DOTS Requirements

Andrew Mortensen

November 2015

IETF 94

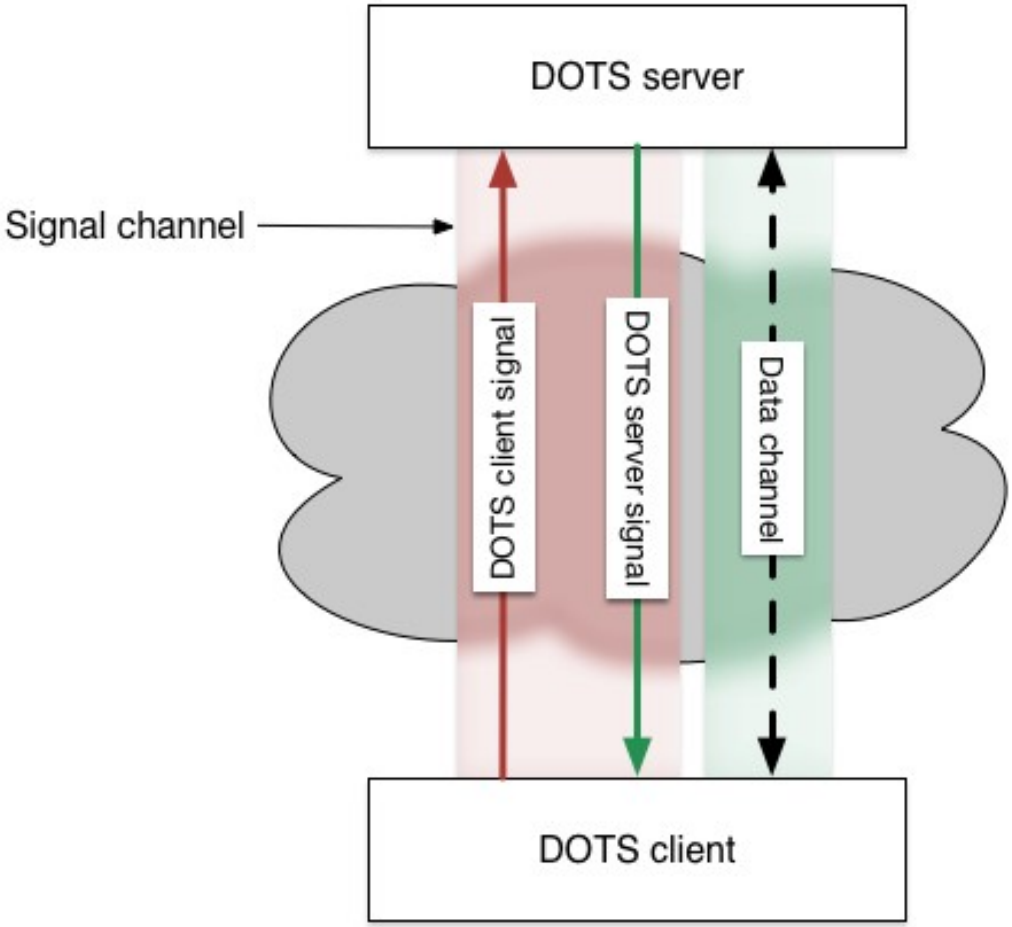
Overview

- DOTS requirements in context
- Establish common terminology (for now)
- General and operational requirements
- Data model TBD
- Status

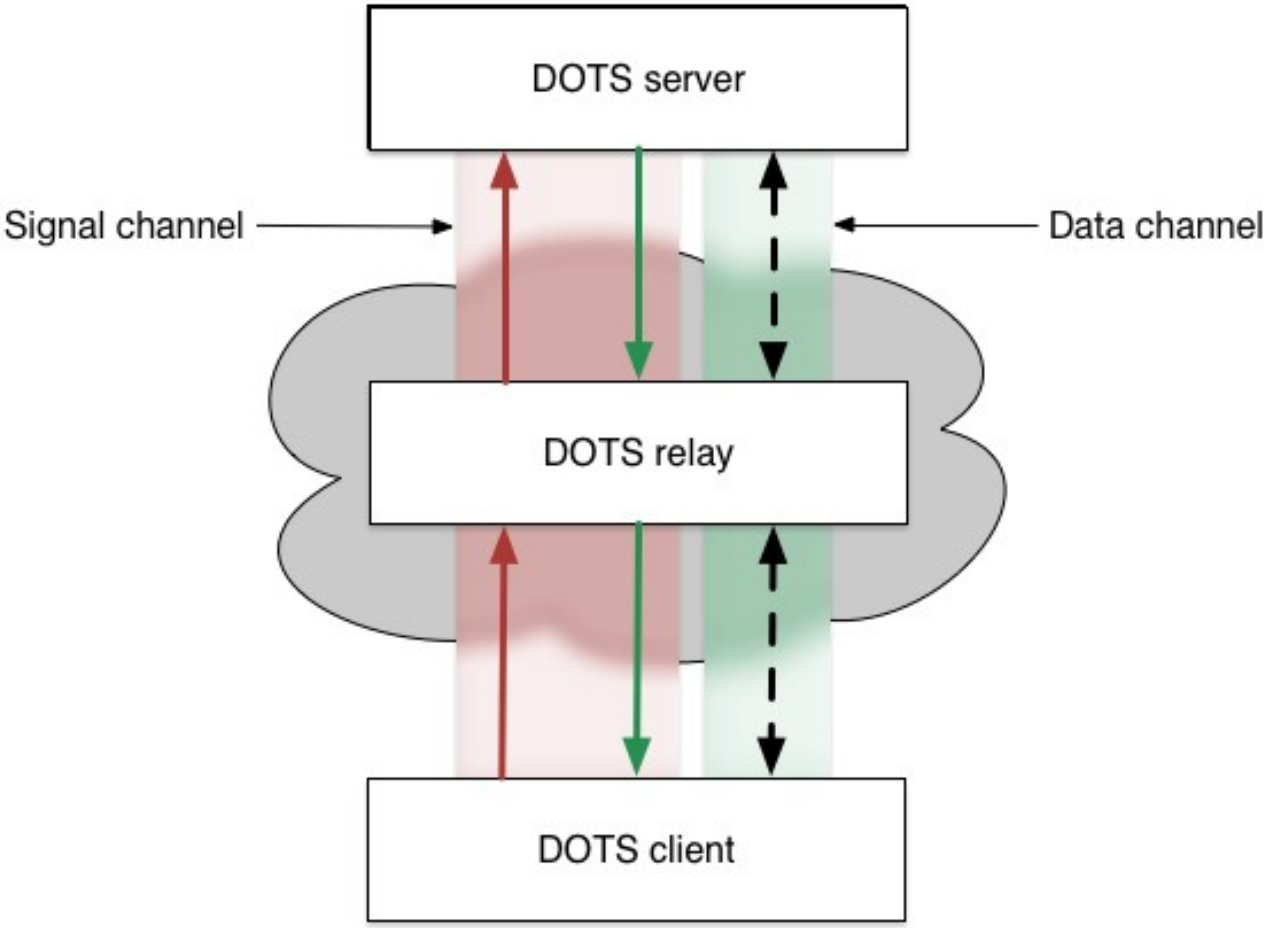
Selected terminology

- **DOTS agent** — DOTS-aware element
- **DOTS client** —agent requesting mitigation
- **DOTS server** — agent handling client signals
- **DOTS relay** — client/server mediating agent
- **DOTS signal** — message between DOTS agents
- **DOTS client signal** — message from DOTS client
- **DOTS server signal** — message from DOTS server
- **Signal channel** — DOTS signal transport layer
- **Data channel** — Bulk data transport layer

DOTS agents — client and



DOTS agents — relay



General Requirements

1. Interoperability
2. Extensibility
3. Resilience
4. Bidirectionality
5. Message size under MTU
6. Message integrity
7. Replay protection
8. Bulk data exchange

Interoperability and Extensibility

- Interoperability is fundamental to DOTS goals
- Extensibility acknowledges current solutions and looks ahead to changing needs

Protocol resilience and bidirectionality

- Protocol must continue operation in “hostile network conditions”
- Need for DOTS agents to signal, monitor peer health, provide feedback

General signal requirements

- Fit within MTU to avoid message loss incurred by possible failed fragment delivery
- Maintain integrity when transmitting signal across transit networks
- Replay protection to prevent protocol abuse

Bulk data exchange

- Supplement/bootstrap signaling relationship
- DOTS agent provisioning and discovery
- Configuration
- Characteristics suggest separate data channel desirable

Bulk data exchange

- Supplement/bootstrap signaling relationship
- DOTS agent provisioning and discovery
- Configuration
- Characteristics suggest separate data channel desirable

Operational requirements

1. Common transports
2. Mutual authentication
3. Session health monitoring
4. Mitigation capability opacity
5. Mitigation status feedback
6. Mitigation scope

Common transports

- Obvious requirement is obvious

Mutual authentication

- DOTS may affect network path or policy, agents must authenticate each other

Session health monitoring

- DOTS agents must be able to detect signal fidelity, peer availability
- Support protocol resilience and bidirectionality

Mitigation capability opacity

- Avoid assumptions about remote agents' defensive capabilities
- DOTS client signal indicates mitigation need and desired outcome: **advisory** signaling
- DOTS server signal describes action taken

Mitigation scope

- DOTS client signal indicates desired address space coverage
- DOTS client signal may further narrow scope using e.g. transports, targeted ports
- DOTS client may request adjusted scope during attack

Bulk data channel requirements

1. Reliable transport
2. Data privacy and integrity
3. Mutual authentication
4. Black- and whitelist management

Data channel transport

1. Reliable transport
2. Data privacy and integrity
3. Mutual authentication
4. Black- and whitelist management

Data model requirements

1. TODO

Status

- Initial draft published 19 October 2015
- Very little WG feedback so far
- Please send feedback on mailing list, or…
- Open github issues against requirements draft

Next Steps

- Align with and inform use cases
- Where does terminology belong?
- Incorporate feedback
- Inform and be informed by new protocol work

Questions?

- http://github.com/dotswg/dots-requirements