International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 - Issue 5, May 2015

An Efficient DDoS Attack Detection Technique using Trace Back Approach

Mrs.Ragendhu.T.R., (M.E),
PG Scholar, Department of Computer Science and Engineering, RVS Technical Campus,
Email ID:ragendhu.rajan@gmail.com

Mrs.S.Subashini., M.E., (Ph.D).,
Assistant Professor, Department of Computer Science and Engineering, RVS Technical Campus.

Abstract:- *Distributed Denial of Service (DDoS) attack is a most widespread collaborative attack it causes serious impact on computing systems. DDoS attack is an attempt to make a network resource unavailable to its intended users. It is usually performed on a large scale by flooding the communication and computing resources to make the resources or service unavailable to the genuine users. Hence, it is vital to protect these critical resources from DDOS attacks. Though prevention against these attacks is not conceivable, detection of these attacks plays a crucial role in preventing their growth. In this paper a trace back algorithm has been proposed that effectively detects the presence of DDoS attack. This algorithm computes the local traffic, and if the traffic is more than a predefined threshold it indicates the presence of DDoS attack.*

Keywords: Internet, DDoS, network resources.

I. Introduction

Distributed Denial of Service (DDoS) attack is a major threat to the security of the cyberspace. It generally consumes the bandwidth, memory or the processing capacity of a network or a system. The DDoS attack is large scale, distributed and collaborative attack. It is prominent on wireless [1] or wired network [2]. They force the target to perform massive computation thereby using its system openness or flooding the target system with huge volume of unnecessary packets. This brings about serious problems to the services operating the target machine.

In DDoS attack fake source IP addresses are utilized in the stack traffic packets. A hacker or attacker desires to utilize such fake source IP address for two reasons: first, the hacker needs to hide the identity of the machine so that the target cannot find the attack. The second is related to the performance of the attack. The hackers want to prevent any effort of the target to clear the malicious traffic. Hence in order to protect the network from DDoS attacks, techniques to detect the presence of the attackers have become significant as a preventive measure against DDoS attack.

Generally the DDoS attack detection metrics are classified into signature based and anomaly based metrics. The signature based approach is based on a technology that uses a set of predefined attack signatures like strings or patterns as signatures that is matched with the incoming packets. The anomaly based detection approach generally models the normal traffic behavior and uses it to find the difference with the incoming traffic. But the anomaly based approach has several drawbacks: first, an attacker can prepare the detection system to consider the anomaly behavior as normal. Second, the false positive rate (FAR) is generally higher than the signature based approach. So it is vital to find a technique to trace the path in which the traffic traversed. Thus in this paper, a trace back algorithm has

been proposed that effectively detects the presence of DDoS attack. This algorithm computes the local traffic and if the traffic is more than a predefined threshold it indicates the presence of DDoS attack.

II. Related work

In [3], the author proposed a system to detect the DOS attack, which uses Multivariate Correlation Analysis (MCA) to characterize the network traffic accurately by extracting the geometrical correlations between features of network traffic. The anomaly based detection principle is employed in the system to recognize the attack. The process of MCA is enhanced and speeds up by using the triangle-area-based technique. The technique has the potential for detecting the DoS attack. The system effectiveness has been evaluated using the KDD CUP 99 dataset and the results shows that it can achieve high detection accuracy.

The flash crowd and DDoS are focused in [4] and proposed Adaptive discrimination algorithm to differentiate the normal traffic, flash crowd and DDoS. A sequential detection and packing algorithm is used to detect and filter out the attacked packets. The detection accuracy is improved and time consuming is reduced by using the method.

A technique has been proposed in [5] based on the Euclidean Distance Map (EDM) for extracting the optimal features to detect the DOS attacks. The extracted features preserve the important discriminative information to characterize the network traffics accurately. The extracted multivariate correlations are the highly capable features to detect the DOS attack. The system effectiveness has been evaluated using the KDD CUP 99 dataset and the results shows that it can achieve high detection accuracy.

In [6], the DDOS attacks are discussed and a defense scheme is to enhance the network performance. The information of medium access control (MAC) layer is used in the system for detecting number of RTS/CTS packets received. The frequency of retransmission of RTS/DATA is sensed to detect the attacker, once the attacker is detected then the data packets from those attacker nodes will be blocked. The simulation results show that the system improves the network performance.

A framework has been presented in [7] to detect the denial service attack effectively in the cloud environment. A covariance matrix statistical method is used to detect the attack and the attack source is determined by using TTl (Time_to_Life) value counting method. A Honeypot method is used for attack prevention. The framework has been represented in a UML diagram to implement it in a cloud environment.

An intrusion detection system is presented in [8] for detecting the Denial of Service (DoS) attacks. The system is composed of two stages such as a statistical preprocessor and a neural network classifier. The essential statistical features are extracted in the preprocessor stage in a limited time period from the received traffic by a targeted name server. The different types of DOS attacks are detected and classified using the three different neural networks. These neural networks are compared and the feed-forward back propagation neural network achieves high accuracy of 99% among the other two neural networks.

A novel traceback method is proposed in [9] for detecting the DDoS attacks, which is based on entropy differences between the normal and attack traffic. The method has several advantages over the previous techniques in terms of scalability, effective against packet pollution and independent among different attack traffics. The simulation results show the effectiveness of the system in a large scale attack network.

An Entropy-Based method is proposed in [10] to detect the DDOS attacks on community network. The entropy rate, information theory factors are applied to differentiate the DDOS attacks from the normal traffics. The effectiveness of the system is proved in the simulation results. The future direction of this method is pointed to explore it in future.

III. Trace Back Algorithm for DDoS Attack Detection

IP trace back is a technique that is capable of discovering the sender of the IP packet based on the source IP field contained in the packet that is spoofed. In this paper the attack detection approach is combined with the IP trace back algorithm and the filtering technique to form an effective cooperative defense technique against security threats in internet.

The IP trace back algorithm classifies the traffic types into two types: local traffic and forward traffic, respectively. The local traffic is the traffic created from its LAN and the forward traffic is the sum of its local traffic and the traffic forwarded from its upstream routers. Trace back algorithm computes distance information based on variations of its local and the forward traffic from its upstream routers. Here, the LAN of router is set to include the victim. If the distance information based on its local traffic is more than the specific detection threshold, the proposed detection system identifies an attack in its LAN so that the router will stop disseminating the traffic. The following assumptions are made in the proposed approach

1. Effective features of the network traffic are extracted.
2. It is assumed that we have full control of the routers present in the network.
3. The average normal traffic and the local thresholds are stored in every router.
4. In each router, the attack traffic follows Poisson distribution and the normal traffic follows Gaussian noise distribution.

Collaborative Attack Detection (CAD) Scheme

In the CAD scheme, initially a sampling frequency (f), a sampling time (t) and predefined threshold (t=0.5) are set. It is assumed that the network traffic is induced into the routers R1 and R2 from their upstream routers R3, R4, R5 and R5 and also from LAN1 and LAN2 respectively. Initially calculate the number of packets that have several distinguishable characteristics such as source IP address, packet size and so on at every sampling interval‘t’. Compute the probability distribution of the traffic from router R3 and R4 and LAN1 and from R5, R6 and LAN2 respectively. Then perform distance information (α) computation of R1 and R2 and sum up their distance information using the following expression.

$$S_{\alpha(A,B)} = \alpha(A||B) + \alpha(B||A) \qquad (1)$$

Here α indicates the distance information, A and B are the probability distributions respectively. $\alpha(A||B)$ can be computed as follows

$$\alpha(A||B) = \frac{1}{\beta-1}\log_2\left(\sum_{i=1}^{n} A_i^{\beta} B_i^{1-\beta}\right) \qquad (2)$$

$$\alpha(B||A) = \frac{1}{\beta-1}\log_2\left(\sum_{i-1}^{n} B_i^{\beta} A_i^{1-\beta}\right) \qquad (3)$$

If the resulting distance information is more than a predefined threshold (t), the system identifies the presence of an attacker and an alarm is raised and the packets are discarded, else the packets are forwarded to the downstream neighbors. When the proposed attack detection approach identifies an attack the IP trace back algorithm is immediately launched. The IP trace algorithm is illustrated in fig 1.

1. Define local and forward threshold values as t_{li} and t_{fi}.
2. Verify whether there is attacks in the traffic by computing distance information α_{fi} using the following expression $\left\|\alpha_{fi}(p_f, p_l)\right\| = \left\| \alpha(p_f, \|p_l) + \alpha(p_l, \|p_f) \right\|$ (4)
3. Compare this value with the threshold value t_{fi}
4. If $t_{fi} > \alpha_{fi}$ then compute the local traffic distance information
5. Else forward the packet
6. α_{fi} is computed using the value of t_{li} in the distance information formula
7. If $t_{li} > \alpha_{li}$ stop sending the traffic to downstream neighbors
8. Else forward the packet.

Fig 1 IP trace algorithm

IV. Results and Discussion

The proposed DDoS attack detection approach is evaluated using KDD Cup 99 dataset [11]. The proposed approach is analyzed in terms of false positive rate (FPR), true positive rate (TPR), root square error (RSE) and mean absolute error (MAE).

Fig 2 shows the error rate in terms of RSE and MAE for both the proposed trace back algorithm and anomaly detection approach. The results show that the proposed approach has lower RSE and MAE values than the existing anomaly detection approach.

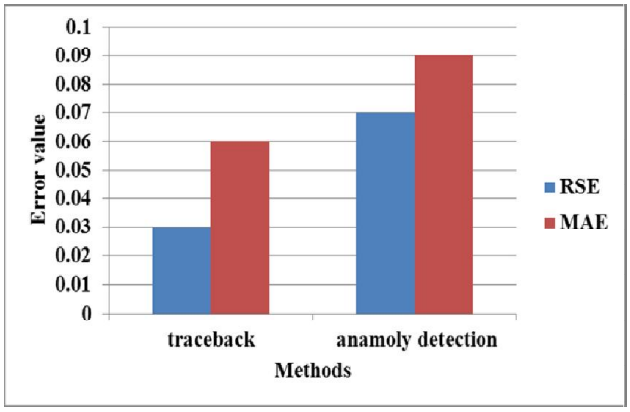

Fig 2 RSE and MAE of the proposed approach

Fig 3 shows the ROC curve for the trace back algorithm and the anomaly detection approach. The results show that the trace back algorithm offers excellent true positive by controlling the false positive.

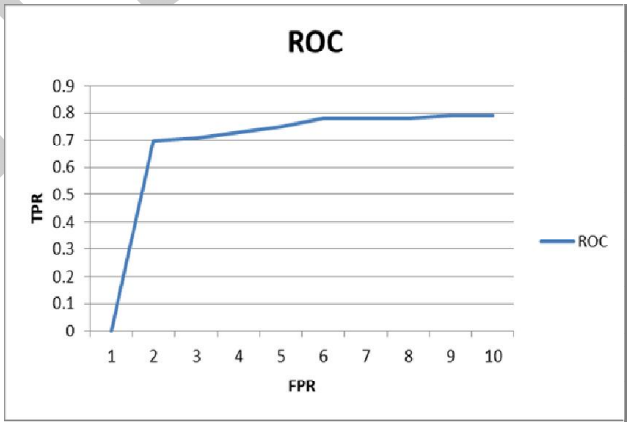

Fig 3 FPR and TPR of the proposed approach

V. Conclusion

Distributed Denial of Service (DDoS) attack is the most widespread collaborative attack that is usually performed on a large scale by flooding the communication and computing resources to make the resources or service unavailable to the genuine users. In this paper a trace back algorithm has been proposed that effectively detects the presence of DDoS attack. IP trace back is a technique that is capable of discovering

the sender of the IP packet based on the source IP field contained in the packet that is spoofed. Trace back algorithm computes information distances based on variations of its local and the forward traffic from its upstream routers. If the information distance based on its local traffic is more than the specific detection threshold, the proposed detection system identifies an attack in its LAN so that the router will stop disseminating the traffic.

References

1. X. Jin et al., "ZSBT: A novel algorithm for tracing DoS attackers in MANETs," EURASIP J. Wireless Commun. Netw., 2006 ,pp. 1–9.
2. A. Chonka et al., "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," J. Netw. Comput. Applicat., 2010.
3. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He,Priyadarsi Nanda, Ren Ping Liu , "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE Transactions On Parallel And Distributed Systems, Vol 25, No 2, 2014
4. N.V.Poorrnima, K.ChandraPrabha, B.G.Geetha "Adaptive Discriminating Detection for DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient with Collective Feedback" Journal of Computer Engineering , Vol 16, No. 1, PP 54-58, 2014.
5. Zhiyuan Tan; Aruna Jamdagni; Xiangjian He, Priyadarsi Nanda1, and Ren Ping Liu, „Multivariate Correlation Analysis Technique Based on Euclidean Distance Map for Network Trac Characterization". IEEE Transactions on Parallel And Distributed Systems, 2007.
6. S.A.Arunmozhi,Y.Venkataramani, " DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, 2011.
7. Mohd Nazri Ismail, Abdulaziz Aborujilah, Shahrulniza Musa & AAmir Shahzad, "New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment", International Journal of Computer Science and Security , Vol 6, No. 4, 2013.
8. Samaneh Rastegari, M. Iqbal Saripan and Mohd Fadlee A. Rasid, " Detection of Denial of Service Attacks against Domain Name System Using Neural Networks", International Journal of Computer Science , Vol. 6, No. 1, 2009.
9. Shui Yu, Wanlei Zhou, Robin Doss and Weijia Jia, "Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on parallel and distributed systems, vol. 22,no.3., 2011.
10. Yu. S and Zhou. W, "Entropy-Based Collaborative Detection of DDoS Attacks on Community Networks", IEEE Transactions on Pervasive Computing and Communications, pp. 566-571, 2008.
11. 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," The DARPA Information Survivability Conference and Exposition , Vol.2, pp. 130-144, 2000