DETECTION AND PREVENTION OF LOW AND HIGH RATE FLOODING DDOS ATTACKS

D. Muruganandam, (PhD) , Dr.J.Martin Leo Manickam, PhD, M.A. Vinoth Kumar, (M.E)

Department of Computer Science, University College of Engineering, Panruti, India

Department of Electronics and Communication Engineering, St.Joseph's College Of Engineering

Department of Computer Science, University College of Engineering, BIT Campus, India

ABSTRACT

The implementation of counter measures against Distributed Denial of Service (DDoS)[Charalampos Patrikakis,] attacks has become a challenging task as the attackers are equipped with vast resources and techniques. DDoS attacks are a major threat to the Internet users and detecting these kinds of attacks as soon as it starts from the source and before it reaches the victim is the key to successfully preventing it. An effective method to deal with both high and low rate flooding DDoS attack is highly desirable in the world of Network Security. The high-rate DDoS attack focuses on denying a services or system components to its intended users. This type of attack is usually detected and prevented at the ISP (Internet Service Provider)[NTC Hosting] level, by forming virtual protection rings around the hosts to defend the network and collaborate by exchanging selected traffic information with multiple IDS/IPS[SANS Institute] using FireCol[Jérôme François, Issam Aib] technique. The low-rate DDoS attack[Mina Guirguis] has the ability to significantly conceal its traffic as it is much similar to normal traffic. A promising approach to prevent this type of attack by using HAWK(Halting Anomaly with Weighted Choking)[Yu-Kwong Kwok] technique, which is based on threshold level of the packet flow is being implemented. By applying both these techniques, the increasing security threats of DDoS attacks can be eradicated to the maximum level and it can also be ensured that a service will never be denied to its intended user.

Keywords

DDoS, Network Security, Passive Attack, High Rate DDoS, Low Rate DDoS.

1. INTRODUCTION

Distributed Denial of Service (DDoS) attacks are starting to become one of the most feared attacks on the Internet. As recently demonstrated by the hacktivist group Anonymous[Wikipedia], even the top Government websites are falling prey to DDoS attacks and the countless security measures to prevent them are rendered useless as the intruders always find a way around them. DDoS victims are subjected to embarrassment as the weakness in the security has been exposed to everyone.

DDoS attacks threaten the most important aspect of the CIA triangle: availability. People usually store most of the sensitive and important information on servers in a belief that the information stored is always accessible to them. The world in which we live in continuously depends upon Internet services to go about their day to day activities. Imagine logging into your bank account to make some important fund transfers and realizing that the server has been taken down!

Our project focuses on preventing both low and high rate DDoS attacks by setting up a protocol which will be able to clearly differentiate between the normal user and the attacker. We promise to achieve this feat by combining the Firecol and HAWK techniques.

2. Related Works

Firecol remains to be one of the most secure algorithms to prevent high rate DDoS attacks as it uses an effective mechanism of placing Intrusion Prevention Systems(IPS) at the Internet service Provider(ISP) levels that successfully eliminates most of the threat from DDoS attacks. Firecol employs a ring like structure to place the IPS around the ISP which ensures that there are multiple layers of security which makes it hard for the intruder to penetrate.

The intruder detection system's algorithm is developed in such a way that it successfully detects High Rate DDoS attacks while it is clueless when it comes to differentiating between a malicious packet and a genuine packet if it is sent at a normal 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" [Rejo Mathew] 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.

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[W. Timothy Strayer] 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.

One of the most popular approaches to detect botnets is by directly locating command and control traffic. Attackers prefer using IRC[Fatima Naseem] 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. 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.

A Multi-Layered Approach[Robert F. Erbacher] 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. 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.

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.

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. 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. 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.

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.

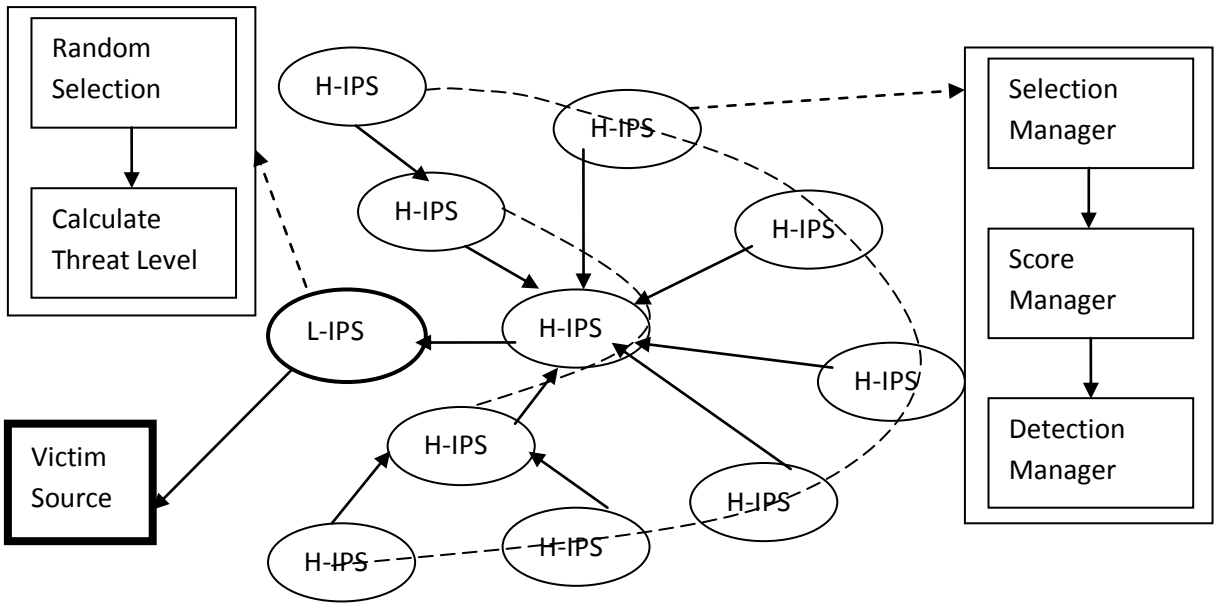

Figure 1. System Architecture

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. 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. 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.

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. 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.

4.1 Thread level calculation

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

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)

Table 1. Thread level calculation

5. Algorithm

5.1 High Rate DDoS Algorithm

If (IRate > ABand)

Block IP and Port

Alert DDoS Attack to all IPS

5.2 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

6. Conclusion

The main aspect of this work that sets it apart from the other DDoS Preventing algorithms is that it provides an extra layer of security that detects and prevents Low Rate DDoS attack. While we focus more on preventing Low Rate DDoS attack, we also take in considerations the threat that high rate DDoS attacks cause and use Firecol to prevent it. Firecol places Intrusion Prevention Systems (IPS) around the Internet Service Provider (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.

7. References

[1] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki National Technical University of Athens http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

[2] NTC Hosting - http://www.ntchosting.com/internet/isp.html

[3] Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute

[4] FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks, Jérôme François, Issam Aib, Member, IEEE, and Raouf Boutaba, Fellow, IEEE

[5] On the Impact of Low-Rate Attacks, Mina Guirguis Azer Bestavros Ibrahim Matta, Computer Science Department Boston University

[6] HAWK: Halting Anomalies with Weighted Choking toRescue Well-Behaved TCP Sessions fromShrew DDoS Attacks, Yu-Kwong Kwok, Rohit Tripathi, Yu Chen, and Kai Hwang University of Southern California

[7] Wikipedia - http://en.wikipedia.org/wiki/Anonymous_(group)

[8] Survey of Low Rate DoS Attack Detection Mechanisms, Rejo Mathew & Vijay Katkar, University, Mumbai, India

[9] Botnet Detection Based on Network Behavior, W. Timothy Strayer, David Lapsely, Robert Walsh, and Carl Livadas

[10] A Survey of Botnet Technology and Detection, Fatima Naseem, Mariam shafqat, Umbreen Sabir, Asim Shahzad, University of Engineering and Technology, Taxila

[11] A Multi-Layered Approach to Botnet Detection, Robert F. Erbacher, Adele Cutler, Utah State University