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

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

Tsinghua University, Zhongguancun Laboratory

Nov 6, 2023

Outline

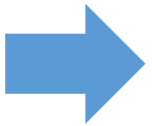
- Problem Statement
- SAV-D Architecture and Workflow
- SAV-D Transmission
- Advantages

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.

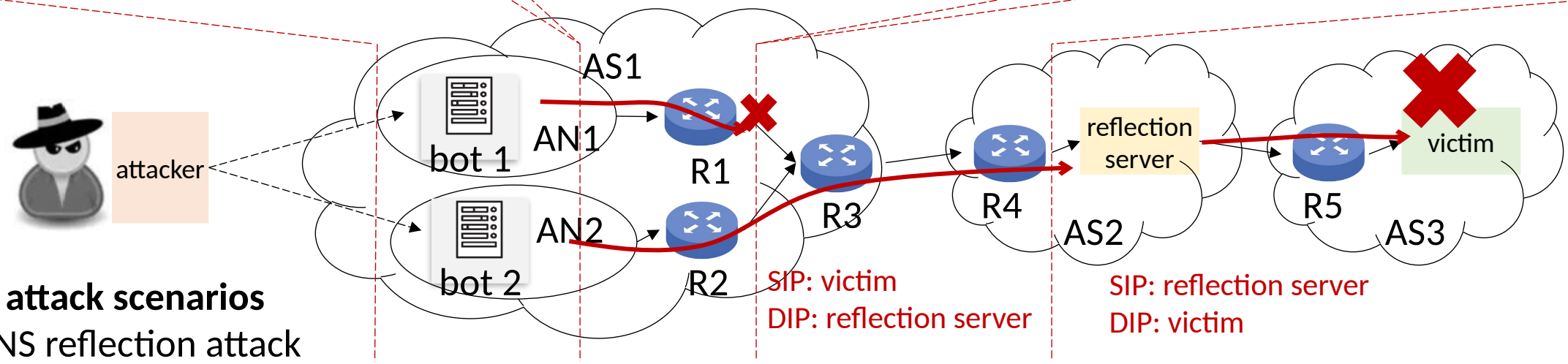
Deployment of SAV devices is necessarily a lengthy process.

Problem Statement

Access Network Deployment
Suitable for host granularity defense, but difficult to require all access networks to deploy SAV.

Intra-domain Deployment
IP prefix granularity defense, difficult to defend source address spoofing within the same address prefix.

Inter-domain Deployment
AS address segment granularity defense, difficult to defend source address spoofing within the same AS.



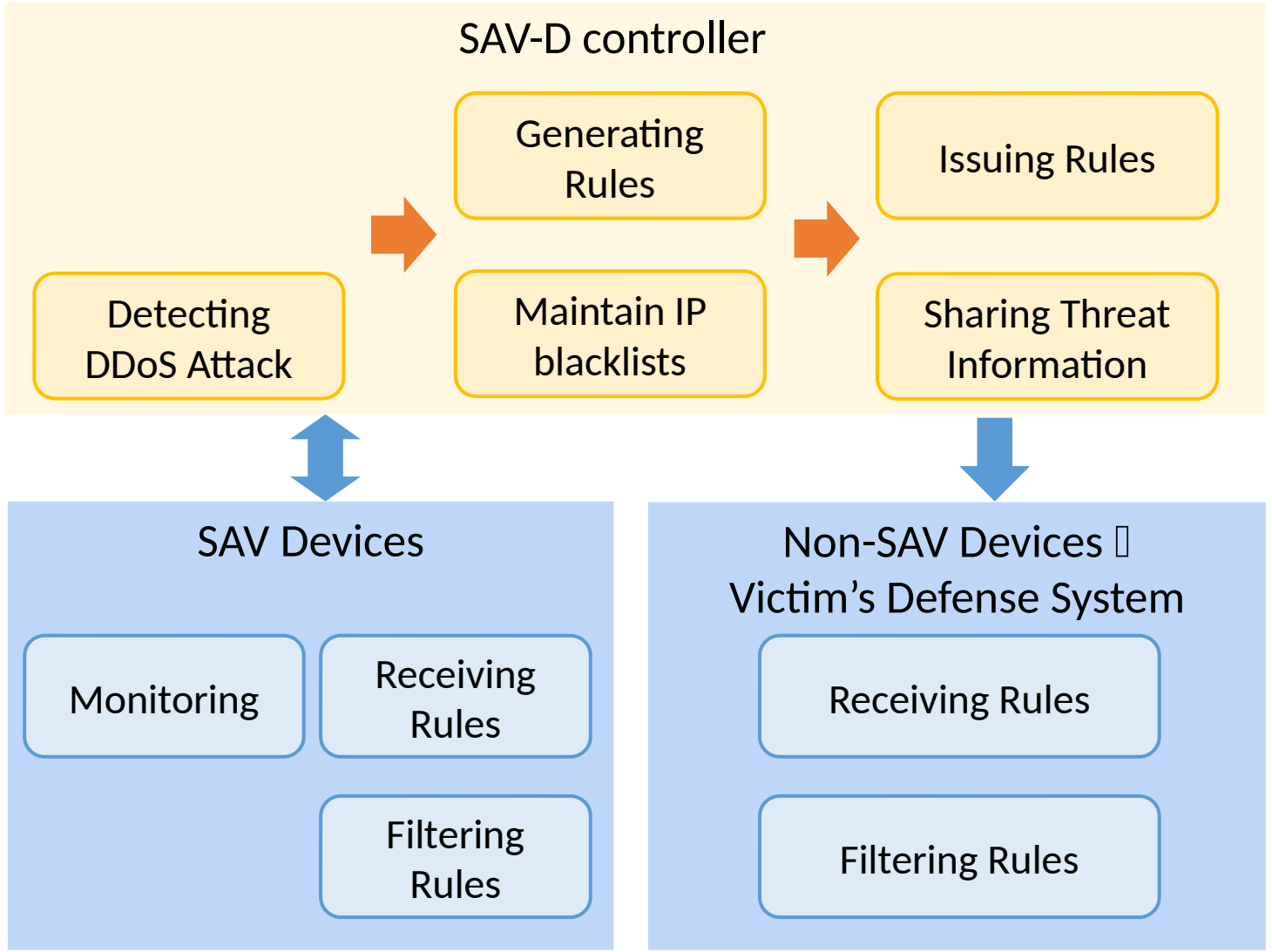
reflection attack scenarios
Such as DNS reflection attack

- **Need a certain scale of SAV deployment to achieve effective DDoS defense.**
- **When SAV deployment scales are limited, attacks still exist in non-deployed areas.**

Problem Statement

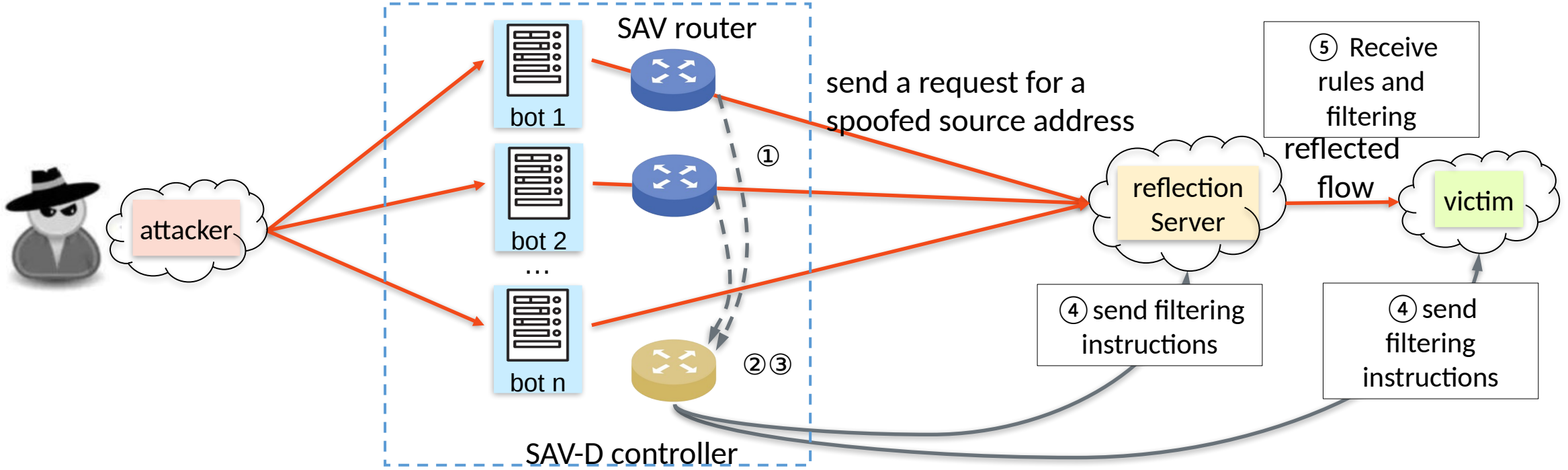
- Status quo: **direct drop** after detecting spoofed source address packets
- Disadvantages of direct drop:
  - In large-scale attacks, bots are widely distributed, and the effect of a few SAV deployments is limited.
  - Continuously dropping the packets, there is a possibility that the bots will migrate to a non-SAV deployment area.
- The core of SAV is the correspondence between binding anchors and IPs, which can be used to perform optional actions after detecting spoofed source address packets.
- 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



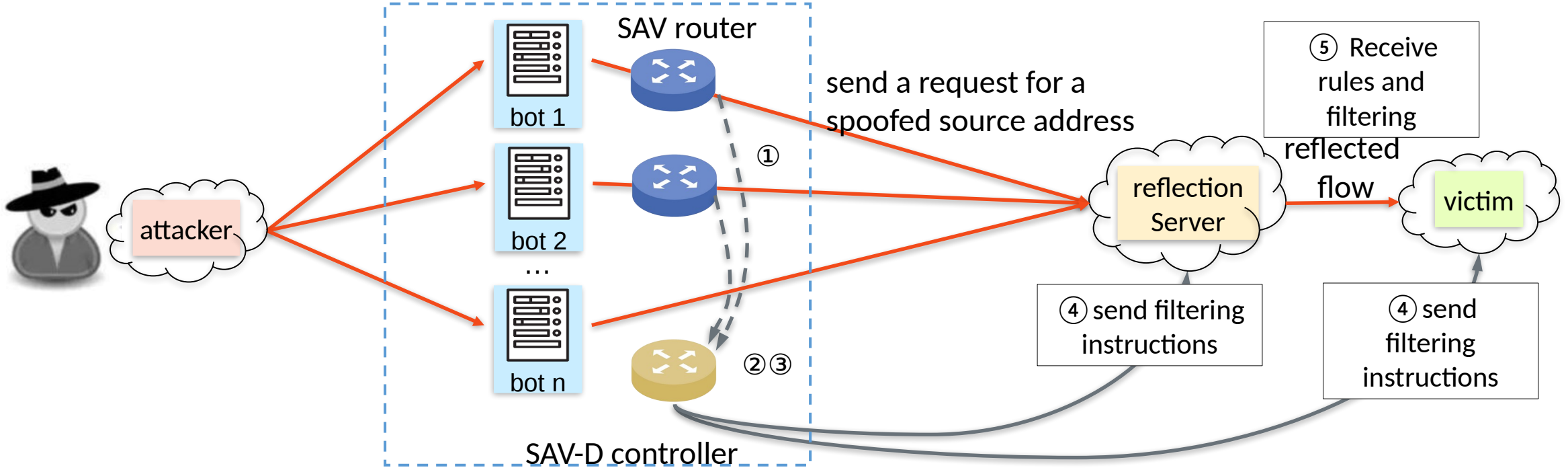
- SAV devices identify and report forged source address packets.
- Based on the collected information, the SAV-D controller identifies security intelligence.
- The security intelligence can be distributed through the SAV-D controller, benefiting the entire network.

SAV-D Workflow



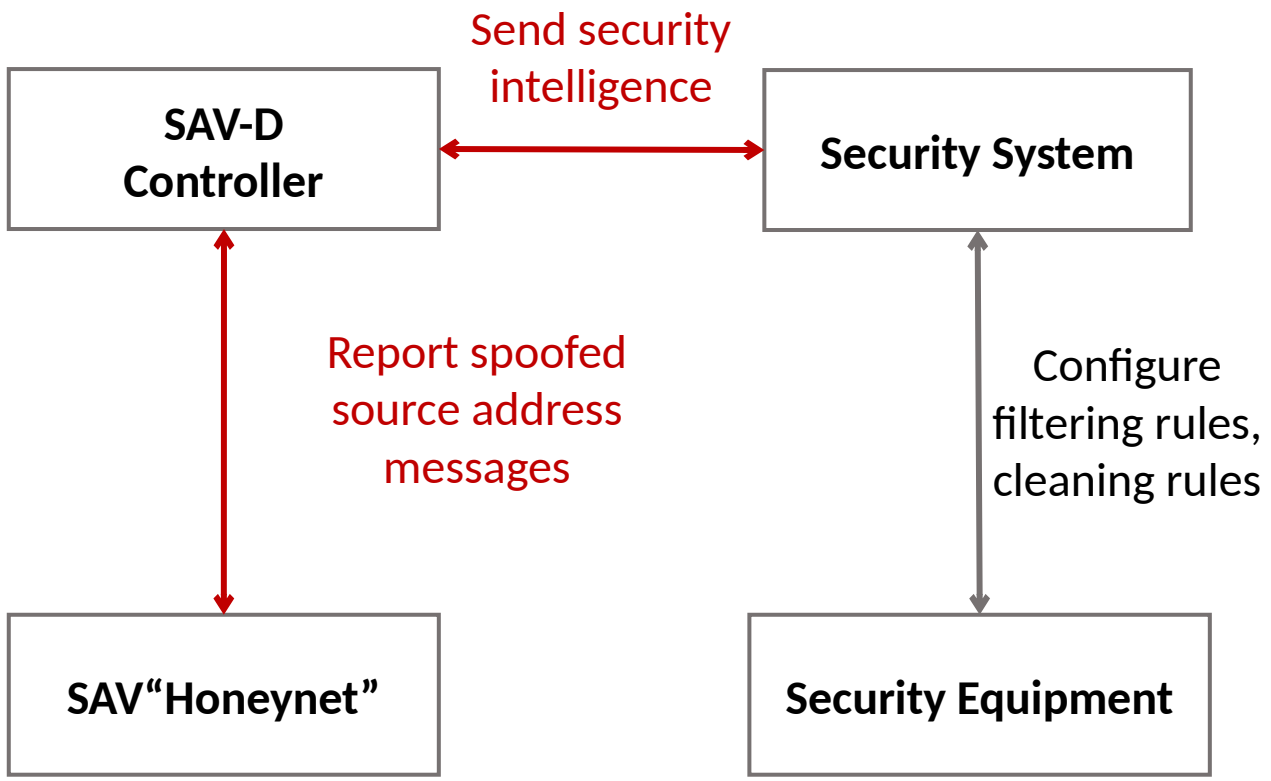
1. The SAV router records the message information of the spoofed source address, and then reports it to the SAV-D controller.
2. The SAV-D controller aggregates and analyzes the information collected from SAV devices, detects whether a DDoS attack occurred.

SAV-D Workflow



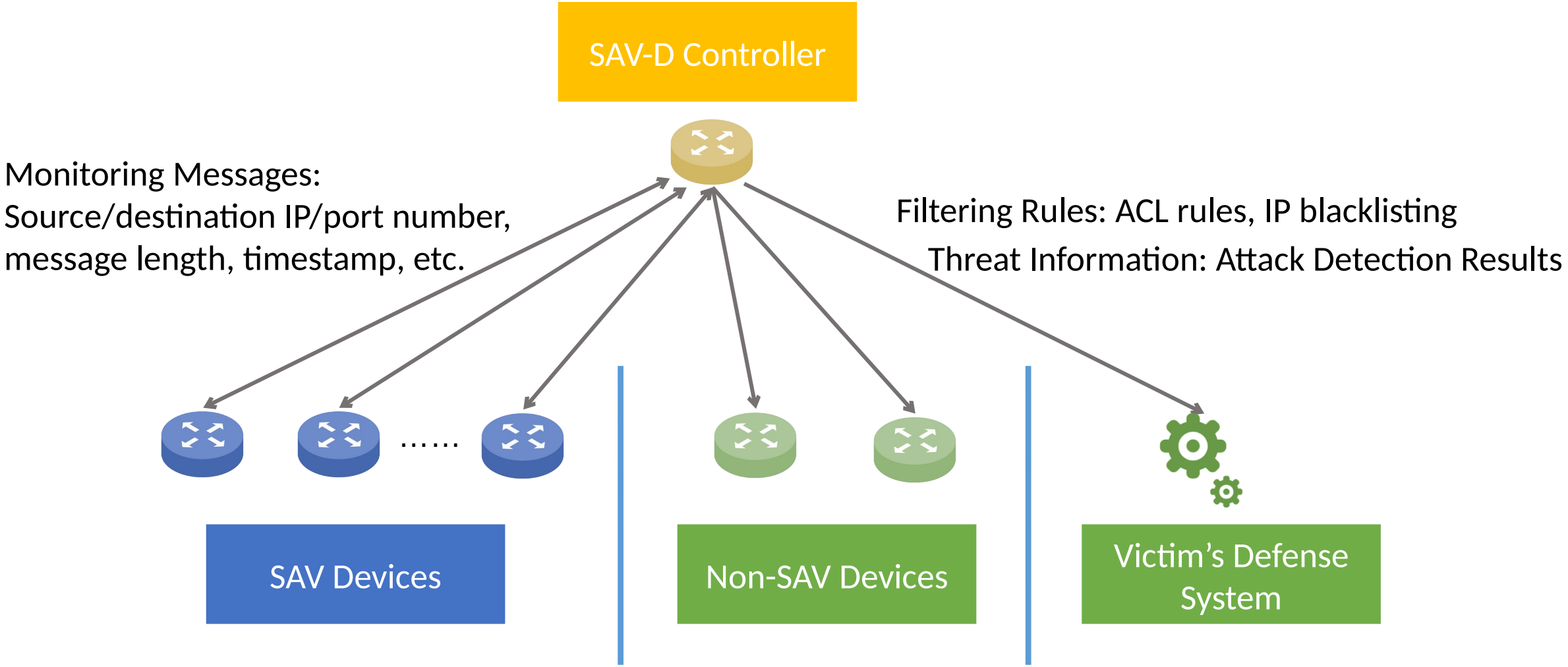
3. Based on attack detection results , the SAV-D controller generates specific filtering rules.
4. The SAV-D controller sends filtering rules to the SAV routers or other non-SAV devices.
5. Network devices receive rules and execute filtering.

SAV-D Information Flow



- SAV routers who do not drop spoofed source IP packets, can be considered as honeypots, and a network deployed with SAV can be seen as a honeynet.
- The SAV-D controller continuously discovers security intelligence, such as zombie network movements and new types of attack behaviors.
- This security intelligence can benefit the security system of the whole network.

SAV-D Transmission



Advantages

- Achieve more accurate detection of DDoS attacks through comprehensive analysis.
- In few SAV devices deployment scenarios, make full use of spoofed source address packets to leverage the advantages of SAV and enhance the revenue of SAV deployers.

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

Thanks!

Q&A