UDC 004.056

PROTECTION AGAINST VARIOUS CLASSES OF DDOS ATTACKS

Pan Huiqin, Master's degree student

Nasonova N.V., Dr.Sc., Assoc.Prof.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Annotation. This paper introduces a DDoS attacks defense technique, which includes the measures for the four stages, such as pre-configuration, detection, blockage and mitigation. The DDoS defense technique is suggested for development of algorithms for defenses against various types of DDoS attacks applying the analysis of their OSI-level characteristics.

Keywords. DDoS-attacks, Defense Technique, OSI levels.

1. Analysis of DDoS attacks

A Distributed Denial of Service attack (DDoS) is a malicious attempt to flood a targeted server, service, or network with massive amounts of Internet traffic, disrupting its normal traffic and rendering it inaccessible to legitimate users. Unlike traditional denial-of-service (DoS) attacks, DDoS attacks utilize multiple infected computer systems as the source of the attack traffic, making defense more difficult. The general DDoS attack model is shown in Figure 1.

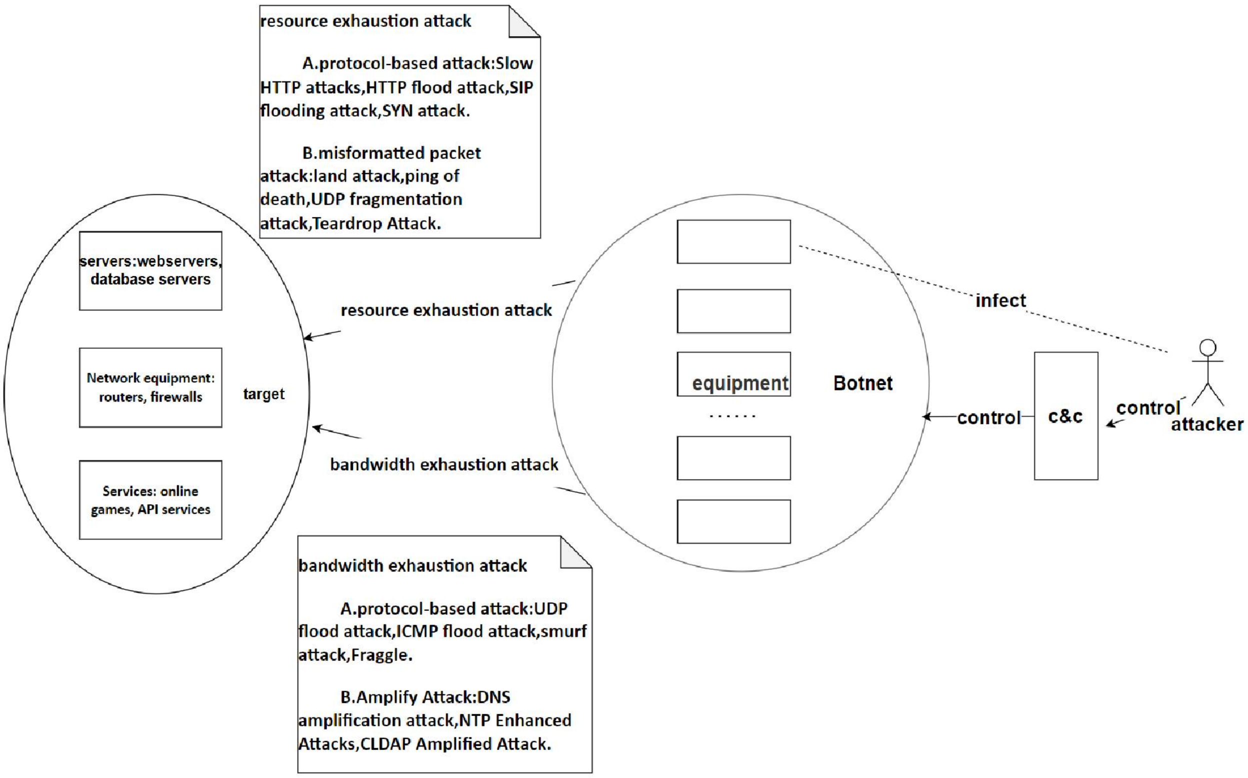
resource exhaustion attack
A.protocol-based attack:Slow HTTP attacks,HTTP flood attack,SIP flooding attack,SYN attack.
B.misformatted packet attack:land attack,ping of death,UDP fragmentation attack,Teardrop Attack.
servers:webservers, database servers
Network equipment: routers, firewalls
Services: online games, API services
target
resource exhaustion attack
bandwidth exhaustion attack
equipment
......
Botnet
infect
control
c&c
control
attacker
bandwidth exhaustion attack
A.protocol-based attack:UDP flood attack,ICMP flood attack,smurf attack,Fraggle.
B.Amplify Attack:DNS amplification attack,NTP Enhanced Attacks,CLDAP Amplified Attack.

Figure 1 – General DDoS Attack Model

The DDoS attack model includes the parts of attacker, botnet, connection between attacker and botnet, attack channel, attack target, connection between attacker and target, and attack result.

Attackers include controllers as well as command and control servers, and controllers are usually the initiators of attacks, using a variety of tools and techniques to control large numbers of botnets. The attacker uses the command and control server to send commands to the controlled devices. Attackers infect a large number of devices with malware, turning them into botnets, which are often distributed across the globe, helping attackers hide their true origins.

Connection between attacker and botnet: Attackers infect a large number of devices in various ways. Incorporating them into a botnet. These devices may include personal computers, servers, IoT devices, etc. After infecting the devices, the attacker needs to install malware on the devices and create a control channel through which the attacker can remotely control these devices. The attacker manages and controls the botnet through a command and control server (C&C server). Communication between the attacker and the botnet typically uses encrypted or obfuscated protocols to avoid detection and interception. Common communication protocols include IRC (Internet Relay Chat), HTTP, HTTPS, DNS, and others.

The attack channels include resource exhaustion attacks and bandwidth exhaustion attacks. Attack targets include servers (web servers, database servers, etc.), network devices (routers, firewalls, etc.), and services (online games, API services, etc.).

Connection between attacker and target: When an attacker initiates a DDoS attack, the C&C server sends commands to each device in the botnet in order to send a large number of requests to the target server. These requests may be HTTP requests, TCP connection requests, UDP packets, etc., depending on the type of attack. There are two results of the attack, either exhausting system resources or exhausting system bandwidth.

2.Classification of DDoS attacks

The OSI (Open Systems Interconnection) model categorizes network communications into seven layers, each with its own specific functions and protocols. DDoS attacks can be categorized based on the OSI layer they target. The classification of DDoS attacks with reference to the seven-layer network architecture is shown in Table 1.

Table 1 – Classification table for DDoS attacks

OSI level	Classification of attacks	Characteristics of the attack
data link layer	MAC Flood	ARP Spoofing Attackers launch DDoS attacks mainly by manipulating MAC addresses, ARP protocols, or switch forwarding logic, with the core objective of disrupting normal frame forwarding or exhausting link resources.
network layer	ICMP Flood IP Fragmentation Attack	Magnification effect Fake source IP Attackers mainly use IP protocol flaws and routing mechanisms to launch DDoS attacks and achieve damage by forging, amplifying, or exhausting target resources.
transport layer	SYN Flood attack UDP Flood attack ACK Flood attack	Halfway connection High flow rate and low power consumption Attackers primarily exploit TCP/UDP protocol flaws to launch DDoS attacks by exhausting connection resources or bandwidth.
session layer	Session Exhaustion Attack	Encryption overhead Session fixation attack Attackers mainly exploit vulnerabilities in the session management mechanism to launch DDoS attacks by exhausting encrypted resources, spoofing sessions, or maintaining malicious long connections.
presentation layer	SSL/TLS Flood attack	data malformation Attackers mainly use vulnerabilities in data format parsing, encryption/decryption process or encoding conversion to launch DDoS attacks and consume target system resources by constructing malformed data.
	DNS Flood Attack	low-flow, high-kill Protocol Abuse Precise targeting

application layer	DNS Reflex Attack HTTP Flood attack Slowloris attack CC attack	Attackers usually spoof the source IP, mimic legitimate traffic, and take advantage of protocol design flaws to exhaust the resources of the attack target with low traffic and high kills.

3. DDOS attack defense technique

DDoS attack is a complex network security threat that requires a comprehensive defense from multiple perspectives [1]. The principle mechanism of defense against various attacks generally includes the four steps, such as pre-configuration of the system to be protected, detection of attacks [2], blockage of attacks and mitigation the consequences of the attacks. In relation to DDoS attacks this mechanism was transformed into a defense technique against DDoS attack, which includes the following measures, shown in Figure 2.

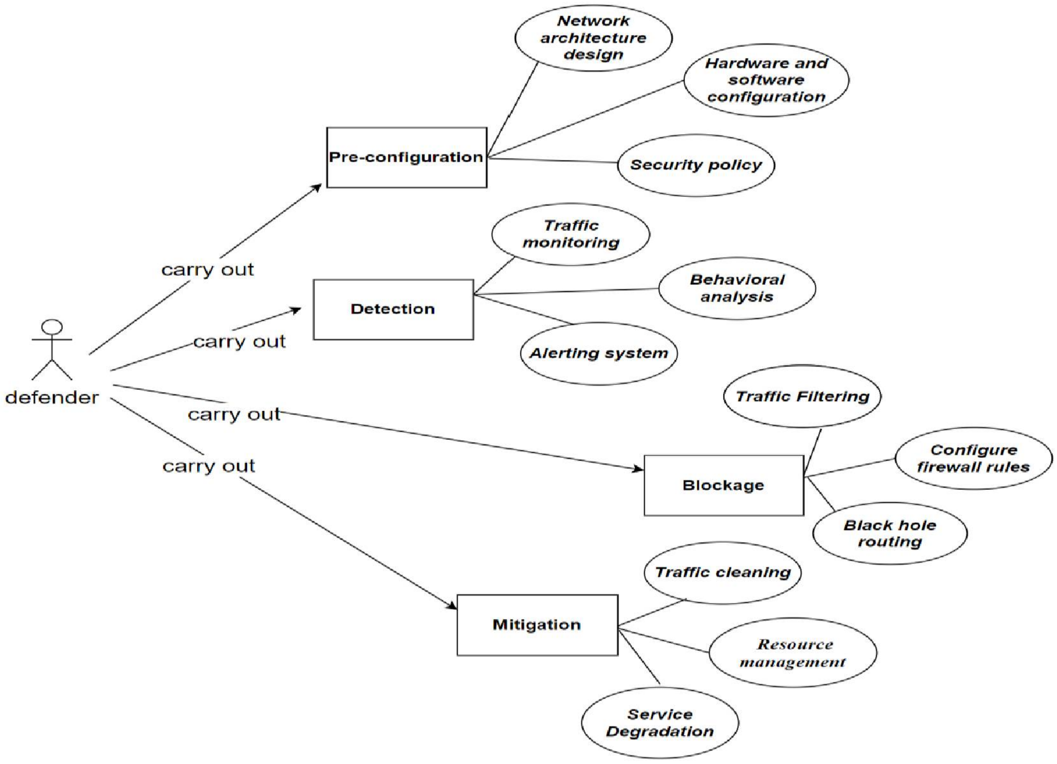

Figure 2 – Step-by-step diagram for DDoS defense technique implementation

1. Pre-configuration.

Network architecture design: deploy multiple servers and multiple data centers to disperse traffic pressure; use load balancers to evenly distribute traffic to multiple servers to avoid a single point of failure; distribute content via CDN to reduce direct access to the source server.

Hardware and software configuration: Enable firewall rules to filter abnormal traffic; configure routers to limit the traffic rate of protocols such as ICMP, UDP, etc.; optimize server configurations to improve processing power (e.g., increase connection limits, enable SYN cookies).

Security policy: Limit access to critical services and allow access only to trusted IP addresses; disable unnecessary protocols (e.g., ICMP, UDP) to reduce the attack surface; and update operating systems and applications in a timely manner to patch known vulnerabilities.

2. Detection.

Detecting DDoS attacks in real time is the first step in defense, and through early detection action can be taken quickly[3].

Traffic monitoring: establish a baseline of normal traffic and monitor traffic changes in real time; use tools (e.g., NetFlow, sFlow) to detect traffic anomalies (e.g., traffic spikes, abnormal protocol ratios).

Behavioral analysis: Identify abnormal behavior (e.g., a large number of requests coming from the same IP address) by analyzing user behavioral patterns; detect complex attack patterns using machine learning algorithms.

Alerting system: Setting traffic thresholds and triggering alerts when the traffic exceeds the thresholds; analyzing server logs regularly to find signs of potential attacks.

3. Blockage.

After a DDoS attack is detected, rapid measures are taken to block the attack traffic and reduce the impact on the target system.

Traffic Filtering: Add the source IP address of the attack to the blacklist and block its access; filter abnormal protocol traffic (e.g. ICMP Flood, UDP Flood); block traffic from a specific region based on the geographic location of the IP address[4].

Configure firewall rules to filter malicious traffic; utilize Intrusion Detection Systems (IDS) to detect and report attack traffic in real time; utilize Intrusion Prevention Systems (IPS) to automatically block detected attack traffic.

Black hole routing: direct attack traffic to the “black hole” to avoid affecting the target server; dynamically adjust black hole routing rules according to traffic conditions.

4. Mitigation.

While blocking attack traffic, take steps to mitigate the impact of the attack on the system and ensure service availability.

Traffic cleaning: Use professional DDoS protection services (e.g. Cloudflare, Akamai) to filter malicious traffic; deploy local traffic cleaning equipment to filter attack traffic in real time[5].

Resource management: Dynamically adjust resource allocation and prioritize the operation of critical services; in a cloud environment, resources are automatically expanded based on traffic.

Service Degradation: Temporarily shut down non-critical services during an attack and focus resources on securing core services.

The **algorithm for defenses against SYN Flood-type attacks** was developed according to the general technique described above and the OSI-level characteristics for this type of attacks. The algorithm is shown below:

For the Pre-configuration stage:

1.Enable SYN Cookie: Instead of allocating resources immediately upon receiving a SYN request, the server generates a SYN cookie (a hash containing connection information) as a SYN-ACK response. Only after receiving a legitimate ACK response does the server allocate resources.

Firewall Configuration: Configure rules on the firewall to limit the rate of SYN requests per IP address.

For the Detection stage:

2.Analyze the source IP address of SYN requests to identify abnormal behavior (e.g., a large number of SYN requests coming from the same IP address); monitor the status of the server's half-connection queue to find out when the half-connection queue is full.

Sets the threshold for SYN requests and triggers an alert when a SYN request exceeds the threshold.

For the Blockage stage:

3.Using a SYN proxy device, the proxy server handles SYN requests and filters malicious traffic. Utilizes Intrusion Detection System (IDS) to detect and report SYN Flood attack traffic in real-time. Using Intrusion Prevention System (IPS), automatically blocking detected SYN Flood attack traffic.

For the Mitigation stage:

4.Switch dynamic websites to static pages to reduce server load; during an attack, temporarily shut down non-critical services and focus resources on safeguarding core services.

The DDoS defense technique is suggested for development of algorithms for defenses against various types of DDoS attacks applying the analysis of their OSI-level characteristics. The proposed defense algorithm against SYN flooding attack is tested in the lab environment, and it is found that the half-connection queue occupancy rate decreases by more than 80% and there is no queue overflow record in the kernel logs, the success rate of TCP connection establishment for normal users increases, and the attacking traffic is significantly reduced, which proves that the algorithm is effective.

List of references

1. Li Xiaoyong,Liu Dongxi,Gu Dawu,et al.Research on DDoS Defense and Response Technology[J]. Computer Engineering and Application, 2003, 39(12):4. DOI:10.3321/j.issn:1002-8331.2003.12.018.

2. Han Zhu,Fan Lei,Li Jianhua. DDoS defense mechanism based on source detection[J]. Computer Engineering, 2007, 33(19):150-151. DOI:10.3969/j.issn.1000-3428.2007.19.052.

3. Shang Zhanfeng,Zhang Dengyi.Research on DDoS defense mechanism[J]. Computer Technology and Development, 2008, 18(1):7-10.DOI:10.3969/j.issn.1673-629X.2008.01.002.

4. Wang Hui. A method and device for detecting forged source IPs in a DDOS defense system.2017[2025-03-27].

5. Wang, Xiaoling. Design and implementation of a DDoS defense system using source address information[J]. Journal of Southwest University for Nationalities:Natural Science Edition, 2015(41):467.