International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

A COLLABORATIVE SYSTEM TO DETECT DDOS ATTACK IN THE NETWORK

Bharathi R [1] and ArunaDevi [2]

[1, 2] *Assistant Professor, Dept. of ECE, GSSSIETW, Mysuru*

ABSTRACT

Distributed denial-of-service (DDoS) attacks remain a major security problem, the mitigation of which is very hard. The early discovery of these attacks, although challenging, is necessary to protect end-users as well as the expensive network infrastructure resources. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms. The core of the proposed system is composed of Intrusion Prevention Systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of the proposed system using simulations is presented.

Keywords: Detection, DDoS, Flooding, Entropy, Collaboration, Network Security, IP Network

I. INTRODUCTION

A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources.

Distributed denial-of-service attacks can paralyze even the well-structured network for days, costing millions of dollars in lost sales, freezing online services and crippling a company's reputation.

DDos attacks can also lead to problems in the network 'branches' around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by an attack, compromising not only the intended computer, but also the entire network.

Specific controls to combat DDoS attacks can include:

1. Working with the Internet Service Provider (ISP) to establish quality of service rates to limit the amount of bandwidth one customer can utilize
2. Using firewalls and filtering devices to filter all unnecessary ports and protocols
3. Incorporating redundancy and resiliency into designs of key systems
4. Utilizing IDS/IPS to identify and block attacks in progress

A single Intrusion Prevention System (IPS) or intrusion detection system (IDS) can hardly detect such DDoS attacks, unless they are located very close to the victim. However, even in that latter case, the IDS/IPS may crash because it needs to deal with an overwhelming volume of packets (some flooding attacks reach 10–100 Gb/s). In addition, allowing such huge traffic to transit through the Internet and only detect/block it at the host IDS/IPS may severely strain Internet resources.

In this paper we propose the solution to prevent the DDOS attack

II. LITERATURE SURVEY

- **In paper [1] "Distributed firewalls"** The design where only the firewall rules are exchanged and each firewall detect the attacks on its own.
- **In [3] "A protocol and simulation for distributed communicating firewalls"** similar to the previous work but instead of distributed firewalls a Gateway is requested to block the traffic of an attack.
- **A distributed defense framework for flooding-based DDoS attacks"[4]** where the detection system should be located close to the victim and detection is based on the traffic control method.
- **"A DDoS-oriented distributed defense framework based on edge router feedbacks in autonomous systems**" **[5]** the attack is defended on the traffic in the boundary of AS near to the attacking sources by measuring its ingress traffic rate which has the limits to the boundary of an autonomous system.

III. PROPOSED SYSTEM MODEL

Collaborative System is a new collaborative system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source at the Internet service provider (ISP) level. Collaborative System relies on a distributed architecture composed of multiple IPSs forming networks of protection rings around subscribed customers. Collaborative System is designed in a way that makes it a service to which customers can subscribe. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging belief scores on potential attacks. The IPSs form virtual protection rings around the host they protect. The virtual rings use horizontal communication when the degree of a potential attack is high.

A. Ring-Based Overlay Protection

The Collaborative System (Fig. 1) maintains virtual rings or shields of protection around registered customers. A ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer. As shown in Fig. 1, each Collaborative System IPS analyzes aggregated traffic within a configurable detection window. The metrics manager computes the frequencies and the entropies of each rule. A rule describes a specific traffic, which can be based on IP addresses or ports. Following each detection window, the selection manager measures the deviation of the current traffic profile from the stored ones, selects out of profile rules, then forwards them to the score manager.

Using a decision table, the score manager assigns a score to each selected rule based on the frequencies, the entropies, and the scores received from upstream IPSs (vertical collaboration/communication). Using a threshold, a quite low score is marked as a low potential attack and is communicated to the downstream IPS that will use to compute its own score. A quite high score on the other hand is marked as high potential attack and triggers ring-level (horizontal) communication. However, since the entire traffic cannot be possibly monitored, we promote the usage of multiple levels and collaborative filtering described previously for an efficient

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

selection of rules, and so traffic, along the process. In brief, to save resources, the collaboration manager is only invoked for the few selected candidate rules based on resource-friendly metrics.

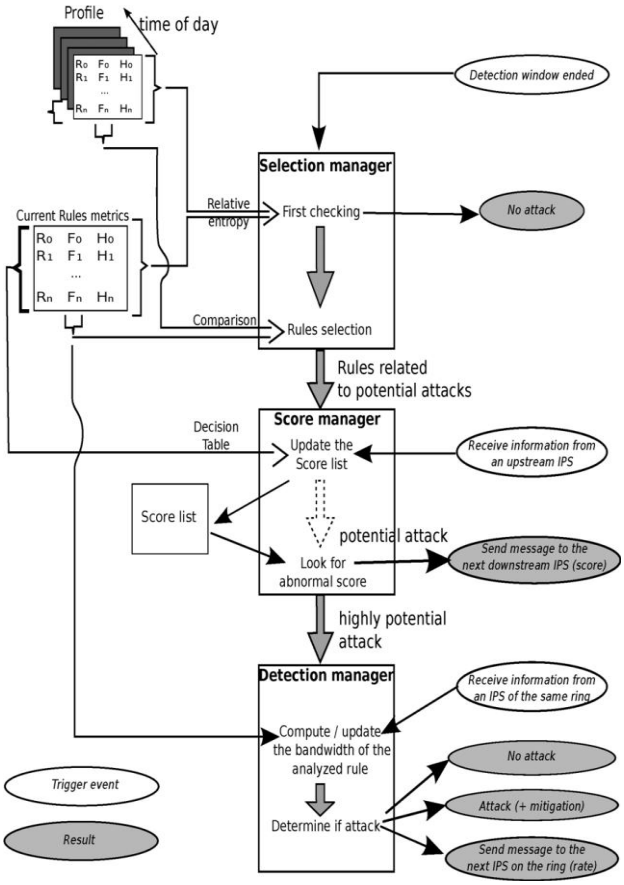

Fig1: Collaborative System Architecture

B. Subscription Protocol

Collaborative System protects subscribers based on defined rules. A Collaborative System rule matches a pattern of IP packets. Generally, this corresponds to an IP subnetwork or a single IP address. However, the rule definition can include any other monitorable information that can be monitored, such as the protocols or the ports used. Collaborative System is an added value service to which customers subscribe using the protocol shown in Fig. 2. The protocol uses a trusted server of the ISP that issues tokens. When a customer subscribes for protection service, the trusted server adds an entry with the subscribing rule along with its subscription period (TTL) and the supported capacity. The server then issues periodically a corresponding token to the customer with a TTL and a unique ID signed using its private key.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

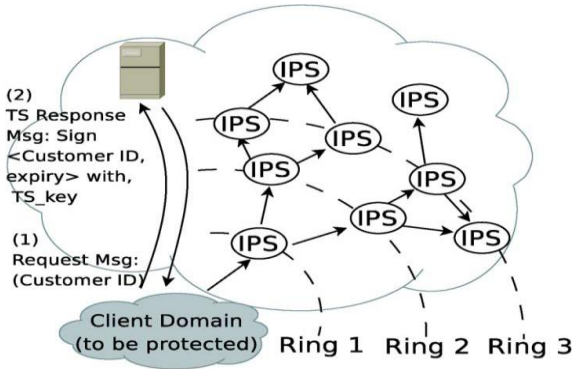

Fig 2: ColSys subscription protocol

All communications between subscribers and the server are secured using private/public key encryption scheme. The ring level of a Collaborative System enabled router (IPS) is regularly updated based on the degree of stability of IP routing. This is done using a two phase process. First, the router sends a message RMsg to the protected customer containing a counter initialized to 0. The counter is incremented each time it passes through a Collaborative System -enabled router. The customer then replies to the initiating router with the value of its ring level. This procedure is optimized through aggregation when several routers are requesting a ring-level update. The ring level value is network-dependent.

C. Multiple Customers

Because of their inherent complete independence, Collaborative System allows the coexistence of multiple virtual protection rings for multiple customers across the same set of IPSs. Therefore, a single IPS may act at different levels with respect the customers it protects as depicted in Fig. 3. Although most of the figures in this paper represent overlay networks with a single route, from an ISP to a customer, this figure highlights that alternative paths are possible.

IV. SOFTWARE IMPLEMENTATION OF THE PROPOSED SYSTEM

4.1.1. Metrics

With set of rules, Collaborative System maintains the following frequency and entropy-based metrics.

1) Frequency: The frequency fi is the proportion of packets matching rule ri within a detection window.

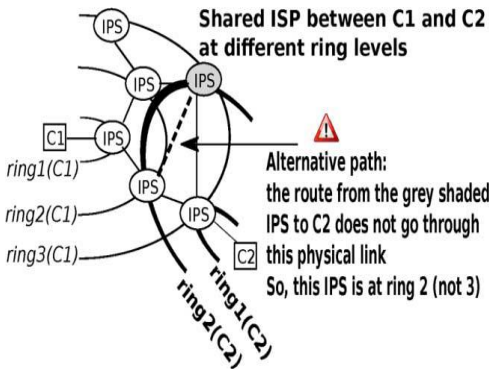

Fig 3: Collaborative System with two customers C1 & C2

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

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

Where fi is the number of packets matched by rule during the detection window. Every customer rule set R={ri| I ε[0,n] is complete, in the sense that every packet must match at least one rule. This is ensured by always having a default rule matching all traffic not covered by the supplied rules. The frequency distribution is then defined as f={ f1----------fn}

2) Entropy: The entropy H measures the uniformity of distribution of rule and frequencies. If all frequencies are equal the entropy is maximum and if frequencies are not equal, lower the entropy.

$$H = -E[\log_n f_i] = -\sum_{i=1}^{n} f_i \log_n(f_i).$$

3) Relative Entropy: The relative entropy metric k (f, f') measures the dissimilarity between two distributions (f and f'). If the distributions are equivalent, the relative entropy is zero, and the more deviant the distribution, entropy becomes higher.

$$\psi_i = \log \frac{f_i}{f_i'}$$
$$K(f, f') = \sum_{i=1}^{n} f_i \ \psi_i.$$

4.1.2. Components

The Collaborative System is composed of several collaborating IPSs each enriched with following components.

1) Packet Processor: The packet processor examines traffic and updates counters whenever a rule is matched.

2) Metrics Manager: The metrics manager computes entropies and relative entropies.

3) Selection Manager: The detection window (Fig.1) is processed by the selection manager, which checks whether the traffic during the elapsed detection window is within profile. It does so by checking whether the traffic distribution represented by frequencies follows the profile. This corresponds to check if, where the current distribution of frequencies is, is the stored distribution of the traffic profile, and the maximum admitted deviation from it. If the traffic is marked as abnormal requires further investigation. If there is a flooding DDoS attack, the traffic volume increases and so does the frequency of the traffic profile is based on a weighted moving average some rules.

$$\frac{f_i}{f_i'} > 1 + \gamma, \qquad 0 \le \gamma \le 1$$
$$f_i(t) > \epsilon.$$

fi is updated as follows

$$f_i' \leftarrow a \times f_i + f_i' \times (1 - a).$$

Here α is fixed to 0.5 to give an equivalent weight to the current and past traffic activities.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

4) Score Manager: The score manager assigns a score to each of the selected rules depending on their frequencies and the entropy. The entropy and the frequency are considered high if they are respectively greater than a threshold α and β.

Table below shows different cases

Case	Entropy	Frequency	Conclusion	Score
1	High(>α)	High (>β)	Potential	b1
2	Low (<_α)	High (>β)	Medium threat	b2
3	High (>α)	Low(<_β)	Potential later	b3
4	Low(<_α)	Low (<_β)	No threat	b4=0

1) High entropy and High rule frequency: In this case, the traffic is well distributed, meaning that most rules have the same frequency. Hence, having one rule that is quite different from the others is a good sign that it is a potential attack.

2) Low entropy and High rule frequency*:* In this case, the attack is only potential, but not as much as when the entropy is high.

3) High entropy and Low rule frequency*:* This case represents a potential threat. Here, all frequencies are about the same, making it not a threat as the frequency is low. However,

since it is increasing and deviates from the profile it may surpass other frequencies later on in time.

4) Low entropy and Low rule frequency: This case includes both high and low frequencies because of the low entropy. Thus, it is not possible to conclude about any threat.

Each of the above cases is associated with a score factor bj indicating the aggressiveness of the attack where b1>b2>b3>b4 (Table I).

The score Si of rule i is then obtained as follows:

$$S_i = f_i \times b_j.$$

the rules, which the score is lower than a small threshold , are automatically discarded as they no longer represent potential attacks. If the rule score is greater than parameter τ>>v, the attack is considered highly potential, and this alert is forwarded to the collaboration manager for aggressiveness checks. This process of vertical communication is illustrated in Fig. 3.

Finally, scores are also affected by an aging factor as follows:

$$S_i\{t+1\} = \lambda_{\text{age}} \times S_i\{t\}.$$

From a practical point of view, scores sent by the same IPS to the same downstream IPS are combined in one message to reduce the overhead.

5) Collaboration Manager: The collaboration manager is the last component in charge of confirming potential attacks. We claim that detecting a flooding attack can be confirmed only if the traffic it generates is higher than the customer's capacity. Hence, the IPS where the alert is triggered has to initiate a ring level communication to calculate the average traffic throughput for subsequent comparison with the subscribers capacity.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

V. EXPERIMENTAL SETUP & RESULTS

Above model can be implemented by using jdk 1.5/1.6 and above versions, client, server, IPS (routers) can be monitored using netbeans 7.2.1 development tool. Performance can be measured using maps.

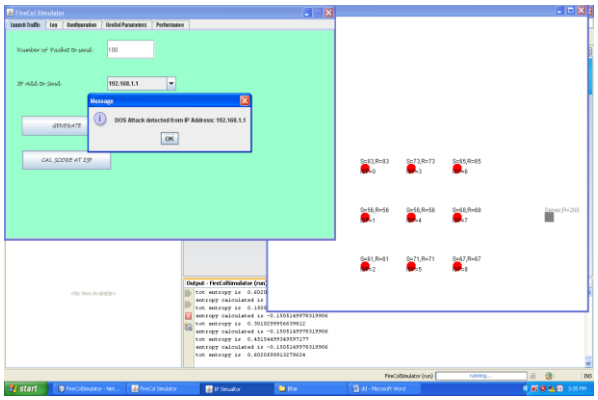

Fig 4: Attack Detected

VI. CONCLUSION & FUTURE ENHANCEMENT

This paper proposed Collaborative System, is a scalable solution for the early detection of flooding DDoS attacks. Belief scores are shared within a ring-based overlay network of IPSs. It is performed as close to attack sources as possible, providing a protection to subscribed customers and saving valuable network resources. Being offered as an added value service to customers, the accounting for Collaborative System is therefore facilitated, which represents a good incentive for its deployment by ISPs. As a future work, we plan to extend Collaborative System to support different IPS rule structures also the system can be implemented to wireless networks.

REFERENCES

[1] S. M. Bellovin, "Distributed firewalls," *Login Mag.*, vol. 24, no. 5, pp. 37–39, Nov. 1999.

[2] S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith, "Implementing a distributed firewall," in *Proc. 7th ACM CCS*, 2000, pp.190–199, ACM Press.

[3] R. N. Smith and S. Bhattacharya, "A protocol and simulation for distributed communicating firewalls," in *Proc. COMPSAC*, 1999, pp.74–79.

[4] Y. You, M. Zulkernine, and A. Haque, "A distributed defense framework for flooding-based DDoS attacks," in *Proc. 3rd ARES*,Mar. 2008,pp. 245–252.

[5] X. Bi, W. Tan, and R. Xiao, "A DDoS-oriented distributed defense framework based on edge router feedbacks in autonomous systems," inOct. 2008, pp. 132–135.

[6] S. H. Khor and A. Nakao, "Overfort: Combating DDoS with peer-to peer DDoS puzzle," in *Proc. IEEE IPDPS*, Apr. 2008, pp. 1–8.

[7] www.wikipedia.com