Cybersecurity considerations for CBTC

Simone Soderi^{*‡}, Matti Hämäläinen[‡], Jari Iinatti[‡]

^{*}Alstom Signalling Solutions, Florence, Italy. email:simone.soderi@transport.alstom.com

[‡]Centre for Wireless Communications, University of Oulu, Oulu, Finland email:firstname.lastname@ee.oulu.fi

Abstract—Communication Based Train Control (CBTC) and the European Rail Traffic Management Systems (ERTMS) are prevailing radio controlled systems for railway. As a part of the ERTMS standard, the European Train Control System (ETCS) implements on-board control systems throughout multiple radios. CBTC makes use of RF-based data communication systems (DCSs) for train control and traffic management. Even if ERTMS and CBTC have different origins, both make use of wireless communications for safety related systems. This paper describes cybersecurity considerations for CBTC. First, authors studied the impact of security on intra-vehicular communications in a real tunnel scenario, e.g. for urban transit where the usage of security is mandatory in order to maintain the system safety. Secondly, the impact of a jamming attack against ETCS radio has been analyzed. Measurement campaigns confirmed Host Identity Protocol (HIP) as an effective security solution at layer 3 in terms of the protocol overhead introduced. On the other hand, the Balise Transmission Module (BTM), included in ETCS standard, is sensitive to jamming attack and the measurements presented here would offer the sights for further security considerations around the CBTC.

Index Terms—CBTC; HIP; Security; Vehicle; Wireless; ETCS.

I. INTRODUCTION

Since 1990's Communication Based Train Control (CBTC) increased its popularity among railway operators because the performance of these systems allow the maximization of railway capacity. CBTC throughout vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) radio communications collects information on train position and consequently adapts trains speed. On the other hand, urban transit systems make use also of the European Train Control System (ETCS) as signaling train protection system. ETCS is a state of the art of signaling systems and is specified in four levels. In this paper, authors focused only on the spot transmission between train and wayside *balises* implemented in ETCS Level 1 and Level 2. The on-board balise transmission module (BTM) communicate with balises via an antenna placed under the vehicle. Balises are inductive transponders installed on the railway track. When the train passes over the balise, it energizes this passive transponder throughout a telepowering signal at 27.095 MHz. When activated, each balise sends back to the train a telegram via the up-link signal at 4.234 MHz [1].

These systems require high safety levels which increase the complexity of design and test. Lately, safety depends on computer systems and with the evolution of wireless technology, railway products are fully connected throughout

DCSs. First of all should be clear the difference between safety and security: safety avoids physical harm to humans and things whereas security applies defenses from malicious attacks [2]. Hacking a safety system in the best case could bring that to fail safe state, compromising the system availability [3]. In the worst case scenario, fatal accidents occur to people.

This paper overviews the CBTC security scenario with focus on DCS and BTM subsystem analyzing results achieved during the measurements campaign.

II. CBTC SECURITY SCENARIO

The worldwide proliferation of wireless local area networks (WLAN) started many years ago and today Wi-Fi confirms its maturity. Nowadays, Wi-Fi based on IEEE 802.11 standard is often selected in safety related applications like V2V and V2I in CBTC. Furthermore, CBTC employs ETCS' radios balises to get the exact train position and then implement accurate vehicle positioning close passengers' platforms. ETCS was designed in the 1990s with security mechanisms available at that time and these need to be updated to face with current security threats [4]. This scenario makes railway market possible for hackers as well as researches to provide new mechanisms to improve security.

Fig. 1. CBTC cybersecurity scenario.

Figure 1 shows the CBTC cybersecurity scenario analyzed in this paper. Authors assumed two adversaries. The first jams balises close the passengers platform whereas the second embarked on the train attacks Wi-Fi based networks, such as V2V or intra-vehicular wireless communication.

Security services included in wireless communications can be grouped in categories, such as authentication, confidentiality, integrity and availability. Table I lists possible security attacks in CBTC against vehicular communications and balises.

TABLE I
SUMMARY OF POTENTIAL ATTACKS IN CBTC.

TARGET	TYPE	SECURITY SERVICE	SECURITY THREATS	CONSEQUENCES	RISKS	OCCURRENCE LIKELIHOOD	MITIGATIONS
Balise-BTM	Active	Integrity	Jamming	Train DoS Error Train Stop	High	Possible	Real Time interference detection
V2V or V2I	Passive	Confidentiality	Eavesdropping	Loss Information	Medium	Likely	HIP/IPSec
V2V or V2I	Active	Authentication	Man in the Middle	Insert False Information	High	Likely	HIP/IPSec
V2V or V2I	Active	Availability	Flooding attack	DCS DoS	High	Likely	HIP/IPSec

A. Attack to Wi-Fi based DCS

An adversary on-board the train with his laptop can perform various attacks against the intra-vehicular Wi-Fi communication. For unified communications in rail systems, CENELEC classifies Wi-Fi as an open communication, i.e. category 3 in CENELEC 50159 [5], requiring a cryptographic defense in order to resist to malicious attacks. Host Identity Protocol (HIP) is selected to secure V2V/V2I and intra-vehicular communications because it offers end-to-end security and resistance to previous attacks [6], listed in Table I. HIP with the Base Exchange (BEX) initial stage establishes a Secure Association (SA) between end-nodes, then both hosts use IP Security (IPSec) in order to exchange data via a secure tunnel, as shown in Figure 2. Measurements campaign in a tunnel scenario has shown that HIP IPSec is a promising protocol to secure intra-vehicular communications in terms of throughput, jitter and packet loss [7].

Fig. 2. Protected traffic.

B. Jamming attack to BTM/Balises

During the coupling between ETCS on-board system, i.e. BTM, and balises, these send to the train telegrams through-out up-link signal. It is a narrow-band signal modulated by Frequency Shift Keying (FSK) with characteristics as follows

- frequency: $4.234 \text{ MHz} \pm 5 \text{ kHz}$;
- data-rate: 564.48 kbps;
- telegram coding: BCH;
- telegram length: 341/1023 bits.

ERTMS standard doesn't take jamming into consideration as a security threat that can interrupt the communication between BTM and balise [4]. Authors reproduced the attack in laboratory with a real railway equipment and one balise. Figure 3 shows a single tone jamming swept over 1 ms

in the range of one frequency utilized by FSK modulation, i.e. $3.92 \div 3.98 \text{ MHz}$. We assumed that adversary without particular knowledge of the system can jam balises close the passengers platform in a metro station interfering in the train stop. The real time interference detection and its cancellation should be a valid system countermeasure against this security threat.

Fig. 3. Jamming attack to Balise.

REFERENCES

- [1] FFFIS for Eurobalise. [Online]. Available: <http://www.era.europa.eu/Document-Register/Pages/Set-2-FFFIS-for-Eurobalise.aspx>
- [2] J. Gronbaek, T. Madsen, and H. Schwefel, "Safe Wireless Communication Solution for Driver Machine Interface for Train Control Systems," in *Systems, 2008. ICONS 08. Third International Conference on*, April 2008, pp. 208–213.
- [3] K. Hansen, "Security attack analysis of safety systems," *Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pp. 1–4, 2009.
- [4] I. Lopez and M. Aguado, "Cyber security analysis of the european train control system," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 110–116, October 2015.
- [5] "CENELEC EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems," 2012.
- [6] D. Kuptsov, A. Khurri, and A. Gurtov, "Distributed user authentication in wireless LANs," in *World of Wireless, Mobile and Multimedia Networks Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*, June 2009, pp. 1–9.
- [7] S. Soderi, H. Viittala, J. Saloranta, M. Hamalainen, J. Iinatti, and A. Gurtov, "Security of wi-fi on-board intra-vehicular communication: Field trials of tunnel scenario," in *2013 13th International Conference on ITS Telecommunications (ITST)*, Nov 2013, pp. 278–283.