Assessing the Threats Targeting Low Latency Traffic: The case of L4S

Marius Letourneau, Kouame Boris N'Djore, Guillaume Doyen, Bertrand Mathieu, Rémi Cogranne

1st Workshop of the European Research Institute (ERI)
on Telecommunication and Networks
15 March 2022

Context: New network requirements

- Low latency (LL) deployment becomes a hot topic, with strong latency requirements. Target e2e latency:
  - $\approx$ 1ms for Factory 4.0 and haptic Internet
- We chose to focus on L4S, an architecture actively discussed at the IETF
- What an attacker can do to harm LL requirements?
  - Some vulnerabilites have been found in precedent work, but how can they be characterized?
- We propose a classification of undesirable flows, and highlight their respective impacts on low latency services
- To that aim, we modified user-space protocols easily to exploit the over-sensitivity of such applications




Low latency: known threats (1/2)

We studied the following undesirable flows and propose to classify them as such:

- **Misbehaving flows**:
  - Protocol manipulations
    e.g.: Hacked ACK [KOT11, SHE05, LAR21], hacked ECN[ELY01, KOT11, LAR20]
  - Abnormal behavior in traffic pattern
    e.g.: Low rate DoS[ZHI20]
- **Unresponsive flows**:
  - Flows not subjected to the congestion control (UDP, VoIP, live streaming ...)
  - Are usually legitimate but can be generated by a malicious user
- **Malformed flows**:
  - Emitting pattern complex to handle
    e.g.: micro-bursts due to radio access point and/or bufferization at different levels in the endpoint's network stack [OLJ20, STE17])

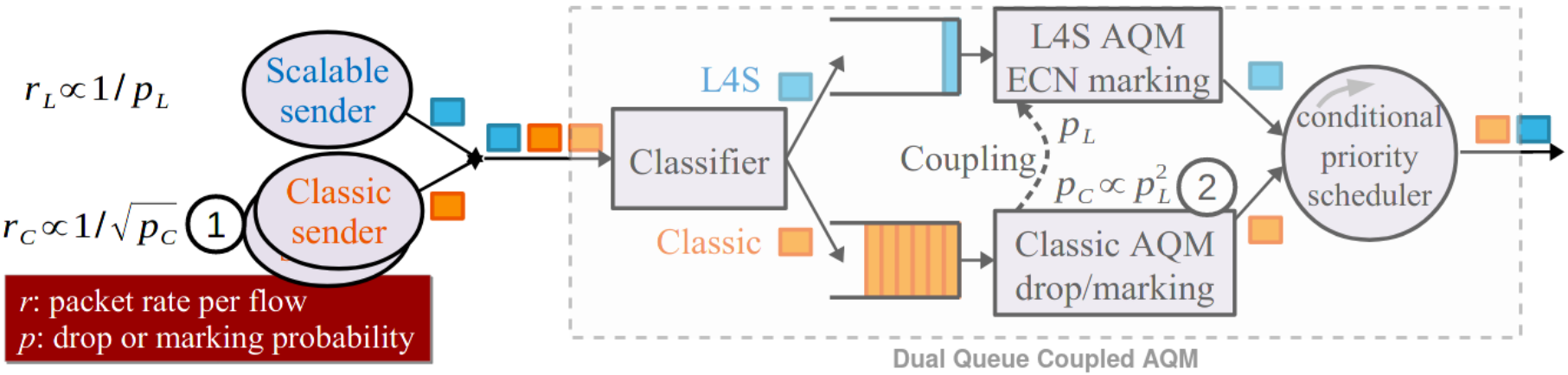
$\Longrightarrow$ Unresponsive flows and Malformed flows are usual on the today's Internet

Low latency: L4S architecture (2/2)

L4S: Low Latency, Low Loss and Scalable throughput

General principle:

- Classic flows (C) and Low Latency flows (L) must coexist
- Latency isolation between (C) flows and (L) flows

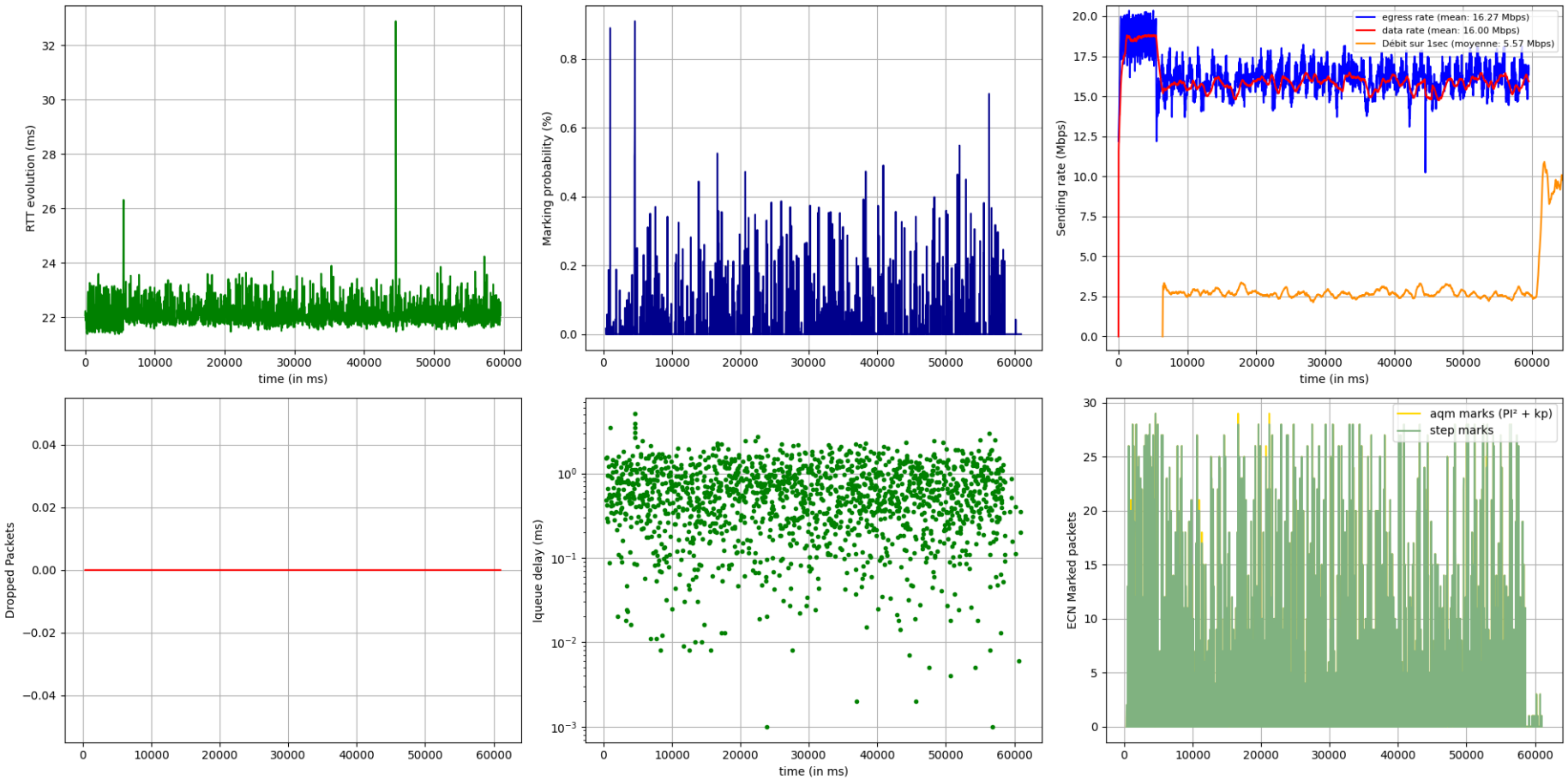


Based on *Implementing the 'Prague Requirements'for Low Latency Low Loss Scalable Throughput (L4S) Netdev 0x13, 2019*

$\Longrightarrow$ The reference implementation of the Dual Queue Coupled AQM is DualPI²

Reference situation

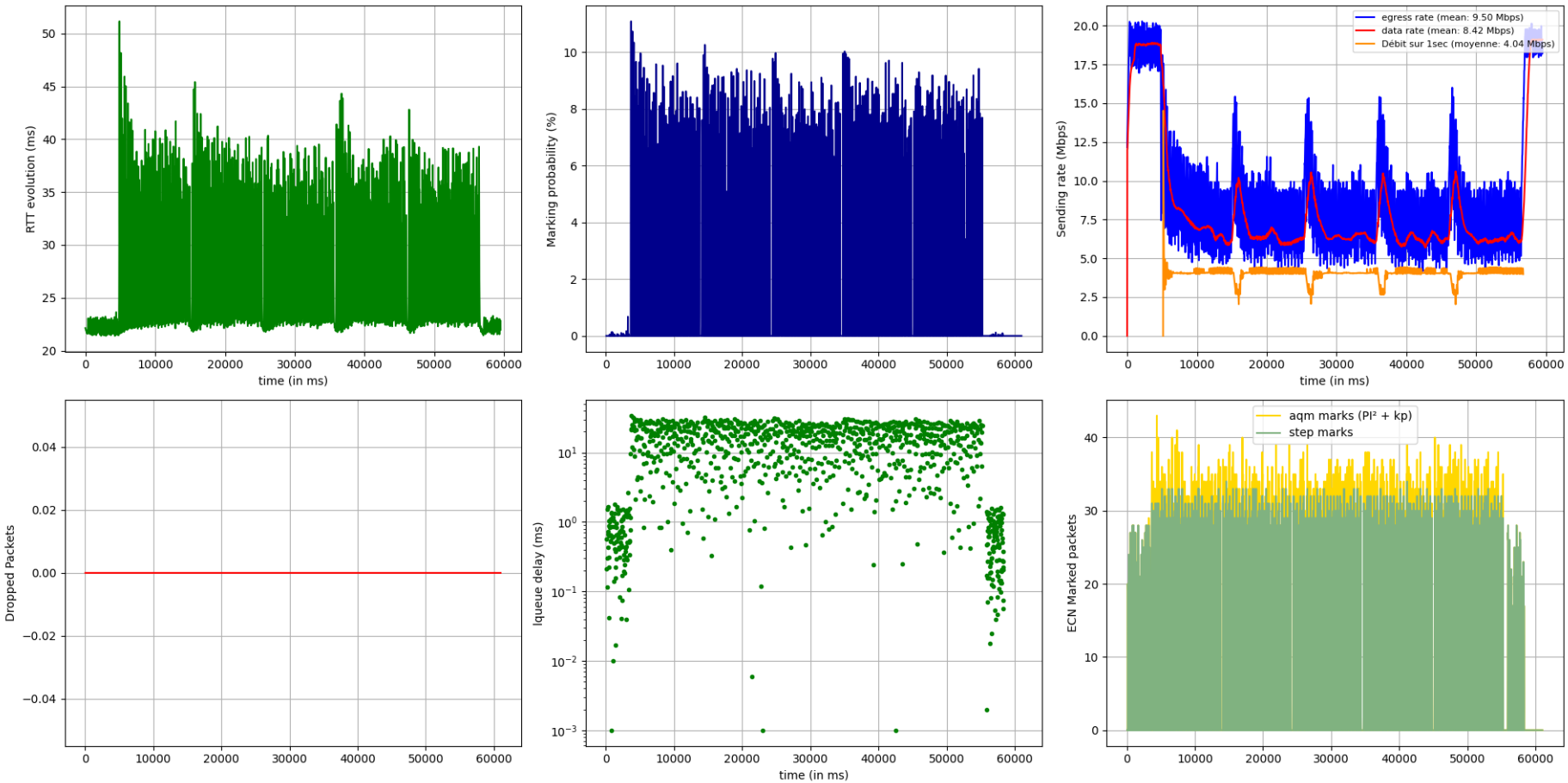
This is the reference situation used as a control sample



Standard behavior of the L4S architecture with one LL and one classic flows.
Horizontal axis is the time in ms.

Undesirable flows comparison: An example

Example of an undesirable flow: connection bursts (loop requesting a 80kO file)



Impacts of connection bursts in (L) queue (AQM Rate: 20 Mbps, Size of file requested 80ko)

Conclusion

- The L4S architecture is promising but still needs security enforcements to protect the LL requirement
- Three main categories of threats have been identified and implemented
- Impacts of each category were evaluated independently but further studies need to be conducted
- Some characteristics are remarkable and statistical analysis lead us to a better understanding of how DualPI2 behaves
- These characteristics may hopefully be reused for detection purpose ...
- ... that is the topic of our ongoing work!

Thank you !

References

- [KOT11]: *Finding protocol manipulation attacks* - SIGCOMM, 2011
- [SHE05]: *Misbehaving TCP Receivers Can Cause Internet-Wide Congestion Collapse* - ACM Conference on Computer and Communications Security, 2005
- [LAR21]: *Mitigating TCP Protocol Misuse With Programmable Data Planes* - TNSM, 2021
- [ELY01]: *Robust congestion signaling* - International Conference on Network Protocols, 2001
- [LAR20]: *Defeating Protocol Abuse with P4: Application to Explicit Congestion Notification* - IFIP, 2020
- [ZHI20]: *Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey* - IEEE Access, 2020
- [OLJ20]: *Validating the Sharing Behavior and Latency Characteristics of the L4S Architecture* - SIGCOMM, 2020
- [STE17]: *Destruction Testing: Ultra-Low Delay using Dual Queue Coupled Active Queue Management* - Masters Thesis Univ. Oslo, 2017