Proposal to Conduct a Comparison of Network Protocols: TCP vs QUIC

Carl Masri, Jakob Roberts, Kjalen Hansen

Feb 26, 2016

***Abstract*—QUIC is a new transport layer protocol built by Google that aims to provide the guaranteed transport layer service of TCP with lower overhead and latency. QUIC is built entirely upon UDP which allows flexibility in implementation, as UDP is lightweight and very low overhead. Google maintains that there are many performance benefits of using UDP instead of TCP, including reduced connection time, improved congestion control, and forward error correction. This project aims to test these claims by comparing the QUIC protocol against TCP and UDP on a number of quantitative metrics by use of a purpose built server-client architecture. The security aspects will be examined with respect to impact on protocol and resistance to some basic attacks in a comparative analysis with current protocols.**

I. Problem Description

Although used by the majority of internet traffic, the TCP protocol is by no means perfect. Highly regulated and deeply ingrained into the heart of most devices including O/S kernels and middlebox firmware, making significant changes to TCP is next to impossible. Additionally, RTT delay created by the 3-way handshake and TLS encryption have left room for improvement. QUIC aims to mitigate these challenges by utilizing an improved ”reliable UDP” protocol as a proof-of-concept for future generations of TCP.

Should QUIC live up to its hype, the benefits of lower-latency packet transmission would have numerous implications. Google has disclosed that approximately half of all requests from Chrome to its servers are being delivered via QUIC [1], and the protocol offers a 3 percent improvement in mean page load times on Google Search [2]. These improvements may seem small, but they can add up. This is especially true in the case of mobile data; Gartner Research reported that there was an estimated 59 percent increase in mobile video traffic in 2015 [3]. If QUIC's enhancement claims are true, this could lead to large improvements of current networking infrastructure.

II. Related Work

The TCP network protocol has been the dominant form of point-to-point communication via the internet for many years due to the robustness of it compared with UDP. As the established leader in this area, much research has been done into both improving the existing infrastructure as well as comparing it to other newer networking protocols such as QUIC that could eventually replace TCP.

P. Megyesi et al. [4] have studied the bottle-necking that is caused by modern internet traffic and the failure of TCP to handle it properly. They elaborate on the limitations of TCP when used by the new HTTP protocol SPDY, and show how QUIC addresses these limitations. Googles ”SPDY” protcol brought multiplexed connections to HTTP requests. However, TCP in its current state cannot handle multiplex connections, and so must open several connections at once. With QUIC, SPDY is able to have non HOL blocking multiplex connections.

Additional research by R. Lychev et al. [5] delves into the security standards implemented by the QUIC protocol. The research shows that it is not quite as good as existing TLS implementations as there is no forward secrecy, it is vulnerable to replay attacks, and security downgrade attacks. They show how these vulnerabilities are caused by low latency mechanisms and may give us an idea of how it could be fixed with QUIC.

Carlucci provides an overview of the basic functionality of QUIC [6]. How it performs over lossy channels compared to existing protocols and how its Forward Error Connection module impacts performance.

[7]Alshammari discusses QUIC in terms of the current status of HTTP, goes into detail on the specific performance issues experienced by HTTP and shows how QUIC aims to address those issues. He speaks about HTTP/2 in Modern Web and Mobile Sensing-based Applications Analysis, Benchmarks and Current Issues.

III. Approach

QUIC's efficacy will be measured against existing protocols in three major areas: ability to maintain high throughput while experiencing packet loss, efficient re-transmission through high latency, and the secure implementation in the transport layer. As QUIC primarily acts as a replacement for TCP, most of the comparisons will be made between these two protocols. UDP comparisons will primarily serve to quantify the overhead QUIC adds to UDP to achieve Quality of Service.

Google currently provides the QUIC code source under the Creative Commons Attribution 2.5 license. This will be used to set up a formal testing environment. Through this custom server-client architecture the protocols will be examined and compared in a controlled setting. Primary focus will be on latency reduction as a function of QUICs added overhead. Multiple traffic classes will be tested and measured on QOS, throughput, latency, and packet loss under different simulated traffic conditions. Traffic will be artificially adjusted to simulate ranges of packet loss and delay. QUIC will also be tested under conditions of malicious attack such as deauthentication, DNS poisoning and ARP poisoning.

IV. Estimated Timeline

Three deliverables will be completed during the course of the semester. In addition to this proposal, the results of this study will be formally presented and a final written report will be handed in. Upon approval of the project, the authors will commence work according the the following proposed timeline:

1) Feb 13: Build QUIC runtime and testing environment (client and server, certificates).
2) Feb 27: Begin performance analysis.
3) Mar 13: Finalize results.
4) Mar 27: Begin final report write-up and presentation preparation.
5) Apr 10: Final edits and report submission.

References

[1] S. Bouzas. (2016, Feb 19) *Why is Googles QUIC Leaving Network Operators in the Dark?* [Online]. Available: http://owmobility.com/blog/why-is-googles-quic-leaving-network-operators-in-the-dark/

[2] Google, Inc. (2015, Apr 17) *A QUIC update on Googles experimental transport* [Online]. Available: https://blog.chromium.org/2015/04/a-quic-update-on-googles-experimental.html

[3] J. Rivera. (2015, Feb 5) *What's Driving Mobile Data Growth?* [Online]. Available: http://www.gartner.com/newsroom/id/2977917

[4] P. Megyesi et al. (2016, May 10) *How Quick is QUIC?* [Online]. Available: https://www.researchgate.net/publication/302585207_How_quick_is_QUIC

[5] R. Lychev et al. (2015, Sep 16). *How Secure and Quick is QUIC? Provable Security and Performance Analyses* [Online]. Available: http://www.cc.gatech.edu/~aboldyre/papers/quic.pdf

[6] G. Carlucci et al. (2015, Apr 13). *HTTP over UDP: an Experimental Investigation of QUIC* [Online]. Available: http://c3lab.poliba.it/images/3/3b/QUIC_SAC15.pdf

[7] A. Alshammari & A. Al-Mogren. (2016, Aug 29). *HTTP/2 in Modern Web and Mobile Sensing-based Applications Analysis,Benchmarks and Current Issues* [Online]. Available: https://www.omicsgroup.org/journals/seqsplithttp2-in-modern-web-and-mobile-sensingbased-applications-analysisbenchmarks-and-current-issues-2332-0796-1000193.pdf