Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

SPONSORED BY THE
Federal Ministry of Education and Research

Erik Sy, Christian Burkert, Tobias Mueller, Hannes Federrath, Mathias Fischer

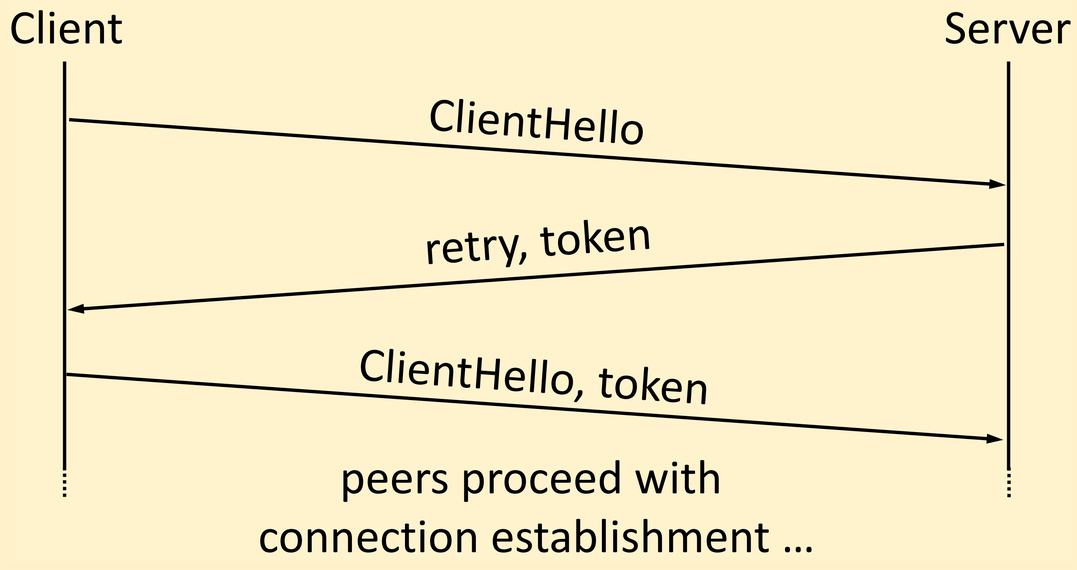
QUICker Connection Establishment with Out-Of-Band Validation Tokens

QUIC is a secure transport protocol that will replace TLS over TCP within the upcoming HTTP/3. An initial QUIC handshake requires two round-trips. The first round-trip accounts for a challenge-response mechanism known as **stateless retry.** This mechanism validates the claimed source address to prevent IP spoofing attacks. The second round-trip is used to conduct the cryptographic connection establishment.

QUIC's Address Validation Token

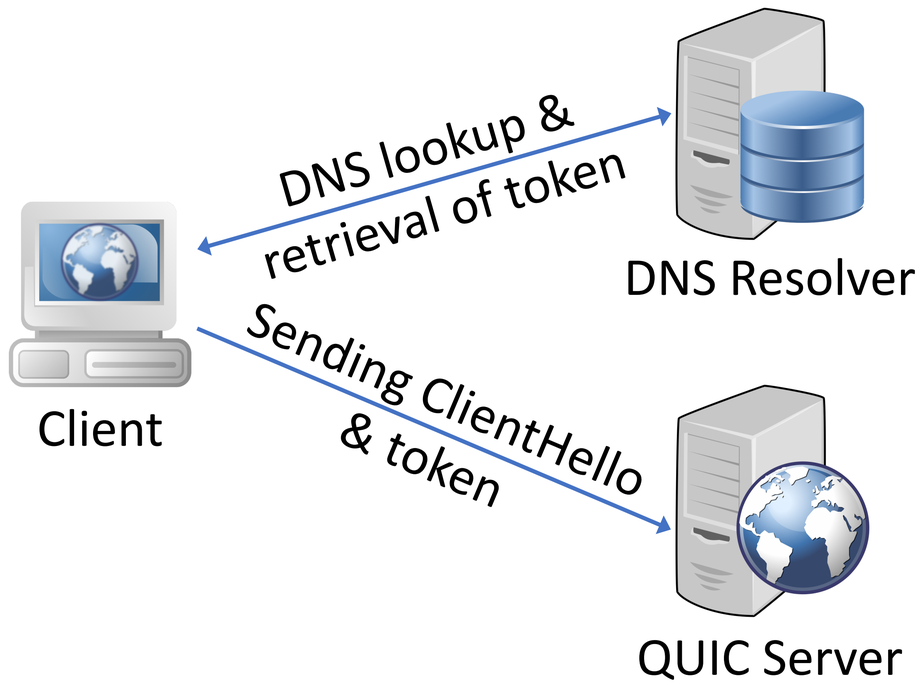
- Opaque to the client
- Difficult to guess
- Single-use to prevent privacy leaks
- Contains information on the client's address
- Lightweight validation of tokens to prevent DoS attacks
- Shared secret key enables multiple entities to issue tokens

QUIC's Stateless Retry



Novel Out-Of-Band Validation Tokens

- Proposal permits a shared address validation between a QUIC server and trusted entities
- Server can revoke trust at any time with immediate effect
- Out-of-band tokens can be issued via QUIC connections to other hosts or via DNS resolvers

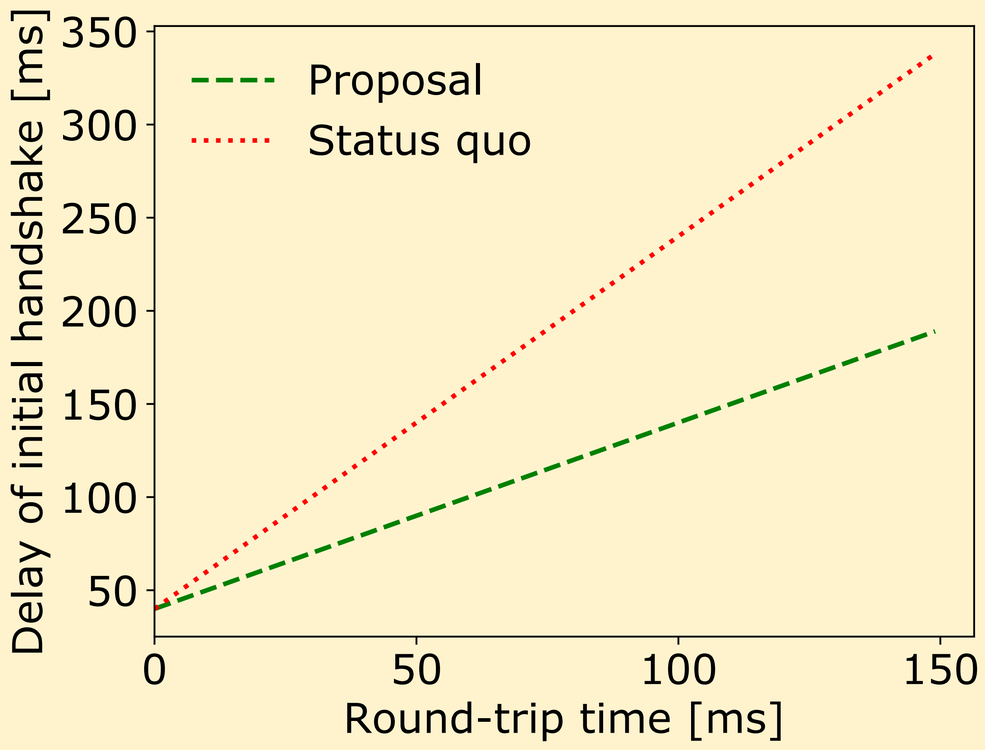


Evaluation

- Proposal allows saving up to 50% of the delay overhead of initial QUIC handshakes
- Distribution via DNS resolvers allows saving a round-trip time for almost all initial QUIC connections

Future Work

- Protocol to establish the required trust-relations and subsequently share, update, and revoke the secret keys required for issuing these tokens



44th IEEE Conference on Local Computer Networks (LCN), October 14-17, 2019, Osnabrück, Germany