ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

An Efficient DDOS TCP Flood Attack Detection and Prevention System in a Cloud Environment

Mr. S. Sambasivam, MCA, MPhil., Associate Professor/MCA,
Mr. P. Nandhagopal, Final MCA,
Department of MCA, Nandha Engineering College, Erode 52.
Email ID: sammy2173@gmail.com, pgopal211293@gmail.com

***Abstract*- Distributed Denial of Service (DDOS) attacks in cloud computing environments are growing due to the essential characteristics of cloud computing. software-based traffic analysis, centralized control, global view of the network, dynamic updating of forwarding rules, make it easier to detect and react to DDOS attacks. Distributed denial-of-service (DDOS) attacks remain a major security problem, the mitigation of which is very hard especially when it comes to highly distributed bonnet-based attacks. The early discovery of these attacks, although challenging, is necessary to protect end-users as well as the expensive network infrastructure resources. In this thesis, we address the problem of DDOS attacks and present the theoretical foundation, architecture, and algorithms of Fiercely. The core of Fiercely is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of Fiercely using extensive simulations and a real dataset is presented, showing Fiercely effectiveness and low overhead, as well as its support for incremental deployment in real networks. Load balancing is one of the main challenges, important technique, critical issue and play an important role which is required to distribute workload or task equally across the nodes or servers. and also this thesis address and provides a detailed summary of the load balancing optimization techniques of evolutionary and swarm based algorithms.**

Key Words: classification, DDOS attack, cloud computing, LS-SVM.

I. INTRODUCTION

Cloud computing develops rapidly in both academia and industry due to its essential characteristics, including on demand self-service, broadband network access, resource pooling, rapid elasticity, and measured service. Cloud computing would not be possible without the underneath support of networking. Recently, software defined networking (SDN) has attracted great interests as a new paradigm

in networking. In SDN, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications. Integration of these two promising technologies, cloud computing and SDN, can greatly improve cloud manageability, scalability, controllability and dynamism. The forwarding call is determined strictly supported the situation of every node and it will be done even once there area unit irregular radio ranges and localization errors. Recently, the analysis focus of geographic routing is centering on WSNs with duty-cycles, since duty cycled WSNs have a natural advantage of saving energy by dynamically swing nodes to sleep and waking them according to some sleep programming algorithms.

However, nearly of these works overlook one necessary fact that sensors will really be mobile to realize higher energy efficiency, data rate, etc., and alter plenty of latest application scenarios. As an example, as a result of sensors will move, they'll transmit their knowledge from totally different locations and avoid the matter that sensors close to the entryway or sink continually exhaust their energy first; so, energy usage will be a lot of economical. Also, mobile sensors like mobile phones or cars can become the interface between the knowledge center and the mobile customers; so, period of time data (e.g., traffic information) transmitted from the knowledge center to those mobile objects will be provided to close customers. Moreover, the majority current works regarding geographic routing in duty-cycled WSNs attempt to amendment the geographic forwarding mechanism to traumatize the dynamic topology caused by some nodes being cycled off or aiming to sleep mode. For instance, it's recommended in to attend for the looks of the expected forwarding successor initial and choose a backup node if the primary mechanism fails. In the detector field is sliced into some k-coverage fields, then some always-on cluster heads area unit chosen to gather the info from their close sensors and at last transmit all knowledge to the sink. excluding the connected-k neighborhood (CKN) sleep programming rule proposed in [22] and therefore the geographic routing familiarized sleep scheduling (GSS) rule given in [23], few analysis works have tackled the node accessibility uncertainty issue in duty-cycled WSNs from the read of sleep programming.

II. RELATED WORK

The main purpose of the research is to detect the misbehaving nodes in a network and also separate true node, false node to prevent defense against DDOS attack. Reject that attacker node from network. Distributed denial of service (DDOS) attacks is the second most prevalent cybercrime attacks after information theft. DDOS TCP flood attacks can exhaust the cloud's resources, consume most of its bandwidth, and damage an entire cloud project within a short period of time. The timely detection and prevention of such attacks in cloud projects are therefore vital, especially for health clouds. In this paper, we present a new classifier system for detecting and preventing DDOS TCP flood attacks (CS_ DDOS) in public clouds. The proposed CS_ DDOS system offers a solution to securing stored records by classifying the incoming packets and making a decision based on the classification results. During the detection phase, the CS_DDOS identifies and determines whether a packet is normal or originates from an attacker. During the prevention phase, packets which are classified as malicious will be denied access to the cloud service and the source IP will be blacklisted. The performance of the CS_ DDOS system is compared using the different classifiers of the least squares support vector machine (LS-SVM), naïve Byes, K-nearest, and multilayer perception. The results show that CS_ DDOS yields the best performance when the LS-SVM classifier is adopted. It can detect DDOS TCP flood attacks with about 97% accuracy and with a Kappa coefficient of 0.89 when under attack from a single source, and 94% accuracy with a Kappa coefficient of 0.9 when under attack from multiple attackers. Finally, the results are discussed in terms of accuracy and time complexity, and validated using a K-fold cross-validation model.

III. 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 increases 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 attackers is not implemented.

.

Disadvantages

- If the attacker identifies the port, he 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 requests by the attacker, which leads to decrease in bandwidth, and low latency time.

IV. PROPOSED SYSTEM:

In the proposed thesis collect network traffic packets and flow information in real-time and Pre-process network traffic with and then predict DDOS.

- Firebox which it has "Invite the Attacks" with confidentially.
- Use of Firefox provides effective solution to increase the security and reliability of the network.
- The process of forwarding requests to the Balancer detects traffic as an attack on the server; it is then directed to an alternative server – a type of Firebox.
- Conventional detection and forensics methodology can then be used to gather information on the intruder who will be unaware that they are not using "real" server.

Advantages

- More reliable communication between server and clients
- Active communications remains unaffected even in the presence of DDOS attacks.
- Difficult to intrude into communications

- Less probability of hacking
- Effective and efficient response processing for incoming requests.
- Proposed concept includes Load balancing.

IV. METHODOLOGIES

A.APPLICATION SERVER

This model acts as an application server module, which initially, is started up on different access points. Then the 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 on all the available access points on which the server is started up.

B.NETWORK USER

This model represents the normal network clients, where the user can test the latency of the application server by ping 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 client system. The client can connect to the application server via any available access points, and can make request to the server and can receive response for the requested service.

C. ATTACKER

This model acts as a network attacker or intruder, who *try* 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 attack and sin 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 our proposed framework for detecting rogue access points by using Firebox .The core of Foreclose 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 points. 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.VM LOAD BALANCING

The Load balancing algorithm is divided into three parts. The first phase is the initialization phase. In the first phase, The expected response time of each VM is to be find. In second Phase find the efficient VM, in Last Phase return the ID of efficient VM.

1. Efficient algorithms find expected response time of each Virtual machine.

2. When a request to allocate a new VM from the Data Center Controller arrives, Algorithms find the most efficient VM (efficient VM having least loaded, minimum expected response time) for allocation.

3. Efficient algorithms return the id of the efficient VM to the Datacenter Controller.

4. Datacenter Controller notifies the new allocation

5. Propose algorithm updates the allocation table increasing the allocations count for That VM.

6. When the VM finishes processing the request, and the Data Center Controller receives the Response. Data center controller notifies the efficient algorithm for the VM de-allocation.

V. RESULT ANALYSIS

We consider the network size is 800 × 600 m2. the amount of deployed sensing element nodes ranges from a hundred to one thousand (each time magnified by 100) and also the worth of k in CKN is changed from one to ten (each time magnified by 1). The default transmission radius of every node is sixty m, and also the most transmission radius of every node is one hundred twenty m. there's one constant source node deployed at location (50, 50) and that we take into account 2 mobility cases: 1) the sink remains at location (750, 550) and every one normal sensing element nodes haphazardly move a random range between 100 to a hundred0 times; 2) all traditional sensing element nodes area unit static and the sink moves a random range between ten and a hundred times in 100 totally different network topologies. The quality model in each cases is that the random waypoint model illustrated. In addition, the initial energy of every traditional node is a hundred. The energy consumption of a sensing element by sending, receiving one computer memory unit and sending electronic equipment area unit zero.0144 MJ, 0.00576 , and 0.0288 NJ/m2, severally [23], [41]. Every packet is 12 bytes long, and every node transmits one thousand packets for every time epoch that is one min.

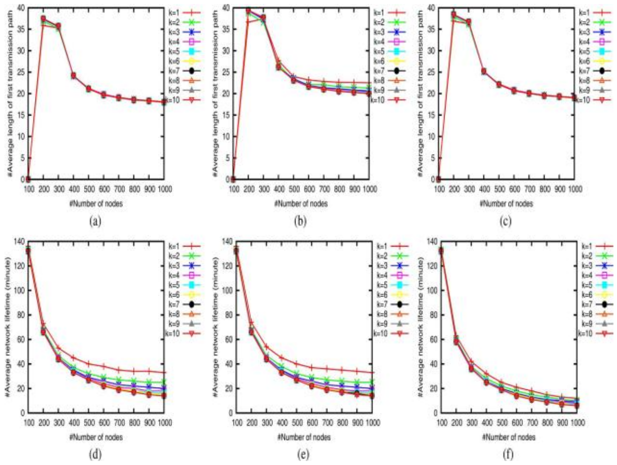

Fig 5.1 Result Analysis

GCKNA Versus CKN Versus GSS—Static Sink With Mobile Sensor Nodes: Fig. 5.1(a)–(c) describe the common length of all transmission methods explored by TPGF in GCKNA and CKN as well as GSS-based WSNs with mobile detector nodes. From these 3 figures, we are able to clearly see that the common lengths of all transmission methods explored by TPGF in GCKNA-based WSNs with mobile detector nodes square measure largely a lot of shorter than that in CKN and GSS-based WSNs with mobile detector nodes. It is as a result of additional nodes nearer to the sink square measure unbroken awake in GCKNA-based WSNs than that in CKN and GSS-based WSNs. Moreover, there's not an excessive amount of distinction relating to the average network time period in GCKNA-based WSNs with mobile detector nodes and therefore the average network time period in CKN based WSNs with mobile detector nodes, that square measure shown in Fig. 5(d) and (e), severally. additionally, each the common network lifetimes in GCKNA and CKN-based WSNs with mobile detector nodes square measure greatly more than that in GSS-based WSNs given in Fig. 5(f). 4) GCKNA Versus CKN Versus GSS—Mobile Sink With Static detector Nodes: presents the common lengths of all transmission methods explored by TPGF in GCKNA and CKN similarly as GSS-based WSNs with a mobile sink. From these 3 figures, we are able to conjointly clearly see that the common length of all transmission methods explored by TPGF in GCKNA based WSNs with a mobile sink is nearly invariably a lot of shorter than that in CKN and GSS-based WSNs with a mobile sink. That conjointly results from the additional awake nearer nodes to sink in GCKNA-based WSNs than that in CKN and GSS-based WSNs. Apart from that, it's arduous to tell apart the common network lifetime in GCKNA-based WSNs with a mobile sink from that in CKN-based WSNs with a mobile sink, that square measure shown in and therefore the average network time period in GSS based WSNs with a mobile sink given in sort of lower than that in GCKNA and CKN-based WSNs.

VI. CONCLUSION AND FUTURE WORK

In this research described The use of cloud computing in many sectors is becoming widespread, as this helps to improve the system in many respects. However, this cloud project is vulnerable to certain types of attacks, such as DDOS TCP flood attacks. Therefore, we propose a new approach called CS_ DDOS for the detection and prevention of DDOS TCP flood attacks. The system is based on classification to ensure the security and availability of stored data, especially important for health records for emergency cases. In this approach, the incoming packets are classified to determine the behavior of the source within a time frame, in order to discover whether the sources are associated with a genuine client or an attacker. The results show that using LS-SVM the CS_DDOS system can identify he attacks accurately.

REFERENCES

[1] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. Modicum*, 2000, pp. 243–254.

[2] B. Leong, B. Lisbon, and R. Morris, "Geographic routing without planarization," in *Proc. NSDI*, 2006, pp. 339–352.

[3] Y.-J. Kim, R. Goninan, B. Karp, and S. Shankar, "Lazy cross-link removal for geographic routing," in *Proc. Senses*, 2006, pp. 112–124.

[4] L. Zhang and Y. Zhang, "Energy-efficient cross-layer protocol of channel aware geographic-informed forwarding in wireless sensor networks," *IEEE Trans. Vet. Technol.*, vol. 58, no. 6, pp. 3041–3052, Jul. 2009.

[5] Z. Jiang, J. Maw. Lou, and Jaw, "An information model for geographic greedy forwarding in

wireless ad-hoc sensor networks," in *Proc. IEEE INFOCOM*, 2008, pp. 825–833.

[6] H. Zhang and H. Shan, "Energy-efficient beaconless geographic routing in wireless sensor networks," *IEEE Trans. Parallel Diatribe. Syst.*, vol. 21, no. 6, pp. 881–896, Jun. 2010.

[7] C.-F. Shin and M. Liu, "Network coverage using low duty-cycled sensors: Random & coordinated sleep algorithms," in *Proc. IPSN*, 2004, pp. 433–442.

[8] Q. Cao, T. Abdel hazer, T. He, and J. Stank, "Towards optimal sleep scheduling in sensor networks for rare-event detection," in *Proc. IPSN*, 2005, pp. 20–27.

[9] H. Le, J. V. Eck, and M. Takizawa, "An efficient hybrid medium access control technique for digital ecosystems," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 1070–1076, Mar. 2013.

[10] P. Cheng, F. Zhang, J. Chen, Y. Sun, and X. Sheen, "A distributed TDMA scheduling algorithm for target tracking in ultrasonic sensor networks," *IEEE Trans. Ind. Electron.*, vol. 60, no. 9, pp. 3836–3845, Sep. 2013.

[11] K. Morioka, J.-H. Lee, and H. Hashimoto, "Human-following mobile robot in a distributed intelligent sensor network," *IEEE Trans. Ind. Electron.*, vol. 51, no. 1, pp. 229–237, Feb. 2004.