ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

FUZZY BASED SYSTEM FOR ANALYSIS OF DDOS ATTACKS

Mitesh Bhopale, Aditi Kshatriya, Prakash Kumar, R Jagdeesh Kanan*
School of Computer Science and Engineering, VIT University Chennai.
Email: jagadeeshkannan.r@vit.ac.in

Received on 02-08-2016 *Accepted on 25-09-2016*

Abstract

Distributed denial-of-service (DDoS) flood attack remains great threats to the Internet. This kind of attack consumes a large amount of network bandwidth or occupies network equipment resources by flooding them with packets from the machines distributed all over the world. To ensure the network usability and reliability, real-time and accurate detection of these attacks is critical.

To date, various approaches have been proposed to detect these attacks, but with limited success when they are used in the real world. In this paper we propose a Technique which uses Fuzzy based system for the detection of the malicious node present inside the network. The schemes uses Fuzzy If-Then rules and the membership functions to define the threshold limit through which it will identify the misbehaviour of the nodes present in the network and declares it as a flooder or malicious node. The measurements were taken in the light of recurrence IP address, Number of packets and time delay. The test results demonstrate that the proposed method can detect the DDoS flood attack timely, effectively and intelligently.

Keywords: Cloud Security, DDoS attacks, Information Security.

1. Introduction

With the increasingly extensively range of network applications, network security becomes increasingly important. As DDOS (distributed denial of Service) is simple, diversity, strong attack and a very high hidden, it becomes one of the most popular attacks. This attack is to use by sending large amounts of data packet and flooding the destination network, which eventually cause the target system overload or link saturation, making it impossible to provide normal services to customers.

1.1. **Principle of DDOS:** DDOS attacks in understanding before a look of its predecessor: DOS (denial of Service) attacks. DOS attack is such a means of attack: the attacker within a certain time sends a large number of service requests over the network, consuming system resources or network bandwidth, occupy and beyond the processing capacity of the attacked host, leading to overload the network or system, to stop legitimate users to provide normal network services. DDOS attack is a further evolution of DOS attack. Simple DOS attack is an attack from a target source which is one-to-one mapping, the DDOS attacks on the introduction of the client I Server system to enhance the concept of distributed, is a many-to-one mapping. It is this change makes the DDOS attack is more powerful damage and destructive than the DOS attack. DDOS attack used a three-tier client I server architecture, the attacker use the console to issue attack orders to attack the server, control multiple host, which had been attacked the illegal invasion and installed a number of host-specific program. It receives a variety of command come from the attacker, but also controls a large number of agencies. They attack the host to send a large number of useless packets occupy the attacked host's system resources and network bandwidth, leading to depletion of the attacked host or network congestion, so that paralysis does not work.

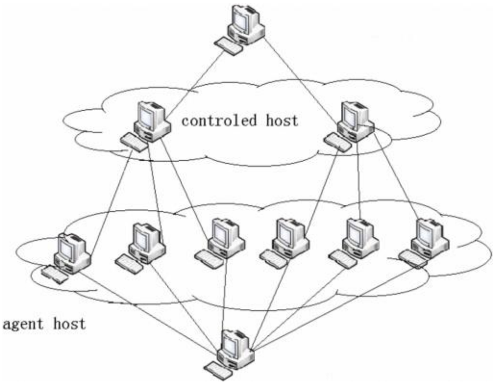


Figure 1: illustration of DDOS Attack.

2. Problem Statement

Cloud Computing is an emerging paradigm by which we can access the applications over the Internet. It permits us to make, design, and modify applications on the web. To make cloud computing convenient and accessible to the users, some services and models have to be run in the background like Deployment models (Public, Private, Hybrid and Community) and Service models (SaaS, PaaS and IaaS). The rule behind the cloud is that any PC associated with the Internet is joined with the same pool of registering force, applications, and documents. Clients can store and get to individual documents, for example, pictures, recordings, music and bookmarks or play amusements or word handling on a remote server as opposed to physically bearing a storage medium, for example, a DVD or thumb drive. Even the persons who has email or email client program can use the cloud email servers. Thus, desktop applications which interface with cloud email can likewise be considered cloud applications.

But there are some security issues. Data of the customer travels over the internet and stores in some remote locations. Customer might not know if some other users use his data. So a cloud customer should be careful in setting up strong passwords for their accounts and a cloud service provider must be careful about the infrastructure provided to customers are free from attacks. Mainly the attack aims at reducing the service reduction and increase the financial cost of the customer. So, particular measures have to be taken to ensure that the data is secure.

At the point when any association decide to store information or host applications on people in general cloud, it loses its capacity to have any entrance to the servers where data is facilitated. Thus, business related information and secret information is at danger from attacks. As per a late Cloud Security Alliance Report (CSAR), insider assaults are the greatest risk in the cloud computing. Along these lines, Service providers must keep an eye the employees who have the direct access to the servers in the data centre. Moreover, the server farms must be as often as possible checked for suspicious action.

3. Related Work

Many researchers have been conducted and as many number of different DDoS detection techniques have been proposed. Among these was a simple and efficient hidden Markov model scheme for host based anomaly intrusion detection. An entropy based anomaly detection framework to prevent DDoS attacks in cloud was reviewed, explored, investigated and proposed as an alternative solution. After investigating the correlativity changes of monitored network features during flood attacks, a covariance-Matrix modelling and detecting various flooding attacks was proposed. An experimented result was also analysed and presented to support a model that was instrumental to propose a model to detect flood based DDoS attack in cloud environment. It gave research results which support how effectively the flood attacks are detected.

Researchers also discussed how entropy based collaborative detection of DDoS attacks on community networks could effectively works in theory by applying information theory parameter called entropy rate. Different types of DDoS attacks at different layers of OSI model were discussed and presented, and finally, analysed the impact of DDoS attacks on cloud environment. The analysis of covariance model for DDoS Detection was discussed and the researchers described how the method can effectively differentiate the traffic between the normal and attack traffic. They also showed how the linear complexity of the method makes its ongoing identification in practical. Another detecting solution framework to predict multi-step attacks before they represent a serious security hazard is by using hidden Markov model. The study based the real time intrusion prediction on optimized alerts since alerts correlations play a critical role in prediction.

The design of two independent architectures for HTTP and FTP which uses an extended hidden semi-Markov model to describe the browsing habits of web searchers and detecting DDoS attacks were used in integration of fuzzy method [13]. A survey of different mechanism of DDoS attacks, its detection, and the various approaches to handle them was discussed and explored, to enable the clients review and understand those different parameters having impacts in their decision making process while selecting the right DDoS detecting scheme .

The scopes of DDoS flooding attack problems and attempts to combat them have been explored by categorizing the DDoS flooding attacks and classifying existing countermeasures based on different parameters. A comprehensive survey presented DDoS attacks, detection methods, detection tools used in wired networks and internet, and future research direction. The Security problem associated with cloud computing becomes more complex due to entering of new dimensions in problem scope related to its own main attributes. Researchers also proposed a detection scheme based on the information theory based metrics. The proposed scheme has two phases: Behaviour monitoring and Detection. Based on the observation, Entropy of requests per session and the trust score for each user is calculated. DDoS attacks could be detected using the application of Dumpster Shafer Theory. The theory was applied to detect DDOS threat in cloud environment.

It is an approach for combining evidence in attack conditions. The effectiveness of an anomaly based detection and characterization system highly dependent on accuracy of threshold value setting. And this approach described a novel framework that deals with the detection of variety of DDoS attacks. Cloud specific Intrusion Detection System was proposed and described a defence mechanism against the DDoS attacks. This defence mechanism discusses how to detect the DDoS attack before it succeeds.

Effectively detecting the bandwidth limit of a cloud network and the bandwidth currently in use helps to know when a DDOS attacks begin. An approach described based on fundamentals of information theory specifically Kolmogorov complexity to detecting distributed denial of service (DDoS) attacks was proposed. Despite its complexity the scheme enabled early detection.

4. Methodology

Detection of DDoS Attack is a basic measure towards defence. A sensible measure for performance of any detection method would be the area that it provides. Since such attacks is not based on exploitation of bugs or vulnerabilities but the definite volume of attack traffic , the attack traffic would be very similar to legitimate traffic increasing the risk in spiked traffic as an attack. One reasonable metric towards detection is the rate of resource degradation.

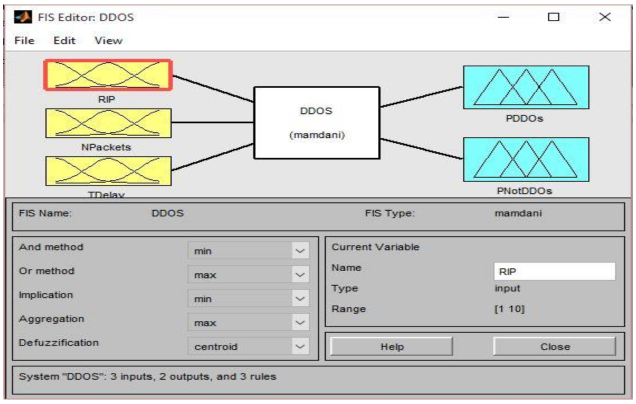
4.1. Experimental Setup

We carried the experimental setup in controlled environment of Matlab Software with a basic config of the laptop with 8 GB RAM. We have provided three input with different parameters and we are getting 2 output for the proposed work. This paper used Mamdani type fuzzy inference system on automated cloud computing framework [11,12].

This system used the three input parameters i.e. Total no. of roes in the trace file, total no. of packets sent by the node, total no. of packets received by the node and output parameters are With attack and without attack, the input parameters are responsible to check the behaviour of the node and based on that behaviour it is concluded that which node is Intruder node.

4.2. Fuzzy Inference Components:

We have taken Gaussian Membership function type for all the three input parameters, and Trigonometric membership function type for output parameters.



FIS Name: DDOS

FIS Type: mamdani

And method: min

Or method: max

Implication: min

Aggregation: max

Defuzzification: centroid

Current Variable

Name: RIP

Type: input

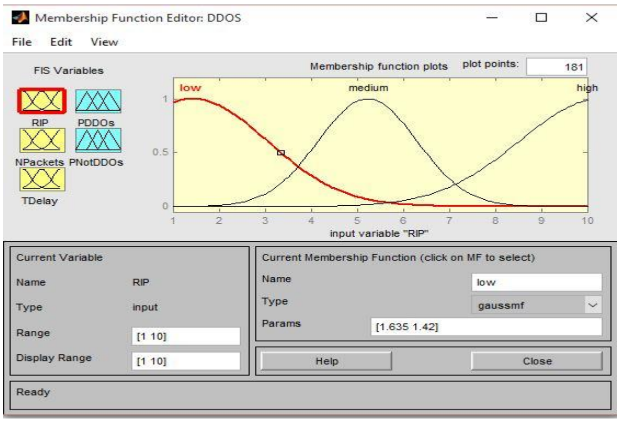
Range: [1 10]

System "DDOS": 3 inputs, 2 outputs, and 3 rules

Input 1: Recurrence IP address

Recurrence IP address is to generate recurrent IP at a continuous interval of time, thus it keep sending packets in occurrence to have a DDoS attack.

The Range and Display Range for this input parameter were set to 1 to 10 and Membership functions were set as Low, Medium and High.



plot points: 181

Current Variable

Name: RIP

Type: input

Range: [1 10]

Display Range: [1 10]

Current Membership Function (click on MF to select)

Name: low

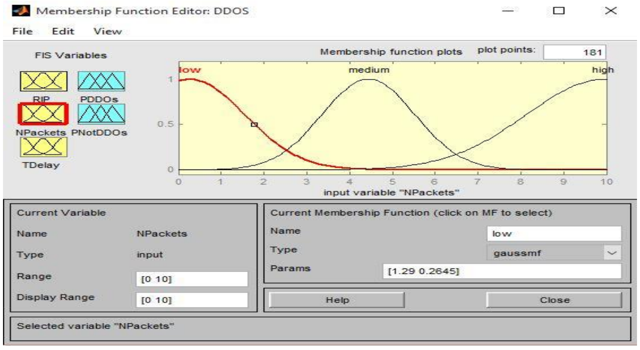
Type: gaussmf

Params: [1.635 1.42]

Ready

Input 2: Number of Packets

Number of packets depends upon the recurrent IP, the more the number of packets the more denial of service will take place.The Range and Display Range for this input parameter were set to 1 to 10 and Membership functions were set as Low, Medium and High.



plot points: 181

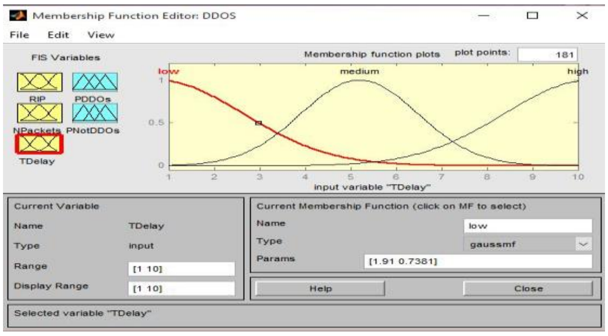
Current Variable
Name NPackets
Type input
Range [0 10]
Display Range [0 10]

Current Membership Function (click on MF to select)
Name low
Type gaussmf
Params [1.29 0.2645]

Selected variable "NPackets"

Input 3: Time Delay

The number of packets also depends on Time Delay. The more the time delay the lesser is the denial of service and vice versa.The Range and Display Range for this input parameter were set to 1 to 10 and Membership functions were set as Low, Medium and High.



plot points: 181

Current Variable
Name TDelay
Type input
Range [1 10]
Display Range [1 10]

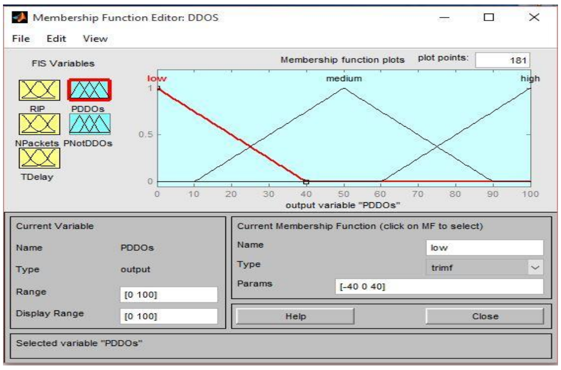
Current Membership Function (click on MF to select)
Name low
Type gaussmf
Params [1.91 0.7381]

Selected variable "TDelay"

Output 1: DDoS attack has been taking Place

DDoS has been detected depending upon the fuzzy rule system if the packets are more, then the DDoS attack has been taking place.

The Range and Display Range for this output parameter were set to 0 to 100 and Membership functions were set as Low, Medium and High.



plot points: 181

Current Variable
Name PDDOs
Type output
Range [0 100]
Display Range [0 100]

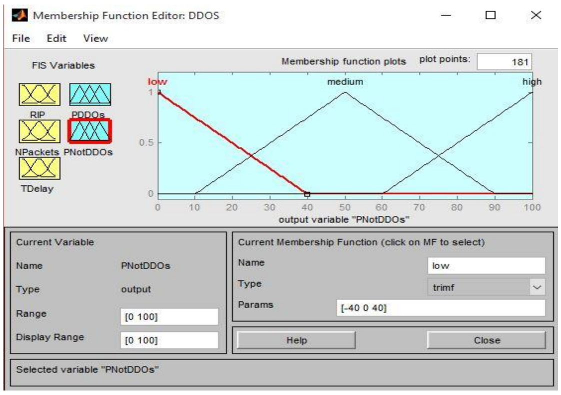
Current Membership Function (click on MF to select)
Name low
Type trimf
Params [-40 0 40]

Selected variable "PDDOs"

Output 2: DDoS is not detected

The number of packets are less thus the denial of service does not take place.

The Range and Display Range for this output parameter were set to 0 to 100 and Membership functions were set as Low, Medium and High.



plot points: 181

Current Variable
Name: PNotDDOs
Type: output
Range: [0 100]
Display Range: [0 100]

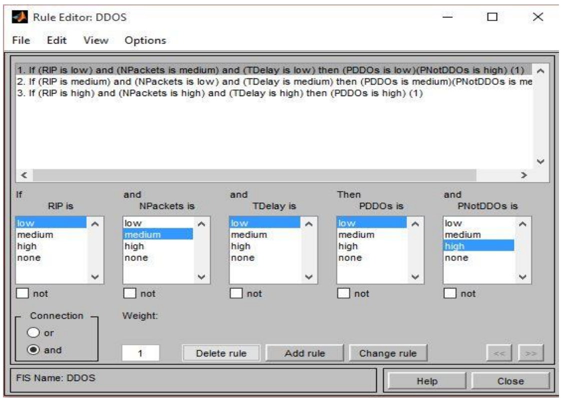
Current Membership Function (click on MF to select)
Name: low
Type: trimf
Params: [-40 0 40]

Selected variable "PNotDDOs"

Using Rule Editor Fuzzy rules were created according to low, medium and high parameters of all the input and output parameter.

Fuzzy rules:

1. IF (RIP is low) and (NPackets is medium) and (TDelay is low) THEN (PDDoS is low) (PNotDDoS is high).
2. IF (RIP is medium) and (NPackets is low) and (TDelay is medium) THEN (PDDoS is medium) (PNotDDoS is medium).
3. IF (RIP is high) and (NPackets is high) and (TDelay is high) THEN (PDDoS is high).



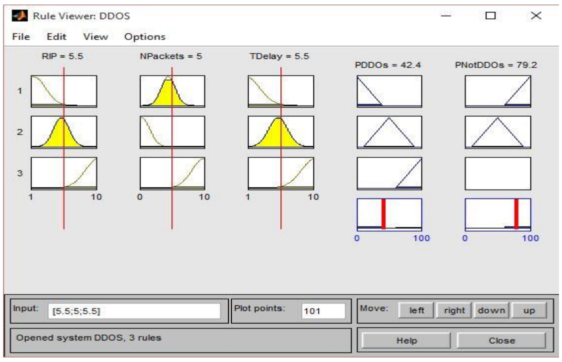
1. If (RIP is low) and (NPackets is medium) and (TDelay is low) then (PDDOs is low)(PNotDDOs is high) (1)
2. If (RIP is medium) and (NPackets is low) and (TDelay is medium) then (PDDOs is medium)(PNotDDOs is me
3. If (RIP is high) and (NPackets is high) and (TDelay is high) then (PDDOs is high) (1)

RIP is: low
NPackets is: medium
TDelay is: low
PDDOs is: low
PNotDDOs is: high

Connection: ○ or ● and
Weight: 1

FIS Name: DDOS

5. Results

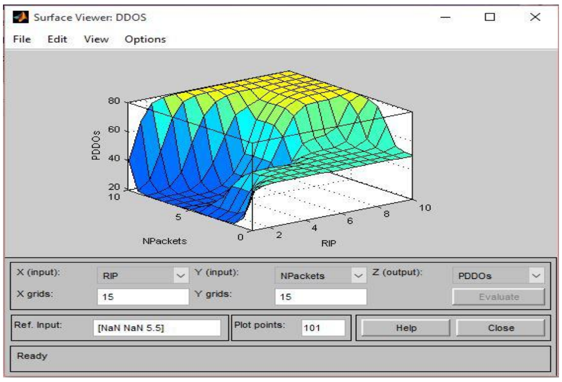


Input: [5.5;5;5.5]
Plot points: 101

Opened system DDOS, 3 rules

In the above diagram the probability of the parameters are changed and monitored accordingly to check how the model of rules we generated works.

According to the above fuzzy rules the 3D view of the rules were generated using surface viewer. In which the dark blue surface represents low packets of DDoS, light blue represents medium packets of DDoS and yellow surface represents high packets of represents.



X (input): RIP
Y (input): NPackets
Z (output): PDDOs
X grids: 15
Y grids: 15
Ref. Input: [NaN NaN 5.5]
Plot points: 101
Ready

6. Conclusion

The fuzzy systemsmodel has the unique feature to scale computer resources on demand, andgive users a number of advantages to advance their conventionalCluster system. In addition, there is no upfront investment toupdate infrastructure, labour and no increasing expenses. However, we being securityexperts, the problem we see is recurrence of the same mistakes. Those were made with the development of the internet. Thesemistakes are compared to functionality and performance whichtook precedence over security. Security should in fact beimplemented it alongside functionality and performance. Thus in this study we have build a fuzzy systems for the DDoS attack by providing the rules and detecting whether a DDoS attack has been taken place or not.

References

1. An NTT Communications, “Successfully combating DDoS Attacks”, White Paper, August 2012.
2. Sanjay B Ankali and D.V Ashoka, “Detection Architecture of Application Layer DDoS Attack for Internet”, Advanced Networking and Applications, volume 03, issue 01, Pages 984-990, 2011.
3. A.B. Kulkarni, S.F.Bush, and S.C. Evans, “DetectingDistributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics”, GE Research & Development Center, February 2002.
4. S. Abdelsayed, D. Glimsholt, C. Leckie, S. Ryan, and S.Shami, “An Efficient Filter for Denial-of-Service Bandwidth Attacks”, Proc. of the 46th IEEE Global Telecommunications Conference (GLOBECOM03), pp. 1353-1357, 2003.
5. Ankush Rai, Automation In Computation, Journal of Advances in Shell Programming, Volume 1, Issue 2 2014.

6. Lau F, Rubin S H, Smith M H, et al. Distributed denial of serviceattacks[C] Proceedings of IEEE International Conference on Systems Cybernetics. New York IEEE Press,2000:2275-2280.
7. P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.
8. S. M. Specht, and R. B. Lee, Distributed Denial of Service:Taxonomies of Attacks, Tools and Countermeasures, in Proc. 17thInternational Conference on Parallel and Distributed Computing Systems, pp.543-550, 2004.
9. A.M. Lonea, Daniel Elena Popescu, Huaglory Tianfield,“Detecting DDoS attacks in cloud computing environment”, International Journal of Computer communication, ISSN 1841-9836, 8(1):70-78, February, 2013.
10. R. Chen, J. M. Park, and R. Marchany, TRACK: A novel approachfor defending against distributed denial-of-service attacks, TechnicalReport TR-ECE-06-02, Dept. of Electrical and Computer Engineering,Virginia Tech, Feb. 2006.
11. X. Liu, A. Li, X. Yang, and D. Wetherall, Passport: secure andadoptable source authentication, in Proc. 5th USENIX Symposium on Networked Systems Design and Implementation (NSDI’08), San Francisco, CA, USA, pp. 365-378, 2008.
12. Ankush Rai, Automation of Community from Cloud Computing, Journal of Advances in Shell Programming, Volume 1, Issue 2 2014.
13. Ankush Rai,Shell Implementation of Neural Net Over The Unix Environment for File Management: A Step Towards Automated Operating System, Journal of Operating Systems, Vol 1, Issue 2 (2014).

Corresponding Author:

R Jagdeesh Kanan*

Email: jagadeeshkannan.r@vit.ac.in