Article

An Extended Object-Oriented Petri Net Model for Vulnerability Evaluation of Communication-Based Train Control System

Ye Zhang ^{1,*}, Yatao Wang ², Lin Wang ² and Guoqiang Cai ²

¹ Beijing Key Laboratory of Traffic Engineering, Beijing University of Technology, No.100 Pingle Yuan, Chaoyang District, Beijing 100124, China

² State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, No.3 Shang Yuan Cun, Haidian District, Beijing 100044, China; 13120967@bjtu.edu.cn (Y.W.); 19125766@bjtu.edu.cn (L.W.); gqcai@bjtu.edu.cn (G.C.)

* Correspondence: zhangye@bjut.edu.cn or yezhangbing@126.com

Received: 10 August 2020; Accepted: 21 August 2020; Published: 8 September 2020

Abstract: Communication-based train control systems (CBTCs) have been widely used as crucial systems in urban rail transit networks. CBTCs typically utilizes different levels of symmetry structure according to different geographic deployments. While, in practice, CBTCs crashes have destroyed the transportation systems of the whole city level for many times. Based on the extended object-oriented Petri net (EOOPN), this paper proposes a vulnerability model and an evaluation procedure, which are capable of considering the vulnerability factors in both inner system level and equipment level. On the system level, it establishes a complex dynamic communication structure model among the distributed subsystems, while on the equipment level, it details the equipment changing state during train operation. The searching algorithm of EOOPN depicts possible failed paths of CBTCs via the token transition among train-ground communication EOOPN subnets. The vulnerability calculation is applied to the metro company's in situ CBTCs to illustrate the effectiveness of the approach.

Keywords: OOPN; vulnerability; urban rail transit; CBTC system

1. Introduction

Urban rail transit has become one of the mainstream public transport systems over the world. Its advantages include punctuality, large capacity, and convenience. The train operation and control system is the critical system that supports the main line's fluid operation [1]. The most popular train operation and control system is the communication-based train control system (CBTCs), which consists of a complex and large scale symmetry train-ground distributed networked topological structure. CBTCs utilizes in-vehicle equipment and rail communication facilities to share information with stations and control centers. It dynamically controls the speed of trains to keep safe braking distances, ensuring that the dispatching commands are transmitted to the train in time. In the past, the failure of CBTCs has resulted in disastrous accidents, which cause disruption to trains' normal operation schedules. Therefore, studies on the vulnerability of CBTCs have significant implications. The purpose of these studies is to control the key failure of CBTCs, and to provide guidance for the maintenance working management for improving both operational efficiency and to ensure safe operations.

Vulnerability is related to performance degradation or failure due to disruptive events. The vulnerability of the system is determined by the degree of threat of the disturbance factors and the degree of damage to the system after the disturbance attack. The evaluation method based on specific strategies is an effective method to identify the vulnerabilities of different network configurations. Vladimir et al., suggested a quantities measurement approach to study hierarchy networks based on

the analysis of their vulnerability [2]. Haimes discussed the issue of vulnerability in relation to risk assessment in infrastructures. The aim was to assess the likelihood of a threat, modeling the responses of various interdependent variables affecting the consequences of any dysfunctionality in the system [3]. Ouyang reviewed and categorized the modeling and simulation approaches into six types, including empirical, agent, system dynamics, economic theory, and network based approaches [4]. Blandine focused on railway engineering to improve the cohabitation between railways and rivers, and to better manage hydraulic risk [5]. Irene et al. introduced a framework that attempted to challenge European rail traffic management system security by evaluating the exploitability of these vulnerabilities [6]. Xing et al. investigated the Shanghai Metro Network vulnerability of a weighted metro network in its response to random failures as well as malicious attacks [7]. Wu et al., introduced a novel model for the attack vulnerability of complex networks with a tunable attack information parameter [8]. Ouyang analyzed the vulnerability models and critical components of railway and airline systems vulnerability [9]. Eduardo et al., investigated the reliability and vulnerability similarities as well as the differences of road networks [10]. Rodriguez analyzed the role of circular lines in network vulnerability and obtained a worst-case scenario for the successive disruption of links by simulating a targeted attack on the network [11]. Balijepalli et al., proposed a new vulnerability index considering the serviceability of road links and illustrated its computation [12]. Demirel et al., proposed a framework to explore the concepts of exposure, vulnerability and connectivity in EU road networks, and to assess the potential transportation infrastructure sensitivities towards sea-level rises and storm surges [13]. Jenelius et al., derived several link importance indices and site exposure indices to avoid causing unnecessary disturbances in the roadwork planning [14]. Zenil et al., presented a method for estimating the complexity of an image based on Bennett's concept of logical depth for the physical world [15]. The complex network analysis method and graph theory are used to analyze the vulnerability of the networked system [16]. Berdica et al. believed that the vulnerability of the road transportation system is a characteristic of reduced accessibility caused by various reasons and was sensitive to abnormal events. It is closely related to network reliability, disaster risk, robustness and service level [17]. Liu et al., used the comprehensive evaluation model of cloud matter elements to build the vulnerability evaluation index system of urban road traffic networks [18]. Jenelius et al., used the degree of change in path cost before and after road segment failure to characterize the importance of the road segment, and used travel costs from different regions to evaluate the degree of impact in that region [19]. Minciardi et al. assessed the possibility of damage to the regional unit under external pressure and vulnerability, and evaluated the possibility of loss of the regional unit function [20]. Myung et al. took the connected path between s–t as the initial input of the model and found all potential connected paths between s–t, and optimized the design of the connected network [21]. Feng et al. simulated the performance of the network vulnerability when the stations are failed under random and malicious attacks [22]. Khanmoha

Madi et al. presented a security vulnerability analysis approach to find critical areas along railway transportation routes regarding dangerous goods [23]. The classical Petri net is a simple process model, which consists of two kinds of nodes: the place and the transition, the directed arc, and the token. Mogens et al. generalized causal nets to occurrence nets by adding forwards conflict [24]. Eike et al. developed the way that handle the Petri net algebra so as to allow for further application-oriented extensions and modifications [25]. Koch described Petri net concepts based on minimal, semi-positive transition invariants that fulfill steady-state conditions [26]. Murata discussed introductory modeling examples, behavioral and structural properties, three methods of analysis, subclasses of Petri nets and their analyses [27]. The Petri net can be used in discrete and qualitative modeling of railway fail-safe signalization and interlocking design [28], synchronization protocol [29], construction of abstract state spaces tools [30], railway networks and train schedules [31] and on-board subsystems of a satellite-based train control system [32]. The ability of the Petri net to describe distributed and concurrent systems also makes the application of a Petri net in train control systems more advantageous [33]. When a Petri net is applied to the modeling of CBTCs, the intuitiveness and simplicity of describing the complex system are not comparable with other modeling methods [34]. The Petri net gives a full description

of the behavior mechanism of concurrent system on two levels. First, the Petri net directly shows the physical structure of concurrent system and the initial state of resources in the system. Second, it can indirectly show the dynamic behavior mechanism of the concurrent system under the function of the transition enabling rule of the Petri net. These two levels are interrelated, forming a set of physical structure and rows. Hua et al. combined object-oriented with a colored Petri net, using the characteristics of object encapsulation and inheritance, reducing the complexity of the system model [35]. As the complexity of the system increases, the establishment and analysis of the Petri net model of the system will be extremely complicated. Meanwhile, the extended object-oriented Petri net (EOOPN) combines object-oriented modeling technology with colored Petri nets, using the characteristics of object encapsulation and inheritance to reduce the structural complexity of the established system model and enhance its encapsulation and re-usability. When analyzing the behavior of the entire system, the work just pays attention to the information interface among the object and the outside world and the information transfer between different object interfaces. The model is simple and efficient. Therefore, this paper uses the object-oriented colored Petri net model to study the vulnerability of CBTCs.

The research of CBTCs now mainly focuses on its reliability and safety risks, and analyzes the degree of use and working ability of the equipment under the existing conditions. Vulnerability is different from reliability and risk. The purpose of vulnerability research is to analyze the potential vulnerabilities of the system equipment itself, and to analyze the inherent vulnerabilities to help fundamentally examine the causes and key points of the failure, to provide guidance for the equipment managers' maintenance work and equipment designing, and also to provide support to improve operational efficiency and ensure operational safety. In this study, we employ an extended object-oriented Petri net (EOOPN) for vulnerability modeling and evaluation of the CBTCs. EOOPN introduces some new features and modeling elements to describe vulnerability in a more convenient and clear way, which makes it more suitable for complex system analysis. Based on EOOPN, we propose a general modeling procedure performed in two levels: system and equipment level. On the system level, the model describes the networked data flow transfer among train-ground subsystems, while on the equipment level, it depicts state transition process of each equipment, such as in-vehicle units. EOOPN can be used in various complex system scenarios. Modeling, searching algorithm and computation of vulnerability approach are applied to this EOOPN model. Examples of CBTCs illustrate the modeling procedures.

This paper is organized as follows. Section 2 provides a vulnerability framework for CBTCs and introduces the formal specifications of EOOPN. The vulnerability modeling and computation procedure are discussed. Section 3 describes general modules of CBTCs based on EOOPN. Section 4 offers the quantitative cases model and experiment of CBTCs. Section 5 presents the conclusions and future works.

2. Vulnerability Modeling Framework with EOOPN

2.1. Formal Specification of EOOPN

The EOOPN is defined as an 2-tuple, $EOOPN N = \{ops, RT\}$, where $ops = \{ob_i, i \geq 0\}$ is a finite set of object subnets representing the dynamic behavior of the system. $RT = \{T_{ij}, i \geq 0, j \geq 0, i \neq j\}$. It is a finite set of message transfer transitions among different objects. The input place of T_{ij} is the information output place of ob_i . The output place of T_{ij} is the information input place of ob_j .

Object subnet ob_i is a finite set of 9-tuple, $ob_i = \{SP_i, AT_i, IM_i, OM_i, I_i, O_i, C_i, NC_i, \varepsilon_{ij}\}$, where:

- SP_i is a finite places set of ob_i , and it is divided into three types: state place, input place and output place;
- AT_i is a finite transitions set of ob_i ;
- IM_i is a finite input information places set of ob_i ;

- OM_i is a finite output information places set of ob_i ;
- $I_i(P, T)$ is the input map from place P to transition T , $P = SP_i \cup IM_i$, $T = AT_i$, $C(P) \times C(T) \rightarrow N$. It is a colored arc from P to T ;
- $O_i(P, T)$ is the output map from transition T to place P , where $P = SP_i \cup OM_i$, $T = AT_i$, $C(T) \times C(P) \rightarrow N$. It is a colored arc from T to P ;
- $C(SP_i)$ is the color set for state places of ob_i ;
- $C(IM_i)$ is the color set for input places of ob_i ;
- $C(OM_i)$ is the color set for output places of ob_i ;
- $C(AT_i)$ is the color set for active transitions of ob_i ;
- NC_i is the network relevance degree. It is connection relationship among subnet ob_i and other subnets;
- ε_{ij} is the attack severity when place p_j of ob_i is attacked.

2.2. Vulnerability Computing Framework

The quantitative analysis method of the system vulnerability based on EOOPN can be summarized in the following steps. Firstly, analyze the data flow relationship and extract vulnerability factors based on failure information in the system. Secondly, divide the complex system into several object subnets and establish subnets models. Thirdly, determine the attack rules according to the characteristics of EOOPN and the data flow relationship of the system. Finally, the vulnerability calculation formula is substituted to evaluate the vulnerability of the system. The quantitative analysis method of system vulnerability based on EOOPN is summarized in the following steps, as shown in Figure 1:

Figure 1. Quantitative analysis procedure of system vulnerability.

2.2.1. Vulnerability Attack Path Searching Algorithm

Vulnerability analysis is generally aimed at complex and large systems. Due to the complexity of the system, it is difficult to analyze all elements of the system using the same method. Industrial control systems like CBTCs have many components, and the components and functions of different devices are very diverse. In addition, there are many causes of equipment failure, and there are many kinds of failure causes for each failure phenomenon. Therefore, mapping the same type of equipment failure causes to the same type of vulnerability factors and implementing the vulnerability by analyzing a small number of vulnerability factors is important.

The system vulnerability analysis is to trace the dynamic change process of the vicissitude. The attack rule of the vulnerability factor is the successive failure path of the change. It is the

disturbance path to the entire system. The basis for determining the attack sequence of the vulnerable node is attack path searching. In the multi-level system, the effect of attack to a subsystem is transmitted to other subsystems through information transition. In EOOPN, it is reflected in the flow of object resources, that is, the dynamic tokens transferred. The transition changes the successive system enabling state, and the state subsequently changes one after another. This kind of attacked state degrades the system performance.

In order to facilitate the analysis of successive failure paths of transitions in each subsystem model, we propose an attack path searching algorithm for EOOPN. The algorithm steps are as follows:

- (1) Obtain input matrix $I_{m \times n}$ and output matrix $O_{m \times n}$ of the model from the Petri net structure, and make the counting variable $i = 0$ and paths $Route = \{t_i\}$;
- (2) Search for the columns corresponding to the transition in the output matrix $O_{m \times n}$. If $O_{pi} = 1$ ($p = 1, 2, 3, \dots, m$) exists, go to step 3. Else $i = i + 1$, Loop $i \leq n$;
- (3) Search for the rows corresponding to the input matrix $I_{m \times n}$ in which the place is located. If $I_{pq} = 1$, go to next step. Otherwise $p = p + 1$, go to step 3;
- (4) Judge the structural relationship between the transition t_i and t_q , if $\exists p_j \in t'_i \wedge |p_j| > 1 \wedge \exists t_0 \in \cdot p_j \wedge p_j \wedge p_j \wedge p_i \in \cdot t_q \wedge I_{jq} = 1$, then $Route = \{t_i\}$, all nodes in the system end traversal and exit the program. Else $Route = \{t_i\} + \{t_q\}$, go to step 2;

Different association structures have different effects and record the successive attack path of transitions according to the relationship between related structures. The input matrix and output matrix are separated in the description of Petri net structure, so the algorithm adopts double-layer cyclic structure, and the complexity of the algorithm is $O(mn^2)$. We use the depth first search algorithm to search out all accessible paths.

2.2.2. Attack Rules of Vulnerability Influencing Factors

The basis of determining the attack order of the vulnerable nodes is the attack threat degree. The greater the attack threat degree, the greater the global hazard to the system. In fact, the failure effect of one equipment to the subsequent equipment is reflected by the transmission of information data. In the EOOPN model, it causes the enabling state of system transition and the place state change one after another, which eventually damage the system model and degrade the system performance. The action process of vulnerability factors on the whole system is the dynamic change process of transition, and the attack rule is the successive failure path of transition [36].

According to the path searching algorithm, the transition t_i is the vulnerable node under attack. The route is the transition set of successive failures, and the initial state is $Route = \{t_i\}$. For the input matrix I_{mn} and output matrix Q_{mn} , m and n are the number of nodes of the place and the transition respectively. First, judge whether the transition t_i is the end of transition. If it is, the search ends. Otherwise, continue to judge the relationship between the subsequent transition of transition t_i and itself. If it is a selection structure, the searching procedure will end. If it is not a selection structure, add the subsequent transition to the route set. Following this rule, the end point and attack path of vulnerability factors can be determined [37].

2.2.3. System Vulnerability Calculation

In the object-oriented Petri net model, the mutual communication and association between different object partitions constitute the network structure model of the signal system. Network vulnerability refers to whether the overall performance of the system is intact, or the size of performance loss after certain routines in the system are destroyed by certain attack rules, thereby determining the weak links in the system. Vulnerability influencing factors are only one node object in each object subnet, and cannot fully reflect the influence of a single factor on the entire network. The association relationship between the node objects reflects the connectivity between the node objects on the network,

and the threats to highly correlated node objects on the network caused by the attack is greater [27]. Therefore, when calculating the threat degree of vulnerability influencing factors, not only the threat degree of a single vulnerability factor, but also the correlation degree of the target subnet where the vulnerability factor is located in the entire system should be considered. This paper considers that the object subnets communicate with each other, and the number of communication relationships between different object subnets and other subnets is different. Therefore, this paper introduces the concept of association degree in the calculation of the connection complexity of the object subnets.

When calculating the threat degree, we cannot only consider the single vulnerability factor, but also need to combine its object sub-nets in the overall system correlation. Since the object sub-nets of a system communicate with each other, and the number of communication relationships between different object sub-nets is different. We introduce the concept of correlation degree to calculate the connection complexity of the object sub-net, and determine the quantitative calculation formula of vulnerability. EOOPN has the advantages to simplify and encapsulate network connections. The vulnerability of a complex system is affected by the threat degree of the disturbance factor and the damage degree of the system after the disturbance attack.

The system vulnerability calculation formula V is given by

$$V = NC_i \times \varepsilon_{ij} \times \Delta A \quad (1)$$

where V is the vulnerability of the target system.

NC_i is the network association degree of the object subnet where the node exists. It determines the degree of influence of the elements in the target subnet on the entire system.

ε_{ij} is the degree of attack damage of the warehouse node, it is represented by the affected area of the attacked object—the greater the degree of harm, the greater the degree of threat to the influencing factors of vulnerability. The degree of attack damage refers to the range of influence on the subsequent system process after the vulnerability factors in the system are attacked. In Petri net, it is the successive failure effect of a certain transition on subsequent transition.

The greater the degree of attack damage of vulnerable nodes, the greater the degree of attack threat; the greater the network association of the object, the greater the degree of attack threat.

ΔA is the loss rate. It is impact of attacked nodes to the system.

The terms are defined in the following,

Definition 1. Network correlation degree for object subnets:

$$NC_i = \frac{\text{num}_{\text{in}}(\text{ob}_i) + \text{num}_{\text{out}}(\text{ob}_i)}{\sum_{\text{ob}_i \in \text{ops}} \{ \text{num}_{\text{in}}(\text{ob}_i) + \text{num}_{\text{out}}(\text{ob}_i) \}} \quad (2)$$

where $\text{num}_{\text{in/out}}(\text{ob}_i)$ refers to the number of relationship records related to an object ob_i .

NC_i refers to the ratio of the number of relationships of ob_i to the number of all relationships in the system and it determines the influence degree of the elements in the object subnet on the whole system.

Definition 2. Attack severity of vulnerability influencing factors:

$$\varepsilon_{ij} = \sum_{i=1}^4 \left(\frac{\sum'_{ij} 1 - \sum''_{ij} 1}{n} \right) \quad (3)$$

where ε_{ij} is the degree of attack severity of a place p_j in an object ob_i , $\sum'_{ij} 1$ is the transition number of node that lead to successive failures when the transition node t_j fails, $\sum''_{ij} 1$ is the number of transitions that change from death to enabling transition in the same situation, n is the total number of transitions in the assessed system.

Definition 3. Topological efficiency of system network:

$$A = \frac{1}{N_p N_t} \sum_{i \in P} \sum_{j \in T} \frac{\min W(P_{p_i}, T_{t_j})}{|d_{ij}|} \quad (4)$$

where N_p and N_t are the number of place p and transition t in the Petri net. $|d_{ij}|$ is the shortest distance between the place i and the transition j . $\min W(P_{p_i}, T_{t_j})$ is the smallest value of the weight between the place i and transition j .

Definition 4. The loss rate ΔA of the network efficiency is the impact of the attacked node.

$$\Delta A = \frac{A - A'}{A} \times 100\% \quad (5)$$

where ΔA is the impact of vulnerable nodes on network efficiency after being attacked, A and A' are the network topological efficiency value in normal operation and after being attacked, respectively.

3. CBTCs Modeling Based on EOOPN

3.1. Architecture of CBTCs

A common CBTCs is divided into four subsystems, which are control center system, trackside system, in-vehicle system and depot system according to geographical areas. The control center system realizes the operation supervision and adjustment of trains, so that dispatchers can manage all trains and complete the train operation schedule. The vehicle-mounted system periodically obtains the movement authorization by means of vehicle-ground communication, calculates the current allowable speed of the train, and controls the train operation. The trackside system generates the train's movement authorization in real time according to the operation schedule, guarantees the intervals between trains, and handles the route for the train. The depot system completes the safety management of train entry and exit depot. The control center system includes a traffic dispatching workstation, a running map editing workstation, a database server and an application server. The trackside system includes the station automatic train supervision system (ATS), computer interlocking system (CI), zone controller (ZC), a transponder, an axle counter, a switch, platform screen doors (PSD), emergency stop button (ESB), lineside electronic unit (LEU), data communication system, etc. The in-vehicle system includes balise transmission module (BTM), a beacon antenna, a coded odometer, a speed sensor, a radar, in-vehicle computer, in-vehicle cabinet, a wireless antenna, in-vehicle recording system, human-machine interface (HMI), etc. The depot system includes an ATS extension, a computer interlocking system (CI), a switch, a signal light, zone controller (ZC) and a transponder, and etc. Figure 2 shows a universal CBTCs structure.

CBTCs needs to meet the following key functional requirements within its four subsystems:

- (1) Control center system communicates with in-vehicle system. The control center ATS displays the train number, online running position, running direction and other information on the large screen through two-way communication with the train. The train receives the temporary shunting command from the control center ATS for schedule adjustments.
- (2) Control center system communicates with depot system. The control center sends the completed train operation map and operation plan to the depot ATS extension. The depot system dispatches according to the train operation plan and sends the train identification number to the control center through the depot ATS extension. The control center sends the temporary adjustment commands, train shunting arrangement and return commands to the ATS extension of the depot. Then, the depot equipment executes the operation and the procedure are monitored by the control center.

- (3) Control center system communicates with trackside system. The control center system communicates with the ATS extension of the station to provide information, such as train schedule, route control commands, real-time train position, train identification number and equipment status. The trackside system transfers equipment operating status information to the control center.
- (4) Depot system communicates with in-vehicle system. The depot system realizes the driving mode management for train access sections through communication with the in-vehicle equipment. It also administers train entering and shunting within the depot.
- (5) In-vehicle system communicates with trackside system. The data communication between the in-vehicle equipment and the trackside equipment is the key to the normal operation of the train. The two-way communication between the vehicle and the trackside is used to detect the train position, calculate the train movement authorization and link the safety equipment. It remotely controls the train and the screen door, and route management.

To guarantee the trains operation safely controlled under the above communication interactive network environment, a clear and understandable modeling approach is critical. The key problem of model-based approach is to establish a system model. The EOOPN realizes the complete process of system analysis and design by adopting mechanisms such as object, class, inheritance, abstraction and encapsulation. It is a promising representation method to accomplish CBTCs modeling and vulnerability analysis.

Figure 2. A universal structure of communication-based train control systems (CBTCs).

3.2. CBTCs Modeling Based on EOOPN

CBTCs can be seen as a communication link between multiple units. The integrated system is actually the “input–output” relationship between the data flow. The relationship between the state and action of the “location” and “transition” is the reflection of the different states of the device in the Petri net model.

Each unit represents the operation control and data transmission of a train, and the equipment actions between adjacent units restrict each other. Therefore, analyzing the working process of a unit can characterize the general principles of the entire network system. The EOOPN models essentially integrate various object subnets, encapsulating the internal structure of each object subnet, leaving

only the places that have input and output relationships with other object subnets as interfaces. In this section, the EOOPN model will be established according to the data flow relationship between the CBTCs subsystems.

According to the functional requirements of CBTCs and the data flow relationship between the objects, we establish the system level model and equipment level model of CBTCs as following,

(1) CBTCs system level model

$$MSS = \{TSNet \cup TrNet \cup CCNet \cup CDNet, RT\}. \quad (6)$$

TSNet is the trackside subnet; TrNet is the in-vehicle subnet; CCNet is the control center subnet; CDNet is the depot subnet. $RT = \{G_1, G_2, G_3, \dots, G_{16}\}$ is the set of transitions. Figure 3 and Table 1 show its implications.

Figure 3. Object Petri net model of the CBTCs.

Table 1. Transition implications of CBTCs.

Transition	Implication	Transition	Implication
G1	Train departure request	G9	Train operation status information
G2	Train departure authorization	G10	Train adjustment command
G3	Beacon antenna pulse information	G11	Train operation status information
G4	Line information	G12	Door status information
G5	Train schedule	G13	PSD linkage command
G6	Device status information	G14	Beacon antenna pulse information
G7	Route control command	G15	Line information
G8	Device status information	G16	Mobile authorization

(2) Control center system subnet model

Control center system subnet $CCNet = \{SP_3, AT_3, IM_3, OM_3, I_3, O_3, C_3, NC_3, \varepsilon_{3j}, \mu_{3j}\}$ is shown in Figure 4.

Figure 4. Control center system subnet.

(3) Trackside system subnet model

Trackside system subnet $TSNet = \{SP_1, AT_1, IM_1, OM_1, I_1, O_1, C_1, NC_1, \varepsilon_{1j}\}$ is shown in Figure 5.

Figure 5. Trackside system subnet.

(4) In-vehicle system subnet model

In-vehicle subnet $TrNet = \{SP_2, AT_2, IM_2, OM_2, I_2, O_2, C_2, NC_2, \varepsilon_{2j}\}$ is shown in Figure 6.

Figure 6. In-vehicle system subnet.

(5) Depot system subnet model

Depot system subnet $CDNet = \{SP_4, AT_4, IM_4, OM_4, I_4, O_4, C_4, NC_4, \varepsilon_{4j}, \mu_{4j}\}$ is shown in Figure 7.

Figure 7. Depot system subnet.

4. Vulnerability Analysis Based on EOOPN for CBTCs

According to the analysis of major international rail traffic crashes, the reason for train rear-end collisions is the failure of CBTCs equipment and improper command, that is, the unstable state of the equipment and the unsafe operation of two factors. Vulnerability analysis of the CBTCs system is the root of improving system security from the perspective of the system itself. Vulnerability is an inherent property of the system, and it is hidden. It cannot be reflected during the normal operation of the system. The influencing factors of vulnerability can be understood through system failures. This paper analyzes 5929 failure phenomena of an urban rail transit company from 2012 to 2014. Extract the reason of the failure and its phenomenon, divide the cause of the failure according to the structural attributes of the device.

4.1. Case of Attack Paths Search

The trackside system connects with each other to realize the information interaction, safety protection and other functions for operation. The trackside system includes station equipment and trackside equipment. The depot equipment and station equipment are basically the same in structure. So, we take trackside system as the example to study. Figure 8 shows the trackside system according to the correlation structure between the transitions of Petri net. In Figure 8, transitions T10, T12 and T23 are the transmission ends of the sequential structure, and the subsequent transitions are the selective structure. Considering the different situations of the transitions themselves, they will not affect the subsequent transition enabling. While transitions T25, T26 and T29 are the transmission ends of the trackside system, and will not affect the enabling of other transitions in the system.

Figure 8. Schematic diagram of transition failure of trackside system. (a) T1 failure transfer relationship, (b) T8 failure transfer relationship, (c) T6 failure transfer relationship, (d) T30 and T31 failure transfer relationship, (e) T13 and T14 failure transfer relationship, (f) T25 and T28 failure transfer relationship, (g) T24 failure transfer relationship.

According to the attack path search algorithm, the failure transfer relationship of each transition can be obtained as shown in Table 2.

Table 2. Failure transfer relationship of transitions of trackside system.

Failure Transition	Successive Failure Transitions	Failure Transition	Successive Failure Transitions	Failure Transition	Successive Failure Transitions
T1	T2, T3, T4, T5, T7, T10, T23	T12	–	T23	–
T2	T3, T4, T5, T7, T10, T23	T13	T15, T16, T22, T23	T24	T26, T27, T29
T3	T4, T5, T7, T10, T23	T14	T22, T23	T25	–
T4	T5, T7, T10, T23	T15	T16, T22, T23	T26	–
T5	T7, T10, T23	T16	T22, T23	T27	T29
T6	T21, T22, T23	T17	T15, T16, T22, T23	T28	T27, T29
T7	T10, T23	T18	T15, T16, T22, T23	T29	–
T8	T9, T7, T10	T19	T15, T16, T22, T23	T30	T12
T9	T8, T7, T10	T20	T15, T16, T22, T23	T31	T11, T12
T10	–	T21	T22, T23		
T11	T12	T22	T23		

Take transition T1 as an example. If T1 fails, it will cause successive failures, since T2 and T3 belong to the sequential structure. Transition T4 and T5 have concurrent relationships with each other, and transition T3 belongs to a special sequential structure relationship, so transition T4 and T5 will also fail. While T7, T10 and transition T4, and T23 and T5 belong to the sequential structure relationship, so transition T7, T10 and T23 will totally fail when T1 fails. According to the algorithm, the successive failure transitions of transition T1 are T2, T3, T4, T5, T7, T10 and T23, which are consistent with the actual correlation structure. Therefore, the algorithm is effective.

The subnet model of the trackside system is simulated with the Petri net analysis software PIPE (Platform Independent Petri Net Editor). The model can be run normally. Each activity change and place in each subnet of the object are under the initial identification. Through appropriate transition and excitation of the gate, it can be excited, that is, all states are reachable. Moreover, each transition in the network were triggered again by the enabling of a series of transition sequences, which shows that the built EOOPN model is alive too.

4.2. Vulnerability Quantitative Evaluation Cases of CBTCs Based on EOOPN

In this paper, the trackside system and the in-vehicle system were taken as research examples by selecting a vulnerable node to analyze the vulnerability of the CBTCs. The main purpose is to verify the proposed quantitative calculation method of its vulnerability.

(1) Calculation of network correlation

In the object-oriented Petri net system, the trackside system has information exchange with the control center system and the in-vehicle system, and there are one input and one output relationships with the control center system, and four input and two output relationships with the in-vehicle system. The network correlation degrees of the trackside system and the in-vehicle system are calculated:

$$NC_{trackside} = 0.25 \quad (7)$$

$$NC_{in-vehicle} = 0.375 \quad (8)$$

(2) Calculation of attack severity degree of vulnerable nodes

The attack threat degree of the vulnerability factors of the trackside system and the in-vehicle system obtained are shown in Tables 3 and 4.

Table 3. Trackside vulnerability factor attack threat degree.

NO.	Vulnerability Factor	Threat Degree T
1	Interlocking host	0.0565
2	Tuning unit	0.0484
3	TCOM	0.0484
4	Sending module	0.0484
5	Receiving module	0.0484
6	Axial head	0.0484
7	Code generator	0.0484
8	HMI workstation	0.0484
9	HMI	0.0484
10	Axis card	0.0484
11	Console	0.0484
12	Monitoring computer	0.0484
13	ZC host	0.0403
14	Conversion force	0.0323
15	Representation loop	0.0323
16	Relay	0.0323
17	Switch control circuit	0.0160
18	Switch machine	0.0081
19	Drive loop	0.0081
20	Connecting rod	0.0081
21	Signal control circuit	0.0081

Table 4. In-vehicle system vulnerability factor attack threat degree.

NO.	Vulnerability Factor	Threat Degree T
1	In-vehicle computer	0.1167
2	Antenna	0.0441
3	HMI	0.0221
4	Button	0.0221
5	Speed measuring motor	0.0221
6	Coded odometer	0.0221
7	Wireless loss	0.0726
8	Doppler radar	0.0221

(3) Determine the attack path

According to the above analysis of attack path search algorithm in Section 2.2.1 and attack rules in Section 2.2.2, the attack paths of the interlocking host and the in-vehicle computer are determined as follows:

$$Route1 = \{T_{21}, T_{22}, T_{23}, T_{25}, T_{28}, T_{27}, T_{29}\}_{TS} \quad (9)$$

$$Route2 = \{T_{14}, T_{15}, T_{16}\}_{TR} + \{T_6, T_{22}, T_{23}, T_{25}, T_{28}, T_{27}, T_{29}\} \quad (10)$$

(4) Network efficiency loss calculation

According to the attack path of the vulnerability factor, the path efficiency of the attack is recorded as 0, that is, the path efficiency between the upper transition and the place is 0.

- (1) Assuming that the interlocked host is attacked and fails, the successive failure are in *Route1* and the network loss rate is obtained:

$$\Delta A_{interlock-host} = 12.79\% \quad (11)$$

- (2) Assuming that the in-vehicle computer is attacked and fails, the successive failures are in *Route2*, and the network efficiency loss rate is obtained:

$$\Delta A_{in-vehicle-computer} = 25.65\% \quad (12)$$

(5) Node vulnerability calculation

Available from Formula (7) is as following. The vulnerability of interlocking host:

$$V_{interlock-host} = 0.0565 \times 12.79\% = 0.7226\% \quad (13)$$

The vulnerability of in-vehicle computer:

$$V_{in-vehicle-computer} = 0.1167 \times 25.65\% = 2.9934\% \quad (14)$$

From the above calculation results:

$$V_{in-vehicle-computer} > V_{interlock-host} \quad (15)$$

That is, the vulnerability of in-vehicle computer is greater than interlocking host. So, when the in-vehicle computer is attacked by certain disturbance factors, the damage is greater than interlocking host. This mechanism implies that reliability, availability, maintainability and safety work of in-vehicle computer are more important than that of interlocking host.

4.3. Discussions

The vulnerability of CBTCs is determined by the structure and function of the system. It is the sensitivity to reflect the degree of lack of function of the system after a threat and changes dynamically. We proposed calculation steps and attack route search algorithms of CBTCs system's vulnerability, according to the dynamic characteristics of Petri net. The vulnerability is an inherent property reflected into the following categories:

- (1) Vulnerability contains a series of concepts such as risk, sensitivity, adaptability and resilience. It not only considers the influence of internal conditions of the system, but also includes the characteristics of the interaction between the system and the external environment. Therefore, when calculating the attack threat degree of vulnerability influencing factors, not only is the threat degree of a single vulnerability factor, but also the correlation degree of the object subnet where the vulnerability factor is located in the entire system should be considered.
- (2) Vulnerability is the degree of damage or threats from adverse effects. It is the loss of functions to system components under the influence of external factors. Selecting a certain high-vulnerability device as the object, the proposed vulnerability method is used to conduct an in-depth analysis and grasp the vulnerability of the internal components of the device, so it will support the designers from the perspective of intrinsic safety.
- (3) Vulnerability is the ability to withstand external disturbances. It is the system's ability responding to external disturbance factors, including resistance and recovery. The process of vulnerability factors to the entire system is the dynamic process of change. The attack rule of the vulnerability factor is the successive failure path of change. According to the attack path search algorithm of influencing factors, the disturbance path of a certain vulnerability factor to the system can be determined.

5. Conclusions

Vulnerability is different from reliability and risk. This paper proposed a general modeling procedure based on EOOPN for vulnerability evaluation. Models are constructed in system and component levels. According to the historical failure record of CBTCs equipment, we divide the symmetry geographic system into four subsystems. They are trackside, in-vehicle, control center and depot according to the region. Then, we establish their EOOPN model, design and verify the attack path search algorithm. Results of modelling shows that the EOOPN can effectively analyze the distributed multi-level structure. The attack rules are determined based on the characteristics

of the Petri net and the data flow relationship, and then substituted into the vulnerability formula for quantitative evaluation. The approach is easy to understand and flexible enough to describe the complex characteristics and vulnerability calculation. Analyzing the inherent vulnerabilities of CBTCS will help to fundamentally examine the causes of system failures, find design flaws or management loopholes, provide guidance for equipment managers' maintenance work and provide support for equipment design and improvement to improve operational efficiency and safety.

Author Contributions: Conceptualization, Y.Z. and G.C.; Formal analysis, Y.W. and G.C.; Funding acquisition, Y.Z.; Investigation, G.C. and Y.Z.; Methodology, G.C. and Y.W.; Software, Y.Z.; Supervision, L.W.; Validation, Y.W. and G.C.; Writing—original draft, Y.W.; Writing—review & editing, Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Beijing Municipal Commission of Education Social Science Foundation (SM201810005002), and National Key Research and Development Plan (2018YFB1201601-12).

Acknowledgments: I want to thank Qisen Zhou for language support.

Conflicts of Interest: The authors declare that there are no conflicts of interest regarding the publication of this article.

Data Availability: The data used to support the findings of this study are available from the corresponding author upon request.

References

1. Crawford, E.; Kift, R.L. Keeping track of railway safety and the mechanisms for risk. *Saf. Sci.* **2018**, *110*, 195–205. [\[CrossRef\]](#)
2. Gol'Dshtein, V.; Koganov, G.A.; Surdutovich, G.I. Vulnerability and hierarchy of complex networks. *arXiv* **2004**, arXiv:cond-mat/0409298.
3. Haimes, Y.Y. On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Anal.* **2006**, *26*, 293–296. [\[CrossRef\]](#) [\[PubMed\]](#)
4. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 43–60. [\[CrossRef\]](#)
5. Chazelle, B.; Lambert, L.; Capoccioni, C.P. Railway vulnerability in case of extremes floods. Knowledge and risk management. *Houille Blanche* **2014**, *2*, 48–54. [\[CrossRef\]](#)
6. Arsuaga, I.; Toledo, N.; Lopez, I.; Aguado, M. A framework for vulnerability detection in european train control railway communications. *Secur. Commun. Netw.* **2018**, *2018*, 5634181. [\[CrossRef\]](#)
7. Xing, Y.; Lu, J.; Chen, S.; Dissanayake, S. Vulnerability analysis of urban rail transit based on complex network theory: A case study of Shanghai Metro. *Public Transp.* **2017**, *9*, 501–525. [\[CrossRef\]](#)
8. Wu, J.; Deng, H.-Z.; Tan, Y.-J.; Li, Y.; Zhu, D.-Z. Attack vulnerability of complex networks based on local information. *Mod. Phys. Lett. B* **2007**, *21*, 1007–1014. [\[CrossRef\]](#)
9. Ouyang, M.; Pan, Z.; Hong, L.; He, Y. Vulnerability analysis of complementary transportation systems with applications to railway and airline systems in China. *Reliab. Eng. Syst. Saf.* **2015**, *142*, 248–257. [\[CrossRef\]](#)
10. Eduardo, L.D.; Licínio, D.P.; Walter, P.J. Indicators of reliability and vulnerability: Similarities and differences in ranking links of a complex road system. *Transp. Res. Part A Policy Pract.* **2016**, *88*, 195–208.
11. Rodríguez-Núñez, E.; Palomares, J.C.G. Measuring the vulnerability of public transport networks. *J. Transp. Geogr.* **2014**, *35*, 50–63. [\[CrossRef\]](#)
12. Balijepalli, C.; Oppong, O. Measuring vulnerability of road network considering the extent of serviceability of critical road links in urban areas. *J. Transp. Geogr.* **2014**, *39*, 145–155. [\[CrossRef\]](#)
13. Demirel, H.; Kompil, M.; Nemry, F. A framework to analyze the vulnerability of European road networks due to Sea-Level Rise (SLR) and sea storm surges. *Transp. Res. Part A Policy Pract.* **2015**, *81*, 62–76. [\[CrossRef\]](#)
14. Jenelius, E.; Petersen, T.; Mattsson, L.-G. Importance and exposure in road network vulnerability analysis. *Transp. Res. Part A Policy Pract.* **2006**, *40*, 537–560. [\[CrossRef\]](#)
15. Zenil, H.; Delahaye, J.-P.; Gaucherel, C. Image characterization and classification by physical complexity. *Complexity* **2011**, *17*, 26–42. [\[CrossRef\]](#)
16. Zio, E. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 137–150. [\[CrossRef\]](#)

17. Berdica, K. An introduction to road vulnerability: What has been done, is done and should be done. *Transp. Policy* **2002**, *9*, 117–127. [\[CrossRef\]](#)
18. Liu, X.; Sun, L.; Sun, Q. Cloud matter-element comprehensive evaluation on vulnerability of urban road traffic network. *J. Chongqing Jiaotong Univ. (Nat. Sci.)* **2019**, *38*, 6–11.
19. Jenelius, E.; Mattsson, L.G. *Developing a Methodology for Road Network Vulnerability Analysis*; Royal Institute of Technology: Stockholm, Sweden, 2006.
20. Minciardi, R.; Sacile, R.; Taramasso, A.; Trasforini, E.; Traverso, S. Modeling the vulnerability of complex territorial systems: An application to hydrological risk. *Environ. Model. Softw.* **2006**, *21*, 949–960. [\[CrossRef\]](#)
21. Myung, Y.-S.; Kim, H.-J. A cutting plane algorithm for computing k-edge survivability of a network. *Eur. J. Oper. Res.* **2004**, *156*, 579–589. [\[CrossRef\]](#)
22. Feng, C.; Zhu, Q.; Yu, B.; Zhang, Y. Complexity and vulnerability of high-speed rail network in China. In Proceedings of the 2017 36th Chinese Control Conference (CCC), Dalian, China, 26–28 July 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2017; pp. 10034–10039.
23. Khanmohamadi, M.; Bagheri, M.; Khademi, N.; GhannadPour, S.F. A security vulnerability analysis model for dangerous goods transportation by rail—Case study: Chlorine transportation in Texas-Illinois. *Saf. Sci.* **2018**, *110*, 230–241. [\[CrossRef\]](#)
24. Nielsen, M.; Plotkin, G.; Winskel, G. Petri nets, event structures and domains, part I. *Theor. Comput. Sci.* **1981**, *13*, 85–108. [\[CrossRef\]](#)
25. Best, E.; Devillers, R.; Koutny, M. *Petri Net Algebra*; Springer: Berlin, Germany, 2001.
26. Blätke, M.A.; Heiner, M.; Marwan, W. *Tutorial: Petri Nets in Systems Biology*; Otto-von-Guericke University: Magdeburg, Germany, 2011.
27. Murata, T. Petri nets: Properties, analysis and applications. *Proc. IEEE* **1989**, *77*, 541–580. [\[CrossRef\]](#)
28. Malakar, B.; Roy, B. Railway fail-safe signalization and interlocking design based on automation Petri Net. In Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 27–28 February 2014; pp. 1–4. [\[CrossRef\]](#)
29. Shen, J.J.; Feng, D.Q. Vulnerability analysis of clock synchronization protocol using stochastic Petri Net. In Proceedings of the 2014 IEEE International Conference on High Performance Computing and Communications, Paris, France, 20–22 August 2014; pp. 615–620.
30. Berthomieu, B.; Ribet, P.O.; Vernadat, F. The tool TINA—Construction of abstract state spaces for petri nets and time petri nets. *Int. J. Prod. Res.* **2004**, 14–16. [\[CrossRef\]](#)
31. Giglio, D.; Sacco, N. A Petri net model for analysis, optimisation, and control of railway networks and train schedules. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2442–2449. [\[CrossRef\]](#)
32. Wu, D.; Schnieder, E. Scenario-based modeling of the on-board of a satellite-based train control system with colored petri nets. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 3045–3061. [\[CrossRef\]](#)
33. Zhao, J.; Chen, Z.; Liu, Z. A novel matrix approach for the stability and stabilization analysis of colored Petri nets. *Sci. China Inf. Sci.* **2019**, *62*, 98–111. [\[CrossRef\]](#)
34. Boudi, Z.; Koursi, E.; Collard-Dutilleul, M.E.; Khaddour, M. High Level Petri Net Modeling For Railway Safety Critical Scenarios. In Proceedings of the 10th FORMS-FORMAT Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems, Braunschweig, Germany, 30 September–2 October 2014; pp. 65–75.
35. Hua, Y.Z.; Li, C.Y. A novel object-oriented petri nets and its applications. *Mech. Sci. Technol.* **2005**, *24*, 8–11.
36. Wu, J.; Yuan, J.; Gao, W. Analysis of fractional factor system for data transmission in SDN. *Appl. Math. Nonlinear Sci.* **2019**, *4*, 191–196. [\[CrossRef\]](#)
37. Li, T.; Yang, W. Solution to chance constrained programming problem in swap trailer transport organisation based on improved simulated annealing algorithm. *Appl. Math. Nonlinear Sci.* **2020**, *5*, 47–54. [\[CrossRef\]](#)