MAMI Management and Measurement Summit (M3S)

March 16, 2018

London

mami

measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

Welcome!

- Thanks for participating and thanks for presenting!

- How-to for WiFi access provided on paper!

- Agenda and participants list as well!

The MAMI Project

Measurement and Architecture for a Middleboxed Internet

measurement

of deployed middleboxes

experimentation

of use case applicability and deployability

architecture

for middlebox cooperation

- Strong interaction with relevant standards organizations for impact on deployment
- FIRE testbed (MONROE) for measurement as well as experimentation, especially on mobile broadband access networks
- Learn more at http://mami-project.eu/ and follow us on twitter **@mamiproject**

Scope and Goals

- Discussion about challenges in network management and measurement
  - Review existing techniques
  - Challenges that arise based on new protocols
  - Approaches to address these challenges

- Collect input and develop a common understanding
  - Publish white paper to provide a common basis for a broader discussion in the Internet community!

Chatham House Rules and White Paper

- Please let me know if it is okay to publish your slides after the meeting, or send me a publishable version
- We have note takers assigned for each session
  - Thanks to Tobias Bühler, Gorry Fairhurst, and Diego Lopez!
- White paper will be based on slides and notes!
  - We will ask for feedback and confirmation before we publish the white paper!
  - Let us know if you'd like to be involved early and help!

Dinner Reservation

- for 10-20 people at Mele e Pere, 6:30pm
- http://www.meleepere.co.uk

Today's Agenda

9:00 Welcome and Intro

9:15 Where we are? Overview of new technologies in the IETF (Mirja Kühlewind, ETH)

9:35 Related work items in IEEE, ETSI, ITU, and 3GPP (Arnaud Taddei, Symantec)

9:40 Impacts of Encryption (Gorry Fairhurst, University of Aberdeen)

10:00 Path Signals and Wire Image (Brian Trammell, ETH)

10:30 *Coffee Break*

11:00 **Session I: Monitoring** (chair: Brian Trammell, ETH)

12:30 *Lunch*

13:30 **Session II: Performance Enhancing Proxies** (chair: Thomas Fossati, Nokia)

15:00 *Coffee Break*

15:30 **Session III: DDoS Protection** (chair: Gorry Fairhurst, University of Aberdeen)

17:00 Wrap up and Conclusion

Session I: Monitoring

- Current monitoring practices (Al Morton, AT&T) - 5 minutes
- How we do Network Performance Monitoring (Pavel Minarik, Flowmon) - 10 minutes
- Use of TCP headers to monitor network health and customer experience (Chris Seal, HWEL - 3 Solutions) - 10 minutes
- Analyzing OTT video over QUIC (Craig Radcliffe, Netscout) - 15 minutes
- Distributed Security Operations Use Case (Roman Danyliw, CERT) - 10 minutes

Session II: Performance Enhancing Proxies

- Transport-split proxying for encrypted traffic (Thomas Fossati, Nokia) - 15 minutes
- Use case: HTTP proxy for network multicast support (Roni Even, Huawei) - 5 minutes
- Use-case differences for "Transport Only Intercept" vs "Application Layer Intercept“ (David Wells, Symantec) - 20 minutes

Session III: DDoS Protection

- Akamai's DDoS Protection (Aaron Falk, Akamai) - 15 minutes
- DDoS Open Threat Signaling (Roman Danyliw, CERT)
  - 10 minutes
- Challenges in building learning models when traffic is encrypted (Vijay Gurbani, Nokia) - 15 minutes

Where we are?
Overview of new technologies in the IETF

Mirja Kühlewind

M3S, March 16, 2018, London

mami

measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.The opinions expressed and arguments employed reflect only the authors' view. The European Commission is not responsible for any use that may be made of that information.

Supported by the Swiss State Secretariat for Education, Research and Innovation under contract number 15.0268. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

Overview
Encryption in the IETF

- TLS 1.3 and DTLS - improved end-to-end encryption
- QUIC - encrypted transport
- DoH - encrypted DNS over HTTPS
- ACME Star - Short term certificates to enable delegation

- Not covered: object security (e.g. jose, cose)

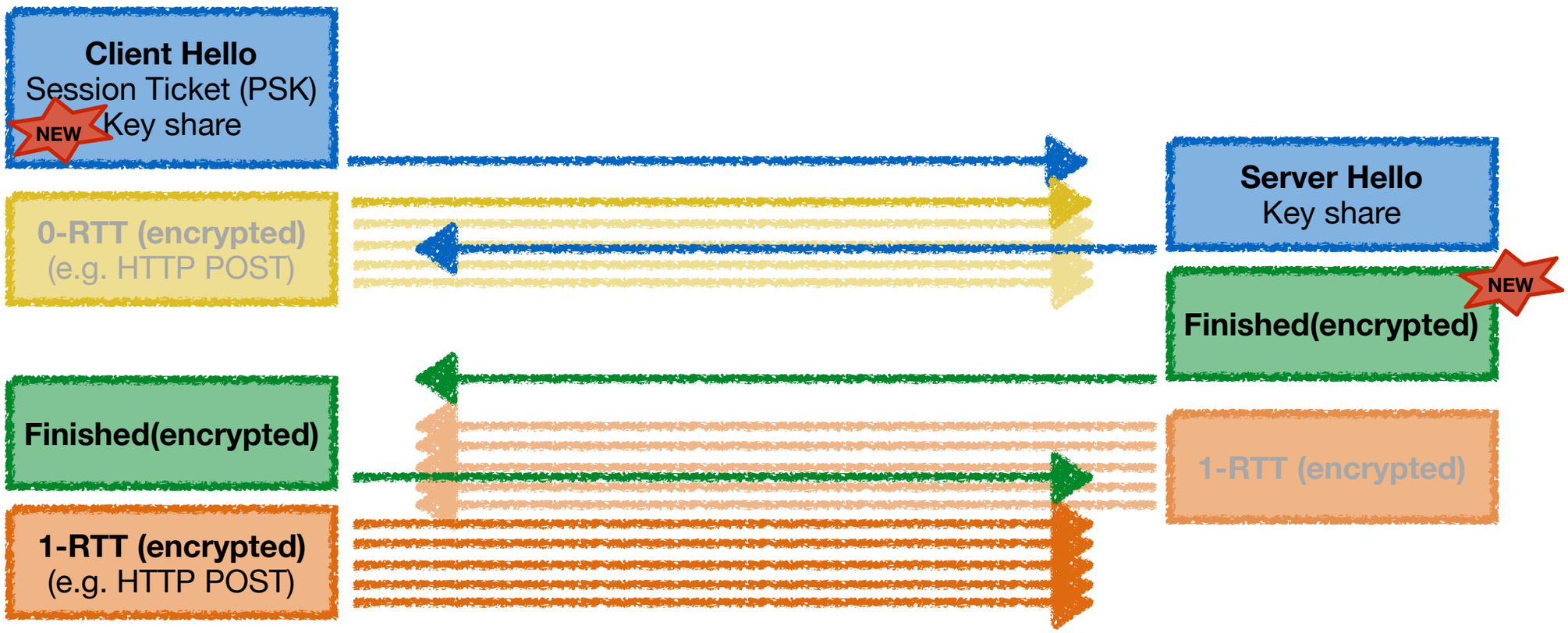
Why encryption?

1. Improvements in data and privacy protection (Snowden revelations)
   - "Encrypt it all!“
2. Reaction to ossification
   - Endpoint control about exposure to maintain evolution
   - Increase transparency on in-network handling
   - Middlebox traversal
   - Implementation correctness

TLS1.3

- draft-ietf-tls-tls13 (approved for publication by IESG)
- Use of Authenticated Encryption with Associated Data (AEAD)
- Perfect Forward Secrecy
  - Static RSA and Diffie-Hellman cipher suites removed
- All handshake messages after the ServerHello now encrypted
- New version negotiation mechanism based on extension due for (server and network) compatibility
- Session resumption in 0-RTT mode

TLS 1.3 Handshake (with session resumption)



- Session Tickets servers are stateless
  - 0-RTT PSK provides no Forward Secrecy if Session Ticket key is compromised
  - Replay attack requires idempotent data for 0-RTT

TLS1.3 Interception

- see also draft-camwinget-tls-use-cases

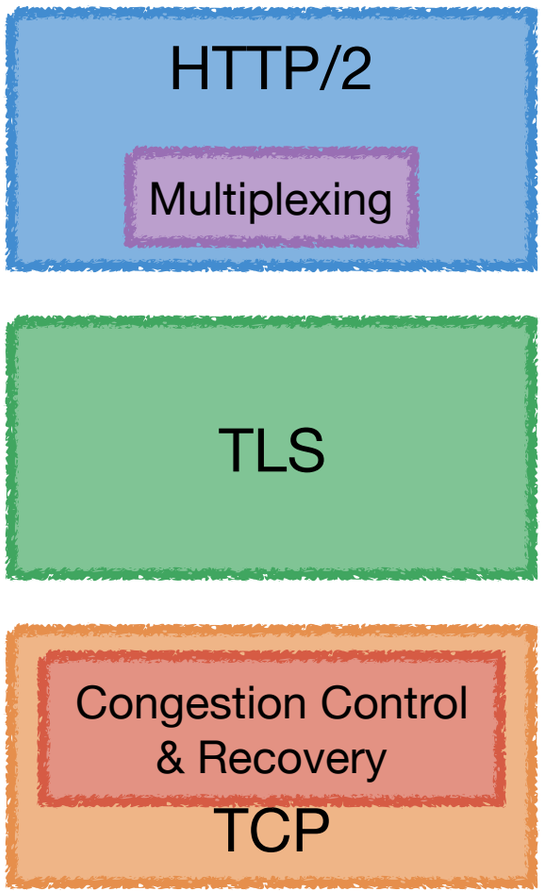
- Perfect Forward Secrecy
  - Keys cannot be shared apriori with middlebox
  - (see also draft-green-tls-static-dh-in-tls13)
- Encrypted Server Certificate
  - Server Identity hidden (as SNI might not match)
- Downgrade Protection
  - detects stripping of "supported_versions" extension

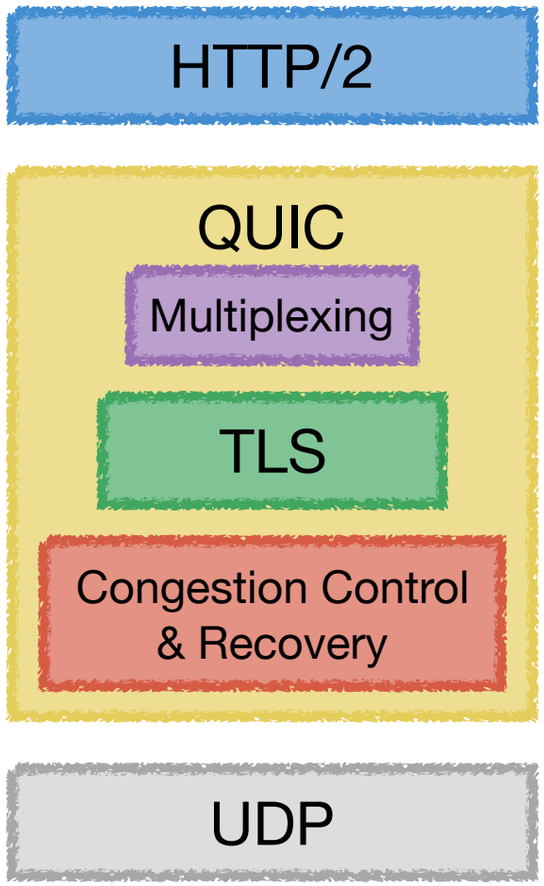
- Certificate pinning
  - see also draft-sheffer-tls-pinning-ticket

DTLS Connection ID

- draft-ietf-tls-dtls-connection-id
- Support for connection migration, e.g. NAT rebinding
  - provides additional information for security context selection when 5-tuple changes
- Extension is negotiated during handshake and connection ID is provided in TLS record layer
- Proposal for a generic DTLS Record Header (Wire Image) extension mechanism to make information more easily accessible
  - see draft-fossati-tls-ext-header

HTTP/2 over QUIC

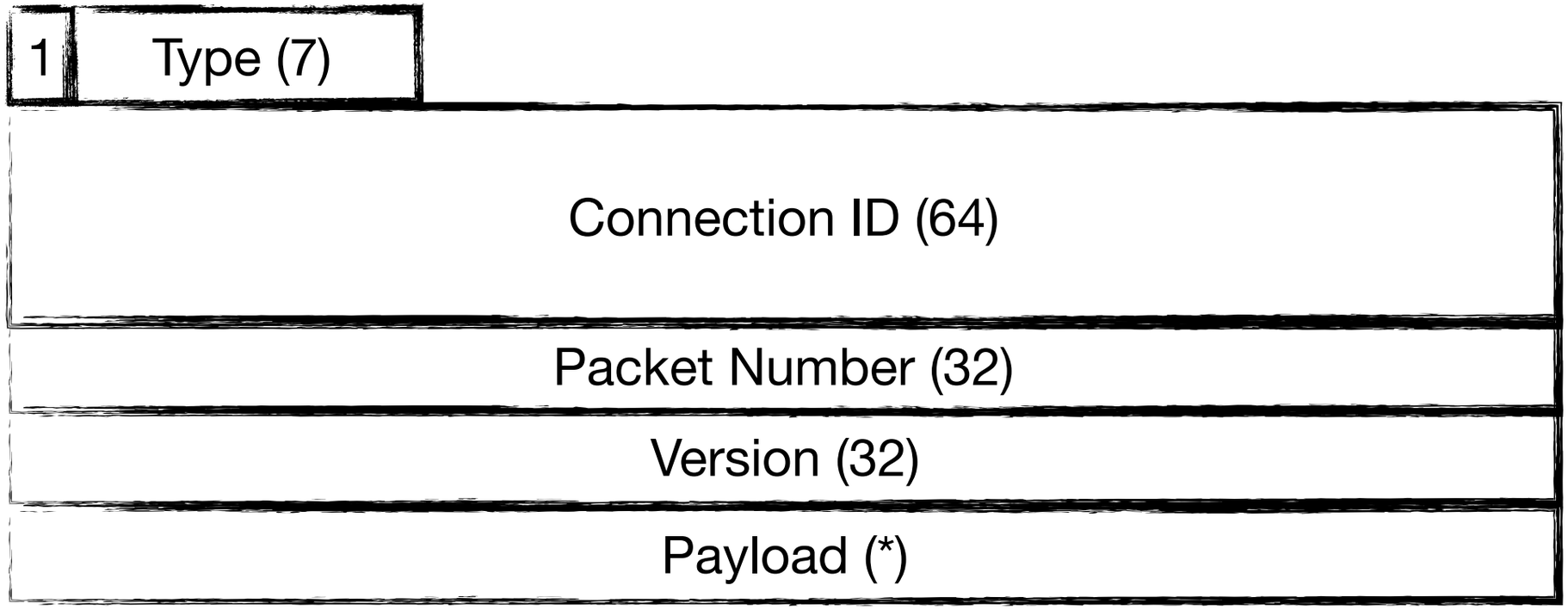




- Stream multiplexing avoids HoL of independent data resources
- Always authenticated and payload is fully encrypted

➡ **Stream & other control information (for e.g. recovery) is not visible to the network anymore!**

The QUIC wire image — Long header format (handshake & 0-RTT)



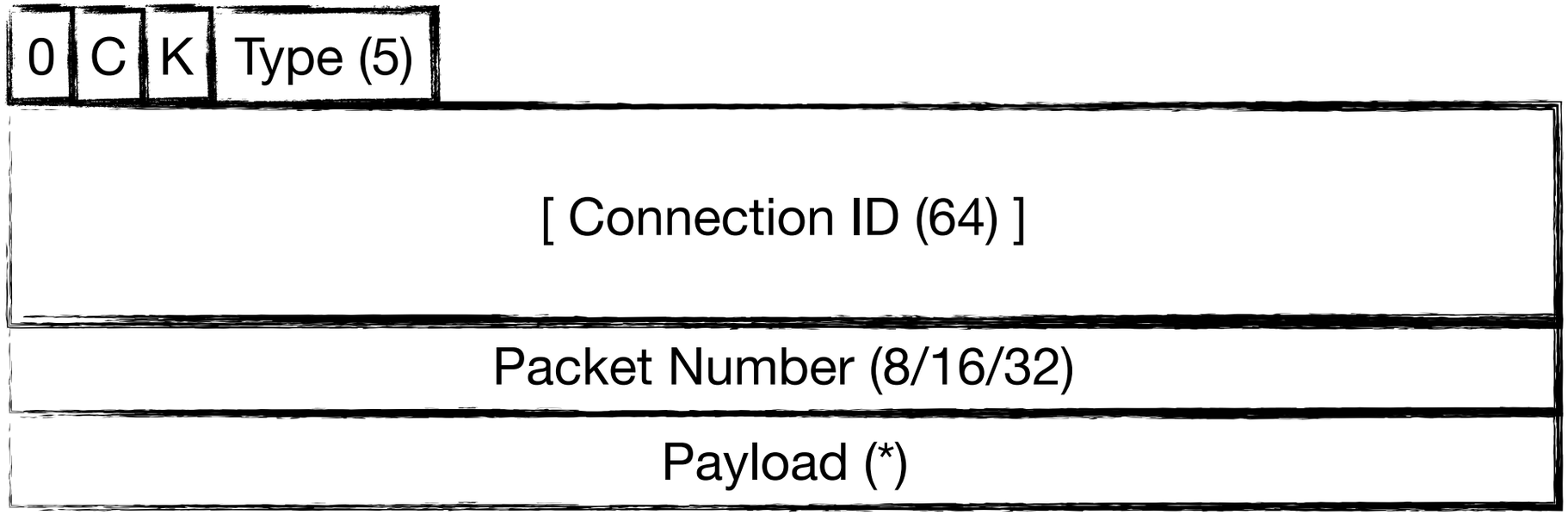
- Connection ID for migration and resilience to NAT rebinding
- Packet number is initiated to a random values and is unique within a connection
  - Packet Number also provides input to decryption

QUIC Long Header Types

Type	Name
0x7F	Initial
0x7E	Retry
0x7D	Handshake
0x7C	0-RTT **Protected**

- Cleartext packets for (Client) Initial, (Server Stateless(Retry, and (Server/Client) Handshake
- Encrypted payload for 0-RTT and short header 1-RTT data

The QUIC wire image — Short header format (only 1-RTT)



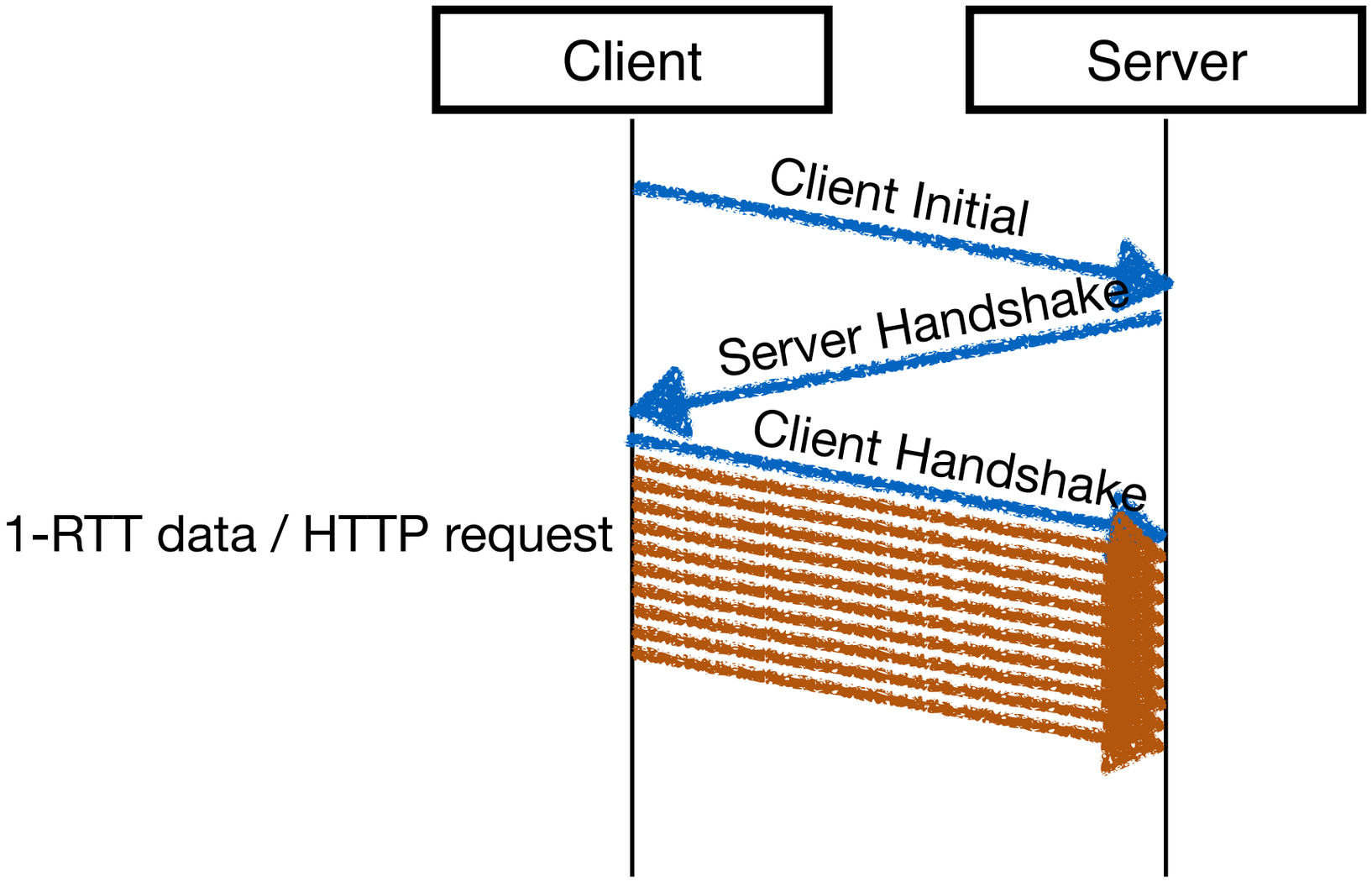
- Connection ID is optional as indicated by the C flag
- Packet Number length is indicated by the header type
- K bit indications key phase for decryption
- Payload is always encrypted

QUIC
Invariants

- Basically everything can change between QUIC version, except a few invariants that are needed for version negotiation!

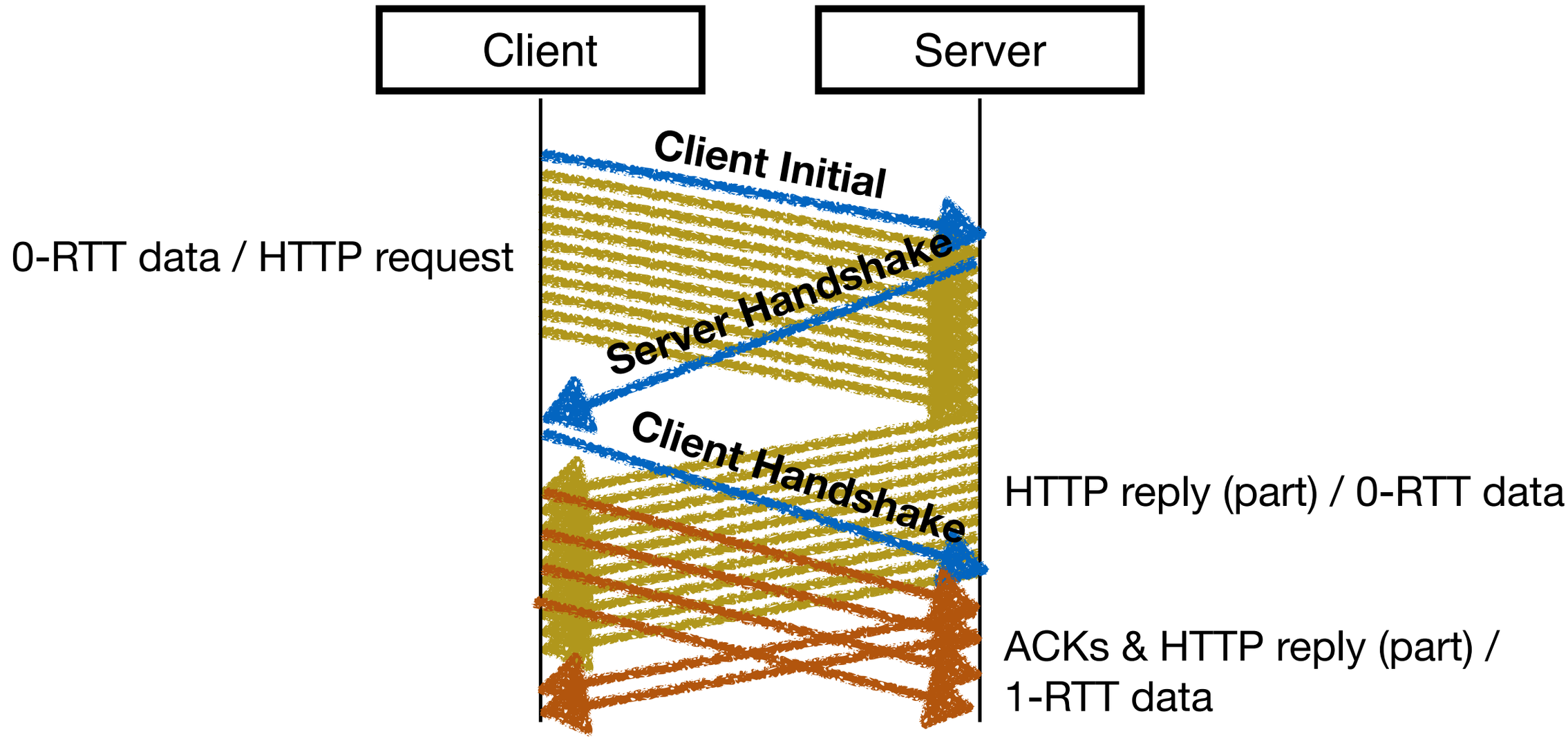
- Only to make version negotiation work, between different versions the following things need to remain the same:
  - the location and meaning of the header form flag,
  - the location and meaning of the Connection ID flag in the short header,
  - the location and size of the Connection ID field in both header forms,
  - the location and size and meaning of the Version field in long headers, and
  - the whole version negotiation packet.

QUIC Handshake



- Copy of the Client Initial and Server Cleartext are included in the encrypted part to verify content

QUIC Handshake — 0-RTT Session Resumption



- Client can send an initial window of data (10 packets) together with Client Initial

QUIC wire image — Measurements and Monitoring

- Packet Number can be utilized to measure **packet loss (or reordering) so far** (from the sender to the observation point)
  - ➡ Packet number is monotonously increasing
    - ➡ But gap can also be introduced by the sender
    - ➡ Retransmissions and ECN congestion indications are not visible to the path (to estimate whole-path congestion)
    - ➡ Packet might be encrypted as well

- **Round-Trip Time (RTT)** can be estimated during the handshake
  - ➡ No easy was to correlate two packets in both direction during the rest of the connection
  - ➡ Proposed spin-bit provides minimal explicit information to estimate one RTT sample per RTT

DNS Over HTTPS (doh)

- New working group: draft-ietf-doh-dns-over-https-03
- Confidentiality and connectivity between DNS clients and recursive resolvers (over port 443)
  - Prevents on-path network devices from interfering with DNS operation
- Also implementation in web browsers
  - Gives web applications access to DNS information
- "Filtering or inspection systems that rely on unsecured transport of DNS will not function in a DNS over HTTPS environment"

ACME
Short-Term, Automatically Renewed certificates (STAR)

- Protocol machinery to handle issuance of "short-term" certificates (with minutes-hours-days TTLs) in an automated fashion
  - Built on top of ACME / Let's Encrypt
- Allows Relying Parties to avoid checking revocation of End Entity certificates
- Better privacy & latency compared to existing revocation status protocols (CRL, OCSP)
- Building block for an efficient name-delegation protocol, for example one that exists between a Content Provider (identity owner), a CDN (delegate), and the end users
- Use cases: Delegation for CDNs, Distributed Network (Security) Functions in multiple data centers, Corporate networks

Use Case Overview

- Explicit exposure of information for network consumption (integrity protected)
- Network to endpoint signaling (PLUS)
- Split-transport proxying (higher layer is encrypted)
- Full visibility for content inspection (no modification)
- Content modification (requires trust relationship)

Backup

measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

Path Layer UDP Substrate (PLUS)

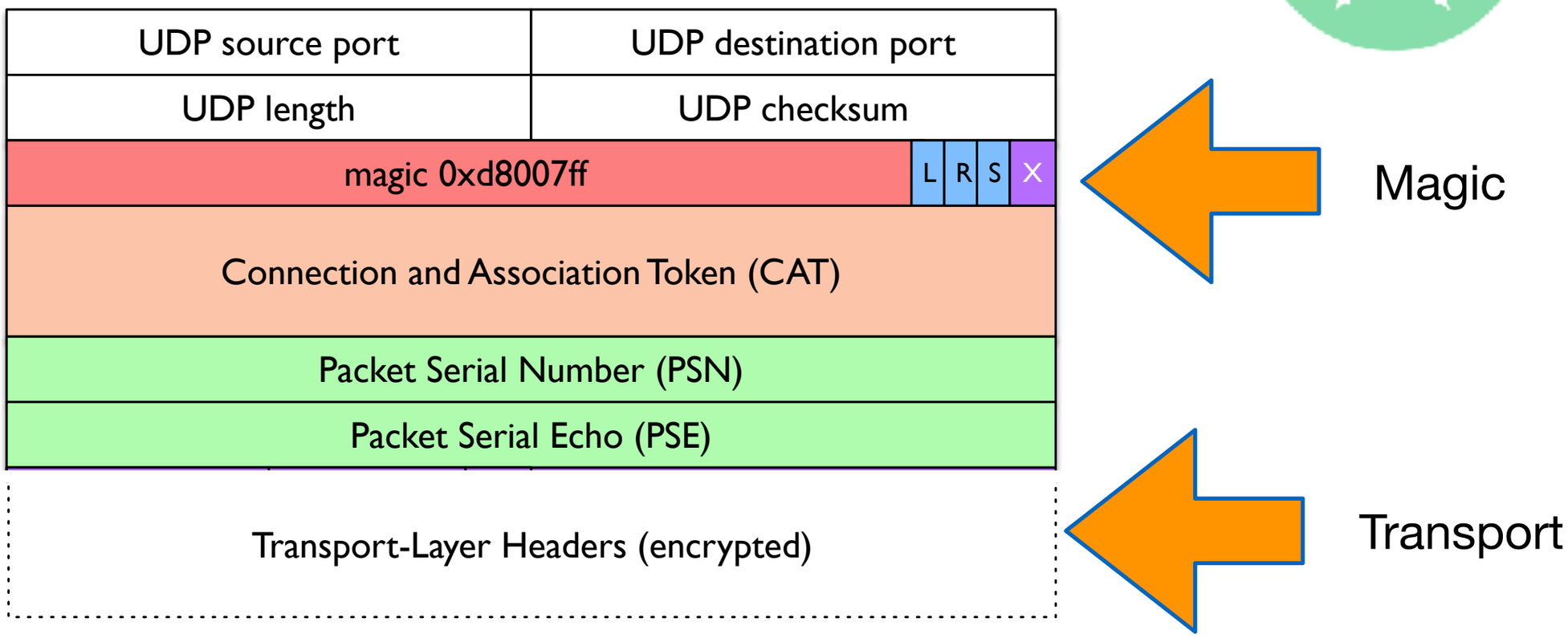
measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

PLUS Design Goals

- **Sender-to-path signaling:** An endpoint should be able to explicitly expose any signals used by on-path devices.
- **Path-to- receiver signaling:** An endpoint should be able to request signals from devices on the path.
- **End-to-end integrity protection:** An on-path device should not be able to forge, change, or remove a signal sent by an endpoint.
- **Integrity protection over a scratch space:** An endpoint controls signaling between endpoints and the path, or from one on-path device to another.
- Does not assume a**uthentication of signals from on-path devices:** Possible to request and receive signals from a previously unknown on-path device.
- **Robust to attack**: The mechanism should present no significant surface for amplification attacks.

PLUS Basic Header Format



Header on top of UDP identified by magic number

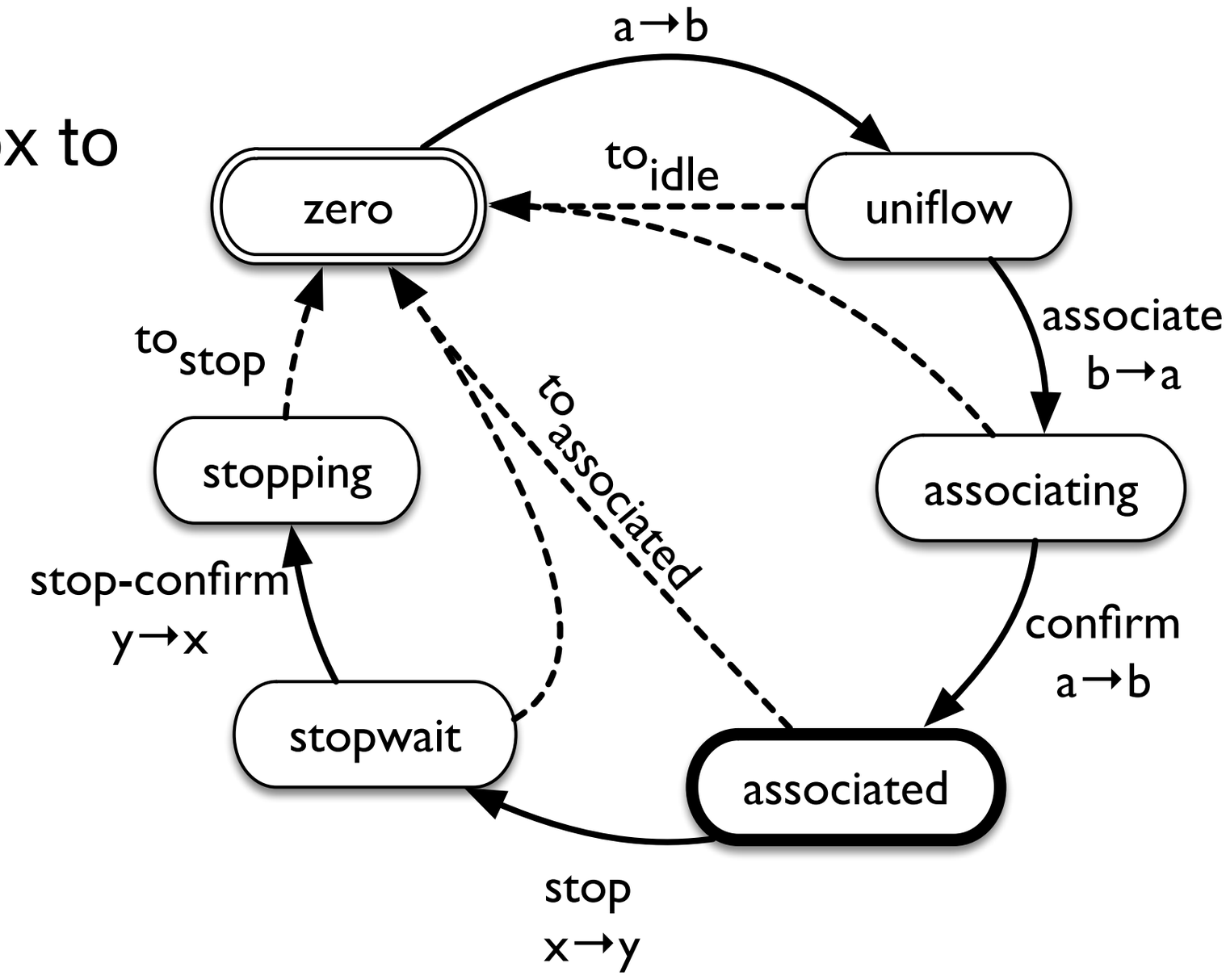
Basic and extended formats

L= Lola, R= May be reordered, S= Stop

Provides a common wire image for encrypted transports

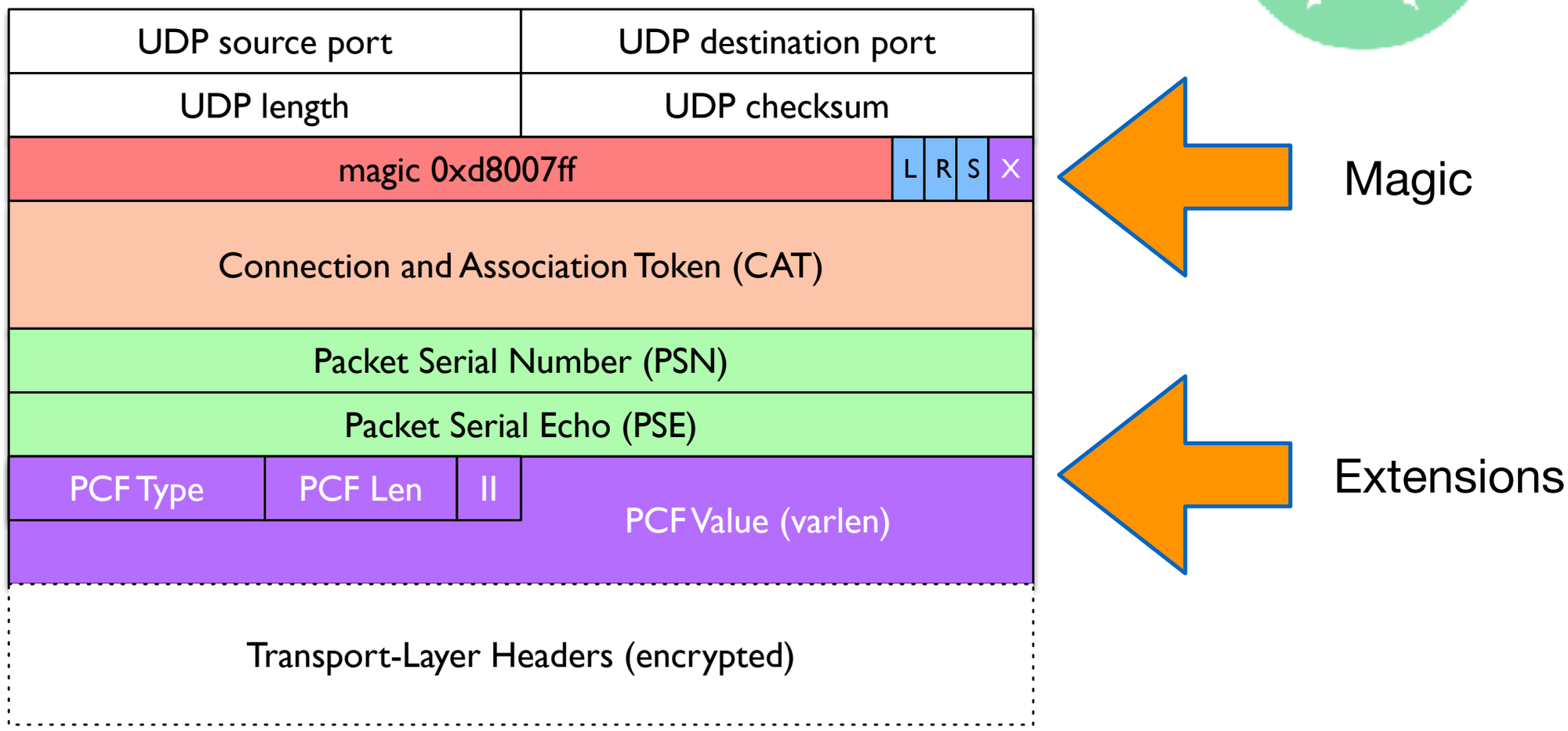
A transport-independent on-path state machine

- Enables a middlebox to track the flow state
- e.g. NAT/Firewall



[draft-trammell-plus-statefulness]

PLUS Extended Header Format



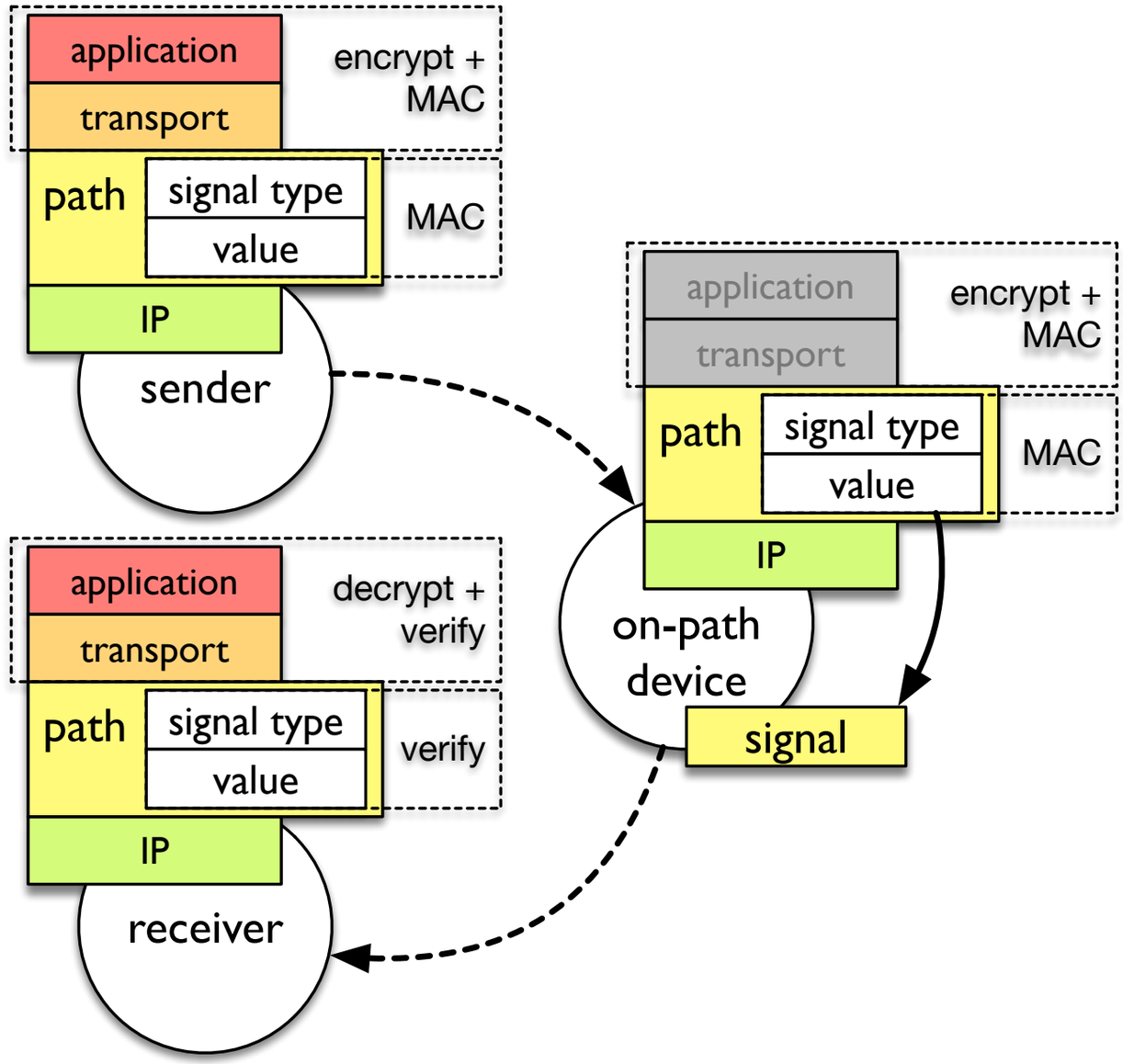
X=1

Each PLUS packet can carry only one PCF at a time

Sender decides which PCF is supported in a packet

Transport-independent in-band signaling: Sender to Path Signal

- Unencrypted signal
- Integrity protection
- Path can not verify
- Receiver may verify



L: LoLa

R: Reordering

S: Start of Session

PCF 1: Loss/Congestion Exposure

Transport-independent in-band signaling: Path to Receiver Signal

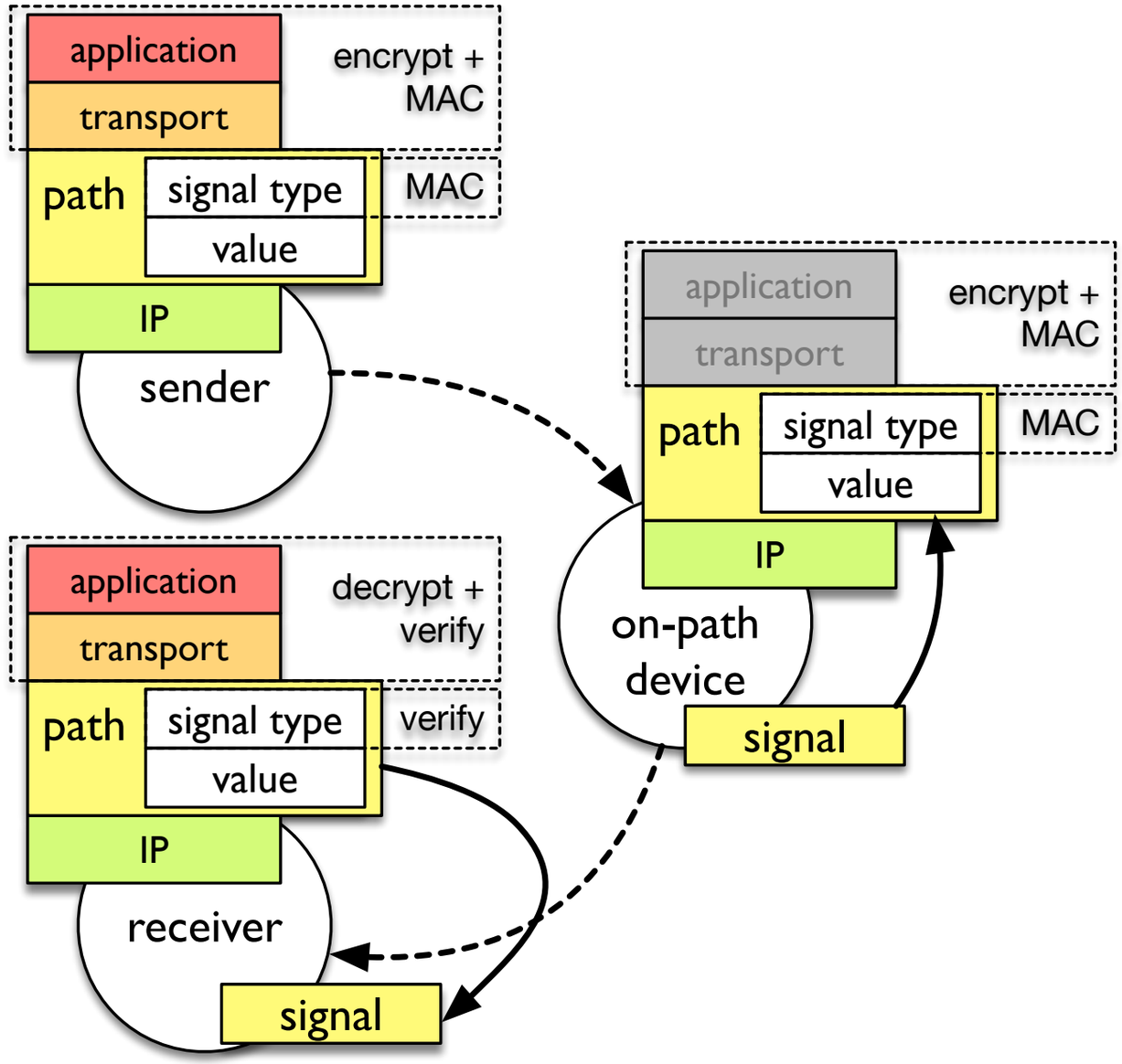
- Sender enables
- Unencrypted signal
- No integrity protection
- Use of info advisory

PCF 2: PMTU

PCF 3: Path tracing

MCP throughput guidance

…



IETF Documents

draft-trammell-spud-req

draft-trammell-plus-abstract-mech

draft-trammell-plus-statefulness

draft-trammell-plus-spec