ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Enhanced DDoS Attack Prevention Method Using Temporal and Spatial Locality

[I]Sujina mol M , [II]Aneesh M Hanee
[I]Student (MTech, CSE), [II]Assistant Professor (CSE)

Abstract
Activities such as telecommunication, on-line banking and on-line shopping have recently are being integrated through the internet. In such a situation security is an important criteria. The attacks which are commonly occurring are: Eavesdropping, Data Modification, Denial-of-Service Attack, Man-in-the-Middle Attack. Distributed Denial of Service (DDoS) attacks has been a continuous critical threat to the Internet since 10 years ago. A lot of researches are being conducted to detect DDoS attack. Some such innovations are analysed here. The methods are: Web proxy's behavior, User browsing behaviors, Trust Management Helmet (TMH), Sequence-order-independent network profiling, Flow correlation coefficient, Information metrics, Temporal and spatial locality behavior. Here a mechanism is developed in order to protect the origin server from the Web proxy based HTTP attacks. In implementation stage the attack traffic is assumed to begin from Web proxies instead of its real sources. The victim can only observe the proxies and the goal is to filter malicious traffic instead of trace back. In order to overcome the drawback of false negative ratio an improvement is done in implementation stage.

Keywords
Web proxy; Trust Management Helmet (TMH); sequence-order-independent; flow correlation coefficient; temporal locality; spatial locality; soft control

I. Introduction

Many methods designed to create defences against distributed denial of service (DDoS) attacks are focused on different layers of a network model. The importance of developing detection mechanism is because of complex business applications that are now delivered over the web (HTTP). Distributed Denial of Service attack has caused severe damage to servers and will cause even greater intimidation to the development of new internet services. The intent of these attacks is to consume the network bandwidth and deny service to legitimate users of the victim systems. The methods for attack detection depend on correlation coefficient, trust spatial locality, temporal locality, etc. DoS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to its customers. DoS: when a single host attacks. DDoS: when multiple hosts attack simultaneously

II. Literature Survey

Researches are always being conducted to detect and remove DDoS attacks. Some of the innovative approaches to attack detection are:

A. Measuring the Normality of Web Proxies Behavior Based on Locality Principles

It is a server-side detection scheme based on the behavior characteristics of proxy-to-server Web traffic [1]. Proxy's access behavior is extracted from the temporal locality and the bytes of the requested objects. A stochastic process based on Gaussian mixtures hidden Semi-Markov model is applied to describe the dynamic variability of the observed variables. The entropies of those pending Web traffics launched by proxies fitting to the model are used as the criterion for attack detection. Stack distance model is utilized to capture the temporal locality relationships. By using this technique it is practical in monitoring the attacks hidden in the proxy-to server traffic.

B. A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors

The main aim of this method is detection and filtering for DDoS attack by using HsMM and entropy of user's HTTP requests [2]. This kind of detection mechanism is mainly intended for application layer based DDoS attack.

C. A Lightweight Mechanism to Mitigate Application Layer DDoS Attacks

Trust Management Helmet (TMH)[3], a lightweight mitigation mechanism that uses trust to differentiate legitimate users and attackers. Its key insight is that a server should give priority to protecting the connectivity of good users during application layer DDoS attacks, instead of identifying all the attack requests.

D. Sequence-Order-Independent Network Profiling for Detecting Application Layer DDos Attacks

With the profiling of web browsing behavior, the sequence order of web page requests can be used for detecting the application-layer DDoS (App-DDoS) attacks. However, the sequence order may be more harmful than helpful in the profiling of web browsing behaviors because it varies significantly for different individuals and different browsing behaviors. A sequence-order-independent method [4] for the profiling of network traffic and the detection of a new type of App-DDoS attacks. In this case four attributes are extracted from web page request sequences without consideration of the sequence order of requested pages. A model based on the multiple principal component analysis is proposed for the profiling of normal web browsing behaviors, and its reconstruction error is used as a criterion for detecting DDoS attacks.

E. Discriminating DDos Attacks from Flash Crowds Using Flow Correlation Coefficient

Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient [5] is another technique for finding DDoS attack. It uses the concept of botnets, which are the engines behind the attack.

F. Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics

Another method which is focused on DDoS attack in network layer is, Low-Rate DDoS Attacks Detection and Trace back by Using New Information Metrics [10]. In his case detect attacks earlier by using the detection approach because traffic can be analysed in upper stream routers instead of just in the victim's router. IP trace back scheme trace all attacks in a short time.

G. Resisting Web Proxy-Based HTTP Attacks by Temporal and Spatial Locality Behavior

A server-side defence scheme that is proposed to resist the Web proxy-based distributed denial of service attack based on Spatial and temporal locality behavior [7] is another technique. In this method attack traffic is assumed to begin from proxies. Thus the victim observes the proxies and filter malicious traffic instead of trace back. In order to detect attack web proxy's access behavior is used. Proxy's access behavior can be represented as the combination of external manifestation and intrinsic driving mechanism. External manifestation means Temporal and Spatial Locality (TSL) and Intrinsic driving mechanism is the normality or abnormality. Proxy's access behavior is mapped to HsMM. Hidden Semi Markov state represent driving mechanism of traffic. Resisting proxy based attack is equivalent to searching abnormality state and filtering those suspicious requests caused by abnormality state. Here the temporal locality and spatial locality is determined by using stack distance model and joint entropy. Data extraction, training and detection and control are the major phases in this model. The main advantage is that it converts the suspicious traffic into normal one.

III. Comparison of various DDoS attack detection scheme

Parameters			
Method	Layer	Remarks	Objective
Web proxy's behavior	Application	Temporal locality & bytes of requested objects	Detection & drop
User browsing behavior	Application	Entropy	Detection & drop
Trust Management Helmet	Application	TMH	Protect legitimate users, detect session flooding attacks
Sequence-oreder-independent network profiling	Application	Attribute of web page request	Detection & drop
Flow correlation coefficient	Network	Size of botnets & correlation coefficient	Distinguish DDoS attack from flash crowds
Information matrics	Network	IP trace back analysis	Detection and source identification
Temporal and spatial locality behavior	Network	Temporal & spatial locality	Detection & drop

IV. Temporal and spatial locality behaviour

The primary aim of the proposed scheme is to protect the origin server from the Web proxy-based HTTP attacks. To simplify the problem, attack traffic is assumed to begin from Web proxies instead of its real sources. This assumption is reasonable since the victim can only observe the proxies and our goal is to filter malicious traffic instead of trace back. Like most of other physical processes in nature, a Web proxy's access behavior can be regarded as a combination of external manifestations (e.g., temporal and spatial locality(TSL)) and intrinsic driving mechanisms (e.g., normality or abnormality). The external manifestations are observable and usually controlled by the intrinsic driving mechanisms that cannot be accurately obtained by the origin server but can be estimated by the observable features of proxy to server traffic. Regarding with the HsMM, a Web proxy's access behavior can be directly mapped to an HsMM. The basic HsMM consists of a pair of stochastic processes: The observed process and the hidden semi-Markov state process. To model a Web proxy's access behavior by an HsMM, each hidden semi-Markov state represents a driving mechanism of a type of proxy-to-server traffic. Transition between two different Markov states represents the changes of driving mechanism. Duration of a particular semi-Markov state represents the dwell time of its corresponding driving mechanism. The architecture for spatial and temporal locality behavior is as shown below.

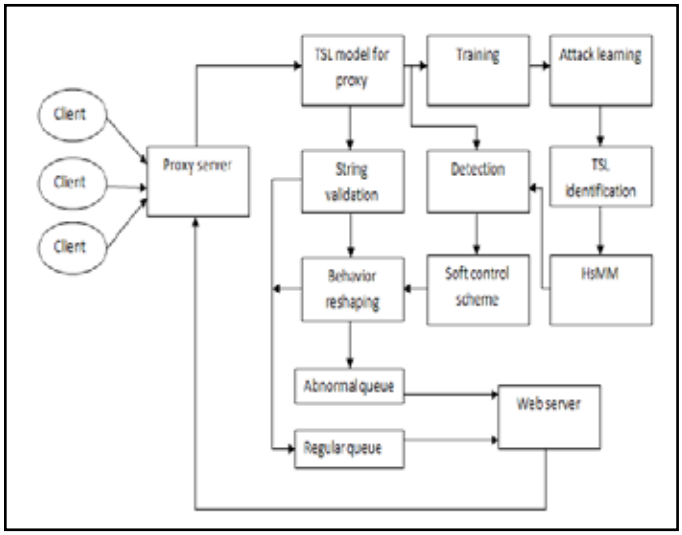

Fig. 1: Architecture

Resisting web-proxy based attack by using temporal and spatial locality behavior made certain assumptions to implement the model. Attack traffic is assumed to begin from Web proxies instead of its real sources. Thus the source of attack can't identify. Requests are grouped based on proxy server ID. So the requests from attackers and non attackers through proxy server are reached at web server side in a mixed manner. Due to the use of HsMM, state information

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

does not keep. So we cannot separate web requests based on user. Web server has no facility to split this requests. From this request, web server detects spatial and temporal behavior. But this will increase false positive and false negative ratio when number of non attacking client increases. Which means, some requests (which are not attack actually) considered as attack, some request (which are attacks) considered as non attack request. The request pattern and arrival rate are only considered for attack detection and does not consider header information in packets. The proposed system is to design and implement a new HTTP protocol for detecting client based attack instead of Proxy based. The above scenario can be achieved by varying the HTTP protocol by including HTTP request header information and client ip address fields in the actual request sent from the client to the proxy. The false negative ratios can be controlled by analysis of the requests based on the checksum generated from the browser information and ip address of client. This will resist more number of denial of service attacks from proxy or client. The enhanced system aims at reducing the number of detected false negative counts. HTTP protocol is modified by adding two more fields, one carrying the ip address of client and the other with the details about the browser that the client uses. The requests from each client are classified based on the ip address and browser information of the client. The simulation results in turn prove that the false negative ratio of the proposed method is considerably less than that of the existing system.

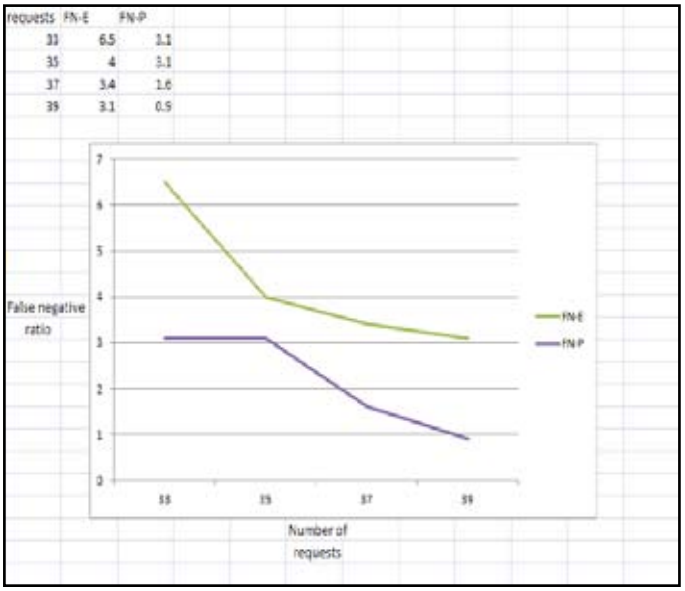

Fig. 2. Existing system Vs proposed system

V. Conclusion

Existing system, tried to filter the attack traffic from the aggregated proxy-to-server traffic, which is a new problem for the DDoS detection. A novel resisting scheme was proposed based on TSL. HsMM and soft-control scheme were proposed to improve the detection performance. Experiments confirmed the effectiveness and robustness of the scheme. The main advantages of this approach shown in the experiments include: 1) its detection performance is better than the pure statistical methods; 2) it is independent of the traffic intensity and the frequently varying Web contents; 3) it can realize the early detection. The proposed system is to design and implement a new HTTP protocol for detecting client based attack instead of Proxy based. This takes into account the client ip address as well as a checksum generated from the browser information of each client. Experiments show that more than 95 percentages of the attacks are identified and the false negative counts have reduced to a great extent. In addition to reduce false negative ratio another enhancement done in the proposed work is to identify the session hijacking attack. In the proposed work only false negative ratio is reduced, there is no change in number of false positive request. So it can be done as a future work in this field.

References

[1] *Y. Xie and S. Yu, "Measuring the normality of web proxies behaviour based on locality principles", Network and Parallel Computing, 2008.*

[2] *Yi. Xie and Shun-Zheng.Yu, "A large scale hidden semi-markove model for anomaly detection on user browsing behaviors", IEEE/ACM transaction on networking, February, 2009.*

[3] *Jie.Yu, Chengfang Fang, Liming U and Zhoujun Li, "A lightweight mechanism to mitigate application layer DDoS attacks", springer, 2009.*

[4] *S.Lee, G. Kim and S. Kim, "Sequence order independent network profiling for detecting application layer DDoS attacks", wireless communication and networking, 2011.*

[5] *S. Yu, W. Jia, S. Guo, Y. Xiang and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient", IEEE transaction on parallel and distributed systems, June, 2012.*

[6] *P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia Fernandez, and E. Vazquez, "Anomaly based network intrusion detection: Techniques, systems and challenges", Computers and security, 2009.*

[7] *Yi. Xie, S. Tang, Y. Xiang, and J. Hu, "Resisting web proxy based HTTP attacks by temporal and spatial locality behavior", IEEE transaction on parallel and distributed systems, July, 2013.*

[8] *R.Bharathi, R.Sukanesh, Y.Xiang, and J.Hu, "A PCA based framework for detection of appication layer DDoS attacks", wseas transactions on information science and applications, December, 2012.*

[9] *P. Denning, "The locality principle", ACM, 2005.*

[10] *Yang Xiang, Ke. Li, and Wanlei Zhou, "Low rate DDoS attacks detection and traceback by using new information metrics", IEEE transactions on information forensics and security, June, 2011.*

Sujina mol M S, Received the bachelor's degree in Computer Science and Engineering from Cochin University of Science and Technology, Kerala in 2012. Presently she is pursuing her M.Tech in the department of Computer Science and Engineering from Calicut University, Kerala. Her research interests include computer networks.

Aneesh M Haneef, Received the bachelor's degree in Information Technology from Mahatma Gandhi University, Kerala in 2004 and master's degree in Computer Science and Engineering from Anna University, Coimbatore in 2009. Currently working as an Assistant Professor in Computer Science and Engineering Department, MES College of Engineering, Under the Calicut University Kerala. He has teaching experience of five years. Research interests Includes computer networks.