A Survey of Defence Mechanism Against DDOS Flooding Attacks

Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE

By Ufuk Özkanlı
Famous DDOS Attacks

DDoS Timeline

First Hacktivist event: Zapatista National Liberation Army

First Public Cyberheist: $10M Citibank

MafiaBoy DDoS: Yahoo!, Amazon, Dell, CNN, EBay, Etrade

Packeting for bragging rights.

Spammers discover botnets

Georgia/Russia

Estonia: Parliament, banks, media, Estonia Reform Party

Organized crime: Extortion

Spamhaus Attack: Reported to reach 310 Gbps

Coordinated Attacks on banks: Attack sizes to 170 Gbps continues today

Lockheed Martin: Suspected breach

DDOS Attackers Motivation

• Financial/economical gain (Experinced)
• Revenge (Fraustrated)
• Ideological belief (Major)
• Intellectual Challenge (Estonia, Iran, WikiLeaks)
• Cyberwarfare (Unit 61398)
PLA Unit 61398
DDoS flooding attacks

A. Network/transport-level DDoS flooding attacks
   1. Flooding Attacks
   2. Protocol exploitation flooding attacks
   3. Reflection-based flooding attacks
   4. Amplification-based flooding attacks

B. Application-level DDoS flooding attacks
   1. Reflection/amplification based flooding attacks
   2. HTTP flooding attacks
      1. Session flooding attacks
      2. Request flooding attacks
      3. Asymmetric attacks
      4. Slow request/response attacks
A. Network/transport-level DDoS flooding attacks

- These attacks have been mostly launched using TCP, UDP, ICMP and DNS protocol packets.
A1. Flooding Attacks

- Spoofed/non-spoofed UDP flood
- ICMP flood
- DNS flood
- VoIP Flood and etc. [32], [35]
A.2. Protocol exploitation flooding attacks

• (e.g., TCP SYN flood, TCP SYN-ACK flood, ACK & PUSH ACK flood, RST/FIN flood and etc. [32], [35])
A.3. Reflection-based flooding attacks

• (e.g., Smurf and Fraggle attacks)
A.4. Amplification-based flooding attacks

- Attackers send requests with spoofed source IP addresses (Reflection) to a large number of reflectors by exploiting IP broadcast feature of the packets (Amplification)
B. Application-level DDoS flooding attacks

- HTTP flooding
- DNS amplification flooding attack
- and the SIP flooding attack
B.1. Reflection/amplification based flooding attacks

• DNS amplification attack employs both reflection and amplification techniques.

• The attackers (zombies) generate small DNS queries with forged source IP addresses which can generate a large volume of network traffic since DNS response messages may be substantially larger than DNS query messages. Then this large volume of network traffic is directed towards the targeted system to paralyze it.
B.2. HTTP flooding attacks

- B.2.1. Session flooding attacks
- B.2.2. Request flooding attacks
- B.2.3. Asymmetric attacks

Attackers send sessions that contain high-workload requests
  - Multiple Http get/post flood
  - Faulty Application (Sql injections, Lockup database queries)

- B.2.4. Slow request/response attacks
  - Slowloris attack
  - Http Fragmentation
  - SlowPost
  - Slow Reading
Botnet Based DDOS Attacks

• Based on how bots are controlled by the masters, botnets are classified into three major categories [8], [44]:
  1. IRC-based
  2. Web-based
  3. P2P-based
Ultimate Goal Of DDOS defence

• Detecting DDoS attack as soon as possible and before it reaches the victims,
• identifying the attack sources
• stopping the attack as close as possible to the attack sources

best achieved through hybrid (Distributed) DDoS defense mechanisms.
Basic Defence Methods

The diagram illustrates the flow of network traffic from attack sources to victims in a DDoS attack. The network is divided into three main sections:

1. **Immediate upstream network to the Victim**
   - This is the closest network to the victim and is the first point of contact.

2. **Upstream intermediate network**
   - This is a network that processing traffic comes from further upstream.

3. **Further upstream intermediate network**
   - This is the most remote network from the attack sources.

The prevention and response mechanisms are better suited for attacking these networks in descending order. This strategy increases detection accuracy and Efficiency of response.

The diagram also shows the number of normal packets in the middle of a DDoS attack increases as the attack progresses, highlighting the importance of early detection and response.
Basic Defence Methods

- Combining source address authentication (to prevent IP spoofing), capabilities,
- and filtering

trade-off between performance and accuracy in any DDoS defense solution
DDOS Defence Mechanisms

• Classification criteria are important in devising robust defense solutions. Divided two categories.

A. Location where the defense mechanism is implemented (i.e., Deployment location).

B. Point of time when the DDoS defense mechanisms should act in response to a possible DDoS flooding attack.
A. Classification based on the deployment location
A.1. Source Based Defence

• Filter the attack traffic at the sources of the attack;
• not entirely effective against DDoS flooding attacks.
  • Source of attacks can be distributed in different domains making it difficult for each of the sources to detect
  • difficult to differentiate between legitimate and attack traffic near the sources
  • it is unclear who (i.e., customers or service providers) would pay the expenses
A.1.1.a. Ingress/Egress filtering at the sources’ edge routers

• Ingress/Egress filtering mechanisms to detect and filter packets with spoofed IP addresses at the source’s edge routers based on the valid IP address range internal to the network

• Cons
  • Pool of zombie genuine IP address
  • valid internal IP address range
  • Mobile IP users
A.1.1.b D-WARD

- Aims to detect DDOS flooding attack traffic by monitoring both inbound and outbound traffic of a source network and comparing the network traffic information with predefined normal flow models.

- Cons
  - consumes more memory space and CPU cycles than some of the
  - No incentive to protect other networks
  - Attack within a normal range traffic
A.1.1.c MUlti-Level Tree for Online Packet Statistics (MULTOPS) [60]

• a significant difference between the rates of traffic going to and coming from a host or subnet can indicate that the network prefix is either the source or the destination of an attack

• Cons
  • Multimedia streams
  • Dynamic Tree Structure vulnerable to memory exhaustion attack (use alternative TOPS)
A.1.1.d MANAnet’s Reverse Firewall [62]

• the reverse firewall protects the outside from packet flooding attacks that originate from within a network

• Cons
  • requires the administrators’ involvement.
  • the reverse firewall’s configuration cannot be dynamically changed at runtime.
  • there is no benefit (e.g., financial gain) for the source networks to deploy costly reverse firewalls since there is no benefit for the source networks.
A.1.2. Destination-based mechanisms

- In the destination-based defense mechanisms, detection and response is mostly done at the destination of the attack (i.e., victim).
- These mechanisms can closely observe the victim, model its behavior and detect any anomalies.
A.1.2.a IP Traceback mechanisms

• The process of tracing back the forged IP packets to their true sources rather than the spoofed IP addresses that was used in the attack is called traceback.
  • packet marking
    Storing the entire path in the IP identification field are not able to assign each mark to a unique path
  • link testing
    starts from the router closest to the victim and iteratively tests its upstream links until it can be determined which link is used to carry the attacker’s traffic (i.e., the traceback process is recursively repeated on the upstream router until the source is reached).

Cons
  Routers support traceback
A.1.2.b Management Information Base (MIB) [70]

• MIB data is comprised of parameters that indicate various packet and routing statistics

• Continuously analyzing MIB can help victims to identify when a DDoS attack is occurring

• These destination-based DDoS defense mechanisms drop suspicious packets when the network links are congested to a certain level
A.1.2.c Packet marking and filtering mechanisms [73],[74], [76]

• aim to mark legitimate packets at each router along their path to the destination

• so victims’ edge routers can filter the attack traffic.

• These mechanisms let the receivers install dynamic network filters to block the undesirable traffic
  • History-based IP filtering [73] (keep IP addresses that frequently appear)
  • Hop-count filtering [74](Keep IP and hops from dest.)
  • Path Identifier
A.1.2.d Packet dropping based on the level of congestion

- These destination-based DDoS defense mechanisms drop suspicious packets when the network links are congested to a certain level.
- Score of a packet is computed at Detecting-Differentiating-Discarding routers (3D-R) by employing a Bayesian-theoretic metric,
- a score-based selective packet discarding method at the destination is performed.
- The dropping threshold for the packet discarding method is dynamically adjusted based on (1) the score distribution of recent incoming packets.
A.1.3. Network-based mechanisms

- These mechanisms are deployed inside networks and mainly on the routers of the ASs [78]
- Cons
  - lead to high storage and processing overheads at the routers. These overheads get even worse if each router does redundant detection and response
  - To reduce the amount of redundant detection and response between the routers requires coordination among them
  - Large overhead of network communication
A.1.3.a Route-based packet filtering [79], [80]

• extends ingress filtering

• if an unexpected source address appears in an IP packet on a link, then it is assumed that the source address has been spoofed

• Cons
  • if attackers either use genuine IP addresses instead of spoofed ones or spoof with carefully chosen source IP addresses that are not going to be filtered.
A.1.3.b Detecting and filtering malicious routers [81]

- Router anomaly detector (Watchers[82])
- Cons
  - it cannot detect spoofed packets.
  - Even worse, such packets could be used by the attacker to misidentify a target as a bad router.
  - Watchers can only detect compromised routers and it is vulnerable to misbehaving hosts.
  - It also assumes that every router knows the topology of the network
  - Requires explicit communication
  - routers still do redundant jobs
A.1.4. Hybrid (Distributed) mechanisms

- A.1.4.a Hybrid packet marking and throttling/filtering mechanisms
- Hybrid packet throttling mechanisms usually place the attack detection modules near the victims and execute packet filtering close to the attack sources.
- A.1.4.b DEFensive Cooperative Overlay Mesh (DEFCOM) [93]
- A.1.4.c COSSACK [94]
- A.1.4.d Capability-based mechanisms [95]
- A.1.4.e Active Internet Traffic Filtering (AITF) as a filter-based (datagram) mechanism [103]
- A.1.4.f StopIt [101]
<table>
<thead>
<tr>
<th>Features</th>
<th>Disadvantages</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-based</td>
<td>Sources are distributed among different domains; hence, it is difficult for each of the sources to detect and filter attack flows accurately. Difficult to differentiate legitimate and DDoS attack traffic at the sources, since the volume of the traffic is not big enough. Low motivation for deployment; since, it is unclear who would pay the expenses associated with these services.</td>
<td>Aims to detect and respond (i.e., filter) to the attack traffic at the source and before it wastes lots of resources.</td>
</tr>
<tr>
<td>Destination-based</td>
<td>Detection and response are deployed at the destination hosts (i.e., victims).</td>
<td>They cannot accurately detect and respond to the attack before it reaches the victims and wastes resources on the paths to the victim.</td>
</tr>
<tr>
<td>Network-based</td>
<td>Detection and response are deployed at the intermediate networks (i.e., routers).</td>
<td>High storage and processing overhead at the routers. Attack detection is difficult because of the lack of availability of sufficient aggregated traffic destined for the victims.</td>
</tr>
<tr>
<td>Hybrid/Distributed</td>
<td>Detection and response are deployed at various locations: detection usually occurs at destinations &amp; intermediate networks, and response usually occurs at the sources &amp; upstream routers near the sources. There is a cooperation among various defense components.</td>
<td>Complexity and overhead because of the cooperation and communication among distributed components scattered all over the Internet. Lack of incentives for the service providers to cooperate/collaborate. Need trusted communication among various distributed components in order to cooperate/collaborate.</td>
</tr>
</tbody>
</table>
A.2. Defense mechanisms against application-level DDoS flooding attacks

• Most of these mechanisms closely observe the server and model its clients’ behavior so that they can detect any anomalies and drop or rate limit the malicious requests. Some of these major mechanisms against application-level DDoS flooding attacks are as follows:
A.2.1. Destination-based (server-side) mechanisms

• A.2.1.a Defense against Reflection-Amplification attacks:[106], [108]
  aim is to detect malicious traffic from different protocols such as DNS and SIP by employing various mechanisms such as machine learning techniques

• A.2.1.b DDoS-Shield [3], [109]
  uses statistical methods to detect characteristics of HTTP sessions and employs rate-limiting as the primary defense mechanism

• Cons
  • However, it is not clear if a legitimate session is given another chance to receive the service if it is dropped by the DDoS-resilient scheduler.

• A.2.1.c Anomaly detector based on hidden semi-Markov model [110]
  They use the entropy of document popularity fitting to the model to detect the potential application-layer DDoS attacks

• Cons
  • high complexity of its algorithm

• A.2.1.d DAT (Defense Against Tilt DDoS attacks) [111]
  monitors users' features (e.g., instant traffic volume, session behavior, etc.) throughout a connection session to determine whether users are malicious or not
A.2.2. Hybrid (Distributed) mechanisms

This mechanism tries to decrease the number of malicious requests is to encourage all the clients to automatically send higher volumes of traffic. The reasoning behind this approach is that attackers are already using most of their upload bandwidth so cannot react to the encouragement.

- A.2.2.a Speak-up [112]
  - tries to decrease the number of malicious requests is to encourage all the clients to automatically send higher volumes of traffic. The reasoning behind this approach is that attackers are already using most of their upload bandwidth so cannot react to the encouragement.
  - Speak-up is applicable mainly against session flooding attacks and it is not applicable in case of request flooding attacks and asymmetric attacks.

- A.2.2.b DOW (Defense and Offense Wall) [113]
  - employs the encouragement method which is presented in the Speak-up mechanism with an anomaly detection method based on K-means clustering to detect and filter session flooding attacks, request flooding attacks, and asymmetric attacks.
A.2.2. Hybrid (Distributed) mechanisms

• A.2.2.c Differentiate DDoS flooding bots from human [114],[115]
  • Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA [116])
• Cons
  • Annoying for the users introduce more delay for legitimate users.
  • disables web crawlers’s access to the web sites
A.2.2. Hybrid (Distributed) mechanisms

- **A.2.2.d** Admission control and congestion control [117]
  - Admission control works based on port hiding that renders the online service invisible to unauthorised clients by hiding the port number on which the service accepts incoming requests.

- **A.2.2.e** TMH (Trust Management Helmet) [118]
  - The key idea is that servers should give priority to protecting the connectivity of good users during the application layer DDoS attacks instead of identifying all the attack requests. In doing so, each user is assigned a license, which is cryptographically secured against forgery or replay attacks, and a trust value, which is based on users’ history.

- **A.2.2.f** Hybrid detection based on trust and information theory based metrics [119]
  - This mechanism initially filters suspicious flows based on the trust value scored by the client. Then an entropy, which is the information based metric, is applied for final filtering of suspicious flows.
B. Classification by the point in time (i.e., between the start and end of a DDoS attack)

- Defending against DDoS flooding attacks should be initiated at earlier points in time and as near as possible to the sources of the attacks.

- Detecting (defending) at either intermediate networks or sources of the attacks have two main advantages:
  1. the detection is more concealed since it is deployed in a separate location from attack target and
  2. the detection mechanism is less vulnerable to DDoS attacks. However, accurate detection is not easy or it is even impossible to achieve since there is not enough evidence to detect attacks at these stages (e.g., source and upstream routers).
B. Classification by the point in time (i.e., between the start and end of a DDoS attack)

- Two fundamental challenges to detect DDoS flooding attacks in time and as near as possible to the attack sources are:
  
  - (1) the lack of a wide deployment of DDoS defense mechanisms at different points of the Internet, and
  
  - (2) the lack of collaboration and cooperation among distributed deployed defense mechanisms in order to increase the detection accuracy, decrease unnecessary redundant tasks (because of the lack of coordination),
B.1. Before the attack (attack prevention)

- B.1.1. System & Protocol security mechanisms to increase the overall security of the systems
  - Removing bugs, updating installed protocols, installing software patches, removing unused software
- B.1.2. Fail-safe protection
  - Possible anticipations in case something goes wrong (e.g., replication of services and applications in diverse locations in case DDoS attack occurs successfully, business continuity and disaster management plans, etc.)
- B.1.3. Resource allocation & accounting
- B.1.4. Reconfiguration mechanisms
  - These mechanisms alter the topology of either the victim network to add more resources to tolerate the DDoS attack
- B.1.5. Installing firewalls and improved Intrusion Detection & Prevention Systems (IDPSs):
- B.1.6. Employing local filters
  - (e.g., Ingress/Egress [55], History-based IP filtering [73], hop-count filtering [74], Pi [76], route-based packet filtering [79], [80], etc.) and globally coordinated filters (e.g., ACC [89], Pushback [89], [90], AD and parallel-AD [91], TRACK [92], etc.)
B.1. Before the attack (attack prevention)

• B.1.7. Load balancing [120] and Flow control
• B.1.8. Server-side specific security considerations
  • Such security mechanisms or policies can protect servers from various attacks
    • Do not accept connections with abnormally small advertised window sizes.
    • Do not enable persistent connections and HTTP pipelining unless performance really benefits from it.
    • Limit the absolute connection lifetime to some reasonable value.
• B.1.9. Service providers can have strategies
  • Cisco in their IPS 7.0 code upgrade [54]. IPS 7.0 upgrade has global correlation feature that can be configured on every service provider IPS sensors so that they are aware of the network devices with a reputation for malicious activity
B.2. During the attack (attack detection)

• Attack Detection

• (e.g., MIB information analysis [70], D-WARD [58], [59], MULTOPS [60], TOPS [61] [127]– [129], DDoS-Shield [3], [109], DAT [111]. There are many IDPSs that are based on these detection mechanisms. They employ data mining and artificial intelligence techniques for more accurate detection.
B.3. After the attack (attack source identification and response)

• B.3.1. Attack source identification
  • IP traceback mechanism must find out the real source address of the attacker

• B.3.2. Initiating a proper response
  • apply throttling (rate limit) or packet filtering on upstream routers and hosts for the traffic coming from those identified attack flows (e.g., spoofed IP addresses) after identifying the source of the attack. For instance, history-based IP filtering [73], hop-count filtering [74], Pi [76], AD [91], TRACK [92], and Stoplt [101], [105] employ packet filtering upon detection of DDoS attacks and ACC [89], Pushback [89], [90], PAD [91], AITF [103], and DEFCOM [93] employ throttling upon detection of DDoS attacks. Other mechanisms specially in the case of application-level DDoS flooding attacks employ some encouragement models in which servers ask the legitimate clients to increase their session rates to crowd out the malicious clients (e.g., Speak-up [112], and DOW [113]).
5. DDoS Defence: Performance Measurement Metrics

<table>
<thead>
<tr>
<th>DDoS defense decision</th>
<th>Desirable decision of the DDoS defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative</td>
<td>Positive</td>
</tr>
<tr>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>C</td>
<td>D</td>
</tr>
</tbody>
</table>
5. DDos Defence: Performance Measurement Metrics

• 1. Defence Strength
  • Accuracy \( \frac{(A+D)}{(A+B+C+D)} \)
  • Sensitivity \( \frac{D}{(B+D)} \)
  • Specificity \( \frac{A}{(A+C)} \)
  • Precision \( \frac{D}{(C+D)} \)
  • Reliability \( \frac{C}{(C+D)} \)
  • False Negative Rate \( \frac{B}{(A+B)} \)
5. DDoS Defence: Performance Measurement Metrics

- 2. Compromise-ability
  - Delay in detection/response
  - System performance degradation
  - Passive, reactive or proactive
  - Holistic defense
  - Implementation complexity
  - Usability
  - Deployment location
  - Scalability
### TABLE III
Qualitative Comparison of Defense Mechanisms Against Network/Transport-Level DDoS Flooding Attacks Based on Their Deployment Location

<table>
<thead>
<tr>
<th></th>
<th>Defense strength (Accuracy)</th>
<th>Scalability</th>
<th>System performance</th>
<th>Implementation complexity</th>
<th>Holistic defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>Source-based</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Destination-based</td>
<td>High</td>
<td>Low</td>
<td>Good</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Network-based</td>
<td>Low</td>
<td>Medium</td>
<td>Moderate</td>
<td>Medium</td>
</tr>
<tr>
<td>Distributed</td>
<td>Hybrid (Distributed)</td>
<td>Medium</td>
<td>Medium-high</td>
<td>Poor-moderate</td>
<td>Medium-high</td>
</tr>
</tbody>
</table>

### TABLE IV
Qualitative Comparison of Defense Mechanisms Against Application-Level DDoS Flooding Attacks Based on Their Deployment Location

<table>
<thead>
<tr>
<th></th>
<th>Defense strength (Accuracy)</th>
<th>Scalability</th>
<th>System performance</th>
<th>Implementation complexity</th>
<th>Holistic defense</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Destination-based (server-side)</td>
<td>High</td>
<td>Low</td>
<td>Moderate-good</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Hybrid (Distributed)</td>
<td>Medium</td>
<td>Medium</td>
<td>Moderate</td>
<td>Medium-high</td>
</tr>
</tbody>
</table>
Ideal comprehensive DDoS defense mechanism

- must have specific features to combat DDoS flooding attacks in real-time and as close as possible to the attack sources. These features are as follows:
  - 1. More nodes in the Internet should be involved in preventing, detecting, and responding to DDoS flooding attacks (i.e., Hybrid (Distributed) defense).
  - 2. There should be collaboration and cooperation among the key defensive points within and between service providers in the Internet.
  - 3. More reliable mechanisms are required to authenticate the sources of the Internet traffic so that malicious users could be identified and held accountable for their activities (i.e., Anti-spoofing mechanisms).
  - 4. Trusted communication mechanisms for cooperation and collaboration among various distributed components are needed.
References