

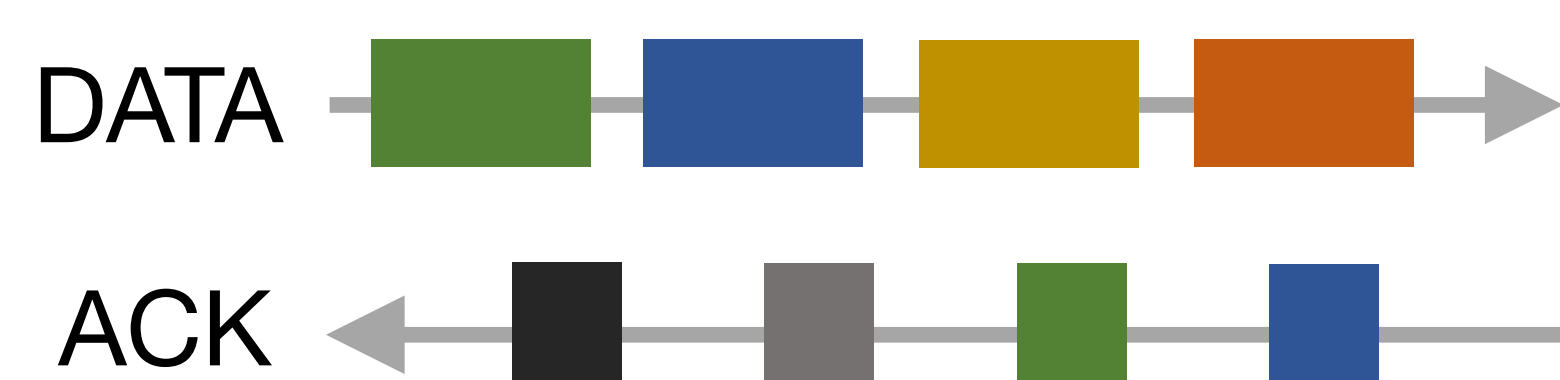
Enhancing encrypted transport protocols with passive measurement capabilities

Tobias Bühler, Mirja Kühlewind, Brian Trammell - ETH Zürich

Transport Protocol Measurement Development

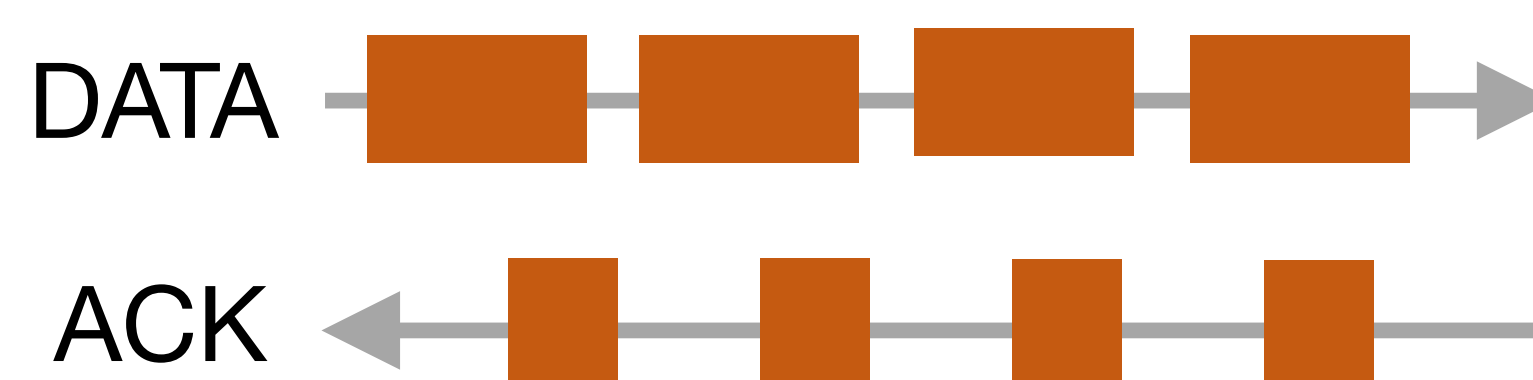
TCP/IP

Cleartext header fields. TCP or higher level information is (mis)used for measurements. No proprietary measurement capabilities.

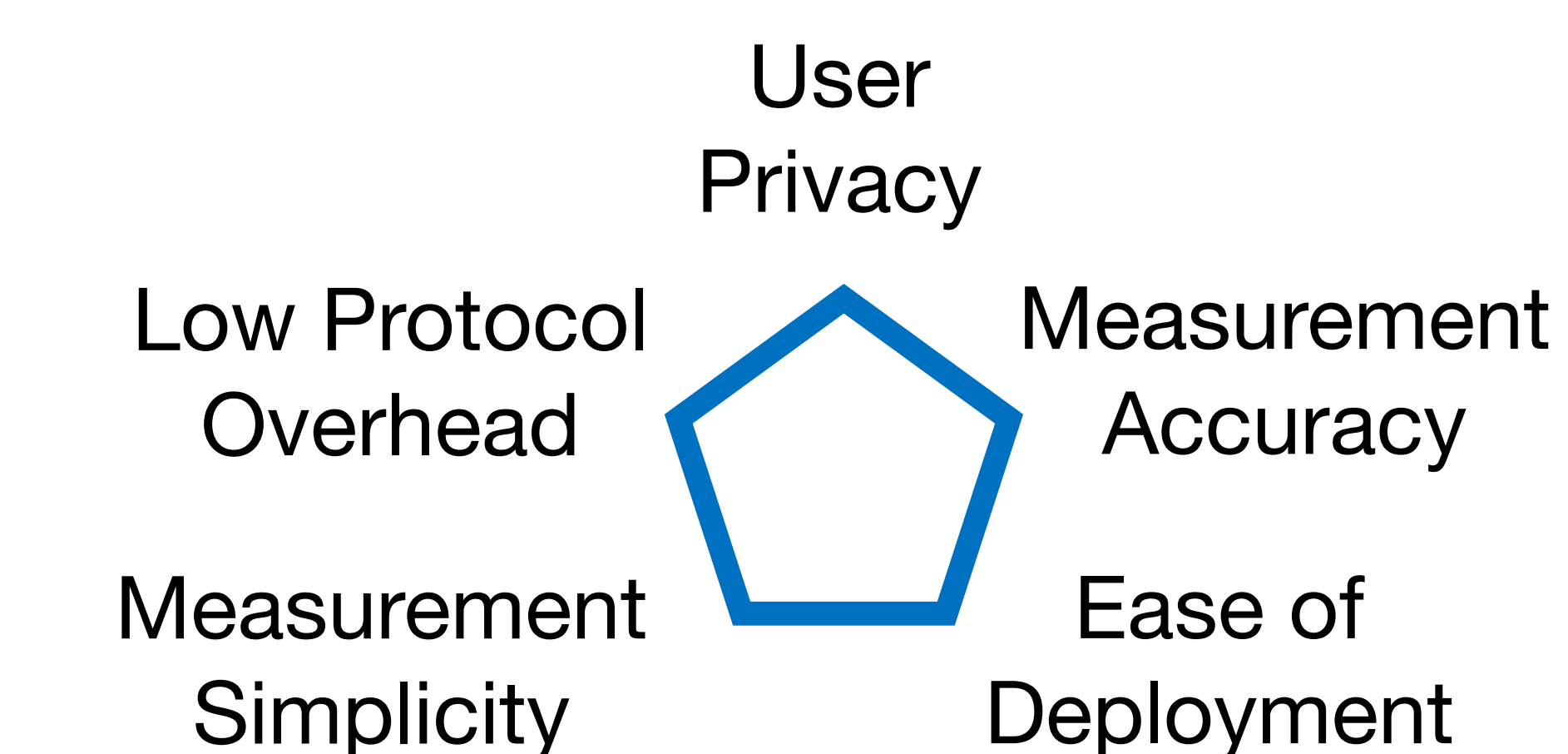


Encrypted (e.g. QUIC)

ACK frames and some header fields are **encrypted**. No packet matching is possible. E.g. RTT measurements are difficult for middleboxes.



Conflicting Goals



Operators still need measurements.

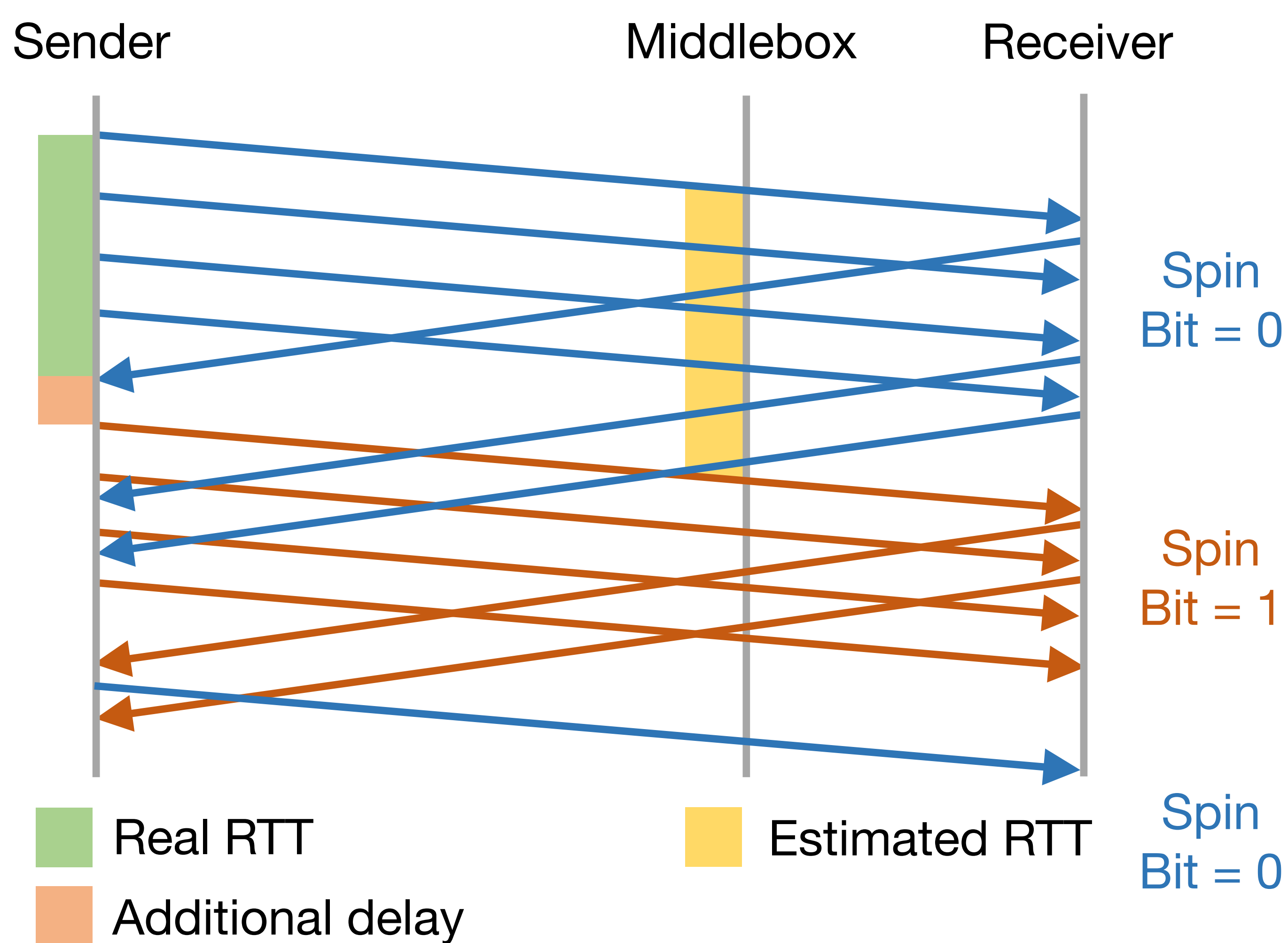
Measurement Approaches

Protocol provides measurement-specific data:

Partially unencrypted wire image.

Packet matching is possible. Examples are:

Packet Number Echo, **Spin Bit**, additional flags



User/endpoints control the amount of dedicated measurement data and the time to expose this data. An endpoint could expose data if:

- problems are detected (e.g. losses or high delay);
- the user privacy is not influenced.

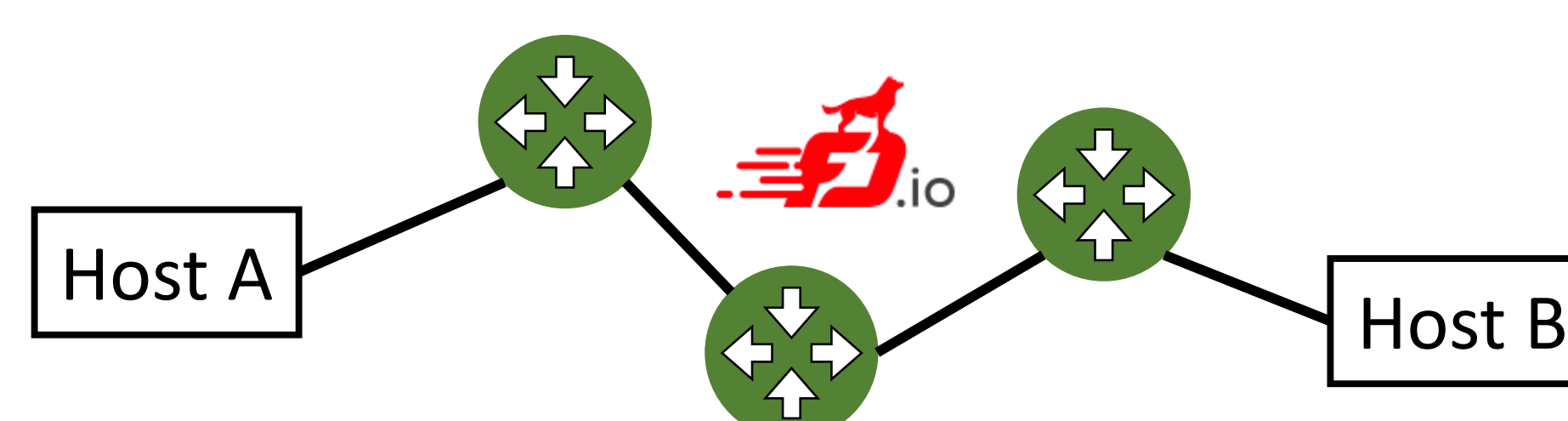
Track encrypted traffic:

Use the observed encrypted packets/payloads to estimate e.g. RTT or packet loss. Possible techniques:

- Use ML to learn traffic patterns which can be used for measurements;
- Infer measurements from coexisting TCP flows.

Implementation

Middlebox implementation: Using the **Fast Data Project (FD.io)**: Fast data processing on generic hardware (in user space/C). Realistic performance.



Endpoint implementation: Tests with an early QUIC implementation in **Go** and custom changes for e.g. packet number echo tests. Comparison with results based on TCP/IP flows.