INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SYSTEM FOR DISTRIBUTED DENIAL OF SERVICE ATTACK DETECTION BASED ON MULTIVARIATE CORRELATION ANALYSIS

S. Priyanka[1], N.Vidhya[2], S.Vinmathi[3], A.Amali Angel Punitha[4]

[1]*BE (CSE), ULTRA college of Engineering, Madurai, India*
[2]*BE (CSE), ULTRA college of Engineering, Madurai, India*
[3]*BE (CSE), ULTRA college of Engineering, Madurai, India*
[4]*Assisstant Professor, ULTRA college of Engineering, Madurai, India*

Abstract: - The network attackers produce threats to the interconnected systems, such as Web servers, db servers and cloud servers. Common and aggressive means, Distributed Denial-of-Service (DDoS) attacks cause serious impact on these computing systems. DDOS attacks sternly degrade the presence of victim who can be a router, host or a entire system. In this paper, we represent a DDoS attack which is a detection system that uses multivariate correlation analysis (MCA) for accurate network traffic characterization by extracting the correlations between network traffic features. Here, the MCA-based DDoS attack detection system employs the regulations of anomaly based detection in attack recognition .This solution is capable of detecting the known and unknown DDoS attacks effectually by learning the legitimate traffic patterns. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of the proposed system is evaluated using data packets.

Keywords: Distribution Denial-of-service attack, Triangle-area-based, geometrical correlation, MCA (multivariate correlation analysis) based detection system

1. Introduction

Authors DDoS attack detection mainly cynosure on the improvement of network-based detection mechanisms. Detection systems are based on some of the routine i.e., monitor traffic transmitting over the confined network. Distributed-Denial-Of-service (DDoS) attacks are one type of aggressive and menacing intrusive behavior to online servers. DDoS vitiate the possibility of the victim, imposing an intensive computation task to the victim by exploiting its system vulnerability or flooding with huge amount of useless packets. Hence, the victim can be forced out of services from a few minutes to even several days and this cause severe damage to the services running on the victim. Therefore, effective detection of DDoS is essential to the protection of online services. DDoS attack mainly converges on the development of network-based detection mechanisms.

Detection system endures these mechanisms monitor traffic transmitting on the protected networks. This mechanism discharges the protected online servers from monitoring attacks and ensures the servers can dedicate themselves to provide quality services with minimum delay in response. Typically, network based detection systems can be classified into two categories, specifically, misuse-based detection system and anomaly based detection systems. The misuse-based detection system observes attack by monitoring network activities and looking for rivalry with the existing attack signatures. Misuse attacks are easily evaded by any new attacks and also variants of existing attacks. Furthermore, it is complicated and labor intensive task to keep signature database updated as signature generation is a manual process and involves expertise.

Anomaly based detection monitors and flags every network activities presenting significant deviation from legitimate traffic profiles as suspicious objects. This owes to the principle of detection, which monitors the significant deviation from legitimate traffic profiles as objects show more anomaly based detection techniques promising in detecting intrusions that exploit unknown system vulnerabilities. The system that suffers from high positive rate are data mining, machine learning, and statistical learning. The DDoS attack detection system in this paper employs MCA. This is done by, monitoring and analyzing at the destination network it may reduce the overhead of detecting malicious activities by concentrating only on inbound traffic which is relevant. Detector is enabled to provide protection which is the best fit for the targeted internal network because of the traffic profiles used by the detector are developed for a smaller number of network services. Then, we stimulate multivariate correlation analysis, in which "triangle area map generation" module is applied to extract the correlation between two distinct features within each traffic record coming from the traffic record normalized by the "feature normalization". Intrusion network occurrence cause changes to these correlation so that the changes can act as indicators to identify the intrusive activities. All the correlation extracted, namely, triangle areas stored in triangle area maps (TAMs). Internet based network attacker can be categorized in 2 ways,

a) Directed Denial of service attack model, where the specific Dos is developed and rolled out by an attacker with an aim to take down a specific network or computer.
b) Indirect Denial of service attack model, where a worm or virus is at large in the wild, which causes Dos and interruption as a result of its spreading.

This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records. Here, we also adopt sample-by-sample detection method, network formation method and performance analysis. The detection system equip with capabilities of accurate characterization for traffic behaviors.

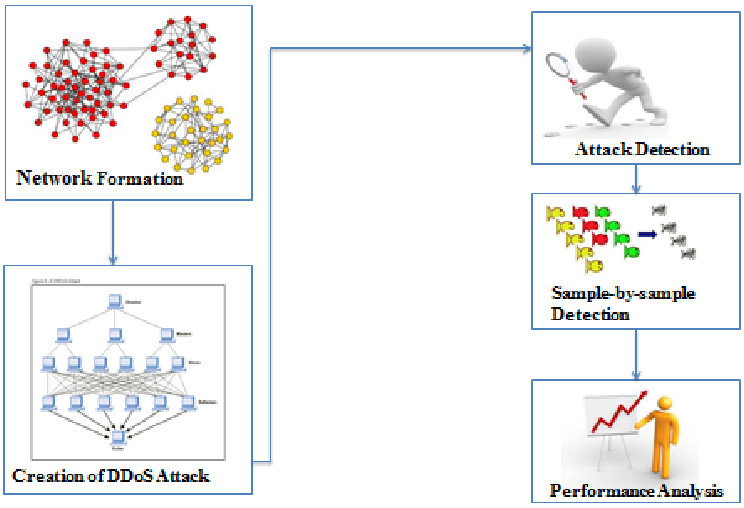

Figure. 1. Network Formation of DDOS Attack

2. Related Techniques

There are several techniques to overcome DDoS attack.

a) Handling Multivariate correlation analysis by Firewall

Correlation between any two distinct features within each single network traffic record is through this analysis. It estimates the relationship between two variables and also plays an important role in Dos attack. DDoS attack traffic behaves differently from the legitimate network traffic; due to the statistical properties the behaviour of the network is reflected. To define these statistical properties, we present a novel MCA approach in this section. A triangle area is employed for MCA approach extracting the correlative information between the features within an observed data object (i.e., a traffic record). Firewalls can be set up to have simple rules such to allow or deny protocols, ports or IP addresses. In case of a simple attack coming from a small number of unusual IP addresses for instance, one cloud put up a simple rule to drop (deny) attackers incoming traffic. More complex attacks will however be hard to block with some regulations. Take as instance, there is an ongoing attack on port 80 (web service), it is no possible to drop all incoming traffic on this port because doing so will prevent the server from some traffic which is legitimate. All the firewalls may be deep in the network hierarchy. Routers may be affected before the traffic gets to firewall. Nonetheless, firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Usage of open BSD's packet filter which act as connection for handshake proxy (with the client) instead of simple forwarding the packet to the destination. And also available for other BSD's as well. This can be named as "proxy".

b) Algorithms and techniques used

In our paper representing the attack we use two algorithms namely,

- A triangle based technique to enhance and to speed up the process of MCA.
- Normal Profile Generation Algorithm
- Attack Detection Algorithm

The algorithm for normal profile generation, in which the normal profile *Pro* is built through the density estimation of the MDs between individual legitimate training traffic records TAM(normal) and the expectation of the 'g' legitimate training traffic records. Moreover, the mean of the (j, k)-the elements of TAMs over the legitimate training traffic records defined as,
The normal profiles and thresholds have direct influence on of a threshold-based detector the performance is detected. The process based on Normal Profile Generation, Threshold Selection and Attack Detection. The normal profile generation algorithm built through the density estimation of the MDs between individual legitimate training traffic records. The threshold given is used to differentiate attack traffic from the legitimate training traffic records. To detect DDOS attacks, the lower triangle of the TAM of an observed record needs to be generated using the proposed triangle-area-based MCA approach.

c) Detection of Attacks using Sample-by-Sample Detection

The group based detection technique maintained a high probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism. This proof was based on assumption that the samples in a tested groups distribution are belongs to same. Predication of the traffic, which are belongs to same group. To overcome the above problem we can classifying the group individually .This benefits are not found in group based mechanisms. The group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism. In this system investigates individuality of samples. The attacks can be detected in a prompt manner in comparison with the group-based detection mechanism, intrusive traffic samples can be labeled individually, there are probability of correctly classifying a sample into its population is higher than the one achieved using the group-based detection mechanism in a general network scenario.

3. Techniques Used

Many system and techniques are used to detect the DDos attack efficiently. Yu Chen, Kai Hwang developed a distributed change-point detection (DCD) architecture using change in aggregation trees (CAT). The idea is to detect abrupt traffic changes across multiple network domains at the earliest time. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider. Majority ISPs do not share their AS domains with competitors. Zhiyuan Tan Aruna Jamdagni – Xiangjian detected the effectiveness of the proposed multivariate correlation analysis approach is evaluated on the KDD CUP 99 dataset.
A multivariate correlation analysis approach investigates the extraction second-order statistics from the observed network traffic records. This comparatively contains high false positive rates and do not work under the situation where an attack linearly changes all monitored features. Selecting effective MIB variables and compares some different classification algorithms based on chosen variables. The advantage of this system is its features. Optimization of the system model is activated after receiving the new data. It is stated that KST is able to detect more attacks in all situations even at low traffic intensities.
The MCA approach employs triangle area for extracting the correlative information between the features within an observed data object (i.e., a traffic record). It does not require the knowledge of historic traffic in performing analysis. If does not require, the Covariance matrix approaches proposed in existing is vulnerable to linear change of all features, our proposed triangle-area-based MCA withstands the problem. It provides

characterization for individual network traffic records rather than model network traffic behavior of a group of network traffic records. The proposed system is analysed on original data packets using ROC curve to the Accuracy detection compared with Existing system.
The packet delivery ratio is analysed to get the probability of sending and receiving packets. The analysis of computational complexity and time cost analysis is performed with respect to Throughput and time at which the total number of packets is received. The End-to-End Delay is calculated for two way communication between nodes with their density and time. The creation of DDOS attack is processed here with one attacker to show the transmission among the other five nodes. The data packets are transferring from attacker node to other nodes by samples. The attacker node increases its samples transferring rate at each level for detection.
Here, the data packet samples are increased to higher probability to degrade the performance of those data which have been sent for transmission among each other nodes. The packets of data are increased to huge number for providing a denial-of-service in a distributed manner among the neighbour nodes. When the samples are transferred in a huge amount from the source to the destination, those data packets gets dropped from the particular node and the requests will be provided as response later.

4. Conclusion

In this paper, we fix up the drawbacks of the existing system by providing security to the attacks and upgrade these attacks flexibility and accuracy. The problem in our paper however, can be solved by utilizing statistical normalization technique to eliminate the bias from the data. This technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offer extra true characterization for network traffic behaviors. Evaluation can be conducted using KDD data set to give an effective performance. In future, DDos attack detection will be tested further using real-world data and employ more sophisticated classification techniques to further alleviate the false-positive rate.

REFERENCES

[1] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", VOL. 25, NO. 2, FEBRUARY 2014.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] S.J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, "Cost- Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project," Proc. DARPA Information Survivability Conf. And Exposition (DISCEX '00), vol. 2, pp. 130-144, 2000.
[7] 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.
[8] 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.
[9] M. Tavallaee, E. Bagheri, L. Wei, and A.A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," Proc. IEEE Second Int'l Conf. Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009.
[10] 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.
[11] D.E. Denning, "An Intrusion-Detection Model," IEEE Trans. Software Eng., vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.
[12] 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.
[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] 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.
[15] 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.
[16] 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.

(Cont.)

S.Priyanka, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

N.Vinmathi, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

N.Vidhya, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

A. Amali Angel Punitha received her bachelor's degree (B.Tech -Bachelor of Information Technology) from Raja College of engineering and Technology, Madurai, and affiliated to Anna University, Chennai, in 2005 and then did her Master Degree in computer science and engineering from Raja College Of Engineering and Technology, Madurai, affiliated to Anna University, Chennai, in 2007. She is currently working as an Asst Prof in Ultra College of Engineering & Technology for Women, Madurai. Her current research interests include the area of Network Security and Cloud Computing.