The Extended DDoS Open Threat Signaling Use Cases

draft-xia-dots-extended-use-case-00

Liang Xia Huawei

Haibin Song Huawei

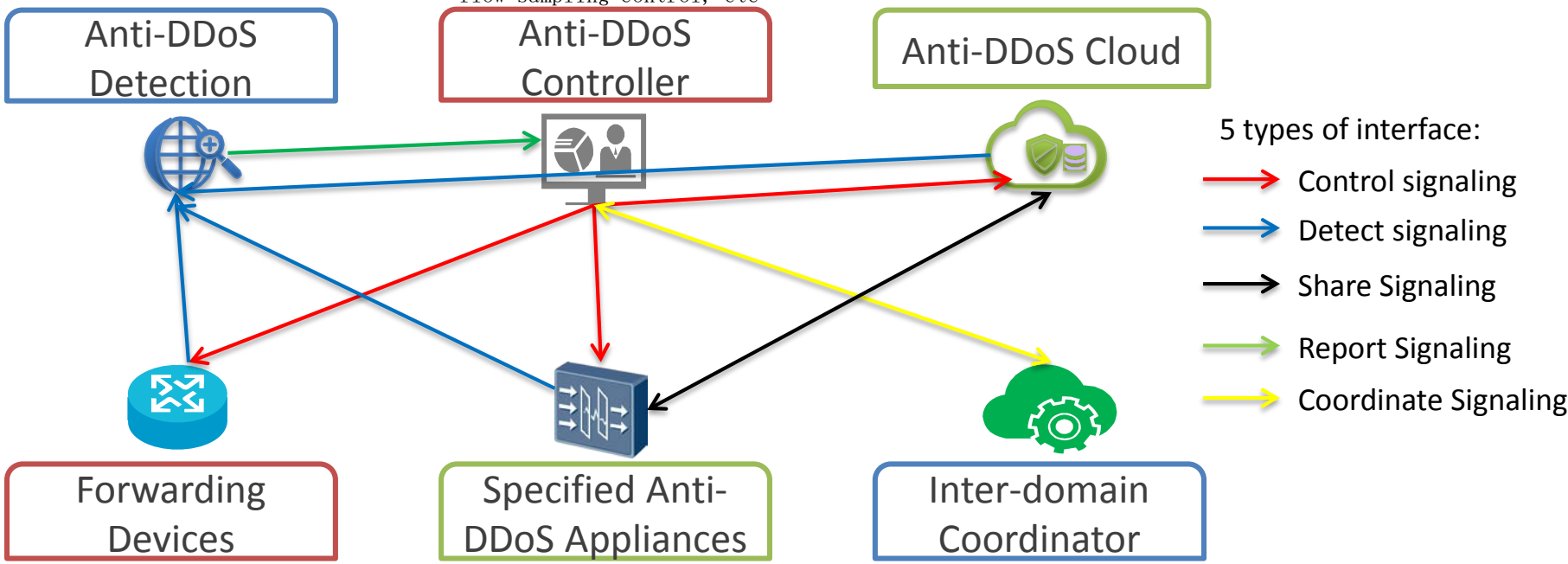
July 2015 Prague

DOTS Overview: A Collaborative Anti-DDoS System

- Centralized, holistical picture of network attacks
- Data mining, big data analysis can enhance the detection
- Rich statistics info: TopN, Trend...

- Centralized, optimized control of network devices
- traffic supression, traffic diversion, source traceback, flow sampling control, etc

- Key part of a layer Anti-DDoS solution
- Mainly mitigate the network flood DDoS attack with high scalability
- Signal mechanism support



- Router and switch send their flow sampling (IPFIX) info to detection node
- Low cost and high flexibility
- layer 4 connection oriented sampling

- DPI + scrubbing, integrative vs distributed
- Mainly mitigate the application layer DDoS attack on network premise with limited scalability
- Signal mechanism support

- A coordinator for near source mitigation across multiple domains
- Integrate global resources for Anti-DDoS, save bandwidth, new business opportunity
- Threat info sharing, open and win-win

Goal of this Draft

- A specific Anti-DDoS system is influenced by many variables:
  - Architecture: centralized vs distributed;
  - Detection means: forwarding devices vs specific Anti-DDoS appliances;
  - Deployment means: static vs dynamic (VNF);
  - Others: traceback, network operators vs security service providers, traffic suppression vs traffic scrubbing, inter-domain coordination, etc
- Identify the valuable and promising use cases to derive the requirements for a multi-technology integrated and collaborative Anti-DDoS solution, and the related DOTS works.

Two Extended DOTS Use Cases

- This draft proposes two new use cases which illustrate more scenarios and multiple ways of implementation within the existing DOTS work scope:
  - Collect and correlate security related flow information from network forwarding devices and proactively detect the DDoS attack by centralized analysis or data mining;
  - Dynamic and distributed Anti-DDoS solution by creating VNFs and deploying them to the edge network on demand.

Use Case 1

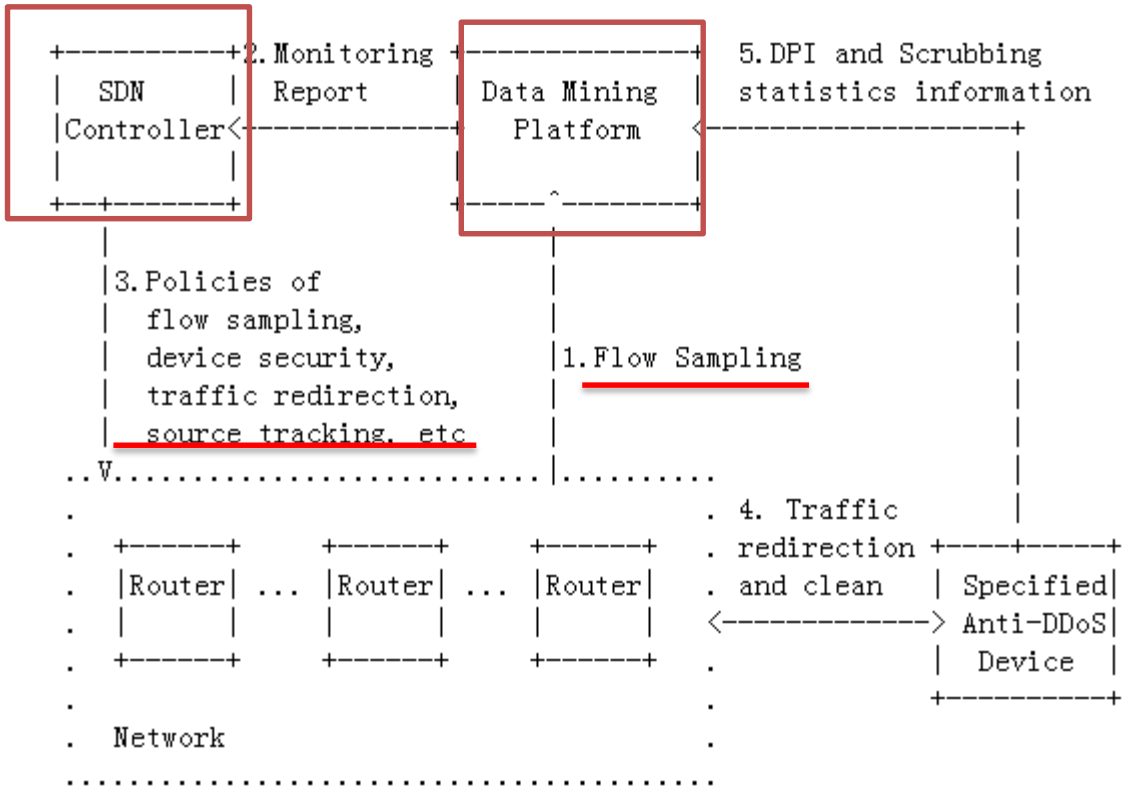


Figure 1. Data Mining and SDN Based Centralized Anti-DDoS Use Case

Use Case 2

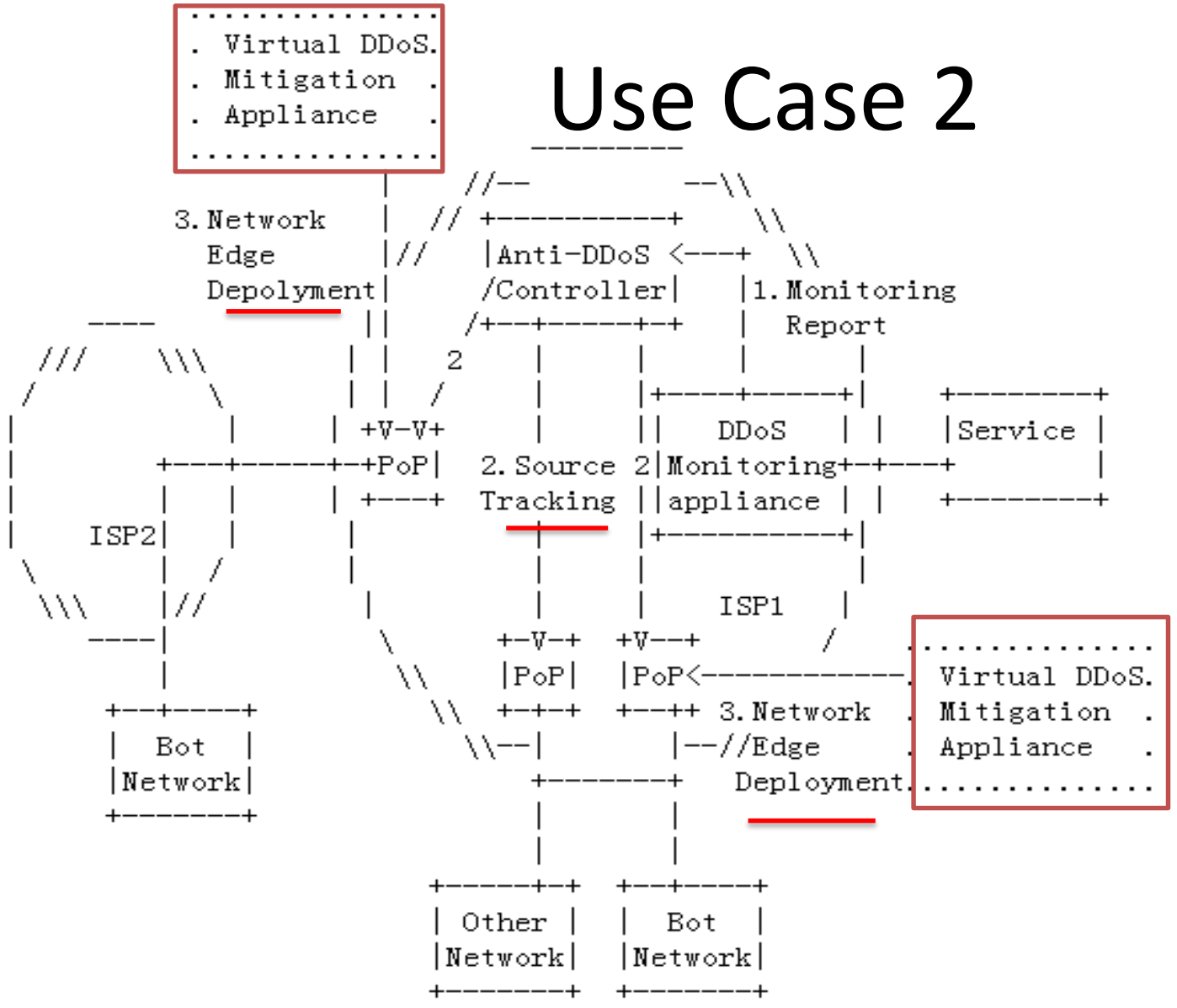
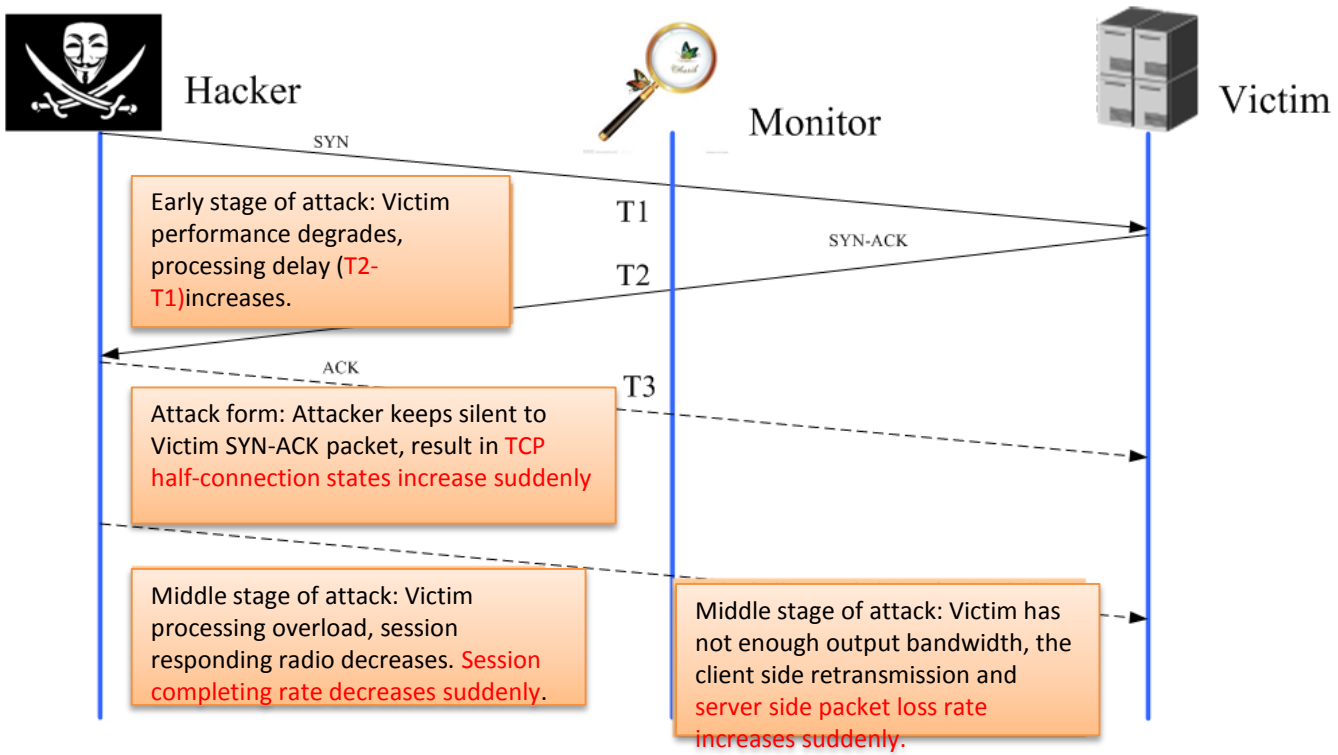


Figure 2. NFV Based Distributed DDoS Mitigation Use Case

IPFIX Security Extension

- draft-fu-ipfix-network-security-01

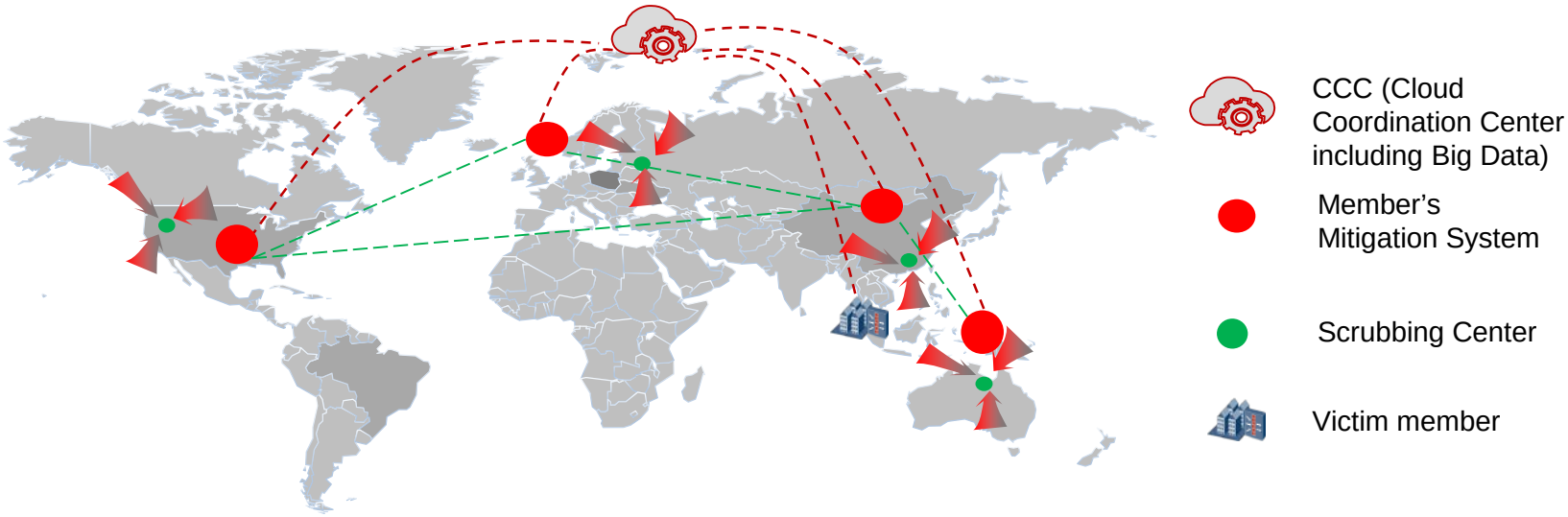


Key Metrics for Attack Detection
IP quintuple
Session delay(handshake time T2-T1）
Abnormal connection state(Setup、Terminate，half-connection, RST，ACK/SYN-ACK/FIN-ACK)
Session completing rate
Session packet loss rate
Packet payload signature
Fragment packet radio
SNMP statistics (reflection)
NTP statistics (reflection)
DNS statistics (UDP Flood）
Session packet statistics (FSD, Flow Size Distribution)
Other IPFIX IEs

Use Case 3 (not yet in draft)

Inter-domain Anti-DDoS Coordination

Carriers and MSSPs unite to coordinate global mitigation resource to carry out near source mitigation.



① One of the alliance members mitigates traffic within the bandwidth, application-layer attacks using a local DDoS mitigation system and detects large-traffic attacks.

② When not being able to defend large-traffic attacks, the victim member sends cloud signal to the CCC (Cloud Coordination Center) request global near source mitigation.

③ The CCC notifies the corresponding alliance members to initiate near-source mitigation.

Next Step

- Solicit Comments and keep on improving current draft

- Possibly develop the architecture draft for DOTS works

Thanks!

Liang Xia (Frank)