Security in Hybrid ITS Networks

Ricardo Filipe Quelhas Severino

Orientadores: Doutor José Manuel de Campos Lages Garcia Simão
Doutor Nuno Miguel Soares Datia

Presidente: Doutor Nuno Miguel Machado Cruz

Vogais: Doutor João Carlos Ferreira
Doutor José Manuel de Campos Lages Garcia Simão

Mestrado em Engenharia Informática e de Computadores
Instituto Superior de Engenharia de Lisboa

Master Thesis Presentation

Lisboa, Portugal

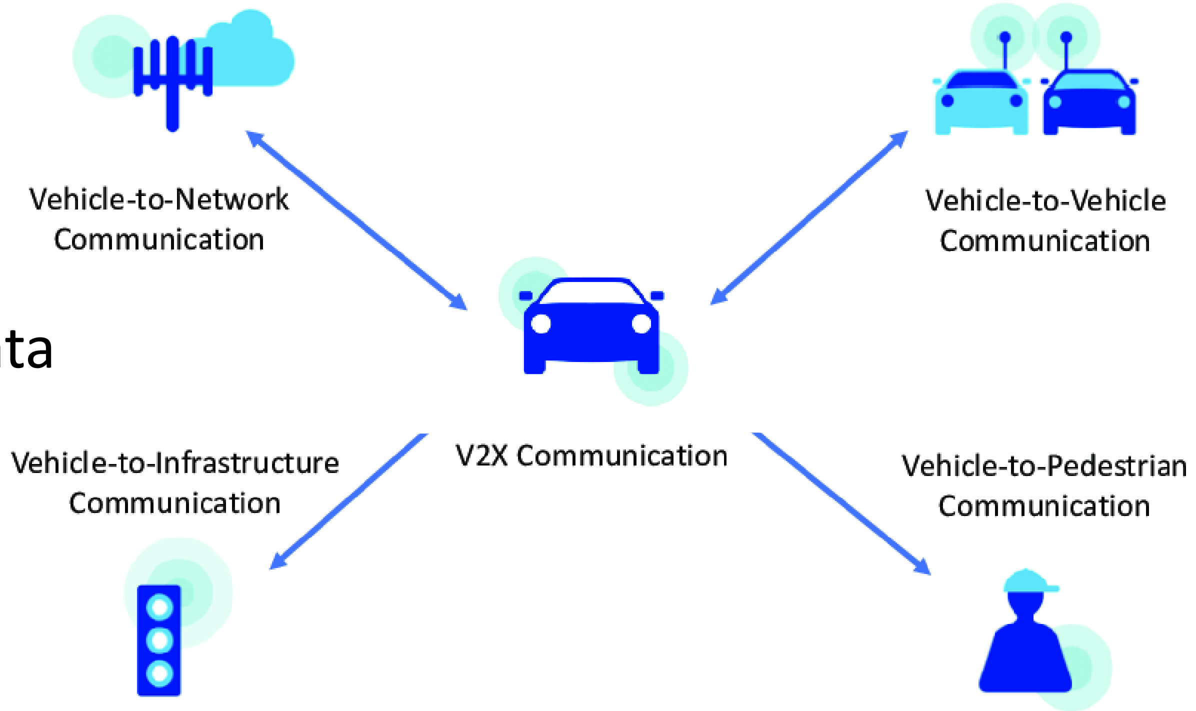
December 15th, 2023

ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Introduction

- Intelligent transport systems (ITS) aims to improve transportation
  - safety
  - efficiency

- Cooperative ITS
  - subset of standards for ITS
  - services based on the exchange of data
  - V2V, V2I, V2P, V2X



Source: https://doi.org/10.3390/fi11030070

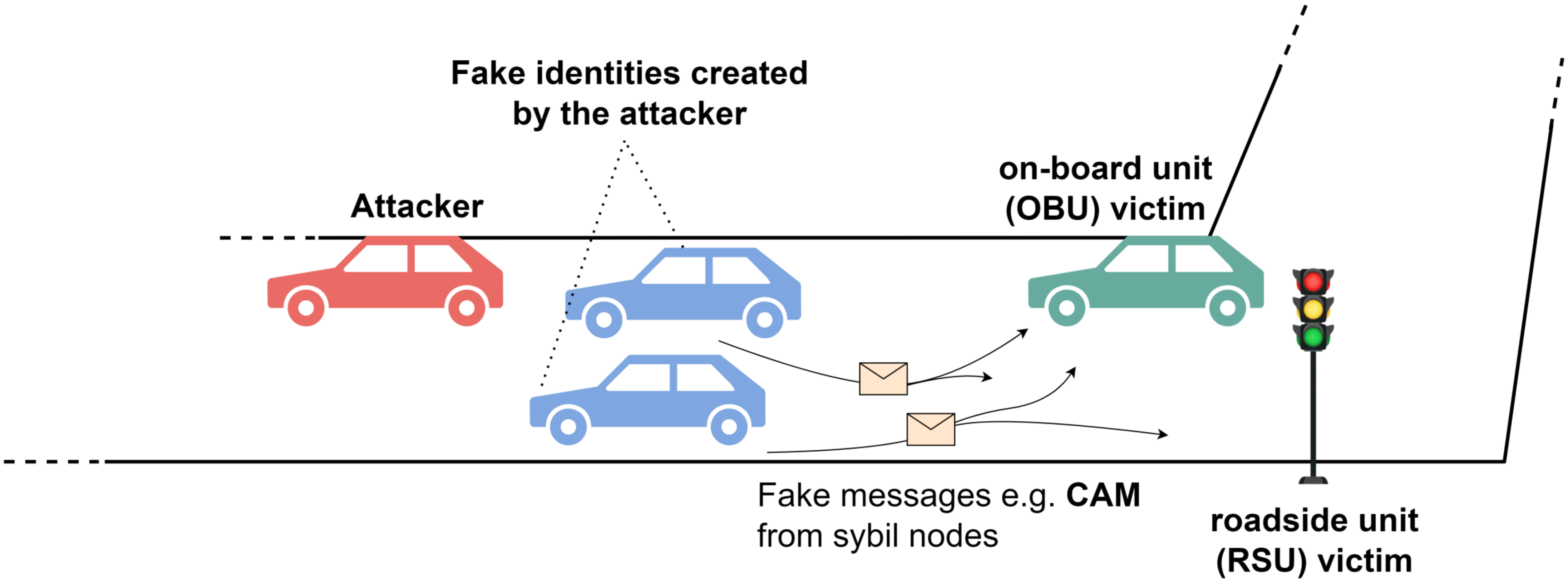
Introduction – ITS Security

- The **major threats** are against
  - privacy
  - authenticity and integrity
  - non-repudiation

- **Standard approach – PKI** (Public Key Infrastructure)
  - C-ITS trust model architecture
  - achieves high-security level
  - has limitations given the nature of V2X communications

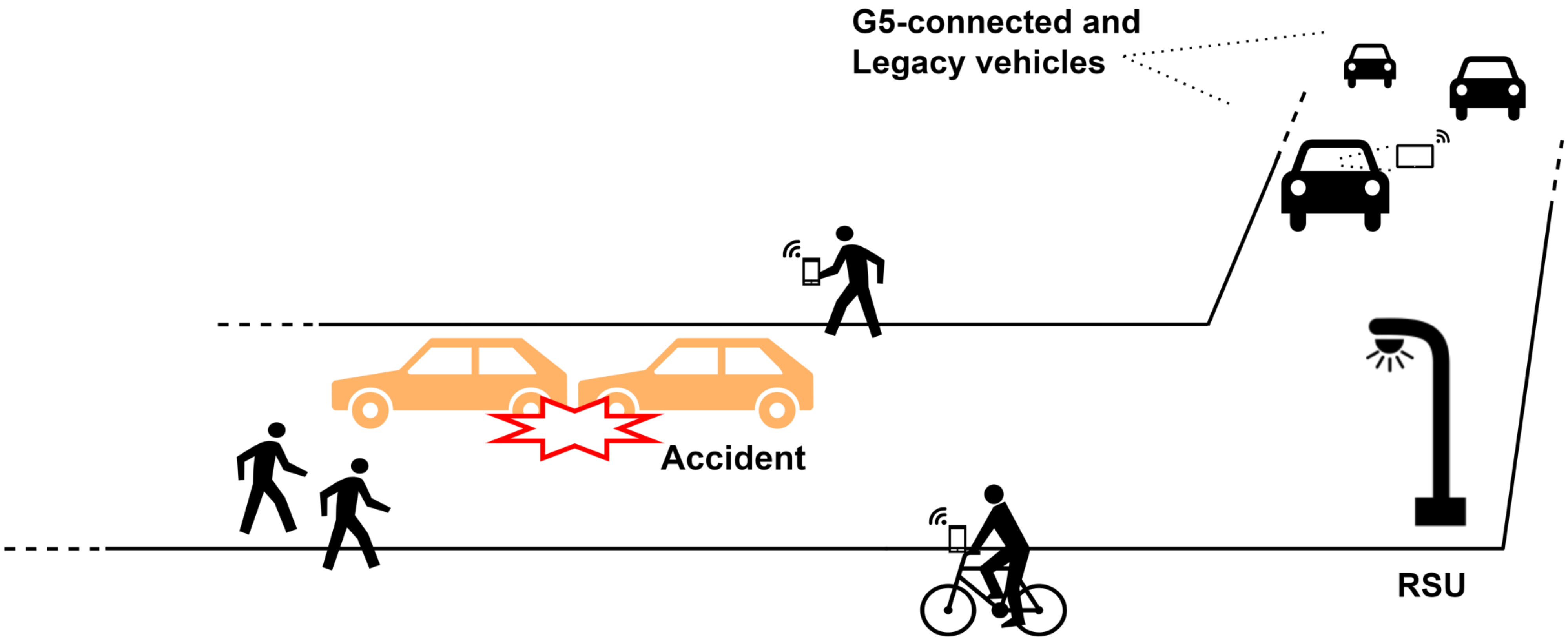
Problem

- Example: sybil attack



Problem

- Vulnerable modes of transportation



ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Goals

- Introduce security guarantees within a C-ITS ecosystem, while including vulnerable modes of transportation and legacy vehicles
- Implement, evaluate and compare security protocols using real equipment
- Assess how security affects performance
- Determine the performance cost of incorporating soft-mobility users and legacy vehicles

Approach

- Develop proof-of-concept applications that employ a security protocol in a C-ITS hybrid environment
- Combining intelligent transport systems operating at 5.9 GHz (ITS-G5) and cellular networks
- Implement two security protocols, DLAPP and MFSPV
  - using OBUs, RSUs and smartphones
- Measure computational, transmission and end-to-end latencies to assess the performance

Non-standard ITS security protocols

DLAPP

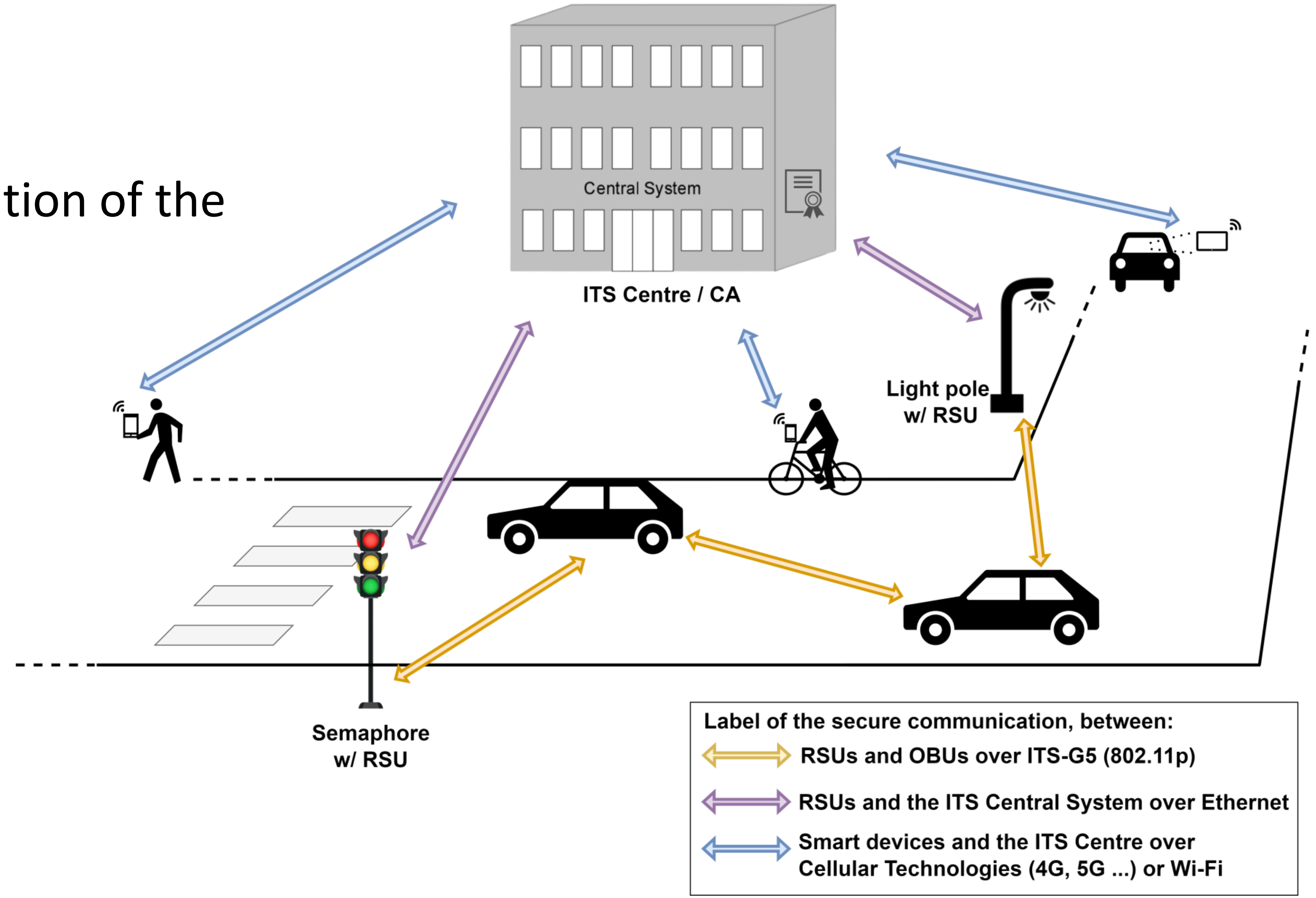
MFSPV

DLAPP and MFSPV

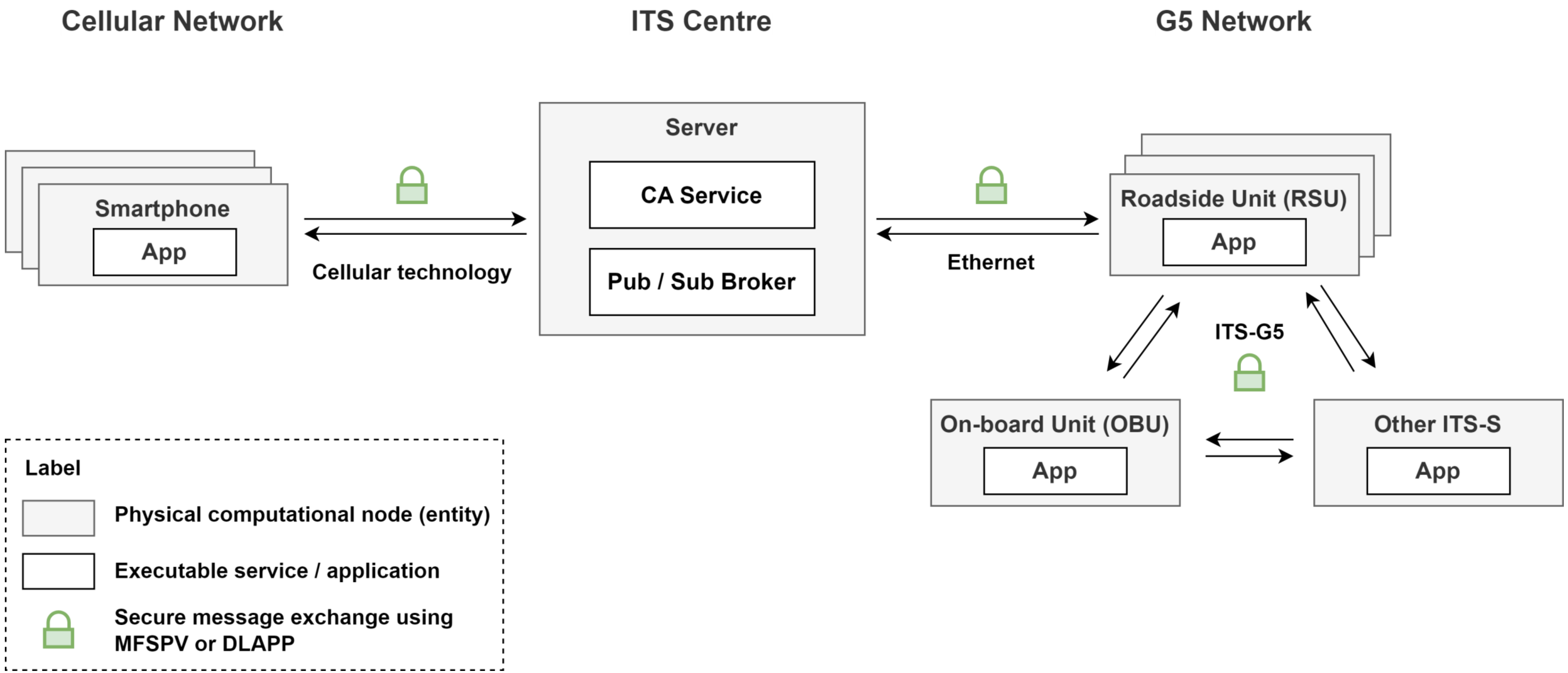
- Authentication and privacy-preserving solutions
  - essential security requirements
- Lightweight security schemes
- Symmetric cryptography mechanism
- Certification Authority (CA) decentralization
  - reduce the communication burden
- Minimise communication overhead

Proposed Approach

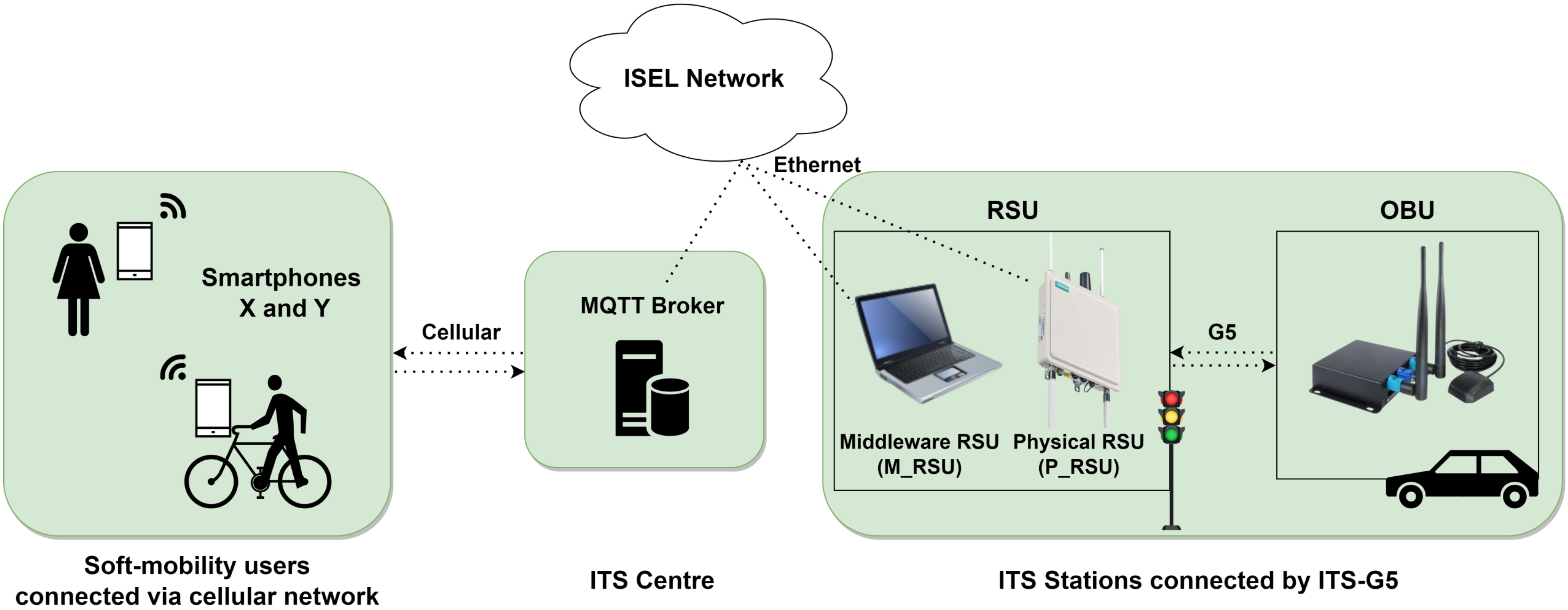
- High-level representation of the approach



Proposed Approach



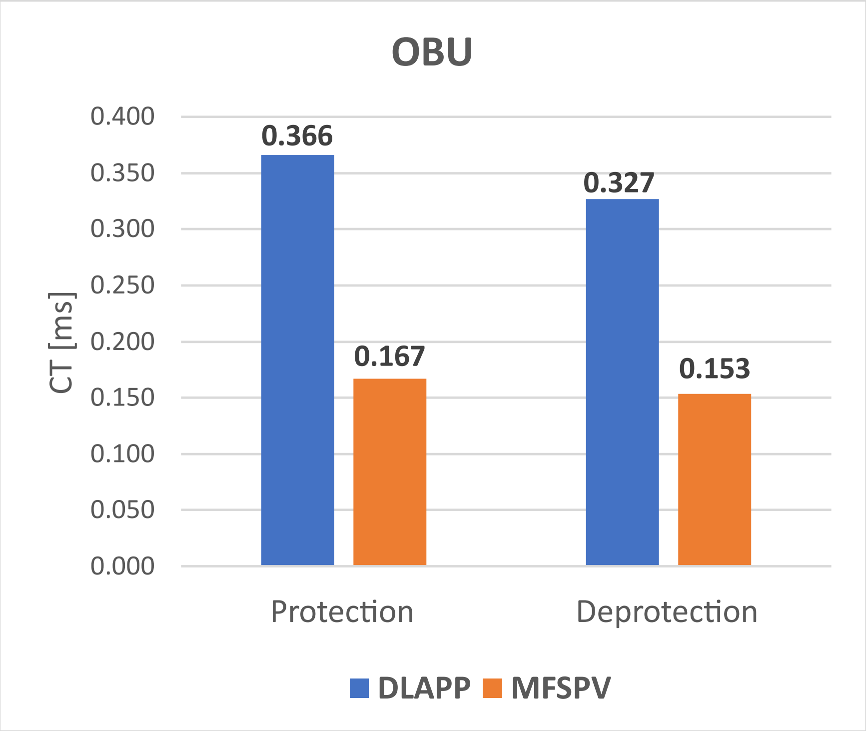
Experimental Environment

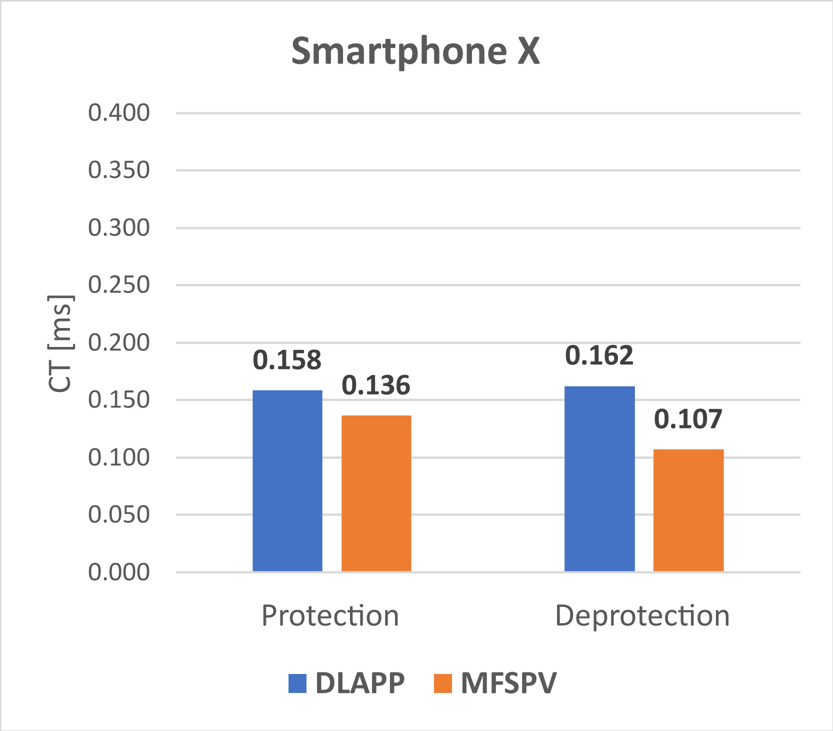


Experimental Evaluation and Results Analysis

1. **Computation**
2. Network
3. End-to-End (E2E)

1. Computation – Evaluation and Results

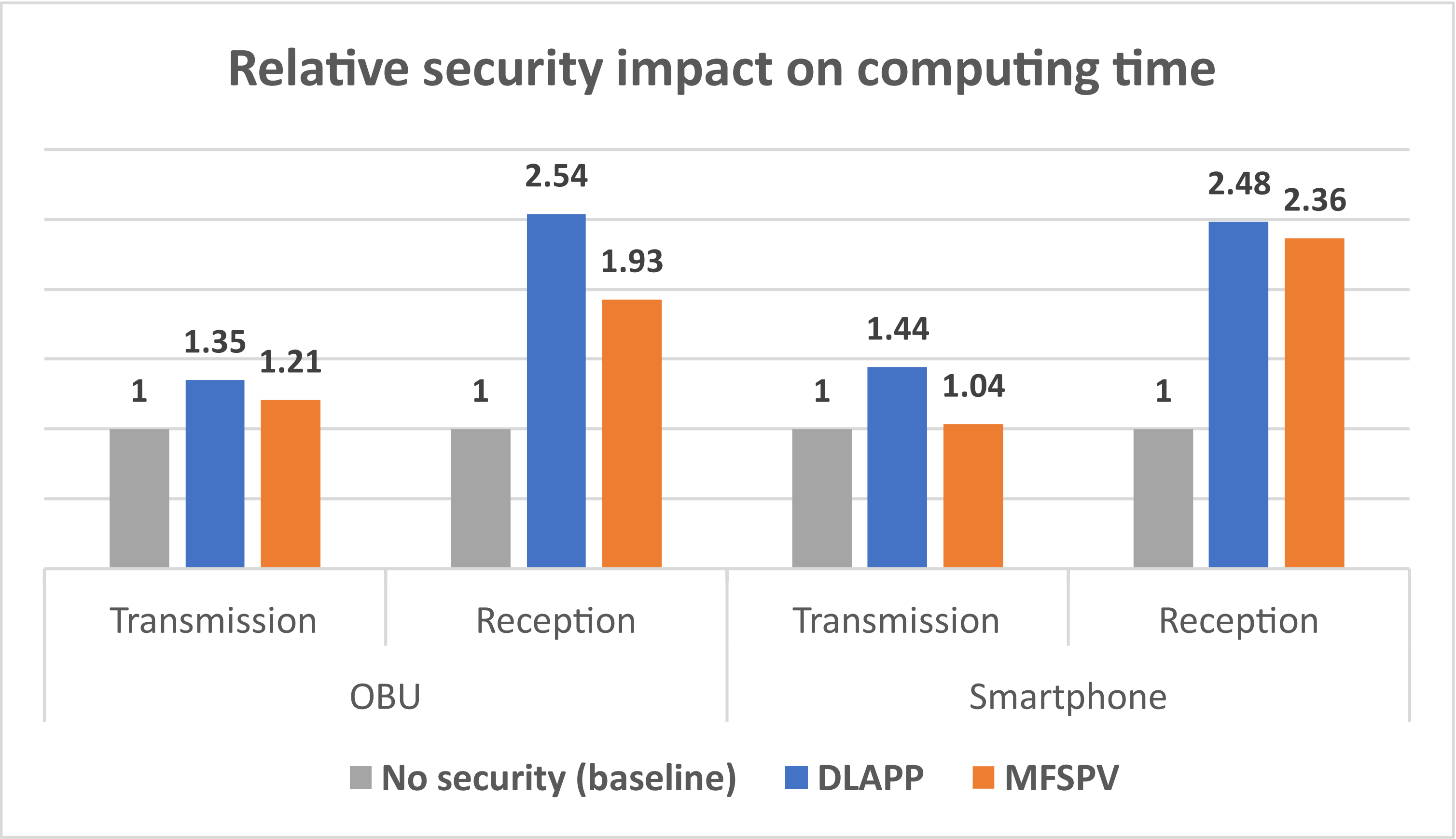




- MFSPV outperforms DLAPP (due to the exclusive use of hashes)
  - Decrease in processing time ranging from 13.9% to 54.4%
- The results do not match the ones claimed by the protocols' authors
- Both protocols are light enough to manage high-node density scenarios

1. Computation – Evaluation and Results

- Security **impact** on performance
  - DLAPP has more impact on computing time than MFSPV
  - greater relative increases can be seen in reception
  - magnitude of the times involved is minimal, tenths of milliseconds
  - both presented a low impact on local computing time



Experimental Evaluation and Results Analysis

1. Computation
2. **Network**
3. End-to-End (E2E)

ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

2. Network – Evaluation and Results

- Measurements of the **cellular** network segment

Communication Flow			No security [ms]	DLAPP [ms]	MFSPV [ms]
M_RSU	→	Smartphone X	23.08	25.23	24.66
Smartphone X	→	M_RSU	29.74	31.90	32.32
Smartphone X	→	Smartphone Y	31.78	33.22	33.97

  - Lower latency is observed in flows involving M_RSU
  - DLAPP exhibits slightly lower latency on two occasions

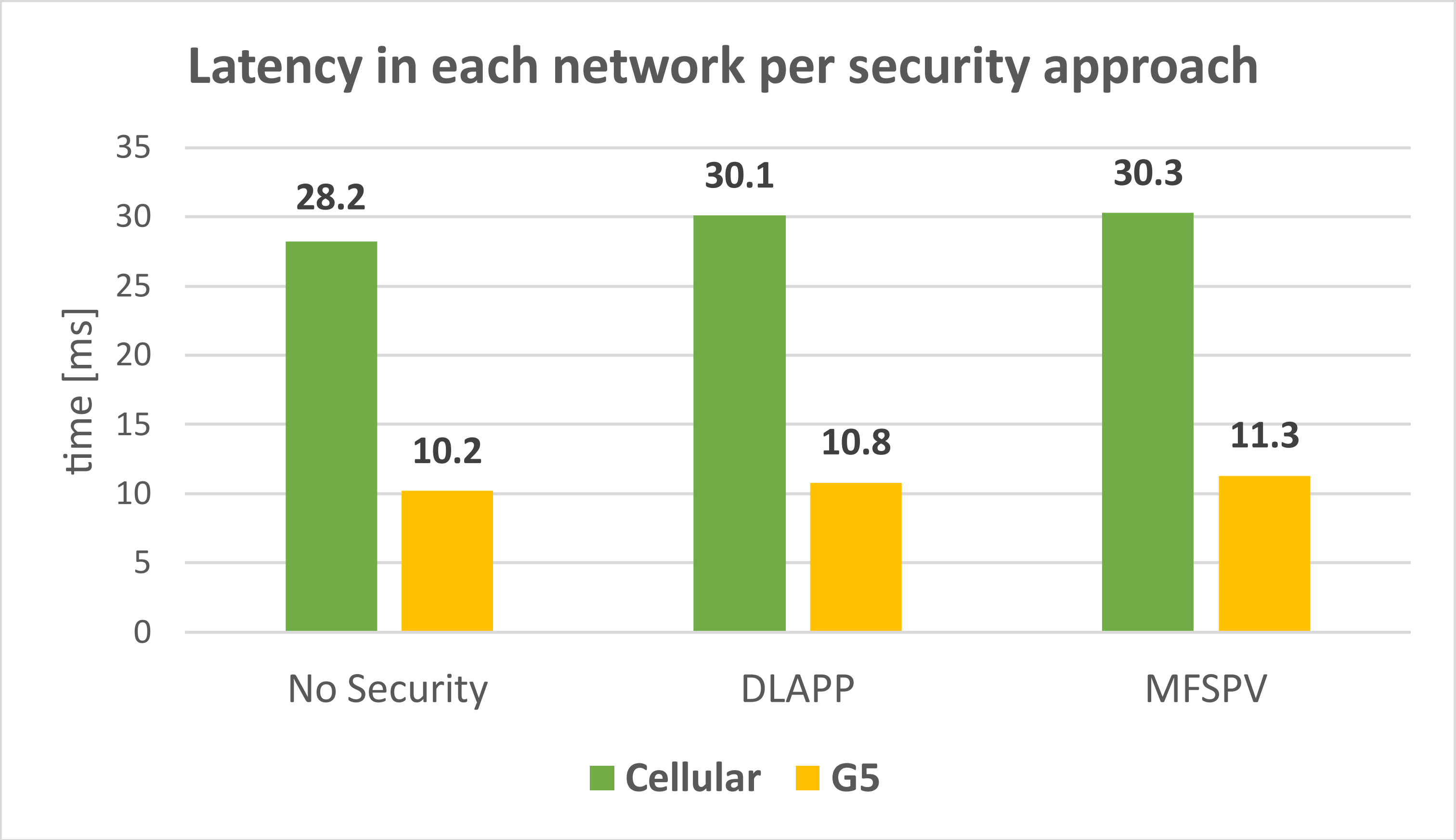
- Measurements of the **G5** network segment

No security [ms]	DLAPP [ms]	MFSPV [ms]
10.196	10.792	11.251

ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

2. Network – Evaluation and Results

- Cellular and G5's latency measurements comparison
  - G5 network attains 63.6% lower latency
  - transmission in G5 is ad-hoc
  - the impact of security protocols on latency: 7.1% on the cellular and 8.0% on the G5 network



Experimental Evaluation and Results Analysis

1. Computation
2. Network
3. **End-to-End (E2E)**

ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

3. E2E – Evaluation and Results

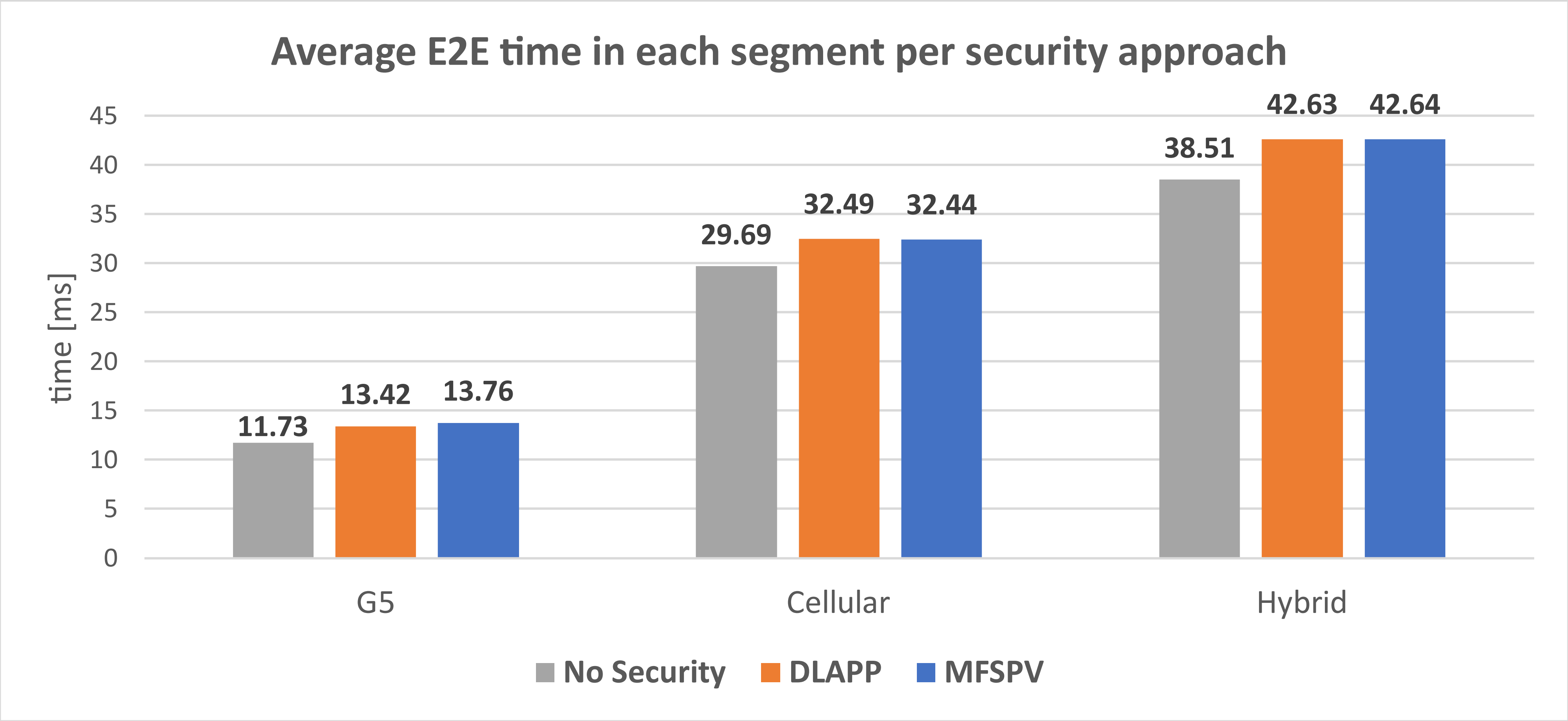
- E2E time for each flow, with different security approaches

Network Segment	Communication Flow			No Security [ms]	DLAPP [ms]	MFSPV [ms]
G5	OBU	$\rightarrow$	RSU	**11.63**	13.24	13.55
	RSU	$\rightarrow$	OBU	12.24	13.61	13.97
Cellular	RSU	$\rightarrow$	Smartphone X	**24.59**	27.71	27.19
	Smartphone X	$\rightarrow$	RSU	31.72	34.99	34.98
	Smartphone X	$\rightarrow$	Smartphone Y	32.76	34.77	35.16
Hybrid	Smartphone X	$\rightarrow$	OBU	42.18	46.46	46.75
	OBU	$\rightarrow$	Smartphone X	**34.94**	38.81	38.53

- **Analysis per network segment**
  - Hybrid network segment flows have the highest E2E latencies (~41.3 ms on average)
  - G5 network segment flows have the lowest E2E latencies (~13.0 ms on average)
  - Hybrid communication flows impose an extra 28.3 ms of E2E time

3. E2E – Evaluation and Results

➢ Analysis per security approach



3. E2E – Evaluation and Results

➢ Applicability considerations

- Various use cases have defined specific requirements for maximum latencies
- the median E2E latencies do not surpass ~**47** ms
  Smartphone X → OBU with MFSPV
- the highest E2E latency reached ~**190** ms
  Smartphone X → OBU with DLAPP
- excluding outliers, the highest E2E latency was **86** ms
  Smartphone X → OBU with MFSPV
- the results obtained in this study remain 14% below the maximum latency requirements for many use cases

Conclusions

- The developed approach allowed to:
  - introduce security guarantees within a C-ITS ecosystem
  - include vulnerable modes of transportation

- The used experimental setup:
  - Avoids modification of equipment software
  - DLAPP and MFSPV have shown a similar and low performance impact
  - Smartphones outperforms Unex OBU (resource-constrained device)
  - Incorporating users through mobile networks imposes, on average, an extra 28.29 ms of E2E latency

- The obtained results align well with the latency requirements for many C-ITS use cases

Future Work

- CA should be developed
- Acquire greater proficiency in interacting with ITS equipment
- Experiments with more OBUs and RSUs from different manufacturers
- Carry out evaluations under more stress/overload conditions

Contributions

- Development and assessment of a novel approach that employs a security protocol in a C-ITS hybrid environment by combining ITS-G5 and radio-mobile networks
- Extend the literature by going beyond the traditional focus on connected vehicles to include soft mobility users and legacy vehicles in C-ITS
- Assessing the effectiveness of security protocols, thus filling the gap between theory/simulation and real-world implementations
- Enrichment of the literature regarding the implementation of security protocols in real ITS equipment

- Public *GitHub* repository for the developed code

- Ricardo Severino; José Simão; Nuno Datia; António Serrador,

Protecting Hybrid ITS Networks: A Comprehensive Security Approach,

Future Internet journal, 2023