FireCol: A Collaborative Protection Network for the Detection of Flooding DDOS Attack

Ketki Nanadikar
Computer Department
P.E.S's Modern College
Engineering Pune,
University Of Pune, India

Aishwarya Kachi
Computer Department
P.E.S's Modern College
Of Engineering, Pune,
University Of Pune, India

Apoorva Karkhanis
Computer Department
P.E.S's Modern College
Of Engineering, Pune,
University Of Pune, India

Shweta Patole
Computer Department
P.E.S's Modern College Of
Of Engineering, Pune,
University Of Pune, India

Abstract- Distributed denial-of-service (DDoS) attacks are a major threat to security issues. The control and resolving of DDoS attacks is difficult in a distributed network. The primary problem till date is the attacks are detected close to the victim and hence cannot be resolved. It is essential to detect them early in order to protect vulnerable resources or potential victims. FireCol comprises multiple intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. These multiple Intrusion Prevention Systems (IPSs) act as traffic filters. Based on threshold values it passes information. The efficient system of FireCol is demonstrated as a scalable system with low overhead.

Keywords-FireCol; IPS; DDoS; IDS; URL;

I. Introduction

DDoS attacks are still a major concern. Flooding DDoS attacks are popular because they are high effective against any kind of service as there is no need to identify and exploit any particular service-specific flaw in the victim. That is why these attacks are used. A single intrusion prevention system (IPS) or intrusion detection system (IDS) cannot detect such DDoS attacks efficiently. They should be located very close to the victim for detection which is not possible all the time. FireCol system is developed using IPSs located at internet service provider level. The IPSs form virtual protection rings around the hosts. These rings help to defend attacks. FireCol systems goal is to protect users from attacks.

II. IMPLEMENTATION

A. System Modules

The FireCol system is developed using java programming language and MySQL database. In FireCol system we have two user access, one for Normal User and another is Admin i.e. FireCol System itself. Admin of the system will be able to access database and database will be stored only on one node.

Clients (i.e. Normal User) can only install system and take the benefits of the system. Client can't access database.

1) Admin:

Admin is the one who handles the systems features and services. He can add or remove Resources i.e. URLs. He maps specific resource to particular user. He can deny access of particular site to user. He hits the URLs and checks whether they are DDoS affected services. According to result he activates or deactivates the URL for user.

2) Normal User:

Normal user is the subscribed user to FireCol system. When user gets logged in to the system, he can hit URLs he wanted. If they are DDoS affected he won't be able to access as admin has deactivated them for users. If they are normal pages, web pages will get open and he can use them.

B. Algorithm:

In FireCol system, we have used the following technique or algorithm to find out whether it is a DDoS attack or not.

- Request resource
- Record request time in Millis
- Hit resource with input URL
- Open resource in browser
- Get response code
- Get response status
- Then get resource data stream
- Calculate content size(bytes/characters)
- Calculate packets being received
- Capture time after getting response
- Calculate total time taken to serve request
- Retrieve stored resource details(min response time, average response time, max Response time, expected # of packets etc)
- If status code =500

  Then resource is down

  Else If status code =200

  If total time> average response time for resource and packets received>expected # of Packets for resource

  Then request not completed successfully and DDoS attack detected

  Else If status code =400

Then resource not found

C. *Results Analysis*

FireCol system is developed and tested successfully. On the basis of that we are presenting some results in the form of graphs.

1) Effect of Time Interval on Response Time on DDoS affected pages:

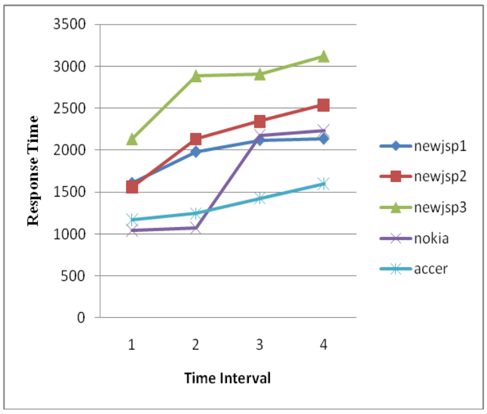

Fig. 1. Effect of Time Interval on Response Time

We have created 5 DDoS affected pages namely newjsp1, newjsp2, newjsp3, nokia, accer. In the above Fig.1, we have plotted a graph, time interval verses response time. From this graph we conclude that response time increases after specific time interval of 30sec.

2) Study of Content size verses Response time of Normal Pages:

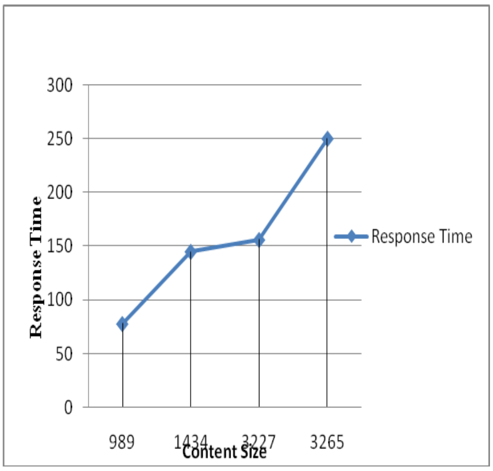

Fig. 2. Content size verses Response time

In Fig. 2, we have described graph of content size verses response time. The response time also varies according to the content size of the pages. As it is an increasing graph the content size too increases with an increasing response time. In the normal servlets also the response time varies according to the content size of page.

TABLE 1
Result Table of DDoS attack

	Response Time			
Resource ID	**RT1**	**RT2**	**RT3**	**RT4**
1	1607	1981	2122	2137
2	1560	2135	2345	2456
3	2137	2887	2983	3108
4	1045	1076	2169	2231
5	1030	1089	2100	2245
6	1170	1245	1351	1560
7	1139	1204	1467	1653
8	1279	1987	2103	2365
9	1030	1170	1345	1622
10	1298	1400	1571	1644

The table above depicts the values of the response time T1, T2, T3, T4 corresponding to the specific time interval with respect to the content size of the page. Response time increases after specific time interval of 30sec.

Thus from the above analysis we can conclude that,

- A DDoS attack being the execution of multiple threads, the response time increases which help us to detect DDoS attack.
- The response time increases as the content size of the servlet increases. The content size of the servlet varies with respect to data.

III. CONCLUSION

We have developed a system for detection of flooding DDoS attacks. FireCol provides the protection to the subscribed customers and saves the network resources. FireCol is robust, light weighted system. Internet users can easily get subscribed to system and take the benefits of system. In future we'll try to implement different IPS structures.

REFERENCES

[1] 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.

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

[4] N.Hanusuyakrish, D.Kapil, P.Manimekala, M.Prakash , "Detection of DDoS Attack Using Virtual Security",(IJESIT) Volume 2, Issue 2, March 2013

[5] Jérôme François, Issam Aib, *Member, IEEE*, and Raouf Boutaba, *Fellow, IEEE, "FireCol*: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks*"*, IEEE/ACM transactions on networking, vol. 20, no. 6, December 2012.

[6] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao,"Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", *Department of Computer Science and Software Engineering, The University of Melbourne, Australia*, ACMJ258-03, ACM-CSUR, March 21, 2007.