View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Institutional Knowledge at Singapore Management University

Singapore Management University
Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems | School of Information Systems

4-2017

# Vulnerabilities, attacks, and countermeasures in Balise-based train control systems

Yongdong WU
*Institute for InfoComm Research*

Jian WENG
*Jinan University - China*

Zhe TANG
*Central South University*

Xin LI
*Sinocloud Wisdom Technology Co Ltd*

Robert H. DENG
*Singapore Management University*, robertdeng@smu.edu.sg

**DOI:** https://doi.org/10.1109/TITS.2016.2590579

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research


Part of the Information Security Commons, and the Transportation Commons

Citation

WU, Yongdong; WENG, Jian; TANG, Zhe; LI, Xin; and DENG, Robert H.. Vulnerabilities, attacks, and countermeasures in Balise-based train control systems. (2017). *IEEE Transactions on Intelligent Transportation Systems*. 18, (4), 814-823. Research Collection School Of Information Systems.
**Available at:** https://ink.library.smu.edu.sg/sis_research/3817

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Published in IEEE Transactions on Intelligent Transportation Systems, 2017 April, Volume 18, Issue 4, Pages 814-823
http://doi.org/10.1109/TITS.2016.2590579

# Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems

Yongdong Wu, Jian Weng, Zhe Tang, Xin Li, and Robert H. Deng, *Fellow, IEEE*

***Abstract*—In modern rail transport systems, balises are widely used to exchange track–train information via air-gap interface. In this paper, we first present the vulnerabilities on the standard balise air-gap interface, and then conduct vulnerability simulations using the system parameters that were specified in the European Train Control System. The simulation results show that the vulnerabilities can be exploited to launch effective and practical attacks, which could lead to catastrophic consequences, such as train derailment or collision. To mitigate the vulnerabilities and attacks, we propose to implement a challenge–response authentication process in the air-gap interface in the existing transport infrastructure.**

***Index Terms*—Cyber–physical system security, ETCS, Balise.**

## I. Introduction

THE rail transport system has been in operation for over 180 years and has proved to be the most efficient form of land transportation in terms of capacity, speed, distance and punctuality. For example, there were 94.68 million Chinese passenger trips by train on 24 February 2015 (Peak period of Chinese New Year) [1]. Nowadays, RITS (Railway Intelligent Transportation System) is deployed with advanced information and communication technologies in order to meet the growing demand on higher availability, speed, and efficiency. In an RITS, a train localization system shall guarantee localization precision high enough to detect intersecting points in all conditions [2], so that the train control system is able to determine the train speed profile and alarm operators in a timely manner. Thus, the precise train localization and intelligent control operation form the core part of RITS.

Although GPS is able to provide location and time information in all weather conditions, and is freely accessible to anyone with a receiver, it is merely used as a supplement tool of a transport localization and control system due to its weaknesses such as unavailability in tunnels and insufficiently accurate/reliable to distinguish between adjacent tracks. Instead, wayside infrastructure elements and communication systems are widely used for localization and control in modern RITSs. Particularly, a well-known RITS,[1] called ETCS (European Train Control System), uses ground-based Eurobalises (or balises for short) for train localization and control by sending telegrams to on-board BTMs (Balise Transmission Module), where the telegrams comprise balise location, rail gradient, train speed limit etc.

As balises are usually used as position markers which are the sources of movement authority ("permission to proceed"), the failure to detect a balise or a series of balises requires immediate actions such as stopping the train. This is because degraded balise detection may contribute to serious consequences [5]. As the telegram transmitted from balise to BTM is considered to be safety critical, ETCS SUBSET-036 [6] states that "*The worst case for the Balise input-to-output characteristic and field conformity shall be considered*. . . ., *The worst case situation for the On-board Transmission Equipment and for air-gap propagation shall be considered*." Furthermore, it specifies methods to correct errors due to air-gap noises to ensure integrity of the telegram. In order to provide better air-gap transmission performance, telepowering signal modeling [7], discrete point positioning [5], position optimization [8], reliability analysis [9], crosstalk interference analysis [10] and sensor-fused virtual balises [11] are proposed as improvements on ETCS SUBSET-036.

Nonetheless, all of the above proposals only concern the random air-gap noises for improving position accuracy and/or communication robustness, totally ignoring malicious attacks on the wireless transmission channels, such as signal jamming, and telegram tampering. Unfortunately, the attacks can be easily conducted as railways are publicly accessible. Both theoretical analysis [12] and service failure events [13], [14] demonstrate the possibility of the accidental interference of MiFi (Mobile WiFi) on CBTC (Communication-Based Train Control) radio communication. Even worse, because almost all balises are localized in open air and the balise-BTM air-gap interfaces lack cryptographic protection, a train may receive malicious telegrams which could result in wrong safety-related response [15], [16]. That is to say, adversaries such as terrorists are able to maliciously manipulate air-gap interface to cause inaccurate stops or even fatal accidents.

Manuscript received February 24, 2016; revised May 15, 2016; accepted July 2, 2016. Date of publication August 5, 2016; date of current version March 27, 2017. This work was supported in part by the Guangdong Innovative and Entrepreneurial Research Team Program under Grant 2014ZT05D238. The associate editor coordinating the review of this paper and approving it for publication was M. Snyder. The Associate Editor for this paper was A. Amditis. *(Correspoding author: Zhe Tang.)*

Y. Wu is with the Institute for Infocomm Research, Singapore 138632 (e-mail: wuyd007@qq.com).

J. Weng is with Jinan University, Guangzhou 510632, China (e-mail: cryptjweng@gmail.com).

Z. Tang is with the School of Information Science and Engineering, Central South University, Changsha 410083, China (e-mail: tz@csu.edu.cn).

X. Li is with Sinocloud Wisdom Technology Co. Ltd., Beijing 100093, China (e-mail: li.xin@yunkouan.com).

R. H. Deng is with Singapore Management University, Singapore 188065 (e-mail: robertdeng@smu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2016.2590579

[1] As of 2012, more than 62 000 km of railway tracks and 7500 vehicles are either already operating or being equipped with ETCS in 38 countries around the world [3], and ETCS is quickly recognized by CTCS (Chinese Train Control System) [4].

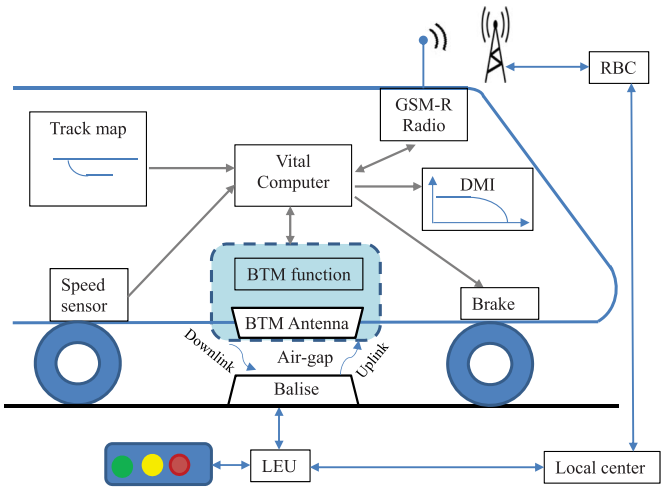


Fig. 1. ETCS system diagram. Radio block center (RBC) is used in the GSM-R communication.


Fig. 2. Balise is mounted between the tracks, and a Balise Transmission Module (BTM) is mounted on the train. They cooperate to fulfill the track–train telegram transmission [16].

The contributions of the paper are fourfold. First, we point out that the air-gap interface between balise and BTM is totally insecure as the telegram is sent in cleartext, without integrity protection and timestamping. While this "open-door" design makes it easy to realize the inter-operability for pan-European railways since it does not ask for complicated cryptographic key management, the design makes the air-gap interface the weakest security link in the rail communication system. Secondly, we present a jamming attack on the balises along a rail track to cause "balise missing" hazard [6]. This jamming attack is so powerful that it invalidates the defense mechanism of using a dedicated wireless spectrum band for rail transport system, as suggested in [17]. Thirdly, by exploiting the inaccuracy of on-board positioning mechanisms, we show how a balise displacement attack is able to convey erroneous position information to BTM even if telegrams were authenticated. Using ETCS example parameters [18], we show by simulations that all the proposed attacks are effective and cost-efficient in causing fatal train accidents. Finally, we propose countermeasures to mitigate the attacks.

The reminder of this paper is organized as follows. Section II introduces the preliminaries. Section III presents the vulnerabilities and the attacks in Balise-based Train Control Systems, and Section IV shows the results of our attack simulations. Section V presents countermeasures. Section VI draws conclusions.

## II. Preliminaries

With reference to [6], this section introduces ETCS model, balise transmission system, telegram and train speed control curve.

### A. ETCS Model

As shown in Fig. 1, an ETCS consists of a train control component and a train-ground communication component. The former captures the train's inputs, calculates the train brake mode curve according to the received ground information and train characteristics [19], provides DMI (Driver Machine Interface), and takes some actions directly. The latter[2] is widely used for exchanging information between train and control center. The two components are connected via internal interface between on-board VC (Vital Computer) and BTM.

A balise[3] is a wayside device placed between the rails of a railway, serving as a beacon giving the traffic information (e.g., location of balise, curve and gradient of rail, and speed restriction) to any train passing over it. There are two classes of balises: Fixed Balises and Controllable Balises. The former merely transmits its locally stored data to on-board BTM; while the latter is able to bi-directionally forward variable messages between wayside LEU (Lineside Electronic Unit) and BTM. LEU may further communicate with a wayside signaling device and/or a local center, and BTM enables bi-directional intermittent transmission between track and train VC. In order to distinguish travel directions, balises must be deployed in pairs, usually consisting of a fixed balise and a controllable balise.

When a train passes over a balise as shown in Fig. 2, its BTM *Antenna* telepowers and activates the balise to send stored messages (called as Uplink data). After obtaining the uplink data, the on-board BTM *Function* decodes the uplink data to geographical position, route data and temporary speed limit etc. (see Section II-B) and calculates the moving direction (see Section II-C). Although the received balise position is accurate and used as location marker, it cannot provide the real-time position information. To continuously localize the train, other input sources such as on-board speed sensors may be used and fused (see Section II-D). With the train position information, track map and rail data, VC continuously calculates the safe brake curve (see Section II-E), and real-time supervision limits of train speed (see Section II-F). VC may send train information to LEU via BTM-balise downlink, render them on DMI to the driver, or even take action automatically to prevent the top-level hazards (see Section II-G) from happening. Briefly, after obtaining the input, VC determines the train speed control curves so as to ensure the safety and comfort.

[2]The train-ground communication component may be GSM-R (GSM Communications-Railway) communication, train-track communication or both. As GSM-R communication system is not popular yet, we omit it unless otherwise stated in the following.

[3]Euroloop is an extension to balise so as to allow continuous data transmission up to 1000 m using a leaky coaxial cable.

### B. VC Input 1—Balise Telegram

Considering balise's crucial role in safety and train operation, ETCS SUBSET-036 [6] specifies balise telegrams in order to serve as a solid basis for the inter-operability with any ETCS compliant on-board equipment. Each telegram includes data structure, packet type, etc.

*1) Data Structure:* A balise telegram is either 341-bit "short telegram" or 1023-bit "long telegram." It consists of transformed payload, integrity check bits, and synchronization bits.

- Shaped data (913 bits or 231 bits): contains the payload information (830 or 210 bits). To avoid burst transmission errors, the payload is scrambled, substituted with code of different Hamming distance.
- Control bits (3 bits): is a constant binary string "$001_b$" at present.
- Scrambling bits (12 bit): is the initial state of the scrambler.
- Extra shaping bits (10 bit): is used to enforce the shaping constraints on the check bits independent of the scrambling.
- Checksum (85 bit): consists of 75 parity bits of the error correcting code and 10 bits for synchronization.

*2) Packet Type:* In order to ensure inter-operability for trains of different countries, ETCS defines the packet types according to the payload in the balise specifications [6]. The Uplink packet types which are related to our study are:

- Position and geographical information.
- Train target running information.
- Permanent speed restrictions.
- Temporary speed restrictions.
- Movement authority which defines the maximum speed that may be used for a given maximum distance and maximum time.
- Gradient of rail which contains pairs of rail section length and gradient (uphill/downhill flag and a number in percentage).
- Linking data for the relationship of neighbor balises which informs the train about the distance to the next balise or balise group and the required train reaction if the next balise (or balise group) is missing (e.g. train stop).
- Other information.

Every balise telegram must include a 14-bit balise group identity, a unique balise identity, and packet types such that the VC can check the source and interpret the telegram.

### C. VC Input 2—Travel Direction

As the train direction is critical to decide movement authority, ETCS proposes to determine the train's travel direction from the sequence of telegrams sent from at least two linked consecutive balises (e.g., the balises within a multi-balise Group) [6].

Every balise group has its own coordinate system. With reference to Fig. 3, balise $B_1$ is the origin (called position reference) of the coordinate system for the group. The nominal direction of the group is defined by increasing internal balise numbers as $B_1, B_2, \ldots$ etc.

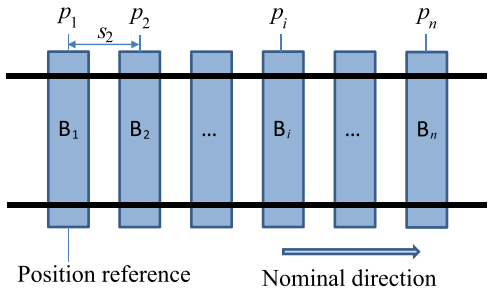


Fig. 3. Balise layout. Each group consists of at most eight balises. Each balise $B_i$ stores its exact position $p_i$ in the rail coordinate system.

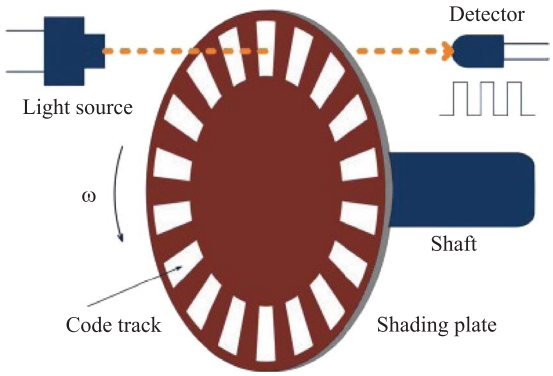


Fig. 4. Wheel angular speed sensor [22].

### D. VC Input 3—Real-Time Location

As a balise only provides its physical position rather than train's real-time position, reliable measurement of speed and/or location by dead reckoning becomes the base of a safe and efficient ATP (Automatic Train Protection) system. Specifically, to enable continuous positioning for re-calculating the safe train-to-train distance, a train obtains its real-time travel distance via sensors. The sensors typically include wheel angular speed sensors, Doppler radars, accelerometers, and gyroscopes. For instance, the ATP system named SCMT (Sistema di Controllo Marcia Treno) for Italian railways measures wheel angular speed to estimate train speed by counting impulses generated from a sensor per second and calculates distance between fixed balises [20], [21].

With regard to Fig. 4, a wheel angular speed sensor transforms the rotating velocity of a train wheel into electric pulse signals according to photoelectric transformation principle [22]. Denote the impulse counter by $\Lambda_t$ within a sampling interval $t$, the average wheel angular speed $\omega$ is evaluated as

$$\omega = \frac{2\pi}{N} \cdot \Lambda_t \cdot \frac{1}{t} \tag{1}$$

where $N$ is the number of impulses per wheel revolution. Thus the measured travel distance is

$$\tilde{s} = \omega r t = \frac{2\pi}{N} \cdot \Lambda_t \cdot r \tag{2}$$

where $r$ is the radius of the train wheel. Therefore, the on-board system is able to continuously measure the real-time travel distance. Nonetheless, the reliability of the on-board measurement is tightly related to operative conditions which are often unpredictable and unquantifiable due to wheel sliding/skidding, raining, snowing etc.

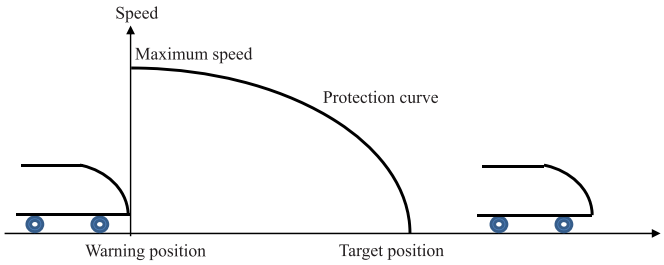


Fig. 5. Safe braking distance curve. Train speed must be 0 at the target position.

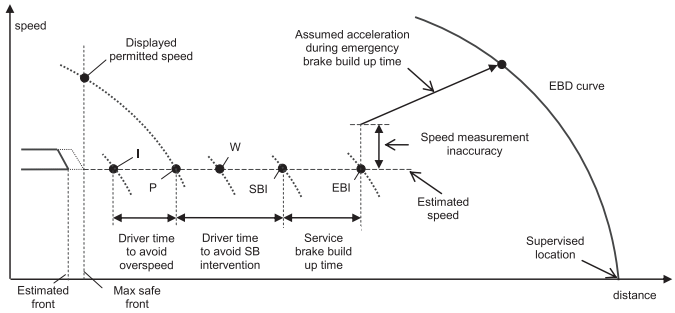


Fig. 6. Emergency braking distance (EBD) curve and supervision limits [18].

According to [19], if two consecutive linked balises (groups) announced by the linking field in the telegram are not detected and the end of the expectation window of the second balise (group) has been passed, the on-board ETCS device shall command the service brake. Based on the on-board distance measurement above, the detection method can be as follows. Denote the impulse counter for traveling between balises $B_i$ and $B_{i-1}$ as $\Lambda_{t_i}$, and the position of balise $B_i$ as $p_i$ which is included in the telegram and the train route map. For simplicity, the balise position $p_i$ (i.e., coordinate) is defined along the rail in this paper. For any two balises $B_i$ and $B_{i-1}$, their distance calculated with telegram payload is

$$s_i = p_i - p_{i-1} \tag{3}$$

and according to (2), the measured distance is given by

$$\tilde{s}_i = \frac{2\pi}{N} \cdot \Lambda_{t_i} \cdot r. \tag{4}$$

If $|\tilde{s}_i - s_i| > \epsilon_i$ for some predefined threshold $\epsilon_i$, the VC regards that balise $B_i$ is missing, and alerts the driver.

### *E. VC Output 1—Safe Braking Distance Curve*

Since every rail section has a permitted speed limit due to operational or environmental conditions, in case of violation of the permitted speed limit, the on-board VC must activate service or emergency brake [23]. To be compliant with the rail restriction, using the input such as brake, train and track characteristics as well as real-time measured speed as (1), VC calculates the safe braking distance curve as shown in Fig. 5. When a train is at the warning position, the braking distance is the difference between warning position and target position, and the protected curve shows the maximal admissible speed to enable the train to stop at the target position. For instance, the train braking distance for a 410 m long German ICE train at a speed 300 km/h is found as 4000 m [24]; and the emergency brake distance of China CRH2-300 is about 3634 m in a smooth and straight high speed railway when the brake initial speed is 300 km/h [25]. Similar braking distance curves can be found in the literature [26]–[32].

### *F. VC Output 2—Train Supervision Limit*

Although the safe braking distance curve is able to guide the travel safety, it does not ensure the travel comfort if the driver brakes the train frequently. Since DMI is very important in the train control process to drive comfortably by maintaining the speed of the train within the appropriate limits, ETCS specifies DMI of "Cab Signaling," especially for full supervision [18], with 5 supervision limits shown in Fig. 6:

- Indication (I)—leave the driver enough time to act on the service brake so that the train does not overpass the Permitted speed (P).
- Permitted speed (P)—leave the driver an additional time to act on the service brake so that the train will not overpass the point beyond which VC will trigger a brake command.
- Warning (W)—give an additional audible warning after the Permitted speed has been overpassed.
- Service Brake Intervention (SBI)—take into account the service brake building up time so that the EBI supervision limit is not reached after the command of the full service brake effort.
- Emergency Brake Intervention (EBI)—bypass the driver and command the intervention of the emergency brake.

When the train crosses any of these supervision limits, the driver shall be alerted through appropriate graphics, colors and sounds on DMI.

### *G. Balise-Related Hazards*

On account of the importance of position information, ETCS [6] emphasizes the following requirements on BTM:

R1) Predicate position references (see Fig. 3).
R2) Filter out erroneous telegrams. Section II-B introduces one of the filtering methods.
R3) Repeatedly detect the existence of a balise as long as the vehicle is in driving mode (running or stationary). Section II-D introduces one detection method.

Whenever a rail transport system is in operation, the above requirements R1)–R3) shall be ready for non-intentional interference. Otherwise, there are top-level ETCS hazards [6]:

H1) Erroneous report of the existence of a balise.
H2) Erroneous telegram interpretable as correct.
H3) Erroneous localization of a balise with reception of a valid telegram.
H4) Balise Missing.

## III. Security Vulnerabilities in Balise-Based Train Control Systems

In the ETCS speed control mechanism introduced in Sections II-E and F, accurate balise position information is crucial for the trains. If the balise position information are accidentally or maliciously wrong, disasters, such as derailment, collision and infrastructure damage, could happen [33].

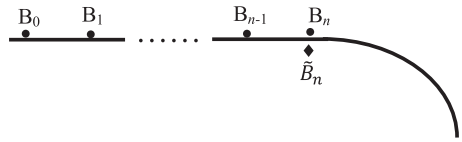


Fig. 7. Faking the attack. The faked balise $\tilde{B}_n$ sends the wrong rail information to the passing-over BTM. (Circle) Position of $B_i$ and (diamond) position of $\tilde{B}_i$ along a rail.

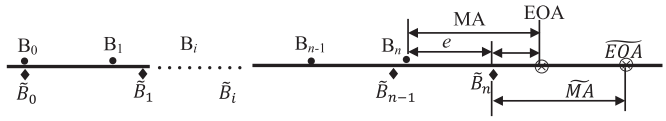


Fig. 8. Displacement attack on the movement authority. (Circle) Position of $B_i$ and (diamond) position of $\tilde{B}_i$ along a rail. $\otimes$ is End of Authority (EOA) or $\widetilde{\text{EOA}}$.

### A. Security Model

An adversary aims to cause top-level hazards H1)–H4) by invalidating the requirements R1)–R3) mentioned in Section II-G. To this end, he will attack the balise-based transport system assume that he is

1) Able to interfere the air-gap wireless communication. As the telegram is sent in open air via a wireless channel, it can be easily interfered by an attacker with a powerful wireless emitter.
2) Able to fake telegrams. According to the balise specification, telegrams are sent in cleartext and hence the attacker is able to fake a telegram according to the specification ETCS SUBSET-036 without being filtered out by the BTM.
3) Able to install fake balises around/near rails. A fake balise may be a real balise or merely a transponder.
4) Able to replay telegrams. As a balise will send the telegram once activated by a BTM, an adversary is able to know the telegram by impersonating as a BTM.
5) Able to know the train control mechanism and its parameters (Kerckhoffs's Principle [34] or the open design principle in information security).
6) Restricted to (virtually) displace one balise only a small distance which will not compromise the security of transport system. If the displacement is bigger than a predefined threshold, the displacement can be detected according to R1 in Section II-G and/or distance estimate in Section II-D.
7) Unable to destruct balises without being detected.
8) Unable to extract the internal secret data or states of balises.

Since ETCS telegrams are not integrity and timestamp protected, and on-board distance measurement mechanisms shall tolerate some errors due to rail conditions and weather dynamics, an adversary is able to exploit these vulnerabilities to start attacks with malicious wireless signals as follows.

### B. Faking Telegrams

In the balise communication system, there are no cryptographic primitives used to defeat malicious adversaries, but error correction method and mechanical protection against external interference only. Therefore, a naïve attack is to fake a balise to send arbitrary uplink telegrams. The on-board BTM cannot filter them out as the faked telegram can pass the verification process in Section II-B. For instance, if the faked balise $\tilde{B}_n$ in Fig. 7 sends a bogus telegram which enables a train to move along the bend rail at full speed, a derailment tragedy may be unavoidable. As this faking attack is easy to implement and cost-effective, the attacker will launch it at the first priority if possible, otherwise, the following attacks.

### C. Jamming Attack

One straightforward way for an adversary to generate "balise missing" hazard is to disable air-gap communication by covering the balise with a Faraday cage. However, this simple attack can be detected easily by railway workers who carry on surveillance on the tracks periodically.

A more advanced stealth method is to jam the telegrams when a train passes over a balise by transmitting signals to BTM at the same frequency band as the balise does [35]. As introduced in Section II-B, the telegram message is public, hence the adversary can start the selective and intelligent interfering so as to be energy-efficient and stealthy. When a train passes over a balise, the attacker jams a crafted signal to the BTM antenna. As each telegram has 75 parity bits to correct at most $\lceil 75/2 \rceil = 38$ random bit errors, if an adversary is able to randomly change more than 38 bits of the telegram, BTM will reject the whole telegram and miss the balise.

As an illustrative example, the communication time between BTM and balise is about 7 ms when train speed is 350 km/h [7]. Hence, if an adversary randomly interferes with the telegram channel for at most $38/341 \times 7 \approx 0.78$ ms, the BTM will reject the telegram and VC shows the top-level hazard H4 "balise missing" on DMI. As a result, the driver has to manually operate the train and the railway operator has to re-schedule all the trains affected.

Note that the above attack process is not only able to disrupt the original telegram transmission, but also able to transmit any bogus message to the BTM if the jamming signal energy is always larger than that of the genuine telegram. In this case, the jamming attack is regarded as a joint jamming-faking attack.

### D. Displacement Attack on Movement Authority

As fixed balises always send invariable telegrams, an adversary can easily replay the telegrams anywhere to mislead the passing trains and control centers. For example, if the balise $B_n$ is (virtually) moved to the position of $\tilde{B}_n$ in Fig. 8, its telegram can still pass the verification of BTM although the balise position is incorrect. Nonetheless, due to the distance restriction in Section II-D, the small balise displacement has little threat to the transport system. Hence, an attacker aims to displace a balise by a larger distance while without being detected. This can be achieved by accumulating several balise displacement as follows.

With reference to Fig. 8, assume that balises $B_0, B_1, \ldots, B_n$ are placed in a row. The attacker (virtually) displaces them to new positions, marked as $\tilde{B}_0, \tilde{B}_1, \ldots, \tilde{B}_n$. For ease of exposition, we assume that $B_0$ stays in its original position, i.e., $\tilde{B}_0$ is $B_0$. Thus the distance between two consecutive balises (group) are

$$s_i = p_{i+1} - p_i \tag{5}$$
$$\tilde{s}_i = \tilde{p}_{i+1} - \tilde{p}_i \tag{6}$$

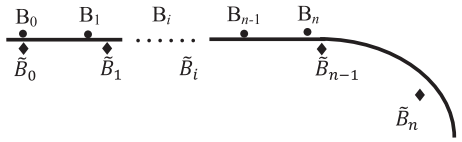


Fig. 9. Displacement attack on the chosen rail sections. (Circle) Position of $B_i$ and (diamond) position of $\tilde{B}_i$ along a rail.

where $s_i$ is the accurate distance calculated from the replayed telegrams of balises $B_{i-1}$ and $B_i$, and $\tilde{s}_i$ is the distance between balises $\tilde{B}_{i-1}$ and $\tilde{B}_i$ measured with a distance sensor. However, because BTM cannot distinguish a faked balise from a genuine balise by checking the format of their telegrams, it is misled to believe that $\tilde{s}_i$ is the measured distance between $B_{i-1}$ and $B_i$. In other words, from the viewpoint of BTM, $\tilde{s}_i$ is an acceptable estimate of $s_i$. Meanwhile, BTM cannot discover the displacement attack by checking the measured distance because the attacker ensures the error of measured distance is smaller than the detection threshold value $\epsilon_i$, i.e.,

$$\forall\, i, \quad \tilde{s}_i = s_i + \alpha\epsilon_i \leq s_i + \epsilon_i \tag{7}$$

where $\alpha \in (0, 1]$ is a scalar. In normal conditions, the on-board sensors are able to approximately measure the travel distance, especially several sensors are used together, hence $\alpha \approx 1$ is chosen in (7). By iteratively applying (5)$\sim$(6), we have the total displacement of balise $B_n$ as

$$\begin{aligned} e &= \tilde{p}_n - p_n = (p_{n-1} + s_n) - (\tilde{p}_{n-1} + \tilde{s}_n) \\ &= \sum_{i=1}^{n} s_i - \sum_{i=1}^{n} \tilde{s}_n \approx \sum_{i=1}^{n} \epsilon_i. \end{aligned} \tag{8}$$

According to (8), an attacker successfully displaces a balise arbitrarily far away without being found by BTM given that the number of displaced balises is sufficiently large.

With reference to Fig. 8, when a train passes over balise $\tilde{B}_n$, its VC (or control center) will calculate EOA (End of Authority) based on the replayed telegram of genuine balise $B_n$. As the distance between $\tilde{B}_n$ position (the true train position)[4] and EOA is MA $-e$ only, much smaller than the expected/allocated distance, the train will pass through EOA, thus train collision disaster may happen.

### *E. Displacement Attack on Chosen Rail Sections*

Based on the law of physics, a train must reduce its speed at a curved rail section due to centripetal force. Therefore, if an adversary chooses to fake the balise close to the curved rail section, the attack can be more effective than the displacement attack above. For instance, in Fig. 9, $B_{n-1}$ is a balise indicating the normal high speed, and $B_n$ is a balise indicating the speed restriction for the following curved rail section. As elaborated in Section III-D, BTM will miss balise $B_n$ according to the wrongly measured distance. As fake balise $\tilde{B}_{n-1}$ replays the telegram of balise $B_{n-1}$ such that VC allows the train to run at full speed between balises $\tilde{B}_{n-1}$ and $\tilde{B}_n$, hence the train may derail due to the same reason as the wreck of Amtrak 188 in USA [37].

[4]BTM shall read the balise data within $\pm 1$ m around balise center, with a confidence interval of 0.998 [6]. To improve the performance of balise-BTM connection, optimization technologies such as [36] are proposed.

TABLE I
COMPARISON OF THE DIFFERENT ATTACKS

| Attack w/ jamming | Telegram requirement | #Balises affected | Attack time | Top-level hazard |
|---|---|---|---|---|
| Jamming only | no | 1 | milliseconds | H4 |
| Faking (J) | unsecured | 1 | milliseconds | H2 |
| Displacement (J) | no | $\geq 2$ | minutes | H1,H3 |

### *F. Joint Attack*

In the above attacks, jamming attack may result in a minor "balise missing" threat on any genuine BTM-balise communication, while faking attack and displacement attack may cause significant threats but can be mitigated by a genuine BTM-balise communication. Thus an attacker may launch a joint attack. Specifically,

- In a joint jamming-faking [or Faking (J)] attack, when a train passes over a genuine balise, a faked balise creates a bogus telegram which has correct telegram format, balise identifier and checksum; then the faked telegram is sent to the train with higher electromagnetic power than the genuine one such that VC will accept the faked telegram rather than the genuine one.
- In a joint jamming-displacing [or Displacement (J)] attack, the attacker installs a faked balise $\tilde{B}_i$ on the attack positions $\tilde{p}_i$. When a train passes over a genuine balise $B_i$, a jamming signal is used to override the communication of balise-BTM communication by inducing errors. On the contrary, when a train passes over a faked balise $\tilde{B}_i$, the data stored in balise $B_i$ will be replayed by $\tilde{B}_i$. As VC cannot distinguish faked balises from genuine balises, the attacker realizes balise displacement successfully in a stealth way.

Table I summarizes the proposed joint attacks. As the Faking (J) attack has to change the telegram content, it is only applicable to unsecured telegrams (column 2). Unlike the other attacks, Displacement (J) attack needs to tamper more balises' telegrams so as to induce a sufficiently large distance error. Hence, it requires more bogus balises (column 3) and attack time (column 4) than any other attack. The last column lists the top-level hazards caused by the attacks. Jamming-only attack makes the train miss a balise such that the driver has to reduce the train speed or even stop the train, hence the railway's availability or quality of service is reduced; Faking (J) attack can fabricate any message to pass the verification such that an erroneous message is accepted by the train; and Displacement (J) attack misleads the BTM to report the erroneous position of balise.

## IV. SIMULATIONS

The most important task in the train control technology of balise-based ATP system is to establish the safety braking model according to the movement authority. However, the train control curve model technology is believed to be the key protected and proprietary technology due to commercial considerations [38] and hence is not available for academic analysis. Thus, the train system is modeled as in Section II based on

ETCS standards in the following simulations. As the faking attack simulation is trivial, we will omit it, and pay attention on the displacement attack only. In the simulations, we assume that the measured distance is the accurate travel distance for simplicity, but the distance calculated from balise telegrams is inaccurate due to the displacement attack.

### A. Displacement Attack on Trains Without Supervision Limits

When two neighbor trains move in the same direction on the same rail, supervision limits are made available to the train behind so as to ensure the safe separation distance and travel comfort. With reference to Section II-F, if the train behind is beyond P limit, the driver shall be alerted for initiating the service brake. Moreover, if the train is beyond EBI limit, the trains may collide with a high probability. In other words, if the distance error is more than the limits, but VC thinks the train is still in a safe region by mistake, there are potentially tragic consequences. Thus the attacker aims to cause a distance error which is beyond the supervision limits, without being detected by the VC.

As a compromise between on-board measurement accuracy and safety, ETCS SUBSET-041 specifies the accuracy of the distance measured by on-board sensors: for every measured distance $\tilde{d}$ the accuracy shall be better or equal to $\pm(5 + 5\%\tilde{d})$ in meters [39]. i.e., the VC will not report the "balise missing" hazard if the error

$$e' = \tilde{d} - d \leq 5 + 5\%\tilde{d} = 5 + 0.05(d + e') \tag{9}$$

where $\tilde{d}$ is the measured distance of two neighbor balises, and $d$ is obtained from their telegrams. Rewriting (9) as

$$e' \leq \frac{(5 + 0.05d)}{0.95} = \epsilon. \tag{10}$$

For simplicity, assume the distance $d$ between any two original balises to be fixed, and each balise is displaced with the same distance $e'$. Then according to (8), after $n$ faked balises are passed over, VC can accept the total travel distance error $e = ne' \leq n\epsilon = n(5 + 0.05d)/0.95$, i.e., the minimal number of displaced balises required for a successful displacement attack is

$$n = \left\lceil \frac{0.95e}{5 + 0.05d} \right\rceil. \tag{11}$$

As the number of displacement balises varies with the tolerable error $e$ which is related to the train characteristics, the following subsections illustrate the attack effect according to the train classes. Assume that $d = 3000$ m as that in [20], the detection threshold $\epsilon = 161.2$ m for ETCS trains according to (10).

*1) High-Speed Train:* Table II illustrates the attack effect on a high-speed train (300 km/h) whose control curve is shown in Fig. 10. Using the last row of Table II as an example, the attacker can lead the train into EBD status if the position error is above $e = 417 + 333 + 365 + 208 = 1323$ m according to Fig. 10. To incur such a distance error $e$, the attacker shall use at most $n = 9$ fake balises for an ETCS victim train. That is, the adversary can cause an ETCS train accident by repositioning at most 9 balises, which is moved $e/n = 147$ m each. Within the 340-second attack period, the train actually travels $\tilde{s} = n(d + e/n) = 28323$ m, rather than $s = nd = 27\,000$ m obtained from the telegrams. As the total distance error $e = \tilde{s} - s = 28\,323 - 27\,000 = 1323$ m, the train will pass over EBD limit. Meanwhile, as the distance error 147 m for the any track section between two balises is below the detection threshold $\epsilon = 161.2$, the train cannot identify the attack. Thus, the attack is launched successfully.

TABLE II
REQUIREMENTS FOR THE ATTACK EFFORT (300 km/h)

| Missing limit | $e$ (m) | ETCS | | | SCMT | | |
|---|---|---|---|---|---|---|---|
| | | $\tilde{s}$(m) | $n$ | time(s) | $\tilde{s}$(m) | $n$ | time(s) |
| P | 417 | 9,417 | 3 | 113 | 3,417 | 1 | 41.0 |
| EBI | 750 | 15,750 | 5 | 189 | 3,750 | 1 | 45.0 |
| EBD | 1,323 | 28,323 | 9 | 340 | 7,323 | 2 | 87.9 |

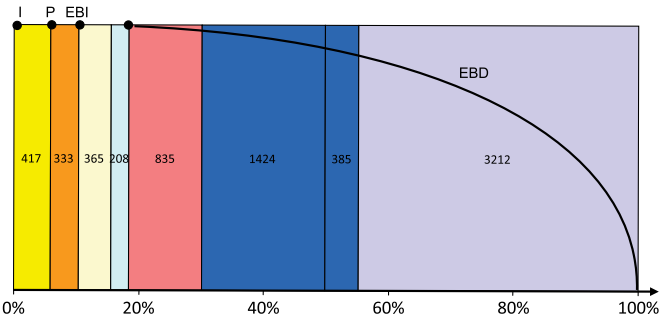


Fig. 10. Distance apportionment for trains at the highest speed of 300 km/h. Target distance is at 7179 m [18].

TABLE III
REQUIREMENTS FOR THE ATTACK EFFORT (160 km/h)

| Missing limit | $e$ (m) | ETCS | | | SCMT | | |
|---|---|---|---|---|---|---|---|
| | | $\tilde{s}$(m) | $n$ | time(s) | $\tilde{s}$(m) | $n$ | time(s) |
| P | 222 | 6,222 | 2 | 140 | 3,222 | 1 | 72.5 |
| EBI | 400 | 9,400 | 3 | 212 | 3,400 | 1 | 76.5 |
| EBD | 637 | 12,637 | 4 | 284 | 3,637 | 1 | 81.8 |

As a comparison, to cause the same accident on an SCMT train whose measurement error may be up to 20% of the travel distance [20] [40], an adversary is required to tamper with $n = \lceil 0.8e/(5 + 0.2d) \rceil = 2$ balises only, within 87.9 seconds. Hence, from Table II, we observe that it is easier to attack the SCMT train than ETCS counterpart in terms of attack efficiency and attack effort because SCMT allows the attacker to displace a balise further.

*2) Low-Speed Train:* Table III lists the missing limits for a low-speed train (160 km/h) whose control curve is shown in Fig. 11. Tables II and III show that it is easier to attack a low-speed train than a high-speed train. This observation seems to be in contradiction with our intuition: the slower, the safer. Indeed, a low-speed train usually has worse brake characteristics and hence its target distance is shorter. As a result, the required displacement distance is smaller such that an adversary is able to use a small amount of fake balises to start the attack.

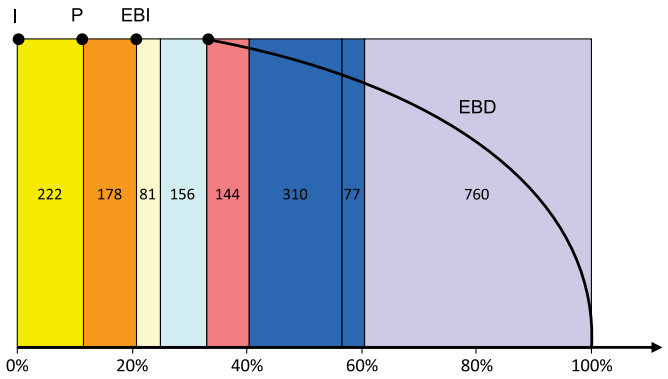


Fig. 11. Distance apportionment for trains at the highest speed of 160 km/h. Target distance is at 1929 m [18].

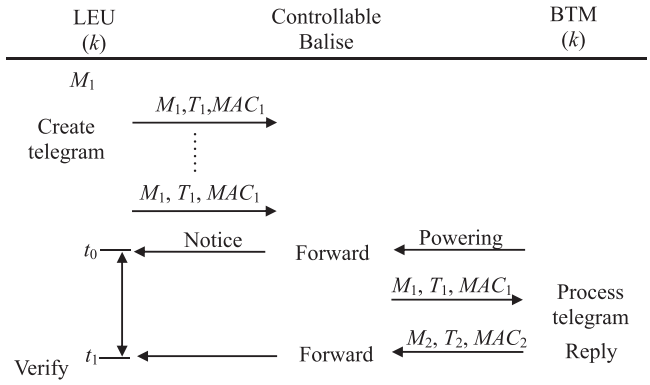


Fig. 12. Antireplay attack protocol.

### B. Displacement Attack on Trains Without Supervision Limits

If the control mechanism of a train does not have supervision limits, but only using the braking distance curve elaborated in Section II-E, the attack becomes easier. For instance, given that the German ICE train is at the speed 300 km/h, the emergency braking distance is no more than 4000 m [24], which is much smaller than the supervised distance 7179 m in Fig. 10. Thus, the number of faked balises required for a successful attack is smaller according to (11).

## V. Countermeasures

As a railway system always spreads over a very large area and even through different regions or countries, it is costly to upgrade the transport infrastructure to defense against malicious attackers. Preferably, the defenses are applicable to the existing infrastructure without much investment on hardware, as the following three methods do.

### A. Detecting Jamming Attack

In order to exchange messages between trains and operation centers, wireless communication is the most important means at present. Clearly an attacker is always able to interrupt the wireless channel by starting jamming attack. In other words, the "balise missing" hazard cannot be avoided theoretically if jamming attack is launched. Nonetheless, the jamming signal can be detected and alerted by the BTM such that the effects of the joint attacks shown in the Table I can be significantly weakened, and then the hazards are greatly alleviated.

Denote by $u(t) = u_b(t) + u_a(t)$ the signal received by BTM, where $u_b(t)$ is the component sent from the balise and $u_a(t)$ is the counterpart sent from the attacker. According to [35], if the energy $\|u_a(t)\|$ is sufficiently greater than the energy $\|u_b(t)\|$, the telegram is erroneous. That is to say, if there is a successful jamming attack, the received energy

$$\|u(t)\| = \|u_a(t) + u_b(t) + n(t)\| \geq 2\,\|u_b(t)\| + \|n(t)\|$$

otherwise

$$\|u(t)\| = \|u_b(t) + n(t)\| \approx \|u_b(t)\| + \|n(t)\|$$

where $\|u_b(t)\|$ is approximately constant or known to BTM in advance. Therefore, if the received electromagnetic power is larger than a predefined threshold, the BTM will report the existence of jamming attack, and alarm the driver and/or control center. Unfortunately, this countermeasure does not work if the attacker tampers/covers the target balises in order to fake or replay telegrams. In this case, advanced countermeasures such as the ones given below, are needed.

### B. Mitigating Faking Attack

The faking attack presented in Section III-B exploits the vulnerability that the telegram is in plaintext. Hence, if a telegram is protected with message authentication code (MAC) or digital signature, this attack can be defeated. Luckily, it is easy to append the authentication data to the "other information" field of the telegram such that the extended telegram is compatible with non-upgraded trains.

For a controllable balise, authentication data can be created together with the message whenever the message is changed by LEU/center. But for a fixed balise, the telegrams cannot be updated online. Nonetheless, ETCS specifies that "*there is an optional interface defined for programming the Fixed Telegram (for Fixed Balises) . . . into the Balise using wire aided programming when applicable*" [6]. Thus, it is also possible to insert authentication data to fixed balises offline so as to defeat the faking attack.

The cryptographic primitives are effective tools in defeating telegram faking, but they fail to deter replay attacks such as Displacement attack. To defeat these attacks, a challenge-response protection mechanism shall be employed.

### C. Defeating Replay Attack

Although the balise specification [6] defines both uplink and downlink channels between balise and BTM, the downlink is not used in most of the deployed systems in practice. We propose to use the downlink channel for controllable balise so as to defeat the replay attacks, including Displacement attack, presented in Section III. With regard to Fig. 12, the anti-replay attack protocol works as follows.

1) Assume a train shares a crypto-key $k$ with each LEU along the route, and synchronizes with all the LEUs before the train starts to be on duty.

2) The LEU generates a telegram which includes message $M_1$, current timestamp $T_1$, and the message authentication code $\text{MAC}_1 = \mathcal{H}(M_1, T_1, k)$ where $\mathcal{H}(\cdot)$ is a one-way function. Both $T_1$ and $\text{MAC}_1$ are inserted into the "other information" field of the telegram for compatibility with non-upgraded trains. The telegram is transmitted to the controllable balise.
3) LEU will repeat step 2) periodically.[5]
4) When a train passes over the balise, BTM telepowers and activates the balise. At the beginning of its start-up, the balise sends an activation notice to the LEU [6], and the LEU notes down the activation time $t_0$ and starts a clock.
5) After the balise starts up, the uplink telegram is transferred to the BTM via air-gap interface. After reading the telegram, BTM carries on the normal verification in Section II-G. If positive, BTM will parse the "other information" to extract the $\text{MAC}_1$. If the telegram is authentic and timestamp $T_1$ is within a reasonable interval, the BTM creates a message $M_2$ which links to the received uplink telegram, and replies to the balise a downlink telegram which includes reply message $M_2$, timestamp $T_2$ and authentication code $\text{MAC}_2 = \mathcal{H}(M_2, T_2, k)$.
6) The balise forwards the downlink message to the LEU.
7) Upon receiving the downlink message, the LEU stops the clock and notes down the time $t_1$. The LEU verifies the telegram with $\text{MAC}_2$, and checks whether time lapse $T = t_1 - t_0$ is less than a predefined threshold. If any of them is negative, the LEU reports the existence of attacks.

In this countermeasure, because the train passage time $T$ is restricted to be smaller than a threshold value, the replay attack fails as explained below. To start the replay/displacement attack, a determined attacker may take the following strategy:

1) Place a fake balise $\tilde{B}_n$ which has distance $e$ away from $B_n$ in advance.
2) Once $B_n$ is passed over by a train and automatically sends activation signal to the LEU, the attacker will jam the uplink such that the train cannot receive the correct telegram.
3) Once $\tilde{B}_n$ is passed over and receives the reply message via the downlink, the message is forwarded to the LEU via $B_n$.

In this process, the LEU knows the activation time $t_0$ in step 2) and the reply time $\tilde{t}_1$ in step 3). Thus, the LEU calculates the lapse time as $\tilde{T} = \tilde{t}_1 - t_0 = (t_1 + (e/v)) - t_0 = T + (e/v)$, where $t_1$ is the reply time if there is no attack. Given that the train speed $v = 300$ km/h (i.e., 83.3 m/s) and the displacement distance $e = 100$ m, the lapse difference $\tilde{T} - T = 100/83.3 = 1.2$ s. As the lapse difference is sufficiently large, the LEU is able to detect the displacement attack. Correspondingly, the train can detect the displacement attack by calculating the time difference $T_2 - T_1$ if the period which the LEU updates the telegram is short (e.g., 100 ms).

[5]According to specification [6], upon receiving the activation signal, LEU shall block telegram switching for a minimum time of 10 ms. The maximum blocking time is dependent on system requirements.

In addition, when the above protocol is deployed, the faking (J) attack fails if the attacker does not compromise the cryptographic key.

## VI. Conclusion

Balises play an important role in the positioning mechanism of modern rail transport systems. If balises are positioned incorrectly, the movement authority of a train will be wrong such that serious accidents may happen.

Although the ETCS specifications are designed to correct accidental position errors, they totally ignore malicious tampering of the air-gap communication channel. This paper exploits the potential security flaws in the channel, including jamming, faking telegram, re-positioning of balise and telegram replaying. It also proposes countermeasures to improve security of ETCS. In our countermeasures, the downlink channel is used for delivering train messages to the ground devices so as to detect the attacks. Furthermore, if a continuous train-to-track channel is available, the real-time control signal can be sent to the train so as to fully defeat the attacks.

## References


[1] F. Yan and Y. Man, *A New Record of 295 Million Train Trips in Spring 2015*, (in Chinese), Mar. 16, 2015. [Online]. Available: http://news.china.com.cn/zhuanti/2015cy/2015-03/16/content_35068970.htm

[2] W. Zhou and L.-M. Jia, *The Theory and Method of Design and Optimization for Railway Intelligent Transportation Systems (RITS)*. Sharjah, UAE: Bentham Sci., Jan. 1, 2011.

[3] European Rail Traffic Management System (ERTMS). [Online]. Available: http://www.railway-technology.com/projects/european-rail-traffic-management-system-ertms/

[4] K. Li, X. Yao, D. Chen, L. Yuan, and D. Zhou, "HAZOP study on the CTCS-3 onboard system," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 1, pp. 162–171, Feb. 2015.

[5] S. Dhahbi and T. Abbas, "Study of the high-speed trains positioning system: European signaling system ERTMS/ETCS," in *Proc. IEEE Int. Conf. Logist.*, 2011, pp. 468–473.

[6] *ERTMS/ETCS Class 1, FFFIS for Eurobalise, Ref. SUBSET-036, ver 2.4.1*, Sep. 27, 2007. [Online]. Available: http://www.era.europa.eu/Core-Activities/ERTMS/Pages/Set-of-specifications-1.aspx

[7] L.-H. Zhao and Y. Jiang, "Modeling and optimization research for dynamic transmission process of balise tele-powering signal in high-speed railways," *Progress Electromagn. Res.*, vol. 140, pp. 563–588, 2013.

[8] M. Sandidzadeh and A. Khodadadi, "Optimization of balise placement in a railway track using a vehicle, an odometer and genetic algorithm," *J. Sci. Ind. Res.*, vol. 70, no. 3, pp. 210–214, 2011.

[9] J.-F. Sevillano, J. Mendizabal, and I. Sancho, "Reliability analysis of an ERTMS on-board balise transmission equipment," *Rel., Risk Safety, Theory Appl.*, vol. 1, no. 3, pp. 2317–2324, 2010.

[10] R. Sharma and R.-M. Lourde, "Crosstalk reduction in balise and infill loops in automatic train control," in *Proc. IEEE Int. Conf. Intell. Eng. Syst.*, 2007, pp. 39–44.

[11] M. Lauer and D. Stein, "A train localization algorithm for train protection systems of the future," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 970–979, Apr. 2015.

[12] C. Song, B. Han, H. Yu, and X. Zhang, "Study on coexistence and anti-interference solution for subway CBTC system and MiFi devices," in *Proc. IEEE IC-BNMT*, 2013, pp. 174–180.

[13] Y. Huang and Y. Shi, "Shenzhen Metro disruption leads to call to ban Wi-Fi devices on subways," *Chin. Daily*, Nov. 6, 2012. [Online]. Available: http://usa.chinadaily.com.cn/epaper/2012-11/06/content_15880678.htm

[14] H. He, "Passenger Wi-Fi freezes third Shenzhen Metro train in a week," *South Chin. Morning Post*, Nov. 9, 2012. [Online]. Available: http://www.scmp.com/news/china/article/1078165/passenger-wi-fi-freezes-third-shenzhen-metro-train-week

[15] D. Chen, R. Chen, Y. Li, and T. Tang, "Online learning algorithms for train automatic stop control using precise location data of balises," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 3, pp. 1526–1535, Sep. 2013.

[16] T. Kurz, R. Hornstein, H. Schweinzer, M. Balik, and M. Mayer, "Time synchronization in the eurobalise subsystem," in *Proc. IEEE*

*Symp. Precision Clock Synchronization Meas., Control Commun.*, 2007, pp. 70–77.
[17] M. Fitzmaurice, "Wayside communications—CBTC data communications subsystems," *IEEE Veh. Tech. Mag.*, vol. 8, no. 3, pp. 73–80, Sep. 2013.
[18] "Introduction to ETCS braking curves," Eur. Railway Agency, Valenciennes, France, Eur. Railway Agency Tech. Doc., Ver. 1.2, 2012.
[19] "ERTMS/ETCS—Baseline 3, system requirements specification," Eur. Rail Traffic Manage. Syst. (ERTMS), Valenciennes, France, Chapter 3, Principles, Subset-026-3, Issue 3.0.0.23, Dec. 2008.
[20] M. Malvezzi *et al.*, "Train position and speed estimation by integration of odometers and IMUs," in *Proc. World Congr. Railway Res.*, 2011, pp. 1–11.
[21] B. Allotta, V. Colla, and M. Malvezzi, "Train position and speed estimation using wheel velocity measurements," *Inst. Mech. Eng. F, J. Rail Rapid Transit*, vol. 216, no. 3, pp. 207–225, 2002.
[22] Z. Xu, W. Wang, and Y. Sun, "Performance degradation monitoring for onboard speed sensors of trains," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1287–1297, Sep. 2012.
[23] D. Barney, D. Haley, and G. Nikandros, "Calculating train braking distance," in *Proc. 6th Australian Workshop Safety Critical Syst. Softw.*, 2001, vol. 3, pp. 23–29.
[24] A. Zimmermann and G. Hommel, "A train control system case study in model-based real time system design," in *Proc. IEEE Int. Symp. Parallel Distrib. Process.*, 2003, pp. 1–8.
[25] H. Yang, J. Yan, and K. Zhang, "Braking process modeling and simulation of CRH2 electric multiple unit," in *Proc. Int. Conf. Digital Manuf. Autom.*, 2012, pp. 264–267.
[26] S. Wei, J.-J. Wang, H.-S. Wang, J. Wang, and S.-H. Li, "The braking mode simulation and analysis for high-speed railway," in *Proc. IEEE Int. Symp. Microw., Antenna, Propag., EMC Technol. Wireless Commun.*, 2011, pp. 683–686.
[27] P. D. Booth, "Intermittent and continuous automatic train protection," in *Proc. IEEE RSCS*, 2010, pp. 86–102.
[28] IEEE Vehicular Technology Society, IEEE Guide for the Calculation of Braking Distance for Rail Transit Vehicles, 2009.
[29] H. A. Ahmad, "Dynamic braking control for accurate train braking distance estimation under different operating conditions," Mech. Eng., Virginia Polytech. Instit. State Univ., Blacksburg, VA, USA, 2013.
[30] P. Presciani, M. Malvezzi, G. Luigi Bonacci, and M. Balli, "Development of a braking model for speed supervision systems," in *Proc. World Congr. Railways Res.*, 2001, pp. 1–18.
[31] M. Palumbo, *The ERTMS/ETCS Signalling System—An Overview on the Standard European Interoperable Signalling and Train Control System*, Aug. 27, 2014.
[32] IEEE Std. 1698-2009, *IEEE Guide for the Calculation of Braking Distances for Rail Transit Vehicles*, C1-31, 2009.
[33] D. Hersmam, C. Hart, R. Sumwalt, E. Weener, and M. Rosekind, "Railroad accident report—Collision of two Washington metropolitan area transit authority metrorail trains near Fort Totten station, Washington, D.C., June 22, 2009," Accid. Investigation, USA Nat. Transp. Safety Board, Washington, DC, USA, Rep. NTSB/RAR-10/02-PB2010-916302, Jul. 2010.
[34] D. Kahn, *The Codebreakers: The Story of Secret Writing*, 2nd ed. New York, NY, USA: Scribners, 1996, p. 235.
[35] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming in wireless networks: The case of several jammers," in *Proc. Int. Conf. Game Theory Netw.*, 2009, pp. 585–592.
[36] S. Gong, Z. Liu, L. Luo, G. Zhou, and S. Wang, "The optimization study of the on-board antenna of BTM based on electromagnetic model," in *Proc. IEEE Conf. Intell. Rail Transp.*, 2013, pp. 37–41.
[37] M. Shaer, "The Wreck of Amtrak 188: What caused the worst American rail disaster in decades?" The New York Times, New York, NY, USA, Jan. 31, 2016. [Online]. Available: http://www.nytimes.com/2016/01/31/magazine/the-wreck-of-amtrak-188.html?_r=0
[38] J.-J. Wang, H.-S. Wang, B.-G. Cai, S. N. Wei, J. Wang, and H. Zhang, "European train control system speed-distance mode curve analysis and simulation," in *Proc. Int. Symp. Microw., Antenna, Propag., EMC Technol. Wireless Commun.*, 2011, pp. 679–682.
[39] "Performance Requirements for Interoperability," Eur. Rail Traffic Manage. Syst. (ERTMS)/Eur. Train Control Syst. (ETCS), Brussels, Belgium, SUBSET-041, 3.1.0, Mar. 01, 2012.
[40] B. Allottaa *et al.*, "Design and test of an innovative localization algorithm for railway vehicles based on odometry and INS," in *Proc. World Congr. Railway Res.*, 2013. [Online]. Available: https://www.researchgate.net/publication/268615163_Design_and_Test_of_an_Innovative_Localization_Algorithm_for_Railway_Vehicles_based_on_Odometry_and_INS

**Yongdong Wu** received the Ph.D. degree from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 1997.

He is currently with the Institute for Infocomm Research, Singapore. He has published more than 100 papers. He is the holder of seven patents. His research results and proposals were incorporated in the ISO/IEC JPEG 2000 security standard 15444-8 in 2007. His research interests include multimedia security, cyber–physical system security.

Dr. Wu was the recipient of the 2012 International Federation of Information Processing Conference on Communications and Multimedia Security Best Paper Award.

**Jian Weng** received the Ph.D. degree from Shanghai Jiaotong University, Shanghai, China, in 2008.

He is currently a Professor and Dean with the School of Information Technology, Jinan University, Guangzhou, China. He has published more than 60 papers in cryptography conferences and journals.

Dr. Weng was the recipient of a number of awards including the 2014 Chinese Association for Cryptographic Research Cryptographic Innovation Award, the 2011 Symposium on Cryptography and Information Security Best Paper Award, and the 8th International Conference on Provable Security Best Student Award in 2014.

**Zhe Tang** received the Ph.D. degree from Tsinghua University, Beijing, China, in 2006.

He is an Associate Professor with the School of Information Science and Engineering, Central South University, Changsha, China. He is the author or coauthor of more than 30 technical papers. His research interests include computer vision, intelligent control, robotics, and industrial control.

Dr. Tang was the recipient of the Second Prize of the Hunan Provincial People's Government, Hunan Science and Technology Progress Award.

**Xin Li** received the B.Eng. degree from Xi'an Jiaotong University, Xi'an, China, in 1992.

He is the Founder and CEO of Sinocloud Wisdom Technology Co. Ltd, Beijing, China. His research interests include computer image processing, pattern recognition, public safety and security, and cloud computing.

**Robert H. Deng** (F'16) received the Ph.D. degree from Illinois Institute of Technology, Chicago, IL, USA, in 1985.

Since 2004, he has been a Professor with the Singapore Management University (SMU), Singapore. His research interests include data security and privacy, multimedia security, and network and system security.

Dr. Deng is the Cochair of the Steering Committee of ACM Asia Symposium on Information, Computer and Communications Security. He was the recipient of the University Outstanding Researcher Award in 1999, the Lee Kuan Yew Fellow for Research Excellence from SMU in 2006, the Distinguished Paper Award from the Annual Network' Distributed System Security Symposium 2012, and the Conference on Communications and Multimedia Security Best Paper Award in 2012.