Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

SECURING INTERCONNECTED SYSTEMS FROM DENIAL-OF-SERVICE ATTACK BASED ON CORRELATION ANALYSIS OF TRAFFIC FEATURES

Suketha[1], K H Naz Mufeeda[2]

[1] *Department of Computer Science and Engineering,SCEM,Mangalore*
[2] *Department of Computer Science and Engineering,SCEM,Mangalore*

Abstract- Web servers, database servers , routers, cloud computing servers and also some end systems are now facing severe problems from network attackers. One of the attack known as Denial-of-Service (DoS) attack causes major impact on these end systems by consuming their bandwidth and resources. DoS attack traffic behavior is completely different from the legitimate network traffic behavior so this paper presents a DoS attack detection system at the sender side that uses multivariate correlation analysis (MCA) of traffic features for accurate characterization of legitimate and illegitimate traffic. MCA based DoS attack detection system employs the principle of network based detection in attack recognition hence making the technique capable of detecting all known and unknown DoS attacks efficiently. Furthermore, a triangle based technique is proposed to speed up the process of MCA. Triangle containing the current traffic features is compared with history of traffic triangles in the database in order to distinguish between legitimate and illegitimate traffic. Later allowing only the legitimate traffic to enter the network and blocking the illegitimate traffic hence prohibiting the attacker from consuming the bandwidth.

Keywords-Denial-of-Service, Multivariate Correlation Analysis, Network Based Detection,Triangle Based Technique,Traffic Features.

I . INTRODUCTION

Security is most important aspect in interconnected systems such as web servers, database servers, cloud computing servers and so on. Denial-of-Service attacks are serious threat for such interconnected systems. This attack can consume memory, network resources, CPU and also shutdown or damages the operation of the resource which is under attack. These attacks are launched against network bandwidth or server resources by preventing access to these resources to the authorized users.

Denial-of-Service attack is an event that diminishes or eliminates networks capability to perform the expected functionality. The main aim of the DoS attack is to consume the resources of the victim or the resources on the way to communicate with the victim. The victim can be a host, a router or an entire network. The major effect of these attacks varies from temporarily blocking service availability to misrepresenting the information in the network permanently. Therefore, accurate detection of DoS attacks are necessary for the protection of interconnected systems.

Dos Classification: Dos attempts to delay the services of targeted system from its legitimate users. Depending on how this attack uses the resources unfairly, DoS can be categorized as

1. Vulnerability DoS: exploits the weakness in system implementation, configuration or system design to crash the system completely or to reduce the system performance. As an example, a teardrop attack

attempts to destroy the target system by sending intentionally modified packets which are incorrectly handled by the victim machine.

2.Flood DoS: exploits the resources for communication between the victim and attacker, and attempts to tire out the network resource or computation capability of the victim by sending huge amount of malicious traffic at the same time.

A DoS attack detection system based on multivariate correlation analysis is mainly for the accurate detection of network traffic characteristics by extracting the geometrical correlations between various features of network traffic. This mechanism based detection systems monitors the traffic transmitting over the protected networks. This technique employs network based detection mechanism in order to detect the DoS attack mainly because, the configuration of network based detection mechanism is less complicated than the host based detection mechanism.

II. RELATED WORK

2.1 Flow Correlation Coefficient Analysis Method

An algorithm to detect DDoS attacks from crowds of traffics by analyzing the flow correlation coefficient among suspicious flows was proposed in [2].The principal component analysis (PCA) technique is used here.

Advantages

- PCA finds the features in a high dimension data by reducing the dimension of the data without losing the information in it.

Disadvantages

- This approach fails to produce better results in terms of better detection rate and lesser false alarm rate.

2.2 Covariance Matrix Based Method

A covariance matrix based approach was proposed in [3] to extract the correlation of the features in the form of sequential samples.

Advantages

- The advantage of this approach is it improves detection accuracy.

Disadvantages

- This approach is vulnerable to attacks because it linearly changes all the monitored features.
- In addition this approach considers a group of features rather than individual feature and labels the entire group of observed feature as either legitimate or illegitimate but not the individual feature in the group.

2.3 Triangle Area Based Method

An approach based on triangle area was presented in [4] to generate better discriminative features.

Advantages

- Generates better discriminative features.

Disadvantages

- This approach has dependence on prior knowledge of malicious behaviors. That means it will compare the observed traffic features with already known malicious behaviors.
- If there is no prior knowledge about the observed illegitimate traffic then this approach is of no use to analyze the attacks and also it not accurately detects the attack.

2.4 Geometrical Structure Based Method

Geometrical structure based approach is proposed in [5] where Mahalanobis Distance(MD) was used to extract the correlations between the selected packet payload features.

Advantages

- This approach not depends on prior knowledge of malicious behaviors.

Disadvantages

- The main problem with approach is it works with network packet payloads.

2.5 Covariance Matrix Sign Method

An approach called Covariance Matrix Sign (CMS) for detection of DoS attack is proposed in [6].

Advantages

- The approach achieves high detection rates.

Disadvantages

- Suffers from problems such as high false positive rates.
- This approach do not work properly in case of an attack changing all the previously monitored features.

III .PROPOSED SYSTEM

This paper is about securing the interconnected systems from DoS attack, using a technique of Multivariate Correlation Analysis. The aim is to analyze correlations of traffic feature inorder to diffrentiate between legitimate and illegitimate traffic because of important reason that DoS attack traffic behavior is entirely different from the normal network traffic behavior. In this project features such as IP Address, Timestamp, Message Length are mainly used to obtain the correlative information. The correlative information between the features of observed traffic are extracted by applying triangle generation method. This correlative information is compared with normal traffic features correlative information. The effect of DoS attack on the observed traffic causes large variation in the correlative information. So the change in correlation indicates presence of intrusive activities. Thereby blocking such a traffic entering the network and hence protecting the interconnected systems from DoS attack.

3.1 System Architecture

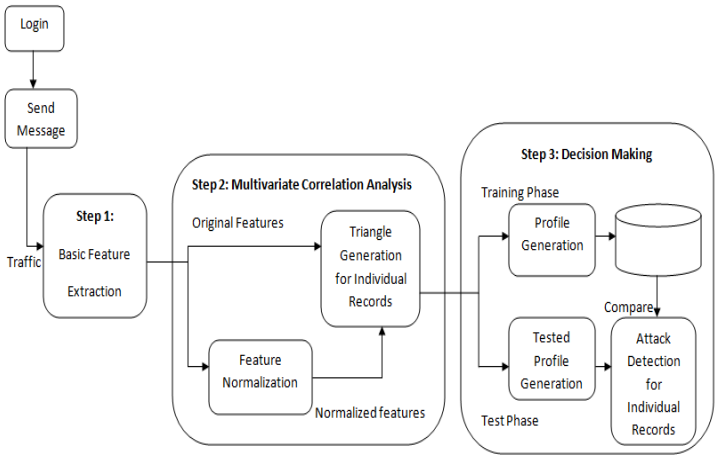

Figure. 1 Proposed system architecture

The entire detection mechanism consists of following three major steps [1] as shown in Figure.1.

Step 1. Basic Feature Extraction
Basic features are extracted from the place where traffic entering the network. These basic features are later used to form traffic records. The basic features are IP address ,Timestamp and Message Length etc. Monitoring and analyzing the network traffic at the sender side will help to reduce the bandwidth consumption by the attacker.

Step 2. Multivariate Correlation Analysis
DoS attack traffic shows variation from the legitimate network traffic and the behavior of network traffic is reflected by its statistical properties. Correlation Analysis helps to visualize and understand the relationship between the pairs of variables. In this step triangle generation module is applied to extract the correlation between the two distinct features coming from the step1 or the traffic feature normalized by feature normalization module[9].The occurrence of DoS attack cause changes to these correlations and hence it can be used as indicator to identify the intrusive action. This provides greater discriminative information for the application to diffrentiate between legitimate traffic and illegitimate network traffic records.

Step 3. Decision Making
Network based detection mechanism is applied in this step. It helps the accurate detection of DoS attacks by comparing the various traffics. Two phases are involved in decision making.
1.Training Phase: To generate profiles for various types of traffic records, the profile generation module is operated in this phase. The profiles are generated as either trusted or untrusted depending upon the state of the application. The generated profiles are then stored in the database.
2.Test Phase: To build the profiles for individual observed traffic records, tested profile generation module is operated in this phase. Tested profiles are then given to the Attack Detection module. In Attack Detection module individual tested profiles are compared with the respective stored normal profiles. If the observed traffic record gives more match with respect to the trusted traffic then declares the observed traffic as legitimate one and allows that traffic to enter the network otherwise declares it as illegitimate one and blocks it hence illegitimate traffic does not consume bandwidth required to communicate with the end systems.

3.2 System Implementation
Sign Up Page: In this application to send message to some other system the sender needs to be registered to the application using their IP Address and Name. Without registration one cannot send message to some other system. If someone tries to register to the application with already existing IP Address and with different name in such situation application rejects such a registration.
Login Page: After successful registration sender must login to the application using IP Address and password.
Compose Message Page: In this page sender enters the receiver IP Address, subject and message content. When the sender clicks the send button, features such as IP Address, Message Length and Timestamp are extracted from the current traffic. The triangle involving these three features is generated and following conditions are checked in order to determine whether the current traffic is trusted or blacklist.
1.In many applications such as Email ,twitter etc there is a limit to the user input like that this application requires that the message length must be less than 5KB because many computer systems cannot handle such a message or it may fill the buffer capacity of the receiver or may sometimes crash

the receiver system. Hence message length lesser than 5KB is considered as trusted and application sends that message to the receiver.

2.If a sender continuously sending message to the same receiver and it crosses certain limit means either they are creating the network congestion or they are trying to make that receiver services unavailable to its intended users then such a traffic is considered as blacklist and application blocks such a message.

3.Some attackers are sending message at particular time everyday like spam message in order to learn about the state of the receiver systems. Hence such a traffic is also considered as blacklist and application blocks such a message.

Every time the current traffic triangle is compared with all the previous traffic triangles in order to determine the current traffic as either trusted or blacklist as shown in Figure. 2 and Figure 3. There must be 2:1 comparision between the current traffic and the previous one.

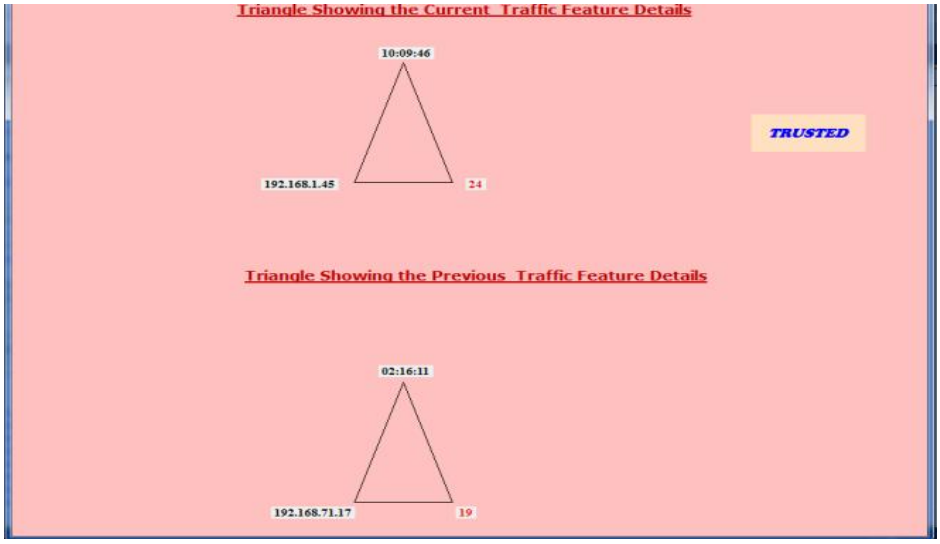

Figure. 2 Triangle showing the trusted traffic

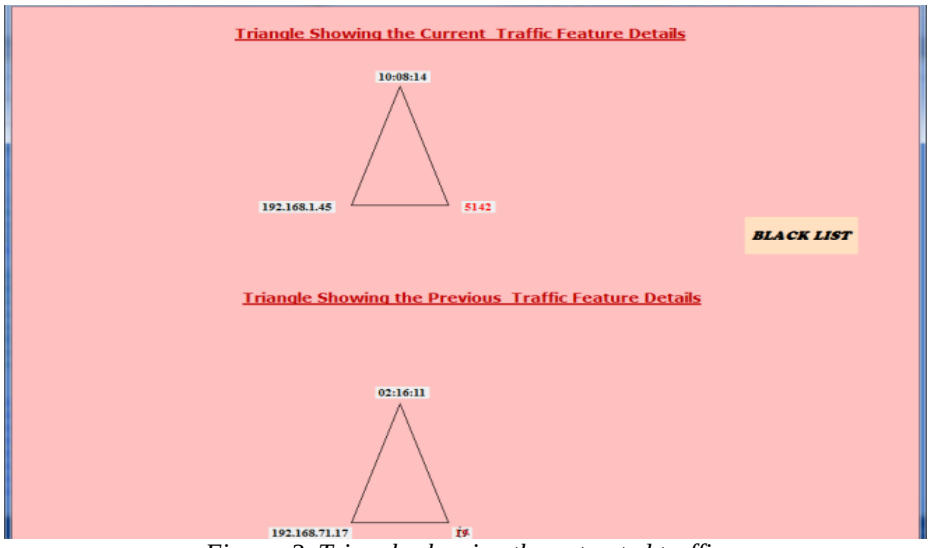

Figure. 3 Triangle showing the untrusted traffic

IV. CONCLUSION

Proposed DoS attack detection system acts like a protocol at the sender side to detect the DoS attack by extracting the traffic features such as IP Address, message length and timestamp and also distinguishes between legitimate and illegitimate network traffic and allows only legitimate traffic to flow across the network . Hence this method will be helpful for the detection of known and unknown DoS attacks.

REFERENCES

[1] Zhiyuan Tan,Aruna Jamdagni,Priyadarsi Nanda,"A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis ," IEEE Trans.,vol. 25,February 2014.
[2] S. Yu, W. Zhou,W. Jia, S. Guo, Y. Xiang, and F. Tang,"Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems,vol. 23, June 2012.
[3] S. Jin, D.S. Yeung, and X. Wang,"Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, 2007.
[4] C.F. Tsai and C.Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," Pattern Recognition, vol. 43,2010.
[5] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R.P. Liu,"RePIDS: A Multi Tier Real-Time Payload Based Intrusion Detection System," Computer Networks, vol. 57, 2013.
[6] Tavallaee, S.A., Ghorbani, " A Novel Covariance Matrix Based Approach for Detecting Network Anomalies". IEEE, 2008.
[7] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez,"Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28,2009.
[8] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," IEEE/ACM Trans.Networking, vol. 19, Apr. 2011.
[9] W. Wang, X. Zhang, S. Gombault, and S.J. Knapskog, "Attribute Normalization in Network Intrusion Detection," Proc. 10th Int'l Symp. Pervasive Systems, Algorithms, and Networks ,2009.
[10] K. Lee, J. Kim, K.H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, 2008.

