ISSN: 2349 - 4891

International

Journal of Recent Research and Applied Studies

(Multidisciplinary Open Access Refereed e-Journal)

SDN BASED DISTRIBUTED DENIAL OF SERVICE ATTACK

Dr.S.Selvakani[1], Mrs.K.Vasumathi[2], A.Kavitha[3]

[1]Assistant Professor and Head, PG Department of computer science, Government Arts and science college, Arakkonam, Ranipettai,Tamilnadu,India

[2]Assistant Professor and Head, Department of Computer Applications, Government Arts and science colege, Arakkonam, Ranipettai,Tamilnadu,India

[3]PG Scholar, PG Department of computer Science, Government Arts and Science College, Arakkonam, Ranipettai,Tamilnadu,India

Received 15th February 2021, Accepted 18th March2021

Abstract

DOS attacks are carried out by attack tools, worms and botnets using different packet-transmission strategies and various forms of attack packets to beat defense systems. These problems lead to defense systems requiring various detection methods in order to identify attacks. Moreover, DOS attacks can mix their traffics during flash crowds. By doing this, the complex defense system cannot detect the attack traffic in time. In this project a behavior-based detection using Crowd Correlation Analysis that can discriminate DOS attack traffic from traffic generated by real users. in the Euclidean space to express as a diagonal matrix proposed can master the capacity of network system against each attack means and the defense capability of network system. cyber-attack such as DDOS attack is still the most powerful attack that disrupts the genuine users from accessing the essential services. In application layer-based DDOS attack, attacker uses other machine instead of using his own IP address to flood the targeted system and disrupts the services SDN (software defined networks) for cost efficiency and network Application layer distributed denial of service (DDOS) attacks have become a severe threat to the security of web servers. These attacks evade most intrusion prevention systems by sending numerous benign HTTP requests flexibility, but DDOS is one of the most launched attack on SDN layer. DDOS attack in this type of environment leads to system failure DDoS is one of the most launched attack on SDN layer. DDOS attack in this type of environment leads to system failure financial loss, data theft, and performance degradation extensive survey has been made to detect and prevent DDOS based attack in application layer and SDN based environment. we propose a effective defense system, named Sky Shield, which leverages the sketch data structure to quickly detect and mitigate application layer DDOS attacks. novel calculation of the divergence between two sketches, which alleviates the impact of network dynamics and improves the detection accuracy.

KEY WORDS

Distributer denial of service,SDN,Application Layer.

Introduction

Denial of service (DOS) attacks have become a major threat to current computer networks. Early DOS attacks were technical games played among underground attackers. For example, an attacker might want to get control of an IRC channel via performing DOS attacks against the channel owner. Attackers could get recognition in the underground community via taking down popular web sites. Because easy-to-use DOS tools, such as Trinco (Dmitritch 1999), can be easily downloaded from the Internet, normal computer users can become DOS attackers as well. They sometime coordinately expressed their views via launching DOS attacks against organizations whose policies they disagreed with. DOS attacks also appeared in illegal actions. Denial-of-Service attack is a cyber-attack that makes network resources unavailable to the intended users by disrupting the services Distributed Denial-of-Service (DDOS) attack is a large scale denial of service attack where attacker uses different IP addresses to the flood the victim. collection of internet connected devices controlled by a third party by breaching its security attack traffic to simulate legitimate user behavior software-defined network (SDN) environment, that is, legitimate traffic that looks similar. Information distance metric is used scribe the variations of traffic behavior of such events. AL DDoS attack and defense utility is proposed to calculate the effects of AL-DDoS attack. By comparing the simulation experiment data with the related technical data the effectiveness, objectivity, and accuracy of the method software defined networks.

Correspondence

Dr.S.Selvakani Assistant Professor and Head, PG Department of computer science, Government Arts and science college, Arakkonam, Ranipettai,Tamilnadu,India

I. DDOS ATTACKS IN APPLICATION LAYER

Important factor for users. DDOS attack on web server is growing rapidly and has caused huge economic loss for the victim The traffic created by the flash crowd leads to increase in the distribution of source IP address. HTTP based attack is an application layer-based DDOS attack. In these types of attacks, attacker make use of attributes of HTTP to connect to the server so that they stay connected until the request is completed. by sending incomplete HTTP requests. Either incomplete HTTP header will be present in HTTP GET requests or the length of HTTP headers content field will be very huge compared to the message body of HTTP DDOS attack can be created using the BOTNET that compromise large number of bots. Bots are controlled by the attacker that has neither firewall nor antivirus and are used for internet relay chat (IRC).

Fig1 Overview of Denial of Service attack

A. TYPES OF ATTACKS

- UDP flood attack
- SYN flood attack
- SNMP Reflection attack
- Single web page attack
- Main Page Attack
- Dominant web page attack

III. LITERATURE SURVEY

botfilter - An Approach to Defend Application Layer Distributed Denial of Service Attacks Sini Thankachan1 Bibin Varghese2 Smita C Thomas3

Various studies have taken place to design systems to defend DDoS attacks. Major concerns of a DDoS attack defense system are: i) System should mitigate the attacks as soon as possible. ii) Quality of Experience (QOE) of user. iii) System should not impose much overhead to legitimate users. iv)DDoS attacks involve huge volume of traffic that these demand an efficient data structure to process the traffic. Filter-based approaches using deployed filters [2],[3] are used to block unwanted traffic. A frame work called Kill-bots [4] which provides authentication using graphical passwords is an approach to capture Denial of Service attacks mounted by professionals using botnets Admission control is provided as a function of total load to ensure the consistent service of server.

B*ro: A System for Detecting Network Intruders in Real-Time Vern Paxson,*

Stand-alone system for detecting network intruders in real-time by passively monitoring a network link over which the intruder's traffic transits. We give an overview of the SYSTEM'S DESIGN, WHICH EMPHASIZES HIGH-SPEED (FDDI-RATE) monitoring, real-time notification, clear separation between mechanism and policy, and extensibility. To achieve these ends, Bro is divided into an "event engine" that reduces a kernel filtered network traffic stream into a series of higher level events, and a "policy script interpreter" that interprets event handlers written in a specialized language used to express a site's security policy. Event handlers can update state information, synthesize new events, record information to disk, and generate real-time notifications via syslog. And discuss a number of attacks that attempt to subvert passive monitoring systems and defenses against these, and give particulars of how Bro analyzes the four applications integrated into it so far: Finger, FTP, Port mapper and Telnet. The system is publicly available in source code form.

Intrusion Detection System Based on Fuzzy Association Rule with Genetic Network programming Harinee.K, Veeramuthu.A

Intrusion detection which classifies the attacks on the Internet from usual behavior of usage on the Internet. Here intrusion detection systems are vital tool in the cluster environment fight to keep its computing resources secure .It is an unavoidable portion of the information security system. Emerging variety of network behaviors and the rapid development of attack scenarios, it is vital to develop fast machine-learning-based intrusion detection algorithms with high detection rates and low false positive and false negative -alarm rates with the help of association rule mining. In this course of work a fuzzy class-association rule mining method based on genetic network programming (GNP) for intrusion detection. GNP is an evolutionary optimization technique, which uses directed graph structures leads for enhancing the representation ability .In combination with fuzzy set theory and GNP, the proposed work can deal with mixed database that contains both discrete and continuous attributes and also extract many important class association rule.

.

.Improving Attack Detection Rate in Network Intrusion Detection Using Adaboost Algorithm with

Multiple Weak Classifiers P. Natesan, P. Balasubramanie, G. Gowrison

With the tremendous growth of network-based services and users of the Internet, it is important to keep the data and transactions in the Internet more secure. Intrusion detection system has emerged as an essential component and an important technique for network security. In this article, an Ad boost algorithm for network intrusion detection system with combination of multiple weak classifiers is proposed. The classifiers such as Bayes Net, Nave Bayes and Decision Tree are used as weak classifiers. A benchmark dataset is used in these experiments to demonstrate that boosting algorithm can greatly improve the classification accuracy of weak classification algorithms. Our approach achieves higher detection rate with low false alarm rates and is scalable for large datasets, resulting in an effective intrusion detection system.

FLOODING ATTACKS DETECTION IN BACKBONE TRAFFIC USING POWER DIVERGENCE ALI MAKKE, OSMAN SALEM, MOHAMAD ASSAAD, HASSINE MOUNGLA, AHMED MEHAOUA

Flooding attacks detection in traffic of backbone networks requires generally the analysis of a huge amount of data with high accuracy F and low complexity. In this paper, we propose a new scheme to detect flooding attacks in high speed networks. The proposed mechanism is based on the application of Power Divergence measures over Sketch data structure. Sketch is used for random aggregation of traffic, and Power Divergence is applied to detect deviations between current and established probability distributions of network traffic.

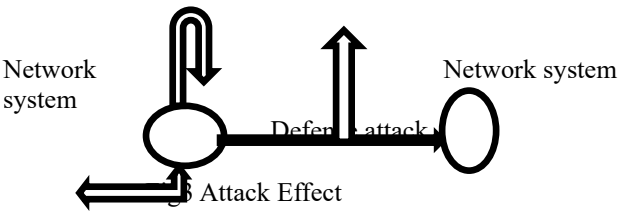
We focus on tuning the parameter of Power Divergence to optimize the performance. We evaluate our approach using real Internet traffic traces, obtained from MAWI trans Pacific wide transit link between USA and Japan. Our results show that the proposed approach outperforms existing solutions in terms of detection accuracy and false alarm ratio.

Fig2 ARCHITECTURE DIAGRAM

IV. PROBLEM DEFINITION

Companies might use DOS attacks to knock off their competitors in the market. Extortion via DOS attacks were on rise in the past years (Pappalardo et al. 2005). Attackers threatened online businesses with DOS attacks and requested payments for protection. Known DOS attacks in the Internet generally conquer the target by exhausting its resources, that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. Because it is difficult for attackers to overload the target's resource from a single computer, many recent DOS attacks were launched via a large number of distributed attacking hosts in the Internet. These attacks are called distributed denial of service (DDoS) attacks. In a DDoS attack, because the aggregation of the attacking traffic can be tremendous compared to the victim's resource, the attack can force the victim to significantly downgrade its service performance or even stop delivering any service.

Attack effect change the network system status



V. EXISTING SYSTEM

Generally, it is classified into two main categories: use-based detection systems and anomaly-based detection system.The Sky Shield systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. The main disadvantage is the large amount of alerts produced

V. PROPOSED SYSTEM

In this project, a DoS attack detection system that uses Traffic Crowd Analysis (TCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our TCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition.

The DoS attack detection system presented in this paper employs the principles of TCA and anomaly-based detection. They equip the detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A triangle area technique is developed to enhance and to speed up the process of TCA. A statistical normalization technique is used to eliminate the bias from the raw data.

A. ADVANTAGES OF PROPOSED SYSTEM

- ❖ More detection accuracy
- ❖ Less false alarm
- ❖ Accurate characterization for traffic behaviors and detection of known and unknown attacks respectively.

VI. EXPERIMENTAL RESULT

In this paper, we first describe the collection of datasets and then report the extensive evaluation results of DDos Attack using the real datasets in the SDN Based Distributed Denial of Service Attack Node Formation

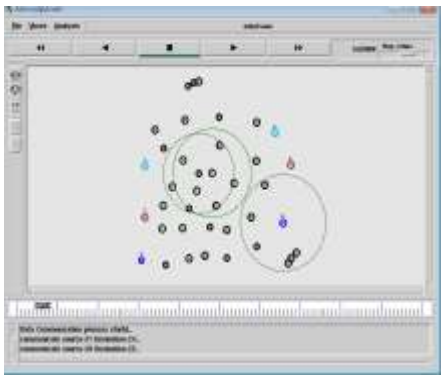


Fig4. NODE FORMATION

This screen four Destination and two source and sixty eight nodes one node to another node data transmission. Network based on Data communication process start communicate source 21 Destination 24 and communicate source 20 Destination 25 in the node formation.

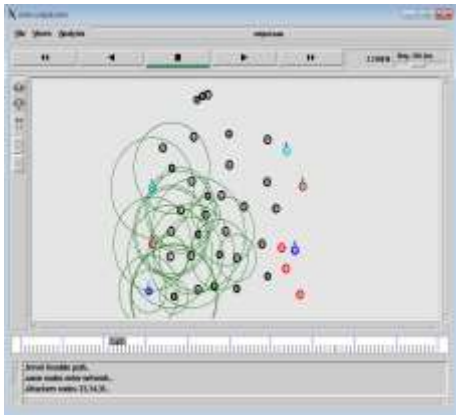


Fig 5. NODE COMMUNICATION

In the paper one node to another node communicate to the Node Communication. It is data transmission of the Distributed Denial of Service.

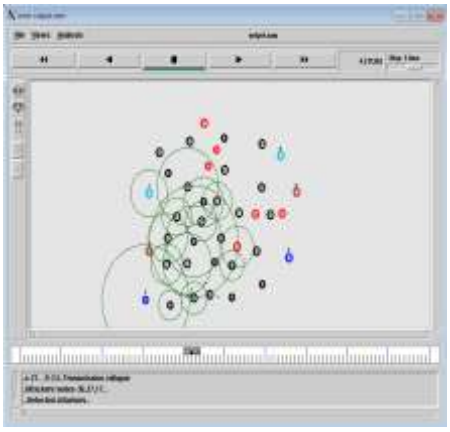


Fig 6. NETWORK ATTACK

Many resent Dos attack also called DDos attacks were distributed attacking hosts. A DDos attack is launched in two phases. First an attacker builds an attack network which is distributed and consists of thousand's of compromised computers. Then attacking hosts flood tremendous volume of taffic towards victims either under the command of the attacker or automatically.

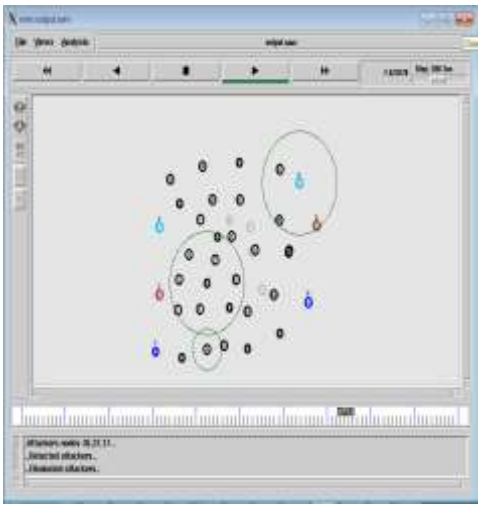


Fig7. ATTACK DETECTION

[1]

DDoS attacks mainly take advantage of the Internet architecture and this is that makes them even more powerful. The Internet was designed with functionality, not security, in mind. Its design opens several security issues that can be exploited by attackers. More analytically

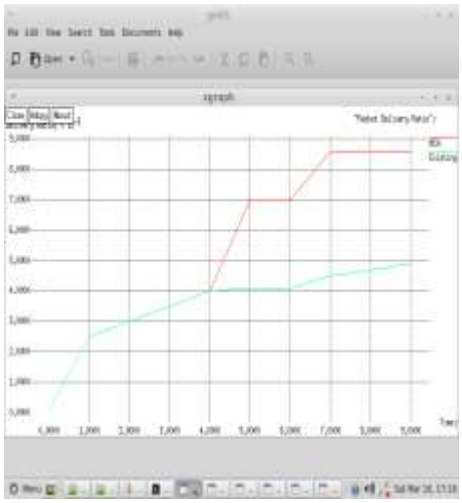


Fig 8. THROUGHPUT RATIO

The analyzing the attack and defense measures used in experiment we can obtain the attack utility value caused To the application layer of the current network under *DIFFERENT ATTACK*

VII. FUTURE ENHANCEMENTS

In future, there are many approaches used to detect and mitigate the effect of DDOS attack. Different approaches have different limitations like legal users have to wait more time for service, high false positives, high false negatives, more time consuming and complex, require more memory usage etc. Here, I propose one light weight mechanism to detect and mitigate the DDOS attack against web server. My proposed solution divided into three phase.

- ❖ Identify DDOS attack.
- ❖ Differentiate DDOS attack traffic from normal traffic.
- ❖ Mitigate the effect of DDOS attack.

VIII. CONCLUSION

This project has presented an TCA-based DoS attack detection system which is powered by the triangle-area based CCA technique and the anomaly-based detection technique. The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

REFERENCES

[2] [1] Sini Thankachan1 Bibin Varghese2 Smita C Thomas3 BOTFILTER - An Approach to Defend Application Layer Distributed Denial of Service Attacks

[3] [2] Bro: A System for Detecting Network Intruders in Real-Time

[4] Vern Paxson

[5] [3] Harinee.K, Veeramuthu.A Intrusion Detection System Based on FuzzyAssociation Rule with Genetic Network programming

[6] [4] P.Natesan, P.Balasubramanie, G. Gowrison Improving Attack DetectionRate in Network Instrusion Detection Using Adaboost Algorithm with Multiple Weak Classifiers

Please cite this article as: **Dr.S.Selvakani, Mrs.K.Vasumathi, A.Kavitha** (2021). **SDN BASED DISTRIBUTED DENIAL OF SERVICE ATTACK** . *International Journal of Recent Research and Applied Studies*, 8, 3(5), 35-39.