Search for Effective Data Mining Algorithm for Network Based Intrusion Detection (NIDS)-DDOS Attacks

S.Sumathi
Department of CSE
University V.O.C College of Engineering
Anna University-Thoothukudi Campus
sumock123@yahoo.com

N.Karthikeyan
Department of CSE
Syed Ammal Engineering College
Affliated to Anna University-Chennai
Ramanathapuram
nkarthikkeyan@gmail.com

***Abstract*— Cloud Security can be effectively implemented using data mining techniques. Distributed Denial of Service (DDoS) has been classified as one of the most common as well as damaging forms of attack on the cloud environment. Hence it is important to detect DDOS attack in cloud platforms. Previously various detection strategies have been proposed by researchers and used as defense mechanisms against DDOS attack . Analysis and comparison of these detection strategies are important to derive an efficient strategy to detect DDOS attack in a cloud scenario. Data mining technique is one of the efficient strategy that can be used to detect DDOS. This review paper dicusses the efficiency of various data mining algorithms in detecting DDOS attacks.**

Keywords— ***Data Mining techniques, DOS, Distributed Denial of Service (DDoS) attack, Cloud security***

I. INTRODUCTION

The denial-of-service attack(DOS) is defined as an attack which prevents the valid users from using the computer or network . The attacker who gains access to the network can perform any one of the actions .An attacker can send invalid data to various network applications or services, which in turn causes their abnormal termination or behaviour. A Distributed Denial of Service attack(DDOS) is defined as a type of DOS attack in which a large number of computers can be used to impair either a web page ,website or a web based service.

In Cloud, the various requests for virtual machines(VM) are accessible by anyone through Internet, which may cause DoS (or DDoS) attack. In short DDOS attack is an attack in which a person or group of persons attempt to immobilize an online service.

An attacker can flood an Individual computer or entire network causing its shutdown as flooding causes overload. DOS attack blocks the traffic which prevents the authorized users from accessing the network resources.

II. ARCHITECTURE OF DDOS ATTACK

DDOS attack architecture is powerful because it takes advanatage of the architecture of Internet. The prime concern of Internet architecture is to provide users with functionality. It does not focus on security as a result it leads to various security issues which gets easily exploited by attackers.

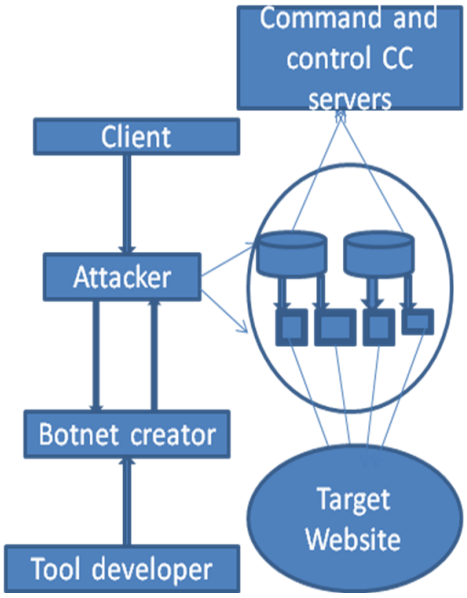

Fig.1. DDOS Attack Architecture

III. STRATEGY FOLLOWED IN DDOS

There are various components and steps involved in order to launch a DDOS attack.

A. Agent selection

The Agents are chosen by the attacker to launch an attack Compromised machine is a computer system which can be interrupted without any authorization. Attackers exploit these compromised machines which have enormous resources inorder to generate a powerful attack flow.

B. *Zombies*

Zombies are machines with compromised nodes and they are located in between the attacker and the victim. Zombies are selected by the attackers from the pool of hosts that are not protected.

C. *Communication via protocols*

Handlers are software packages that are distributed through out the Internet. Attackers communicate with these handlers This communication is done using protocols such as TCP,UDP,ICMP etc and this enable us to

- Identify agents that are on top and running.
- scheduling of attacks
- Upgradation of agents

D. *Initialisation of DDOS attack*

Attacker is the one who initiates the attack.Attacker not only identifies the victim,attack duration but also detects special features such as attack length,type,Transistor-Transistor Logic(TTL) and even adjust port numbers. In case if there are huge variations in the attack packet properties it becomes added advantage to the attacker as detection of DDOS attack gets complicated.

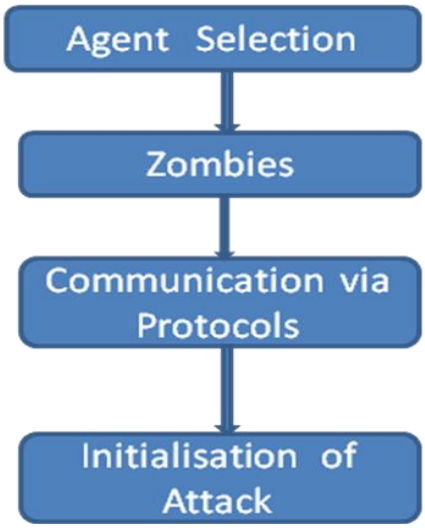

Fig.2. Strategy followed in DDOS

IV. THE CLASSIFICATION OF DDOS

A. *Classification based on attack rates*

1) Continuous rate attacks

2) Variable rate attacks

a) increasing rate

b) fluctuating rate

B. *Classification based on impact attacks*

1) Disruptive attacks: These attacks are further classified as follows

a) Self recoverable attack

b) Human recoverable attack

c) non recoverable attack

V. TOOLS USED TO PERFORM DDOS ATTACK

There are variety of DDOS attack tools that are available in the internet and attackers make use of these tools to perform a attack on a particular target system. Few common DDOS attack tools are discussed below

A. *Trinoo*

This tool is used to perform a UDP based flooding attack. It is based on master–slave architecture.TCP and UDP protocols are used for communication between master and slave.

B. *Tribe Flood attack(TFA):*

This tool uses command line interface for communication between master and slave. It fails to provide encryption between master and slave. ICMP echo rely packets are used to establish communication between master and slave. This tool is used to perform ICMP, SYN and UDP flood attacks.

C. *TFA 2K:*

It is an advanced version of TFA and it is used to perform flood and vulnerability attack. In this , encryption between master and slave is done using key- based CAST-256 algorithm.

D. *Stacheldraht*

This is the combination of the best features of Trinoo and TFN.This performs automatic updation on slave machines. Encrypted TCP connection is used for communication between attacker and master. Similarly,the communication between master and attacker is done using TCP and ICMP. This tool is used to implement smurf and flooding attacks

E. *Shaft*

In real-time, shaft has the capacity to switch control between master server and ports. Master and slave machines communicate through UDP packets.A simple TCP connection is used for communication between attackers and control masters. Implementation of TCP,UDP and ICMP flooding attack is done using shaft.

F. *M Stream*

In M Stream TCP ACK ,flood is used to attack a target machine.TCP and UDP packets are used for communication wheras master is connected through telnet to zombie. Password protected interactive login is used for remote control on masters. Random spoofing is performed on source addresses placed in attack packets.

G. *Knight*

Control channel that is used in knight is Internet Relay Chat(IRC). UDP,SYN and urgent pointer flood attacks can be implemented by Knight. Knight runs on Operating Systems such as Windows. Automatic updation in Knight is done using checksum generator,http,ftp etc;.

H. Trinity

Trinity is also based on IRC.UDP,TCP SYN,TCP ACK,TCP RST are some of the flood attacks that can be implemented by Trinity. Authorized IRC service is used for communication between agents and attacker and this raises the level of threat.

VI. DEFENSIVE STRATEGIES AGAINST DDOS ATTACKS IN CLOUD

A. Prevention of attacks

Attack Prevention is a technique in which reqests by suspected attackers that affect the servers are either filtered or dropped.

List Of DDOS Attack Prevention Techniques:

1) Text Puzzles
2) Graphical tests
3) Challenge Response
4) Selective access
5) Delayed access
6) Reputation based access
7) Hidden server/ports
8) Resource limits

B. Mitigation and recovery of attacks

Mitigation keeps the server alive even in case of attack.

List of Mitigation and Recovery Techniques

1) Mitigation and Recovery
2) Resource scaling
3) Shut down
4) Migration
5) Backup resources
6) Software defined networking(SDN)
7) Third party mitigation

C. Detection of attacks

Various parameters involved in DDOS detection

1) Scalability
2) Detection of unknown attacks
3) Real-time(R) and Non Real -time datas
4) Defense Strength: The defense strength is based on the following measurements
   a) Accuracy
   b) Sensitivity
   c) Specificity
   d) Precision
   e) Reliability
   f) False negative rate
5) Request –Response time
6) Probability of request dropping
7) Throughput
8) Degradation of System Performance
9) Detection/Response delays:Detection/Response delay classification is as follows
   a) One-Way
   b) Jitter
   c) Request-Response

In general Attack Detection has been classified into two types

1) Pattern Detection
2) Threshold Filtering

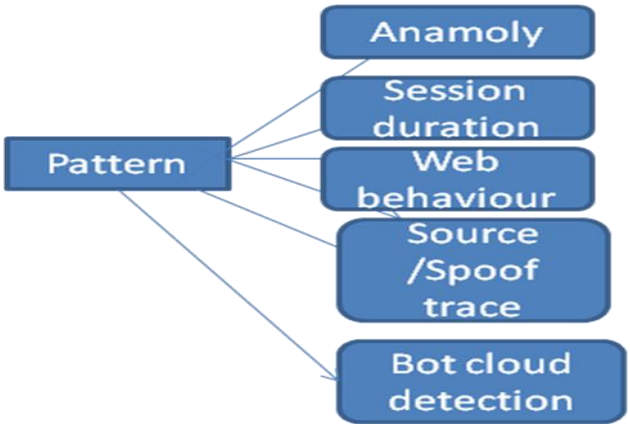

Fig. 3. Classification of Detection Techniques based on Pattern

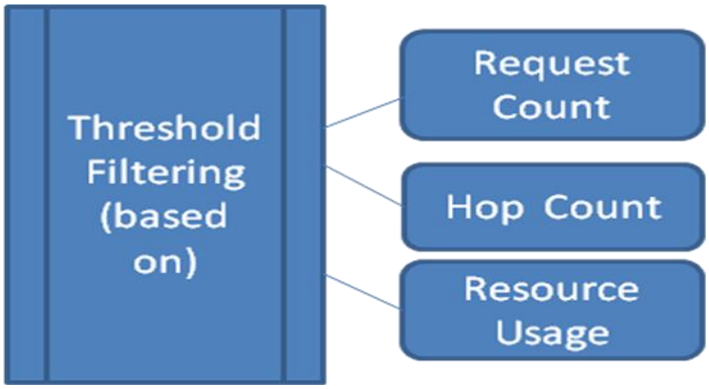

Fig. 4. Classification of Detection Techniques based on Threshold Filtering

VII. DATA MINING TECHNIQUES FOR DDOS ATTACK DETECTION IN CLOUD

Data Mining is used to discover patterns in very large datasets using intersection of various methods of Statistics,Database Systems and Machine Learning Techniques. Cloud security against DDOS attacks can be successfully implemented using Data mining Techniques. Common Data Mining Techniques are Clustering,Classification and Regression.

*1.Clustering:*It is the way to discover similar groups and structures in data provided not using known structures in data.

*2.Classification:*It is a method in which known structures are generalized when applied to new data.

*3.Regression:*This is a Technique which tries to find function for the purpose of modeling data with least error.

A. Datasets to detect DDOS

Datasets contains data that are tested and analyzed.So the best way is to use datasets to detect DDOS .These datasets are classified into three types.They are as follows

1) Private Datasets

Creating a real network with numerous network and host components is the best approach for DDOS attack detection.

2) Simulated Datasets

In this case a particular environment is stimulated using various tools like cloudsim,ns2,Qualnet etc;

3) Benchmark Datasets

KDDcup99 and DARPF Intrusion detection datasets are some of the datasets that are publicly available. But no separate benchmark datasets are available for DDOS attacks.

VIII. SURVEY OF DATA MINING ALGORITHMS FOR DDOS ATTACK DETECTION

This survey contains the various data mining algorithms that are used to detect DDOS. Apart from basic algorithms in data mining techniques, hybrid techniques which are combination of these basic algorithms are also found to be effective in detecting DDOS attack in a cloud Platform.

TABLE I. SURVEY OF ASSOCIATION AND CLASSIFICATION ALGORITHMS THAT ARE USED TO DETECT DDOS

ASSOCIATION	CLASSIFICATION
Multivariate correlation analysis	SVM
Fuzzy Association Rules	Multiagent pattern recognition
Frequent structure mining	Class construction
Apriori	Classification tree
Sequence analysis	Genetic algorithm
	Ensemble neural
	Entropy-based
	Case-based reasoning
	Nave Bayes
	k-Nearest Neighbour
	Decision tree (DT)
	Bayesian Network
	Neural network(NN)
	Ripper
	Fuzzy estimators
	Extreme learning machine (ELM)
	Particle swarm optimization (PSO)

TABLE II. SURVEY OF HYBRID AND CLASSIFICATION ALGORITHMS THAT ARE USED TO DETECT DDOS

HYBRID	CLUSTERING
Hierarchical clustering + SVM	Hierarchical clustering
Wavelet + SVD	Outlier detection
DT + SVM	k-Means
Genetic algorithm + k-NN	
Fuzzy Association rule + genetic optimization	
Clustering + Ant-Colony + SVM	
SOM + k-Means	
ensemble of adaptive + hybrid neuro fuzzy	
RBF + PSO	
genetic fuzzy systems + pairwise	
Hybrid PSO + DT	

IX. SURVEY OF EFFECTIVENESS OF CLASSIFICATION ALGORITHMS IN DETECTING DDOS

TABLE III. EFFECTIVENESS OF CLASSIFICATION ALGORITHMS

ALGORITHM USED	PERCENTAGE OF CORRECT CLASSIFICATION
Decision Tree	95.6
SVM	96.4
KNN	96.6
K-Means	96.7
Naive Bayesian	97.2
Fuzzy C Means	98.7

From the above tabular column it can be inferred that the Fuzzy C Means Classification algorithm is efficient in detecting DDOS when compared to other classification algorithms that are listed in the above tabular column.

TABLE IV. DETECTION TIME TAKEN BY CLASSIFICATION ALGORITHMS

ALGORITHM USED	TIME TAKEN FOR DETECTION IN SECONDS
Decision Tree	0.25
SVM	0.23
KNN	0.26
K-Means	0.20
Naive Bayesian	0.52
Fuzzy C Means	0.15

The above tabular column lists out the time taken by various classification algorithms .Among the classification algorithms analysed Fuzzy C Means takes fewer seconds to detect DDOS when compared to other classification algorithms listed above in the tabulation. Taking into account the two parameters percentage of detection as well as time taken for detection Fuzzy C Means is efficient in detecting DDOS among the classification algorithms.

X. CONCLUSION AND FUTURE WORK

This paper initially defines DDOS definition, architecture,strategy followed as well as taxonomy of attacks.The tools that are used to perform DDOS attack are also discussed.Though various defensive strategies are used against DDOS this paper focuses on detection technique based on data mining algorithms.A literature survey is made based on detection results of Data Mining algorithms. In

future more hybrid data mining algorithms can be derived for detecting DDOS in a cloud environment to ensure Cloud Security.

REFERENCES

[1] Bekeneva, Y., Borisenko, K., Shorov, A., Kotenko, I.: Investigation of DDoS attacks by hybrid simulation. In: Khalil, I., Neuhold, E., Tjoa, A.M., Xu, L.D., You, I. (eds.)

[2] ICT-EurAsia 2015 and CONFENIS 2015. LNCS, vol. 9357, pp. 179–189. Springer,Heidelberg (2015). doi:10.1007/978-3-319-24315-3_18

[3] Zolotukhin, M., Hamalainen, T., Kokkonen, T., et al.: Data mining approach for detection ofDDoS attacks utilizing SSL/TLS protocol. In: 15th International Conference, NEW2AN2015, pp. 274–285. St. Petersburg, Russia (2015)

[4] Delimitrou, C., Kozyrakis, C.: Security implications of data mining in cloud scheduling. IEEE Comput. Archit.Lett. 1-1 (2015)

[5] Adebowale, A., Olutayo, A., Sunday, I., Ogbonna, A. C., & Oluwabukola, O. (2017). Scalable Unsupervised Ensemble Algorithm For Effective Insider Threat Detection. Universal Journal of computer and Technology (UJCT), 1(3), 76-83.