Extended YANG Data Model for DOTS

Yong Cui, **Linzhe Li**

Tsinghua University, Beijing Zhongguancun Laboratory

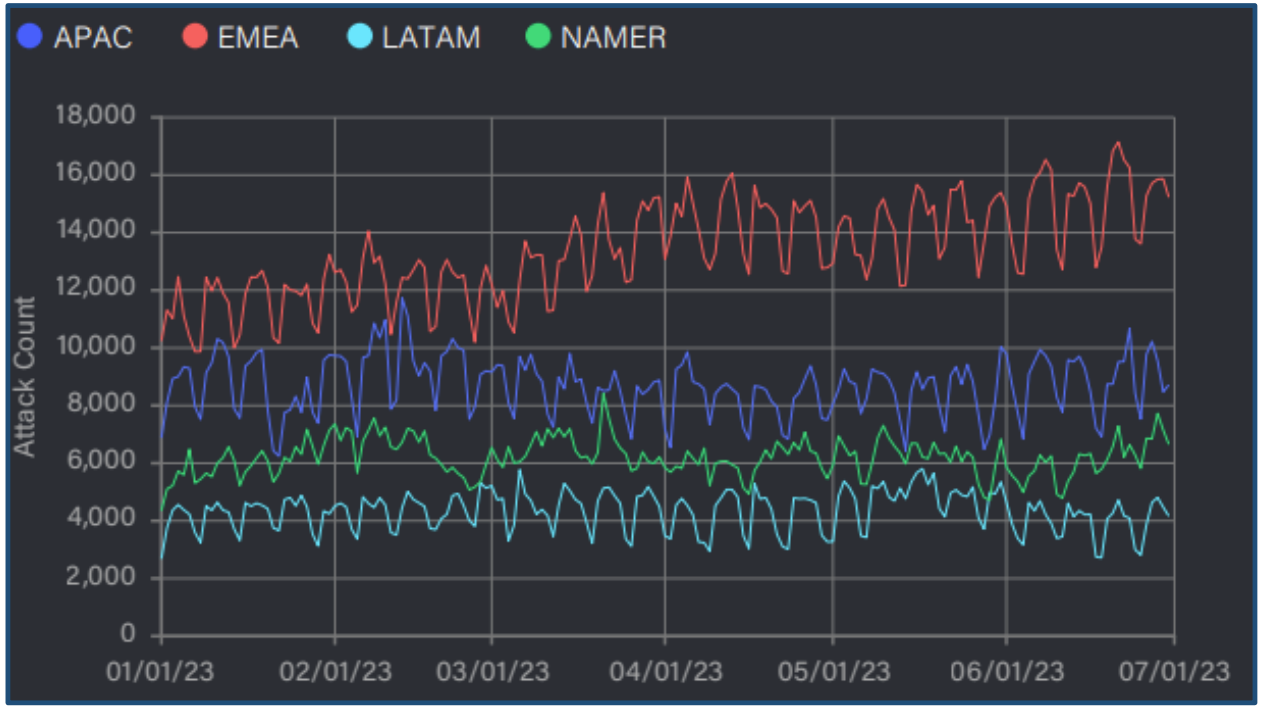
March 18, 2024

Outline

- DDoS Attack Trends and Problems
- Potential Solution and Implementation
- Questions

DDoS Attack Trends and Problems

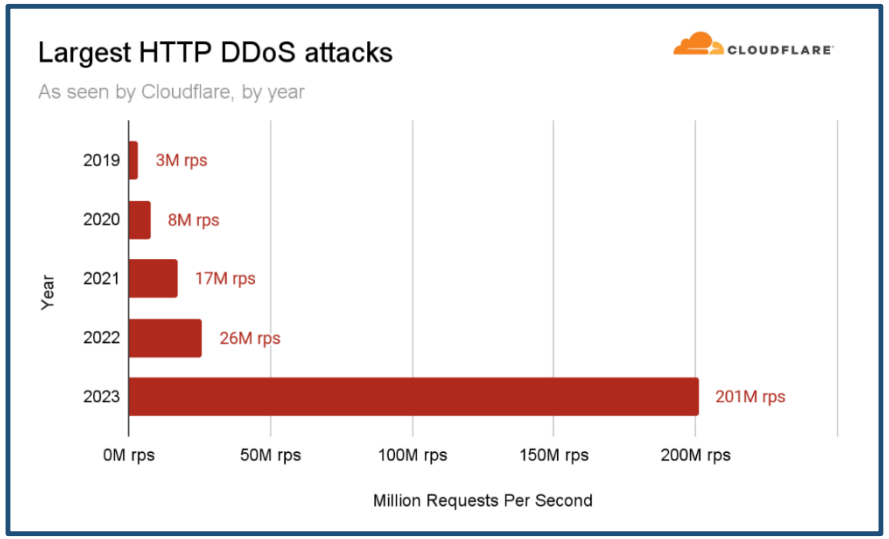
- **More frequent**
  - 7.9 million DDoS attacks happened in the first half year of 2023, 31% increase year over year.



DDoS Attack Trends and Problems

➢ Hyper-volumetric

- The largest attack in 2023 — 201M requests per second (rps), almost 8 times larger than 2022's.



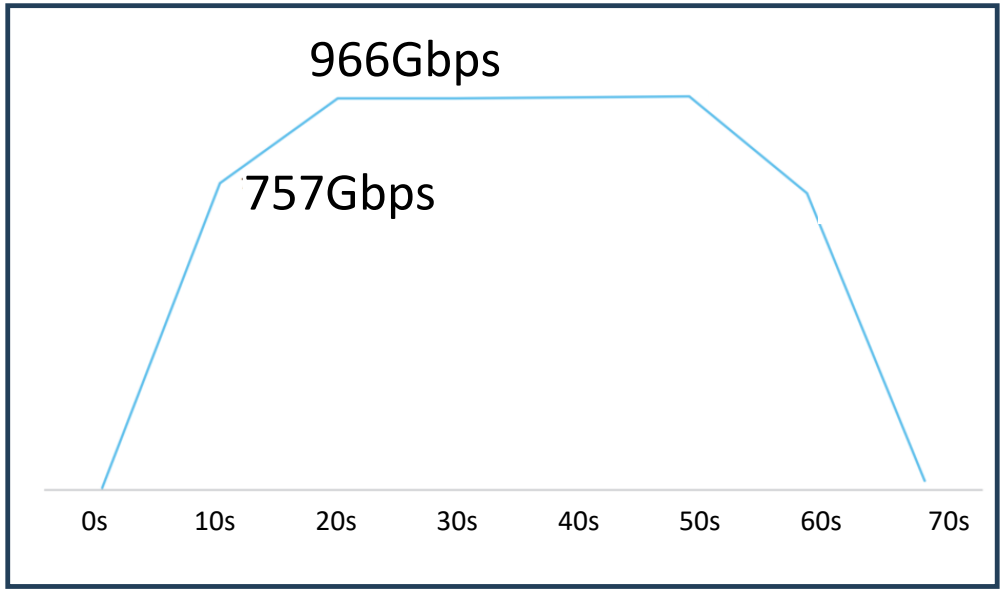
➢ High defense costs

- To counter randomly occurring DDoS attacks, long-term procurement and operation of large-scale DDoS defense resources come at a very high cost.

DDoS Attack Trends and Problems

➢ More Intelligent

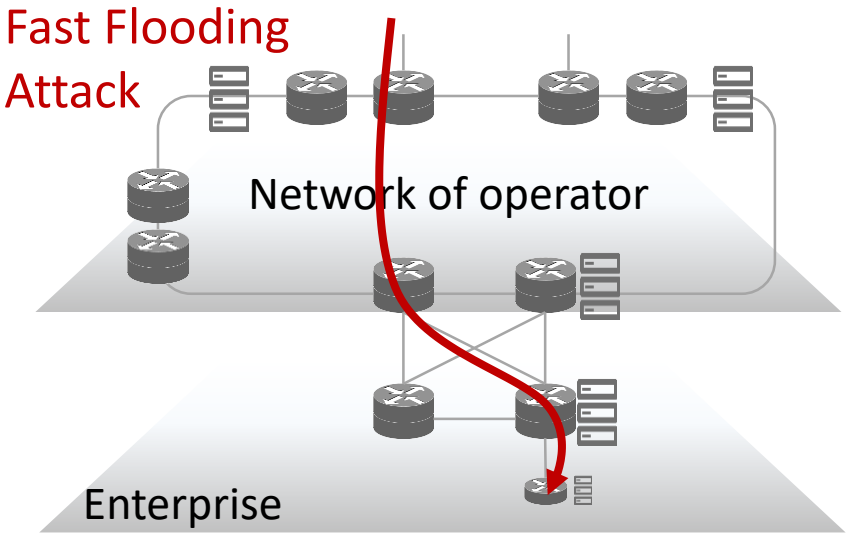
- 50% of DDoS use more than two vectors.
- "Fast Flooding" can suddenly spike to a high level for a short duration.



➢ Hard to detect

- For ISP, Sampling-based attack detection usually takes more than 1 minute.
- New types of attacks are emerging, and intelligent attacks occur more frequently, both are difficult to detect.

Problem 1



For operator：

- Detect attacks in minutes （sampling based）
- Have enough resources

For enterprise:

- Detect attacks in seconds
- Limited resources, can not mitigate Gbps-level attack traffic

The enterprise (DOTS Client)

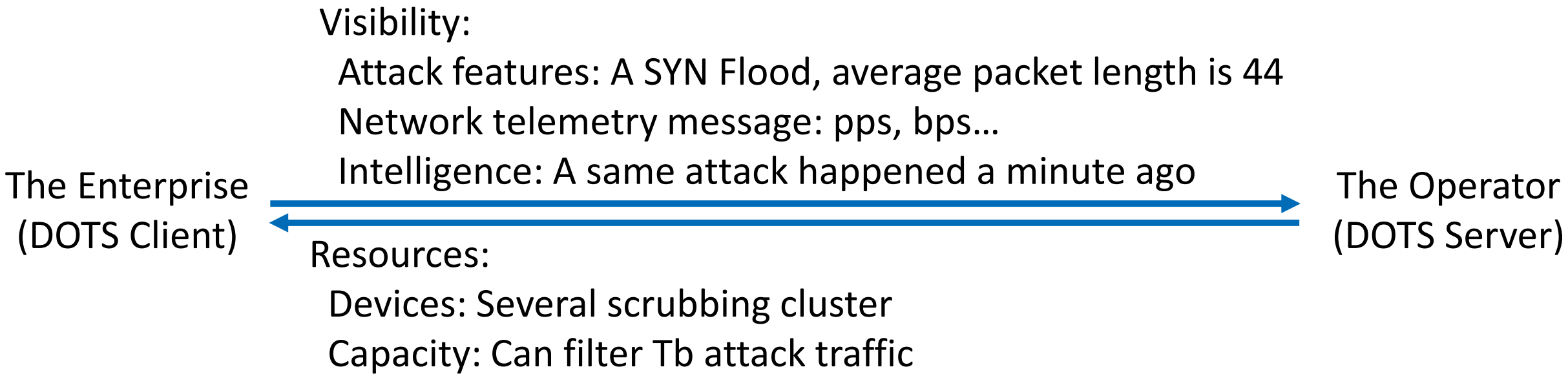
1. Mitigation Request →

← 3. Collaborative Mitigation

The operator (DOTS Server)

2. Acknowledge the attack(in minutes) and develop mitigation strategies

Problem 1

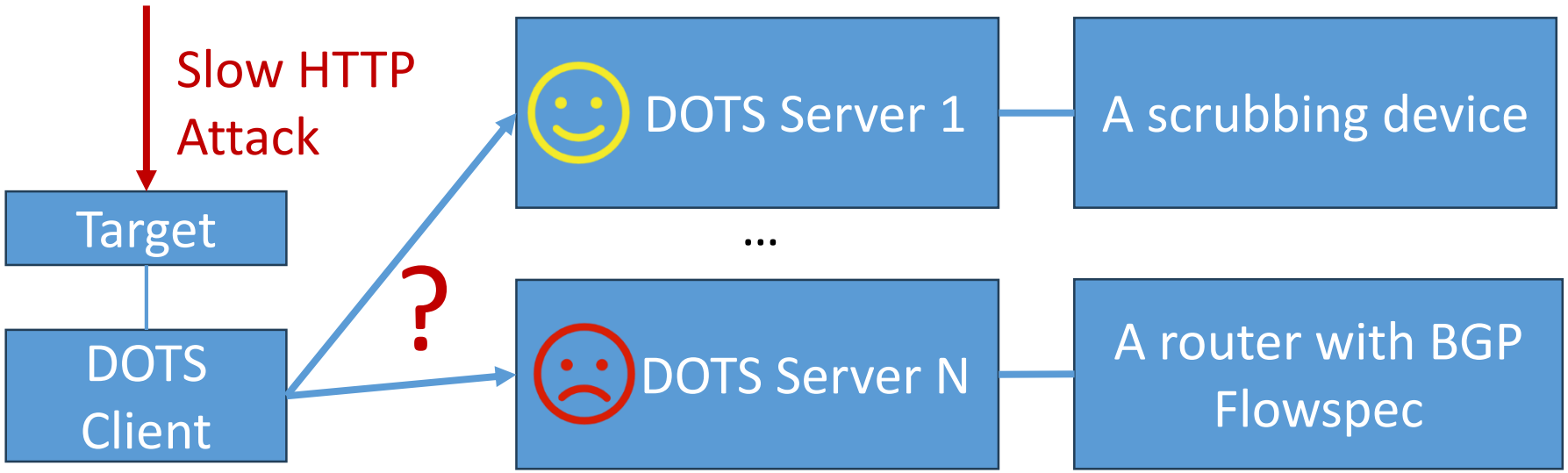


- Original DOTS

```
"vendor-id": 32473,
"attack-id": 92,
"start-time": "1641172809",
"attack-severity": "high"
"attack-description": "DNS amplification Attack: \ This
attack is a type of reflection attack in which attackers \
spoof a target's IP address. The attackers abuse
vulnerabilities \ in DNS servers to turn small queries into
larger payloads."
```

- What we need
  - Structured attack feature data model

Problem 2



- Client needs to know the mitigation capabilities that the server can provide in order to make the right decision.
- What we need
  - mitigation capacity data model, including strategy and capacity

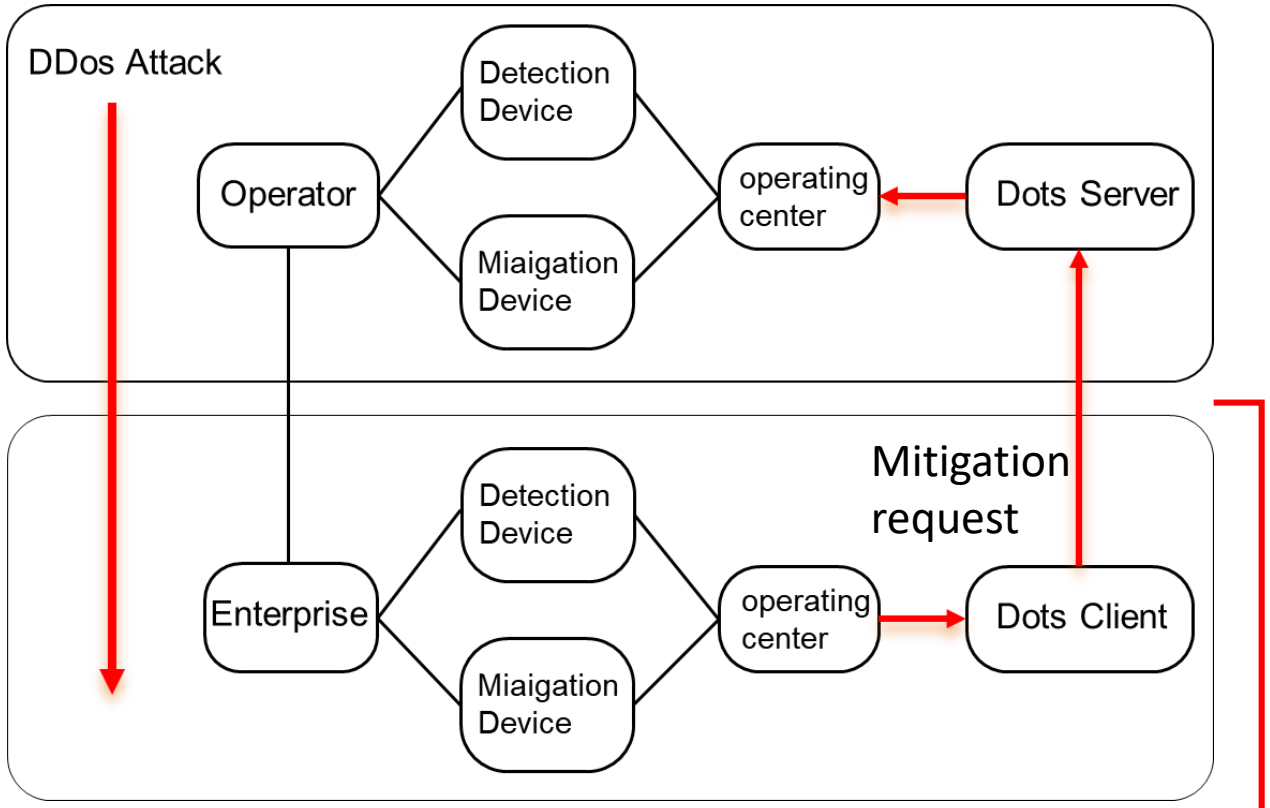
Requirement： Data Model Extension

- DOTS Signaling Function
  - Issue and response mitigation requests
    - Need attack features for and mitigation recommendations
  - Exchange network telemetry information
    - Need more detailed baseline and intelligence
  - pre-configuration
    - Need mitigation capacity and baseline
  - Registration and certification

Implementation & Experiment

➢ Topology Diagram

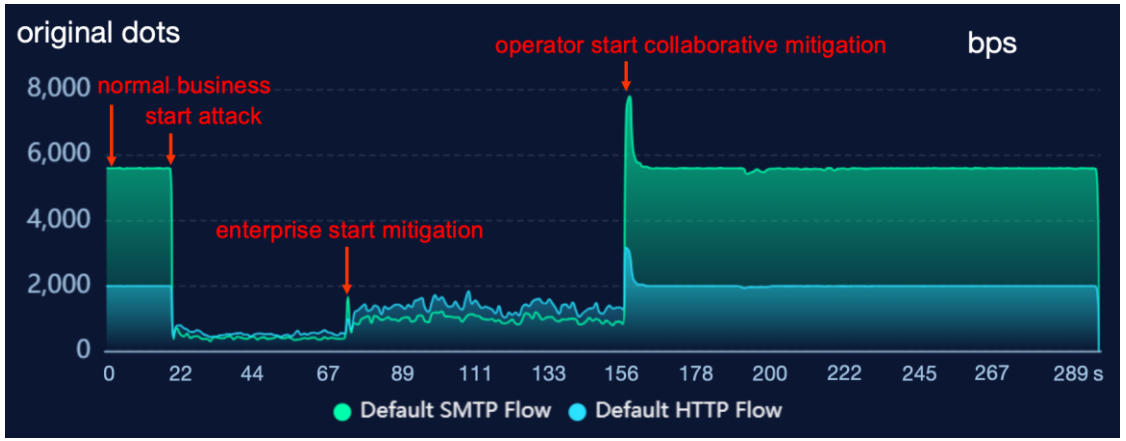
- We built a test bed to verify the mitigation effects of DDoS attacks.
- We developed a simplified DOTS client and server.
- We realized the extended data model for transportation using HTTP.
- Experimental scene is same as Problem 1.

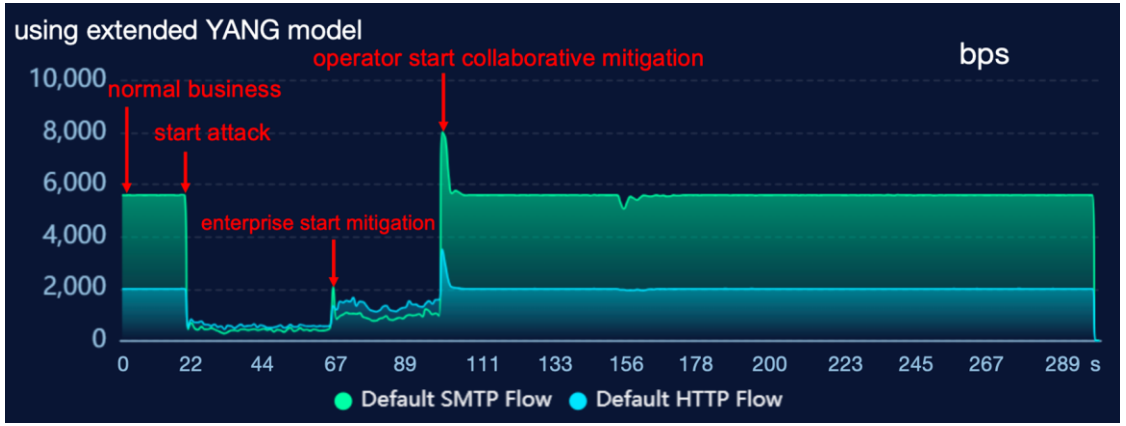


Type： SYN Flood
Feature： {
avg-packet-length: 33,
duplicate-message": “xxxx"}

Experiment

- Results





- Using the attack features, The time to start mitigation was reduced by 43%(139s→79s).
- The devices in the test bed have a data forwarding delay of 30s.
- By inference, in the network, the mitigation time can be reduced from minute level to second level.

Questions

- We were applying DOTS to our collaboration framework but found some important data models(e.g. attack features) that were not yet defined.
- Operators and security vendors are both care about the extended data model, it determines the capacity of co-mitigation.
- For DOTS has concluded, where can we advance this I-D?

Welcome to contact me：lilz@zgclab.edu.cn, Linzhe.

Thanks!