Denial-of-Service Attack Detection Using Anomaly with Misuse Based Method

R. Suganya
Student ME, Department of Computer Science and Engineering P.A. College of Engineering and Technology, Pollachi, Tamilnadu, India

Abstract-
Denial-of-Service attack is an attempt to make a system, machine or network resources unavailable to its user by blocking or denying the services. The Denial-of-Service attack is identified with the help of detection algorithm. The anomaly detection mechanism not provides the better results so the user need to implement the hybrid detection algorithm which is the combination of anomaly detection with misuse based detection. The new techniques have the advantage of reduce the false alarm rate and improve the detection rate. The detection technique use time as a parameter to detect the intrusions. Denial-of-Service attack detection system that uses Multivariate Correlation Analysis for accurate network traffic characterization by extracting the correlations between network traffic features and increase the speedup of the process.

Index Terms-
Denial-of-Service attack, Anomaly detection, Misuse based detection, Hybrid detection, Multivariate Correlation Analysis.

1. Introduction

Network security is used to provide the security to the network that is freedom from risk or danger. Network security provides authorization to access the data that is controlled by the network administrator. It must ensure the following things. In confidentiality, only sender and receiver must understand the message by encryption and decryption process. In authentication, sender and receiver want to confirm the identity of each other. In integrity sender, receiver want to ensure the message not altered before transmission or after receives the message. In access and availability all the services that are provided by the system must be accessible and available to the users.

A. Intrusion Detection System

Intrusion Detection System (IDS) is a security mechanism used to detect the attack with the aim of preserving system from large damages and identify the vulnerabilities and give warning if unauthorized user enters into the system [12].
Intrusion detection technique can be categorized into two types Misuse based detection and Anomaly based detection [9] [10]. The combination of two detection method called as hybrid detection.

Manuscript received April 5, 2016
Manuscript revised April 20, 2016

Misuse based detection also called as signature based detection that misuse-based detection attempts to detect attacks by monitoring network activities and looking for matches with the existing attack signatures or rules [13]. Disadvantages of misuse based detection is to have high detection rates to known attacks and low false positive rates, systems using misuse based detection methods are easily escaped from any new attacks and slight modification in the existing attacks. It is a complicated and labor intensive task to keep signature database updating so overcome the disadvantage of misuse based detection the anomaly detection technique was introduced. Anomaly detection technique is used to detect both known and unknown attack by learning the pattern of legitimate network traffic [13]. The action that is significantly deviates from normal the normal behavior is considered as an intrusion. The intruder may be from outside the network or legitimate user of the network. Anomaly detection is better compared to the misuse based detection.

2. Related Work

Recent studies focused on Denial of service attack detection. D. E. Denning proposed an efficient methodology called statistical model that detect the DoS attack in an efficient manner [1]. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. Then S. T. Sarasamma et al. solved the problem of implementing individual page fault in a practical manner and also considered the problem of data leakage. Multilevel hierarchical Kohonen Net for an intrusion detection system is presented [5]. Each level of the hierarchical map is modeled as a simple winner-take-all K-map. Advantage of this multilevel hierarchical K-Map is its computational efficiency and the reduced network size.
C. Yu et al. introduced collaborative detection method for detecting intrusion [6]. The new defense system is suitable for efficient implementation over the core networks operated by Internet service provider. S. Jin et al. proposed covariance matrix based approach to improve

the detection accuracy compared to other various methods previously available in the practical. The covariance matrices of sequential samples used to detect multiple network attacks and also it constructs a covariance feature space where the correlation differences among sequential samples are evaluated. Then, W. Hu and S. Maybank introduced Adaboost Algorithm for reducing false alarm rate and improve the detection accuracy [10]. Due to the variety of network behaviors and the quick development of attack that is important to develop fast machine-learning-based algorithms with high detection rates and low false-alarm rates.

K. Lee et al. considered cluster analysis is easy to implement and it detect the attack in the early phase. After that, perform cluster analysis for proactive detection of the attack [8]. The disadvantage of this method is not suitable for extracting more variables. P. Garcia et al. introduced various techniques, system and challenges for Anomaly intrusion detection [12]. A Statistical-based technique captures the network traffic activity and a profile representing its behavior.

A. Tajbakhsh et al. proposed the method called fuzzy association rules for efficient classification of dataset [13]. A framework based on data mining techniques is proposed for designing IDS. A new method is also used to speed up the rule induction algorithm via reducing items that may be included in extracted rules. W. Wang et al. introduced the Normalization in network intrusion detection [11]. Anomaly intrusion detection is an important issue in networks. The data preprocessing, attribute normalization are important to perform detection. Anomaly detection methods do not normalize attributes before training and detection. S. Yu and W. Zhou developed the new idea called flow correlation coefficient methodology to work independent of any DDOS attack [18]. The various disadvantages are needed to investigate the possibility of organizing a super botnet that has a sufficiently large number of live bots. The compromise between detection accuracy and cost deserves a further investigation. Once the detection strategy is known to attackers, the attacker may develop new strategies to disable our detection.

A. jamdagni et al. focused the method Geometrical structure based analysis to discriminate normal patterns and attack patterns in real time, to detect the attack against web application. A number of relevant approaches have been proposed continuously and inaccurate detection is the problem of detecting malicious activities and large number of false alarm is sent to the admin. To overcome all the above disadvantages use hybrid detection algorithm which reduces the false alarm and increases the intrusion detection rate.

3. Motivation

The motivation of proposed system is to improve the detection accuracy compared to other various methods available related to the DoS attack detection. The new system must reduce the false positive since in previous methods most of the normal users are identified as intruder so our main goal is to avoid that problem. The hybrid detection method takes very less time to identify the attacker and the real time data is consider as normal user.

4. Denial-Of-Service Attack

Attack is any attempt to destroy, alter, disable or gain unauthorized access or use of a resource. Attack has two types are active attack and passive attack. Passive attack does not affect the system resources. Passive attacks are very difficult to detect because no alteration of data. Active attack will affect the system information or resources. Active attack will change the content of the data. Modification of data or creations of false data are the examples of active attack. Denial of service (DoS) attack comes under the category of active attack. DoS attack is an attempt to make a system, machine or network resources unavailable to its user by blocking or denying the services [18].

The intruder attacks the user and the other type is to attack the server itself are two types of attack. Denial of service attack have various types of DoS attacks are Buffer Overflow attack, Neptune attack, Teardrop attack, Smurf attack, Ping of Death(PoD) attack, Back attack and Land attack.

Buffer Overflow attack the user receives more data than the capacity; the result is overflow of data that leads to system crash. The attacker may be aware of the target system has a weakness. Neptune attack, attacker sends more requests to the user rapidly and the system will not give proper response for the request.

The disadvantage of DOS is difficult to set the parameter and metrics. The attacks are highly dependent on one another and it consumes more resources. A program leaks the data by page fault not detected. Difficult to compare and test set because researcher use only part of train and test set. The hybrid detection method is used to overcome all the limitations. Hybrid detection improves the DoS attack detection from various network resources in the easy manner and it is easy to implementable. A number of relevant approaches have been proposed continuously and inaccurate detection is the problem of detecting malicious activities and large number of false alarm is sent to the admin. The algorithm reduces the false alarm and increases the intrusion detection rate.

5. System Architecture

Develop a complete framework for our DoS attack detection system use sample by sample detection mechanism [20]. The system performs intrusion detection process through various stages of development process. The processes are happen continuously one by one.

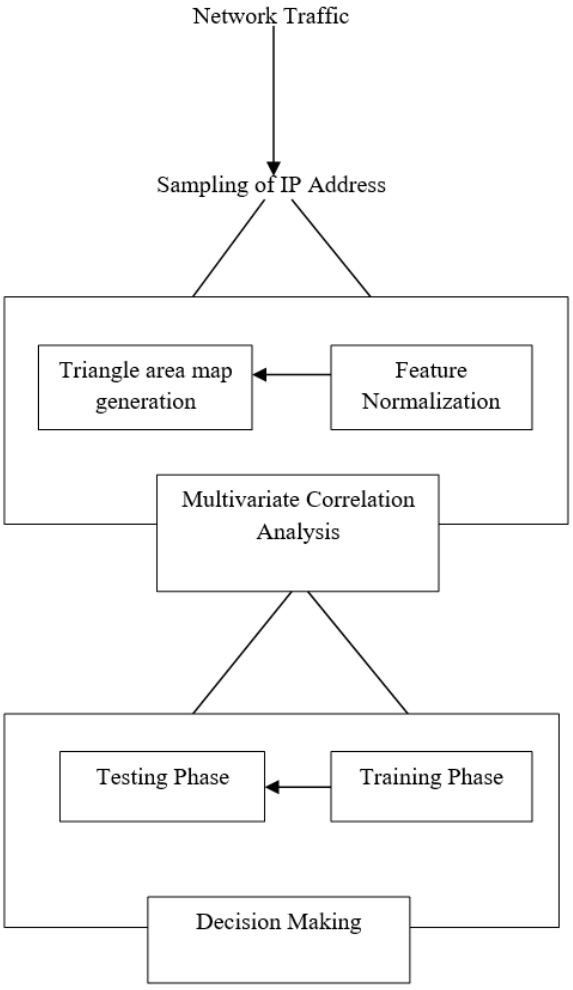

Fig. 1. Intrusion Detection Framework

A. Network Traffic

The numbers of traffic records are generated from the client. Each record is identified by using the IP address after the sampling process of IP address. Once the traffic records enter into the system the basic features are normalized the form the traffic records for well defined time interval. The user monitoring only the destination network that reduces the overhead of detecting malicious activities because user only concentrate on inbound network traffic.

B. Sample By Sample Detection

Sample by sample detection maintains the higher probability than the group based detection [17]. In group based detection, it is difficult to achieve group of sequential sample only from the same distribution so sample by sample detection is better. The benefits of sample by sample detection able to detect the attack in a prompt manner and intrusive samples are sampled individually. Traffic samples are independent of one another and traffic records follow normal distribution.

C. Multivariate Correlation Analysis

MCA approach employs triangle area for extracting the correlative information between the features within an observed data object [20]. Attack traffic behaves differently than the legitimate network traffic and their properties are identified by the statistical properties. MCA approach reveals the correlation between distinct features using geometrical analysis. It provides characterization for individual network traffic rather than group based.

Triangle area map generation technique is applied to extract the correlation between two distinct features. The extracted correlation called triangle area that is stored in the TAMs. This provides higher discriminative features between legitimate and illegitimate network traffic. TAM is a symmetric matrix so all the diagonal element in the matrix are zero. The matrix is divided into upper triangles and lower triangles. Both triangles have the same elements. Changes of these structures represent anomaly detection present in the network. Observed traffic record and normal traffic are given as the input for the triangle area based algorithm. Both of the traffic records are compared on by one that is called as sample by sample detection. Mean, covariance and standard deviation are calculated from observed and normal traffic.

Lower triangle and upper triangle value are determined from the triangle area based technique and detection method used either upper triangle or lower triangle since both are having same value. The threshold value is calculated from the mean and variance of the legitimate and illegitimate network traffic records. Normal traffic is legitimate traffic and observed traffic may be legitimate or illegitimate traffic. Both traffics are compared if the value is greater than particular threshold then it if considered as an intrusion otherwise it is written as normal.

D. Decision Making

Hybrid detection mechanism is used for decision making. So the system can detect the attack without requiring relevant knowledge. Here, the misuse based detection is first applied to distinguish the normal and attack record then the normal records are comes under the process of anomaly detection. The normal records that are identified in the previous step are analyzed without any relevant knowledge. This mechanism enhances the robustness of the detector by using intrusion detection. It reduces the time to detect the attack.

The decision making process have two different phases. Training phase is used for generating normal profile and details are stored in the database. The testing phase take the individual observed traffic and form the tested profile. Then, tested profile and normal profile are compared to detect the attack. If the dissimilarity is greater than particular threshold then it is considered as an intrusion. The threshold is used to differentiate normal traffic from attack traffic.

If the decision making based on low quality normal profile then it causes an inaccurate characterization to legitimate network traffic. The triangle-area based MCA approach is applied to analyze the records for generating normal profile. Mahalanobis Distance (MD) also used to measure the dissimilarity between traffic records. The threshold is used for differentiating legitimate and illegitimate network.

$$\text{Threshold}=\mu+\sigma*\alpha \qquad (1)$$

α is usually ranged from 1 to 3. μ is the mean of the network traffic record and σ is the standard deviation of the records.

6. Evaluation and Results

Denial-of-Service is an attack that makes an information or data unavailable to its intended hosts. The various methods to carry out this attack and the strategies are available and there are also other ways of making service unavailable. The attack may come in various forms and to detect the attack user will consider the time, distance and path as a parameters.

The virtual server was initialized to start the server process. The server is connected to the back end server that establishes connection with the client program. The client selects the data or files that are going to run. The file is selected from the particular path and run the program. Selected sample java program is used to determine the intrusion. After sending the request, the response is received from the server for that particular file had selected. The response from the server is output for the program that may receive in various time intervals.

The user can able to determine the origin IP address of the new requests and number of times the request received from the client. The normal profile was generated back end which is based on timing as shown in fig 2. The time as a basic parameter so if any requests are received before the particular interval or after the long interval is considered as an intrusion and the particular IP address will blocked by the system automatically.

Fig. 2. Profile Generation

The internal server is initialized for running the client program. Clients make the program request to the server and server process the request and produce the output continuously. The normal profile is generated for each request and if any variation from normal profile is generated then it is identified as attack and the particular IP address is blocked. The smurf attack and pod attack are completely identified by changing the threshold. The user can identify the intruder and block that particular IP address permanently without affecting all other system. The user compares various detection methods shown in table 1.

Table. 1 Detection Methods Comparison

Method	Detection Time	Reliability	Detect New Attack	False Positive
Misuse	Fast	Yes	No	Very Low
Anomaly	Vary	Yes	Yes	High
Hybrid	Fast	Yes	Yes	Low

7. Conclusions

The hybrid detection mechanism is used for Denial of Service attack detection that is the combinations of misuse based detection and anomaly based detection. Multivariate Correlation Analysis based attack detection system uses the triangle-area based technique to extracts the geometrical correlations between individual pairs of two distinct features within the network traffic which offers accurate differentiation for network traffic records. So the system to be able to distinguish both known and unknown attacks from legitimate network traffic. The normal network traffic activity is captured and the profile representing its behavior from that the user will detect the attacker and block the particular IP address.

The scope for future work is based on finding the Denial of Service attack detection system that must implement techniques for avoiding Internet Protocol spoofing attack and further reduce the false positive rate. The attacker may be attacking network from misusing the IP address of

normal user so the different attack prevention technique should be developed.

References

[1] D.E. Denning, "An Intrusion-Detection Model," IEEE Trans. Software Eng., vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.

[2] G.V. Moustakides, "Quickest Detection of Abrupt Changes for a Class of Random Processes," IEEE Trans. Information Theory, vol. 44, no. 5, pp. 1965-1968, Sept. 1998.

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

[4] A.A. Cardenas, J.S. Baras, and V. Ramezani, "Distributed Change Detection for Worms, DDoS and Other Network Attacks," Proc. The Am. Control Conf., vol. 2, pp. 1008-1013, 2004.

[5] S.T. Sarasamma, Q.A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 35, no. 2, pp. 302-312, Apr. 2005.

[6] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.

[7] S. Jin, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185- 2197, 2007.

[8] 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.

[9] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB Using SVM," Computer Comm., vol. 31, no. 17, pp. 4212-4219, 2008.

[10] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," IEEE Trans. Systems, Man, and Cybernetics Part B, vol. 38, no. 2, pp. 577-583, Apr. 2008.

[11] 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 (ISPAN), pp. 448-453, 2009.

[12] 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, pp. 18-28, 2009.

[13] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion Detection Using Fuzzy Association Rules," Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[14] 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.

[15] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512-525, Apr. 2011.

[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," Proc. Conf. Neural Information Processing, pp. 756-765, 2011.

[17] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective Denialof-Service Attack Detection," Proc. IEEE 11th Int'l Conf. Trust, Security and Privacy in Computing and Comm., pp. 33-40, 2012.

[18] 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, no. 6, pp. 1073-1080, June 2012.

[19] 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, pp. 811-824, 2013.

[20] Z. Tan, A. Jamdagni and P. Nanda "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 447-456, 2014.