

Minimizing Application Layer DDOS Attacks Using Website Customization

¹P. Ram Mohan Rao, ²Dr. K. Venkateswara Reddy, ³S. V. Hemanth

^{1,3}Dept. of CSE, ACE Engineering College, Hyderabad, AP, India

²MLRITM Hyderabad, AP, India

Abstract

DDOS attacks are continuous and critical threat to Internet especially commercial websites. The Application Layer based attacks use genuine HTTP requests and creates devastating effect on the computing resources and in turn results into denial of service. An anomaly detector based on Hidden Markov Model (HMM) can be used to detect the attack. The model needs to be trained by using complex algorithms which may affect response time significantly. Some useful customizations during website design can minimize the application layer DDOS attacks.

Keywords

Distributed Denial of Service, HMM, Http Requests

I. Introduction

Distributed Denial of service attacks cause serious damage to web servers leading to unavailability of the services to legitimate users. Major victims of DDOS attacks are commercial web servers, banks and also government websites. DDOS attacks are even used by terrorists as a weapon to create data integrity and availability problems [1]. Application layer DDOS attacks are carried out using HTTP GET requests. MyDoom [2] is an example of such attack. SCO group a US based organization became victim of HTTP Flooding. Examples of Application layer DDOS attacks. (1) Pulling large image files from the server in large numbers to compromise the computing resources. (2). Making huge number of queries on the victim server to bring it down. (3). Writing worms which can self propagate and use them as part of HTTP GET request to bring the server down. (4). Sending an email to all contacts in the address book with an attachment which will obviously overload mail server and if it is done in large numbers then the email server will go down which is denial of service. (5). Sobig worm was a computer worm which affected millions of interconnected Microsoft windows computers. (6). Slowloris and Rudy are the recent attacks. 7. Worms can become dangerous types of Application layer DDOS attacks [3] because of their self propagating nature. In all these cases the attack is carried out by making typical requests which consume more and more computing resources of the web server leading to collapse of the server. Since the attack is carried with genuine credentials it becomes very difficult to differentiate attacker and legitimate user. Application layer DDOS attacks can be detected by studying the behavioral patterns of the users. An anomaly based detection principle called Hidden Markov Model [4-5] can be used to study the user's behavioral patterns. Application layer DDOS attacks are difficult to detect because the surge in the traffic can also be caused by simultaneous accesses. To detect the anomalies the HMM model has to be trained. To train the HMM model several algorithms are available. The objective of this paper is to identify an effective method which can detect and block the application layer DDOS attacks. To identify the attack we need to study the behavioral patterns of users and try to identify anomalies if any.

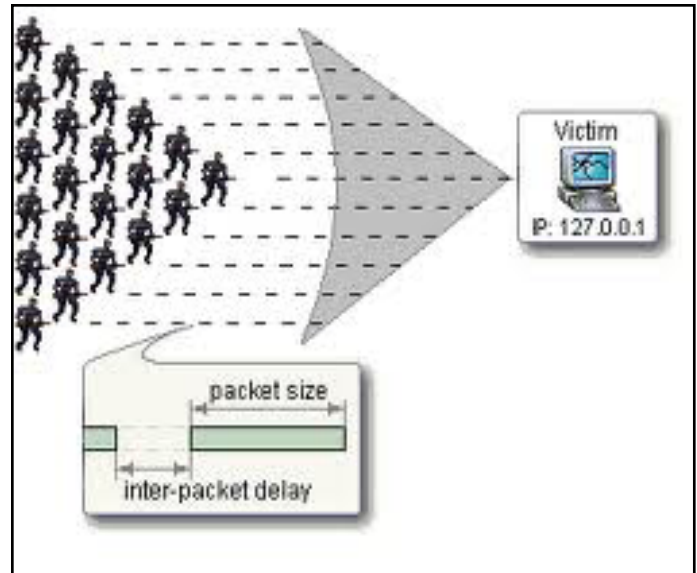


Fig. 1: Typical DDOS Attacks

II. Related Work

In order to develop an effective method to study behavioral patterns and to detect Application layer DDOS attacks, we have designed a website which is modeled as a Finite State Machine. We expect the user to navigate from one web page to other in a systematic manner. A static binary sequence is maintained for every user in the database. When user navigates a binary sequence will be generated dynamically which will be compared with the existing one. If the user attempts any attack then it will be a typical HTTP request which will differ from normal behavioral patterns. HMM is used to study the unobservable state. The probability of change in hidden state is based on the amount of time elapsed since entry into current state.

A. Session Management

Whenever a new user logs in, a session will be created. For every user a session id is maintained to keep track of the activities made by the user. For a legitimate user a binary sequence will be generated which is compared with the existing one. But when an attempt is made to attack the site i.e. by making some typical requests like pulling large images, bypassing the web pages, Flooding HTTP GET requests etc. an anomaly is observed because the sequence generated will not match with sequence which is predefined. In such cases the anomaly user can become a suspect and if it's repeated again we can block that user.

B. Training HMM

A HMM is a statistical Markov model in which the system being modeled is assumed to be a Markov Process with unobserved (hidden) states. In the Markov model state is not visible but the output dependent on the state is visible. Each state has a probability distribution over the possible output tokens. Therefore sequence of output tokens generated by HMM gives some information about sequence of states. To model a website as a FSM we should train

the HMM model. To train an HMM model we use an access matrix to capture temporal patterns.[6] For every request initial parameters are computed and access matrix is used to monitor navigation patterns which are recorded in the server. To train HMM model forward backward algorithm is used.

The forward-backward algorithm is an inference algorithm which computes the posterior marginal's of all hidden state variables given a sequence of observations/emissions $O_{1:t} := O_1, \dots, O_t$, i.e. it computes, for all hidden state variables $X_k \in \{X_1, \dots, X_t\}$ the distribution $P(X_k | o_{1:t})$.

This inference task is usually called smoothing. The algorithm makes use of the principle of dynamic programming to efficiently compute the values that are required to obtain the posterior marginal distributions in two passes. The first pass goes forward in time while the second goes backward in time. Hence the name forward-backward algorithm.

Whenever a user logs in forward backward algorithm generates a binary sequence. Since the website is modeled as FSM a standard sequence is assumed and any variation in dynamically generated sequence is treated as anomaly. When anomaly is observed the user can be blocked. This application will also generate a text file in hard drive which contains list of blocked IP addresses also the user will be navigated to error page as shown below.

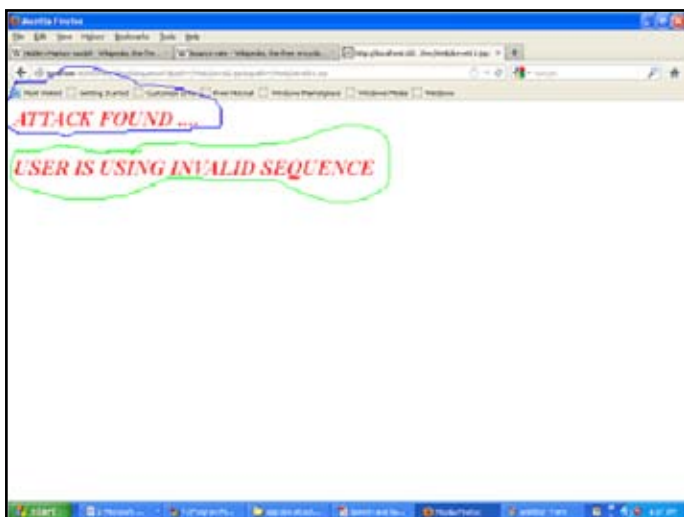


Fig. 2: Error Page When Attack is Found

Whenever an anomaly is detected and the user is blocked, all the parameters of that user are recorded in the server which can be seen in the below.

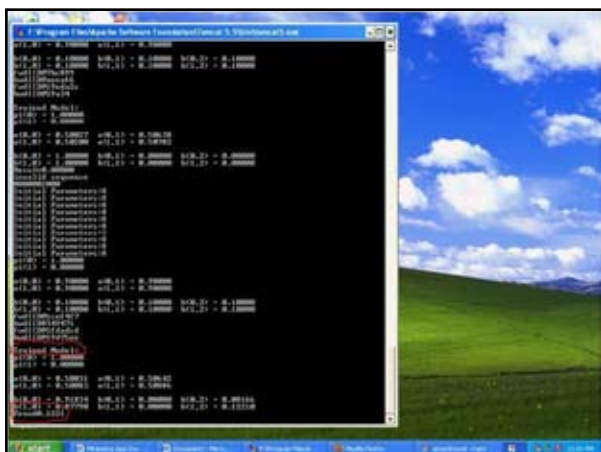


Fig. 3: Forward Backward Parameters of Attack Recorded at Tomcat Server

III. Observations

In this application some interesting observations were made. The most desirable feature in a web application is the response time. Normal response time of the web server before applying HMM algorithm and after applying HMM was studied. The response time of the application has increased considerably and will be even more when requests are made in large numbers. The graph below describes the difference in response time which was studied from web server's status log values. Therefore detecting Application Layer DDOS attacks using HMM will definitely increase the response time which is not at all desired. As part of our work we have observed that some of the application layer DDOS attacks can be avoided by customized web design, which is discussed in our next section.

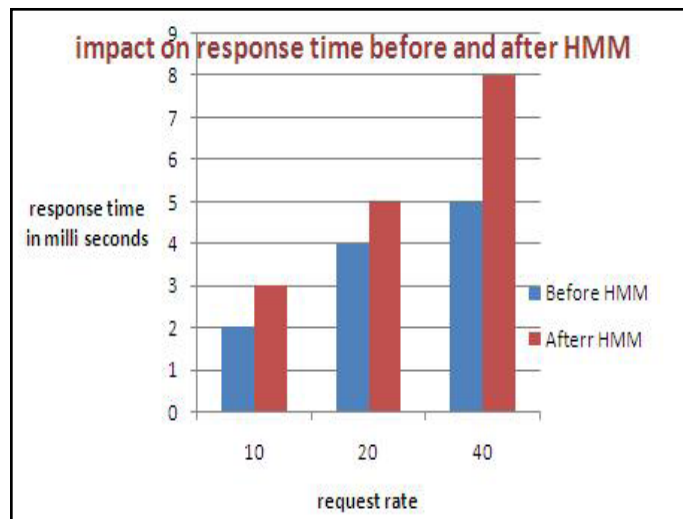


Fig. 4: Increase in Response Time After Applying HMM

IV. Analysis

Not all but many Application Layer DDOS attacks can be avoided by proper web site design. Generally Application layer DDOS attacks are carried out with genuine credentials and by using HTTP GET requests to make a typical request which consumes huge computing resources of the server. Some of the examples of Application Layer DDOS attacks which can be prevented by proper website design and customization.

1. For example pulling large images from a web site in large numbers will create overwhelming effect on computing resources of the web server. Generally it is done by right clicking mouse button and downloading image into local machine. This is one type of Application layer DDOS attack which can be simply avoided by disabling right click option in your web page. Simple script can serve the purpose there by successfully we can avoid one Application layer DDOS attack.
2. Application layer DDOS attacks are carried out from large number of nodes simultaneously i.e. in a distributed environment. Here the attacker makes HTTP GET requests to create surge in the traffic. The attacker may not have genuine credentials and may try to bypass the gate keeper mechanism of a website which can also be blocked by simple script at the client side.

```

If (((HttpServletRequest) request).getSession ( ).getAttribute
("user") == null) {
    //response.sendRedirect ("AfLogin.htm"); // Logged in, so
just continue.
} //else {

```

```
out.print ("u bypassed");
response.sendRedirect ("CustomerLogin.htm"); }
```

3. Application layer DDOS attacks are carried out generally by using compromised nodes referred as Zombies. A simple CAPTCHA can help us in identifying compromised hosts and thus blocking that particular node. Even this can also be done using simple script. This will also help us in preventing few Application Layer DDOS attacks. But CAPTCHA will also incur some cost in terms of response time.

4. Bounce rate: When a user leaves the web page without visiting any other pages then it is referred as bounce. Bounce rate is used in web traffic analysis.

$$B = \left(\frac{T_v}{T_e} \right)$$

B=Bounce rate

T_v = Total number of visitors viewing one page only.

T_e = Total entries to page

Bounce rate is also an important factor in predicting the anomalies and detecting Application layer DDOS attacks. Generally a legitimate user will not visit a single page whereas an attacker may visit a particular page to make a typical request which may lead to anomaly. For example the attack can be carried out like this. The attacker will select several nodes to perform the attack from a distributed environment. The attacker may pull large image files from one node, attacker may try to make typical request which consume lot of computing resources etc.... So the attacker may not visit all pages. Therefore when an Application Layer DDOS attack is made then definitely there would be significant difference in the bounce rate. Hence Bounce rate can also be used as a method of detecting anomalies. Major difference in Bounce rate can be a matter of concern, so bounce rate should also be monitored continuously which can help in predicting anomalies.

V. Conclusion

We have applied HMM model to monitor Application Layer DDOS attacks on web servers. By applying forward backward algorithm to train HMM model, it has increased the response time of the application. As part of our work we have noticed that little customization of web site design can help in minimizing Application layer DDOS attacks which we have presented in this paper in our observations. Application Layer level DDOS are not limited. New types of Attacks are being carried out, so it became area of continuous research. Application layer level DDOS attacks are now used by terrorists to seize confidential information and also to collapse various government websites. Many countries became victims of such attacks.

Generally Application layer DDOS attacks are similar to Flash Crowd event [7] which is a normal situation when huge number of legitimate users tries to access the server and in turn server goes down. This makes detecting Application layer DDOS attacks more and more difficult. As part of our work we think minimizing Application layer DDOS attacks is very important which can be done by proper website design and ensuring performance or response time of the application is an area of research. Our motto is to develop counter solutions to various upcoming Application layer DDOS attacks.

VI. Acknowledgement

The authors would like to thank Mr. G.Kiran Kumar, Professor and Head, Department of Computer Science, MLR Institute of

Technology, Hyderabad and Mr. Vinod, Associate Professor, ACE Engineering College, Hyderabad for their comments and useful suggestions.

References

- [1] K. Poulsen, "FBI Busts Alleged DDOS Mafia", [Online] Available: <http://www.securityfocus.com/news/9411>
- [2] "Incident Note IN-2004-01 W32/Novarg. A Virus," CERT, 2004, [Online] Available: http://www.cert.org/incident_notes/IN_2004_01.html
- [3] Christous Douligeris, Aikaterini, Mitrokotsa, "DDOS Attacks and Defense Mechanisms: A Classification".
- [4] Y. Xie, S. Yu, "A detection approach of user behaviors based on HsMM", in Proc. 19th Int. Teletraffic Congress ITC19), Beijing, China, Aug. 29-Sep. 2 2005.
- [5] Y. Xie, S. Yu, "A novel model for detecting Application Layer DDoS attacks", in Proc. 1st IEEE Int. Multi-Symp. Comput. Computat. Sci. (IMSCCS|06), Hangzhou, China, Jun. 20-24, 2006, Vol. 2, pp. 56-63.
- [6] Yi Xie, Shun-Zheng Yu, "Monitoring Application Layer DDOS Attacks on Popular Websites", IEEE transactions on networking. Feb 2009.
- [7] J. Jung, B. Krishnamurthy, M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites", in Proc. 11th IEEE, Int. World Wide Web Conf. May 2002.



The author is doing his research in web security, HMM models, Application layer security services, cloud security, web mining. He has done his Master's degree in computer science engineering from Department of Computer Science, JNTU Hyderabad. Currently he is working as Assistant Professor in Department of Computer Science, ACE Engineering College, Ghatkesar, Hyderabad.



Dr K Venkateswara Reddy is principal of MLRITM, Hyderabad, received his M.Tech and PhD from JNTU and Osmania University. He checquered a dynamic career in reputed engineering colleges as a professor, Head and Vice-principal and is found to be disciplinary and dynamic personality in academic and administrative spheres. He bagged several national and international journals to his credit in 20 years length of his service. He is life member of ISTE. Presently he is working in Cloud computing, Network security, MANET and other emerging fields of computer science.



S.V.Hemanth is a faculty of ACE Engineering College working Asst Prof from Dept of CSE. He has done his Master's from JNTU Hyderabad and his Research areas include Data Mining, Information Security, Cloud Computing, Cloud security, HMM models. He has published two international journals on information security.