# DDoS Mitigation Offload: A DOTS Applicability and Deployment

IETF#105, Montreal, July 2019

Yuhei Hayashi (NTT)
Mohamed Boucadair (Orange)
Kaname Nishizuka (NTT Communications)

# Agenda

1. Goals
2. Summary of DMS offload scenario
3. Technical Contributions
4. What is Next?

# 1. Goals

- Exemplify the use of DOTS in typical deployment contexts

- Assess to what extent current DOTS specifications can be applied in a particular deployment context and whether there are voids

- Close the design loop:

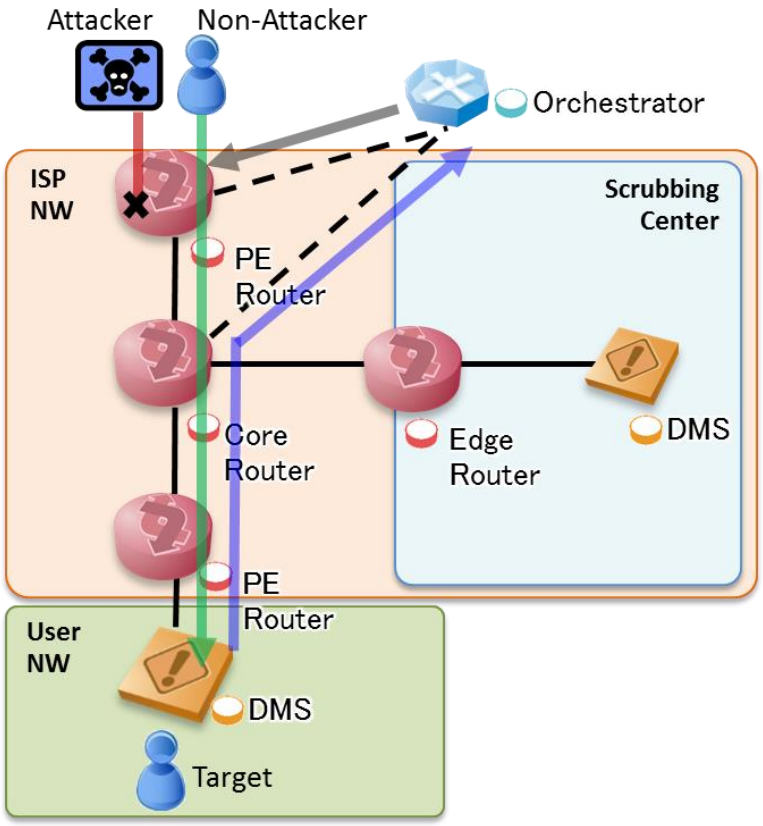
Use cases ➔ Specifications ➔ Deployment applicability checks

Update?

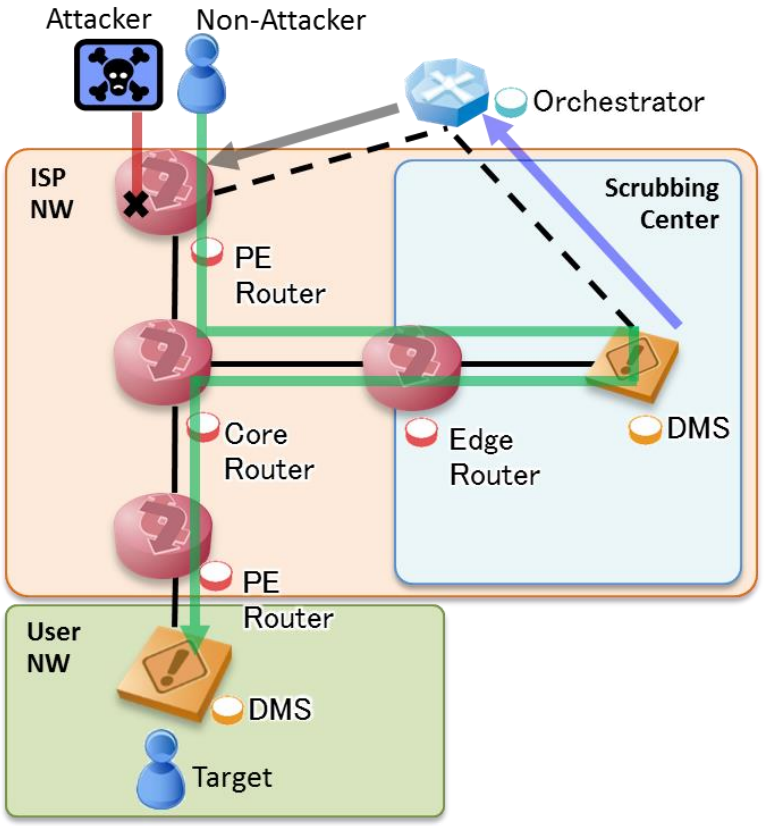
# 2. Summary of DMS offload scenario

- A DMS whose utilization rate is high sends its blocked traffic information to an orchestrator using DOTS protocols.
- The orchestrator requests forwarding nodes such as routers to filter the traffic.

DOTS Request via In-band Link

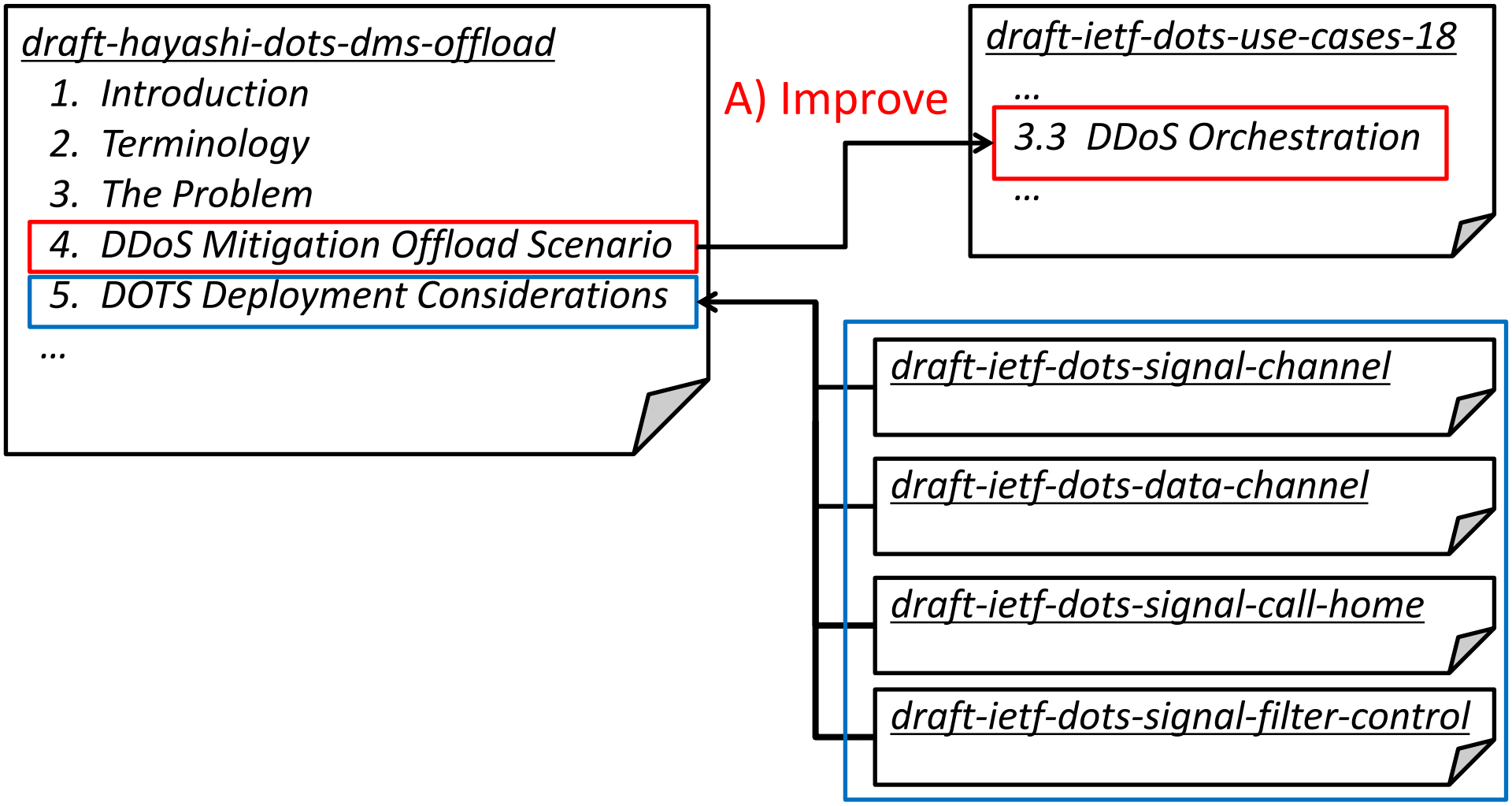



DOTS Request via Out-of-band Link




# 3. Technical Contributions (1/3)

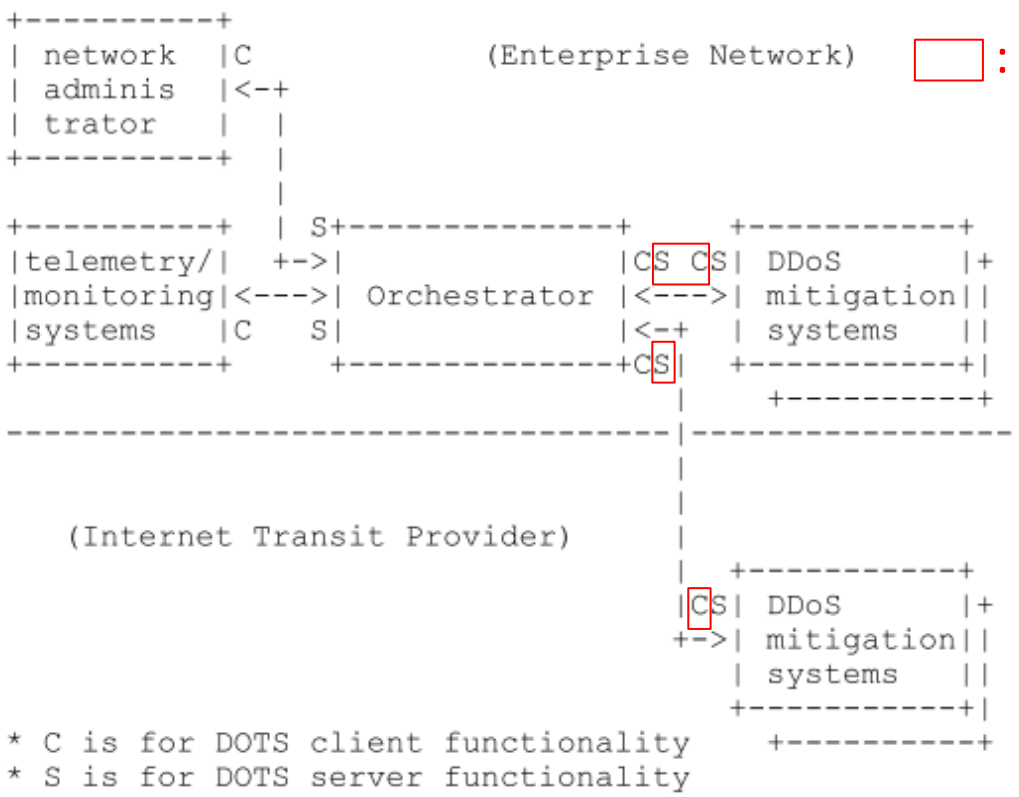
1. Improve “3.3 DDoS Orchestration” in Use case WG draft.
2. Check applicability of DOTS protocol and describe deployment considerations.




B) Check DOTS applicability and describe “Deployment Consideration”

# 3. Technical Contributions (2/3)

A) Improve “3.3 DDoS Orchestration” in Use case WG draft.




: modification point

...

The orchestrator DOTS client is notified that the DDoS Mitigation is effective by the selected DDoS mitigation systems. The orchestrator DOTS servers returns back this information to the network administrator. When the DDoS attack become severe and the DDoS mitigation systems utilization rate reach its maximum capacity, its DOTS client can request offloading mitigation with its blocked traffic information to the orchestrator DOTS servers. Then the orchestrator requests forwarding nodes such as routers to filter the traffic.

...

# 3. Technical Contributions (3/3)

B-1) DOTS applicability check : These specs are enough to carry out the scenario.
B-2) Describe “Deployment Consideration” : What type of information can be conveyed and effective to carry out the scenario.

*dst_port* information can’t be sent when the link is congested

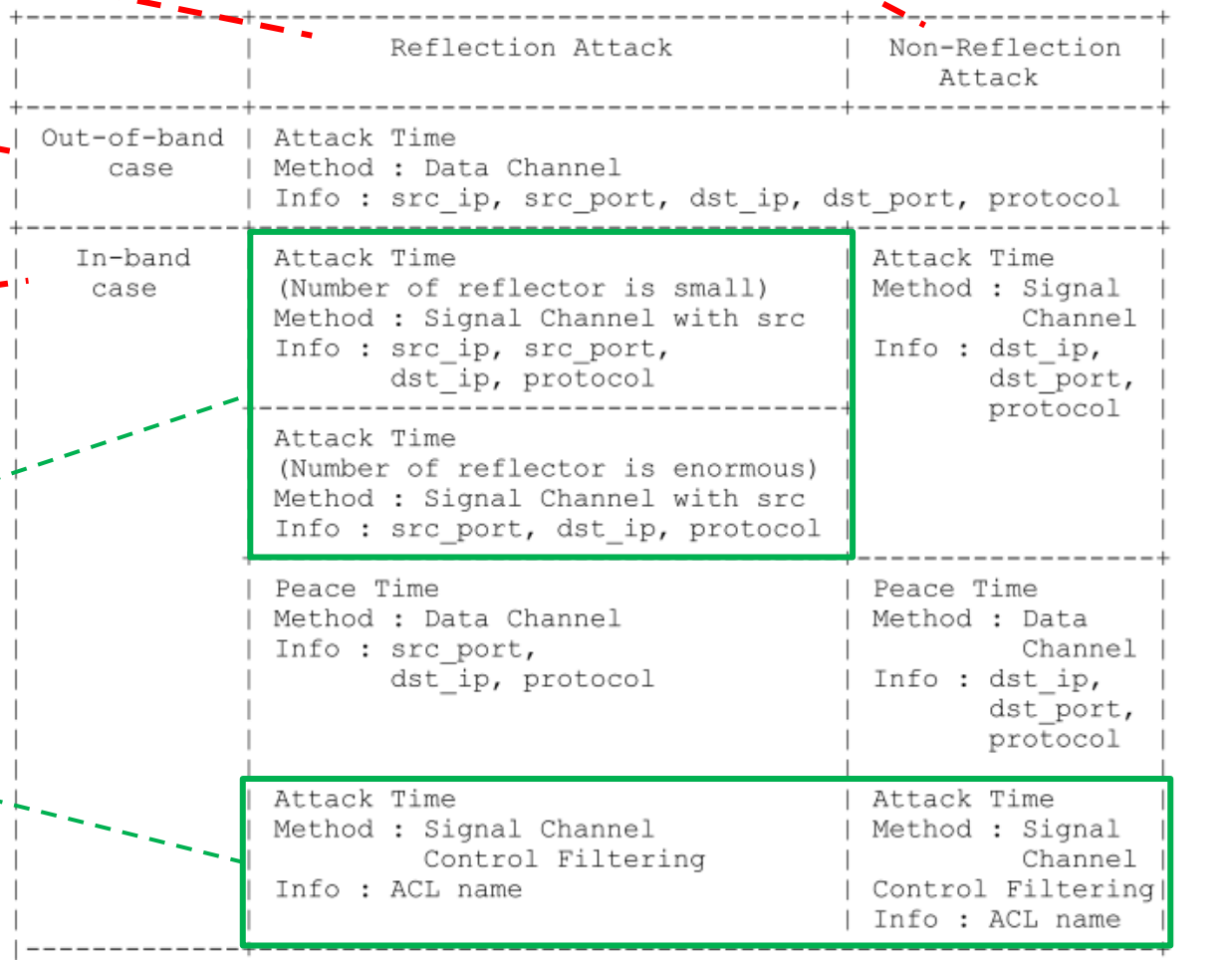
*src_ip* and *src_port* information can’t be sent when the link is congested

The link is not congested under attack time

The link is congested under attack time

Using *src*-* attributes defined in call-home draft

Using attributes defined in Controlling Filtering draft



# 3. What is Next?

- Request WG adoption about “Deployment Consideration”
- Discussion
  1. Make a new WG draft?
  2. Add “Deployment Consideration” to each spec draft?