draft-cui-savnet-anti-ddos-02 IETF 118 Secdispatch WG

SAV-based Anti-DDoS Architecture (SAV-D)

Yong Cui, Jianping Wu, Lei Zhang, **Linzhe Li**

Tsinghua University, Zhongguancun Laboratory

Nov 6, 2023

Outline

- Problem Statement
- SAV-D Architecture and Workflow
- SAV-D Transmission
- Advantages

Problem Statement

- ➢ Spoofing source addresses is one of the common technological means used in DDoS attacks.
- ➢ Detection and defense of **Target Side**
  - Detection □ Diversion □ Cleaning □ Reinjection
  - Weaknesses □ Limitations on defense capabilities
- ➢ Detection and defense of **Middleware Networks**
  - NetFlow-based sampling analysis
  - Weaknesses □ Accuracy limitation,

    Timeliness limitation,

    Sampling continuity.

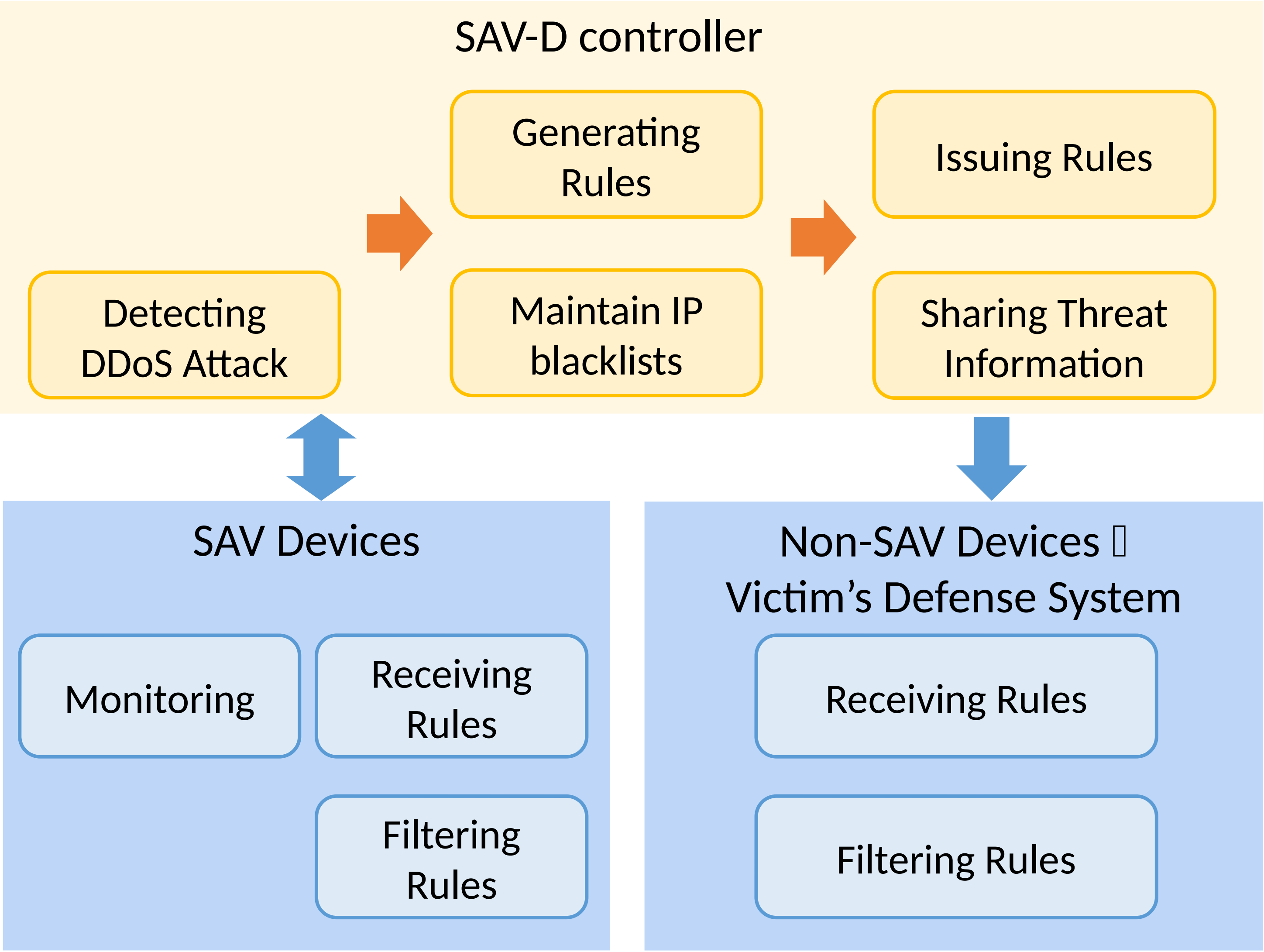
- SAV: a source address validation technique that can detect packets with spoofed source addresses, discovering and blocking attacks at the source.

Deployment of SAV devices is necessarily a lengthy process.

Problem Statement

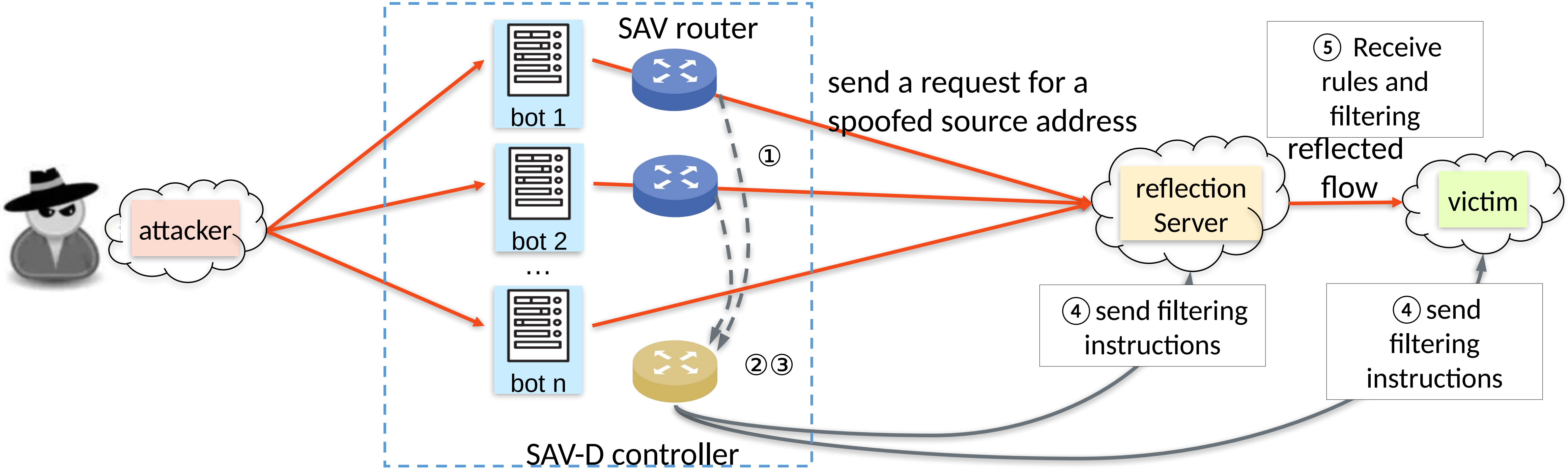
- Status quo: **direct drop** after detecting spoofed source address packets
- Disadvantages of direct drop:
  - In large-scale attacks, bots are widely distributed, and the effect of a few SAV deployments is limited.
  - Continuously dropping the packets, there is a possibility that the bots will migrate to a non-SAV deployment area.
- During **incremental SAV deployment**, **information uploading** should be prioritized instead of direct dropping.
  - By spoofing source address message information (IP, port number, TCP identifier, geographic location, etc.), it is possible to **detect a variety of reflection attacks and direct attacks**
  - Able to detect potential threats **more accurately and earlier**, and respond to large-scale attacks before forming

SAV-D Architecture



- SAV devices identify and report forged source address packets.
- Based on the collected information, the SAV-D controller identifies security intelligence.
- The security intelligence can be distributed through the SAV-D controller, benefiting the entire network.

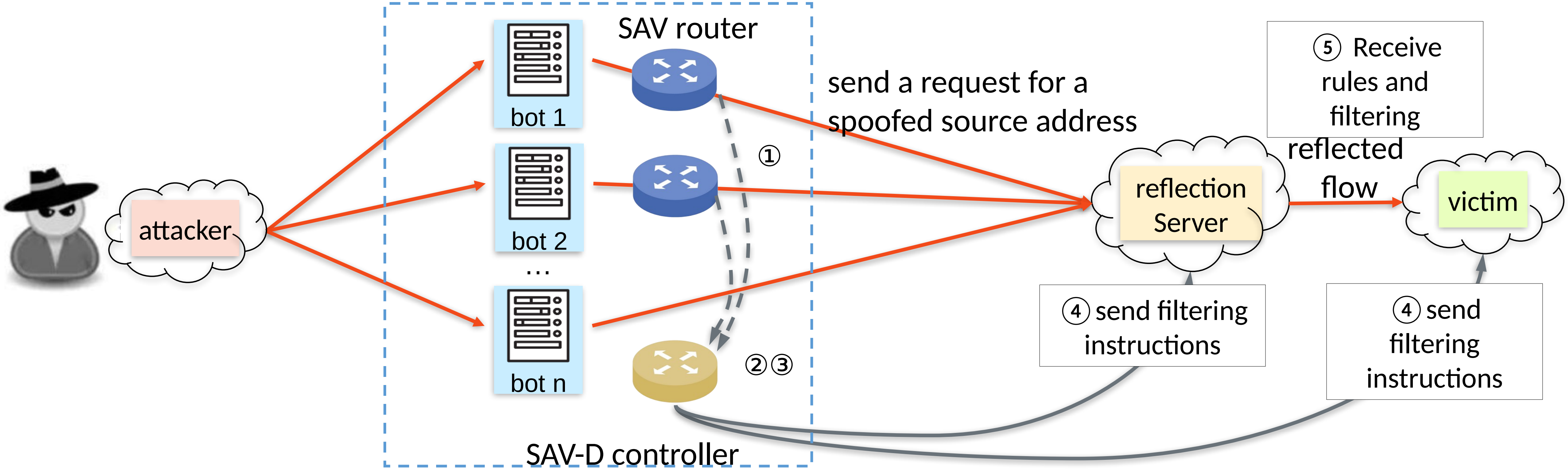
SAV-D Workflow


SAV router
⑤ Receive rules and filtering
send a request for a spoofed source address
①
reflected flow
attacker
bot 1
bot 2
…
bot n
reflection Server
victim
②③
④ send filtering instructions
④ send filtering instructions
SAV-D controller

1. The SAV router records the message information of the spoofed source address, and then reports it to the SAV-D controller.

2. The SAV-D controller aggregates and analyzes the information collected from SAV devices, detects whether a DDoS attack occurred.

SAV-D Workflow



attacker
bot 1
bot 2
…
bot n
SAV router
①
②③
SAV-D controller
send a request for a spoofed source address
⑤ Receive rules and filtering
reflected flow
reflection Server
victim
④ send filtering instructions
④ send filtering instructions

3. Based on attack detection results , the SAV-D controller generates specific filtering rules.
4. The SAV-D controller sends filtering rules to the SAV routers or other non-SAV devices.
5. Network devices receive rules and execute filtering.

Advantages

- Achieve more accurate detection of DDoS attacks through comprehensive analysis.
- In the current scenario with low SAV deployment rates, fully utilizing forged source address packets to mine security intelligence can benefit the entire network.

Next, we will implement SAV-D to show its effectiveness.

Thanks!

Q&A