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

- Sender
- Observer
- Receiver

RTT, seq n

RTT$_{fwd}$, ack n+1

RTT$_{rev}$, TSecr t

TSecr t

 Observer

- $t_{rev_{ack}} - t_{fwd_{seq}}$
- $t_{rev_{tsecr}} - t_{fwd_{tsval}}$
QUIC packet header

0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|   Type (7)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Connection ID (64)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Packet Number (32)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Version (32)                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Payload (*)                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Matching packets with QUIC

Sender

seq n

RTT
delay

seq n+m

TSval t

ack n+1

TSecr t

Observer

RTT

delay

what now?

Receiver

t_{ack} - t_{fwd_{seq}}

t_{rev_{secr}} - t_{fwd_{tsval}}
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

+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+
| 1  |   Type (7)   |
+----+--------------------------------+
|                                             |
| Connection ID (64)                         |
+--------------------------------------------+
|                                             |
| Packet Number (32)                         |
+--------------------------------------------+
|                                             |
| Version (32)                               |
+--------------------------------------------+
|                                             |
| Payload (*)                                |
+--------------------------------------------+
Handshake RTT measurement in QUIC

- **Sender**
  - RTT delay
  - type = Client Initial
  - type = 0RTT protected
  - type = Server Cleartext
  - type = Client Cleartext

- **Receiver**
  - RTT delay
  - RTT$_{fwd}$
  - RTT$_{rev}$

- **Observer**
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

Sender

Observer

Receiver

RTT

delay

RTT_{est}

\[ t_0 \rightarrow 1 - t_1 \rightarrow 0 \]

\[ t_1 \rightarrow 0 - t_0 \rightarrow 1 \]

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

• General issues in wire image utility addressed in draft-ietf-quic-manageability