中国移动
China Mobile

Attack informations

1.draft-chen-dots-attack-information-00

Meiling Chen, Li Su, Jin Peng

China Mobile Research Institute

July 2019

Goal: add parameters in the mitigation request to meet requirements

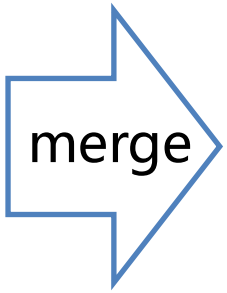
Last meeting

draft-chen-dots-attack-bandwidth-expansion-01

- add **attack-andwidth** in mitigation request

draft-meiling-dots-attack-type-expansion-00

- add **attack-type** in mitigation request
- unify the attack-type definition

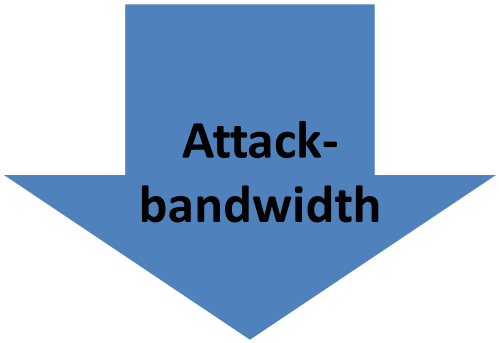


ietf105

draft-chen-dots-attack-informations-00

- add parameters:
  Attack-bandwidth
  Attack-type
  Attack-src-ip-number
  Target-attack-type-threshold
- unify the attack-type definition

Use of parameters: mitigation

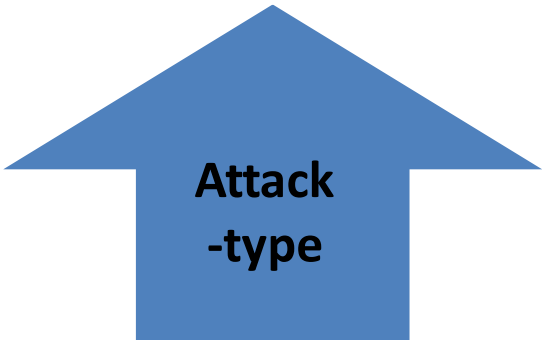


Attack traffic disposition:

- Clean device selection
- Redirection path selection
- Offload extreme attack traffic

Co-processing:

- Consistent detection type and cleaning interface, then co-processing ;
- Detection alarm is based on the attack type;



Attack Type A

Fig.1

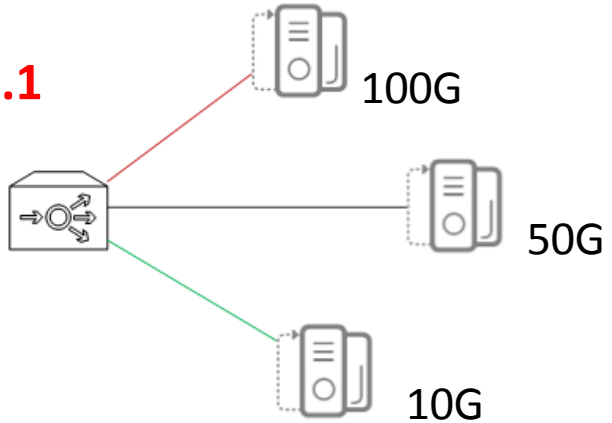
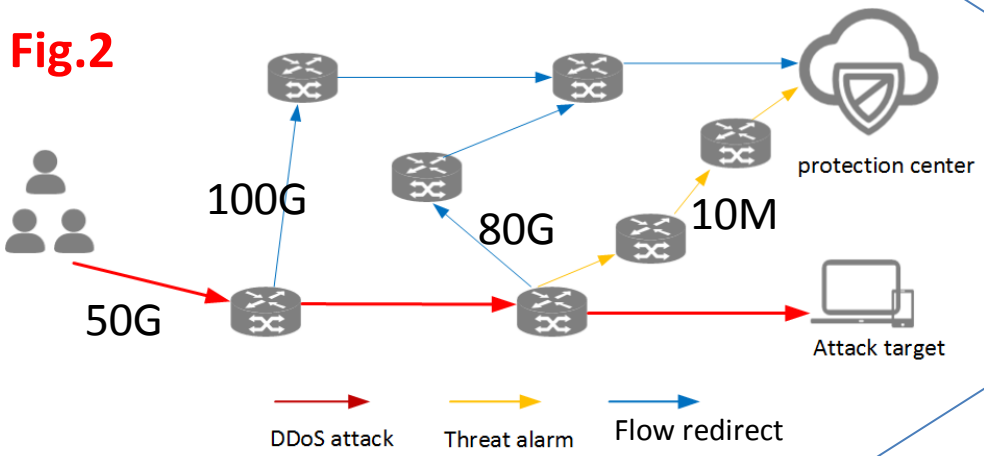
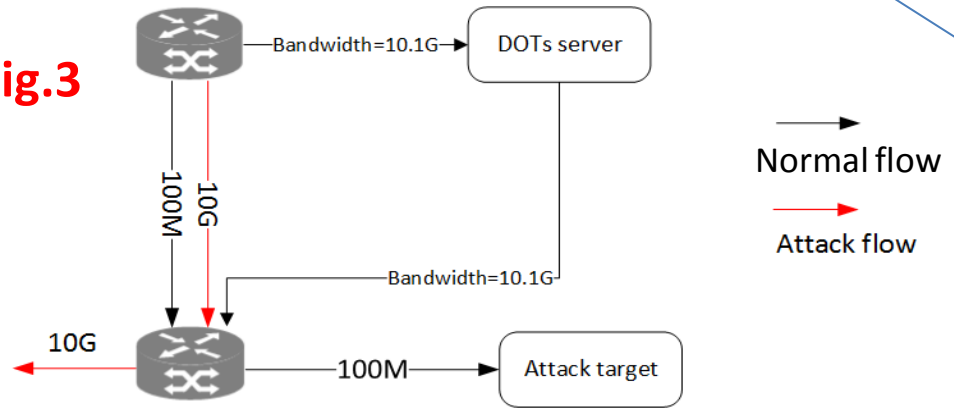


Fig.2



Attack-bandwidth

Fig.3



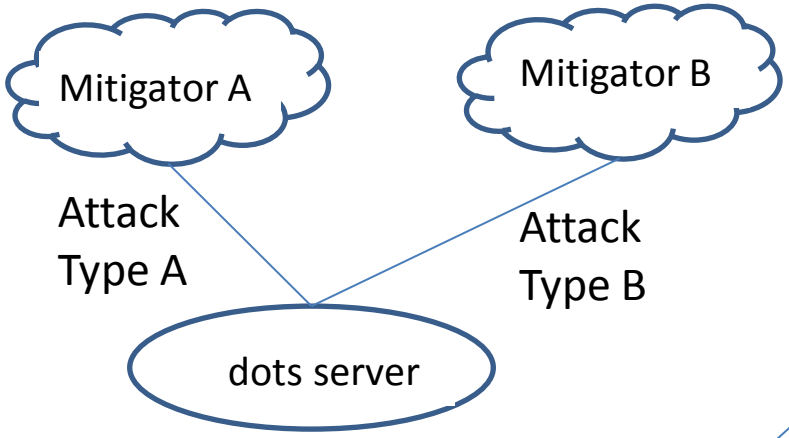


Fig.1 Mixed attack

Attack type

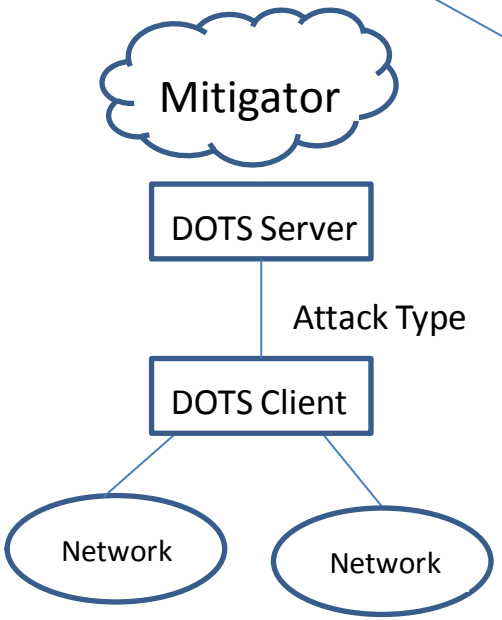


Fig.2 direct mitigation

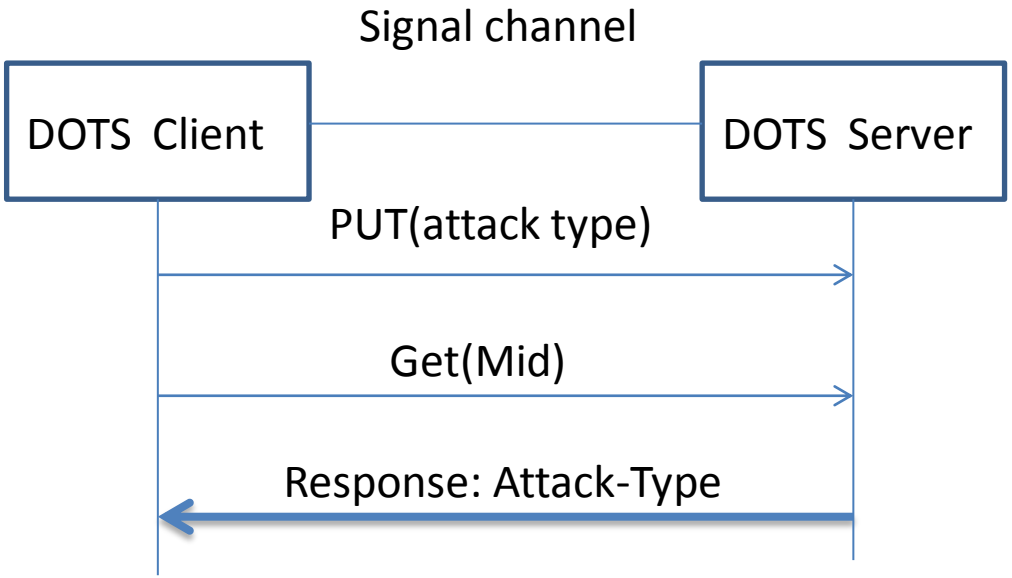
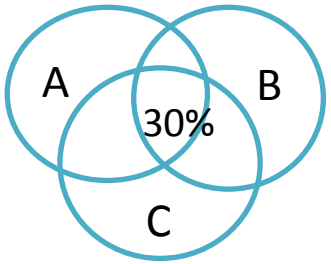


Diagram: Request with attack type

Standard attack type definition(syntax)

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

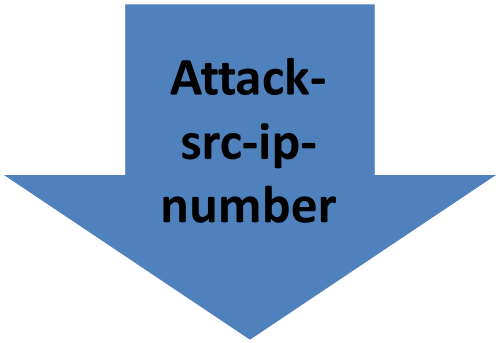
Problem



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

Use of parameters: adjust alarm baseline



Assess attack size：

- Distributed attacks each attack source attack traffic size is similar；
- Reporting all attack source IPs will overload the packet;

Adjust the attack warning threshold：

1、 Reduce false alarms

Next steps:

1. Comments
2. Questions?