Cooperative Performance Enhancement Using QUIC Tunneling in 5G Cellular Networks

Zsolt Krämer, Budapest University of Technology and Economics (presenter)
Mirja Kühlewind , Ericsson Research
Marcus Ihlar, Ericsson
Attila Mihály, Ericsson Research

Transport layer performance in 5G networks

- 5G deployments are going to introduce new characteristics to cellular networks:
  - Very high peak data rates
  - Significantly decreased delay
  - High volatility in available bandwidth

- Increased need for a shorter control loop and local optimizations

- In LTE networks, this has been implemented by PEPs (Performance Enhancing Proxies)

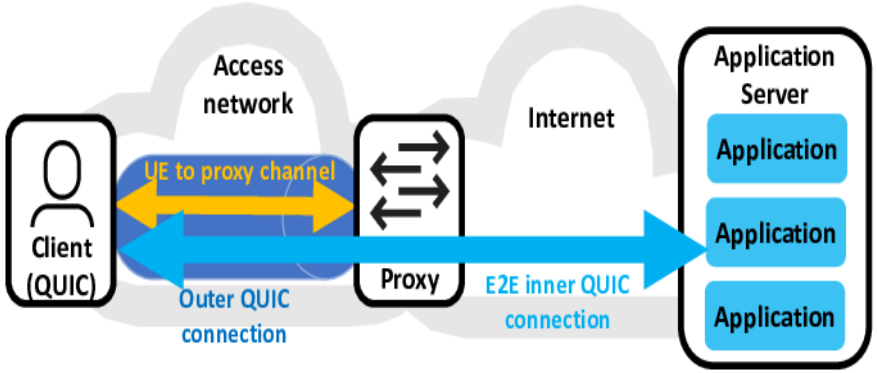
QUIC: Challenges of managing encrypted traffic

- Standardized recently as RFC 9000, and already widely deployed by Google
- Fully encrypted transport, resulting in enhanced privacy for users
- The end-to-end encryption makes connection-splitting solutions impossible
- A new approach is needed to enable network-assisted performance optimization for QUIC in cellular networks

Cooperative Performance Enhancement I

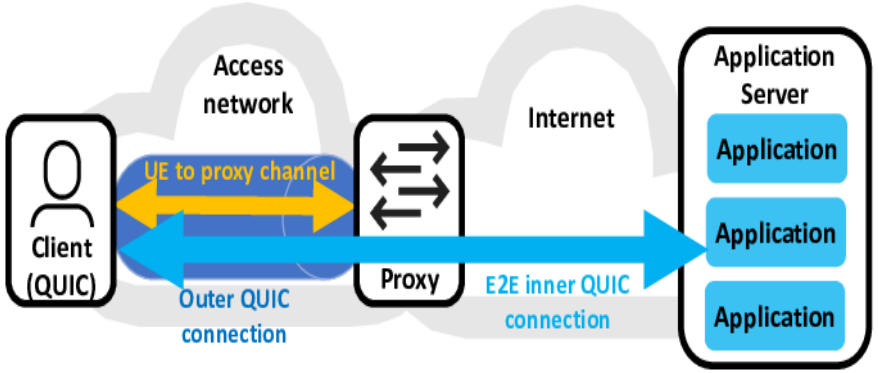
- Using MASQUE as the signaling protocol towards the proxy

- Two layers of connections:
  - QUIC tunnel between client and proxy
  - End-to-end QUIC connection between client and server



Cooperative Performance Enhancement II

- The security context of the end-to-end connection is unmodified
- Explicit consent is required for requesting a service
- Separate QUIC streams for communication channel data and tunnel data

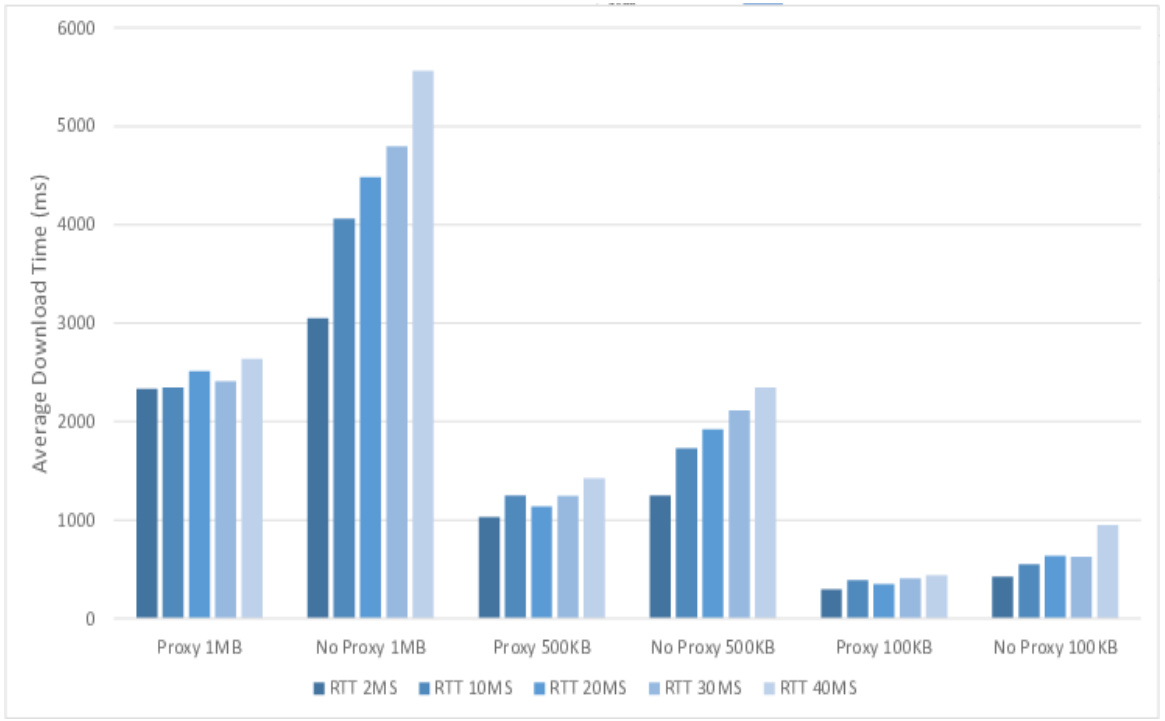


Use cases

- Based on a different granularity of cooperation between the server, the client and the proxy
  - Local loss recovery
  - Promise signaling
  - Declarative messages to the server

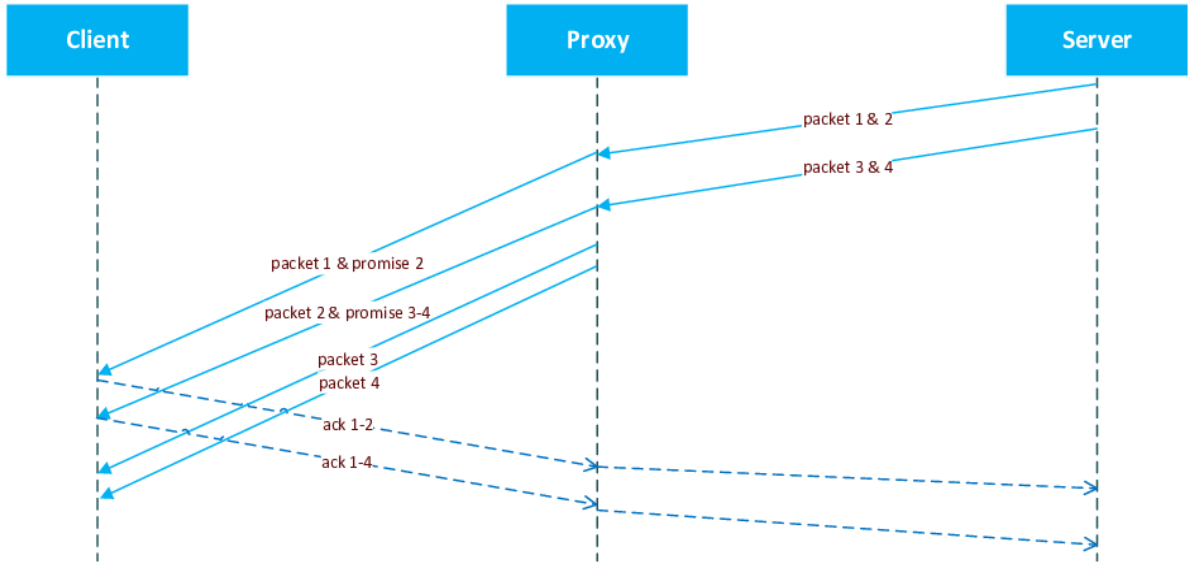
Local loss recovery

- Using the reliable data stream service of the QUIC tunnel
- Besides the initial explicit request, no additional signaling is needed
- May improve the performance of Unacknowledged Mode (UM)



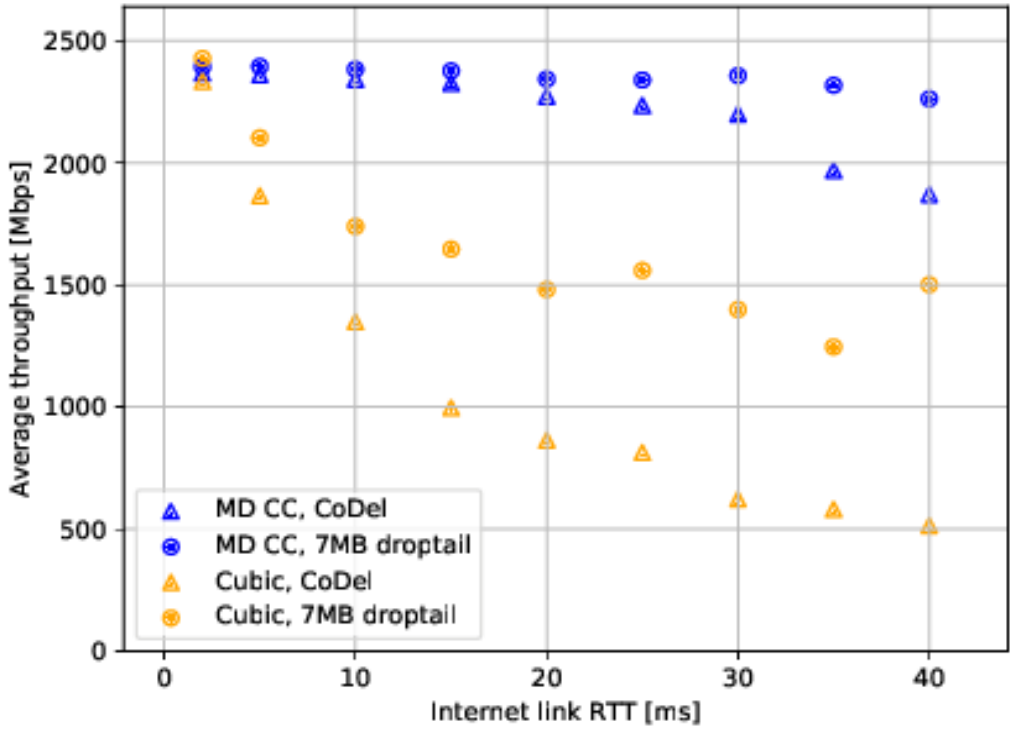
Promise signaling

- Useful if the bottleneck is between the client and the proxy
- A promise signal can indicate the reception of a packet by the proxy to the client
- The client can progressively acknowledge the "promised" packets



Declarative messages to the server

- Explicit cooperation between the proxy and the server
- Declarative, safe-to-ignore messages from the proxy, containing ACK/NACK info
- The server may apply a Multi-Domain congestion control algorithm
  - Two control loops for the wired and wireless domains
  - Provide fairness in the wired domain and fast utilization in the wireless domain



Conclusion and future work

- Transparent, connection-splitting PEPs are not feasible for QUIC traffic

- We propose a cooperative performance enhancing framework
  - Based on MASQUE
  - Explicit consensus by the endpoints
  - Unmodified security context of the original end-to-end connection

- Three different use-cases: local loss recovery, promise signaling, declarative messages to the server
- Promising early performance results
- Future work: Detailed performance evaluation in 4G/5G network conditions