Modeling and Verification of CBTC system security Communication protocol based on time Automaton

Yan Zhao¹,², Tao He¹,², Qiang Li¹,²

¹School of Automation & Electrical Engineering, Lanzhou Jiaotong University, Lan Zhou, Gan Su, 730070, China
²Gansu Research Center of Automation Engineering Technology for Industry & Transportation, Lan Zhou, Gan Su, 730070, China

¹Corresponding author’s e-mail: 806911892@qq.com

Abstract. With the rapid growth of population and economy, passengers' demand for urban rail transit is increasing, and it is difficult for single-line rail transit to meet passengers' demand for rapid transfer. Therefore, the interconnection between urban rail lines has been the focus of development in recent years. Therefore, the secure communication between various devices is a very important link in the interconnection test. Chongqing Metro Line 10 is the first metro line to realize the interconnection based on the secure communication protocol, in which the specific parameter setting in the secure communication protocol is specified, so the method is needed to verify the security of the protocol. In this paper, the time automaton theory is adopted to carry out the corresponding modeling work for the two key safety key contents of the safety communication protocol in the railway, namely the protocol chain building process and the protocol retransmission process, and verify its security and timeliness. Finally, a test platform is built to test the communication function between the systems.

1. Introduction
"National urban planning and construction of municipal infrastructure" much starker choices-and graver consequences-in planning "in the clear requirements: give full play to the key role of urban rail transit in urban public traffic, the metropolitan area should actively build the urban rail transit network, optimize the function level of rail transit, meet the conditions of big cities, and adjust measures according to local conditions in combination with urban development and traffic demand, so as to build an urban rail transit system covering the main framework of the urban rail transit passenger corridor[1]. By the end of 2019, urban rail construction plans of 58 cities (including 14 cities approved by local governments) in mainland China (excluding Hong Kong, Macao and Taiwan) have been approved, with a total investment of 3499.54 billion yuan and a planned length of 7,305.3 km. The scale of lines under construction and planned is further expanded, the investment continues to grow, and the construction speed is steadily improved. In the new round of urban rail transit construction, the network operation CBTC (train control based on communication) interconnection system is its remarkable characteristic[2].

At present, there is no unified standard for subway signal equipment in China. Each manufacturer has different ways to realize the safe communication between systems, and relevant technologies are kept confidential[3]. As a result, the interface protocol of each subsystem of CBTC system varies from one to another, making it impossible to realize the interconnection and interworking. So secure
communication between all equipments is very important part of the connectivity test, chongqing subway line 10, which is based on the safety communication protocol implementation, interconnection of the first subway lines, which has been clear about the security of communication protocol specific parameter Settings, so you need to adopt the method of formal verification protocol security, and using the system test platform to test the interconnection and interoperability of different manufacturer's equipment the accuracy, timeliness and news[4].

2. Development background of CBTC interconnection system

2.1. Overview of CBTC system

The technology of communication-based Train control (CBTC) originates from the European continuous Train control system. After years of development, it has made great progress. Independent of the track circuit, the system adopts high-precision train positioning and continuous, high-speed and two-way data communication, and realizes the control of the train through on-board and ground safety equipment. Now it has become the development direction of the train control system, which can meet the high-speed, information and network development of railway transportation[5].

Common CBTC systems include ground wireless block control center, vehicle-mounted equipment of trains, and two-way information transmission system of ground and one vehicle. Schematic diagram of CBTC system is shown in Figure 1. The most significant feature of CBTC system is the introduction of communication subsystem to establish continuous, two-way and high-speed communication between vehicles and ground. The command and state of train can be reliably exchanged between vehicles and ground, so that the main body of CBTC ground equipment and the controlled object train are closely connected. Therefore, "vehicle-to-ground communication" is the foundation of CBTC system and one of the pillars of the whole system. In terms of communication methods, there are mainly two ways: one is the induction loop communication system based on induction loop cable in the initial stage of the system, and the other is the newly developed fast wireless communication system[6].

![Fig.1 Diagram of CBTC system](image)

2.2. Problems existing in urban rail transit construction

2.2.1. The need to interconnect CBTC systems

Think in terms of urban scale, interconnectivity of the importance of CBTC system mainly embodied in two aspects: (1) conform to the requirements of urban regional rail transit development, megacities
30 ~ 70 km circle, forming a large number of commuter traffic, interconnectivity CBTC system can improve the utilization rate of circuitry and equipment to form network traffic and passenger organization; (2) In line with the requirements of rail transit in small and medium-sized cities, the city center needs high frequency of service, the suburbs need higher travel speed and extend the operation time of the service. In addition, for urban rail transit construction units, connectivity CBTC systems are also necessary, such as Shared rolling stock, multi-line common rail operation, customized operation lines, segmenting construction and purchase of additional vehicles, resource sharing and allocation, reduction of training costs, inter-network operation.[7]

2.2.2. Cross testing of connectivity
The challenge of Chongqing rail transit connectivity is the cross test of each signal manufacturer to verify the connectivity. The foundation of cross testing is a cross test platform to verify the interconnection CBTC function. The technical support function of cross-test platform in engineering implementation is shown in Figure 2.

![Cross test of connectivity](image)

CBTC system is a complex system for security protection, and reliable data communication between each subsystem naturally becomes the basis for ensuring the security of the whole system. Therefore, it is necessary to establish a complete data communication protocol to ensure the security of application data transmission[8].

3. Time automata and UPPAAL

3.1. Time automaton concept
In order to effectively and objectively test and analyze the communication protocol, many research methods have emerged, among which the formal method is a technique of modeling and verifying the system with strict mathematical method, which has been successfully applied to the communication protocol, reaction system and control system[9].

Formal method is a technique and tool to describe and verify hardware and software systems. At present, there are many formal analysis methods to analyze protocols, among which the time automaton is one of the model inspection methods. Real-time system is a system with certain time constraints, and people increasingly require the correctness and security of real-time system design. In order to solve the modeling and verification of real-time system, R.Arlur and Dill proposed the time automaton theory on the basis of the automaton theory in 1994[10]. As a formal description method, time automata is often used as a formal modeling tool to describe real-time systems because it has a stronger ability to express time than traditional automata.
3.2. UPPAAL briefly

UPPAAL was jointly proposed by the University of Aalborg and the University of Uppsala in 1995 for systems that can be described as the product of nondeterministic parallel processes. Each process is described as a time automaton consisting of a finite control structure, a real numerical clock, and variables, communicating between processes through pipes and/or Shared variables, which are used to ensure that two transformations between different automata are executed simultaneously. UPPAAL verifies clock constraints and reachability mainly through a fast search mechanism. Its main advantages are efficiency and convenience[11]. It can also be used to validate more complex systems. The UPPAAL user interface consists of three main parts: a System Editor, a Simulator, and a verifier. The system editor is used to create and edit the system to be analyzed. A system is described as a series of process templates, some global declarations, process assignments, and a system definition. The emulator is a validation tool that checks to see if there are any errors in the possible execution of the system model that you have built, in order to find some errors before validation. The validator checks for clock constraints and response constraints by quickly searching the state space of the system. It also provides a requirements specification editor for the required specifications and files of the system. UPPAAL provides a BNF syntax for validation. The meaning of this grammar is shown in Table 1.

| BNF syntax                  | Specific meaning                                                                 |
|-----------------------------|----------------------------------------------------------------------------------|
| E <>                          | E <> is true if and only if there is a path s_0 → s_1 → …… → s_n, so that p     |
|                              | is satisfied in a certain state s_i in the path state sequence                   |
| E[[]]p                       | E [ ] p is true if and only if there is a path s_0 → s_1 → …… → s_n, so that p   |
|                              | is satisfied in all states s_i                                                  |
| A<>p                         | Equivalent to not E [] not p, A <> p is true means that all possible path state  |
|                              | sequences will eventually pass through a state, which satisfies the expression p |
| A[]p                         | Equivalent to not E <> not p, A [] p being true means that every reachable state |
|                              | in all possible path state sequences satisfies the expression                      |
| p→q                          | Equivalent to A [] p, A [] p is true means that when the expression p occurs,    |
|                              | the expression q will eventually occur                                           |

4. System modeling and simulation

Because the CBTC system for open transmission system mostly, so mostly used in the agreement RSSP - II security communication protocols, protocol, is responsible for the security function module adopts hierarchical structure, the safety of the upper rely on the lower and upper lower constraint way, to a clear stratification of module, realize the full protection of the data, the hierarchical diagram 3 as shown:
CBTC system is composed of three large nodes. Wireless up-and-down link, on-board subsystem model and ground subsystem model. The ground subsystem model includes ATS subsystem, DSU subsystem and ZC subsystem. The on-board subsystem is equipped with on-board equipment. Wireless channels are divided into uplink and downlink, and their channel characteristics, fading, Doppler frequency shift and other characteristics are not the research content of this paper. Therefore, simplified processing is carried out to simplify the transmission of the link in the channel into a channel. In the interconnected CBTC system, the complexity of communication is mainly in its protocol chain building and protocol retransmission, so the performance of protocol chain building and retransmission will be analyzed in the protocol modeling analysis[12].

4.1. Protocol building chain model
Build chain in RSSP - II security communication protocol of process, mainly the receiver (such as ZC system) and the sender message identification (such as a train of ATP) security layer (MASL) interact, application layer and security application layer does not build chain message processing. Therefore, in order to simplify the model, these two parts are omitted in the simulation to analyze the performance of the system model intuitively.
Above for upper RSSP - II protocol built chain model. The whole model is divided into uplink and downlink, and uplink and downlink are represented by two channels. We added 10 units of time when considering TCP's transmission delay. The message structure in the link is simplified in the form of local device ID, ZC device ID and message type (request for chain establishment, first reply confirmation, pre-establishment chain status, second reply confirmation). The processing of messages at the security layer of the train sending end and the ZC receiving end is completed by the corresponding sub-layer. The interface between the upper model and the sub-layer model is connected by the replacement change TrainMASL and ZCMASL. The general process is as follows.

The VOBC ZC Type processed in the train safety layer is sent to the uplink Linkup by the train sending end, TrainSend, and then received by the receiving end, ZCRec, and processed in the safety layer of ZC. The message returned by ZC (VOBC ZC Type) through downlink Linkdown is accepted by train receiver TrainRec and processed in the safety layer of on-board equipment.

4.2. Protocol build chain timeout retransmission model
In order to study the influence of retransmission on the protocol transmission delay, a message transmission model including the time-out retransmission mechanism is established. For packet loss, retransmission mechanism, according to the RSSP - II protocol, packet loss, the link will release a secure connection and to establish a secure connection and transfer data packets. The processing of packet loss and timeout retransmission is mainly realized in the sub-model of the train. Figure 5 is the sub-model of the train. The LINKStat position in the model is the core of the link state of the whole sub-model, including idle (IDL), waiting for confirmation (WA) data transmission (DATS), data receiving (DATR) and timeout (TO). Through IDL, WA state TO complete the establishment of a secure connection through the DATS and DATR two data transmission on the condition, when the timeout the ZC receiving, train submodel receive a timeout TO inform ZC, become TO link-state, link exception TO stop data transmission and TO establish a secure connection retransmission data, TO build chain need 2 times handshake implementation, respectively by link-state PRE, PREREPLY, EST and ESTREPLY implementation control. In order to count the delay of transmission and retransmission, we set the train's sending cycle as 200 time units.
4.3 Protocol model performance simulation

Verification with UPPAAL system is mainly divided into two aspects: activity and function. The verification results are shown in Figure 6.

1) activity

The activity of the system, the absence of deadlocks, means that the system will continue to run no matter where it goes. The property is represented by $A[\neg \text{deadlock}]$, and if the deadlock is passed, the system is deadlocked.

2) functionality

When the train enters the ZC control area, it can realize protocol chain construction and protocol retransmission. $E<>((ZC.MASL) \lor (ZC.Send) \lor (Train.Rec) \lor (Train.MASL))$.

Fig. 5 The train submodel containing message retransmission

Fig. 6 Code sequence verification scene model verification diagram
5. Interconnection CBTC system test platform
Because of the huge manpower and material resources required for field test, most of the functional tests of the system need to be set up for testing in the laboratory. Therefore, on the basis of proving that the secure communication protocol is safe and reliable, corresponding system needs to be developed for the communication test of CBTC equipment. In this paper, on the basis of the existing CBTC test platform, Microsoft Visual Studio development software is used to design the communication test module, simulate the data transmission between the systems, and design test cases for the development of test scripts. The following figure is the CBTCTest software.[13].

Fig.7 Diagram of communication test module

6. Conclusion
The CBTC National Demonstration Project for connectivity has overcome the world's difficult problems and achieved initial breakthroughs so far. Aiming at the communication test project in CBTC simulation test, this paper adopts time automaton UPPAAL to model and analyze the communication protocol and verify its security. At the same time, a communication test module is designed for the existing test platform to achieve the indoor communication test of the interconnected CBTC system.

Acknowledgments
This publication is based upon work supported by the National Natural Science Foundation Regional Science Foundation Project under Project approval number: N2019G017; GSITA201910. The authors would like to thank anonymous referees whose comments and suggestions have improved the content and presentation of this work.

References
[1] Gao Chunhai. Train Operation Control (CBTC) System based on communication [M]. China Railway Publishing House, 2018:101-110.
[2] Liu Yu,China Railway Corporation. Design and formal analysis of communication protocol for CBTC system [D]. Beijing Jiaotong University, 2007.
[3] Yang Sen. Research on automatic analysis method of test results of CTCS-3 Train control and on-board Equipment interconnection [D]. Beijing Jiaotong University, 2018.
[4] Shan Zhenyu. Design and verification of CTCS-3 vehicle-ground communication protocol [D]. Beijing Jiaotong University, 2009.
[5] Li Yan. Research on consistency test of VEHICLE-ground communication protocol of CTCS-3 Based on TTCN-3 [D]. Beijing Jiaotong University, 2009.
[6] An Bin. Analysis of the main problems in realizing the interconnection of the train control system based on communication in urban rail transit [J]. Research on urban rail transit: 2017,20(S1):18-19.

[7] Li Zhaoling. Research on the Interconnection of urban rail transit Signal System [J]. Railway communication signal engineering technology, 2016,13(05):50-53.

[8] Zhang Guoru. Research on THE INTERFACE of ATS System based on CBTC under interconnection condition [D]. Chengdu: Southwest Jiaotong University. 2017.

[9] Li Zhen. Routing protocol validation based on UPPAAL [D]. Beijing Jiaotong University, 2013.

[10] Wang Jing. Modeling and verification of CTCS-3 level train-controlled on-board equipment based on time automata [D]. Zhengzhou university, 2014.

[11] Xu Dan. Formal modeling and validation of real-time systems based on time automata [D]. Suzhou university, 2007.

[12] Shen Peng. Research on protocol conformance testing based on finite state machine model [D]. Beijing University of Posts and Telecommunications,2014.

[13] Praveen Ranjan Srivatsava,B. Mallikarjun,Xin-She Yang. Optimal test sequence generation using firefly algorithm[J]. Swarm and Evolutionary Computation,2013,8.