


Article

Security Analysis for CBTC Systems under Attack–Defense Confrontation

Wenhao Wu ^{*,†} and Bing Bu [†] 

State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China

* Correspondence: wenhaowu@bjtu.edu.cn; Tel.: +86-132-418-29208

† These authors contributed equally to this work.

Received: 30 June 2019; Accepted: 2 September 2019; Published: 5 September 2019



Abstract: Communication-based train controls (CBTC) systems play a major role in urban rail transportation. As CBTC systems are no longer isolated from the outside world but use other networks to increase efficiency and improve productivity, they are exposed to huge cyber threats. This paper proposes a generalized stochastic Petri net (GSPN) model to capture dynamic interaction between the attacker and the defender to evaluate the security of CBTC systems. Depending on the characteristics of the system and attack–defense methods, we divided our model into two phases: penetration and disruption. In each phase, we provided effective means of attack and corresponding defensive measures, and the system state was determined correspondingly. Additionally, a semiphysical simulation platform and game model were proposed to assist the GSPN model parameterization. With the steady-state probability of the system output from the model, we propose several indicators for assessing system security. Finally, we compared the security of the system with single defensive measures and multiple defensive measures. Our evaluations indicated the significance of the defensive measures and the seriousness of the system security situation.

Keywords: GSPN; game theory; security; attack–defense confrontation

1. Introduction

With the advancement of urban modernization, urban rail transit has been considerably developed. Due to the development of the city and the growth of the population, urban rail transit is under tremendous pressure [1]. Therefore, researchers have obtained the communication-based train controls system based on modern communication, control technology, computer and traditional signal technology to improve operational efficiency and capabilities [2].

The CBTC system has many characteristics compared to traditional railway signal systems, such as high-resolution train location determination, independent of track circuits, and continuous, high capacity, bidirectional train-to-wayside data communications [3]. It is an automated train control system utilizing a variety of advanced technologies and equipment to ensure that trains operate at minimum safe distances for maximum transport capacity [4]. The CBTC system, with currently over 100 installations worldwide, is one of the most popular signaling systems among mass-transit rail operators today [5].

As a contemporary industrial control system, the CBTC system applies a large number of networked and information components, facing the risk of cyber attacks [6]. The system faces security issues such as high-risk vulnerabilities in devices, industrial network viruses, advanced persistent threats, and wireless technology vulnerabilities. In recent years, information security incidents in urban rail transit have emerged one after another. In March 2012, the Shanghai Shentong Metro Station information release system and the operation and dispatch system wireless network were attacked. In November 2012, the Shenzhen subway signal system was disturbed, resulting in frequent

emergency braking of multiple trains during operation. Finally, in 2016, hackers attacked the computer fare system of the Muni subway in San Francisco, USA, and used it to blackmail. These incidents have had a huge impact on urban traffic, disrupted traffic order, and brought huge economic losses. As mentioned above, urban rail transit is a significant urban infrastructure that is closely related to people's lives. When security problems occur in urban rail transit, emergency braking may occur on the train, which may disrupt train operation, increase urban traffic pressure and cause huge economic losses. Furthermore, train derailment or train collision events may come to happen, which will lead to unmeasurable life and property damage. Therefore, it is significant to capture the interactions between attack and defense and analyze the security of the CBTC systems. In this way, more researchers and industry experts can realize the significance of security for the CBTC system and how to improve the security of the system.

There are some previous works on modeling and evaluating the security of CBTC systems. Based on the continuity of urban rail transit operation services, Wang et al. [7] proposed a resilience-based security assessment approach that divides security risks into three phases: pre-attack, under attack, and after attack. In [8], a comprehensive analysis method of security and safety based on an extended fault tree was proposed. This paper synthesized the safety and security features of the urban rail transit train control system, comprehensively considered the security threats and vulnerabilities and the hazard sources of the train control system, and analyzed the relationship between security risks and safety risks. Dong et al. [9] used attack tree to evaluate the vulnerability of a CBTC system based on its network topology, redundant structure, and operation principles. Assessments covered the current security states, port auditing, password policies, and communication protocols of systems. Ferrari et al. [10] proposed a stochastic activity networks (SAN) model to conduct an availability assessment of CBTC systems. Lee et al. [11] defined the security requirements considering characteristics of the radio train control system using LTE-R and analyzing the risk of attack.

The CBTC system is one kind of cyber-physical system (CPS) consisting of two major components: a physical process and a cyber system [12]. To analyze the impact of offensive and defensive behavior on CBTC systems, we also refer to the research results of cyber-physical systems. In [13], a nonfunctional requirement (NFR) method was utilized to assess the safety and security of CPS. The intuitiveness of the NFR approach allowed us to determine the reasons for the poor security and to identify the techniques that will help to improve security. Mitchell et al. [14] simulated the dynamic Interaction between attack and defense behavior of cyber-physical systems based on a stochastic Petri nets model. Furthermore, the paper analyzed the impact of the intrusion detection interval and attack strength on the modernized electrical grid's mean time to failure (MTTF). In addition, in [15,16], authors used game theory to describe the state changes process of CPS under the strategies of attackers and defenders. Several quantitative indicators such as steady-state probability and MTTF were applied to evaluate system reliability. Depoy et al. [17] described a top-down functional assessment methodology for risk assessment of the system under four types of attacks: physical-only, cyber-enabled physical, cyber-only, and physical-enabled cyber attacks. A Boolean logic driven Markov processes (BDMPs) formalism proposed modeling attack steps and evaluate security risk in [18,19]. In [20,21], a hidden Markov model (HMM) was utilized to describe the stochastic dynamics of CPSs in the attack scenario. In addition, the authors in [22–24] analyzed a smart grid security situation based on Q-learning, which can display the attack–defense confrontation process well.

Referring to the multistage attack process for CPS, we divided the attack process of CBTC systems into two phases: the penetration phase and disruption phase [25]. In the penetration phase, the attacker invades the system through a wired or wireless approach, and the system will not be substantially damaged. After the successful invasion, the attacker launches substantial physical damage to the system, and the attack enters the disruption phase. In this paper, we can better grasp the vulnerability of the system through the phased research of the attack process.

In this paper, we utilized a generalized stochastic Petri net (GSPN) to describe attack and defense behavior and changes in the system state. We chose several typical attacks against the CBTC system

and the corresponding defenses to enrich our model. Different from papers about CPS security analysis, we used concrete attack and defense strategies instead of general strategies such as attack and no attack. The proposed model not only conforms to the characteristics of CPS but also combines the characteristics of CBTC with state changes and strategy choices. To more accurately simulate the attack and defense confrontation in the CBTC system, we introduce the game theory in the paper. By solving the Nash equilibrium, we got the probability that the attacker and the system would choose the attack and defense strategy, which is the most likely behavior choice for decision-makers on both sides under the rational premise. By doing this, we can get a complete GSPN model. We conducted attack and defense drills on the semiphysical simulation platform of the laboratory to help model parameterization. Our GSPN model can be combined with a continuous-time Markov process. We can get the steady-state probability of the system in each state by solving the Markov chain. Finally, we propose several security indicators to evaluate the security of CBTC systems under attack–defense confrontation based on model solution results.

The rest of the paper is organized as follows: In Section 2, security issues and attack–defense methods in CBTC systems are mentioned. In Section 3, we propose the security analysis model of CBTC systems under attack–defense confrontation. In Section 4, we present the process of the model solution. In Section 5, we utilize several indicators to analyze the system security. Finally, in Section 6, we conclude the paper and outline future areas.

2. Security Issues and Attack–Defense Strategies in CBTC Systems

2.1. A Typical CBTC System

This section presents the structure and composition of CBTC systems. The CBTC system is mainly composed of on-board equipment and wayside equipment. The basic composition of the CBTC system is shown in Figure 1. On-board equipment includes automatic train protection (ATP) equipment and automatic train operation (ATO) equipment for train operation monitoring, speed measurement positioning, and human–computer interaction. Wayside equipment includes a zone controller (ZC), automatic train supervision (ATS), computer interlocking (CI), and a database storage unit (DSU). The ATS is divided into the central ATS and the station ATS.

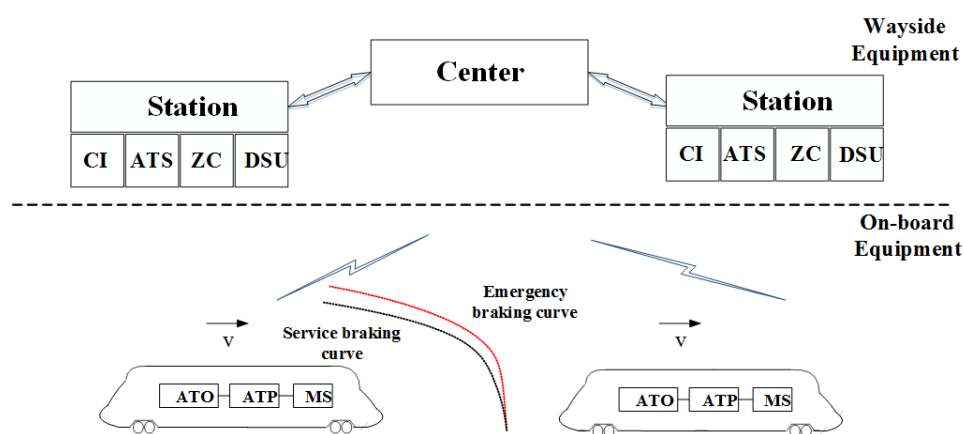


Figure 1. A typical communication-based train controls (CBTC) system.

The data communication system (DCS) of the CBTC system consists of two parts: the backbone network and the radio access network. The backbone network provides transparent data transmission channels for ground equipment. Most of the existing wireless access networks of the CBTC system use IEEE 802.11-based wireless local area networks (WLAN) equipment to realize real-time transmission of two-way and large-capacity information of the vehicle. To meet the high availability requirements of the CBTC system, the DCS adopts a ring network redundancy architecture. When a network cannot work normally due to equipment failure, the system can still send and receive data through another

network. At the same time, the ground backbone network is divided into several different subnets according to different subsystems. Generally, it is divided into five networks, two redundant signaling networks, two redundant ATS networks, and one maintenance network. The ATS network connects the central ATS and the station ATS and communicates with the signal network through the ATS gateway. The maintenance network consists of distributed maintenance machines and maintenance centers for fault diagnosis and routine maintenance.

2.2. Security Issues in CBTC Systems

A large number of network and information components are used in the CBTC system, such as communication technology, general computer technology, control technology, commercial Windows, a VxWorks operating system, and standard TCP/IP communication protocols. The use of these advanced technologies has greatly improved the automation and information level of the CBTC system but also introduced new security risks to the system. The main information security risks of the CBTC system are as follows:

1. Communication protocol risks. At present, DCSs use WLAN technology to complete wireless communication. WLAN works in the open industrial scientific medical (ISM) band, and there are vulnerabilities in key technologies such as authentication, encryption, and transmission [26]. The weaknesses of WLANs themselves provide the possibility of denial of service (DoS) attacks and jamming attacks [27].
2. Operating system risks. Some servers and hosts in the CBTC system use commercial systems such as Windows and VxWorks. These commercial systems have many vulnerabilities. Through vulnerabilities exploitation, the attacker can gain system privileges, crash systems, and remote code execution [28].
3. Network equipment risks. The CBTC system uses a large number of network equipment as nodes for information exchange, such as switches, or gateways. If these key information exchange nodes are attacked, network communication will be affected.

Attackers utilizing these security risks may cause equipment failure, communication disruption, and service stops. Thanks to the redundant design and fail-safe principle of the CBTC system, the safety of urban rail transit can be guaranteed. However, under attack, the sensitive fail-safe mechanism will reduce train efficiency and disrupt traffic. When the equipment fails or communication is disrupted, the safety mechanism will start the train emergency braking, which may introduce huge economic losses. Therefore, security analysis for CBTC systems is a significant event.

2.3. Attack–Defense Strategy of CBTC Systems

To realistically simulate the interaction process between the attacker and the defender, we selected several attack methods for the CBTC system and developed corresponding defensive measures.

According to the vulnerability of WLAN, attackers can crack the password of WLAN to invade wireless networks. Due to the wireless network and the wired network in the signal network being connected, the attacker successfully invaded the CBTC intranet, laying the foundation for their next physical damage. The weakness of WLAN technology lies in its encryption method: Wi-Fi protected access (WPA). WPA handshake packets that are transmitted in cleartext include many parameters such as the MAC address of the client, BSSID (basic service set identifier) of AP, MIC (message integrity code), and so on. The MIC of the client which is equal to the MIC of AP is obtained by the WLAN password and these parameters through a specific algorithm. Therefore, we can use the password dictionary to calculate the MIC in combination with the parameters in the packet and compare it with the MIC of the AP (access point). If the two are the same, the password is the password of the wireless network, which indicates we have invaded the signaling networks. The prerequisite for successful password cracking is that the system uses a weak password. A complex password requires an extensive dictionary and a lot of time to crack. Therefore, the defense strategy against this attack is to dynamically change strong passwords.

The VxWorks operating system is widely used in signaling equipment, and wind debug (WDB) vulnerability is a system-specific vulnerability which can be utilized by an attacker to read or modify arbitrary memory locations, perform function calls, or manage tasks. Devices using the VxWorks operating system will reboot if we exploit the vulnerability to initiate the reboot program. In this paper, We made this sort of attack against vehicle on-board controller (VOBC) to interrupt the communication between AP and VOBC. To deal with this attack, we can install a specific patch.

ARP spoofing is an attack technology for an ethernet address resolution protocol (ARP). This type of attack allows an attacker to obtain packets on the LAN or even tamper with the packet and can prevent a particular computer or all computers on the network from connecting properly. In this paper, we adopted an ARP spoofing attack to interrupt the communication between ZC and CI. First, send an ARP reply packet, which contains the real IP and the fake MAC address of ZC, to the CC (communication controller) of the CI. After receiving the reply packet, the CC stores the wrong MAC address in the ARP cache table, which interrupts the communication between ZC and CI. ARP spoofing can be effectively addressed through IP-MAC binding.

A SYN flood attack is a denial of service (DoS) attack based on TCP protocol flaws. When TCP initiates a connection, it needs to go through three handshakes. If a client sends a large number of SYN requests to the server and it does not return an ACK packet in the meantime, then, there will be a large number of SYN queues on the server-side, which will cause a large number of server resources to be occupied, so that other normal users cannot access the server normally. In this paper, we used the SYN flood to exhaust the server resources of the CC in the ZC to achieve the purpose of interrupting ZC communication. We used a firewall to defend the attack. A cookie is assigned to each IP address of the request connection. If a duplicate SYN packet of the same IP is received within a short period of time, the packet from the IP address will be discarded.

The above is the attack and defense method for the CBTC system in this paper. Therefore, the strategy sets of attacker and defender in the penetration phase and disruption phase are determined:

$$\begin{aligned} \Pi_P^a &= (\Phi_P^{a1}, \Phi_P^{a2}), \\ \Pi_P^d &= (\Phi_P^{d1}, \Phi_P^{d2}), \\ \Pi_D^a &= (\Phi_D^{a1}, \Phi_D^{a2}, \Phi_D^{a3}, \Phi_D^{a4}), \\ \Pi_D^d &= (\Phi_D^{d1}, \Phi_D^{d2}, \Phi_D^{d3}, \Phi_D^{d4}). \end{aligned}$$

And the meaning of these values are shown in Tables 1 and 2.

Table 1. Attack–defense behaviors in the penetration phase.

Attack Behaviors	Meaning	Defense Behaviors	Meaning
Φ_P^{a1}	Wireless intrusion attack	Φ_P^{d1}	Dynamically update strong passwords
Φ_P^{a2}	No attack	Φ_P^{d2}	No defense

Table 2. Attack–defense behaviors in the penetration phase.

Attack Behaviors	Meaning	Defense Behaviors	Meaning
Φ_D^{a1}	WDB vulnerability attack	Φ_D^{d1}	Patch Installation
Φ_D^{a2}	ARP spoofing attack	Φ_D^{d2}	IP-MAC binding
Φ_D^{a3}	SYN flood attack	Φ_D^{d3}	Firewall
Φ_D^{a4}	No attack	Φ_D^{d4}	No defense

3. Security Model of CBTC System under Attacks–Defense Confrontation

In this section, we propose an analytical model of system security under attacks and counter defense schemes. The overall framework of the model is shown in Figure 2. We used the steady-state probability of the system obtained by the GSPN model to analyze and evaluate several indicators of

system security, and the game model and simulation platform to assign values to parameters of the GSPN model.

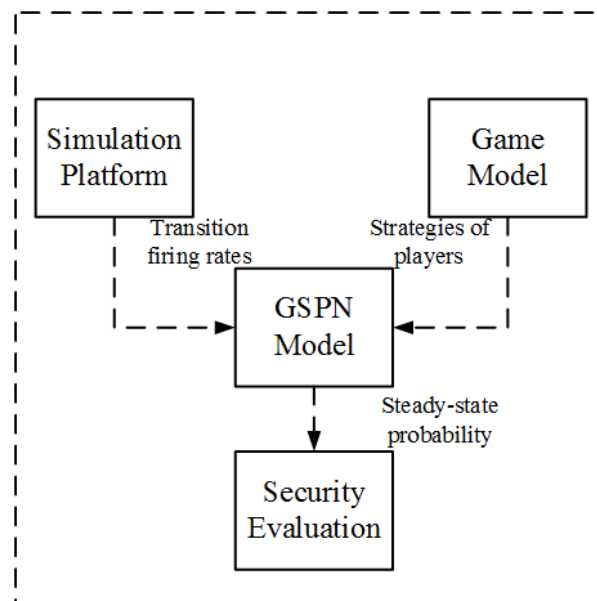


Figure 2. Overall framework of the model.

3.1. Generalized Stochastic Petri Net Model

Petri nets are suitable for describing asynchronous, concurrent system models [29]. SPN is used to depict specific business processes in [30,31]. The proposed model analyzes system availability by describing changes in system state under attack–defense confrontation. Our model is represented as a 6-tuple:

$$GSPN = (P, T, F, \lambda, \pi, M_0), \text{ where}$$

1. P is a finite set of places which represent the condition, resource or state;
2. T is a finite set of transitions which indicate the occurrence of an event or action. T is divided into two subsets: $T = T_t \cup T_i$, $T_t \cap T_i = \emptyset$, timed transitions T_t consider the time factor of the process of transitions and immediate transitions T_i takes zero time to fire and represent transient processes;
3. $F \subseteq I \cup O$ is a set of arcs, where $I \subseteq P \times T$ and $O \subseteq T \times P$ such that $P \cap T = \emptyset$, $P \cup T \neq \emptyset$. Arcs have directionality, connecting libraries and transitions;
4. λ is a set of transition firing rates associated with the transitions;
5. π is a routing policy representing the probability of choosing a particular transition;
6. M_0 is the initial marking.

We divided the model into two phases: penetration and disruption, according to the attack process of the attacker. The penetration phase is the process of an attacker invading from the extranet to the intranet. Only by accessing to internal control network of the CBTC systems such as ATS networks and ATC networks can attackers damage the systems. It is well known that industrial control systems such as CBTC systems are relatively close compared to the Internet. In fact, with the continuous integration of industrialization and informatization, industrial control systems are increasingly using standardized communication protocols and hardware and software, and remote control and operation through the Internet, breaking the closure and specialization of the original system [32]. Therefore, it is possible for an attacker to invade an industrial control network. Even if the industrial control network is entirely physically isolated from the external network, we still have a way to get it down. The US Stuxnet virus is an example.

In this paper, the wireless transmission network between train and ground became our approach to invade the CBTC system. We utilized vulnerabilities of WLAN to access CBTC control networks,

namely, signaling networks. Further, there are the following intrusion methods: virus transmitted by USB flash disk, phishing, and wired network connection. To simplify the model for research, this paper adopts the method of wireless intrusion. In contrast, we also have several ways to combat this attack. In terms of hardware, NFC (near field communication) is used in some cellphones to magnetically link data in a range of just an inch or so, and could be integrated into the train power systems, as could similarly secure optical “synapses” at train car junctions. Additionally, a newly developed ELF (extremely low frequency) antenna might be able to evade most hacking attempts while allowing a train-length wireless communication data link. In terms of software, the method that is used in this paper is to improve the password strength of the wireless network.

The penetration phase model is shown in Figure 3, and the parameters description is shown in Table 3. At first, the system is in a normal state P_N which represents that the CBTC system is running normally. Then, the attacker will decide their strategy and choose their behavior. Correspondingly, the defender will decide their strategy and choose their behavior. This is a confrontation process between attacker and defender. If the attacker launches a wireless intrusion attack and the defender has no resistance, the system will enter the intrusion state P_I, which indicates that the attacker has successfully entered the intranet of the CBTC system. Conversely, if the defender takes defensive measures, the attacker will fail. In this case, the system will not be affected by the attack, and the attacker needs to bear the loss of the attack failed. Obviously, when the attacker chooses behavior (Φ_D^4), regardless of the strategy adopted by the defender, the system remains in a normal state.

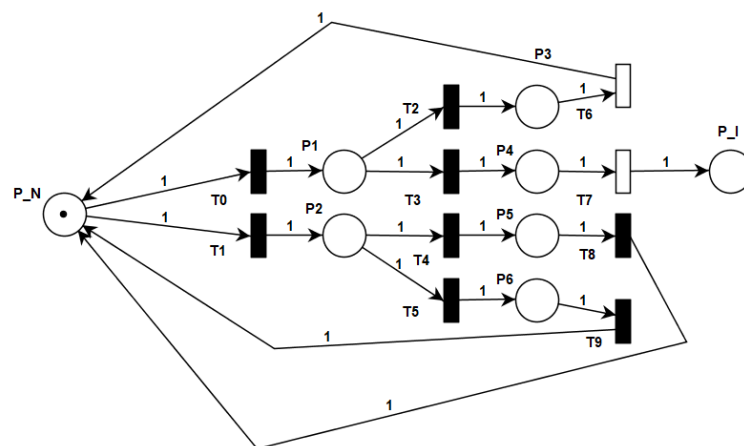


Figure 3. Attack–defense confrontation model in the penetration phase.

Table 3. Model parameters in the penetration phase.

Parameters	Type	Physical Meaning
P_N	Place	The system is in a normal state
P1/P2/P3/P4/P5/P6	Place	Intermediate state of attack–defense confrontation
P_I	Place	Attacker successfully invade the system
T0	Immediate Transition	The attacker chooses to initiate a wireless intrusion attack
T1	Immediate Transition	The attacker does not launch an attack
T2/T4	Immediate Transition	The defender adopt strong password in wireless network
T3/T5	Immediate Transition	Defenders do not take defensive measures
T8/T9	Immediate Transition	The system remains normal without attack
T6	Timed Transition	The process of successful attack
T7	Timed Transition	The process of failed attack

The disruption phase is based on the system having been invaded. There is no point in considering the disruption phase if the system state cannot transition to the intrusion state. In the penetration phase, the attacker has not yet performed the damaging attack against the system, and therefore the attacker needs to perform specific damaging attacks on the system. Thanks to the contribution of the penetration phase, the attacker can initiate damage on the intranet of the CBTC system. Various vulnerabilities of the system are exposed to the attacker, especially one who has an understanding of the internal architecture of the system in the disruption phase.

Our disruption phase model is shown in the right part of Figure 4, and the parameters description is shown in Table 4. Just like the penetration phase, the attacker chooses the attack behavior and the defender takes countermeasures, and then the state of the system changes. The disruption phase starts from the place P_I, which indicates the attacker has entered the internal network of the system. In this case, the attacker and the defender choose behaviors for the attack–defense game with a certain probability. The next attack–defense confrontation process is as follows:

1. If the attacker adopts behavior (Φ_D^{a1}) and the defender does not take the right defensive behavior, emergency braking will occur on the train because of the communication between VOBC and AP is interrupted. The train can be restarted and operate in BLOC (block-based train control) mode after stopping.
2. If the attacker adopts behavior (Φ_D^{a2}) and the defender does not take the right defensive behavior, the attacker interrupts the communication between ZC and CI, which causes the system to enter the emergency braking state. Furthermore, the train cannot operate in BLOC mode because the CI cannot handle the route automatically.
3. If the attacker adopts behavior (Φ_D^{a3}) and the defender does not take the right defensive behavior, the CBTC system will enter the emergency braking state again because of ZC is crashed by the attacker. In this case, the train can be restarted and operate in BLOC (block-based train control) mode after stopping.
4. If the defensive measure of the defender works, the system state will return to normal state. In this paper, one defensive measure only works for one type of attack. The corresponding offensive and defensive behavior is as follows: (Φ_D^{a1}, Φ_D^{d1}), (Φ_D^{a2}, Φ_D^{d2}), (Φ_D^{a3}, Φ_D^{d3}).
5. After a system failure, it will eventually return to normal after a period, which is described by timed transit T_R.

Table 4. Model parameters in the disruption phase.

Parameters	Type	Physical Meaning
P_N	Place	The system is in a normal state
P11-23/P7-10	Place	Intermediate state of attack–defense confrontation
P_I	Place	Attacker successfully invade the system
P_B1/ P_B2/ P_B3	Place	Train emergency braking state
P_D	Place	Train degraded operation state
T10	Immediate Transition	The attacker initiate a WDB vulnerability attack
T11	Immediate Transition	The attacker initiate an ARP spoofing attack
T12	Immediate Transition	The attacker initiate a flood attack
T13	Immediate Transition	The attacker does not launch an attack
T14/T18/T22/T26	Immediate Transition	Patch Installation by defender
T15/T19/T23/T27	Immediate Transition	IP-MAC binding by defender
T16/T20/T24/T28	Immediate Transition	Firewall by defender
T17/T21/T25/T29	Immediate Transition	Defenders do not take defensive measures
T42	Immediate Transition	The system remains normal without attack
T31-34/ T36-39/T41	Timed Transition	The process of successful attack
T30/T35/T40	Timed Transition	The process of failed attack
T33/T34	Timed Transition	The process of the train degraded operation
T_R	Timed Transition	The process of the system returns to normal

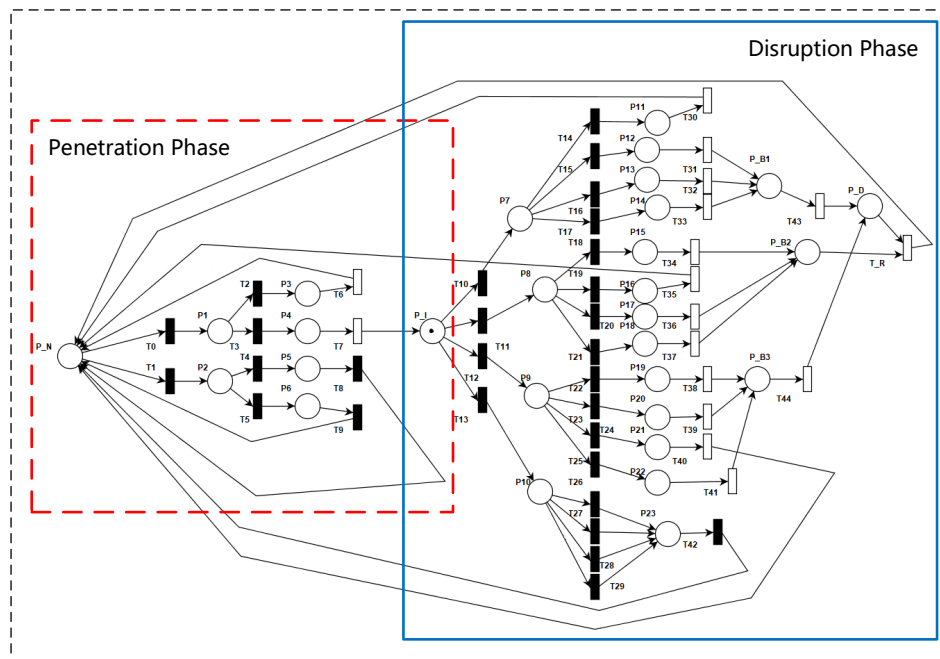


Figure 4. Attack–defense confrontation model.

Since the GSPN model is isomorphic with the continuous time Markov chain (CTMC), we found a way to solve the model. By transforming the model into CTMC, we can analyze the steady-state probability of the model. In Petri nets, the states which associate with the immediate transition should be eliminated. The time the token stays in these states approaches zero; therefore, these states have no steady-state probability. According to the correlation theorem of Markov chain stationary distribution and the Chapman–Kolmogorov equation, we get:

$$WQ = 0, W = [P(M_0), P(M_1), \dots, P(M_k)] \tag{1}$$

$$\sum_i^k P(M_i) = 1, \tag{2}$$

where W is the steady-state probability vector of Markov chain marker M_i which represents the steady state of CBTC systems. Q is a transfer rate matrix with element q_{ij} ($i, j = 0, 1, \dots, k$). If $i \neq j$, q_{ij} is equal to the rate from M_i to M_j and when $i = j$, q_{ij} is equal to the inverse of the sum of the rate of arcs from M_i . In addition, the rate from M_i to M_j is obtained by multiplying the transition firing rate λ by the probability of choosing an immediate transition π . After quantifying the parameters such as λ and π , we can obtain the steady-state probability.

3.2. Attack–Defense Game Model

In this paper, we propose the game model to assist the GSPN model in completing the parameterization process. Through the attack–defense game model, we can predict the behavior of attackers and defenders and obtain the strategies of both players. In this paper, we believe that the attacker is not a reckless person who blindly pursues the proceeds but a wise man who fully considers the gains and losses, and the defender is rational similarly. For the attack–defense confrontation model, both rational players in the process of an attack–defense game aim to maximize their income, which is their criterion for choosing attack–defense behavior. Since the profit of the attacker and the defender is based on the loss of the opponent, there is no win–win between the two players, that is, there is no

pure-strategy Nash equilibrium. To predict how rational players would choose their behaviors and play the game, we need to solve the mixed strategy Nash equilibrium.

$U^a (\Phi^{a_i}, \Phi^{d_j})$ represents the payoff function of the attacker under the attacker behavior Φ^{a_i} and the defender behavior Φ^{d_j} . $U^d (\Phi^{a_i}, \Phi^{d_j})$ represents the payoff function of defender under the attacker behavior Φ^{a_i} and the defender behavior Φ^{d_j} . We can obtain the specific payoff of the attacker and defender through the following equations:

$$U^a (\Phi^{a_i}, \Phi^{d_j}) = R_a - C_a, \tag{3}$$

$$U^d (\Phi^{a_i}, \Phi^{d_j}) = R_d - C_d. \tag{4}$$

where C_a and R_a represent the cost and return of attack behavior, and C_d and R_d represent the cost and return of defense behavior.

Let Π^{a^*} and Π^{d^*} denote the attacker and the system defender optimal mixed strategies. $E^a (\Pi^a, \Pi^d)$ and $E^d (\Pi^a, \Pi^d)$ are income expectation of the attacker and defender when the attacker adopts strategy Π^a , and the defender adopts strategy Π^d . We can obtain the E^a and E^d through the following equations:

$$E^a (\Pi^a, \Pi^d) = \sum_{\Phi^{a_i} \in \Pi^a} \sum_{\Phi^{d_j} \in \Pi^d} \Pi^a \Pi^d U^a (\Phi^{a_i}, \Phi^{d_j}), \tag{5}$$

$$E^d (\Pi^a, \Pi^d) = \sum_{\Phi^{a_i} \in \Pi^a} \sum_{\Phi^{d_j} \in \Pi^d} \Pi^a \Pi^d U^d (\Phi^{a_i}, \Phi^{d_j}), \tag{6}$$

Therefore, the Nash equilibrium of the attack–defense game should satisfy the following two conditions:

- (1) $E^a (\Pi^{a^*}, \Pi^{d^*}) \geq E^a (\Pi^a, \Pi^{d^*}), E^d (\Pi^{a^*}, \Pi^{d^*}) \geq E^d (\Pi^a, \Pi^{d^*}),$
- (2) $E^a (\Pi^{a^*}, \Pi^{d^*}) \geq E^a (\Pi^{a^*}, \Pi^d), E^d (\Pi^{a^*}, \Pi^{d^*}) \geq E^d (\Pi^{a^*}, \Pi^d).$

4. Model Solution

4.1. Obtaining Model Parameters from a CBTC Simulation Platform

To solve the GSPN model to obtain the steady-state probability of the system, some values of the model parameters need to be determined. In this subsection, we rely on the semiphysical simulation platform to obtain transition firing rate λ of each timed transition. The composition of the platform is shown in Figure 5. The platform which represents a real CBTC system combines simulation software and actual signal equipment to truly restore the operation of Beijing Line 7. The platform consists of VOBC, WGB, AP, ZC, and simulation software such as ATS, CI, and DSU simulation software and actual signal equipment to truly restore the operation of Beijing Line 7. The platform consists of VOBC, WGB, AP, ZC, and simulation software such as ATS, CI, and DSU.

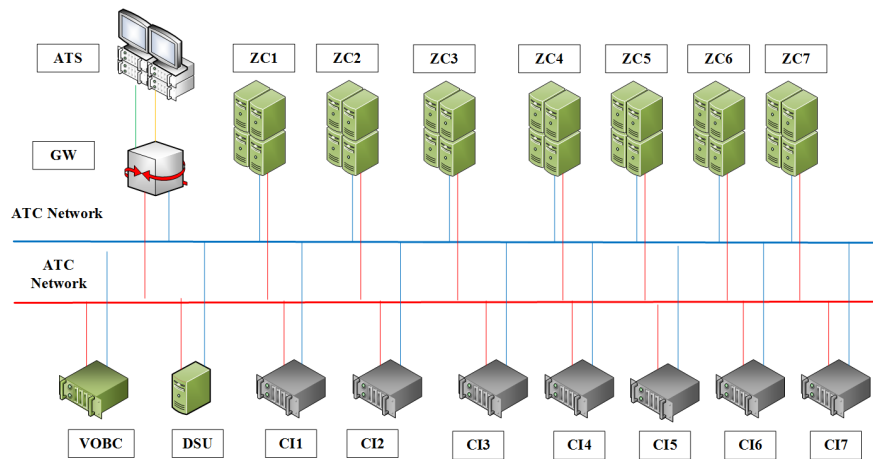


Figure 5. CBTC simulation platform.

We drilled the attack and defense methods proposed in this paper on the simulation platform and record the time spent to complete the transitions. After a lot of experiments, we obtained the mean time spent to complete the transitions. According to the mean transition time equal to $1/\lambda$, we can get the transition firing rates, which are shown in Table 5.

Table 5. Transition firing rate of timed transition.

Transition Firing Rate	Value
λ_6/λ_7	0.0017
$\lambda_{34}/\lambda_{35}/\lambda_{36}/\lambda_{37}$	0.012
$\lambda_{38}/\lambda_{39}/\lambda_{40}/\lambda_{41}$	0.0055
$\lambda_{30}/\lambda_{31}/\lambda_{32}/\lambda_{33}$	0.016
$\lambda_{42}/\lambda_{43}$	0.018
λ_R	0.001

4.2. Nash Equilibrium Solution

In this subsection, we got the attacker and defender’s strategies, which are the probabilities (π) that both two players choose their respective behaviors by solving the Nash equilibrium. We solved the Nash equilibrium for the penetration phase and the disruption phase, respectively, in this paper. The key to solving the Nash equilibrium is to obtain the game matrix. Therefore we first needed to quantify the payoffs of attack–defense behavior based on Equations (3) and (4). In this paper, the attacker’s benefit is the damage caused to the system, and the cost of the attack is deducted when the attack is successful. Further, the defender’s loss is system loss plus defensive cost. When the defense is successful, the defender’s gain is the attacker’s loss minus the defense cost, and the attacker’s loss is the attack cost.

In this paper, we quantified the cost and return of attack–defense behaviors in combination with the CVSS (common vulnerability scoring system) and the characteristics of CBTC systems. Attack cost considers attack path, attack complexity, and whether authentication is required. Defense cost takes into account defense complexity and defense against negative effects. The system loss in the disruption phase is determined by the loss of the running distance in the case of emergency braking and the loss of the running distance in the case of degraded operation, and the system loss can be obtained using the following equation:

$$P_{loss}(t) = \int_{t_0}^t (v_p - v_a) dt, \tag{7}$$

where t_0 indicates the time when the train running performance begins to decrease, v_p indicates the ideal running speed of the train, and v_a indicates the actual speed of the train after the attack.

We considered the long-term impact of invading the system to determine the system loss during the penetration phase. Therefore, the two phases of the attack–defense game matrix are shown in Tables 6 and 7.

Table 6. Game matrix in penetration phase.

Attack Behavior	Defense Behavior	
	Φ_P^{d1}	Φ_P^{d2}
Φ_P^{a1}	(−2, 4.5)	(3.5, −5.5)
Φ_P^{a2}	(0, −1)	(0, 0)

Table 7. Game matrix in disruption phase.

Attack Behavior	Defense Behavior			
	Φ_D^{d1}	Φ_D^{d2}	Φ_D^{d3}	Φ_D^{d4}
Φ_D^{a1}	(−1, 4.5)	(4.5, −7.5)	(4.5, −8.5)	(4.5, −5.5)
Φ_D^{a2}	(6.8, 9.5)	(−1.7, 6.5)	(6.8, −11.5)	(6.5, −8.5)
Φ_D^{a3}	(4, −8)	(4, −7.5)	(−1.5, 3)	(4, −5.5)
Φ_D^{a4}	(0, −1)	(0, −2)	(0, −1.5)	(0, 0)

We can obtain the optimal mixed strategy by solving the Nash equilibrium based on the max–min algorithm [15]:

$$\begin{aligned} \Pi_P^a &= (0.0909, 0.9091), \\ \Pi_P^d &= (0.6364, 0.3636), \\ \Pi_D^a &= (0.3312, 0.2348, 0.4341, 0), \\ \Pi_D^d &= (0.3099, 0.4711, 0.2190, 0). \end{aligned}$$

Therefore, we can obtain the probabilities of choosing immediate transition π .

4.3. Attack–Defense Confrontation Model Solution

Through the above subsections, we parameterized the attack–defense model. Next, we solve the GSPN model to get the steady-state probability of the system in each state, which lays the foundation for security analysis. At first, we transformed the Petri net model into a continuous time Markov chain, which is shown in Figure 6.

As shown in the figure, there are four states in CBTC systems: normal state, intrusion state, train emergency braking state, and train degraded operation state. By solving the above Equations (1) and (2), we obtained the steady-state probability of the analytical model. The final steady-state probability results are shown in Table 8.

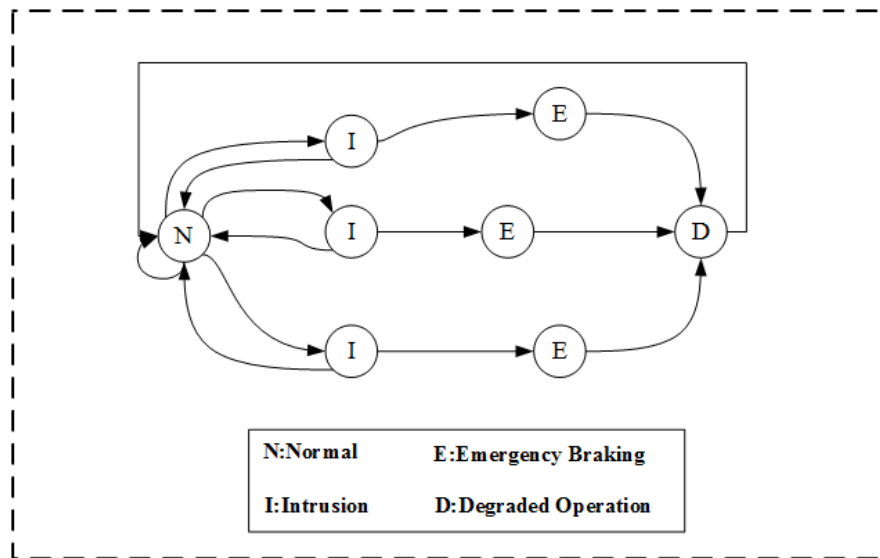


Figure 6. Continuous time Markov chain (CTMC) model.

Table 8. Steady-state probability of communication-based train controls (CBTC) systems.

State	Steady-State Probability
Normal state	66.323%
Intrusion state	5.747%
Train emergency braking state	5.014%
Train degraded operation state	22.916%

5. Analysis and Evaluation

In this section, we analyze and evaluate the security of the CBTC system based on the solution results of the GSPN model. Several indicators are proposed to complete the assessment of system security.

One indicator is the availability of the system. Availability denotes the probability or proportion of time a system is in a functioning condition. The equation for the calculation is as follows:

$$Availability = \sum_{s \in A} P_s \tag{8}$$

where s represents the state of the system, and A is the state sets where the system is operating properly. In this paper, the system can perform business normally in the normal state and intrusion state. Therefore, we obtained the availability with value 72.1% under attack–defense confrontation, which indicates that although there are defensive measures, the security of the CBTC system is still greatly threatened. Therefore, improving the security of CBTC systems is an urgent task for system operators.

To explore the impact of defense on system security, we adjusted the probability that the system does not use defensive measures in the GSPN model. As shown in Figure 7, the solid line is the change of system availability with the probability of the nondefense behavior in the disruption phase. We kept increasing the weight of $\Phi_D^{d_4}$ while keeping the original ratio of $\Phi_D^{d_1}$, $\Phi_D^{d_2}$, and $\Phi_D^{d_3}$ unchanged. We can see that as the probability of nondefense increases, the availability of the system continues to decrease. When the system is completely undefended in the disruption phase, the availability reaches 63%. The dotted line represents the same situation in penetration. In this case, strategies of the attacker and defender in the disruption phase are still the optimal strategies Π_D^a and Π_D^d obtained above. Comparing the two results, we can find that the defensive measures are more effective in the

penetration phase, which means that it is more significant to adopt the defensive measures in the penetration phase.

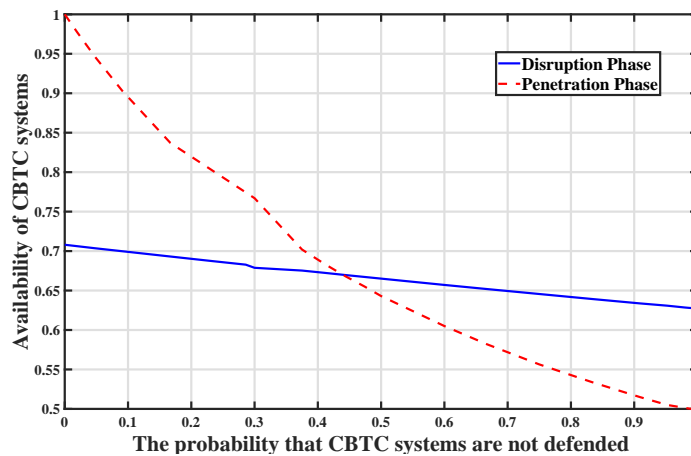


Figure 7. The defense scheme impact on CBTC availability.

In the same way, we kept the other parameters unchanged and only adjusted the probability of the attacker launching the attack. In the disruption phase, the probabilities of Φ_D^{a1} , Φ_D^{a2} and Φ_D^{a3} are adjusted according to the original ratio. Results are shown in Figure 8. The lowest point of the two lines is 71%, which indicates that, with specific defensive measures, even if an attacker frequently launches attacks, the availability of the system can remain above 70%. This result fully demonstrates the importance of defensive measures for system security.

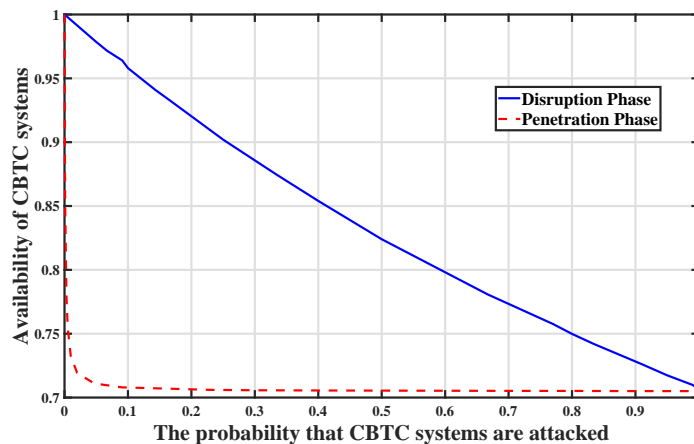


Figure 8. CBTC availability with attack action probability.

Another security indicator is the mean time to security failure (MTTSF), which draws on the experience of the MTTF in the reliability field. MTTSF is defined as the measure for quantifying the security of systems [33]. MTTSF is the duration time for which the model stays in an intermediate state before it finally enters the absorbing state. Different from the steady-state probability of the system, to calculate MTTSF, we assume that the failure state is the absorption state, that is, it does not recover after the train failure. The MTTSF can be obtained by the following equation:

$$MTTSF = \sum_{a \in S} V_a S_a, \tag{9}$$

where V_a is the visit rate of state a and S_a is the mean sojourn time in the state a . The average visit rate is defined as the average number of times that a state is visited before the model reaches absorbing states. Further, the visit rate can be calculated by this equation:

$$V_a = q_a + \sum_b V_b q_{ba}, a, b \in S, \tag{10}$$

where q_{ba} is the probability of the transition from state b to state a , and q_a is the probability that the model starts in the state a . The probability of transition can be calculated by the probability of choosing immediate transition π . In addition, we assume the $q_N = 1$ in the normal state, and $q_a = 0$ in other state.

According to the solution result of the Petri nets and Equations (9) and (10), the MTTSF under attack–defense confrontation is 2546.2 s. Honestly, this is not a desired result, and the security of CBTC systems needs to be improved.

Like the analysis of system availability above, we get the Figures 9 and 10. Simulation results show that, compared to the penetration phase, the security of CBTC systems is not sensitive to defensive measures in a disruption phase. Therefore, defense protection work during the invasion phase is more significant. Further, the existence of defensive measures determines the lower limit of MTTSF, that is, the MTTSF of the system can remain 2546 s in the worst situation.

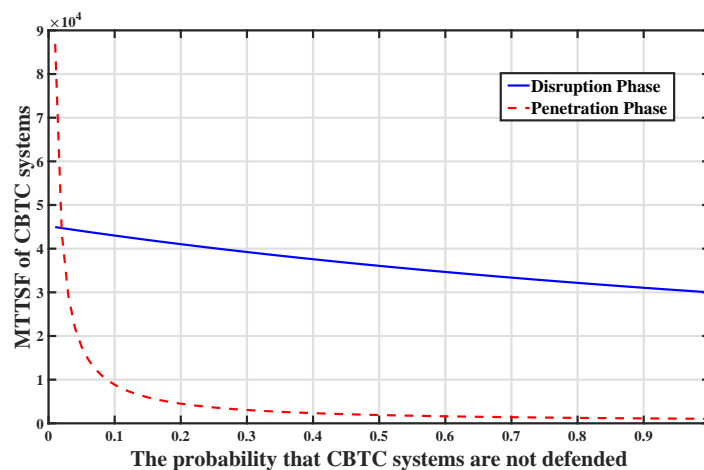


Figure 9. The defense scheme impact on CBTC mean time to security failure (MTTSF).

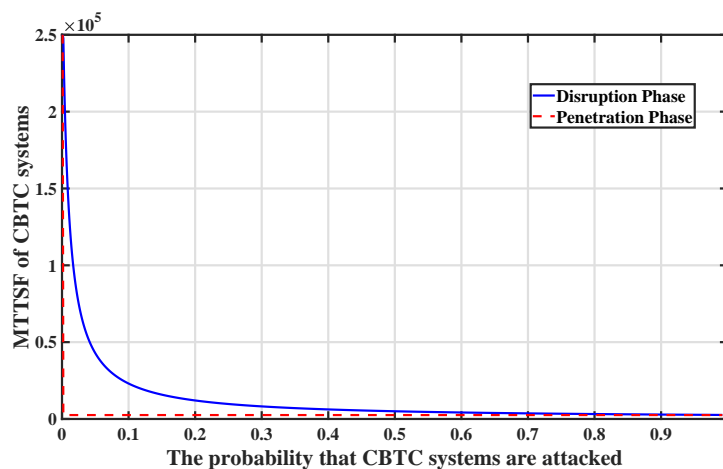


Figure 10. CBTC MTTSF with attack action probability.

Therefore, the system operator should spend a lot of effort to resist the attacker’s invasion from the extranet to the intranet. We recommend using a more efficient and secure LTE-M instead of WLANs.

The defense of the destruction phase is equally important because internal attackers and certain special jamming attacks can directly skip the penetration phase to damage the system.

Based on the above analysis and evaluation results, we found that under the attack of the attacker, the availability of the system is only 71%, and the MTTSF is only 2546 s. For an urban rail transit system that is related to people’s livelihood, such security is too low. We speculate that the cause of this result is insufficient defense input. In this article, defenders used only one defensive measure at a time. Next, the defender uses the combined measures to complete the attack–defense confrontation process, compared with the security under the previous single measure. Since the offensive and defensive methods are single during the penetration phase, we made a combination of the defense methods of the disruption phase. Therefore, the new attack–defense strategy sets are as follows:

$$\begin{aligned} \Pi_P^a &= (\Phi_P^{a1}, \Phi_P^{a2}), \\ \Pi_P^d &= (\Phi_P^{d1}, \Phi_P^{d2}), \\ \Pi_D^a &= (\Phi_D^{a1}, \Phi_D^{a2}, \Phi_D^{a3}, \Phi_D^{a4}), \\ \Pi_D^d &= ((\Phi_D^{d1}, \Phi_D^{d2}), (\Phi_D^{d1}, \Phi_D^{d3}), (\Phi_D^{d2}, \Phi_D^{d3}), \Phi_D^{d4}). \end{aligned}$$

The new attack–defense confrontation model is shown in Figure 11. In this model, the definition of the places and the transitions has not changed. The only change is the path between the places and the transitions. For comparison, we used the probability of the previous model:

$$\begin{aligned} \Pi_P^a &= (0.0909, 0.9091), \\ \Pi_P^d &= (0.6364, 0.3636), \\ \Pi_D^a &= (0.3312, 0.2348, 0.4341, 0), \\ \Pi_D^d &= (0.3099, 0.4711, 0.2190, 0). \end{aligned}$$

According to Equations (1) and (2), we obtained the steady-state probability of the new model in Table 9.

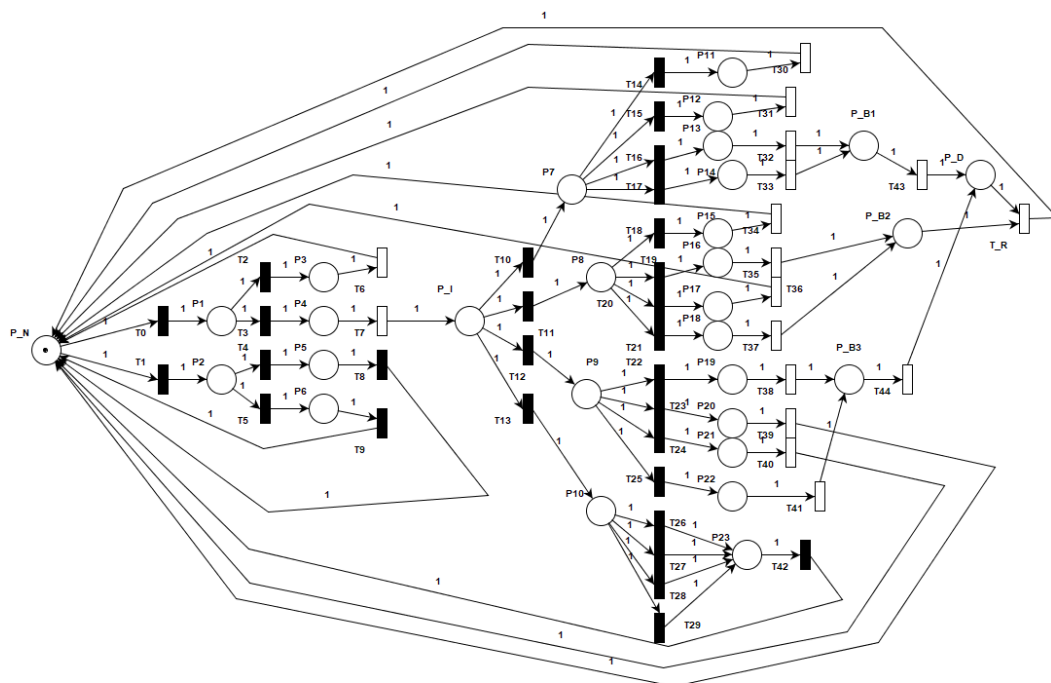


Figure 11. Attack–defense confrontation model with combined defensive measures.

Table 9. Steady-state probability of CBTC systems.

State	Steady-State Probability
Normal state	78.612%
Intrusion state	4.988%
Train emergency braking state	5.777%
Train degraded operation state	10.623%

Then, we can calculate the security indicators of the CBTC system:

Availability: 83.5%, MTTSF: 14523.6 s.

This result reveals that the combined defense measures can indeed improve the security of the system. Therefore, for security reasons, urban rail transit operators should invest heavily in system defense. For example, disabling unused equipment ports, installing vulnerability patches, and deploying firewalls at the network perimeter are significant to improve system security.

6. Conclusions

In this paper, we proposed a generalized stochastic Petri net model to catch the process of attack–defense confrontation in a CBTC system. We divided this process into two phases of penetration phase and disruption phase according to the characteristics of the system and attack–defense methods. The entire security analysis model consisted of the GSPN model, game theory and the semiphysical simulation platform. Using the steady-state probability of the system output from the model, we proposed several indicators such as availability and MTTSF for assessing system security. Comparing the security of the system with single defense measures and combined defense measures, we had drawn an urgent need to increase defense investment.

For future work, we plan to introduce multiple indicators to evaluate the security of the CBTC system and deeply analyze the impact of an attack–defense confrontation process on the system. We hope to enrich the attack–defense methods against the CBTC system. We also intend to further study game theory [34,35] to reflect the attack–defense behavior more clearly and combine game theory with cybernetics [36,37] to improve system security.

Author Contributions: W.W. proposed the attack–defense confrontation model, designed the experiments, and was responsible for writing the paper. B.B. made substantial contributions to the game theory model and data analysis. In addition, all authors have jointly written and revised the manuscript.

Funding: This paper was supported by the Innovation Fund of Beijing TCT grant (No.9907006607), the project (No.I18JB00110) and the Beijing Laboratory for Urban Mass Transit. And also supported by National Natural Science Foundation of China (61973026, and Project (2018JBZ002,L171004)).

Acknowledgments: The authors wish to thank the State Key Laboratory of Rail Traffic Control and Safety and the Beijing Laboratory for Urban Mass Transit, for their continuous support of the presented research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gao, S.; Hou, Y.; Dong, H.; Stichel, S.; Ning, B. High-speed trains automatic operation with protection constraints: a resilient nonlinear gain-based feedback control approach. *IEEE/CAA J. Autom. Sin.* **2019**, *6*, 992–999. [[CrossRef](#)]
2. Wang, X.; Liu, L.; Tang, T.; Sun, W. Enhancing Communication-Based Train Control Systems Through Train-to-Train Communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1544–1561. [[CrossRef](#)]
3. Schifers, C.; Hans, G. IEEE standard for communications-based train control (CBTC) performance and functional requirements. In Proceedings of the Vehicular Technology Conference Proceedings, VTC, Tokyo, Japan, 15–18 May 2000; pp. 1581–1585.
4. Wang, X.; Fei, R.Y.; Li, Z.; Tao, T.; Ning, B. A Cognitive Control Approach to Communication-Based Train Control Systems. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 1676–1689. [[CrossRef](#)]

5. Farooq, J.; Soler, J. Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1377–1402. [[CrossRef](#)]
6. Knowles, W.; Prince, D.; Hutchison, D.; Disso, J.F.P.; Jones, K. A survey of cyber security management in industrial control systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *9*, 52–80. [[CrossRef](#)]
7. Wang, H.; Ni, M.; Gao, S.; Bao, F.; Tang, H. A Resilience-Based Security Assessment Approach for Railway Signalling Systems. In Proceedings of the 2018 37th Chinese Control Conference (CCC), Wuhan, China, 25–27 July 2018; pp. 7724–7729. [[CrossRef](#)]
8. Yi, S.; Wang, H.; Ma, Y.; Xie, F.; Zhang, P.; Di, L. A Safety-Security Assessment Approach for Communication-Based Train Control (CBTC) Systems Based on the Extended Fault Tree. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–5. [[CrossRef](#)]
9. Dong, H.; Wang, H.; Tang, T. An attack tree-based approach for vulnerability assessment of communication-based train control systems. In Proceedings of the 2017 Chinese Automation Congress (CAC), Jinan, China, 20–22 October 2017; pp. 6407–6412. [[CrossRef](#)]
10. Ferrari, A.; Itria, M.L.; Chiaradonna, S.; Spagnolo, G.O. Model-Based Evaluation of the Availability of a CBTC System. In *Software Engineering for Resilient Systems*; Avgeriou, P., Ed.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 165–179.
11. Lee, J.; Jang, C.; Yi, O. Analysis of radio based train control system using LTE-R and analysis of security requirements: The security of the radio based train control system. In Proceedings of the 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta, Bali, 8–10 August 2017; pp. 1–4. [[CrossRef](#)]
12. Wang, E.K.; Ye, Y.; Xu, X.; Yiu, S.M.; Hui, L.C.K.; Chow, K.P. Security Issues and Challenges for Cyber Physical System. In Proceedings of the IEEE/ACM Intl Conference on Green Computing & Communications & International Conference on Cyber, Beijing, China, 20–25 September 2010.
13. Subramanian, N.; Zalewski, J. Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using the NFR Approach. *IEEE Syst. J.* **2016**, *10*, 397–409. [[CrossRef](#)]
14. Mitchell, R.; Chen, I. Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber Physical Systems. *IEEE Trans. Reliab.* **2016**, *65*, 350–358. [[CrossRef](#)]
15. Lalropuia, K.; Gupta, V. Modeling cyber-physical attacks based on stochastic game and Markov processes. *Reliab. Eng. Syst. Saf.* **2019**, *181*, 28–37. [[CrossRef](#)]
16. Orojloo, H.; Azgomi, M.A. A Stochastic Game Model for Evaluating the Impacts of Security Attacks Against Cyber-Physical Systems. *J. Netw. Syst. Manag.* **2018**, *26*, 929–965. [[CrossRef](#)]
17. Depoy, J.; Phelan, J.; Sholander, P.; Smith, B.; Varnado, G.B.; Wyss, G. Risk assessment for physical and cyber attacks on critical infrastructures. In Proceedings of the Military Communications Conference, Atlantic City, NJ, USA, 17–20 October 2005.
18. Kriaa, S.; Bouissou, M.; Colin, F.; Halgand, Y.; Pietre-Cambaces, L. *Safety and Security Interactions Modeling Using the BDMP Formalism: Case Study of a Pipeline*; Springer: Cham, Switzerland, 2014.
19. Piètre-Cambacédès, L.; Bouissou, M. *Attack and Defense Dynamic Modeling with BDMP (Extended Version)*; Tech. Report 2010D021; Telecom ParisTech: Paris, France, 2010.
20. Zonouz, S.; Rogers, K.M.; Berthier, R.; Bobba, R.B.; Sanders, W.H.; Overbye, T.J. SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures. *IEEE Trans. Smart Grid* **2012**, *3*, 1790–1799. [[CrossRef](#)]
21. Shi, D.; Elliott, R.J.; Chen, T. On Finite-State Stochastic Modeling and Secure Estimation of Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2016**, *62*, 65–80. [[CrossRef](#)]
22. Wu, J.; Ota, K.; Dong, M.; Li, J.; Wang, H. Big data analysis-based security situational awareness for smart grid. *IEEE Trans. Big Data* **2016**, *4*, 408–417. [[CrossRef](#)]
23. Ni, Z.; Paul, S. A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, 1–12. [[CrossRef](#)]
24. Chen, Y.; Huang, S.; Liu, F.; Wang, Z.; Sun, X. Evaluation of reinforcement learning-based false data injection attack to automatic voltage control. *IEEE Trans. Smart Grid* **2018**, *10*, 2158–2169. [[CrossRef](#)]
25. Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Comput. Ind.* **2017**, *88*, 44–57. [[CrossRef](#)]
26. Park, J.S.; Dicoi, D. WLAN security: Current and future. *IEEE Internet Comput.* **2003**, *7*, 60–65. [[CrossRef](#)]

27. Wang, X.; Jiang, H.; Tang, T.; Zhao, H. The QoS Indicators Analysis of Integrated EUHT Wireless Communication System Based on Urban Rail Transit in High-Speed Scenario. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 2359810. [[CrossRef](#)]
28. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-Physical Systems Security*; Homeland Security: Washington, DC, USA, 2009; Volume 5.
29. Robidoux, R.; Xu, H.; Xing, L.; Zhou, M. Automated Modeling of Dynamic Reliability Block Diagrams Using Colored Petri Nets. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2010**, *40*, 337–351. [[CrossRef](#)]
30. Xia, Y.; Luo, X.; Li, J.; Zhu, Q. A Petri-Net-Based Approach to Reliability Determination of Ontology-Based Service Compositions. *IEEE Trans. Syst. Man Cybern. Syst.* **2013**, *43*, 1240–1247. [[CrossRef](#)]
31. Xia, Y.; Liu, Y.; Liu, J.; Zhu, Q. Modeling and Performance Evaluation of BPEL Processes: A Stochastic-Petri-Net-Based Approach. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2012**, *42*, 503–510. [[CrossRef](#)]
32. Taheri, M.; Ansari, N.; Feng, J.; Rojas-Cessa, R.; Zhou, M. Provisioning Internet Access Using FSO in High-Speed Rail Networks. *IEEE Netw.* **2017**, *31*, 96–101. [[CrossRef](#)]
33. Madan, B.B.; Goševa-Popstojanova, K.; Vaidyanathan, K.; Trivedi, K.S. A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Perform. Eval.* **2004**, *56*, 167–186. [[CrossRef](#)]
34. Xue, L.; Sun, C.; Wunsch, D.; Zhou, Y.; Yu, F. An adaptive strategy via reinforcement learning for the prisoners? dilemma game. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 301–310. [[CrossRef](#)]
35. Lu, J.; Xin, Y.; Zhang, Z.; Liu, X.; Li, K. Game-Theoretic Design of Optimal Two-Sided Rating Protocols for Service Exchange Dilemma in Crowdsourcing. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2801–2815. [[CrossRef](#)]
36. Mazouchi, M.; Naghibi-Sistani, M.B.; Sani, S.K.H. A novel distributed optimal adaptive control algorithm for nonlinear multi-agent differential graphical games. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 331–341. [[CrossRef](#)]
37. Zhang, F.; Zhou, M.; Qi, L.; Du, Y.; Sun, H. A Game Theoretic Approach for Distributed and Coordinated Channel Access Control in Cooperative Vehicle Safety Systems. *IEEE Trans. Intell. Transp. Syst.* **2019**, 1–13. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).