Design and Implementation of Intrusion Detection System (IDS) for Detecting Denial- of-Service in Wireless Network

Preetha M
4th Semester, M.Tech
Dept. of CS&E
SJM Institute of Technology
Chitradurga, India

Aravinda T V
Professor, Dept. Of Cs&E
SJM Institute of Technology
Chitradurga, India

Nagabhushan
Professor, Dept. Of Cs&E
SJM Institute of Technology
Chitradurga, India

Abstract: **A denial-of-service (DoS) attack is denying of network based services to its intended users or making an attempt to prevent the availability of resources (e.g., network bandwidth, memory or CPU processing time) and machine to its legitimate users and it is most prevalent attack. One common method of DoS attack involves saturating the target machine with external communication requests, such that it cannot respond to its legitimate traffic or responds so slowly that rendered resources are effectively unavailable. Building strategy or technology to handle this type of attack is the main ambition of this paper. In this paper, first we propose a complete framework of DoS detection system and then we present a Multivariate Correlation Analysis (MCA) technique, that make use the principle of anomaly-based detection system for detecting DoS attack.**

Keywords: Denial-of-Service (DoS), legitimate, Intrusion Detection System (IDS), Multivariate Correlations

1 INTRODUCTION

. The major and serious attack that affects the current computer networks in the modernized group of interconnected systems is Denial of Service Attack (DOS). Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in adhoc network is DoS attack. A DoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DoS attack is flagged by sending huge amount of packets to the destination node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and will not allows any other important packets reached to the victim DoS is an attack on a computer network, it will forcefully stop network from running, not used to gain unauthorized entry, just to mess it up, user or organization is deprived of ervices that are usually expected, destroy the network's usability and make it unable to function properly. Denial-of-Service(DoS) attacks are one type of most aggresive and prevalent behavior to online servers. It cause serious impact on the interconnected systems like Database servers, Web server, Cloud Computing server etc. DoS attacks severly make unavailability to the victim, (e.g., node, router, system, or entire network) . In earlier days local attackers use DOS attack for attacking one particular system by stopping the network from running or denying all the messages or network communication they get. The attacker wants to get control and information of an interrelated channel through performance of DOS attack against the person who possesses the channel. As the attacker gets control over popular websites they could not be recognized by the underlying community people. As the basic DOS attack codes or tools are available from internet even normal computer users can use these codes well and become a DOS attacker. The main aspiration of DoS attack is to disrupt or block the network connections between the two machines and there by preventing access to service, and DoS attack attempt to prevent the service to the indivisual or particular system. DoS attack can essentially make your system or network disable. Depending on the type of enterprise, the DoS attack will essentially may disable your organization. DoS attacks can occur in variety of forms and aim to variety of services. DoS attacks are mainly categorized into three types, consumption of limited resources, distruction/alteration of configuration items and physical alteration of network components. The DoS attacks can be executed within a limited resource against large sophisticated site, this type of an attack is called asymmetric attack, for eg, an attack with old PC and slow modem may essentially disable the fast network. The emergence of the Internet as a communication tool and the growth of network technologies in accessing critical information in real-time manner raise cyber offense cases as the attacker's interest on this valuable information radically increased the amount of cyber attacks. All these activities are identified by the Intrusion Detection System (IDS) that diminish security and privacy either in network or in computer system surroundings. IDS can be classified into two categories, namely misuse-based detection system or signature-based detection (SBD) and anomaly-based detection system (ABD).

II PROBLEM DEFINATION

The main objective of the DoS attack is to consume limited, scarce and non-renewable resources (e.g., CPU processing time, network bandwidth, memory) and making these resources unavailable to its legitimate users by making an attempt to prevent or disrupting network communication between the two machines or by denying access to services.

III OBJECCTIVE OF THE SYSTEM

The main objectives of the system are:

- First, we propose a complete framework for the DoS attack detection system
- Propose an algorithm for normal profile generation and detection system respectively
- Design a network intrusion detection system that achieves high detection accuracy and with stand zero attacks

IV RELATED WORK

Many system and techniques are used to detect the Dos attack efficiently. Garcia describes by using Gaussian mixture model, they find the irregular packets in the network to identify the intrusion discovery in the system.

Vern Paxson developed a system called “Bro” a system for finding a network attacker in real time. It is a standalone system, which emphasizes high speed monitoring, real time, clear separation to achieve this Bro system.

Warusia Yassin, Nur Izara Uder, Zaiton Muda and Md. Nasir Sulaima explained anomaly- based detection through K-means clustering and naives bayes classification

J.Welkin eyes, S. Karthirem and E. Thanagadurai explained detecting the Denial-of- Service attack based on multivariate correlation that employs the principle of anomaly-based technique, which provides high accuracy

Zhiyuan Tan has excellently explained about detection of Denial-of-Service attack based on computer vision technique and he also used multivariate correlation analysis technique based on triangle area map and Euclidean distance

Theerasak explain about Dos attack is carried out by attack tools like worms, botnet and also the various forms of attacks packets to beat the defense system, so they propose a technique called “Behavior based Detection ” that can discriminate Dos attack traffic from real method.

The above method is comparable detection method; it can extract the repeatable features of packets arrival. The Behavior Based Detection can differentiate traffic of an attack sources from legitimate traffic work with a quick response. The resulting performance so far is good enough to protect the server from crashing during a DoS attack.

V SYSTEM DESIGN

Software requirements and specification find their reflection in design system. The following section outlines proposed solution

A Architecture

The overview of architecture is given in this section, where system framework sample-by-sample detection and MCA based detection techniques are discussed.

Architecture is an overall structure of a system. It deals with the overall working of the system. The design process for identifying the sub- systems making up a system and the framework for sub-system control and communication is architectural design. Figure shows depict the architecture of proposed Denial-of-Service detection system.

The proposed detection system for detecting DoS attack mainly consists of three main steps as shown in Figure 2.1

Step1: Generation of basic features for individual records

The basic features are generated from network traffic to the network where protected servers and Intrusion detection system (IDSs), IDSs is not a separate module, it will be in the server only and it is one of the functionality of the sever, and these IDSs and server reside internal and are used to form traffic records for a well-marked time period. Observing and analyzing at the destination network, it will breach the overhead of detecting serious and prevalent activities by concentrating only on related inbounded traffic. This will also allow our detection system to give best protection and privacy which is the fit for the targeted internal network because legitimate traffic profiles used by the detection system are developed for a smaller number of network services (e.g., to transfer the file by the server, which is requested by the user and in some cases server serves an intermediate node, when there is no connection between source and destination, it will send the data in the form of packets and here there will be receiver perception rate and some users will send more packets intentionally,

because to degrade the performance of the system, that time load will be more on server and it will fail to give services)

Step2: Multivariate Correlation Analysis

In this step, the detailed process of novel Multivariate Correlation Analysis (MCA) is proposed. The MCA technique plays a vital role in detecting DoS attacks. The proposed model employs Triangle Area Map module to extract the geometrical correlation between two unique features within individual observed data object (i.e., traffic record) either from step1 (i.e., raw/original features are generated for each record) or from normalized traffic record in this step (i.e., step2). For accurate and complete analysis, permutation of any two unique features within each record should be computed. The network attacks/intrusions that have been occurred can cause changes to the extracted correlation and the caused changes can be used as labels to detect the network intrusive attack/activities. All extracted geometrical correlations, namely triangle areas, which is stored in triangle area map (TAMs), are then used to replace the original/raw features or normalized feature to represent the traffic record. These triangle areas differentiate between known and unknown traffic records.

Basic features or the standardized features to represent the traffic report. This provides higher discriminative and detailed information to differentiate between legitimate and illegal traffic reports. Our MCA method is explained in further sections

Step3: Decision Making

The generated TAMs are used in this step. Anomaly- based detection (ABD) system is used in this step. This detection system overcomes the disadvantages of misuse-based detection system, such as ABD does not require any manual work and no frequent update of the database. Thus, ABD system detect unknown attacks more precisely and also ABD system does not require any previous knowledge or history of attacks for detecting attacks and moreover, this system requires no network security expertise. A relevant algorithm is used in this step and it is explained in section 6 and 7.

This step consists of two main phases:

- Training phase and
- Test phase

In the training phase Normal Profile Generation Module is used and normal profiles are generated by observing different types of legitimate traffic records and generated profiles are stored in the database

In the test phase Tested Profiles are operated to build profiles for the observed traffic record and this is handover to the “Attack Detection” module, which compare and evaluate the individual generated and stored normal profiles with tested profile. This module uses the threshold classifier to distinguish

between DoS attack and normal legitimate traffic record.

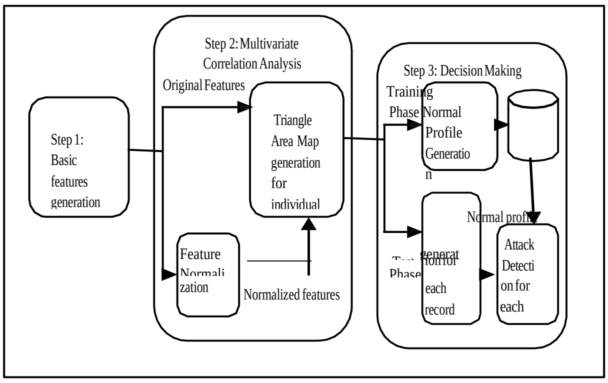

Figure 5: Process of Multivariate Correlation Analysis and Decision Making

B Sample-by-sample detection

The group-based detection mechanism monitors traffic records as groups such that any attack detector designed based on this mechanism can only label the traffic records within a group as attack records or normal traffic records entirely more accurately than sample-by-sample method. The above advantage of group-based detection system is restricted to some situations, because the tested samples in a group belongs to the same distribution. It is very difficult to predict the traffic in general, which belongs to the same distribution. To overcome the above disadvantage, our system in this paper monitors traffic samples individually in a group. This application is not available in group-based detection system.

VI MULTIVARIATE CORRELATION ANALYSIS

Multivariate correlation analysis has been a rising trend in the research areas of network intrusion detection. Recent studies on feature correlation analysis have gained progresses and helped improve the accuracy of attack detection. Various kinds of analysis techniques were introduced by these early research works to the task of multivariate correlation extraction. These analysis techniques are systematically classified into two different categories (i.e., the payload-based analysis techniques and the flow-based analysis techniques) with respective to the types of objects, which they are intended to study. These correlations are extracted from the basic statistical properties (e.g., the number of packets send from source to destination, time taken to forward the packets, 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 behaviors 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. The details are shown in the following section.

VII ALGORITHM FOR DETECTING INTRUDER

network through a self-organized, fully distributed and localized procedure. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks. To be part of the future work, we can use classification techniques to reduce false positive rate and increase the detection accuracy and performance of the system.

Step 1: Here Users and Service Provider is ready for Communication.
Step 2: User is send request to connect to service Provider and wait for connection to get.
Step 3: Service Provider System is receives Request from User and Process and send Result to User.

Figure : Algorithm for User And Service Provider Interaction

Intrusion Detection System is implemented in The Service Provider System itself.

.

Step 1: User node Is Send request to Service Provider and wait for response from Service Provider.
Step 2: If Attacker Node, attacks the service Provider which make Server work down.

Figure : Algorithm for Service Provider and Intruder Detector

VIII RESULTS AND DISCUSSIONS

The Denial-of-Service attack is identified and detected by Intrusion detection system (IDS).This functional module (IDS) will detect DoS attack through two services one is through by transferring the files and another through by acting as intermediate node between source and destination, only when source and destination nodes are not actively communicating, it will transfer the data files in terms of packets

IX CONCLUSION AND FUTURE WORK

The results demonstrate that the presence of a DOS increases the packet loss in the network considerably. The proposed mechanism protects the

ACKNOWLEDGEMENT

I consider it as a privilege to express my gratitude and respect to all those who guided me in completion of paper work. I extend my sincere and heart full thanks to Dr. Aravinda T V **M.Tech, Ph.D•,** Professor, Dept. of Computer Science & Engineering, SJM Institute of Technology, Chitradurga for providing the right ambience and constant inspiration and support for carrying out this paper work successfully. I profoundly indebted to, Dr. Nagabhushan **M.Tech.,Ph.D.,** HOD, Department of Computer Science & Engineering**,** SJM Institute of Technology, Chitradurga for innumerable acts of timely advice, encouragement and I sincerely express my gratitude to him. I express my immense pleasure and thankfulness to all Teaching and Non- Teaching Staff of the Department, Computer Science & Engineering.

REFERENCES

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

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vazquez, “Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,” Computers & Security, vol. 28, pp. 18-28, 2009.

[3] D. E. Denning, “An Intrusion-detection Model,” IEEE Transactions on Software Engineering, pp. 222-232, 1987.

[4] 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, no. 3, pp. 1659-1665, 2008.

[5] Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion detection using fuzzy association rules,” Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic flooding attack detection with SNMP MIB using SVM,” Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[7] W. Hu, W. Hu, and S. Maybank, “AdaBoost-Based Algorithm for Network Intrusion Detection,” Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[8] Weiming Hu, Wei Hu, and S. Maybank, AdaBoost- Based Algorithm for Network Intrusion Detection, Trans. Sys. Man Cyber. Part B **38** (2008), no. 2, 577– 583.

[9] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, and Sehun Kim, DDoS attack detection method using cluster analysis, Expert Systems with Applications **34** (2008), no. 3, 1659 – 1665.

[10] Arman Tajbakhsh, Mohammad Rahmati, and Abdolreza Mirzaei, Intrusion detection using fuzzy association rules, Applied Soft Computing **9** (2009), no. 2, 462 – 469.