Deployable Overlay Network for Defense against distributed SYN flood attacks

Yuichi Ohsita\textsuperscript{(1)} Shingo Ata\textsuperscript{(2)} Masayuki Murata\textsuperscript{(1)}

\textsuperscript{(1)}Osaka University
\textsuperscript{(2)}Osaka City University
What is DDoS?

- An attacker hacks remote hosts and installs attack tools
- The hosts attack the same server at the same time
What is DDoS?

- The number of attacks is increasing
- The number of attack nodes is very large and attack nodes are highly distributed
- The most are SYN flood Attacks
  - Because SYN flood can put servers into denial-of-service state easily
  - More than 90% of DoS Attacks
What is SYN flood?

- **Normal 3-way handshake**

  - The in-progress connection requests are held in the backlog-queue
  - The queue length is limited

Client PC

```
SYN
ACK
SYN/ACK
```

Server

```
backlog-queue
```
What is SYN flood?

Mechanism of SYN flood

- The backlog queue is filled by malicious requests.
- Legitimate new connection requests are rejected.

No ACK packets are replied.
The connection requests remain in the backlog-queue till timeout.
Traditional firewall against SYN flood

We need distributed defense mechanism

Single-point defense lacks scalability

Relaying only legitimate packets

Attackers can increase attack rate by increasing attack nodes
Our goal

- Problems of traditional defenses
  - Lack in scalability
    - Unable to protect legitimate packets in the case of a high-rate and highly distributed attack

- Our goal
  - Defense mechanism having enough scalability
    - Distributed defense
      - Attack packets are blocked at distributed places
    - Deployment in a phased manner
      - Using a overlay network mechanism
Overview of our method

This method has enough scalability because defense nodes are distributed.

Defense nodes construct an overlay network.
Defense nodes communicate with each other.

Legitimate packets are forwarded via the overlay network.

Block attack packets.
Operations of Defense nodes

- Attack detection mode
  - Detecting attacks

- Defense mode
  - Alerting all defense nodes
  - Delegation of SYN/ACK packets
  - Relay of legitimate packets
  - Ending the defense mode
Detecting attacks

- Attacks are detected at server-side
  - Attacker-side
    - Few attack packets ➔ difficult
  - Server-side
    - Many attack packets ➔ easy

- Method to detect attacks
  - Detection by comparing the SYN arrival rates with normal distributions[1]
    - Able to detect attacks fast regardless of time variation of traffic.

Alerting all defense nodes

Defense nodes move into defense mode

Sending the alert message (including victim’s IP address)

Detecting attacks

Attacker

Client

Victim

Detection mode

Defence mode

ICCCN 2005

2005/10/18
Delegation of SYN/ACK packets

- Legitimate packets are identified by delegation of SYN/ACK packets
  - Attacker cannot respond to SYN/ACK packets

Connections under 3-way handshake must be held by defense node

Connection to the server is established only when ACK of SYN/ACK is received
Holding connection under 3-way handshake

- We use the same approach as the SYN cache
  - The hash value is computed from the source and destination IP addresses and the source and destination port.
  - Entries having the same hash value are kept on a forward linked list.
  - The length of the list is limited. When the list is full, the oldest entry is removed.
Relay of legitimate packets

- Legitimate packets are forwarded via overlay network
  - By using overlay network, we can distinguish legitimate flows from others

A flow is identified as legitimate traffic

The connection to the server is established via the overlay network

Each defense node connects two TCP flows
When to end defense mode

- When a defense node should end defense mode?
  - The defense node receives no attack packets
    - The number of connection requests which time out or dropped is under a threshold
      - Ideally the threshold is 0, but some legitimate request may time out
  - Finishing defense mode does not cause high load on other nodes
    - No attack packets exist on intermediate defense nodes on the way to the victim node.
Ending the defense mode

- Client -> Victim
  - Sending message indicating the end of attack

- Client
  - Detecting the end of attack
  - Ending the defense mode if the attack ends

- Client
  - Detecting the end of attack
  - Ending the defense mode

ICCCN 2005
Evaluation of effectiveness of attacker-side defense

- We evaluate the effectiveness of attacker-side defense by simulation
  - We assume that single-attacker attacks.
  - We compare attacker-side defense with victim-side defense

**Environment supposed in our simulation**

- Client
- Attacker
- Internet
- Victim
Effectiveness of attacker-side defense

- We compare the probability of dropping a legitimate SYN packet.
- The attacker-side defense can protect legitimate packets much better than the victim-side defense.
  - Because of small RTT, the average holding time for each connection request on the SYN cache is short.
Evaluation of effectiveness of distributed defense

- We evaluate the effectiveness of distributed defense by simulation
  - Each attacker generates 200,000 SYN packets a second
  - We compare probability of dropping a legitimate SYN packets for client A

![Diagram of attacker and defense nodes](image)
Probability of dropping SYN packets

- In the case of single-point defense, probability of dropping a SYN packet remains high.
- With our method, probability of dropping a packets becomes very low soon after the attack started.
  - Our method quickly detects attacks and distinguish legitimate packets from attack packets.
Conclusion and future work

Conclusion

- We have proposed a distributed defense mechanism against distributed SYN flood attacks.
- Simulation results show that our method has both effectiveness of attacker-side defense and effectiveness of distributed defense.

Future work

- Identification of attack packets at the points where the routes of packets may vary.
Thank you