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

Yong Cui, Jianping Wu, **Mingzhe Xing**, Lei Zhang

Tsinghua University, Beijing Zhongguancun Laboratory

Nov 6, 2024

Draft: *SAV-based Anti-DDoS Architecture (https://datatracker.ietf.org/doc/draft-cui-savnet-anti-ddos/)*
Paper: *Linbo Hui et al. "SAV-D: Defending DDoS with Incremental Deployment of SAV," in IEEE Internet Computing*
Code: *https://github.com/sava-anti-ddos/SAV-D*

Outline

- Problem Statement
- SAV-D Architecture and Workflow
- SAV-D Data Transmission
- Preliminary Experiments

Problem Statement

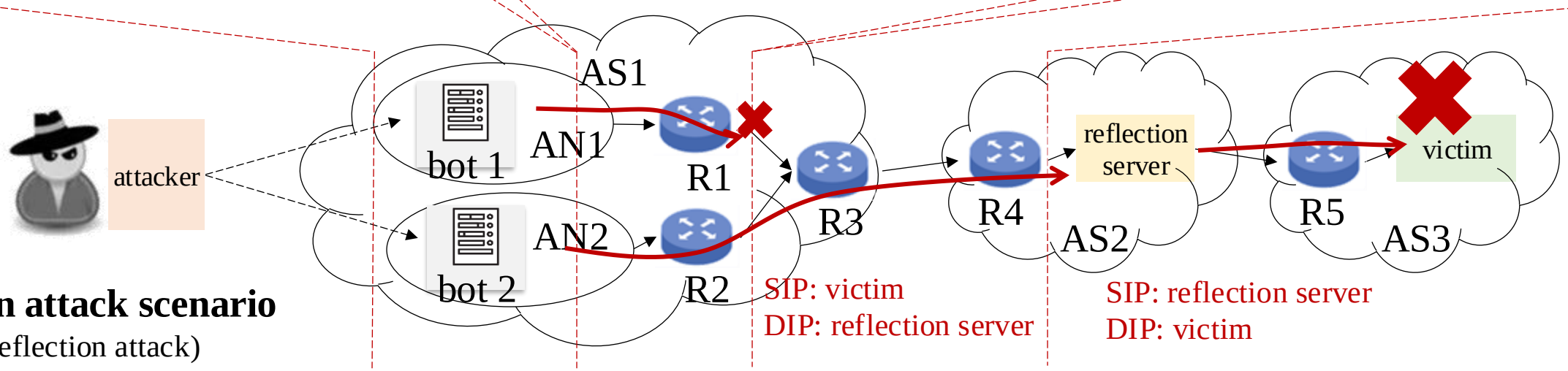
- Spoofing source IP address is a commonly used technique in DDoS attacks
- Detection and Defense at **Target Side**
  - Packet-level detection
  - Limitation: Relatively weak defense capabilities at target side
- Detection and Defense at **Middleware Networks**
  - NetFlow-based sampling analysis
  - Limitation: Low accuracy and timeliness
- Detecting and Defense at **Attack Source Side**
  - Source Address Validation (SAV) detects packets with spoofed source addresses, discover and block attacks at the source side
  - Limitation?

Limitation 1: **Limited Deployment Scale**

Access Network Deployment
Host granularity defense
Difficult to require all access networks to deploy SAV

Intra-domain Deployment
IP prefix granularity defense
Difficult to defend spoofing within the same address prefix

Inter-domain Deployment
AS address granularity defense
Difficult to defend spoofing within the same AS



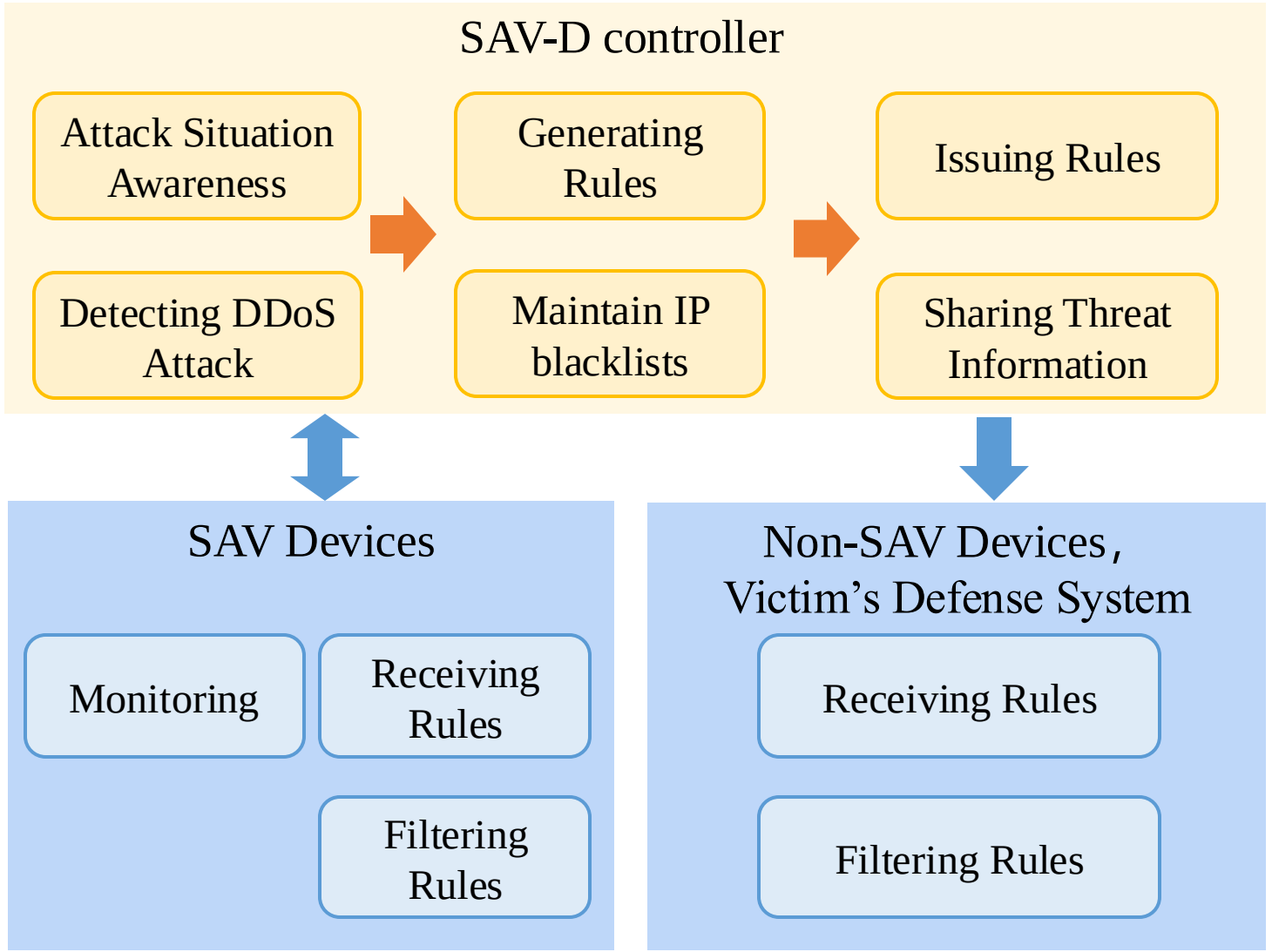
Reflection attack scenario
(e.g., DNS reflection attack)

- **Need a certain scale of SAV deployment to achieve effective DDoS defense**
- **Deployment of SAV devices is necessarily a lengthy process**

Limitation 2: **Lack Collaboration**

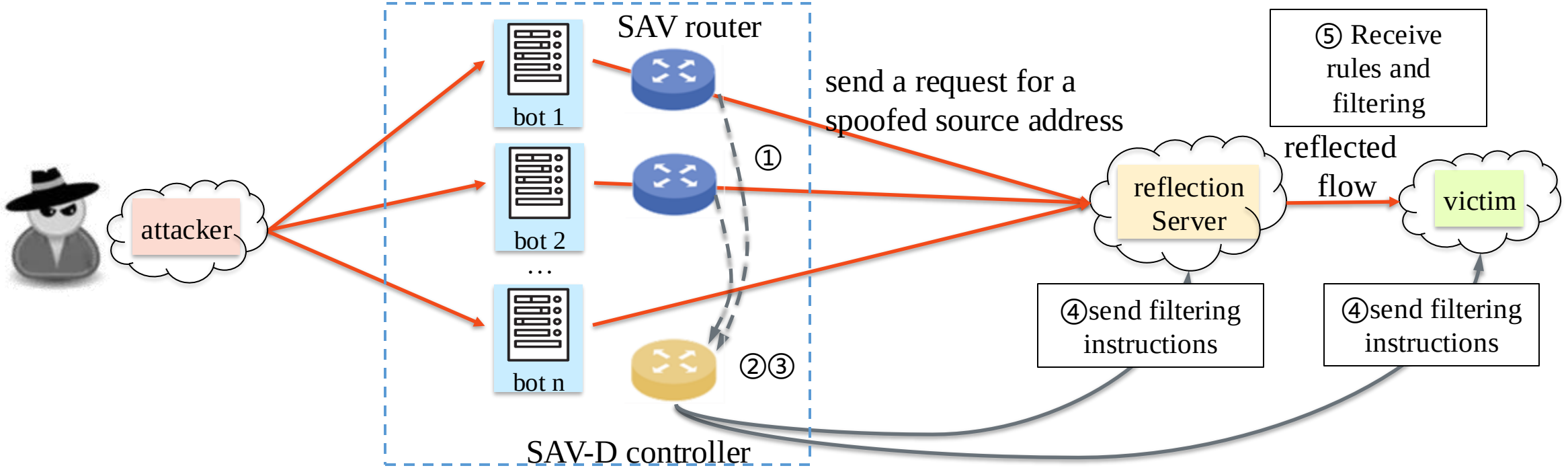
- SAV devices directly drop spoofed packets, without sharing the attack intelligence
- **Insight:** Threat data collaboration among SAV devices
  - Each **SAV device maintains the spoofed packets information** including IP, port number, TCP identifier, geographic location, etc.
  - **Threat information sharing** should be prioritized instead of direct dropping
- **Pros:**
  - **SAV devices can be aware of a variety of reflection attacks and direct attacks**
  - Detect potential threats **more accurately and earlier**, and respond to large-scale attacks before forming
  - Provide a **global view of attack situation**, which can benefit security operation

SAV-D Architecture



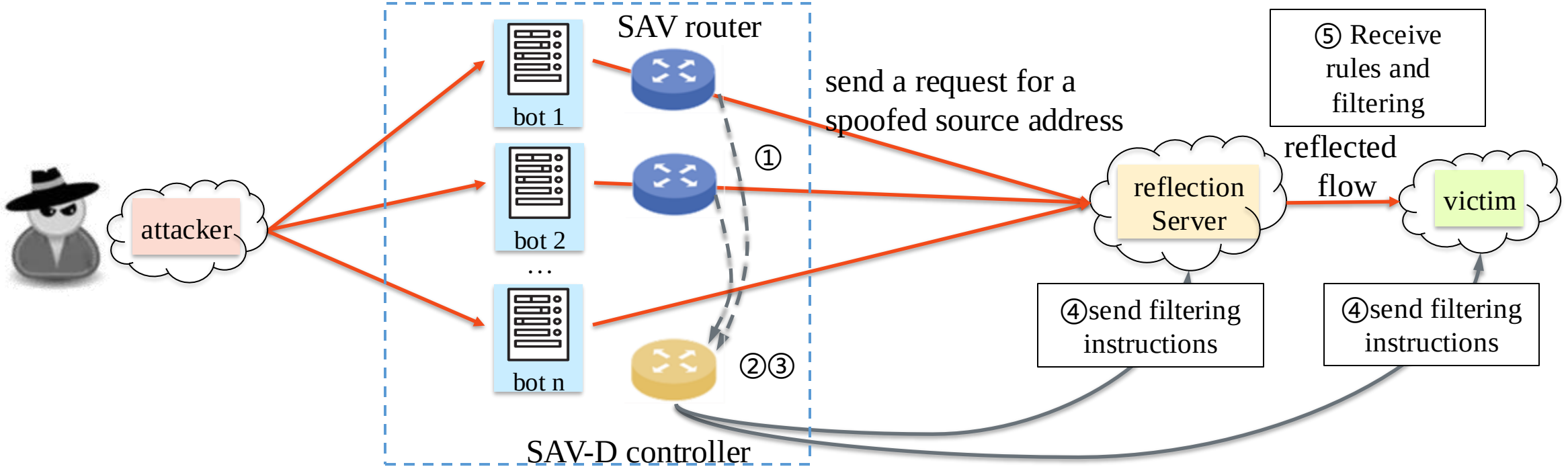
- SAV devices identify and report forged source address packets
- Based on the collected information, the SAV-D controller identifies security intelligence
- The security intelligence can be distributed through the SAV-D controller, benefiting the entire network

SAV-D Workflow



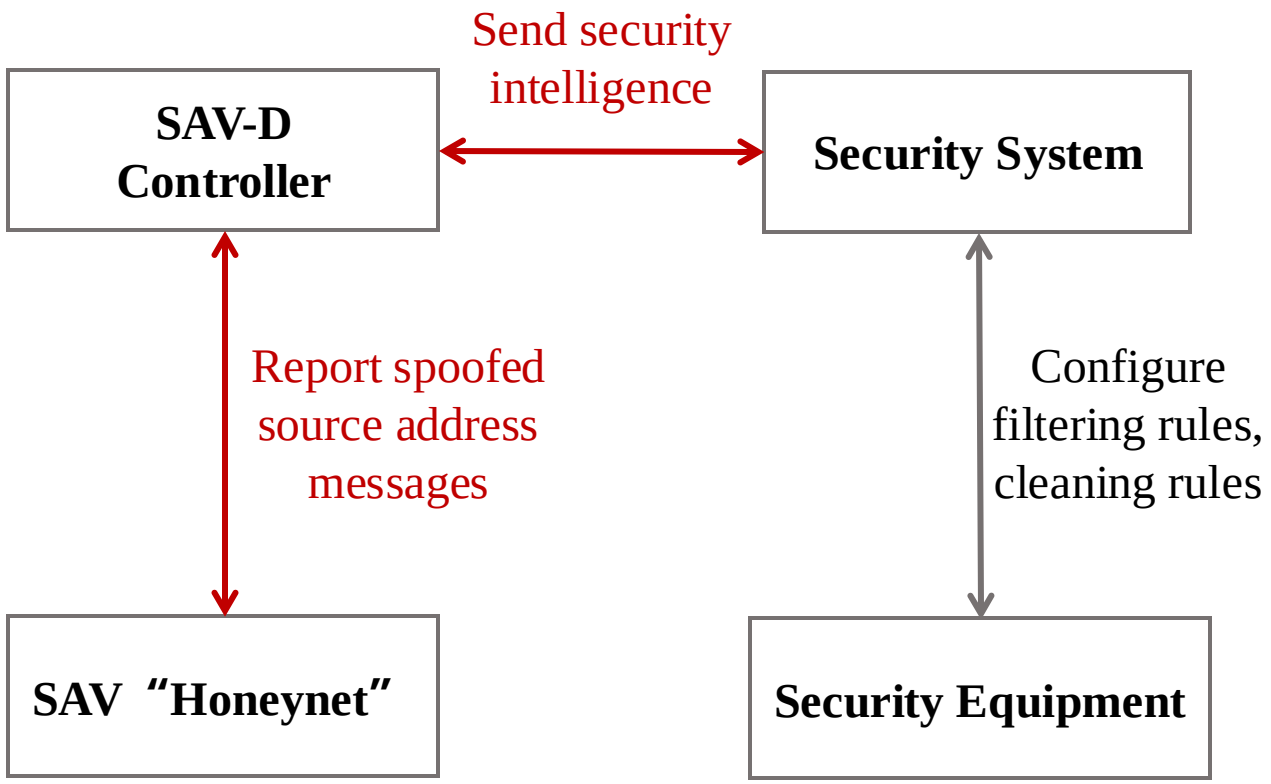
1. The SAV router records the spoofed packets information, and then reports it to the SAV-D controller
2. The SAV-D controller aggregates and analyzes the collected information, and then detects whether a DDoS attack occurred

SAV-D Workflow



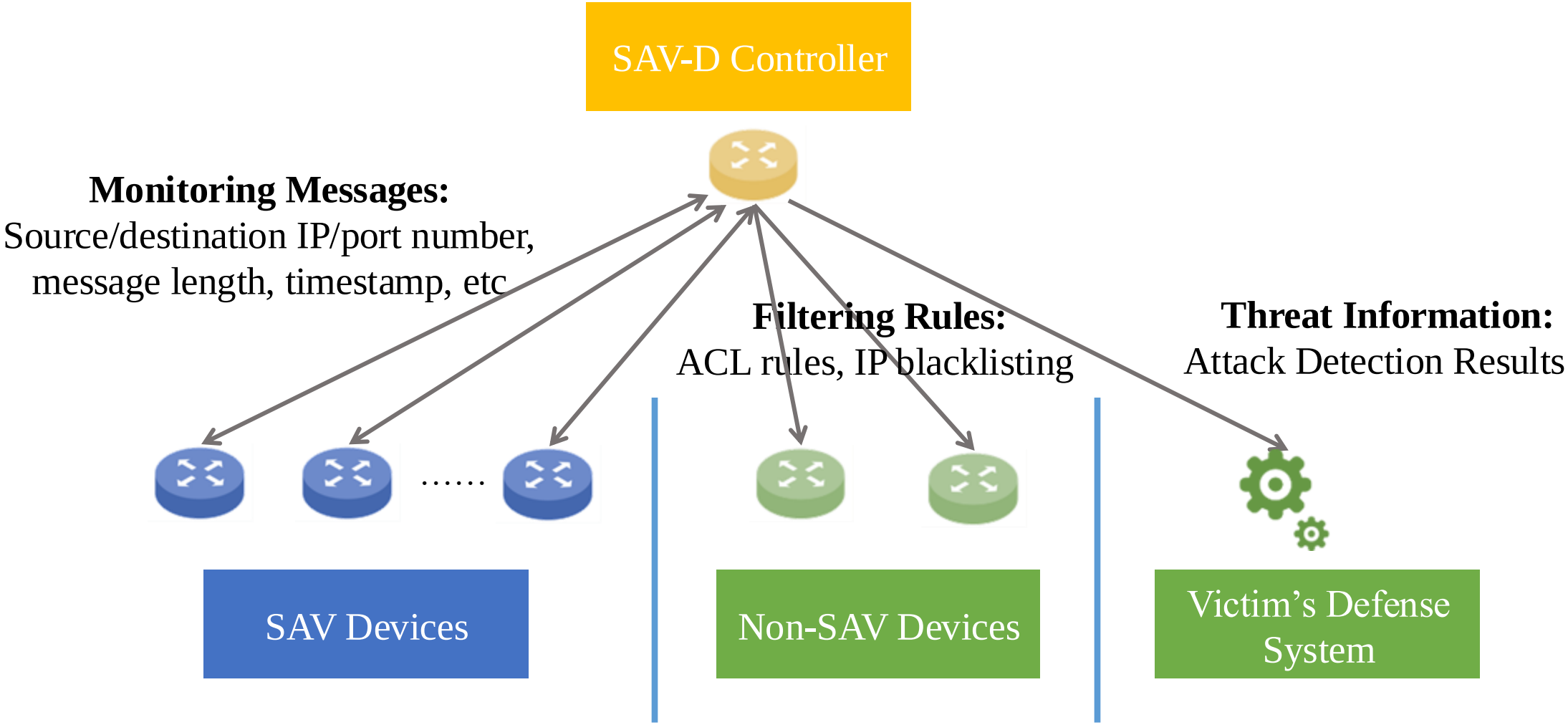
3. Based on attack detection results, the SAV-D controller generates specific filtering rules
4. The SAV-D controller distributes filtering rules to the SAV routers and other non-SAV devices
5. Network devices receive rules and execute filtering

SAV-D Information Flow

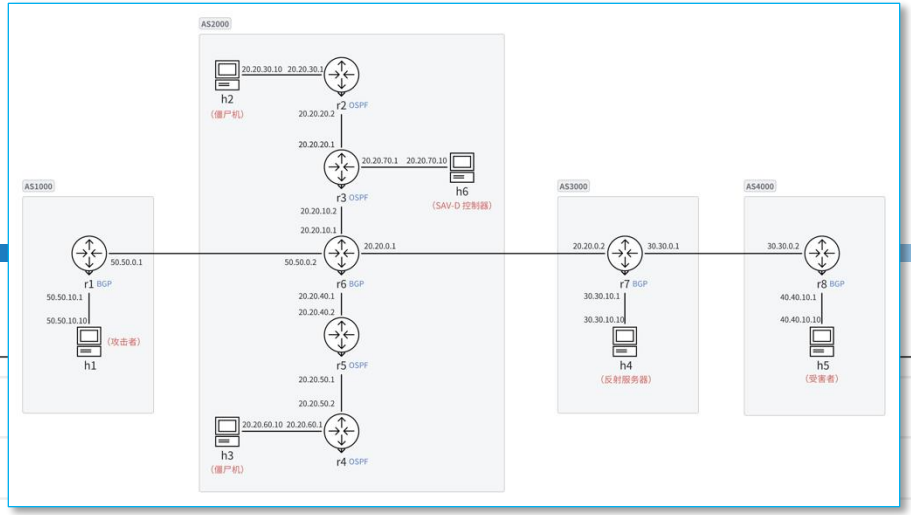


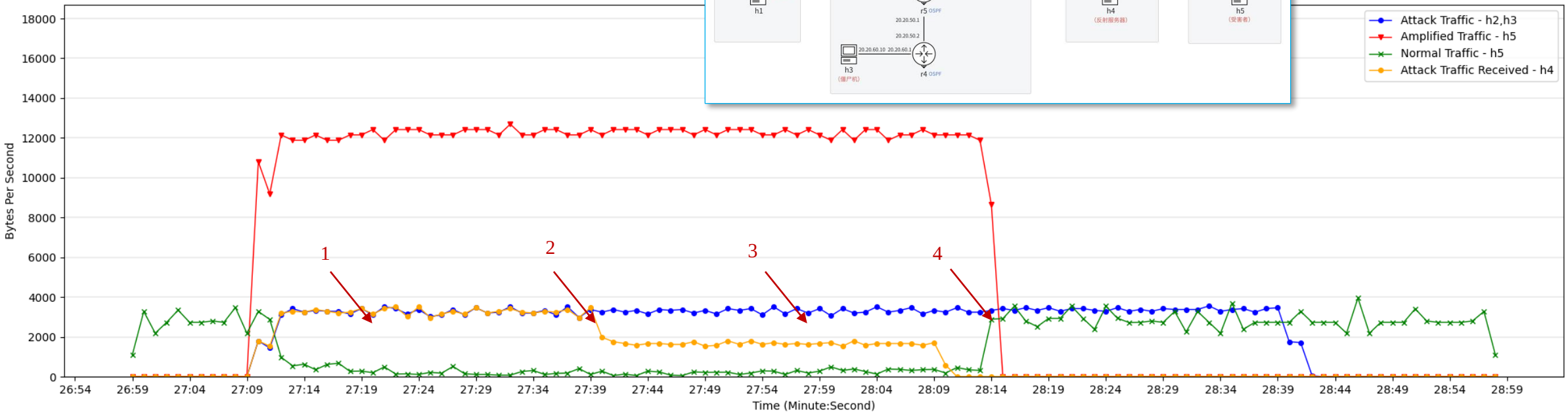
- SAV routers that do not drop spoofed source IP packets can be considered as honeypots, and a network deployed with SAV can be seen as a honeynet
- The SAV-D controller continuously discovers security intelligence, such as zombie network movements and new types of attack behaviors
- This security intelligence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

SAV-D Data Transmission



Experiments

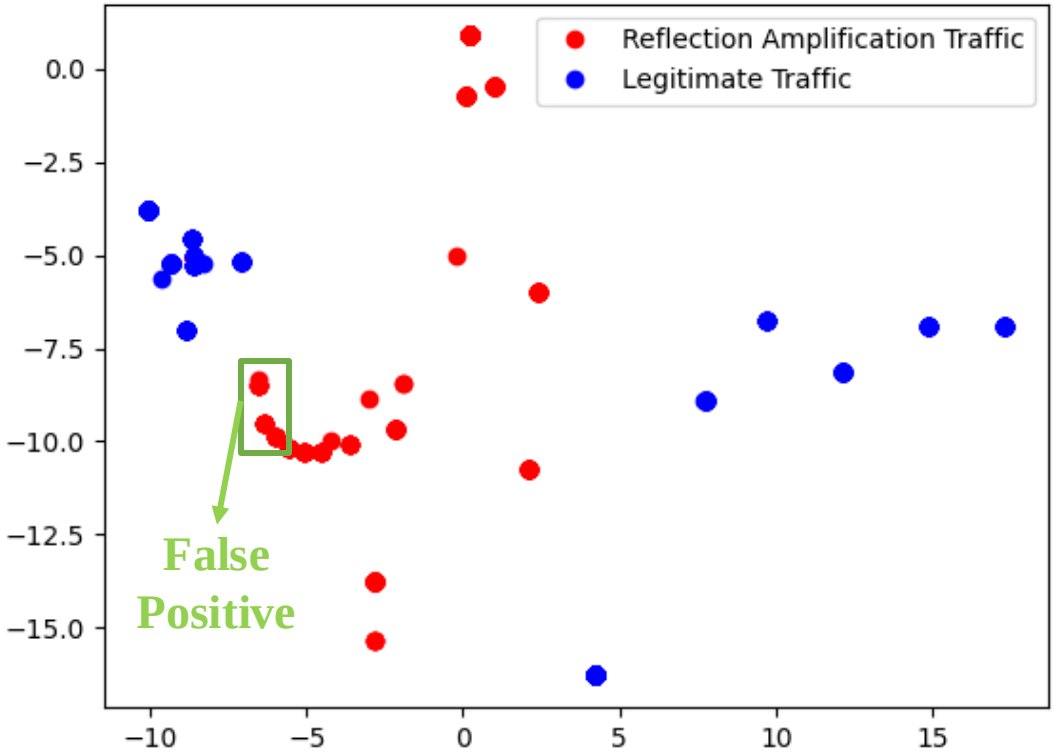




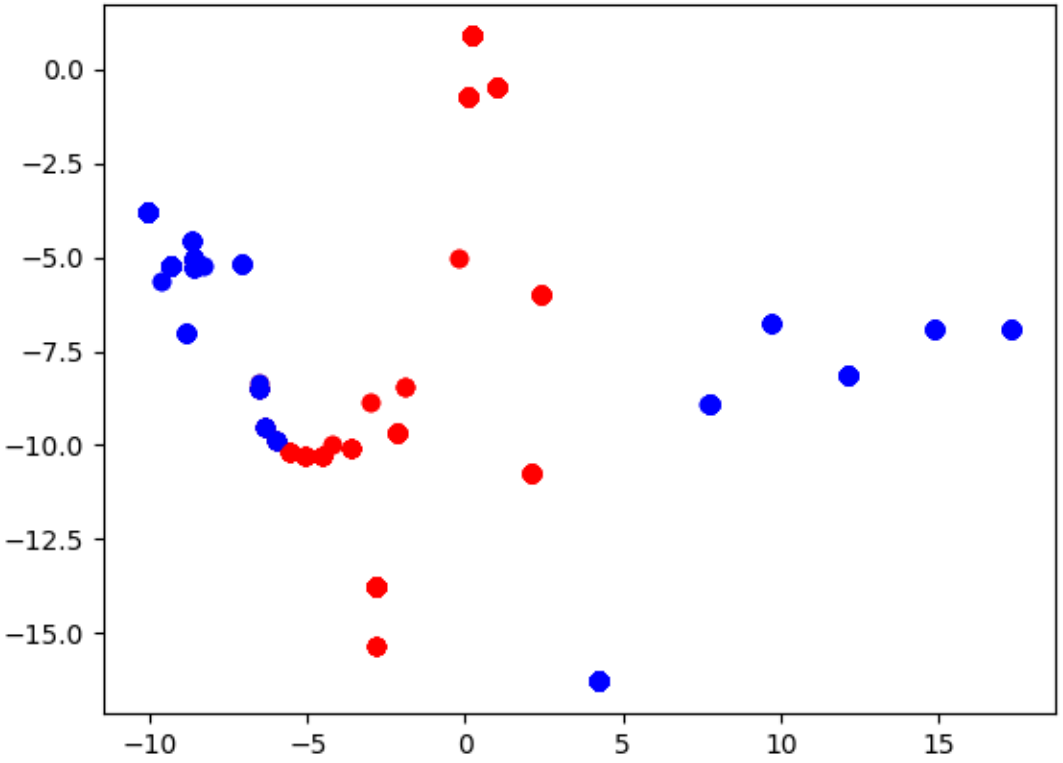
1. Information uploading (r2) instead of direct dropping
2. DDoS attacks are detected and blocked at r2 first
3. SAV-D controller selects the device that will receive the filtering rule
4. R6 receives filtering rules and executes blocking

Experiments

Ground Truth



Clustered by K-Means



The visualized clustering results of ground truth (with labels) and the traffic without labels

The proposed SAV-D architecture enables security operators to be easily aware of the characteristic of malicious traffic and global attack situation

Thanks!

Q&A

Mingzhe Xing
xingmz@zgclab.edu.cn

Draft: *SAV-based Anti-DDoS Architecture (https://datatracker.ietf.org/doc/draft-cui-savnet-anti-ddos/)*
Paper: *Linbo Hui et al. "SAV-D: Defending DDoS with Incremental Deployment of SAV," in IEEE Internet Computing*
Code: *https://github.com/sava-anti-ddos/SAV-D*