6-2018

Position manipulation attacks to balise-based train automatic stop control

Yongdong WU
Institute for Infocomm Research

Zhuo WEI
Huawei International Pte Ltd

Jian WENG
Jinan University - China

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

DOI: https://doi.org/10.1109/TVT.2018.2802444

Published in IEEE Transactions on Vehicular Technology,
Vol 67, Issue 6, June 2018, Pages 5287–5301
DOI 10.1109/TVT.2018.2802444

Position Manipulation Attacks to Balise-Based Train Automatic Stop Control

Yongdong Wu, Zhuo Wei, Jian Weng, and Robert H. Deng, *Fellow, IEEE*

***Abstract*—Balise is a popular wayside device to provide accurate location information for subway station parking by sending telegrams to passing trains. By craftily disturbing wireless signals of balise telegrams, this paper proposes three attacks that may make passengers fall and even cause injury. Concretely, the first attack is to jam telegrams such that balises cannot be detected by a passing train; the second attack changes the location of transmitting telegrams by jamming and replaying; and the third attack is to change the total time of transmitting telegrams. All the attacks exploit the train localization mechanism such that a passing train localizes its position inaccurately and then takes improper control actions. Furthermore, since these attacks are independent, they can be launched at the same time to achieve advanced attacks. As the attacks do not require to tamper with the balises, they can be launched easily. Our simulations demonstrate the effectiveness of the proposed attacks. To defeat these attacks, the received telegrams need be verified by a train based on fidelity of telegram data.**

***Index Terms*—Cyber-physical system security, train-ground communication security, train automatic stop control (TASC), balise.**

I. Introduction

SINCE 1863, subway system has been a major public transport mechanism to transport a large number of passengers at a high frequency over short distances. For examples, in 2016, the subway system has a daily ridership of over 3 million passengers in Singapore [1]. Due to its high speed, punctuality and safety merits, subway has been developed rapidly, especially in the developing countries to meet the requirement of rapid urbanization.

As train parking on stations is a mandatory train operation and required to be highly secure and accurate, automatic stop control techniques are essential in any subway system. If a train stops suddenly, passengers may fall, get hurt or even die [2]. Conversely, if the train stops very slowly for the sake of safety, the subway system does not operate efficiently and wastes the time of passengers. Meanwhile, as passengers choose train cars to minimize walking distance to exits at destination stations [3], [4], inaccurate parking positions may cause inconvenience to passengers, especially on platforms installed with Platform Screen Doors (PSD) [5], [6]. Hence Train Automatic Stop Control (TASC) [7] is an indispensable control function in any automatic subway transport system.

In reality, it is not trivial to meet the parking requirements. During the process of braking, stopping accuracy of an urban rail vehicle is affected by at least fifteen uncertainty factors [8] including different braking positions and speeds, line conditions, brake shoe friction coefficients, braking system time delay, braking control law, basic resistance changes, and random noises. To handle these uncertain conditions for precise parking, braking model, remaining distance measurement device and control law need to be properly designed and employed in TASC.

A braking model reflects the principle and the dynamic characteristics of the braking system including brake shoe friction coefficient, braking delay, time-varying resistance and unmeasured actual traction [9]. In the braking model for control design and analysis, a train is described as either a single-point mass rigid object [10] or a multiple-point mass elastics object [11]. As the multiple-point mass train model takes into account the reaction forces among cars, it is more practical and accurate. However, its complexity is much higher in order to reflect the impact of the linear/nonlinear parametric uncertainties. For instance, a seven-car train is described by a total of 84 differential equations [12], [13]. Therefore, a single-point mass rigid object is popularly used for TASC design in the academic community.

Remaining distance to the target stop position is the major input to determine the deceleration in TASC (e.g., [14]). It is estimated by the moving distance from a reference point. The moving distance is measured by an on-board positioning device such as radar detector, photoelectric speed sensors and axle generators, which are key components of train control systems [15]. Although the on-board device offers continuous distance

Manuscript received February 22, 2016; revised September 27, 2016 and May 29, 2017; accepted January 16, 2018. Date of publication February 5, 2018; date of current version June 18, 2018. This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme under Award NRF2014NCR-NCR001-31 and administered by the National Cybersecurity R&D Directorate, in part by Guangdong Innovative and Entrepreneurial Research Team under Program 2014ZT05D238, in part by the National Natural Science Foundation of China under Grants 61402199, U1636209, 61472165, 61373158, U1636101, and U1736211, in part by Guangdong Provincial Engineering Technology Research Center on Network Security Detection and Defence under Grant 2014B090904067, and in part by Guangdong Provincial Special Funds for Applied Technology Research and Development and Transformation of Important Scientific and Technological Achieve under Grant 2016B010124009. The review of this paper was coordinated by Prof. J. Sun. *(Corresponding author: Jian Weng.)*

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

Z. Wei is with the Shield Laboratory, Central Research Institute, Huawei International Pte, Ltd., Singapore 486066 (e-mail: phdzwei@gmail.com).

J. Weng is with the Department of Computer Science, Jinan University, Guangdong 510632, China (e-mail: cryptjweng@gmail.com).

R. H. Deng is with the School of Information Systems, Singapore Management University, Singapore 178902 (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/TVT.2018.2802444

measurement, its measurement error may increase with the travel distance. To manage the total measurement error, European Train Control System (ETCS) SUBSET-041 specifies the accuracy of on-board distance measurement: "*for every measured distance s the accuracy shall be better or equal to* $\pm(5 + 5\%s)$" in meters [16]. To correct the error, reference points are provided along the rail by the wayside devices such as balises [17]–[20], wireless access points [21] and leaky coaxial cables [22]–[24]. Although a wayside device is able to transfer its accurate location information to a passing train via a wireless channel [25], it is not used to provide continuous location information by densely installing wayside devices because it is expensive. In all, although the accurate reference positioning devices are of great value for TASC [26], train control systems using them still fail to get correct continuous remaining distance for automatic, accurate and comfortable parking. As mixtures of on-board and wayside devices, range sensors [27] exploit the radar principle to obtain the accurate position continuously, while dedicated stopping measurement devices precisely detect stopping errors based on platform information [28]. However, these mixture devices need to update the existing infrastructure.

With the braking model and remaining distance, an on-board train controller will determine the train braking force from time to time. A straightforward Proportional-Integral-Derivative (PID) controller is widely used in industrial applications, but it performs well only in invariant control systems, and hence is not suitable for a complex system such as train braking system. In order to improve the performance of the traditional PID controller, Model Predictive Control (MPC) technology is incorporated with the train models running on Beijing Yizhuang subway line [29], and a PID variant called as PIQ (Proportional Integral Quadratic) is proposed to overcome the adverse effect of actuator delays in the braking system [30]. Besides PID-like controllers, there are other controllers for TASC such as machine learning technique for TASC [31], on-line approximation based robust adaptive controller [32], fuzzy inference [33], terminal iterative learning controller [34], and neuro-adaptive fault-tolerant controller [35].

The performance of a TASC controller is tightly related to the accuracy of the remaining distance. An inaccurate remaining distance will significantly degrade the parking accuracy and comfortability. To tolerate the distance errors, the existing TASC controllers employ the knowledge of train operation environment and historic data to reduce the uncertainties. However, all of them only concern the accidental distance errors, but ignore technical and malicious attacks, such as telegram jamming and tampering with the location messages in telegrams. In comparison with non-technical attacks such as the suicide bomber attack in Moscow subway [36], technical attacks are stealthy, which protect the attackers from being traced, arrested and punished by governments and international societies.

This paper presents three stealth attacks which aim to create erroneous remaining distance such that the train can not park properly. Every attack exploits the security vulnerabilities of the wireless channel between on-board device and wayside device. Specifically, the remaining distance is maliciously manipulated by jamming balise-train wireless channel, replaying balise telegrams, and/or change the total time of the telegram transmission. As a result, the on-board controller generates an improper deceleration profile such that passengers can not align on platforms properly. Our simulations show that the attacks can be easily and effectively launched with only very short-time interference signals. To defeat the attacks, four countermeasures are presented to ensure the soundness of the received telegrams.

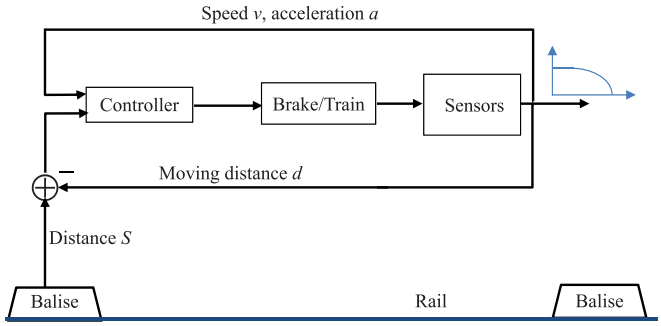

Fig. 1. TASC model based on balise information.

The reminder of this paper is organized as follows. Section II introduces the preliminaries for subway parking systems. Section III presents a train automatic stop controller. Section IV presents the attacks for train parking. Section V analyzes the attack feasibility, parameter sensibility, and their countermeasures. Section VI shows the results of attack simulations using a real subway line configuration as an example. Section VII draws conclusions.

II. Preliminaries

This section introduces the TASC model and its components including wayside positioning device, and balise-based train positioning mechanism.

A. TASC Model

As shown in Fig. 1, a TASC model consists of sensor, balise, and controller. An on-board sensor, such as wheel angular speed sensor, Doppler radar, accelerometer, and gyroscope, measures the train moving distance d, speed v and acceleration a in a real-time manner; and a balise is a wayside device which provides the passing train an accurate location as a distance maker [37] for correcting possible sensor measurement errors, and setting the target distance to the destination station. As the measurement error from an on-board sensor accumulates over time, several balises near the destination station are usually installed to reduce the total measured moving distance error and/or the remaining distance error. With the input from sensors and balises, the controller continuously decides the remaining distance to the destination station, and calculates the parking acceleration/speed profile such that the actuator can brake the train for comfort travel experience and precise parking location.

Usually, a balise-based TASC works as follows. When the train passes over the first balise that shows the start point of the fixed positional stop control, the train controller begins to run the parking control law to calculate the deceleration profile for desired stop smoothness and accuracy, and then apply the

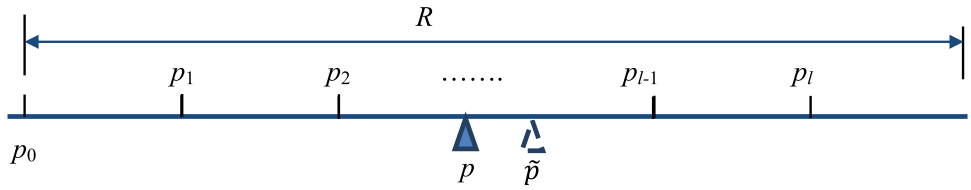

Fig. 2. The same telegram received at different positions $p_i, i = 1, 2, \ldots, l$. At position p_0, the balise is activated to send the telegram. Note that all the p_i are unknown to the train. p is the actual balise position which can be extracted from the telegram and $\tilde{p}$ is the estimated train position at the estimated time $\tilde{t}$.

brake to stop at the desired location of the target station [14], [33], [38]. As long as a new balise is passed over, the moving distance d will be reset to 0 to prevent the error accumulation, and then the deceleration profile will be updated with the new balise information.

B. Wayside Positioning Device

A balise is a wayside device placed between the rails of a railway, serving as a beacon giving traffic information (e.g., location of the balise, curve and gradient of the rail, and speed restriction) to any train passing over it. Balise Transmission Module (BTM) is an on-board module for intermittent transmission between balise and train controller. Considering balise's crucial role in safety and train operation, ETCS SUBSET-036 has detailed specifications [17] on balise telegram in terms of structure, type, and physical format in order to serve as a solid basis for the interoperability with any ETCS compliant on-board equipment.

The balise telegram is either 341-bit "short telegram" or 1023-bit "long telegram" including 75 parity bits for parity-checking. It is transmitted to the train in the form of binary FSK (Frequency-Shift Keying) with a 4.23 MHz center frequency. A '0'-bit corresponds to approximately 7 periods of 3.951 MHz, while a '1'-bit corresponds to approximately 8 periods of 4.516 MHz. Denote the waveform signal received by a BTM as $u(t)$, the BTM calculates a bit

$$\tilde{\rho} = \begin{cases} 0 & u(t) * f_0(t) > u(t) * f_1(t) \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

where '$*$' is the detector, and $f_0(t)$ (or $f_1(t)$) is a match filter with frequency 3.951 MHz (4.516 MHz resp.).

Although IAGO (Informatisation et Automatisation par Guide d'Onde) waveguide is installed in some subway lines (e.g., Singapore Northeast Line [39]), it is not as popular as balise, most likely because they are more costly, require more effort for installation, and (when used outdoors) may be more susceptible to signal degradation due to rain/snow/ice accumulation [40]. Hence, without loss of generality, balise is used to represent wayside positioning devices in the following.

C. Balise-Based Train Positioning

Usually, when a train passes over a balise, its BTM emits electromagnet wave to power the balise. For instance, with a 20 W on-board antenna, a BTM emits a continuous electromagnetic wave at frequency 27.095 MHz ($\pm$5 kHz) to power a balise up to a distance of 60 cm [41]. With reference to Fig. 3, the balise induced voltage is variable with the distance between BTM and

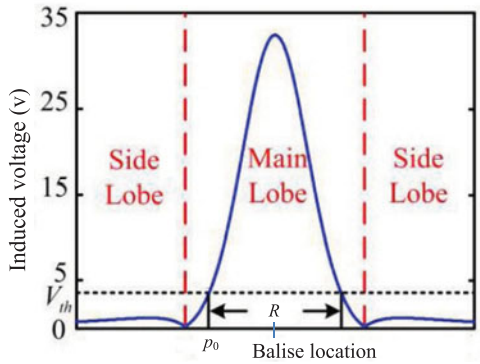

Fig. 3. Balise induced voltage vs Balise-BTM distance (adapted from [18]). If and only if the induced voltage is above a threshold value, the balise is able to send the telegram to BTM. The actual effect range R varies with the balise, BTM and train speed.

balise center point. If the induced voltage becomes higher than a threshold value V_{th} (e.g., 3.3 V), the balise is activated to send the telegram to the train, and will transmit the telegram repeatedly as long as the induced voltage is higher than V_{th}. Therefore, the moving train may receive a multiple of telegram copies at different positions as shown in Fig. 2.

Denote the balise transmission time as effective time T, the train moving distance within T as effective range R, the total length of the telegram as L and telegram bitrate as b_r, the number of received copies is

$$l = \lfloor \frac{T \times b_r}{L} \rfloor = \lfloor \frac{R \times b_r}{Lv} \rfloor \tag{2}$$

for a train moving at a constant speed v within the effective range. Rewriting (2) as

$$R = \frac{Lvl}{b_r} + \delta, \;\; 0 \leq \delta < \frac{Lv}{b_r} \tag{3}$$

Due to the symmetry of induced voltage shown in Fig. 3, the actual balise position

$$p = p_0 + \frac{R}{2} = p_0 + \frac{Lvl}{2b_r} + \frac{\delta}{2} \tag{4}$$

where p_0 is the unknown position where the balise is activated.

Denote t_i as the time when the train receives the ith copy of the telegram. After extracting the balise position p from the telegram, the train needs to know when it passes over the balise. A naïve method is to choose the middle time $t_{\lceil \frac{l}{2} \rceil}$ as the balise passage time. As it is certain that the train velocity is variable in the parking process, a better solution is to estimate the balise

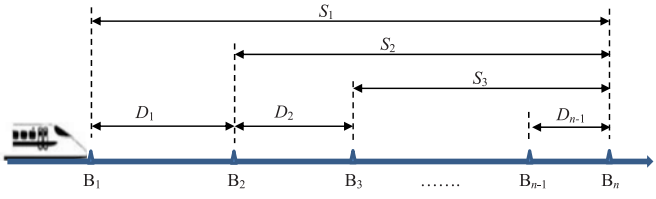

Fig. 4. Control procedure of TASC [31].

passage time

$$\tilde{t} = \frac{\sum_{i=1}^{l} t_i}{l} \tag{5}$$

In other words, the controller estimates that the train passed over the balise at time $\tilde{t}$. In fact, with reference to Fig. 2, the train position at time $\tilde{t}$ is

$$\begin{aligned} \tilde{p} =& \frac{\sum_{i=1}^{l} p_i}{l} = \frac{\sum_{i=1}^{l} (p_0 + iL/b_r \times v + \varepsilon_i)}{l} \\ \approx& \ p_0 + \frac{Lv \sum_{i=1}^{l} i}{l b_r} = p_0 + \frac{Lv}{l b_r} \times \frac{l(l+1)}{2} \\ =& \ p_0 + \frac{Lv(l+1)}{2 b_r} \end{aligned} \tag{6}$$

where the random variable ε_i is the error of the estimated position p_i. Thus the error of the estimated balise position is

$$\begin{aligned} e =& \ \tilde{p} - p \approx \left(p_0 + \frac{Lv(l+1)}{2 b_r} \right) - \left(p_0 + \frac{Lvl}{2 b_r} + \frac{\delta}{2} \right) \\ =& \ \frac{Lv}{2 b_r} - \frac{\delta}{2} \in \left(0, \frac{Lv}{2 b_r} \right] \end{aligned} \tag{7}$$

With reference to (7), the train location error is bounded to a small value when the balise passage time is estimated as $\tilde{t}$ assuming the effective range is symmetric with balise center. For instance, according to the introduction of balise in Section II-B, assume the length L of balise telegram be 341 in bits, and the train speed be 10 m/s. According to the average data rate $b_r = 564.48$ kbps [17], the error e in (7) is no more than $\frac{Lv}{2b_r} = \frac{341 \times 10}{2 \times 564.48 \times 10^3} \approx 3 \times 10^{-3}$ meters.

However, if the symmetry assumption does not hold, e.g., either the balise activation time or the effective range is manipulated, there may be significant difference between the estimated train position and the balise position at time $\tilde{t}$. This difference will be exploited in Section IV-D below by an attacker.

III. Train Automatic Stop Control

With the measured travel speed v, acceleration a, moving distance d, and remaining distance to destination platform addressed in Section II, the on-board controller will calculate the braking force profile so as to stop the train accurately and comfortably.

A. System Model

With regard to Fig. 4, suppose there are n balise B_i near the target platform. B_n is localized at the stop position. Denote S_i as the distance between balise B_i and the target stop position, and D_i as the distance between balises B_i and B_{i+1}. Obviously $S_n = 0$. All the S_i and D_i are extracted by the train from the telegram sent from balise B_i, and $S_i - S_{i+1} = D_i$. Let v_i (or a_i) be the train's speed (acceleration respectively) at balise B_i. We further assume that the train moves at a constant speed before it passes over the first balise B_1, i.e., $a_1 = 0$.

This paper will adopt the single-point mass model for investigating the train performance due to its popularity and simplicity [42], [43]. Therefore, if the train with mass M is expected to run at a constant deceleration from balise B_i, we have

$$M a_i d_i = \frac{1}{2} M v^2 - \frac{1}{2} M {v_i}^2 \tag{8}$$

based on the relationship between work and train kinetic energy. Rewriting (8) as

$$v^2 = {v_i}^2 + 2 a_i d_i \tag{9}$$

Suppose the train stops accurately, $v_n = 0$ and moving distance $d_i = S_i$, the expect deceleration

$$a_i = -\frac{{v_i}^2}{2 S_i} \tag{10}$$

Hence, after passing any new balise, the train controller shall re-calculate the expect deceleration and adjust the actuator. Equation (10) describes the train stop principle in an ideal condition, e.g., the acceleration can be changed immediately after the actuator is driven. Nonetheless, as the acceleration $a_n = -\frac{(v_{n-1})^2}{D_{n-1}} \neq 0$ at the last balise B_n according to (10), the train does not stop comfortably. Therefore, a practical TASC shall complete the distance D_{n-1} by continuously adjusting the expect deceleration based on the on-board measured remaining distance.

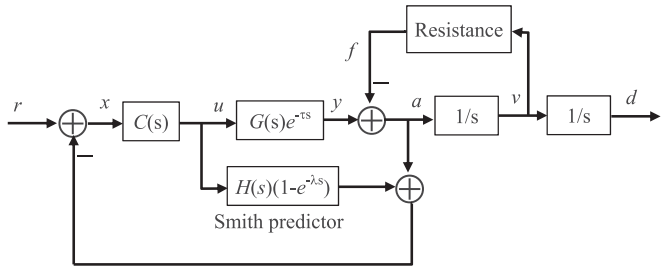

Fig. 5. TASC control diagram with Smith predictor $H(s)(1 + e^{-\lambda s})$.

B. Controller Diagram

Any practical train control system shall handle the uncertainties such as system delay and resistance. In this paper, we adopt the Heuristic Online Learning Algorithm (HOA) [31] as it is used in a real subway.

Fig. 5 illustrates our TASC diagram, where the Smith predictor is used to compensate the pure system delay, the forward controller $C(s)$ is used to generate the braking force, and the transfer function

$$G(s)e^{-\tau s} = \frac{y(s)}{u(s)} = \frac{a_0}{1 + qs} e^{-\tau s} \tag{11}$$

is the braking model [31], where a_0 is the braking performance gain, τ and q represent the time delay and the time constant of the braking system. Assume Smith predictor is employed with estimated braking model $H(s)$ and estimated delay λ, we have

$$\begin{cases} x = r - (a + uH(1 - e^{-\lambda s})) \\ u = xC \\ a = y - f = uGe^{-\tau s} - f \end{cases} \tag{12}$$

where r is the reference signal for the deceleration so that the actual acceleration can be close to a_i in (10). In (12), we denote $C(s), G(s)$ and $H(s)$ as C, G, and H respectively for the sake of simplicity. According to [31], the basic resistance acceleration can be modeled as $f = \alpha v^2 + \beta v + \gamma$ for some constants α, β, and γ. By simplifying (12), we have the actual train acceleration function

$$a = \frac{rCGe^{-\tau s} - f(1 + CH - CHe^{-\lambda s})}{1 + C(H - He^{-\lambda s} + Ge^{-\tau s})} \tag{13}$$

If Smith predictor is ideally chosen, the estimated delay $\lambda = \tau$ and the estimated braking model $H = G$, then (13) can be rewritten as

$$a = \frac{rCGe^{-\tau s} - f(1 + CG - CGe^{-\tau s})}{1 + CG} \tag{14}$$

As there is no delay factor in the denominator of (14), the delay has no effect on the stability of the whole train system according to control theory. In this case, Smith predictor completely compensates the adverse effect of delay.

C. Reference Signal

According to (13), if the forward controller $C(s)$ is designed to ensure the actual acceleration a approaches to the reference signal r gradually, r can be close to the expected deceleration in (10). But in fact, the actual deceleration a is not always equal to the reference signal r due to the delay and/or inertia in the forward transfer function $C(s)G(s)e^{-\tau s}$, hence the train may stop away from balise B_n. Meanwhile, if $r = a_i$ is used to update the braking force directly with the new acceleration a_i when the train passes over balise B_i, the change of the actual train acceleration may be too large such that the passengers do not feel well. To provide an accurate and comfort parking, the relationship between the expect deceleration a_i in (10) and the reference signal r in (13) is represented with a transfer function

$$Q(s) = \frac{r(s)}{a_i(s)} = \frac{k}{1 + hs} \tag{15}$$

with gain k for adjusting stop location and inertia coefficient h for reducing jerk rate, when the train moves between two neighboring balises.

IV. The Present Attacks

As introduced in Section III, a TASC aims to provide good stop performance in terms of accuracy and comfortability. Specifically, due to the physical limitation of train platform, especially for the platform installed with PSD, the train shall stop at an accurate position in a passenger-friendly way. For instance, regulation for precise stopping of the urban train requires 0.3 m in Korea [28] and 0.3 m$\sim$ 0.5 m in China [30]. Meanwhile, in order to operate the train smoothly, the changing rate of acceleration, called as jerk rate designed into the automatic train operation [42], shall be restricted. For instance, the jerk rate is limited to be 0.75 m/s^3 in the commercial subway system [44].

On the contrary, an attacker aims to make the train stop at a wrong place or a high jerk rate. Indeed, both wrong place or high jerk rate motivations are correlated. For instance, if a train passes over balise B_n, an emergency brake shall take effect such that the train has a high jerk rate. Thus, the following Sections elaborate the attacks which incur erroneous parking positions only.

A. Security Model

According to the balise specification [17], the telegram transmission process does not include any security protection mechanism. Therefore, it is easy for an attacker to generate a bogus telegram [45], [46] to cheat the train such that the parking position is incorrect, or even does not stop on the target station. As the bogus telegram attack is very simple, and can be defeated with cryptographic tools, this paper will ignore this attack in the following.

As the IT subsystems of the train system are private, it is not easy for an attacker to break into them. However, the train-ground communication channel, especially the BTM-balise channel is open to public. To violate the parking requirements, the attacker may manipulate the telegram or balise electromagnet signals such that the train parks at an inaccurate position. To this end, the attacker is assumed to be

- Able to jam the balise signals due to the public accessibility of the wireless BTM-balise communication. Theoretical analysis, simulation and practical events in subway environments demonstrate the possibility of the interference of wireless communication [47], [48];
- Able to replay the balise telegrams because the telegram information is accessible to any one; but
- Unable to tamper with the wayside devices and on-board devices.

B. Balise Missing Attack

According to (10), the remaining distance S_i extracted from a balise telegram is used to update the expected acceleration in TASC when the train passes over balise B_i. But if a telegram is missing, the update process will be omitted such that the train parks in an unusual manner.

To cause balise missing, an attacker can jam the BTM-balise gap when a train passes over a balise by transmitting signals to BTM antenna at the same frequency band as the balise transmits [49]. As introduced in Section II-B, the telegram format and frequency band are public, hence the adversary can start the selective and intelligent interfering to block the balise transmission so as to be energy-efficient.

Fig. 6 illustrates the attack workflow. When a train passes over a balise, the attacker jams a crafted signal $u_a(t)$ to the

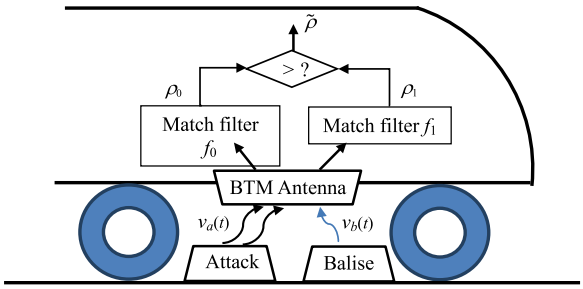

Fig. 6. Balise missing attack diagram.

TABLE I
BALISE MISSING ATTACK STRATEGY

message bit ρ	Telegram waveform u_b	Jamming waveform u_a
0	7 periods of 3.951 MHz	8 periods of 4.516 MHz
1	8 periods of 4.516 MHz	7 periods of 3.951 MHz

BTM antenna. Upon receiving the electromagnetic waveform $u(t)$, BTM decodes the waveform with two match filers so as to determine the binary bit based on (1).

Table I shows the jamming waveforms for different message bits. For any target telegram binary bit ρ in column 1, the genuine balise will emit the waveform as column 2. However, the attacker will simultaneously transmit a complementary bit $(1-\rho)$ to BTM as indicated in column 3. For instance, as shown in row 2, given a message bit $\rho = 0$, the genuine balise will transmit approximately 7 periods of 3.951 MHz, but the attacker will transmit approximately 8 periods of 4.516 MHz at the same time.

When the signal $u(t) = u_b(t) + u_a(t) + n(t)$ is received by BTM, where $u_b(t)$ is the component sent from the genuine balise, $u_a(t)$ is sent from the attacker, and $n(t)$ is random noise in air-gap channel. Upon receiving the signal $u(t)$, the on-board device calculates the correlation

$$\begin{aligned}\rho_0 =\ & u(t) * f_0(t) = (u_b(t) + u_a(t) + n(t)) * f_0(t) \\ =\ & u_b(t) * f_0(t) \end{aligned} \tag{16}$$

where the last equality "=" holds due to independencies among filter $f_0(t)$, jamming signal $u_a(t)$ and random noise $n(t)$. Similarly

$$\begin{aligned}\rho_1 =\ & u(t) * f_1(t) = (u_b(t) + u_a(t) + n(t)) * f_1(t) \\ =\ & u_a(t) * f_1(t) \end{aligned} \tag{17}$$

If the power of the jamming signal $u_a(t)$ is higher than the power of the genuine signal $u_b(t)$, then $\rho_0 < \rho_1$ with a high probability. As a result, according to the detection formula (1), $\tilde{\rho} = 1 \neq \rho$. It is easy to verify that the on-board device will make mistake for message $\rho = 1$ too. According to the 75 parity bits in the balise telegram [17], the on-board device will reject the telegram erroneously if the parity-check fails, and hence miss to update the expected acceleration in (15) as shown in Fig. 7.

Let's show this balise missing attack using an extreme case that the attacker is able to disrupt all the balises except the first

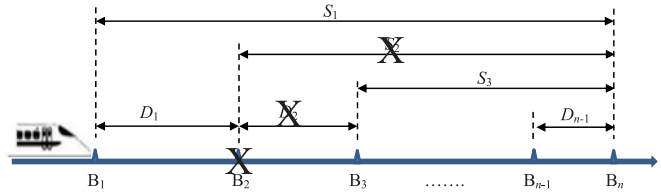

Fig. 7. Balise missing attack. "X" means that the data is unknown to the passing train.

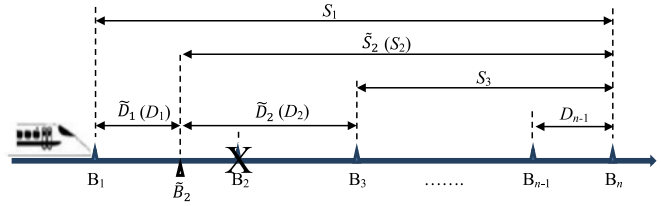

Fig. 8. Attack by displacing balise away from the destination station, where $\tilde{D}_i\,(D_i)$ indicates the manipulated (original) distance, "X" means that the balise is missing.

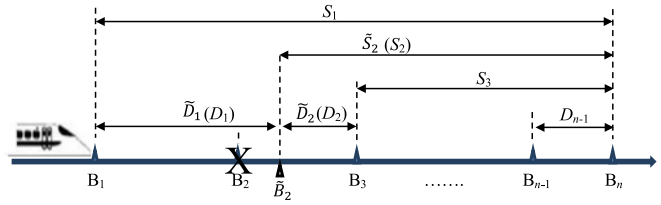

Fig. 9. Attack by displacing balise towards the destination station.

one B_1. Suppose that the actual accelerate error is 0.1m/s^2 on average due to unpredictable weather reasons, and the parking process takes 10 seconds. Because there is no balise update in the parking process due to balise missing attack, the parking location error is approximately $1/2 \times 0.1 \times 10^2 = 5$ meters !

The balise missing attack can be detected by the on-board device if the train has the rail map which includes the balises' positions. With this detection, the train service quality will only degrade a little bit when the train moves slowly. Hence an attacker may prefer to stealth attacks to have better attack effect as elaborated in the following.

C. Balise Displacement Attack

In balise specification [17], the telegram transmission mechanism does not include the challenge-response security protection mechanism, thus, the attacker is able to replay the balise telegram such that the victim balise seems to be displaced around its actual position. To realize this attack, the adversary shall jam the genuine balise as Section IV-B introduces, and replay the telegram of the balise. Considering the attack starts before or after the train passage, there are two balise displacement attacks.

With regard to Fig. 8, a balise B_i (B_2 is used as an example in Fig. 8) is virtually moved toward balise B_{i-1}, the actual moving distance between B_{i-1} and B_i becomes shorter. Thus, the acceleration update algorithm will be executed ahead of schedule.

On the contrary, with regard to Fig. 9, a balise B_i is virtually moved toward balise B_{i+1}, the actual moving distance between B_{i-1} and B_i becomes longer. Thus, the acceleration update algorithm will be executed behind schedule.

Denote the balise B_i is displaced at a distance θ. According to (10), the train speed at the faked balise position is

$$\tilde{v}_i^2 = {v_{i-1}}^2 + 2a_{i-1}\tilde{D}_{i-1} = {v_{i-1}}^2 + 2a_{i-1}(D_{i-1}+\theta) \quad (18)$$

and according to (10), we have

$$a_{i-1} = -\frac{{v_{i-1}}^2}{2S_{i-1}} \quad (19)$$

$$\tilde{a}_i = -\frac{\tilde{v}_i^2}{2S_i} \quad (20)$$

Therefore, the train speed at balise B_{i+1} is

$$\begin{aligned}
\tilde{v}_{i+1}^2 &= \tilde{v}_i^2 + 2\tilde{a}_i\tilde{D}_i = \tilde{v}_i^2 + 2\tilde{a}_i(D_i-\theta) \\
&= \tilde{v}_i^2 - \frac{\tilde{v}_i^2}{S_i}(D_i-\theta) = \tilde{v}_i^2 \times \frac{S_i - D_i + \theta}{S_i} \\
&= \left({v_{i-1}}^2 + 2a_{i-1}(D_{i-1}+\theta)\right) \times \frac{S_{i+1}+\theta}{S_i} \\
&= \left({v_{i-1}}^2 - \frac{{v_{i-1}}^2}{S_{i-1}}(D_{i-1}+\theta)\right) \times \frac{S_{i+1}+\theta}{S_i} \\
&= {v_{i-1}}^2 \times \frac{S_i-\theta}{S_{i-1}} \times \frac{S_{i+1}+\theta}{S_i} \quad (21)
\end{aligned}$$

That is

$$\tilde{v}_{i+1} = v_{i-1} \times \sqrt{\frac{S_i-\theta}{S_{i-1}} \times \frac{S_{i+1}+\theta}{S_i}} \quad (22)$$

If there is no displacement attack, i.e., $\theta = 0$, then

$$v_{i+1} = v_{i-1} \times \sqrt{\frac{S_i}{S_{i-1}} \times \frac{S_{i+1}}{S_i}} = v_{i-1} \times \sqrt{\frac{S_{i+1}}{S_{i-1}}} \quad (23)$$

Thus the change of entry speed at balise B_{i+1} due to displacement attack is

$$\begin{aligned}
\Delta_{i+1} &= \tilde{v}_{i+1} - v_{i+1} \\
&= v_{i-1}\left(\sqrt{\frac{S_i-\theta}{S_{i-1}} \times \frac{S_{i+1}+\theta}{S_i}} - \sqrt{\frac{S_{i+1}}{S_{i-1}}}\right) \quad (24)
\end{aligned}$$

It indicates that the change Δ_{i+1} is a function of displacement θ as shown in Fig. 10. That is to say, after receiving the telegram from the displaced balise, the train re-calculates the parking profile with an incorrect speed and position. Therefore, parking process will be not satisfactory.

D. Transmission Time Extension Attack

With reference to Section II-C, if the attacker extends the induced power time and/or replays the telegrams, the number l of telegrams transmitted will increase and result in the erroneous balise position. For instance, after the normal balise telegrams complete as shown in Fig. 11, the attacker continues to telepower the balise or directly replay the telegram such that m more

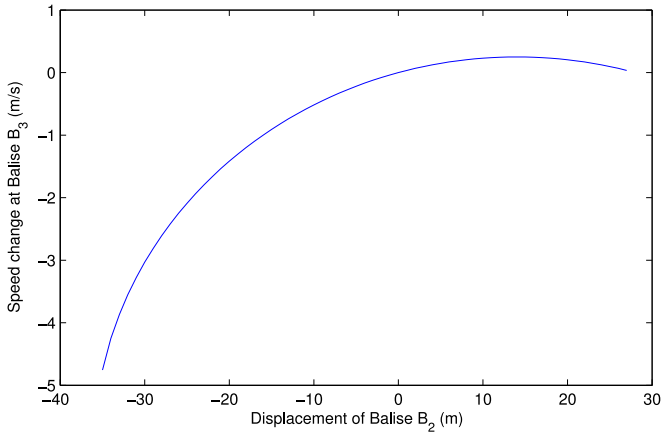

Fig. 10. Displacement effect on the speed change Δ_3 when balise B_2 is attacked, where $v_1 = 10$ m/s, $S_1 = 100$ m, $S_2 = 64$ m, and $S_3 = 36$ m.

telegrams are received by the train. Then, with reference to (6), the estimated train position is

$$\tilde{p} = p_0 + \frac{Lv(l+m+1)}{2b_r} \quad (25)$$

Thus the estimation error is

$$\begin{aligned}
e &= \tilde{p} - p \approx \left(p_0 + \frac{Lv(l+m+1)}{2b_r}\right) - \left(p_0 + \frac{Lvl}{2b_r} + \frac{\delta}{2}\right) \\
&= \frac{Lv(m+1)}{2b_r} - \frac{\delta}{2} = \frac{m}{2l} \cdot \frac{Lvl}{b_r} + \left(\frac{Lv}{2b_r} - \frac{\delta}{2}\right) \\
&= \frac{m}{2l} \cdot R - \frac{m}{2l} \cdot \delta + \left(\frac{Lv}{2b_r} - \frac{\delta}{2}\right) \approx \frac{m}{2l} \cdot R \quad (26)
\end{aligned}$$

According to [18], R is estimated to be 0.75 m for some BTM-balise pair. In other words, the error of park location will be 0.375 m as long as the attacker merely re-transmits the telegram or continuously powers the balise such that $m = l$. If so, the attack takes $\frac{lLv}{b_r}$ seconds.

Alternatively, if the effective range R is unknown but the train speed is known, with reference to Fig. 11, the position error can be obtain as

$$e \approx \frac{1}{2}\int_{t_0}^{t_{n+m}} v dt - \frac{1}{2}\int_{t_0}^{t_n} v dt = \frac{1}{2}\int_{t_n}^{t_{n+m}} v dt \quad (27)$$

where $v(t)$ is the train speed function, t_0 is the time when the balise starts to send telegram, and t_n (or t_{n+m}) is the time when the nth (or $(n+m)$th resp.) telegram is received by the train.

Similarly, the attacker can send the telegram ahead of p_0 as shown in Fig. 12. In this attack, if the effective range R is known, the position error is

$$e = \tilde{p} - p \approx \frac{-mLv}{2b_r} \approx -\frac{m}{2l} \times R \quad (28)$$

otherwise

$$e = \tilde{p} - p \approx \frac{1}{2}\int_{t_{-m}}^{t_n} v dt - \frac{1}{2}\int_{t_0}^{t_n} v dt = \frac{1}{2}\int_{t_{-m}}^{t_0} v dt \quad (29)$$

if the train speed function is known.

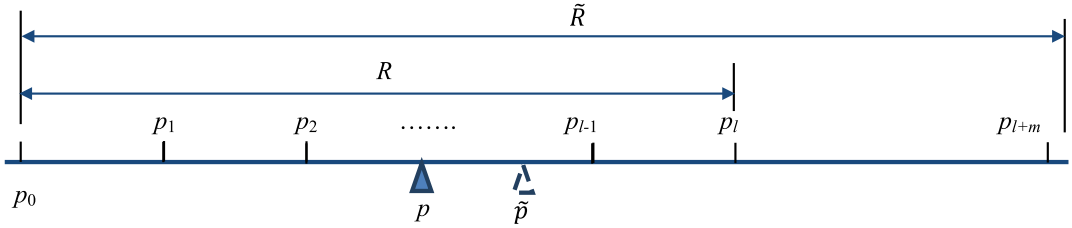

Fig. 11. Displacement attack after balise passage.

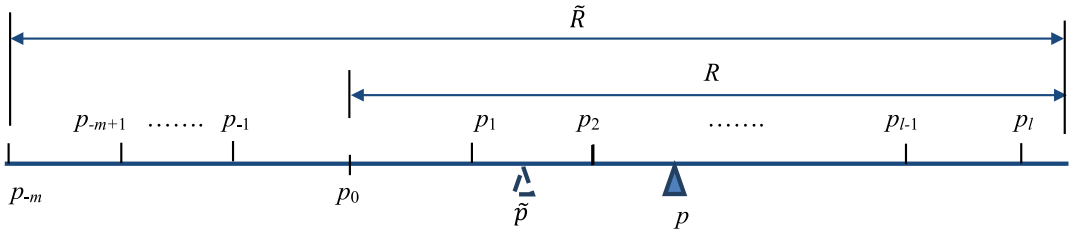

Fig. 12. Displacement attack before balise passage.

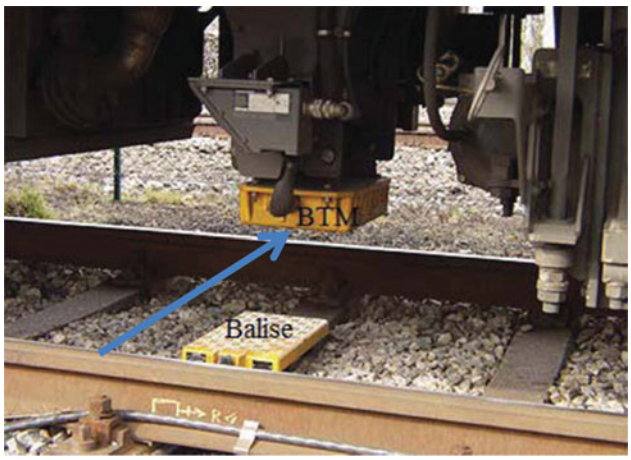

Fig. 13. Roadside attack (Adapted from [50]). The arrow indicates the potential attack direction.

Fig. 14. Attack beneath the bridge. In the two-layer public transport system, the train moves above the ground, and buses moves on the ground. The arrow indicates the potential attack direction.

V. Discussions

A. *Feasibility of Attacks*

Although the subway operators regard safety and security as the first priority in train services and take much effort in guarding subway, subway is still an "ideal" target of the attacker because a successful attack to subway will severely ruin the reputation of the railway operator and its authority. Meanwhile, the present attacks are technically feasible in several aspects.

First, as a telegram transmitter is very small and lightweight, it can be installed on any vehicle, or even put into a small handhold bag. Therefore, the attacks are stealthy such that the attackers have much lower risk than non-technical attackers (e.g., bomb attacker). In addition, a small attack tool enables the attacker to choose the target balise flexibly and launch the attack quickly.

Secondly, as the train car is made of metal, an attacker is unable to emit the interference signal on the train due to the effect of Faraday cage. Nonetheless, in some train services as shown in Fig. 13, the BTM-balise gap is more than 0.5 m, and is open to anyone. Therefore, a trackside attacker is able to easily inject signals to this kind of train services.

Thirdly, as shown in Fig. 14, some balises are installed on the bridges (or above the ground), the attacker may emit attack signals under the bridge. In this case, the attack success probability is related to the bridge material, interference frequency, interference antenna and interference signal power. To the best of our knowledge, there is no real result on the penetration of

TABLE II
COMPARISON OF DIFFERENT ATTACKS

Attack method	Attack action	Attack time	Attack EM signal	Reference error
Balise missing	interfere	T	high energy	unknown
Balise displacement	interfere & replay	$(T, 2T]$	high energy & more time	displacement
Time extension	replay	variable	more time	$0.5\bar{v} \cdot T_{\text{attack}}$

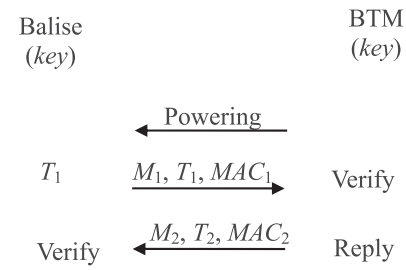

Fig. 15. The BTM-balise authenticated communication protocol.

4.23 MHz radio wave on metal-reinforced concrete structure which is used to build rail bridges. Thus we can not estimate the attack success probability directly. However, we can evaluate the attack feasibility as follows. In the experiments [51], conventional WiFi signal (Omni-directional antenna, 2400 MHz) can penetrate a 0.45 m metal-reinforced concrete structure. As the depth of radio penetration is inversely proportional to the square root of the frequency [52], [53], the penetration depth of the attack frequency (4.23 MHz) is roughly $\sqrt{\frac{2400}{4.23}} = 23.8$ times as high as that of WiFi frequency (2400 MHz). Moreover, if the attacker emits higher-energy electromagnetic signals with a directional antenna, the penetration effect will be increased significantly. Thus, the attack beneath the bridge is feasible.

B. Comparison of Attacks

The attacks elaborated in Section IV have different requirements on the interference means, time and power, and may have different attack effects. Table II shows the comparison results of the proposed attacks listed in column 1.

The second column shows which attack action is taken by the adversary, where the original telegram signals are interfered in balise missing attack, replayed in time extension attack, interfered and replayed in the displacement attack. Thus, replacement attack is more complicated than others.

The third column presents the attack time required. In the missing attack, the attacker has to jam the BTM-balise gap within the BTM-balise communication time period, hence the attack time is almost the same as the telegram transmission time T. In the displacement attack, the attacker has to replay the balise telegram and jam the original balise signal to cause erroneous telegrams, hence, the attack time is within the interval $(T, 2T]$. In the time extension attack, the attacker will replay a telegram continuously such that the train obtains the balise position with sufficiently large error. Therefore, his attack time varies with the train speed.

In the fourth column, both missing attack and displacement attack require higher EM (Electro-Magnetic) energy according to (16) and (17) to jam the genuine balise. In addition, the displacement attack requires extra attack time to replay the telegram. In the time extension attack, the time for emitting the attack signal is longer than the time for transmitting normal BTM-balise telegram.

The last column shows the reference distance errors which are the attack results. Here reference distance is the value d_i in (9) when a parking profile is updated. In balise missing attack, the process for parking profile update is missed and the reference distance is unknown to the train. The reference distance error due to displacement attack is the displacement, and the reference distance error is about $0.5\bar{v} \cdot T_{\text{attack}}$, where $\bar{v}$ is the average speed within the attack period T_{attack}. Thus, both displacement attack and time extension attack are flexible from the viewpoint of the attackers.

C. Countermeasures

The above attacks exploit the fidelity vulnerabilities of the balise telegram such that the train obtains an erroneous balise location data at the balise passage time. In order to defeat these attacks, the train shall check the fidelity of the received balise telegrams using the following methods.

1) Cryptographic Protocol: The first method is to authenticate the telegrams with an interactive cryptographic protocol between on-board device and balise. This countermeasure is able to thwart the replay attacks including displacement attack and time extension attack. Specifically, with reference to Fig. 15, suppose both on-board BTM and balise share a key key (or each side has an authentic public/private key pair). Whenever a train passes over a balise which can produce telegrams, the balise presents a telegram including telegram content M_1, its timestamp T_1 and MAC (Message Authentication Code) $MAC_1 = \mathcal{H}(M_1||T_1||key)$ to the train BTM, where $\mathcal{H}(\cdot)$ is a one-way function, and $x||y$ is the concatenation of string x and string y. Afterwards, the train checks the authenticity of the balise and timestamp. Optionally, the train can reply with a telegram including message M_2, its timestamp T_2 and the MAC $MAC_2 = \mathcal{H}(M_2||T_2||key)$ to the balise, such that the balise is able to verify the messages from the train (if any).

This protocol is a trivial/standard application of cryptographic primitives, hence it guarantees to defeat faking attack and replay attack. However, its implementation is not trivial as it shall be compliant with the balise specification on telegrams [17], [54].

Balise telegram consists of packet types which are strictly defined in the specifications, especially for the uplink telegrams sent from balise to train. Hence, the telegram in the above protocol shall follow the specifications, otherwise, it may be dangerous due to incompatible format. To this end, we customize the telegram packet type 72 which is used to send text messages from balise to driver-machine interface via BTM. Table III shows the customized data structure of packet type 72 for the above protocol.

TABLE III
AUTHENTIC UPLINK TELEGRAM

Variable/field	Length	Comment	value
NID_PACKET	8	packet type	72
Q_DIR	2	direction	x
L_PACKET	13	packet length	x
Q_SCALE	2	scale	2
Q_TEXTCLASS	2	class	0
Q_TEXTDISPLAY	1	event relation	1
D_TEXTDISPLAY	15	start event	32766
M_MODETEXTDISPLAY	4	start event	0
M_LEVELTEXTDISPLAY	3	start event	4
L_TEXTDISPLAY	15	end event	0
T_TEXTDISPLAY	10	end event	0
M_MODETEXTDISPLAY	4	end event	x
M_LEVELTEXTDISPLAY	3	end event	x
Q_TEXTCONFIRM	2	confirmation	0
L_TEXT	8	text length	$\|\mathbf{M}\|$
X_TEXT	x	text	$\mathbf{M}$

In the Table III, the first column is the variable or field in packet type 72, the second column is the length of the field in bits, the third column is the meaning of the field. The first three columns are specified in the balise specification [54], and the last column is the value chosen for the above protocol, where 'x' means that the value depends on usage case. Let's explain the customized fields one by one.

Q_TEXTCLASS field specifies whether the message is auxiliary or important for rendering to the driver. As the protocol message is only useful to the on-board computer, hence, its class can be auxiliary information (i.e., Q_TEXTCLASSb=0).

In order to render the telegram text in a controllable manner, the balise specification defines five kinds of events which are the conditions to render the texts. Q_TEXTDISPLAY field is used to decide whether any or all of relevant events shall occur for text rendering. For the sake of driver-friendly, safety and reliability, we choose Q_TEXTDISPLAY=1 which requires to fulfill all the following events:

1) D_TEXTDISPLAY indicates the distance from where on the text shall be displayed. The distance is in the interval (0, 327660) meters. As we do not want to render the telegram text to the driver, we choose the maximum value, i.e., D_TEXTDISPLAY = 32766 and the scale Q_SCALE = 2 for 10-meter scale.
2) M_MODETEXTDISPLAY indicates the on-board operating mode for rendering the text. In the full supervision mode, the driver will not be interfered with. Hence, the start event M_MODETEXTDISPLAY = 0 (i.e., full supervision mode), and the end event M_MODETEXTDISPLAY shall be chosen as the present mode (i.e., no mode change).
3) M_LEVELTEXTDISPLAY indicates on-board operating level for text display. As the probability of the highest level is low, the start event M_LEVELTEXTDISPLAY = 4, and the end event M_MODETEXTDISPLAY shall the same as the present level in order to avoid the interference on the train operation.
4) L_TEXTDISPLAY shows how far the message shall be displayed. As we do not want to render the text message on the driver-machine interface, we choose the minimal distance, i.e., L_TEXTDISPLAY=0.
5) T_TEXTDISPLAY shows how long the message shall be displayed. We choose T_TEXTDISPLAY=0 which indicates the display time is 0 (i.e., the text disappears from the driver's screen soon after it is rendered).

The field Q_TEXTCONFIRM=0 means that the driver is not required to confirm text messages. Finally, L_TEXT is the length of telegram message $\mathbf{M} = \{M_1, T_1, MAC_1\}$ and X_TEXT is the message $\mathbf{M}$.

2) Cross-Checking With On-Board Devices: The second countermeasure is to detect the attacks by the trains. As a balise only provides its discrete physical position rather than the train's real-time position, almost all Automatic Train Protection (ATP) systems have the on-board continuous speed/location measurement devices. Although the on-board measurements are inaccurate, their errors are usually restricted to a small range. For instance, when a train receives telegrams from two consecutive balises, it is able to calculate the distance $\tilde{d}$ of the balises from the telegrams. Suppose the error of the qualified on-board distance sensor is no more than $5 + 5\%\tilde{s}$ for the measured travel distance $\tilde{s}$ [16], then

$$|\tilde{d} - \tilde{s}| < 5 + 5\%\tilde{s}, \text{ i.e., } \tilde{d} \in (0.95\tilde{s} - 5, 1.05\tilde{s} + 5). \quad (30)$$

The train is able to detect the displacement attack and/or time extension attack if (30) does not hold.

It is also easy to detect the balise missing attack if the train schedule/map indicates the balise distance $\tilde{d}$ or each balise telegram includes its distance $\tilde{d}$ to the next balise. Specifically, after passing over a balise, the train expects to meet the next balise after traveling $\tilde{s} \in (\frac{\tilde{d}-5}{1.05}, \frac{\tilde{d}+5}{0.95})$. Therefore, the train knows that it misses a balise if it does not detect an expected balise after traveling $\frac{\tilde{d}+5}{0.95}$. Once the attacks are found, the train usually moves slowly for safety reasons and reports to the control centers.

With reference to Table II, the telegram transmission time shall be within a suitable interval for a given train speed. Hence, if the transmission time of a balise telegram is beyond the interval, the train may detect the potential attacks and then defeat it by moving cautiously.

3) Non-EM Balise: The third countermeasure is that the train actively reads "balise" data via non-electromagnetic methods. For example, based on computer vision technology [55]–[57], the train takes pictures of the barcode (or QR code) at the balise position and then extracts the balise position information, or takes pictures of the rails and then counts the number of sleepers for continuous positioning. As this AI-based countermeasure completely removes the weakness of electromagnetic communication in noise tolerance, it defeats all the present attacks. However, its performance is restricted by rain, snow, environment brightness etc.

4) Anti-Jamming: There are many research works on wireless jamming and anti-jamming [58]. Hence, the fourth countermeasure is to adopt the well-known anti-jamming technologies, such as dynamic telegram waveform format or frequency such as frequency-hopping [59]. As the attacker can not predict the telegram waveform, he fails to jam the signal such that all the

attacks fail. Nonetheless, this countermeasure is not compatible with ETCS standards. Moreover, as the first countermeasure, this countermeasure has to spend much effort on the cryptographic key management so as to synchronize the keys of BTM and balise. If the keys are not properly managed, the security strength may not be guaranteed and/or the BTM-balise communication may fail.

Each of the above countermeasures has its strength and weakness, and they are complementary to each other. In order to have the best defence effect, their combination is preferable.

VI. Simulations

This section describes a simulation configuration with a real subway system and the performance of the present attacks on the subway system.

A. Configuration

In order to facilitate the accurate and comfortable station parking, balises are installed near each station. As a balise is expensive, only a small number of balise is installed in practice so as to make trade-off between cost and stop accuracy. In this simulation, we adopt the same parameters as [31], [60], i.e., the stop area has 6 balises which are localized at positions $S_1 = 100$ m, $S_2 = 64$ m, $S_3 = 36$ m, $S_4 = 16$ m, $S_5 = 4$ m, and $S_6 = 0$ m. In addition, the maximum velocity for a train to enter into the stop area is $v_{\max} = 11.5$ m/s, the maximum actual deceleration $a_{\max} = -1$ m/s^2. Meanwhile, the braking deceleration model is $G(s)e^{-0.6s} = e^{-0.6s}/(1 + 0.4s)$ and the resistance factor $f = 10^{-4} \times (1.36v^2 + 145v + 1244)$.

As addressed in Section III, PID controller with Smith predictor is used to control the parking process. The PID controller is $C(s) = 7 + 2/s + 0.1s$ and the Smith predictor perfectly matches the braking deceleration model, i.e., the Smith predictor is $G(s)(1 - e^{-0.6s})$. In order to patch up the delay and inertia mentioned in Section III, an empirical adjustment scalar array $k = \{1.46, 1.30, 1.11, 1.02, 1.0\}$ is used for balises B_1 to B_5 respectively, and the decay rate $h = 0.7$ for restricting the jerk rate in (15). In addition, when the train speed is 0.05 m/s, the train is forced to stop immediately.

The parking curves in Fig. 16 indicate the TASC has satisfactory merits in terms of small jerk rate, admissible deceleration and accurate parking position. Hence, the system configuration makes sense. In the following sections, we will show that the attacker can invalidate the parking process with the present attacks.

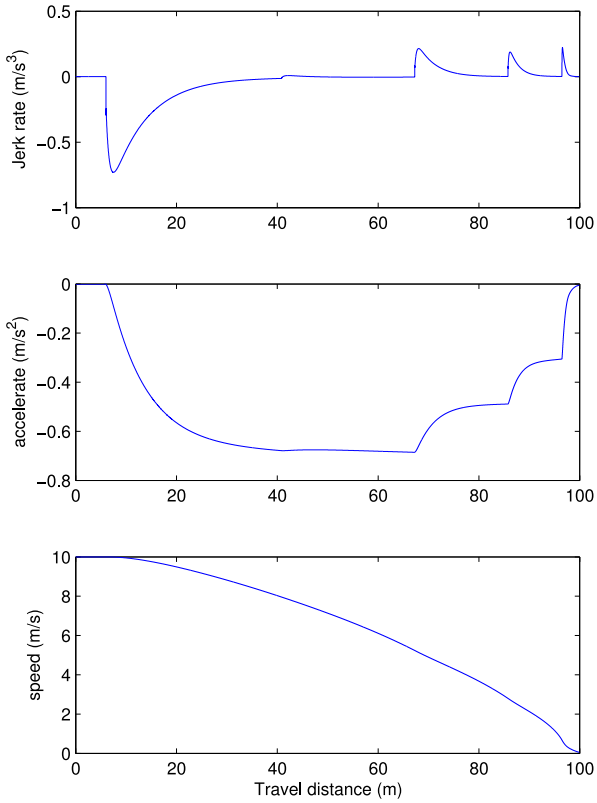

Fig. 16. TASC simulation with the parameters in [60].

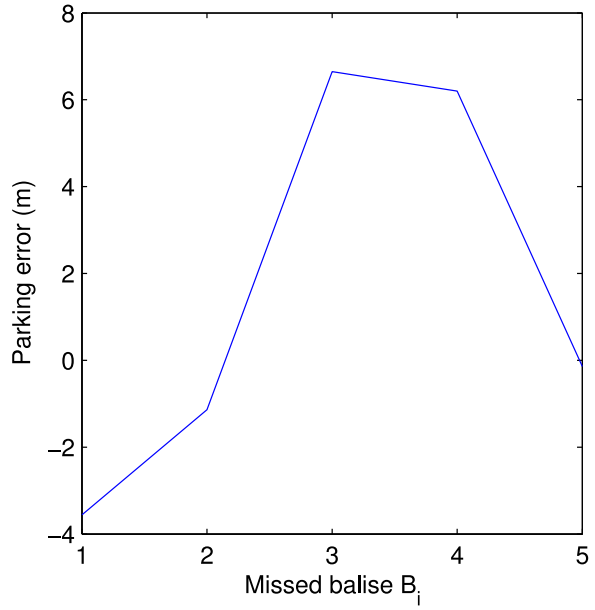

Fig. 17. Parking errors due to different balise missing.

B. Balise Missing Attack

To demonstrate the effectiveness of balise missing attack, the attacker will jam one balise such that the train misses its telegram information. In this case, the train will continue to run with the current control process after passing over the missing balise. Fig. 17 shows the parking error when a balise at different position is missed. It indicates that the parking error may be more than 2 meters in case of one balise missing, far beyond the allowable error 0.3 m in China and Korea. Especially, when balise B_3 is jammed to be missing, the parking curves in Fig. 18 show the erroneous parking position is 6.65 m away from the station platform, and the "stop" deceleration is -0.695 m/s^2 when the train speed is 0. Obviously, this attack is so successful that the train has to be re-started after "stop" in order to transfer the passengers to the destination station.

Furthermore, we carried on a simulation to jam two balises B_2 and B_3, the parking error is up to 9.46 m. This result is in

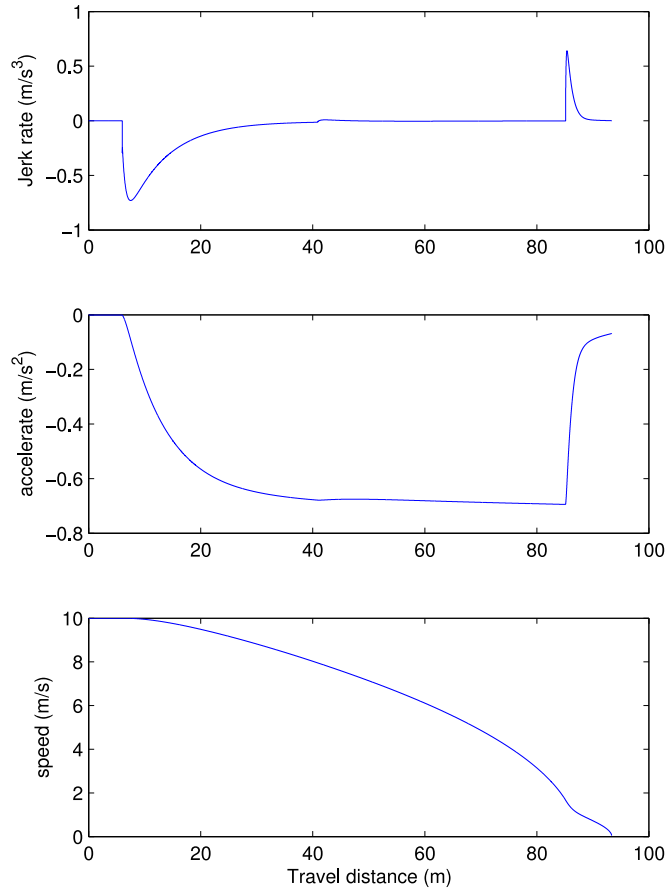

Fig. 18. Parking curves with jammed balise B_3.

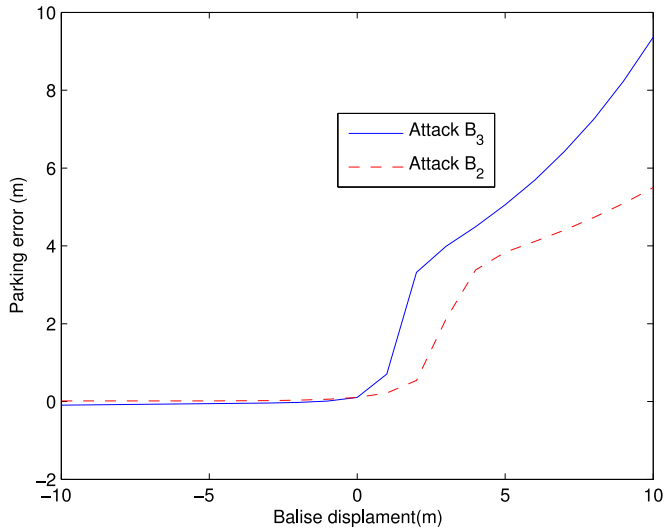

Fig. 19. Parking error vs the displacement of balise B_3.

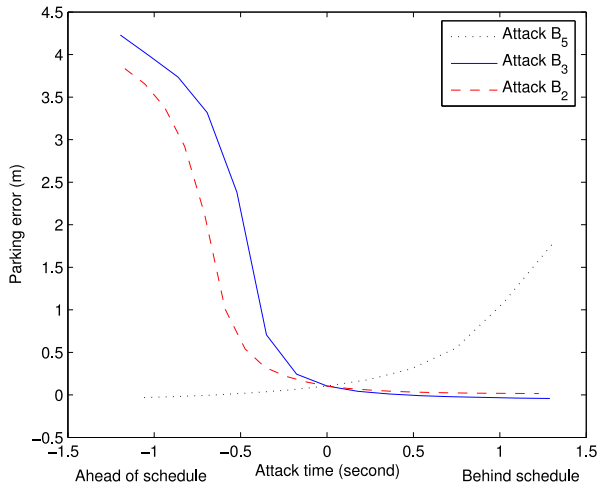

Fig. 20. Parking errors due to extended time for transmitting the telegram of the balises B_5, B_3 and B_2. Negative attack time (x-coordinate) means that the attack is started before the train passes over the balise, i.e., ahead of time.

concert with our intuition: The more the balises are jammed, the higher the parking error is.

C. Balise Displacement Attack

As introduced in Section IV-C, a displacement attack blocks a balise and then replays its telegram at a target position so as to control the deceleration update.

Fig. 19 shows the attack effect of different displacement, where the displacement is evaluated with displaced distance. When the attacked balise is closer to the platform, the attack effect is higher.

D. Transmission Extension Attack

In this attack, when a train is around a balise, the number of received telegrams is increased by extending the telepowering time or telegram replaying time. According to Section IV-D, the train will obtain a wrong balise passage time, and/or an erroneous balise position.

According to the introduction of balise in Section II-B, assume the length of balise telegram is 341-bit, the average bitrate is $b_r = 564.48$ kbps [17]. Thus a telegram transmission time is $T_x = 341/(564.48 \times 10^3) \approx 6 \times 10^{-4}$ s. When the extension time is 6 m $\times\ 10^{-4}$ seconds for m replayed telegrams, the position error can be estimated with (26) (or (28)) if the effective range R is known, or (27) (or (29)) when the train speed function $v(t)$ is known.

As an illustrative example, the balises are attacked by extending its telegram transmission time. Fig. 20 shows the attack effect. When the attacker replays the telegram of balise B_2 or B_3 before the train passes over the balise (i.e., ahead of schedule), the attack works well. Nonetheless, if he replays the telegram after the train passes over the balise B_5 (i.e., behind schedule), the parking error is small. The reason is as follows. When the attacker launches time extension attack on balise B_2 or B_3 for some time, he induces larger displacement if the attack time is ahead of schedule as the train moves fast. With reference to Fig. 19, larger displacement will result in higher parking error.

However, when an attacker performs the attack experiments on the balise B_5, the attack effect are different. As the train speed is almost constant when the train is localized around the balise B_5, i.e., the displacement distance is almost the same whether the attack time is ahead of schedule or behind schedule. But

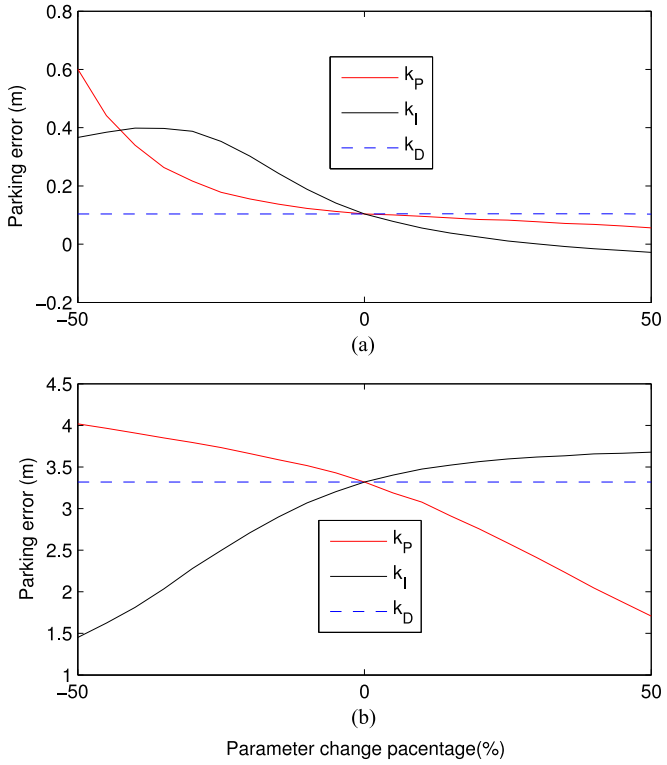

Fig. 21. Parking error vs. PID parameter. (a) No attack, (b) Balise B_3 displacement is 2 meters.

the train has only a short time to control the parking distance if the attack time is behind schedule, therefore the parking error is higher.

E. Parameter Sensitivity Analysis

As the controller is in the closed-loop system, its parameters will impact the system response. Naturally, the parameters will also impact the attack performance. With reference to Fig. 21(a), when there is no attack, we adjust the PID controller parameters (k_P, k_I, k_D) from -50% to 50% one by one. When the PID parameters become larger, parking accuracy becomes better. However, large PID parameters do not significantly reduce parking errors. However, as shown in Fig. 21(b), if we displace balise B_3 2 meters away, small integral parameter k_I or large proportional parameter k_P will the weaken the displacement attack. Hence, large proportional parameter is able to reduce the parking no matter whether the displacement attack is started. In other words, large proportional parameter k_P is preferable. Nonetheless, large proportional parameter may result in high jerk rate. For example, if the proportional parameter is 4 times the original one in [60], the parking error is decreased to 0.76 m from 3.32 m, but the jerk rate value will be increased to 0.918 m/s^3 from 0.724 m/s^3 when the Balise B_3 displacement is 2 meters. Hence, considering the restrictions on parking error (0.3 m) and jerk rate (0.75 m/s^3), it is difficult to defeat the attacks by tuning the PID parameters.

In the above simulations, we assume that Smith predictor knows the system delay τ exactly. In practice, this assumption

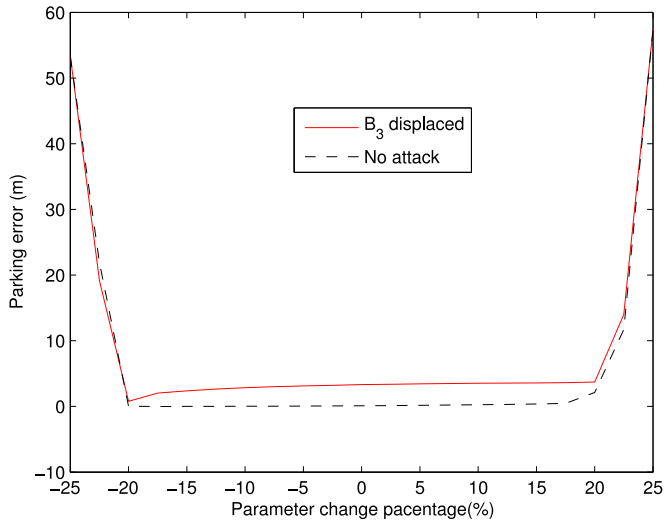

Fig. 22. Parking error vs. Smith predictor parameter. In the attack case, balise B_3 displacement is 2 meters.

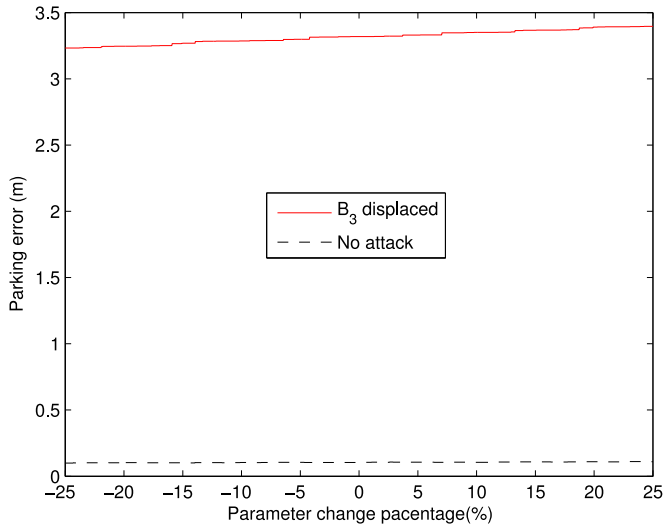

Fig. 23. Parking error vs. train braking parameter. In the attack case, balise B_3 displacement is 2 meters.

does not hold. Fig. 22 indicates that the change of parking error is small when Smith predictor parameter error varies within $[-10\%\tau, 10\%\tau]$ whether there is displacement attack or not. However, if the parameter error is large, the parking error will increase abruptly.

Furthermore, we performed simulations on the change of train braking parameter q. As shown in Fig. 23, the train time parameter does not have significant effect on the attack performance.

VII. Conclusions

Train automatic stop control is very important in ensuring accurate and friendly parking on subway station platforms. Inaccurate parking will cause great inconvenience to passengers, especially in those platforms installed with screen doors, while unfriendly parking such as emergency stop with high jerk rate may make passengers fall and even cause injury. However, as the

rail curvature and slope have impact on the station stop distance, the parking pattern varies with the stations, and can not be fixed.

In the current subway system, the balise/transponder communication subsystem plays a crucial role in offering accurate and friendly parking on stations. However, it is lack of cryptographic protection such that the train accepts any format-compliant balise telegram without any security verification. Thus, for the sake of security and safety, the BTM-balise communication protection needs to be improved.

This paper proposed three attacks to violate the parking requirements on accuracy and comfortability. By simply disturbing the BTM-balise channel, an attacker forces the train to obtain an erroneous balise location which is used in the parking control. As the attacks merely exploit the wireless property and do not require to tamper with the balise, they can be launched easily. The simulations demonstrated the effectiveness of the attacks. Additionally, four countermeasures were presented to defeat the attacks.

Due to the lack of access to subway infrastructure, we were not able to perform real attack experiments on the balises. Nonetheless, the simulation was based on a real subway line configuration and we hope that our results have shed some light on the importance of security and safety of public infrastructures.

ACKNOWLEDGMENT

The authors thank the insightful comments from anonymous reviewers. In particular, one reviewer suggested the fourth countermeasure.

REFERENCES

[1] "Public transport utilisation—Average daily public transport ridership," Land transport authority of Singapore. [Online]. Available: https://data.gov.sg/dataset/public-transport-utilisation-average-public-transport-ridership. Accessed on: Feb. 2, 2018.

[2] P. Mcgeehan, E. Rosenberg, and E. G. Fitzsimmons, "Hoboken train crash leaves at least one dead and dozens injured," The New York Times, Sep. 29, 2016. [Online]. Available: http://www.nytimes.com/2016/09/30/nyregion/new-jersey-transit-train-crash-hoboken.html?_r=0. Accessed on: Feb. 2, 2018.

[3] K. Sohn, "Optimizing train-stop positions along a platform to distribute the passenger load more evenly across individual cars," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 994–1002, Jun. 2013.

[4] H. Kim, S. Kwon, S. K. Wu, and K. Sohn, "Why do passengers choose a specific car of a metro train during the morning peak hours?" *Transp. Res. Part A, Policy Pract.*, vol. 61, pp. 249–258, 2014.

[5] ST Electronics, "Platform Screen Door (PSD)." [Online]. Available: https://www.stengg.com/en/products-solutions/psd. Accessed on: Feb. 2, 2018.

[6] W. M. Sim, M. Thong, and C. F. Chan, "Touch voltage protection on Singapore MRT system," in *Proc. Int. Conf. Power Eng.*, 2005, pp. 1–6.

[7] W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, W. H. Sanders, "On train automatic stop control using balises: Attacks and a software-only countermeasure," in *Proc. IEEE Pac. Rim Int. Symp. Dependable Comput.*, 2017, pp. 274–283.

[8] L. Ma and X. Zeng, "Analysis on train stopping accuracy based on regression algorithms," *J. Softw.*, vol. 9, no. 5, pp. 1237–1244, 2014.

[9] W. Liao, Y. Song, and W. Cai, "Traction/braking control design for high speed trains based on force estimation—An more implementable approach," in *Proc. Chin. Control Decis. Conf.*, 2014, pp. 4437–4442.

[10] X. Zhuan and X. Xia, "Optimal scheduling and control of heavy trains equipped with electronically controlled pneumatic braking systems," *IEEE Trans. Control Syst. Technol.*, vol. 15, no. 6, pp. 1159–1166, Nov. 2007.

[11] H. Dong, B. Ning, B. Cai, and Z. Hou, "Automatic train control system development and simulation for high-speed railways," *IEEE Circuits Syst. Mag.*, vol. 10, no. 2, pp. 6–18, Apr.–Jun. 2010.

[12] Q. Song, Y.-D. Song, T. Tang, and B. Ning, "Computationally inexpensive tracking control of high-speed trains with traction/braking saturation," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1116–1125, Dec. 2011.

[13] Y.-D. Song, Q. Song, and W.-C. Cai, "Fault-tolerant adaptive control of high-speed trains under traction/braking failures: A virtual parameter-based approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 2, pp. 737–748, Apr. 2014.

[14] J. Zuo, M. Wu, H. Peng, and Z. Chen, "Feedback control of pneumatic brake of urban railway train under ATO mode," in *Proc. Int. Conf. E-Product E-Serv. E-Entertainment*, 2010, pp. 1–4.

[15] Z. Xu, W. Wang, and Y. Sun, "Performance degradation monitoring for on-board speed sensors of trains," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1287–1297, Sep. 2012.

[16] ERTMS/ETCS, "Performance requirements for interoperability," SUBSET-041, ver. 3.1.0, Mar. 1, 2012.

[17] ERTMS/ETCS, "FFFIS for Eurobalise," SUBSET-036, ver. 3.0.0, Feb. 24, 2012.

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

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

[20] M. A. Sandidzadeh and A. Khodadadi, "Optimization of balise placement in a railway track using a vehiclean odometer and genetic algorithm," *J. Sci. Ind. Res.*, vol. 70, pp. 210–214, 2011.

[21] H. Wang, F. R. Yu, L. Zhu, T. Tang, and B. Ning, "A cognitive control approach to communication-based train control systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1676–1689, Aug. 2015.

[22] M. Heddebaut, "Leaky waveguide for train-to-wayside communication-based train control," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1068–1076, Mar. 2009.

[23] N. Zhang, X. Zhu, W. Ji, and G. Zheng, "An attempt of using leaky cable at 400MHz in CBTC system," in *Proc. IEEE Conf. Commun. Probl.-Solving*, 2014, pp. 95–98.

[24] V. A. Minin, V. A. Shishliakov, J. N. Holyoak, D. A. Johnston, and N. A. Lepsky, "Development of the communications-based train control system for Moscow Metro," in *Proc. IEEE/ASME Joint Conf. Railroad Conf.*, 1997, pp. 201–210.

[25] J.-h. Baek, "The study on train separation control & safety braking model technology using balise for conventional lines," in *Proc. Int. Telecommun. Energy Conf.*, 2009, pp. 1–4.

[26] J. Wang and Z. Lin, "Research on intelligent control strategy used in CTCS-3 train control system," in *Proc. IEEE Conf. Serv. Oper., Logist., Informat.*, 2011, pp. 447–450.

[27] K. Yoshimoto, K. Kataoka, and K. Komaya, "A feasibility study of train automatic stop control using range sensors," in *Proc. IEEE Conf. Intell. Transp. Syst.*, 2001, pp. 802–807.

[28] M.-T. Ha, C.-G. Kang, H.-Y. Kim, and T. H. An, "A precision stopping measurement device for data acquisition of urban trains," in *Proc. Int. Conf. Control, Autom. Syst.*, 2014, pp. 726–729.

[29] A. Lindgren, "A driverless control system for the Beijing Yizhuang metro line," KTH Electronic Engineering, Stockholm, Sweden, Tech. Rep. XR-EE-RT 2011:007, 2011.

[30] M. Zhang and H. Xu, "Adaptive PIQ stopping control of urban rail vehicle," in *Proc. Chin. Control Decis. Conf.*, 2013, pp. 7–12.

[31] 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.

[32] S. Gao, H. Dong, Y. Chen, B. Ning, G. Chen, and X. Yang, "Approximation-based robust adaptive automatic train control: An approach for actuator saturation," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 4, pp. 1733–1742, Dec. 2013.

[33] S. Yasunobu, S. Miyamoto, and H. Ihara, "A fuzzy control for train automatic stop control," *Trans. Soc. Instrum. Control Eng.*, vol. E-2, no. 1, pp. 1–9, 2002.

[34] Z. Hou, Y. Wang, and C. Yin, "Terminal iterative learning control based station stop control of a train," *Int. J. Control*, vol. 84, no. 7, pp. 1263–1274, 2011.

[35] Q. Song and Y.-D Song, "Data-based fault-tolerant control of high-speed trains with traction/braking notch nonlinearities and actuator failures," *IEEE Trans. Neural Netw.*, vol. 22, no. 12, pp. 2250–2261, Dec. 2011.

[36] L. Harding and M. Tran, "Moscow metro bombs kill dozens," Mar. 29, 2010. [Online]. Available: https://www.theguardian.com/world/2010/mar/29/moscow-metro-bombs-explosions-terror. Accessed on: Feb. 2, 2018.
[37] C. Semet, P. Meganck, R. Gabillard, R. Lardennois, and D. Minesi, "Feasibility and security for a new automatic train localization system by electronic beacon," *Proc. IEEE Veh. Technol. Conf., Mobile Technol. Human Race*, 1996, vol. 3, pp. 1604–1608.
[38] F. Bu and H.-S. Tan, "Pneumatic brake control for precision stopping of heavy-duty vehicles," *IEEE Trans. Control Syst. Technol.*, vol. 15, no. 1, pp. 53–64, Jan. 2007.
[39] Alstom.com, "Singapore Northeast Line: Will soon be the largest, fully automatic metro system in the world." [Online]. Available: www.tsd.org/cbtc/projects/SIG_Singapore_AutomaticMetro_en.pdf. Accessed on: Feb. 2, 2018.
[40] M. Fitzmaurice, "Wayside communications—CBTC data communications subsystems," *IEEE Veh. Technol. Mag.*, vol. 8, no. 3, pp. 73–80, Sep. 2013.
[41] 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.
[42] *IEEE Guide for the Calculation of Braking Distances for Rail Transit Vehicles*, IEEE Std 1698-2009, C1-31, 2009.
[43] Y. Wu, B. Qiu, Z. Wei, and J. Weng, "Secure subway train-to-train communications via GSM-R communication systems," in *Proc. IEEE Veh. Technol. Conf.*, 2016, pp. 1–6.
[44] F. Lu and M. Song, "Subway train motion modeling and the event-based optimal control," in *Proc. IEEE Conf. Ind. Electron. Appl.*, 2006, pp. 1–6.
[45] Y. Wu, J. Weng, Z. Tang, X. Li, and R. H. Deng, "Vulnerabilities, attacks, and countermeasures in balise-based train control systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 4, pp. 814–823, Apr. 2017.
[46] 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 Pac. Rim Int. Symp. Dependable Comput.*, 2017, pp. 274–283.
[47] 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 Int. Conf. Broadband Netw. Multimedia Technol.*, 2013, pp. 174–180.
[48] A. Leow, "Expect Circle Line delays for the 4th straight day: LTA, SMRT," The Straitstimes, Sep. 1, 2016. [Online]. Available: http://www.straitstimes.com/singapore/transport/expect-circle-line-delays-for-the-4th-straight-day-lta-smrt. Accessed on: Feb. 2, 2018.
[49] 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.
[50] 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.
[51] B.-W. Jo, J.-H. Park, and K.-W. Yoon, "The experimental study on concrete permeability of wireless communication module embedded in reinforced concrete structures," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 6, Jan. 2013, Art. no. 520507.
[52] A. Ghasemi, A. Abedi, and F. Ghasemi, *Propagation Engineering in Wireless Communications*, 2nd ed. Cham, Switzerland: Springer, pp. 26–27, 2016.
[53] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjorungnes, *Game Theory in Wireless and Communication Networks: Theory, Models and Applications*. New York, NY, USA: Cambridge Univ. Press, U.K., p. 15, 2011.
[54] ERTMS/ETCS, "System requirements specification chapter 7: ERTMS/ETCS language," SUBSET-026-7, v.3.4.0, May 12, 2014.
[55] X. Liu, Z. Sun, and H. He, "On-road vehicle detection fusing radar and vision," in *Proc. IEEE Conf. Veh. Electron. Safety*, 2011, pp. 150–154.
[56] R. Shenton, "Video train positioning," in *Proc. IRSE Aust. Tech. Meeting*, 2011, pp. 1–8.
[57] Reliable Data Systems International, Ltd., "Video train positioning system." [Online]. Available: http://www.rdsintl.com/train-positioning-system/2-video-train-positioning-system/. Accessed on: Feb. 2, 2018.
[58] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, pp. 197–215, 2014.
[59] H. Wang, L. Zhang, T. Li, and J. Tugnait, "Spectrally efficient jamming mitigation based on code-controlled frequency hopping," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 728–732, Mar. 2011.
[60] K. Li and J. Yin, "Heuristic algorithms for train station parking using information of transponders," *TELKOMNIKA Indonesian J. Elect. Eng.*, vol. 12, no. 2, pp. 1320–1326, 2014.

Yongdong Wu received the B.Eng. and M.S. degrees from Beihang University, Beijing, China, the Ph.D. degree from the Institute of Automation, Chinese Academy of Science, Beijing, China, and the Master for Management of Technology from the National University of Singapore, Singapore.

He is currently a Senior Scientist with Infocomm Security Department, Institute of Infocomm Research (I^2 R), Agency for Science Technology and Research (A*STAR), Singapore. His research interests include cyber-physical system security, IoT security, multimedia security, and network security. He has authored or coauthored more than 100 papers, and 7 patents. He is an Associate Editor for the *International Journal of Security and Communication Networks*, as well as *Security and Communication Networks*, and was a Program Co-Chair of the 11th International Conference on Information Security Practice and Experience in 2015.His research results and proposals was incorporated in the ISO/IEC JPEG 2000 security standard 15444-8 in 2007. He was the recipient of the Best Paper Award of IFIP Conference on Communications and Multimedia Security 2012. He was awarded by China-Singapore Joint Research Programme, National Research Fund, Singapore, and Energy Management Agency, Singapore.

Zhuo Wei received the B.A. degree from Jilin University, Changchun, China, and the M.S. and Ph.D. degrees from the Huazhong University of Science and Technology, Wuhan, China. He is currently a Research scientist with Huawei International Company, Singapore. His research interests include vehicle security and privacy, multimedia security, image processing, and video processing. He was the recipient of the Best Paper Award of CMS 2012.

Jian Weng received the Ph.D. degree from Shanghai Jiaotong University, Shanghai, China, in 2008. He is currently a Professor and an Executive Dean with the School of Information Technology, Jinan University, Guangzhou, China. He has authored or coauthered more than 60 papers in cryptography conferences and journals including CRYPTO, EUROCRYPT, TCC, ASIACRYPT, etc. He 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.

Robert H. Deng (F'16) is currently the AXA Chair Professor of Cybersecurity, the Director of the Secure Mobile Centre, and the Dean of Postgraduate Research Programmes, Singapore Management University (SMU), Singapore.

He has 26 patents and has authored or coauthored more than 300 papers on cybersecurity. His research interests include data security and privacy, cloud security, and Internet of things security. He was the recipient of the Outstanding University Researcher Award from the National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence from SMU, and Asia-Pacific Information Security Leadership Achievements Community Service Star from International Information Systems Security Certification Consortium.

His professional contributions include Editorial Boards of the IEEE SECURITY & PRIVACY MAGAZINE, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *Journal of Computer Science and Technology*, and the Steering Committee Chair of the ACM Asia Conference on Computer and Communications Security, etc.