International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

DFAA- A Dynamic Flow Aggregation Approach against SDDOS Attacks in Cloud

S.Ezhilarasi.,M.E.,M.B.A.,

Assistant Professor
Department of Computer Science and Engineering
Velammal College of Engineering and Technology
Madurai, India.

Abstract— Through the research of periodic shrew distributed DoS Attacks among excessive normal end-users' flow in Cloud, I proposed a new method to take frequency-domain characteristics from the autocorrelation series of network flow as clustering feature to group end-user flow data by BIRCH (Balanced Iterative Reducing and Clustering using Hierarchies) algorithm is an unsupervised data mining algorithm used to accomplish hierarchical clustering upon specifically large data-sets., and re-morse these clustering solutions into new groups . The result proves that the evaluation of simulation confirms that the proposed methodology categorizes strange network flows with rapid response time and greater detection accuracy, and avoids strange network flow groups with lower impaction.

Keywords— Cloud Computing, SDDoS, DFAA, Network Flow Grouping, Clustering Feature, Detection Accuracy, Response Time

1. INTRODUCTION

Classical DDoS attacks, identified by brute-force, maintained greater rate or categorically outlined to analyze the protocol disadvantages or software vulnerabilities in services, are well-known and can be detected with many methods. But distributed low-rate DoS attacks, as a new category, are becoming a deliberate threat to Internet, especially to cloud computing with enormous normal end-users. Compared with traditional DDoS attacks, they have three characteristics: (i) hard to identify because it has same flow classified features with normal flow (ii) low-cost because the attacks could be finished in single node with small flow data (iii)long term attacked-target insensitive attacks because attacked-target has self-adapt mechanism to adjust network flow. Thus, DLDoS attacks are hard to be detected. Thus, the scope of this paper is to have a DFAA(Dynamic Flow Aggregation Approach) with high detection accuracy, fast response time and light-weight implementation to detect and mitigate periodic TCP targeted Shrew DDoS Attacks.

1.1. DDOS Attack

DDoS (Distributed denial of service) attack is some sort of malicious activity or a typical behavior, which cooperate the availability of the server's resources and prevents the normal users from using the service. DDOS attacks are not indicated to modify data contents or accomplish prohibited access, but in that place they aim to crack the servers, mainly by transiently interrupting or suspending the services of a host linked to the Internet. DOS attacks could occur from either multiple sources or a single source. Multiple source DOS attacks are called DDOS (distributed denial-of service) attacks.

1.2. Types of DDOS Attacks

DDOS attacks could be categorized into mainly five types:

Volume Based Attacks - These types of attack includes ICMP floods, UDP floods, and other spoofed packet floods. The scope of this attack is to deluge the bandwidth of the targeted site.

Protocol DOS Attacks - These types of DDOS attack deplete the supplies of either of the transitional communication equipment, such as routers, or the servers, some firewalls and load balancers. Examples of protocol attacks are Ping of Death, Smurf DDOS, SYN floods, disjointed packet attacks. Protocol base attacks are generally determined in Packets per second.

Application Layer Attacks - The most hazardous kind of DDOS attack, application layer attacks are consist of seemingly sensible and effortless requests. The aim of these attacks is to crash the web server. Some of the application layer attacks are DDOS attacks that target Apache, Slowloris, Windows or Open BSD vulnerabilities, Zero-day DDOS attacks.

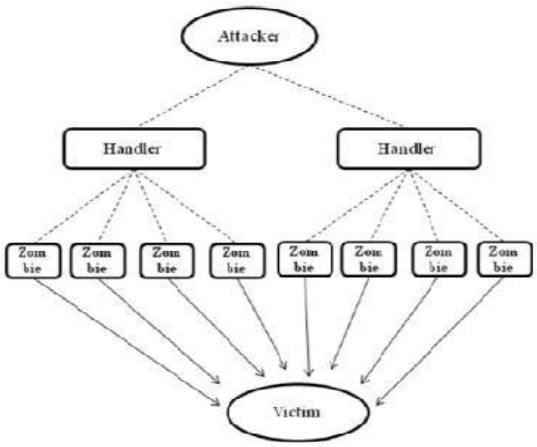


Fig.2. DOS Architecture

The Application layer attack is determined in Requests per second. R-U-Dead-Yet attack, HTTP POST DOS attack, slow read attacks are some of the examples

Distributed attacks-

The low rate DoS (LDoS) attacks and Reflected / spoofed attack are hard to identify in comparison with other forms of DoS attacks as it exploits many factors and vulnerabilities

Shrew DoS attacks-

The shrew attack is a DOS attack on the Transmission Control Protocol. It uses brief synchronized bursts of traffic to agitate TCP connections on identical links, by employing vulnerability in TCP's retransmission timeout method.

2. SHREW DDOS (SDDOS) ATTACKS IN CLOUD COMPUTING

The TCP targeted shrew DDoS attacks launched by multiple zombies could lower their individual traffic rates further, compared with single shrew attack stream in cloud computing. Since the distributed attack sources can lower its average traffic either by lowering the peak rate (known as Synchronous DLDoS Attacks), or by using longer attack periods (known as Asynchronous DLDoS Attacks). Thereby it makes detection using existing traffic volume analysis method at time domain ever harder.

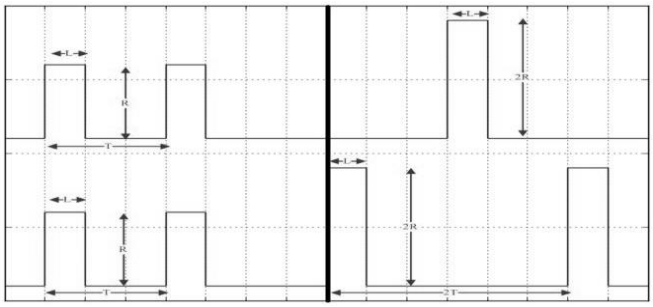
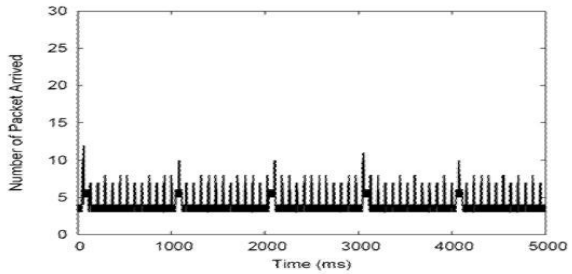
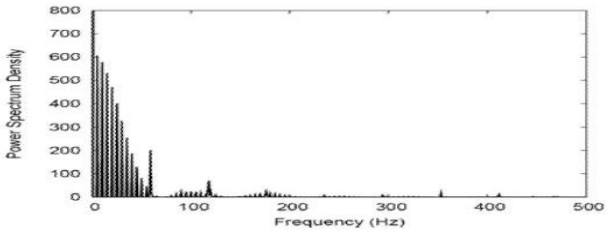


Fig. 1. Periodic Characteristics of Shrew Attack from Multiple Sources

As shown in Fig1-1, we have a shrew attack with the peak rate of 200Kb/sec and the attacking period of 1000ms. And we can see that the shrew attack stream hides itself among normal traffic by making its peak rate even lower than the normal traffic rate. Thus, before the link is saturated, the traffic volume analysis scheme may not be able to detect such a stealthy attack. Yet, the autocorrelation sequence will amplify the impact of the periodical pattern of shrew attack stream has after it is converted into frequency domain. In Fig1-2, what exactly happens is that more power of the autocorrelation function is distributed in the lower frequency band if there is shrew stream contained in the traffic.



1-1: Traffic Time Series Patterns



1-2: Power Spectrum Density

Fig- 2. Traffic Time Series Patterns and Power Spectrum Density with Shrew Attack

This paper introduces DFAA(Dynamic Flow Aggregation Approach) based on the analysis above, and chooses the

normalized cumulative amplitude spectrum (NCAS) value as its clustering feature (CF).

3. DFAA (DYNAMIC FLOW AGGREGATION APPROACH)

In the designed flow aggregation model, the network flow data is sampled per user and his real-time flow every 1 ms. And then, the flow data is directly converted from the time series to its frequency-domain representation using DFT (Discrete Fourier Transform), and take its ($NCAS_{F,K}$, F is a constant Hz at K-Point) as clustering feature. Aggregation approach takes use of BIRCH algorithm to aggregate network flow into different user group based on above feature. The group merging algorithm overcame the case that same user belongs to different group, and yields the final aggregation result.

3.1. Network Flow Clustering Feature Extraction

The core router starts to sample incoming packets per user flow and starts one timer as Fig 3. When the timer is ceased, the router alters the time domain series into it frequency domain illustration using DFT, and the NCAS at K-point will abstain to BIRCH algorithm as CF.

01: IF sampling is not done THEN

02: Continue sampling packets number per 1 ms;
03: ELSE
04: Convert the time-domain series into frequency domain;
04: Convert the time-domain series into frequency domain;
5: Calculate the NCAS value at K-Point;

6: IF NCAS < Threshold THEN
7: Mark the flows as legitimate, routing it;
8: ELSE
9: Start BIRCH algorithm with NCAS value;

3.2. Grouping Network Flows by Clustering Feature

This paper is using BIRCH to aggregate mass flow users into different groups. Given a set of N $NCAS_{F,K}$ data points, the clustering feature of the set is defined as the triple $CF = (N, \sum(NCAS_{F,K}), \sum(NCAS_{F,K}^2))$, where $\sum(NCAS_{F,K})$ is the linear sum and $\sum(NCASF,K^2)$ is the square sum of data points. Each non -leaf node contains at most B (Branching Factor) entries of the form [CF_i , $Child_i$], where $Child_i$ is a pointer to its i^{th} child node and CF_i representing the associated sub cluster. The tree size depends on the parameter T (Threshold).

The algorithm searches every leaf entries in the first CF tree to fix a reduced CF tree, while excluding outliers and aggregating crowded sub clusters into bigger ones. And then, an existing clustering algorithm is used to group all leaf entries. An algorithm (agglomerative hierarchical clustering) is used precisely to the sub clusters represented by their CF vectors. After this act a set of clusters is acquired that obtains leading distribution pattern in the data. Finally, the centroids of the clusters obtained in previous act are used as seeds and rearrange the data points to its nearest seeds to get a new set of clusters.

3.3. Group Merging

Pertaining about the imperfection of BIRCH, which declines to grasp the scenario of "same user, different group", the clustering event has to be corrected. Luckily, the user with same clustering feature always continues for a bit long time. That is, the feasibility of clustering the user into the same group is pretty high. Thus, the successive merging cluster schema is proposed: Firstly, all the users are divided into a group (known as current group) when starting to cluster. And every user is given a "Time to Live" (TTL, says T_i) and a initialized valueT_{i0} . Secondly, when a new set of clusters is generated by BIRCH algorithm, each of clusters performs intersection operation with current group. The one who has max intersection is merged into current group. In this new current group, if the user belongs to both cluster, its TTL is up to T_{i+1} , which should be less than T_{max} . If the end user only exists in the last current group, its TTL is down to T_{i-1} , when T_{i-1} =1, the end user is cleaned from this group. If the end user only happens in new merged group, its TTL equals to T_{i0} . After above steps, a new current group is here. Taking into account of this method, if a user doesn't belong to some group, it is cleaned out from these group after several clustering's.

4. SIMULATION ANALYSIS AND RESULTS

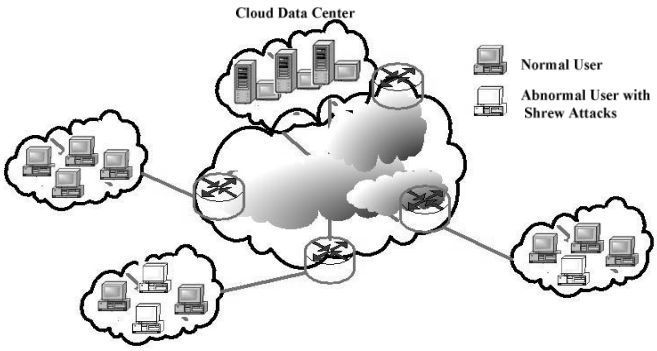


Fig- 4. Simulated Cloud Data Center Network Topology

With regard to verify the method having greater detection efficiency and rapid response time, and less impaction to common network flow groups, the following simulation scenario is designed. In cloud data center of Fig 4, three kinds of business flow types are used by 1000 users, and 300 users of them are abnormal ones. They onset shrew attacks with the peak rate of 200Kb/sec and the intrusion period of 1000ms, which can lead to whole data center network traffic jam.

4.1. Detection Efficiency of DFAA

With regard to describe that the proposed method has high detection efficiency, we define the detection accuracy (α) as the ratio between abnormal users and all users in the abnormal group.

Fig.5 presents the simulation results. Before shrew attacking, the ratio is nearly the same with the pre-defined ratio. While shrew attacking starts, the ratio bumps to

70%, even 100% after a little training time. That is, the group approach has a greater detect efficiency.

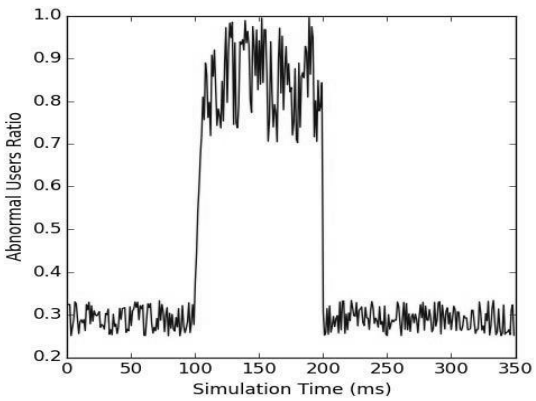


Fig- 5. Detection Efficiency Line of the Unusual Group

4.2. Response Time of DFAA Method

The response time is analytical parameter to evaluate the accomplishment of the flow grouping method. Here, we define it as the time when grouping method finds whether malicious flows exists or not. When the shrew attacking starts, the abnormal user number is increasing in the abnormal group. And in imitation 5 ms, the detected number is larger than 200 as Fig 6.

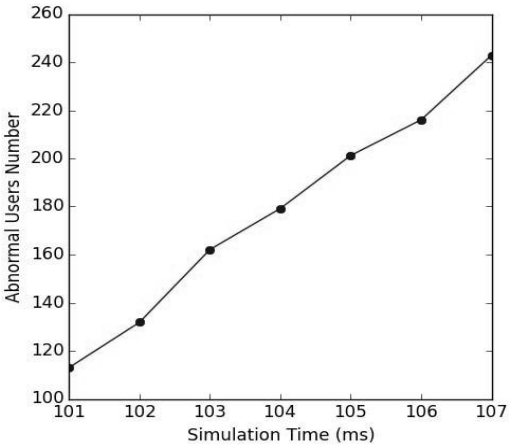


Fig- 6. Unusual User Number Line During Shrew Attacks.

5.CONCLUSIONS

The presented DFAA in cloud computing based frequency-domain feature can resolve the imperfection of BIRCH's lacking of soft clustering. And it is able to block malicious shrew flows with efficiency greater than 70% and response time less than 5ms. But the threshold T, time to live T_i and branching factor B are all needed to well tune manually per real network environment. Thus, we plan to investigate an efficient method to help work out above values in continued work.

REFERENCES

[1] Wu ZhiJun, Pei BaoSong. The detection of LDoS attack based on the model of small signal, Acta Electronica Sinica, 2011.06

[2] Chen Yu, Hwang Kai, Kwok YuKwong. Collaborative defense against periodic DDoS attacks in frequency domain, ACM Transactions on Information and System Security, 2005.05

[3] Zargar ST, Joshi J, Tipper D. A survery of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 2013.04

[4] Liu XiaoMing, Li Qi, Liu XiaoGuang. A novel pattern of distributed low-rate denial of service attack disrupts internet routing, Computing Technology and Information Management (ICCM), 2012

[5] Discrete wavelet transform-based time series analysis and mining, ACM Computing Surveys [J], 2011.01

[6] Li ChunLin, Huang YueJiang, Niu ChangXi. Network abnormal flow grouping method for cloud computing, Application Research of Computers [J], 2014.12.

[7] Khalid A. Fakeeh, King, Jeddah, An Overview of DDOS Attacks Detection and Prevention in the Cloud, International Journal of Applied Information Systems (IJAIS), Volume 11 – No. 7, December 2016.

[8] Pimwadee Chaovalit, Aryya Gangopadhyay, George Karabatis, A New Network Flow Grouping Method, ICACT2016.

[9] Neha Agrawal, Shashikala Tapaswi, Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing, Feb 2017.

[10] Zhenqian Feng, Bing Bai, Baokang Zhao, Jinshu Su, Shrew Attack in Cloud Data Center Networks, Seventh International Conference on Mobile, 2011.

BIOGRAPHIES

She received B.E(CSE) from Raja College of Engineering and Technology, Madurai, M.E(CCE) from Pavendar Bharathidasan College of Engineering and Technology, Trichy, M.B.A(ISM) form Bharathiyar University, Coimbatore and PGDB from Bharathiyar University, Coimbatore. She is currently working as Assistant Professor in department of CSE in Velammal College of Engineering and Technology, Madurai. She has published various papers in three different International journals and published papers at eight International conferences and sixteen National conferences.