On Wire Images

Brian Trammell – NDSS QUIPS
San Diego USA — 23 February 2020

Sources, Acknowledgments, and Disclaimer

Much of this work was done at ETH Zurich with Mirja Kühlewind, under the auspices of the H2020 MAMI project.

We are both now seeking refuge in industry. Many thanks to Google, my employer, for the time to come give this talk.

TL;DL: you can read the following instead of paying attention to this talk (but do so quickly, there's a Q+A afterward):

- Revisiting the Privacy Implications of Two-Way Internet Latency Data (at PAM 2018)
- Three Bits Suffice: Explicit Support for Passive Measurement of Internet Latency in QUIC and TCP (at IMC 2018)
- The Wire Image of a Network Protocol (RFC 8546)

What is a Wire Image and Why do I Care?

From RFC 8546:

"The wire image of the set of protocols in use for a given communication is the view of that set of protocols as observed by an entity not participating in the communication. It is the sequence of packets sent by each participant in the communication, including the content of those packets and metadata about the observation itself: the time at which each packet is observed and the vantage point of the observer."

More poetically:

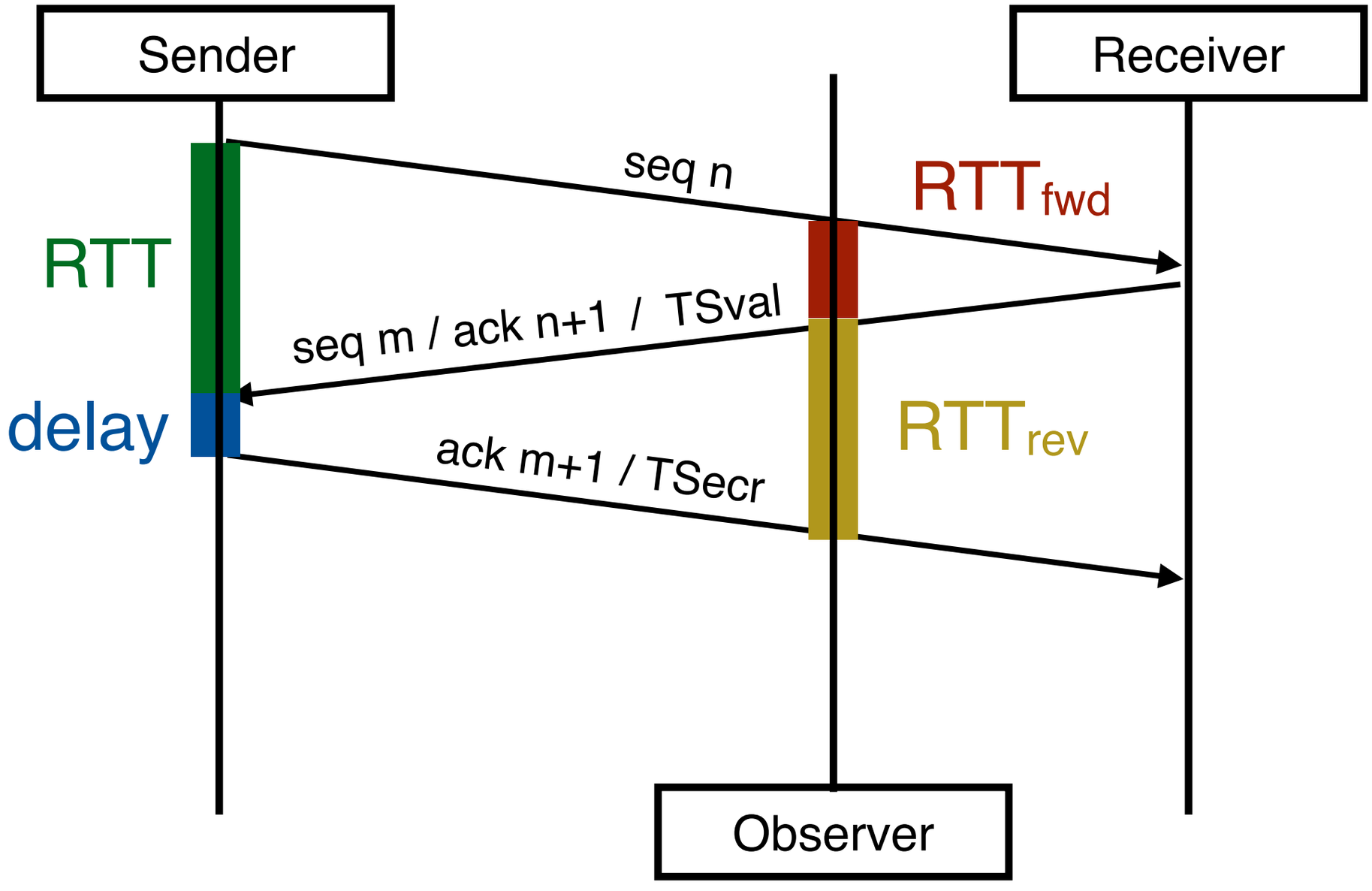
The wire image is the shadow a protocol casts on the Internet, and everything you can know from that shadow.

The Spin Bit

More practically: the case of the spin bit

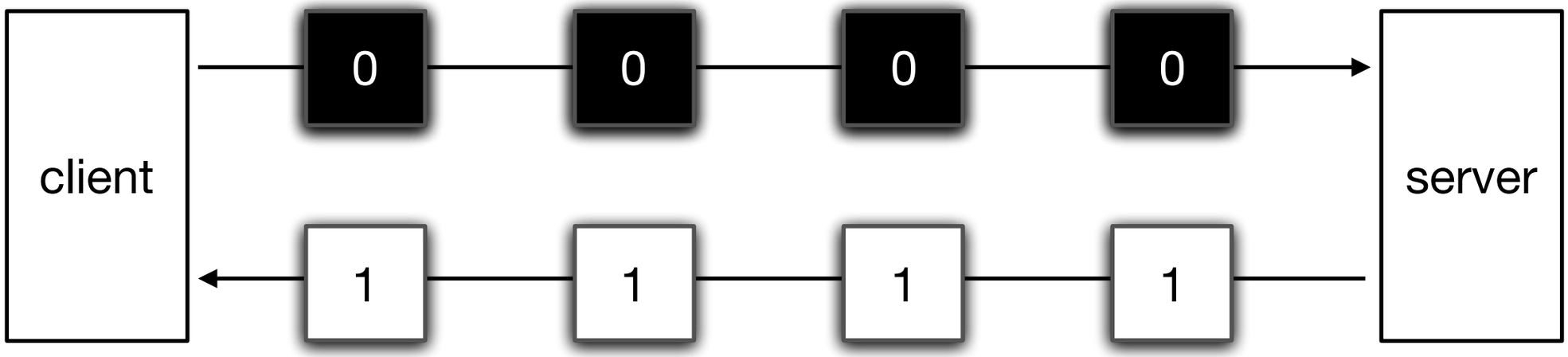
- TCP radiates loss and latency information that can be used for passive measurement.
- QUIC encrypts the control information that exposes these parameters.
    - Indeed, that's the point: an encrypted wire image reduces ossification and makes evolution possible.
- Proposal: change the QUIC wire image to add back RTT information.

Passive RTT estimation with TCP

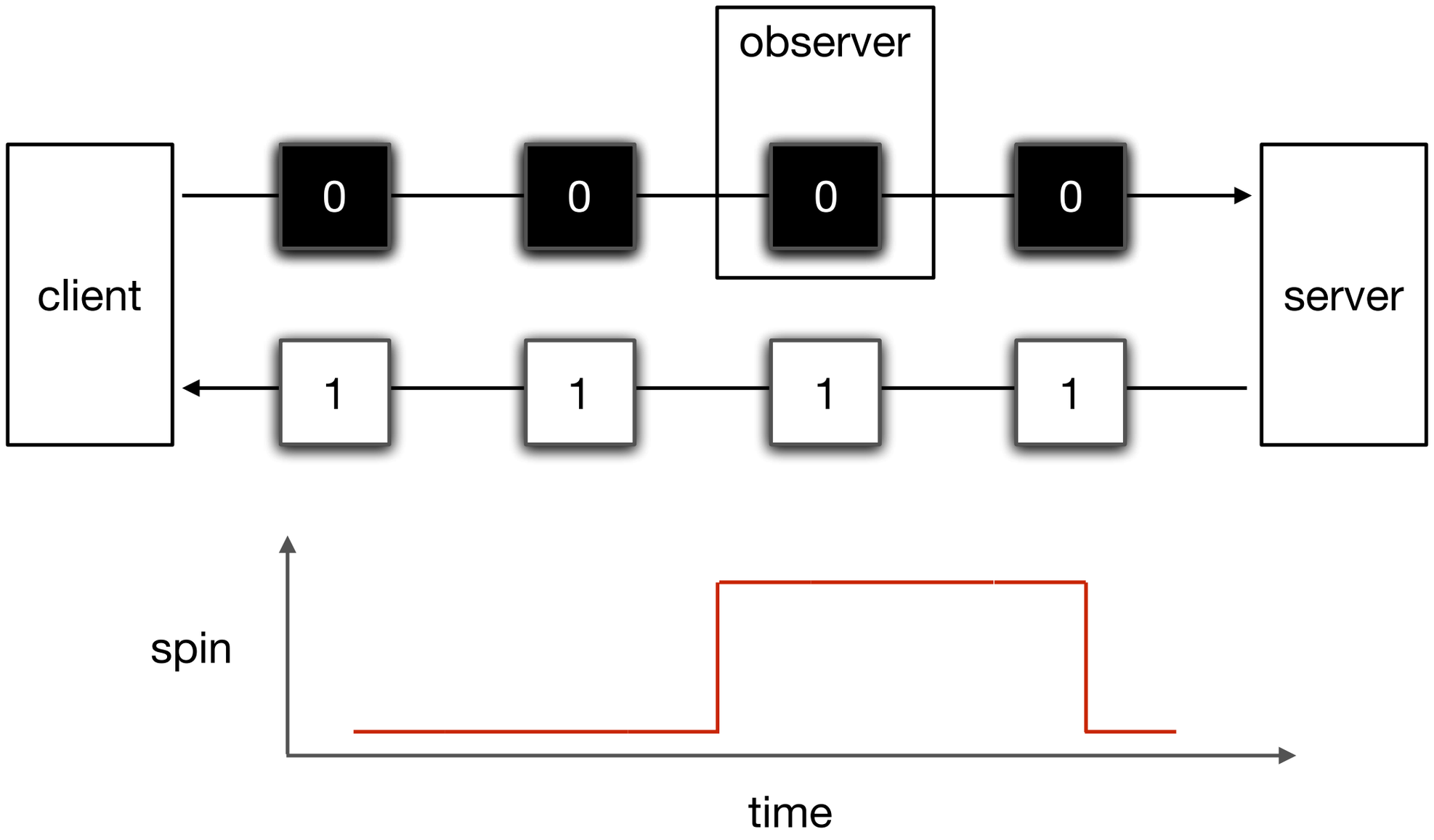


- Uses SEQ# and ACK# and/or TCP Timestamp Option

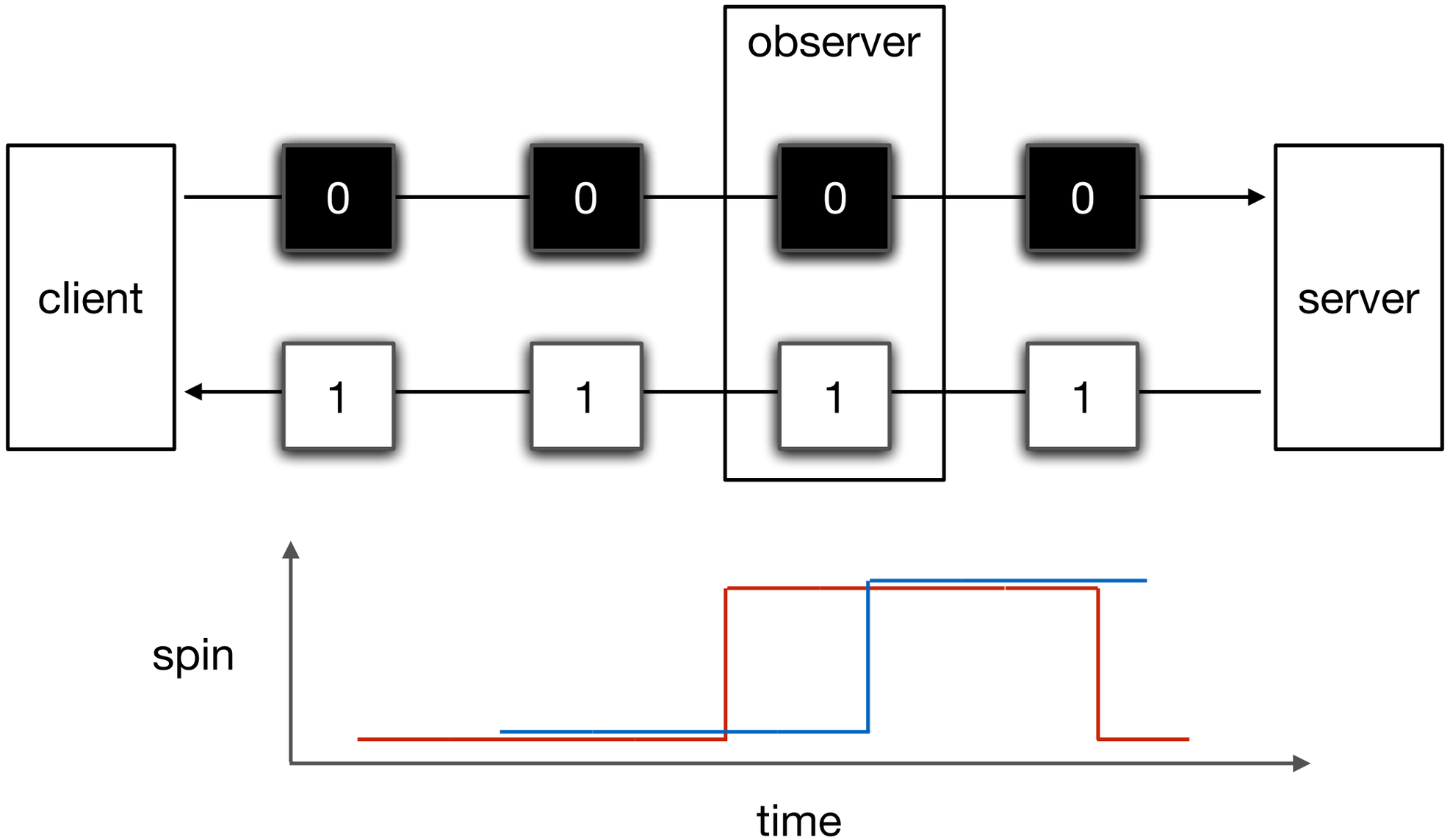
Passive RTT estimation with the QUIC spin bit



Unidirectional one-point measurement

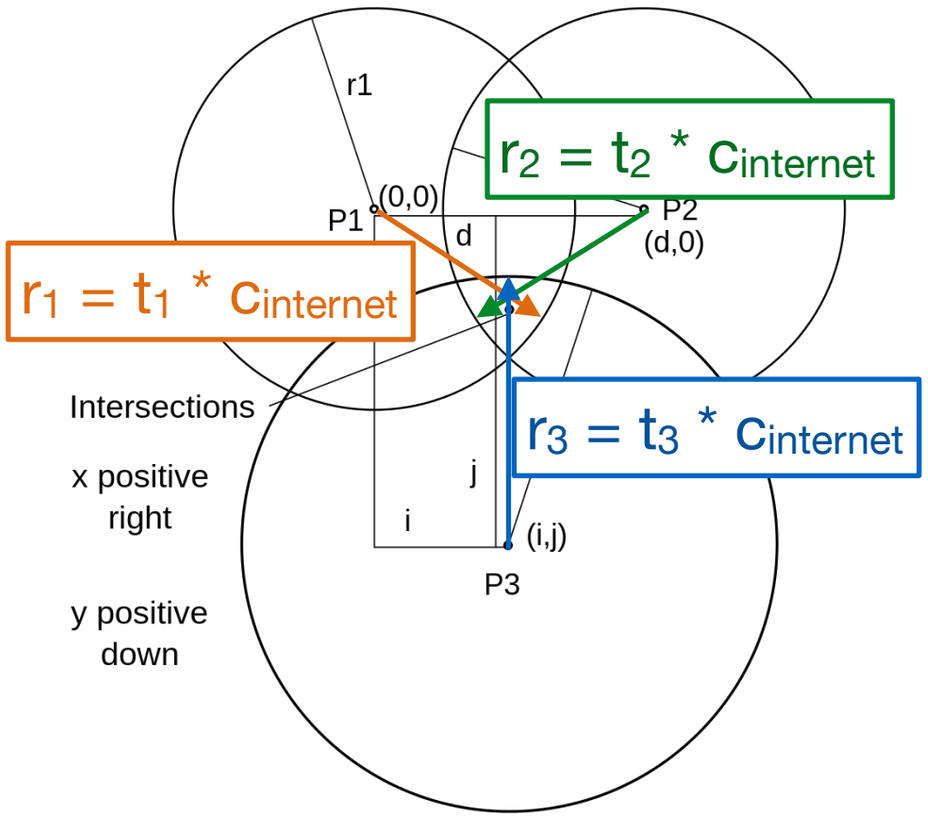


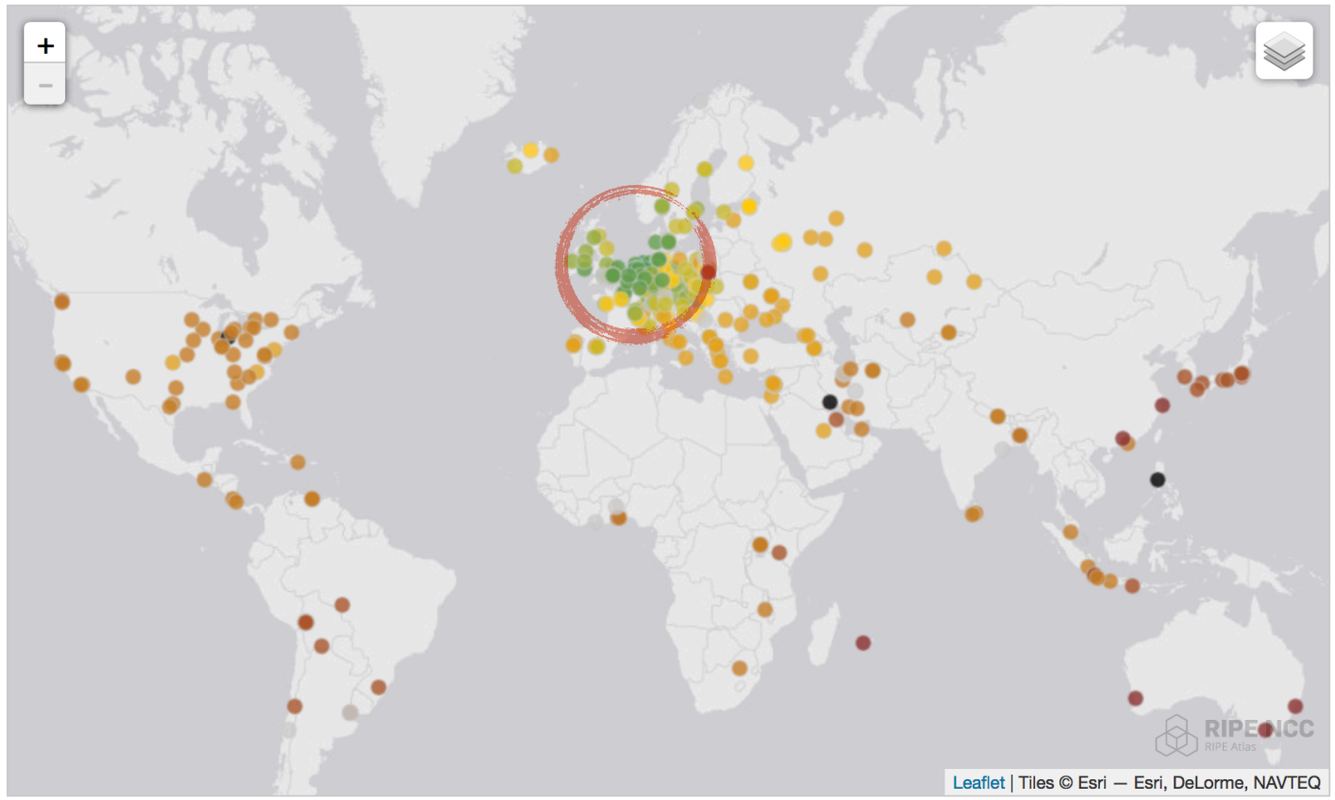
Bidirectional one-point measurement



The Spin Bit and Privacy

"If I can ping you,
I know where you are"





https://atlas.ripe.net/measurements/11583536/#!map

But it's not quite so simple

- Internet RTT is the sum of delays at each hop, some terms of which are variable:

$$RTT_{obs} = \sum_{n=0}^{f}(D_{prop_{n\to n+1}} + D_{queue_n} + D_{proc_n})+$$
$$\sum^{r}(D_{prop_{m\to m+1}} + D_{queue_m} + D_{proc_m})+$$
$$D_{stack} + D_{app}$$

- Distance can be derived only when queueing, stack, and application delay are held to zero:

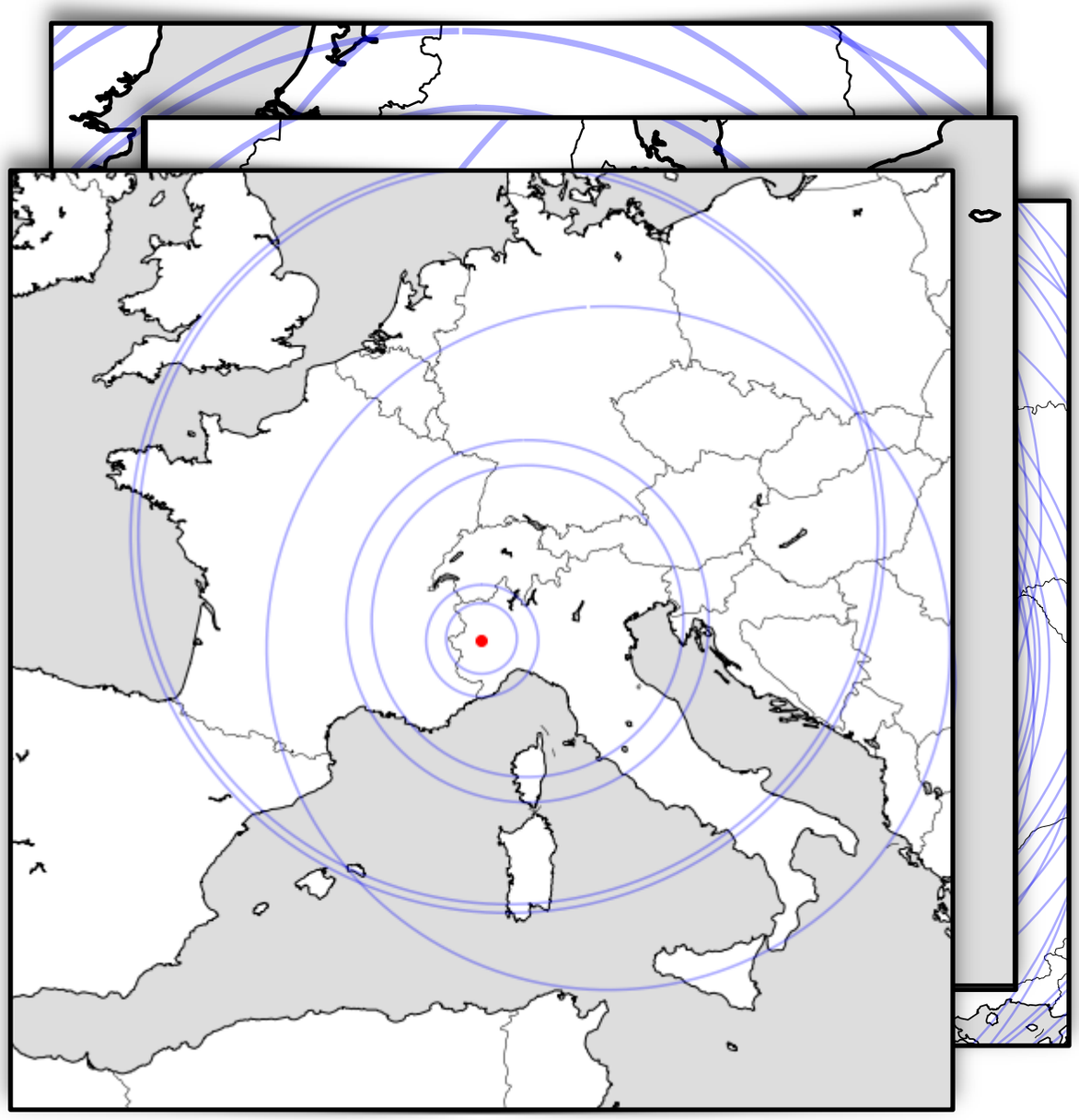
$$dist < \frac{\sum_{n=0}^{f} D_{prop_{n\to n+1}} + \sum_{m=0}^{r} D_{prop_{m\to m+1}}}{2} \times c_{internet}$$

- Research question: What is the privacy impact of internet RTT information, presuming that *location* and *endpoint activity* are private?

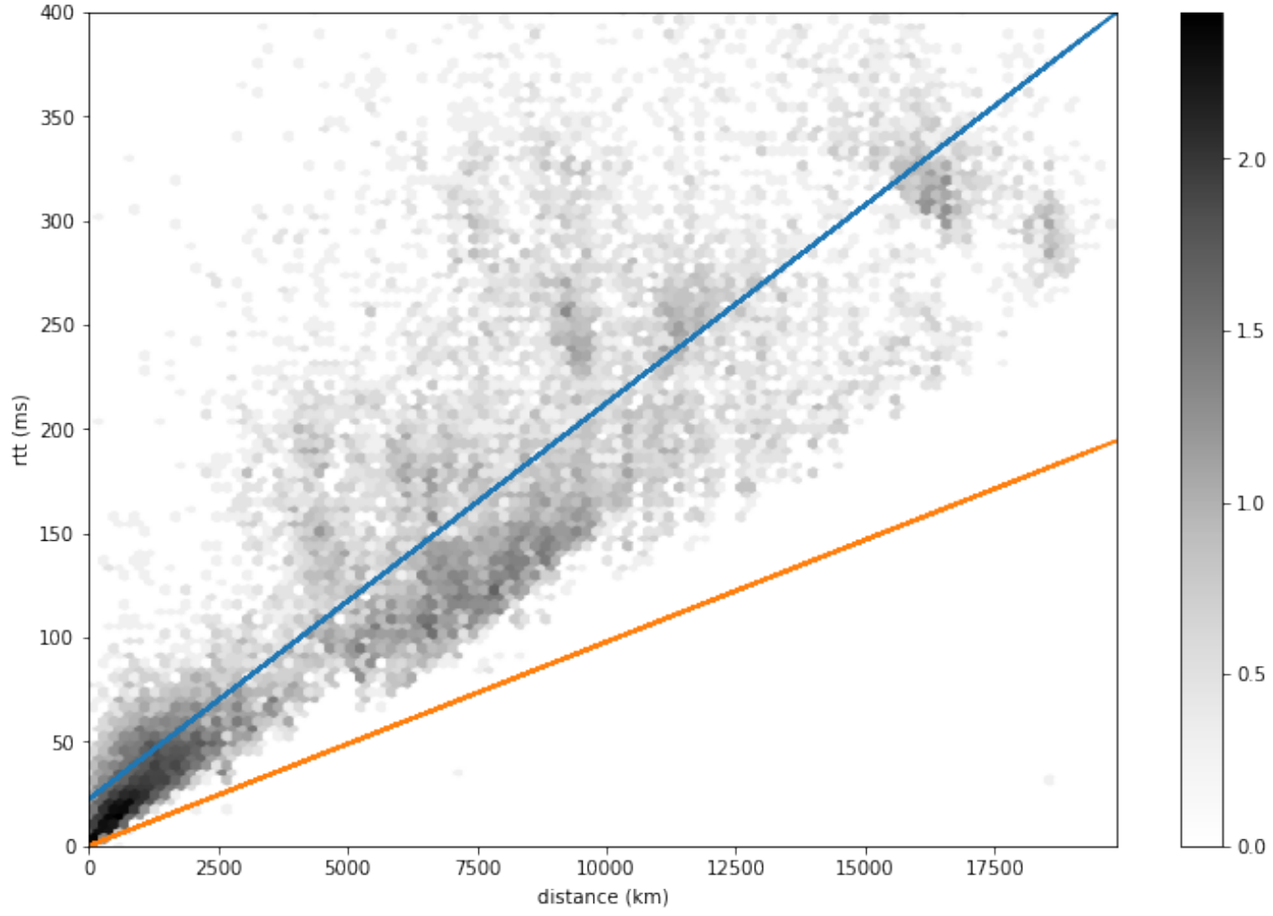
Geolocation by exclusion

$$dist < \frac{min(\text{RTT}_{obs})}{2} \times c_{internet}$$

- Overlap circles centered at each probe with radius derived from $min(\text{RTT}_{obs})$
- Compare region to known anchor location and MaxMind GeoLite
- Results: resolution entirely a matter of luck in probe placement



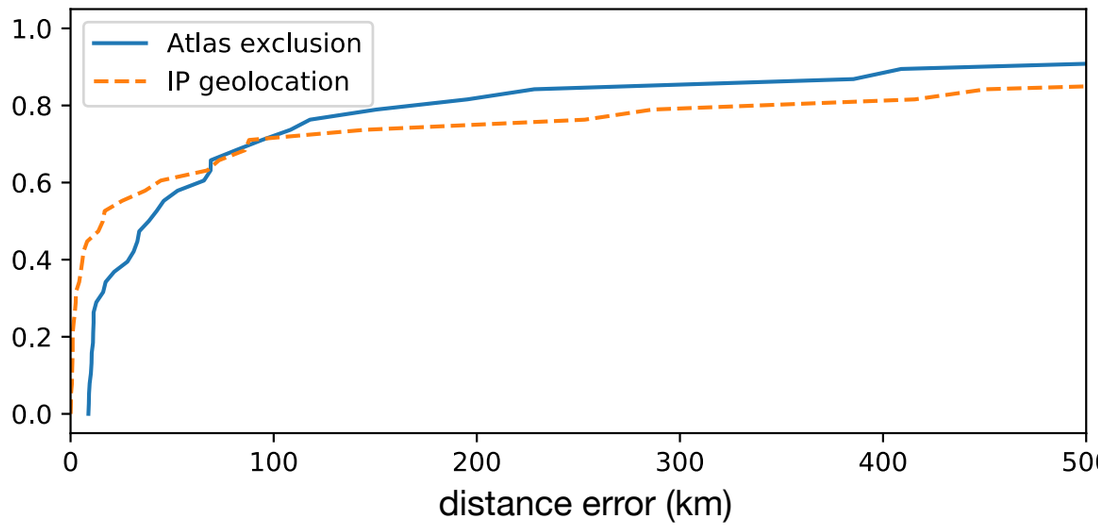
1ms RTT = 100km (± a lot)



- Every network engineer already knows this, right?

Location privacy recommendations

- When target address is known, even freely-accessible geolocation databases have better distance accuracy:



- When target address is redacted, the risk is entirely dependent on how close the known address is to the unknown address:
  - 1ms RTT → <100km distance
- ***RTT > 10ms not very useful for better than national location.***
  - ...this advice applies to active as well as passive measurement
  - ...and has been used in the design of RIPE infrastructure geolocation

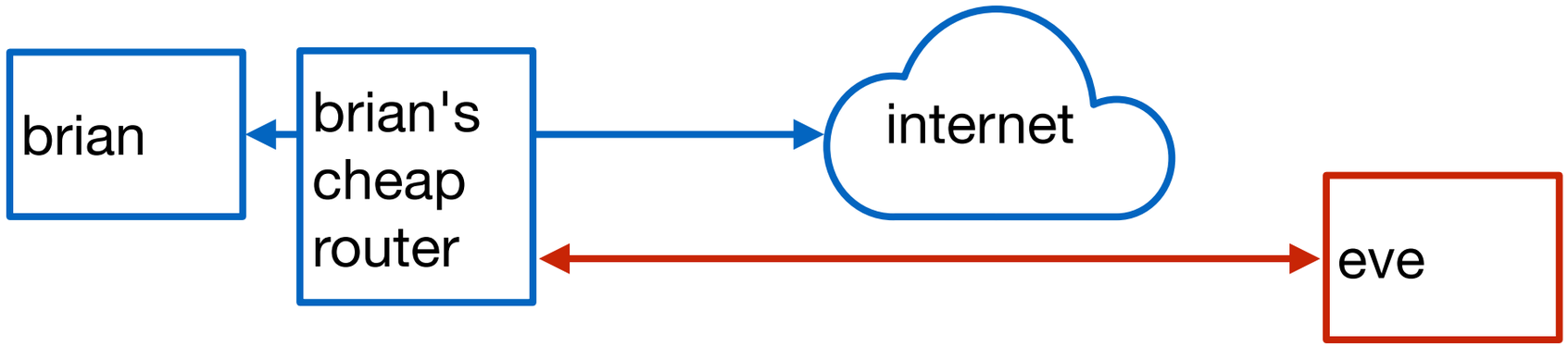
Probabalistic nonparticipation

- The marginal location privacy risk of the spin bit mechanism is negligible.
- But support (or non-support) for the spin bit itself adds to a connection's fingerprint.

- Recommendation: for each connection, roll 1d8, fail to spin if 1. Redo this on path change.
  - Measurement devices can easily separate participating from nonparticipating flows
  - Even with lots of nonparticipation, there's enough signal to get a good RTT on most relevant aggregates

Is Bufferbloat a Privacy Problem?

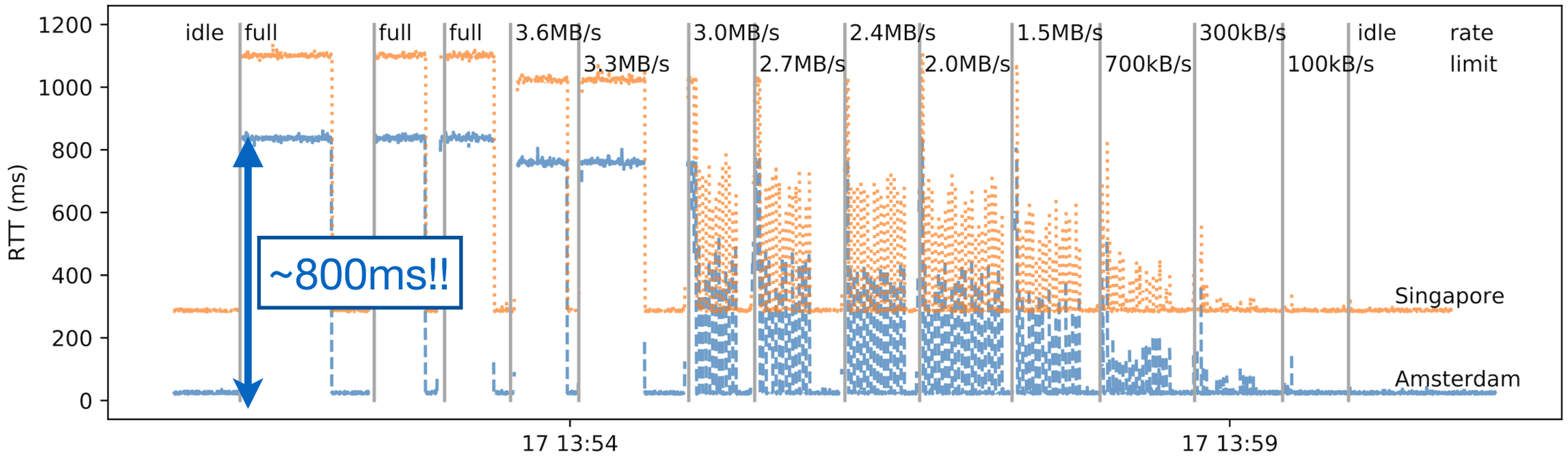
Remote Load Telemetry



- Can a remote entity armed only with *ping* extract information about the operation of machines on my network?

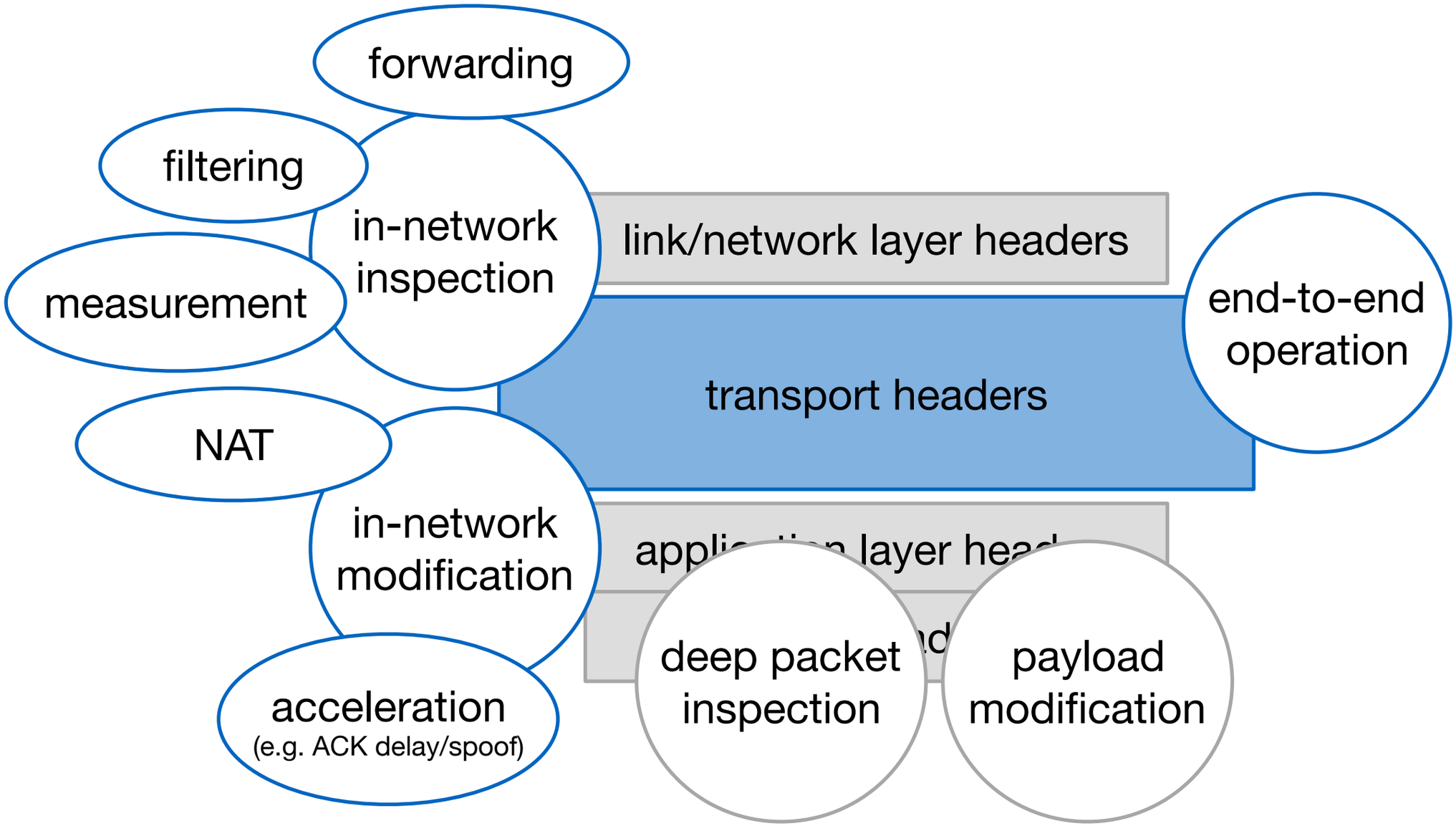
$$load_{net} \propto \sum_{n=0}^{f} D_{queue_n} + \sum_{m=0}^{r} D_{queue_m}$$

Remote Load Telemetry

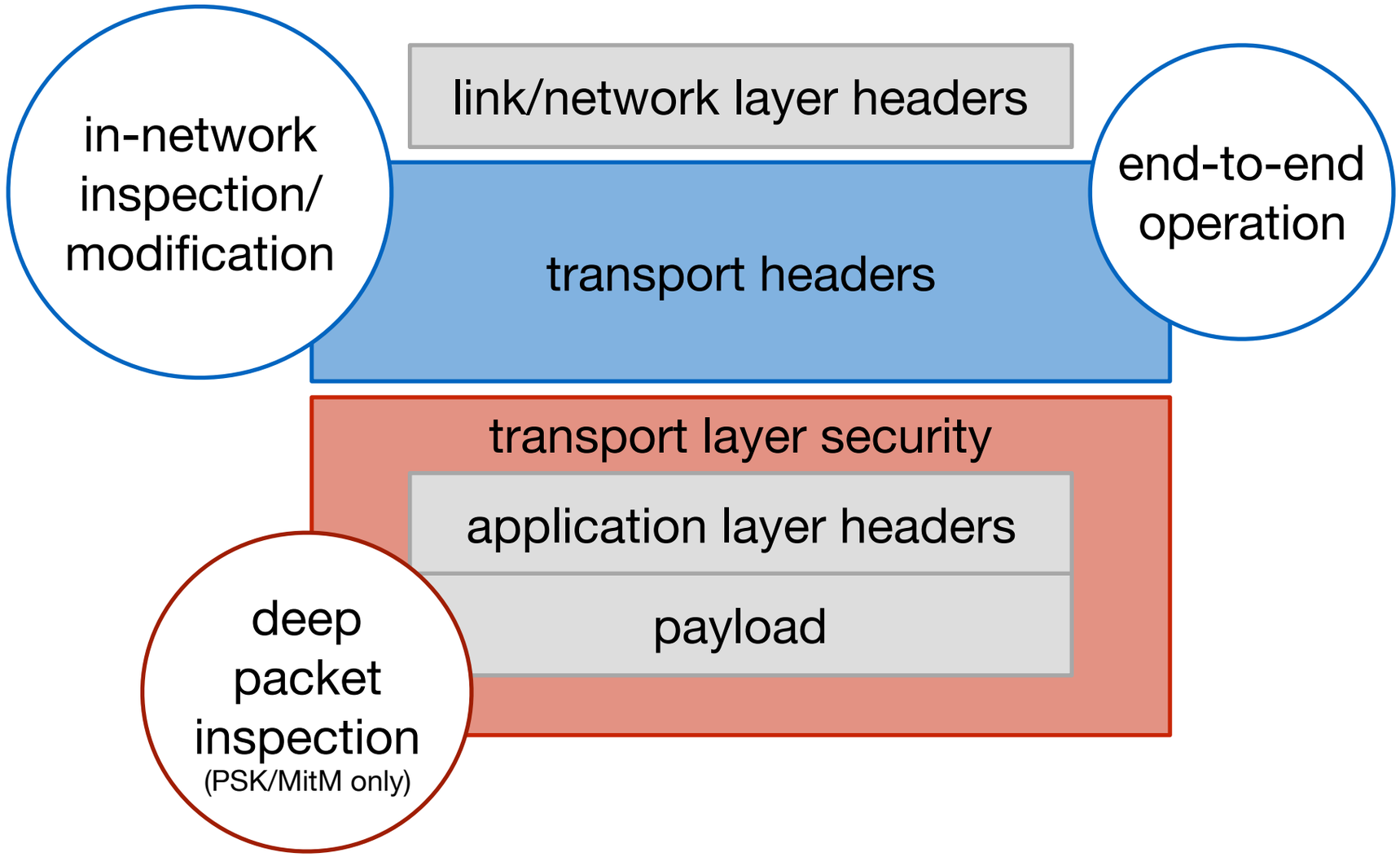


Parting Thoughts

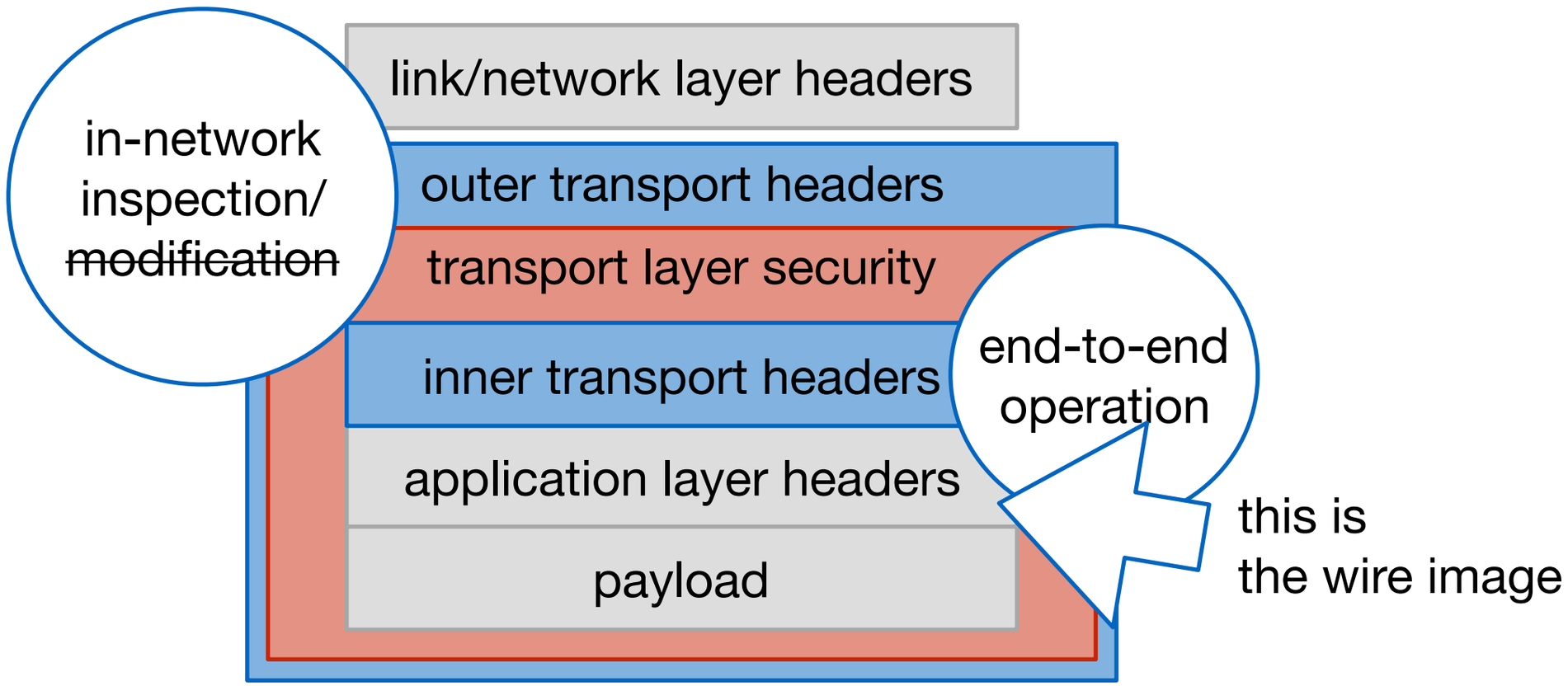
Transport Protocol Design ca. 1990



Transport protocol design ca. 2000



Encrypted transport protocol design: introducing the wire image



The Wire Image: Three levels of accessibility

- Unprotected (as TCP today): all bits can be seen at all points along the path, and can be modified without endpoint knowledge.
  - Supports manipulation of transport internals.
- Integrity-protected (e.g. QUIC outer header): all bits can be seen at all points along the path, but modification is endpoint detectable (and leads to packet rejection).
- Encrypted (e.g. QUIC frame headers): no bits can be interpreted, modification leads to corruption and rejection.

- BUT! the wire image isn't just the bits...
  - Metadata (esp. packet sizes and interarrival sequences) can be used to infer protocol behavior.
  - There is a tradeoff between ease of inference and efficiency on the wire for which there is no universal solution.

RFC 8546 (again)

"A protocol that encrypts its header can be deliberately designed to have a specified wire image that is separate from the protocol machinery."

"When designing the wire image of a network protocol, care must be taken to expose only that information to the network deemed necessary in the protocol's design, and careful design is necessary to reduce the risk that information not explicitly included in the wire image is derivable from its observation."