CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Conference Paper

A Wireless Safety and Security Layer Architecture for Reliable Co-CPS

Enio Filho*
Ricardo Severino
Anis Koubâa*
Eduardo Tovar*

*CISTER Research Centre

CISTER-TR-210604

2021/06/28

A Wireless Safety and Security Layer Architecture for Reliable Co-CPS

Enio Filho*, Ricardo Severino, Anis Koubâa*, Eduardo Tovar*

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: enpvf@isep.ipp.pt, sev@isep.ipp.pt, aska@isep.ipp.pt, emt@isep.ipp.pt

https://www.cister-labs.pt

Abstract

Modern multicore processors have the potential to provide raw computing power while being energy-efficient and cost-effective. While many of the systems have already deployed multicore processors for their operation, their adoption in time-sensitive applications is still active research. The main reason behind this is the architecture of a typical multicore processor. The typical architecture used in COTS platforms makes use of shared resources such as shared system bus, main memory, shared caches, etc., among all/several cores. A task can suffer inter-core interference from the co-running tasks while accessing these shared resources. This inter-core interference can impact the temporal behavior of the tasks and analyzing the worst-case timing behavior of a task becomes extremely challenging. The 3-phase task model was proposed to circumvent this problem by dividing the execution of each task into memory and execution phases. In the 3-phase task model, the memory accesses can only happen during a memory phase and a core can execute a memory phase while other cores are busy executing the execution phases. Even though some existing approaches focus on analyzing the schedulability of the 3-phase task model under partitioned scheduling, several open issues exist. In this paper, we identify the key open issues that are important to address in order to derive the schedulability analysis for the 3-phase task model using partitioned scheduling.

A Wireless Safety and Security Layer Architecture for Reliable Co-CPS

Enio Vasconcelos Filho [1], Ricardo Severino[1], Anis Koubaa[2], Eduardo Tovar[1]
[1]CISTER – Research Centre in Real-time & Embedded Computing Systems, Instituto Superior de Engenharia do Porto, Rua Alfredo Allen 535, 4200-135 Porto, Portugal; ({enpvf,rarss,emt}@isep.ipp.pt), ORCID 0000-0001-5459-6821, 0000-0002-4215-3238, 0000-0001-8979-3876
[2]Prince Sultan University, Saudi Arabia; (akoubaa@psu.edu.sa), ORCID 0000-0003-3787-7423

Abstract
The advancements in wireless communication technologies have been enabling an unprecedented pervasiveness and ubiquity for Cyber-Physical Systems. Such technologies can now empower true Systems-of-Systems which cooperate to achieve more complex and efficient functionalities, such as vehicle platooning. However, for such Cooperative Cyber-Physical Systems (Co-CPS) applications to become a reality and fulfill their potential, safety and security must be guaranteed, particularly in critical systems, since they heavily rely on open communication systems, prone to intentional and non-intentional interferences.
To address these issues, in this work, we propose the design of an architecture of a Wireless Safety and Security Layer (WSSL), to be implemented in critical Co-CPS to increase the reliability of these critical communications by enabling the detection of communication errors. Our approach is based upon a safety standard (IEC 61508) directed at open communication systems, which suggests a Black Channel strategy. Thus, the WSSL does not rely on the equipment's safety functionalities or uncertified proprietary mechanisms. Instead, aiming at reducing development and validation costs, it intermediates network communications, implementing a set of defense mechanisms, while additionally guaranteeing security parameters.

Author Keywords. Safety Communication, Wireless Networks, Cyber-Physical Systems, Cooperative Systems.

1. Introduction

The type of integration between devices in Co-CPS makes them subject to various types of safety or cybersecurity flaws, be them intentional or not (Yaacoub et al. 2020). Such a condition implies the need for error detection and subsequent action that does not cause a network overload or compromises the application's response time.

In this work, we present a modular Wireless Safety and Security Layer (WSSL) architecture, developed over a ROS (Robot Operating System) environment, to enable the validation of the communication transactions between Co-CPS, establishing a safe way for the exchange of information.

2. Context and Motivation

Cyber threats have been thoroughly studied in the literature, including the causes, impacts, and the development of attack models, including in Co-CPS scenarios (Yaacoub et al. 2020). Also, several works like (Kholidy 2021), (Mousavinejad et al. 2020), and (Chen and Park 2020) presents solutions to some of these threats. However, the lack of a broader model that allows validating the cooperation between devices in a broad Co-CPS scenario, with devices from different manufacturers, is still an obstacle for implementing more complex solutions.

These cyber threats are also pointed in safety standards like IEC 61508 and EN 50159. These define the guidelines by which such threats should be mitigated, towards a certification that is independent of the network interface vendor, enabling for instance the exchange of a radio transceiver, while maintaining the inherent safety guarantees of the communication system. IEC 61508 defines a safety certification for network communications systems, using a White

or Black Channel approach. The White channel approach assumes that all the equipment are individually certificated, while in the black channel, just the network communication interfaces must be certificated, reducing the implementation costs (Creech 2007). Thus, the proposal of a WSSL that can be implemented over a non-secure or safe transmission system can allow communication systems from different manufacturers to interact freely, as long as they are compatible radio-wise, while increasing communications security and reducing safety risks.

3. Wireless Safety and Security Layer (WSSL) Architecture

The implementation of WSSL seeks to increase trust between the various players in a Co-CPS scenario where communication failures or malicious interactions can have critical consequences. The WSSL consists of an additional layer to the adopted communication system, implementing defenses against all relevant communication errors, and where by establishing a safe and secure connection between each WSSL end-point, one can provide an extra level of safety and security to the Co-CPS systems, as it is presented in Figure 1.

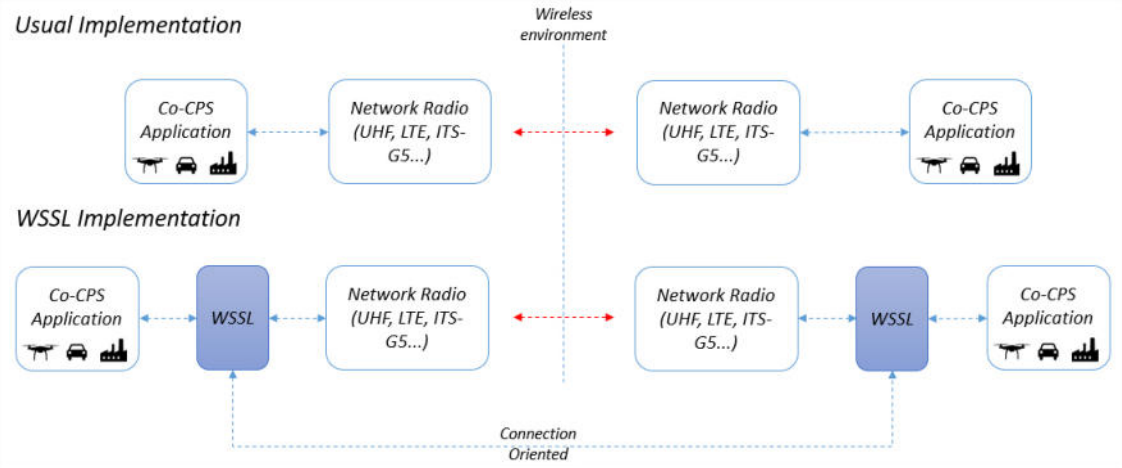

Figure 1: WSSL architecture implementation

A challenging scenario in Co-CPS is the Cooperative Vehicular Platooning (Co-VP), as it deals with a critical operation in a dynamic environment that involves vehicles and eventually passengers, which increases the need to guarantee the safety parameters of the system. Thus, to develop and test the WSSL, we will implement it to the CopaDrive (Filho et al. 2020), a ROS based simulator. By integrating WSSL within a ROS environment, we will achieve much higher flexibility in the layer development, allowing the integration with several communication systems and Co-CPS devices.

The WSSL will establish and guarantee connections between vehicles, protecting communications, acting as an intermediate layer between the application and the ITS-G5 communications stack of the On-Board Unit communications module.

The objective of WSSL is to build a modular architecture that can be easily implemented in low-cost devices that can adapt to the needs of the Co-CPS application, using ROS. In Figure 2, we present the general network threats that the WSSL addresses and the defenses that must be implemented, at least one per threat.

Although, some of the defenses involve verifying the origin and destination of the messages sent, the WSSL is agnostic to the message contents or application payload, guaranteeing the data's trust and privacy. In addition, its implementation is independent, as much as possible, of the communication stack used. An example sequence connection diagram is presented in Figure 3.

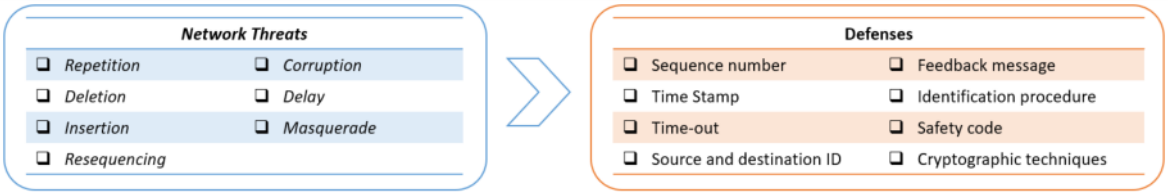

Figure 2: WSSL Threats and Defenses

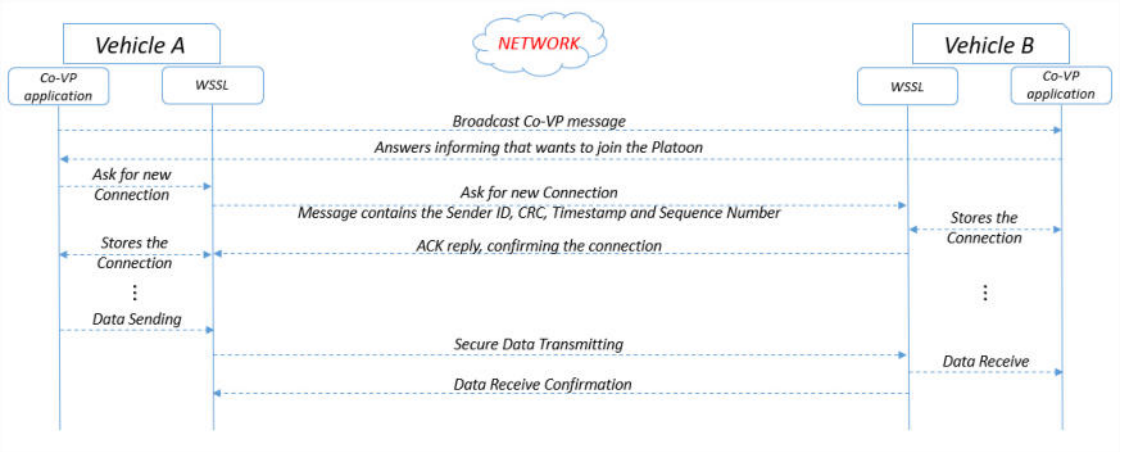

Figure 3: Sequence Connection Diagram

4. Conclusions

The safety and security requirements for Co-CPS systems must be urgently addressed given the criticality of many of these systems. We believe the adoption of WSSL in a modular way is a fundamental proposal to mitigate a series of problems in currently unsecured and unsafe wireless communication systems.

References

Chen, Zheng, and Byungkyu Brian Park. 2020. "Preceding Vehicle Identification for Cooperative Adaptive Cruise Control Platoon Forming." *IEEE Transactions on Intelligent Transportation Systems* 21 (1): 308–20. https://doi.org/10.1109/TITS.2019.2891353.

Creech, Gerry. 2007. "Black Channel Communication: What Is It and How Does It Work?" *Measurement and Control* 40 (10): 304–9. https://doi.org/10.1177/002029400704001003.

Filho, Enio Vasconcelos, Ricardo Severino, Anis Koubaa, and Eduardo Tovar. 2020. "An Integrated Lateral and Longitudinal Look Ahead Controller for Cooperative Vehicular Platooning." In *4th EAI International Conference on Intelligent Transport Systems (EAI INTSYS 2020).*, 18. Online.

Kholidy, Hisham A. 2021. "Autonomous Mitigation of Cyber Risks in the Cyber–Physical Systems." *Future Generation Computer Systems* 115 (February): 171–87. https://doi.org/10.1016/j.future.2020.09.002.

Mousavinejad, Eman, Fuwen Yang, Qing-Long Han, Xiaohua Ge, and Ljubo Vlacic. 2020. "Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning." *IEEE Transactions on Intelligent Transportation Systems* 21 (9): 3821–34. https://doi.org/10.1109/TITS.2019.2934481.

Yaacoub, Jean-Paul A., Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli. 2020. "Cyber-Physical Systems Security: Limitations, Issues and Future Trends." *Microprocessors and Microsystems* 77 (September): 103201. https://doi.org/10.1016/j.micpro.2020.103201.

Acknowledgments

This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (UIDP/UIDB/04234/2020); also by the FCT and the EU ECSEL JU under the H2020 Framework Programme, within project(s) ECSEL/0010/2019, JU grant nr. 876019 (ADACORSA). Disclaimer: This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.