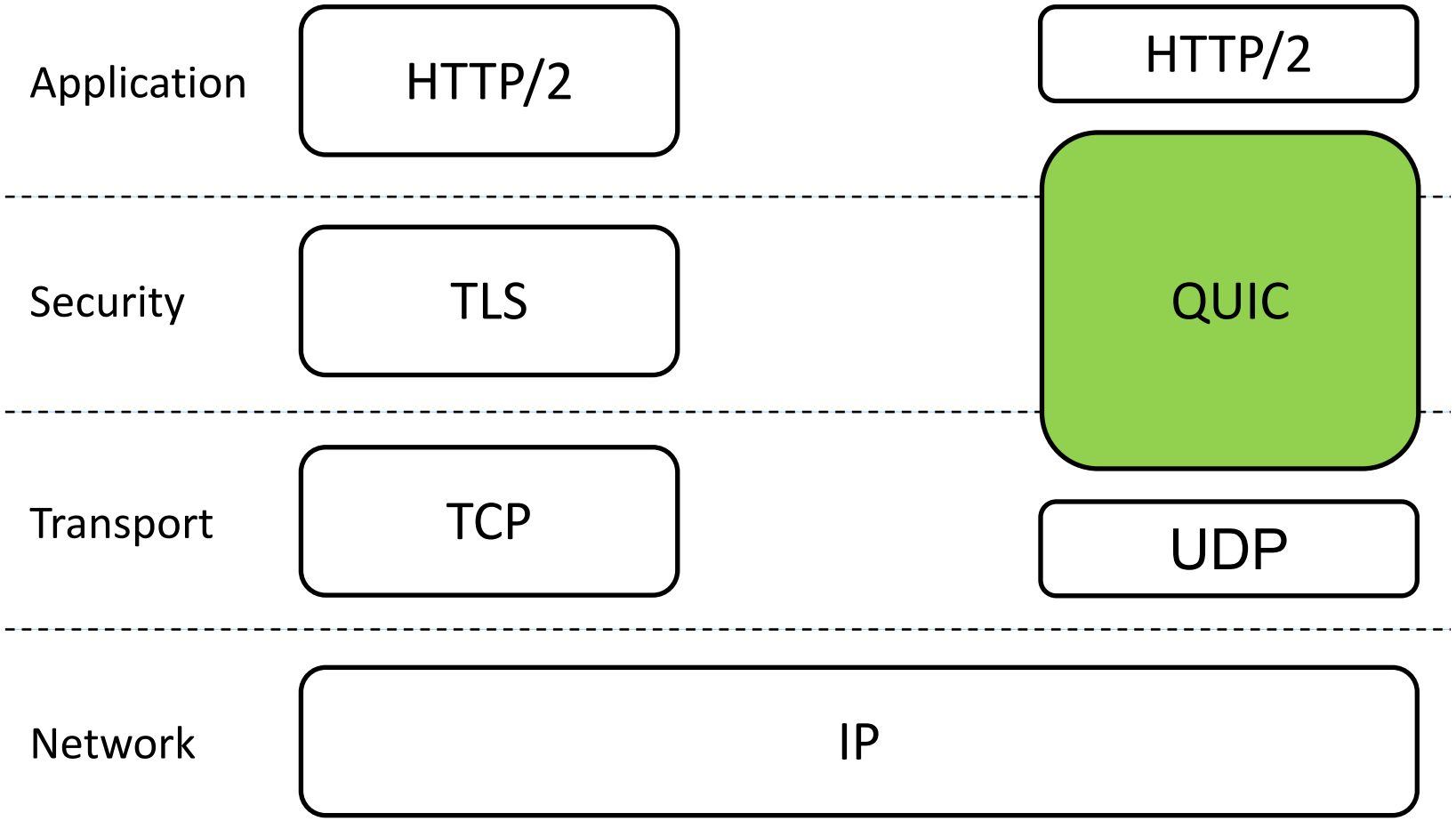
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

21st September 2019
SoftCOM 2019

Surfing the Web Quicker Than QUIC via a Shared Address Validation

Erik Sy

Introducing QUIC

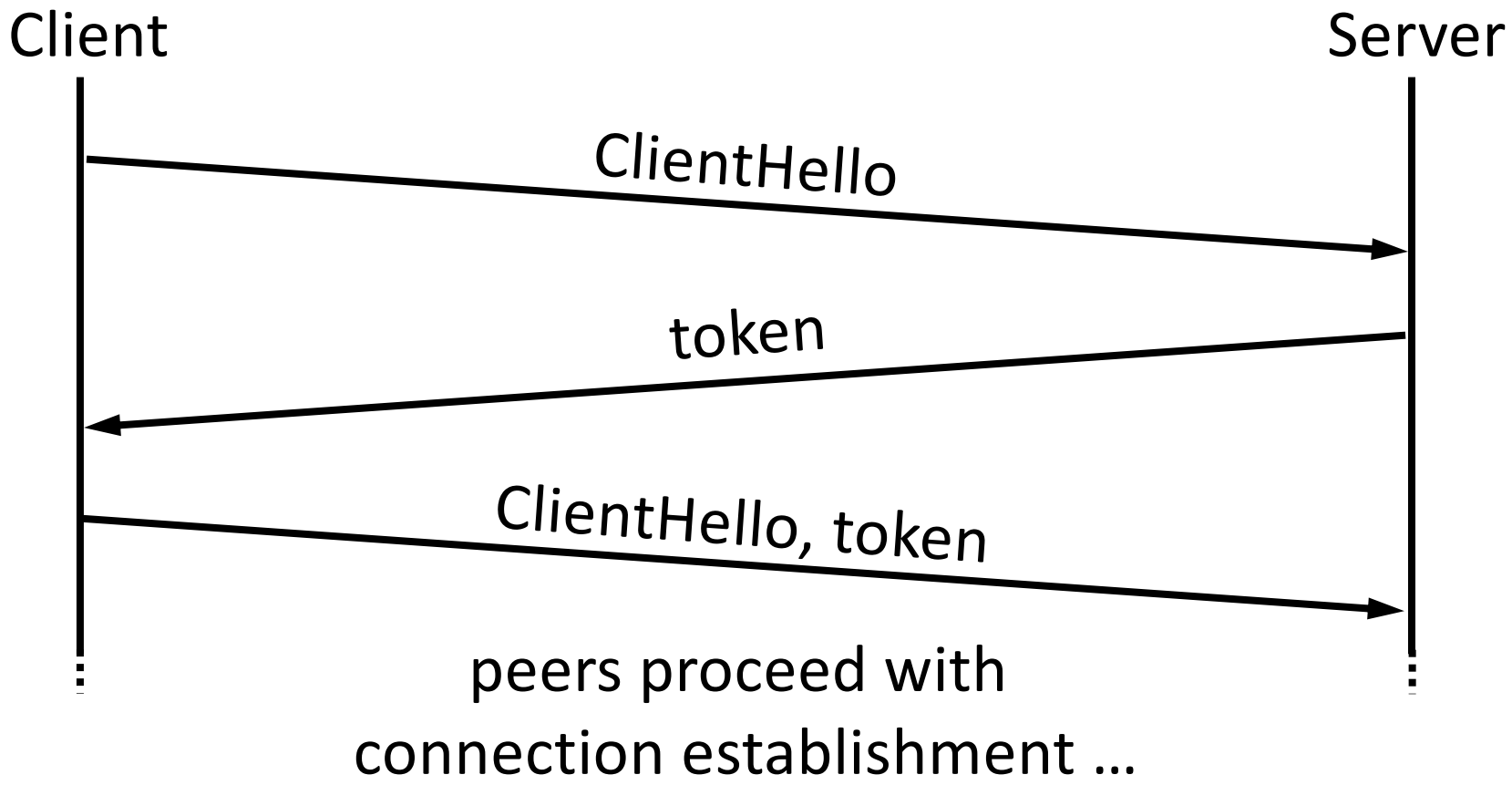


Introduction to the QUIC Transport Protocol

- QUIC is going to replace TLS over TCP in HTTP/3
- Improves problems of TLS over TCP
  - Protocol Entrenchment
  - Implementation Entrenchment
  - Handshake Delay
  - Head-of-line Blocking
  - Mobility

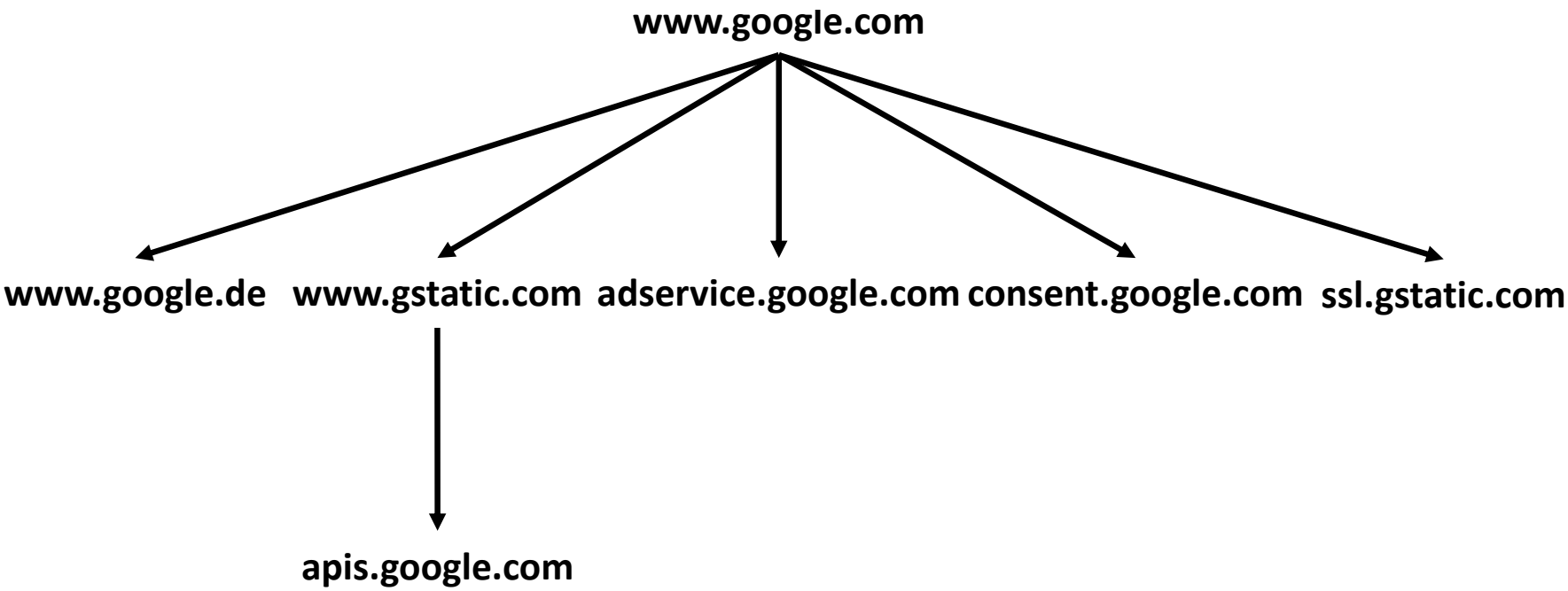
QUIC's Source-Address Validation

- Source-address token speed up the validation of the client's IP address in subsequent connections between the same peers



Domain Trees of popular Websites

- Alexa Top 1K Site requires on average 20.24 connections to different hosts
- These hostnames form on average 9.49 TLS trust groups[1]



1: Sy et al. “Enhanced Performance for the encrypted Web through TLS Resumption across Hostnames” (2019)

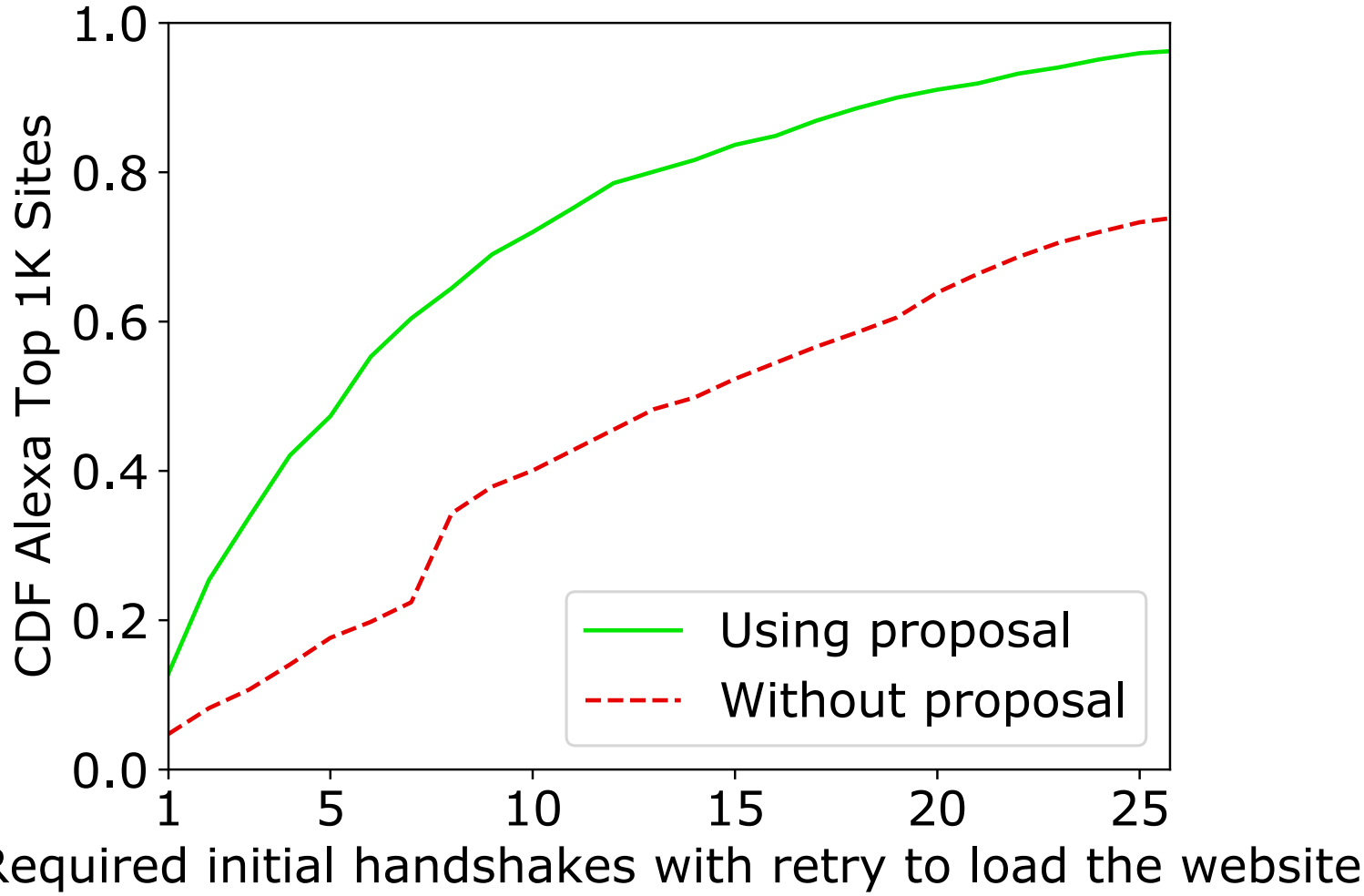
Shared Client IP Address Validation

- QUIC server having a TLS trust-relation accept source-address tokens generated by each other
  - each accepted source-address token allows client-server pair to save a round trip time during the connection establishment

- Novel QUIC transport parameter is used to inform the client about other hosts accepting a provided validation token

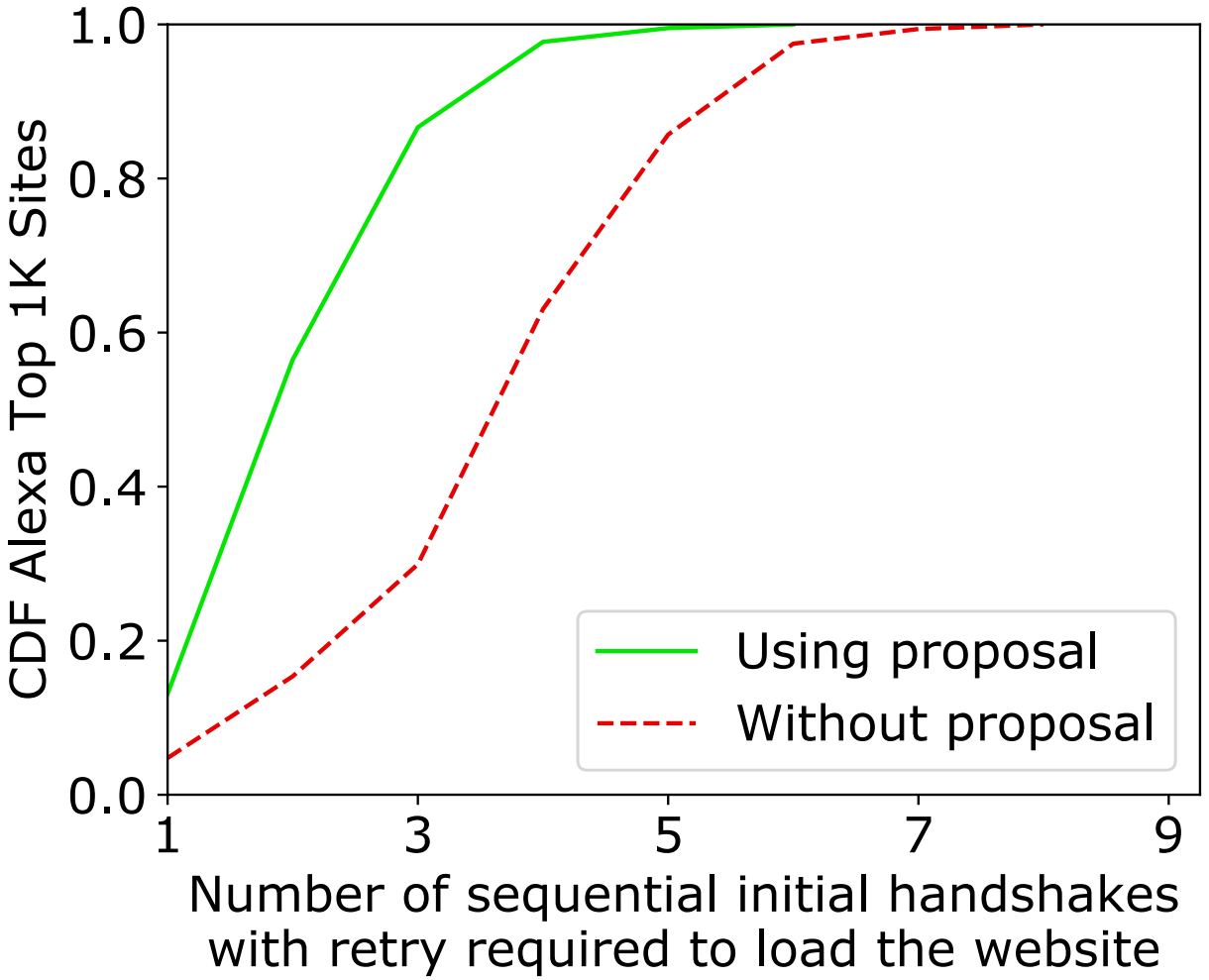
Performance Improvements for the average Website (1/2)

- Proposal saves a round-trip time on 58.75% of the established connections



Performance Improvements for the average Website (2/2)

- Longest path of sequential connections with retry is reduced by 39.1%



Conclusion

- Proposal provides great performance improvements for QUIC's connection establishment during web browsing
- IETF aims to include a shared address validation in a future QUIC version

Thank you

Questions and Answers

E-mail: SoftCOM@erik-sy.de

Slides: https://erik-sy.de/softcom