Co-operative DDoS Mitigation

draft-reddy-dots-transport-03

April 2016

IETF 95

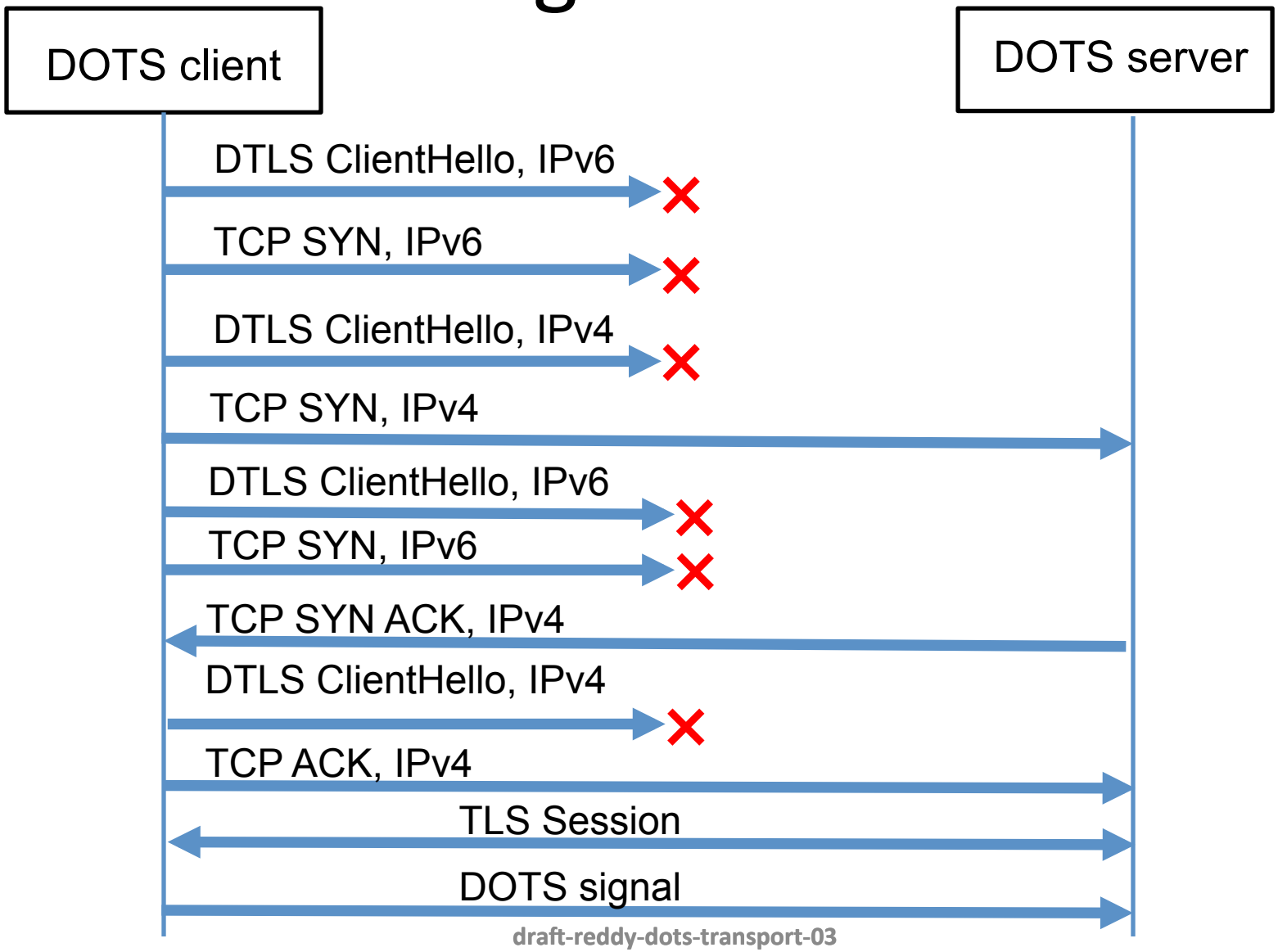
Authors: T. Reddy, D. Wing, P. Patil, M. Geller,
M. Boucadair, R. Moskowitz

Presenter : Dan Wing

Changes to draft

- Meets most of the requirements in draft-ietf-dots-requirements-01
  - Happy Eyeballs-like technique for DOTS Signal Channel (v6/v4, UDP/TCP)
  - DOTS Signal Channel, UDP/TCP
  - DOTS Data Channel, TCP
  - CoAP for lightweight communication
  - Performance considerations

Happy Eyeballs-like technique for DOTS Signal Channel

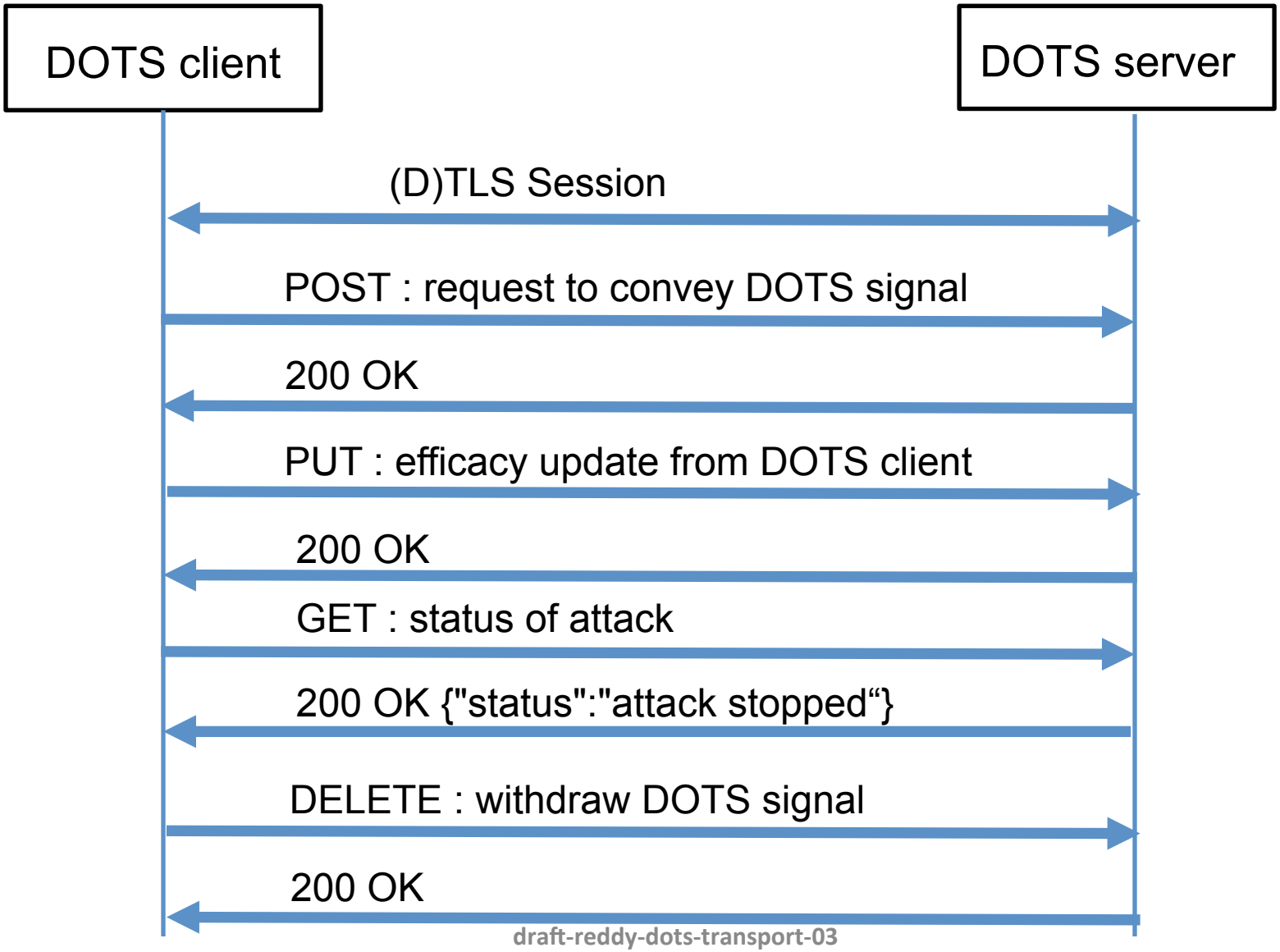


draft-reddy-dots-transport-03

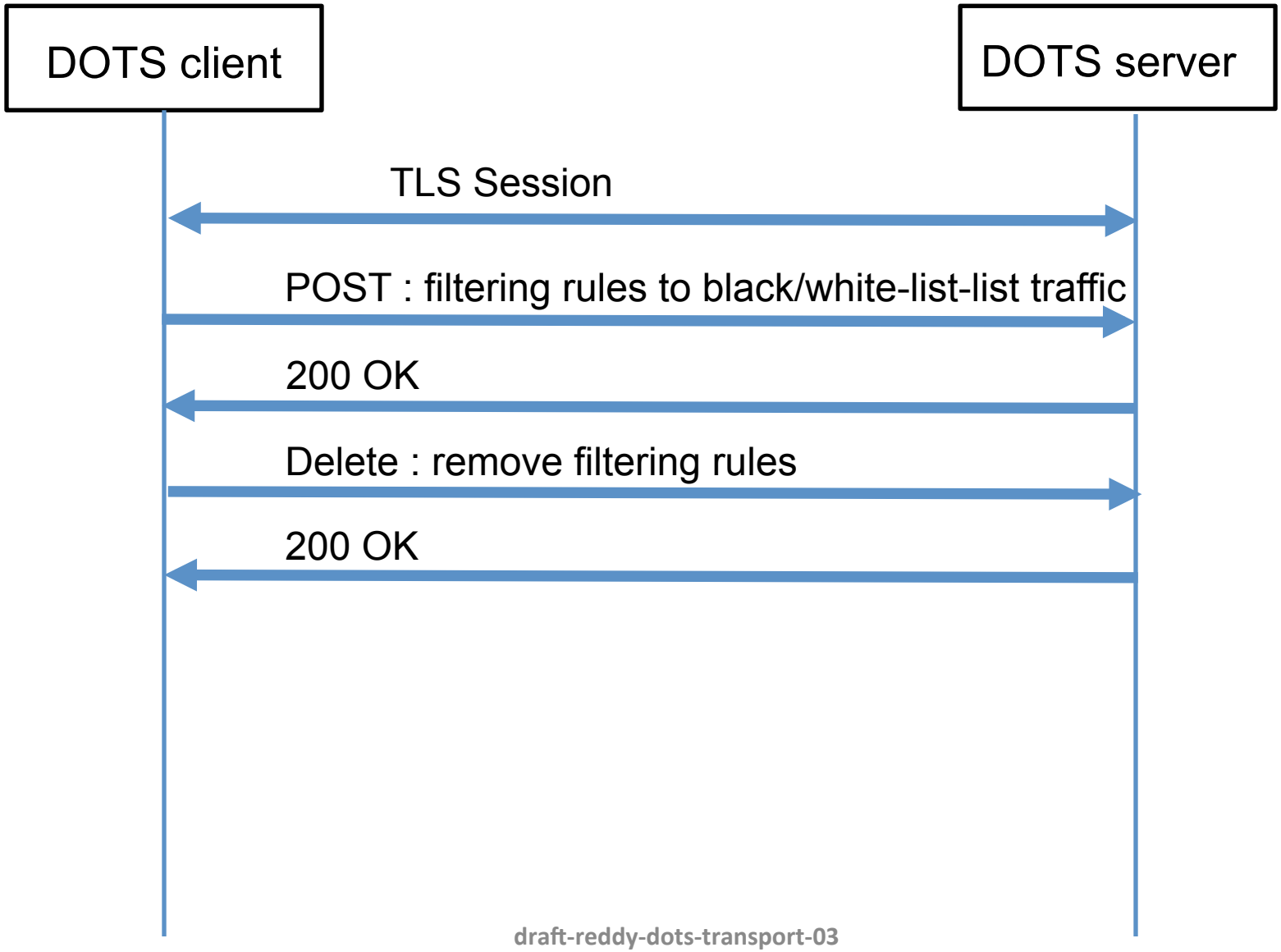
Happy Eyeballs for DOTS Signal Channel

- Order of preference (aligns with RFC6724)
  - IPv6 over DTLS over UDP
  - IPv6 over TLS over TCP
  - IPv4 over DTLS over UDP
  - IPv4 over TLS over TCP
- DNS lookup during peacetime.
  - DNS-SD will be aligned with requirements

DOTS signal channel



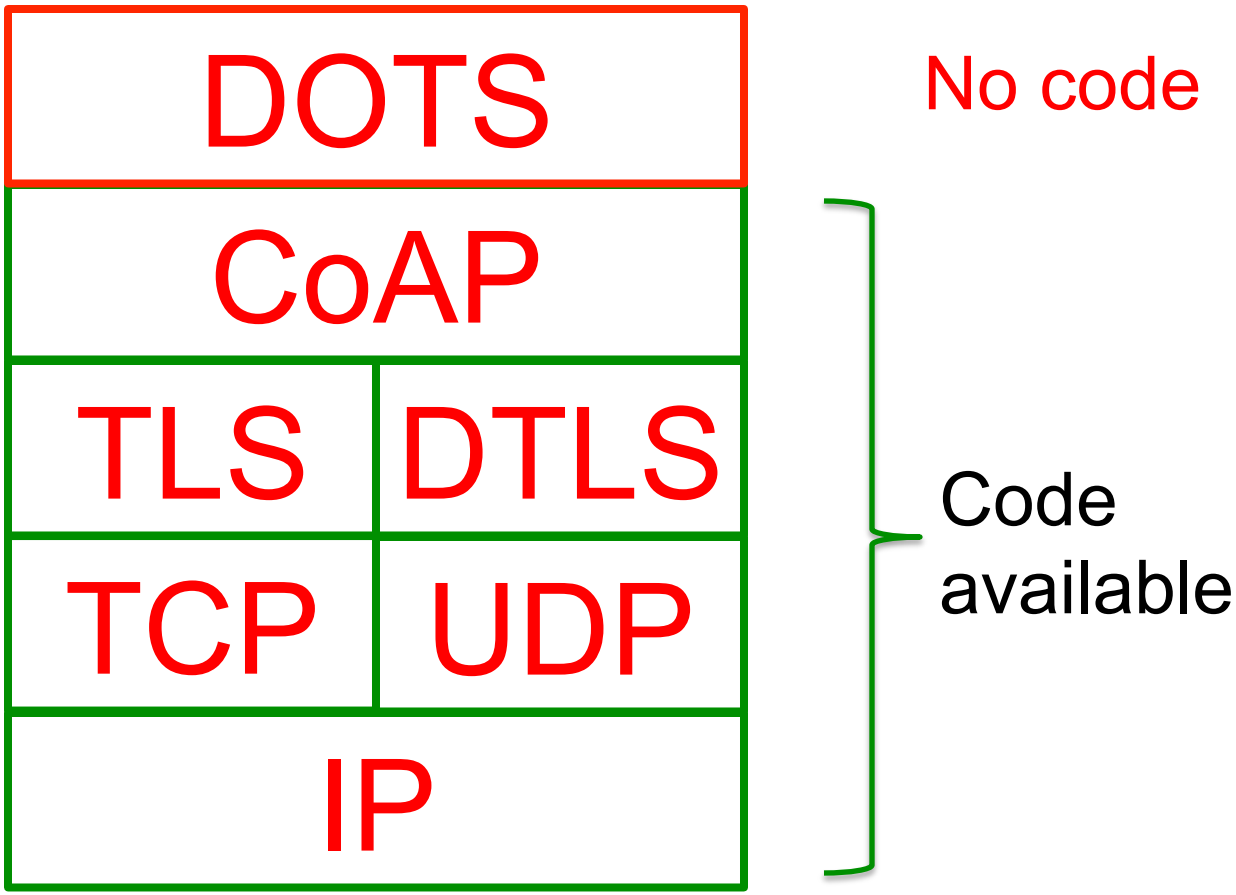
DOTS data channel



Why CoAP for DOTS ?

- Constrained Application Protocol (CoAP)
- CoAP runs over both DTLS over UDP (RFC7252) and TLS over TCP (draft-ietf-core-coap-tcp-tls).
- CoAP is designed according to the REST architecture.
- CoAP integrates with JSON, CBOR or any other data format.
- Asynchronous message exchanges.
- CoAP proxy.

Running Code



http://coap.technology/impls.html

Use Cases

Section	Description	Addressed?
3.1.1	Request mitigation, from mitigator	Yes
3.1.2	Request mitigation, from network infrastructure	Yes
3.1.3	Request mitigation, from telemetry system	Yes
3.1.4	Request mitigation, from targeted application	Yes
3.1.5	Request mitigation, from web portal	Yes
3.1.6	Request mitigation, from mobile device application	Yes
3.1.7	Unsuccessful mitigation request	Yes
3.2.1	DOTS client registration	Yes
3.2.2	Auto-provisioning of DDoS countermeasures	Yes
3.2.3	Attack notification to 3rd party	**NO**

Reference: draft-ietf-dots-use-cases-01

Performance considerations

- (D)TLS session resumption without server-side state [RFC5077].
- TLS False Start [I-D.ietf-tls-falsestart].
- Cached Information Extension [I-D.ietf-tls-cached-info].
- Raw public keys [RFC7250].
- (D)TLS Heartbeat.
- TCP FastOpen [RFC7413].

draft-reddy-dots-transport-03

- Consensus on Happy Eyeballs-like technique?
- Consensus on CoAP?