* .

Trossend, D (ed.). (2009). Architechture Definition, component descriptions and requirements. *Deliverable D2.3 PSIRP Project, Tech, Rep* .

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.*

Appendix I

MATLAB Program Source Codes

CLASSICAL FORMULA

```
m = input ('enter the value of m ');
k = input ('enter the value of k ');
%n = input ('enter the value of n ');
n=2:2:16;
y2=(1-(1-1./m).^(k.*n)).^k;
plot(n,y2);
title('Graph of FPr using Classic and Bose formulars')
xlabel('Number of Harsh Functions(k)')
ylabel('False Positive Probability (FPr)')
axis auto
grid on
legend ('Classic')
```

EXPERIMENTAL FORMULA

```
for Nn=2:2:16
for i=1:5000
Nn=input ('enter number of node Nd ');
Nd = input ('enter node degree Nd ');
m = input ('enter number of Bits m ');
k = input ('enter number of hash functions k ');
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Links=zeros((Nn*Nd),m);
Hash=randi(m,(Nn*Nd),k);
for j=1:(Nn*Nd)
    Links(j,Hash(j,:))=1;
end
H=Links(1:Nd:Nd*(Nn-1),:);
C=setdiff(Links,H, 'rows');
%H=Links(1:Nd:Nd*(Nn-1),:);
[a,b]=size(H);
[t,n]=size(H);
% m is the number if columns in the matrix%
final=0;
for e=1:t
     %check if counter is less than num of columns%
    if (e ~= t)
    %check if first column%
      if (e==1)
    %if first column compare first item with seconf item%
    BF = H(e,:) | H(e+1,:);
      else
          %if not first column compare previous result with the next column%
    BF = final | H(e+1,:);
      end
   % store answer in another variable and use it to process other rows%
      final = BF;
    end
end
[q,u] = size(C);
FP=0;
% q is the number if rows in the matrix%
for k=1:q
     %check if counter is less than num of columns%
    if (k ~= q)
      %if not first column compare previous result with the next column%
      R = final & C(k,:);
        if (R==C(k,:))
```

```
          FP=FP+1;
                end
          end
end
Fp=FP/q;
Q(i,1)=FP;
%Q is the array of false positives%
W(i,1)=Fp;
%W is the array of false positives probability%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
end
MFP=mean(Q);
MFp=mean(W);
%if (mod(Nn,2)==0)
        Z(Nn,1)=MFp;
%else
  %      YU(Nn,1)=MFp;
end
%end
y1=Z(2:2:16);
%x=(2:2:16);
%plot(x,y)
```

BOSE FORMULA

```
m = input ('enter the value of m ');
k = input ('enter the value of k ');
%n = input ('enter the value of n ');
for n=2:2:16
for i=1:m
        for j=0:i
                r(j+1,1)=((-1)^j)*factorial(i)/((factorial(i-j)*factorial(j)))*((i-j)^(k*n));
        end
y(i,1)=i^k* factorial(i)*(factorial(m)/(factorial(m-i)*factorial(i)))*(1/factorial(i))*(sum(r));
end
d=sum(y);
v = m^(k*(n+1));
r=1/v * d;
w(n,1)=r;
end
```