Hindawi
Complexity
Volume 2021, Article ID 2175780, 10 pages
https://doi.org/10.1155/2021/2175780

Research Article

A Resilience-Based Security Assessment Approach for CBTC Systems

Ruiming Lu,[1] **Huiyu Dong**,[1] **Hongwei Wang**,[2] **Dongliang Cui**,[3] **Li Zhu**,[4] **and Xi Wang**[4]

[1]*National Research Center of Railway Safety Assessment, Beijing Jiaotong University, Beijing, China*
[2]*State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China*
[3]*State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang, China*
[4]*State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China*

Correspondence should be addressed to Hongwei Wang; hwwang@bjtu.edu.cn

Received 29 June 2021; Accepted 28 September 2021; Published 21 October 2021

Academic Editor: Xuzhen Zhu

With the rapid development of urban rail transit systems, large amounts of information technologies are applied to increase efficiency of train control systems, such as general computers, communication protocols, and operation systems. With the continuous exposure of information technology vulnerabilities, security risks are increasing, and information is easy to use by malicious attackers, which can bring huge property and economic losses. The communication-based train control (CBTC) system is the most important subsystem of urban rail transit. The CBTC system ensures safe and efficient operation of trains, so the quantitative assessment of cyber security is quite necessary. In this paper, a resilience-based assessment method is proposed to analyze the security level of CBTC systems based on indicators of both the cyber domain and the physical domain. The proposed method can demonstrate the robustness and recovery ability of CBTC systems under different security attacks. Based on the structural information entropy, the fusion of different indicators is achieved. Two typical attacking scenarios are analyzed, and the simulation results illustrate the effectiveness of the proposed assessment approach.

1. Introduction

At present, railway is developing rapidly around the world, especially in China, where the high-speed railway (HSR) has a total length of 35,000 kilometers, accounting for approximately 66.7% of the world's high-speed railways [1]. China has also made significant progress in urban rail transit; there are more than 200 lines, and the total operation length is more than 6000 km [2]. Ensuring the punctuality of trains is the most significant goal of railways, and it can promote the sustainable development and bring the maintenance of social stabilization.

Communication-based train control (CBTC) is the key technology of urban rail transit to keep trains operation safe and efficient, which can provide real-time operation information for trains and generate control and dispatch strategies. In order to increase the automation and informatization level of CBTC systems, communication, computer, and control technologies have been widely applied [3]. Additionally, security risks are introduced in CBTC systems and can cause the destruction of railway transportation organization, which is the same as the other industrial control systems [4, 5].

Generally, a CBTC system can be taken as a typical cyber-physical system [6], where the computer network is working at the cyber domain while trains are running at the physical domain. Cyber attacks are usually carried out on computer nodes or communication links, which will cause information delay and tampering. Considering the principles of CBTC systems, the normal operation of trains could be disturbed, such as emergency braking. For example, wireless local area networks (WLANs) are adopted as the main method of bidirectional train-ground communications of train control systems [7, 8], which could be easily

interfered and attacked [9] as WLANs work at the public frequency and the authentication mechanism is unidirectional. Once wireless links are cut off under denial of service (DoS) attacks, trains cannot receive the movement authority (MA) from the control center, and emergency braking must be implemented in order to keep trains safe. Obviously, the operation efficiency is seriously reduced.

As urban railways are designed to deliver passengers, CBTC systems are safety-critical, and the fail-safe mechanisms are applied in order to achieve the demanded performance including reliability, availability, maintainability, and safety (RAMS) [10, 11]. In the traditional assessment approach to CBTC systems, RAMS is the significant statistical indicator system [12, 13] according to IEC 62278 [14], where qualitative measures include failure probabilities, mean time to failure (MTTF), mean time between failures (MTBF), and two-dimensional risk matrixes (risk probabilities and risk consequences). Therefore, the existing assessment approach focuses on the large time scale, which cannot determine in real time the effects caused by the temporal or sudden disruption. However, security events are often unexpected, and malicious attacks are implemented depending on the subjective will of attackers, being random. As a result, it is not appropriate to adopt traditional statistics indicators to evaluate performance of train control systems under attack.

As mentioned above, CBTC systems are designed to provide transportation service, and the robustness and recovery capability are critical when cyber attacks are performed. The Department of Homeland Security developed a plan to achieve critical infrastructure security and resilience in 2013 [15]. The transportation systems sector-specific plan [16] was also proposed. It identifies the transportation system's security and resilience priorities and describes the approach to managing critical infrastructure risks, where the railway system is included. Therefore, a novel assessment approach based on resilience is proposed in this paper.

The resilience of a CBTC system could be illustrated as Figure 1 according to [17]. Generally, a CBTC system keeps at the normal operation level, and trains are running according to the predesigned timetable. At t_i^o, the cyber attacks are implemented, and system performance is still kept at the same level. From t_i^o to t_i^d, attackers search the target and inject malware to affect the normal operation. Therefore, system performance begins to go down at t_i^d, and it reaches the lowest point at t_i^m. Meanwhile, some protection mechanisms are triggered to mitigate effects of attacks. From t_i^s, the system begins to recover and reaches a new stable level at t_i^r. Therefore, when a security assessment approach is applied, there are three stages which should be considered: the preevent stage ($t < t_i^o$), the during-event stage ($t_i^o < t < t_i^n, t_i^m < t_i^n < t_i^s$), and the postevent stage ($t_i^n < t < t_i^r, t_i^m < t_i^n < t_i^s$). Considering the characteristics of cyber-physical systems, performance of a train control system should contain both indicators of network from cyber domain and those of train operation performance from physical domain. Generally, the cyber domain is discrete while the physical domain is continuous. Therefore, the structure information entropy is applied to fuse different indicators [18], which can measure consequences of cyber attacks and demonstrate overall performance changes of CBTC systems versus the whole process of security events. In this paper, the resilience of CBTC system is assessed by the structure information entropy.

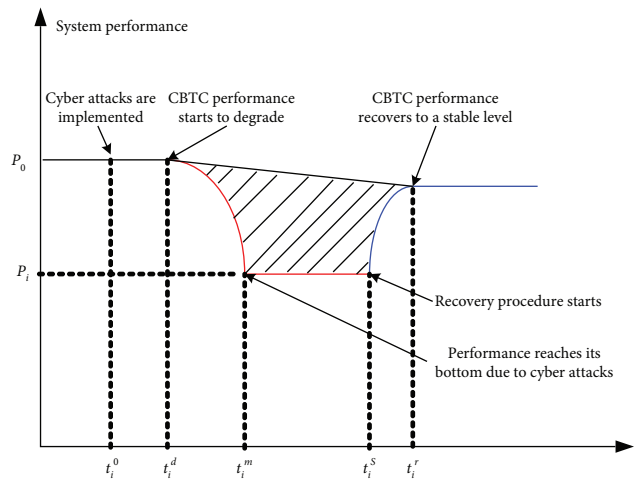

Figure 1: The resilience of a CBTC system.

The rest of this paper is organized as follows. A typical CBTC system is shown in Section 2. Section 3 describes the assessment model based on structural information entropy. Section 4 presents simulation results and some discussions. Finally, we conclude the study in Section 5.

2. Overview of CBTC Systems

Figure 2 demonstrates a typical CBTC system for urban rail transit, which includes some critical equipment, e.g., automatic train supervision (ATS), data storage unit (DSU), computer interlock (CI), zone controller (ZC), and vehicle on-board controller (VOBC). VOBC receives the control command from ZC and transmits the train status through wireless communications, where WLANs and long-term evolution for metro (LTE-M) are usually applied. WLANs-based train-ground communication systems consist of wayside access points (APs) and on-board mobile stations (MSs).

Generally, trains are running at a high speed and sending the corresponding information including velocity, position, and direction to the ZC. ZC generates movement authorities (MAs) to trains to inform the train about the location of the nearest obstacle, which could be a running train, a station, or a turnout. The train obtaining the MA should calculate the permitted maximum velocity to keep a safe distance to the nearest obstacle. During the process, messages between trains and ZCs are transmitted through WLANs or LTE-M. Obviously, the reliability and dependability of wireless communications are significant to CBTC systems.

As mentioned above, the fail-safe mechanisms are embedded in the operating principle of the CBTC system so that when a specific type of failure occurs, it will not cause harm to other equipment, the environment, or the personnel or cause minimal harm. Therefore, redundant and fault tolerance architectures are applied, such as double 2-vote-2 architecture for ZC, DSU, and CI. On the left part of

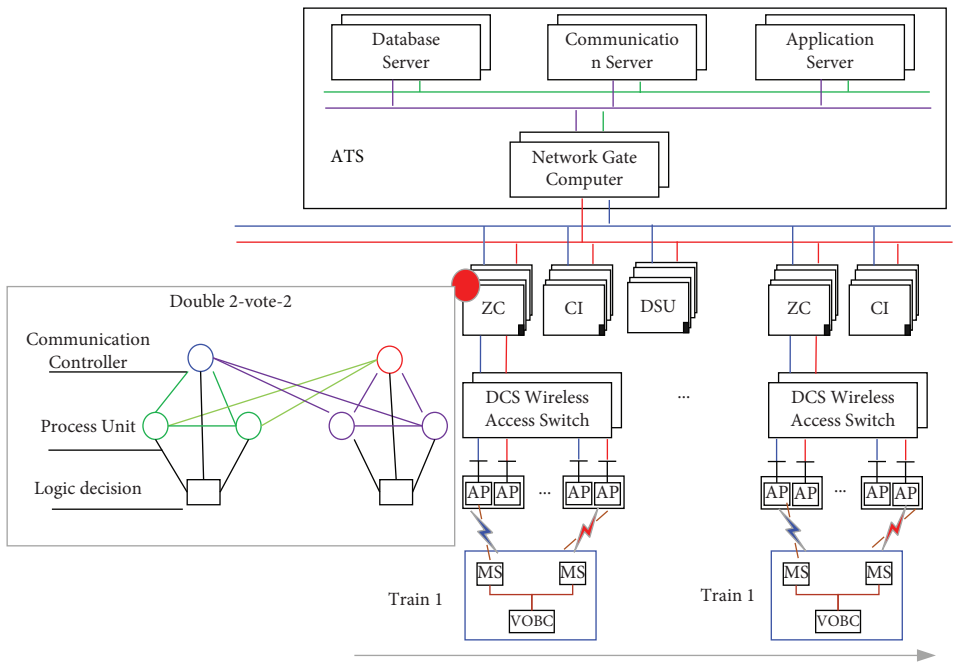

Figure 2: A typical CBTC system.

Figure 2, the double 2-vote-2 architecture is demonstrated, where there are two communication controllers (CCs), four processing units (PUs), and two logic decision makers. In the architecture, one CC, two PUs, and one logic decision maker make up the main system while the others are the standby system. Generally, when the main system does not work well, the standby system switches to the main role. Therefore, ZC, DSU, CI, and ATS are not standalone devices but subsystems. For example, ATS includes database servers, communication servers, application servers, and network gate computers. Some dedicated protocols are developed to keep the confidentiality, integrity, and availability of information, such as railway signalling safe protocols (RSSP) derived from EN 50159.

Conversely, applications of general information technologies could bring security risks, such as server message block (SMB) protocol vulnerabilities, remote code execution vulnerabilities, authentication vulnerabilities, DoS threats on wireless communications, and false data injection threats. The combined effects of security threats and vulnerabilities can generally bring changes of CBTC network topology, such as the downtime of one server due to virus, which can lead to interruptions of communications from the server to any other equipment. For some specific scenarios, under protection of fail-safe mechanisms, changes of CBTC topology cannot affect the normal train operation. With dual-network redundancy of wireless communications, although one wireless link between a train and ZC is blocked due to jamming attacks or DoS attacks, the train could still keep the preset running trajectory as the other wireless link can provide one channel to transmit the control command. Therefore, a security assessment approach should consider effects of the existing fail-safety mechanisms, which can precisely evaluate the practical robustness and the recovery capability of train control systems.

3. The Resilience Assessment Model of CBTC Systems

As mentioned above, cyber domain of CBTC system is a computer network with different computer nodes and communication links. The physical domain consists of trains with effects of traction and braking according to commands from the cyber domain. Obviously, abnormal performance of cyber domain could affect the operation of trains and bring on disturbance to the transportation service of urban rail transit.

According to the definition of resilience, system performance indicators should be determined based on the characteristics of CBTC. As a cyber-physical system, there are amounts of performance indicators of cyber domain and physical domain. Therefore, the performance variance due to cyber attacks should be described based on difference indicators. In this section, we develop a novel method based on the structural information entropy to demonstrate the real-time system performance of both the cyber domain and the physical domain.

3.1. Cyber Domain. As a CBTC system could be treated as a computer network, we built a graph model $G(V, E)$, where $v_i \in V$ is the device of CBTC systems and $e_i \in E$ is the communication link among devices. Two-dimensional structural information of graphs is proposed to quantitatively measure the force of the network to resist cascading failures caused by intentional virus attacks, as the general Shannon's information entropy failed to support

communication network. The definition of two-dimensional structural information entropy is shown as follows:

$$H^s(G) = \sum_{j=1}^{L} \frac{V_j}{2m} \cdot H\left\{\frac{d_1^{(j)}}{V_j}, \ldots, \frac{d_n^{(j)}}{V_j}\right\} - \sum_{j=1}^{L} \frac{g_j}{2m} \log_2 \frac{V_j}{2m},$$

$$= -\sum_{j=1}^{L} \frac{V_j}{2m} \sum_{i=1}^{n_j} \frac{d_i^j}{V_j} \log_2 \frac{d_i^j}{V_j} - \sum_{j=1}^{L} \frac{g_j}{2m} \log_2 \frac{V_j}{2m}, \tag{1}$$

where L is the number of modules in partition $\mathbb{P}$ which could be the subsystem of a CBTC system, n_j is the number of nodes in module X_j, $d_i^{(j)}$ is the degree of the i_{th} node in X_j, V_j is the volume of module X_j (i.e., the sum of degrees of all the nodes in X_j), g_j is the number of edges with exactly one endpoint in module j, m is the number of edges in G, and $2m$ is the volume of G.

Equation (1) assumes that each vertex and each edge is completely the same. However, in CBTC systems, different operation systems and hardware platforms are adopted based on functional attributes of devices. Meanwhile, according to safety-critical requirements, RSSP-1 and RSSP-2 are individually applied to the closed network and the open network. As a matter of fact, some private protocols (PPs) are also developed due to specific requirements. For some unsafe communication links, information is transmitted in clear text. Therefore, there are a few types of vertexes and edges, which means every element of a CBTC graph model should be described with specific parameters according to its inherent features.

Based on the password strength, the security protection policies, and the number and level of vulnerabilities, a security factor of a node could be designed. Vulnerabilities could be classified into five levels according to the common vulnerability scoring system (CVSS), where the corresponding weight of a node can be determined.

$$VN_i = \chi \times \frac{\nu_\alpha}{\max(\nu_\alpha)} \times \frac{\nu_\beta}{\max(\nu_\beta)},$$

$$\chi = \frac{n_{pp}}{n_{dp}},$$

$$\nu_\alpha = \sum_{k=1}^{N} n_k * w_k, \tag{2}$$

$$\nu_\beta = -\log_2 N_{\text{op}}^L,$$

where χ denotes the security protection situation of a device, ν_α is the index which demonstrates the overall state of vulnerabilities, ν_β is the measure of the password strength, n_{pp} is the number of practical security protections, n_{dp} is the number of desirable security protections, N is the number of vulnerability classifications, n_k is the number of the k_{th} vulnerabilities, w_k is the weight of the k_{th} vulnerability, N_{op} is the number of the password character sets, and L is the length of the password.

Similarly, for an edge, based on protocols of communication links, the weight of each edge could be determined as follows:

$$\omega_e = S_j \times R_j \times \frac{N_s}{N_d}, \tag{3}$$

where S_j is the security level of the protocol adopted by the communication link j, R_j is the reliability level of the protocol, N_s is the number of protection methods practically adopted by the protocol, and N_d is the number of protection methods which should be adopted by the protocol. Therefore, S_j is determined by the openness of the standard protocol, where the private protocol can be assigned to the maximum value. R_j depends on whether the communication link is wireless, where the value of a wireless link is obviously smaller than that of a wired link. N_d is the maximum value of N_s in the system.

Therefore, the structural entropy of a CBTC system can be formulated as follows:

$$H^s(G(t)) = -\sum_{j=1}^{L} \frac{V_j(\omega_e)}{2m} \sum_{i=1}^{n_j} \frac{d_i^j(\omega_e, VN_i)}{V_j(\omega_e)} \log_2 \frac{d_i^j(\omega_e, VN_i)}{V_j(\omega_e)} - \sum_{j=1}^{L} \frac{g_j(\omega_e)}{2m} \log_2 \frac{V_j(\omega_e)}{2m}, \tag{4}$$

where $V_j(\omega_e)$ is the weighted V_j in (1), $d_i^j(\omega_e, VN_i) = VN_i \times d_i^j(\omega_e)$, $d_i^j(\omega_e)$ is the weighted d_i^j in (1), and $g_j(\omega_e)$ is the weighted g_i in (1).

3.2. Physical Domain. The structural entropy in (4) can demonstrate changes of network typologies due to node failures and interruptions of communication links caused by security issues, which is the performance variance of cyber space. However, due to cyber-physical characteristics of CBTC systems, performance variances of physical space should also be considered. Based on the transportation service attribute of CBTC systems, the achievement rate of timetables can be used to describe effects caused by security attacks on train operation. Firstly, the normalized value of the performance loss of a train is expressed as follows, where the min–max principle is applied.

$$\begin{aligned}
\Delta p_{\text{norm}} &= \alpha \Delta s_{\text{norm}} + \beta \Delta v_{\text{norm}} + \gamma \Delta t_{\text{arr-norm}}, \\
\Delta s_{\text{norm}} &= \frac{\Delta s - \Delta s_{\min}}{\Delta s_{\max} - \Delta s_{\min}}, \\
\Delta v_{\text{norm}} &= \frac{\Delta v - \Delta v_{\min}}{\Delta v_{\max} - \Delta v_{\min}}, \\
\Delta t_{\text{norm}} &= \frac{\Delta t_{\text{arr}} - \Delta t_{\text{arr-min}}}{\Delta t_{\text{arr-max}} - \Delta t_{\text{arr-min}}},
\end{aligned} \tag{5}$$

where $\Delta s_{\min}$, $\Delta v_{\min}$, $\Delta t_{\text{arr-min}}$, $\Delta s_{\max}$, $\Delta v_{\max}$, and $\Delta t_{\text{arr-max}}$ are the minimum and maximum value of the variation of the displacement, velocity, and arriving time, and α, β, and γ are the weight of three parameters.

Therefore, the performance of a whole subway line under attack can be formulated as follows, which is the y axis of Figure 1.

$$AR(t) = \frac{p_p(t) - p_l(t)}{p_p(t)} = 1 - \sum_{i=1}^{N} \frac{\Delta p_{\text{norm}}^i}{N}, \tag{6}$$

where $p_p(t)$ is the train operation performance of the entire line under normal conditions and $p_l(t)$ represents the performance loss of the whole line under attack.

3.3. Resilience of CBTC Systems. Equation (6) demonstrates the overall performance of CBTC systems under attack. With the attacking process being implemented, states of nodes and edges are changing. Therefore, $AR(t)$ and $H^s(G(t))$ are time-varied functions. By combining AR and $H^s(G(t))$, the performance of cyber space and physical space can be monitored, which can demonstrate effects of security attacks on CBTC systems shown as follows:

$$H(t) = AR(t) \times H^s(G(t)). \tag{7}$$

According to the metric proposed in [19], there are three attributes to measure resilience: absorptive capacity, adaptive capacity, and restorative capacity, and the corresponding expression is shown as follows:

$$\rho_j\left(S_p, H_r, H_d, H_o\right) = S_p \frac{H_r}{H_o} \frac{H_d}{H_o}, \tag{8}$$

where j is the j_{th} cyber attack, S_p is the recovery speed factor, H_r is the stable level after the system recovers from cyber attacks, H_d is lowest performance level of the system due to attacks, and H_o is the normal performance level of the systems. Obviously, H_r/H_o describes the adaptive capacity while H_d/H_o presents the absorptive capacity.

In addition, the recovery speed factor is determined according to some key timing.

$$S_p = \begin{cases} \dfrac{t_\delta}{t_{r^*}} \exp^{-a\left(t_r - t_{r^*}\right)}, & t_r > t_{r^*}, \\ \dfrac{t_\delta}{t_{r^*}}, & \text{else}, \end{cases} \tag{9}$$

where t_{delta} is the tolerable time before the recovery measures are implemented, t_{r^*} is the time when some initial measures are performed to decrease the effects of attacks, t_r is the time when CBTC system recovers to a stable operation level, and a is a decay factor.

Considering operation principles of CBTC systems, when attacks are performed and cause failures of critical equipment such as ZC, trains will implement emergency braking to keep safe based on fail-safe mechanisms. Obviously, the performance of the whole subway line will fall down to a lowest level H_d, and the corresponding time is t_δ. Due to the existence of backup operation mode, CBTC system can still operate with ZCs and trains will recover from the emergency braking state, which is the initial measure to keep the continuous service. Therefore, t_{r^*} is determined. Finally, after cyber attacks finish, ZCs being attacked can run at a normal state and CBTC systems can return to a stable level H_r which is generally smaller than the normal level H_o. Hence, t_r can also be obtained.

4. Simulation Results and Discussions

4.1. Simulation Description. Take Beijing Subway Yizhuang Line, for example, where there are 13 stations, 6 ZCs, and 6 CIs and the length is 23.3 km. Based on the structure of CBTC systems and the architectures of ZCs, CIs, and ATS, a computer network of CBTC is demonstrated in Figure 3, where the double 2-vote-2 architecture is applied in ZC and CI subsystems.

The normal timetable of Beijing Subway Yizhuang Line is taken as the input of simulations as shown in Figure 4. The typical jamming attack is implemented on train-ground wireless communications. There are two scenarios:

Scenario 1 took ZCs as attacking targets. Generally, ZC failures could cause serious disturbances to train operations, as trains have to perform the emergency braking when they cannot receive MAs from ZCs. Therefore, operators must try their best to repair failures or implement some other emergency response

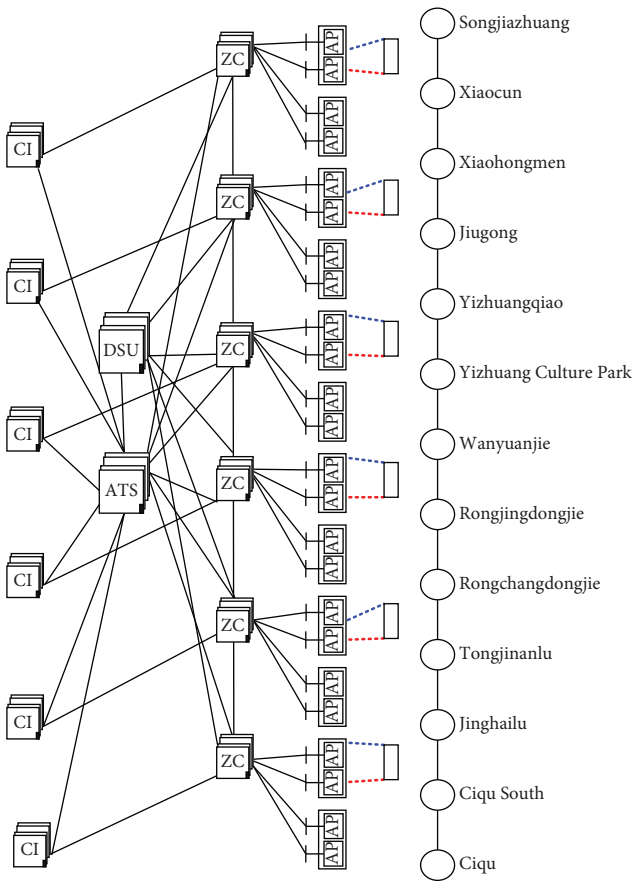

Figure 3: The computer network of Beijing Subway Yizhuang Line.

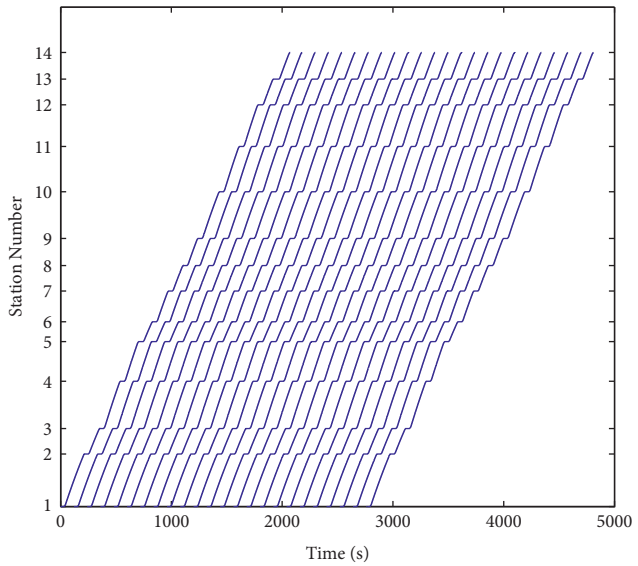

Figure 4: The timetable of Beijing Subway Yizhuang Line.

measures. We assume that operators should take several minutes to make the system recover from ZC failures. According to the architecture in Figure 2, the attacking path is CC1 (300 s) ⟶ PU1 and PU2 (400 s) ⟶ CC2 (600 s) ⟶ PU3 and PU4 (700 s). In the scenario, there were three ZC systems being attacked and crashing. After several minutes, the three ZC systems successively recovered at 2500 s, 2900 s, and 3300 s, respectively.

Scenario 2 took trains as attacking targets, where DoS attacks were implemented on wireless communications between ZCs and VOBCs. Through sending a large number of data packets to exhaust bandwidth resources, communication interruptions could be caused, and trains have to perform the emergency braking to keep safe based on "fail-safe" mechanisms. Therefore, trains worked under the degraded mode depending on operation of drivers until wireless communications recovered to normal. In the scenario, we attacked the 5th, 10th, and 15th trains, respectively, at $t = 1000$ s, $t = 2000$ s, and $t = 2500$ s. Successively, trains ran under the normal mode at $t = 1500$ s, $t = 2500$ s, and $t = 3000$ s.

4.2. Simulation Results

4.2.1. Performance of Cyber Space. Figure 5 shows the network performance based on the two-dimensional structure information entropy under scenario 1, where A, B, C, and D, respectively represent failures of CC1, PU1 and PU2, CC2, and PU3 and PU4 of ZC2. The initial network performance under the normal mode was 7.6754. During the attacking process, the main system and the standby system of ZC2 crashed, and the network performance fluctuated. When ZC3 and ZC4 successively crashed, the network performance reached 7.4068. Then, some measures were implemented to make ZCs recover to normal. Therefore, ZC2, ZC3, and ZC4 started to work normally in sequence, and the network performance quickly returned to the original value before the attack.

Figure 6 demonstrates the network performance under scenario 2, where wireless communications between trains and ZC were blocked by DoS attacks. The network performance had little influence, which means attacks on single or several wireless links could hardly bring obvious changes of the network topology. However, communication interruptions could lead to the emergency braking of trains, which obviously affected the operation of a subway line. Therefore, gentle changes of network performance cannot describe effects of DoS attacks on CBTC systems.

4.2.2. Performance of Physical Space. Figures 7 and 8 present practical timetables under two different scenarios. It can be seen from the timetable that, in the two attack scenarios, the normal operation of the train was greatly affected. Figure 7 indicates that after the first ZC system was compromised, the timetable began to be delayed under scenario 1. With the restoration of the ZC system one by one, the timetable began to recover, but it still had an impact on subsequent train operations. Figure 8 shows that even if there was no impact on the network domain, due to the DoS attack on the wireless communication between ZCs and VOBCs, the train could not obtain MAs, so it led to emergency braking, which still had an impact on the timetable. Therefore, cyber attacks

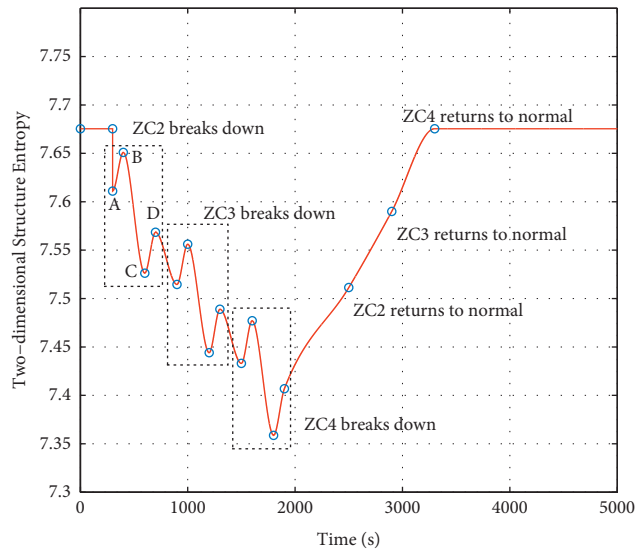

Figure 5: Network performance changes of the CBTC system under scenario 1.

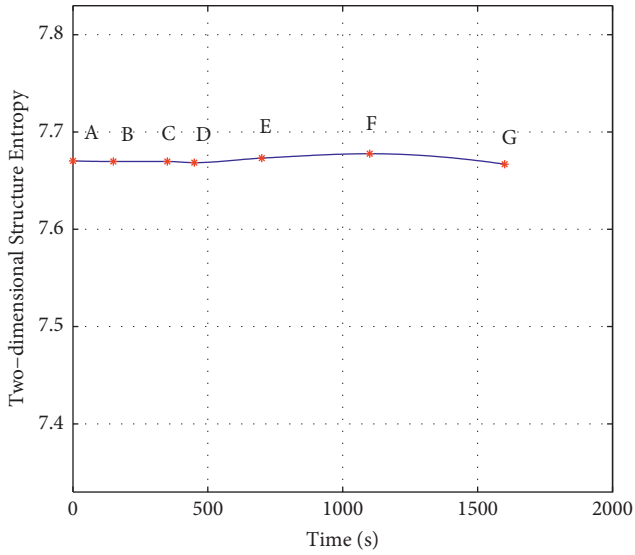

Figure 6: Network performance changes of the CBTC system under scenario 2.

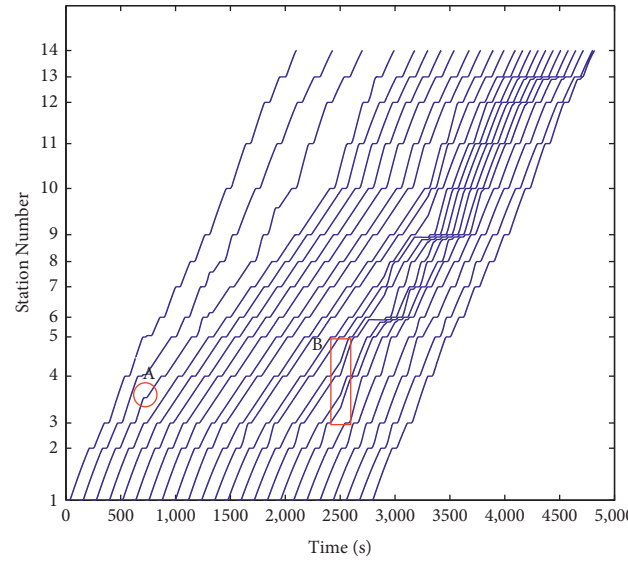

Figure 7: Practical timetable under scenario 1.

can badly affect the normal operation of a whole subway line. It is necessary to evaluate the train performance loss of a whole subway line under cyber attacks.

As shown in Figure 9, the train operation performance (defined in (6)) of the subway line decreased as several ZCs broke down (A ~ B) and then increased with the recovery of ZCs (B ~ C). With the recovery of ZCs, each train returned to the normal operation state. However, the performance loss is irreparable, and the curve could not reach the normal operation level as shown in area C.

The train operation performance of the subway line under DoS attacks on wireless communications is shown in Figure 10. It began to decrease (area A) and fell to the lowest point (area B) at $t = 2300$ s. In order to keep the continuity of transportation service, trains had to recover to the normal operation mode, and then the curve started rising. However, trains performing the emergency braking could affect normal operation of following trains in a certain area, and those far from the attacked ones could keep the normal model.

4.2.3. Resilience Assessment of CBTC Systems. As shown in Figures 11 and 12, the performance of the cyber domain and that of the physical domain were integrated, which could demonstrate the security state of the whole subway line under attack, and the corresponding polynomial fitting results were also included.

According to fitting results, the key parameters of (8) and (9) were determined as shown in Table 1. The lowest value of the security level under the two scenarios was close. In scenario 1, failures of one single ZC could affect all the trains within its control. Meanwhile, with the longer attacking

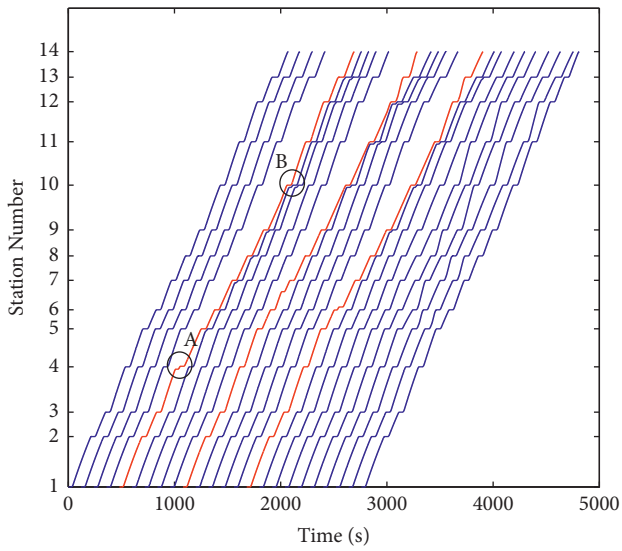

Figure 8: Practical timetable under Scenario 2.

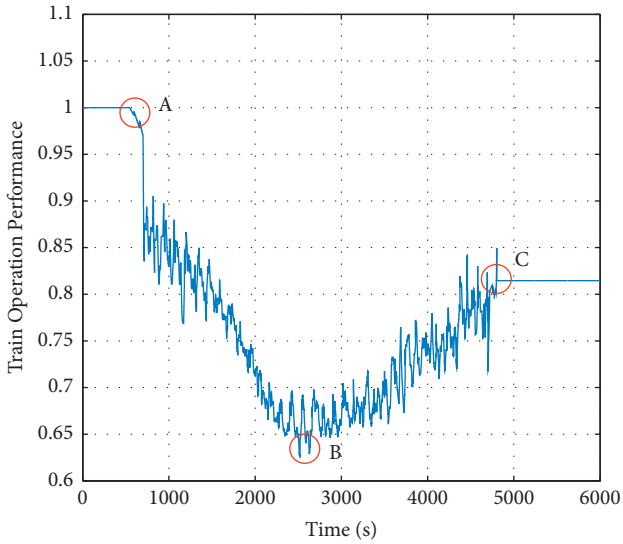

Figure 9: The train operation performance of the subway line under Scenario 1.

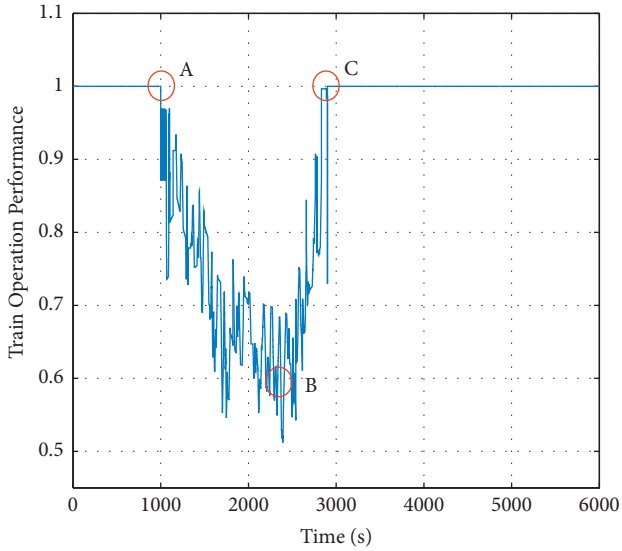

Figure 10: The train operation performance of the subway line under scenario 2.

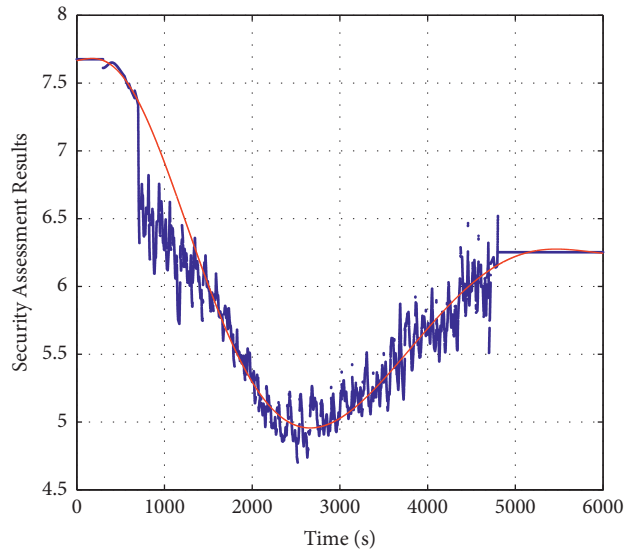

Figure 11: The overall performance of the subway line under scenario 1.

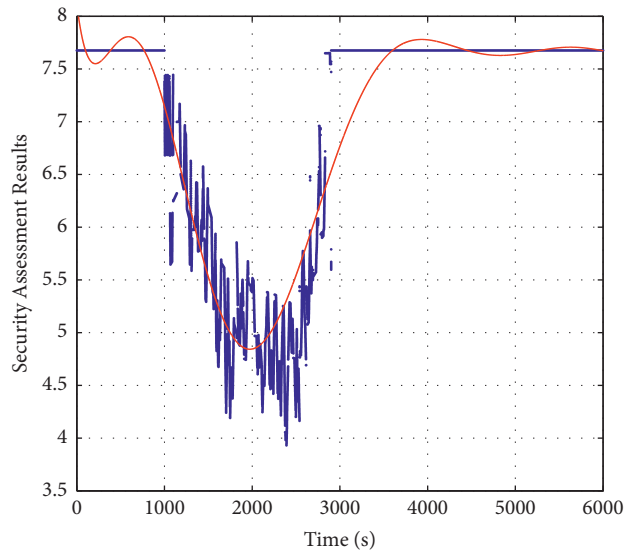

Figure 12: The overall performance of the subway line under scenario 2.

Table 1: Resilience parameters of CBTC system under two different scenarios.

Resilience parameters	Scenario 1	Scenario 2
H_o	7.6754	7.6754
H_d	4.9438	4.8213
H_r	6.2394	7.6754
t_δ (s)	3400	2500
$t_{r^*}(s)$	2119	3672
t_r (s)	4821	3672

time, the affected area was wider. Hence, it should take more time to recover to the normal level compared with scenario 2. In addition, interruptions of wireless communication could directly affect performance of trains. Therefore, the performance fading rate of scenario 2 was larger. In scenario 2, due to the DoS attack on the wireless communication between ZCs and VOBCs, although it still causes train delays, system performance will return to normal levels after the attack ends.

Table 2: Resilience assessment results of CBTC systems under two scenarios.

Assessment metrics	Scenario 1	Scenario 2
Absorptive capacity	0.6441	0.6281
Adaptability	0.8129	1
Recovery capacity	1.6049	1.2310
Resilience index	0.6446	1.7734

We could calculate three attributes of resilience as shown in Table 2. The absorptive capacities under the two scenarios were almost the same, which indicated that the CBTC system had similar robustness. As one ZC can control several trains, adaptability and recovery capacity of CBTC systems were weaker under scenario 1. Therefore, resilience can be quantitatively assessed according to the process of attacks.

5. Conclusion

In this paper, a resilience-based assessment approach is proposed to measure the security level of CBTC systems. The two-dimensional structure entropy is adopted to describe the performance of the cyber domain, and that of physical space is calculated according to the practical timetable and running states of trains. Based on stages of attacks, resilience metrics are utilized to analyze the security level of the whole subway line, where both cyber space and physical space are considered. Two typical attacking scenarios were built, and a practical subway line was taken as an example. Simulation results show that the resilience-based approach can efficiently evaluate the security level of CBTC systems under different attacks.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported by grants from the Fundamental Research Funds for the Central Universities (No. 2021QY007), National Natural Science Foundation of China under Grant (U18341211, 61925302, 61971030, 61973026), the Railway Traffic joint fund of Beijing Natural Science Foundation and TCT Technology (L181004), Traffic Control Technology (TCT) Innovation Funding under Grant 9907006509, the open project of State Key Laboratory of Synthetical Automation for Process Industries, Beijing Natural Science Foundation: L201002, and Natural Science Foundation of China under Grants: 61973026.

References

[1] S. Peng, X. Yang, H. Wang et al., "Dispatching high-speed rail trains via utilizing the reverse direction track: adaptive rescheduling strategies and application," *Sustainability*, vol. 11, no. 8, p. 2351, 2019.

[2] X. Yang, H. Yin, J. Wu, Y. Qu, Z. Gao, and T. Tang, "Recognizing the critical stations in urban rail networks: an analysis method based on the smart-card data," *IEEE Intelligent Transportation Systems Magazine*, vol. 11, no. 1, pp. 29–35, 2019.

[3] R. Pascoe and T. Eichorn, "What is communication-based train control?" *IEEE Vehicular Technology Magazine*, vol. 4, no. 4, pp. 16–21, 2009.

[4] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "Real time security assessment of the power system using a hybrid support vector machine and multilayer perceptron neural network algorithms," *Sustainability*, vol. 11, pp. 1–18, 2019.

[5] S. M. Wu, D. Guo, Y. J. Wu, and Y. C. Wu, "Future development of taiwans smart cities from an information security perspective," *Sustainability*, vol. 10, pp. 1–18, 2018.

[6] L. Bu, D. Xie, X. Chen, L. Wang, and X. Li, "Demo abstract: bachol- modeling and verification of cyber-physical systems online," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*, p. 222, Washington, DC; USA, April 2012.

[7] L. Zhu, F. R. Yu, B. Ning, and T. Tang, "Cross-layer handoff design in MIMO-enabled WLANs for communication-based train control (CBTC) systems," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 4, pp. 719–728, 2012.

[8] H. Wang, F. R. Yu, L. Zhu, T. Tang, and B. Ning, "A cognitive control approach to communication-based train control systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1676–1689, 2015.

[9] H. Wang, F. R. Yu, and H. Wang, "A cognitive control approach to interference mitigation in communications-based train control (cbtc) coexisting with passenger information systems (piss)," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, Article ID 17-0959-3, 13 pages, 2017.

[10] Y. Cao, H. Lu, and T. Wen, "A safety computer system based on multi-sensor data processing," *Sensors*, vol. 19, no. 4, p. 818, 2019.

[11] Y. Cao, Y. Zhang, T. Wen, and P. Li, "Research on dynamic nonlinear input prediction of fault diagnosis based on fractional differential operator equation in high-speed train control system," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 1, Article ID 013130, 2019.

[12] S. Hiraguri, K. Iwata, and I. Watanabe, *A Method of Evaluating Railway Signalling System Based on Rams Concept*, Springer, New York, NY, USA, pp. 97–105, 2011.

[13] F. Yan, C. Gao, T. Tang, and Y. Zhou, "A safety management and signaling system integration method for communication-based train control system," *Urban Rail Transit*, vol. 3, no. 2, pp. 90–99, 2017.

[14] E. CENELEC, *Railway Applications the Specification and Demonstration of Reliability, Availability, Maintainability and Safety (Rams)*, The European Standard, Brussels, Belgium, 1999.

[15] S. O. Johnsen and M. Veen, "Risk assessment and resilience of critical communication infrastructure in railways," *Cognition, Technology & Work*, vol. 15, no. 1, pp. 95–107, 2013.

[16] U. DHS, *Nipp 2013: Partnering for Critical Infrastructure Security and Resilience*, CreateSpace, Scotts Valley, CA, USA, 2013.

[17] Q. Zhu, D. Wei, and K. Ji, *Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics and Design Principles*, CRC Press, Boca Raton, FL, USA, 2015.

[18] A. Li, Q. Hu, J. Liu, and Y. Pan, "Resistance and security index of networks: structural information perspective of network security," *Scientific Reports*, vol. 6, no. 1, p. 26810, 2016.

[19] R. Francis and B. Bekera, "A metric and frameworks for resilience analysis of engineered and infrastructure systems," *Reliability Engineering & System Safety*, vol. 121, pp. 90–103, 2014.