ISSN:0975-9646

Hybrid Technique for DDoS Attack Detection

Pooja Redekar[#1], Madhumita Chatterjee[#2]

[#]*Department of Computer Engineering, University of Mumbai*
PCE, New Panvel, Maharashtra, India

***Abstract*— The Distributed Denial of Service (DDoS), special type of Denial of Service attack, has become one of the major threats to the Internet. Generally, attackers launch DDoS attacks by directing a massive number of attack sources to send useless traffic to the victim. The victim's services are disrupted when its host or network resources are occupied by attack traffic. The threat of DDoS attacks has become even more severe as attackers can compromise a huge number of computers by spreading a computer worm using vulnerabilities in popular operating systems. With the Internet of Things (IoT) in place the DDoS attack will have an enormous attack surfaces available to unleash its full potential. This type of attack has no full-proof prevention technique. Therefore, next step in attack defense is attack detection. This paper focuses on hybrid approach, that is, finding solution to this problem by combining two approaches of attack detection viz., anomaly-based and misuse-based detection.**

***Keywords*— Distributed Denial of Service(DDoS) Attack, Hybrid Detection approach, Anomaly-based detection, Misuse-based detection.**

I. Introduction

A Denial of Service(DoS) attack is an malicious attempt by an attacker to disrupt the online services of a service provider (server) and to make it unavailable to its legitimate users. The DDoS attack can be seen as amplified version of DoS attack. A DDoS attack against an online service provider can target a computing resource such as CPU, or a network resource such as the bandwidth of the victim's network link or a combination of both. The effect of a DoS attack can range from a minor increase in the service response time to complete inaccessibility, and at times having financial implications on organizations heavily reliant on the availability of their service. Therefore, it is very important to detect DDoS attack in its early stage to avoid further nuisance.

II. Literature Survey

This section presents the relevant literature surveyed for various techniques of DDoS Attack Detection. DDoS attack sometimes mimics legitimate but dramatic increase in network traffic referred to as Flash events. It is very necessary for the detection approach to distinguish between Flash event traffic and actual attack traffic.

Nazrul Hoque et al. [1] have used Feature Feature Score generation technique. For attack detection they have used deviation of traffic sample from legitimate traffic as a metric. This method gives 100% attack detection accuracy on MIT DARPA 2000 and CAIDA DDoS 2007 datasets. Threshold value should be selected properly for the best results.

Zhiyuan Tan et. al. [2] have proposed multivariate correlation analysis based approach for DDoS detection. As authors claim, the system outperforms Euclidean distance map based approach and Triangle area based nearest neighbors approach. KDDCup99 dataset is used for evaluation for their system. This dataset, though benchmarked, is very old & thus, system's performance against new DDoS attacks cannot be evaluated.

Komal More et. al. [3] have performed thorough survey on attack detection approaches using multivariate correlation analysis. In the system proposed by them, geometrical features from network traffic are extracted and correlation is applied. The authors claim that the system has improved detection rate but also false-positive rate is high.

Ozge Cepheli et al. [4] have used Gaussian Mixture Models as anomaly detector and SNORT as signature detector to make Hybrid IDS. Here first time two detection approaches are combined. The authors claim to have high detection accuracy. But the test were conducted on Bank penetration dataset which is not benchmarked and hence performance of this system cannot be compared to other systems.

Alan Saied et. al. [5] have used Artificial Neural Networks. This method gives 100% attack detection accuracy with Known Attacks and 95% accuracy with Unknown Attacks. This system cannot handle DDoS attacks that use encrypted packet headers. Detection accuracy depends hugely on Training Data.

Ilker Ozcelik et. al. [6] have used CUSUM algorithm with entropy calculation. Their system have higher DDoS Detection efficiency as compared to using only entropy method.

Xi Qin et. al. [7] have used Flow entropy method. Threshold is not necessary as cluster distance is used as parameter to distinguish attack traffic from legitimate traffic. Here cluster distance is calculated using Euclidean Distance formula.

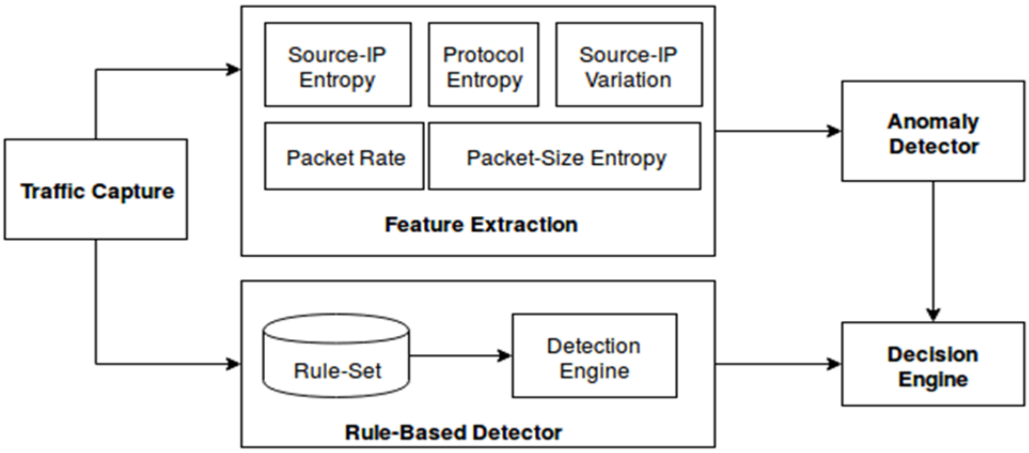

Fig. 1 Architecture of Proposed System

III. Proposed System

The architecture of proposed detection system has 5 main modules, namely, Traffic Capture, Feature Extraction, Anomaly detector, rule-based detector and decision engine [Refer Fig. 1].

A. Traffic Capture

This module performs task of intercepting packets that are traveling across particular network. There are many tools that can capture live traffic for example, Wireshark. It is free and open source packet analyzer. This module will act as an input to detection system. The Input to the detection system can be provided: (1) On wire, that is Live Traffic (2) Datasets or Captured Traffic . Live Traffic as direct input to system can be harmful. Therefore, new systems are always analyzed and tested frequently using datasets. Datasets (KDDCup99[13], MIT DARPA 2000[14], CAIDA UCSD DDoS 2007[15] etc.) are used for training of systems also.

B. Feature Extraction

There are five features extracted in this module namely, Source-IP Entropy, Protocol Entropy, Source-IP variation, Packet rate and Packet-Size Entropy.

1) Source-IP Entropy: It is measure of specificity or randomness of source IP in traffic. It is calculated as:

$$H(X) = -\sum_{i}^{n} P(x_i) log_2 P\,(x_i)$$

2) Protocol Entropy: It is measure of specificity or randomness of source IP in traffic. It is calculated as:

$$H(protocol) = -\sum_{i}^{n} P(pr_i) log_2 P\,(pr_i)$$

3) Source-IP Variation: It is calculated as Rate of change of IP addresses with respect to time.

$$V_{sip} = \frac{no.of\ unique\ IP\ addresses}{time\ interval}$$

4) Packet-Rate: The packet rate is calculated as total number of packets received/ captured in unit time.

5) Packet-Size Entropy: Randomness of Packet size is called entropy of packet size. This can be calculated using technique mentioned in [6].

C. Anomaly Detector

The flow of anomaly detector is depicted in Fig. 2. Extracted 5 feature vector from feature extraction module acts as an input to this detector. The distance between input vector and normal traffic centers is calculated using Mahalanobis distance method. Distance vector is used to save distances. Based on the shortest distance to the center the cluster is assigned. Radius calculation is used finally to detect attack traffic.

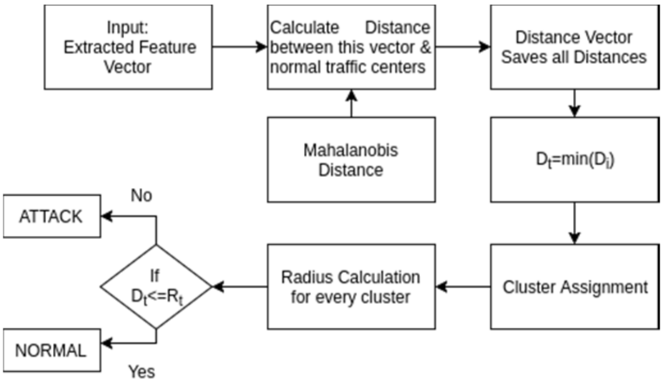
Input:
Extracted Feature Vector
Calculate Distance between this vector & normal traffic centers
Distance Vector Saves all Distances
Mahalanobis Distance
D_t=min(D_i)
No
ATTACK
If D_t<=R_t
Radius Calculation for every cluster
Cluster Assignment
NORMAL
Yes

Fig. 2 Flow of Anomaly detector

D. Rule-Based Detector

The rule-based detector or signature-based detector or misuse-based detector finds patterns of known attacks in data-sample[12]. This type of detector has less false positive rate of detection. At the same time, it cannot detect unknown attack or variations of known attack if the signature base is not updated. There are two main components of rule-based detector, namely, detection engine and rule set.

1) Detection Engine: It is nothing but a comparator. It compares incoming sample with the rules in the rule-set.

2) Rule-Set: It is database containing rules. The rules form the core of the rule-based detector. The detection of attack depends greatly on how efficiently and correctly the rule is described in Rule-Set.

E. Detection Engine

This module is responsible to combine the output of two detector modules, namely anomaly detector and rule-based detector. This can be implemented using OR logic.

III. Conclusions

The distributed denial of service attack is very old, well-known and has become the biggest threat to Internet with its ability to disrupt services. With the availability of online rental booter services at very cheap price, even a kid with minimal knowledge of computer and networks, can take down numerous websites in no time. The available attack technologies are advanced. There is no permanent solution to this problem. So, the detection of attack on time becomes very crucial step. Thus, the proposed method tries to reduce the disadvantages of rule-based and anomaly detector, by combining them. The known attacks are detected by rule-based detector and unknown attacks /Zero day attacks are detected by anomaly detector. In anomaly-based detection, final attack detection decision is based on clustering. Therefore, need of manual threshold selection will be removed. Rate of attack detection will be improved.

References

[1] N. Hoque, D. Bhattacharyya, J. Kalita, *A Novel Measure for Low-rate and High- rate DDoS Attack Detection using Multivariate Data Analysis*, IEEE COMSNETS 2016-Poster Track, 2016.

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

[3] K. More, P Gosavi, "A Survey on E_ective way of Detecting Denial-of-Service attack using Multivariate Correlation Analysis", iCATccT, 2015.

[4] O. Cepheli, S. Buyukcorak, G. Kurt, "Hybrid Intrusion Detection System for DDoS Attacks", Journal of Electrical and Computer Engineering, 2015.

[5] A. Saied, R. Overill, T. Radzik, "Detection of known and unknown DDoS attacks using Arti_cial Neural Networks", Neurocomputing, vol. 172, pp. 385-393, 2016.

[6] I. Ozcelik, R. Brooks, "Cusum-Entropy: An e_cient method for DDoS attack detection", IEEE, 2016.

[7] X. Qin, T. Xu, C. Wang, "DDoS Attack Detection using Flow Entropy and Clustering Technique", ICCIS, 2015.

[8] D. Bhattacharyya, J. Kalita, "Network Anomaly Detection-Machine Learning perspective"

[9] T.B. Manohar, E.V.N.Jyothi, B.Rajani, I.Rajesh Kumar, "A Novel Entropy Based Detection of DDoS Attacks"

[10] F Iglesias, T Zseby, "Analysis of network tra_c features for anomaly detection", Springer, 2015.

[11] H. Kayacak, A. Zincir-Heywood, M. Heywood, "Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets"

[12] S. Manjari, K. Raja Sekhar, "DDoS Counter Measures Based on Snort's detection system", IJDCST, 2013.

[13] KDD Cup 1999 Data, Available at http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[14] MIT DARPA 2000, Available at http://www.ll.mit.edu/ideval/data/2000data.html

[15] The CAIDA UCSD DDoS 2007, Available at http://www.caida.org/datasets/security/ddos-20070804/