Assessing the threats targeting low latency traffic: the case of L4S

Marius Letourneau[1], Kouame Boris N'Djore[1], Guillaume Doyen[2], Bertrand Mathieu[3], Rémi Cogranne[1]
[1]LIST3N – University of Technology of Troyes, France
[2]OCIF – IRISA (UMR CNRS 6074), IMT Atlantique Rennes, France
[3]Orange Innovation, Lannion, France

Topic: Cybersecurity in Telecommunication and Networks ; Signal processing applied to telecommunications
Keywords: Security, L4S, low latency, networking

New services are designed for the future of Internet, and some of them will require the network to provide low latency traffic. Many optimizations targeting latency reduction have been proposed. Among them, re-architecting congestion control and active queue management (AQM) has been particularly studied. L4S [1,2,3] (Low Latency, Low Loss and Scalable Throughput) is a new network architecture that aims at allowing coexistence between low latency traffic and classic traffic within a single node, involving a dual queue coupled AQM.
Although this architecture sounds promising for latency improvement, an attacker can exploit some vulnerabilities to defeat its low-latency features and consequently make some services unusable. In addition, we prove that application-layer protocols such as QUIC can easily be hacked in order to exploit the over sensitivity of those new services to network variations. By implementing undesirable flows in a testbed and evaluating how they impact the delivery of low-latency flows, we demonstrate their reality and the need of research in the detection of this new kind of threats [4,5].

References:

[1] B. Briscoe & al., "*Low Latency, Low Loss, Scalable Throughput (L4S) Internet Service: Architecture.*", IETF IETF, Transport Area Working Group, ietf-tsvwg-l4s-arch-10, 2022.
[2] O. Albisser & al., "*DUALPI2-low latency, low loss and scalable (L4S) AQM.*", Proc. Netdev 0x13, 2019.
[3] B. Briscoe & al., "*Implementing the'Prague Requirements' for Low Latency Low Loss Scalable Throughput (L4S).*", Proc Netdev 0x13, 2019.
[4] M. Letourneau & al., "*Assessing the Threats Targeting Low Latency Traffic: the Case of L4S.*", Proc. IEEE International Conference on Network and Service Management (CNSM), pp. 544-550, 2021.
[5] M. Letourneau, G. Doyen and R. Cogranne, "*Defeating Architectures for Low-Latency Services: The Case of L4S*", 2021.

Additional information

Contact details: marius.letourneau@utt.fr + remi.cogranne@utt.fr
Researcher profile on the web: https://www.researchgate.net/profile/Marius-Letourneau
Member of labs / working groups / institutes: LIST3N - UTT
Topics of research: Cybersecurity in Telecommunication and Networks ; Signal processing applied to telecommunications
Interest in the institute: Find collaboration within my topic of research (or perhaps explore novel research opportuinities)