Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

E-FireCol to Detect Multiple DDOS Attacks

Ravi Chandra.K
Student of M.Tech(CSE)
JNTUK UCEV, Vizianagram, India

Madhavi Gudavalli
Assistant Professor, IT Department
JNTUK UCEV, Vizianagram, India

Abstract: A denial of service (DOS) attack targets the denial of access by legitimate users to shared resources or services. This is due to wide variety of context from operating systems to network-based services. The first form aims to crash a system by sending one or more carefully constructed packets that exploit software vulnerability in the target system. The second form is to use massive volumes of useless traffic to occupy all the resources that could service legitimate traffic. Distributed denial-of-service (DDOS) attacks are major problems in terms of security for the networks. The mitigation of which is very hard especially when it comes to highly distributed botnet-based attacks. The early discovery of these attacks is necessary to protect end-users as well as the expensive network infrastructure resources. This paper presents the extended FireCol (E-FireCol) composed of intrusion prevention systems located at the Internet service providers (ISPs) level. Intrusion prevention systems form virtual protection rings around the hosts to defend against DDOS attacks and collaborate by exchanging selected traffic information. Our experimental results proves that E-FireCol is effective and supports the different ISP rule structures there by detecting more DDOS attacks when compared with the FireCol.

Keywords:- Distributed denial-of-service attacks (DDOS), Internet service providers (ISPs), network security, botnet attacks, EFireCol

I. INTRODUCTION

Now a days providing security to the network has become a mandatory for the survival of many entities that depend on their Internet presence. Protection against network attacks is a necessary to stay in today's global market. So Denial of Service Attacks (DOS) have been considered one of the main threat against computer networks. There are two aims for DDoS attacks. The first is to consume the resources of the host and second is to consume the bandwidth of the network. Normally, a huge set of machines are used to launch a Distributed Denial of Service (DDOS) attack against a certain server or set of servers. The attack, originating from different sources, is very hard to detect via any single border firewall or IDS as each device has only a local view. Besides, attackers try to generate packets that look like normal traffic. On the other hand, protecting the server at the close vicinity of its network is also inefficient because it becomes overwhelming for a single device to perform all the packets classification of the huge concentrated amount of traffic that it receives. Another traffic type called a "flash crowd" is experienced when many legitimate users start to access one particular site at the same time.

The impact of DDOS attacks can vary from minor inconvenience to users of a Web site to serious financial losses for companies that rely on their online availability to do business [2]. DDOS attack defense the problem in terms of attack detection and packet filtering and addressing some of the technical challenges posed by those tasks. Most recent works aim at countering DDOS attacks by fighting the underlying vector that is usually the use of botnets. The master can launch synchronized attacks by sending orders to the bots via a Command & Control channel. To avoid the issue on the detection of DDOS attacks and per se not their underlying vectors. Non-distributed denial-of-service attacks usually exploit vulnerability by sending few carefully forged packets to disrupt a service. DDOS attacks are mainly used for flooding a particular victim with massive traffic as highlighted. Network administrators expect the research community to provide useful techniques for detecting and mitigating these problems but until now their weapons are spoofing prevention techniques.

The original aim of the Internet was to provide an open and scalable network among research and educational communities [3]. With the rapid growth of the Internet over the past decade, the number of attacks on the Internet has also increased rapidly. The aim of a bandwidth attack is to consume critical resources in a network service. The attacker can prevent legitimate users from accessing the service. As shown in the fig.1 typical DDoS attack contains two stages:

- To compromise vulnerable systems that are available in the Internet and install attack tools in these compromised systems
- The attacker sends an attack command to the "zombies" through a secure channel to launch a bandwidth attack against the targeted victim(s)

There are several unique features of DDOS attacks that make effective defenses extremely difficult to design.

A. Botnets

Online computers especially those with a high-bandwidth connection have become a desirable target for attackers. Direct attacks refer to sending packets containing a malicious payload that exploits a vulnerable computer.

These attacks are conducted via automated software so that the number of compromised computers can be maximized in a short period. A common way for attackers to control the bots is to use Internet Relay Chat (IRC) channels [4]. The IRC is a form of real-time communication over the Internet. It is mainly designed for group communication in discussion forums called *channels.* These compromised computers that can be managed by the attacker through the IRC channel are called a *botnets*. IRC channels are not the best solution for an attacker to communicate with the bots in terms of efficiency and robustness.

B. FireCol Architecture

The FireCol system maintains [5] virtual rings or shields of protection around registered customers as shown in the Figure 1.

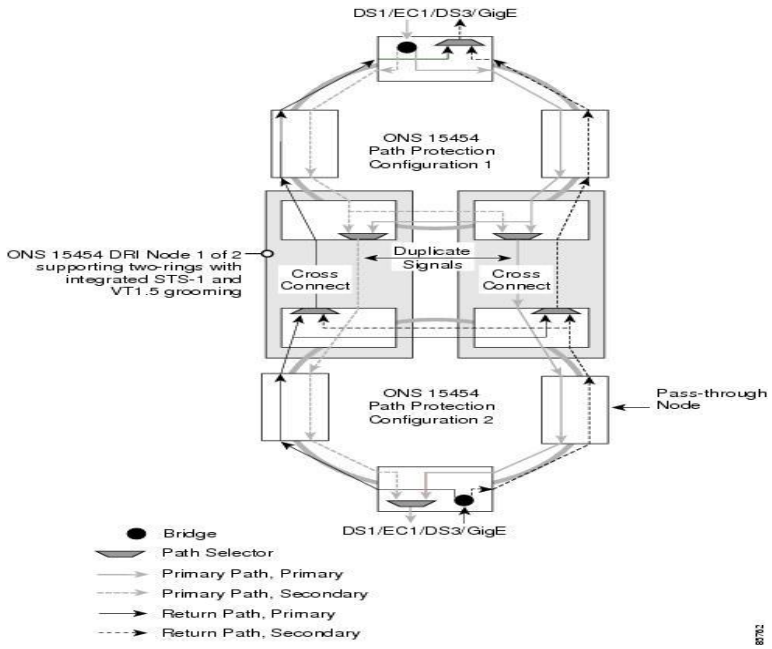

Figure 1. *FireCol* Architecture

The ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer as shown in Figure 2.

FireCol protects the registered subscribers based on the defined rules. FireCol rule matches a pattern of IP packets and it corresponds to an IP sub network or a single IP address. The rule definition can include any other monitorable information that can be monitored. FireCol is a benefit service to which customers subscribe using the protocol depicted. The trusted server adds an entry with the subscribing rule along with its subscription period (TTL) and the supported capacity. All communications between subscribers and the server are secured a using private/public key encryption scheme. Rule capacities can be provided either by customers or by the ISP. IT services of large companies should be able to provide such information regarding their infrastructure. FireCol allows the coexistence of multiple virtual protection rings for multiple customers across the same set of IPSs because of their inherent complete independence.

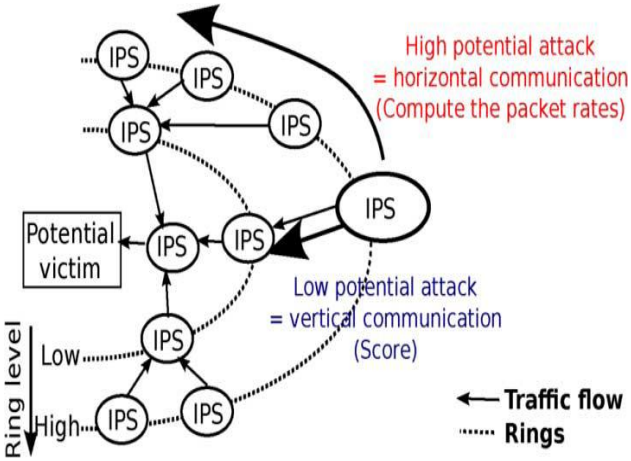

Figure 2. Horizontal and Vertical communication in *FireCol*

C. *FireCol SYSTEM*

FireCol maintains the following frequency and entropy-based metrics.

Frequency: The frequency f_i is the proportion of packets matching rules r_i within a detection window.

$$f_i=\frac{F_i}{\sum_{j=1}^{n} F_j}$$

Where F_i=number of packets matched by rule r_i by detection window

Entropy: The entropy measures the uniformity of distribution of rule frequencies. If all frequencies are, equal then the entropy is maximal and the more skewed the frequencies.

$$H = -E[\log_n f_i] = -\sum f_i \log_n(f_i)$$

Relative Entropy: The relative entropy metric measures the dissimilarity between two distributions. If the distributions are equivalent then the relative entropy are zero and the more deviant the distributions.

D. Firecol Attack Detection Algorithm

The collaboration manager [6] computes the corresponding packet rate using rule frequencies and the overall bandwidth consumed during the last detection window. An alert is raised if the rate is higher than the rule capacity. Else, the computed rate is sent to the next IPS on the ring.

Algorthim:

```
1: if bi ^(IPS_id≠ null) then
2: if IPS_id = = myID then
3: bi = false;
4: return
5: else
6: ratei ← ratei+Fi
7: if ratei > capi then
8: bi = false;
9: raise DDOS alert;
10: return
11: else
12: next IPS check Rule (IPS_id,i,rate,capi)
13: endif
14: endif
15: else
16: bi = true
17: next IPS.check Rule(my ID,I,0,capi)
18: end if
```

It first checks if it was the initiator when an IPS receives a request to calculate the aggregate packet rate for a given rule. It deduces that the request has already made the round of the ring, and hence there is no potential attack. Else, it calculates the new rate by adding in its own rate and checking if the maximum capacity is reached, in which case an alert is raised. Algorithm 1 shows the details of this procedure. Rate computation can be performed based on the number of packets per second (pps) or bytes per second (bps). The method is more suitable for detecting flooding DDoS attacks having a small packet pattern. Bytes-based method is better for detecting flooding attacks with large packet payloads. While FireCol already gives us an effective solution to the high rate attacks, and a system needs to be designed that could successfully detect LDoS attacks as well.

The high rate DDoS attack can be detected by computing the entropy and frequency values of the incoming packets. The incoming bandwidth level exceeds the ISP allocated bandwidth. The ring level protection of FireCol is assigned only to the subscribed users of that particular ISP. Intruders now resort to Low Rate DDoS attacks [7], as there are not many algorithms that successfully prevent it. Successful DDoS prevention algorithm must be equipped to prevent both High Rate and Low Rate DDoS attacks. Hence, it is always necessary to be one-step ahead of the intruders and our system promises to limit the DDoS attacks up to a maximum extent. There are Intrusion Prevention Systems deployed around the user in a ring like structure that has H-IPS in the outer ring that primarily focuses on preventing High Rate attacks. If the incoming bandwidth exceeds the allocated limit then it is understood that the system is under attack and the incoming packet will be immediately dropped. Some Low Rate attacks can pass through the system when this ensures that the High Rate attacks are successfully blocked.

II. PERFORMANCE EVALUTION

The objective [8] of the experiments is to evaluate the accuracy of *FireCol* in different configurations. The robustness of *FireCol* is evaluated in abnormal situations such as the existence of non-cooperative routers or configuration errors.

A. Simulations

Although obtaining real router traces is possible getting synchronized traffic and host states of a real network along with its detailed topology is quite difficult for security and privacy reasons. We tested different topologies with a variable number of rings. A sample topology of five customers with a specific rule for each is shown in the Figure 3.

The *fan-out* effect is taken into consideration with the number of IPSs between rings. This fan-out effect generates enough routers for highlighting the collaboration. The varying it does not significantly impact the results except a little delay in the time needed to detect an attack due to a larger number of collaborating routers.

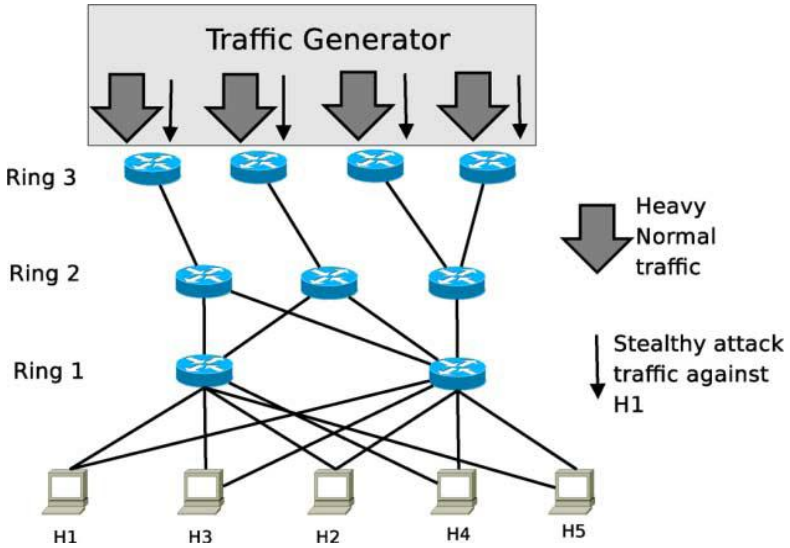

Figure 3.Sample Simulation Topology

B. Ring Levels of the Attack

A skilled attacker might launch an attack from within the vicinity of the victim. The extreme case corresponds to a single ring. This rare case implies that the attack is no more distributed and can be detected without collaboration since its traffic is more concentrated and distinguishable. Using only one or two rings is not efficient because all traffic is also analyzed by only these rings and so is not really distinguishable from attack traffic. By using a five-ring topology with attacks injected at the first or the second rings the benign traffic is also analyzed by the upper rings. Figure 4 highlights that such a five-ring topology is also suited to detect attacks emanating from lower-order rings. It also depicts both the number of false positives and true positives as a ratio compared to an attack launched at the first ring.

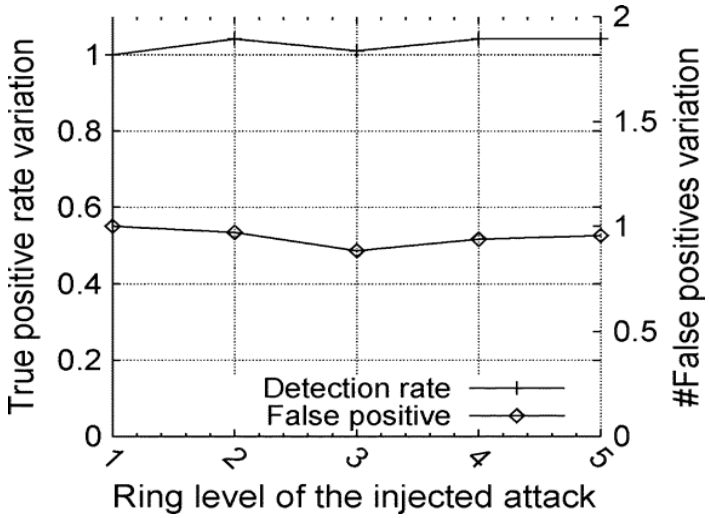

Figure 4.Insignificant impact of the attack injection location

III. EXPERIMENTAL RESULTS

The Figure 5 shows the transfer of packets from source to destination and the attacker nodes sends continuously packets to the source**.** This E-FireCol detects the attacks which are bound to single IPS rule structure level only. The Figure 6 shows the comparison of throughput between FireCol and E-FireCol. The proposed extended FireCol named as E-FireCol supports the different IPS rule structures and detects more DDOS attacks compared to FireCol by observing the graph of E to E delay between FireCol and E-FireCol shown in Figure 7. Throughput is the average rate of *successful* message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second and sometimes in data packets per second or data packets per time slot. End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

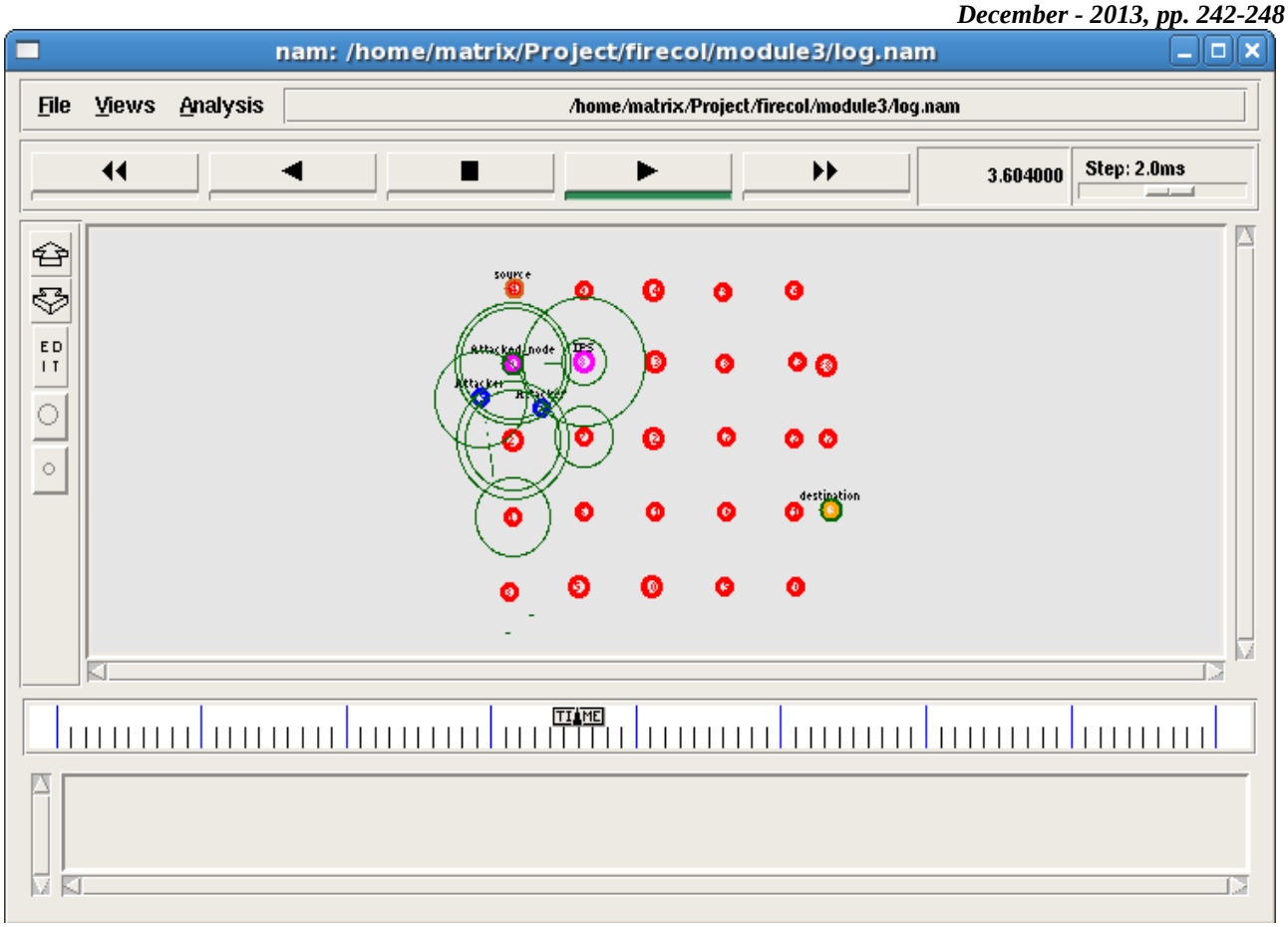

Figure 5. Transfer of packets from source to destination

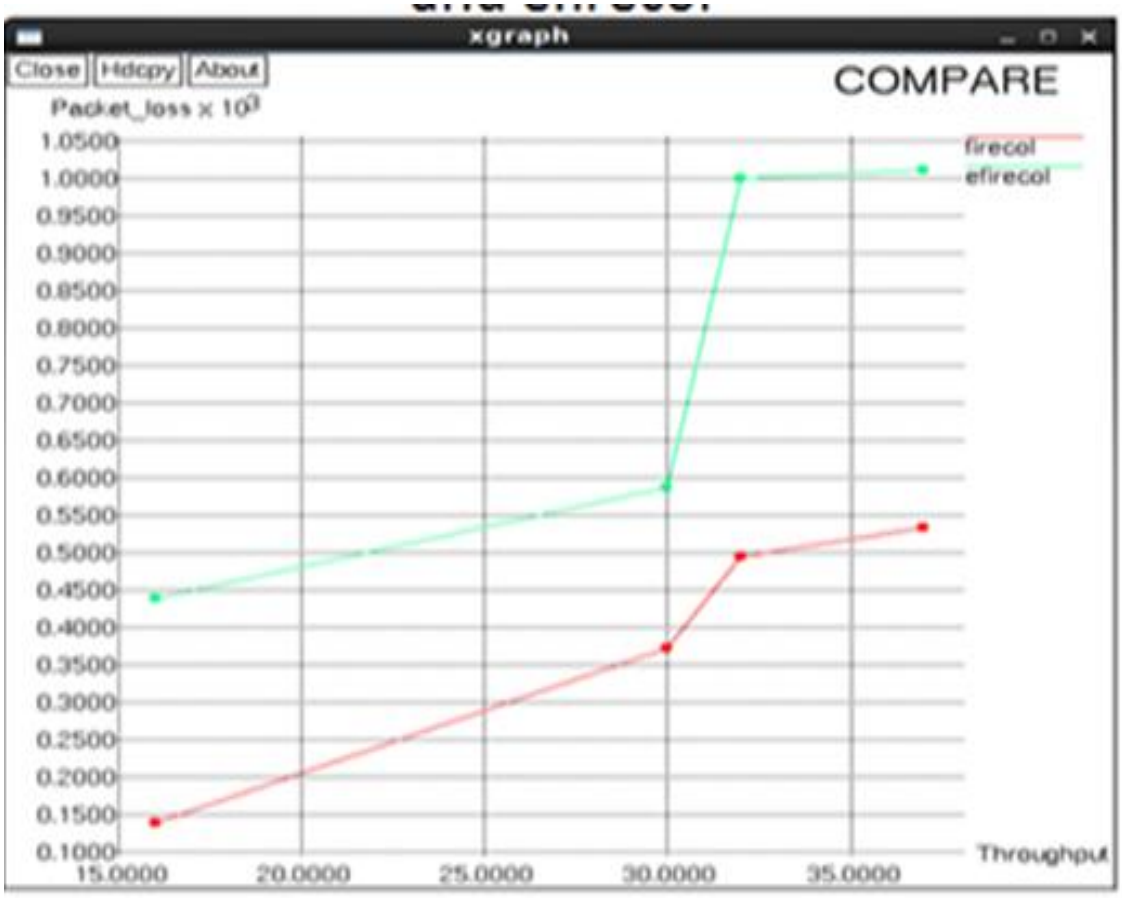

Figure 6.Comparison of throughput between FireCol and e-FireCol

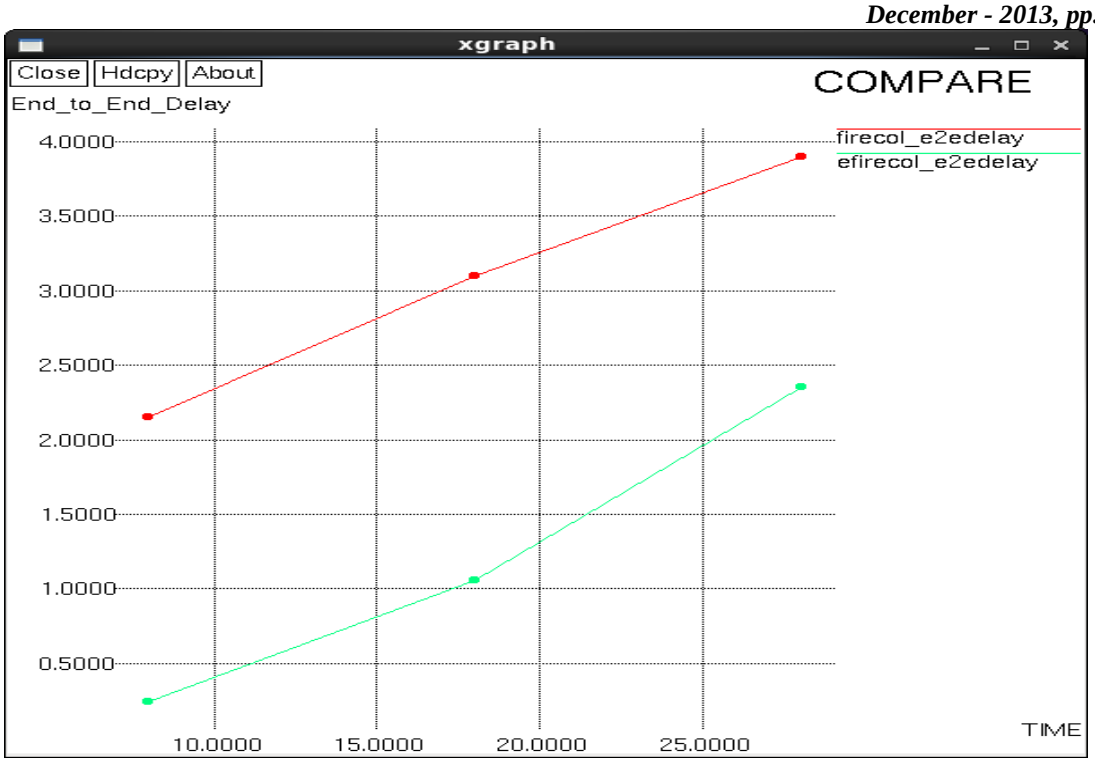

Figure 7.Comparison of E to E delay between FireCol and e-FireCol

IV. CONCLUSION

Proposed EFireCol is a scalable solution for the early detection of flooding DDOS attacks. Expect that Internet Service Providers will begin to deploy more distributed defense mechanisms at the ingress and egress points of their networks. The longer-term challenge for defense against DOS attacks is how to achieve cooperation between ISPs. Belief scores are shared within a ring-based overlay network of IPSs. Experiments showed good performance and robustness of EFireCol and highlighted good practices for its configuration. The analysis of EFireCol demonstrated its light computational as well as communication overhead. The accounting for EFireCol is therefore facilitated as a benefit service to customers.

REFERENCESS

[1] Jéerôme François, Issam Aib, Raouf Boutaba, "*FireCol*: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," IEEE/ACM Transactions on Networking.

[2] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network- based defense mechanisms countering the DoS and DDoS problems," *Comput. Surv.*, vol. 39, Apr. 2007, Article 3.

[3] E. Cooke, F. Jahanian, and D. Mcpherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in *Proc. SRUTI*, Jun. 2005, pp. 39–44.

[4] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm," in *Proc. USENIX LEET*, 2008, Article no. 9.

[5] J. Françcois, A. El Atawy, E. Al Shaer, and R. Boutaba, "A collaborative approach for proactive detection of distributed denial of service attacks," in *Proc. IEEE MonAM*, Toulouse, France, 2007, vol. 11.

[6] A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs, "Locating Internet routing instabilities," *Comput. Commun. Rev.*, vol. 34, no. 4, pp. 205–218, 2004.

[7] A. Basu and J. Riecke, "Stability issues in OSPF routing," in *Proc. ACM SIGCOMM* , 2001, pp. 225–236.

[8] A. Networks, Arbor, Lexington,MA, "Worldwide ISP security report," Tech. Rep., 2010.

AUTHORS BIOGRAPHY

Ravi Chandra K received B.Tech (Information Technology) from JNTU and pursuing M.Tech(CSE) in JNTUK University College Of Engineering Vizianagaram. His areas of research includes Computer Networks, Image Processing and Information Retrieval Systems

Madhavi Gudavalli received the B.Tech(CSIT) from JNTU , M.Tech(CSE) from JNTU Hyderabad and registered Ph.D in Computer Science & Engineering discipline from JNTU Hyderabad in 2011. She is currently working as Assistant Professor in the Department of Information Technology at **JNTUK University College Of Engineering Vizianagaram**. She guided many projects in the area of image processing for CSE & IT Departments. Her research interests are in the areas of Biometrics and Image Processing. Her research articles are accepted in peer reviewed journals, international Conferences and

proceedings are published in IEEE, ACM digital libraries. She played a vital role in AICTE-NBA Accreditation work at CVR college of Engineering, Hyderabad in 2007. She conducted several workshops/seminars/conferences at institutional level. She was sanctioned with Major Research Project entitled **A Next Generation Identity Verification System To Provide Security** in the area of Biometrics as Co-Principal Investigator by **AICTE** under Research Promotion Scheme. In recognition of her outstanding scientific contributions her research articles received Travel grant from **DST** and **UGC**. She has filed three **PATENTS** entitled *Hybrid Approach for Multimodal Biometric Template Security, Automotive Security System Using Embedded Biometrics* and *Enhancing The Security Strength Of Cloud Computing Through Biometric Template Protection Scheme* which are published in Indian Patent Journal. She is a Life member of different Professional bodies such as ISTE and CSI. Her research contributions are not only confined to subject area but also extended to other related domains arising out of the new education system, assessment and accreditation, and their impact on Indian Higher Education. As an off shot of research endeavour's her papers were accepted and presented in **World Education Summit (WES 2012-AICTE)** entitled *International Practices In Assessment, Accreditation & Quality Standards In Higher Education*. The hallmarks of her illustrious career include teaching Engineering and Technology and pursuing exemplary research on improving security by using advanced tools of Biometric systems.

