International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

ANOMALY BASED MECHANISM FOR DETECTING DENIAL OF SERVICE ATTACK USING TRIANGLE AREA TECHNIQUE

SUSHMA A[1], SMEJA K[2]

[1]M.Tech Student, Department of Computer Science & Engineering, Visvesvaraya Technological University,Belgaum, Karnataka, India

[2]Assistant Professor, Department of Computer Science & Engineering, Visvesvaraya Technological University,Belgaum, Karnataka, India

Article Received: 11/03/2015 | Article Revised on; 15 /03/2015 | Article Accepted on:19/03/2015

SUSHMA A

ABSTRACT

In this paper, we propose a mechanism which is based on anomaly based detection of denial of service (DoS) attack using triangle area technique. The aspire of DoS attack is to send a enormous number of messages to the server so that it can be worn-out or not be capable to full fill the legitimate users request. It will be implementing by using Multivariate Correlation analysis approach. It is much better than misuse based detection system. It does not need the information of historic traffic study and is not susceptible to linear modification of all features. In this first we are making to by considering a router and number of nodes from client to server, and from these nodes and router only transforming the packets to the specified server. In this mechanism a threshold based classifier is used to differentiate normal traffic from dos attack based on the consumption of the bandwidth by a malicious node in the network. The performance of our proposed system is evaluated based on high detection speed when compared to other techniques and also tells the bandwidth consumption in attack and normal traffic.

Keywords— *Denial of service attack, triangle area technique, anomaly based detection, intrusion detection system, network traffic.*

I. INTRODUCTION

Organizations that depend on the internet for their trade needs constant and rapid response to their client request. Usually internet will always be under failure. This failure may be unintended or intended. Denial of Service (DoS) is one of the intended attack which is impulse of attacking the target's computer or any other resources that use internet. The DoS attacks aim the service accessibility should disallow the authorized users from accessing the services. It can be divided into two types. Bandwidth flooding and Resource flooding. In bandwidth flooding, Intruder avoids the legitimate User's request to reach the network by overflowing the network with huge request and In resource flooding the resources get busy by attackers which results in services to legitimate users is not available by the target machines. In both condition DoS degrades the availability of services/resources that has to be given to the legitimate user.

The attacks which are related to denial of service are smurf, teardrop, Neptune, land, pod, and back [1]. In smurf attack, attacker spoofs the host's ip address and

sends huge amount of request to victim. In teardrop attack, attacker tries to send fragmented packets to target machine. In Neptune attack, the attacker sends session establishment message to host with similar ip address as source. Host waits until acknowledgement is received. So that it is unavailable to valid network. In land attack, attacker sends forged message to host and makes it busy in replying to its request. In pod attack, attacker sends an oversized packet. In back attack, attacker forges ip address with ip packets.

The dos attack detection system which is proposed in this paper is based on the theory of multivariate correlation approach where correlation between two different features is extracted and anomaly based detection which is used to detect all known and unknown attack. These two approaches helps in accurate discrimination of normal and attack traffic behaviors. To speed up the detection process triangle area technique is used which takes geometrical correlation between each network features.

II. LITERATURE SURVEY

As Denial of service attack is increasing day by day and makes the availability of service to deny from actual users. Many techniques are developed to detect denial of service attack. Some methods involve misuse based detection systems and some methods involve anomaly-based detection systems. Anomaly based detection system is one which monitors the network activates and identifies divergence from legitimate traffic profiles.

In an adaptive sampling algorithm with applications to denial-of-service attack detection [2] by *Animesh Patcha and Jung-Min Park*, it uses weighted least squares prediction to select the next sampling interval. This sampling approach is adapted to enhance the capability of detecting denial-of- service (DoS) attacks. It reduces the amount of data that would be evaluated by IDS and also eliminates redundant characteristic of network traffic by normalization technique. A key element in adaptive sampling is to adjust the sampling rate based on the observed sampled data and making predictions of future behavior based on the observed samples. An inaccurate prediction specifies a change in the network traffic behavior. But this approach uses previous samples to estimate or predict a future measurement.

Fast entropy computation method [3] by *Giseop No and Ilkyeun Ra, Denver*, to detect dos attack tells that the compression entropy method is not suitable for validating real network attacks and creates many false negatives. But proposed fast entropy approach that can overcome the problem of false negatives and will not increase the computational time. This DoS attack detection method considerably increases detection accuracy and decreases computational time using fast entropy approach which has better performance in speed as well as accuracy. But this fast entropy computation method doesn't reduce the false positives and false negative rate much.

Bro: A system for detecting network intruders in real-time [4] by *V. Paxsonis*, is an individual system for detecting network intruders in real-time by reflexively monitoring a network connection over which the intruder's traffic travels. It involves two principles. Event engine and policy script interpreter. In event engine the series of higher level events are normalized by a kernel filtered network traffic stream. And in policy script interpreter, event handlers which are written in a specialized language used to express a site's security policy are interpreted. Event handlers can update state information, synthesize new events, record information to disk, and generate real-time notifications via syslog. But this BRO technique does not monitor actively terminating misbehaving connections by sending RST packets to their end points. And it does not monitor the communication with intermediary routers. This system does not balance both security and openness.

Collaborative detection of DoS attacks over multiple network domains [5] by *Yu Chen, Kai Hwang, and Wei-Shinn Ku*, is one more approach to detect DoS flooding attacks at the traffic flow level. In this, change aggregation tree (CAT) is developed by distributed change-point detection (DCD) architecture. The detection of unexpected traffic changes over multiple network domains at the earliest time is incorporated. To aggregate the flooding alerts reported by the routers each ISP domain has a CAT server. CAT domain servers are collaborated to make the final decision. A new secure infrastructure protocol (SIP) is developed to resolve policy conflicts at different ISP domains. The global CAT tree detects the network anomalies acquired on the fly. In this approach to support global CAT tree, construction across multiple domains and SIP (Secure

Infrastructure Protocol) is proposed. But to implement CAT mechanism and SIP protocol it requires the integration of signature based IDS with anomaly detection system which is a labor intensive task.

Contributions in our solution are highlighted as follows. Denial of service attack detection is done based on anomaly based detection mechanism using triangle area technique which takes geometrical correlation of two or more network traffic features. Multivariate Correlation Analysis (MCA) [6] is adopted to find correlative information between the features within an observed data object (traffic record). Threshold-based attack detector is used to detect normal and attack network traffic. Here the detection is considered on two factors. Based on bandwidth consumption by a node and based on the number of packets sent to the server. Our proposed approach gives best result in detecting denial of service attack.

Objective of the proposed solution is highlighted as follows.

- Triangle area based MCA approach is a non-payload based DOS detection approach.
- Our proposed technique does not require the knowledge of historic traffic analysis.
- This method is not vulnerable to linear change of all features.
- This approach provides an efficient characterization for individual network traffic records.
- It provides low false positive rates, minimum delay in response and high quality of services.
- Our proposed approach improves the detection accuracy

III. SYSTEM ARCHITECTURE

The complete overview of our proposed DoS attack detection system architecture is explained in this section. It will describe the detection of dos attack with triangle area technique and multivariate correlation analysis which is based on anomaly based detection mechanism. The whole detection process consists of three major modules. Basic feature generation, Triangle Area Map (TAM) generation, and attack detection module.

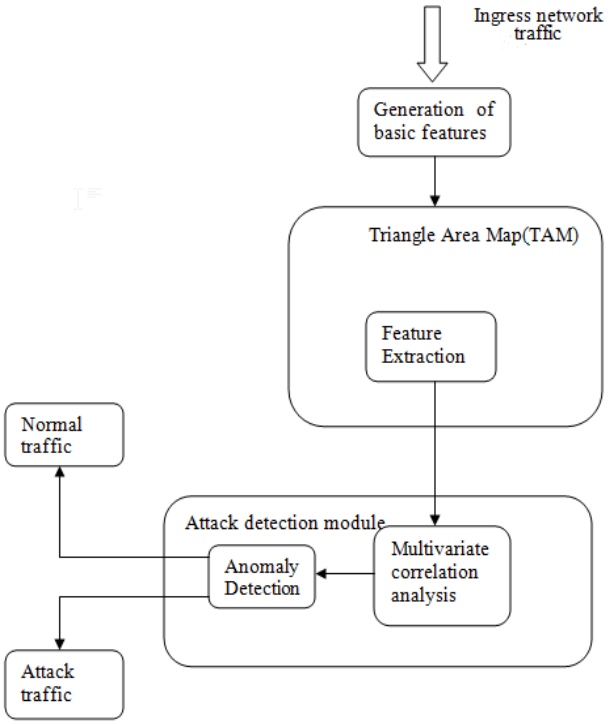

Fig. 1. System Architecture

Fig. 1 shows the complete system architecture. Each module description is as follows.

Basic feature generation: In this module the basic features are generated from network traffic only. We created network which consists of a client, router, intermediate nodes, and a server. When client wants to send request to server, first he searches a router and sends to the router. Router sends this particular request to intermediate node and node will transfer request to server. Here basic features of the network are generated once network connection is established.

Triangle Area Map (TAM) generation: In this module feature extraction approach is used. Feature extraction module estimates the selected features from feature set which are generated in basic feature generation module. These features can be used to recognize and classify incoming attack packets and will be analyzed in Correlation analysis step. Our Experiments shows that these features include considerable information related to the presence of a DoS attack. Extracted features involve source ip address, destination ip address, port number, number of requests (packets), time interval, bandwidth consumption, and action. Source and destination ip address indicates client and server ip address, port number includes port number of client, router, nodes, and server. Number of request indicates amount of packets sent to server both in normal and

attack mode. Time interval indicates client got response from server, Bandwidth consumption indicates the amount of bandwidth which is required by node in both cases. Finally the extracted features are stored in Triangle area map (TAM). Triangle area technique is used to correlate extracted features because occurrence of network intrusions makes changes to these correlations so that the changes can be used as indicators to identify the attacking behavior.

Attack detection: In this module Multivariate analysis approach is used to analyze the features which are stored in TAM. Attack detection is based on mahalanobis distance algorithm. Threshold based classifier is used in this module to differentiate normal traffic from attack traffic. This is applied for bandwidth consumption of the node to transfer request to server which is sent by client. If bandwidth consumption of a node exceeds the threshold it is considered as attack traffic or else normal one. Other factors such as number of request to send, and time interval are also used discriminate normal or attack traffic. Our proposed system also detects the malicious node by anomaly detection in this module.

IV. SIMULATION SETUP AND RESULTS

In this paper for experimental purposes, we used eclipse java simulator tool. The implementation is done using Java Swing and Java programming language. Java Swing provides a very well-engineered, flexible, powerful GUI tool kit. JFreeChart is used for performance evaluation graph. It is a free Java chart library that makes it easy to display professional quality charts in their applications.

Table. I shows the results of the Feature Extraction Module process and attack detection process. In this, client ip address, destination ip address, port number, number of requests (packets), time interval, bandwidth consumption, and action features are extracted. But features such as number of request, bandwidth consumption, and time interval are considered to determine the attack detection process. In normal case of attack detection process the number of request sent to server by client is 1. But in attack mode the number of request reached to server is 30. So in normal mode the consumption of bandwidth is less when compared to attack mode because malicious node simply sends large number of request to server and requires more bandwidth than in normal case. The time taken to send response to the client by server in normal mode is less than the attack mode because in normal mode client is sending only one request to server and server processes the request quickly and sends response.

TABLE I: Extracted Features

Client IP address	12.23.128.110	12.23.128.110
Server IP address	23.44.67.1	23.44.67.1
Router IP address	69.1.1.13	69.1.1.13
Node IP address	38.120.120.5	38.120.120.5
Client port number	5353	5353
Server port number	6091	6091
Router port number	4123	4123
Node port number	2236	2236
Number of request	1	30
Bandwidth consumption	210kbps	689kbps
Time interval	2 min	10 min
Action	Normal	Attack

In case of attack mode, server gets large amount of requests to process from malicious node. Client waits for a long time and gets service unavailable. So by correlating these features it differentiates the attack traffic from normal one.

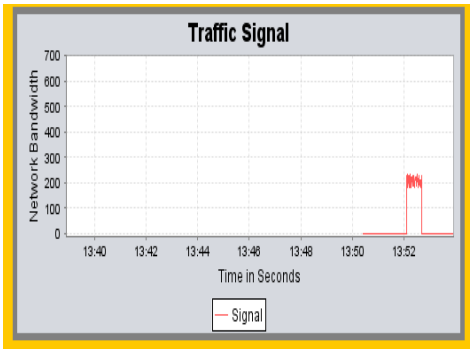

Fig. 2. Bandwidth consumption in Normal case

Fig. 2 represents the bandwidth consumption by a node in normal mode. In this a threshold based classifier is used. In normal case server gets only few

requests to response and does not require maximum bandwidth by node to transmit to server. This bandwidth consumption is less than the threshold. So it is considered as normal traffic. Time taken to process the request from server is also less in normal mode which is shown along with time axis.

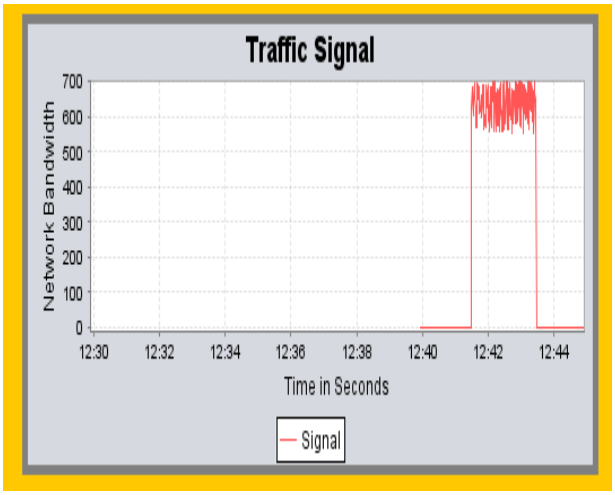

Fig. 3. Bandwidth consumption in Attack case

Fig.3 represents the bandwidth consumption by an intruder node in attack mode. In this also a threshold based classifier is used. In attack case server gets large number of requests from intruder node to response. So maximum bandwidth is required by intruder node to transmit large number of request to server and consumes more bandwidth. This bandwidth consumption by an intruder node is greater than the threshold. So it is considered as attack traffic. Time taken to process the request from server is also high in attack mode because server will become busy in processing the request which is coming from intruder node. So in attack case an intruder degrades the availability of server to legitimate user.

V. CONCLUSION

In this paper, we developed new approach to detect denial of service attack using triangle area technique based on anomaly based detection. It is implemented by Multivariate Correlation analysis approach. In this mechanism a threshold based classifier is used to differentiate normal traffic from dos attack based on the consumption of the bandwidth from a malicious node in the network. The performance of our proposed system is evaluated based on threshold classifier. Our performance evaluation results show that our proposed approach gives high detection speed within seconds when compared to other techniques and also gives comparison of the bandwidth consumption by a node in attack and normal traffic and gives more accurate detection of DoS attack.

REFERENCES

[1] *Adrian Brindley*, "Denial of Service Attacks and the Emergence of Intrusion Prevention Systems", *SANS GSEC* Practical Assignment v1.4b, November 1, 2002.

[2] *Animesh Patcha and Jung-Min Park*, "An Adaptive Sampling Algorithm with Applications to Denial-of-Service Attack Detection" ISCIT 2009.

[3] *Giseop and Ilkyeun Ra*, "An Efficient and Reliable DDoS Attack Detection Using a Fast Entropy Computation Method" ISCIT 2009.

[4] *Paxson*, "Bro: A System for Detecting Network Intruders in Real-Time Computer Networks", vol. 31, pp. 2435-2463, 1999.

[5] *Yu Chen, Kai Hwang, and Wei-Shinn Ku*, "Collaborative Detection of DDoS Attacks over Multiple Network Domains parallel and distributed systems", TPDS-0228-08061.

[6] *Zhiyuan Tan, Aruna Jamdagni, Xiangjian Priyadarsi Nanda, Ren Ping Liu,Harish Kumar Kaura*, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", parallel and distributed systems, vol:25 No:2 Year 2011.