

On The Passive Measurability of QUIC

Brian Trammell, ETH Zürich

RIPE 75 Plenary Lightning Talk
Dubai — 23 October 2017

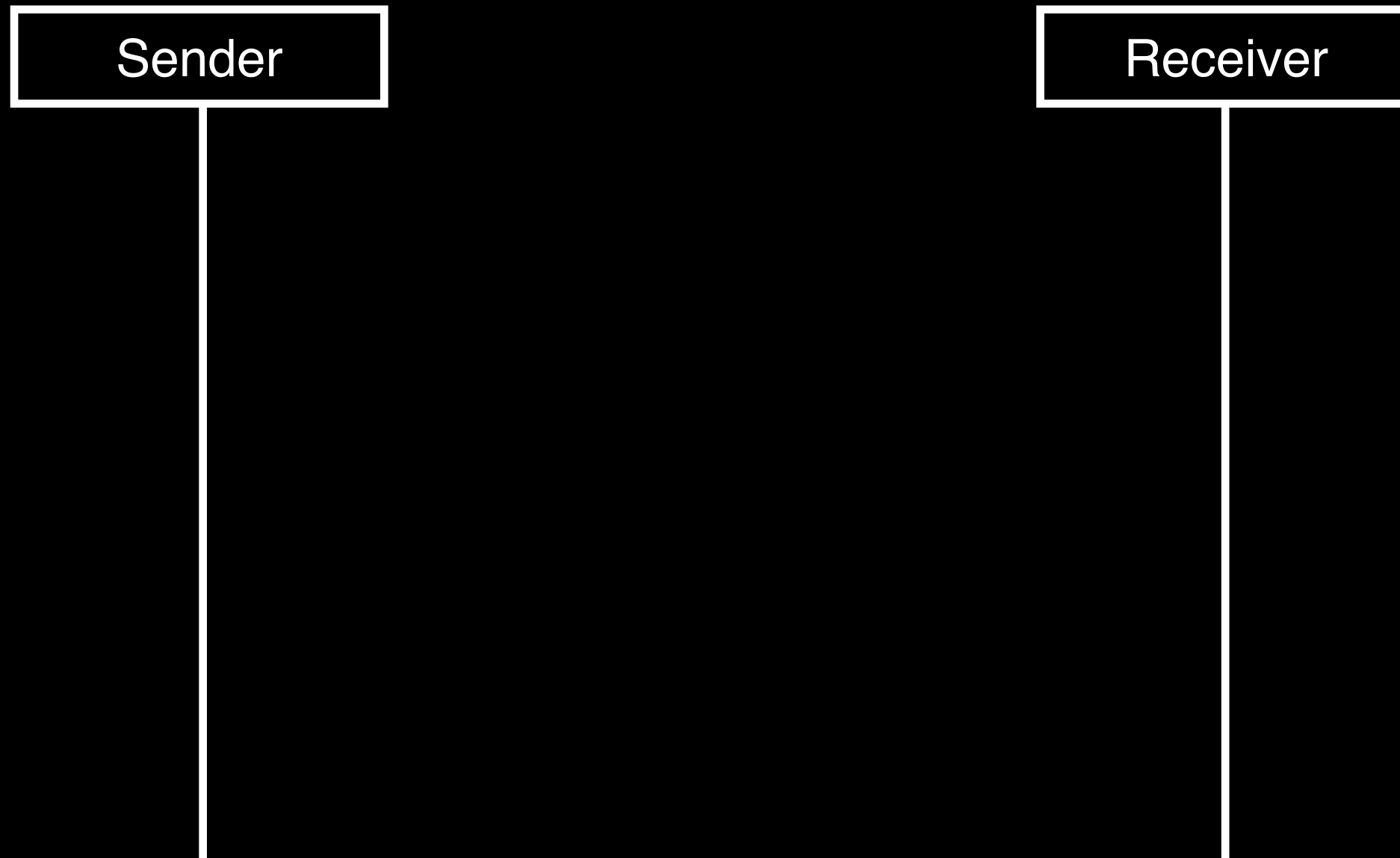
QUIC in review

- UDP-encapsulated transport protocol being standardized by the IETF.
 - Rolled out by Google since 2014:
35% of Google traffic, 7% of Internet traffic.
- Designed for deployability, evolvability, low-latency, and security.
- Initial focus on support for HTTP/2, but is a new, general-purpose Layer 4 protocol.

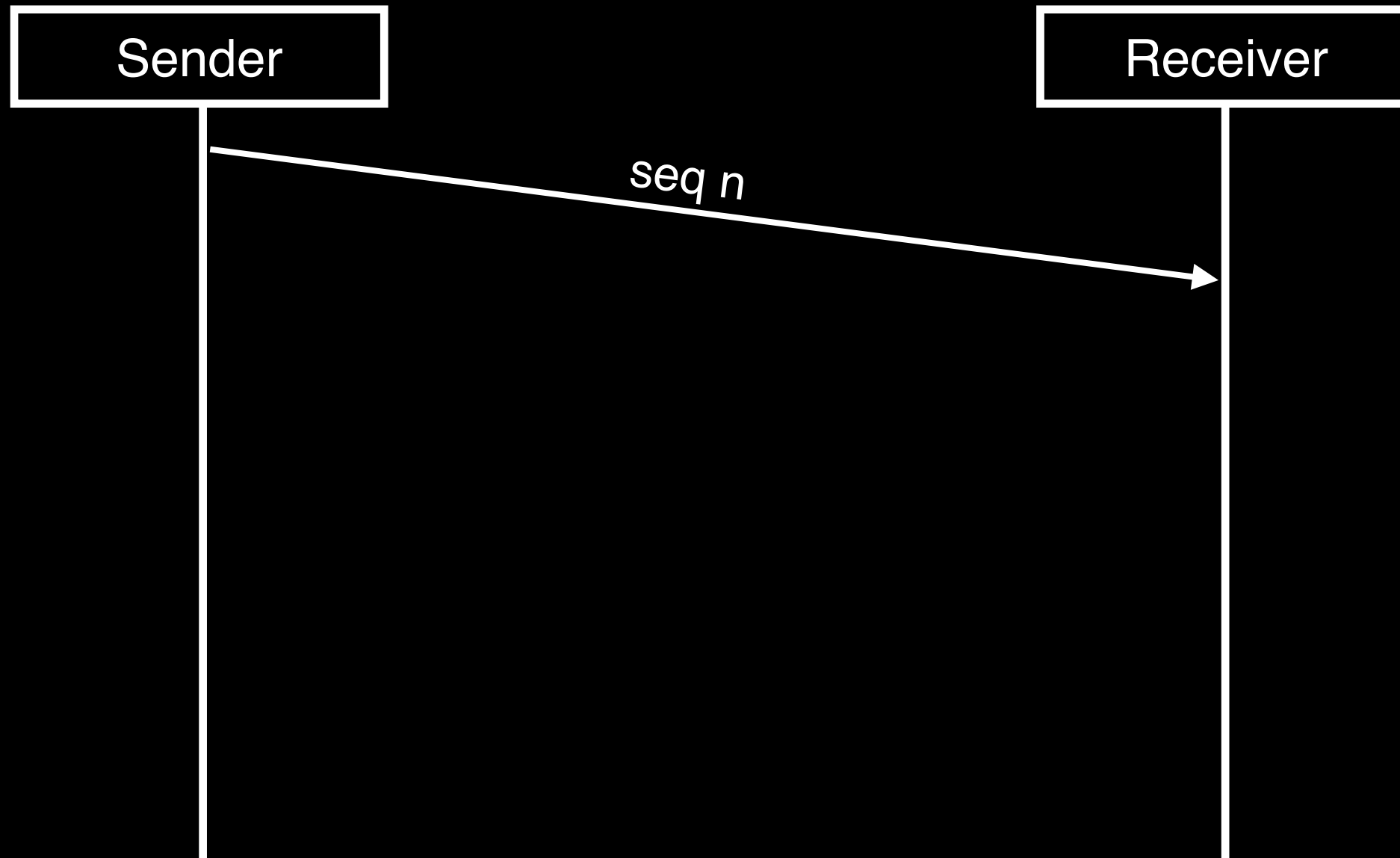
What's up and why should I care?

- TCP continuously radiates information about loss and RTT to passive observers along the path.
 - Loss and RTT measurement useful for intra- and inter-network health monitoring and troubleshooting.
 - Ruru is an excellent illustration of this.
- QUIC (as presently defined) doesn't do this.
 - QUIC traffic on your network is of limited use for passive measurement
 - ***Is this a problem?***

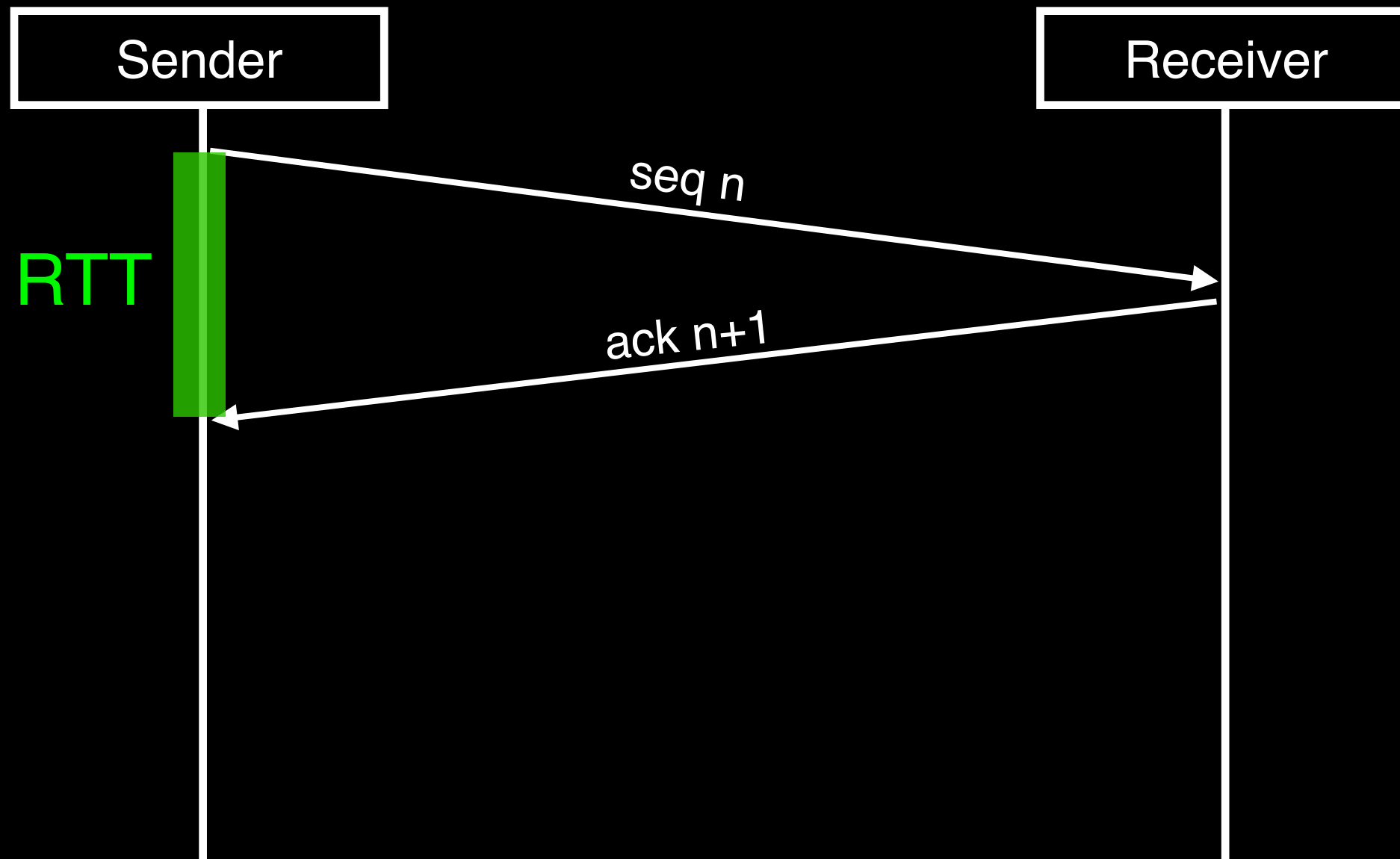
Back to TCP School: Passive RTT Measurement



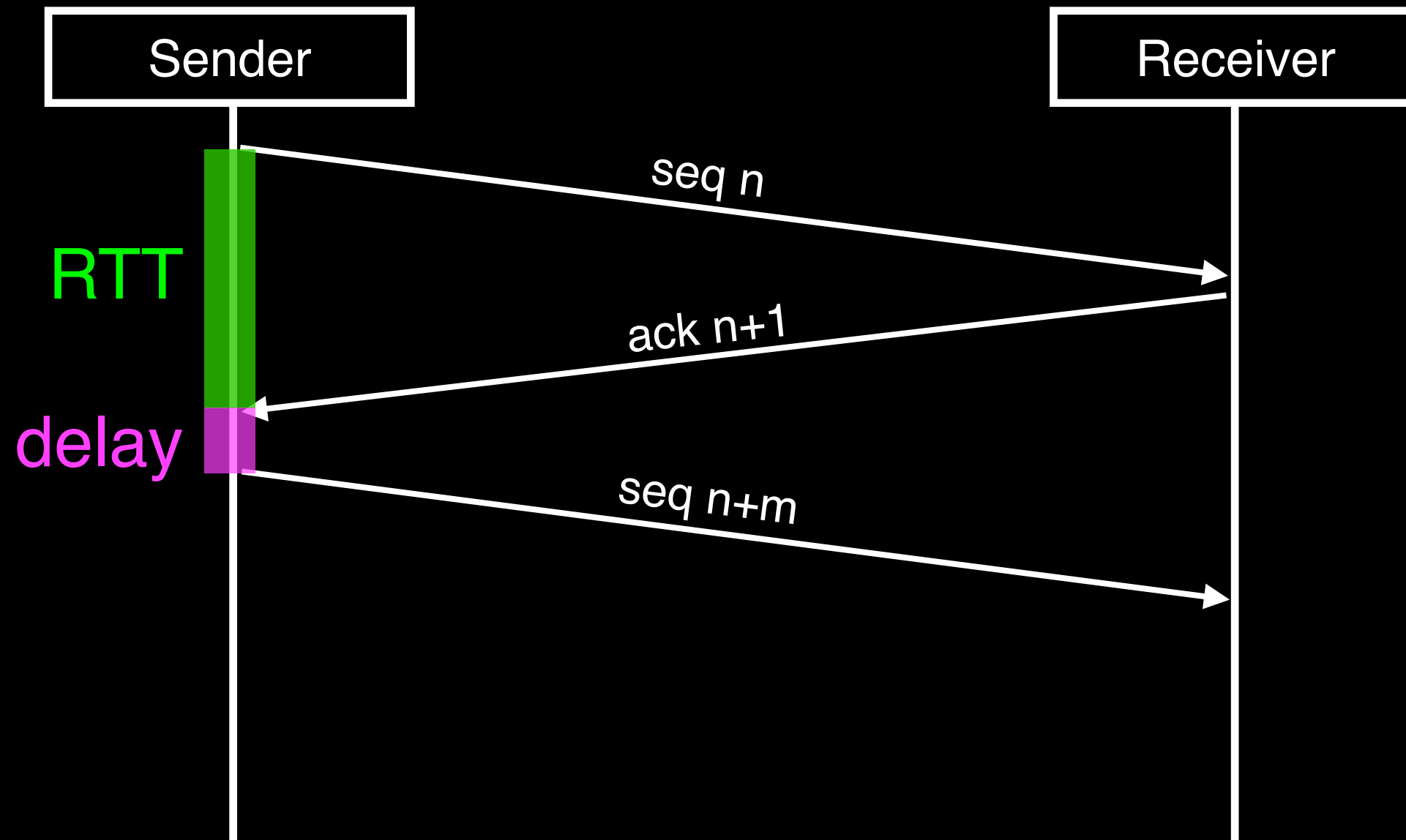
Back to TCP School: Passive RTT Measurement



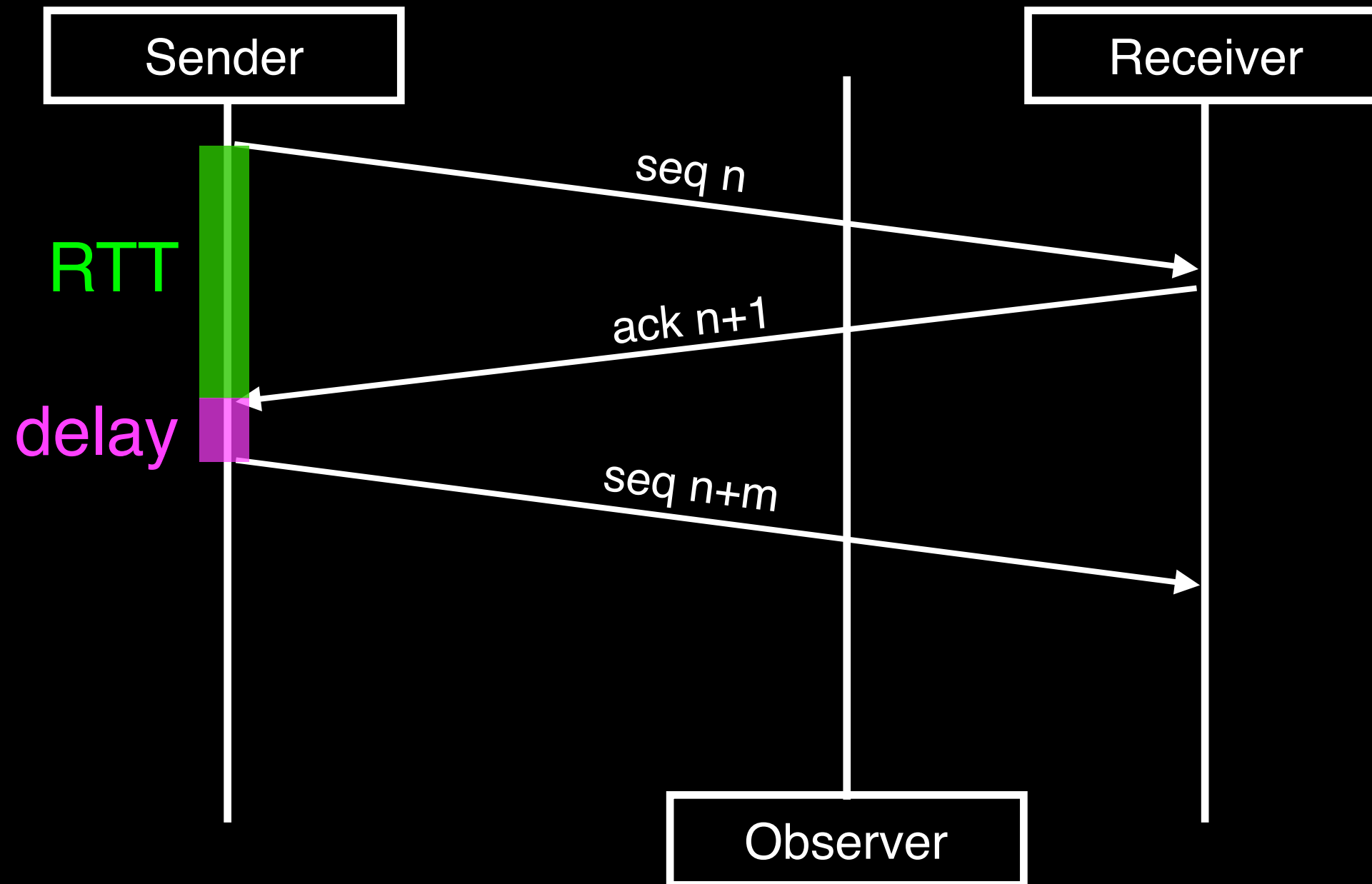
Back to TCP School: Passive RTT Measurement



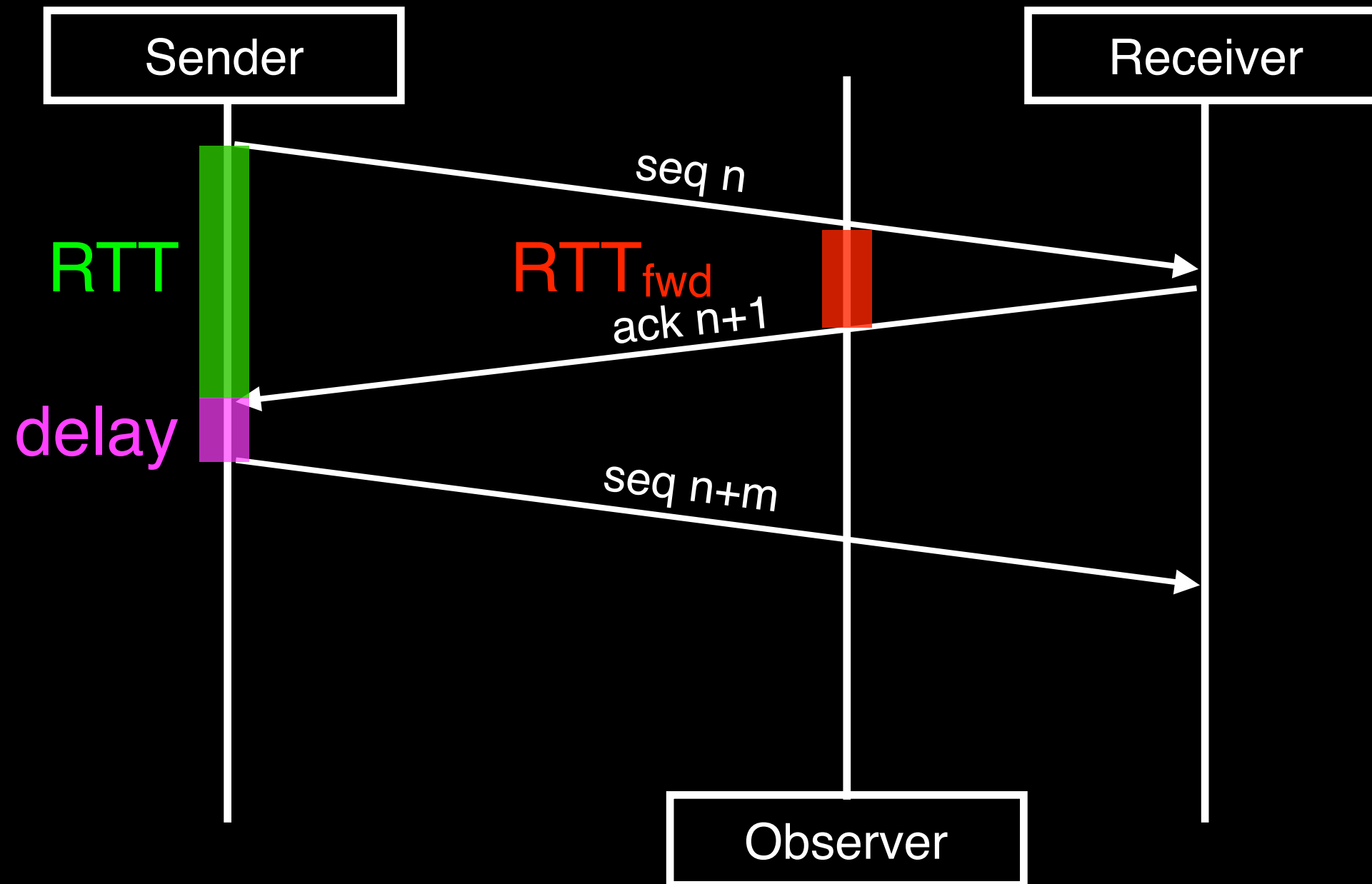
Back to TCP School: Passive RTT Measurement



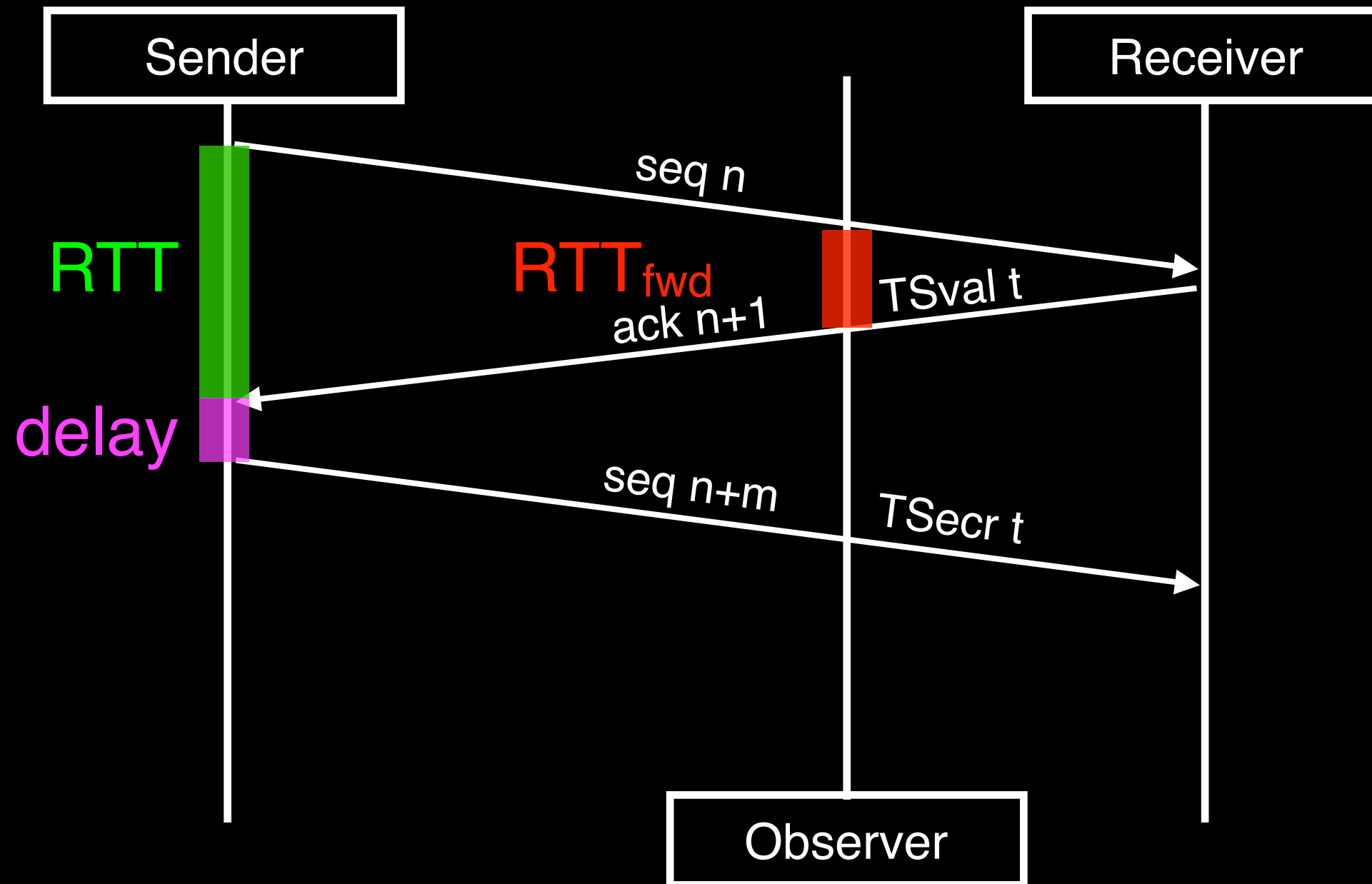
Back to TCP School: Passive RTT Measurement



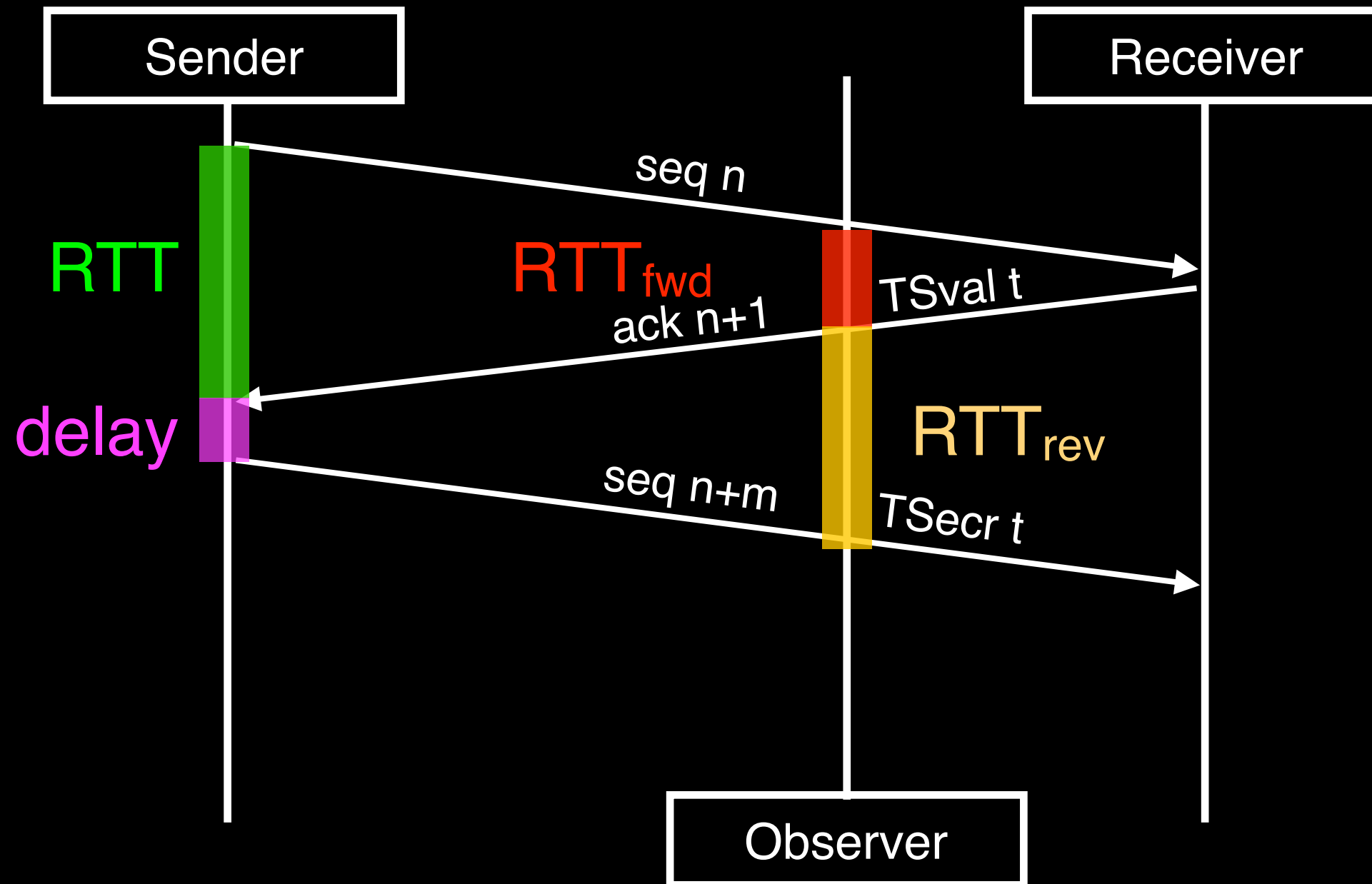
Back to TCP School: Passive RTT Measurement



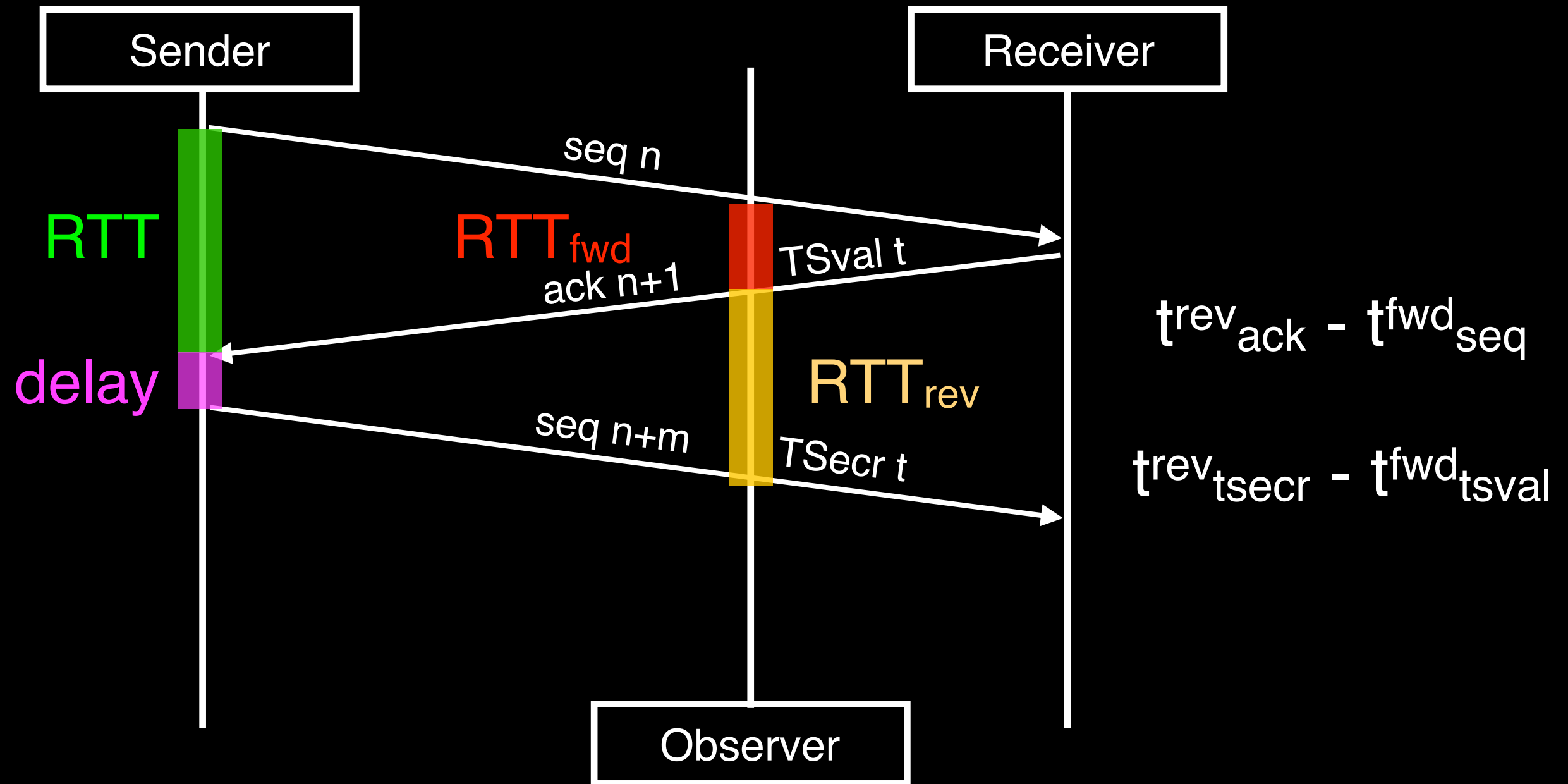
Back to TCP School: Passive RTT Measurement



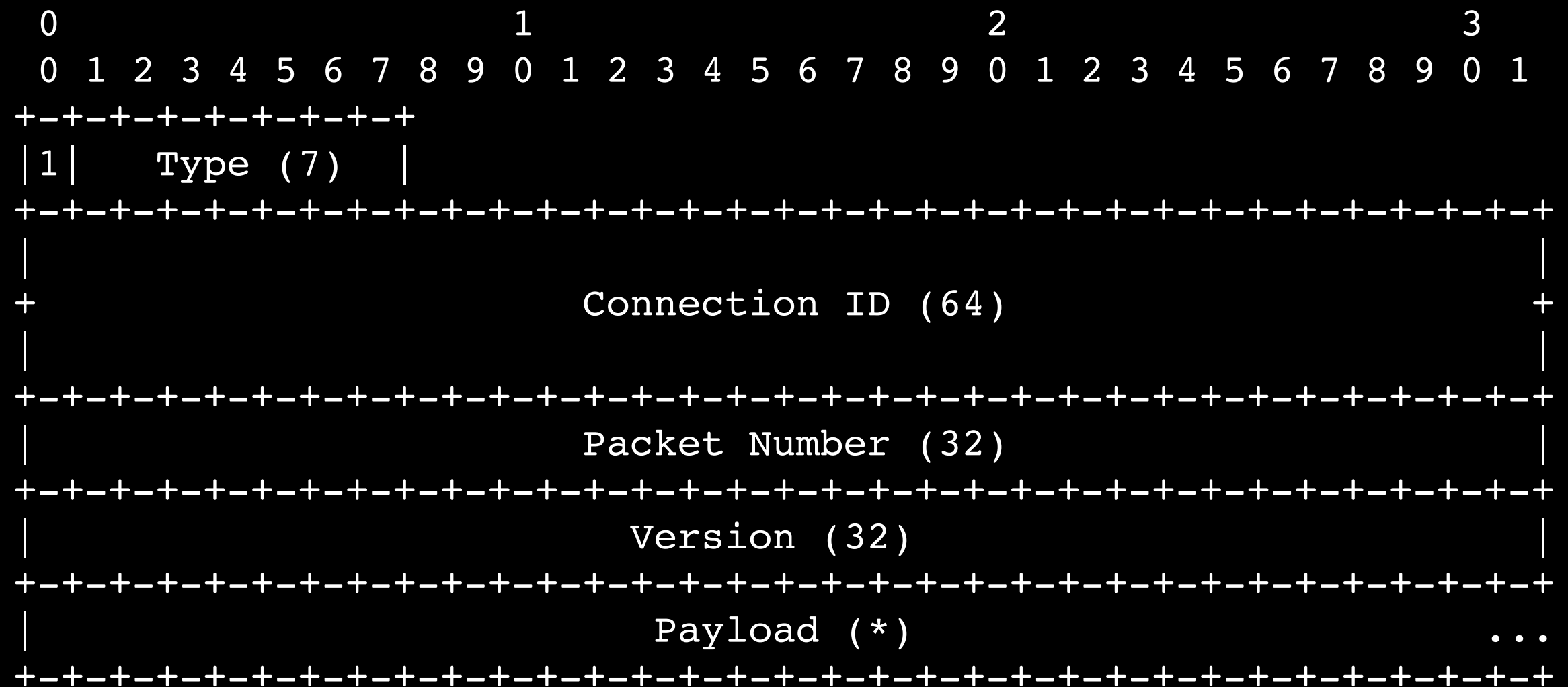
Back to TCP School: Passive RTT Measurement



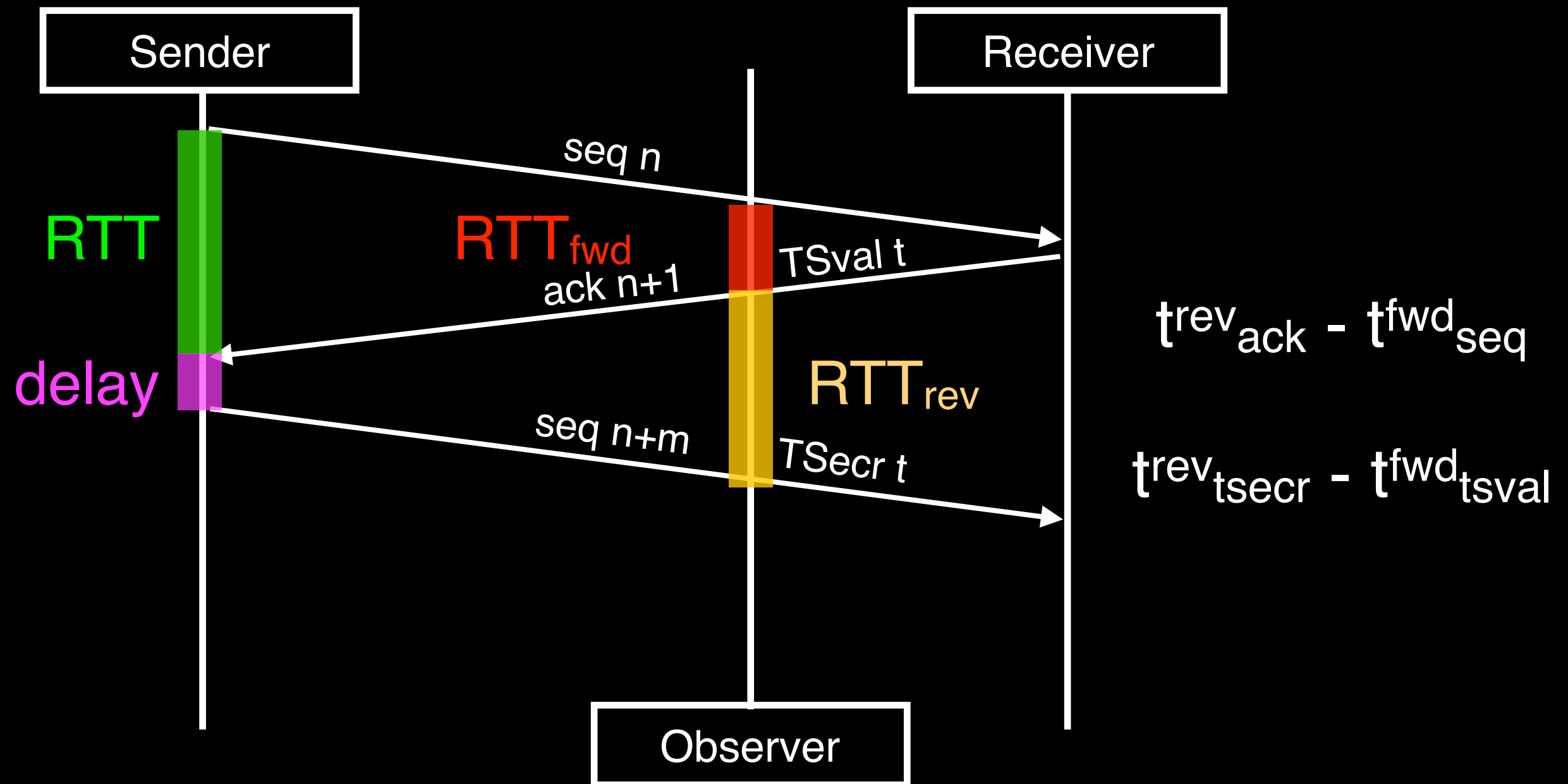
Back to TCP School: Passive RTT Measurement



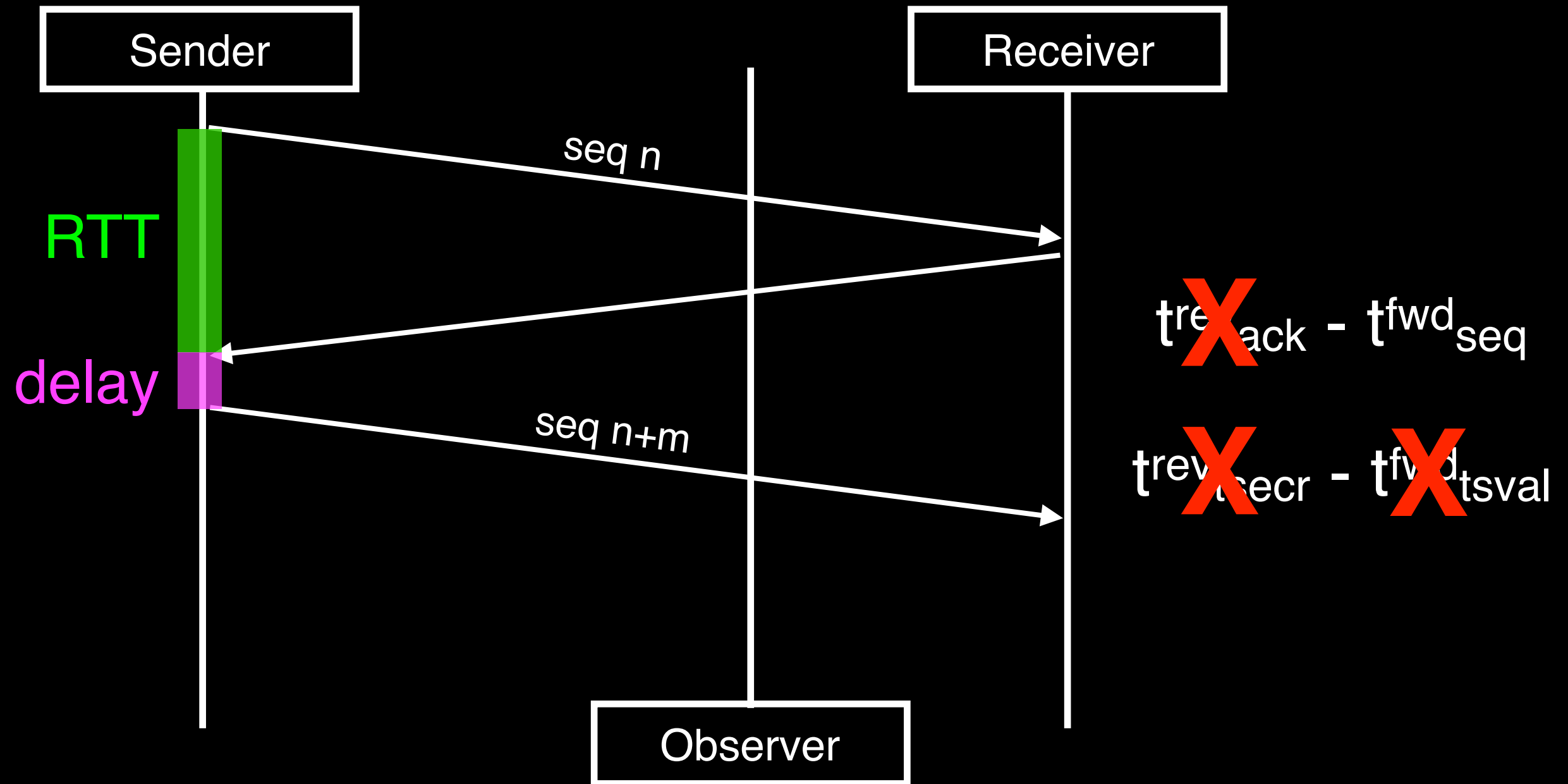
QUIC packet header



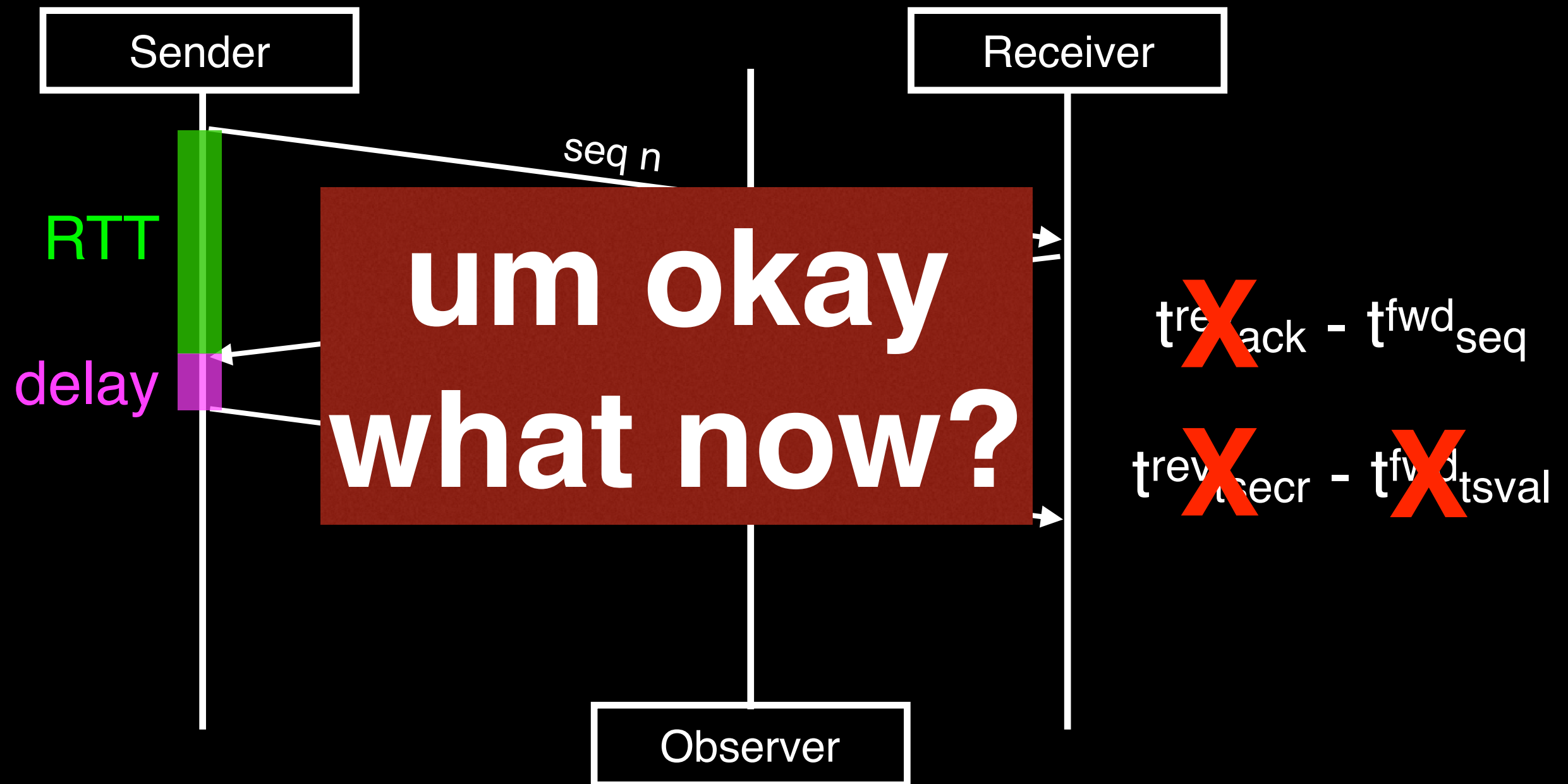
Matching packets with QUIC



Matching packets with QUIC



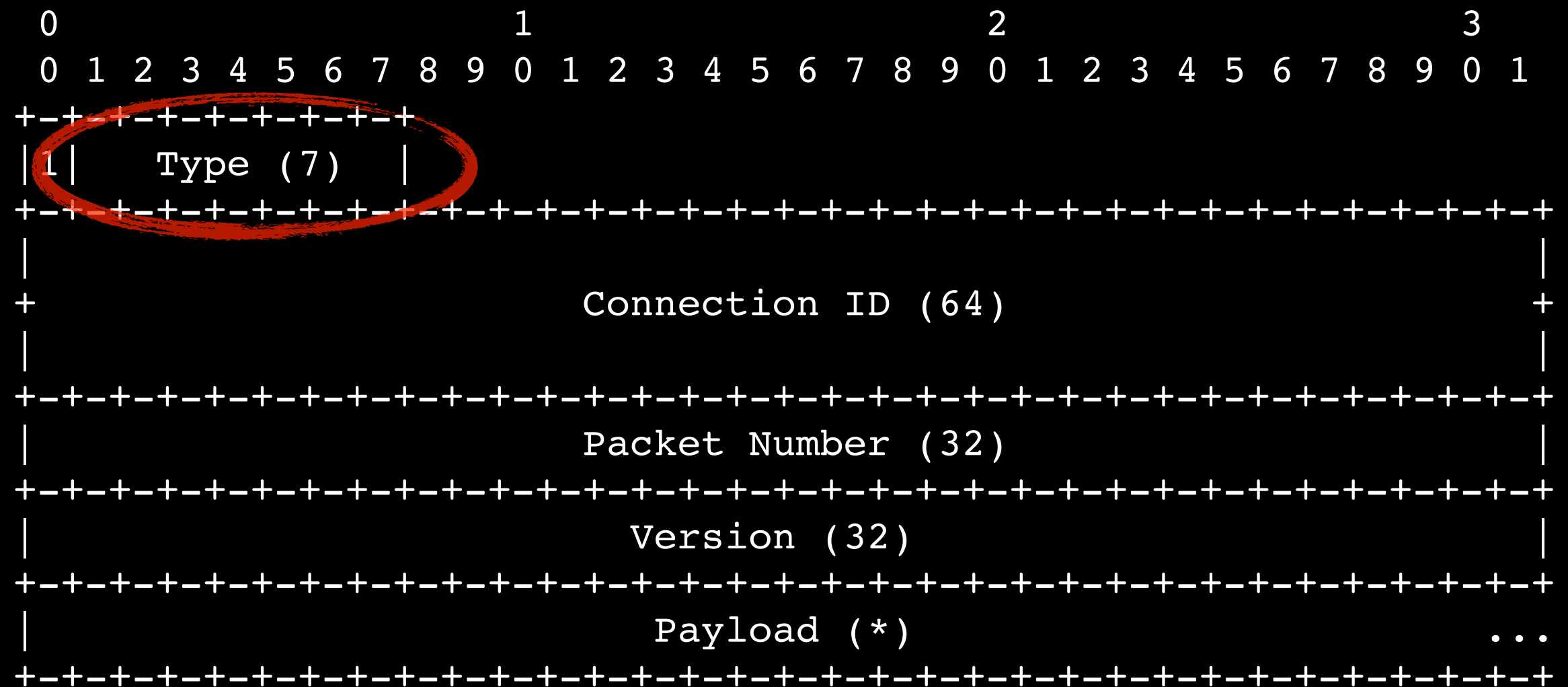
Matching packets with QUIC



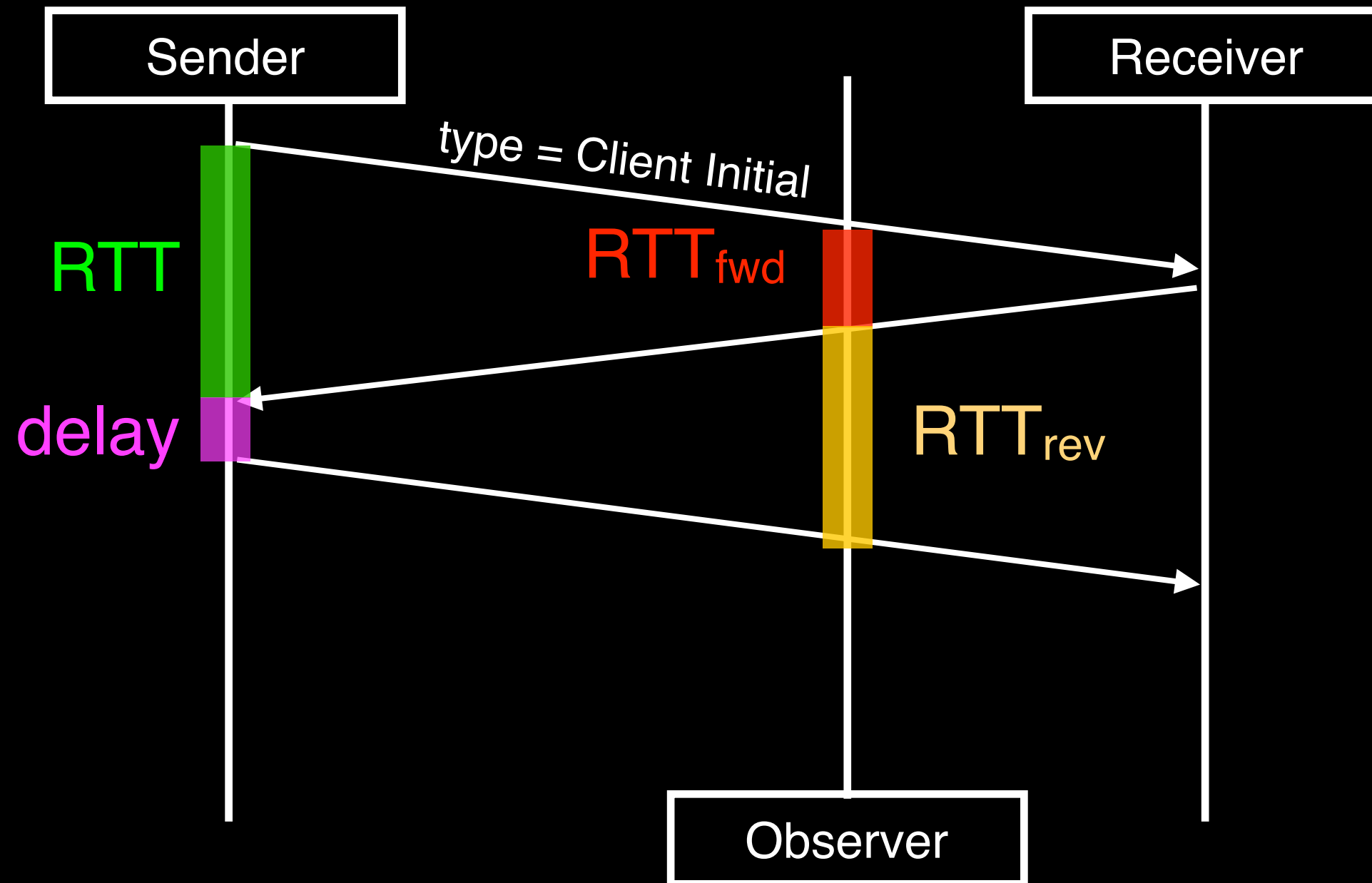
Why encrypt SEQ/ACK/TS?

- A **minimal wire image** is a design goal of QUIC:
 - Defense against “collect it all” is “encrypt it all”
 - Every bit we put on the wire is a bit we won’t be able to change in the future.
 - Every bit we put on the wire is a bit that might be used against us in the future.

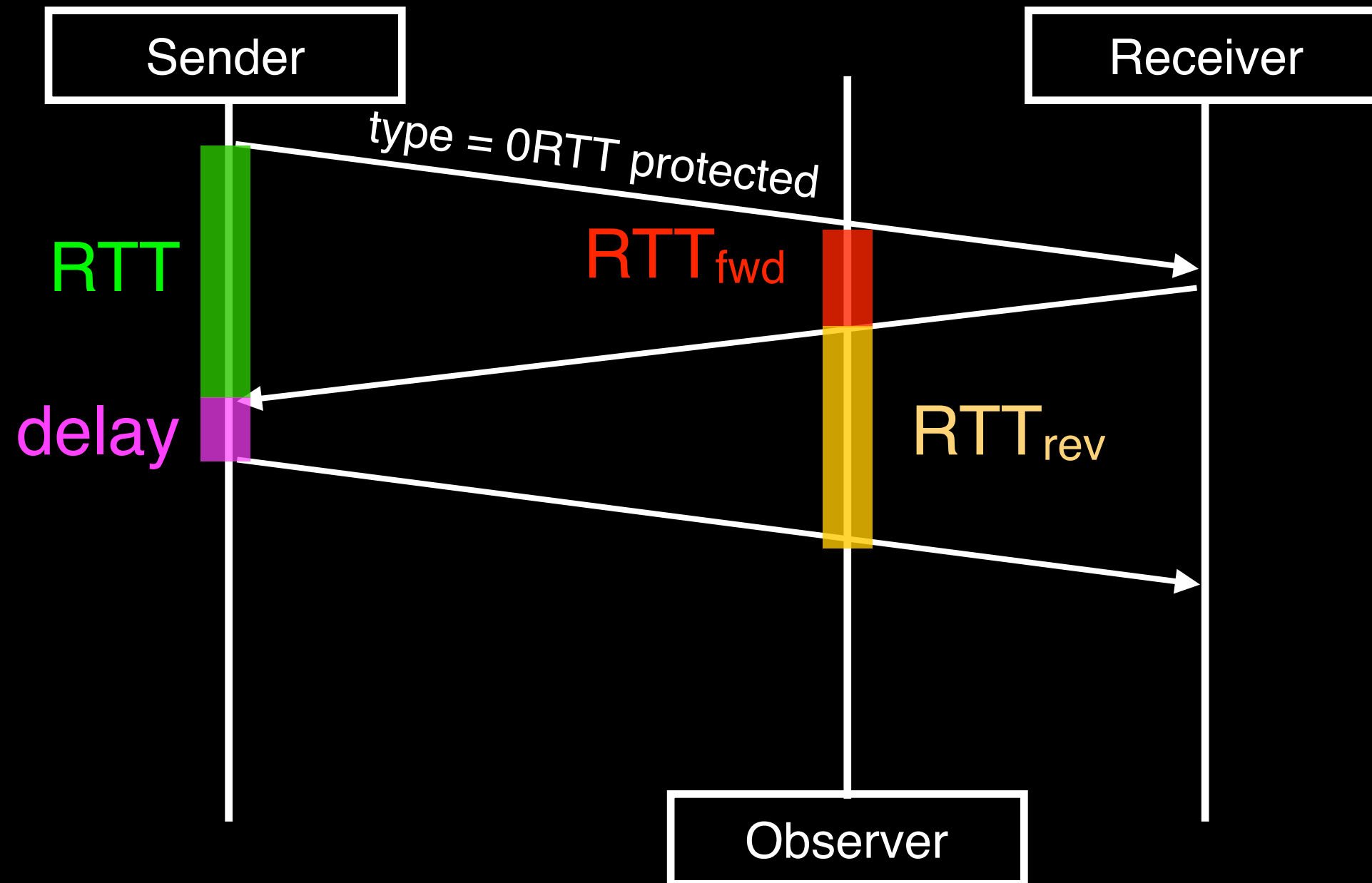
QUIC packet header



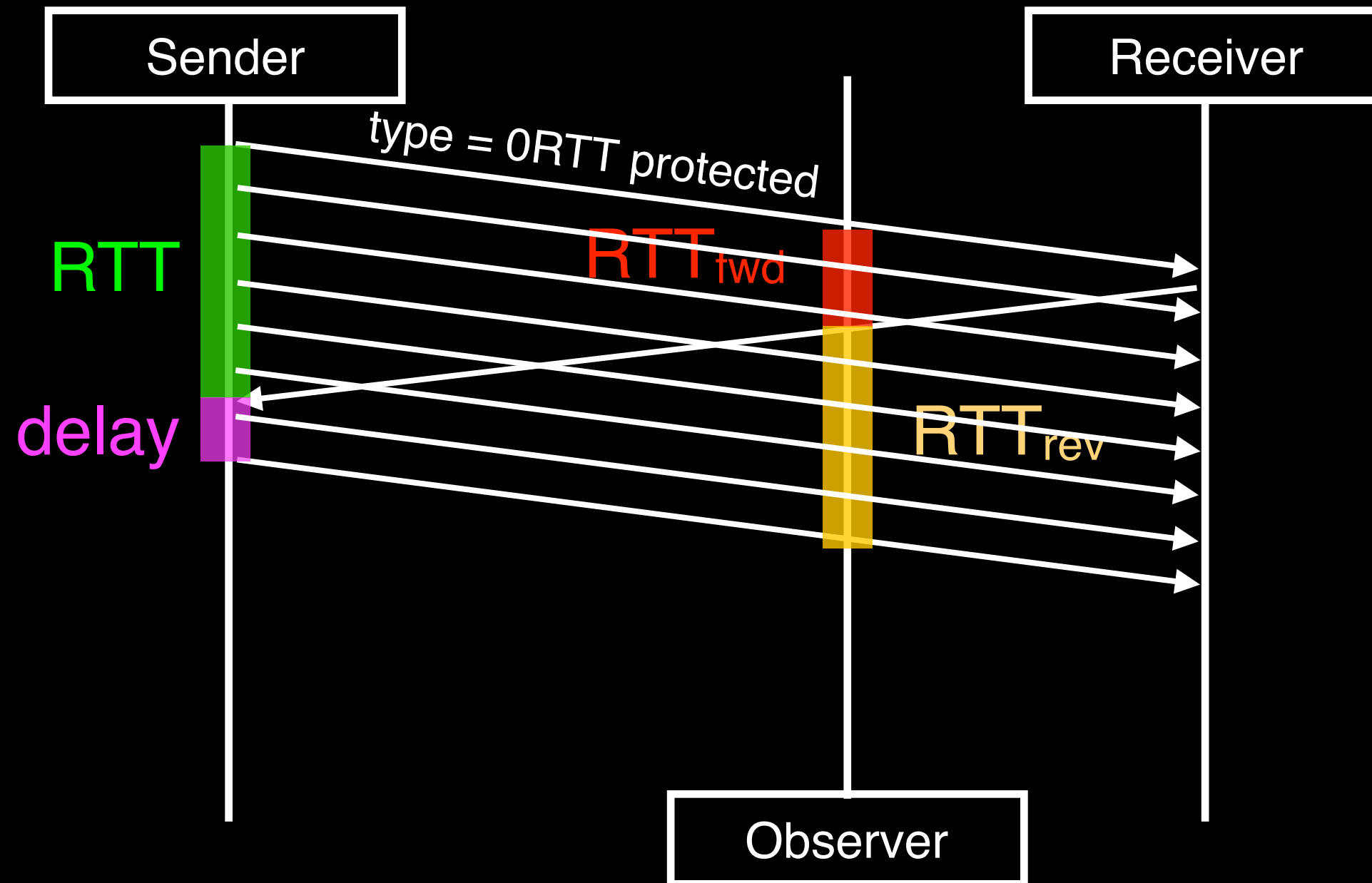
Handshake RTT measurement in QUIC (1-RTT handshake)



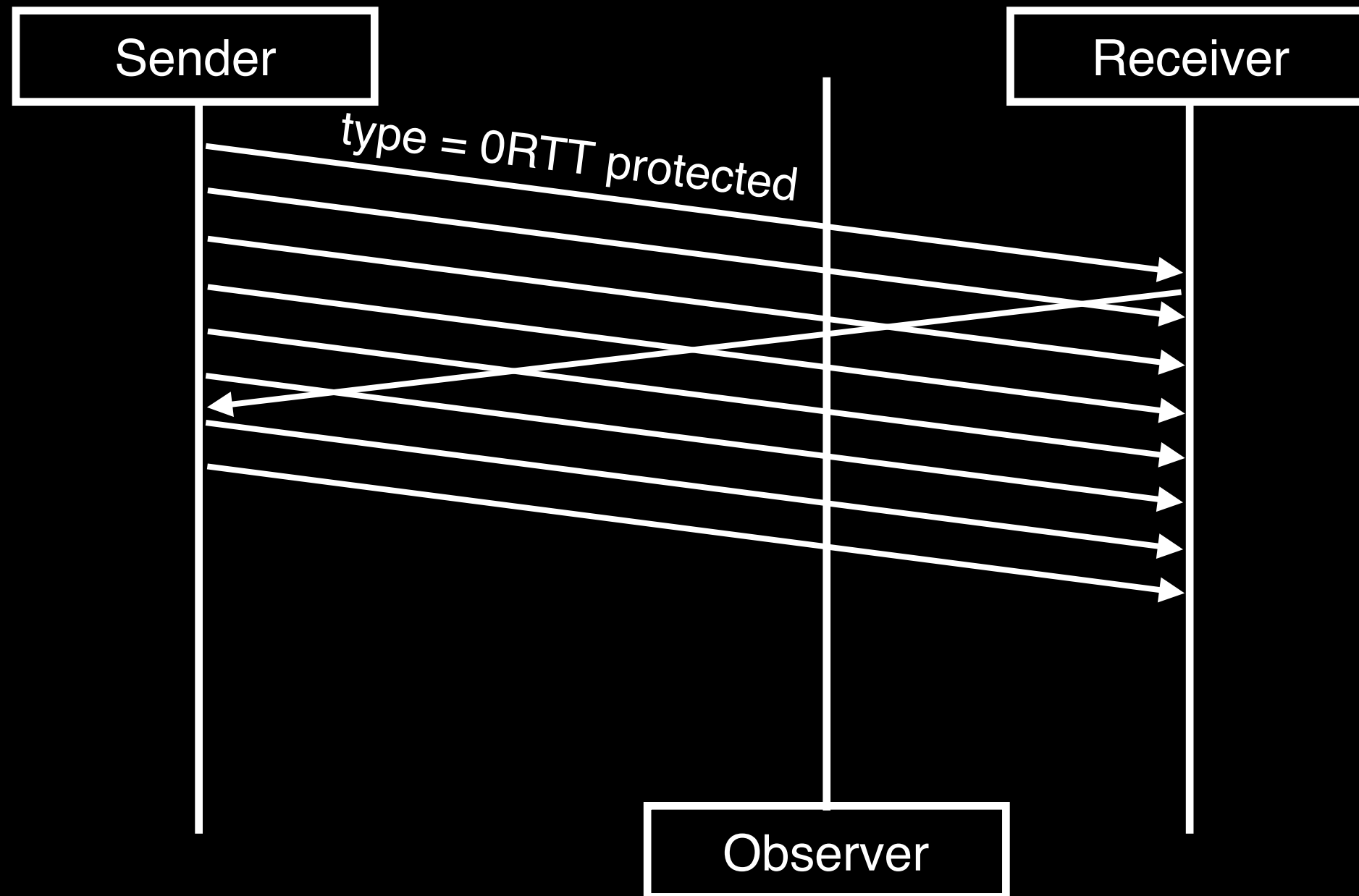
Handshake RTT measurement in QUIC (0-RTT Handshake)



Handshake RTT measurement in QUIC (0-RTT Handshake)



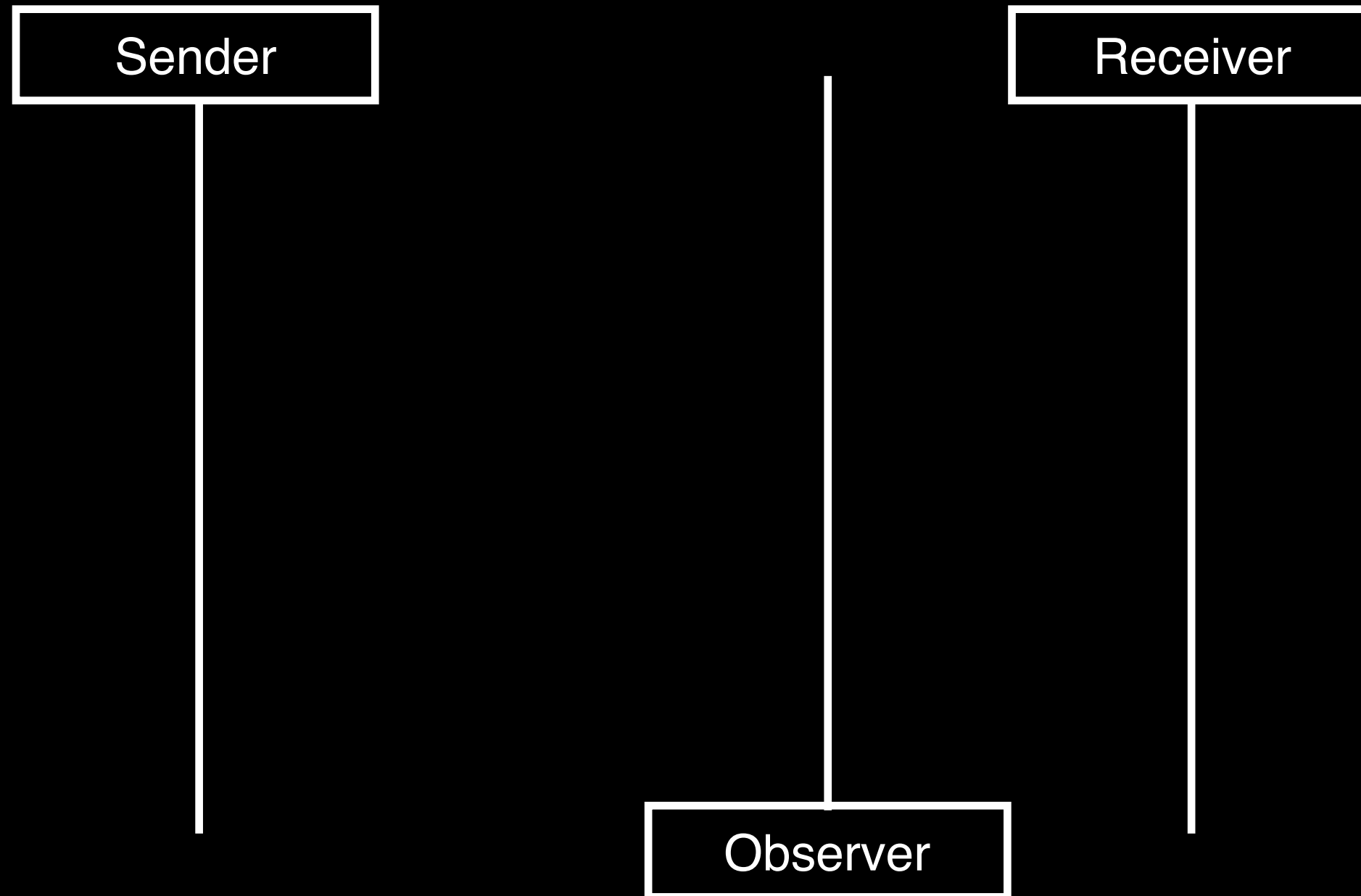
Handshake RTT measurement in QUIC (0-RTT Handshake)



Explicit passive measurability of RTT

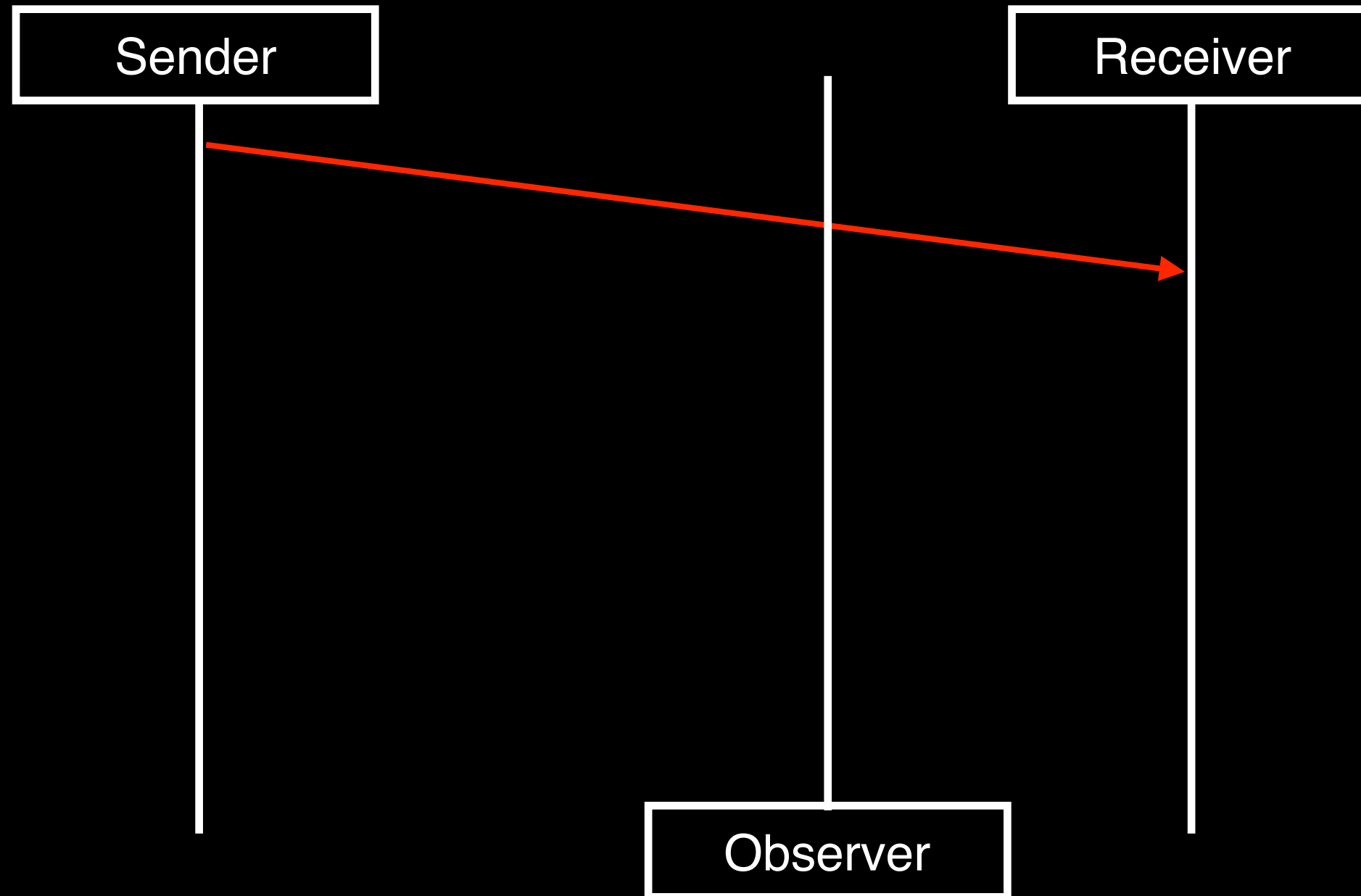
- If passive measurability of a protocol is a desirable feature, then it should be explicitly supported by the design of the protocol.
- Is there a way to do this with a minimal impact on the wire image?
 - One sample per flow: ensure handshake is distinguishable in both directions
 - Multiple samples per flow: latency spin bit

The Latency Spin Bit



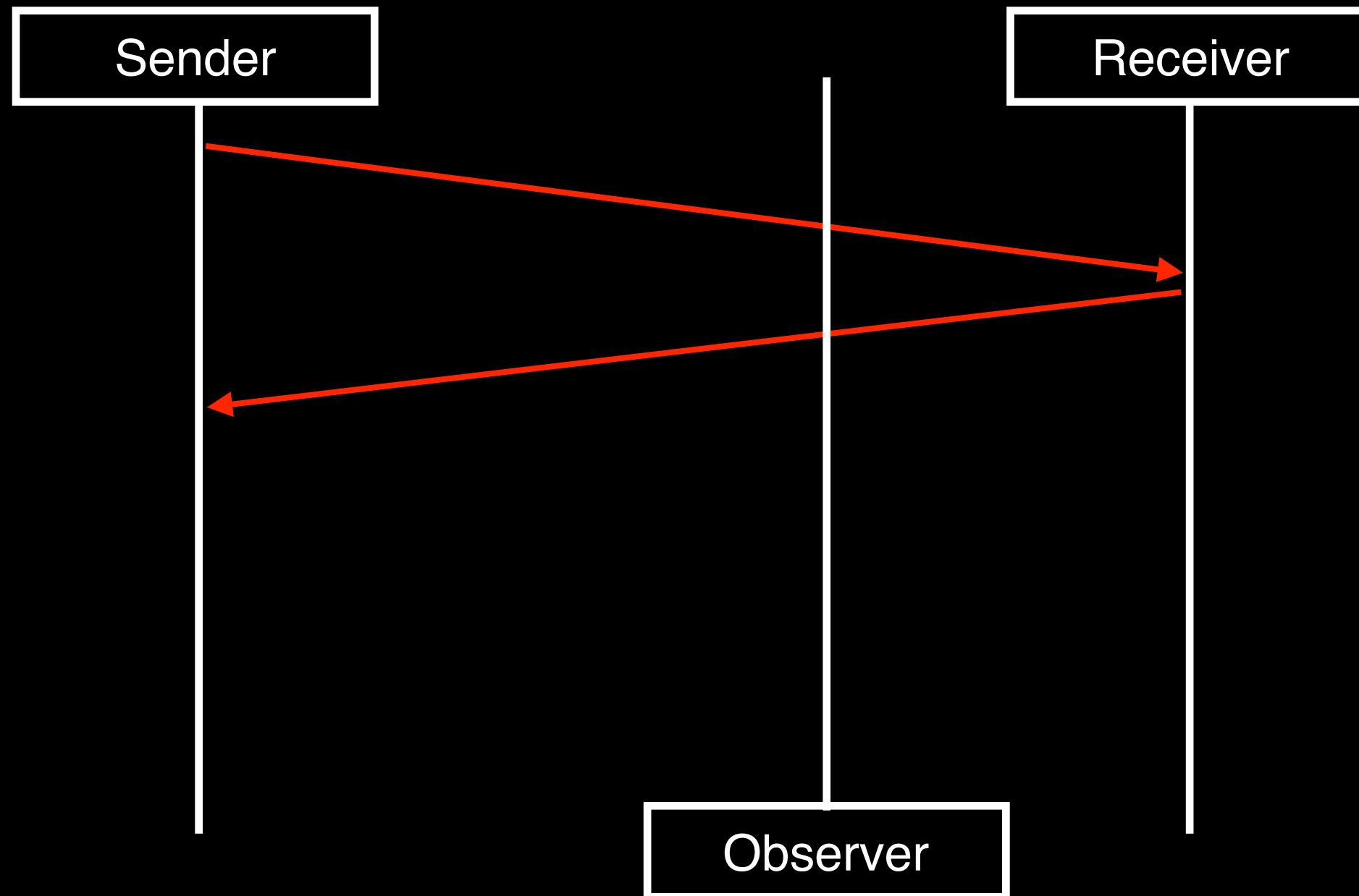
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



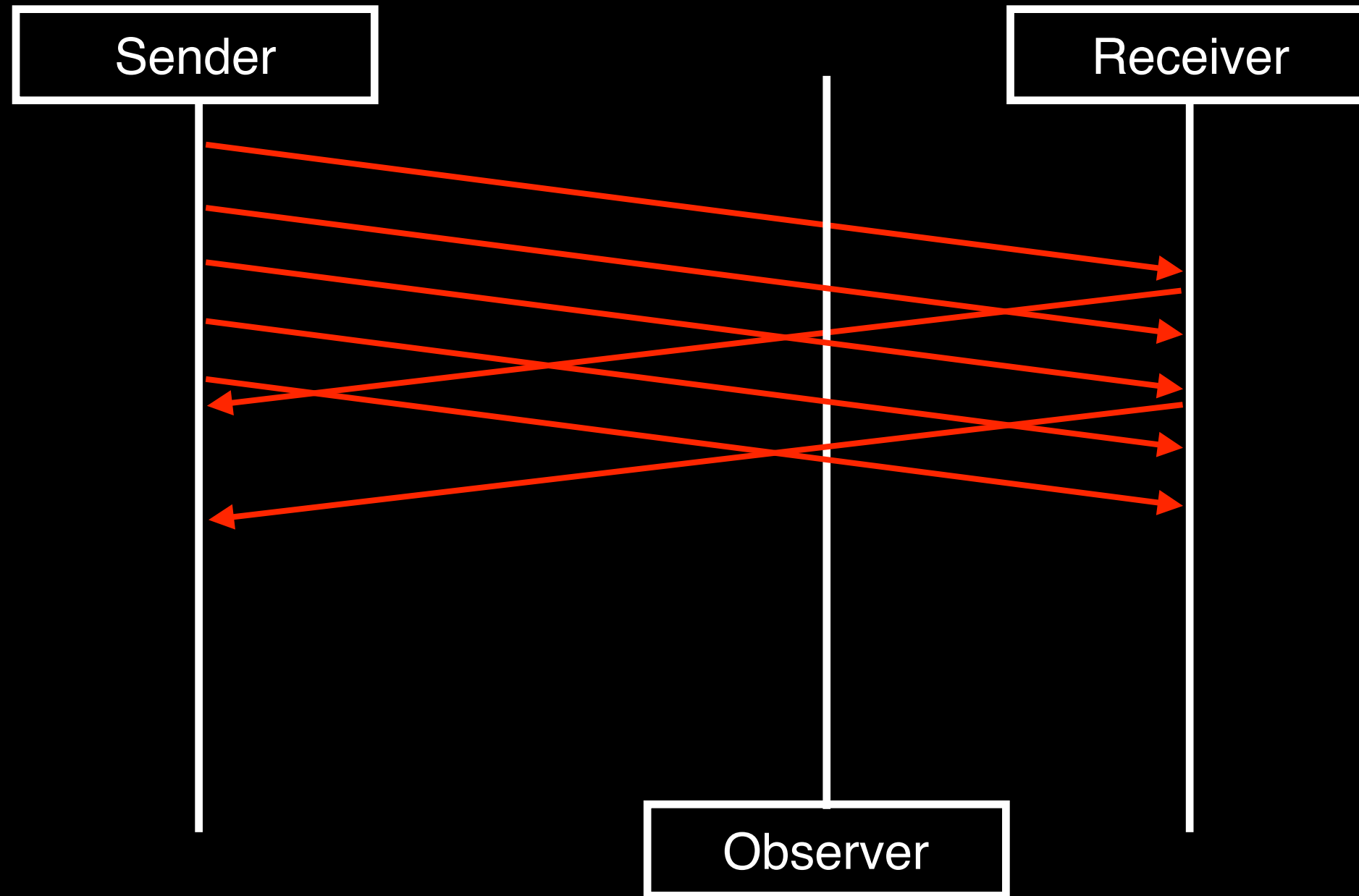
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



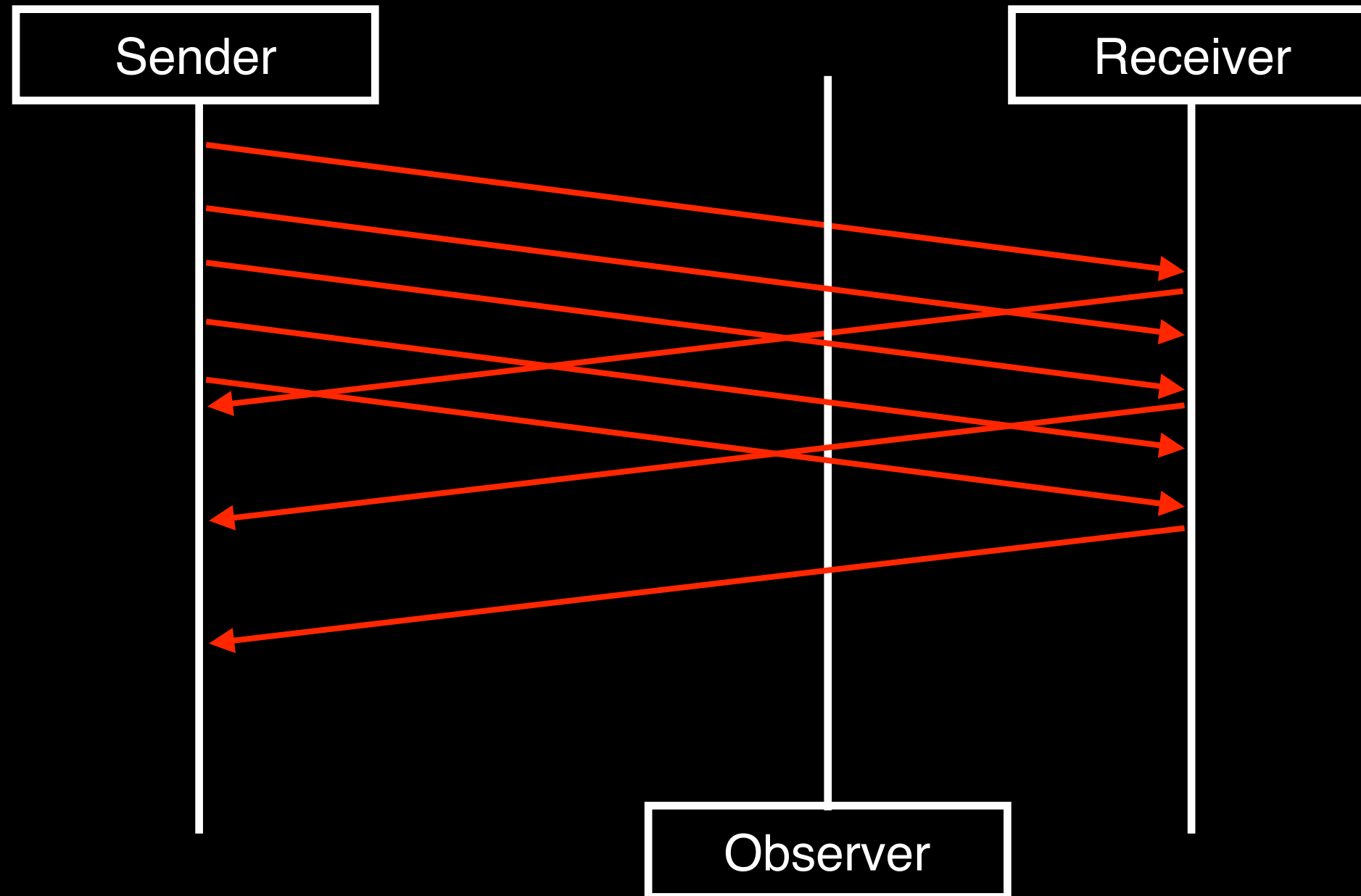
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



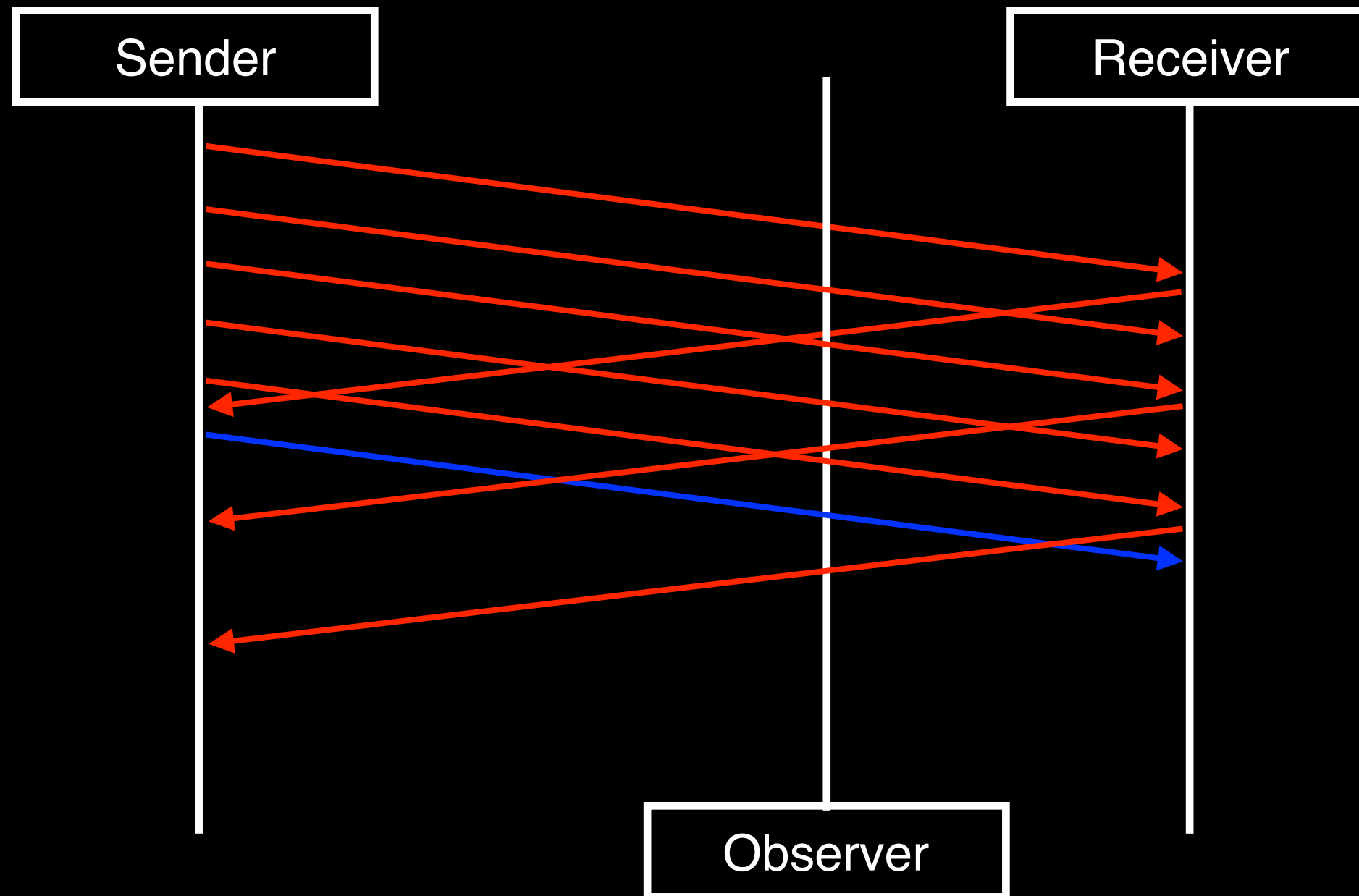
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



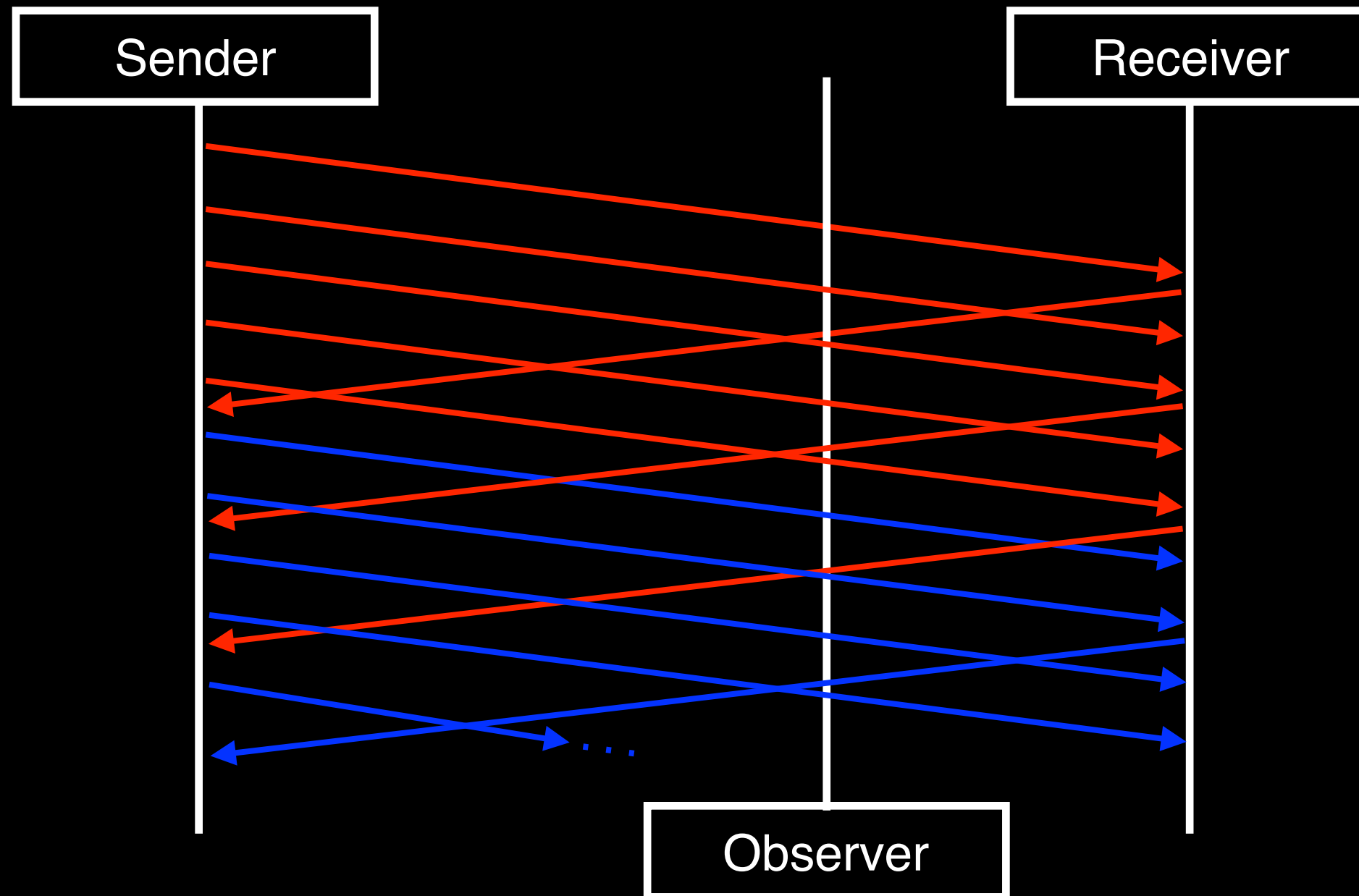
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



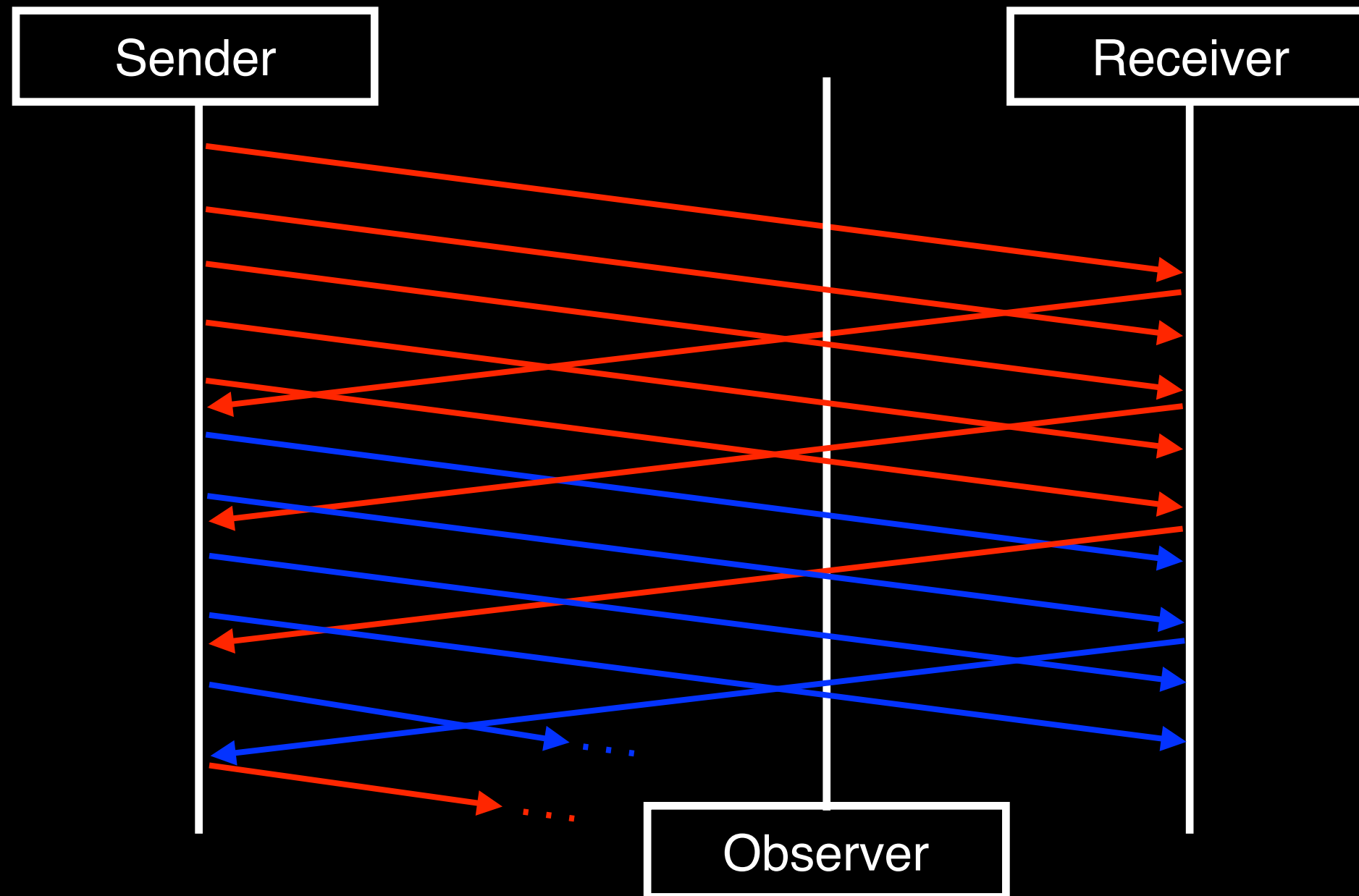
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



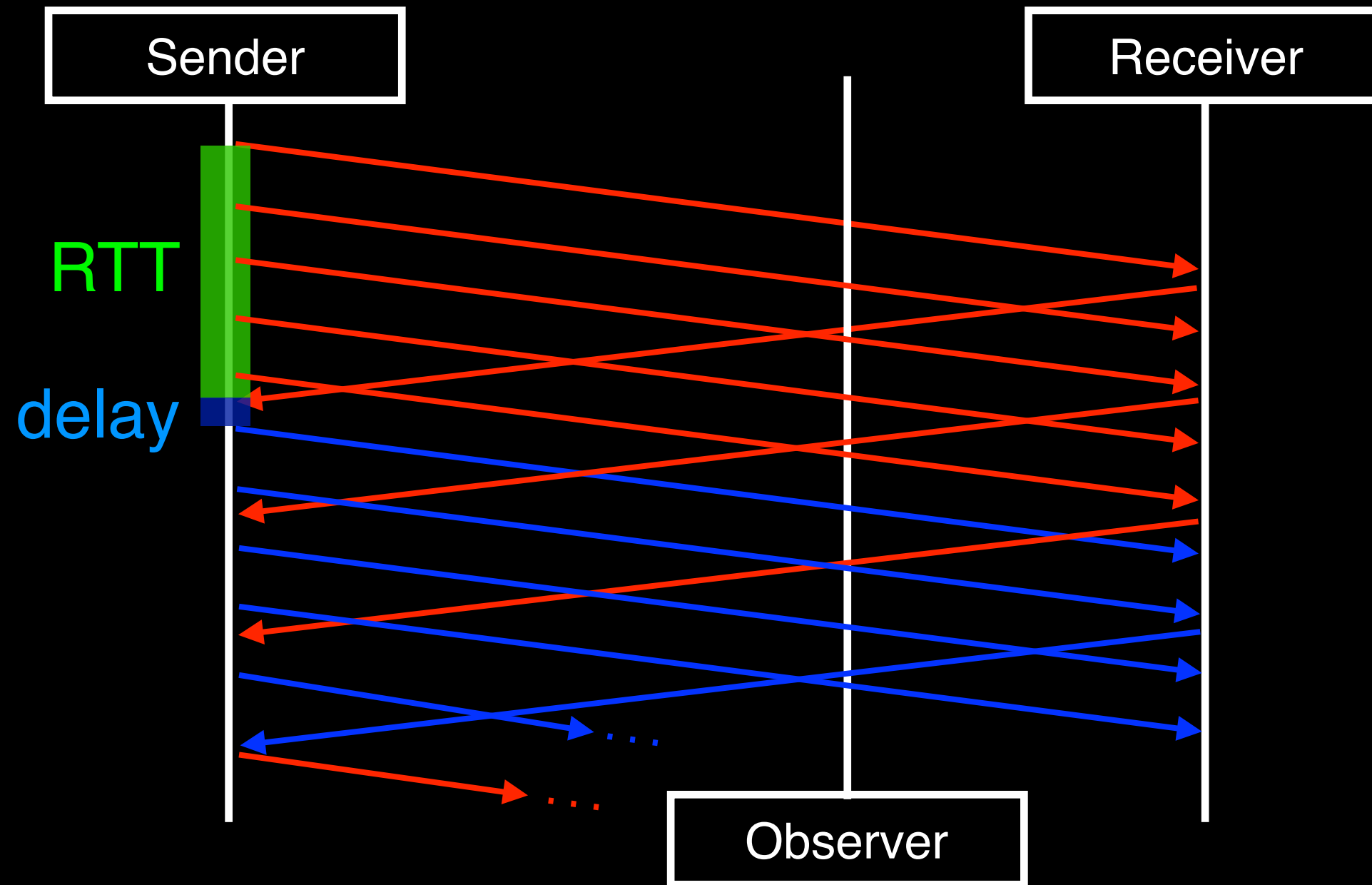
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



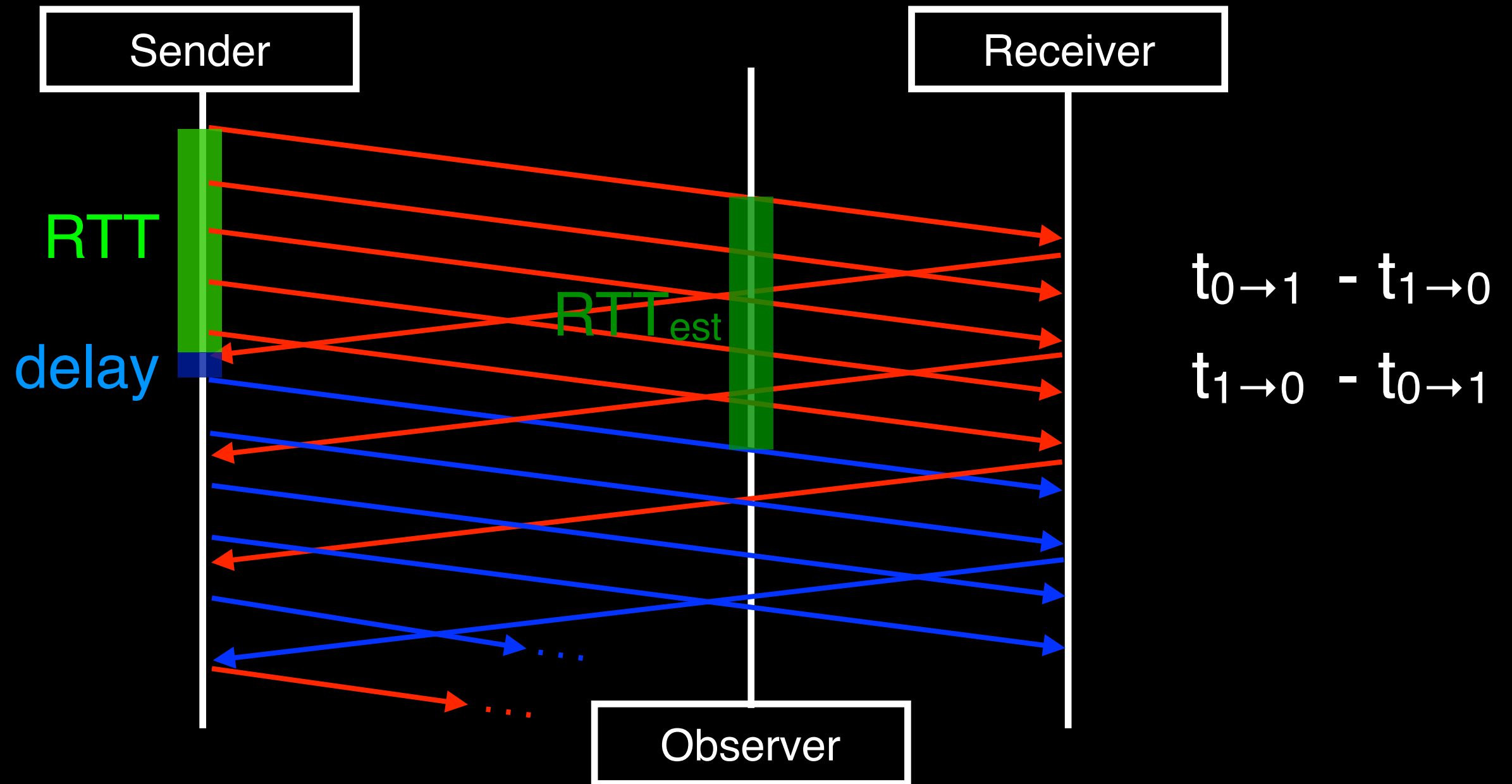
see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



see <https://github.com/quicwg/base-drafts/pull/609>

The Latency Spin Bit



We need your input

- Do you presently use, or do you plan to use, passive RTT measurement on your network?
- IETF QUIC WG has appointed a design team to weigh utility v. risks, will (hopefully) come to conclusion at IETF 100 in Singapore in November.
- Come talk to me,
or send mail to <ietf@trammell.ch>