Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

19th June 2019
COSIC Seminar

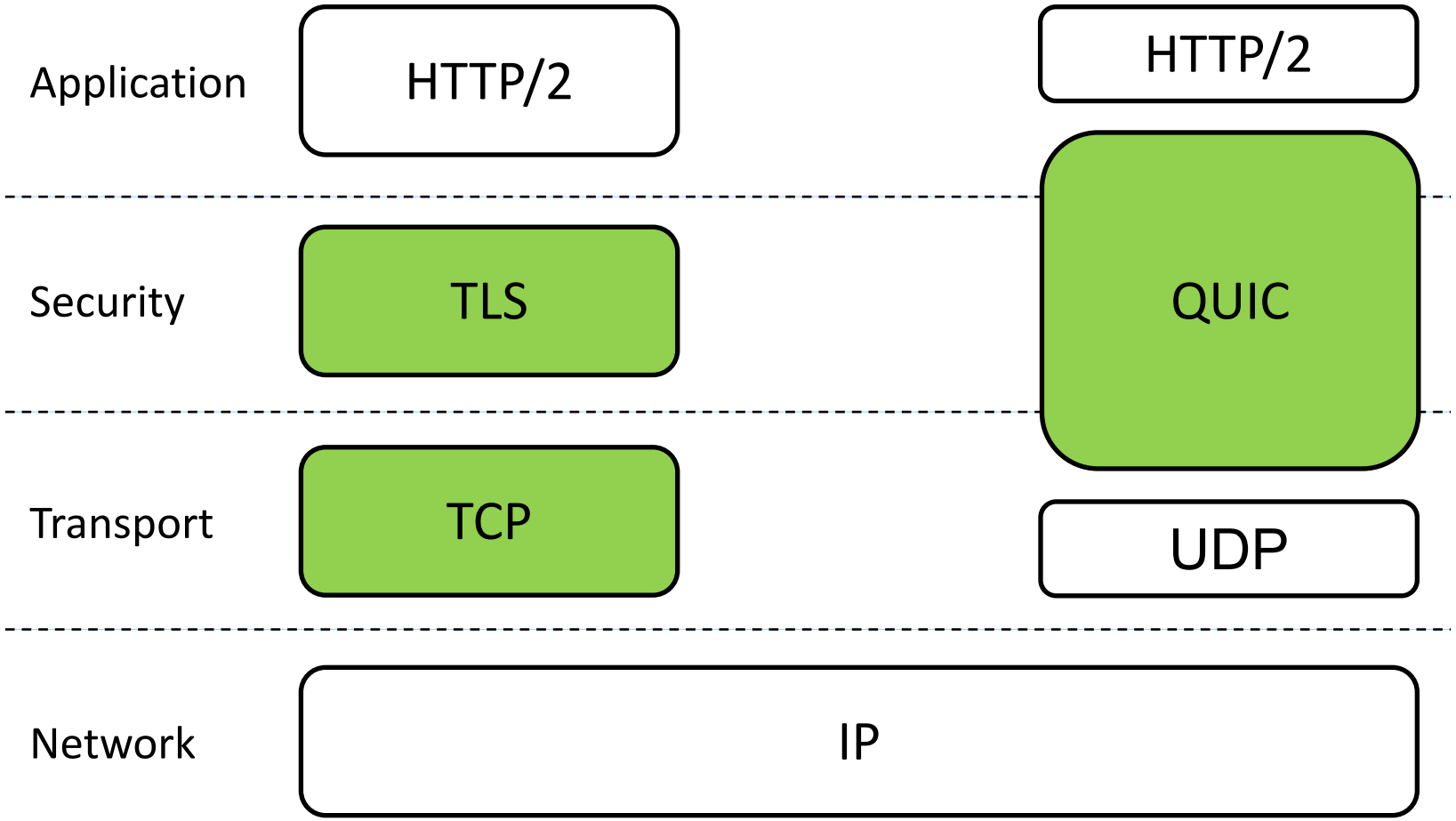
Improving the Performance and Privacy of TCP Fast Open, TLS 1.3 and QUIC

Erik Sy

Motivation

- Faster connection establishments
  - increase the revenue of online service provider
  - increase the quality of experience for web users
- Better privacy protections
  - web tracking through network-based attackers has no user consent
  - transport protocols are not designed to provide a mechanism for legitimate web tracking

Investigated Protocols



Deployed Attacker Model

- Attacker can only use the investigated protocol to learn the client's identity
- Attacker is able to conduct passive as well as active attacks
- Attacker cannot compromise the client's endpoint
- Attacker cannot break the deployed cryptography
- Attackers include online service provider and internet service provider

(CC BY 4.0) from Twitter

Introduction to TLS Resumption

- Allows a client-server pair to establish a new TLS connection with a previously exchanged symmetric key
  - Provides temporal and computational performance gains
  - The client is identified by the server through knowledge of this secret key

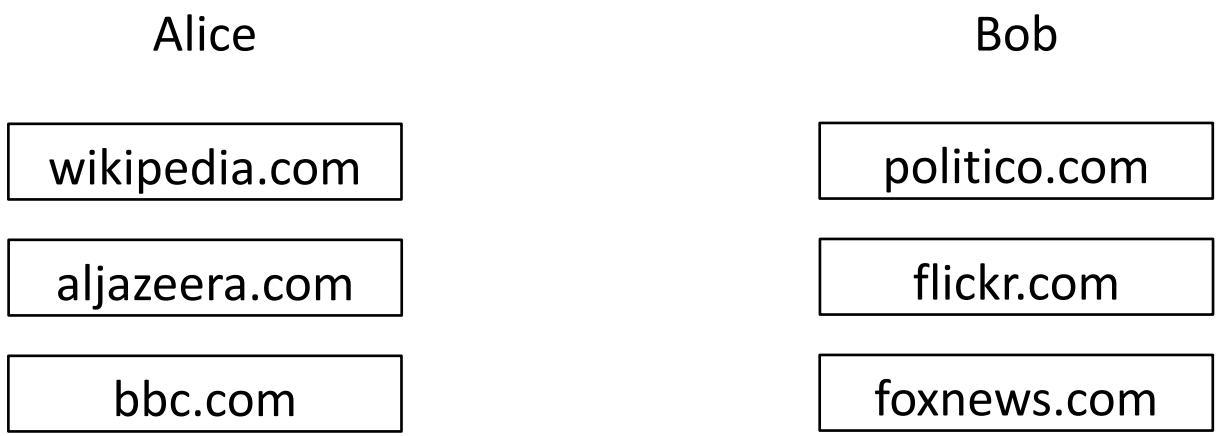
- Deployment on the Internet
  - 96% of TLS-enabled Alexa Top Million Sites support TLS resumption
  - Google/Cloudflare report a share of approx. 50% of their connections to be established through TLS resumption

Introduction to Token-based Source Address Validation

- Aims to validate the client's source address without the delay of an additional round-trip
- Client receives opaque token in a previous connection
- Token is consumed by the server issuing the token
- Token contains information on the client's publicly visible source address
- Upon receiving the connection request, the server validates the claimed source address by comparing it to the address encoded in the token

Privacy Considerations for Transport Protocols

- User identification becomes feasible across two connections if the latter connection reuses cached state of the previous one
- These mechanisms do not rely on tracking via IP addresses, HTTP cookies, browser fingerprinting, ...
- Third-party trackers can identify users across several websites



Tracking via TCP Fast Open Cookies

- TCP Fast Open (TFO) was standardized in 2014
- Supported by Chrome, Microsoft Edge, and Firefox
- TFO cookies are cached by the client and presented during a future connection establishment to the same server IP address and port

- Main findings
  - allows unrestricted tracking periods
  - enables tracking across private browsing modes, browser restarts and different applications

- Countermeasures
  - Mozilla stopped using TFO within Firefox
  - Microsoft stopped using TFO within the private browsing mode of Edge

Tracking via TLS Session Resumption

- Affects all SSL and TLS versions including TLS 1.3
- All major browsers support TLS session resumption mechanisms
- As a performance optimization, peers authenticate each other in a resumed session based on a previously exchanged cryptographic secret

- Main findings
  - browsers limit feasible tracking periods but prolongation attack allows to extend the tracking periods for frequently visited domains

- Countermeasures
  - Mozilla mitigates third-party tracking via this mechanism by allowing session resumption only for matching websites

Tracking via QUIC's Address Validation Tokens

- Affects Google QUIC (gQUIC) and IETF QUIC
- Supported by Chrome with more than 60% browser market share
- Tokens are cached by the client to abbreviate the handshake of a future connection

- Main findings
  - allows unlimited tracking periods by online service provider
  - protects against tracking via network-based attackers

- Countermeasures
  - Google Chrome restricts tracking periods to one week

Tracking via QUIC's Server Config

- Affects only gQUIC
- Server config is cached by the client across several connections to conduct the cryptographic connection establishment
- Tracking feasible, if server issues unique server config's to it's clients

- Main findings
  - allows unlimited tracking periods
  - may enable a network-based attacker to track user's

- Countermeasure
  - Chrome's transition from gQUIC to IETF QUIC solves the problem

Future Work: Privacy Configuration of connection-oriented DNS

- Connection-oriented, encrypted DNS becomes more popular
  - makes uses of TLS session resumption, TFO to accelerate connection establishment

- Research question
  - Do the default configuration of DNS implementations protect against tracking?
  - real-world impact evaluation based on our DNS traffic data set

Future Work: 0-RTT TLS Handshakes with Client Unlinkability

- Using a hybrid cryptosystem for repeated connections between endpoints instead of reusing a previously exchange symmetric encryption key

- Research questions
  - What are the costs (computations, network traffic, storage) of such privacy-friendly design compared to the status quo?
  - Can we achieve a stateless design?
  - How do we protect against server that decrease the size of anonymity sets by rotating their public keys too quickly?

Future Work: Privacy-friendly Address Validation Tokens

- Applying concepts of anonymous e-cash to QUIC's token generation
- Authentication based on a previously successfully established connection

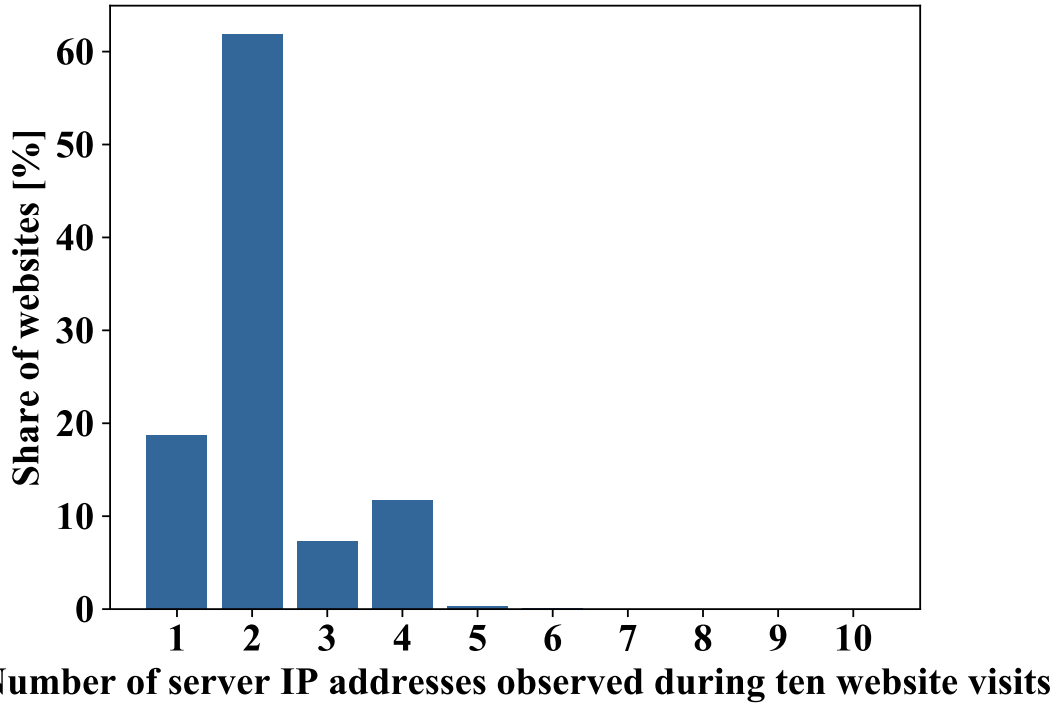
- Research questions
  - What are the costs (computations, network traffic, storage) of such privacy-friendly design compared to the status quo?
  - Can we achieve a stateless design?
  - How do we protect against servers that decrease the size of anonymity sets by rotating their public keys too quickly?

Performance-optimizations for Transport Protocols

- The delay of the connection establishments presents a significant overhead of an average web flow
- Accelerating handshakes can be achieved by reducing the number of required round-trips

Improved Performance with TCP Fast Open Privacy

- Hosting of websites uses several IP addresses
  - TFO has a high failure rate for revisits of websites
- Token should be bound to domain name
  - saves about 83.4 ms during 1st revisit using LTE connection (RTT= 60ms)

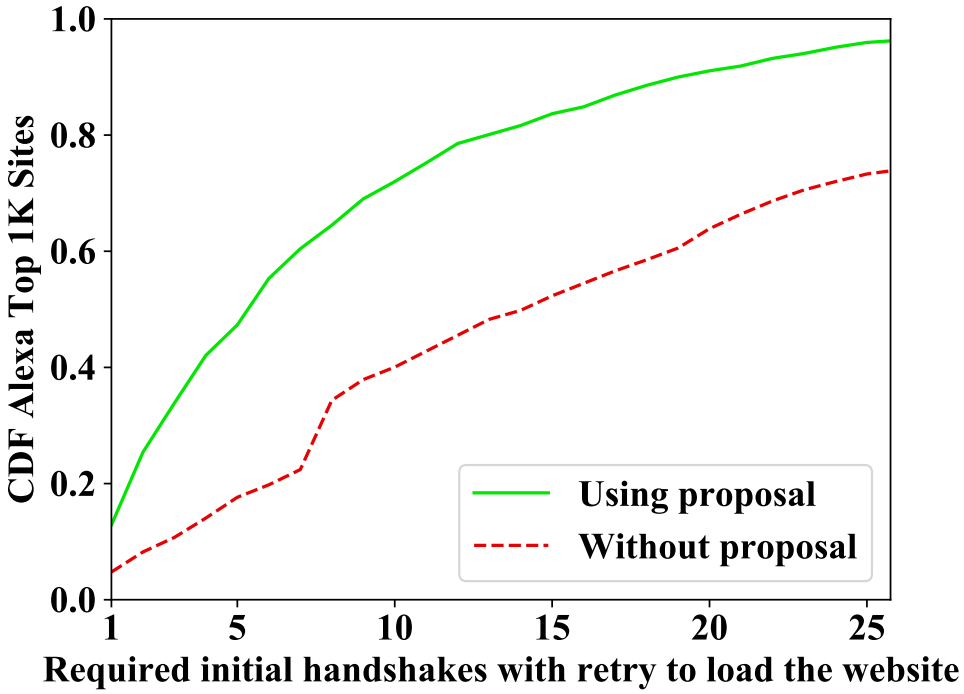


Improved Performance with TLS Resumption across Hostnames

- Currently, TLS recommends resumption handshakes only for matching hostnames
- Proposal to resume sessions among all hostnames for which the presented server certificate is valid
- Savings for an average website visit
  - converts about 59% of the required full handshakes to resumed connection establishments
  - up to 30.6% of the time to establish all TLS connections
  - up to 44% of the CPU time to establish all TLS connections
- Proposed as an TLS extension within the TLS working group (IETF)

Improved Performance with Address Validation across Hostnames

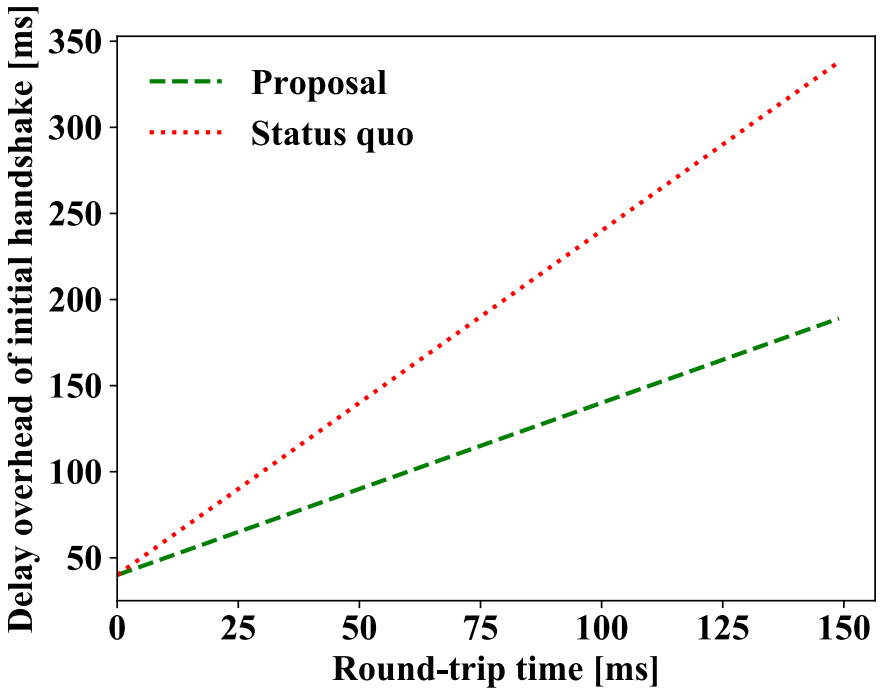
- Currently, QUIC uses address validation tokens only for matching hostnames
- Proposal to do address validation among all hostnames for which the presented server certificate is valid



- QUIC working group (IETF) considers this to become a feature of QUICv2

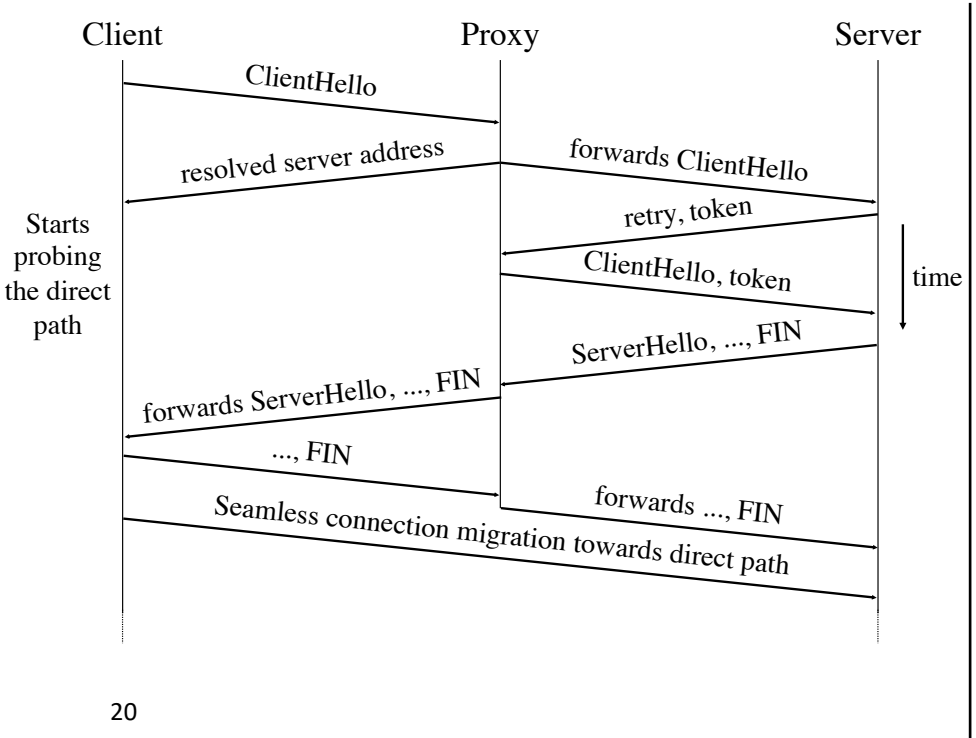
Improved Performance with QUIC's Out-of-Band Tokens

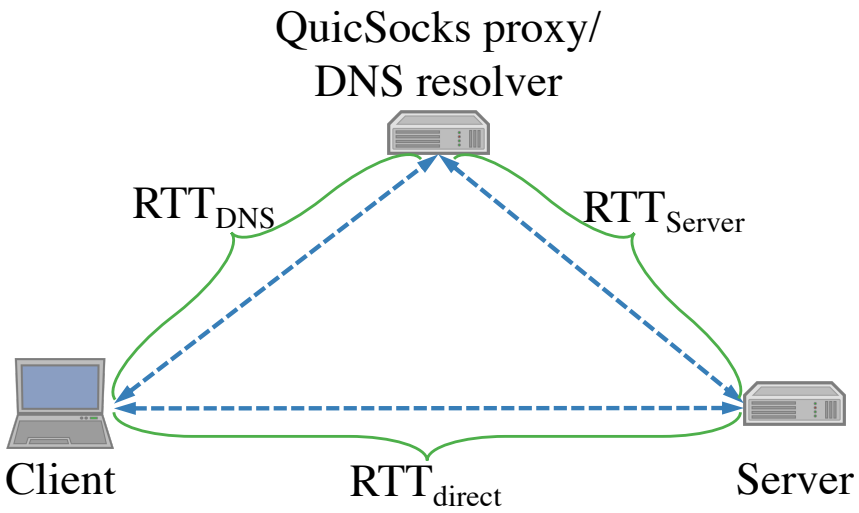
- Distribution of address validation tokens via DNS resolver or other QUIC server
- Consuming QUIC server can always revoke keys of issuing entity
- Up to 100% of connection establishments enforcing address validation can save a round-trip time via this proposal



Future Work: QuicSocks Proxy collocated with DNS resolver

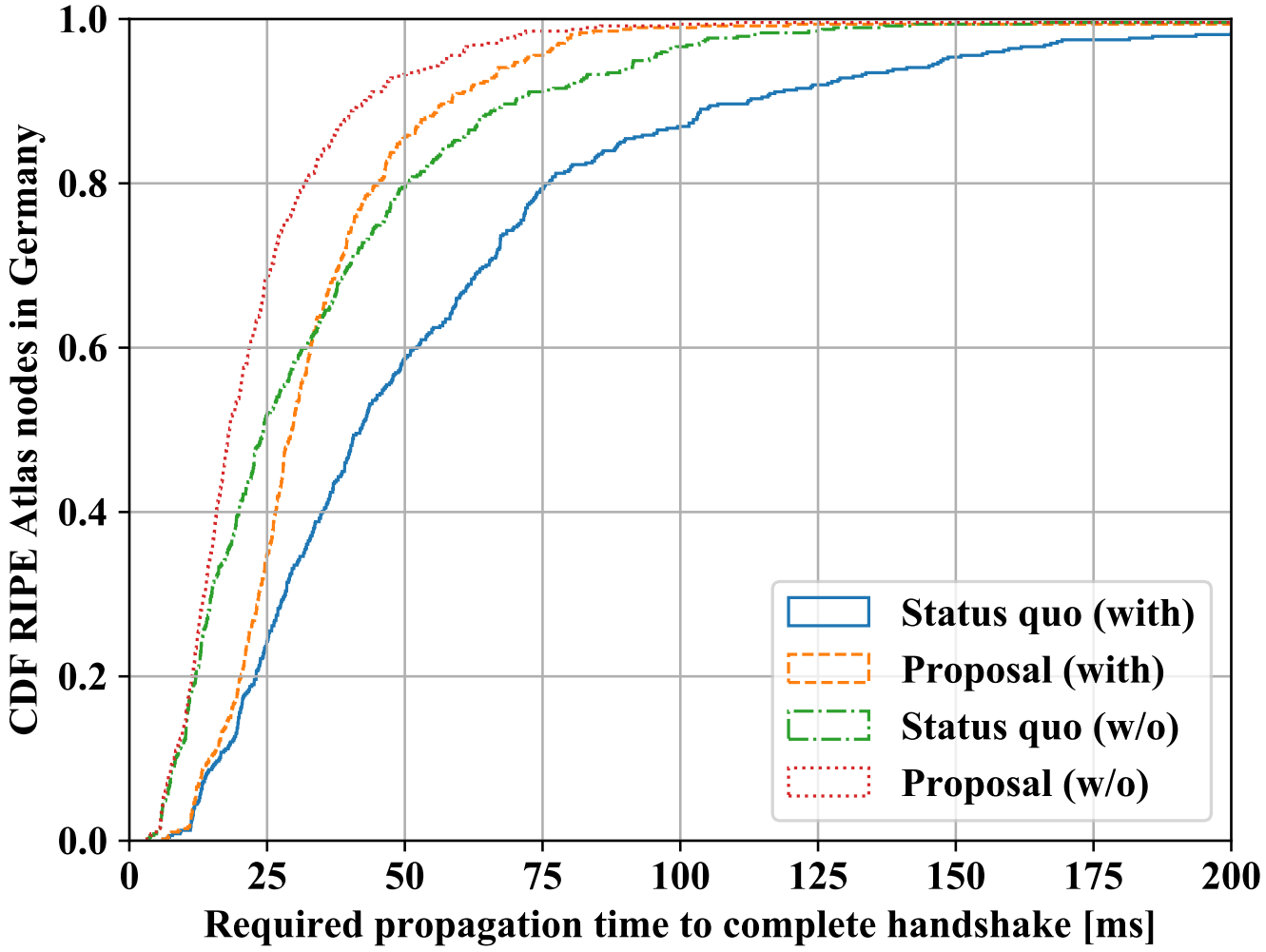
- High latency networks exists
  - plans for Global Low Earth Orbit Satellite Internet Access by OneWeb, SpaceX, Telesat with latency > 30 ms
- Proposal beneficial if $RTT_{Server} < RTT_{direct}$
- Connection migrates to direct path after the handshake





Early results: QuicSocks Proxy collocated with DNS resolver

- Experiments with 800 RIPE Atlas nodes in Germany



Future Work: Resolver-less DNS

- DNS resolver present a privacy and performance problem
- Why doesn't a web server provide the client DNS records for it's linked third-party resources?
  - saves the delay and privacy effects of DNS lookups
  - server does EDNS client subnet whenever required (may start early upon receiving TCP SYN)
- Web is moving towards an encrypted ecosystem
  - trusts received DNS records if the domain name is authenticated via TLS
- Trust in DNS records is anyway a problem and currently unsolved

Conclusion

- Let’s make the web faster
- Let’s make transport protocols privacy-friendly

Improving the Performance and Privacy of TCP Fast Open, TLS 1.3 and QUIC

Erik Sy