Fast Entropy based Detection of DDoS in Cloud

Dr. Mansi Gyanchandani[1], Siteash Mishra[2], Dr Rajesh Wadhvani[3], Dr. Sanyam Shukla[4]

Assistant Professor[1, 3, 4], M.Tech Scholar[2]
Maulana Azad National Institute of Technology Bhopal, 462003

Abstract
Distributed Denial of Service(DDoS) attacks are not a new threat,but remain a major security challenge and topic of ongoing research interest.Mitigating DDoS attack in cloud presents a new dimension to solutions proffered in traditional registering due to its architecture and features. Impacts of Distributed Denial of Service (DDoS) attacks in distributed computing are not fundamentally the same as what they were in the conventional "fixed" on-premise base. With regards to DDoS attacks in the multi-inhabitant mists,it is found that not only the casualty server, various different partners are included. Some of these vital partners are co-facilitated virtual servers, physical server(s), system assets and, cloud administration suppliers. This paper mainly focuses on framework investigation, tests and simulations.// Harms/Effects to these partners incorporate execution impedance, web administration execution, re-source race, administration downtime and, business misfortunes. Cloud scale tests have uncovered that general vitality utilization and number of VM movements are unfavorably influenced because of DDoS attacks. To the best of our insight, this work is the main novel commitment toward impact portrayal on non-focuses in distributed computing space. This paper attempts to distinguish the spots of these impacts and their birthplaces like auto-scaling, multi-occupancy and bookkeeping in cloud.There is a colossal need to re-take a glance at DDoS arrangements in the cloud space in which quality efforts are expected to minimize these impacts

Keywords:
Cloud,DDoS,Network level Threats,Service level Threats,Entropy based detection

1. Introduction

Cloud computing is a much awaited dream of computing as a service.In this era of boom in internet users, industries are in search of novel and commercial ways to curb down the investments meanwhile expanding up the revenues. Cloud computing has emerged as the eminent technology of all traditional computing archtype by the IT world. In recent past, it has evolved as a major computing platform for sharing resources including infrastructure resources, software resources, application resources and business processes [2].It can be narrated as the supply of on-demand scalable resources as services on pay-as-you-go basis. Users can access these services anytime, anywhere through internet. Besides these benefits, the security concerns have become an profuse challenge for Cloud Service Providers (CSP). Distributed Denial of Service (DDoS) attacks are the most hazardous and the most common of all, in a cloud environment. This kind of attack chokes the CSP in a way that the datacenter resources will get exhausted and CSP is not able serve the service request from legitimate users. The attackers often compromise insecure hosts, called zombies, on the network and install attack tools basically malwares on them. These zombies group to form a botnet and will generate enoromous amount of distributed attack(useless) packets targeting at the victims under the control of the attackers. This attack either hinders or blocks the loss to small and large organizations.. CSPs will suffer from both financial and reputational losses. Thus, it is burning issue now to devise some techniques to eradicate these two kinds of DDoS attacks and make the cloud secure from DDoS. This paper proposes a novel mathematical formulation of detecting and removal of DDoS attack by using Safe Environment for Cloud users (SEC) in cloud environment. SEC authenticates users in both of the above mentioned form of DDoS.

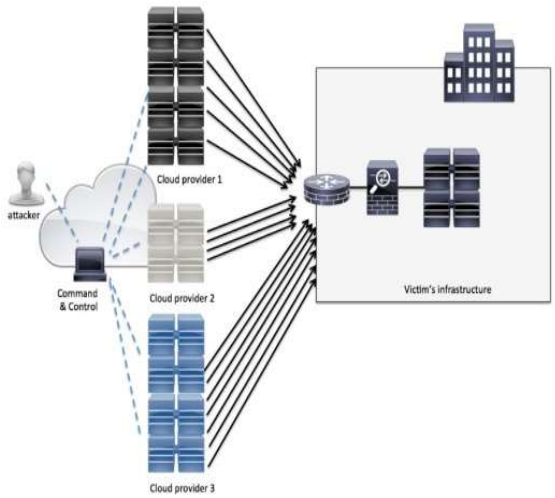

Figure. 1. DDoS attck in cloud

Manuscript received February 5, 2026
Manuscript revised February 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.2.22

2. Related Work

Numerous research works have been going on in various parts of world to rescue the cloud from the DDoS threat. Packet Score[1] generates value distributions of some attributes in the TCP and IP headers, and then uses Bayes Theorem to score packets. Packet Score has a reasonably high filtering accuracy and can be effortlessly deployed . But as its scoring and discarding are more or less related to attack intensity, it is not appropriate for handling huge amounts of attack traffic. Also it is not suitable for real time processing, as it can be slow sometimes. Overcourt[2] ,defends the network from DDoS threat. The users are given credits based on the response they receive from the protected server and are classified as well-behaving and ill-behaving, accordingly. VIP path with full access to protected servers is assigned to well-behaving clients and Non-VIP path with limited access is assigned to ill-behaving clients. The clients whose credits got exhausted meanwhile are blocked. The method has various advantages such as no need of changing the underlying infrastructure, credit decaying mechanism to deal with issue of dynamic IP allocation, etc. But the criterion chosen by the authors to discriminate attack traffic from legitimate will not sound good in all cases.Entropy-based approaches have significant benefits in DDoS detection. When the monitored network runs in normal way, the entropy values are relatively smooth. Otherwise, the entropy value of one or more features would change significantly[3]. The use of entropy can increase the sensitivity of detection to uncover anomalous incidents. Even though using Entropy has several advantages, it still needs an efficient algorithm to reduce computational time and mem- ory usage in a high speed network. In the work of G.No [4] developed fast entropy approach to reduce computation time. Here fast entropy of packet count is calculated. Liu [5], suggested a Trust Guard which gives credits to users who show miscellany in the size of request packets. They assumed that the attackers always send small sized packets which are numerous in number. The method fails if the attacker sends large sized packets or mimics the legitimate packets. Mirkovic[6],used ticket granting mechanism based on credits and penalties acquired by the clients during their past interactions with the protected server. The attacker can turn hostile after attaining the ticket and also the scheme fails if the attacker is a human. The information distance[7], flow correlation coefficient and inter arrival time of packets are various other methods proposed in this regard. Some authors have used the expectedness of packet arrival rates to discriminate between attackers and legitimate users. The users authenticated this way are given services after being listing to them and others are blocked. A major advantage of this method is that the attack traffic and legitimate traffic are distinguished at the entry level themselves using the search engine and edge routers. This will reduce the traffic aggregation near the victim. Communication overhead among the edge routers is also a problem in this approach. This method fails in front of human intelligence. Walfish [8] proposed speak up mechanism which encourages the users to send more and more request using the available resources. It is assumed that attackers will be using all the available resources and legitimate users will have spare resources. So, those who respond to this encouragement are classified as legitimate users and others as attackers. The method is simple to implement and attackers cannot fool the defensive mechanism by any means. The increased cost at server, network as well as end user, uncertainty of extra resource availability and failure in discriminating DDoS from Flash crowd are the limiting factors. Agrawal[9] have proposed a multilevel authentication mechanism by providing different passwords to different levels of users in an organization. This method reduces the probability of breaking the credentials as multiple level passwords are there. Strict authentication and authorization are possible with this method.

As authentication is at different levels, each user does not need to know all passwords. But this kind of authentication would not work when there is no intermediate level between end user and CSP. Schneider [10] proposed HTTP reject to discriminate DDoS from Flash crowd. They have suggested that when flooding is detected, the server should provide each user with a small but informative message about the situation. It is assumed that a legitimate user will not retry again, whereas the attackers do and hence the requests from such users can be dropped.The compromised system can be either human controlled or a robot. This can be judged by inquiring the clients to solve puzzles or simple mathematical equations, which will not entail more processing time. The robots can perform only the tasks assigned to them, i.e., to send request as per the bot masters command, fails to solve the puzzle. The requests coming from these systems can be dropped immediately and their IP address is blacklisted for blocking them in future also. Human controlled systems could solve the puzzle; succeed in this phase. Hence, this phase is able to segregate man and machine but fails to identify the zombies.

3. Proposed Methodology: Secure Environment for Cloud (Sec)

The proposed probabilistic based authentication mechanism (SEC) will be able to distinguish between network as well as service level attack by continuous tracking of the entropy of the cloud system. In Network Level DDoS,the similarity in the packet is considered as the parameter for concluding the DDoS attack.In this particular attack the entropy of the system falls severely as the system is dominated by a single or a group of systems (zombies) only . In case of Service Level DDoS, as all users, whether legitimate or forged,will send request.The traffic analysis of users along with the entropy will be used to detect the Service Level DDoS. Those who manage fixed entropy are further monitored for elimination whereas others are considered as legitimate users. After authenticating the users, they are given individual entropies and this is considered as their initial value and based on these values, the users are given services.

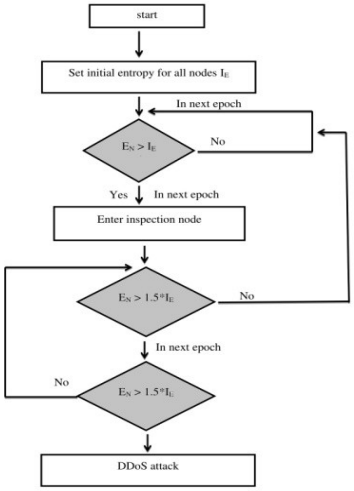

Figure. 2. Attack detection: Network layer

3.1 W o r k i n g Mechanism of SEC

More entropy means more randomness. Its range is between 0 to log(n) where n is the total sample space. The rate of entropy change i:e the the fluctuation in entropy in a given unit of time can provide a mechanism for detecting changes in the randomness and hence DDoS attacks.

1. Network Level attack: If we are considering IPV4, the number of bits in the source or destination field is 32. Hence
, the total sample space or the maximum value of source or destination is 2^{32}. Let us assume there is a set
$s=v_1$, v_2 ,
$v_3..v_n$

with n distinct values which the entropy (H(x)) of a random variable (here the source and destination nodes) can take. Now the probability,
$p\ (n_i) = s_i/s$

where s_i s_i is the total number of occurrences a node picks the value as n_i and s being the total traffic in terms of packets associated with the given node.In case of attack the entropy drops quite rapidly as there is one flow count that is dominating the whole system. In case of non-attack scenario the entropy will be in a constant and limited range.Fig2 picturises the flowchart of the algorithm.

2. Service Level attack: In service level attack , Software as a Service and Infrastructure as a Service are basically targeted. Resources either physical or virtual are more or less same. Here virtual process and virtual resources are our main concern. The major resources are CPU, Memory and Disk. The total resources in a virtual process for a virtual process $V_S = (C_s, M_s, D_s)$
whereC_s , M_s D_s represents the amount of CPU ,Memory,
Disk utilized by the virtual process V_S . Here the assumption
is that the resources are being distributed equally initially as

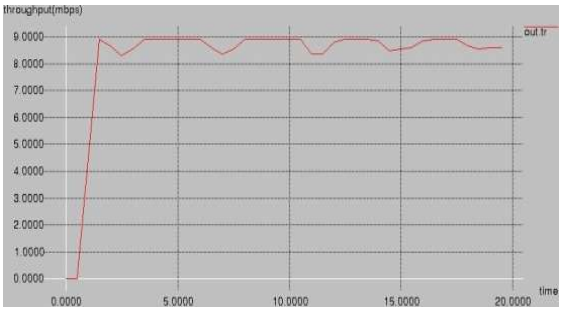

Figure. 4. Throughput vs Time

$C_{js} = C_j /n$ $M_{js} = M_j /n$ $D_{js} = D_j /n$

Where n is the total number of virtual processes and C_{js}, M_{js}, D_{js} Are the total CPU, Memory, Disk resources available for the virtual processes. The equal distribution of resources serve as the initial threshold for monitoring state of these resources. If any resource is being utilized for more than its initial threshold value , it is sent to the monitoring state. In this state if the utilization of that resource grows with factor of 1.5 of the initial value for two epochs ,the DDoS attack is confirmed. The IP responsible for this very situation is blacklisted and the same is notified to the controller.

4. Experimental Setup:

The machine used is Pentium enabled. It is dual core with 1.7 Ghz processor.It is equipped with 2GB RAM and 500GB of hard disk.The algorithm has been simulated on NS2.The simulation environment is being depicted in Fig 6.

5. Result and Discussions

An effective DDoS attack location technique utilizing Fast entropy approach is proposed. The stream tally is Figured for every association at specific time interim. From the percep- tion unmistakably the quick entropy worth is significantly diminished for specific association and specific time interim of which stream number is substantial quality contrasted with rest.

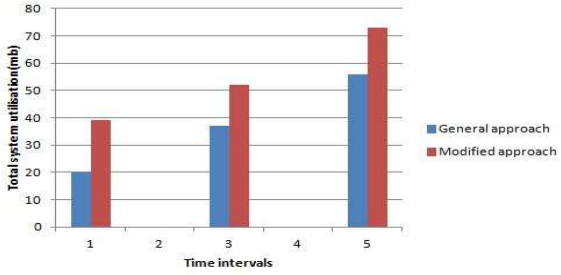

Figure. 6. Experimental Simulation

DDoS attack is identified, when the distinction between entropy of stream tally at every moment and mean estimation of entropy in that time interim is more prominent than the limit esteem. Since the limit worth is redesigned adaptively taking into account activity design condition, the exactness of discovery is made strides. In the wake of distinguishing DDoS attack, as a future work it is conceivable to discover the malicious node and operators of DDoS attack utilizing the en- tropy approach, as the identification framework can performed proficiently in view of stream conglomeration strategy.Fig4 shows the fluctuation in Throughput with respect to time.Fig5 depicts the overall system utilisation in normal approach and modified approach. Normal approaches takes more time in detecting the attack as it measures increment in the utilization gradually.

6. Conclusion

In case of DDoS various methods have been proposed but the identification of root malicious node is a very tedious and time taking process in previous approaches. But the robust strategy of allocation of resources and continuous monitoring of requests can bring the identification time down. The simulation of the proposed methodology shows it's worth as the mean time taken for detecting the malicious nodes is 23% lesser than the previous approach. The proposed approach could be implemented for online monitoring also.But during online monitoring it could take some time to identify the malicious node as we first need to gather data and then the analysis part will come in picture.

References

[1] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "Packetscore: a statistics-based packet filtering scheme against distributed denial-of- service attacks," IEEE transactions on dependable and secure comput- ing, vol. 3, no. 2, p. 141, 2006.

[2] P. Du and A. Nakao, "Overcourt: Ddos mitigation through credit-based traffic segregation and path migration," Computer Communications, vol. 33, no. 18, pp. 2164–2175, 2010.

[3] J. Wang, X. Yang, and K. Long, "A new relative entropy based app-ddos detection method," in Computers and Communications (ISCC), 2010 IEEE Symposium on. IEEE, 2010, pp. 966–968.

[4] G. No and I. Ra, "Adaptive ddos detector design using fast entropy computation method," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on. IEEE, 2011, pp. 86–93.

[5] H. Liu, Y. Sun, V. C. Valgenti, and M. S. Kim, "Trustguard: A flow-level reputation-based ddos defense system," in Consumer Communications and Networking Conference (CCNC), 2011 IEEE. IEEE, 2011, pp. 287–291.

[6] M. Natu and J. Mirkovic, “Fine-grained capabilities for flooding ddos defense using client reputations,” in Proceedings of the 2007 workshop on Large scale attack defense. ACM, 2007, pp. 105–112.
[7] S. Yu, T. Thapngam, J. Liu, S. Wei, and W. Zhou, “Discriminating ddos flows from flash crowds using information distance,” in NSS 2009: Proceedings of the third International Conference on Network and System Security. IEEE, 2009, pp. 351–356.
[8] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, “Ddos defense by offense,” in ACM SIGCOMM Computer Communica- tion Review, vol. 36, no. 4. ACM, 2006, pp. 303–314.
[9] H. Dinesha and V. K. Agrawal, “Multi-level authentication technique for accessing cloud services,” in Computing, Communication and Ap- plications (ICCCA), 2012 International Conference on. IEEE, 2012, pp. 1–4.
[10] J. Schneider and S. Koch, “Httpreject: handling overload situations without losing the contact to the user,” in Computer Network Defense (EC2ND), 2010 European Conference on. IEEE, 2010, pp. 29–34.
[11] Priyank Jain, Manasi Gyanchandani, Nilay Khare, "Big data privacy: a technological perspective and review", Journal of Big Data, vol. 3, pp. , 2016, ISSN 2196-1115.