Open Access Library Journal
2025, Volume 12, e13938
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Research on Vehicle-Ground Communication Security Protocol for Urban Rail Transit

Lifeng Chen

Shanghai Shen-Tie Investment Co., Ltd., Shanghai, China
Email: justin23@mail.nutn.edu.tw

How to cite this paper: Chen, L.F. (2025) Research on Vehicle-Ground Communication Security Protocol for Urban Rail Transit. *Open Access Library Journal*, **12**: e13938.
https://doi.org/10.4236/oalib.1113938

Received: July 11, 2025
Accepted: August 4, 2025
Published: August 7, 2025

Abstract

Most urban rail transit signaling systems use communication-based train operation control systems (CBTC). In order to ensure the safety of train operation, the safe communication between the vehicle and the trackside must meet the safety and reliability index requirements. Therefore, this article starts from the perspective of safe vehicle-ground communication protocol design between the vehicle and the trackside, and adopts two technical methods: customized network packet sequence method and cyclic redundancy check code encryption to ensure the real-time performance of vehicle-ground information transmission. Authentication and data security integrity verification. At the same time, this method also takes into account the efficiency of vehicle-to-ground communication and avoids the time-consuming shortcomings of complex algorithms.

Subject Areas

Transportation Engineering

Keywords

Vehicle-to-Ground Communication, CRC32, Network Packet Sequence, Safety

1. 概述

城市轨道交通信号系统大部分采用的都是基于通信的列车运行控制系统(CBTC)。为了保证列车运行的安全性，车地通信必须保证其自身的安全性和可靠性。其中,安全性要求对数据进行加密和保密，同时要保证信息的完整性，要具有抗干扰和抗攻击的能力，要进行身份认证和访问控制。为了满足列车运行的实际要求，车地通信要求有高可靠性，避免因系统出现故障而导致信

息传输错误或者信息传输延时，保证低时延，高准确性，抗干扰。因此，车地通信的安全可靠技术是整个 CBTC 系统的关键技术之一。

林鹏程等[1]主要从抗干扰的角度，分析了无线通信抗干扰技术与 CBTC 信号系统的特点，构建了 CBTC 系统传输模型、无线干扰 CBTC 系统和 CBTC 系统抗干扰技术。殷琴等[2]在开放式网络传输环境下，提出了一种安全通信协议优化方案。任继伟等[3]研究了基于 LTE 技术的车地无线通信传输方案。徐国平等[4]主要针对互联互通的需求，提出了支持互联互通功能的 CBTC 系统车地安全通信解决方案。

基于上述文献分析总结，缺少对于车地通信的应用层安全协议研究。因此，本文主要从车载与轨旁之间的安全车地通信协议设计的角度去分析车地通信的安全和效率问题。

2. 车地通信的功能分析

CBTC 车地通信系统主要由中心设备，车站设备，轨旁设备和车载设备四部分组成[5] [6]。如图 1 所示，数据通信子系统(DCS)使控制中心能够实时获取列车的位置、速度等基本信息，并通过数据通信技术与车载设备进行交互。DCS 系统需要符合开放性的原则，对于列车控制子系统之间发送和接受 IP 报文的信息完全透明，DCS 子系统设备传送的是安全的控制信息，但它自身处于非安全的状态，既不是一个安全子系统。

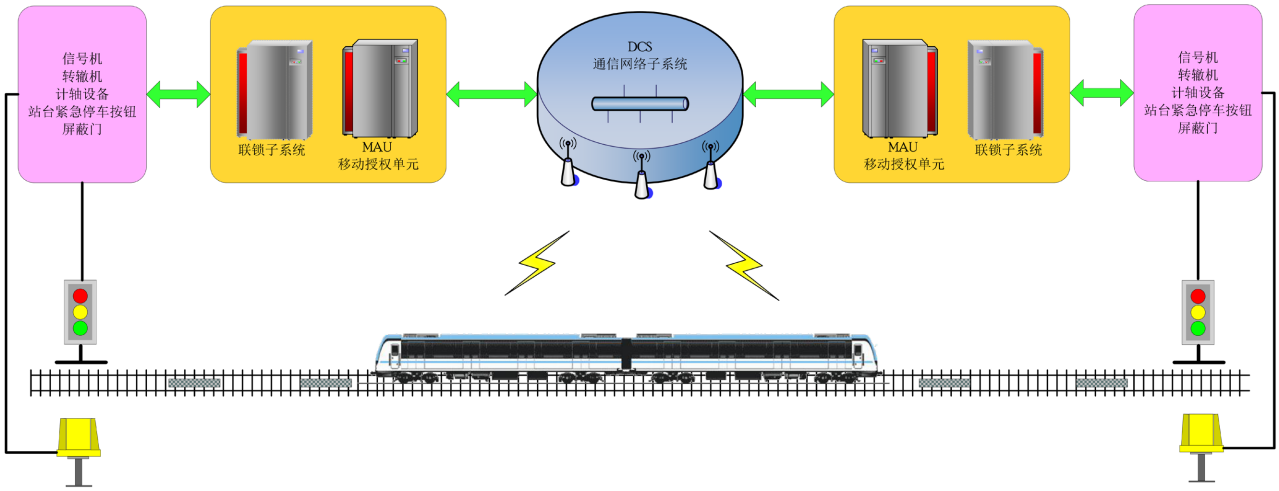

图 1. 常见的 CBTC 车地通信系统

如图 2 所示，车载与区域控制器(简称 ZC)之间采用 UDP 的方式进行通信。由车载发起通信连接，ZC 根据车载报告的位置等信息，发送给车载相应的移动授权数据信息。如果相互之间的数据出现错误，或者严重的滞后性，则可能会导致事故发生。

因此，为了保证车地信息传输的安全，可靠和高效，要求协议能够抵御各种形式的攻击和干扰，包括但不限于数据篡改、窃取和伪造等，确保信息在传输过程中的机密性、完整性和可用性。

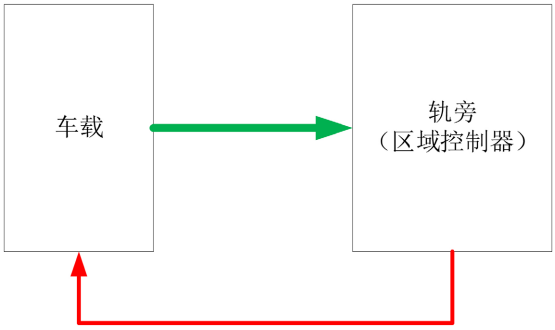

图 2. 车载与 ZC 之间的通信示意图

3. 车地通信安全协议研究与设计

车载和轨旁之间的报文信息传输从应用层开始，发送到安全层，首先由车载向轨旁发送一个数据包，数据包内包含了车载的身份信息，当轨旁收到后可以通过其中的内容来判断收到报文的种类。同时轨旁要通过其中的内容来自己进行判断，此报文是否有效，包括是否在时效内，是否出现传输错误，多传，漏传，报文传送顺序出错等问题。

当出现错误时，轨旁将会发送一个报文给发送方，请求数据发送校准，当车载接收到校准请求，将会对发送的数据报文进行校准，同时会发送一个应答报文给轨旁，告知已经收到校准请求并且进行校准。校准后的车载系统会重新发送正确的报文，双方会一直重复上述过程，直至信息传输结束。通过安全层的信息将会进一步由设备传输到通信层，再逐层传递。

报文的结构主要由 3 部分，即报文头，报文主体部分以及报文尾。报文的主体部分是报文的核心，报文头和报文尾实际上都是为了保证报文安全传输对主体内容所进行的“包装”，用来进行数据的加密保护。为了使报文更加安全，在报文主体，本协议设计加入一个安全校验的区域，用来储存对传输数据也就是用户数据包的加密校验信息如校验码等。具体的安全通信协议的报文结构设计如表 1 所示。

表 1. 车地安全通信协议结构

报文头	安全校验区	用户数据	报文尾
6 字节	≤16 字节	≤480 字节	2 字节

基于前述章节的分析，本文主要在报文头和安全校验去中，采用网络包序方法的设计和循环冗余校验码(CRC)加密角度来保证车地通信的安全和可靠性。

3.1. 车地通信网络包序方法的设计

如图 3 所示，时间序列号用 4 个字节来描述。它的作用是用于表示当前某方所处于的系统周期，每进行一次报文送，都要将当前的系统周期传输给对方作为时钟校准。若将发起方和接收方工作周期分别记为 T_I 和 T_F，将周期

定为发送数据间的时间间隔，发起方的工作周期可以表示为 T_I - T_{I+1}。同理，接收方的工作周期表示为 T_F - T_{F+1}。序列号 SN，以接收方 T_{F+1} 时刻为例，双方正常通信后，本次的发送序列号 SN_{F+1}，上次接收的信息的接收序列号 SN_{I+1}，如图 3 所示。

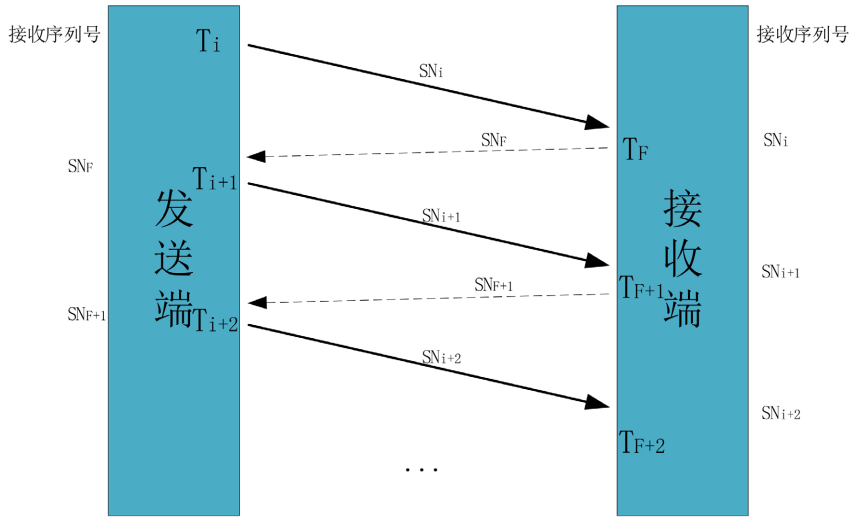

图 3. 包序设计示意图

为了保证车地通信数据的实时性，如果接收端长时间收不到发送端的 SN 网络包序列号，超过了预定的时间长，则认为车地之间的通信断开，需要发送端重新发起连接的请求。同时，从信号冗余角度考虑，车地通信之间还会检查相互发送的时钟信息值。如果 T_F 和 T_{F+1} 之间的时间差值超过了预设的时间值，即使包序号连续也是超时了，车地数据“新鲜度”不够，从而认为车地之间的通信已经断开。

为了兼顾车地通信的稳定性，采用上述的机制，如果报文无法通过安全校验和时效性检验时，虽然丢弃了该报文数据，但是，为了后续的数据接收正确，给发送端提供一个报错信息，同时进行时间校验，检验号更新等等操作。这样可以避免反复地车地通信断开的故障现象，提高系统的可用性。

通过这样的网络包序设计方式，可以保证车地信息传输数据的时效性以及连续性，从而保证列车运行的安全性。同时也兼顾了系统一定的可用性。

3.2. CRC 技术研究

在数据包发送前，发送端会对数据包进行 CRC 计算，然后将计算得到的校验码附加在数据包中。接收端在接收到数据包后，再进行 CRC 计算，然后将计算得到的校验码与接收到的校验码进行比较，以判断是否存在传输错误。这种校验方式能够确保数据的完整性和准确性。本文主要设计的是 32 位的 CRC 校验码，多项式见式(1)。

$$G_{32}(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \quad (1)$$

假设要发送的信息多项式为 m(x)，生成多项式对应码为 P = 10000010011 得到 M(x)，用 M(x)对 P 做除二运算，得到余数 r(x)所对应的代码，即冗余码，再将得到的 32 位 r(x)冗余码添加到 m(x)后，形成 CRC 码 V(x)，得到最后的发送信息，计算公式为式(2)所示。

$$V(x) = x^{32}m(x) + r(x) \tag{2}$$

CRC 校验码具有相当强的检错、纠错能力，并且实现编码和检码的电路比较简单。相对于其他校验方法，CRC 具有更高的可靠性和安全性，并且可以检测到更多类型的误码。CRC 广泛应用于网络通信、存储系统等领域。比如，以太网帧中的 FCS 字段就是采用 CRC 校验的方法。

结合车地通信场景，如图 4 所示。为了方便进行 CRC 校验，轨旁发送给车载的数据包被设计为偶数，当数据位数不足时会在数据的末尾进行补 0 从而保障了总字节数一直为偶数以便于后续的加密。在补成偶数的安全数据后面，系统会自动根据规定的生成多项式加入 32 位 CRC 冗余用于保护前部分的数据的安全。

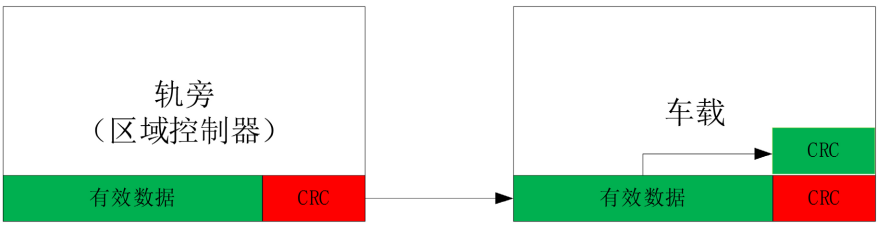

图 4. CRC 应用场景

车载在接收到完整的网络包数据后，根据有效数据在本地根据公式(1)和公式(2)的方法，计算本地 CRC 值，通过对比本地 CRC 值与网络包传输过来的 CRC 值是否相等，来判断数据是否在传输过程中被篡改。

因此，通过上述的 2 种技术结合，保证了报文内容的准确信，没有在传输过程中出现错误。而且，在数据报文的内部加入了这两个安全校验信息，从而来确认内部用户信息等的安全性。同时，在传输过程中也可以保证车地数据通信的实时性，没有受到复杂安全加密算法的延时影响。

因此，本文设计的车地通信协议相比于其他车地通信协议的对比如表 2 所示。

表 2. 车地通信协议指标对比分析

	通信效率	数据安全性	传输可靠性	扩展性
传统车地通信协议		相同		
本文设计的车地通信协议	优	相同	优	优

4. 结论

本文从抗干扰的方面出发，在进行安全协议设计的时，在其中加入了 32

位 CRC 校验码，从而一定程度上保证了报文的可靠性，防止来自不安全的设备发出的错误干扰信息。同时，为了保证信息传输保证在看可容许的误差范围内，确保低时延的特点，本文设计在车地通信的报文中加入自定义的包序号检验方法，保证每一次的信息都在规定的误差范围内，确保信息的有效性，保证列车运行的安全。但是，本文设计的车地通信协议涉及到比较多的数据验证工作，可能会影响车地通信的效率和判断车地通信延时等经验参数值的定义，需要在后续的实际测试中进行验证分析。

因此，后续工作主要是将本文设计的车地信息传输协议方法在仿真系统中进行验证和分析，以证明其可行性和可用性。

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] 林鹏程, 陈志超. 城市轨道交通 CBTC 信号系统中的无线通信抗干扰技术分析[J]. 集成电路应用, 2023, 40(12): 306-307.

[2] 殷琴, 张立伟. 一种基于开放网络的安全通信协议实现方法[J]. 铁路通信信号工程技术, 2023, 20(1): 24-27+45.

[3] 任继伟. LTE 车地无线通信传输在城市轨道交通中的应用[J]. 智能城市, 2021, 7(8): 7-8.

[4] 徐国平, 吕新军. 基于 LTE 和《RSSP-I 铁路信号安全通信协议》的互联互通 CBTC 系统车地安全通信方案分析[J]. 城市轨道交通研究, 2018, 21(12): 142-144+148.

[5] 夏伟, 蒋建金, 傅林泰, 等. 基于冗余编码系统的循环冗余校验方法[J]. 城市轨道交通研究, 2019, 22(8): 141-143+147.

[6] 蒋志毅. 地铁信号系统无线通信传输抗干扰技术研究[J]. 技术与市场, 2017, 24(2): 67-68.

Appendix (Abstract and Keywords in Chinese)

城市轨道交通车地通信安全协议研究

摘要：城市轨道交通信号系统大部分采用的都是基于通信的列车运行控制系统(CBTC)。为了保证列车运行的安全性，车载与轨旁之间的安全通信必须要满足安全性和可靠性的指标要求。因此，本文从车载与轨旁之间的安全车地通信协议设计的角度出发，采用自定义的网络包序方法和循环冗余校验码加密 2 种技术方法，保证车地信息传输的实时性验证和数据安全完整性验证。同时，该方法也兼顾了车地通信的效率，避免了复杂家吗算法的耗时缺点。

关键词：车地通信，CRC32，网络包序，安全性