IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 July 2023, accepted 14 August 2023, date of publication 28 August 2023, date of current version 31 August 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3309005*

PERSPECTIVE

# Cybersecurity Considerations for Communication Based Train Control

**SIMONE SODERI**[1,2], **(Senior Member, IEEE), DANIELE MASTI**[1,2], **MATTI HÄMÄLÄINEN**[3], **(Senior Member, IEEE), AND JARI IINATTI**[3], **(Senior Member, IEEE)**
[1]IMT School for Advanced Studies, 55100 Lucca, Italy
[2]CINI Cybersecurity Laboratory, 67503 Rome, Italy
[3]Centre for Wireless Communications, Faculty of Information Technology and Electrical Engineering, University of Oulu, 90570 Oulu, Finland

Corresponding author: Simone Soderi (simone.soderi@imtlucca.it)

This work was supported in part by Consorzio Interuniversitario Nazionale per l'Informatica (CINI) through Research Project under Grant CA 01/2021 a.i. 2. Daniele Masti is a member of INdAM-GNAMPA.

**ABSTRACT** The CENELEC TS 50701 is the first encompassing standard aiming at governing cybersecurity risk management processes within the railway industry. Although the technical maturity of this framework is undeniable, its application in practical projects is still an active field of discussion among practitioners, especially when dealing the communication-heavy subsystems. Among such subsystems, signalling is among the most critical ones. Both Communication-based Train Control (CBTC) and European Railway Traffic Management Systems (ERTMS) heavily rely on wireless communications for their operation. This paper describes two cybersecurity attack scenarios regarding wireless communications for CBTCs that can impact the safety of these systems using the lens of the framework provided by the novel CENELEC TS 50701. In doing so, we discuss the implications of using such guidance, especially concerning the different interpretations found in the literature regarding zoning communication systems, to assess and mitigate the cybersecurity risk and improve the posture of CBTC systems concerning the examined attacks. Experimental tests conducted in controlled laboratory environments and high-fidelity simulations have been conducted to support the cybersecurity analysis.

**INDEX TERMS** Railway security, jamming, TS 50701, railway communications, telecommunication security, railway signalling.

## I. INTRODUCTION

Railways have been one of the primary commodities to move passengers and freight since at least the late 19th century. Yet, railway operators continuously face constant pressure to increase performance and the availability of their services [1]. Despite the recent technological advances, however, increasing the performance of such well-tuned systems without compromising their already excellent safety characteristics is nothing short of a titanic challenge. This is even more true if one considers the high degree of control that the general public (which is both a final user and one of the biggest sponsors for much infrastructure) imposes on railway industry players.

Given this premise, it should be no surprise that the railway industry has quickly become a massive user of the novel networked and computerized systems to handle most aspects of its operations, thus replacing the ancient electromechanical systems onboard the train and off-board. Indeed, computer-based systems offer an almost unparalleled level of flexibility and performance, enabling operators to offer additional services like infotainment to passengers. Moreover, using this kind of technology, practitioners have access to a vast array of off-the-shelf components already for affine industries, thus significantly bringing down costs and speeding up deployments.

Unfortunately, the use of such modern technology has brought a novel set of issues to the railway community: one of them is cyber security. Indeed, these novel systems offer both a broader attack surface than past dedicated systems and require far less specialized knowledge to be attacked due to the high degree of commonality between different parts. These facts, coupled with the relative lack of security

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

awareness among industry players and the high profile of the target, make railway systems a golden target for all kinds of attackers, ranging from "script kiddies" to state-sponsored actors. Indeed, many attacks on railway infrastructure have been carried out in recent years. Even if we limit ourselves to attacks against signaling [2], [3], one must cite the event in Lodz, Poland, in 2008, in which a teenager was able to derail four trams using a replay attack [4].

While the topic of security in railway systems has been significantly explored in the literature (we refer the interested reader to [5], [6], [7], and [8] and the references therein), as we said before, the industry has severely lagged on this issue, possibly due safety certification concerns. Indeed, one might argue that novel CENELEC Technical Specification 50701 [9] is the first, and arguably far from too early, attempt to merge together the topic of safety and security in the railway sector [10].

The CENELEC TS 50701 aims to govern the cybersecurity risk management process within the railway industry. Briefly, Its general structure loosely follows the EN 50126 [11] and requires one to carry out several steps to achieve a secure and safe design of a railway system. The TS 50701 describes a seven-step process (each called "Zone and Conduit Requirements" (ZCR)) to improve the security posture of railway systems. The procedure covers the security process's implementation, from its beginning to the final approval of the developed cybersecurity plan by the Asset Owner. For the first step, the regulation demands one to identify the so-called *System under Consideration* (SuC) ("ZCR 1"), which will be further divided into *zones* according to the context. In particular, each zone will comprise devices carrying out a specific task and subject to the same security requirements. Different zones communicate with each other through the use of *conduits* that define how communications can occur. At this stage, we perform an initial risk evaluation in which the threat landscape and the corporate risk matrix are evaluated ("ZCR 2" phase). Using such information, the initial zoning is further refined ("ZCR 3" phase) to individuate the most critical parts of a SuC and to draw the communications avenues (the *conduits*) between different zones or SuCs. Following this stage, we then delve into defining the "Security Level - Target" to achieve in each zone, analyzing each zone's threats, and proposing the necessary countermeasures to flatten the risk to an acceptable level.

Although this norm has practically reached its maturity, how to apply the often overreaching prescription dictated by the norm to practical projects is still an active field of discussion among practitioners. In this study, we try to address this crucial issue by examining the application of TS 50701 by taking as use cases two attacks targeting wireless communication apparatuses introduced at the 2016 Seventh Nordic Workshop on System and Network Optimization for Wireless.[1] By investigating how TS 50701 can be applied to mitigate and resolve these challenges, we aim to provide valuable insights into the practical implementation of the norm. In doing so, we will also expand the original discussion of the two considered attacks and discuss the security risks, the consequences, and the mitigation of the analyzed attacks.

In Figure 1, we depict the scenarios we analyze in this paper. In particular, we analyze a first scenario in which an adversary jams a Balise near the passenger platform. In the second scenario, we consider an attacker on a train trying to compromise Vehicle-to-Vehicle (V2V) or Intra-Vehicular (IV) Wi-Fi-based communication systems.

The paper is organized as follows: Section II illustrates the operation framework provided by the TS 50701, taking the security of signalling systems at a physical level from a telecommunications perspective as a use case. In Section III, we explore how off-the-shelf network systems can be exploited to attack onboard communications networks onboard a train, focusing on wireless-based communications. In doing so, we provide several considerations regarding how the security process of communications systems should be analyzed in the TS framework, especially analyzing how communications infrastructure should be treated within this framework. Finally, Section IV concludes the paper with a brief recap and a perspective on future works.

## II. IDENTIFYING THE SYSTEMS UNDER CONCERN: SIGNALING SYSTEMS

Signalling comprises all the machinery necessary to ensure the safe movement of rolling stocks on railway infrastructure. It is part of the so-called wayside systems, including other critical components such as the electrification systems and level crossings, fulfilling several essential roles in maintaining safe and efficient railway and urban transit services [13], [14].

Among the many systems and standards proposed for signalling, the European Rail Traffic Management System/European Train Control System (ERTMS/ETCS) and Communication Based Train Control (CBTC) arguably belong among the most deployed and used. In particular, CBTC [14], [15], [16] was designed with the metro market [17] in mind, but has found applications in non-urban railway systems. ETCS, instead, has *de facto* become the global standard [18] in the high-speed and mainline railway market segment [3], [19], [20].

ETCS relies on a safe spot transmission system called *EuroBalises* for conveying safety-related information between the wayside infrastructure and the train to achieve high headway performance and provide continuous Automatic Train Protection functions and vice-versa [21]. Similar technology is also used in CBTC, which relies on "continuous, high-capacity, bidirectional train-to-wayside data communications" [14], which heavily exploits the accurate positioning guaranteed by EuroBalises. As EuroBalises are such a vital component of railway systems, it is no surprise that both the safety and security aspects of this apparatus must be guaranteed. For this reason, in the remainder of this

[1] The original contribution was accepted for oral presentation only. A preprint of the presented material can be found at in [12] to facilitate the review process.

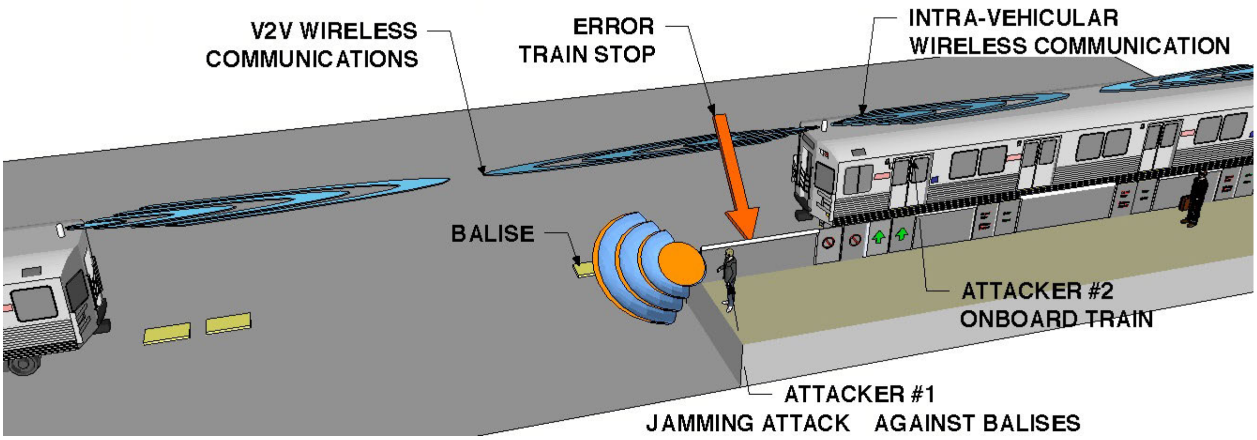

V2V WIRELESS COMMUNICATIONS
ERROR TRAIN STOP
INTRA-VEHICULAR WIRELESS COMMUNICATION
BALISE
ATTACKER #2 ONBOARD TRAIN
ATTACKER #1 JAMMING ATTACK AGAINST BALISES

**FIGURE 1.** CBTC cybersecurity scenario in which the attacker disrupts BTM-Balise (attack #1) communication or violates the wireless communications on board the train (attack #2).

Section, we will provide a security analysis of this communications subsystem according to the approach defined by TS 50701.

### A. ZONING: A CLOSER LOOK TO EUROBALISES COMMUNICATIONS

Following the line of reasoning in the previous Section, it is apparent that, within the Signaling SuC, Vehicle to Infrastructure (V2I) systems, including the spot communications system built around Eurobalises, are very natural candidates to become a *zone*. From a technological point of view, the EuroBalises (in the rest of the article, they will also be called simply Balises) are inductive transponders installed on the railway track that store infrastructure data in "telegrams" (which encode information such as speed limits, line gradient, etc.) and send their data to the train when energized by power from the train's antenna. In most cases, these telegrams are static, but in particular scenarios, they can also be varied dynamically by the rail traffic control room. In such a case, EuroBalises are connected to the Lineside Equipment Unit installed at the trackside. When the train passes above the Balise, the Balise Transmission Modules (BTM) mounted under passing trains broadcast radio frequency energy to energize this passive transponder through a tele-powering signal at 27.095 MHz. Each Balise returns the telegram to the train when activated via the up-link signal at 4.234 MHz [21].

### B. THE THREAT LANDSCAPE: A ZOOM ON JAMMING ATTACKS

Since EuroBalises are a vital component of railway systems, it is no surprise that many Authors have explored how robust such systems are against different kinds of attacks. Among the many types of attacks, *jamming attacks* [22] are among the most studied. These attacks can be loosely defined as all those events in which a malicious actor injects noise or interference signals to disrupt wireless communications. Looking carefully at the ERTMS standard that defines the technical aspects of this communications scheme, however, it can be noticed that no particular care is employed to prevent and or mitigate jamming phenomena [21], [23]. The effect of this type of attack can be very significant. Indeed, as noted in [24], simply making one or more Balises unavailable in a metro rail context can severely hinder the train's ability to successfully perform an automated train stop, possibly compromising the system's overall safety. This kind of attack could bring severe consequences beyond the domain of a single train: as noted in [5], even short delays can cascade into a generalized disservice.[2]

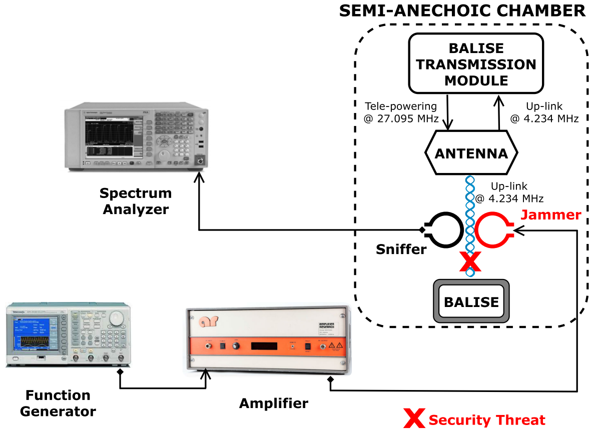


**FIGURE 2.** Test bed in the semi-anechoic chamber to simulate a jamming attack (attack #1) on the BTM communications system.

To summarize, a successful attack of this kind can significantly impact the operation and possibly the safety of a railway system. However, this datum alone is insufficient to deliver a proper risk analysis. Indeed, to evaluate the risk, the TS 50701 [9, Chapter 6] asks for two additional data on top of the already mentioned impact evaluation: the vulnerability (which measures the knowledge to achieve and the technical difficulties that one has to overcome to build the necessary

[2] Although the Authors in [5] consider a slightly different scenario, their method should also be well applicable to the use case presented in this work.

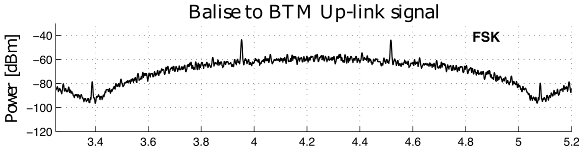


**FIGURE 3. FSK modulated up-link signal transmitted from Balise to BTM during its normal operation.**

machinery to carry out an attack) and the exposure (the level of difficulty to overcome to reach the attacked apparatus) ratings. These two factors are weighted into a likelihood rating assessment, which will be then used to compute the risk rating.

### *C. A CASE STUDY FOR RISK EVALUATION*

As a case study to further delve into the application of the TS 50701, we recall and expand the attack reported in [12] and show how electromagnetic interference can be used to disrupt the wireless spot communications between the train and a Balise installed on the tracks.

As previously mentioned, during the train's passage, the ETCS onboard subsystem BTM energizes the Balise on the ground. This latter device will, in turn, responds with an up-link telegram. It is a narrow-band signal modulated by Frequency Shift Keying (FSK) with characteristics as follows [21]

- *frequency*: 4.234 MHz ± 5 kHz;
- *data-rate*: 564.48 kbps;
- *telegram coding*: BCH coding is used to synchronize Balieses with the BTM;
- *telegram length*: 341/1023 bits.

Starting from this basic observation, we now define our working conditions for conducting the attack. Figure 2 shows the test bed created to simulate the attack on real systems. We can see how the BTM system was placed on a wooden stand inside a semi-anechoic chamber to reproduce the correct distance from a Balise placed under it at $\approx$ 50 cm. Using a magnetic sniffer connected to a spectrum analyzer, we verified that the BTM correctly exchanged telegrams with the Balise once activated, Figure 3 shows the BTM system during regular operations while receiving telegrams from Balise.

A simple wire loop of the same size as the Balise was then used to simulate jamming. This loop was fed by a function generator whose signal was first amplified. With this setup, two different attacks have been simulated: one based on Continuous Wave (CW), i.e., a single frequency tone (see Figures 3- 5), and one which involved a swept tone close to the up-link frequency (see Figures 6- 7).

Knowing that the up-link signal is at 4.234 MHz and is FSK modulated at a rate of 564.48 kbps, for example, the frequencies we need to jam for the first FSK tone are at 3.95176 MHz and 4.51624 MHz. The same principle holds in case one wants to jam the other FSK tone as long as the correct shifted frequencies are used. The frequencies were selected considering the technical specifications of the uplink. It is also helpful to remember that it is sufficient to interfere with only one of the two tones used to block an FSK modulation.

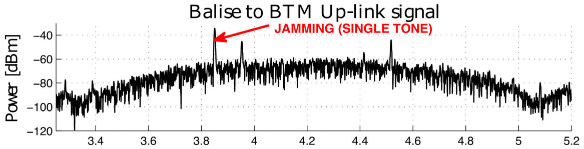


**FIGURE 4. Continuous wave jamming attack to Balise: start of jamming attack.**

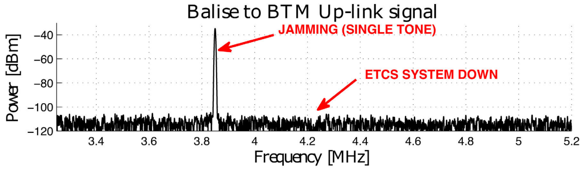


**FIGURE 5. Continuous wave jamming attack to Balise: effect of the attack, i.e., communications between BTM and Balise breaks down. The spectrum analyzer shows only the jamming signal.**

Figure 4 shows the beginning of the single-tone jamming type attack. After a few moments, the communication between BTM and Balise is disturbed, the up-link stops, and we have no more telegram transmission (see Figure 5). Similarly, Figure 6 shows a single tone jamming swept over 1 ms in the range of one frequency utilized by FSK modulation, i.e., 3.92 . . . 3.98 MHz. Once again, like in the first attack, the communication between BTM and Balise is disturbed, the up-link stops, and we have no more telegram transmission (see Figure 7).

### *D. BIT ERROR RATE ANALYSIS WHEN UNDER JAMMING ATTACKS*

The *black-box* nature of railway systems severely limits the kind of analysis that can be performed on the system under test. This consideration also applies to the possibility to communicate quantities such as the Bit Error Rate (BER) to the external world. However, given the significant consequences

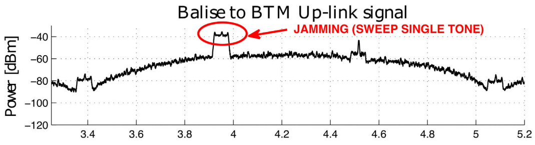


**FIGURE 6. Sweeping the CW jamming signal to disrupt BTM-Balise spot communications: start of jamming attack.**

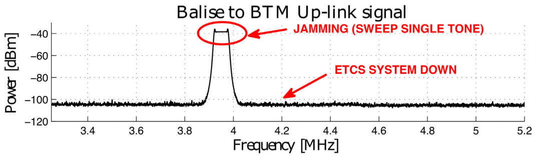


**FIGURE 7. Sweeping the CW jamming signal to disrupt BTM-Balise spot communications: effect of the attack, i.e., communications between BTM and Balise breaks down. The spectrum analyzer shows only the jamming signal.**

of these jamming attacks on the wireless communication between Balise and the train, the need for a complete understanding of the system's behaviour in these circumstances is crucial.

To overcome this issue, we designed simulation-based experiments for our security analysis using MATLAB. The aim here was to replicate the non-coherent FSK modulation of the communication system and to simulate the potential impact of jamming attacks under varying Signal-to-Noise Ratio (SNR) conditions, ranging from 0 dB to 10 dB. These simulations provided a more detailed view of the system response to jamming interference and allowed us to measure the BER, an accomplishment inaccessible in our laboratory tests. Thus, the FSK up-link signal (i.e., $x_U$) can be expressed as [25]

$$x_U(i) = \begin{cases} \sqrt{\frac{2E_S}{T}} cos(2\pi f_1 n), & \text{for } 0 \leq n \leq T \text{ (bit 1)}, \\ \sqrt{\frac{2E_S}{T}} cos(2\pi f_2 n), & \text{for } 0 \leq n \leq T \text{ (bit 0)}, \end{cases} \tag{1}$$

where $E_S$ is the energy of the signal, $f_1 = f_c + \frac{1}{2T}$ and $f_2 = f_c - \frac{1}{2T}$ are the two frequencies needed to transmit two binary digits, $T$ is the symbol time, and $f_c$ is the carrier frequency of the modulated signal.

For the first attack, we used a CW jamming tone with a power higher than the legitimate signal, with a frequency of 500 kHz, far from the FSK tones. Thus, the $i$-th sample of the received signal in the presence of CW jamming and Additive Gaussian White Noise (AWGN) can be represented as follows

$$r(i) = x_U(i) + \underbrace{\sqrt{\frac{2E_J}{T}} cos(2\pi f_J n)}_{\text{Single-tone Jamming}} + \nu(i), \tag{2}$$

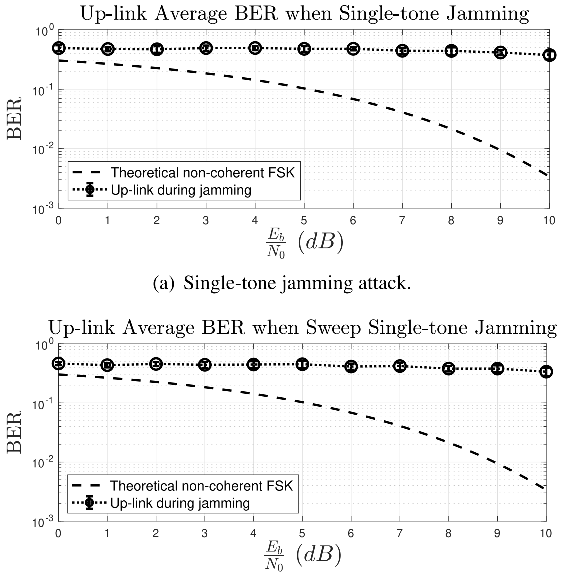
where $E_J$ is the energy of the jamming signal, $f_J$ is the jamming frequuency and $\nu$ denotes the complex zero-mean Gaussian noise with variance $\sigma^2$.

Instead, for the second case, we simulated single-tone jamming in a range of frequencies that included at least one of the FSK tones and swept in 1 ms. Thus, the $i$-th sample of the received signal in the presence of sweep jamming and Additive Gaussian White Noise (AWGN) can be represented as follows

$$r(i) = x_U(i) + \underbrace{\sqrt{\frac{2E_J}{T}} cos\left(2\pi \left(f_{Ja} n + \frac{kn^2}{2}\right)\right)}_{\text{Sweep Single-tone Jamming}} + \nu(i), \tag{3}$$

where $E_J$ is the energy of the jamming signal, $k = \frac{f_{Jb} - f_{Ja}}{\Delta t}$ is the sweep step in the $\Delta t$ sweep time, $f_{Ja}$ and $f_{Jb}$ are the start and final jamming frequencies, and $\nu$ denotes the complex zero-mean Gaussian noise with variance $\sigma^2$.

To create sufficient statistics, we transmitted for both attacks 100k bits for each SNR per bit $\frac{E_b}{N_0}$ value. Where $N_0$ represents the noise spectral density. The simulation results depicted in Figure 8 showed a higher BER under attack (in both cases described by equations (2) and (3)) than what expected under theoretical non-coherent FSK,[3] thereby validating our observations from the real-world experiments. These findings support our assertion that jamming attacks could severely disrupt the integrity of railway wireless communication systems.



(a) Single-tone jamming attack.

(b) Sweep jamming attack.

**FIGURE 8. BER comparison of theoretical non-coherent FSK with AWGN and in the presence of jamming attacks.**

The simulations also agreed with laboratory results regarding the system's response strategy, namely the halting of communication — observed through the spectrum analyzer — upon encountering jamming interference underlines the safety-critical aspect of this subsystem. This automatic shutdown is indeed a fail-safe operation intended to prevent potentially disastrous outcomes from using corrupted data.

This study underscores the critical vulnerability of railway signalling subsystems to jamming attacks. The system's automatic termination of communication under jamming interference indicates its safety-centric design philosophy, but it also highlights the need for improved defences against such disruptive tactics. The challenge is to design ways to support the system's robustness without compromising the indispensable safety features of our railway communication systems.

Please note that although simulations should only be considered in support of real experiments conducted in the laboratory, given the seriousness of the potential security problems, any tool that improves our understanding of the effect of this type of attack is justified.

### E. RISK EVALUATION AND POSSIBLE COUNTERMEASURES

To carry this attack, one can hypothesize that the adversary has no specific knowledge regarding the internal

[3] Recall that the theoretical BER for a non-coherent BFSK in the presence of AWGN noise can be written as [25] $BER_t = \frac{1}{2} e^{(-E_b/2)}$, where $E_b$ is expressed in the linear form.

implementation details regarding the Balises or the onboard equipment as the attack exploits publicly available information only. Building the machinery to implement such an attack is also potentially very simple as it does not require complex control electronics or none. An adequately dimensioned and energized electrical conductor loop might be enough to generate a magnetic field that can disturb the operation of the Balises. As such, it is apparent that this kind of attack warrants a high vulnerability rating.

Regarding the exposure, we note that the train antenna is directed toward the ground, and the distance between this onboard antenna and the Balises is on the order of 40 . . . 60 cm. In other words, placing the necessary machinery to carry out this attack presents non-negligible difficulties. This fact suggests assigning a medium exposure rating to this kind of attack.

This analysis is summarized in the first row of Table 2.

As a whole, this attack warrants a high level of risk, meaning proposing mitigations is imperative to achieve security and safety.

To carry this attack, one can hypothesize that the adversary has no specific knowledge regarding the internal implementation details regarding the Balises or the onboard equipment as the attack exploits publicly available information only. Building the machinery to implement such an attack is also potentially very simple as it does not require complex control electronics or even any electronics at all. An adequately dimensioned and energized electrical conductor loop might be enough to generate a magnetic field that can disturb the operation of the Balises. As such, it is apparent that this kind of attack warrants a high vulnerability rating.

Regarding the exposure, we note that the train antenna is directed toward the ground, and the distance between this onboard antenna and the Balises is on the order of 40 . . . 60 cm. In other words, placing the necessary machinery to carry out this attack presents non-negligible difficulties. This fact suggests assigning a medium exposure rating to this kind of attack.

This analysis is summarized in the first row of Table 2.

As a whole, this attack warrants a high level of risk, meaning proposing mitigations is imperative to achieve security and safety. Fortunately, mitigating such an attack nowadays is relatively simple and can be done by operating at the onboard system level as many technologies to do so exist (see, for instance, [26]). Indeed, as depicted in Figure 9, a simple interference detector can be utilized to identify disturbances in the radio channel, thus distinguishing between faults within the V2I subsystem and the action of external actors. This information can then be relayed to the central onboard unit, enabling it to make informed decisions, such as discarding the affected Balise or engaging in interference cancellation strategies. Such countermeasures should be able to bring the *achieved security level* to acceptable levels without requiring significant modifications of the already existing subsystems.

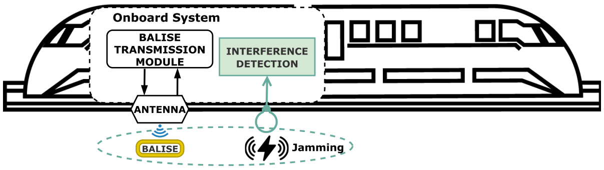


**FIGURE 9. Interference detection system to mitigate jamming-type attack on BTM/Balise.**

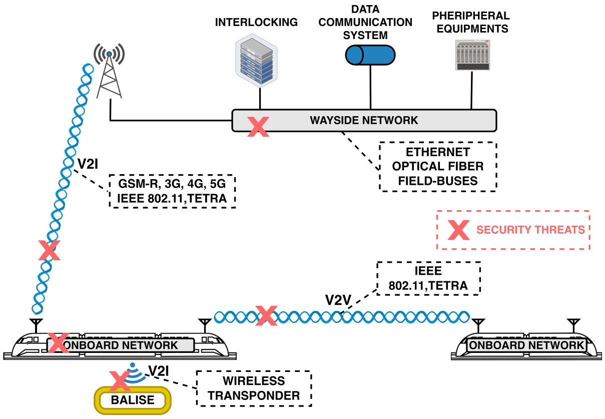


**FIGURE 10. A schematic representation of the many communications channels used by railways systems. Dashed boxes list possible technological solutions.**

## III. CYBERSECURITY CONSIDERATIONS: A VIEW ON CONDUITS

According to TS 50701, different zones can be interconnected through *conduits*, which nature designates the type of communications between different zones. This concept is not a novelty by itself. Indeed, as also acknowledged by norm itself [9, Annex A], a very similar concept is also present (for instance) in the IEC 62443 [27] and the EN 50159 [28] regulations.

In particular, the TS 50701 describes three types of conduits: i) the transparent gateway (which connects without filtering different zones with the same security level); ii) the diode types (which allows for unidirectional communication); iii) and the firewall type (which allows for bidirectional filtered communications). This granularity is a novelty introduced by the framework.

While the TS 50701 suggests that a conduit is more a logical than a physical asset, it also leaves unanswered if the machinery used to build the conduits (e.g., routers) belong only to the zone they protect or only to the conduit or to both. In the following, we provide a view on this issue, taking the use of Wi-Fi communications as a test case.

### A. A VIEW ON WI-FI BASED DCS

The worldwide proliferation of wireless local area networks (WLAN) started many years ago, and today Wi-Fi confirms its maturity. Nowadays, Wi-Fi communications technologies based on IEEE 802.11 and other standards are often selected in CBTC for safety-related applications such as V2V and V2I (see Figure 10).

Unfortunately, these general-purpose communications technologies have often been designed without explicit industrial security/safety characteristics in mind. Thus, as shown in Figure 10, they may have security vulnerabilities that, if exploited, can compromise systems availability and, in some cases, put passengers at risk. Despite these limitations, the already mentioned constant struggle for better performance and lower costs has also pushed the use of such technology in the railway industry. An example is the use of cellular communications technology for ERTMS, which has raised many security concerns [8]. In such a case, wireless communications is a common choice because it minimizes the hardware modification to trains as it requires limited rewiring. This is especially interesting because Wi-Fi-based DCSs have become popular to *revamp existing CBTC installations*, where a customer must upgrade an old signaling system based on old buses whose performance is no longer adequate. Indeed, we will consider this use case for the remainder of this Section.

In this case, however, wireless communications become the very conduit interconnecting the already existing zones. In order to maintain the security of the overall system, it is necessary to analyze the threat model and mitigate the risks associated with this technology.

### B. ZONING

As introduced, also in this case, the SuC analyzed is the one related to signalling systems, although we focus primarily on its onboard components. As we want to explore the role of conduits and connectivity in general, we also assume, without loss of generality, that two zones (in the head and tail of the train) with the same high-security level exist and that they have to be interconnected by means of a transparent conduit, which is our Wi-Fi network.

### C. THREAT MODELS FOR IV COMMUNICATIONS

In this Section, we collect some types of attacks on IV communications often discussed in the literature (see, for instance, [29], [30], [31]).[4] Consider an adversary onboard the train (see Figure 11) with his laptop that performs various attacks against IV Wi-Fi communications. These attacks can be grouped into the following categories:

- *eavesdropping attacks.* As with any wireless communications, a Wi-Fi link between the head and tail of the train can be intercepted by an attacker onboard the train using, for example, his laptop or other similar devices. These attacks passively breach the *confidentiality* of the communication;
- *Man-in-the-Middle (MITM) attacks.* In this attack model, the attacker could generate false rail signalling information, putting passengers on the train at risk. Any spoofed messages fed into the onboard network can cause emergency failures, unplanned travel delays, and affect vehicle speed. In addition, an attacker could reply to some messages causing an unwanted event while the train driver remains unaware of the actual state of the vehicle. These attacks actively violate both the *authentication* and the *integrity* of the communication;
- *DoS Flooding attacks.* They happen when an attacker inserts an overwhelming number of false messages into the wireless communications inside the vehicle to exhaust network resources. As a result, the system becomes unresponsive to legitimate traffic, which means that emergency failures and system malfunctions can occur. These attacks actively violate the *availability* of the onboard wireless network.

**TABLE 1. Summary of potential attacks in CBTC.**

| TARGET | SECURITY PROPERTY | KIND OF THREAT | ADVERSE EFFECT |
|---|---|---|---|
| Balise-BTM | Integrity | Jamming | DCS DoS; Train stop error |
| IV, V2V and V2I | Confidentiality | Eavesdropping | Information loss |
| IV, V2V and V2I | Authentication, Integrity | MITM | Insertion of false information |
| IV, V2V and V2I | Availability | Flooding attack | DCS DoS |

### D. A RISK ANALYSIS

MITM and DoS attacks aim at breaking integrity, confidentiality (for the former), and availability (for the latter) of the communication channel between the zones. Attacks like these happen in environments that are easy to access for attackers and therefore have a high *exposure* rating. Similarly, the vulnerabilities of off-the-shelf Wi-Fi technology require only moderate technical efforts, corresponding to a high-to-medium *vulnerability* rating according to the norm. At the same time, these kinds of attacks have a high *impact* rating as they can disrupt normal train operations and possibly compromise safety. This situation warrants a high level of risk, according to TS 50701. Similar reasoning also holds for the eavesdropping attacks, although in this case, the impact can be considered very low as it threatens only the confidentiality of the communication. For this reason, the overall risk can be considered more manageable.

These considerations are summarized in Tables 1 and 2.

In all cases, it is apparent that simply substituting a cable connection with a Wi-Fi connection without considering security is, at best, a naive approach. In the next Section, we explore a possible idea to reduce the risk associated with such threats.

### E. BUILDING A SECURE CONDUIT: AN APPROACH BASED ON HOST IDENTITY PROTOCOL

Typically, a communications system is made secure if designers implement security services that guarantee authentication, confidentiality, integrity, and availability. As shown in Table 1, all these services can be attacked; therefore,

[4] Although in this work we restrict our analysis to IV communications, the same considerations also holds for V2V and V2I communications.

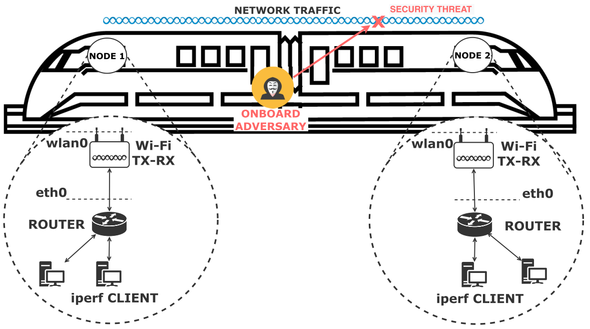


**FIGURE 11.** **Attack and mitigation to the onboard wireless network (attack #2). Principle diagram of an attack against a Wi-Fi-based network.**

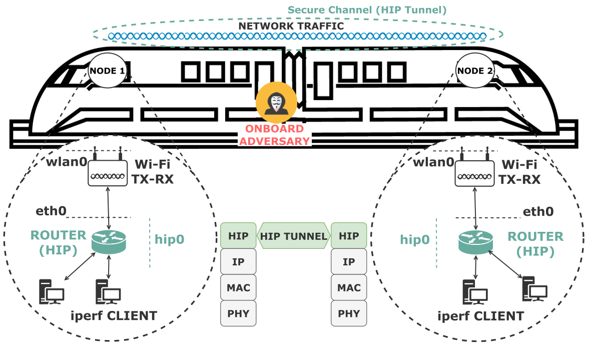


**FIGURE 12.** **Attack and mitigation to the wireless onboard network (attack #2).Use of Host Identity Protocol to mitigate MITM-type attacks.**

to enable Wi-Fi communication as a means for transparent conduits in highly secure zones such as the CBTC systems, we need to find suitable mitigations.

To do so, Soderi et al. [29], [30], [31] proposes using Host Identity Protocol (HIP) for industrial and railway applications to secure the IV communication system architecture.

HIP [32] exploits a new idea in which the communication node's identity and location are separated, unlike in the TCP/IP stack, where each node is identified in the network by its IP address. This new paradigm enables the HIP to negotiate cryptographic keys (called *host identities*) that enable Internet Protocol Security (IPSec), making host mobility and multihoming between different address families (IPv4 and IPv6) secure. HIP also provides end-to-end data encryption and mutual authentication that fits the scenario we need to protect, as shown in Figure 12.

The host identity consists of the public key component of a private-public key pair, providing strong authentication, a feature that is useful against MITM attacks. Furthermore, with this mechanism, any end-node can implement multiple identities exporting this feature to the application layer.

HIP can be thus used to secure IV communications because it offers end-to-end security and resistance to all the attacks listed in Table 1 [33]. Figure 13 presents the results of using HIP in a tunnel scenario similar to the one where a CBTC typically operates. The measurements, extracted from [30], used OpenHIP [34], an open-source version of HIPv1 [35]. Results show how HIP introduces an acceptable overhead of throughput loss, jitter, and packet loss up to 300 m without any repeater and in Non-Line-of-Sight (NLOS) configurations [30]. HIP also makes the conduit resilient to MITM-type and eavesdropping attacks and makes the communication between the two zones (i.e., between two physical areas of the train) transparent and secure, significantly reducing the security risk associated with these attacks. From an implementation point of view, adopting HIP is generally uncomplicated due to the availability of industrial-grade network appliances that inherently support it [36], [37]. This, together with the very promising performance shown in the test, ensures that the associated costs of implementing this technology remain manageable.

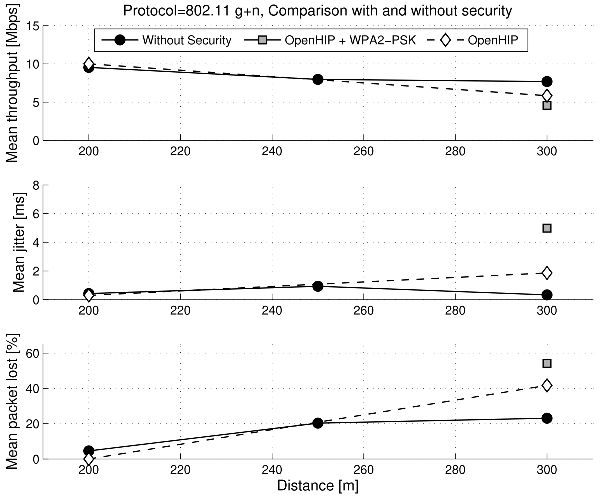


**FIGURE 13.** **HIP performance evaluation in a tunnel scenario in which a CBTC normally operates [30].**

## *F. A CONDUIT OR A ZONE?*

While the mitigations mentioned above are able to mitigate the security posture of Wi-Fi communications, one may ask if, after all these considerations, communications systems are still "only" a conduit or rather a zone itself. The answer to this question is not trivial. Indeed, this point is covered by the TS 50701 itself when its relationship with the EN 62443 is discussed in [9, Annex A.2] where, as mentioned, the belonging of network apparatus to the zone is discussed. Another consideration is made in [38, Page 33], in which it is analyzed that WAN connections can be considered "transparent" for the zoning process as long as there cannot be any possible impact on the dataflow by the provider, and it is theoretically possible to change the nature and the provider of the link without further (or at most minimal) operations on other systems, including the security ones. Although the analysis provided by ENISA is primarily meant for WAN connection, in our opinion, as long as these conditions hold, any network should be considered transparent. This idea is even more true if one considers that such recommendations are very unlikely to hold for WAN connections due to external factors (such as dynamic routing convergence, congestion arising from different customers, etc.) that may alter the

**TABLE 2. Risk estimation of the analyzed attacks to CBTC according to TS 50701 [9]. The likelihood is computed by summing the vulnerability and exposure rating minus one. For all the rating levels, we followed the examples provided in the norm. The risk level is assigned using the risk matrix provided in [9, Table 4].**

| ATTACK | VULNERABILITY RATING | EXPOSURE RATING | LIKELIHOOD | IMPACT RATING | RISK LEVEL |
|---|---|---|---|---|---|
| Jamming on the Balise-BTM link (Section II) | 2 out of 3 | 3 out of 3 | 4 out of 5 | A | High (4 out of 5) |
| MITM attacks (Section III) | 3 out of 3 | 2 out of 3 | 4 out of 5 | A | High (4 out of 5) |
| DoS attacks (Section III) | 3 out of 3 | 2 out of 3 | 4 out of 5 | A | High (4 out of 5) |
| Eavesdropping attacks (Section III) | 3 out of 3 | 2 out of 3 | 4 out of 5 | D | Medium (2 out of 5) |

characteristics of the link while, at the same time, they are likely to hold for a dedicated local area network. To summarize, while defining a zone dedicated to network devices is not an error, we believe such a thing is often unnecessary.

## IV. CONCLUSION

In this paper, we explored the applications of the TS 50701 to improve the security posture of railway systems. In detail, in the first part, we investigated a common weak point of V2I communication based on Eurobalises, discussed the implication of these attacks, and proposed mitigations to negate their adverse effects. In the second part of the paper, we instead focused on the emerging trend of applying general-purpose wireless technology for intra-vehicular (but also V2V and V2I) communications. We showed how such technology needs to improve its application to railway operations.

This work represents an important step in the cybersecurity assessment of onboard railway signalling systems. The practical implications of the proposed mitigations and their implementation within new regulatory constraints are open questions that require extensive experimental validation. Furthermore, exploring novel high-fidelity hardware-in-the-loop simulation environments presents an exciting opportunity to verify our proposals, which we plan to investigate in future research.

In conclusion, while this work represents a significant advancement in securing railway systems, it also emphasizes the necessity for continuous research. The dynamic nature of cybersecurity threats and the evolving landscape of railway communication technologies demands an unrelenting commitment to research, experimentation, and innovation in this critical field.

## REFERENCES

[1] C. N. Pyrgidis, *Railway Transportation Systems: Design, Construction and Operation*. Boca Raton, FL, USA: CRC Press, 2016.

[2] G. Theeg and S. Vlasenko, "Railway signalling & interlocking," in *International Compendium*, vol. 448. Hamburg, Germany: Eurail-Press, 2009.

[3] J. Pachl, "Railway signalling principles," Brunswick, Germany, Oct. 2021. [Online]. Available: https://leopard.tu-braunschweig.de/servlets/MCRFileNodeServlet/dbbs_derivate_00048517/Pachl_eBook_RSP_2-0.pdf

[4] J. Leyden. (2008). *Polish Teen Derails Tram After Hacking Train Network*. [Online]. Available: https://www.theregister.com/2008/01/11/tram_hack/

[5] Z. Wang and X. Liu, "Cyber security of railway cyber-physical system (CPS)—A risk management methodology," *Commun. Transp. Res.*, vol. 2, Dec. 2022, Art. no. 100078.

[6] R. Kour, A. Patwardhan, A. Thaduri, and R. Karim, "A review on cybersecurity in railways," *Proc. Inst. Mech. Eng., F, J. Rail Rapid Transit*, vol. 237, no. 1, pp. 3–20, Jan. 2023.

[7] S. Soderi, D. Masti, and Y. Z. Lun, "Railway cyber-security in the era of interconnected systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 6764–6779, Jul. 2023.

[8] M. Kiviharju, C. Lassfolk, S. Rikkonen, and H. Kari, "A cryptographic and key management glance at cybersecurity challenges of the future European railway system," in *Proc. 14th Int. Conf. Cyber Conflictm Keep Moving*, vol. 700, May 2022, pp. 265–284.

[9] *Railway Applications—Cybersecurity, European Committee for Electrotechnical Standardization Technical Specification*, Standard CLC/TS 50701, CENELEC, Jul. 20221.

[10] CENELEC. (2021). *A Major Step for Railways Cybersecurity: The New CLC/TS 50701*. [Online]. Available: https://www.cencenelec.eu/news-and-events/news/2021/eninthespotlight/2021-06-10-new-clc-ts-50701-railways-cybersecurity/

[11] *Railway Applications—The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, Standard EN 50126, European Committee for Electrotechnical Standardization, CENELEC, 2018.

[12] S. Soderi, M. Hämäläinen, and J. I. Iinatti, "Cybersecurity considerations for CBTC," Jun. 2016. [Online]. Available: https://www.techrxiv.org/articles/preprint/Cybersecurity_considerations_for_CBTC/14701554, doi: 10.36227/techrxiv.14701554.v1.

[13] A. Fantechi, "Connected or autonomous trains?" in *Proc. Int. Conf. Rel., Saf., Secur. Railway Syst.* Cham, Switzerland: Springer, 2019, pp. 3–19.

[14] *Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements*, Standard IEEE 1474.1, The Institute of Electrical and Electronics Engineers Standard, Feb. 2005.

[15] R. D. Pascoe and T. N. Eichorn, "What is communication-based train control?" *IEEE Veh. Technol. Mag.*, vol. 4, no. 4, pp. 16–21, Dec. 2009.

[16] *Railway Applications—Urban Guided Transport Management and Command/Control Systems*, Standard IEC 62290, International Electrotechnical Commission Standard in 3 Parts, Jul. 2014.

[17] A. Ferrari, G. O. Spagnolo, G. Martelli, and S. Menabeni, "Product line engineering applied to CBTC systems development," in *Leveraging Applications of Formal Methods, Verification and Validation, Applications and Case Studies*. Berlin, Germany: Springer, 2012, pp. 216–230.

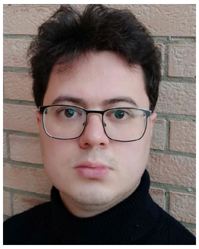
[18] M. Ghazel, "A control scheme for automatic level crossings under the ERTMS/ETCS level 2/3 operation," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2667–2680, Oct. 2017.

[19] F. Flammini, S. Marrone, R. Nardone, A. Petrillo, S. Santini, and V. Vittorini, "Towards railway virtual coupling," in *Proc. IEEE Int. Conf. Electr. Syst. Aircr., Railway, Ship Propuls. Road Vehicles Int. Transp. Electrific. Conf. (ESARS-ITEC)*, Nov. 2018, pp. 1–6.

[20] C. Di Meo, M. Di Vaio, F. Flammini, R. Nardone, S. Santini, and V. Vittorini, "ERTMS/ETCS virtual coupling: Proof of concept and numerical analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2545–2556, Jun. 2020.

[21] *FFFIS for Eurobalise—SUBSET-036*, UNISIG, Menomonee Falls, WI, USA, 2012.
[22] S.-Y. Chang, B. A. N. Tran, Y.-C. Hu, and D. L. Jones, "Jamming with power boost: Leaky waveguide vulnerability in train systems," in *Proc. IEEE 21st Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2015, pp. 37–43.
[23] I. Lopez and M. Aguado, "Cyber security analysis of the European train control system," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 110–116, Oct. 2015.
[24] W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and W. H. Sanders, "On train automatic stop control using balises: Attacks and a software-only countermeasure," in *Proc. IEEE 22nd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Jan. 2017, pp. 274–283.
[25] P. Massoud Salehi and J. Proakis, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2007.
[26] J. Villain, V. Deniau, C. Gransart, A. Fleury, and E. P. Simon, "Characterization of IEEE 802.11 communications and detection of low-power jamming attacks in noncontrolled environment based on a clustering study," *IEEE Syst. J.*, vol. 16, no. 1, pp. 683–692, Mar. 2022.
[27] *Security for Industrial Automation and Control Systems, International Society of Automation & International Electrotechnical Commission Series of Standards*, Standard ISA/IEC 62443, Jul. 2009.
[28] *Railway Applications—Communication, Signalling and Processing Systems—Safety-Related Communication in Transmission Systems*, Standard EN 50159, European Committee for Electrotechnical Standardization Standard, CENELEC, Sep. 2010.
[29] M. Liyanage, P. Kumar, S. Soderi, M. Ylianttila, and A. Gurtov, "Performance and security evaluation of intra-vehicular communication architecture," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2016, pp. 302–308.
[30] S. Soderi, H. Viittala, J. Saloranta, M. Hämäläinen, J. Iinatti, and A. Gurtov, "Security of Wi-Fi on-board intra-vehicular communication: Field trials of tunnel scenario," in *Proc. 13th Int. Conf. ITS Telecommun. (ITST)*, Nov. 2013, pp. 278–283.
[31] S. Soderi, "Evaluation of industrial wireless communications systems security," Ph.D. dissertation, Fac. Inf. Technol. Elect. Eng., Centre Wireless Commun., Univ. Oulu, Oulu, Finland, Jun. 2016, doi: 10.13140/RG.2.2.31155.78880.
[32] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Hoboken, NJ, USA: Wiley, 2008.
[33] D. Kuptsov, A. Khurri, and A. Gurtov, "Distributed user authentication in wireless LANs," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. Workshops*, Jun. 2009, pp. 1–9.
[34] *OpenHIP*. [Online]. Available: http://www.openhip.org
[35] R. Moskowitz, P. Jokela, T. Henderson, and P. Nikander, "Host identity protocol," Tech. Rep., RFC 5201, 2008.
[36] *Tofino Security*. [Online]. Available: https://www.tofinosecurity.com
[37] *Tempered Networks*. [Online]. Available: https://www.tempered.io/
[38] K. Helmut, C. Schlehuber, K. Ooms, M. Theocharidou, and R. Naydenov, *Zoning and Conduits for Railways*, K. Ooms, M. Theocharidou, and R. Naydenov, Eds. Athens, Greece: European Union Agency for Cybersecurity, 2022.

**SIMONE SODERI** (Senior Member, IEEE) received the M.Sc. degree from the University of Florence, in 2002, and the Dr.Sc. degree from the University of Oulu, Finland, in 2016. His expertise ranges from cybersecurity and wireless communications to embedded systems. He is currently an Assistant Professor with the IMT School for Advanced Studies, Lucca, Italy, and an Adjunct Professor with the University of Padua, Italy, where he teaches the master's degree program in cybersecurity. He has published journal and conference papers and book chapters. He holds five patents on wireless communications and positioning. His research interests include cybersecurity for critical infrastructure systems, 6G, covert channels, network security, physical layer security, electromagnetic emission security, VLC, and UWB. He has been a TPC member of several conferences and served as a reviewer of many IEEE Transactions.



**DANIELE MASTI** was born in Siena, Italy, in 1993. He received the bachelor's degree in computer and information engineering from the University of Siena, in 2015, the master's degree in electric and automation engineering from the University of Florence, Italy, in 2018, and the Ph.D. degree in systems science from the IMT School for Advanced Studies, Lucca, Italy, in 2021. Since 2022, he has been a Researcher of cyber security with the IMT School for Advanced Studies. His research interests include the border between control theory and machine learning, with the overall aim of bridging the gap between the two, and network security.

**MATTI HÄMÄLÄINEN** (Senior Member, IEEE) received the M.Sc., Lic.Tech., and Dr.Sc. degrees from the University of Oulu, Finland, in 1994, 2002, and 2006, respectively. He has been a fix-termed IAS Visiting Professor with Yokohama National University, Japan, from 2016 to 2018. He is currently an Adjunct Professor (Docent) and a University Researcher with the Centre for Wireless Communications, University of Oulu. He is a member of the European Telecommunications Standards Institute (ETSI) and the Smart Body Area Network (SmartBAN) Group. He has published more than 200 scientific publications. He is the co-editor of one book, coauthor of one book and five book chapters, and holds one patent. His research interests include ultrawideband systems, radio channel modeling, wireless body area networks, and medical ICT. He served as a reviewer for IEEE and IET journals. He was a technical program committee member for numerous IEEE conferences. He was the General Chair of the Bodynets 2018. He is the Steering Committee Co-Chair of the ISMICT Conference Series.

**JARI IINATTI** (Senior Member, IEEE) received the M.Sc., Lic.Tech., and Dr.Tech. degrees in electrical engineering from the University of Oulu, Oulu, Finland, in 1989, 1993, and 1997, respectively. From 1989 to 1997, he was a Research Scientist with the Telecommunication Laboratory, University of Oulu. From 1997 to 2002, he was a acting Professor of digital transmission techniques, a Senior Research Scientist, a Project Manager, and the Research Director of the Center for Wireless Communications, University of Oulu. Since 2002, he has been a Professor of telecommunication theory. He was an IAS Visiting Professor with Yokohama National University, from 2016 to 2018. He is currently the Head of the Centre for Wireless Communications-Networks and Systems and the Dean of Education with the Faculty of Information Technology and Electrical Engineering. He has authored more than 250 international journal and conference papers and holds six patents. He has supervised 19 Ph.D. thesis and more than 60 master's theses. His research interests include future wireless communications systems, transceiver algorithms, wireless body area networks (WBANs), and medical ICT. He has been a technical program committee (TPC) member in about 25 conferences. He was the TPC Co-Chair of the IEEE PIMRC2006, BodyNets2012, and the PIMRC2014; the TPC Chair of the ISMICT2007; the General Co-Chair of the ISMICT2011, ISMICT2014, and the ISMICT2015; and the TPC Program Track Co-Chair of the BodyNets 2012. He was an Organizer of the FEELIT 2008, the FEELIT2011, the UWBAN2012, and the UWBAN2013. He is the Steering Committee Co-Chair of ISMICT series. He is a Co-Editor of the book *UWB: Theory and Applications* (Wiley and Sons Ltd., Chichester, U.K., in 2004).

Open Access funding provided by 'Scuola IMT Alti Studi Lucca' within the CRUI CARE Agreement