Second International Conference on Nexgen Technologies
Sengunthar Engineering College, Tiruchengode, Namakkal Dist. Tamilnadu (India)
8th - 9th March 2019 www.conferenceworld.in ISBN : 978-93-87793-75-0

AN EFICIENT DDOS TCP FLOOD ATTACK DETECTION AND PREVENTION SYSTEM IN A CLOUD ENVIRONMENT

B. Raj Kumar[1], S. Manoj Kumar[2], A. Reshma[3],

D. MUTHU SANKAR[4]

[1,2,3]*Final year students of Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode,(India)*

[4]*Associate professor of Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode,(India)*

ABSTRACT

Nowadays the number of cloud projects has been increasing still the privacy, security and availability of data in the cloud resource is a crucial and challenging research issue. Generally, DDoS is the major cybercrime attacks it mostly happen in website to hack all the data. DDoS or TCP flood attack can consume the bandwidth and damage the entire cloud project within a short period of time. Detection and prevention of those attacks in cloud projects are important, especially for eHealth clouds. In public clouds this system present a new classifier system for detection and prevention of DDoS TCP flood attack. In this CS_DDoS system offered a solution to stored records or data in a secured manner by classified the incoming packets and made a decision based on the classification result. In detection phase the CS_DDoS identify and determines whether this packet is originated from a normal client or attacker. In other case the prevention phase some packets are classified as malicious those packets will be denied access to the cloud service provider and finally client IP will be blacklisted. In CS_DDoS system performance can be classified by using the different classifiers such as LS-SVM, naive Bayes, K-nearest, and multiplayer perceptron. This CS_DDoS system gives the best performance when LS-SVM classifier is used. It easily find out the TCP flood attacks with about 97%accuracy and with a kappa coefficient of 0.89 when the attacker from a single source and 94% accuracy with kappa coefficient of 0.9 form a multiple source or attackers. The result of this system is discussed in terms of accuracy, time complexity and finally validated by using a K-fold cross validation model.

Keywords: CS_DDOS- Classification System_Distributed Denial Of Service Attack,LS_SVM- Least Square_Support Vector Machine,IDS- Intrusion Detection System,IPS- Intrusion Prevention System.

I. INTRODUCTION

The DDoS attack or TCP flood attack in which attackers flood of data packets is used to remove all its resources and consume its bandwidth. This attack easily spread over to all the machines and it is not easy to differentiate the authenticated users from attackers. DDoS attack could be established in two different ways one is either direct or indirect attack. In direct attack it directly targets the victim machine and damage the victim machine entirely. In indirect attack not target the victim machine directly it will prey on other elements with which the victim machine or client machine directly associated with that machine and hinder their work. This attack which is the second most attack in cybercrime attack which is based on the investigation of United States Federal Bureau of Investigation(FBI).

In many of the public and private sectors are quickly increasing the usage of cloud computing technology, specifically in health sector. Day by day the most of the cloud users are under threat. In 2009,electronic cyber crime study published the KPMG in collaboration with eCrime congress it tells about privacy,data security and other threats. Most of the cloud users could understand the cloud resources and their privacy, as time increases at the same time threat also increases.In general there are many procedures are adopted to mitigate the DDoS flood attacks in such kind of huge classification, encryption technique. Those DDoS attacks are implemented in many forms the form of these attacks cannot be foreseen. This DDoS classifier system is totally classifier based and it can be arrive at different cloud system. This kind of classification system can be varied by certain procedures such as Least square vector machine, naive Bayes, K-nearest and multiplayer perceptron.

There are many mechanisms proposed to detect and prevent the DDoS attack, many of the proposed system do not provide high accuracy. In industrial deployment this DDoS attack protection mechanism face scalability issues due to network problem like larger and smaller bandwidth. This proposed cloud computing system is not an efficient system and it will rise many problems during classification of incoming packets.

II. EXISTING SYSTEM

The exponential growth of computer/network attacks are becoming more and more difficult to identify the need for better and more efficient intrusion detection systems increase in step. The main problem with current intrusion detection systems is high rate of false alarms. The design and implementation of traffic coming from clients and the traffic originated from the attacker is not implemented. If the attacker identifies the port, he/she can intrude or interfere in the communication and flood DOS attack and can hack communicating data. Clock drifts method is not reliable because, DDOS attacks are flooding of large number of request by the attacker, which leads to decrease in bandwidth, and low latency time.

III. PROPOSED SYSTEM

In our proposed system we need to collect network traffic packets and other flow data information in real time and pre-process network traffic and finally predict the DDoS attack. This proposed system uses firecol it manually "Invite the Attacks" with confidentially. This firecol provides effective solution to increase the security and reliability of the network. This type of firecol it acts as an alternative server for the process of forwarding request to the balancer detects traffic as an attack on the server. There are different detection and forensics methodology can can be used to collect all information on the intruder those who are not aware of that they are not using "real" server. It provides active communication between server and client and then in this system it is difficult to intrude into communications, probability of hacking is very low. And then it is an effective and efficient response processing for incoming request. Even in presence of DDoS attack active communications could not be affected.

IV. IMPLEMENTATION

MODULES

A.*Application Server:*

This model acts as application server module, which initially, is started up on different access points. Then application server waits for any incoming connection that is from network clients for communication and service providing. In this module, the server can handle multiple clients o all the available points on which the server is started.

B.*Network User:*

This module represents the normal network clients, where the user can test the latency of the application server by pinging the server with test packets. Moreover, the user can check the Ethernet and protocol statistics of the client machine and can monitor active connections of the clients system. The client can connect to the application server via any available access points, and can make requests to the server and can receive response for the requested service

C.*Attacker:*

This model acts as a network attacker or intruder, who tries to intrude into the network and perform some malicious activities by probing and compromising the access points for misuse. In this module, POD (Ping Of Death) attack, port scanning and syn flooding attack has been implemented and liberated into the network for accessing the server by compromising access points.

D.*Intrusion Detector:*

This module we implemented out proposed frame work for detecting rogue access points by using FireCol. The core of FireCol composed of intrusion prevention systems (IPSs) located at the internet service providers (ISPs) level.

Initially the RAP detection system is trained with observables and the hidden states. Secondly, RAP detection system is started monitoring the network traffic for detecting malicious network activities such as probing and compromising the access pints.

All the registered traffic and their activity results are tracked in the RAP detector logs and the statistics for the individual access points about their own network activities are represented graphically and the overall detection accuracy of our proposed system is also depicted graphically.

E.*METHODOLOGY*

FIRECOL ALGORITHM:

1. If b_i ^(IPS_id ≠ null) then
2. If IPS_id == myID then
3. b_i = false;
4. Return
5. else
6. $rate_i \leftarrow rate_i + F_i$
7. if $rate_i > cap_i$ then
8. b_i= false;
9. raise DDoS alert;
10. return
11. Else
12. nextIPS.CheckRule(IPS_id,i,rate,cap_i)
13. end if
14. end if
15. Else
16. b_i = true;
17. next IPS.checkRule(myID,I,0,cap_i)
18. end if

PSO ALGORITHM

PSO is influenced by social behavior of animal like flock of birds finding food source. A Particle is analogue to bird flying through problem space. Each Particle contains velocity and solution. The performance of particle is measured by fitness value which is problem specific.

In this algorithm particles are initialized randomly. Each Particle contains fitness value which is calculated by fitness function. Each Particle known its best position p^i_k and best position among entire group of particles p^g_k

$$V^i_{k+1} = v^i_k + c_1 r_1 (p^i_k - x^i_k) + c_2 r_2 (p^g_k - x^i_k)$$

$$X^i_{k+1} = x^i_k + v^i_{k+1}$$

V^i_k is the particle velocity, x^i_k is the current particle. P^i_k and p^g_k are defined as stated before. R_1 and r_2 is a random number between (0,1). $C_{1,}c_2$ are learning factors. Usually C1=C2=2.

For each particle

Initialize particle

END

DO

For each particle

Calculate fitness value

If the fitness value is better than the fitness

value (p^i_k) in history

set current value as new p^i_k

End

Choose the particle with the best fitness value of all

the particle as the p^g_k

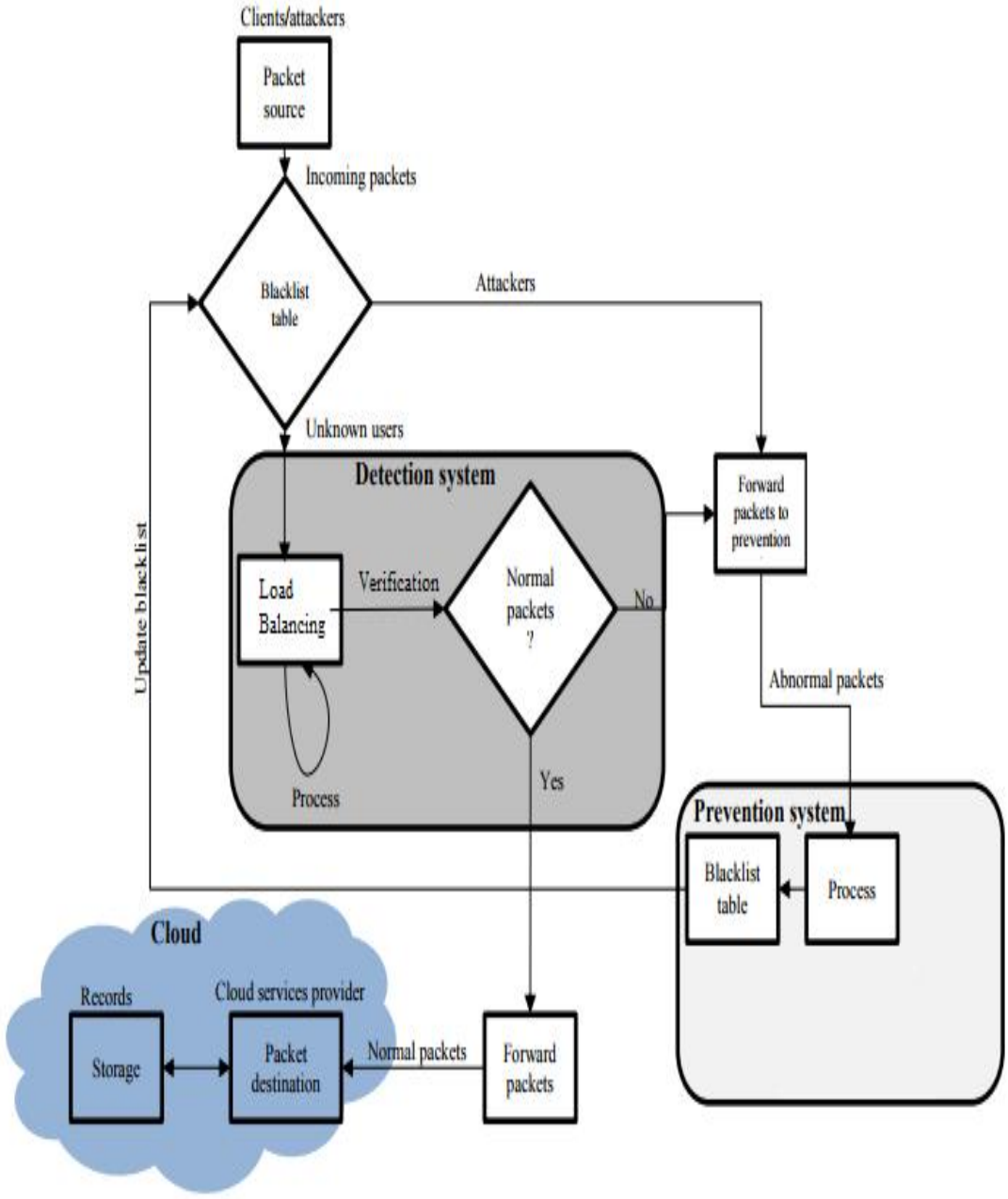
For each particle

Calculate particle velocity according equation (a)

Update particle position according equation (b)

End

V. FIGURE



VI. CONCLUSION

The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self organizing nature. The results demonstrate that the presence of a DDOS increase the packet loss in the network considerably. The proposed mechanism protects the network trough a

self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certificate by their neighbours. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. We believe that this is an acceptable performance, given that attack prevent has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

VII. ACKNOWLEDGEMENTS

We acknowledge DST - File No.368. DST – FIST (SR/FIST/College - 235/2014 dated 21–11–2014) for financial support and DBT-STAR College-Scheme ref.no: **BT/HRD/11/09/2018** for providing infrastructure support.

VIII. REFERENCES

[1] Braga. R, Mota. E, and Passito. A, ”Light DDoS flooding attack detection using NOX/Open Flow,” in Local Computer Networks (LCN), 2010 IEEE 35th conference on, 2010, pp.408-415.

[2] Lee. K, Kim. J, Kwon. K. H, Han. Y, and Kim. S, “DDoS attack detection method using cluster analysis,” Expert Systems with Applications, vol 34, pp. 1659-1665, 2008.

[3] Lu. K, Wu. D, Fan J, Todorovic. S, and Nucci, “Robust and edicient detection of DDoS attacks for large-scale internet,” Computer Networks, vol. 51, pp. 5036-5056, 2007.

[4] Girma. A, Abayomi. K, and Garuba. M, “The Design Data Flow Architecture, ND Methodologies for a Newly Researched Comprehensive Hybrid Model for the Detection of DDoS Attacks on Cloud Computing Environment,” in Information Technology : New Generations, ed .: Springer, 2016, pp. 377 – 387.

[5] Wang. B, Zheng. Y, Lou. W, and Hou. Y. T, “DDoS attack protection in the era of cloud computing and software-defined networking,” Compute Networks, vol. 81, pp. 308-319,2015.

[6] Chonka. A, Xiang. Y, Zhou. W, and Bomti. A, “Cloud security defence to protect cloud computing against HHTP-DoS and XML-DoS attacks,” Journal of Network and Computer Applications, vol. 34,pp.1097-1107,2011.

[7] Dou. W, Chen. Q, and Chen. J, “A confidence-based filtering method for DDoS attack defense in cloud environment,” Future Generation Computer Systems, vol. 29,pp.1838-1850,2013.

[8] Keromytis. A. D, Misra. V, and Rubenstein. D, “SOS: An architecture for mitigating DDoS attacks,” IEEE Journal on selected areas in communications, vol.22,pp.176-188,2004.

[9] Mirkovic. J and Reiher. P, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Computer Communication Review, vol.34,pp. 39-53, 2004.

[10] Somani. G, Gaur. M. S, Sanghi. D, and Conti. M, "DDoS attacks in Cloud Computing: Collateral Damage to Non-targets," Computer Networks, 2016.

[11] Yan. Q, Yu. F. R, Gong. Q, and Li. J, "software-denied networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Survey & Tutorials, vol.18, pp. 602-622, 2016.

[12] Ayres. P. E, Sun. H, Chao. H. J and Lau. W. C, "ALPi: A DDoS defense system for high- speed networks," IEEE Journal on Selected Areas in Communications, vol. 24, pp. 1864-1876, 2006.

[13] Khanna. S, Venkatesh. S. S, Fatemieh. O, Khan. F, and Gunter. C. A, "Adaptive selective verification: An efficient adaptive countermeasure to thwart dos attacks," IEEE/ACM Transactions On Networking, vol. 20, pp. 715-728, 2012.

[14] Salah. K, Elbadawi. K, and Boutaba. R, "Performance modeling and analysis of network firewalls," IEEE Transactions on network and service management, vol. 9, pp. 12-21, 2012.

[15] Moradi. M, and Zulkernine. M, "A neural network based system for intrusion detection and classification of attacks," in proceedings of the 2004 IEEE international conference on advantages on intelligent systems-theory and applications, 2004.

[16] Madyastha. R. K and Aazhang. B, "An algorithm for training multilayer perceptron for data classification and function interpolation," IEEE Transactions on Circuits and Systems l: Functional Theory and Applications, vol 41, pp.866-875,1994.

[17] Lippmann. R, "An introduction to computing with neural nets," IEEE Assp magazine, vol. 4-22,1987.