A Reactive Defense Mechanism based on an Analytical Approach to Mitigate DDoS Attacks and Improve Network Performance

Palvinder Singh Mann
Department of Information Technology
DAV Institute of Engineering & Technology
Jalandhar, Punjab, India 144008

Dinesh Kumar
Department of Information Technology
DAV Institute of Engineering & Technology
Jalandhar, Punjab, India 144008

ABSTRACT
The Distributed denial of service attacks (DDoS) have become more and more frequent and caused some fatal problems in the recent time. Internet users experience denial-of-service (DoS) attacks every day. Our inboxes are swamped with spam containing subject lines that sometimes fool us; our search-engine queries return many irrelevant results; and online auctions are plagued by corrupt database records filled with intentionally misleading keywords and many more .Intense research have been done to detect and defend such attacks, however, many solutions are still in the phase of theoretical studies. Some of them may have certain practical value, but they have to reconstruct the existing network and the routing instruments with great cost.
In this paper we are going to present an Analytical approach which will employ Reactive Defense Mechanism to mitigate the DDoS attack and further improve network performance in terms of less computation time. Further the simulation result proves it to be a better result oriented approach.

Keywords
Distributed denial of service, Denial-of-service.

1. INTRODUCTION
Internet is growing, so as its penetration in day to day applications. This utility of the century is on a soft target of attackers for obvious reasons. One of the potential threat is denial of service attack. Recent studies estimate that farms of compromised hosts, popularly known as "botnets " are as growing as twice to Internet. Moreover, the SYN flood attack, the most popular DDoS attack to date, is giving way to sophisticated application-layer attacks.

These attacks will fall in the category of Flooding Attacks [2], which basically consist of an attacker sending a huge amount of nonsense requests to a certain service, which is providing various services under cloud. As each of these requests has to be processed by the service implementation in order to determine its invalidity, this causes a certain amount of workload per attack request, which in the case of a flood of requests usually would cause a Denial of Service to the server hardware.

1.1 Denial of Service (DoS) Attack
Denial of Service (DoS)[9] attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. When the operating system notices the high workload on the flooded service, it will start to provide more computational power to cope with the additional workload. The attacker can flood a single, system based address in order to perform a full loss of availability on the intended service.

1.2 Distributed Denial of Service (DDoS) Attack
A Distributed Denial of Service (DDoS) [11] attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims". The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack, while making it more difficult to track down the original attacker. A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service attack.

To keep in view the gravity of DDoS attack's we focus our research to provide a mechanism to mitigate these attacks by using an Analytical approach.

2. DDoS MITIGATION MECHANISM-AN ANALYTICAL APPROACH
As in the case of DDoS attacks the attacker sends large volume of malicious packets which later prevent the legitimate user to access the services, therefore our prime concern is to find out the no of packets being malicious in the legitimate requests and then mitigates them by an appropriate mechanism.

In this paper we are presenting a Analytical approach based on mathematical equation which will be used to find out the no of packets being malicious under legitimate data packets and an algorithm which is a refined method of traditional hoop count inspection mechanism to mitigate the malicious packets which are coming along with the legitimate data from the attacker side and can pause a threat to the network performance.

2.1 Proposed Analytical Approach for Malicious packets
Let us suppose

p = probability of a packet being malicious
q or 1-p = probability of a packet being non-malicious or legitimate

Suppose the packets are being arriving at server end with a Poisson's distribution 'λ'.

m = no of malicious packets

l = no of non-malicious or legitimate packets.

M = total no of packets arrived with Poisson's distribution 'λ'.

Now Conditional Probability of each packet being malicious under legitimate packets is

$$P(m, l) = P(m+l, m) \cdot P(m+l) \quad (1)$$

Where $P(m+l, m)$ is the Probability of exactly occurrence of *'m'* success and is given by Binomial Experiment as

$$P(m+l, m) = {}^{m+l}C_m \, p^m q^l$$

$$P(m+l, m) = m+l\,!\,/\,m\,!\,l\,!\; p^m q^l \quad (2)$$

Further form Poisson's Distribution

$$P(m+l) = e^{-\lambda} \lambda^{m+l} / m+l\,! \quad (3)$$

From equation (2) and (3), we can rewrite equation (1) as:

$$P(m, l) = P(m+l, m) \cdot P(m+l)$$

$$= m+l\,!\,m\,!\,l\,!\, p^m q^l \cdot e^{-\lambda} \lambda^{m+l} / m+l\,!$$

$$= p^m (1-p)^l \cdot e^{-\lambda} \lambda^{m+l} / m\,!\,l\,! \quad \text{(replacing } q = 1-p\text{)}$$

$$= p^m (1-p)^l (e^{-\lambda p} e^{-\lambda(1-p)} \lambda^m \lambda^l / m\,!\,l\,!$$

$$= e^{-\lambda p} (p^m \lambda^m) / m\,! \cdot e^{-\lambda(1-p)} (1-p)^l \lambda^l / l\,! \quad (4)$$

Now from equation (4) , the Joint probability of malicious packets in total traffic is given by

$$P(M = m) = \sum_{m=0}^{\infty} e^{-\lambda p} (p^m \lambda^m) / m! \quad (5)$$

From the above equation (5) , by putting the value of Joint Probability to 1 (As the aim of the attacker is to exceed the total channel bandwidth capacity by sending as much as malicious packets as possible) , the value of Poisson's distribution 'λ (rate of arrival of packets) and approximate probability of malicious packet *'p*', we can find the value of *'m'* , the number of packets that are being malicious in the traffic .So now by the help of this analytical approach based on mathematical equations we can get the no. of packets that are malicious in legitimate data and then these packets can be mitigated on the basis of hoop count value stored in their TTL (Time to Live) filed.

2.2 Proposed Mitigation Algorithm

We now propose a algorithm named *Hoop Count Inspection with Malicious Probability Rate (HCI-MPR) based* on Hoop count Inspection to mitigate these malicious packets.

Step 1: For given value of '***λ***' and 'p' **calculate 'm'** (no of malicious packets) such that P(M = m) = 1(From equation (5) joint probability of malicious packets)

Step 2: Initialize count = 1

Step 3: For each value of count =1 to m

Extract final value of TTL (Time to Live) as T_f

Investigate the initial value of TTL as T_i

Compute Hoop count $H_c = T_f - T_i$

Retrieve the stored Hoop count index as H_s

For each packet

if (H_c != H_s)

then

'discard the packet' // Packet is malicious

else

'allow the packet' // Packet is legitimate

Step 4: Increment count as count ++

Step 5: Repeat step 3 until count < = m.

Step 6: if count > m exit.

3. SIMULATION RESULTS

We have simulated our Proposed Algorithm *Hoop Count Inspection with Malicious Probability Rate (HCI-MPR)* against Traditional *Hoop count inspection Method (HCIM)* under CloudSim simulator toolkit the various parameters set for the simulations are

- Simulation Time 120 s
- No of Nodes 2
- Node Placement Uniform
- Terrain Dimension 2000*2000 m^2
- Noise Figure 10 db
- Temperature 295k
- Bandwidth 8kbps

3.1. Computation Time

For Computation Time simulation of both the algorithms the sample inputs are taken as rate of arrival as '***λ***' with probability of malicious packet *'p*' for proposed *HCI-MPR* algorithms and the same rate of arrival will be considered for HCIM without ant probability rate (Table 1.) and the various results has been analyzed.

The results are analyzed based on computational time and detection rate as performance matrices. The various findings of the simulation are discussed as

Table 1. Sample Inputs

Sample	Sample Inputs	Detection Rate HCI-MPR (%)	Detection Rate HCIM (%)
1	λ = 1000 (packets/sec) , p = 0.5	99.8	99.2
2	λ = 2000 (packets/sec) , p = 0.6	99.6	98.3
3	λ = 4000 (packets/sec) , p = 0.7	98.1	97.3
4	λ = 6000 (packets/sec) , p = 0.8	97.5	96.4
5	λ = 8000 (packets/sec) , p = 0.9	96.4	95.3
6	λ = 9000 (packets/sec) , p = 0.8	96.1	94.3
7	λ = 10000 (packets/sec) , p = 0.7	95.2	92.8

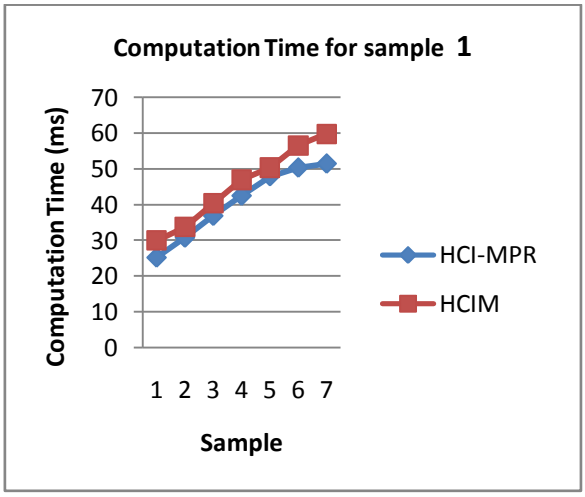

Figure 1. Graphs showing Computation Time

The graph (Figure. 1) shows that our proposed approach saves on potential computation time as compared to the HCIM over a much better rate and hence improves network performance. The Computation time is a much relevant factor for the performance measurement of the network as it improves the processing power of the Server and there is minimum loss of the available resources which support the network. The various recourses can be available to the clients if the computational speed will improve.

3.2 Detection Rate

The detection rate is the no of packets discarded as malicious over legitimate ones. The sample input for detection rate is taken (Table 2.) and analyzed.

Table 2. Sample Inputs

Sample	Sample Inputs	Computation Time HCI-MPR (ms)	Computation Time HCIM (ms)
1	λ = 1000 (packets/sec) , p = 0.5	25.26	29.98
2	λ = 2000 (packets/sec) , p = 0.6	30.81	33.78
3	λ = 4000 (packets/sec) , p = 0.7	36.89	40.35
4	λ = 6000 (packets/sec) , p = 0.8	42.52	46.95
5	λ = 8000 (packets/sec) , p = 0.9	47.94	50.36
6	λ = 9000 (packets/sec) , p = 0.8	50.35	56.58
7	λ = 10000 (packets/sec) , p = 0.7	51.47	59.78

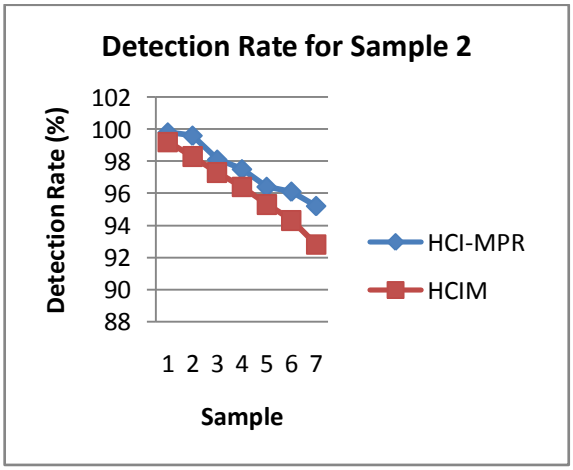

Figure 2. Graphs showing detection rate

As seen in the graph (Figure. 2) the detection rate of the proposed algorithm is 100% for sample inputs 1 and 2 and much better then HCIM for further corresponding sample inputs. The algorithm performance is very much impressive over a large data flow of packets which is a general trend in DDoS attacks.

4. CONCLUSION

As it is obvious fact that DDoS attacks are posing a vital threat to the emerging Cloud Computing environment, it now become very essential to provide a effective mechanisms that Mitigate these attacks. In this paper we proposed an analytical approach to address the DDoS attacks problem and simulation results shows that our proposed Algorithm saves on potential computation time while provide a impressive detection rate too. Further we add that the mechanism can work out well at

large data rates by providing some potential inputs in the future.

5. FUTURE WORK

There are still several issues regarding the DDoS attacks on Cloud Computing environment that warrant further research as the existing network may connect multiple stub networks which could make a single IP address to appear and have multiple valid hop-counts at the same time which further require enchantment in the our proposed algorithm HCI-MPR to check the credential of the sender for legitimate packets .Secondly we need a systematic procedure for setting the parameters according to the cloud environment for our proposed algorithm so that it show effective results against real spoofed DDoS traffics.

6. REFERENCES

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia *"Above the Clouds: A Berkeley View of Cloud Computing"* Technical Report No. UCB/EECS-2009-28.

[2] Balachandra Reddy Kandukuri, Ramakrishna Paturi Vand Dr. Atanu Rakshit "*Cloud Security Issues*" IEEE International Conference on Services Computing, 2009, DOI 10.1109/SCC.2009.84.

[3] Marios D. Dikaiakos, George Pallis, Dimitrios Katsaros, Pankaj Mehra and AthenaVakali"CloudComputing-*Distributed Internet Computing for IT and Scientific Research*" IEEE Internet Computing, 2009.

[4] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "*Ensuring Data Storage Security in Cloud Computing"* IEEE 2009.

[5] Kaiqi Xiong and Harry Perros "*Service Performance and Analysis in Cloud Computing*" Congress on Services – I, IEEE 2009, DOI 10.1109/SERVICES-I.2009.121

[6] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros *"Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities"* IEEE 2009Conference on Automation and Logistics Shenyang, China August 2009.

[7] John Viega, McAffee "*Cloud computing and the Common Man*" Computer, Published by the IEEE Computer Society 2009.

[8] Mladen A. Vouk *"Cloud Computing – Issues, Research and Implementations*" Proceedings of the *ITI 2008 30th Int. Conf. on Information Technology Interfaces*, June 23-26, 2008, Cavtat, Croatia.

[9] Arun Raj Kumar and P. and S. Selvakumar "*Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms*" 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[10] Qingtao Wu, Ruijuan Zheng , Jiexin Pu and Shibao Sun "*An Adaptive Control Mechanism for Mitigating DDoS Attacks*" Proceedings of the IEEE International Conference on Automation and Logistics Shenyang, China August 2009.

[11] Monika Sachdeva, Krishan Kumar, Gurvinder Singh and Kuldip Singh "*Performance Analysis of Web Service under DDoS Attacks"* 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009

[12] Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo and Pedro García-Teodoro "*Mathematical Model for Low-Rate DoS Attacks Against Application Servers*" IEEE Transactions On Information Forensics and Security, Published by the IEEE Computer Society 2009.Vol. 4, No. 3, September 2009.

[13] Li Xinlei, Zheng Kangfeng and Yang Yixian "*A DDoS attack defending scheme based on network processor"* 2009 WASE International Conference on Information Engineering.

[14] Yi Xie and Shun-Zheng Yu "*Monitoring the Application-Layer DDoS Attacks for Popular Websites*" IEEE/ACM Transactions on Networking, Vol. 17, NO. 1, Feb. 2009.

[15] Simon Liu, *US National Library of Medicine "Surviving Distributed Denial-of-Service Attacks" C*omputer.org/ITPro, Published by the IEEE Computer Society 2009