IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 20, 2019, accepted June 30, 2019, date of publication July 5, 2019, date of current version July 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927048

Joint Security and QoS Provisioning in Train-Centric CBTC Systems Under Sybil Attacks

XIAOXUAN WANG[1], (Student Member, IEEE), LINGJIA LIU[2], (Senior Member, IEEE), LI ZHU[1], AND TAO TANG[1]

[1]State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China
[2]Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24060, USA

Corresponding author: Li Zhu (zhulibjtu@gmail.com)

This work was supported in part by the National Crucial Research Plan under Grant 2018YFB1201501, in part by the National Natural Science Foundation of China under Grant 61790575 and Grant 61603031, and in part by the Beijing Natural Science Foundation under Grant L181004 and Grant Z191100010818001, and Project 2018JBM076, Project RCS2019ZT010, and Project RCS2018K008.

ABSTRACT The security and Quality-of-Service (QoS) provisioning are two critical themes in urban rail communication-based train control (CBTC) data communication systems, which can directly affect the train's safe operation. In this paper, we design the novel train-centric CBTC systems using train-to-train (T2T) wireless communication with the innovative security check scheme. The local security certification and cooperative security check are proposed to detect and defense the Sybil attack based on the CBTC T2T communications. The quantized Age of Information (AoI) is used as an integrated QoS and security indicator of the train-centric CBTC data communication systems. The proposed AoI indicator fully considers the impact of the packet drop and re-transmission, Sybil attack, and the cooperative security check on CBTC systems. The policy-based asynchronous reinforcement learning is utilized to improve the integrated AoI performance. The simulation results show that the proposed cooperative security check scheme with the optimization model can achieve improved integrated AoI performance, compared with the traditional security check scheme. Moreover, with the help of the cooperative security check scheme, we detect and defense the Sybil attack against the train-centric CBTC systems with much higher probability.

INDEX TERMS Train-centric CBTC, security, cooperative security check, age of information.

I. INTRODUCTION

The rapid development of urbanization offers great hope for a smart city in near future. For the environmentally effective public transport mode, urban rail transit plays an essential role in a smart city. Moreover, in order to relieve traffic pressure during rush hours, urban rail transit systems are built in more and more developing cities, which can meet the growing need of people's mobility [1]. Efficiency and reliable train control system is desired to ensure smooth and efficient operation of urban rail transit systems and good QoS for customers. With the development of communication and computer techniques, train control systems have radically improved, which have gradually developed from Track-Based Train Control (TBTC) systems to CBTC systems [2].

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

In existing CBTC systems, the Train-to-Wayside (T2W) wireless communication, including wireless local area networks (WLANs) and Long-Term Evolution for Metro (LTE-M), plays vital role in urban rail transit applications [3]. However, because of the disadvantages of T2W wireless communication, poor operability and inefficiency exert significant negative effect on QoS and security of current CBTC systems. Until now, some research has been done to improve the QoS and security performance of CBTC systems, but most studies focus on conventional ground-centric CBTC systems with T2W wireless communication [4], [5].

The development of device-to-device communications [6], [7] offers vehicle-to-vehicle (V2V) wireless communications as a future technology in intelligent transportation. Therefore, as part of V2V, train-to-train (T2T) based wireless communications have become a novel research area in vehicular communication systems. However, although

high-quality service can be provided by direct communication, some researchers [8], [9] have indicated that V2V network is facing plenty of security threats, which can impact the operation efficiency and even life safety. One of these threats is Sybil attack, where a malicious vehicle masquerades as some fabricated identities [10]. Sybil attacks can result in serious harm to V2V/T2T traffic. Malicious drivers can fabricate registered vehicles and broadcast the spurious information to create the illusion of traffic congestion. Then, other vehicles will choose another route and make way for malicious drivers [11]. The consequence of Sybil attack happening in urban rail transit can be more severe than that in a road network. In urban rail transit, wrong safety-critical information, such as train position, movement authority, and emergency text, caused by a Sybil attack, can lead to emergency brake or rear-end collision. These incidents and accidents not only reduce the operation efficiency, but sometimes influence the life safety of passengers as well. Although some methods, such as timestamp series approach and temporary certificate approach in [12] and footprint Sybil attack detection mechanism in [13], have been proposed to detect Sybil attacks, few of them jointly consider the QoS and security performance in T2T based wireless communication systems. Therefore, in this paper, we first design the train-centric CBTC systems with T2T based wireless communications, which can overcome most of the problems in traditional systems without sacrificing system performance. Then, to detect Sybil attacks from the very beginning when they are happening, the local security certification and cooperative security check scheme are proposed for the designed systems, which can help train to detect and defense Sybil attacks more efficiently.

To improve integrated QoS and security performance of wireless communication systems in CBTC, an integrated QoS and security indicator, AoI, is used to capture the freshness of the safety-critical information. The asynchronous reinforcement learning with advantage actor-critic (A3C) is used to optimize the integrated performance of the underlying wireless system in train-centric CBTC. The distinct features of this paper are shown as follows:

1) Novel train-centric CBTC systems with T2T communication for urban rail transit are designed. In the designed systems, the back train can receive the safety-critical information from preceding train directly through T2T communication, which can improve the QoS performance of the CBTC systems. In addition, proposed train-centric CBTC systems with T2T can get more timely safety-critical information. Besides, the topological structure of the total system is simpler than that of traditional CBTC systems.

2) Local security certification and cooperative security check are proposed as Sybil attacks detection and defense scheme in train-centric CBTC systems. In local security certification, the improved public-private key pair, session key, and timestamp are used to guarantee the system security in T2T link establishment phase. In the cooperative security check scheme, we make use of the trackside base station to assist trains to detect Sybil attacks when a suspicious Sybil message is received by trains. The detection method in the proposed security check scheme includes security key check, timestamp check, and physical position check.

3) Based on the proposed train-centric CBTC systems and innovative security check scheme, we adopt the quantized AoI as the integrated performance indicator, which jointly considers system QoS and security of the underlying wireless system in CBTC.

4) To optimize integrated QoS and security performance, asynchronous reinforcement learning method, which has been successfully used to solve handoff problem in CBTC wireless networks [14], among others, is used to solve the QoS and security problem. In order to optimize the integrated performance, the link selection and security check decision are considered as actions related to the system performance.

5) Extensive simulation results based on real field measurements are presented. It is illustrated that the integrated QoS and security performance of CBTC systems can be significantly improved with the proposed scheme. The successful detection probability about Sybil attack can also be increased in the T2T based train-centric CBTC systems.

The rest of this paper is summarized as follows. The designed train-centric CBTC systems with T2T communications and existing security scheme are presented in Section II. Section III introduces the improved local security certification scheme and cooperative security check scheme for train-centric CBTC systems. The novel security indicator AoI and the influence factors are proposed in Section IV. Section V introduces the asynchronous reinforcement learning model to solve the QoS and security problem. Section VI shows the simulation results and discussions. Finally, we conclude the study in Section VII.

II. DESIGNED TRAIN-CENTRIC CBTC SYSTEMS WITH TRAIN-TO-TRAIN COMMUNICATION

A. THE OVERVIEW OF TRAIN-CENTRIC CBTC SYSTEMS WITH T2T TECHNOLOGY

The designed novel train-centric CBTC systems are shown in FIGURE. 1. It consists of three subsystems, which are control center subsystem, trackside subsystem, and onboard subsystem. Although the new systems are similar to the traditional CBTC systems, the Zone Controller (ZC) no longer belongs to the control center subsystem. Instead, we set the On-ZC located at onboard subsystem to generate the control command [15]. Therefore, the control center subsystem only includes the Evolved Packet Core (EPC) and unsafe-related traffics center. The trackside subsystem, including Building Baseband Unit (BBU) and Remote Radio Unit (RRU), is the main part of the wireless communication in train-centric CBTC systems. It is connected with the control center subsystem through the backbone network and provides the wireless coverage to operating trains. Based on the wireless coverage, operating trains can exchange unsafety-related information with control center through air interface and transmit safety-critical information with adjacent trains through

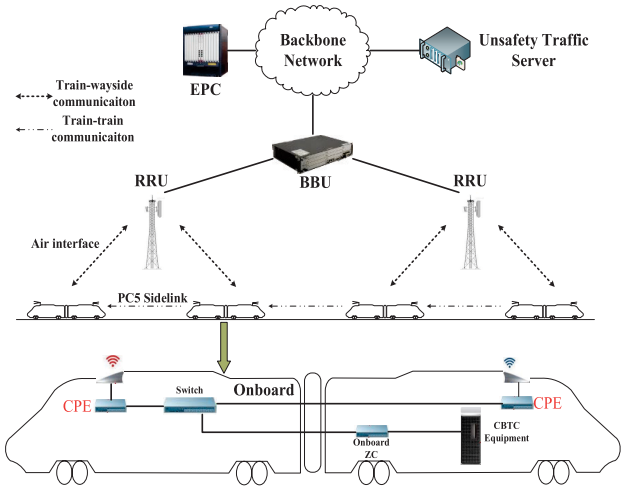


FIGURE 1. Integrated train-centric CBTC systems with T2T.

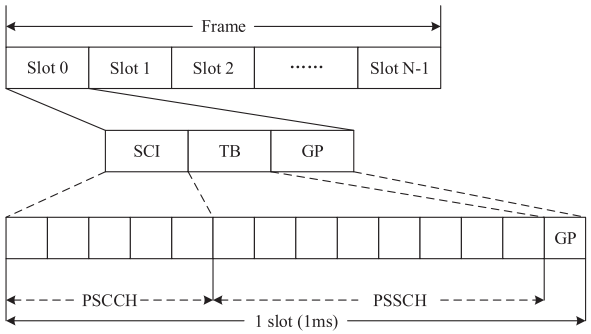


FIGURE 2. Frame structure of T2T based wireless communication systems.

PC5 interface with sidelink [16]. The onboard antennas, customer premise equipment (CPE), On-ZC, mobile stations for different traffics and CBTC equipment make up the onboard subsystem. In this subsystem, there are two antennas located at the front and rear of the train, which are used to communicate with the preceding train and back train respectively. Moreover, when the cooperative check scheme is activated, the signal from these two antennas can be used for the physical position check on the base station side. The main task of On-ZC is to analyze the safety-critical information from the preceding train and compute its movement authority (MA). The main task of onboard CPE is to exchange information with RRU and other trains through T2W and T2T communication link. As the most important part, CBTC equipment consists of Automatic Train Operation (ATO) unit and Automatic Train Protection (ATP) unit. For ATO, the main task is to calculate the optimal guidance trajectory called velocity vs. distance curve, which is used to control the optimal velocity at the indicated position. ATP, an onboard safety protection unit, is used to update the online train protection curve. When the velocity of the train exceeds the curve, the emergency brake command will be activated to protect operating safety [17], [18].

According to the T2T transmission link in train-centric CBTC systems, operating trains can direct exchange safety-critical information without the re-transmission of a base station. Furthermore, instead of generating the control command for all operating trains in its management area, on-ZC only needs to calculate its control command. Based on this advantage, the computation pressure of CBTC systems could be reduced obviously. Moreover, the novel $SCI + TB$ scheme is used in train-centric CBTC systems as well. The underlying architecture of this scheme is shown in FIGURE. 2. In this scheme, Transport Block (TB) is transmitted following the associated Sidelink Control Information (SCI) in the same subframe. With this novel scheme, the back train can get channel status information and secret information, such as secret key and train identification, through the SCI information. On the basis of the secret information in SCI, trains could make a decision about the trust level about the received information and determine whether the cooperative security check should be activated or not.

B. EXISTING SECURITY CHECK SCHEME FOR T2T IN TRAIN-CENTRIC CBTC

In the existing research about T2T and V2V wireless network, the security check scheme is only restricted to the link establishment stage. At this stage, the T2T control function checks the authenticity and legality of request train according to the received ID. In general, the traditional security check scheme including Configuration, Security authorization, and Data exchange can be introduced in detail as follows:

1) CONFIGURATION PHASE

When a train wants to establish a T2T link, the onboard CPE exchanges the configuration message with the ID control center to apply the secret keys and also be pre-configured by using the address of the ID control center.

2) SECURITY AUTHORIZATION PHASE

As the onboard CPE gets the T2T arguments from the control center. it sends the Key Request to the ID control center with its own ID and security configuration. If the ID control center gets the ID and security configuration from the train, it will check the authenticity and legality of them. With a successful check result, the ID control center starts the phase about the service ID authorization and security credential calculation. However, if the security check result fails, the train will restart this phase. Finally, the ID control center sends a response information with a secret key to onboard CPE.

3) DATA EXCHANGE PHASE

When the last phase successfully fulfills security authorization, adjacent trains will use the pre-configured security certificate, such as ID or secret key check, to exchange safety-critical messages.

As we can see, after the link establishment stage, the only security check scheme between T2T transmission is the secret

key check. However, with the development of technology, the simple secret key check is not safe and effective anymore. Terrorists and attackers could break the key and send wrong information by using the same identity as an operating train. In this case, the lack of effective security check may affect the train operation efficiency or cause some serious accidents, such as rear-end collision between adjacent trains. Therefore, to protect the safe and efficient operation of urban rail transit, an applicable security check scheme should be proposed.

III. IMPROVED SECURITY CHECK SCHEME FOR TRAIN-CENTRIC CBTC

A. THE SYBIL ATTACK IN TRAIN-CENTRIC CBTC

As the new technology in urban rail transit, the security of train-centric CBTC network is inadequate. Therefore, it is more likely to be attacked by some vicious attackers than before. Sybil attack, which is first described by Douceur [19] in device-to-device networks, is the most representative attack in the context of device-to-device networks. The Sybil attack allows a malicious sender to create Sybil nodes (not real nodes) to impersonate other (virtual) nodes. Then the Sybil nodes will play the role of multiple distinct nodes to cheat other vehicles or destroy security rules with its multiple identities which are illegally obtained by the way of forgery, theft or conspired sharing [11]. In this way, some malicious purposes of attackers can be realized.

The Sybil attack is particularly harmful in train-centric CBTC network because the mendacious information of the preceding train can lead to wrong control command of the back train. As we can see, FIGURE 3 (a) is the normal wireless communication scenario between two adjacent trains. In this scenario, train i periodic receives the safety-critical information from train j and generates its MA and control command. However, when the train i is under attack from a Sybil attacker, not only is it unable to get timely safety-critical information from train j, but also makes a wrong decision based on the wrong information, including wrong train location, velocity, and acceleration, from Sybil train. As is shown in the subfigure (b), the Sybil train created by Sybil attack is located between train i and train j. In this scenario, train i may make the decision that it is too close to the front train. To ensure the safe operation, the emergency brake is activated by train i, which may affect the operating efficiency of itself or of all the operating trains. Subfigure (c) is the scenario where Sybil train is located in front of train j. Train i may make the decision that there are no other trains between Sybil train j and itself. Therefore, the wrong MA and control command may be generated by train i, which will cause some serious incidents and accidents, such as rear-end collision.

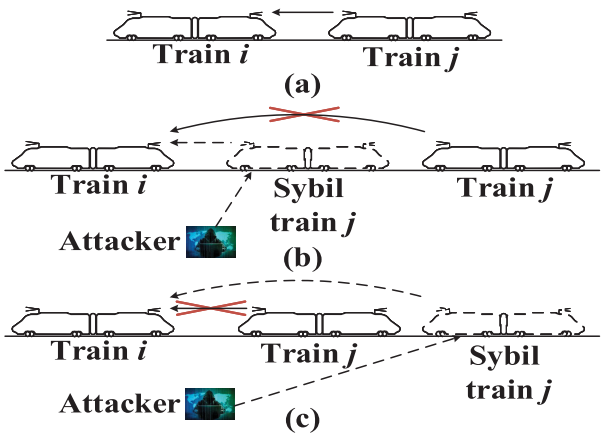


FIGURE 3. Impacts of Sybil attack.

Therefore, to guarantee the safe and efficient operation, an effective security scheme should be proposed for the train-centric CBTC. In the rest of this section, we will first introduce a local security certification scheme for the train-centric CBTC at the link establishment phase. Then, to improve the security level of train-centric CBTC systems, a cooperative security check scheme for train-centric CBTC systems is proposed to detect and defense the Sybil attack from malicious attackers.

B. LOCAL SECURITY CERTIFICATION SCHEME FOR TRAIN-CENTRIC CBTC

In this subsection, we first introduce a local security certification scheme for train-centric CBTC at link establishment phase, which is more efficient than the existing security authorization scheme. Moreover, this security certification scheme can lay a foundation for cooperative security check as well. As is shown in FIGURE 4, public-private key pair, session key, and train identification are used to certificate authenticity and legality of trains. The detailed process is shown as follows:

1. When train i establishes a link with base station r for the first time, it makes a time synchronization with the base station r. After the time synchronization, train i can generate a secret public-private pair (PU_i, PR_i) according to elliptic curve cryptography (ECC) algorithm

$$PU_i = PR_i \cdot P \bmod n \tag{1}$$

where n is a random number for the prime secret key of train i, and hash function for $hash : \{0, 1\}^* \rightarrow Z_q^*$.

2. When the secret key pair and temporary train identification are completed, train i sends PU_i and PID_i to the control center through the re-transmission of base station r. Once the control center receives the message, it verifies the authenticity and legality of the train i. If the verification is passed, it will send a confirmation message to base station r. Otherwise, train i is marked as an attacker by base station r.

3. After receiving the confirmation message, base station r starts the secret key generation phase. In this phase, base station r first records a timestamp TP_{ir} related to train i, which is the moment when train i is linked with base station r. Then, it continues to calculate its secret public-private key

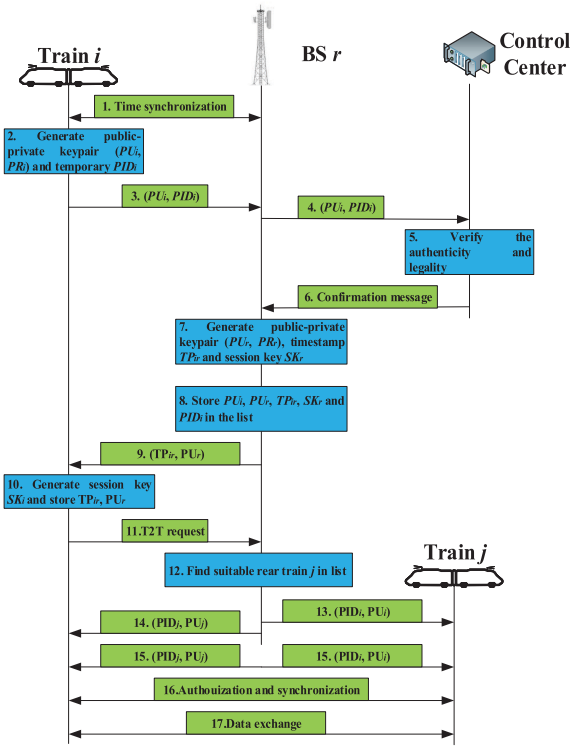


FIGURE 4. Procedure of local security certification.

pair and a special session key using the following formulas

$$PU_r = PR_r \cdot P \mod n \tag{2}$$

$$SK_r = PU_r + PU_i \mod n \tag{3}$$

where the session key is used to verify the authenticity and legality of train i when there is a security check request. After that, base station r sends (PU_r, TP_{ir}) to train i and puts $(PU_i, PU_r, TP_{ir}, SK_r, PID_i)$ into its certificate list.

4. As the message of (PU_r, TP_{ir}) is received by train i, the train first completes the calculation about session key using the same formula

$$SK_i = PU_i + PU_r \mod n \tag{4}$$

5. Up to now, if train i has already established the T2T link, the local security certification is completed. Otherwise, it sends base station r a T2T request to ask for suitable adjacent train j. After that, base station r sends the information of train identification and public key, to train j and train i. Then, the verification between train i and train j can be completed. Finally, after the authorization and synchronization, adjacent trains can establish the T2T link start the exchange of safety-critical information.

Therefore, with this local security certification scheme, the base station can first check the certificate authenticity and legality of a train before the data exchange, which can guarantee the transmission quality between train and base station. Moreover, the stored information, such as public-private key pair, session key, and train identification, can be used for cooperative security check.

C. COOPERATIVE SECURITY CHECK SCHEME FOR TRAIN-CENTRIC CBTC

In this subsection, we propose a cooperative security check scheme for train-centric CBTC systems. The main task of the cooperative security check is to reduce or avoid the hazards from the Sybil attack. Unlike the existing security check in the last section, the associated base station assists the train to check whether the information source train is a Sybil train or not. As shown in FIGURE 5, there is a T2T link between train i and train j. Under the normal condition, train i can update its control command according to the received train status from train j. However, when train i decides that the received message is a suspicious Sybil attack message, it will start the cooperative security check immediately to protect the safe operation. The detailed process is shown as follows:

1. When train i receives suspicious wrong safety-critical information from suspicious train j, it makes a judgement whether this information is a suspicious Sybil Attack message or not. If true, train i will send a security check request $(TP_{ir}, PU_{ir}, SK_i, PID_i, ST_j)$ to associated base station r. In this request message, timestamp TP_{ir}, public key PU_{ir}, session key SK_i and train identification PID_i are used to check the authenticity and legality of the request train. $ST_j = (PID_j, TP_{jv}, PLoc_j, BSid_v)$ is the information from suspicious

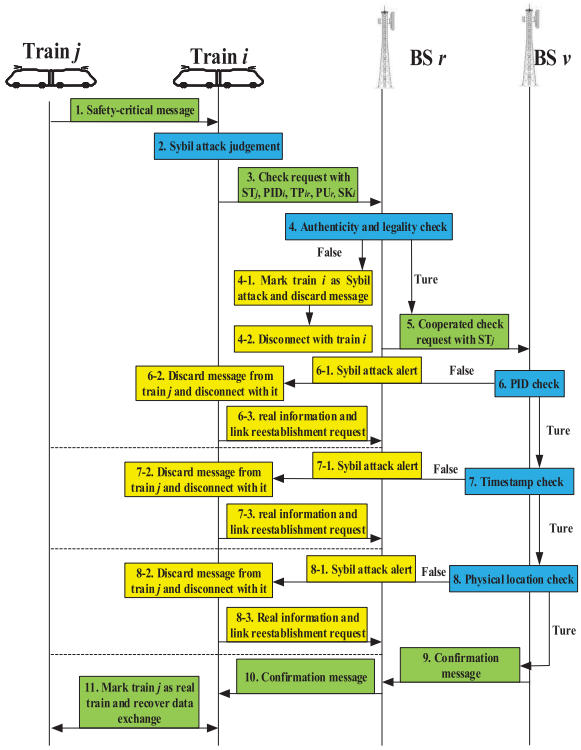


FIGURE 5. Procedure of cooperative security check.

train j, where PID_j and $PLoc_j$ are the asserted identification and physical location of train j, TP_{jv} is the asserted timestamp of train j with associated base station v, $BSid_v$ is the asserted base station ID from train j.

2. Once the base station r receives a security check request, it will first check the authenticity and legality of the request train through TP_{ir}, PU_{ir}, SK_i and PID_i as follows:

$$\begin{aligned} Ch^j_{re} = &\, ver.\left(TP_{ir}, TP^r_{ir}\right) \cap ver.\left(PU_{ir}, PR_{ir}\right) \\ &\cap\, ver.\left(SK_i, SK_r\right) \cap ver.\left(PID_{ir}, PID^r_{ir}\right) \end{aligned} \tag{5}$$

where TP^r_{ir} and PID^r_{ir} are the timestamp and identification of train i stored in base station r, and $ver.$ is the result of each single check. When the single check result is true, we have $ver. = 1$; otherwise, $ver. = 0$. If and only if all the four results are true, the final result can get $Ch_{re} = 1$. Therefore, if the final check result is true, base station r will send the cooperative check request and ST_j to the base station v on the basis of $BSid_v$. If false, base station r will mark train i as a Sybil attacker and disconnect with it.

3. As the security check request is achieved by base station v, it starts the authenticity and legality check about train j. The check can be divided into two phases. The first is identification and timestamp check

$$Ch^j_{re-1} = ver.\left(TP_{jv}, TP^v_{jv}\right) \cap ver.\left(PID_{jv}, PID^v_{jv}\right) \tag{6}$$

The main task of this phase is to check whether train j is in the associated list of base station v or not. If the check result is true, the next check phase will be activated. If false, base station v will send a Sybil alert to train i. Then train i will discard messages from Sybil train j and disconnect with it.

4. If the identification check is passed, the base station v begins the real physical position check. To estimate the physical position accurately in this phase, we measure the estimated physical position of train j through Time Difference of Arrival (TDOA) measurement mode. In this mode, the signal from the front antenna and rear antenna of the train are used to estimate the physical position. We first set the position of the front antenna and rear antenna as $P^{front}_j = \begin{pmatrix} x^{front}_j \\ y^{front}_j \end{pmatrix}$ and $P^{rear}_j = \begin{pmatrix} x^{rear}_j \\ y^{rear}_j \end{pmatrix}$ respectively. Obviously, there is a relationship between these two antennas. The relationship can be written as

$$P^{front}_j = P^{rear}_j + |L| \cdot \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \tag{7}$$

where α is the angle between train j and x axis, which lies on the operating direction of train j, $|L|$ is the relative length of train j and can be written as

$$|L| = \begin{cases} L_{train\,j}, C_{cur} = 0 \\ L_{train\,j} \cdot \dfrac{360}{\beta\pi} \cdot \sin\dfrac{\beta}{2}, C_{cur} = 1 \end{cases} \tag{8}$$

where $L_{train\,j}$ is the real length of train j, and C_{cur} is a curve indicator. When the train is operating on a curve track, we have $C_{cur} = 1$; otherwise $C_{cur} = 0$, β is the angle of curve. During the position estimation, base station first measures the time of arrival of the source signal based on particular signal features transmitted by the front antenna and rear antenna of train j. Given a line of sight propagation path, the time of arrival measurement at base station is

$$t^{front}_j = \frac{1}{c}\left\|P_{BS} - P^{front}_j\right\| + t_0 + n^{front}_j \tag{9}$$

$$t^{rear}_j = \frac{1}{c}\left\|P_{BS} - P^{rear}_j\right\| + t_0 + n^{rear}_j \tag{10}$$

where c is the speed of light, $\|\cdot\|$ denotes the Euclidean norm, $P_{BS} = \begin{pmatrix} x_{BS} \\ y_{BS} \end{pmatrix}$ is the position of the associated base station, t_0 is the unknown time instant where the source transmits the signal to be measured, and n^{front}_j and n^{rear}_j are the random error in the measurement. Recognizing that the unknown t_0 is not of direct interest in train j localization, a TDOA measurement method is used for the t^{front}_j and t^{rear}_j

$$\begin{aligned} \Delta^{fr}_j &= t^{front}_j - t^{rear}_j \\ &= \frac{1}{c}\left(\left\|P_{BS} - P^{front}_j\right\| - \left\|P_{BS} - P^{rear}_j\right\|\right) + n_j \end{aligned} \tag{11}$$

where $n_j = n^{front}_j - n^{rear}_j$. With the estimated position, the base station v can verify whether train j is operating at this position area or not. In this novel scheme, the LiDAR, which can provide highly resolute $3-D$ point data and is basically used for object recognition and tracking, is used to verify the physical position of train j [20]. If there is a train operating at the estimated position, the response of LiDAR should follow the normal distribution of the transmit pulse. Therefore, the result of real physical position check is

$$Ch^j_{re-2} = LiDAR.\left(Pos^{mea}_j, Pos^{est}_j\right) \tag{12}$$

where Pos^{mea}_j and Pos^{est}_j are the measurement and estimated position of train j. If the check result is true, the base station v sends a confirmation message to train i. Then train i will mark train j as a trusted T2T source and recover the data exchange with it. If false, base station v will send a Sybil alert to train i with the re-transmission of base station r. Then train i will discard the message from Sybil train j and disconnect with it.

With this security check scheme, trains can determine whether the received suspicious information is true or not with the help of base station. Thus, trains can detect the Sybil attack and recover from the impact from that as soon as possible.

IV. USING AOI AS THE INTEGRATED QOS AND SECURITY INDICATOR OF TRAIN-CENTRIC CBTC

As is known, timely updated safety-critical information is related to the safe and efficient operation of each train on the track. Large communication latency and successive packet drop caused by any reason or vicious attack in continuous communication periods may jeopardize the safe operation and QoS of the train, even the whole railway systems [21].

However, the traditional indicators of CBTC are not suitable to mirror the integrated QoS and security performance. Therefore, an emerging concept of AoI will be introduced to be an ideal candidate for integrated QoS and security indicator of train-centric CBTC.

A. THE ANALYSIS OF AOI AS INTEGRATED QOS AND SECURITY INDICATOR

Unlike the traditional indicator, AoI captures the freshness of the authentic information from the perspective of a destination. The freshness refers to the time that has elapsed since the generation of the authentic packet that is most recently processed by destination. Thus, when the authentic information is affected by any reason, such as the influence from source train, wireless channel or Sybil attack, the performance of AoI can be decreased. The introduction about AoI is shown as follows:

As shown in FIGURE 6, we use a positive real number AoI_i to represent the AoI status of T2T communication link between train i and train j. In addition, initial status of AoI_i is set as $AoI_i[0]$. In FIGURE 6, nth communication period begins at time $T_n, n = 1, 2, 3, \cdots, l$. Then, AoI_i increases linearly until the authentic packet is delivered and processed by destination successfully at time $T'_n, n = 1, 2, 3, \cdots, l$. After processing the packet with a time stamp T_n, AoI_i is reset to a smaller value $Y_n = T'_n - T_n$, and then increases linearly again until next packet is delivered and processed. However, when the packet is not delivered and processed by destination for some reason, AoI_i will increase without a break. For example, we assume that the T_* is a packet from Sybil node. Because of this Sybil packet, the authentic safety-critical information cannot be received or processed by the destination. Therefore, the AoI curve is increased without a normal reset until the authentic information is received. In this example, we assume that the destination can recover from the Sybil attack immediately. Therefore, the authentic safety-critical packet T_4 can be received and processed successfully. However, because of the impact from Sybil packet T_*, the area of S_4 is larger than before, which means that the AoI performance is decreased.

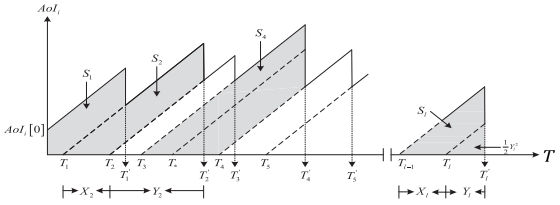


FIGURE 6. Example of AoI.

As depicted in FIGURE 6, the AoI_i curve can be indicated as (13), as shown at the bottom of this page, where $P_i[n]$ is the packet sent by sender at time T_n. In this paper, we use the area under AoI curve to indicate AoI_i's performance. Thus, in order to analyze the AoI area more clearly, the total area under AoI curve can be divided into polygon area S_1, the trapezoidal areas $S_n, n \geq 2$, and the end triangular 2 area whose area is $\frac{1}{2}Y_l^2$. Thus, the AoI status of this T2T communication link can be written as:

$$AoI_i = S_1 + \sum_{n=2}^{l} S_n + \frac{1}{2}Y_l^2 \tag{14}$$

where S_1 and $\frac{1}{2}Y_l^2$ are indicated in FIGURE 6. To calculate the S_n easily, $X_n = T_n - T_{n-1}$ is defined as the inter-departure time between packet $n-1$ and n. Therefore, S_n can be written as

$$S_n = \frac{1}{2}(X_n + Y_n)^2 - \frac{1}{2}Y_n^2 = X_nY_n + \frac{1}{2}Y_n^2 \tag{15}$$

The average status of AoI_i over an interval $(0, T)$ is

$$AoI_i^{avg} = \frac{AoI_i}{T} \tag{16}$$

To make a better analysis of the AoI, we introduce another indicator named peak AoI [22]. The peak AoI can give us the performance of the worst AoI during each transmission. As shown in FIGURE 6, the peak AoI is defined as the maximum AoI immediately before the packet is processed by destination, which can be expressed as

$$AoI_n^{peak} = X_n + Y_n \tag{17}$$

Through analysis, the computation complexity of peak AoI is easier than that of average AoI. Thus, the peak AoI is a valuable integrated QoS and security indicator as well.

It is found that in the wireless communication systems in CBTC, the lower the AoI value, the better the integrated QoS and security performance. Moreover, as shown in (14) to (17), the average and peak AoI value are all related to X_n and Y_n. Therefore, to achieve a better integrated QoS and security performance, the influence factor about X_n and Y_n will be analyzed in the rest of this section.

B. THE AOI INDICATOR CONSIDERING PACKET DROP AND RE-TRANSMISSION

Based on the normal condition of wireless communication systems in train-centric CBTC, X_n is fixed when there is no packet drop [18]. Therefore, if the packet drop is taken into consideration, X_n can be written as

$$X_{n\_PD} = (M+1) \cdot T_{inter} \tag{18}$$

$$AoI_i^n = \begin{cases} AoI_i^{n-1} + t - T'_{n-1}, \textit{ if no packet is processed durning } T'_{n-1} \leq t \leq T'_n \\ T'_n - T_n, \textit{ if } P_i[n] \textit{ is processed by train } i+1 \textit{`at } t = T'_n \\ 0, \textit{ if the last packet is processed at } t = T'_l \end{cases} \tag{13}$$

where T_{inter} is the pre-set period interval, M is the total packet drop number in this communication period, which is related to the packet drop rate. The relationship between the packet drop rate and SINR has already been established in our previous works [15].

The influencing factor of Y_n is related to the re-transmission in the T2T transmission link. In the LTE-T2T based wireless communication systems, the Hybrid Automatic Repeat re-Quest (HARQ) scheme is used to protect the successful transmission. Under this scheme, if train i succeeds in receiving the safety-critical information, it sends an Acknowledgement (ACK) back to train j. However, if train j does not receive the ACK from receiver within fixed time for any reason, it should retransmit this information and continue to send until the information get to the destination or the retransmission limitation is reached. Therefore, due to the re-transmission caused by random transmission errors, Y_{n_PD} can be calculated as follows:

$$Y_{n\_re} = T_{CPE\_j} + T_f + T_p + k \times T_{HARQ} + T_{CPE\_i} \tag{19}$$

where the T_f is the framing control latency, T_p is the Transmission Time Interval (TTI), T_{HARQ} indicates the HARQ Round Trip Time (RTT), k indicates the total number of re-transmission times, T_{CPE_j} and T_{CPE_i} are processing latency of onboard CPE on train j and train i, respectively. For T_{HARQ}, we have

$$T_{HARQ} = T_{f\_i} + T_{data} + T_{CPE\_i} + T_{f\_i} + T_{feedback} + T_{CPE\_i} \tag{20}$$

where T_{f_i} and T_{f_j} are the sending time of onboard CPE on train i and train j, T_{data} indicates transmission time from train i to train j, T_{CPE_i} and T_{CPE_j} represent processing delay of onboard CPE on train i and train j, $T_{feedback}$ is transmission time from train j to train i.

C. THE AOI INDICATOR CONSIDERING SYBIL ATTACK

As is introduced in section III-A, the Sybil train can cut off the T2T link between train i and train j firstly. Then it plays the role of train j to send wrong safety-critical information to train i. Thus, if train i is under attack from Sybil attackers, it cannot receive and process the authentic packet in continuous communication period. In this case, the X_n in AoI is increased due to the Sybil attack

$$X_{n\_Sybil} = \left\lceil 1 + M + \frac{T_{effect} + T_{recover} + T_{re-est}}{T_{inter}} \right\rceil \cdot T_{inter} \tag{21}$$

where during T_{effect}, train i is under attack from the Sybil train, $T_{recover}$ is the time required to cut off the connection with Sybil train when train i is aware of the Sybil attack, T_{re-est} is the time to re-establish T2T link with train j after the recovery from Sybil attack, and $\lceil * \rceil$ is ceiling operation.

As we can see, if train i cannot recover from the Sybil attack as soon as possible, the value of T_{effect} will be very large, which leads to the excessive increase of AoI Curve. The large value of AoI means that train i cannot update safety-critical information or control command for long-period, which affects the efficient operation or leads to some serious incidents and accidents, such as emergency brake and rear-end collision. Moreover, although train i recovers from Sybil attack after a while, it also needs time to cut off the connection with Sybil train and re-establish the T2T link with train j, which affects the AoI's performance.

The influencing factor of Y_n is simpler than that of X_n. As the train i recovers from the Sybil attack and re-establishes the T2T link with real train j, it can receive the correct safety-critical information after a period of Y_{n_Sybil}. At this moment, we assume that there is no other influencing factor except the re-transmission caused by random transmission errors. Therefore, we set the Y_{n_Sybil} the same as Y_{n_re} in this condition.

D. THE AOI INDICATOR CONSIDERING COOPERATIVE SECURITY CHECK

The cooperative security check scheme can help trains to detect the Sybil trains more efficiently and reduce the effects from Sybil attack on the one hand. However, the check process also has some impacts on the AoI. To analyze the X_{n_Ch} in detail, we set an index pair (Ac, Re) to indicate the actual Sybil attack status and check result respectively, where 1 means that the train is under attack from Sybil train and 0 means the train is operating normally. Therefore, with this index pair, the X_{n_Ch} can be written as formula (22), as shown at the bottom of this page.

As is shown in the formula, based on different Sybil attack status and check result, there are four different scenarios in X_{n_Ch}. The first (0, 0) scenario represents the no-attack status with the correct check result. In this scenario, X_{n_Ch} has the same value as X_{n_PD} because of the matching check result. However, the unnecessary security check also has some impacts on Y_{n_Ch}. In (1, 0), the check result is no-attack when train i is actually under attack from Sybil attacker. In this scenario, because of the incorrect check result, the Sybil train

$$X_{n\_Ch} = \begin{cases} (M+1) \cdot T_{inter}, (Ac, Re) = (0, 0) \\ \left\lceil 1 + M + \dfrac{T_{effect} + T_{recover} + T_{re-est}}{T_{inter}} \right\rceil \cdot T_{inter}, (Ac, Re) = (1, 0) \\ \left\lceil 1 + M + \dfrac{R\,(T_{recover} + T_{re-est})}{T_{inter}} \right\rceil \cdot T_{inter}, (Ac, Re) = (1, 1) \\ \left\lceil 1 + M + \dfrac{R\,(T_{recover} + T_{re-est})}{T_{inter}} \right\rceil \cdot T_{inter}, (Ac, Re) = (0, 1) \end{cases} \tag{22}$$

will be linked with train i for a long time, which leads to the result that X_{n_Ch} is the same as X_{n_Sybil} when there is no security check. For the scenario $(Ac, Re) = (1, 1)$, train i successfully detects the attack from Sybil train. According to the correct check result, train i can cut off the connection with Sybil train immediately and re-establish the T2T link with real train j. Therefore, the impact from Sybil train can be reduced, where the T_{effect} can be set as 0. In this scenario, the X_{n_Ch} can get a much smaller value than X_{n_Sybil}. In the last scenario, $(Ac, Re) = (0, 1)$, due to the incorrect check result, train i cuts off the normal transmission link and then re-establishes it, which leads to an unnecessary latency. Therefore, although the X_{n_Ch} in this scenario is the same as that in (1, 1), this unnecessary latency caused by incorrect check result is harmful to both X_{n_Ch} and Y_{n_Ch}.

The value of Y_{n_Ch} is based on the check result. If the cooperative security check is not activated by train i, Y_{n_Ch} has the same value as Y_{n_re}. Otherwise, though train i decides to activate cooperative security check, security check latency should be an extra value appearing in the Y_{n_Ch}

$$Y_{n\_Ch} = D[T_{Ch\_r} + R_1\left(T_{Ch\_v1} + R_2 T_{Ch\_v2}\right) + T_{pr}] + Y_{n\_re} \tag{23}$$

where D is the check decision result. if the cooperative security check is activated, we have $D = 1$; otherwise, $D = 0$. R_1 is the check result of the base station r, where $R_1 = 1$ indicates that the check in base station r is passed and the next check phase is activated, $R_1 = 0$ means that the check is failed and train i is marked as a Sybil train. R_2 is the check result of the first phase in base station v, where $R_2 = 1$ indicates that the first phase check in base station v is passed and the next check phase is activated, $R_2 = 0$ means that the check is failed and a Sybil attack alert is sent to train i. T_{Ch_r} indicates the check latency of base station r. T_{Ch_v1} is the check latency of the first phase in base station v. T_{Ch_v2} is the check latency of the second phase in base station v. T_{pr} is the processing latency of train i after the security check.

As we can see, the check decision command and the check result are the most important factors related to the X_{n_Ch} and Y_{n_Ch}. If and only if the check decision command and the check result are all correct, the AoI's performance can be improved. The extra latency caused by wrong decision or result is harmful to the AoI's performance. Therefore, in the next section, we will find a suitable method to find a more effective check decision command and a check result.

V. INTEGRATED AOI OPTIMIZATION OF TRAIN-CENTRIC CBTC

In this section, we formulate the integrated QoS and security performance optimization problem in LTE-T2T based train-centric systems as a policy-based asynchronous reinforcement learning problem, which can generate the appropriate policy for link selection decision and security check decision to reduce the system AoI curve.

A. POLICY-BASED ASYNCHRONOUS REINFORCEMENT LEARNING WITH A3C

Compared with value-based methods, policy-based model-free approaches can directly parameterize the policy $\rho(a|s, \varepsilon)$ and update the parameters ε through performing, typically approximate, gradient ascent on $E[a]$ [23]. Furthermore, it can get better convergence properties and have effective performance in high-dimensional or continuous action spaces.

In contrast to the normal Q-learning, a baseline is added to asynchronous advantage actor-critic (A3C) algorithm. In A3C algorithm, policy $\rho(a|s, \varepsilon)$ is defined as the actor to optimize the policy and generate the action. The baseline is set as the critic in A3C, which is used to evaluate the policy through Temporal-Difference (TD) error. With the help of the baseline, state $s(t)$ and reward based estimated value function $V_\rho\{s(t); \varepsilon_u\}$ is expressed as

$$V_\rho\{s(t); \varepsilon_u\} = E_{\rho\{s(t)\}}\left\{\sum_{i=0}^{k-1}\lambda^j r(t+i) + \lambda^k V_\rho\{s(t+k); \varepsilon_u\}\right\} \tag{24}$$

where $\lambda \in [0, 1]$ is the discount factor, ε_u is the value-function parameter, and $r(t)$ is the system reward function, which will be introduced in the follow subsections.

Based on the value function, an action-value function, which is used to express the expected discounted reward with the selected policy, can be defined as

$$Q_\rho\{s(t), a(t); \varepsilon_u\} = \sum_{i=0}^{k-1}\lambda^j r(t+i) + \lambda^k V_\rho\{s(t+k); \varepsilon_u\} \tag{25}$$

where k with an upper limit of t_{max} can change from state to state.

In A3C algorithm, the actor-critic uses the n-step returns to update both the policy and the value-function after every t_{max} actions or when a final state is reached [28]. The update performed by the algorithm can be seen as $\nabla_{\varepsilon^*}\log\rho(a_i|s_i; \varepsilon^*)\cdot A_\rho\{s(t), a(t); \varepsilon, \varepsilon_u\}$ and $\partial\{R - V(s_i; \varepsilon_u^*)\}^2/\partial\varepsilon_r^*$. The detailed algorithm is presented in **Algorithm 1**.

B. ACTION

As is introduced in last section, in T2T based CBTC systems, the train needs to decide whether to activate the cooperative security check or not when it receives a suspicious message. The reliable decision can help the train get lower X_n and Y_n in this communication period. Moreover, the train makes the transmission link decision according to the link status and Sybil attack status as well. The action $a(t) \in A$ of the train can be written as

$$a(t) = \{a_{csc}(t), a_{link}(t)\} \tag{26}$$

where $a_{csc}(t)$ represents the cooperative security check action with $a_{csc}(t) \in (0, 1)$. $a_{csc}(t) = 0$ means that the cooperative security check is not activated by train i and 1 indicates that train i activates the cooperative security check in this

Algorithm 1 Asynchronous Reinforcement Learning With A3C Process

// Set global shared arguments vector ε and ε_u and global shared counter $T = 0$
// Set thread-specific arguments vectors ε^* and ε_u^*
Initialize thread step counter $t \leftarrow 1$
repeat
  Reset gradients: $d\varepsilon \leftarrow 0$ and $d\varepsilon_u \leftarrow 0$;
  Synchronize thread-specific parameters $\varepsilon^* = \varepsilon$ and $\varepsilon_u^* = \varepsilon_u$;
  $t_{begin} = t$;
  Obtain state $s(t)$;
  repeat
    Perform $a(t)$ according to policy $\rho(a|s, \varepsilon^*)$;
    Acquire reward $r(t)$ and a fresh state $s(t+1)$;
    $t \leftarrow t + 1$;
    $T \leftarrow T + 1$;
  until terminal $s(t)$ or $t - t_{begin} == t_{max}$
  $R = \begin{cases} 0, for\ final\ s(t+1) \\ V\{s(t); \varepsilon_u^*\}, for\ non-final\ s(t) \end{cases}$
  for $i \in \{t-1, \cdots, t_{begin}\}$ **do**
    $R \leftarrow r_i + \gamma R$;
    Accumulate gradients wrt ε^* : $d\varepsilon \leftarrow d\varepsilon + \nabla_{\varepsilon^*} \log \rho(a_i|s_i; \varepsilon^*) \cdot A_\rho\{s(t), a(t); \varepsilon, \varepsilon_u\}$
    Accumulate gradients wrt ε_u^* : $d\varepsilon_u \leftarrow \partial\{R - V(s_i; \varepsilon_u^*)\}^2/\partial\varepsilon_r^*$
  end for
  Perform asynchronous update of ε using $d\varepsilon$ and of ε_u using $d\varepsilon_u$
until $T > T_{max}$

communication period. $a_{link}(t) \in (\mathbf{T}, \mathbf{W})$ is the transmission link action. When train i operates on the railway, it can choose the suitable link to exchange safety-critical information with train j. Here, $\mathbf{T}$ represents the T2T transmission link decision action and $\mathbf{W}$ stands for T2W transmission link decision action.

C. STATE

The train state $x(t) \in X$ can be expressed as

$$x(t) = \{Pos(t), PPos(t), S_{T2T}(t), S_{T2W}(t), \sigma_l(t), \sigma_S(t), \sigma_c(t)\} \tag{27}$$

where $Pos(t)$ is the train position at time t, $PPos(t)$ is the preceding train position at time t, $S_{T2T}(t)$ and $S_{T2W}(t)$ are the measured SINR from the onboard CPE, $\sigma_l(t)$ is the link selection status, $\sigma_S(t)$ is the Sybil attack status, and $\sigma_c(t)$ is the cooperative security check result. The transmission link used currently is completely decided by the current action, which makes $\sigma_l(t) \in (\mathbf{T}, \mathbf{W})$. $\sigma_S(t) \in (0, 1, 2)$ contains all the current Sybil attack status, where 0 is the normal operation status without any attack. $\sigma_S(t) = 1$ means that the train is under attack from Sybil attacker and 2 indicates the recover status. $\sigma_c(t) \in (\mathbf{P}, \mathbf{F}, \mathbf{0})$ means that the security check is passed, failed, or has no result, respectively.

D. STATE TRANSITION MODEL

With the train state $x(t) = \{Pos(t), PPos(t), S_{T2T}(t), S_{T2W}(t), \sigma_l(t), \sigma_S(t), \sigma_c(t)\}$ and the calculated action $a_{csc}(t)$ and $a_{link}(t)$, the transition probability to the next state $x(t+1)$ can be written as

$$\begin{aligned} &P\{x(t+1)\,|x(t), a(t)\} \\ &= P\{Pos(t+1)\,|Pos(t)\} \times P\{PPos(t+1)\,|PPos(t)\} \\ &\quad \times P\{S_{T2T}(t+1)\,|S_{T2T}(t)\} \times P\{S_{T2W}(t+1)\,|S_{T2W}(t)\} \\ &\quad \times P\{\sigma_S(t+1)\,|\sigma_S(t)\} \times P\{\sigma_l(t+1)\,|\sigma_l(t)\} \\ &\quad \times P\{\sigma_c(t+1)\,|\sigma_c(t)\} \end{aligned} \tag{28}$$

where $P\{Pos(t+1)\,|Pos(t)\}$ and $P\{PPos(t+1)\,|PPos(t)\}$ are the transition probabilities for physical position of back train and preceding train respectively, $P\{S_{T2T}(t+1)\,|S_{T2T}(t)\}$ and $P\{S_{T2W}(t+1)\,|S_{T2W}(t)\}$ are the SINR state transition probabilities for the T2T and T2W links of back train respectively, $P\{\sigma_S(t+1)\,|\sigma_S(t)\}$ indicates the Sybil attack state transition probability from the perspective of back train, $P\{\sigma_l(t+1)\,|\sigma_l(t)\}$ is the transition probability for the link selection indicator, and $P\{\sigma_c(t+1)\,|\sigma_c(t)\}$ is the transition probability for security check result of back train.

The transition probability of train position can be obtained from the train dynamic function. The SINR transition probabilities for the two wireless links can be measured in field tests. The Sybil attack state transition probability can be obtained from the pre-set Sybil attacker.

The link selection indicator should change its status if the current link is unable to transmit the safety-critical for some reason, such as the effect from low SINR or Sybil attack. The transition probability of link selection indicator is dependent on the Sybil attack status, and SINR of T2T and T2W link. Given the Sybil attack status $\sigma_S(t)$, T2T SINR status $S_{T2W}(t)$ and T2W SINR status $S_{T2W}(t)$, the $P\{\sigma_l(t+1)\,|\sigma_l(t)\}$ can be expressed as formula (29), as shown at the bottom of this page, where $\oplus$ is Exclusive-Or operation. In this formula, when the train is under attack or recovering from an attack, the link selection indicator will be set as $\mathbf{W}$ with probability 1. When the train is in normal operation status, link selection

$$\begin{cases} 1, if\ \sigma_S(t) \neq 0, a_{link}(t) = \mathbf{W}, \sigma_l(t+1) = \mathbf{W} \\ 1, if\ \sigma_S(t) = 0, a_{link}(t) = \mathbf{W}, s_{T2W}(t) > s_{T2T}(t) + s_{rd} \cdot [\sigma_l(t) \oplus \mathbf{W}], \sigma_l(t+1) = \mathbf{W} \\ 1, if\ \sigma_S(t) = 0, a_{link}(t) = \mathbf{T}, s_{T2T}(t) > s_{T2W}(t) + s_{rd} \cdot [\sigma_l(t) \oplus \mathbf{T}], \sigma_l(t+1) = \mathbf{T} \\ 0, others \end{cases} \tag{29}$$

indicator will transform between **W** and **T** based on the SINR condition.

Security check action determines the correct security check result in next epoch. Therefore, we derive the security check result transition probability $P\{\sigma_c(t+1)\,|\sigma_c(t)\}$ as

$$\begin{cases} P_{Dt}^1 \cdot P_1 \cdot P_2 \cdot P_3, \textit{ if } a_{csc}(t)=1, \sigma_S(t)=1, \sigma_c(t+1)=\mathbf{P} \\ P_{Dt}^1 \cdot (1-P_1 \cdot P_2 \cdot P_3)\,, \textit{ if } a_{csc}(t)=1, \sigma_S(t)=1, \sigma_c(t+1)=\mathbf{F} \\ P_{Df}^1, \textit{ if } a_{csc}(t)=0, \sigma_S(t)=1, \sigma_c(t+1)=\mathbf{0} \\ P_{Df}^2, \textit{ if } a_{csc}(t)=1, \sigma_S(t)=0, \sigma_c(t+1)\neq\mathbf{0} \\ P_{Dt}^2, \textit{ if } a_{csc}(t)=0, \sigma_S(t)=0, \sigma_c(t+1)=\mathbf{0} \\ 0, \textit{ others} \end{cases} \tag{30}$$

where P_1, P_2, P_3 are the check pass probability in three security phases, P_{Dt}^1 and P_{Df}^1 are the security check decision true and false probability as the train is under attack, respectively, P_{Dt}^2 and P_{Df}^2 refer to the true or false probability of the security check decision respectively, as the train operates normally.

In the above formula, when the train is under attack and makes a correct decision, the final check result status is either pass or failure due to the check pass probability in three security phases. When the correct decision is made in normal operation status without attack, the final check result status is 0 with P_{Dt}^2. However, when an incorrect decision is made by the train, the final check result status is 0 with false probability of the security check decision.

E. REWARD FUNCTION

In order for AoI to represent the integrated QoS and security performance for CBTC wireless communication systems, we define the Q-learning reward function with an AoI threshold AoI_{th}

$$r(t) = \begin{cases} e^{1/AoI_n^{peak}(t)}, & AoI_{th} \textit{ is satisfied} \\ R_N < 0, & AoI_{th} \textit{ is violated} \end{cases} \tag{31}$$

As we can see, due to the consequences of the Sybil attack and some random error, the AoI value will change after each action. Therefore, if system peak AoI value satisfies the threshold at the current epoch, a reward is set as a function of real-time AoI value. However, if system AoI value exceeds the threshold, the reward will be a negative value, $R_N < 0$.

VI. SIMULATION RESULTS AND DISCUSSIONS

In this section, simulations are provided to verify the integrated QoS and security performance improvement of our designed system and the AoI indicator. The simulation scenario and parameters from real urban railway scenario are given first. We then discuss the integrated AoI improvement of LTE-T2T based wireless communication systems in train-centric CBTC based on different security schemes. Finally, the number of successful detection times of the Sybil attack for different security schemes is described.

A. SIMULATION SCENARIO AND PARAMETERS

In this paper, the simulation scenario and parameters come from real settings in Beijing Yanfang urban railway line, which is located at the southwest of Beijing and has a total length of 14.4 km with nine stations. The surrounding environment of Yanfang line are cropland and dwellings, where there are no other large-scale wireless equipment. The trackside eNodeBs are deployed along the line with the distance of 1000 meters, which are used to provide the signal coverage for onboard wireless communication systems. The average headway distance between two adjacent trains is set as 1500 meters [15], [24]. The other detailed parameters of the simulation are shown in TABLE 1.

TABLE 1. Simulation parameters.

Parameters	Value
eNB TX power (dBm)	44
Frequency bandwidth (MHz)	1785-1805
T2W link path loss model (dB)	37.6log10(d)+128.1
T2T link path loss model (dB)	40log10(d)+148
Communication period (ms)	100
Velocity limitation (km/h)	80

B. INTEGRATED QOS AND SECURITY PERFORMANCE IMPROVEMENT OF TRAIN-CENTRIC CBTC

In this subsection, we first analyze system AoI of different security check schemes in designed train-centric CBTC, including traditional security check scheme, cooperative security check scheme without asynchronous reinforcement learning (ARL) and cooperative security check scheme with ARL. Then the number of peak AoI violation times of these three different schemes is expressed. Next, we discuss the average AoI performance of these three different schemes under different SINR. Finally, the number of successful Sybil attack detection times based on different security schemes is described.

FIGURE 7 is selected simulation results of system AoI based on different security check schemes from 0 s to 30 s and 80 s to 110 s. Based on the description in Section IV, system AoI is related to the packet drop, re-transmission, Sybil attack, and security check. As we can see in the first subfigure in FIGURE 7, because of the ineffective detection and defense of Sybil attack in traditional security check scheme, a lot of large fluctuations occur in system AoI based on traditional scheme due to the frequent unsuccessful detection of Sybil attack. The large fluctuation of AoI may lead to some unsatisfied integrated QoS and security performance to train-centric CBTC. In the second subfigure of FIGURE 7, we set the cooperative security check scheme as the main security scheme. As we can see, the number of large AoI fluctuation times is less than that in the first subfigure. However, because of some wrong check decisions, the Sybil attack cannot be successfully detected on some conditions. Moreover, the unnecessary latency caused by wrong check decisions

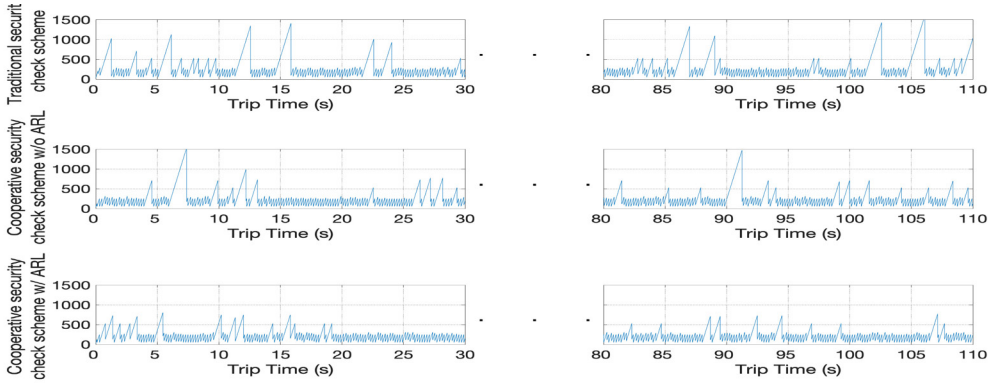


FIGURE 7. System AoI for different security check schemes.

is harmful to system AoI as well. Therefore, although the system AoI performance of the cooperative scheme is better than that of the traditional scheme, the performance is sometimes affected by Sybil attack and wrong check decision. Compared with the other two schemes, cooperative security check scheme with ARL can make the security check decision in good time when the train is under the attack of Sybil train. Moreover, the wrong security check does not occur in the normal operation scenario. Therefore, as shown in the third subfigure of FIGURE 7, the cooperative security check scheme with ARL can achieve the best system AoI performance in these three security check schemes due to a smaller number of large AoI fluctuation times.

Next, to present the benefit of the proposed cooperative security check with ARL in the designed systems clearly, the number of peak AoI violation times of traditional security scheme, cooperative security scheme without ARL and cooperative security scheme with ARL are quantitatively compared. To analyze the number of peak AoI violation times without the effect from random re-transmission and packet loss, a peak AoI threshold and an initial value are marked as 700 and 1 respectively. When peak AoI value exceeds the threshold, it will be configured as a peak AoI violation, and the mark value will be set as 2. Therefore, as we can see in FIGURE 8, the number of peak AoI violation times of traditional scheme, cooperative scheme without ARL and cooperative scheme with ARL during the operation are 23, 13 and 7 respectively. Therefore, the number of peak AoI violation times of proposed cooperative security check with ARL is much lower than that of the traditional scheme and cooperative security scheme without ARL. This result further verifies that the system AoI is enhanced by setting the proposed cooperative security check with ARL as the main security check scheme in train-centric CBTC systems.

FIGURE 9 shows average AoI performance for three security schemes under different SINR, where the x-axis is the value of SINR, and y-axis is the average AoI. It is quite clear that cooperative security check scheme with ARL has the lowest average AoI in these three schemes, which represents the best integrated QoS and security performance. This is

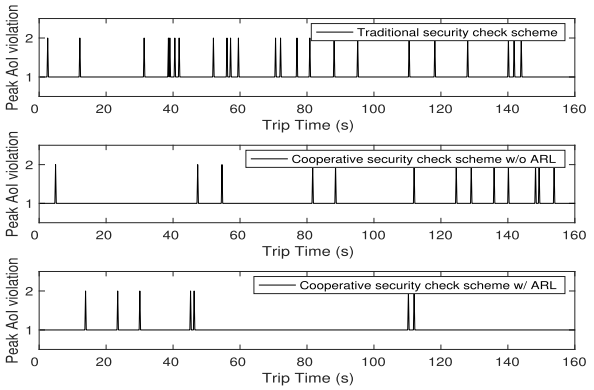


FIGURE 8. The number of peak AoI violation times for different security check schemes.

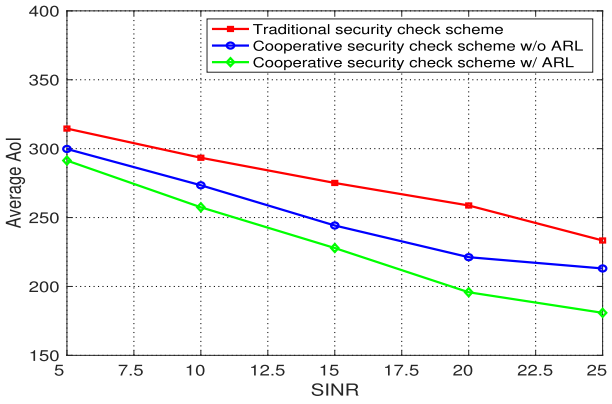


FIGURE 9. System average AoI for different security check schemes under different SINR.

because the cooperative security check scheme with ARL can successfully detect and defense almost Sybil attack compared with the other two schemes. Moreover, unlike the cooperative security check scheme without ARL, whose false probability of check decision is increased due to low SINR and bad wireless condition, the train can make the correct decision with the help of ARL algorithm, whether in good or bad SINR condition.

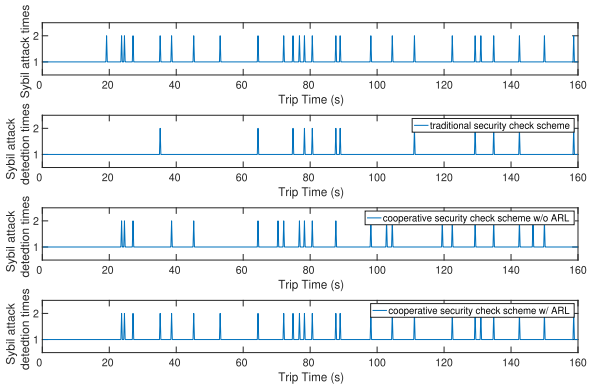


FIGURE 10. The number of successful Sybil attack detection times based on different security schemes.

FIGURE 10 shows the simulation results of the number of Sybil attack detection times based on different security schemes. As we can see in the first subfigure in FIGURE 10, we randomly set plenty of Sybil attacks when a train is running on the track, where the total number of attack times is 26. To analyze of the successful detection rate, we set an initial mark value as 1 in the rest subfigures. When there is a successful detection about the Sybil attack, the mark value is set as 2. As shown in FIGURE 10, in the train-centric CBTC wireless communication systems, the number of successful detection times of cooperative security check scheme with and without ARL are 25 and 18 respectively, while 12 is for the traditional security check scheme. Thus, the successful detection rate for these three schemes are 96%, 70%, and 46% respectively. The reason of an undetected Sybil attack in proposed scheme is that the cooperative security check is not activated due to some shortages of A3C algorithm. But the successful detection rate of the proposed scheme is still the highest one. Moreover, for the unnecessary security check times when there is no Sybil attack, the cooperative security check scheme with and without ARL are 0 and 4 respectively. Therefore, for the train-centric CBTC with T2T, the cooperative security check scheme with ARL can not only protect the operating train from Sybil attack more efficiency than the traditional security check scheme, but also decrease the unnecessary security check times compared with the scheme without ARL.

VII. CONCLUSION AND FUTURE WORK

The QoS of CBTC wireless communication systems is very important in urban rail transit system. The security guarantee performance is even more important. The Sybil attack is one of the security threats, which can impact the operation efficiency of trains and even the life safety of passengers. In this paper, we first formulated a novel train-centric CBTC systems with T2T as the novel CBTC systems for next-generation urban rail transit. To reduce the hazard from Sybil attack and guarantee the security performance of CBTC systems, the local security certification scheme and cooperative security check scheme were proposed for the train-centric CBTC. The AoI was proposed to stand for the integrated QoS and security performance train-centric CBTC systems. Moreover, asynchronous reinforcement learning was adopted to generate the appropriate policies including security check action and link selection action as well. Compared with the traditional security check scheme, simulation results showed that in the train-centric CBTC wireless communication systems, cooperative security check with asynchronous reinforcement learning could achieve the best system AoI, system average AoI and peak AoI performance. Furthermore, the proposed security check scheme could achieve a higher successful Sybil attack detection rate than the traditional security check scheme as well. For future work, we will extend our proposed method to some complex scenario in urban rail transits. Some more details will be added in the reward function of machine learning. Moreover, deep reinforcement learning will be used to improve the integrated QoS of train-centric CBTC systems.

REFERENCES

[1] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2389–2406, 3rd Quart., 2018.

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

[3] S. G. Shirlaw, "Radio and communications-based train control: Migration, interoperation and system engineering issues," in *Proc. Railway Eng.-Challenges Railway Transp. Inf. Age*, 2008, pp. 1–5.

[4] B. Bu, F. R. Yu, T. Tang, and C. Gao, "Performance improvements of communication-based train control (CBTC) systems with unreliable wireless networks," *Wireless Netw.*, vol. 20, no. 1, pp. 53–71, 2014.

[5] L. Zhu, F. R. Yu, T. Tang, and B. Ning, "An integrated train–ground communication system using wireless network virtualization: Security and quality of service provisioning," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9607–9616, Dec. 2016.

[6] H. Chen, L. Liu, T. Novlan, J. D. Matyjas, B. L. Ng, and J. Zhang, "Spatial spectrum sensing-based device-to-device cellular networks," *IEEE Trans. Commun.*, vol. 15, no. 11, pp. 7299–7313, Nov. 2016.

[7] N. Mastronarde, V. Patel, J. Xu, L. Liu, and M. van der Schaar, "To relay or not to relay: Learning device-to-device relaying strategies in cellular networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1569–1585, Jun. 2016.

[8] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop Hot Topics Netw. (HotNets-IV)*, Annapolis, MD, USA, 2005, pp. 1–6.

[9] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Security Ad Hoc Sensor Netw.*, 2005, pp. 11–21.

[10] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, 2013.

[11] X. Feng, C.-Y. Li, D.-X. Chen, and J. Tang, "A method for defensing against multi-source sybil attacks in VANET," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 2, pp. 305–314, 2017.

[12] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 523–538, 2013.

[13] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2011.

[14] L. Zhu, Y. He, F. R. Yu, B. Ning, T. Tang, and N. Zhao, "Communication-based train control system performance optimization using deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10705–10717, Dec. 2017.

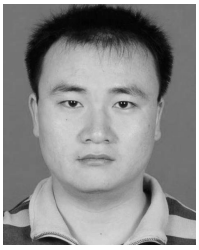
[15] X. Wang, L. Liu, T. Tang, and W. Sun, "Enhancing communication-based train control systems through train-to-train communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1544–1561, Apr. 2019.

[16] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, "Vehicle-to-everything (v2x) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 70–76, Jun. 2017.
[17] X. Wang, H. Jiang, T. Tang, and H. Zhao, "The QoS indicators analysis of integrated EUHT wireless communication system based on urban rail transit in high-speed scenario," *Wireless Commun. Mobile Comput.*, vol. 2018, Apr. 2018, Art. no. 2359810.
[18] H. Zhao, Y. Cao, L. Zhu, and W. Xu, "Integrated train ground radio communication system based TD-LTE," *Chin. J. Electron.*, vol. 25, no. 4, pp. 740–745, Jul. 2016.
[19] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.
[20] S. Eckelmann, T. Trautmann, H. Ußler, B. Reichelt, and O. Michler, "V2v-communication, LiDAR system and positioning sensors for future fusion algorithms in connected vehicles," *Transp. Res. Procedia*, vol. 27, pp. 69–76, Sep. 2017.
[21] L. Zhu, F. R. Yu, B. Ning, and T. Tang, "Design and performance enhancements in communication-based train control systems with coordinated multipoint transmission and reception," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 3, pp. 1258–1272, Jun. 2014.
[22] M. Costa, M. Codreanu, and A. Ephremides, "On the age of information in status update systems with packet management," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1897–1910, Apr. 2016.
[23] V. Mnih, A. P. Badia, M. Mirza, A. Graves, T. Lillicrap, T. Harley, D. Silver, and K. Kavukcuoglu, "Asynchronous methods for deep reinforcement learning," in *Proc. Int. Conf. Mach. Learn.*, 2016, pp. 1928–1937.
[24] S. Su, X. Li, T. Tang, and Z. Gao, "A subway train timetable optimization approach based on energy-efficient operation strategy," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 883–893, Jun. 2013.

XIAOXUAN WANG received the B.S. degree in electronic and information engineering from Beijing Jiaotong University, Beijing, China, in 2014, where he is currently pursuing the Ph.D. degree. He was a Visiting Ph.D. Student with Virginia Tech, Blacksburg, VA, USA, sponsored by the China Scholarship Council, from 2017 to 2018. His research interests include the train-wayside and train-to-train communication technologies in communication-based train control (CBTC) systems, the security of CBTC systems, and the cognitive control in CBTC systems.

LINGJIA LIU received the B.S. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA.

He spent the summer of 2007 and the spring of 2008 at the Mitsubishi Electric Research Laboratory (MERL). He was an Associate Professor with the EECS Department, University of Kansas (KU). He spent over three years working at the Standards and Mobility Innovation Laboratory, Samsung Research America (SRA), where he received the Global Samsung Best Paper Award twice, in 2008 and 2010. He was leading Samsung's efforts on multiuser MIMO, coordinated multipoint (CoMP), and heterogeneous networks in LTE/LTE-advanced standards. He is currently an Associate Professor with the ECE Department, Virginia Tech (VT). His general research interests include emerging technologies for 5G cellular networks, including machine learning for wireless networks, massive MIMO, massive MTC communications, and mmWave communications. He received the Air Force Summer Faculty Fellowship, from 2013 to 2017, the Miller Scholar at KU, in 2014, the Miller Professional Development Award for Distinguished Research at KU, in 2015, and the 2016 IEEE GLOBECOM Best Paper Award. He is currently an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE TRANSACTIONS ON COMMUNICATIONS and an Associate Editor of the *EURASIP Journal on Wireless Communications*, *Networks*, and *International Journal of Communication Systems* (Wiley).



LI ZHU received the Ph.D. degree in traffic control and information engineering from Beijing Jiaotong University, Beijing, China, in 2012. He is currently a Faculty Member with Beijing Jiaotong University and a Visiting Scholar with Carleton University, Ottawa, ON, Canada, and The University of British Columbia, Vancouver, BC, Canada. His research interests include train-ground communication technology in communication base train ground communication (CBTC) systems and cross-layer design in train-ground communication systems.

TAO TANG received the Ph.D. degree in engineering from the Chinese Academy of Sciences, Beijing, China, in 1991.

He is currently the Director of the School of Electronic and Information Engineering and the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing. His research interests include communication-based train control, high-speed train control systems, and intelligent transportation systems. He is also a member of the Experts Group of High Technology Research and Development Program of China (863 Program) and the Leader of the Field of Modern Transportation Technology Experts Group. He is also a Specialist in the National Development and Reform Commission and the Beijing Urban Traffic Construction Committee.