IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

DDoS: Attack Analysis and Countermeasures

[1] Sujina mol M S, [2] Aneesh M Haneef

[1] Computer Science and Engineering, MES College of Engineering, Kuttippuram, Kerala, India

[2] Computer Science and Engineering, MES College of Engineering, Kuttippuram, Kerala, India

Abstract - Activities such as telecommunication, on-line banking and on-line shopping have recently being integrated through the internet. In such a situation security is an important criterion. 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 analyzed 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.

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

1. Introduction

Many methods designed to create defenses 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 method for attack detection depends on correlation coefficient, trust, spatial locality, temporal locality, etc. A.

Distributed Denial of Service attack 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.

2. Literature Survey

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

2.1 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. The detection scheme can be described as follows:

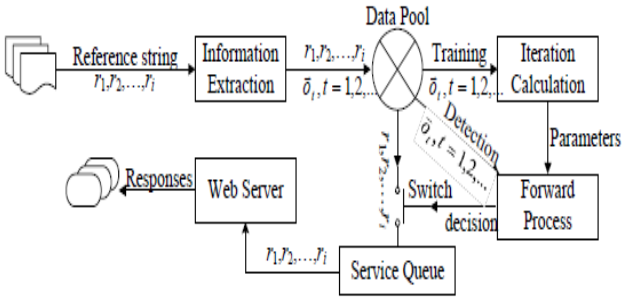

Fig. 1 Detection scheme

2.2 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.

2.3 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. The TMH architecture is as shown below:

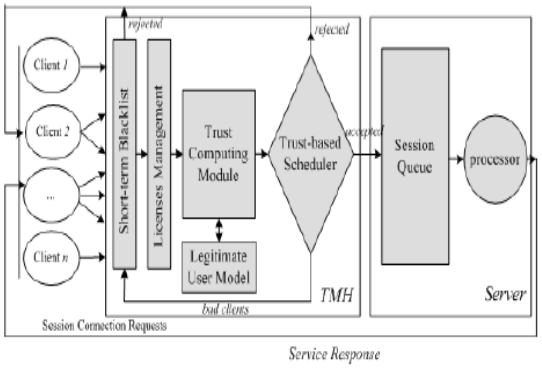

Fig. 2 TMH.

2.4 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.

2.5 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.

2.6 Low-Rate DDoS Attacks Detection and Trace Back 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]. The detection in information metrics can be explained as shown below:

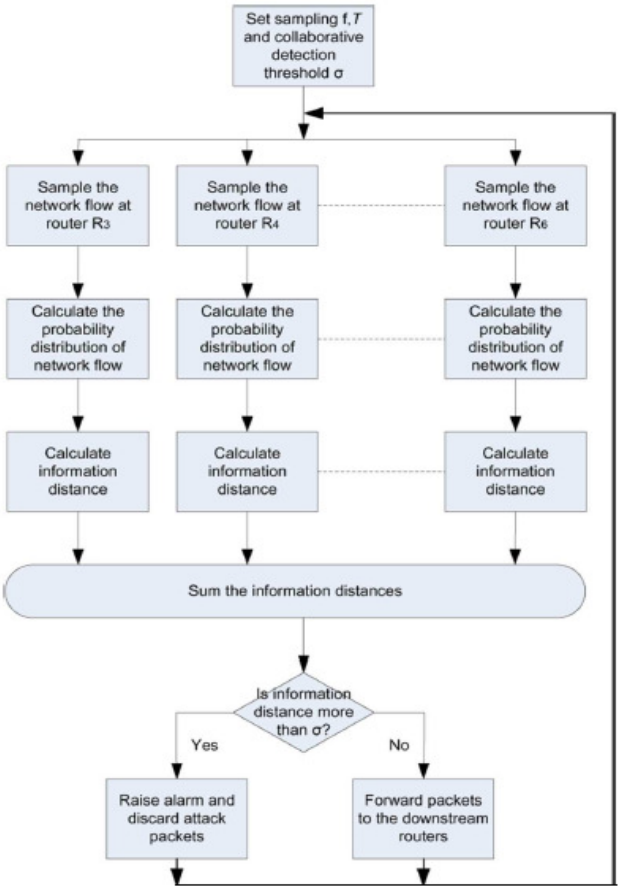

Fig. 3 Detection algorithm.

In this case detect attacks earlier by using the detection approach because traffic can be analyzed in upper stream routers instead of just in the victim's router. IP trace back scheme trace all attacks in a short time.

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

A server-side defense 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.

3. Performance Analysis

The following table gives a comparison for protecting against DDoS attack.

Table 1: Comparison

METHOD	LAYER	REMARKS	OBJECTIVE
Web proxy's behavior	Application	Temporal locality and bytes of requested objects	Detection and drop
User browsing behavior	Application	Entropy	Detection and drop
Trust management helmet	Application	TMH	Protect legitimate users
Sequence order independent network profiling	Application	Attribute of web page requests	Detection and drop
Flow correlation coefficient	Network	Size of botnets and correlation coefficient	Distinguish DDoS attack from flash crowds
Information metrics	Network	IP trace back analysis	Detection and source identification
Temporal and spatial locality behavior	Network	Temporal and spatial locality	Detection and reshaping

4. Conclusions

Various methods for the detection and prevention of DDoS attacks have been studied and compared. By analyzing various methods it is clear that each of them have their own advantages and disadvantages. The detection technique mainly depends on the traffic flow. Certain techniques only concentrate on attack detection and discard of attack flow.

Acknowledgments

We express my sincere gratitude to all the staff of Computer Science and Engineering Department in our college and beloved family members who helped me with their timely suggestions and support. I also express my sincere thanks to all my friends who helped me throughout the successful completion of the work. All glory and honour be to the Almighty God, who showered His abundant grace on me to make this work a success.

References

[1] Y. Xie and S.Yu,"Measuring the Normality of Web Proxies Behavior Based on Locality Principles", Network and Parallel Computing, 2008.

[2] Yi. Xie and Shun- Zheng. Yu,"A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors", IEEE/ACM transaction on networking, February, 2009.

[3] Jie. Yu, Chengfang Fang, Liming Lu 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. Zhou, 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 Application 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 Trace back by Using New

Information Metrics", IEEE transactions on in- formation 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.