Co-operative DDoS Mitigation

draft-reddy-dots-transport-01

Nov 2015

IETF 94

Authors: T.Reddy, D.Wing, P.Patil, M.Geller, M.Boucadair, R.Moskowitz

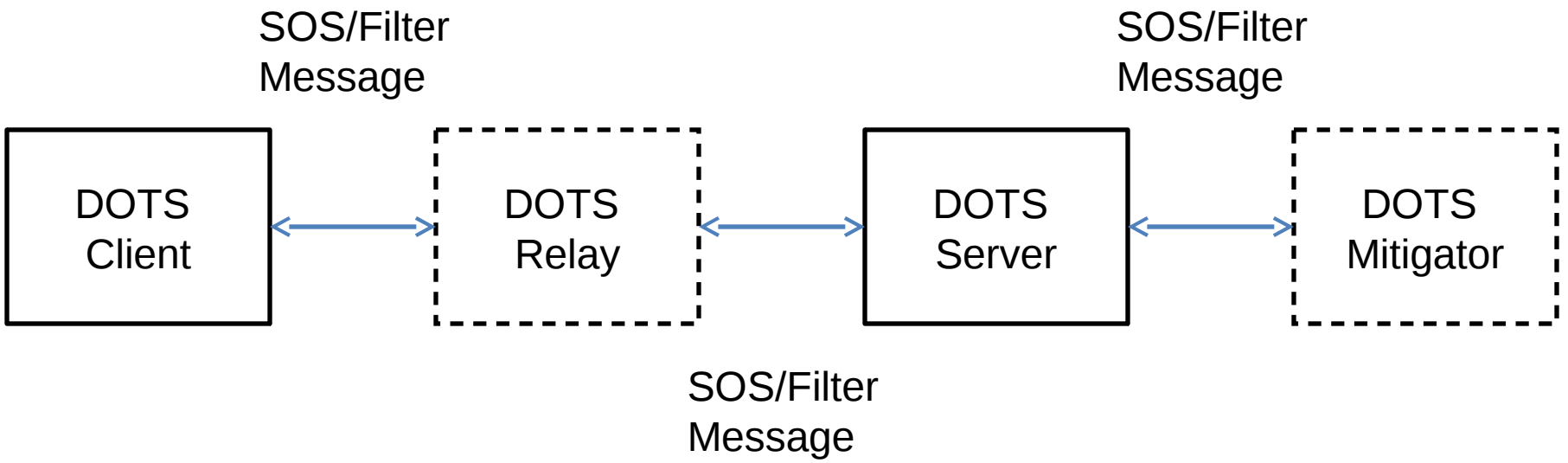
Presenter : Prashanth Patil

Messages:
DOTS client to DOTS server

- SOS
  - "I am getting DoS’d"

- Filter
  - "I am getting DoS'd by attacker <IP> over protocol <protocol> to my port <port> ….. "

Message Flow



SOS

- Emergency signal.
- Sub-MTU message size.

Filter

- Filtering Rules
  - Create, Read, Update, Delete.
- HTTP Request/Response model.

SOS : Transport Choice

- Minimal connection overhead.
- Ability to signal even as attack traffic saturates link.
- Security: Privacy, Integrity, Authentication and Replay protection.

- Proposed Transport: **DTLS over UDP**
  - Session resumption using previously used DTLS security association.

Filter: Transport Choice

- Potentially larger data exchanges.
- Exchange may be transactional, requiring reliable, in-order packet delivery.
- Security: Privacy, Integrity, Authentication and Replay protection.

- Proposed Transport: **HTTPS**

WG Feedback