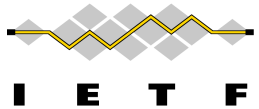
IETF 119 Hackathon

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

Haoran Luo, Shuisong Hu

Tsinghua University, Beijing Zhongguancun Laboratory

16-17 March 2024

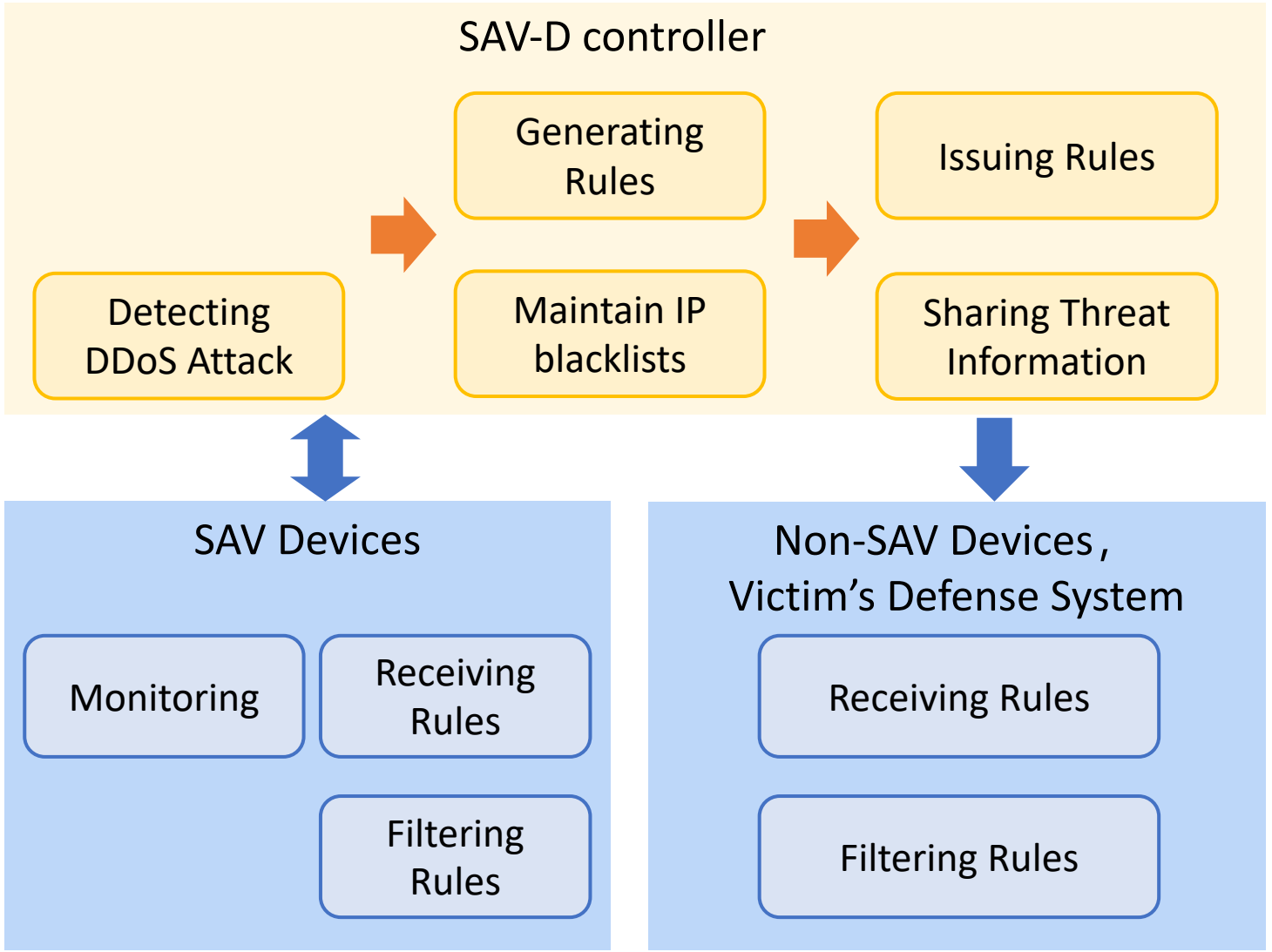


Hackathon Plan

- Relevant Draft
  - SAV-based Anti-DDoS Architecture.
    — draft-cui-savnet-anti-ddos-03 - SAV-based Anti-DDoS Architecture (ietf.org)

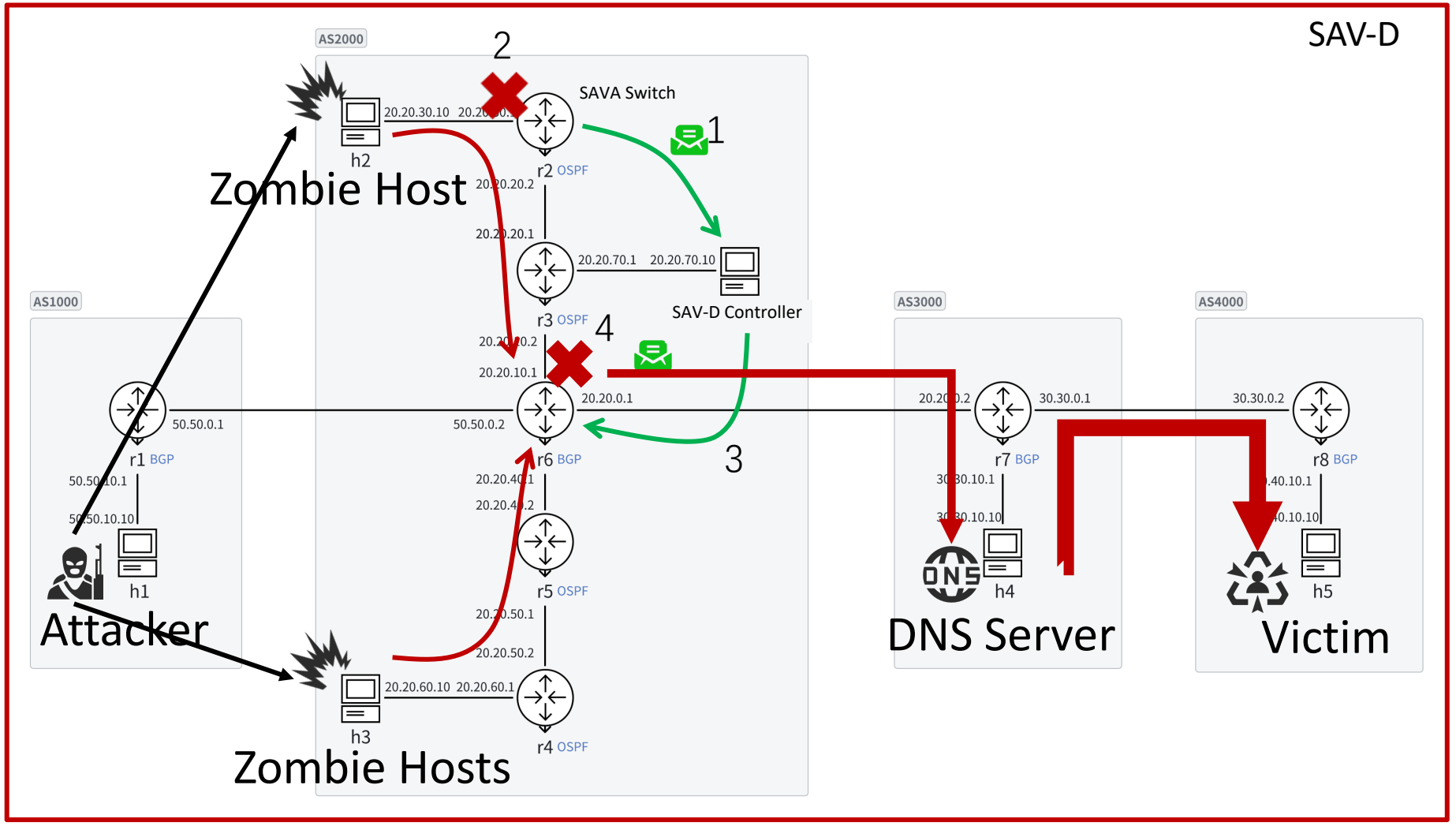
- Running Code
  - Implementation of each component of the SAV-D architecture.
  - Design an experiment to simulate the working process of SAV-D.
  - Demonstrate the effectiveness of the SAV-D architecture in addressing DDoS reflection amplification attacks.

What got done



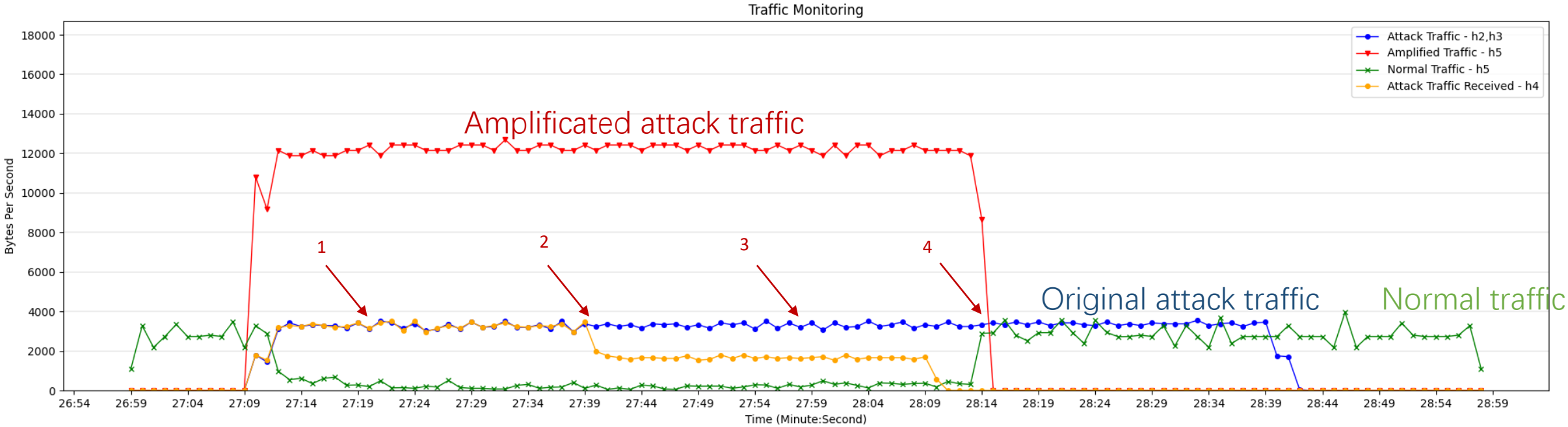
- SAV devices identify and report forged source address packets.
- Based on the collected information, the SAV-D controller identifies security intelligence.
- The security intelligence can be distributed through the SAV-D controller, benefiting the entire network.

What got done



1. SAVA switch(r2) reports spoofed source address information to SAV-D controller near the source of the attack.
2. SAV-D controller detects DDoS attack using the reported information.
3. SAV-D controller generates filtering rules.
4. SAV-D controller sends rules to chosen devices(r6) .
5. Chosen devices execute filtering rules.

What got done



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. As a result, normal traffic returns to normal levels.

What we learned

- SAV-D acts as a defense amplifier, and its goal is to block attack flows as close to the source as possible.
- During incremental SAV deployment, information uploading instead of direct dropping can help collect more threaten intelligence.

Next Step

- This is our first time to participate in the IETF. If you are interested, you can join us, communicate with us, and further promote standards.