DR. QUIC:
Decoy Routing via the QUIC Protocol

Federico Cifuentes-Urtubey, Sanjeev Reddy, Tanya Verma
Department of Computer Science, University of Illinois at Urbana-Champaign

Decoy routing (also known as refraction networking) is an anti-censorship approach that discreetly routes client traffic to blocked sites via 'decoy routers' located outside the censoring ISP [2]. We propose DR. QUIC as a proof-of-concept decoy routing scheme that uses the QUIC protocol to streamline connection interception and rerouting. We aim to simplify the process of connecting to the censored site by avoiding the TCP-based flows of existing decoy routing solutions.

Anti-Censorship with Decoy Routing

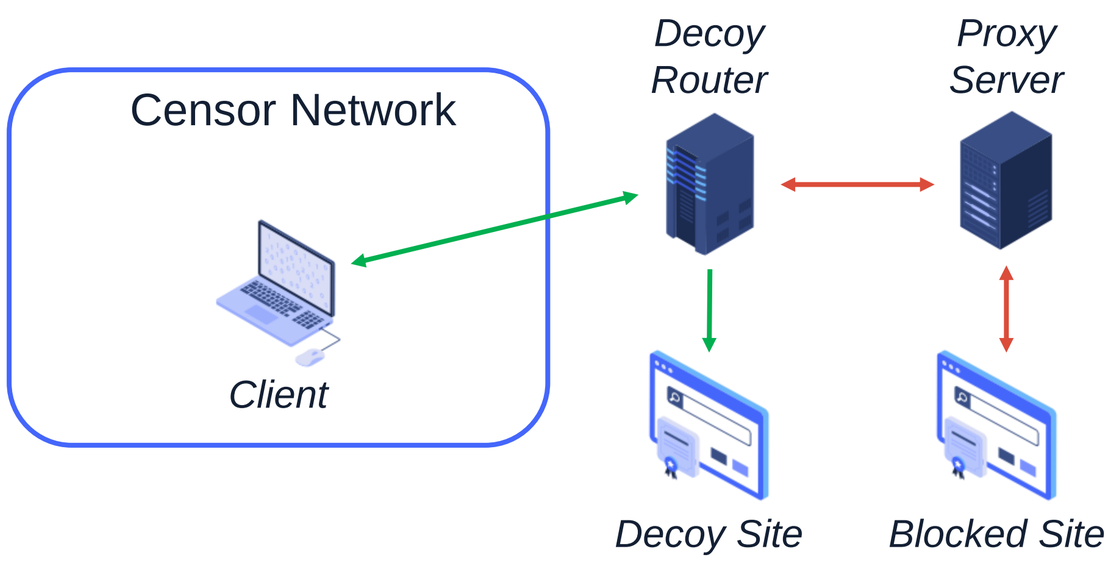

Figure 1: Traditional decoy routing. Green arrows represent censor-allowed traffic. Orange arrows represent a covert (secret) connection.

DR. QUIC's Design and Motivation

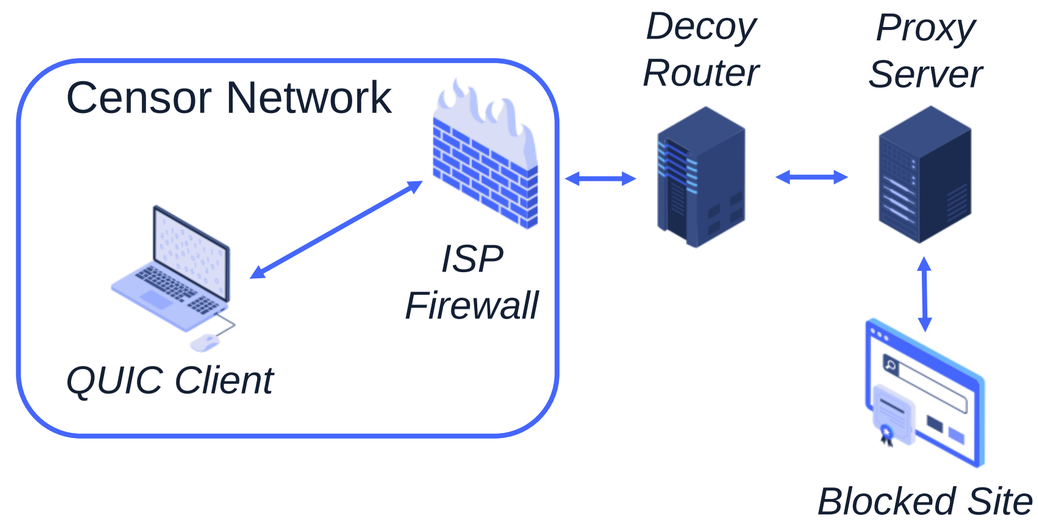

Figure 2: DR. QUIC test topology

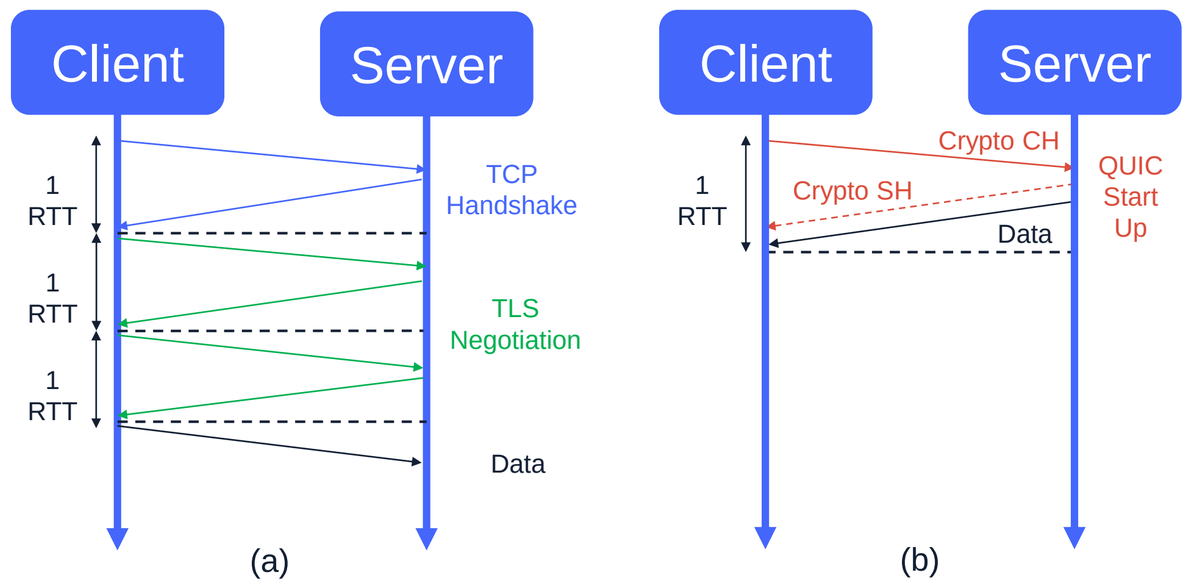

Figure 3: HTTP+TLS (a) vs. QUIC handshakes (b)

Related Work

Telex [4]
Intercepts an HTTPS connection to an unblocked site and redirects to a blocked site via a tag-detecting relay.

Cirripede [1]
Intercepts a TLS connection to an unblocked site. Makes use of a separate registration server to help client and proxy establish a shared TLS secret during the redirect.

Tapdance [3]
Client sends a tagged HTTP request over TLS to a decoy site. A relay station observes the tag and establishes a non-blocking flow to the covert destination.

The Problem
All of these TCP-based solutions require knowledge and maintenance of the initial connection's state, creating logistical overhead during the redirection process.

Evaluation

Can QUIC be used to connect clients to censored websites in a decoy routing scenario?

QUIC traffic is read by routers as encrypted UDP traffic. Decoy connections successfully pass through our destination-based firewall and are detected and forwarded by the decoy router.

Our proxy server establishes a QUIC tunnel between the client and the blocked site. The censor cannot detect the presence of blocked content within incoming packets.

References

[1] Houmansadr, A. et al. Cirripede: Circumvention infrastructure using router redirection with plausible deniability." In *ACM CCS '11. DOI:10.1145/2046707.2046730*

[2] Karlin, J. et al. Decoy Routing: Toward Unblockable Internet Communication. In *USENIX FOCI '11.*

[3] Wustrow, E. et al. Tapdance: End-to-middle anticensorship without flow blocking. In *USENIX Security Symposium '14.*

[4] Wustrow, E. et al. Telex: Anticensorship in the Network Infrastructure. In *USENIX Security Symposium '11.*

Future Work

Analyze latency differences between QUIC and TCP
QUIC eliminates tracking connection state and the 3-way TCP handshake. There may be a noticeable difference in latency when serving (censored) requests.

Test active traffic analysis attacks
Pure UDP connections are uncommon. Active analysis may expose differences between DR. QUIC's and a regular client's traffic to the same overt destination.