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, Special Issue 6, May 2015

Denial-of-Service Attack Prevention Using IP Traceback Input Dubugging

R. Suganya[1], T. Manigandan[2]

P.G. Student, Department of CSE, P. A. College of Engineering and Technology, Pollachi, Tamilnadu, India[1]

Professor/Principal, P. A. College of Engineering and Technology, Pollachi, Tamilnadu, India[2]

ABSTRACT: Denial-of-Service attack causes major problem in the environment that affects most of the hardware, software and networks. The Denial-of-Service attack affects the system and the resources are not accessible by the end user by denying services. Internet Protocol traceback method is used for the prevention of Internet Protocol spoofing that makes the system reliable. The traceback method use Input debugging that trace the origin of attacker by tracking the upward links from the victims. Hybrid detection mechanism also used to differentiate illegitimate user from the normal user. Denial of service attack detection system that uses Multivariate Correlation Analysis for accurate network traffic characterization by extracting the geometrical correlations between network traffic features and enhance the speedup of the process.

KEYWORDS: Denial-of-Service attack, IP Traceback, Input Debugging, Hybrid detection, Multivariate Correlation Analysis.

I.INTRODUCTION

Network security has various policies by network administrator to prevent the system from unauthorized access or modification of data and monitor other illegal access. Denial-of-service (DoS) attack comes under the category of active attack [4]. DoS attack is an attempt to make a system, machine or network resources unavailable to its user by blocking or denying the services [15].

Intrusion Detection System (IDS) is a security mechanism used to detect the attack with the aim of preserving system from large damages and identify the vulnerabilities and give warning if unauthorized user enters into the system. Intrusion detection technique can be categorized into two types Misuse based detection and Anomaly based detection [7].

Misuse based detection also called as signature based detection that misuse-based detection attempts to detect attacks by monitoring network activities and looking for matches with the existing attack signatures or rules. Anomaly detection technique [11] is used to detect both known and unknown attack by learning the pattern of legitimate network traffic. The action that is significantly deviates from normal the normal behavior is considered as an intrusion. The intruder may be from outside the network or legitimate user of the network. Anomaly detection is better compared to the misuse based detection.

Recent studies focused on Denial of service attack detection. D. E .Denning proposed an efficient methodology called statistical model that detect the DoS attack in an efficient manner [1]. S. T. Sarasamma et al. solved the problem of implementing individual page fault in a practical manner and also considered the problem of data leakage. Multilevel hierarchical Kohonen Net for an intrusion detection system is presented [5]. Each level of the hierarchical map is modeled as a simple winner-take-all K-map. C. Yu et al. introduced collaborative detection method for detecting intrusion [6]. The new defense system is suitable for efficient implementation over the core networks operated by Internet service provider. S. Jin et al. proposed covariance matrix based approach to improve the detection accuracy compared to other various methods previously available in the practical.

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, Special Issue 6, May 2015

W. Hu and S. Maybank introduced Adaboost Algorithm for reducing false alarm rate and improve the detection accuracy [9]. K. Lee et al. considered cluster analysis is easy to implement and it detect the attack in the early phase. After that, perform cluster analysis for proactive detection of the attack [8]. The disadvantage of this method is not suitable for extracting more variables. A. Tajbakhsh et al. proposed the method called fuzzy association rules for efficient classification of dataset [12]. A framework based on data mining techniques is proposed for designing IDS. A. Jamdagni et al. focused the method Geometrical structure based analysis to discriminate normal patterns and attack patterns in real time, to detect the attack against web application. A number of relevant approaches have been proposed continuously and inaccurate detection is the problem of detecting malicious activities and large number of false alarm is sent to the admin so to overcome the entire above disadvantages use hybrid detection algorithm that reduces the false alarm and increases the intrusion detection rate.

II.IP TRACEBACK TECHNIQUES

IP (Internet Protocol) trace back is a method to find the source of IP address without depending on source IP field in the packet. IP trace back algorithm work against the DoS attack and prevent the system from attacker [10]. The new method controls the entire router and that extract the effective features of network traffic to sample its distribution. IP trace back methods classified into two types based on their behavior are Reactive and Proactive methods. Proactive method takes the precautionary action in preventing the attacks. Reactive methods try to respond to the attack after detection of attack or else aim to identify the source of attacks that means use some traceback techniques. The proactive method use ingress filtering to prevent the attacker. The reactive IP traceback mechanisms classified as Link Testing, Log-based, Internet Control Message Protocol (ICMP) traceback and Packet marking technique.

Link testing method also called as hop by hop testing that testing network links between routers to determine the origin of the attacker's traffic. Input debugging is implementation of the link testing approach. Administrator determines incoming network links for specific packets [16]. Controlled flooding has test the links by flooding with large network traffic and observing attacker from the traffic. IP address spoofing or IP spoofing refers to the creation of Internet Protocol packets with a forged source IP address, called spoofing, the purpose of identity the sender or impersonating another computing system.

III.IP TRACEBACK INPUT DEBUGGING

Develop a complete framework for our DoS attack detection system use sample by sample detection mechanism [17]. The system performs intrusion detection process through various stages of development process that shown in Fig.1. The processes are happen continuously one by one.

In network traffic the number of new incoming traffic are entered into the system. The numbers of traffic records are generated from the client. Each record is identified by using the IP address after the sampling process of IP address. Once the traffic records enter into the system the basic features are normalized in the form the traffic records for well defined time interval.

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, Special Issue 6, May 2015

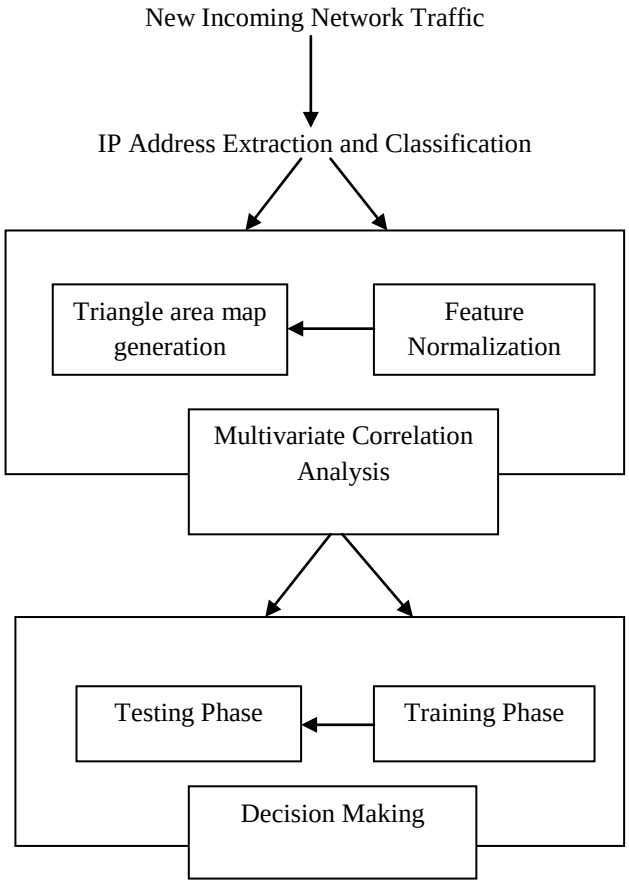

Fig. 1 Intrusion Detection System

The misuse based detection is first applied to distinguish the normal records and the remaining new records are comes under the process of anomaly detection.

Algorithm

Input: Source IP address (ip) of the incoming packets.
Output: Previously unseen or new source IP addresses (newIP).
Step 1: if NOT ((ip in W) OR (ip in R)) then
Step 2: INC(newIP)
Step 3: add ip to R
Step 4: end

IP classification algorithm (ipac) is a form of misuse based detection system that takes the input as source IP address of the incoming packets. The two different lists available are White list (W) and Recent list (R). Initially both the list is set to empty in the process. The normal traffics are stored in the white list and recent list is used to store the new previously unseen IP address. The source IP address is extracted from the new incoming traffic. Then, check whether the new incoming IP address present in the white list or recent list. If it is not present in any of the list increment the value of new IP address and add it to the recent list. The output of ipac algorithm is to written the new IP address.

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, Special Issue 6, May 2015

In sample by sample detection that maintains the higher probability than the group based detection [18]. In group based detection, it is difficult to achieve group of sequential sample only from the same distribution so sample by sample detection is better from the equation (1) and (2). The benefits of sample by sample detection able to detect the attack in a prompt manner and intrusive samples are sampled individually. Traffic samples are independent of one another and traffic records follow normal distribution so the intrusion detection frame work follows sample by sample detection.

$$k = 1, \quad Q(k) = q_1 = q_2 \qquad (1)$$

$$k > 1, \quad Q(k) = \frac{1}{2^k} q_1 = \frac{1}{2^k} q_2 \qquad (2)$$

In Multivariate Correlation Analysis approach that employs triangle area for extracting the correlative information between the features within an observed data object [14]. Attack traffic behaves differently than the legitimate network traffic and their properties are identified by the statistical properties.

Algorithm

Input: Time series of the rate of new source IP addresses.
Output: System State – A or NA
if (in state NA) then
if NOT (StateChange(NA)) then
add R to W
else
state = A
send white-list to the application
R = empty
end
end
else if (in state A) then
if StateChange(A) then
state = NA
inform the application to stop using the white-list
end
end

DoS algorithm is applied on the output of ipac algorithm that is used to determine whether the new IP address is normal traffic or attack traffic. DoS algorithm have two states are Not under Attack (NA) and Under Attack (A). If the system state changes from NA to A then the system will remove the IP address from the recent list and block the particular IP address. The state changes from A to NA then the new IP address is added to the white list.

The hybrid detection system considers only the timing but if it combined with the traceback method that considers the path of the traffic and their corresponding distance. The technique will analyse the path if the particular path having traffic then it choose an alternative path as a new route so the user can avoid the network traffic in the process. The system will choose the busy traffic path as a new route then it slowdown the process and that type of requests are arrived from the attacker. So the user needs to examine the particular request and trace the real origin of the attack.

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, Special Issue 6, May 2015

IV.EXPERIMENTAL RESULTS

Denial-of-Service is an attack that makes an information or data unavailable to user of the system. The server is connected to the back end server that establishes connection with the client program. The cache is used for storing the route of the traffic. The user needs to mention the route for the traffic which is maintained by the trace back manger.

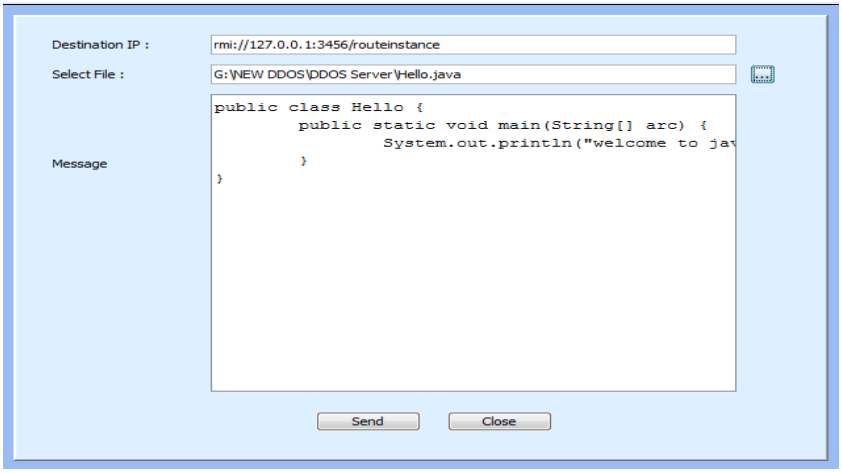

Fig. 2 Client Request to Server

The client will give the program request to the server that includes the destination IP address is shown in Fig. 2. The traffic records should go through the particular path that will generate by the system automatically. The traffic free route selected as a current path by the automatic system. The possible combination routes are stored in the database. The user needs to start the cache and traceback manager. The cache will store the new route and traceback manager will trace the origin of the attack. The user will initialize different ports

For each program request the normal profile was generated in the system which is based on the time interval. The differences between the current and previous requesting time intervals are shown in Fig. 3. The response from the server is output for the program that may receive in various time intervals.

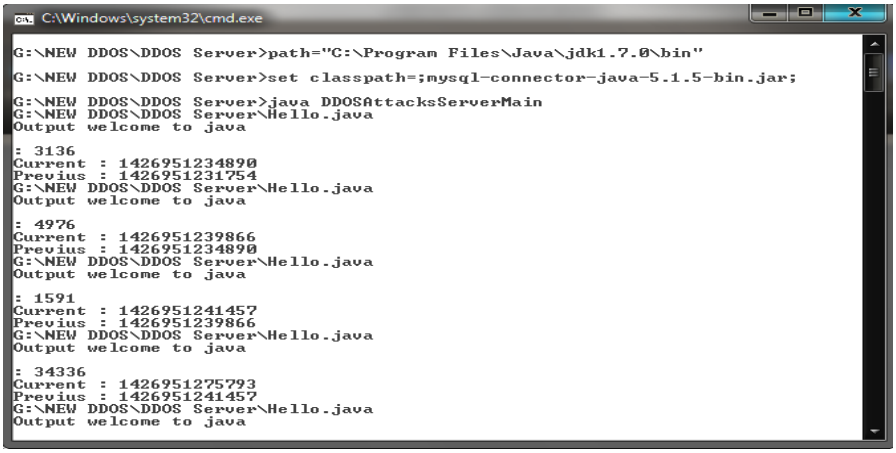

Fig. 3 Profile Generation

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, Special Issue 6, May 2015

The numbers of program requests are given to the server from the client. For each program request to the server the new routes of the requests are added in the cache of the system.

The system must avoid the IP spoofing so it trace the real source of the attack even if having the additional port attached from the server. The user can able to determine the origin IP address of the new requests and number of times the request received from the client. The requests are receive from particular URL then the normal route compared with current rout if it differs identified as hacker. The comparison is done by the traceback manager. The hackers are added to the list 1 and normal users are added to the list 0.

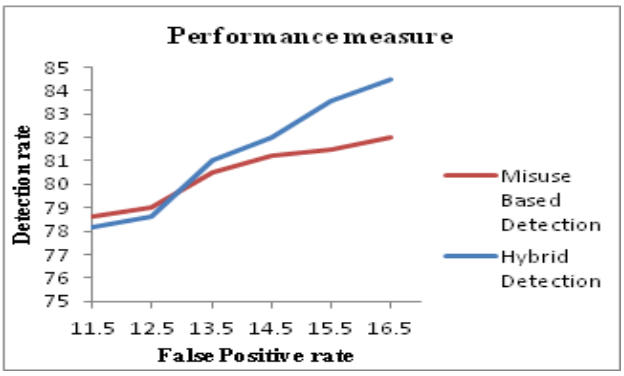

Fig. 4 Detection Method Comparison

Hybrid detection method provides more accurate characterization of attack than the other detection method that is shown in Fig 4. If the detection rate increases then the corresponding false positive rate also increased. Hybrid method provides better result than misuse based detection.

V.CONCLUSION

The IP traceback method with hybrid detection mechanism is used for the prevention and detection of Denial-of-Service attack. The hybrid detection is the combination of misuse based detection and anomaly based detection that detects the attack in less time compared with other various detection method. If the system using hybrid detection alone then it not possible to recover false positive problem but if it combine with the IP traceback the drawbacks are rectified. The traceback method also avoids the problem of IP spoofing and improves the detection rate.

REFERENCES

[1] D. E. Denning, "An Intrusion-Detection Model," *IEEE Trans. Software Eng.*, vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.
[2] G. V. Moustakides, "Quickest Detection of Abrupt Changes for a Class of Random Processes," *IEEE Trans. Information Theory*, vol. 44, no. 5, pp. 1965-1968, Sept. 1998.
[3] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," *Computer Networks*, vol. 31, pp. 2435-2463, 1999.
[4] A. A. Cardenas, J.S. Baras, and V. Ramezani, "Distributed Change Detection for Worms, DDoS and Other Network Attacks," Proc. *The Am. Control Conf.*, vol. 2, pp. 1008-1013, 2004.
[5] S. T. Sarasamma, Q.A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," *IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 35, no. 2, pp. 302-312, Apr. 2005.
[6] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Trans. Parallel and Distributed Systems*, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.
[7] S. Jin, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," *Pattern Recognition*, vol. 40, pp. 2185- 2197, 2007.
[8] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
[9] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," *IEEE Trans.* Systems, Man, and Cybernetics Part B, vol. 38, no. 2, pp. 577-583, Apr. 2008.
[10] C. Gong and K. Sarac,"A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed System, vol. 19, no. 10, pp. 1310–1324, 2008.

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, Special Issue 6, May 2015

[11] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers and Security*, vol. 28, pp. 18-28, 2009.
[12] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion Detection Using Fuzzy Association Rules," *Applied Soft Computing*, vol. 9, no. 2, pp. 462-469, 2009.
[13] C. F. Tsai and C. Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," *Pattern Recognition,* vol. 43, pp. 222-229, 2010.
[14] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," *Proc. Conf. Neural Information Processing*, pp. 756-765, 2011.
[15] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," *IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073-1080, June 2012.
[16] Y. Wang , S. Su, Y. Yang and J. Ren , "A More Efficient Hybrid Approach for Single-Packet IP Traceback," 16th Euromicro Conference on Parallel, Distributed and Network-Based Processing, pp. 275-282, 2012.
[17] Z. Tan, A. Jamdagni and P. Nanda "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," *IEEE Trans. Parallel and Distributed Systems*, vol. 25, no. 2, pp. 447-456, 2014.