DoS Attack Detect Framework Based on Multivariate Correlation analysis

Miss Kanchan D. Sherkar[1], Mr. Sandip A. Kahate[2].

[1] *Student ME(II),Computer Engineering, SPCOE, Maharashtra, India*
[2] *Assistant Prof., Computer Engineering, SPCOE, Maharashtra, India*

ABSTRACT

A Denial-of-Service (DoS) attack is an intrusive attempt, which aims to force a designated resource to be unavailable to its intended users. This attack is launched either by vulnerabilities of a victim (e.g., a host, a router, or an entire network) or by flooding a victim with large volume of useless network traffic. Since 1990s, DoS attacks have emerged as a type of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services. In this paper describe Multivariate Correlation analysis (MCA) .It is an intelligent and effective solution for DoS attack detection that use for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. MCA based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. Multivariate Correlation Analysis approaches are proposed based on two techniques, namely Euclidean distance and triangle area. These two proposed MCA approaches provide accurate description for network traffic records.

Keyword: - *DoS Attack, Multivariate Correlation, Anomaly-based detection, Triangle area.*

1. 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 Trinoo (Dittrich 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. 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. Compared with conventional DoS attacks that could be addressed by better securing service systems or prohibiting unauthorized remote or local access, DDoS attacks are more complex and harder to prevent. Since many unwitting hosts are involved in DDoS attacks, it is challenging to distinguish the attacking hosts and take reaction against them. In recent years, DDoS attacks have increased in frequency, sophistication and severity due to the fact that computer vulnerabilities are increasing fast (CERT 2006, Houle *et al.* 2001), which enable attackers to break into and install various attacking tools in many computers. Wireless networks also suffer from DoS attacks because mobile nodes (such as laptops, cell phones, etc.) share the same physical media

for transmitting and receiving signals; and mobile computing resources (such as bandwidth, CPU and power) are usually more constrained than those available to wired nodes. In a wireless network, a single attacker can easily forge, modify or inject packets to disrupt connections between legitimate mobile nodes and cause DoS effects. In this article, we will provide an overview on existing DoS attacks and major defense

2. LITERATURE REVIEW

In [1], the authors, Pelechrinis K, Iliofotou M and Krishnamurthy S V, University of California have surveyed the various types of denial of service attacks and the performance issues due to the DoS attack in each network. They have provided several intrusion detection techniques in their survey and have mentioned that there must be system implementation to avoid real world adversaries. In all of the jamming techniques and the detection algorithms, throughput is 0 which effectively reduces the performance of the network.
In [2], data forwarding without any delay in the defending jamming in a wireless sensor network is proposed. This proposal consists of sensor nodes as clusters for a particular frequency. Here when a frequency where data forwarding occurs is jammed, the cluster of sensor nodes in that frequency becomes inoperative and the other clusters act as backup.
A covariance matrix based approach was designed in [3] to mine the multivariate correlation for sequential samples. Although the approach improves detection accuracy, it is vulnerable to attacks that linearly change all monitored features.

3. SYSTEM DESIGN

The detailed description of detection mechanism of DoS attack is given in this section, where the system architecture are discussed.

3.1 SYSTEM ARCHITECTURE

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work.

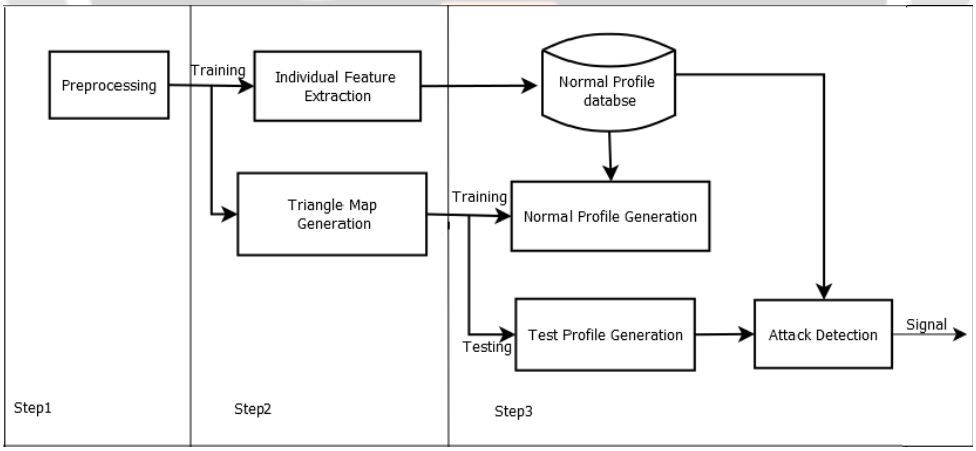

Fig -1: SYSTEM ARCHITECTURE

The detection mechanism consists of three steps as shown in Fig. 1. In Step 1 basic features are generated from network traffic packets captured at the destination network. These feature describes traffic properties at well-defined time interval. These records are preprocessed so that it can be used for further processing and this may include normalization of traffic data. The second step consist of extracting the normal behavior of traffic by monitoring individual features and the relationship between the features. The monitoring individual feature helps us to understand range values of feature in normal conditions. These values are used as normal profile of a traffic and stored in database. The relationship between features also provide strong method of generating normal profile this is called as Multivariate Correlation Analysis. This MCA is define using the Triangle Map Generation module The

intrusions cause changes to these correlations so this changes can be used as indicators to identify the intrusive activities. These correlation feature are stored in Triangle Area Maps(TAMs). The individual feature profile with correlation feature profile is used to represent the normal traffic record. This generated normal profile used to sort out the legitimate and illegitimate traffic records.[4] The third stage consist of monitoring traffic for anomaly. The prepossessed traffic record is given for determining abnormality in individual feature which are monitored and the abnormality in their relationship with other traffic features. These values are compared with the normal profile database and if there is anomalous behaviour seen in both individual features values and correlation values.

4. DETECTION MECHANISM

In this section, a threshold-based anomaly detector was proposed in this whose normal profiles are created using legitimate network traffic records and used for future comparisons with new incoming traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector [5]. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labelled as a legitimate traffic record. So, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. [6] A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed triangle area- based MCA approach to analyse legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

4.1 MULTIVARIATE CORRELATION ANALYSIS APPROACH

The MCA approach is developed based on triangle area map technique,[7] which is used to present the correlations within network traffic data. The occurrence of DoS attacks causes the change of the network traffic behaviour, which in turn affects the correlations. Thus, the correlations can help indicate the suspicious change of the network traffic behaviour. These correlations are extracted from the basic statistical properties (e.g., the number of data bytes from source to destination, the length of a connection and the number of connections to the same host as the current connection in the past two seconds etc.) of the network traffic flows in a prompt fashion. The extracted correlations give accurate descriptions to the behaviours of various types of network traffic. The description vectors representing network traffic records are constructed using these newly extracted correlations of the respective traffic records.

4.2 Normal Profile Generation

Assume there is a set of g legitimate training traffic records Xnormal = {xnormal 1, xnormal 2, …, xnormal g}.The triangle-area-based MCA approach is applied to analyse the records. The generated lower triangles of the TAMs of the set of g legitimate training traffic records are denoted by Xnormal TAMlower ={TAMnormal,1 lower, TAMnormal,2 lower , · ·· , TAMnormal,g lower }. Mahalanobis Distance (MD) is adopted to measure the dissimilarity between traffic records. This is because MD has been successfully and widely used in cluster analysis, classification and multivariate outlier detection techniques.[7]

4.2 ATTACK DETECTION

To detect DoS attacks, the lower triangle (TAMobservedlower) of the TAM of an observed record needs to be generated using the triangle-area-based MCA mechanism and individual monitored features needs to be extracted [7]. Then, the MD between the TAMobserved lower and the TAMnormal lower stored in the respective pre-generated normal profile NormPro is computed and abnormality in individual feature is checked by comparing with normal profile of feature.

5. CONCLUSIONS

This paper has presented a DoS attack detection system that uses Multivariate correlation analysis based technique and individual feature characteristic to flag traffic as anomalous. The MCA mechanism extracts the geometrical relationships between individual features within each network traffic record, and offers more accurate characterization for network traffic behaviour, correspondingly individual features characteristic are calculated. Evaluation has been conducted using KDD Cup 99 dataset to verify the effectiveness and performance of the DoS attack detection system. The influence of original (non-normalized) and normalized data has been studied in this paper.

ACKNOWLEDGEMENT

We would like to thank Prof. Gumaste S.V.(H.O.D. Computer Department) for his continuous help and generous assistance. He helped in a broad range of issues from giving us direction. We would like to thank our colleagues who helped us time to time from preparing paper and giving good suggestions. We also extend sincere thanks to all the staff members of Department of Computer Engineering for helping us in various aspects.

REFERENCES

[1]. Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy(2011), "Denial of Service Attacks in Wireless Networks:The Case of Jammers" Communications Surveys & Tutorials, IEEE, vol 13: issue:2, nos 245-257.

[2]. Proano, A.; Lazos, L.;(2011) "Packet-Hiding Methods for Preventing Selective Jamming Attacks" Dependable and Secure Computing, IEEE, vol. 9 issue 1. Nos 101- 114.

[3]. C. F. Tsai and C. Y. Lin, A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection, Pattern Recognition, vol. 43, pp. 222-229, 2010.

[4]. P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, Anomaly-based Network Intrusion Detection: Techniques, Systems and ChallengesComputers Security, vol. 28, pp. 18-28, 2009.

[5] Gautam Thatte,Urbashi Mitra,John Heidemann.[8] Parametric Methods for Anomaly Detection in Aggregate Traffic

[6] V.Paxson, Bro:A System for Detecting Network Intruders in Real time computer Networks, vol 31, pp.2435-2463,1999.

[7]. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He,Priyadarsi Nanda,Ren Ping Liu.A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis .