



中国移动
China Mobile

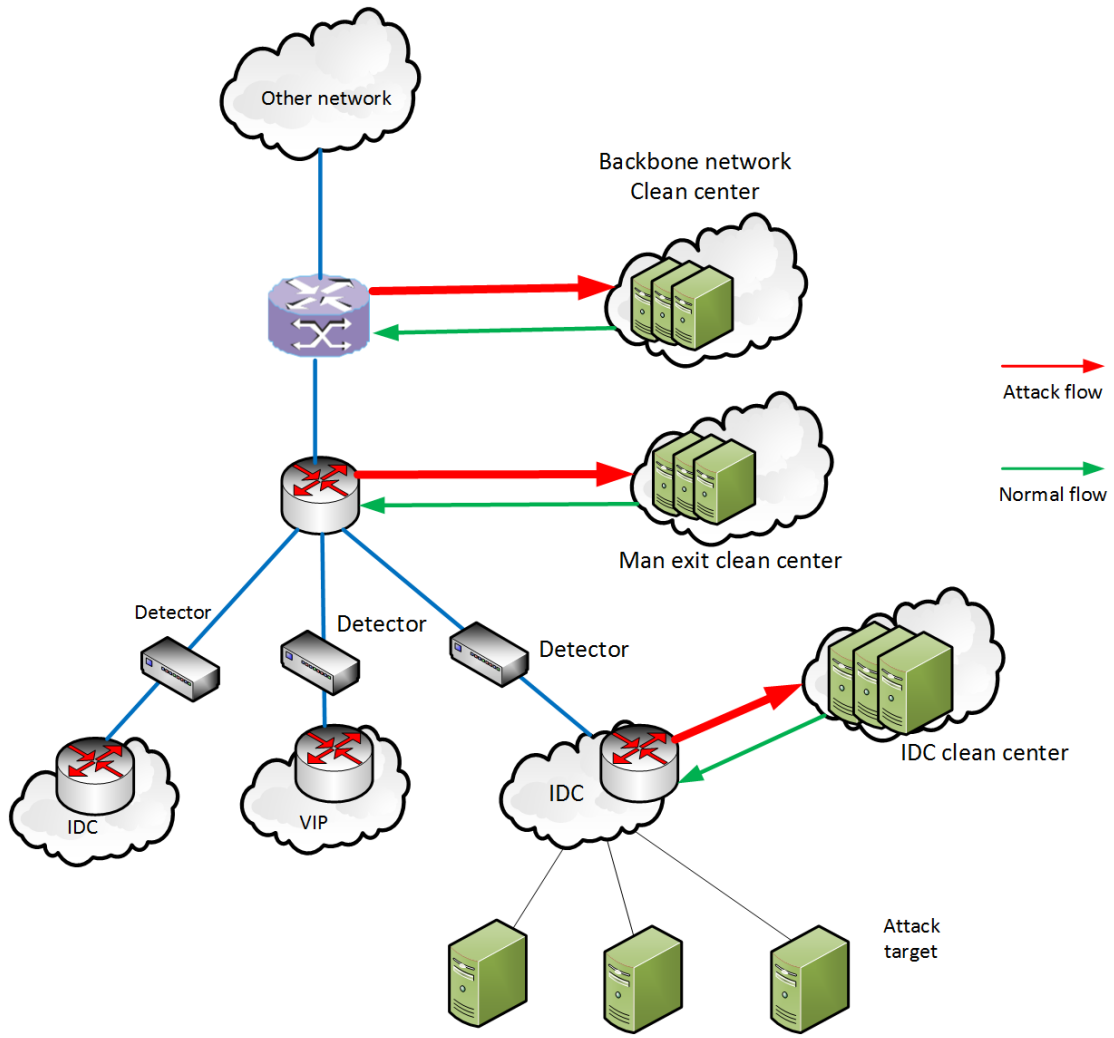
DOTS extension for Attack type and bandwidth

- 1.Draft-chen-dots-attack-type-expansion-00
- 2.draft-chen-dots-attack-bandwidth-expansion-01

Meiling Chen, Li Su, Jin Peng
China Mobile Research Institute

March 2019

China Mobile's mitigation architecture of DDoS



Attack-bandwidth expansion

Draft-chen-dots-attack-bandwidth-expansion-00

Requirements

USE CASE 1

Optimal clean device selection

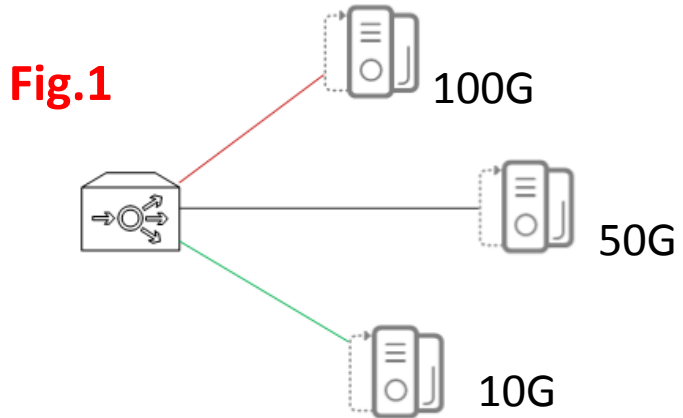
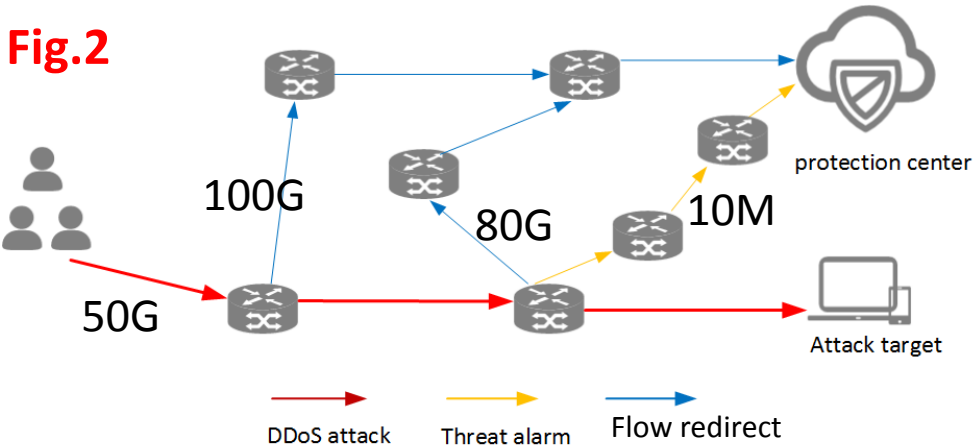


Fig.2



USE CASE 2

Optimum BGP redirect path for mitigation

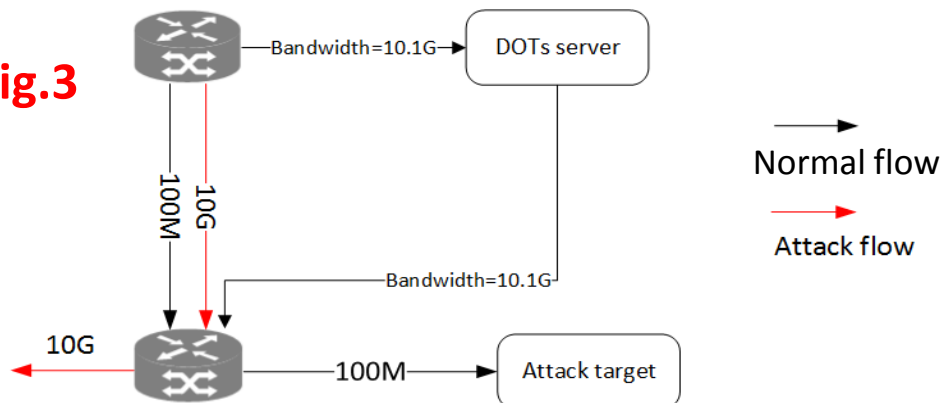
Threshold:70%

USE CASE 3

Offload the extreme large flow

Example: Ensure 10% success rate

Fig.3



Target-Attack-Type expansion

Draft-chen-dots-attack-type-expansion-00

Current status

- ◆ Different vendors are good at handling different types of DDoS attack .

USE CASE 1

- ◆ Mixed traffic attack
- ◆ MitigatorA for connectionless Flood, MitigatorB for CC attack
- ◆ Mitigation coordination

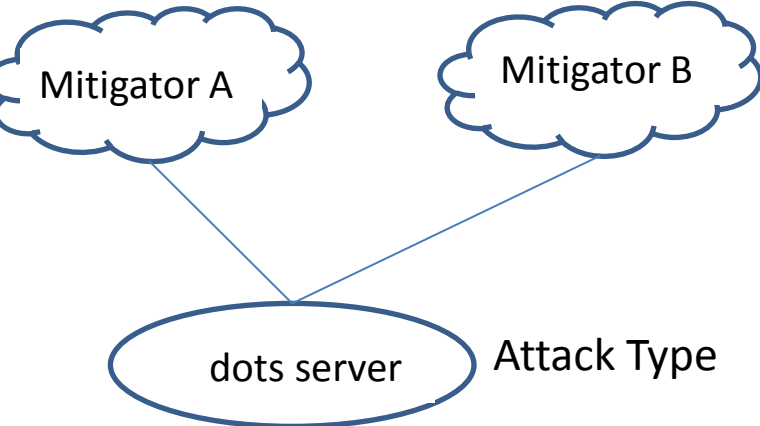


Fig.1 Mixed attack

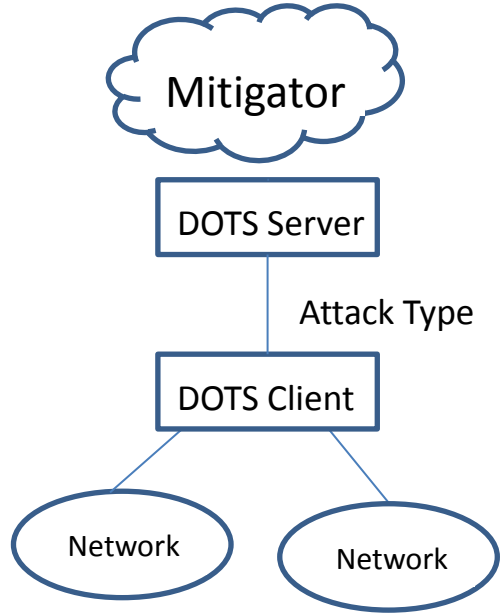


Fig.2 direct mitigation

Benefits

- ◆ Mitigators can coordinate to mitigate attack flow.
- ◆ Shorten mitigation time.

Functions

- ◆ Verification the attack type
- ◆ Adjust detection strategy for different vendors
- ◆ Analysis of malicious reporting nodes
- ◆ Convenient management

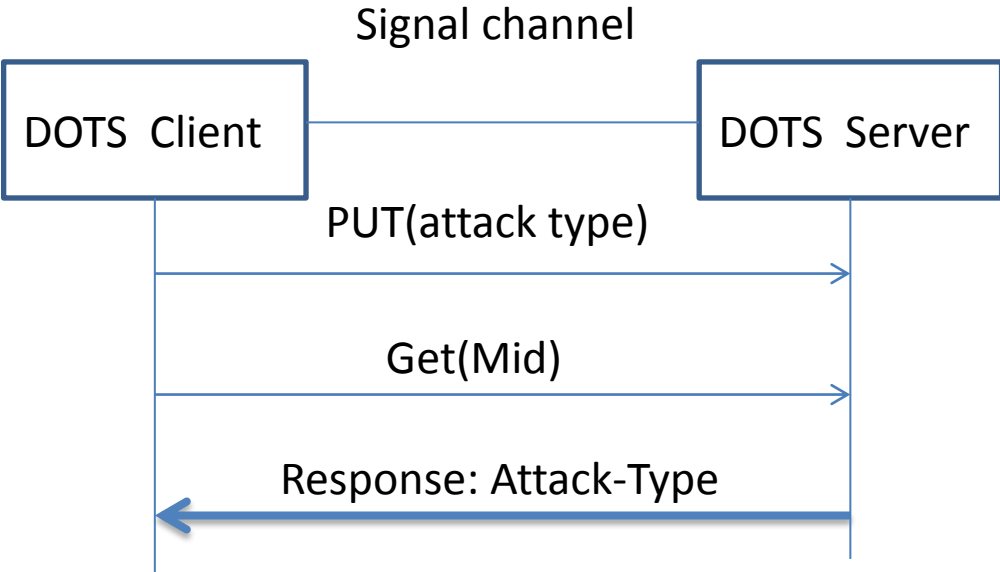
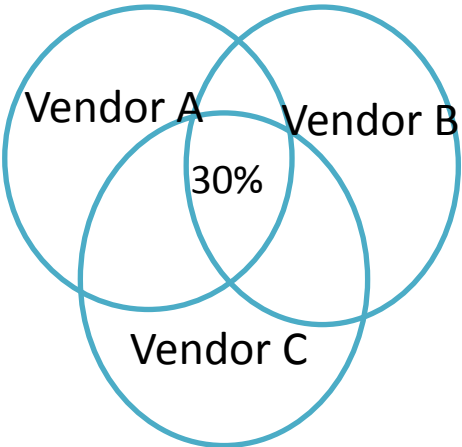


Diagram: Request with attack type



Agreement rate of attack type

Requirements for Unified naming format

- ◆ Equipment of different vendors cooperates each other easy to appear interactive chaos

Standard attack type definition(syntax)

[protocol level] [protocol name] [message name/operation name/port]

[attack methods feature description field 1] [attack methods feature description field 2] [attack methods describe the standard field]

Protocol level (mandatory)	Protocol name (mandatory)	message name/operation name/port (optional)	attack methods feature description field 1 (optional)	attack methods feature description field 2 (optional)	attack methods describe the standard field (mandatory)
Network_Layer	ICMP	---	---	---	Flood
Transport_Layer	TCP	SYN	---	---	Flood
Transport_Layer	UDP	Memcached	Reflection	Amplification	Flood
Application_Layer	HTTP	GET	---	---	Flood

DDoS attack name complete definition and abbreviation definition example

Attack name (complete)	Attack name (abbreviation)
Network_Layer ICMP Flood	ICMP Flood
Transport_Layer TCP SYN Flood	TCP SYN Flood
Transport_Layer UDP Memcached Reflection Amplification Flood	UDP Memcached Flood
Application_Layer HTTP GET Flood	HTTP GET Flood

Next steps:

1. Comments
2. Use case valuable?
3. Questions?