ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

EM-CURE Algorithm for DDOS Attack Detection

Prianka P. Narode[1], Prof.I.R.Shaikh[2]

P.G. Student, Department of Computer Engineering, SND Engineering College, Yeola, SPPU, India[1]

Associate Professor, Department of Computer Engineering, SND Engineering College, Yeola, SPPU, India[2]

ABSTRACT: Distributed Denial of Service (DDoS) attacks have become more difficult because they have evolved in many ways. It has been very critical for any organization to protect their computing environment from unauthorized access or malicious attacks. DDoS attack is a congestion-based attack that makes both the network and host based resources unavailable for legitimate users, DDoS attack detection task is very difficult. In this system, We propose combination of unsupervised data mining techniques as intrusion detection system (IDS). The entropy concept in term of windowing the incoming packets is applied with data mining technique. For detection of the DDoS attack in network flow using Clustering Using Representative(CURE) as cluster analysis. The data is mainly collected from datasets. We propose a clustering data mining technique based on entropy. It gives a way to analyze attacks and using a clustering data mining techniques to construct an efficient detection model.

KEYWORDS: Clustering; Distributed Denial of Service; Anomaly detection; Data Mining; Intrusion Detection.

I. INTRODUCTION

DDoS attack has become one of the most representative threats because its impact and frequency have grown to significant levels. With the rapid progress of the Internet technology and growth of network infrastructure, many service have been implemented online. Distributed Denial of Service (DDoS) is a simple, and yet very powerful technique to attack. System resources as well as Internet resources. Distributed agents consume some critical resources at the target within the short period of time and deny the service to legitimate clients.

Distributed Denial of Services (DDoS) attacks are among the major security threats launched using internet services. Detection process suffers from efficiently differentiating the normal stream and abnormal stream of traffic from network flow. The legitimate requests often uses attack itself to flood the target and this makes it very hard to distinguish an attack traffic from legitimate traffic, fast real time detection is very difficult because in current computer networks huge amount of data involved. We proposed different solutions that help to prevent the security breaches aimed at the secured asset of many organizations using an internet services. Some forms of Intrusion Detection Systems (IDS) have been instrumental in detection and preventing these threats, and identifying intruders from the legitimate users. The analysis of intrusion, the intrusion detection approaches falls into three categories that include: Misuse Intrusion Detection (MID), Anomaly Intrusion Detection (AID), and a hybrid that combines the strategies of both of MID and AID. Misuse Intrusion detection is based on pattern matching with the known signatures. However, The misuse intrusion detection needs to be updated periodically to include the new types of attacks. The main strategies of IDS-DDoS attacks based on data mining are illustrated in following figure:1

DOI: 10.15680/IJIRCCE.2018.0605098

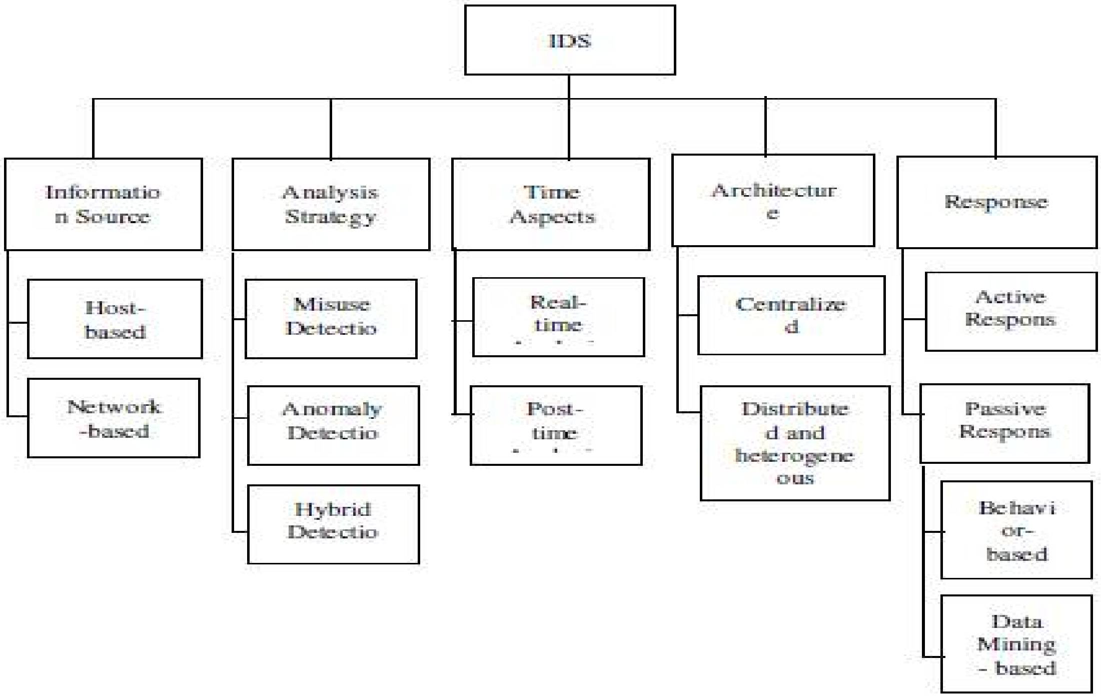


Fig. 1. IDS-DDOS Attack Detection Strategies.

IDS-DDOS strategies based on data mining. The significance of designing and implementing EM-CURE cluster analysis is to analyze and detect DDOS attacks. In this efficient approach based on Shannon Entropy Method with hierarchical CURE cluster analysis (EM-CURE) has been implemented and used to analyze and detect DDoS attacks. The detection approach will test by using datasets collected from real-world attacks by (Defense Advanced Research Projects Agency) DARPA2000.

II. RELATED WORK

W. Cerroni, G. Monti,[2], they use an unsupervised technique to distinguish effectively the normal behavior from malicious network flow using k-means clustering. The proposed technique was tested using the web server as a real test bed for the experimental attacks.

M. Suresh,[3], have been found Fuzzy c means techniques to efficiently detect the DDoS attacks with a better accuracy. DDoS attacks rapidly increase the serious damages, the rapid detection of the DDOS attack they use the machine learning models, like Navies Bayes, K-means and Fuzzy c-means clustering are developed for efficient detection of DDoS attacks. Then in the experimental results they show that the Fuzzy c-means clustering is fast compared to the other algorithms.

H. Om and A. Kundu,[4], they use two classifiers, Knearest neighbors, K-Means,and Nave Bayes, for anomaly intrusion detection. In their proposed hybrid detection solution model, certain attributes have been selected based on entropy. This hybrid method successfully reduced the false alarm rate.

J. Mazel and P. Casas,[5], Detecting DDoS attack using cluster analysis in different size and shapes. They Combining multiple Evidence Accumulation algotithm and sub-space clustering to blindly identify anomalous tracffic flows. They developed a totally unsupervised method to detect and characterize network flow anomalies.

V. Rajyaguru and B. S. Manoj,[6], they described the application of clustering technique to detecting multiple DDoS attacks. The performance of the different clustering analysis techniques is extensively evaluated with real traffic from different datasets.

N. Hoque and M. H. Bhuyan,[8], They proposed Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm to detects compromised nodes in WSN using an energy preserving mechanism that analyzes the traffic inside a cluster and sends warning to the heads of cluster. whenever, an abnormal behavior is detected. The overall Quality of Service (QoS) has been improved as the energy consumption in WSN nodes has been minimized duly. A selforganizing map(SOM) based IDS relates recurring theme in intrusion detection.

Wesam Bhaya and Mehdi Ebady Manaa,[11], have been studying the architecture of DDoS attack.Data mining cluster analysis is used to detect and cluster the DDoS attack. They evaluated the Performance comparison as the ultimate goal is to promote real-time avoidance strategy against DDoS attack.

III. Proposed Algorithm

EM-CURE ALGORITHM: This is mainly used for detecting ddos attack in computing environment. It is combination of Entropy concept and Data mining technique.

A. Data Pre-processing: In the preprocessing phase, the Network Flow features are specified and then the proposed entropy windows are applied.

1. Data Transformation:

Entropy is used mainly with data clustering because it provides a good clustering of data since it can be used with network traffic to convert the network flow to numerical (quantitative) data type. Formally, Entropy considers the measure of uncertainty in random variables (x1; x2; x3…xn)
from an information source that has (n) differeent values. The probability of xi appears in information sample identifid by xi, then the entropy (H) is defined for the random variable (X).

2. Feature Selection and Normalization:

The DDoS attacks and normal traffic are collected from the DARPA 2000 datasets. A proactive system based on centroid-based rules only works on TCP/IP header information of the TCP/IP packets. Since the payload is removed from the Dataset.

B. System Degradation: The EM-CURE cluster analysis is implemented using training and testing features in DARPA2000 dataset. The training and testing values are randomly selected. It defines no.of clusters, E ntropy values, No. of partitions, Shrink factor etc.

C. Anomaly Detection:

1)Anomaly Intrusion Ditection is an established profile of the systems and normal behavior.
2)AIDs is used to detect attack if there are any deviations from the established normal system profiles.

D. Evaluation:

The performance evaluation for a proactive DDoS attack detection system can be measured by a confusion matrix.
True Positive (TP): the number of the malicious packets correctly classiffied as malicious.

False Positive (FP): the number of normal traffic falsely classified as malicious.
False Negative (FN): it occurs when the malicious traffic is classified as normal traffic.
True Negative (TN): the number of benign packets correctly classified as benign.
In this work, the rate of accuracy, detection and false alarm can be calculated.

III. RESULTS AND ANALYSIS

EXPERIMENTAL SETUP:

A. Software and Hardware: The system has been implemented Java (JDK 1.7) with Eclipse -win64 and Apache-Tomcat-7.0.42. With JSP server serving java technologies. The system is tested on Intel(R) Core i-3 2330M CPU @ 2.50 GHz and 4 GB RAM. The System uses My-SOL, an open source relational database management system that uses SQL for adding, managing and accessing content in a database.

B. Dataset Used: We take data from DARPA 2000 dataset. Dataset contains feature attribute as Source IP, Destination IP, Source port, Destination port, Protocol etc. The CURE algorithm randomly divides the dataset into training and testing stages. The training stage is randomly used(25%) entropy features; while the testing stage used 100% of the entropy features.

Results and Analysis: The proposed approach will show the highest accuracy of EM-CURE proposed system as compares to existing system.

Table 1.shows the proposed system analysis for DARPA 2000 Dataset in a Testing phase.

Actual	Predicted	
	Normal	Attack
Normal	TN(7065)	FP(2)
Attack	FN(27)	TP(702)

In following fig, EM-CURE Cluster Analysis performance is shown by tabular value along with graph. The below table 2 contains details about all performance parameter of EM-CURE algorithm like accuracy, detection rate, false alarm rate etc.

Table 2.EM-CURE Performance

Performance Parameter	Parameter Value
Accuracy	99.63%
Detection rate	96.29%
False alarm rate	Approx 0

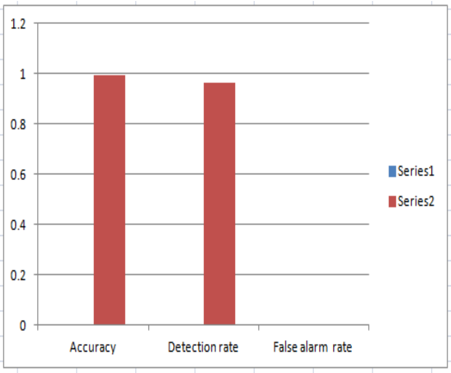
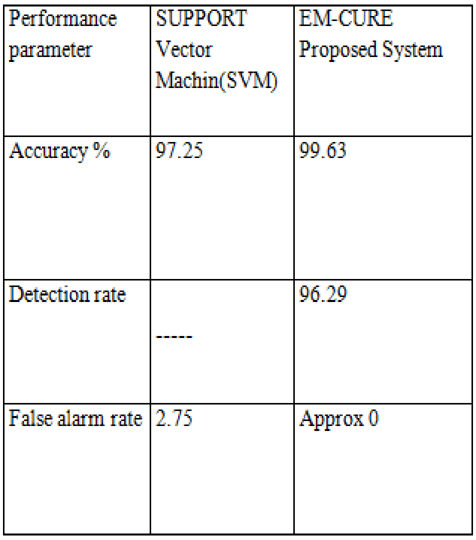


Fig: 2 Analysis Graph for EM-CURE

The below table contains details of EM-CURE parameter value and (other system) SVM parameter value. Table 3 compare details of EM-CURE performance parameter values with SVM parameter value.

Table:3 Comparison table for both system



Performance parameter	SUPPORT Vector Machin(SVM)	EM-CURE Proposed System
Accuracy %	97.25	99.63
Detection rate	-----	96.29
False alarm rate	2.75	Approx 0

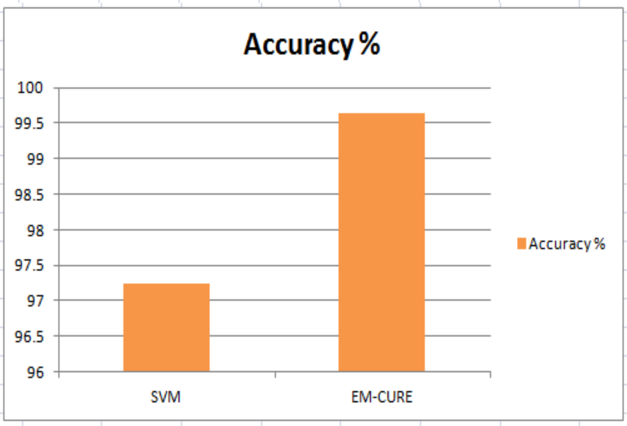


Fig: 3 Comparison graph

IV. Conclusion and Future Work

In this project, System provides a fundamental evaluation of Clustering algorithms on the detection of DDOS attack in large data scale. In this evaluation, system collected the nearly 200 records from DARPA 2000 dataset. System identified that Feature discretization was an important pre-process to Cluster-based DDOS attack detection. System should try to bring more discriminative features or better model to further improve DDOS attack detection rate. System also applies classification and compares their result and measure the performance for them.

In future system will work on the categorization of attack. Also system will extend more database value for better result and to achieve the accuracy. It convert nominal data into numeric data using entropywindows and it is preferable to consider other technique to calculate the frequency of attacks packets during the networkflow.

References

1. Wesam Bhaya and Mehdi EbadyManaa, DDoS Attack Detection Approach using an Efficient Cluster Analysis in Large Data Scale, in Annual Conference on New Trends in Information Communications Technology Applications,(NTICT'2017) 7 - 9 March 2017.
2. W. Cerroni, G. Monti, G. Moro, and M. Ramilli, "Network Attack Detection Based On Peer-To-Peer Clustering Of SNMP Data", , in nternational Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustnes, 2009, vol. 22, no. 213110, pp. 417-430.
3. M. Suresh and R. Anitha, "Evaluating Machine Learning Algorithmsfor Detecting DDoS Attacks", in International Conference on NetworkSecurity and Applications, 2011, pp. 441-452.
4. H. Om and A. Kundu, "A Hybrid System for Reducing the False AlarmRate of Anomaly Intrusion Detection System", in International Conferenceon Recent Advances in Information Technology, 2012, pp. 131-136.
5. J. Mazel, P. Casas, and P. Owezarski, " Sub-space Clustering andEvidence Accumulation for Unsupervised Network Anomaly Detection",in International Conference in Traffic Monitoring and Analysis, 2011,vol. 6613, pp. 15-28.
6. V. Rajyaguru, V. R Tamma, B. S. Manoj, and M. Sarkar, "On Detecting CTS Duration Attacks Using K-means Clustering in WLANs", in InternationalConference on Advanced Networks and TelecommunciationsSystems, 2012, pp. 12-14.
7. R. Suganya , "Denial-of-Service Attack Detection Using Anomaly withMisuse Based Method", International Journal of Computer Science andNetwork Security, 2016.

8. N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, ”Network attacks: Taxonomy, Tools and Systems”, Journal of Network and Computer Applications, pp. 1-18, 2013.

9. Shao Xiufeng, Cheng Wei, ”Improved CURE Algorithm and Applicationof Clustering for Large-scale Data”, sponsor of National 863 project.

10. Sharmila Bista, Roshan Chitrakar, ”DDoS Attack Detection Using Heuristics Clustering Algorithm and Nave Bayes Classification”, Journal of Information Security, 2017.

11. Wesam Bhaya and Mehdi Ebady Manaa, ”Review clustering mechanism of distributed denial of service attacks”, Journal of Computer Science 10 (10): 2037-2046, 2014.

BIOGRAPHY

Priyanka P. Narode is a PG Student **I.R.Shaikh** is Professor and H.O.D. in the Computer Engineering Department, College of Engineering, Yeola, SPPU, Pune. Priyanka P. Narode pursuing Master’s Degree in S.N.D COE,Yeola, SPPU, and Pune India. Her research interests are Data mining etc.