ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

DETECTING AND PREVENTING DDOS IN CLOUD USING AVERAGE DISTANCE ESTIMATION TECHNIQUE

Sujith Kumar Mahakud[1] , J.Jackulin Reeja[2]
Department-MCA, Faculty Of Computing, Sathyabama University, Chennai-600119, Tamil nadu, India.
Email: sujith.kumar1993@gmail.com, reejajackulin@gmail.com

Received on 10-02-2016 *Accepted on 15-03-2016*

Abstract

The DDoS (Distributed Denial-of-Service) or DoS (Denial-of-Service) in area of software defined networking is always attempting to make an attack for making system unavailable for intended users. The protection is mostly needed in the network for better use and safety from the attacker and intrusive behavior by outside network. Where, the devices on open flow network could also be in the target for attacks so a mechanism for preventing this issues are required to solve the problems for communicating with clouds. The cloud system is more innovative and leading platform for computing. Basically, some questions are arising over the security policy that it could be able to prevent the notorious attacks of DDoS in the environment of cloud. There are several researchers have done well job for solving the initial issues and the competition is still on the full phase amid of the attackers and defenders. The cloud system usually possesses the thoughtful activity and not having complete control against the attacker's activity. This paper is proposing a enhanced technology for solving the existing issues over the cloud environment to control the complete resource capability and for preventing the attacker and malicious activities. The proposed technique is employing the dynamic resource allocation strategy for DDoS attack counter over every individual cloud customers. The proposed idle resources are sufficient for making a cloud clone to prevent the intrusion for filtering the packet attacks and providing a surety for the service quality of malicious users. A mathematical module is being implemented for the required approximation on the basis of queueing theory. Through experiments over dataset of real-world and careful analysis of system has been concluded for defeating the DDoS attacks over cloud environment.

Keywords:

DDoS, MMSE, Average Distance Estimation, Firewall.

1. Introduction

The cloud system is now turning into a better platform and an important computing platform. The certain problem and issues are always being raised on the security of cloud services such as DoS and DDoS attack. The attack is collapsing the completet system and making a disturbance for every activity. DDoS (Distributed Denial-of- Services) is affecting the complete cloud system environment. The previous technique or system is facing a serious issue over the security of network [1]. There are so many tools and technique is being derived for identification of Distributed Denial-of-Services (DDoS) and for reducing the damage. But still all the techniques are not capable to achieve the target [6]. This proposed technique is approaching the protection mechanism for solving the issues in the cloud. The DDoS based distance metrics is using a general and effective technique for identifying the lood effect and network blocking by malicious activity. The infrastructure of cloud is also providing the huge hope of resources and making an easily accessible platform for handling the service demand increments [2]. However, it might be possible to shut down the cloud system by any attacks of DDoS. So, the platform of P2P in the client server does not possess the adequate resources for saving the system from DDoS attacks. The customers of individual cloud service couldn't stay away by getting an attack from DDoS behavior. The attacks are having a big disadvantage as significant dangers in the environment of non-cloud computing like online games, independent websites for news and E-commerce websites [3]. The attacks of DDoS are could be accomplished by the botnets assistance. The newly investigated report had rectified the reality that the hackers could easily handle the any computer system at any time [4]. However, there are more numbers of anti-viruses and anti-malware has been launched for compelling the several issues but it couldn't provide a better security always. The proposed technique is providing a better solution over the security of system and cloud server. The firewall enhancement is better move to protect the system and cloud. The destructive damages could be less and prevent the malicious activity from accessing the system [5]. The proposed technique average distance based on the technique of DDoS detection is calculating the distance and measurement of the malicious activity on the system and mapping the address to prevent form accessing the system [7]. Average distance estimation based DDoS detection is using the Minimum Mean Square Error method for approving the more accuracy over the safety and prevention of attackers.

2. Related Work: The Author of [11] has proposed several of application for identifying the attacks in their researches. Till the year of 2013, two attacks have been involved within the 300Gbps of traffic attacks. The author has proposed an

analysis for the amplification attacks, which provide a broad proposal selection for preventing and detecting the amplification attacks and for tracing the attackers [9].

The spoof IP system has proposed and plays a crucial role for making an attack in every type of attacks. A survey of the state of art is defining a spoof is being proposed. The nature of the work is introducing source IP address and attacks amplification for spoof access. The authors of [12] have proposed a biomimicry system to prevent the spoof access by introducing defense system over cloud system. The system has been propelling the power of such invention such as cat's eyes and Velcro tape. Same time the scientist has developed biologically inspired methods such as: sensor networks, neural networks and genetic algorithm and etc [8]. at a first look, there is no direct inspiration over the defensive and offensive technique has been seen in the internet sources that pattern is being presented in the nature and reveals the closer inspection amid of the two eorlds of internet.

The DDoS and Botnets attacks, the Intrusion Prevention/Detection System (IPS/IDSs) and all others strategy has been employ very nearly [13]. The authors of [14] have introduced a resource monitor by implementation on the infrastructure of computing which is having more partition or resources pool. This partition and pool is overbearing the request of the web sites traffic, application and processes separately from the requests of less-resource-demanding. The authors of [15] have introduced the HADEC, which is based on the HADOOP platform for identifying the live DDoS detection platform, which is more capable to analyze the DDoS attacks on time. The HADEC is capturing the current flow of the network process, traffic and information relevant to the HDFS and MapReduce storage by using the DDoS detection algorithm. The solution of HADEC is having a memory, scalability, process complexity and memory shortage problems.

3. Proposed work

3.1 Overview

The proposed concept is introducing Average Distance Estimation Based DDoS detection technique. This technique is being used for identification of mean valu distance for the next periodic time within exponential smoothing estimation technique.

The separation of traffic is being used based on the distance-based metrics for DDoS technique of detection which uses the Minimum Mean Square Error (MMSE) for estimating the rates of traffic within several distance. The real value of the legal scope is detecting the anomaly situation.

The proposed technique is looking for the resource management and intrusion detection, which proposes the description of four models by using algorithmic technique in cloud network.

3.2 Overall Architecture

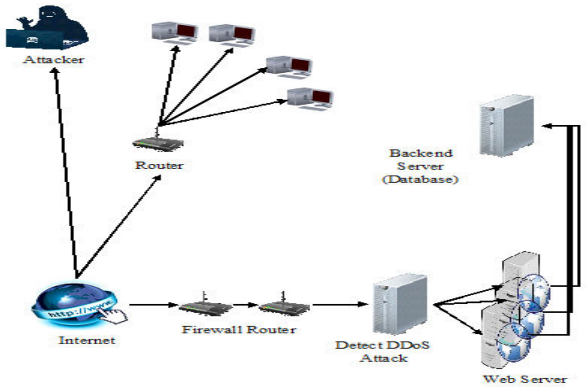

Figure 1: Overall Architecture.

3.3 Proposed Work Methodology

3.3.1 Cloud Application Development

The application of cloud is residing on the server for making a communication within the services and web to the users. The creation of web services is important operation for making a communication within the cloud application.

3.3.2 Web Proxy Implementation

The implementation of the web proxy is playing a middleware in the browser and cloud server. The proxy is residing the cloud server by monitoring the response and request over the server.

a) Proxy Design

The monitoring request is being done by the proxy services by the client application. The proxy services are detecting the same name of the system, URL and IP address by which it invoked the users.

b) Proxy Web Services Implementation

The communication by using proxy within several methods of web services is monitoring the web requests. The sub module of the proxy is responsible for making a web service proxy.

3.4 Firewalls

The Firewall is very popular in every network or a computer that is defending the unwanted traffic of network or machine while accessing or transmitting the useful outbound or inbound traffic. This subsection is discussing the analog of the firewall features:

a) Capable to prevent the threats from outside world and

b) Capable to filter out unwanted entities.

The biological terms like plants and animals are just like a computers and proposing the defensive capacity against of the unwanted activities.

3.5 DDoS Mitigation Algorithm

A DDoS attack is for identifying the real IPS and when the clone of the IPS is proposing an image of the real IP, it's calculating the system average time within the current status.

If *Ta(t,m) > Tn*, the clone is making an IPS system for filtering of task.

Then it's finding the *Ta(t,m) < Ta(t,m-1)*, the time is reducing the one IPS that is releasing the pool resources for available cloud.

3.6 DDoS Attack Prevention

The proposed DDoS detection method Average Distance Estimation is providing the exact estimation of DDoS attack by calculating mean value of distance within exponential technique of smoothing. Distance-based separation of traffic is utilizing the MMSE (Minimum Mean Square Error) for predicting the traffic estimation for several distances.

The calculation of distance value is completely on the basis TTL field within directly IP header during every transmission; every intermediate router is deducing the TTL value form one IP packet. The initial value could be determined by the initializing the smallest value. The smoothing value for estimating the prediction is being defined with distance value d_{t+1} and time t+1

$$d_{t+1} = d_t + w * (M_t - d_t)$$

The d_t is representing the distance value within time t-1, M_t is presenting the distance value at time t. The determination of the value of current distance is normal or abnormal; the value of MAD could be useful for utilizing.

$$MAD = \frac{1}{n} * \sum_{i=1}^{n} |e_t|$$

The *n* is presenting the past error number and e_t is making a prediction error at time t.

The exponential smoothing technique could be able to calculate the MAD within the approximation of below defined equation:

$$MAD_{t+1} = r * |e_t| + (1 - r) * MAD_t$$

Where, the MAD_t is presenting the time value at t and r is smoothing gain.

4. Result and Discussion

4.1 Experimental Setup

The proposed concept and technique has been implemented based on the following system configuration.

Table-1: System Requirements.

S.NO	Requirements
1.	Operating System: windows XP or 7
2.	RAM: 2 GB or above
3.	Hard Disk Drive: 500 GB
4.	Processor: i3 and above
5.	JAVA 1.7
6.	Processor: Intel Pentium 2.90 GHz
7.	CPU: G2020

4.2 Attack Categories.

Table-2: Attack Categories.

S. NO	Attacker category	Attack Types
1.	R2L	15
2.	DOS	10
3.	Probing	6
4.	U2R	7

The attack categories and its types are described below:

- **R2L:** imap, named, ftp-write, guess password, spy, send mail, snmp guess, snmp get attack, worm, xsnoop, xlock, warezmaster, warezclient, phf, multi-hop.
- **DOS:** land, back, apacha2, pod, tear drop, process table, udpstorm, smurf, netpune, mailbomb.
- **Probing:** saint, satan, namp, lpsweep, portsweep, msscan,
- **U2R:** ps, perl, xtreme, rootkit, sqlattack, buffer over flow, load module, httprunnel.

4.3 Comparison Table.

Table-3: Attack result between proposed and existing.

Time in Sec	Existing System Attack Detection	Proposed System Attack Detection
1	**0.94**	**0.936**
2	**1**	**0.98**
3	**1.2**	**0.995**
4	**1.5**	**1.1**
5	**2.1**	**1.8**

The above mentioned table 3 is presenting a comparison amid of the existing and proposed technique.

4.4 Attack Identification.

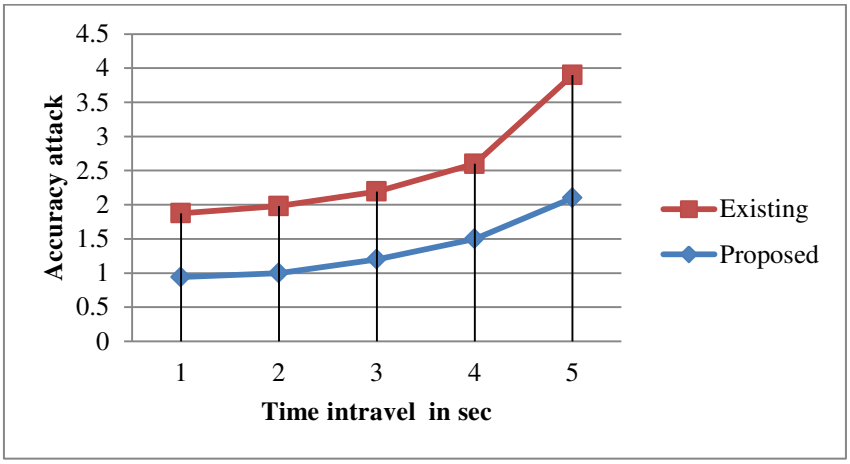

Figure-2: Attack Identification

The above mentioned figure 2 is presenting the attack identification accuracy and the proposed technique is producing better output in compare to existing technique.

4.5 Distance Based Comparison.

Table-4: Proposed technique result compared to existing based on distance.

Distance (km)	Proposed technique	Existing technique
2	191.25	56.02
4	205.23	126.09
2.5	191.25	56.02
4.5	205.23	126.09

The above mentioned table 4 is presenting the distance based comparison table for identifying the attack. The proposed technique is better than existing technique.

4.6 Attack Identification Accuracy

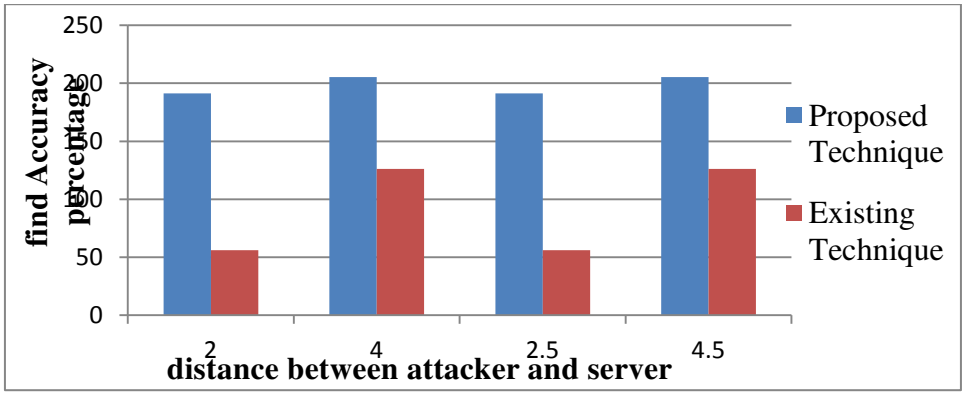

Figure-3: Proposed technique results compared to existing based on distance

Above mentioned figure 3 shows proposed technique result compared to existing based on distance. Both calculated distance are in km. given result is efficiency by proposed.

5. Conclusion and Future Enhancement

This project is presenting an enhanced and efficient technique Average Distance Estimation Based DDoS detection technique. This proposed technique is estimating the mean distance value within the next period by using exponential smoothing estimation technique. This proposed methodology is proposing a problem for attack detection and avoiding the accessing of existing issues. The quality calculation is finding the attacker details within the speed of time for identifying the secure system network. The proposed methodology is proposing the firewall techniques for avoiding the attacks over the database system. The identification and verification of the system accessing is producing the entire security over the network to prevent the malicious activity and attacks. The future enhancement of this concept is to hide the system and encryption of the sensitive data in the storage server for making a better security of the accessible data.

6. Reference

1. Armbrust. M, Fox. A, Griffith. R, Joseph. A.D, Katz. R.H, Konwinski. A, Lee. G, Patterson. D.A, Rabkin. A, Stoica. I, and Zaharia. M, “Above the clouds: A Berkeley view of cloud computing”, EECS Deptartment,University.California, Feb. 2009.
2. Peng. T, Leckie. C, and Ramamohanarao. K, “Survey of network-based defense mechanisms countering the dos and DDoS problems”, ACM Comp. Sur., volume 39, number. 1, pp. 1-3, 2007.
3. Rajab. M.A, Zarfoss. J, Monrose. F, and Terzis. A, “My Botnetis bigger than yours (maybe, better than yours): Why size estimates remain challenging”, in proceed. 1st conf. HotBots, 2007, p. 5.

4. JelenaMirkovic, Peter Reiher and Janice Martin, "A Taxonomy of DDoS attacks and DDoS defense mechanisms", Comp. Sci. Dept., Uni. of California, Los Angeles.
5. The swiss education and research network, (2002) "Default TTL values in TCP/IP,"Available at http://secfr.nerim.net/docs/fingerprint/en/ttldefault.html.
6. Zhou, R. and Hwang. K, "Trust-Preserving overlay networks for global reputation aggregation in scalable P2P systems", IEEE transaction on Parallel and Distributed Systems, March 2006.
7. Houle. K, Weaver. G, Long. N, and Thomas. R, "Trends in denial of service attack technology", CERT Coordination center document, 2001.
8. Dittrich. D, "The 'stacheldraft' distributed denial of service attack tool," http://staff.washington.edu/dittrich/, 2000.
9. Sandeep Singh, (2015) "Prevention mechanism for infrastructure based denial-of-dervice attack over software defined network" International Conference on Computing, Communication and Automation" IEEE 348 Dept. of I.T. B.B.A. Uni. Lucknow, India.
10. Yba. J, Matthias Wahlisch, Matthew Orlinski, Thomas. C, Christian Rossowy, "Amplification and DRDoS attack defense – A Survey and new perspectives", Saarland Univ, Saarbruecken, Germany, HAW Hamburg, Germany.
11. Elbieta Rzeszutko and Wojciech Mazurczyk, "Security - A Perpetual War: Lessons from nature", warsaw Uni. of Tech., Institute of Telecomm. warsaw, poland, 00-665.
12. Janaki Raman and Aaqib Iqbal Wanil, "Identification and avoidance of DDoS attack for secured data communicationin cloud" Inter. Jour. of Science & Research (2013): 6Volume (Issue) 4 (4), April 2015.
13. Alao O. D, Ogu E. C, Izang A. A, Omotunde A. A, & Ogbonna A. C "Partitioning of resource provisions for cloud computing infrastructure against DoS and DDoS attacks" Int. Jour. of Adv. Research in Comp. Science, 5(7), 2014, October.
14. Usman Ali and Sufian Hameed, "On the efficacy of live DDoS detection with hadoop", IT Security Labs, National Univ. of Comp. & Emerging. Sci.

Corresponding Author:
Sujith Kumar Mahakud[*],
Email: *sujith.kumar1993@gmail.com*