The Extended YANG Data Model for DOTS Used in DDoS Mitigation

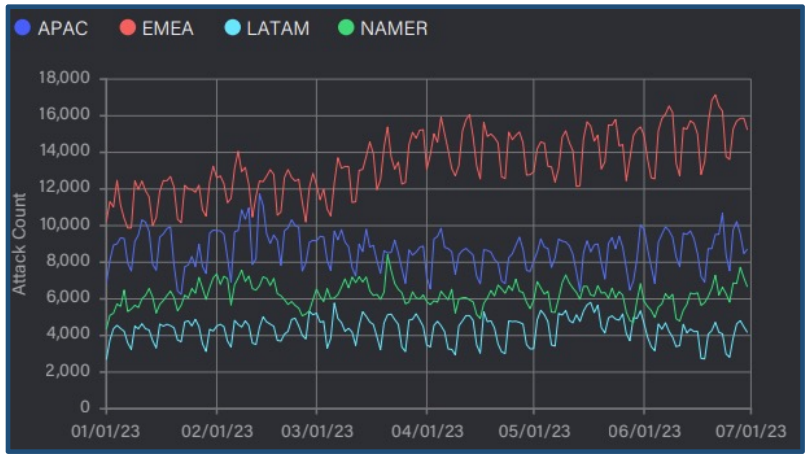
Linzhe Li [‡], Xiaohui Xie[†], Yong Cui [†]

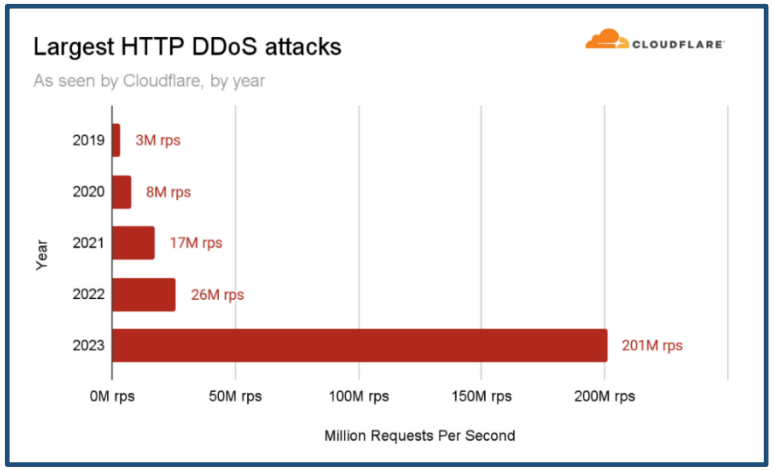
[†] Tsinghua University, [‡] Zhongguancun Laboratory

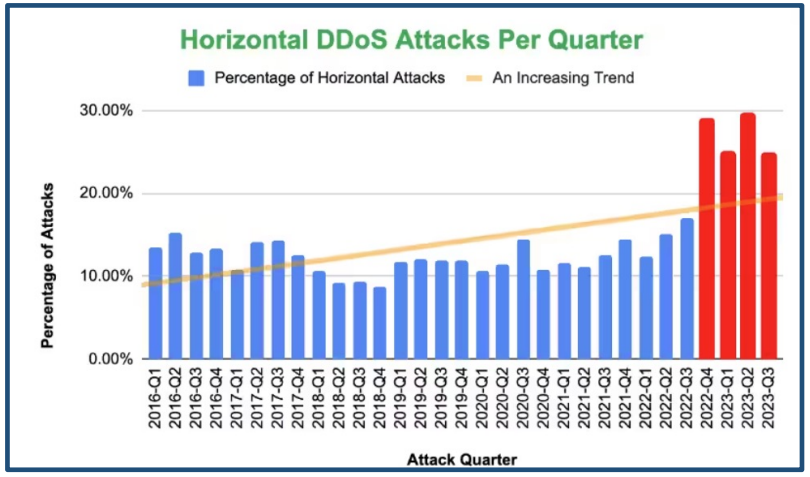
lilz@zgclab.edu.cn

DDoS attack trends

- **The constantly evolving Distributed Denial of Service(DDoS) attacks pose a significant threat to the cyber world**
  - More frequent, Hyper-volumetric, More Intelligent

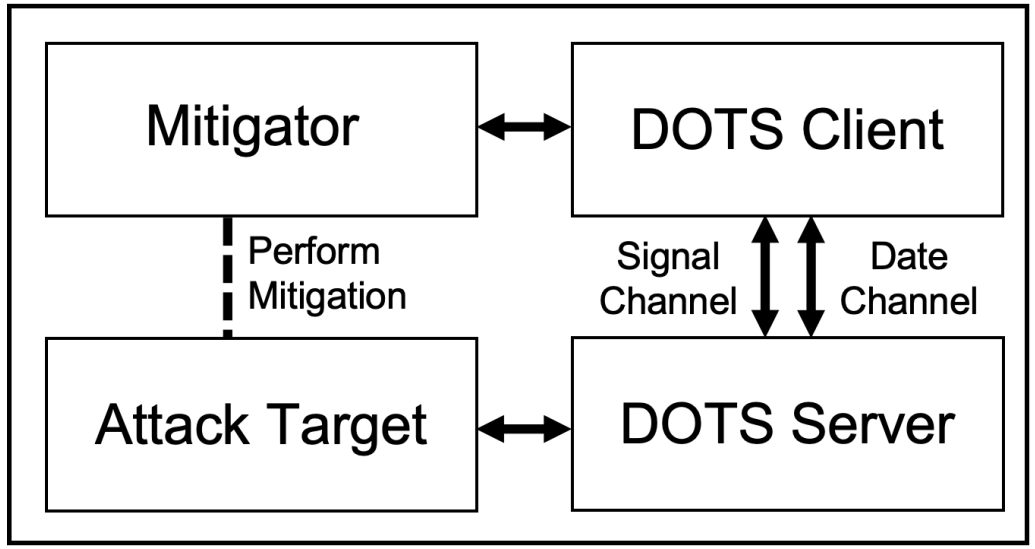






Collaborative Mitigation is Needed!

- **DDoS Open Threat Signaling (DOTS) protocol is used for coordinated response to DDoS attacks**
  - Between any device or software product involved in DDoS mitigation
  - Collaborative information includes collaborative mitigation requests, monitoring data, etc

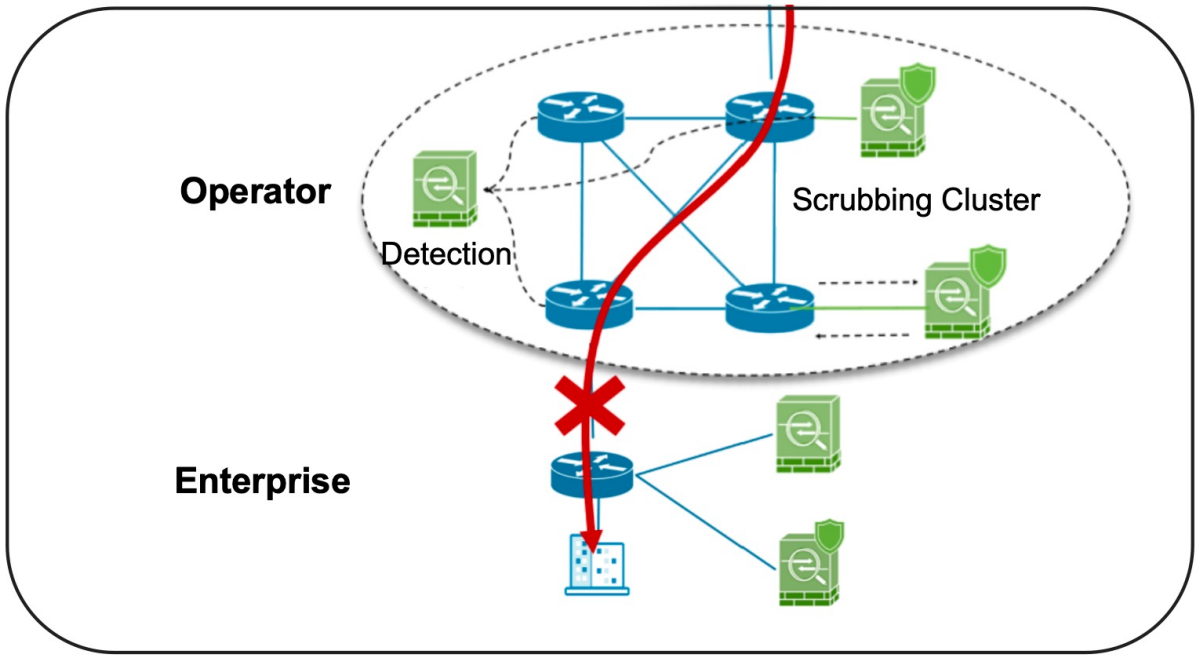


Collaborative Mitigation is Needed!

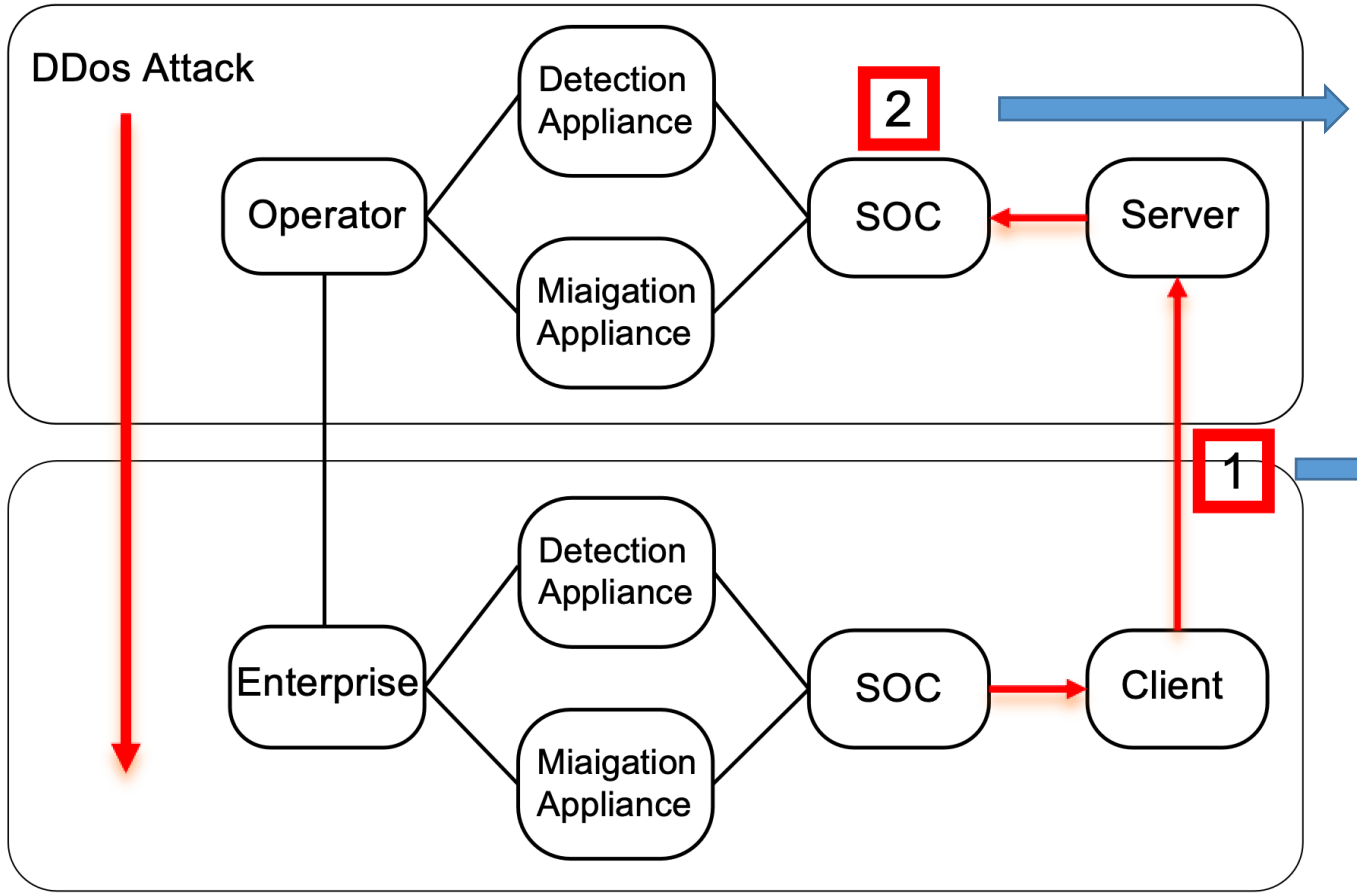
- **However, DOTS protocol no longer meets the requirements for some collaborative mitigation needs due to**
  - Limited pre-configuration information
  - Mitigation requests lack attack characteristics
  - The lack of detailed mitigation requirements …

An Example Scenario

- The scale of transient flooding attack traffic exceeds enterprise bandwidth, requiring collaborative mitigation
- Operators match minute-level attack alarms with **mitigation requests (Only target IP and protocol info)** to formulate collaborative mitigation policies
- Minute-level collaborative response still lead to enterprise breakdown



Extended YANG Data Model for DOTS

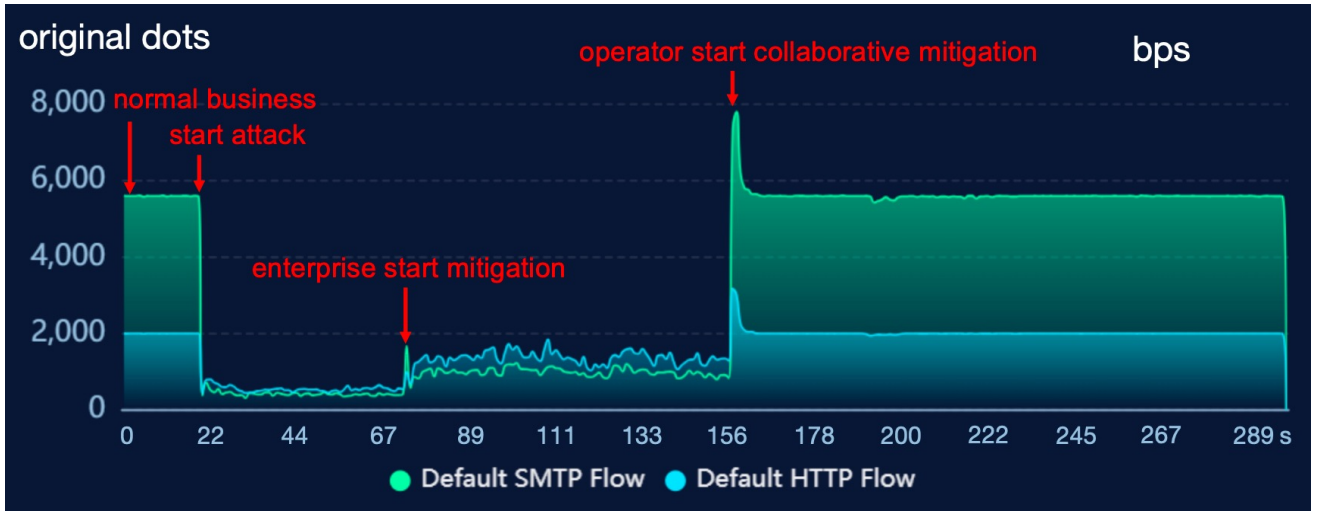


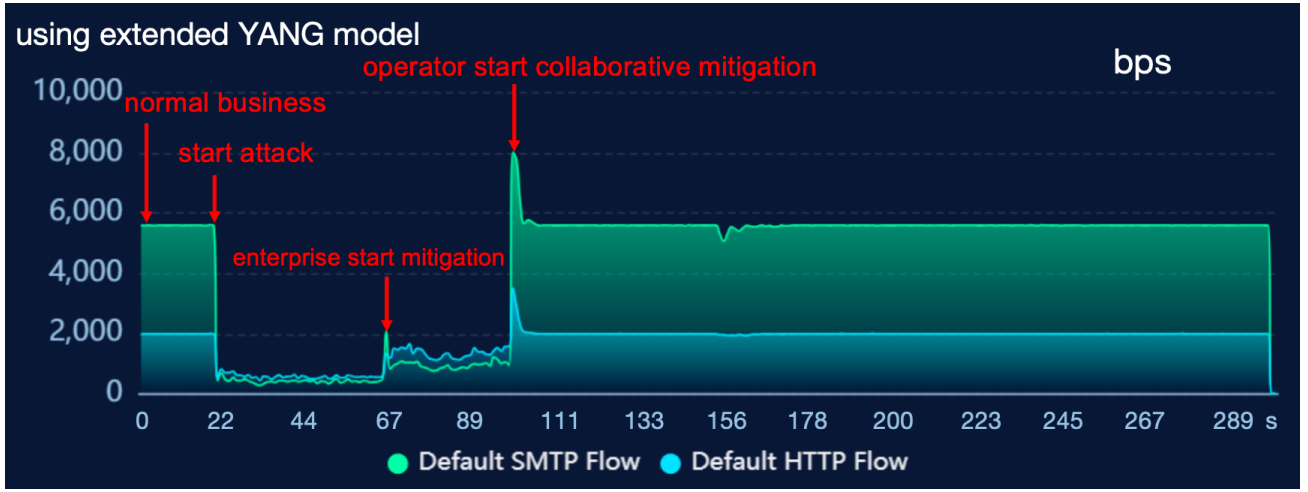
Directly using recent Netflow data match with the attack features in the mitigation request. In order to achieve second level association attack confirmation

The client initiates a collaborative mitigation request to the server, which contains the mitigation requirement(e.g. target IP address, protocol, mitigation resources) and attack features(e.g. type, average packet length and bps).

Validation Results

- We implement the extended data model in a testbed
- With the extended collaborative mitigation model, operators started mitigation **43% faster!**
- By inference, in the network, the mitigation time can be reduced from **minute level to second level**.





For more details Please see draft-cui-dots-extended-yang-01

Thanks!