

A multi bearer adaptable communication demonstrator for train-to-ground IP communication to increase resilience

Christian Pinedo, Marina Aguado, Igor Lopez, Marivi Higuero, and Eduardo Jacob

Faculty of Engineering, University of the Basque Country UPV/EHU,
Alameda Urquijo s/n, 48013 Bilbao, Spain
Tel: +34-946-01-4024 E-mail: christian.pinedo@ehu.eus

Abstract. This paper presents the setup of a demonstrator based on Multipath TCP protocol to provide a multi bearer—WiFi and WiMAX—and resilient agnostic layer to support train-to-ground IP communication. The adaptable communication and resilient architecture consists of three main blocks: an Acquisition System, a Detection System and a Multipath Communication System. Several tests carried out with jamming devices disturbing the data transfer established between the end devices demonstrate the resilient capability and performance of the proposed architecture to overcome electromagnetic attacks.

Keywords: Adaptable communication, resilience, MPTCP, FRMCS

1 Introduction

Nowadays, the European train control industry is facing the challenge of searching a successor of GSM-R—the underlying communication technology in ERTMS. There are multiple alternatives such as the natural evolution from GSM-R towards GPRS, the possibility to migrate directly to LTE or the identified as the Future Railway Mobile Communication System (FRMCS) architecture—a multi bearer technology agnostic reference network.

Under this migration scenario, the European Commission—and in a next step the on-going Joint Undertaking Shift2Rail—provides its support to numerous research projects and initiatives. The EU FP7-SEC- 2011-1 Collaborative Research Project entitled SECURITY of Railways against Electromagnetic attacks (SECRET)¹ is also outlined in this context. SECRET project main goal, carried out from 2012 to 2015, was to identify, assure and cope with intentional electromagnetic interferences that might affect current and future communication technologies in railways.

Our contribution in the SECRET project was focused on the design and implementation of a resilient communication architecture—in accordance to ongoing design of an all-IP multi bearer and agnostic FRMCS—whose aim was

¹ <http://www.secret-project.eu>

the ability to face electromagnetic attacks [3][4]. The architecture is based in three main building blocks: the Acquisition System (AS) which is responsible of collecting and processing electromagnetic data in the train and track-side; the Detection System (DS) which is the entity governing the overall resilient communication system; and, finally, the Multipath Communication System (MCS) which provides to the DS multiple communication interfaces and paths in order to dynamically overcome the electromagnetic attacks.

The basis of the behaviour of the MCS is the Multipath TCP (MPTCP) protocol [1]. MPTCP is an extension to the TCP protocol in order to support multi-homed devices, in other words, to support devices with multiple communication interfaces and multiple IP addresses. Thanks to this protocol it is possible to simultaneously use all the IP interfaces of the host for one MPTCP connection, when due to original constrains of the TCP/IP protocol the normal and current behaviour is to use only one interface and IP address.

In the SECRET project we developed a redundant scheduler for MPTCP, which sends the same information replicated through all the available interfaces with the aim of increasing the resilience of the communication whereas the delay and jitter are reduced because MPTCP/TCP retransmissions are minimized [5]. The code of this new scheduler for MPTCP was made publicly available² once the SECRET project finished and then we also collaborated to achieve the inclusion of a redundant scheduler in the official implementation of MPTCP for the Linux kernel³. The patch⁴ that was finally included in the official MPTCP implementation was not only based on the proposal of the SECRET project but also on a second proposal of a redundant scheduler published afterwards [2].

2 Description of the demonstrator

The demonstrator focuses on showing the increase on the resilience of the wireless communications thanks to the use of MPTCP and, more precisely, thanks to the use of the new redundant scheduler.

The setup, see Fig. 1, consists basically on two devices that needs to transfer real-time MPTCP/TCP information through wireless links. In order to proceed with data transmission, these wireless devices have two different wireless transceivers: one WiFi transceiver at 2,4GHz and one WiMAX transceiver at 5GHz. Under normal conditions, devices are configured to use the WiFi transceiver instead of the WiMAX one.

This baseline setup will be disturbed with the help of a jammer that will interfere and finally raise down the WiFi connection. Thus, it will disturb the data transfer established between the end devices.

The demonstrator will allow to appreciate how established connections can switch from one interface to another without losing connectivity and consequently without requiring to re-establish the connection again.

² <http://github.com/i2t/rmptcp>

³ <http://github.com/multipath-tcp/mptcp>

⁴ <http://github.com/multipath-tcp/mptcp/pull/109>

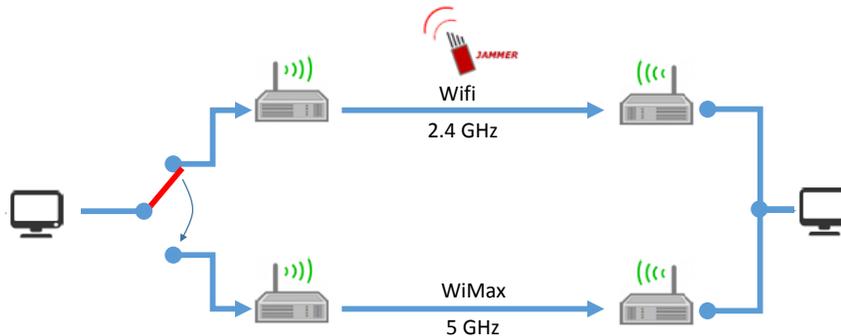


Fig. 1. Setup of the demonstrator.

Acknowledgements

The work described in this paper is partially supported by the EU FP7-SEC-2011-1 Collaborative Research Project entitled SECRET and by the Spanish Ministry of Economy and Competitiveness through the SAREMSIG TEC2013-47012-C2 project (Contribution to a Safe Railway Operation: Evaluating the effect of Electromagnetic Disturbances on Railway Control Signalling Systems). This work is produced within the Training and Research Unit UFI11/16 funded by the UPV/EHU.

References

1. Ford, A., Raiciu, C., Handley, M., Bonaventure, O., Paasch, C.: Tcp extensions for multipath operation with multiple addresses. Internet-Draft draft-ietf-mptcp-rfc6824bis-05, IETF Secretariat (January 2016), <http://www.ietf.org/internet-drafts/draft-ietf-mptcp-rfc6824bis-05.txt>
2. Frömmgen, A., Erbschäuffer, T., Zimmermann, T., Wehle, K., Buchmann, A.: Remp tcp: Low latency multipath tcp. In: Proceedings of the 2015 CoNEXT on Student Workshop, CoNEXT Student Workshop '15, ACM, 2015 (2015)
3. Gransart, C., Pinedo, C., Aguado, M., Heddebaut, M., Jacob, E., Lopez, I., Higuero, M.: Cyber attacks in the guided_transport domain. In: Proc. Computer & Electronics Security Applications Rendez-vous (C&ESAR2014). Rennes, France (Nov 2014)
4. Heddebaut, M., Mili, S., Sodoyer, D., Jacob, E., Aguado, M., Pinedo, C., Lopez, I., Deniau, V.: Towards a resilient railway communication network against electromagnetic attacks. In: Proc. Transport Research Arena 2014 Conference (TRA2014). Paris, France (Apr 2014)
5. Lopez, I., Aguado, M., Pinedo, C., Jacob, E.: SCADA Systems in the Railway Domain: Enhancing Reliability through Redundant MultipathTCP. In: Proc. Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on. pp. 2305–2310 (Oct 2015)