ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Detection of DDoS Attack Using Virtual Security

N.Hanusuyakrish, D.Kapil, P.Manimekala, M.Prakash

Abstract*— Distributed Denial-of-Service attack (DDoS attack) is a machine which makes the network resource unavailable to its intended users. DoS attack consists of the efforts of one or more people to interrupt or suspend the service of a host connected to the Internet. The discovery of this attack is necessary to protect the network infrastructure but it is very challenging to detect such attack. In this paper we discuss the architecture, algorithm of FireCol where the core of FireCol is located at the internet Service Provider level (ISP_s) which consist of Intrusion Prevention System (IPS).The IPS_s forms a virtual protection ring around the host and exchange the traffic information. With that information the IPS came to know the detection of DDoS attack.

***Index Terms* — Denial-of-Service Attack, Intrusion Prevention System, Internet Service Provider**

I. INTRODUCTION

Distributed Denial of Service attacks do not depend on particular network resources. It consists of compromised host which will send the useless packets to the victim to make them unavailable to the network resources. This become a major threat due to availability of a number of user-friendly attack tools [9] on one hand and lack of effective solutions to defend against them on the other. Most recent work is use of botnets [3] which is a large network controlled by one entity that is it work in the concept of Master-Slave. The master can launch the synchronized attack by sending the orders to the bots by using a command. When there is a lack of security in the Master-Slave then that is said to be botnet based attack.DDos attacks are mainly used for flooding the attack over victim and it is very popular because of its efficiency where it can attack any kind of service.DoS attacks typically target sites or services hosted on web servers such as banks, credit card payment gateways.

II. SINGLE INTRUSION SYSTEM

A single intrusion system such as Intrusion Prevention System (IPS) or intrusion detection system is used to detect the DDos attack. These are network security appliances [5] that monitor network and system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. The communication using single intrusion system is shown in the fig.1. Where the detection of DDoS attack is possible only when the IPS is close to the victim. These intrusion prevention system or intrusion detection system is located in the internet service provider (ISP) [1] which is used to control the malicious activity. In Fig. 1.In this IPS is implemented in-line where AN ID is off-line. The traffic is directed through IPS which can block the attack and allow the data packet to reach the server. In a denial of service attack IPS can be a easier target than the server which is a challenging task for the Intrusion Prevention System. The IPS block the attack in action and stops the malware connecting to a command which make the data to be loss.

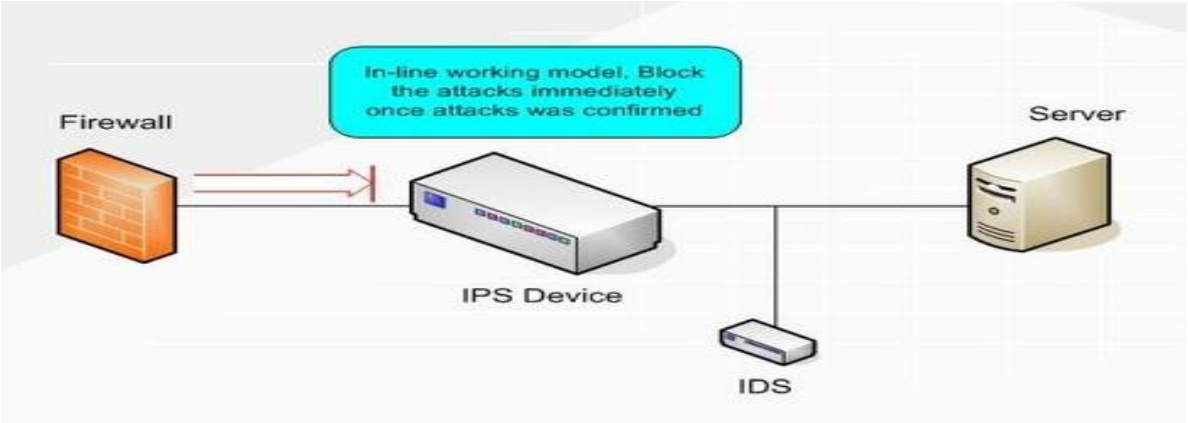


Fig .1.Single IPS System

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

A. Advantage of single system

An IPS (Intrusion Prevention System) is any device, hardware or software that is used to detect the attack. It is a firewall which can detect the irregular routine of network traffic and then stop the malicious activity. There are many reasons why we are using an IPS is the design that gives an extra protection from denial-of-service attack and also gives protection from many critical exposures found in software such as Microsoft Windows[12].

B. Disadvantage of single system

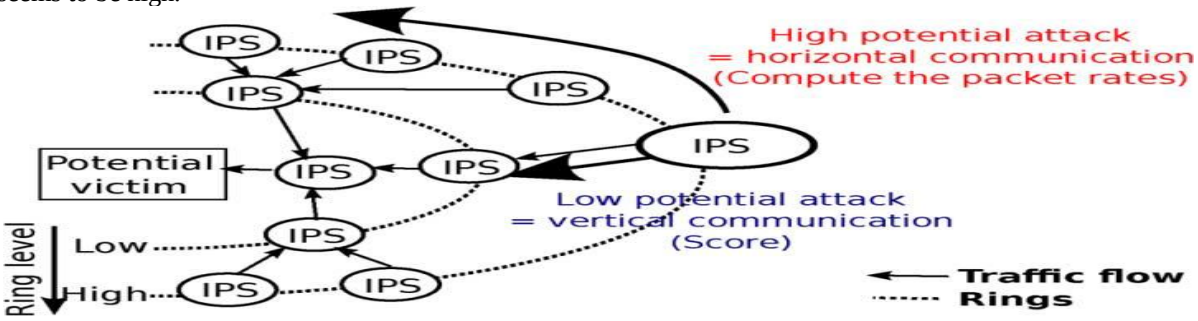
This single IPS or IDS detect DDoS attack only when they are located close to the victim. These IPS/IDS can get crash and made the internet [8] resources to be strain when it deals with the overwhelming volume of packets. The main problem with current intrusion detection systems is high rate of false alarms. The design and implementation of a load balancing between the traffic coming from clients and the traffic originated from the attackers is not implemented.

III. FIRECOL COLLABORATIVE SYSTEM

The intrusion prevention system forms a virtual protection ring around the host to detect the attack and also to monitor the traffic where the FireCol is composed of intrusion prevention system located at the internet service provider level. This collaborative system detect the DDoS [2] attack as possible from the victim host and as close as possible to the attack source at the ISP level.

A. Architecture

This composed of multiple IPS_s forming overlay networks of protection rings around subscribed customer. The virtual ring which is formed around the host by the IPS_s use horizontal communication when the potential attack is seems to be high.



.

Fig. 2. Multiple IPS Systems

When the potential attack is seems to be low it uses a vertical communication [11] around the host by the IPS_s.These horizontal and vertical communication is showed in the Fig. 2.When there is a horizontal communication the attack is dismissed based on the actual packet rate and the customer capacity is evaluated. FireCol allows the multiple virtual protection rings for multiple customers across the same set of IPS_s.The following Fig. 3. Highlights that alternative paths are possible which represent the overlay networks with a single route from an ISP to a customer.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

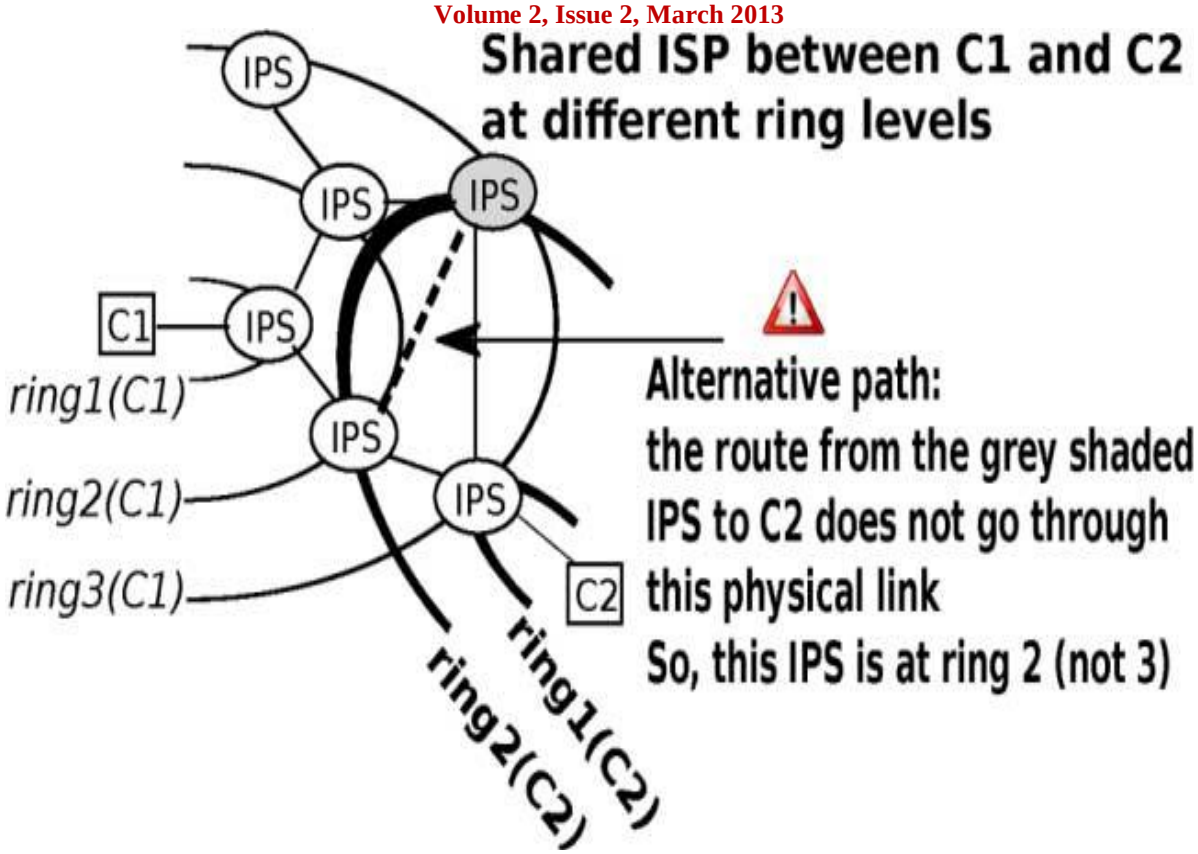


Fig. 3. Multiple Customer in Colloborative System

B. Components of Firecol

It consists of several components as shown below, each work collaboratively to detect the attack and it is shown in Fig.4.

Packet Processor-When a rule is matched it is to examine the traffic[9] and update the traffic information in the detection window.

Metrics Manager-It computes the frequency and entropy with the specified rule as follows,

Frequency- The frequency fi is the proportion of packets matching rule ri within a detection window

$$fi = Fi/\sum nj=1Fj \quad (1)$$

Entropy- The entropy H[2] measures the uniformity of distribution of rule frequencies.

$$H=-E[\log_n f_i] = -\sum_{i=1}^{n} f_i \log_n (f_i) \quad (2)$$

From the equation (1) and (2) we can compute the frequency and entropy value.

Selection Manager-Traffic can be calculated during elapsed time based on traffic profile.

Score Manager-It assigns the score to each rule depending on their frequencies and the entropies.

High entropy and High rule frequency-It is to detect the attack by using the traffic and setting the rule for each one by using the high frequency and high entropy.

Low entropy and High rule frequency-It uses the high frequency which represents the direct threats with low entropy.

High entropy and Low rule frequency-It represents the potential threats by using the low frequency value.

Low entropy and Low rule frequency-This includes both high and low frequencies because of the low entropy.

Collaboration Manager-It will confirm the potential attack when the customer capacity is higher than the current traffic.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

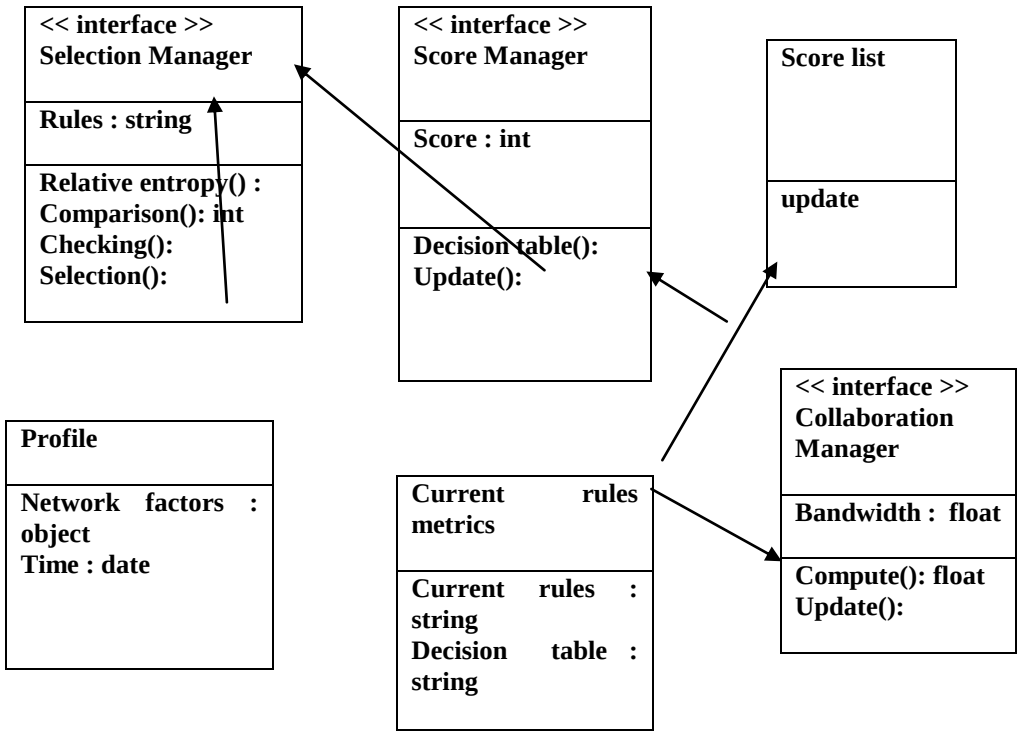


Fig. 4.Collaborating Interface Diagram

This interface diagram shows how the components of the FireCol works with different class and objects that make the system to function properly. In this Selection Manager will get the details of the current rule from the decision table and also the network profile, from this it will calculate the relative entropy and make the comparison between the previous entropy and select the current traffic. The Score Manager will get the updating of each score and the current rules, with that it will assign the score to each traffic in the decision table. The collaboration Manager computes the bandwidth and updates the information from which detection can be confirmed by knowing the details of the current rule traffic.

C. Firecol detection system

FireCol detection is manage by the collaboration manager where an IPS receives a request to calculate the aggregate packet rate for a given rule and checks whether it is an initiator and if it so it first shows that the request has already made the round of the ring and hence there is no potential attack [10].Otherwise, it calculates the new rate by adding in its own rate to check that the maximum capacity is reached, and if so the alert is raised. Further the investigation is proceeding to next horizontal IPS ring. Here describes two ways of protection method where Bytes based method is better for detecting flooding attacks with large packets. FireCol customers can subscribe to both protection types.

D. Firecol mitigation

When an attack is detected, FireCol rings form protection shields around the victim. In order to block the attack as close as possible to its source, the IPS that detects the attack informs its upper-ring IPS which in turn apply the vertical communication and enforce protection at their ring level. The mitigation [4] can also be extended by forwarding the information as by the collaborative [5] manager.

E. Advantage of Collaborative Systems

It is used to detect the DDoS attack even when it is far to the victim host this is the major advantage of this system. Experiments showed good performance and robustness of *FireCol* and highlighted good practices for its configuration.

IV. CONCLUSION

As a result this collaborative system is more efficient to detect the Distributed Denial of Service attack compared to single intrusion system. Experiments showed good performance and providing a protection to subscribed customers providing valuable network resources.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

REFERENCES

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

[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.

[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] V. Paxson, "End-to-end routing behavior in the Internet," IEEE/ACM Trans. Netw., vol. 5, no. 5, pp. 601–615, Oct. 1997.

[9] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1241–1252, Dec. 2008.

[10] Z. Zhang, M. Zhang, A. Greenberg, Y. C. Hu, R. Mahajan, and B. Christian, "Optimizing cost and performance in online service provider networks," in Proc. USENIX NSDI, 2010, p. 3.

[11] M. Dischinger, A. Mislove, A. Haeberlen, and K. P. Gummadi, "Detecting bit torrent blocking," in Proc. ACM SIGCOMM Conf. Internet Meas., 2008, pp. 3–8.

[12] G. Shafer, "A Mathematical Theory of Evidence". Princeton, NJ: Princeton Univ. Press, 1976.