Application Layer Distributed Denial of Service Attacks Defense Techniques : A review

Subhi R. M. Zeebaree[1], Karzan H. Sharif[2], Roshna Muhamad M.Amin[3]
[1]Technical College of Informatics-Akre, Duhok Polytechnic University, Kurdistan Region - Iraq
[2]College of Computer Science, University of Human Development, Kurdistan Region - Iraq
[3]College of Education, University of Sulaimaniya, Kurdistan Region - Iraq

ABSTRACT

Currently distributed denial of service (DDoS) is the most sever attack that effect on the internet convenience. The main goal of these attacks is to prevent normal users from accessing the internet services such as web servers. However the more challenge and difficult types to detect is application layer DDoS attacks because of using legitimate client to create connection with victims. In this paper we give a review on application layer DDoS attacks defense or detection mechanisms. Furthermore, we summarize several experimental approaches on detection techniques of application layer DDoS attacks. The main goal of this paper is to get a clear view and detailed summary of the recent algorithms, methods and techniques presented to tackle these serious types of attacks.

KEYWORDS : DoS, DDoS, Application Layer DDoS Attacks, Defense Techniques of Application Layer, DDoS Attacks.

1. INTRODUCTION

Nowadays internet becomes intermediary facility for human education, exchange, socialization and excitement, among numerous other essential parts of human life. Data sharing, E-commerce and entertainment have taken a new dimension. Obviously, the Internet is the greatest innovation in the computing and communications world. However, with the development of information and communication technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats [1]. Web threats posture a broad run of dangers, counting financial harms, identity theft, misfortune of private data or information, steal of network resources, harmed personal notoriety, and disintegration of consumer certainty in e-commerce and online managing an account. DoS attack is a proposed effort by malicious users to completely deactivate or destroy the availability of services/resources to legitimate users. Distributed denial of service (DDoS) attack is a form of DoS attack which slowdowns the server in responding to the client/refuses the client request. Now-a-days, one of the Internet's reliability and stability major threats is DDoS attack. Morever, the internet security is excessively affected by DDoS attacks. The primary objective of such attack is to consume server resources such as CPU, I/O bandwidth, sockets and memory etc. As the result, the resources available to other normal users/clients get limited or sometimes may not be available[2]. In some other words, the simple strategy behind a DoS attack is to deny the use of system services/resources to legitimate users and degrade system availability. The fundamental mechanism for DoS attack execution is to send a flood of superfluous network traffic to the target so that it cannot respond to genuine requests for services or information. However, in DDOS multiple sources are used by the attackers, and it is much more catastrophic than DoS [3]. Presently, botnet tools available on the Internet provide attackers with massive DDoS resources and a high level of stealth against countermeasures. Furthermore, the DDoS attacks are classified based on different factors. On the basis of network protocol stack, DDoS can be further classified as Network/transport level and Application level DDOS attacks[4]. The main target of this article is to provide a review of application layer DDoS attacks and its defense mechanism which were presented by researchers in the last few years. The rest of the paper is prepared as follows: section two covered DDoS attack. Application layer DDoS attacks is presented in section three. Literature review for defense

Academic Journal of Nawroz University
(AJNU) Volume 7, No 4 (2018).
Regular research paper : Published 21 December 2018
Corresponding author's e-mail : subhi.rafeeq@dpu.edu.krd

doi : 10.25007/ajnu.v7n4a279

techniques of application layer DDoS attacks is offered in section four and finally we concluded the paper.

2. Distributed Denial of Service (DDoS) attack

A postponement of DoS attack is DDoS attack where enormous numbers of compromised sources are launching the attack simultaneously on the web server to deny the services to valid users [5]. Moreover, DDoS attack is extremely simple but powerful type of attack can consume the network bandwidth and connectivity, as the result the attack victimise the network on permanent or temporary basis. DDoS attack stream behave like normal stream therefore it becomes difficult to identify legitimate packets from attack packets [6]. In recent DDOS attack become very severe hazard to web application, cloud application, mobile application. Generally, DDoS attack is launched explicitly from a collection of compromised systems known as botnet by an attacker. Many computers are used for launching a DDoS Attack. It makes use of client server technology. As a whole, DDoS attack comprises of Master, Handler, Agents and victim. The zombies (agents or bots) are the one used by the master to form a botnet. Larger the number of zombies, more disruptive the attack will be. Additionally, the communication between master and agents is done via handlers. Attacker sends command and controls their agent through handlers. Bots are devices that have been compromised by the handlers. The bots actually carry out the attack on the victim’s system. Attacker uses many scanning techniques for finding a vulnerable machine[7].The Most vulnerable layer of OSI TCP/IP stack to DDoS attack is transport layer (layer 3 of OSI layers) and network layer (layer 4 of OSI TCP/IP stack) of a communications system. The attacks directed at these layers are designed to flood a network interface with attack traffic in order to overwhelm its resources and deny its ability to respond to legitimate traffic [8]. Furthermore, application layer or layer seven attacks now become more sophisticated kind of DDos attacks. In layer 7 DDoS attacks a genuine connection is to be established with the target and traffic is almost similar to legitimate traffic.

3. Application Layer DDoS Attacks

An application layer attacks targets the layer 7 of OSI stack that essentially faces the end user includes applications that users are used to accessing online. Moreover, this layer is considered the most reachable and the most visible to the outside world. On the other hand, the application layer DDoS attack produces less network traffic than other layers attacks such as (transport and network) and hence discovering them is hard. Furthermore, causes more overhead on system with the equivalent amount of attacking requests traffic in the server side, and displays higher possibility to bypass intrusion and detection systems than the traditional DDoS attack [8]. According to Talpur and Kechadi [9] 51% of attacks are targeted on application layer and 49% targeted on network layer. In addition, the financial, ISPs, gaming, government, health and education are the most targeted sites. On the other side, Ni et al.[10] and Singh et al. [11] categorized application DDoS attacks into two types: bandwidth consumption (HTTP flooding) and resource exhausting. In the first type and through a flood of legitimate requests attackers attack the victim server. In other word, draining attack huge number of fake HTTP request are sent to the server to download large file as the result full bandwidth is consumed by this traffic and the victim server fails to provide it services. In the second type fake HTTP requests are sending to the server in order to consume server resources such as Sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth. With increasing computational complexity in Internet applications and larger network bandwidth, server resources may become the bottleneck of these applications. This type of attack is able to use fewer zombies but the attack has an even larger damage to the website. However, the traffic will be similar to the bandwidth exhausting DDoS and putting the victim server on the knee.

4. Defense Techniques of Application Layer DDoS Attacks

In recent, application DDoS attacks seriously increased, the detection and defense technology of those attacks become heated argumentation in the system area. Therefore many detecting and defense techniques have been proposed by researchers. Meng et al. [12] created an anomaly detection system to analysis user behavior which were the request sequence of HTTP; and the time interval of adjacent HTTP depending on Discrete-time Markov Chains (DTMC) . While users access to the web server were recorded on the server's log file. For each user request (GET or POST) when user logs in, he created the background server added record to the server log and recording the user's login time, IP, URL and other information. In general the detection system procedure had operated on normal mode for period of time to collect data and extract characteristics of user behavior to setup pattern of normal user behavior. This considered as training part. Furthermore, the system operated in actual environment to setup pattern of a normal user behavior, from collecting data behavior of current users and extracting users’ characteristics behavior. On the other hand, anomaly detection included three phases which were data preprocessing, training and detection part. Experimental result indicated that the proposed system could detect DDoS attacks excellently. Ni et al.[10] proposed a defense method which emulated the vital features of application layer DDoS attacks (HTTP GET request frequency and the distribution of source IP address). The system based on entropy of HTTP GET request per source IP address (HRPI). The researchers have used Kalman filter, while HRPI time series were transformed into a multidimensional vector by approximating the adaptive autoregressive (AAR) model parameters, to raise the accuracy of detection in several conditions. Moreover, AAR parameters of HRPI time series trained support vector machine (SVM) classifier. In addition, SVM have applied to classify the network traffic environment and to detect DDoS attacks. Experimental have tested in two different situations: in first condition, they evaluated the detection of DDoS attacks in normal traffic. The performance result revealed that the detection ratio increased when the traffic volume of attack increased. However in the second condition, they assessed the detection of DDoS attacks in Flash Crowd. The result shown when the flash crowd increased the detection ratio did not dropped immediately. Indraneel and Vuppala [13] proposed a bio inspired anomaly system to detect HTTP flood DDoS attacks in application layer. They evaluated the HTTP transaction similarities by choosing fair and flood data for training. Moreover, in the planned system and from request stream observed during an absolute time interval, user session and packet patterns, the features have extracted. On the other hand, Bat algorithm technique used to execute search from test phase to assessed compatibility. However, to recognize the signatures of given transactions in training phase, the cosine metric were used. The signatures reduced the procedure complexity, because the signatures having similar context in both records of normal and flood formats are obsolete to differentiate. In the experimental result they showed that their systems achieved improvement accuracy. Zolotukhin et al.[14] designed an algorithm for detecting layer 7 DDoS attacks that based on encrypted protocols. They focused on detection of DoS and DDoS which were trivial and intermediate threats beside targets. Therefore, they applied anomaly detection method on statistics frequently extracted from network packet headers. Moreover, they applied some clustering techniques for analyzing the conversations between a web server and its clients and defining normal user behavior model. Aberrant client's conversations were classified as anomalous from normal patterns. Furthermore, conversations groups to the same destination socket by one client and during a short time interval were classified depend on the reconstruction error generated by the stacked auto-encoder. The result showed that the proposed approach could detect attacks accurately. Xu et al.[15] worked with asymmetric application layer DDoS attacks. They focused to differentiate legitimate user requests and asymmetric attack requests by analyzing browsing behavior of users. Hence, they recognized page requests of users firstly to obtain the page-request sequence from accumulated traffic. Thereafter, training page requests sequences of legitimated users have done to establish the unified page state. Then based on the page request sequence in the observation period they constructed the random walk graph and by using random walk model that based on the unified page state transition matrix and the random walk graph to predict the subsequent page request sequence in following observation period. Lastly, the similarity between observed one and predicted page-request sequence computed and evaluated the similarity to judge a page-request sequence whether it is issued by asymmetric attack, and if true, identify the attackers. The experimental results indicated that the proposed method was very efficient to detect asymmetric application layer DDoS attacks.

Sivabalan and Radcliffe[16] proposed a method to detect and block DDoS attacks and letting valid user traffic. They used AYHA (Are You A Human) to generate a signature for each user tried to access a web server and dynamically determine whether a user is a non-human or legitimate. Moreover, blocking of users was occurred only when there was a high load or the load was above the Low Load Threshold (LLT). However, if the server load was low or less than LLT, there was no blocking. Experimental result indicated that using AYHA page let attack signatures real time calibration and differentiated legitimate flash traffic from attack traffic. Shtern et al. [17] proposed defense technique against application layer DDoS attacks which are low and slow by using software defined infrastructure. In the planned system the dubious traffic detected and automatically forwarded to Shark Tank system. Furthermore, they worked and discussed on an approach that was performance based model to detect and mitigate Low and Slow DDoS (LSDDoS) attacks. In addition, they used Commercial Off-The-Shelf components to implement the proposed defense mechanism. The experimental results showed that the performance based model had some tangible benefits. Zhou et al.[18] designed a system to detect application layer DDoS attacks that are target web servers. They worked to detect attacks at backbone where most of current web servers are directly connected. Thus for differentiating normal traffic or flash crowd from application layer DDoS attacks, they designed an algorithm to mining web traffic at backbone. In addition, the mining algorithm was combined with defense system which was modularized. The experimental results indicated that the designed system successfully distinguished between legitimated and attacks traffic on backbones. Yadav and Subramanian[19] proposed a method to detect application DDoS attacks which was based on pattern learning. They built application DDoS dataset of attack by extracting features from web server log, and preprocessing accomplished on the features were extracted. Moreover, to learn well useful features from dataset of application layer DDoS attack, broad learning based model of neural network for instance AutoEncoder was applied. Furthermore, the dataset of the application layer DDoS attack was divided into training and testing dataset. Therefore, to learn high level of application DDoS attack features, the algorithm was trained from training stage and then the algorithm tested for incoming traffic in test stage. The experimental results revealed that proposed algorithm could detect different application DDoS attacks and the ratio of detection was 98.99%. Beitollahi and Deconinck [20] proposed a technique to outline DDoS attacks on application layer by using least level of puzzles. The designed technique based on measuring various statistical attributes of web servers users and their traffic. The measured attributes represented normal user's characteristics and behavior and the web server use these attributes as reference profile. Moreover, during attacks period and based on reference profile, the server assigned scores to the connections. The system relied on the scores to determine whether the connection had normal user attributes and features or it was suspicious connection. The connection who got low scores defined as non-human or non-legitimated connection. The experimental results showed that the application layer DDoS attacks could detected by designed technique effectively. The summary of all the previous literature review of defense techniques of application layer DDoS attacks is presented in Table 1 which contain methods/algorithms, and Data used by the researchers. Additionally the results of all techniques are illustrated.

Table (1) : literature review summarize of application layer DDoS attacks techniques

Researchers	Published year	Methods/ Algorithm	Data	Results
Ni et al.[10]	2013	Kalman filter and Support Vector Machine	Web Server of Changzhou university	Detection ratio of attacks increased when attacks traffic increased.
Meng et al. [12]	2017	Discrete-time Markov Chains (DTMC)	Syskill and Webert Web Page	The proposed system could detect DDoS attacks excellently.
Indraneel and Vuppala[13]	2017	Bat Algorithm and Cosine Metric	Center for Applied Internet Data Analysis	The proposed system had enhancement detection accuracy.
Zolotukhin et al.[14]	2016	Anomaly detection method and Clustering technique	Realistic Global Cyber Environment	The proposed approach could detect attacks accurately.
Xu et al.[15]	2014	Random Walk Model	www.sctv.com	The proposed method was very efficient to detect asymmetric application layer DDoS attacks.
Sivabalan and Radcliffe[16]	2013	AYHA (Are You A Human)	------------	The proposed algorithm differentiated legitimate flash traffic from attack traffic successfully.
Shtern et al. [17]	2014	performance model-based and Commercial Off-The-Shelf	Software Defined Infrastructure	The performance based model had some tangible benefits.
Zhou et al.[18]	2014	Real-time Frequency Vector	Simulated data and Sina web traffic	The system successfully distinguished between legitimated and attacks traffic on backbones.
Yadav and Subramanian [19]	2016	AutoEncoder	nitt.edu	The algorithm detected different application DDoS attacks and the ratio of detection was 98.99%.
Beitollahi and Deconinck [20]	2012	statistical analysis	ClarkNet	The application layer DDoS attacks could detected by designed technique effectively.

5. Conclusion

A comprehensive study of the efforts were presented in the last few years on DDoS attacks especially in Application layer has offered in this paper. In more details abroad review of the most modern and effective techniques or mechanisms against application layer

DDoS attacks is provided. It is clearly noticed from the researches that detecting process of these attacks is difficult and it is more challenge to prevent application layer DDoS attacks since traffic of these attacks is like legitimate traffic. The main goal of these attacks is to down the victims and therefore the resources will be unavailable to normal users. Also we observed from the literature that blocking both abnormal and valid traffic is not permitted because the availability of the resource will decrease. Finally, without an effective defense mechanism which has high detection accuracy the internet resources are vulnerable to these types of attacks and become inaccessible to the normal user\clients.

References

1.Jouini, M., L.B.A. Rabai, and A.B. Aissa,(2014), Classification of security threats in information systems. Procedia Computer Science, 32: p. 489-496.

2.Prasad, K.M., A.R.M. Reddy, and K.V. Rao,(2017), BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web. Journal of King Saud University-Computer and Information Sciences.

3.Kalkan, K., G. Gür, and F. Alagöz, (2016), Filtering-based defense mechanisms against DDoS attacks: A survey. IEEE Systems Journal.

4.Rajkumar, M.N., (2013), A survey on latest DoS attacks: classification and defense mechanisms. International Journal of Innovative Research in Computer and Communication Engineering 1(8): p. 1847-1860.

5.Coulouris, G.F., J. Dollimore, and T. Kindberg, (2005), Distributed systems: concepts and design: pearson education.

6.Kumar, V. and K. Kumar. (2016), Classification of DDoS attack tools and its handling techniques and strategy at application layer. in Advances in Computing, Communication, & Automation (ICACCA)(Fall), International Conference on, IEEE.

7.Deshmukh, R.V. and K.K. Devadkar, (2015), Understanding DDoS attack & its effect in cloud environment. Procedia Computer Science 49: p. 202-210.

8.Zhang, H., et al. SENTRY, (2016) : A Novel Approach for Mitigating Application Layer DDoS Threats. in Trustcom/BigDataSE/I SPA, 2016 IEEE, IEEE.

9.Talpur, S.R. and T. Kechadi. (2016) ,A survey on DDoS attacks: Router-based threats and defense mechanism in real-world data centers. in Future Technologies Conference (FTC), IEEE.

10.Ni, T., et al. , (2013), Real-time detection of application-layer DDoS attack using time series analysis. Journal of Control Science and Engineering 2013: p. 4.

11.Singh, B., K. Kumar, and A. Bhandari, (2015), Simulation study of application layer DDoS attack. in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on IEEE.

12.Meng, B., et al, (2017), DDOS Attack Detection System Based on Analysis of Users' Behaviors for Application Layer. in Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on, IEEE.

13.Indraneel, S. and V.P.K. Vuppala, (2017), HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm. Applied Computing and Informatics.

14.Zolotukhin, M., et al, (2016), Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic. in Telecommunications (ICT), 2016 23rd International Conference on, IEEE.

15.Xu, C., et al, (2014), Detection on application layer DDoS using random walk model. in Communications (ICC), 2014 IEEE International Conference on, IEEE.

16.Sivabalan, S. and P. Radcliffe, (2013), A novel framework to detect and block DDoS attack at the application layer. in TENCON Spring Conference, 2013 IEEE, IEEE.

17.Shtern, M., et al. Towards mitigation of low and slow application ddos attacks. in Cloud Engineering (IC2E), 2014 IEEE International Conference on. 2014. IEEE.

18.Zhou, W., et al., (2014), Detection and defense of application-layer DDoS attacks in backbone web traffic. Future Generation Computer Systems, 38: p. 36-46.

19.Yadav, S. and S. Subramanian, (2016), Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder. in Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on, , IEEE.

20.Beitollahi, H. and G. (2012), Deconinck, Tackling application-layer DDoS attacks. Procedia Computer Science, 10: p. 432-441.