Hindawi
Security and Communication Networks
Volume 2022, Article ID 1781757, 19 pages
https://doi.org/10.1155/2022/1781757

Research Article

A Novel Approach for Estimating Performance of IIoT-Based Virtual Control Train Sets under DoS Attacks

Shuomei Ma,[1] Hongwei Wang,[2] Zhu Li,[1] and Qihe Zhang[1]

[1]State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China
[2]National Research Center of Railway Safety Assessment, Beijing Jiaotong University, Beijing 100044, China

Correspondence should be addressed to Shuomei Ma; 18111055@bjtu.edu.cn

Received 14 July 2022; Revised 2 August 2022; Accepted 22 August 2022; Published 30 September 2022

Academic Editor: Chen Chen

The virtually coupled train sets (VCTS) have been proposed to improve operational capability and passenger satisfaction and ensure punctuality, thus alleviating the rapidly worsening traffic pressure. Recently, due to the lack of reliable wireless communications and accurate perceptual information, VCTS based on industrial internet of things (IIoT) are receiving growing concerns by integrating into the IIoT, AI, and edge computing. However, denial of service (DoS) attacks are feasible for IIoT-based VCTS due to the physically exposed open electromagnetic environment. They would cause severe safety and punctuality problems, such as poor real-time capability, enormous packet dropout rates, extensive train operational delays, and disturbance in the train convoy's dynamic schedule. This paper deeply discusses the effects of DoS attacks on the performances of the IIoT-based VCTS by combing the physical layer with the cyber layer and explores the requirement of an attacker. We consider that the system is under the attack of a rational DoS attacker with limited jamming attacks, which will cause the most system state offset. In the paper, we propose a novel train status estimation approach to compensate for the losing information of the front train by the trade-off between the best gain of the DoS attacker and the punctuality of the IIoT-based VCTS. System performance includes physical dynamic indicators, train operational delay variance, and average waiting time of passengers. Taken together, these findings indicate that the established status estimation approach can effectively mitigate safety concerns and reduce train operational delays.

1. Introduction

The concept of the virtual control train set (VCTS) has received increasing attention as an indicator of the future railway signaling system within the past years. VCTS employs bidirectional wireless data communication to ensure the safety operation of the rail transport and couples two neighbor trains with relative braking distance to increase the transportation capacity and the flexibility of railway organization, rather than the current traditional communication system AND communication-based train control (CBTC) system [1–3]. The physical coupler is cancelled between adjacent trains in the VCTS for meeting the distribution of passengers by making the density of trains. Train members of VCTS have stringent requirements for reliability of wireless communications and the timeliness for supporting the autonomy of a train convoy, which is the same as the unmanned aerial vehicles (UAVs) and classified as a typical industrial Internet of things (IIoT) [4]. With the development of IIoT, an IIoT-based VCTS is proposed in the article based on the popular communication-based train control architecture [2].

In the knowledge of this new IIoT-based VCTS, all trains generate a long virtual train, known as a train convoy or train platoon [2]. Flammini et al. [5] introduced VCTS and presented requirements, which had a tight coupling relationship with the stability of the train convoy, for safety. Quaglietta et al. [6, 7] introduced the need for additional safety constraints, especially at diverging junctions, and presented the train operation's model under ETCS level 3 and virtual coupling. Members of VCTS can be recoupled and decoupled automatically according to transportation demands and plans based on train-to-train (T2T) wireless communications [5]. However, this system is prone to several security threats, especially crucial safety requirements of the train convoy, owing to the fact that it works under an open electromagnetic environment and the common unlicensed band [8, 9]. The allowable minimum relative braking distance between adjacent trains in VCTS would be violated. If DoS attacks were not mitigated, this violation could bring packet loss and time delay and disturb the train convoy operation.

Current studies of VCTS mainly focus on principles and control strategies for improving the efficiency of a train convoy operation. Di Meo et al. [10] assume to enrich ERTMS with virtual coupling instead of defining a fully new signaling system, which is the preferred approach to ensure backward compatibility and minimize the impact on existing infrastructures since it guarantees the reuse of standard operating modes and related safety mechanisms. Felez et al. [11] proposed an MPC approach to reduce the impact of time delays on the operation performance of the train convoy, thus ensuring its safety and stability. Reference [12] has proposed the concept of VCTS and requirements of safety especially for the stability of a train convoy's achievement with a tight coupling relationship of a series of trains. In addition, a smarter and efficient railway system could be achieved by integrating with IIoT, AI, 5G, big data analysis, and edge computing [2, 13]. However, with the continuous advance of the transportation intelligent construction tide, the security of wireless communications is starting to become powerless, especially in terms of large information flows in IIoT-based VCTS [14]. Therefore, DoS attacks are feasible for IIoT-based VCTS due to the unreliability of T2T communications [15], which are ignored in the current study.

The IIoT-based VCTS can be considered a cyber-physical system (CPS) [14]. Its physical layer, which represents the train control system, ensures the safety and the efficiency of the train convoy operation, whereas the cyber layer represents the wireless communication system. Functionally, wireless communication predisposes the system to cyberattackers, who interfere with the train convoy operation schedule, while interference with the transmission of controller command poses security risks during train convoy operations. In the IIoT-based VCTS, a key feature of train convoy operation safety is that the following train can track the trajectory of the one in front while maintaining a known headway distance. Notably, trains are required to abruptly uncouple all members of a train convoy and apply emergency brakes, if this communication is tampered with, a phenomenon that has been associated with disruption of train scheduling and leaving passengers stranded. Therefore, the development of an efficient method for preventing the need for the application of emergency brakes and ensuring the ideal headway distance within unreliable wireless communications, caused by cyberattacks, is significant for the safety and efficiency of a train convoy in the IIoT-based VCTS [16].

To date, various conventional cryptography technologies and intrusion detection systems (IDS) have been developed with the aim of mitigating the impact of cyberattacks [17, 18]. Consequently, these approaches have played a significant role in the defense strategies of the conventional international system. In addition, previous studies have explored the potential for the data network [19], deep reinforcement learning [20], and the blockchain [21] in mitigation of the impact of DoS attacks. Reference [22] has proposed an online intrusion detection cloud system to detect and filter malicious attack with the new spiking neural network architecture called the NeuCube algorithm. Reference [23] has introduced context-aware security (ConSec) protocol to support internet of things applications to reduce the latency while encrypting and decrypting the applications. However, the above literature on cloud computing technology has perpetuated the huge computing flows and data circulation through the Internet; they are insufficient to meet the security challenge of VCTS system, due to the combination of the cyber layer performance with the physical dynamic.

Currently, many studies have applied analyses of the effects of cyberattacks on the network control system (NCS), a type of CPS, to explore the performance of the cyber layer in combination with the physical dynamics [24]. Reference [25] explores a min-max cost-optimal problem to guarantee the convergence rate of federated learning in terms of cost in wireless edge networks. A status estimation approach was proposed in the cyber-physical system (CPS) to ensure the stability of the vehicle platoon under unreliable wireless communication. Reference [26] proposed a linear deception attack strategy and presented the corresponding feasibility constraint on the optimal attack strategy among all linear attacks, while [27] explored the potential for remote status estimation of CPS based on the game-theoretic approach under DoS attacks.

Moreover, in contrast to the Internet and the CPS, the challenge experienced by the defense system in the IIoT-based VCTS comprises a combination of packet losses (i.e., cyber layer), train dynamic operation, and stranded passengers (i.e., physical layer). Recently, some security field studies have developed defense methods from an attacker's point of view [28], which are based on the fact that combining an attacker's strategy and defense method effectively simulates the actual subway environment and explores the performance of DoS attacks under energy limits, which are found that attacks were random and irregular, albeit with a limited sum of attack energy is limited. These methods are shedding new light on the challenge of the defense system in the IIoT-based VCTS. Results from analyses of the energy constraint indicated that an optimal attack strategy causes the most significant effect on wireless communication and packet losses, thereby causing a train to make frequent emergency braking. The study thus adopts the status estimation approach based on the optimal attack strategy to improve estimator accuracy.

In the IIoT-based VCTS, the development of an efficient method for preventing the need for application of emergency brakes is urgently needed to ease traffic jam on the railway. DoS attacks have been shown to be possible attacks that can negatively affect the physical performance of the

IIoT-based VCTS since they target wireless communications [29, 30]. In fact, an intelligent DoS attacker can reduce the signal-to-interference-plus-noise ratio (SINR) of the wireless communication channels, a phenomenon that results in a low packet arrived ratio, and ultimately cause serious train accidents [31]. DoS attacks on the IIoT-based VCTS not only significantly interfered with the wireless communication between the AP and the train but also resulted in frequent packet losses and ultimately the safety and congestion of the transportation owing to the uncoupling of the train convoy and emergency braking by trains.

In the present study, we propose a train status estimation approach for developing a defense against the IIoT-based VCTS during DoS attacks that adopts an optimal attack strategy with an evaluation, which is based on the physical layer performance (physical dynamic) and the cyber layer performance (signal-to-interference-plus-noise ratio (SINR)), is adopted. The train status estimation approach is used to compensate for the status information (i.e., position, velocity, and acceleration) of the front train under DoS attacks. Notably, this study makes the following main contributions:

(i) We propose a train status estimation approach combing the enhanced Kalman filtering with the optimization, the gain of the attacker, and the solution of a Markov stochastic process to mitigate the frequency of emergency braking in the decoupling mode of the IIoT-based VCTS and compensate for the gap of packet losses caused by DoS attacks. The analysis procedure of the enhanced Kalman filtering method provides new ideas for solving the estimation error covariance matrix during unreliable wireless communication while can be generalized to other CPS.

(ii) We consider the IIoT-based VCTS is under the attack of a rational DoS attacker with limited jamming attacks, which will cause the most system state offset. When these attacks happen, the mode of train convoy would decouple by the "fail-safe" rule, but it cannot avoid the eventual traffic jam of the urban transit and enormous packet dropout in the process of T2T communication. To simulate the actual attack environment and improve the accuracy of the train status estimation approach, we consider a trade-off between the best gain of the attacker and the punctuality of the train convey set, which has been decoupled for safety.

(iii) Criterion indicators for evaluating the performance of the status estimation approach are defined. The evaluation principle combines performances across wireless communication, physical dynamics (train speed/distance profile), and passenger satisfaction (train operational delay and passenger waiting time).

The rest of the paper is organized as follows. The framework of the IIoT-based VCTS and the impacts of DoS attacks on the IIoT-based VCTS are proposed in Section 2. Section 3 involves the system model and problem formulation, and Section 4 describes the train status estimation approach based on the optimal attack strategy In Section 5, the evaluation criterion of the effects of DoS attacks on the IIoT-based VCTS system is presented. Section 6 demonstrates the simulation results and discussions. Finally, we conclude this study in Section 7.

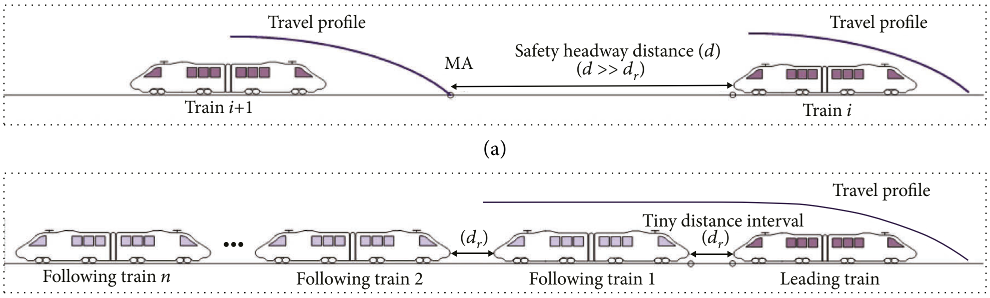
2. Framework of the IIoT-Based VCTS and Impacts of DoS Attacks on the IIoT-Based VCTS

In this section, VCTS is first outlined. Based on the principles of VCTS, a novel structure of the IIoT-based VCTS-based train-centric is proposed, and the effects of jamming attacks on T2T communication are analyzed.

2.1. Overview of Virtual Coupling. Virtual coupling will be a significant feature of the future railway system [6, 7] that can improve the capacity and efficiency of transportation to deal with the forecasted growth of traveling demands. Figure 1 shows the contrast between the traditional moving block (MB) and the virtual coupling. In MB mode, the zone controller (ZC) can monitor the running status of the train and generate train control commands called movement authority (MA) of trains. Generally, MA is defined as the location of the nearest obstacle, which is related to the braking headway distance of trains, including trains, turnouts, and signals.

Additionally, virtual coupling increases the density of trains, which means that the interval between adjacent trains of a formation is much smaller. When trains are coupled via T2T communications, the train movement depends on the status of adjacent trains, including their acceleration, velocity, and position, through onboard sensors and wireless communication modules. In this study, the first train in the train convoy is called the leading train. The control strategy of each following train is also optimized with the approach so that its velocity and acceleration are the same as the last known information of the leading train. When trains are within virtual coupling, IIoT-based VCTS aims to provide a controlling strategy to ensure that each position difference between the ahead train and its following train is close to the objective relative braking distance [32]. In addition, IIoT-based VCTS prefers a train-centric control system, which is different from the traditional MB. One of the challenges for the IIoT-based VCTS is how to meet the high mobility and efficiency of virtually coupled via T2T wireless communications by facility designing and ensure the safety and joint security of VCTS operations. The next subsection presents a new framework of the IIoT-based VCTS.

2.2. A Novel Framework of the IIoT-Based VCTS. This section shows a novel framework of the IIoT-based VCTS based on T2T communications, as illustrated in Figure 2. The proposed structure consists of a control center subsystem, an onboard subsystem, and a trackside subsystem. Onboard



(a)

(b)

Figure 1: Moving block versus virtual coupling: (a) moving block and (b) virtual coupling.

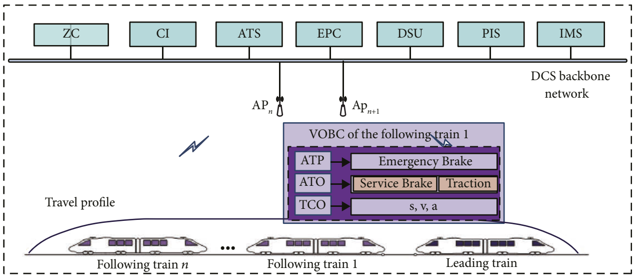


Figure 2: Structure of the IIoT-based VCTS.

subsystems include automatic train protection (ATP), automatic train operation (ATO), and train cooperative controller (TCO). Through the co-work of computer interlock (CI), data storage unit (DSU), and evolved packet core (EPC), zone controller (ZC), operation plans, and the running state of subway lines can be transmitted to trains. Moreover, a cooperative controller is designed to operate the train in the virtual coupling mode. Through T2T wireless communications, TCO can provide optimal control strategies for trains according to velocities and locations of adjacent trains. Additionally, ATP can be secured based on the overall running state of the whole line, which signifies that T2T communications are essential to provide low-latency and high-capacity information exchange among members of a train convoy in the IIoT-based VCTS. When T2T communication links fail or the velocities of trains exceed the limiting speed of ATP, an emergency train braking is executed. In this study, the access point (AP) and customer premises equipment (CPE) of the IIoT-based VCTS via T2T communication links of adjacent trains are established by long-term evolution for metros (LTE-M). The CPE exchanges the status information of train i with RRU and other trains via the T2T communications link [33]. Clearly, T2T communications play an essential role in the IIoT-based VCTS. Therefore, the mechanism is necessary to avoid collisions in T2T communications under unpredictable disturbances.

2.3. Impacts of DoS Attacks on the IIoT-Based VCTS. Generally, attackers can send enormous jamming traffics or fake bits to exhaust the frequency bandwidth, channel capacity, and legitimate communication services. Figure 3 illustrates the comparison of the IIoT-based VCTS and the effects of jamming attacks on the IIoT-based VCTS. In a train convoy, the leading train communicates with the control center via the train-ground (T2G) communications. When the interruption time caused by jamming attacks on T2G is significantly larger than the preset value, the leading train must implement emergency braking. When jamming occurs in T2T communications, the stability of members in a train convoy will be disturbed. Due to the high speed and the tiny interval, jamming may cause safety risks or running as decoupled trains belonging to MB mode.

The security of IIoT-based VCTS, as a new technology in urban rail transit, is a severe challenge because it is more vulnerable to jamming attacks than before [33]. This subsection aims to analyze the constraints of jamming attacks. Considering the distance from the attacker to the victim node, jamming attacks can be classified as constant jamming, deceptive jamming, and reactive jamming [34]. In this study, the effects of constant jamming on T2T for the IIoT-based VCTS are mitigated by the resilience control approach with the ETC condition. In the next section, we will analyze the dynamic model of the train convoy and the indicators of the safety operations of VCTS.

3. System Model and Problem Formulation

In this section, we propose a dynamic control module when trains are coupled. The physical dynamic model for the IIoT-based VCTS also is presented to improve the train operation safety if the train convoy is decoupled caused by DoS attacks. In addition, we also design a cost function to provide a theoretical basis for the train status estimation approach.

3.1. Dynamic Model of the Train Convoy. For the IIoT-based VCTS, stability means that distance intervals between adjacent trains are almost the same while suggesting that all trains are running at the same speed. An objective relative safety distance exists between adjacent trains for optimal performance. The status formulae of the leading train and other trains can be given by

$$\dot{x}_l(t) = A_c x_l(t) + C_c W(t), \tag{1a}$$

$$\dot{x}_i(t) = A_c x_i(t) + B_c u_i(t), \tag{1b}$$

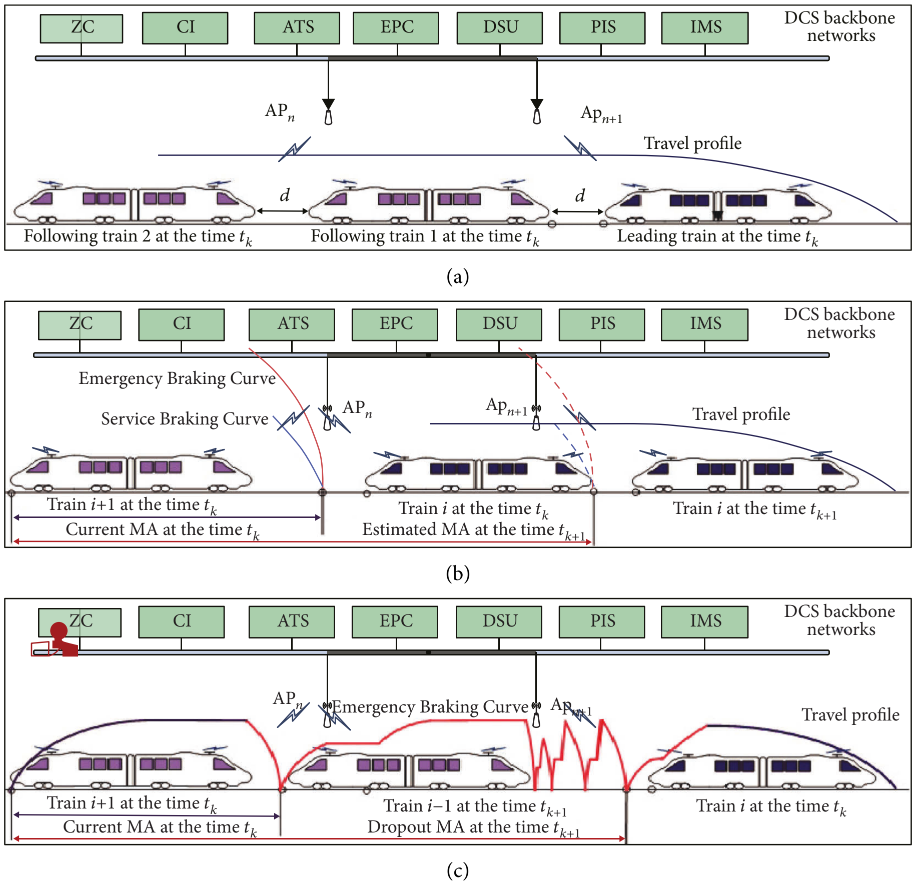

ZC
CI
ATS
EPC
DSU
PIS
IMS
DCS backbone networks
AP_n
Ap_{n+1}
Travel profile
d
d
Following train 2 at the time t_k
Following train 1 at the time t_k
Leading train at the time t_k
(a)
ZC
CI
ATS
EPC
DSU
PIS
IMS
DCS backbone networks
Emergency Braking Curve
Service Braking Curve
AP_n
Ap_{n+1}
Travel profile
Train i+1 at the time t_k
Current MA at the time t_k
Train i at the time t_k
Estimated MA at the time t_{k+1}
Train i at the time t_{k+1}
(b)
ZC
CI
ATS
EPC
DSU
PIS
IMS
DCS backbone networks
AP_n
Emergency Braking Curve
Ap_{n+1}
Travel profile
Train i+1 at the time t_k
Current MA at the time t_k
Train i−1 at the time t_{k+1}
Dropout MA at the time t_{k+1}
Train i at the time t_k
(c)

Figure 3: The impacts of jamming attacks on the IIoT-based VCTS: (a) virtual coupling mode in the IIoT-based VCTS, (b) decoupling trains in the IIoT-based VCTS, and (c) impacts of DoS attacks on the IIoT-based VCTS.

where $x_i(t) = [s_i(t), v_i(t), a_i(t)]^T$ is the train running status information; $W(t)$ denotes the matrix of the resistance force, which subtracts the sum of traction and braking force at times t; $u_i(t)$ is the control law based on ETC that will be proposed in Section 3; A_c is the status matrix; B_c is the control matrix; and C_c is the noise and disturbance matrix, which can be calculated by kinematic equations.

A dynamical model of IIoT-based VCTS is established by applying the cooperative adaptive cruise control (CACC), which can avoid collisions according to the sacrificial part of system performance to ensure the safety and stability of the VCTS system when jamming attacks happen. The details can be founded on our previous work [3]. However, concerning the unreliable wireless communications caused by DoS attacks in the IIoT-based VCTS, the stability condition of the train convoy would be violated. As a result, the train convoy is decoupled after the control command. The physical dynamic model of the IIoT-based VCTS is presented in the next subsection, where the train convoy is decoupled.

3.2. Physical Dynamic Model of the IIoT-Based VCTS on the Impacts of DoS Attacks.

Due to the consensus about the “fail-safe” rule, which means that all techniques in the signaling control system of railways are needed for following the safety and avoiding collision between adjacent trains at the expense of efficiency and punctuality of the transportation, the passengers’ waiting time and traffic paralysis are even. Concerning the DoS attacks, the train convoy would be decoupled [6]. The physical dynamic model of the IIoT-based VCTS is presented in the subsection if the train convoy is decoupled caused by DoS attacks.

In the physical dynamic model of the IIoT-based VCTS, the control objective such as status information plays a significant role in ensuring safety for the operation of trains if the train convoy is decoupled caused by DoS attacks. In the study, the train status information, including the location, speed, and acceleration of the train is defined as follows:

$$x(t) = \left[\, S(t) \;\; V(t) \;\; \widehat{A}(t) \,\right]^T, \tag{2a}$$

$$S(t) = \left[\, s_1(t) \;\; s_2(t) \;\; \ldots \;\; s_n(t) \,\right]^T, \tag{2b}$$

$$V(t) = \left[\, v_1(t) \;\; v_2(t) \;\; \ldots \;\; v_n(t) \,\right]^T, \tag{2c}$$

$$\widehat{A}(t) = \left[\, a_1(t) \;\; a_2(t) \;\; \ldots \;\; a_n(t) \,\right]^T, \tag{2d}$$

where $x(t)$ represents the status information matrix of trains at time t; $S(t)$ represents the position matrix of trains at time t; $V(t)$ represents the speed matrix of trains at time t; $\widehat{A}(t)$

denotes the acceleration matrix of trains at time t; $s_i(t)$ and $v_i(t)$ represent the position and speed of train i at time t, respectively; $a_i(t)$ represents the acceleration of time at time t; and n indicates the number of trains.

Moreover, according to kinematic equations, we can write the status information of train i as follows:

$$s_i(t_k) = s_{i-1}(t_{k-1}) - L_{l,i} - L_s + v_i(t_{k-1}), \tag{3a}$$

$$+\left[a_i(t_{k-1}) + \frac{\kappa_i(t_{k-1}) - w_i(t_{k-1})}{M}\right]h, \tag{3b}$$

$$v_i(t_k) = v_i(t_{k-1}) + \left[a_i(t_{k-1}) + \frac{\kappa_i(t_{k-1}) - w_i(t_{k-1})}{M}\right]h, \tag{3c}$$

$$a_i(t_k) = a_i(t_{k-1}) + \left[\frac{\kappa_i(t_{k-1}) - w_i(t_{k-1})}{M}\right]h, \tag{3d}$$

where $L_{l,i}$ indicates the length of train i, h is the T2T communication cycle of the IIoT-based VCTS, L_s denotes the minimum safe distance between adjacent trains, κ_i indicates the resistance force of train i train i at time t_{k-1}, $w_i(t_{k-1})$ indicates the sum of traction and braking force of train i at time t_{k-1}, t_k represents the beginning of the k^{th} communication cycle, and M represents the mass of the train.

Due to the decoupling of the train convoy, the operation of train i is described using a linear system, for each member of the train convoy, as follows:

$$x(t_k) = Ax(t_{k-1}) + Bu(t_{k-1}) + w_e(t_{k-1}), \tag{4}$$

where $x(t_k) = [x_1(t_k), x_2(t_k), \ldots, x_n(t_k)]^T$, $x_i(t_k) = [s_i(t_k), v_i(t_k), a_i(t_k)]^T$ indicates the status information of the train i at time t_k, $u(t_k) = [u_1(t_k), u_2(t_k), \ldots, u_n(t_k)]^T$, $u_i(t_k)$ indicates the input of the controller, and A and B denote the known matrixes with compatible dimensions. A and B can be designed as follows, and the pair (A, B) is stabilized:

$$\begin{gathered}
A = blk\ di\ ag[A_1, A_2, \ldots, A_n],\\
B = blk\ di\ ag[B_1, B_2, \ldots, B_n],\\
A_1(t) = A_2(t) = \cdots = A_n(t) = \begin{bmatrix} 1 & h & \frac{1}{2}h^2 \\ 0 & 1 & h \\ 0 & 0 & 1 \end{bmatrix},\\
B_1(t) = B_2(t) = \cdots = B_n(t) = \begin{bmatrix} \frac{1}{2}h^2 \\ h \\ 1 \end{bmatrix}.
\end{gathered} \tag{5}$$

The observation equation is expressed as follows:

$$y(t_k) = Cx(t_k) + v_e(t_{k-1}), \tag{6}$$

where

$$\begin{aligned}
y(t_k) &= [y_1(t_k), \ldots, y_n(t_k)]^T,\\
w_e(t_k) &= \left[w_{e,1}(t_k), \ldots, w_{e,n}(t_k)\right]^T,\\
v_e(t_k) &= \left[v_{e,1}(t_k), \ldots, v_{e,n}(t_k)\right]^T,
\end{aligned} \tag{7}$$

where $w_{e,i}(t_k) \sim (0, R)$ and $v_{e,i}(t_k) \sim (0, N)$ represent the process noise and the measurement noise, respectively. Both parameters are independent Gaussian distributions with zero mean and error covariance. In addition, Q indicates the process noise covariance matrix, whereas R and $C = [1, 0, 0]$ denote the measurement noise covariance matrix and the observation matrix, respectively.

When the train convoy is decoupled, the mathematical expression of the control strategy for train i, under DoS attacks at time t_k, is shown as follows:

$$x_i(t_k) = \begin{cases} x_i(t_k), & \vartheta(t_k) = 1,\\ \hat{x}_i(t_k), & \vartheta(t_k) = 0, \end{cases} \tag{8}$$

where $\hat{x}_i(t_k)$ denotes the estimation status information of the front train at time t_k and $\vartheta(t_k) = 1$ implies that train i's status information is transmitted successfully under DoS attacks, whereas $\vartheta(t_k) = 0$ indicates transmission failure.

For the above analyses, the MA can be expressed as follows:

$$lm(t_k) = Dy(t_k) + L, \tag{9}$$

where $lm(t_k) = [lm_1(t_k), lm_2(t_k), \ldots, lm_n(t_k)]^T$, $L = [L_1, L_2, \ldots, L_n]^T$, $L_i = L_{l,i} + L_s$ indicates the sum of the length of train i and the safety margin, and $D = \begin{bmatrix} 0 & 0 \\ I_{n\times n} & 0 \end{bmatrix}$.

The physical dynamic model of the IIoT-based VCTS is prone to mitigate traffic paralysis and is adjusted by sacrificing part of the system performance to ensure the safety and punctuality of the IIoT-based system when DoS attacks happen. In addition, we assumed that the IDS of the IIoT-based system has high precision and detection methods for DoS attacks. Although previous studies have employed several detection methods, such as [35], none of these is discussed in the current study.

3.3. Problem Formulation. DoS attackers intend to intercept and prevent legitimate T2T communication services for legitimate APs. Generally, they achieve this by sending enormous wrong information traffic and by exhausting the wireless network bandwidth or abrogating the connection capacity [36]. DoS attacks on the wireless communication system affect the T2T and T2G communications because members of the train convoy can no longer receive accurate status information during each communication cycle. Communication delays of the IIoT-based VCTS after decoupling are randomly caused by DoS attacks. Therefore, a novel train status information estimation approach is constructed to improve the performance of the IIoT-based

VCTS system during DoS attacks. The accuracy of the estimation approach depends on the minimum estimate error, which forms the basis of the cost function reported in the current study [12]. This is expected to be circumventing the challenges associated with unreliable T2T and T2G communications. In order to improve the accuracy of the train status estimation, the IIoT-based VCTS performance requirement needs to be combined with the attack strategy from the attacker's perspective. Due to random communication delays, we define the cost function with the aim of improving the accuracy of the train status estimation approach, with a focus on the optimal attack strategy from an attacker's standpoint. The study hypothesized that DoS attacks follow a Bernoulli distribution, whereas the energy of a one-time attack follows a Poisson distribution as described by [28, 37].

Next, we analyzed the energy limits of attacks to ascertain the realistic unreliable wireless communication channel, owing to the fact that the rational attacker always looks for a strategy that can significantly compromise the wireless communication system in an IIoT-based VCTS system and is likely to employ an approach that consumes the lowest energy consumption. Summarily, DoS attacks interfere with the wireless communication channel between ZC and VOBC of its control area, thereby causing the retransmitting of the status information before the safety margin of the limited time. These situations indicate that conventional approaches cannot efficiently manage DoS attacks on the IIoT-based VCTS system, owing to the system's strict communication latency. Therefore, there is a need to improve the train status estimation approach, from the view of the energy limits of the attacker, to ensure the effective overcoming of the insufficient status information during DoS attacks. Detailed instructions are described as follows. Firstly, the error estimation covariance matrix is expressed as follows:

$$\chi_i^-(t_k) \triangleq \mathbb{E}\left[\delta_i(t_k)\delta_i^T(t_k)\right], \tag{10}$$

where $\chi_i^-(t_k)$ and $\mathbb{E}[\bullet]$ represent the error estimation covariance matrix of train i at time t_k and an expectation function, respectively, while $\delta_i(t_k)$ represents the estimate error as follows:

$$\delta_i(t_k) \triangleq x_i(t_k) - \widehat{x}_i(t_k), \tag{11}$$

where $x_i(t_k)$ indicates the status information of train i at time t_k, while $\widehat{x}_i(t_k)$ represents the estimation value of the estimator at time t_k.

Next, we propose a cost function for minimizing the estimation error covariance with the energy constraint of one attack, as follows:

$$\min \sup_{\Delta T \longrightarrow \infty} \frac{1}{\Delta T}\left[\sum_{t_k=T_1}^{T_2} \chi_i^-(t_k)\right], \tag{12a}$$

$$s.t. \sum_{t_k=T_1}^{T_2} \rho(t_k) \in [0, \rho_{\max}], \tag{12b}$$

where $\rho(t_k)$ represents the power of interference of DoS attacks at time t_k, $\rho_{\max}$ indicates the maximum attack energy, and T_1 and T_2 denote the start and end times of DoS attacks, respectively, whereas $\Delta T \ = T_2 - T_1$ denotes the duration of DoS attacks.

Thereafter, we analyze the convenience using the cost function shown as follows:

$$\min \sup_{\Delta T \longrightarrow \infty} \frac{1}{\Delta T}\left(\mathcal{J}_e - \lambda_e \mathrm{AE}_T\right), \tag{13a}$$

$$\begin{aligned} \mathcal{J}_e &= E\left[\sum_{t_k=T_1}^{T_2} \delta_i t(t_k)\delta_i^T(t_k)\right] \\ &= \sum_{t_k=T_1}^{T_2} \chi_i^-(t_k), \end{aligned} \tag{13b}$$

$$\mathrm{AE}_T = E\left[\sum_{t_k=T_1}^{T_2} \rho(t_k)\rho(t_k)^T\right], \tag{13c}$$

where $\mathcal{J}_e$ indicates the sum of error estimation covariance for DoS attacks and AE_T denotes the sum of attack energy.

It is significant that the underground environment and tunnels under a subway environment cannot provide the charging point for an attacker. One key feature of DoS attacks, which is the limited energy caused by no charging point, is that they occur randomly. DoS attacks targeting the IIoT-based VCTS system significantly interfere with the wireless communication between the ZC and the train, thereby causing frequent packet losses and congestion of the transportation owing to frequent emergency braking of trains. Notably, it is challenging for the attacker to affect the transportation of IIoT-based VCTS by significantly jamming under energy limit situations. In the current study, we explored the defense strategy from the attacker's standpoint. Therefore, the cost function described herein is based on the optimal attack strategy that the attacker is most likely to choose. In the subsections, we review studies describing the random energy distribution of DoS attacks in the IIoT-based VCTS system as well as the approaches applied to solve the cost function while ensuring the optimal energy strategy and the minimum estimation error covariance, as described in the following sections.

4. The Train Status Estimation Approach Based on the Optimal Attack Strategy

In this section, we propose the train status estimation approach, which refers to an enhanced Kalman filtering scheme based on the optimal attack strategy. The estimation approach seeks to transfer indispensable status information from the front train to the following train.

4.1. Modeling the Train Status Estimation Approach of the IIoT-Based VCTS. When packet loss occurs in the physical dynamics of the IIoT-based VCTS system caused by DoS attacks, based on the "fail-safe" requirement of the

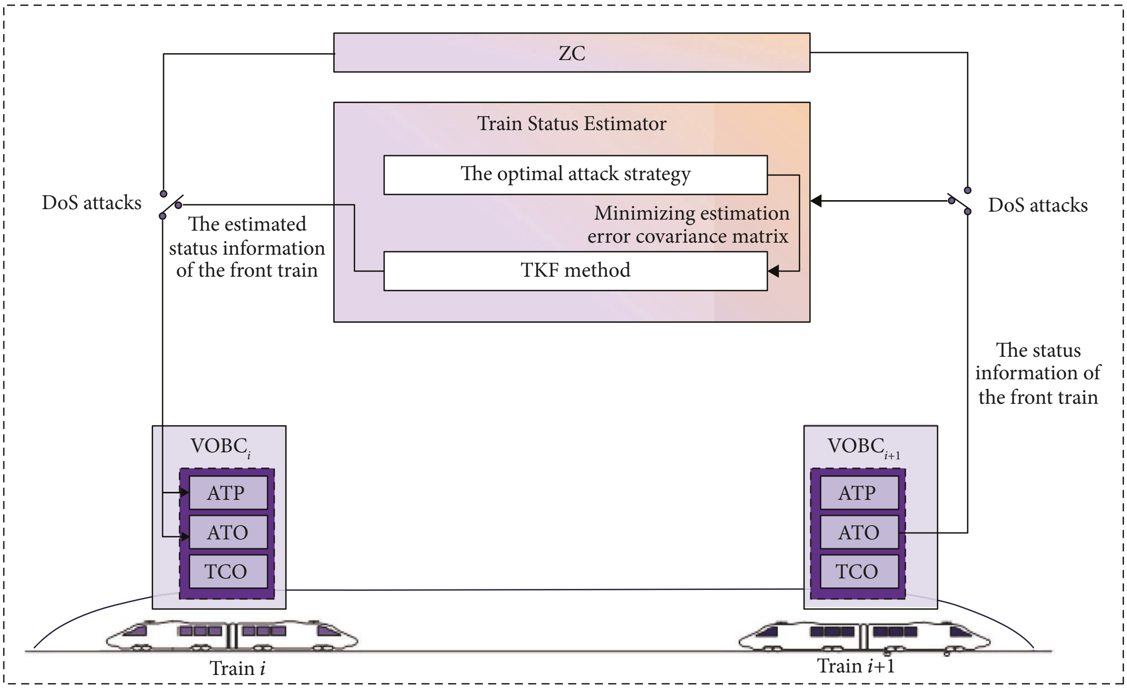

ZC
Train Status Estimator
The optimal attack strategy
Minimizing estimation error covariance matrix
TKF method
DoS attacks
The estimated status information of the front train
DoS attacks
The status information of the front train
VOBC$_i$
ATP
ATO
TCO
VOBC$_{i+1}$
ATP
ATO
TCO
Train i
Train i+1

Figure 4: Structure of the train status estimation approach.

signaling control system, the train convoy would be decoupled. As a result, the virtual coupling mode is instead of the MB mode. Because ZC experiences the transmission failure of that limit MA, which is the maximum safety margin of the following train, at the start instance of each communication cycle. Then emergency braking would be executed when the speed of the following train is violated the safety margin. Moreover, after emergency braking, following trains have to stay stationary until the wireless communication is resolved; thus, it can receive an updated MA in real time when the train convoy is decoupled. Eventually, this situation may cause traffic paralysis and enormous numbers of passengers stranded. Therefore, the train status estimation approach aims to mitigate this traffic paralysis caused by DoS attacks, by combing with the enhanced Kalman filter method and the attack strategy from the attacker's perspective.

The Kalman filter, which is known as the linear quadratic estimation (LQE) algorithm, is an optimal estimator that has been extensively applied as an industry controller [38]. The feasibility of this status estimation approach is mainly constrained by the implementation of minimum error estimation covariance to approach the performance of the IIoT-based VCTS during randomly instantaneous attacks. In addition, the estimation approach is unreasonable if it meets the requirements of the conventional error covariance at each iteration. In the current section, we propose a novel solution to this problem, considering the aforementioned shortcomings of DoS attacks. To achieve a minimum unbiased estimation covariance of the status information, which members of the train platoon are decoupled, we propose combing conventional Kalman filtering with the optimal attack strategy, which is the limited attacks' energy, to obtain the train status information $x_i(t_k)$ in the unreliable communication network under DoS attacks (as shown in Figure 4). Therefore, the Kalman filter is a discrete-time controlled process, and the linear stochastic equation of the train i is expressed as follows:

$$x_i(t_k) = A_e x_i(t_{k-1}) + B_e u_i(t_{k-1}) + w_e(t_{k-1}). \tag{14}$$

Consequently, the observation equation of enhanced Kalman filtering is expressed as follows:

$$y_i(t_k) = C_e x_i(t_k) + v_e(t_{k-1}), \tag{15}$$

where $A_e = \begin{bmatrix} 1 & h & 1/2h^2 \\ 0 & 1 & h \\ 0 & 0 & 1 \end{bmatrix}$, $B_e = \begin{bmatrix} 1/2h^2 \\ h \\ 1 \end{bmatrix}$, and $C_e = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$.

Estimation of the status information for the performance of the IIoT-based VCTS is divided into time-updated (predicting) and measurement-updated (receiving) sections. The prediction equation of enhanced Kalman filtering is thus expressed as follows:

$$\widehat{x}_i^-(t_k) = A_e \widehat{x}_i(t_{k-1}) + B_e \widehat{u}_i(t_{k-1}), \tag{16}$$

where $\widehat{x}_i^-(t_k)$ is the estimated status information of train i at time t_k using measurements up to time t_{k-1}.

The status estimation approach, which is combing the Kalman filtering with the optimal attack strategy, abrogates the effects of packet loss during the transfer of the status information of the front train, a phenomenon that alleviates the train operational delays caused by DoS attacks. Reference [39] indicates that packet dropout in the measurement updating process can be calculated as follows:

$$K_e(t_k) = \chi_i^-(t_{k-1})C_e^T\left[C_e\chi_i^-(t_{k-1})C_e^T + R\right]^{-1}, \tag{17}$$

$$\hat{x}_i(t_k) = \hat{x}_i^-(t_k) + K_e(t_k)[y_i(t_k) - C_e\hat{x}_i^-(t_k)], \tag{18}$$

$$\chi_i(t_k) = [I - K_e(t_k)C_e]\chi_i^-(t_k), \tag{19}$$

where $K_e(t_k)$ denotes the Kalman gain at time t_k and $\chi_i(t_k)$ is the updated error estimation covariance matrix of train *i* at time t_k, whereas I is the identity matrix.

Furthermore, in conventional Kalman filtering, the error estimation covariance matrix at time t_k is predicted based on both the iteration procedure of the error covariance matrix at time t_{k-1} and the prediction noise covariance matrix, which are obtained using the channel noise, mainly referring to Gaussian distribution. However, when the T2T and T2G wireless communications of the IIoT-based VCTS interfere with DoS attacks, which follow the Bernoulli distribution, the traditional Kalman filtering is no longer effective, while the prediction noise covariance matrix is uncertainly due to random and uncertain DoS attacks. Therefore, we consider the regular character of the DoS attacks and energy limits to optimize the estimation error.

In the status estimation approach of the IIoT-based VCTS, formula (17) is used to accurately estimate and update the status information of the front train, which is based on the minimization error estimation covariance matrix of the front train. The cost function and the optimal attack strategy from the attacker's standpoint are provided to minimize the error estimation covariance matrix $\chi_i^-(t_k)$ of the front train. Therefore, the mathematical status estimate at time t_k is calculated as follows:

$$x_i(t_k) = \begin{cases} x_i(t_k), & \vartheta(t_k) = 1, \\ \hat{x}_i(t_k) = \hat{x}_i^-(t_k) + & \\ K_e(t_k)[y_i(t_k) - C_e\hat{x}_i^-(t_k)] & \vartheta(t_k) = 0, \end{cases} \tag{20}$$

where $\vartheta_{t_k} = 1$ indicates that metro *i* information has been successfully transmitted at time t_k, whereas $\vartheta_{t_k} = 0$ indicates failed transmission.

The predicting error estimation covariance matrix, which is different from the conventional Kalman filtering, significantly affects the accuracy of the train status estimation approach. In the study, we present the minimization of the error estimation covariance that depends on the optimal attack strategy. This strategy, together with the predicting error estimation covariance, is discussed in the next subsection.

4.2. Reformulation of the Optimization Model for Analysis of Attack Energy Limits.

In this subsection, we are prone to probe the factor of impact on DoS attacks. Generally, the main aim of an attacker is to jam the T2T and T2G wireless communication of trains and consume the performance of the IIoT-based VCTS by interfering with the SINR and packet transmission successful rate (or packet dropout rate). These two aspects are key in evaluating the quality performance communication of the IIoT-based VCTS system. The success rate of the packet transmission in the IIoT-based VCTS system is affected by SINR as well as attack energy [27], and it can be expressed as follows:

$$f(t_k) = f(g(t_k), \rho(t_k)), \tag{21}$$

where $g(t_k)$ is the signal attenuation at time t_k.

SINR values can be determined on the basis of periodic sampling in the IIoT-based VCTS system, using a specific communication software on train *i* during each communication cycle. The SINR value less than the specific threshold indicates the MA packet dropout. The relationship between symbol error rate (SER) and SINR in the IIoT-based VCTS is defined by the digital communication theory [27] as follows:

$$\begin{gathered} \mathrm{SER}(t_k) = 2S_{\mathrm{Q}}\left(\sqrt{S_\alpha \hat{s}_i(t_k)}\right), \\ \hat{s}_i(t_k) = \frac{\rho^s(t_k) - g(t_k)}{\varpi + \iota + \rho(t_k)}, \end{gathered} \tag{22}$$

where $\hat{s}_i(t_k)$ is the value of SINR at time t_k, $S_Q = 1/\sqrt{2\pi}\int_x^\infty(-\eta^2/2)\mathrm{d}\eta$, S_α is a constant parameter, $\rho^s(t_k)$ is the transmitting power of APs at time t_k, ϖ is the measurement noise power on the wireless channel, and ι is the interference power on the wireless channel. The probability of the success rate of packet transmission in the IIoT-based VCTS system $f(t_k)$ can be described as follows:

$$f(t_k) = f(g(t_k), \rho(t_k)) \triangleq 1 - 2S_{\mathrm{Q}}\left(\sqrt{S_\alpha \hat{s}_i(t_k)}\right). \tag{23}$$

APs provide enough transmission power to support the stabilities of the T2T and T2G communication subsystems, thus ensuring the performance (i.e., improving punctuality, reducing the waiting time of passengers, and avoiding traffic paralysis) of the IIoT-based VCTS [36]. This process can be quantified as follows:

$$\mathbb{E}[f(g)] > f_s \triangleq 1 - \frac{1}{\lambda_{\max}(A_e)}, \tag{24}$$

where $\lambda_{\max}(A_e)$ represents the maximum eigenvalue of the train status estimation matrix A_e.

Following DoS attacks, MA packet dropout is inevitable following DoS attacks. In the study, the MA packet dropout is used to improve the estimate error. Notably, $\phi(t_k) = (1 - \vartheta(t_k))\delta_i(t_k)$ is defined as the estimate error at $\vartheta(t_k) = 1$, implying that DoS attacks cause MA packet dropout at time t_k. It is aimed at minimizing the estimate error with the MA packet dropout. Therefore, the estimate error is highly corrected with the performance indicated by the train-ground communication system, and the cost function in formula (13a)–(13c) can be written as follows:

$$\min \lim_{\Delta T \longrightarrow \infty} \sup \frac{1}{\Delta T} \mathbb{E}\left[\sum_{t_k=T_1}^{T_2} \phi[z(t_k), g(t_k), f(t_k)]\right], \tag{25}$$

where $z(t_k)$ represents the probability of the MA packet dropout with DoS attacks at time t_k.

The estimate error of the train status information during transmission failure caused by DoS attacks in the IIoT-based VCTS is expressed as follows:

$$\begin{aligned}\phi[z(t_k), g(t_k), f(t_k)] \triangleq{} & [[1 - f(t_k)]z(t_k)^T z(t_k) \\ & - \lambda_e \cdot \rho(g(t_k), f(t_k)),\end{aligned} \tag{26}$$

where λ_e represents a weight constant.

For convenience, we write formula (26) as follows:

$$\phi(z, g, f) = (1 - f)z^T z - \lambda_e \cdot \rho(g, f), \tag{27}$$

where z, f, and g indicate abbreviated forms of $z(t_k)$, $f(t_k)$, and $g(t_k)$, respectively.

Moreover, the optimal attack strategy from an attacker's standpoint is to achieve a trade-off between the rate of packet dropout and the cost of attack energy. Therefore, the attack strategy can be given by

$$\begin{aligned}\rho(t_k) &= \rho(g(t_k), f(t_k)) \\ &= \inf\left\{\rho(t_k) | f(t_k) \le \overline{f}, \rho \in [0, \rho_{\max}]\right\},\end{aligned} \tag{28}$$

where it is assumed that $\rho(g(t_k), \underline{f}(t_k))$ is continuous with respect to $f(t_k)$ and $g(t_k)$ [40] and $\overline{f}$ indicates the successful minimum packet transmission rate of the system testing specification, while ρ represents the abbreviated form of $\rho(t_k)$.

The status set $\mho(z(t_k), g(t_k)) \in \mho(z, g)$ is required to quantify the relationship between the attacks power and the packet transmission from the attacker's standpoint. Therefore, the optimal attack strategy is described as follows:

$$\mho(z, g) = \begin{cases} f_{\min}(t_k), & \mathbb{E}\left(z^T z\right) > 1 - \overline{f} \text{ or } g \le \overline{g}, \\ [f_{\min}(t_k), f_{\max}(t_k)], & \text{otherwise,} \end{cases} \tag{29}$$

where $f_{\min}(t_k) = f(g, \rho_{\max})$, while $f_{\max}(t_k) = f(g, 0)$, whereas $\overline{g}$ indicates the maximum signal attenuation of the IIoT-VCTS system testing specification when the train convoy is decoupled.

Packet dropout occurs without DoS attacks when the channel qualities of the T2T and T2G communication systems are lower compared to the minimal performance of the VCTS system. This implies that there is a lack of attacks power in the communication channel.

The cost function is based on the optimal attack strategy; therefore, it is important to evaluate the relationship between energy limits and packet loss. A hypothesize can be formulated based on Theorem 3.5 [41] that a unique function $\Pi(z, g, f)$ exists to satisfy the following equation:

$$\begin{aligned}f^*(z, g, f) = \min_{f(t_k) \in \mho(z,g)} & \sup \phi(z, g, f) - \Pi^* \\ & + \mathbb{E}\{\Pi(z^+, g^+) | z, g, f\},\end{aligned} \tag{30}$$

where $f^*(z, g, f)$ represents the optimal packet reception rate from which the effects of attack strategy have been estimated and z^+ indicates the estimated error in the next step, while g^+ indicates the signal attenuation in the next step. Π^* is expressed as follows:

$$\Pi^* = \mathbb{E}\{\Pi(z, g)\}. \tag{31}$$

The cost function can be converted by formula (30). Therefore, a suboptimal attack strategy can be obtained because the optimal cost function has been transformed to generate an effective solution. However, this expression cannot be used to estimate the status information of the front train in this step; therefore, the cost function is transformed. In the next section, the expression of function $\Pi(z, g, f)$ is described, while the minimum error estimation covariance matrix is generated.

The status transition probability can therefore be defined as $\Pr(z^+, g^+ | z, g, f)$ with $\vartheta(t_k) = 1$. $\mathscr{B}(f)$ represents the distribution of DoS attacks, subject to Bernoulli distribution [42]. Then, the attack strategy is considered as a Markov stochastic process as follows [43]:

$$\Pr(z^+, g^+ | z, g, f) = f \mathscr{N}_{0,W}(z^+) + (1 - f)\mathscr{N}_{Az,W}(z^+), \tag{32}$$

where $\mathscr{N}_{0,W}$ and $\mathscr{N}_{Az,W}(z^+)$ indicate the transition status, $\mathscr{N}_{0,W}$ indicates the absence of DoS attacks at time t_k, and $\mathscr{N}_{Az,W}(z^+)$ indicates the occurrence of the MA packet dropout caused by the DoS attacks. $\Pi^*(z, g, f)$ can be expressed as follows according to formula (32):

$$\begin{aligned}\mathbb{E}\{\Pi(z^+, g^+) | z, g, f\} ={} & f \mathbb{E}_{g^+, w_e}[\Pi(g^+, w_e)] \\ & + (1 - f)\mathbb{E}_{g^+, w_e}[\Pi(g^+, Az + w_e)].\end{aligned} \tag{33}$$

The following final cost function is ultimately expressed as follows:

$$f^*(z, g, f) = \min_{f \cdot (t_k) \in \mho(z,g)} \sup \{-\lambda_e \rho(g, z) + (1 - f) \cdot \Lambda(z, g)\}, \tag{34}$$

with

$$\Lambda(z, g) = \mathbb{E}_{g, w_e}\left[\mathbf{\Pi}(g^+, Az + w_e) - \mathbf{\Pi}(z, g)\right] + z^T z. \tag{35}$$

Therefore, the attack strategy is expressed as follows:

$$\rho^*(z, g, f) = \arg\min_{\rho(t_k) \in [0, \rho_{\max}]} \{-\lambda_e \cdot \rho(z, g) + (1 - f) \cdot \Lambda(z, g)\}. \tag{36}$$

The error estimation covariance matrix depends on the attack strategy as well as the cost function. These parameters are solved in the next subsection.

4.3. Solving the Optimal Attack Strategy with Energy Limits.

The minimum error estimation covariance matrix in the suboptimal attack strategy case is described in this section. The suboptimal solution method is expressed as a π function [44]. The DoS attack power strategy is expressed according to the suboptimal attack strategy from lemmas in references [45, 46].

$$\rho_\pi^*(z,g,f)=\begin{cases}0, & g\le\overline{g}\ \text{or}\ \Lambda(z,g),\\[1em] & >\lambda_e\left(\dfrac{\rho^s(t_k)-g(t_k)}{\widehat{s}_i(t_k)}-\varpi-1\right),\\[1em] \dfrac{\rho^s(t_k)-g(t_k)}{\widehat{s}_i(t_k)}-\varpi-1 & \text{otherwise.}\end{cases}\tag{37}$$

Due to the impact of the DoS attacks on the IIoT-based VCTS, the attacker seeks to interrupt the rapidly growing passengers flow at the station. MA dropout without jamming occurs when the quality of wireless communication channels is lower than the signal attenuation limit. However, it is a challenge for the attacker to cause MA dropout when the T2T and T2G communication environments are effective. In the situation of the quality of the wireless communication channel is the highest, the attack power is zero under the optimal attack strategy (as shown in equation (37)). During the duration of $[T_1,T_2]$, the attacker is required to establish attacks power by the SINR of the route map. The attacker selects a transmission power to make a packet successful rate that is less than the communication limit for the safety of the IIoT-based VCTS system when the train convoy is decoupled caused by DoS attacks. In an actual underground system, the SINR of the entire rail route can be measured by the attacker, posing a serious threat to the system.

The $\Lambda(z,g)$ can be obtained from equation (35); however, it is unsolved. A unique expression of $\Lambda(z,g)$ is described in the current section. Equation (38) can be derived from equation (11) as follows:

$$\begin{aligned}\phi_\pi(t_k)=\min\lim_{\Delta T\longrightarrow\infty}\sup\frac{1}{\Delta T}\mathbb{E}\left[\sum_{t_k=T_1}^{T_2}(1-\overline{f})z^Tz\right]\\ -\lambda_e\mathbb{E}_g\left[\rho(g(t_k),f(t_k))\right],\end{aligned}\tag{38}$$

where $\overline{f}$ larger than f_s, as presented in equation (24).

A hypothesized that the condition formula (24) satisfies is defined to simplify $\phi_\pi(t_k)$ according to [40] as follows:

$$\phi_\pi(t_k)=\mathbf{Tr}\left(\chi_i^-(t_k)\right)-\lambda_e\mathbb{E}_g\left[\rho(g(t_k),f(t_k))\right],\tag{39}$$

where $\mathbf{Tr}(\bullet)$ represents the trace function.

The above analyses indicate that the predicting error covariance matrix, which is iterated at each communication cycle, can be described by formula (41). Notably, the status estimation approach can be obtained from formula (13a)–(13c) and formulae (40)–(42). Therefore, Theorem 1 can be expressed as follows:

$$\rho_\pi^*(z,g,f)=\begin{cases}0, & g\le\overline{g}\ \text{or}\ \dfrac{1}{1-\overline{f}}z^TM_ez>\lambda_e\left(\dfrac{\rho^s(t_k)-g(t_k)}{\widehat{s}_i(t_k)}-\varpi-1\right),\\[1.5em] \dfrac{\rho^s(t_k)-g(t_k)}{\widehat{s}_i(t_k)}-\varpi-1, & \text{otherwise.}\end{cases}\tag{40}$$

Theorem 1. The optimal attack strategy with energy limits from the attacker's standpoint can be expressed as formula (40).

The expected corresponding cost function of the IIoT-based VCTS can be calculated as follows:

$$\Pi_\pi(z,g)(t_k)=\frac{1-f}{1-\overline{f}}z^TM_ez-\lambda_e\mathbb{E}_g\left[\rho(g(t_k),f(t_k))\right],\tag{41}$$

where $\chi_i^-(t_k)$ and M_e follow the Lyapunov equation as shown in the following formulae -(42)-(44) [47]:

$$\chi_i^-(t_k)=(1-\overline{f})\left[A_e\chi_i^-(t_{k-1})A_e^T+Q\right],\tag{42}$$

$$M_e=(1-\overline{f})\left[A_eM_eA_e^T+Q\right].\tag{43}$$

Thus, $\Lambda_\pi(z,g)$ can be expressed as follows:

$$\Lambda_\pi(z(t_k),g(t_k))=\frac{1}{1-\overline{f}}z^TM_ez.\tag{44}$$

Energy constraints are the most important characteristic of DoS attacks; therefore, they are discussed together on the part of the attacker. Under subway environments and tunnels do not provide a charging point for the attacker. Therefore, when the attacker intends to interfere with the T2T and T2G communication subsystems, energy constraints affect DoS attacks. The novel status estimation approach is based on the optimal attack strategy on the part of energy constraints of attacks. Studies would be further conducted to investigate other features of DoS attacks.

Contrary to the traditional method, in the enhanced Kalman filtering approach, the error estimation covariance matrix is calculated based on the optimal attack strategy. First, we have designed a cost function based on attack energy limits of DoS attacks, on the part of the attacker. Then, the optimization model, which consists of energy limits, signal attenuation, as well as the probability of successful rate of the packet transmission in the control system, was proposed. Next, we transformed the cost function into the minimum error estimation covariance matrix, while we defined a Markov stochastic process to match the failed transmission or not. For achieving the combination of the packet dropout rate, the cyber performance, and the attack energy, which is a physical index, we also have transformed those performance into SER and SINR, which can be measured directly. Last, the minimum error estimation covariance matrix in the optimal attack strategy case is obtained on Theorem 1, which was calculated by a combination of the optimization model and feature performance of the IIoT-based VCTS system.

The evaluation criteria for mapping the train status estimation approach in the physical layer of the IIoT-based VCTS system against DoS attacks are described in the next section.

5. Evaluation Criterion of the Effects of DoS Attacks on the IIoT-Based VCTS System

We defined the security criterion to evaluate the performance of the train status estimation approach. The evaluation criterion can be divided into the physical dynamics of train operation and the passenger's satisfaction, which is inversely proportional to the traveling time of passengers. In addition, sensitivity indices including the train dynamic schedule, the train operational delay covariance, and the waiting time of the passenger are introduced to evaluate the effects on the passenger's traveling time [48, 49].

5.1. Train Dynamic Schedule. Train operation should be compliant with the train dynamic schedule and MA of ZC to ensure urban transportation safety and punctuality of urban transportation [48]. Profiles of trains' operation, where they are over space and time from one station to the destination station, are presented in Figure 5. The train dynamic schedule should be sensitive to the train operation. The dotted line in Figure 5 indicates an increased traveling time of train i from the station B to the station D, which is caused by frequent emergency brakes [49]. Notably, this spacing deviation indicates the difference from the train $i+1$ operation schedule, under normal conditions. This operation deviation is proportional to delays, which are caused by frequent emergency brakes and speed limits under DoS attacks.

5.2. Train Operational Delay Covariance. Performance indices including the delay covariance and the average waiting time of passengers are defined to investigate passenger satisfaction, which indicates passenger flow and traveling time [48]. Headway is defined as the time difference between the departure time of train i and the departure time of the train $i+1$ at station k. The delay represents the error between the headway under normal conditions and the actual headway under DoS attacks. In this study, σ_h is defined as the weight sum of train operational delay covariance as described below. This index indicates variations in the passenger travel time, which is accumulated by the train operational delay and the waiting time of the passenger under DoS attacks [49].

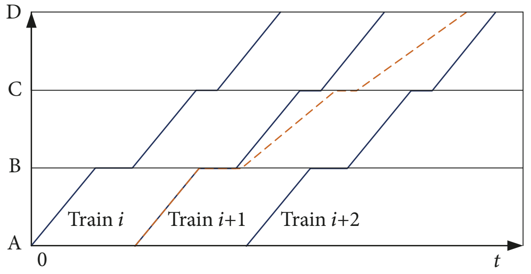


Figure 5: Train dynamic schedule.

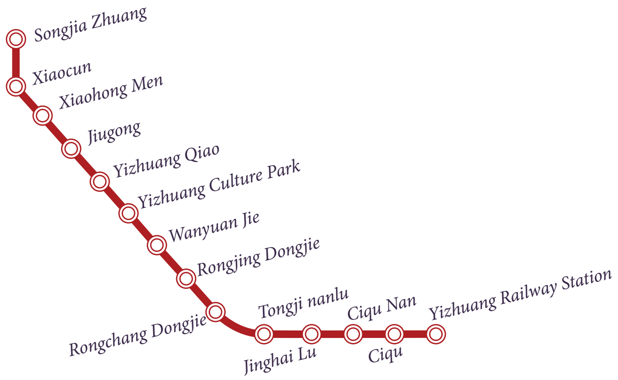


Figure 6: Communication test link between trains and ground terminal.

Table 1: Parameters used in the simulations.

Parameters	Value
Tracing acceleration	1 m/s^2
The resistance acceleration	0.02 m/s^2
Emergency brake deceleration	1.2 m/s^2
Service brake deceleration	1 m/s^2
The length of the train	118 m
The mass of the train	1 ton
The headway between trains	120 s
The speed limits	22.2 m/s
The number of stations	14
The number of trains	12
The communication period	200 m/s
The measurement noise error	6
The passenger's leaving rate	1.7person/sec
n_c	3

$$\sigma_h = \frac{1}{n-1} \sum_{i=2}^{n} \sum_{k=1}^{m} \left(he_{i,k} - he \right)^2 \cdot ws_k, \tag{45}$$

where $he_{i,k}$ and he represent the actual operational headways of train i at station k, under DoS attacks and the operational headway with the original schedule, respectively; ws_k indicates the weight constant to map the passenger flow at station k; and m indicates the station number of the whole rail line, while n indicates the number of trains on the railway. Passenger flow for the underground railway varies among different stations. The term ws_k represents the weight

Table 2: Route parameters referenced to the Yizhuang railway.

Station name	Distance between adjacent stations (m)	Average passenger's arriving rate (person per sec)
Songjiazhuang	2,631	77/600
Xiaocun	1,275	271/600
Xiaohongmen	2,366	74/600
Jiugong	1,982	189/600
Yizhuangqiao	993	16/600
Yizhuang culture park	1,538	31/600
Wanyuanjie	1,280	192/600
Rongjingdongjie	1,354	132/600
Rongchangdongjie	2,338	16/600
Tongjinanlu	2,265	66/600
Jinghailu	2,086	46/600
Ciqunan	1,286	60/600
Ciqu	1,334	50/600
Yizhuangqiao (open soon)	—	0

value at station k to indicate the actual passenger flow in each station. For example, station B is an exchange station in the route map, where passenger waiting time at station B is longer compared to that at other stations (as shown in Figure 5).

The weight value for each station is defined according to the average passenger arrival rate for evaluation of the actual passenger flow at station k as follows:

$$ws_k = \frac{lr_k}{\sum_{k=1}^{m} lr_k}, \tag{46}$$

where lr_k indicates the arriving number per second of passengers at station k. The $\sigma_{h\_\text{average}}^{k}$ denotes the average train operational delay covariance, which represents the average train operational delay at station k.

$$\sigma_{h\_\text{average}}^{k} = \frac{1}{n-1} \sum_{i=2}^{n} \left(he_{i,k} - he\right)^2. \tag{47}$$

6. Simulation Results and Discussion

In this section, the performance effectiveness of the train status estimation approach under DoS attacks is evaluated. The simulation consists of three parts. Firstly, the simulation environments and main parameters are presented. Secondly, the energy distribution of the optimal DoS attack strategy is visualized using the MATLAB 2016 tool. Last, the performance improvement of the IIoT-based VCTS under the status estimation approach is analyzed.

6.1. Simulation Environment and Parameters.

6.1. Simulation Environment and Parameters. The simulation environment and parameters are referenced to the Beijing Yizhuang urban railway route, which is located in the southeast of Beijing, covering a total length of 23.3 km with 14 stations as shown in Figure 6. The simulation route comprises wayside techniques and wayside APs deployed along the track stretching over a 200 m distance. The wireless communication system is LTE-M. All relevant parameters for simulating are outlined in Table 1.

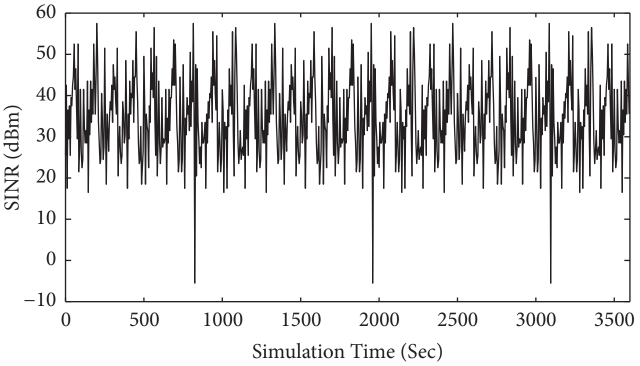
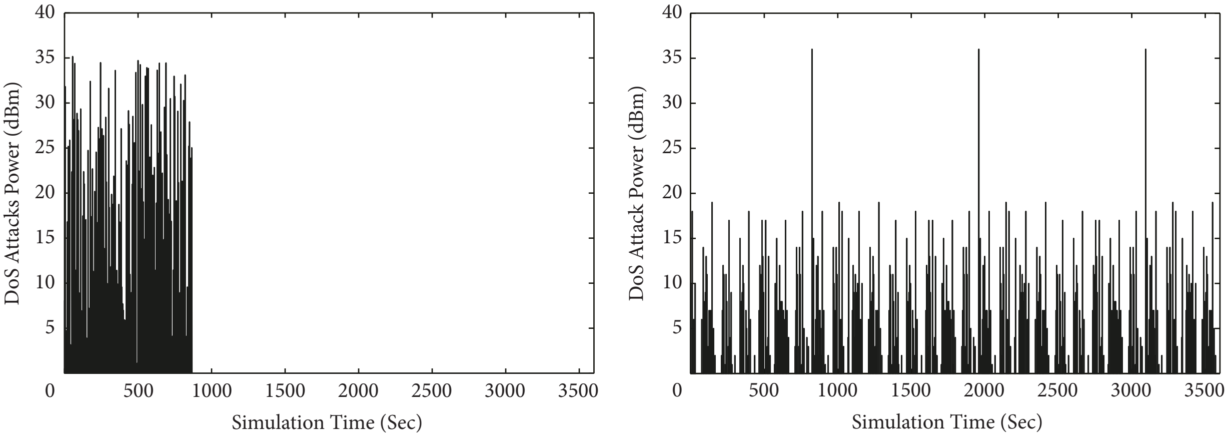


Figure 7: Measurement values of SINR with 1 hour in the Yizhuang line.

The performance of the train estimation approach was analyzed using the number of stranded passengers. In this case, the average departure time is set at 1.7 seconds per person, while the passenger flow varies across stations. Other parameters of the Yizhuang subway line are presented in Table 2.

6.2. The Optimal Attack Strategy. The propagation of signals in the IIoT-based VCTS system is similar to the propagation of electromagnetic waves in the waveguide [50]. This implies that the DoS attacks are proportional to the distance between the attacker and the victim ZC. For accurate simulation, it is assumed that the location of the attacker is adjacent to the position of victim ZC, and the attacker is alone.

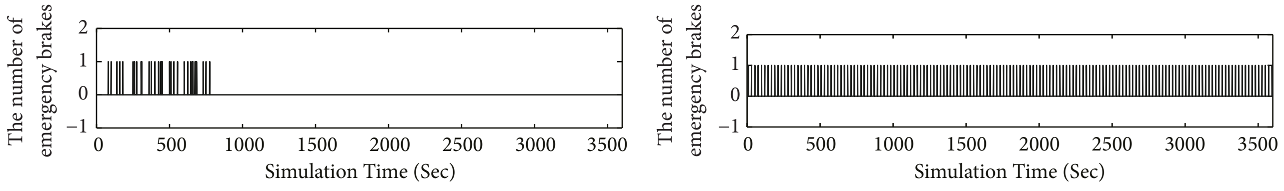
Signal attenuation in the IIoT-based VCTS system is attributed to the accumulation of the fast fading model and the shadow fading model in the tunnel [50, 51]. Moreover, the optimal attack strategy is based on the SINR in the normal underground environment. Therefore, to simulate a practical realistic electromagnetic environment, values of $\hat{s}_i(t_k)$ are measured at the Yizhuang subway line as shown in Figure 7. MATLAB simulation is performed using the train status estimation approach simulation software. In this study, the sum of attack limits on part of the attacker was



(a)

(b)

Figure 8: The energy distribution comparison of specific attacks strategies: (a) the random attacks strategy and (b) the optimal attacks strategy.



(a)

(b)

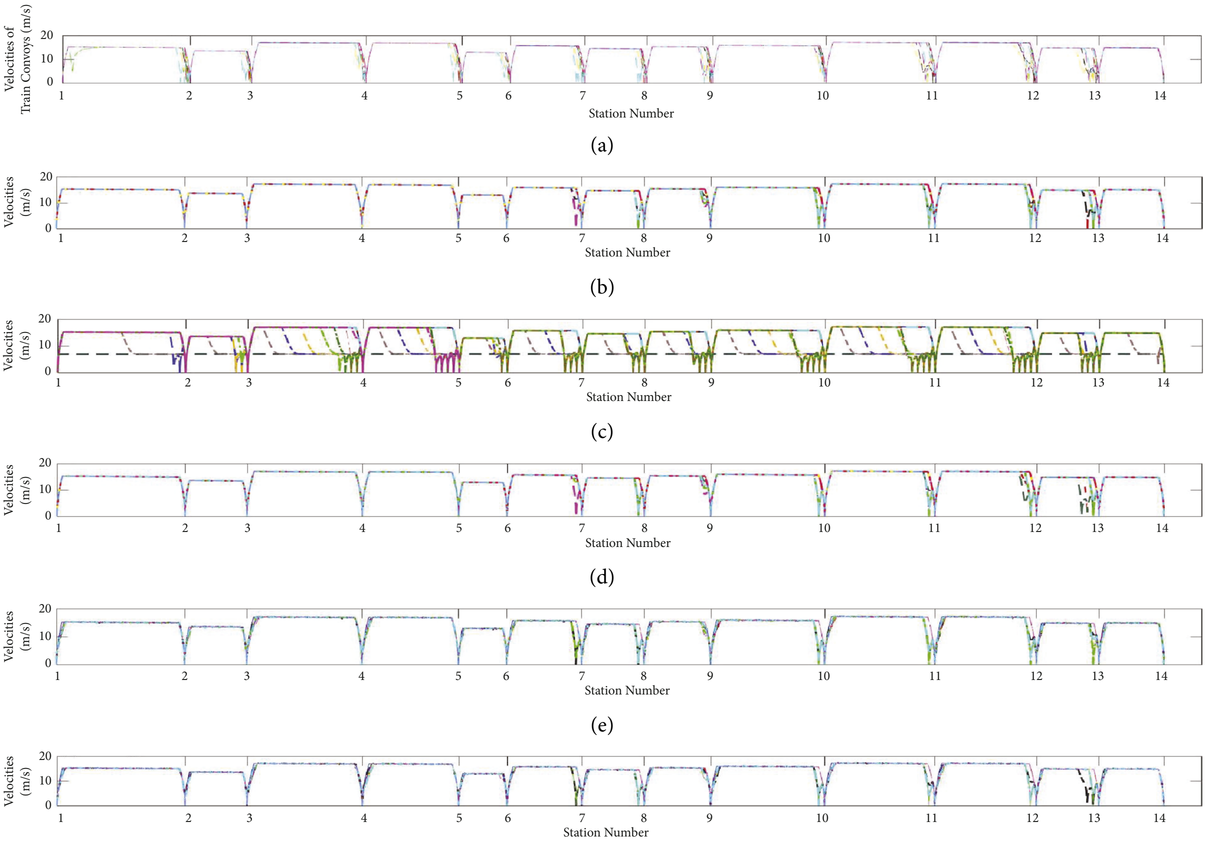
Figure 9: Comparison of the number of emergency brakes caused by specific attacks strategies: (a) the random attacks strategy and (b) the optional attacks strategy.

assumed to be 3000 W. Other parameters used in simulation include, $\rho^s(t_k) = 30\,\mathrm{mW}$, $\varpi = 3\,\mathrm{dBm}$, $\imath = 2\,\mathrm{dBm}$, $\overline{f} = 0.95$, and $\overline{g} = 12\,\mathrm{dBm}$.

The performance of optimal attack strategy and random attacks in determining the impacts of DoS attacks on the IIoT-based VCTS system is presented in Figure 8. The number of attacks power at 867 s is decreased (as shown in Figure 8(a)). Contrary to the energy distribution, the optimal attack strategy performs better with regard to the duration of DoS attacks, compared to the random attack strategy, which is characterized by one energy constraint. The number of emergency brakes, which is a measure of the effects of DoS attacks on the IIoT-based VCTS system, is associated with delays in the dynamic operation of the train. The number of emergency brakes is evaluated to determine the advantage of the optimal attack strategy as shown in Figure 9. The number of emergency brakes in the optimal attack strategy (i.e., 309) is higher compared to that of the random attack strategy (i.e., 32). This can be attributed to the higher energy consumed in the random attack strategy.

6.3. Result of the Physical Layer of the Train Status Estimation Approach. The effects of DoS attacks on the IIoT-based VCTS system were quantified using appropriate evaluation criteria, including speed/distance trajectories of the train, train dynamic schedule, train operational delay covariance, and average waiting time of the passenger, to effectively evaluate the status estimation approach. In addition, the performance of the status estimation approach was compared with that of the conventional methods to assess the effectiveness of the proposed approach. Representative methods used for comparison include the intrusion detection (IDS) method [52], which is widely used to identify DoS attacks and to evaluate the status estimation approach. Several studies have used the estimation approach based on game-theoretic (SEBG) [27]. The SEBG and IDS approaches are compared to the status estimation approach in the subsequent subsection.

6.3.1. Speed/Distance Trajectories of Trains. The x-axis in Figure 10 shows station positions, while the y-axis shows train velocities. The line chart presented in Figure 10(b) shows the trajectories of 12 trains, which are decoupled from three train convoys caused by DoS attacks. The operation speed of members of the train convoy during the control area of ZC represents the region between the third station and the tenth station, which is defined by the multiple ZC control areas in Section 2. However, the speed limits, which are due to emergency braking, disappeared under the estimation approach as shown in Figure 10(c). Train trajectories, which are not limited by speed limits, can reduce the delay in train operation under DoS attacks. The simulation results indicate the validity and stability of the defense strategy. Similarly, SEBG and IDS approaches can limit the



(a)

(b)

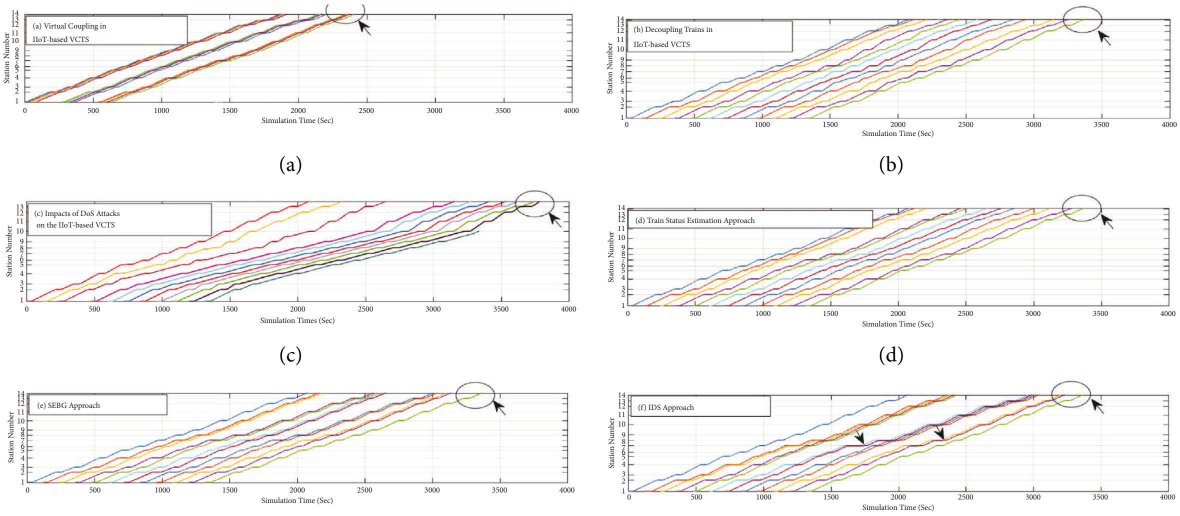
(c)

(d)

(e)

(f)

Figure 10: Train’s trajectories in specific scenarios: (a) virtual coupling in IIoT-based VCTS, (b) decoupling trains in IIoT-based VCTS, (c) impacts of DoS attacks on the IIoT-based VCTS, (d) train status estimation approach, (e) SEBG approach, and (f) IDS approach.



(a)

(b)

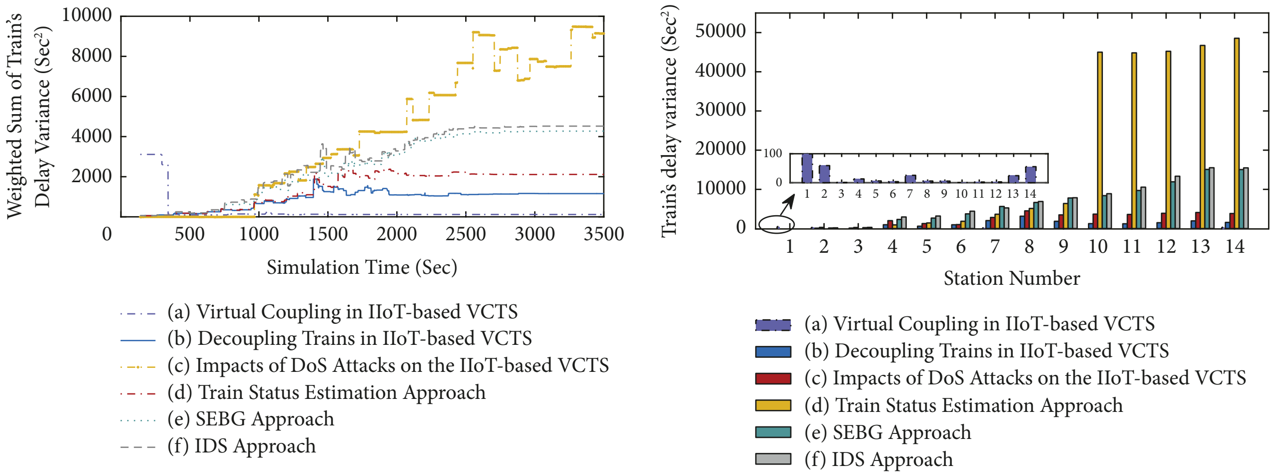
(c)

(d)

(e)

(f)

Figure 11: Dynamic schedule in specific scenarios: (a) virtual coupling in IIoT-based VCTS, (b) decoupling trains in IIoT-based VCTS, (c) impacts of DoS attacks on the IIoT-based VCTS, (d) train status estimation approach, (e) SEBG approach, and (f) IDS approach.



(a)

(b)

Figure 12: Train operational delay variance in specific scenarios.

number of emergency brakes due to DoS attacks. When compared to the effects of the train status estimation approach, the effects of these conventional methods on speed are significant. An increase in effects is attributed to the processing time of SEBG and IDS approaches.

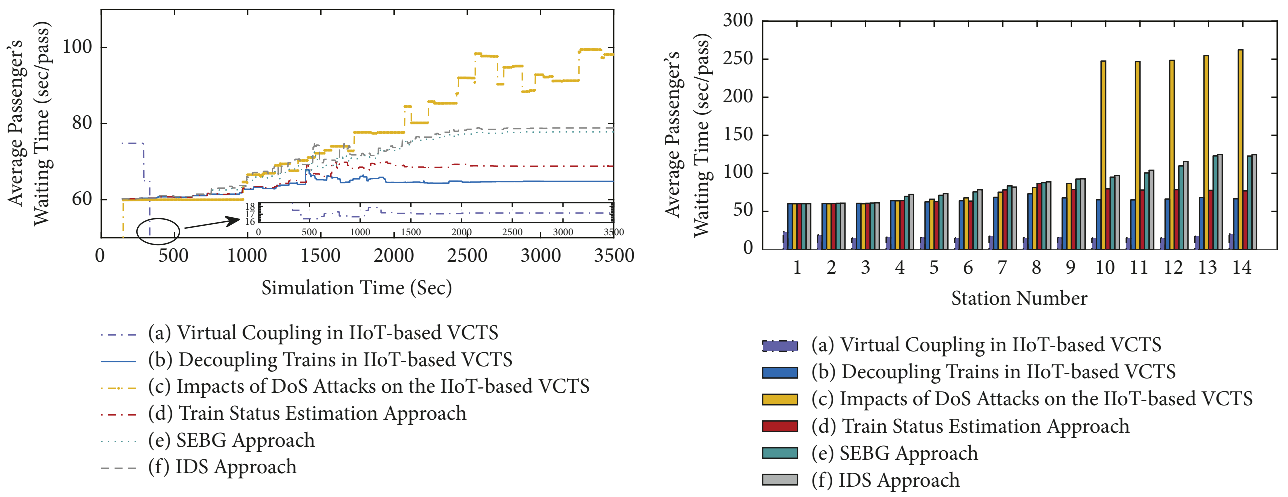
6.3.2. *Train Dynamic Schedule.*

Dynamic schedules of the Yizhuang subway line in specific scenarios with the 12 trains are shown in Figure 11. The simulation represents the 1 hour schedule of the train. The train dynamic schedule under DoS attacks with delays in train operations exceeding normal operations is presented in the chart in Figure 11. MAs overdue or dropout indicates the unreliable communication network under DoS attacks; thus, the subsequent train does not receive the MA in real time, resulting in the frequent emergency braking, occurring between the 1400 s and the 3000 s. Emergency braking causes delays in the arrival time for the train under DoS attacks as shown in Figure 11(c). The simulation result under the train status estimation approach is presented in Figure 11(d). The effects of DoS attacks on train operations are minimal better between the 2400 s to the 3000 s. These findings indicate that the dynamic schedule under the train status estimation approach resembles that of the original timetable and that this approach significantly minimizes delays in train operations (as shown in Figures 11(c) and 11(d)). On the contrary, delays in train operations of SEBG and IDS approaches are superior, compared to the status estimation approach. These results show different degrees of delay within one hour (as shown in Figures 11(e) and 11(f)), mainly with the IDS approach, which were attributed to the ineffective detection time. However, the arrival time of the last train for SEBG and IDS approaches is not significantly different when compared to the arrival time under normal conditions (as shown in Figure 11(e)). This can be attributed to manual interventions when train operation delays are extended beyond the specified limit in the subway. Notably, a small margin between adjacent dynamic operational curves improves the serious safety risk (as shown in Figure 11(f)).

6.3.3. *Train Operational Delay Covariance.*

Variations in the weighed sum of train operational delay variance in the Yizhuang line are presented in Figure 12(a). The findings showed a general upward trend in the weight sum of train operational delay variance. When the train convoy is decoupled, the delay fluctuated from 1,400 to 2,000. However, when the wireless communication is under DoS attacks, the weight sum of train operational delay variance shows an upward trend reaching a maximum value sevenfold higher compared to the maximum value under a normal scenario. The red line in Figure 12(a) indicates that the train status estimation approach in comparison with other specific scenarios is superior. In particular, for the status estimation approach, the weight sum of train operational delay variance shows an upward trend, reaching a peak value below 2,300. This indicates that the status estimation approach is effective and consistent with the normal environment. Analysis shows a steady increase in delay variance of the train under SEBG and IDS approaches, with the maximum values less than 4,500 and 4,100, respectively.

The train operational delay covariance for each station, which is increased for each station, in the Yizhuang line under DoS attacks is shown in Figure 12(b). Notably, between the tenth and the fourteenth stations, operational delay covariance of the train under DoS attacks is higher compared to those under the trains decoupling and under the state estimation approach. These findings indicate that the delay time is proportional to the distance covered under DoS attacks. Findings for the estimation approach under DoS attacks are shown in Figure 12(b). These results indicate that compared to conventional methods, the estimation approach significantly reduces the operational delay time of the train. A steady rise in the number of delays from 0 to 15,000 is observed in the SEBG approach (as shown in



(a)

(b)

Figure 13: Average waiting time of the passenger in specific scenarios.

Figure 12(b)). Notably, when compared to the SEBG approach, the increase in the delay variance of the train in the IDS approach is not significantly different.

6.3.4. Average Waiting Time of the Passenger. Variations in the average waiting time of passengers, which is the average value of the fourteen stations, are presented in Figure 13(a). The average waiting time of the passenger rapidly increases when the DoS attacks are jammed in wireless communication. For the train status estimation approach, SEBG approach, and IDS approach, the average waiting times of passengers increased (as shown in the line chart Figure 13(a)). However, analyses revealed a steady trend in both the normal environment and under the train status estimation approach scenario, with a waiting duration of less than seventies seconds, in the entire process of train operation. These findings indicate that the train status estimation strategy is effective.

Findings for variations in the average waiting time of passengers at each station are presented in Figure 13(b). Significant increases in the average waiting time of passengers are observed under the DoS attacks, SEBG approach, and IDS approach. Notably, the train status estimation approach effectively decreases schedule delay.

7. Conclusion and Future Work

In this study, a novel train status estimation approach was established for the protection safety and punctuality in the IIoT-based VCTS system under DoS attacks. DoS attacks can affect T2T communications; as a result, it causes train convoy decoupling and enormous packet dropout. For mitigating and estimating the effects of DoS attacks on the IIoT-based VCTS system, we consider that the attack strategy of a rational attacker is optimal with the energy limited, which will most cause the system state offset, and explore a trade-off between the best gain of the attack strategy and the performance of the system, such as the real-time capability, train operational delays, the train dynamic schedule, trajectories of trains, and the average waiting time of passengers. In the study, six specific scenarios were defined to investigate the impacts of DoS attacks on the IIoT-based VCTS system. Final findings show that the train status estimation approach can mitigate the effects of DoS attacks on the punctuality of train dynamic schedule and effectively enhance the train operation safety prominently under DoS attacks. Moreover, further studies would be performed to evaluate other features of DoS attacks.

Data Availability

The data are available upon request to the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported by grants from the China Railway Corporation Foundation under grant number K2021X001, the Natural Science Foundation of China under Grants (61973026), the Beijing Municipal Education Commission Funding (I20H100010, I19H100010), the Beijing Natural Science Foundation (L201002), in part by the Beijing Jiaotong University Project under Grant (RCS2021ZZ005), and Fundamental Research Funds for the Central Universities (2021CZ107).

References

[1] R. Parise, H. Dittus, J. Winter, and A. Lehner, "Reasoning functional requirements for virtually coupled train sets: Communication," *IEEE Communications Magazine*, vol. 57, no. 9, pp. 12–17, 2019.

[2] H. Wang, Q. Zhao, S. Lin et al., "A reinforcement learning empowered cooperative control approach for iiot-based virtually coupled train sets," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4935–4945, 2021.

[3] S. Ma, B. Bu, and H. Wang, “A virtual coupling approach based on event-triggering control for cbtc systems under jamming attacks,” in *Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pp. 1–6, IEEE, Victoria, BC, Canada, 18 November 2020 - 16 December 2020.

[4] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial internet of things: challenges, opportunities, and directions,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[5] F. Flammini, S. Marrone, R. Nardone, A. Petrillo, S. Santini, and V. Vittorini, “Towards railway virtual coupling,”vol. 7, pp. 1–6, in *Proceedings of the IEEE International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles International Transportation Electrification Conference (ESARS-ITEC)*, vol. 7, IEEE, Nottingham, UK, Nov 2018.

[6] E. Quaglietta, M. Wang, and R. M Goverde, “A multi-state train-following model for the analysis of virtual coupling railway operations,” *Journal of Rail Transport Planning & Management*, vol. 15, Article ID 100195, 2020.

[7] J. Aoun, E. Quaglietta, R. M. Goverde et al., “A hybrid delphi-ahp multi-criteria analysis of moving block and virtual coupling railway signalling,” *Transportation Research Part C: Emerging Technologies*, vol. 129, pp. 1–22, 2021.

[8] D. Wu, J. Liu, H. Wang, and T. Tang, “A cpn-based approach for studying impacts of communication delays on safety and availability of safety-critical distributed networked control systems,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3033–3042, 2022.

[9] Y. Li, L. Zhu, H. Wang, F. R. Yu, and S. Liu, “A cross-layer defense scheme for edge intelligence-enabled cbtc systems against mitm attacks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2286–2298, 2021.

[10] C. Di Meo, M. Di Vaio, F. Flammini, R. Nardone, S. Santini, and V. Vittorini, “Ertms/etcs virtual coupling: proof of concept and numerical analysis,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2019.

[11] J. Felez, Y. Kim, and F. Borrelli, “A model predictive control approach for virtual coupling in railways,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 7, pp. 2728–2739, July 2019.

[12] W. P. M. H. Heemels, A. R. Teel, N. van de Wouw, and D. Nešić, “Networked control systems with communication constraints: tradeoffs between transmission intervals, delays and performance,” *IEEE Transactions on Automatic Control*, vol. 55, no. 8, pp. 1781–1796, Aug 2010.

[13] K. Wang, P. Xu, C.-M. Chen, S. Kumari, M. Shojafar, and M. Alazab, “Neural architecture search for robust networks in 6g-enabled massive iot domain,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5332–5339, 2021.

[14] A. Razaque, F. Amsaad, M. Abdulgader et al., “A mobility-aware human-centric cyber-physical system for efficient and secure smart healthcare,” *IEEE Internet of Things Journal*, vol. 99, p. 1, 2022.

[15] B. Mokhtar and M. Azab, “Survey on security issues in vehicular ad hoc networks,” *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[16] J. Pan, Q. Peng, S. Zhan, and J Bai, “Multiscenario-based train headway analysis under virtual coupling system,” *Journal of Advanced Transportation*, vol. 10, pp. 1–20, 2021.

[17] A. D. Gupta, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global, USA, 2016.

[18] F. Taylor, *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*, CRC Press, 2018.

[19] C. Chen, C. Wang, T. Qiu, M. Atiquzzaman, and D. O. Wu, “Caching in vehicular named data networking: architecture, schemes and future directions,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2378–2407, 2020.

[20] C. Chen, Y. Zhang, Z. Wang, S. Wan, and Q. Pei, “Distributed computation offloading method based on deep reinforcement learning in icv,” *Applied Soft Computing*, vol. 103, Article ID 107108, 2021.

[21] L. Zhu, H. Liang, H. Wang, B. Ning, and T. Tang, “Joint security and train control design in blockchain-empowered cbtc system,” *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8119–8129, 2022.

[22] A. Almomani, M. Alauthman, F. Albalas, O. Dorgham, and A. Obeidat, “An online intrusion detection system to cloud computing based on neucube algorithms,” *International Journal of Cloud Applications and Computing*, vol. 8, no. 2, pp. 96–112, 2018.

[23] A. Al Dmour, M. Almiani, T. Aidja, and A. Razaque, “Context-aware latency reduction protocol for secure encryption and decryption,” *International Journal of High Performance Computing and Networking*, vol. 12, no. 3, p. 251, 2018.

[24] Y. Wu, Z. Wei, J. Weng, and R. H. Deng, “Position manipulation attacks to balise-based train automatic stop control,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5287–5301, 2018.

[25] J. Feng, L. Liu, Q. Pei, and K. Li, “Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 1–2700, 2022.

[26] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, “Optimal linear cyber-attack on remote state estimation,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 4–13, 2017.

[27] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, “Sinr-based dos attack on remote state estimation: a game-theoretic approach,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 3, pp. 632–642, 2017.

[28] H. Zhang and W. X. Zheng, “Denial-of-service power dispatch against linear quadratic control via a fading channel,” *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3032–3039, 2018.

[29] Q. Geng, L. Zhao, L. Li, and F. Liu, “A dynamic controller design for trajectory tracking control of wheeled mobile robot under stochastic denial of service attacks,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. Early Access, p. 1, 2022.

[30] L. Zhu, Y. Li, F. R. Yu, B. Ning, T. Tang, and X. Wang, “Cross-layer defense methods for jamming-resistant cbtc systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, pp. 7266–7278, 2021.

[31] M. Zhou, C. Liu, A. Abiri Jahromi, D. Kundur, J. Wu, and C. Long, “Revealing vulnerability of n-1 secure power systems to coordinated cyber-physical attacks,” *IEEE Transactions on Power Systems*, vol. Early Access, p. 1, 2022.

[32] S. Stickel, M. Schenker, H. Dittus et al., “Technical feasibility analysis and introduction strategy of the virtually coupled train set concept,” *Scientific Reports*, vol. 12, no. 4248, pp. 1–13, 2022.

[33] X. Wang, L. Liu, T. Tang, and W. Sun, “Enhancing communication-based train control systems through train-to-train communications,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 4, pp. 1544–1561, 2019.

[34] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, Fourth 2009.

[35] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 1–10, 2018.

[36] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[37] C. Fachkha, E. Bou-Harb, and M. Debbabi, "Inferring distributed reflection denial of service attacks from darknet," *Computer Communications*, vol. 62, no. 1/2, pp. 59–71, 2015.

[38] G. Welch and G. Bishop, *An Introduction to the Kalman Filter*, University of North Carolina, 1995.

[39] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, 2004.

[40] L. Shi, P. Cheng, and J. Chen, "Sensor data scheduling for optimal state estimation with communication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693–1698, 2011.

[41] O. Vega Amaya, "The average cost optimality equation: a fixed point approach," *Boletín De La Sociedad Matemática Mexicana Tercera Serie*, vol. 9, no. 1, pp. 85–195, 2003.

[42] C. De Persis and P. Tesi, "Networked control of nonlinear systems under Denial-of-Service," *Systems & Control Letters*, vol. 96, pp. 124–131, 2016.

[43] K. Kinjo, E. Uchibe, and K. Doya, "Evaluation of linearly solvable Markov decision process with dynamic model learning in a mobile robot navigation task," *Frontiers in Neurorobotics*, vol. 7, p. 7, 2013.

[44] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843–852, 2016.

[45] D. E. Quevedo and A. Ahlen, "A predictive power control scheme for energy efficient state estimation via wireless sensor networks," in *Proceedings of the 2008 47th IEEE Conference on Decision and Control*, pp. 1103–1108, IEEE, Cancun, Mexico, 09-11 December 2008.

[46] D. E. Quevedo, A. AhleN, and J. Ostergaard, "Energy efficient state estimation with wireless sensors through the use of predictive power control and coding," *IEEE Transactions on Signal Processing*, vol. 58, no. 9, pp. 4811–4823, 2010.

[47] T. Stykel and V. Simoncini, "Krylov subspace methods for projected Lyapunov equations," *Applied Numerical Mathematics*, vol. 62, no. 1, pp. 35–50, 2012.

[48] D. Canca, E. Barrena, E. Algaba, and A. Zarzo, "Design and analysis of demand-adapted railway timetables," *Journal of Advanced Transportation*, vol. 48, no. 2, pp. 119–137, 2014.

[49] E. Barrena, D. Canca, L. C. Coelho, and G. Laporte, "Single-line rail rapid transit timetabling under dynamic passenger demand," *Transportation Research Part B*, vol. 70, no. C, pp. 134–150, 2014.

[50] H. Wang, F. R. Yu, and H. Jiang, "Modeling of radio channels with leaky coaxial cable for lte-m based cbtc systems," *IEEE Communications Letters*, vol. 20, no. 5, pp. 1038–1041, 2016.

[51] H. W. Wang, B. Ning, H. L. Jiang, W. N. Liu, and D. Beijing, "Research on propagation characteristics of 2.4 GHz WLAN in tunnels for CBTC train ground communication systems," *Journal of the China Railway Society*, vol. 35, no. 10, pp. 52–58, 2013.

[52] J. Li, Z. Zhao, R. Li, and H. Zhang, "Ai-based two-stage intrusion detection for software defined iot networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2093–2102, 2019.