Spin-bit RTT Evaluation Team Report

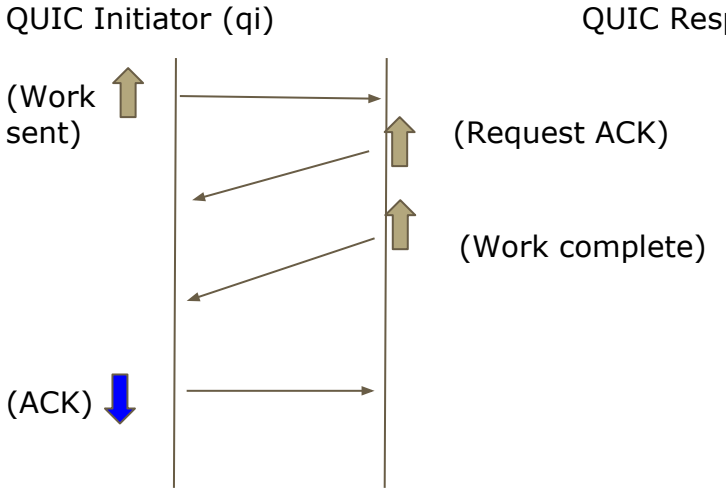
Threat model: geolocation

The design team has consensus that the use of a spin-bit is not a significant new source of geolocation data.

- Tracking handshake RTTs for related IPs gives similar min RTT data.
- The data is very coarse
- Data at better granularity is largely already commercially available.

Beyond Min RTT: Sparse Traffic Issue

Using the spin-bit to track RTT changes requires consistent exchanges between peers. When this is absent, application latency appears as jitter.



Sparse Traffic Examples

Logging applications

Compute-intensive processing applications (e.g. factoring, photo processing)

DNS queries to a caching resolver.

Any unidirectional streams

> For WebRTC-like flows, for example, this would measure the ACK-coalescing responses replacing RTCP

Some examples, like logging, may be insensitive to RTT. App-layer response time can easily dominate the other apps' RTT. All examples ***are*** sensitive to packet loss.

Additional processing

You can reject samples that appear to have sparse traffic characteristics.

- This can be based on fairly simple heuristics, and it will get you aggregate flow latency characteristics that may be better that just tracking handshake RTTs.

You can analyze flow characteristics to infer the traffic type, then conduct the analysis based on the inferred traffic pattern.

- This is somewhat more complex, but you can fall back to sample rejection if it fails. For some traffic types, like ACK-coalesced responses to RTC data, the patterns may be easier to discern than others.

So, is this worth it?

So, is this worth it?

Maybe.

The design team did not come to consensus. The geolocation threat appears negligible and no other threats were identified, but this does provide information to an observer, friendly or adversarial. We're not sure yet what the adversaries would want with it. Network managers would want:

- Rough estimation of the contribution of a leg of a path to latency
- An implicit measure of congestion
- Passive troubleshooting

There are other ways to get each of these, but if present this would get used.

Next steps

Close the design team; we're at stage where full WG discussion would be more appropriate.

The WG should review the output from the hackathon.

We should also consider upleveling this discussion to reconsider other methods for delay and loss detection.

Links

- On the Suitability of RTT Measurements for Geolocation
- Description of a tool chain to evaluate Unidirectional Passive RTT measurement
- Latency-Based Anycast Geolocation: Algorithms, Software, and Data Sets
- Passive Online RTT Estimation for Flow-Aware Routers Using One-Way Traffic
- Passive Measurements in Network for troubleshooting Video Delivery Problems
- QUIC Interdomain Troubleshooting