ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

A Survey for DOS Attack Based on Multivariate Correlation Analysis

Avinash.S.Devare[1], Pratibha Kamble[2], Banu Tamboli[3],Monika Shelake[4], Varsha Vahadne[5]

Assistant Professor, Dept. of Computer Engineering, JSCOE, Hadapsar, Pune, India[1]

UG Student, Dept. of Computer Engineering, JSCOE, Hadapsar, Pune, India[2,3,4,5]

ABSTRACT: In the networking systems, such as Web servers ,database servers ,cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service attacks cause serious impact on these computing systems. We are present a study on the recent approaches in handling Distributed Denial of Service attacks. DDoS attack is the fairly new type of attack to cripple the availability of Internet service and resources. During in the last decade, anomaly detection has attracted to the attention of many researchers to overcome the weakness of signature-based IDSs in the detecting novel attacks, and KDD CUP'99 is the mostly widely used data set for the evaluation of these systems. We are survey different papers describing methods of defence against DDoS attacks based on entropy variations,traffic anomaly parameters, neural networks, device level defence, botnet flux identification and application layer DDoS defence.

KEYWORDS: Denial of Service attack, network traffic characterization, Intrusion Detection System(IDS), Multivariate correlation, KDD cup99, DDoS attacks, DDoS Defence

I. INTRODUCTION

DENIAL-OF-SERVICE (DOS) attacks are one type of aggressive and intrusive behaviour to online servers. DoS attacks degrade the availability of a victim, which can be a host, router, or an entire network[1].Intrusion detection(ID) is defined as "the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges[3][4].securities have been precedence throughout the transmission of the data in wireless network, be it through ad hoc, Wi-Fi or wireless sensor network(WSN)[13].

1) Multivariate Correlation Analysis :

MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition[1].Makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined[7].

2) Denial-of-Service(DoS) :

DoS is an attack that make available or fully consume the memory to its intend users. Denial-of-Service is one type of attacks makes some computing or a memory resources too busy or too full to handle legitimate request, or denies legitimate users access to a machine. Example Ping of Death, Smurfetc[10].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

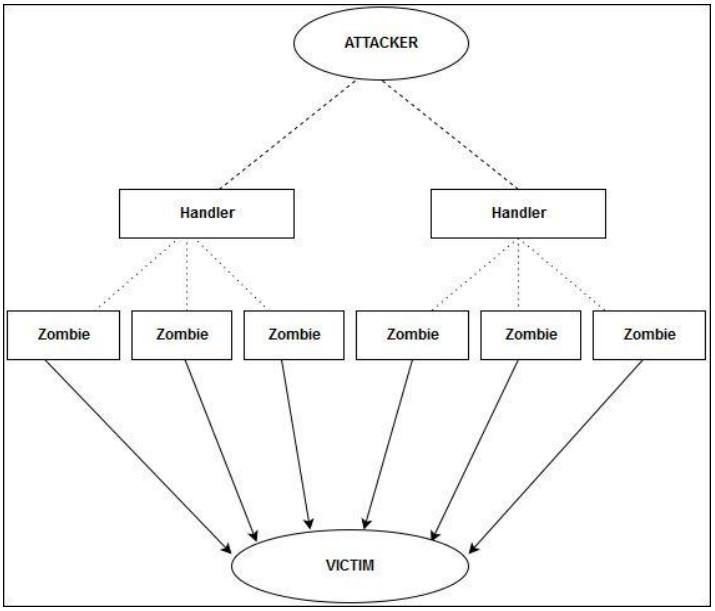

Fig 1: Architecture of DDoS Attack

3) KDD CUP 99 DATASET :

Knowledge discovery in database or KDD datasets in the largest datasets use for IDS.The KDD dataset is employed in international knowledge discovery and the data miming tools.KDD Cup 1999 dataset is consist of large number of redundant records[7].This dataset is given as a input to proposed system to performed training and testing operations[11].

4) Network Intrusion Detection System Using Fuzzy Logic :

The anomaly-based intrusion detection makes use of effective rules identified in accordance with the designed strategy ,which is obtained by mining the data effectively. The fuzzy rules generated from the proposed strategy can be able provide better classification rate in detecting the intrusion behaviour.[7].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

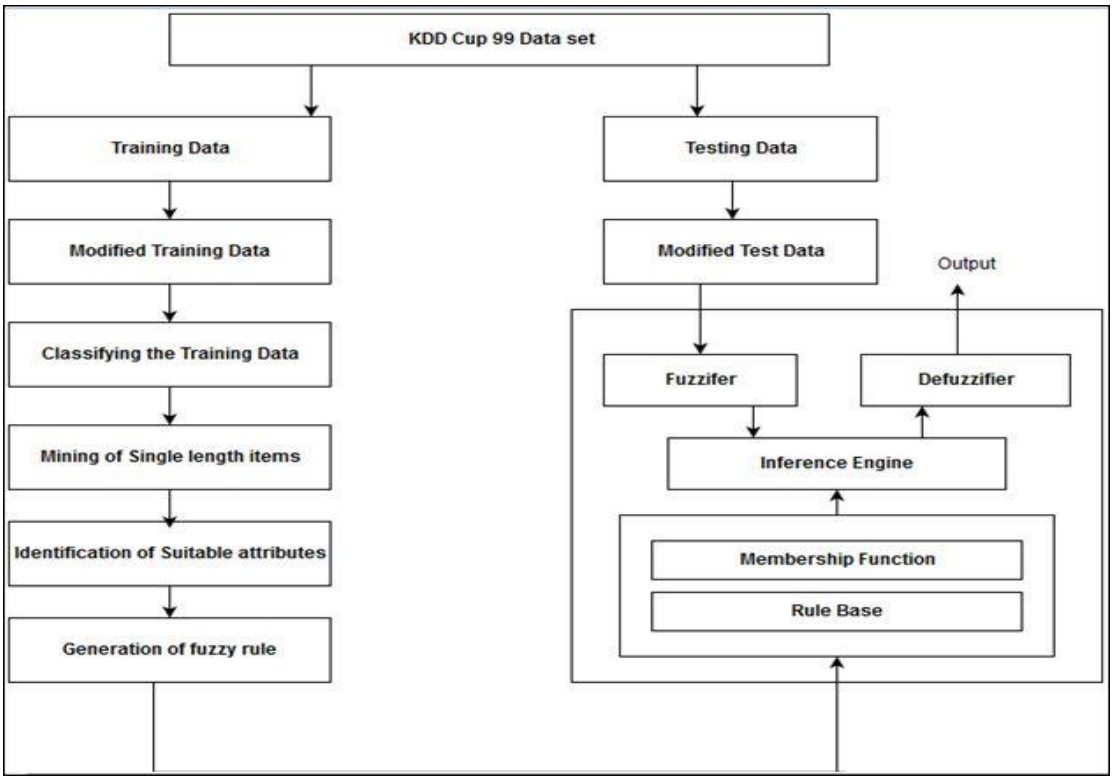

Fig 2: Overall steps of the proposed intrusion detection system

II. SYSTEM ARCHITECTURE

It is a large scale attack in a co-ordinated fashion ,which is typically launched indirectly with the help of other computers in internet.There are several kinds of DDos attacks. There are two main classes of such attacks:(1)bandwidth depletion and (2) resource depletion attacks. In case of bandwidth depletion attack, The victim network is flooded with unwanted traffic that prevents that prevents legitmate traffic from reaching the victim computer.

Step 1: Network traffic to the internal network where protected servers reside in and are used to form traffic records for a well –defined time interval. Monitoring and analysing at the destination network reduce.

Step 2: Multivariate correlation Analysis, in which the "Triangle Area Map Generation" module is applied to extract the correlation between two distinct features within each traffic record coming from the first step or the traffic record normalized by the "Feature Normalization" module.

Step 3: Our MCA method normalization technique are explained ,The anomaly-based detection mechanism is adopted in decision making. It facilitates the detection of any Dos attack without requiring any attack relevant knowledge[15]

Sample-by-Sample Detection:

The group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism[16]

The proof was based on an assumption that the samples in a tested group were all from the same distribution(class).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

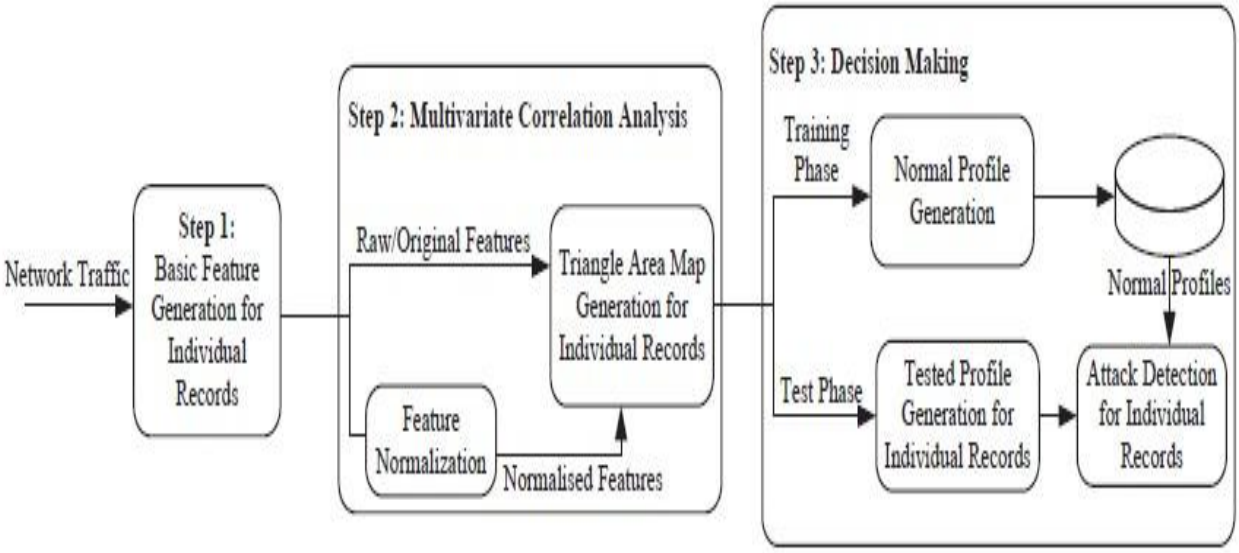

Fig 3: Framework of the proposed denial-of-service attack detection system

III . ADVANTAGES AND DISADVANTAGES

I. Advantages :

1) This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only
2) We begin by presenting a number of preliminary definition ,the network delay are discrete.

II. Disadvantages :

1) This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.
2) We begin by presenting a number of preliminary definition ,the network delay are discrete.

IV . CONCLUSION

We have developed an anomaly based intrusion detection sytem in detecting the intrusion behaviour within a network. A fuzzy decision-making module was designed to build the system more accurate for attack detection, using the fuzzy inference approach. Intrusion detection system is one of the most important security policy of computer. The MCA-based DoS attack detection system which uses the triangle area based MCA technique and the anomaly-based detection technique is very useful to extracts the geometrical correlation in each individual pairs of two distinct features.

REFERENCES

[1] IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014
[2] R. Shanmugavadivu et al./ Indian Journal of Computer Science and Engineering (IJCSE)
[3] www.ijraset.com Volume 3 Issue IV, April 2015 IC Value: 13.98 ISSN: 2321-9653International Journal for Research in Applied Science & Engineering Technology (IJRASET)
[4] Web Intelligence & Distributed Computing Research Lab Green Tower, C-9/1, Golf Green, Calcutta 700095, India debajyoti.mukhopadhyay@gmail.com

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

[5] IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 9, SEPTEMBER 2015 2519
[6] IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.12, December 2009
[7] The Following Paper Was Originally Published In The Proceedings Of The 7th Usenix Security Symposium San Antonio, Texas, January 26-29, 1998
[8] García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers and Security, 28, 1-2, 18-28 (2009)
[9] International Journal of Recent Scientific Research Research Vol. 4, Issue, 9, pp.1314- 1319, September
[10] A. Mitrokotsa, and C. Douligeris, "Denial-of-Service Attacks," Network Security: Current Status and Future Directions (Chapter 8), WileyOnline Library, pp. 117-134, June 2006.
[11] IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308
[12] ISSN (e): **2250 – 3005** || Vol, 04 || Issue, 8 || August – 2014 || International Journal of Computational Engineering Research (IJCER)
[13] Thomas Dubendorfer , Matthies Bossardt,Bernhard Plattner; Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation; Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)-Workshop 17 –Volume 18,2005.
[14] Stephen Specht, Ruby Lee; Taxonomies of Distributed Denial of Service Networks, Attacks, Tools,and countermeasures; Department of Electrical Engineering, Princeton Architecture Laboratory for Multimedia and Security, Technical Report CE-L2003-03, May 16, 2003
[15] D.E.Denning,"An Intrusion-dection Model," IEEE Transactions on Software Engineering, pp.222-232,1987.
[16] S.Jin, D.S. Yeung, and X.Wang, "Network Intrusion Detection in covariance feature Space," Pattern Rcognition ,vol.40.pp.2185-2197,2007