Chinese Journal of Electronics
Vol.32, No.5, Sept. 2023

A Security Defense Method Against Eavesdroppers in the Communication-Based Train Control System

YANG Li[1], WEI Xiukun[2], and WEN Chenglin[1,3]

(1. *School of Cyberspace College, Hangzhou Dianzi University, Hangzhou 310018, China*)

(2. *State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China*)

(3. *School of Automation, Guangdong University of Petrochemical Technology, Maoming 525000, China*)

Abstract — The communication-based train control system is the safety guarantee for automatic train driving. Wireless communication brings network security risks to the communication-based train control system. The eavesdropping of the transmitted information by unauthorized third-party personnel will lead to the leakage of the estimated value of the system state, which will lead to major accidents. This paper focuses on solving the problem of defense against eavesdropping threats and proposes an eavesdropping defense architecture. This defense architecture includes a coding mechanism based on punishing eavesdroppers, an information upload trigger mechanism based on contribution, and a random information transmission strategy, and provides a guarantee for the privacy protection of information. This research makes three contributions. First, it is the first attempt to construct an information encoding mechanism with punishing eavesdroppers as the objective function; Second, for the first time, an information upload trigger mechanism based on contribution is proposed; Third, the strategy of random transmission of information is proposed. The proposed method in this paper is verified by taking the medium and low-speed maglev train as the object. The experimental results show that, compared with Gaussian noise and non-Gaussian noise mechanisms, the coding mechanism proposed in this paper can not only protect the security of information but also make the estimation error of eavesdroppers tend to be infinite. Using the state estimation error as a metric, the average growth rate of the state estimation error of the system using the trigger mechanism in this paper is less than 2% while improving the security of the system. The transmission strategy in this paper does not increase the system state estimation error while improving the security of the system.

Key words — The communication-based train control system, Coding mechanism based on punishing eavesdroppers, Contribution-based information upload trigger mechanism, Random transmission strategy.

I. Introduction

As a key infrastructure in China, the rail transit system has the characteristics of convenience, economy, and safety. In recent years, the construction scale of the rail transit system has developed rapidly [1]–[3]. The rail transit system covers almost all cities in China.

With the rapid development of computing, control, communication, and network technologies, traditional rail systems are also undergoing significant changes. Computers and information technology are used in rail transit systems, and new communication-based train control (CBTC) systems are proposed. The communication-based train control system uses wireless communication to transmit the state and control commands of the train and realizes the automatic control of the train. The communication-based train control system mainly includes automatic train supervision (ATS), automatic train protection (ATP), automatic train operation (ATO), etc. [4]. In the future, communication-based train control systems will play an important role in modern rail transit systems.

The CBTC systems use dedicated wireless communication technologies such as GSM-R, LTE-R, or IEEE 802.11 [5]. However, an isolated network cannot guarantee network security. With the continuous enrichment of network attack methods, the characteristics of open

Manuscript Received July 30, 2022; Accepted Sept. 26, 2022. This work was supported by the National Natural Science Foundation of China (62120106011, 61933013, 61733015, U1934221) and the State Key Laboratory of Rail Traffic Control and Safety Contract, Beijing Jiaotong University (RCS2021K007).

DOI:10.23919/cje.2022.00.248

networks, insider attackers, and the importance of infrastructure make the security of rail transit systems gain extensive attention from researchers [6], [7].

There are two main types of common network threats, namely, active attacks (e.g., denial of service attacks, spoofing attacks, and replay attacks) and passive eavesdropping [8]. Research progress has been made on the problem of active attacks on communication-based train control systems. However, passive eavesdropping on communication-based train control systems remains a major challenge. Eavesdroppers lurk in wireless communications to steal transmitted data. The threat of eavesdropping is different from the threat of attack. The threat of attack will cause packet loss or tampering with information, but the threat of eavesdropping will only cause information leakage. Different from existing research results, in this work, we not only consider an encoding mechanism based on punishing eavesdroppers but also propose a trigger mechanism based on contribution upload and a strategy of random transmission.

The main contributions of this paper are as follows:

1) An information encoding mechanism based on punishing eavesdroppers is proposed. The encoding mechanism not only protects the privacy of the transmitted data but also has a punitive effect on eavesdroppers.

2) A trigger mechanism based on contribution upload is proposed. If the wireless communication is silent, the information will not be stolen. A trigger mechanism based on contribution can assess whether the information is uploaded to reduce the risk of information theft.

3) A random information transmission strategy is proposed. This strategy breaks the fixed order of information transmission. The random order of information transmission will make it difficult for eavesdroppers to collect information.

II. Related Work

Several defense methods have been proposed for communication-based train control systems. In [9], researchers make the system continue to work under DoS attacks by enhancing the robustness of the communication-based train control system. In [10], the researchers proposed an event-based trigger mechanism to enhance the stability of the system under jamming attacks. Of course, there is a phenomenon of packet loss in wireless communication. The nature of the phenomenon is similar to the nature of jamming attacks. Many researchers have proposed several solutions to the problem of packet loss in wireless communications. In [11], the researchers proposed a recursive filtering method for train control systems based on communication packet loss. In [12], researchers developed an algorithm for a communication-based train control system that can improve the accuracy and availability of train positioning.

The main defense against eavesdropping threats is an encoding mechanism. At present, there are few types of research on eavesdropping defense methods for communication-based train control systems, but progress has been made in defense methods against eavesdropping threats in the fields of cyber-physical systems, federated learning, and industrial Internet systems. In [13], [14], researchers adopted noise-based coding mechanisms to defend against information theft. In [15], the authors propose a novel encoding mechanism to defend against eavesdroppers, which employs a combination of linear transformation and noise. The essence of the eavesdropping defense problem is the same as the privacy protection problem. In [16], the researchers proposed a method based on non-Gaussian noise slicing plus noise for the privacy problem of federal learning. Of course, homomorphic encryption is an important technology to ensure the privacy and security of information. Researchers use homomorphic encryption for data privacy protection in federated learning [17], [18]. Differential privacy technology is the latest method to protect data privacy in recent years. In [19], researchers applied differential privacy techniques to in-vehicle cyber-physical systems for protecting the location information of vehicles. In [20], the researchers review the recent research progress and future challenges of differential privacy techniques in industrial Internet systems. Similarly, researchers not only solve the DoS attack defense scheduling problem but also the eavesdropping defense scheduling problem [8], [21], [22].

Based on the above, according to our research, there are few existing eavesdropping threat defense methods for communication-based train control systems. If the defense methods in other fields are applied to the communication train control system, the following problems also exist. First, the researcher uses an encoding mechanism that adds either Gaussian noise or non-Gaussian noise. Of course, in recent years, researchers have proposed some improved coding mechanisms based on Gaussian noise or non-Gaussian noise. These mechanisms add objective functions such as saving transmission energy from the perspective of defenders, but they have not proposed coding mechanisms from the perspective of punishing eavesdroppers. Then, homomorphic encryption-based methods are not efficient in handling big data. The work in [8] defends against eavesdropping threats by scheduling. This does not serve as a primary defense against the eavesdropping threat. Finally, researchers have shown in [21] that an attacker cannot listen to all wireless communication channels at every moment. To this end, we propose an encoding mechanism based on punishing eavesdroppers, supplemented by a contribution-based trigger mechanism for message uploads and a random transmission policy. Compared with Gaussian noise/non-Gaussian noise coding, the method proposed in this paper can achieve the effect of punishing eavesdroppers. Similarly, the proposed message upload trigger mechanism and transmission strategy can further reduce the probability of success of eavesdroppers and achieve information protection.

III. System Model

In this section, we focus on the mathematical modeling of a communication-based train control system. The communication-based train control system is a representative form of a cyber-physical system in the field of rail transit. In a communication-based train control system, the onboard automatic train protection (OATP) on the train transmits the train's operating status (position and speed) via wireless communication to the access point (AP), which transmits the information to the remote ATS via a wired network. Again, this is a two-way process [23]. After the remote ATS has performed a status estimation, the information is sent to the AP via the wired network for train operation instructions. The AP transmits the train operation instructions to the OATP on the train through the wireless network, the OATP determines the speed and position of the train, and the onboard automatic train operation (OATO) will execute the train operation [12]. As shown in Fig.1.

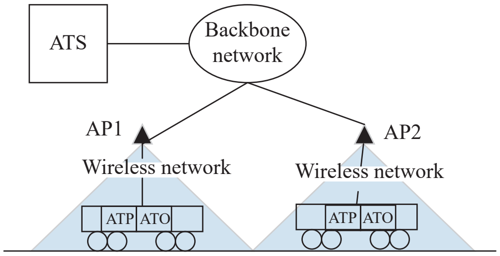

Fig. 1. Schematic diagram of communication-based train control system.

We use Newton's dynamic equations to describe the dynamic equations of the train as follows [24]:

$$\begin{cases} \dfrac{\mathrm{d}x(k)}{\mathrm{d}k} = v(k) \\ M_{\mathrm{tr}} \dfrac{\mathrm{d}v(k)}{\mathrm{d}k} = u(k) - f_r(k) - F_{\mathrm{grad}}(k) \end{cases} \tag{1}$$

wher $x(k)$ is the position of the train; $v(k)$ is the speed of the train; $u(k)$ is the tractive force of the train; $f_r(k)$ is the resistance of the train; M_{tr} is the mass of the train, $M_{\mathrm{tr}} = (1+\lambda)M$, λ is the rotation allowance; $F_{\mathrm{grad}}(k)$ is the force generated by the gradient, $F_{\mathrm{grad}}(k)= Mg\sin(\theta(x(k)))$. Definition $\tilde{x}(k) = [x^{\mathrm{T}}(k)v^{\mathrm{T}}(k)]^{\mathrm{T}}$. The sensor obtains position information and velocity information with a fixed sampling period. The discretization equation of (1) is as follows:

$$\tilde{x}(k+1) = \tilde{A}x(k) + \tilde{B}\tilde{u}(k) + \tilde{E}(\tilde{f}_r(k) + \tilde{F}_{\mathrm{grad}}(k)) \tag{2}$$

$$\tilde{y}(k) = \tilde{C}\tilde{x}(k) + \tilde{v}(k) \tag{3}$$

According to [1], considering the diversity of the train operating environment, multi-sensor systems (GPS, INS, speed sensor) are adopted to obtain the status of the train (e.g., position and speed). To do this, rewrite (3) as follows:

$$\tilde{y}_i(k) = \tilde{C}_i\tilde{x}(k) + \tilde{v}_i(k) \tag{4}$$

Based on (2) and (4), the designed recursive filter is as follows:

$$\begin{aligned} \hat{x}(k+1|k) =& \tilde{A}\hat{x}(k|k) + \tilde{B}\tilde{u}(k) + \tilde{E}(\tilde{f} + \tilde{F}_{\mathrm{grad}}(k)) \\ \hat{x}(k+1|k+1) =& \hat{x}(k+1|k) + K(k+1)(\tilde{y}(k+1) \\ & - \tilde{C}\hat{x}(k+1|k)) \end{aligned} \tag{5}$$

where $\hat{x}(k+1|k+1)$ is the best estimate of the state, $K(k+1)$ is the filter gain, $\tilde{y}(k+1) = [\tilde{y}_1(k+1), \tilde{y}_2(k+1), \dots, \tilde{y}_i(k+1)]$, $\tilde{C} = [\tilde{C}_1, \tilde{C}_2, \dots, \tilde{C}_i]$.

IV. Eavesdropping Defense Mechanism Design

The state information of the train is preprocessed before transmission to prevent leakage to eavesdroppers. In this section, we design a defense architecture against eavesdropping shown in Fig.2, which includes a triggering mechanism based on contribution evaluation, an encoding mechanism based on punishing eavesdroppers, and a random transmission mechanism.

1. Trigger mechanism based on contribution

In this subsection, we focus on solving the contribution of information at the k time compared to time $k-1$. Our goal is to design a mechanism based on contribution evaluation to provide guarantees for the safe transmission of information. Based on the above, we adopt the cosine similarity algorithm as the contribution evaluation mechanism. The cosine similarity algorithm is a method for evaluating the similarity of vectors. The measured values of the i-th sensor at time k and time $k-1$ are $y_i(k)$ and $y_i(k-1)$ respectively (written in short: $y(k)$ and $y(k-1)$), as shown below:

$$\cos(y(k), y(k-1)) = \frac{y(k)y(k-1)}{\|y(k)\|\,\|y(k-1)\|} \tag{6}$$

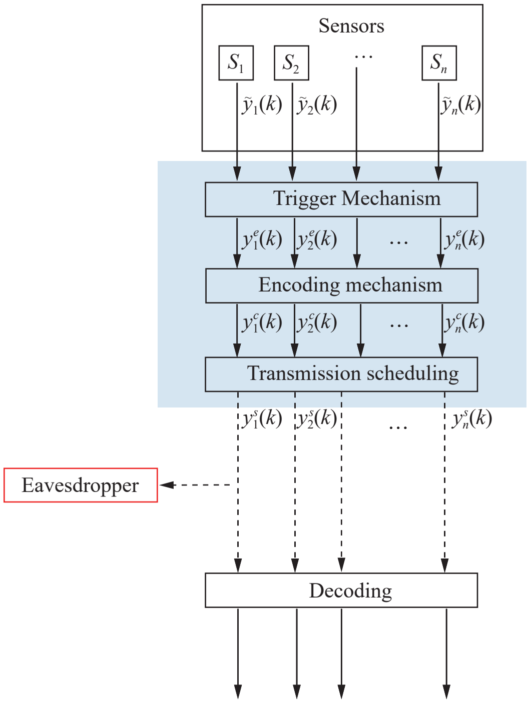

Fig. 2. Eavesdropping defense mechanism framework.

where $y(k)y(k-1)=\sum_{m=1}^{n} y_m(k)y_m(k-1)$, $\|y(k)\|$ is the length of $y(k)$, $\|y(k)\|=\sqrt{\sum_{m=1}^{n}(y(k))_m^2}=\sqrt{y(k)y(k)}$. A cosine similarity close to 1 indicates that the two vectors are similar.

The contribution $G(k)$ of the measurement value at the time k is defined as

$$G(k)=\frac{1}{\cos(y(k),y(k-1))} \tag{7}$$

Therefore, the measurement $y_i^e(k)$ delivered by the i-th sensor at time k is

$$y_i^e(k)=y_i(k), G(k)\geq\delta \tag{8}$$

where, δ represents the contribution threshold. The pseudcode of trigger mechanism based on contribution is shown in Algorithm 1.

Algorithm 1 Trigger mechanism based on contribution

```
Input: Measurements $y_i(k)$, $y_i(k-1)$, Threshold $\delta$.
Ensure: $y_i^e(k)$.
Calculate the cosine similarity based on formula (6): $\cos(y_i(k),y_i(k-1))=\frac{y_i(k)y_i(k-1)}{\|y_i(k)\|\|y_i(k-1)\|}$;
Calculate the contribution of the $i$-th sensor at time $k$ based on (7): $C(k)=\frac{1}{\cos(y_i(k),y_i(k-1))}$;
if $C(k)\geq\delta$
    $y_i^e(k)=y_i(k)$;
else
    $y_i(k)$ does not transmit;
end
```

Remark 1 We use the similarity $\cos(y(k),y(k-1))$ of the measurements at time k and time $k-1$ as the criterion to evaluate the contribution degree $G(k)$ of the measurement value at the time k. If the similarity $\cos(y(k),y(k-1))$ of the measurement values at time k and time $k-1$ is higher, the contribution degree $G(k)$ of the measurement value at time k is lower, and vice versa. According to prior knowledge, if the wireless channel is silent, the information will not be stolen. At k moments, we choose to be silent for the low-contributing wireless channels. At the same time, the recursive filter uses the measurement value at time $k-1$ as the measurement value at time k to estimate the state. For example, a period is defined as k moments, and after the contribution evaluation, there are m moments when the information is not uploaded. Assuming that the probability of information being stolen at each moment is p, then the probability of information theft without triggering mechanism in one cycle is: $(\frac{1}{p})k$, and the probability of information theft with trigger mechanism in one cycle: $(\frac{1}{p})(k-m)$, therefore: $(\frac{1}{p})k\geq(\frac{1}{p})(k-m)$.

2. Encoding mechanism

In this subsection, we will describe the encoding mechanism and the design of the encoding matrix respectively. Firstly, we describe the encoding mechanism. On the basis of what is described in Section IV.1, we encode the measurements that are assessed for contribution. As shown below:

$$y_i^c(k)=y_i^e(k)+\chi_i(k) \tag{9}$$

where $\chi_i(k)$ represents the coding matrix of the designed i-th sensor.

Secondly, we elaborate on the design of the encoding matrix. To punish eavesdroppers, we design the encoding matrix. Since we use the random transmission mechanism of the measurement value (explained in Section IV.3), the recursive filter will use the sequential Kalman filtering algorithm. The sequential Kalman filtering method does not require the inversion of high-dimensional matrices. The sequential Kalman filtering method sequentially processes the measurements of the sensors arriving at the fusion center, which makes efficient use of the wait time of the state estimator and better matches the arrival pattern of the actual measurements. More importantly, according to [25], it has been proved that the sequential Kalman filter method can achieve the estimation accuracy of the centralized extended-dimensional Kalman filter method. The recursive (5) is rewritten as follows:

$$\hat{x}(k|k-1)=F\hat{x}(k-1|k-1) \tag{10}$$

$$\hat{P}(k|k-1)=F\hat{P}(k-1|k-1)F^{\mathrm{T}}+Q \tag{11}$$

$$\hat{x}_1(k|k)=\hat{x}(k|k-1)+K_1(k)-[z_1(k)-H_1\hat{x}(k|k-1)] \tag{12}$$

$$K_1(k)=\hat{P}(k|k-1)H_1^{\mathrm{T}}[H_1\hat{P}(k|k-1)H_1^{\mathrm{T}}+R_1]^{-1} \tag{13}$$

$$\hat{P}_1(k|k-1)=[I-K_1(k)H_1]\hat{P}(k|k-1) \tag{14}$$

$$\vdots$$

$$\hat{x}_n(k|k)=\hat{x}_{n-1}(k|k)+K_n(k)[z_n(k)-H_n\hat{x}_{n-1}(k|k)] \tag{15}$$

$$K_n(k)=\hat{P}_{n-1}(k|k)H_n^{\mathrm{T}}[H_n\hat{P}_{n-1}(k|k-1)H_n^{\mathrm{T}}+R_n]^{-1} \tag{16}$$

$$\hat{P}_n(k|k)=[I-K_n(k)H_n]\hat{P}_{n-1}(k|k) \tag{17}$$

$$\hat{x}(k|k)=\hat{x}_n(k|k) \tag{18}$$

$$\hat{P}(k|k)=\hat{P}_n(k|k) \tag{19}$$

where n is the n-th sensor, $z_i(k)$ is the measured value after decoding.

Assumption The eavesdropper obtains the filtering algorithm-sequential Kalman filtering through long-term lurk. The eavesdropper steals the transmitted measurements to obtain the optimal state estimate of the system. Define the measurement value stolen by the eavesdropper as $y_i^a(k)$, as follows:

$$y_i^a(k)=y_i^e(k) \tag{20}$$

It is defined that the optimal state estimate calculated by the eavesdropper based on the stolen measurements is $\hat{x}^a(k|k)$. Based on the defender's perspective, to punish eavesdroppers, we establish the objective function as follows:

$$\lim_{k\to\infty}\|(\hat{x}^a(k|k)-x(k))-(\hat{x}(k|k)-x(k))\|\to\infty \tag{21}$$

where $\hat{x}^a(k|k)-x(k)$ represents the state estimation error of the eavesdropper to the system, $\hat{x}(k|k)-x(k)$ represents the state estimation error of the defender to the system.

Theorem 1 Using formula (21) as the objective function, the coding matrix was designed as

$$\chi_n(k)=H_nA(\hat{x}^a(k-1)-\hat{x}(k-1))+b \tag{22}$$

$$\chi_{n-1}(k)=H_{n-1}A(\hat{x}^a(k-1)-\hat{x}(k-1)) \tag{23}$$

$$\chi_{n-2}(k)=H_{n-2}A(\hat{x}^a(k-1)-\hat{x}(k-1)) \tag{24}$$

$$\vdots$$

$$\chi_1(k)=H_1A(\hat{x}^a(k-1)-\hat{x}(k-1)) \tag{25}$$

where n is the last sensor to be transmitted, b is a constant. Algorithm 2 provides the encoding mechanism.

Proof See Appendix A.

Algorithm 2 Encoding mechanism

```
Input: $y_i^e(k)$ after evaluation by Algorithm 1.
Ensure: $y_i^c(k)$.
1: Calculate the encoding matrix for the first sensor transmitted: $a_1=H_1A(\hat{x}^a(k-1)-\hat{x}(k-1))$;
   Calculate the encoding matrix for the transmitted second sensor: $a_2=H_2A(\hat{x}^a(k-1)-\hat{x}(k-1))$;
   Calculate the encoding matrix for the last sensor transmitted: $a_n=H_nA(\hat{x}^a(k-1)-\hat{x}(k-1))+b$;
2: At time $k$, encode the first sensor: $y_1^c(k)=y_1^e(k)+a_1$;
   Encode the second sensor: $y_2^c(k)=y_2^e(k)+a_2$;
   Encode the last sensor: $y_n^c(k)=y_n^e(k)+a_n$.
```

3. Packet random scheduling protocol

In this subsection, we design a multi-sensor packet scheduling mechanism. For the problem of jamming attacks, an optimal multi-sensor transmission mechanism is proposed in [21]. The jamming attack behavior is different from the eavesdropping behavior. The jamming attack behavior will destroy the state estimation, but the eavesdropping behavior has no destructive effect. Therefore, unlike [21], we focus on adopting a facile packet scheduling protocol to reduce the risk of information theft. Based on the above, we adopt a random packet scheduling protocol. The protocol randomly assigns communication opportunities to sensor nodes. All sensors are randomly divided into $N(N\geq 1)$ nodes in advance. Without loss of generality, each node is assigned a communication opportunity with equal probability as follows:

$$\Pr\{k=i\}=\frac{1}{N} \tag{26}$$

At the time k, the delivered measurement y_i^s is

$$y_i^s(k)=\eta(k)y_i^{\bar{s}}(k) \tag{27}$$

where $\eta(k)=\mathrm{diag}\{0,0,\dots,0,\vartheta_{i(k)},0,\dots,0\}$, $\vartheta_{i(k)}=I$, $i(k)=\mathrm{random}[1,N]$; $y_i^{\bar{s}}(k)=[y_1^c(k),y_2^c(k),\dots,y_N^c(k)]$.

Remark 2 At present, the CSMA/CA protocol is used for scheduling [12], but the scheduling order of this protocol is fixed. Since the eavesdropper has limited energy, it cannot monitor all wireless communication channels simultaneously for a long time. Compared with the fixed sequential transmission, random transmission can reduce the probability of eavesdroppers obtaining information.

V. Experiments

To verify the effectiveness of the method proposed in this paper, we will conduct a series of simulation experiments in this section. The low and medium-speed maglev trains in [26] were used as experimental subjects. MATLAB was used as the experimental tool on a desktop equipped with an Intel Core i5-10210U processor running at 2.11 GHz and 8 GB of RAM.

1. Simulation analysis of trigger mechanism based on contribution

In this subsection, we will conduct an experimental simulation analysis of the proposed contribution-based triggering mechanism. Fig.3 shows the upload trigger mechanism of the three sensors, where 1 means that the message is not passed at that moment and 0 means that the message is passed at that moment.

It can be seen from Fig.3 that sensor 1 does not transmit information to the remote state estimator at $k = 42$, 44, 69, 70, 79, 80, 81, sensor 2 does not transmit information to the remote state estimator at $k = 17$, 18, 20, 27, 34, 38, 42, 46, 49, 50, 62, 65, 66, 80, 81, 86, 93, 94, 99 and sensor 3 does not transmit information to the remote state estimator at $k = 43$, 51, 75, 79, 80, respectively. Assuming that the probability of information being stolen at each moment is 1/5, the probability of information being stolen by the three sensors using the trigger mechanism and not using the trigger mechanism in one cycle are

$$\begin{cases} (1/5) \times 100 > (1/5) \times 93 \\ (1/5) \times 100 > (1/5) \times 79 \\ (1/5) \times 100 > (1/5) \times 95 \end{cases}$$

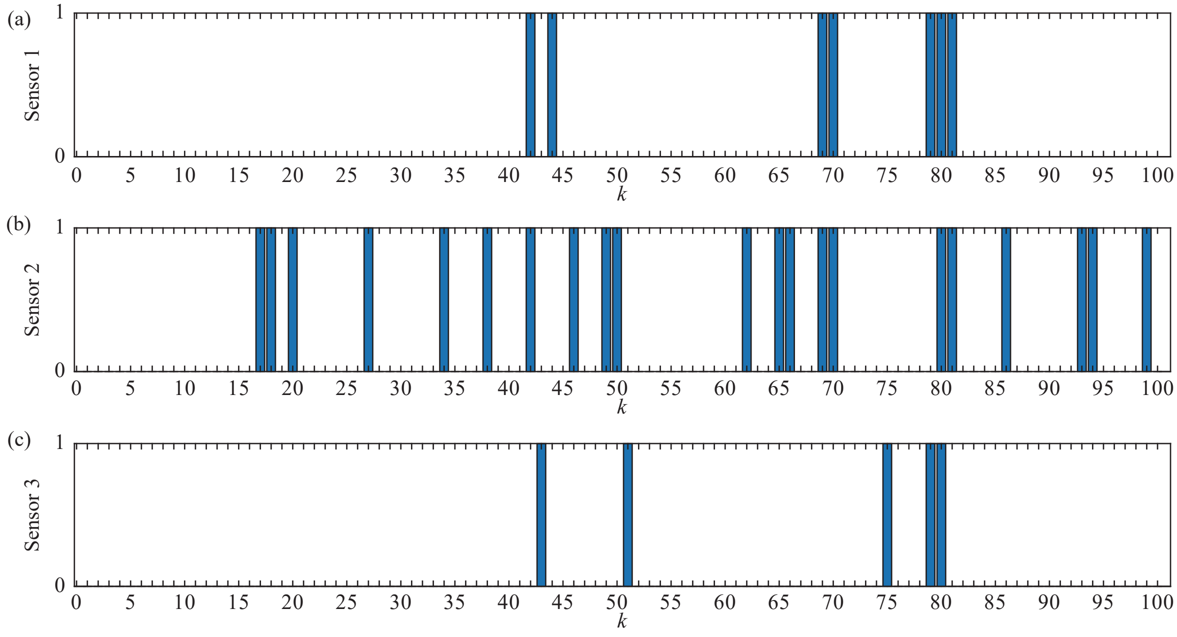

Fig. 3. Information upload. (a) Sensor 1; (b) Sensor 2; (c) Sensor 3.

The estimation error of the recursive filter is used as the evaluation index. Fig.4 shows the estimation error of the recursive filter. The blue dashed line segment represents the state estimation error without using the trigger mechanism, and the red solid line segment represents the state estimation error using the trigger mechanism. Define agv_Error_1 to represent the mean value of state estimation error without triggering mechanism, and agv_Error_2 to represent the mean value of state estimation error using trigger mechanism. Then the mean state estimation error growth rate can be expressed as $gr = \frac{agv\_Error\_2 - agv\_Error\_1}{agv\_Error\_1}$. agv_Error_1, agv_Error_2 and gr are illustrated in Table 1. The state estimated average error growth rate of state 1 is 0.42%, and the state estimated average error growth rate of state 2 is 1.58%.

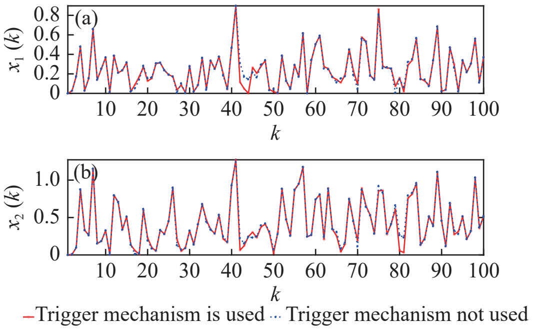

Fig. 4. State estimation error. (a) x_1; (b) x_2.

Table 1. State estimation error mean

agv_Error_1	agv_Error_2	gr
0.2396	0.2406	0.42%
0.4249	0.4316	1.58%

Through the analysis of simulation experiments, it can be seen that the contribution-based triggering mechanism proposed in this paper has little influence on the estimation error of the recursive filter. According to prior knowledge, the longer the wireless channel remains silent, the lower the probability of an eavesdropper obtaining information. Based on the above, the effectiveness of the contribution-based triggering mechanism proposed in this paper is proved.

2. Simulation analysis of coding mechanism

In this subsection, we present an experimental simulation analysis of the proposed coding mechanism. Same as Section V.1, the estimation error of the recursive filter is used as the evaluation index. Fig.5 shows the state estimation error of the recursive filter. Fig.6, Fig.7, and Fig.8 show the state estimation errors of the information sender and the information stealer. The red line segment represents the state estimation error of the information sender, which is the same as shown in Fig.5. The blue line segment represents the information stealer's state estimation error. Specifically, the difference is that Fig.6 uses the coding mechanism proposed in this paper, Fig.7 uses the Gaussian noise-based coding mechanism proposed in reference [27], and Fig.8 uses the non-Gaussian noise-based coding mechanism proposed in [16].

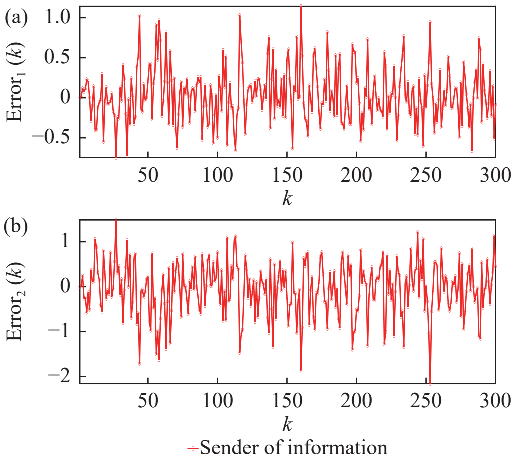

Fig. 5. The state estimation error of the recursive filter. (a) Error$_1$; (b) Error$_2$.

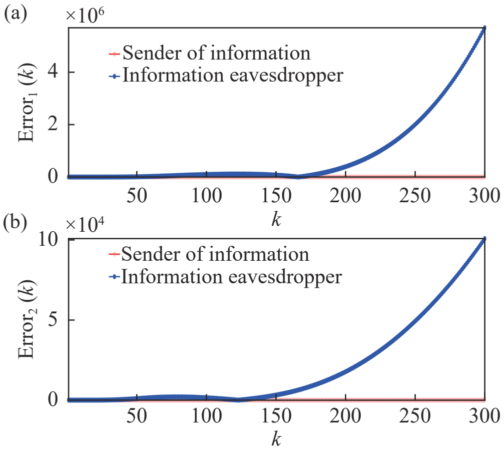

Fig. 6. The state estimation error based on the method proposed in this paper. (a) Error$_1$; (b) Error$_2$.

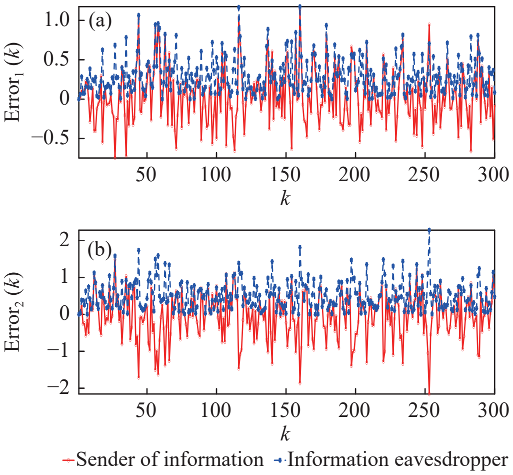

Fig. 7. State estimation error based on Gaussian noise coding [27]. (a) Error$_1$; (b) Error$_2$.

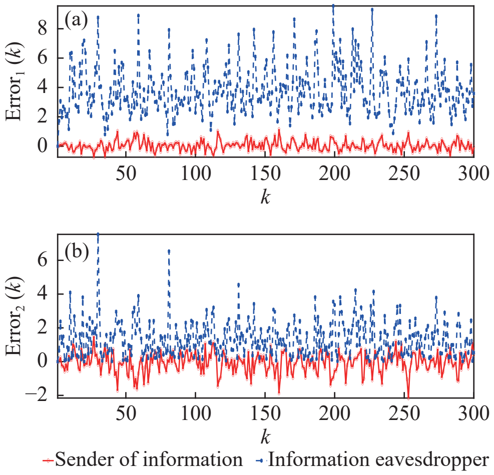

Fig. 8. State estimation error based on non-Gaussian noise coding [16]. (a) Error$_1$; (b) Error$_2$.

Through the analysis of simulation experiments, it can be seen that the mechanism using Gaussian noise coding and the mechanism using non-Gaussian noise coding can increase the state estimation error, but the estimation error will not tend to infinity. The coding mechanism proposed in this paper can also increase the state estimation error, and can cause the state estimation error of the information eavesdropper to tend to infinity, thus achieving the purpose of punishing the eavesdropper. Based on the above, the effectiveness and advanced nature of the coding mechanism proposed in this paper are proved.

3. Simulation analysis of random scheduling protocol

In this subsection, we will perform an experimental simulation analysis of the proposed stochastic scheduling protocol. The same as Sections V.1 and V.2, the estimation error of the recursive filter is used as the evaluation index. We use the transport protocol shown below (this protocol is a randomly defined protocol):

$$\begin{cases} [3,1,2], & \mathrm{mod}(k,2)==0 \\ [2,3,1], & \mathrm{mod}(k,3)==0 \\ [1,2,3], & \text{otherwise} \end{cases}$$

where $[3,1,2]$ indicates the transmission sequence of sensors as sensor 3, sensor 1, sensor 2; $[2,3,1]$ indicates the transmission sequence of sensors as sensor 2, sensor 3, sensor 1; $[1,2,3]$ indicates the transmission sequence of sensors as sensor 1, sensor 2, sensor 3. $\mathrm{mod}(a,b)$ is the remainder of dividing b by a. Fig.9 shows the state estimation error values with and without the random scheduling strategy. Define agv_Error_norm to represent the mean value of state estimation error without using random scheduling protocol, agv_Error_random to represent the mean value of state estimation error using random scheduling protocol, and then the growth rate of mean state estimation error can be defined as $gr\_rd = \frac{agv\_Error\_random - agv\_Error\_norm}{agv\_Error\_norm}$, which are shown in Table 2.

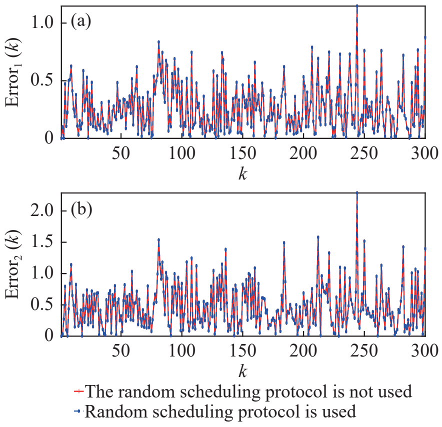

Fig. 9. State estimation error based on random scheduling protocol. (a) Error$_1$; (b) Error$_2$.

Through the analysis of simulation experiments, it can be seen that the protocol based on random transmission proposed in this paper has no effect on the estimation error of the recursive filter. This conclusion is the same as that of the sequential Kalman filtering algorithm. According to a priori knowledge, it takes a lot of energy for an eavesdropper to monitor all communication channels. The eavesdropper needs to choose the order of the eavesdropping channel. For this reason, we use a random transmission protocol to reduce the probability of the eavesdropper to obtain information. Based on the above, the validity of the random transmission protocol proposed in this paper is proved.

Table 2. Estimation error mean of random scheduling protocol

agv_Error_norm	agv_Error_random	gr_rd
0.2629	0.2629	0%
0.4703	0.4703	0%

VI. Conclusions

This paper designs an eavesdropping defense architecture consisting of a coding mechanism based on punishing eavesdroppers, an information upload trigger mechanism based on contribution, and a random information transmission strategy. Our proposed architecture combines an encoding mechanism, an event-triggered mechanism, and an information transfer strategy. First, the contribution of the information is evaluated to determine whether the information is transmitted. Then, an encoding mechanism is performed based on the information after evaluation. Finally, the encoded information is transmitted using a random transmission strategy. The effectiveness of the proposed method has been demonstrated by conducting experiments on low and medium speed maglev trains. There are many challenges exist in the current manuscript version that did not consider the energy saving of the transmitter, and the information at the receiving end cannot be used directly and needs to go through a decoding mechanism. Future research directions include the improvement of Kalman filtering algorithm based on coding mechanism, the coding mechanism based on penalty of eavesdroppers and transmitters with limited energy, and the multiplicative coding mechanism.

Appendix A. Proof of Theorem 1

$$\begin{aligned}
&(\hat{x}^a_n(k|k) - x(k)) - (\hat{x}_n(k|k) - x(k)) \\
=&\hat{x}^a_n(k|k) - \hat{x}_n(k|k) \\
=&\ \hat{x}^a_{n-1}(k|k) + K_n(y^a_n - H_n\hat{x}^a_{n-1}(k|k)) - \hat{x}_{n-1}(k|k) - K_n(y_n - H_n\hat{x}_{n-1}(k|k)) \\
=&\ K_na_n + (I - K_nH_n)(\hat{x}^a_{n-1}(k|k) - \hat{x}_{n-1}(k|k)) \\
=&\ K_na_n + (I - K_nH_n)(\hat{x}^a_{n-2}(k|k) + K_{n-1}(y^a_{n-1} - H_{n-1}\hat{x}^a_{n-2}(k|k)) - \hat{x}_{n-2}(k|k) - K_{n-1}(y_{n-1} - H_{n-1}\hat{x}_{n-2}(k|k))) \\
=&\ K_na_n + (I - K_nH_n)K_{n-1}a_{n-1} + (I - K_nH_n)(I - K_{n-1}H_{n-1})(\hat{x}^a_{n-2}(k|k) - \hat{x}_{n-2}(k|k))) \\
=&\ K_na_n + (I - K_nH_n)K_{n-1}a_{n-1} + (I - K_nH_n)(I - K_{n-1}H_{n-1})(A\hat{x}^a(k-1|k-1) + K_{n-2}(y^a_{n-2} - H_{n-2}A\hat{x}^a(k-1|k-1)) \\
&-A\hat{x}(k-1|k-1) - K_{n-2}(y_{n-2} - H_{n-2}A\hat{x}(k-1|k-1))) \\
=&\ K_na_n + K_{n-1}a_{n-1} - K_nH_nK_{n-1}a_{n-1} + (I - K_nH_n)(I - K_{n-1}H_{n-1})(A\hat{x}^a(k-1|k-1) - A\hat{x}(k-1|k-1) + K_{n-2}(y^a_{n-2} - y_{n-2})
\end{aligned}$$

$$
\begin{aligned}
&+K_{n-2}H_{n-2}A(\hat{x}(k-1|k-1)-\hat{x}^a(k-1|k-1)))\\
=\ &K_na_n+K_{n-1}a_{n-1}-K_nH_nK_{n-1}a_{n-1}\\
&+(I-K_nH_n)(I-K_{n-1}H_{n-1})[K_{n-2}a_{n-2}+(I-K_{n-2}H_{n-2})A(\hat{x}^a(k-1|k-1)-\hat{x}(k-1|k-1))]\\
=\ &K_na_n+K_{n-1}a_{n-1}-K_nH_nK_{n-1}a_{n-1}\\
&+(I-K_{n-1}H_{n-1}-K_nH_n+K_nH_nK_{n-1}H_{n-1})[K_{n-2}a_{n-2}+(I-K_{n-2}H_{n-2})A(\hat{x}^a(k-1|k-1)-\hat{x}(k-1|k-1))]\\
=\ &K_na_n+K_{n-1}a_{n-1}-K_nH_nK_{n-1}a_{n-1}+K_{n-2}a_{n-2}-K_{n-1}H_{n-1}K_{n-2}a_{n-2}-K_nH_nK_{n-2}a_{n-2}+K_nH_nK_{n-1}H_{n-1}K_{n-2}a_{n-2}\\
&+(I-K_{n-1}H_{n-1}-K_nH_n+K_nH_nK_{n-1}H_{n-1})(I-K_{n-2}H_{n-2})A(\hat{x}^a(k-1|k-1)-\hat{x}(k-1|k-1))\\
=\ &K_na_n+(K_{n-1}-K_nH_nK_{n-1})a_{n-1}+(K_{n-2}-K_{n-1}H_{n-1}K_{n-2}-K_nH_nK_{n-2}+K_nH_nK_{n-1}H_{n-1}K_{n-2})a_{n-2}\\
&+[(I-K_{n-2}H_{n-2}-K_{n-1}H_{n-1}-K_{n-1}H_{n-1}K_{n-2}H_{n-2}-K_nH+K_nH_nK_{n-2}H_{n-2}+K_nH_nK_{n-1}H_{n-1}\\
&-K_nH_nK_{n-1}H_{n-1}K_{n-2}H_{n-2})A(\hat{x}^a(k-1|k-1)-\hat{x}(k-1|k-1))]
\end{aligned}
$$

Let: $\chi_n(k)=H_nA(\hat{x}^a(k-1)-\hat{x}(k-1))+b$, $\chi_{n-1}(k)=H_{n-1}A(\hat{x}^a(k-1)-\hat{x}(k-1))$, $\chi_{n-2}(k)=H_{n-2}A(\hat{x}^a(k-1)-\hat{x}(k-1))$.

Therefore: $\hat{x}_i^a(k|k)-\hat{x}_i(k|k)=A[\hat{x}_i^a(k-1|k-1)-\hat{x}_i(k-1|k-1)]+K_nb$ is an increasing function and tends to infinity.

References

[1] Z. X. Deng, H. F. Song, H. Huang, *et al.*, "Multi-sensor based train localization and data fusion in autonomous train control system," in *Proceedings of 2020 Chinese Automation Congress (CAC)*, Shanghai, China, 2020.

[2] T. Wen, G. Xie, Y. Cao, *et al.*, "A DNN-based channel model for network planning in train control systems," *IEEE Transactions on Intelligent Transportation Systems*, vol.23, no.3, pp.2392–2399, 2022.

[3] L. Yang, C. L. Wen, and T. Wen, "Multilevel fine fingerprint authentication method for key operating equipment identification in cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol.19, no.2, pp.1217–1226, 2023.

[4] S. Kim, Y. Won, I. H. Park, *et al.*, "Cyber-physical vulnerability analysis of communication-based train control," *IEEE Internet of Things Journal*, vol.6, no.4, pp.6353–6362, 2019.

[5] H. W. Wang, F. R. Yu, L. Zhu, *et al.*, "A cognitive control approach to communication-based train control systems," *IEEE Transactions on Intelligent Transportation Systems*, vol.16, no.4, pp.1676–1689, 2015.

[6] X. Wang, L. Zhu, H. W. Wang, *et al.*, "Robust distributed cruise control of multiple high-speed trains based on disturbance observer," *IEEE Transactions on Intelligent Transportation Systems*, vol.22, no.1, pp.267–279, 2021.

[7] L. Zhu, Y. Li, F. R. Yu, *et al.*, "Cross-layer defense methods for jamming-resistant CBTC systems," *IEEE Transactions on Intelligent Transportation Systems*, vol.22, no.11, pp.7266–7278, 2021.

[8] L. Wang, X. H. Cao, B. W. Sun, *et al.*, "Optimal schedule of secure transmissions for remote state estimation against eavesdropping," *IEEE Transactions on Industrial Informatics*, vol.17, no.3, pp.1987–1997, 2021.

[9] B. Gao and B. Bu, "Deep reinforcement learning-based resilient control method for CBTC systems through train-to-train communications under adversarial attacks," in *Proceedings of 2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, Indianapolis, IN, USA, pp.3679–3684, 2021.

[10] S. M. Ma, B. Bu, and H. W. Wang, "A virtual coupling approach based on event-triggering control for CBTC systems under jamming attacks," in *Proceedings of the IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Victoria, BC, Canada, pp.1–6, 2020.

[11] T. Wen, L. Zou, J. L. Liang, *et al.*, "Recursive filtering for communication-based train control systems with packet dropouts," *Neurocomputing*, vol.275, pp.948–957, 2018.

[12] L. Zou, T. Wen, Z. D. Wang, *et al.*, "State estimation for communication-based train control systems with CSMA protocol," *IEEE Transactions on Intelligent Transportation Systems*, vol.20, no.3, pp.843–854, 2019.

[13] J. H. Huang, D. W. C. Ho, F. F. Li, *et al.*, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica*, vol.121, article no.109182, 2020.

[14] H. Guo, Z. H. Pang, J. Sun, *et al.*, "An output-coding-based detection scheme against replay attacks in cyber-physical systems," *IEEE Transactions on Circuits and Systems Ⅱ: Express Briefs*, vol.68, no.10, pp.3306–3310, 2021.

[15] W. Yang, D. K. Li, H. Zhang, *et al.*, "An encoding mechanism for secrecy of remote state estimation," *Automatica*, vol.120, article no.109116, 2020.

[16] X. Y. Wang, J. C. Wang, X. Ma, *et al.*, "A differential privacy strategy based on local features of non-Gaussian noise in federated learning," *Sensors*, vol.22, no.7, article no.2424, 2022.

[17] B. Jia, X. S. Zhang, J. W. Liu, *et al.*, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in ⅡoT," *IEEE Transactions on Industrial Informatics*, vol.18, no.6, pp.4049–4058, 2022.

[18] L. Yang and C. L. Wen, "Optimal jamming attack system against remote state estimation in Wireless network control systems," *IEEE Access*, vol.9, pp.51679–51688, 2021.

[19] Y. E. Sun, H. Huang, W. J. Yang, *et al.*, "Toward differential privacy for traffic measurement in vehicular cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol.18, no.6, pp.4078–4087, 2022.

[20] B. Jiang, J. Q. Li, G. H. Yue, *et al.*, "Differential privacy for industrial internet of things: Opportunities, applications, and challenges," *IEEE Internet of Things Journal*, vol.8, no.13, pp.10430–10451, 2021.

[21] L. H. Peng, X. H. Cao, C. Y. Sun, *et al.*, "Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems," *Neurocomputing*, vol.272, pp.571–583, 2018.

[22] C. Y. Li, J. N. Wang, J. Y. Shan, *et al.*, "Robust cooperat-

ive control of networked train platoons: A negative-imaginary systems' perspective," *IEEE Transactions on Control of Network Systems*, vol.8, no.4, pp.1743–1753, 2021.

[23] H. F. Song, S. G. Gao, Y. D. Li, *et al.*, "Train-centric communication based autonomous train control system," *IEEE Transactions on Intelligent Vehicles*, vol.8, no.1, pp.721–731, 2023.

[24] Q. Dong, K. Hayashi, and M. Kaneko, "A new adaptive modulation and coding method for communication-based train control systems using WLAN," *IFAC-PapersOnLine*, vol.49, no.22, pp.139–144, 2016.

[25] X. H. Sun, C. L. Wen, and T. Wen, "Maximum correntropy high-order extended Kalman filter," *Chinese Journal of Electronics*, vol.31, no.1, pp.190–198, 2022.

[26] M. X. Zhang, "*Study on operation control system of medium-low speed maglev train*," *Master's Thesis*, Southwest Jiaotong University, Chengdu, China, 2019. (in Chinese)

[27] L. F. Liu, Z. Y. Xi, *et al.*, "Noise-based-protection message dissemination method for insecure opportunistic underwater sensor networks," *IEEE Transactions on Information Forensics and Security*, vol.17, pp.1610–1623, 2022.

YANG Li was born in 1992. He received the M.E. degree in electronics and communication engineering from the Guangxi Normal University in 2018. He is currently working toward the Ph.D. degree in Cyberspace College of Hangzhou Dianzi University, Hangzhou, China. His main research interests include cyber-physical system security defense and privacy protection, cyber-physical system attack methods. (Email: yl_hhgz@163.com)

WEI Xiukun received the Ph.D. degree from Johannes Kepler University, Linz, Austria, in 2002. From 2006 to 2009, he was a Postdoctoral Researcher with the Delft Center for System and Control, Delft University of Technology, Delft, The Netherlands. From 2002 to 2006, he was a Research Assistant with the Institute of Design and Control of Mechatronical Systems, Johannes Kepler University. He is currently a Professor with the State Key Lab of Rail Traffic Control and Safety, Beijing Jiaotong University, China. His research interests include fault diagnosis and its applications, intelligent transportation systems, and condition monitoring and its applications in a variety of fields, such as rail traffic control, safety, and transportation. (Email: xkwei@bjtu.edu.cn)

WEN Chenglin (corresponding author) was born in 1963. He graduated from Henan University in 1986, graduated from Zhengzhou University with a master degree in 1993 and received a Ph.D. degree from Northwestern Polytechnical University in 1999. He went out of the postdoctoral mobile station of control science and engineering of Tsinghua University in 2002. He is a Professor of Hangzhou Dianzi University and Guangdong University of Petrochemical Technology. His research interests include information fusion and target detection, fault diagnosis and active security control, deep learning and optimization decision-making systems, cyberspace security and attack detection and positioning. (Email: wencl@hdu.edu.cn)