Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
34° cycle

Supervisor
Prof. Fulvio Risso

Service-Oriented Architectures and Security in Automotive Environments

PhD Candidate: Marco Iorio marco.iorio@polito.it

1. Introduction

Modern vehicles are becoming smarter and more ICT oriented. Yet, computerization is posing unforeseen **challenges**, in terms of increased complexity and costs, as well as possible vulnerabilities and security issues.

This thesis proposes a novel approach to transparently **extend the capabilities** of on-board devices through external data-centers, while accounting for constrained latency and resiliency requirements. Second, it addresses the need for **increased security** both within and among vehicles.

2. Liquid Computing

The success of cloud and edge computing paradigms favors at the same time resource fragmentation. Our **liquid computing** vision fosters a transparent **continuum** of resources and services across multiple infrastructures. In addition to easier orchestration, it enables resource **sharing** and **brokering** scenarios. Each application can be bound to **high-level intents** enforcing its requirements, while a **decentralized approach** enables the support for different administrative domains. Liqo[§] concretizes the vision through seamless and dynamic Kubernetes multi-cluster scenarios.

[§] https://github.com/liqotech/liqo

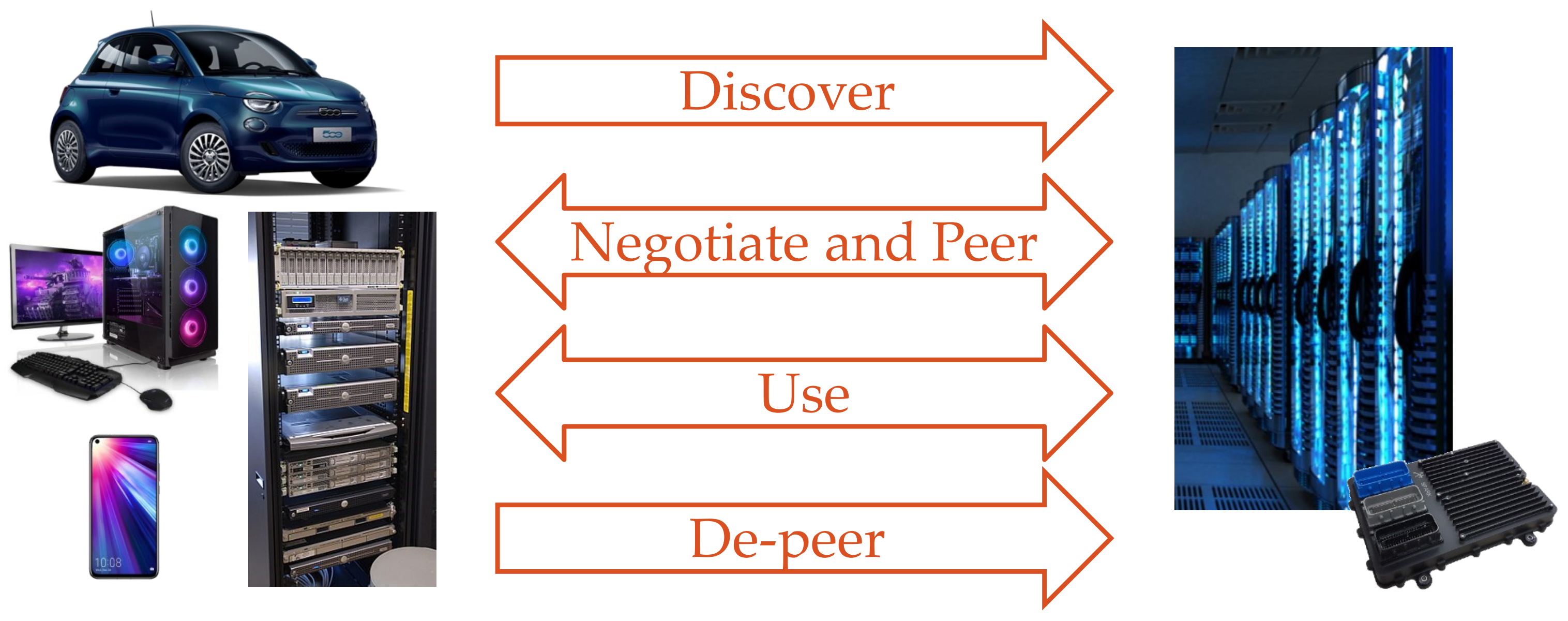
Discover
Negotiate and Peer
Use
De-peer

Figure 1. High-level workflow enabling resource sharing among different devices, including both data-centers and "things".

3. When Latency Matters

Low-latency is essential to enable effective distributed applications and the **network edge** is typically regarded as a key enabler. Yet, reduced propagation delays are only a part of a bigger picture. In [1] we showed **latency is a complex and multi-dimensional problem with no easy panacea**. Collaboration among different actors is required to achieve good performance and prevent subtle pitfalls.

4. In-vehicle Security

With the emergence of **connected vehicles** and high-speed communication buses, the need for security kicks in. In [2] we presented a **policy-based security protocol** to protect **SOME/IP** messages. It leverages high-level rules to describe the traffic matrix, and fully integrates within the middleware to support the different communication patterns, while introducing **limited overhead**.

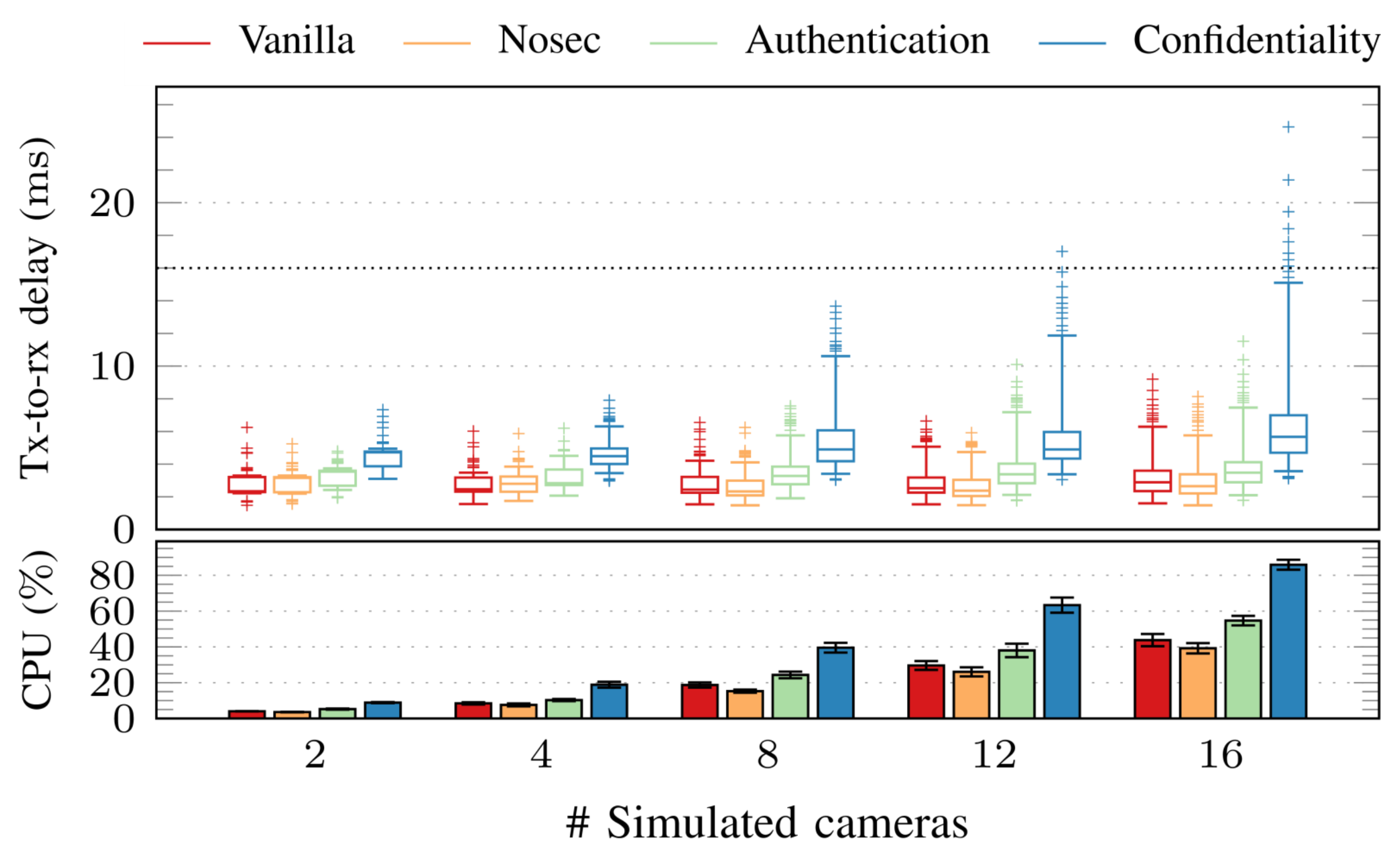

Figure 2. Performance comparison when transmitting messages over enhanced SOME/IP configured at different levels of security.

5. References

1. M. Iorio, F. Risso and C. Casetti, When Latency Matters: Measurements and Lessons Learned. ACM SIGCOMM Computer Communication Review, vol. 51, no. 4, Oct. 2021.
2. M. Iorio, M. Reineri, F. Risso, R. Sisto and F. Valenza, Securing SOME/IP for In-Vehicle Service Protection. IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13450-13466, Nov. 2020.