Indian Journal of Science and Technology, *Vol 8(32), DOI: 10.17485/ijst/2015/v8i32/84409, November 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Identifying and Blocking High and Low Rate DDOS ICMP Flooding

M. A. Vinoth Kumar[1] and R. Udayakumar[2*]

[1]Department of Information Technology,Jerusalem College of Engineering, Chennai - 600100, Tamil Nadu, India; ma.vinothkumar@gmail.com
[2]Department of Information Technology, Bharath University, Chennai - 600073, Tamil Nadu, India; udayakumar.it@bharathuniv.ac.in

Abstract

The technique to prevent and block Distributed Denial of Service (DDoS)[1] attacks has become the most difficult task, because as the attackers have lot of new trend hardware and software devices and techniques to disturb the network resources. DDoS attacks is the most vulnerable threat for all internet users and identifying these kinds of attacks as soon as it initiated from the attackers and successfully preventing it not to cause damage to network. The effective method to protect ICMP flooding DDoS attack is most required technique for these modern network security systems. The high rate of ICMP DDoS attack focuses on denying a ICMP services or its related equipments to its intended users. The high rate of attack is typically detected and blocked by the ISPs (Internet Service Providers)[2] level, by forming protecting virtual rings around the preventing hosts which will defend against the high level of attacks by exchanging selected traffic details with multiple Intrusion Detection System and Intrusion Prevention System[3] using a technique called FireCol[4]. The another most vulnerable attack called low-rate ICMP DDoS flooding[5] has the ability to gradually obscure its traffic as it is much a like to ordinary traffic. The potential technique to stop this form of attack by means of HAWK (Halting Anomaly with Weighted Choking)[6] system, this is based on threshold level of the packet flow is being implemented. By combining both these techniques, the increasing security threats of low and high level of ICMP flooding DDoS attacks may be identified and block to the greatest level and it can also promise that a service will never be denied to its anticipated user.

Keywords: DDoS, Flooding, High Rate ICMP Flooding, ICMP, Low Rate ICMP, Network Security, Passive Attack

1. Introduction

ICMP Distributed Denial of Service (DDoS) attacks are preliminary to grow to be one of the for the most part feared attacks on the Internet. In recent times the hacktivist group Anonymous[7] has demonstrated and published the seriousness of ICMP flooding, even the high level Government websites are diminishing victim to DDoS attacks and the numerous safety actions to avoid them are rendered inadequate as the intruders constantly stumble on a new technique for new type of attacks. Sufferers are subjected to discomfiture as the flaw in the security has been uncovered to everyone.

ICMP flooding threatens the most significant feature of the CIA triangle: 'availability'. People typically engaged their official and commercial work which is high level of sensitive data and information on servers in a idea that the information stored is forever available to them. The world in which we live in continuously depends upon Internet services to go on their regular activities. Consider after logging into your internet banking account to do urgent fund transfers

*Author for correspondence

and realizing that the server has been went down due to ICMP flooding.

This paper completely focuses on preventing both high and low rate of ICMP DDoS attacks by setting up a protocol which will be able to clearly make a distinction between the attackers and normal users. It assures to achieve this feat by mixing the Firecol and HAWK techniques.

2. Related Works

The Firecol residue to be one of the best technique to prevent high rate DDoS attacks as it uses an efficient method of placing IPS at the Internet Service Provider(ISP) levels that effectively eliminates most of the threat from DDoS attacks. Firecol employs a ring like configuration to place the IPS around the ISP which ensures that there are multiple layers of security which makes it hard for the intruder to break in.

The intruder detection system's algorithm is developed in such a way that it successfully detects High Rate DDoS attacks while it is unfeasible when it comes to differentiating between a malicious packet and a original packet if it is sent at a usual traffic rate. However, Firecol's effectiveness and its easy application in real networks makes it very desirable for successfully preventing high rate DDoS attacks.

When we look for successful ways of preventing Low Rate DDoS attacks, Rejo and Vijay's "Survey of Low Rate DDoS Attacks" [8] gives us a clear insight on how dangerous these LDDoS attacks are as they are very hard to detect and easily disguised with normal traffic. They inject short burst of traffic which eventually bottlenecks the buffer. While their paper gives us a clear method to detect DDoS attacks, we had to turn elsewhere for an algorithm that successfully prevents it.

HAWK technique detects malicious packets and drops such packets to allow only genuine packets into the network. This feat is achieved by assigning a threshold value to the packets and comparing the packets with a small flow table.

There are other techniques that can be used to detect malicious packets but the HAWK technique proves to be most desirable because it does not take up a lot of memory space. Pattern matching technique, for example, would require some memory space to store the patterns and that would be counterproductive at router levels as it would slow down the data transfer process considerably. Hence, HAWK technique is the way to go on our path to successfully prevent LDDoS attacks[1].

While all these methods successfully prevent DDoS attacks, the root of these problems lie elsewhere. Thousands of computers are being compromised everyday and being turned into a botnet[9] without the knowledge of its owner. These botnet computers can become a part of an attack and the user would be completely clueless. If we could prevent the attackers from gaining access to these computers, they would be severely weakened as the strength of DDoS attack lies in the number of computers that the attacker has managed to get hold of[2].

One of the most popular approaches to detect botnets is by directly locating command and control traffic. Attackers prefer using IRC[10] to compromise computers as it provides anonymity and IRC also lacks strong authentication. It is ideal for a simple and widely available command and control channel for botnet communication[3]. However, there are certain weaknesses in using IRC that can be used against the attackers. The best way to detect traffic would be to off ramp traffic from the network on known IRC ports and then further inspect the strings to see if it matches botnet commands. They also suggest studying the behavioral characteristics of botnets and could also use non productive resource like a honey pot[4].

A Multi-Layered Approach[11] to Botnet Detection is a much stronger botnet detecting architecture that was designed with a single motive: detect wide ranges of botnets. Not relying on a single technique, the design uses multiple techniques to detect array of botnets[5]. The open architecture enables anyone to follow up and integrate their own idea into the system to make it even stronger. The design uses data mining techniques to detect not only the botnets but also any other kind of anomaly or misuse of the computer[6].

3. Proposed Work

This is one of the most optimal way to detect both High Rate and Low Rate DDoS attacks and prevent them successfully. While Firecol already gives us an effective solution to the high rate attacks, a system needs to be designed that could successfully detect LDoS attacks as well. We can accomplish this feat by combining HAWK and Firecol techniques[7].

The high rate DDoS attack can be detected by computing the entropy and frequency values of the incoming packets. When the incoming bandwidth level exceeds the

ISP allocated bandwidth, we can conclude that the system has been subjected to high rate DDoS attack and the information is communicated to all IPS[8]. The ring level protection of Firecol is assigned only to the subscribed users of that particular ISP.

HAWK technique involves assigning a threshold value for all the incoming packets and the packets which show a large variation from the average threshold value is checked[9]. If it is found to be malicious, then that packet is immediately blocked and the information of that packet is sent across to all IPS[10].

Intruders now resort to Low Rate DDoS attacks as there are not many algorithms that successfully prevent it. A successful DDoS prevention algorithm must be equipped to prevent both High Rate and Low Rate DDoS attacks. It is always necessary to be one step ahead of the intruders and our system promises to limit the DDoS attacks up to a maximum extent[11].

4. Architecture

Our system (Figure 1) is designed in such a way that it provides maximum security to the ISP subscribed users who could turn out to be potential victims of DDoS attacks[12]. There are Intrusion Prevention Systems deployed around the user in a ring like structure that has H-IPS in the outer ring that primarily focuses on preventing High Rate attacks. This can be achieved by comparing the incoming packet's bandwidth level to the ISP allocated bandwidth. If the incoming bandwidth exceeds the allocated limit, then it is understood that the system is under attack and the incoming packet will be immediately dropped[13]. To ensure that the malicious packet does not enter the system in anyway, the IP and Port number are communicated to all other IPS as well[14].

While this ensures that the High Rate attacks are successfully blocked, some Low Rate attacks can pass through the system. To prevent this, an L-IPS which focuses only on prevention of Low rate DDoS attacks exists. This is strategically placed in the level right before the user because it is an extensively analysis oriented security process and such analysis cannot be applied for high rate traffic[15]. LRate attacks are successfully prevented by comparing the threshold value and if it exceeds the average queue size, it is deemed to be a malicious packet and the packet is dropped. This information is also communicated across the IPS to prevent further attack from that source[16].

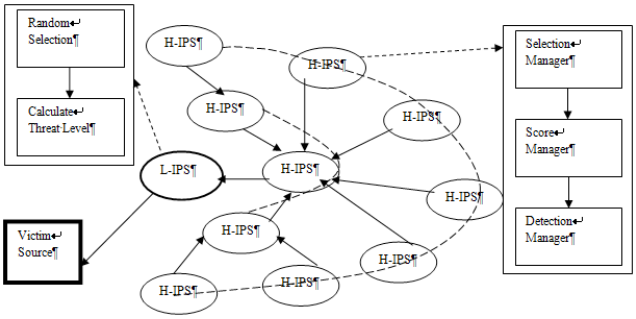

Figure 1. System Architecture.

5. Thread Level Calculation

Thread level can be calculated by comparing the flow table (previous packet's IP and Port) for the following time period

Table 1. Thread level calculation

Packets with Bandwidth	Time (second)	Level
Minimum 3 packets from the same source with high bandwidth	Below 5 seconds	Level 3 (high)
Minimum 3 packets from the same source with high bandwidth	Above 5 seconds and between 30 seconds	Level 2 (medium)
Minimum 3 packets from the same source with high bandwidth	Interval of above 30 seconds	Level 1 (low)

6. Algorithm

6.1 High Rate DDoS Algorithm

If (IRate > ABand)
  Block IP and Port
  Alert DDoS Attack to all IPS

6.2 Low Rate DDoS Algorithm

If (AvgQSize < Min(thr))
 If (Flow Malicious)
  Drop Packets
 else
    Admit Packets
  else
   Select Random Packets from Queue

```
If (Both packet from same source)
Calculate Threat level //Based on multiple occurrences
    if (Threat greater)
      Block the flow
    else
      Drop packet
else
    if (C(brust) > C(Thresh))
      Drop packet
    else
      Admit packet with P
```

Table 2. Network Utilization Comparison Table

Packet SizeW	Network Utilization	
	Existing System	Proposed System
60(Normal Flow)	4%	4 %
400(Low Rate Attack)	27%	Blocked.
500(Low Rate Attack)	34%	Blocked.
900(Low Rate Attack)	60%	Blocked.
1150(High Rate Attack)	Blocked.	Blocked.

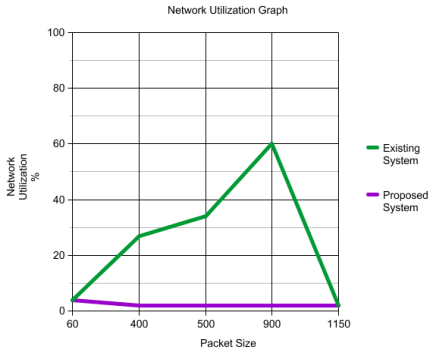

Figure 2. ICMP Flooding Performance Graph.

7. Conclusion

The main aspect of this work that sets it apart from the other ICMP DDoS Preventing algorithms is that it provides an extra layer of security that detects and prevents Low Rate ICMP DDoS attack. While we focus more on preventing Low Rate ICMP DDoS attack, we also take in considerations the threat that high rate ICMP DDoS attacks cause and use Firecol to prevent it. Firecol places IPS around the ISP in a ring like architecture that gives the network multiple layers of security. When it comes to detecting LDDoS attacks, we use HAWK technique that compares the threshold values of the incoming packets and HAWK is the most efficient technique among all other LDDoS detecting techniques as it uses less memory. Both our High Rate and Low Rate detecting techniques are efficient in terms of security and resource usage.

DDoS attacks have caused havoc in many places around the Internet as it has been used as a tool to bring down many important websites. Our system, if implemented, should be able to detect and prevent most of the DDoS attacks and hopes to provide maximum security against DDoS attacks.

8. References

1. Patrikakis C, Masikos M, Zouraraki O. National Technical University of Athens. Available from: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html
2. NTC Hosting. Available from: http://www.ntchosting.com/internet/isp.html
3. Sree Latha R, Vijayaraj R, Azhagiya Singam ER, Chitra K, Subramanian V. 3D-QSAR and Docking Studies on the HEPT Derivatives of HIV-1 Reverse Transcriptase. Chemical Biology and Drug Design. 2011; 78(3):418–26. ISSN: 1747-0285.
4. Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth. SANS Institute. 2004. p. 14
5. Francois J, Aib I, Boutaba R. Fire Col: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. IEEE Transactions on Networking. 2012; 20(6):1828–41.
6. Masthan KMK, Aravindha Babu N, Dash KC, Elumalai M. Advanced diagnostic aids in oral cancer. Asian Pacific Journal of Cancer Prevention. 2012; 13(8):3573–6. ISSN: 1513-7368.

7.Guirguis M, Bestavros A, Matta I. On the Impact of Low-Rate Attacks. IEEE International Conference on Communications; Computer Science Department Boston University ; Istanbul. 2006; 5:2316–21. Science Department, Boston University.

8. Kwok Y-K, Tripathi R, Chen Y, Hwang K. HAWK: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks. Networking and Mobile Computing. 2005; 3619:423–32.
9. Tamilselvi N, Dhamotharan R, Krishnamoorthy P, Shivakumar. Anatomical studies of *Indigofera aspalathoides*

Vahl (Fabaceae). Journal of Chemical and Pharmaceutical Research. 2011; 3(2):738–46. ISSN: 0975–7384.
10. Available from: http://en.wikipedia.org/wiki/Anonymous_(group).
11. Mathew R, Katkar V. Survey of Low Rate DoS Attack Detection Mechanisms. ICWET'11 Proceedings of the International Conference and Workshop on Emerging Trends in Technology. 2011. p.955–8. University, Mumbai, India.
12. Devi M, Jeyanthi Rebecca L, Sumathy S. Bactericidal activity of the lactic acid bacteria *Lactobacillus delbreukii*. Journal of Chemical and Pharmaceutical Research. 2013; 5(2):176–80. ISSN: 0975–7384.
13. Timothy Strayer W, Lapsely D, Walsh R, Livadas C. Botnet Detection Based on Network Behavior. Advances in Information Security. 2008; 36:1–24.
14. Naseem F, Shafqat M, Sabir U, Shahzad A. A Survey of Botnet Technology and Detection. International Journal of Video and Image Processing and Network Security. 2010; 10(1):4.
15. Reddy Seshadri V, Suchitra MM, Reddy YM, Reddy Prabhakar E. Beneficial and detrimental actions of free radicals: A review. Journal of Global Pharma Technology. 2010; 2(5):3–11. ISSN: 0975-8542.
16. Erbacher RF, Cutler A. A Multi-Layered Approach to Botnet Detection. Proceedings of the 2008 International Conference on Security and Management; Las Vegas. 2008. p.14–7.
17. Kimio T, Natarajan G, Hideki A, Taichi K, Nanao K. Higher involvement of subtelomere regions for chromosome rearrangements in leukemia and lymphoma and in irradiated leukemic cell line. Indian Journal of Science and Technology. 2012 April; 5(1):1801–11.
18. Cunningham CH. A Laboratory Guide in Virology. 6th ed. Minnesota: Burgess Publication Company; 1973.
19. Sathish Kumar E, Varatharajan M. Microbiology of Indian Desert. In: Sen DN, editor. Ecology and Vegetation of Indian Desert. India: Agro Botanical Publishers; 1990. p. 83–105.
20. Varatharajan M, Rao BS, Anjaria KB, Unny VKP, Thyagarajan S. Radiotoxicity of Sulfur-35. Proceedings of 10th NSRP; India. 1993. p. 257–8.
21. 01 Jan 2015. Available from: http://www.indjst.org/index.php/vision