

基于 LTE-M 的互联互通全自动运行系统 车地安全通信方案研究

高雪娟 雷成健 刘 泽

(湖南中车时代通信信号有限公司, 410100, 长沙//第一作者, 工程师)

摘 要 阐述了互联互通 FAO(全自动运行)系统车地安全通信的特点。归纳现有互联互通 CBTC(基于通信的列车控制)系统中采用基于 TCP(传输控制协议)的 RSSP-II(铁路信号安全协议 II)在实际工程项目中存在的问题,提出了一种互联互通 FAO 系统车地安全通信解决方案。基于 RSSP-I,通过在 LTE-M(城市轨道交通长期演进系统)的设备中增加祖冲之加密算法,能有效防护开放通信系统中的伪装威胁。提出的互联互通 FAO 系统车地通信方案可有效解决现有互联互通 CBTC 系统车地通信存在的问题。

关键词 城市轨道交通;长期演进系统;全自动运行;铁路信号安全协议

中图分类号 U231+.7

DOI:10.16037/j.1007-869x.2022.01.023

Research on Interoperation FAO system Vehicle-Wayside Secured Communication Scheme Based on LTE-M

GAO Xuejuan, LEI Chengjian, LIU Ze

Abstract The characteristics of interoperation FAO (fully automatic operation) system vehicle-wayside secured communication are expounded. The problems existing in the actual engineering project of the existing interoperable CBTC (communication-based train control) system using RSSP-II (railway signal safety protocol II) based on TCP (transmission control protocol) are summarized. A solution scheme of an interoperation FAO system vehicle-wayside secured communication is proposed. Based on RSSP-I, the ZUC algorithm is added to the equipment of LTE-M system to effectively protect open communication system from camouflage threat. The proposed interoperation FAO system can effectively solve the problems in the existing interoperable CBTC system vehicle-wayside communication.

Key words urban rail transit; LTE (long term evolution); FAO (fully automatic operation); RSSP (railway signal safety protocol)

Author's address Hu'nan CRRC Times Signal & Commu-

nication Co., Ltd., 410100, Changsha, China

FAO(全自动运行)系统是基于现代计算机、通信、控制和系统集成等技术,实现列车运行全过程自动化的新一代城市轨道交通控制系统。它包括信号、车辆、综合监控、通信和站台门等控制子系统,能实现自动控制等级 GoA 3 和 GoA 4 功能要求。相比常规的 CBTC(基于通信的列车控制)系统,FAO 系统能自动控制列车到站停车和启动加速;能提高乘客服务质量,提升列车运行速度,有效缩短列车的追踪间隔,节约能源,降低运营和维护成本。FAO 系统是国际公认的城市轨道交通控制系统的主要发展方向^[1]。线路规模化、网络化是我国城市轨道交通发展的必然趋势^[2],FAO 系统对实现互联互通的网络化运营具有重要的现实意义。

在常规 CBTC 互联互通的基础上,通过增加 FAO 系统所需的休眠、唤醒、自动洗车、门隔离和蠕动模式运行等特殊功能,以及统一硬件、接口、电子地图等,使其可支持更丰富的线路设计;支持 4/8 编组列车混合停车、休眠唤醒和自动连挂/编组,以及统一车地功能接口、统一线路布置以支持全自动车库休眠/唤醒功能,并统一车地安全通信接口协议,由此实现 FAO 系统的互联互通。

1 互联互通 FAO 系统车地安全通信分析

《RSSP-II 铁路信号安全通信协议》^[3]将安全功能模块分成安全应用中间层(SAI)和消息鉴定安全层(MASL)。SAI 层通过序列号、三重时间戳或执行周期计数,防御重复、丢失和重排序;MASL 层通过安全码、源/目的标识符,防御外部入侵。重庆、北京、长沙等城市陆续开展了城市轨道交通互联互通 CBTC 系统的工程建设,其在项目的应用过程中遇到的问题如下^[4-5]:

1) RSSP- II (铁路信号安全协议 II) 只是一个总体的设计协议,在具体的应用中需根据实际的运营状况设计通信架构,其传输层、网络层是基于 TCP/IP (传输控制协议/互联网协议) 的,而 TCP 栈自身比较复杂,各信号厂商实现的底层协议栈会出现不一致,导致通信双方无法建立通信或通信不稳定,影响了车地之间的数据传输。

2) 由于车地安全通信协议的实现必须依赖特定的软、硬件平台,车地通信的实现必须依赖于通信传输系统,因而在实际的工程施工中,为保证设备间通信的可靠性和可用性,RSSP- II 中各个配置参数的选取是一个问题。

3) 由于车地无线通信需要在高速移动环境下切换无线接入点,且目前城市轨道交通 LTE-M (城市轨道交通长期演进系统) 使用的专有频段与相邻的移动通信之间存在邻频干扰,因而不可避免地存在数据丢包的情况。而 TCP 栈具有重传机制,当检测到丢包时,TCP 栈会等待丢失包重传,即使有新数据,也不会传输,因而增加了数据包的通信延时。若该通信延时超过系统容忍时间,将会影响或中断系统的正常运营。

因此,RSSP-II 并不是实现互联互通的最佳车地通信协议。尤其是 FAO 系统,当车载设备与地面设备通信中断时,会导致列车紧急制动、降级运行;若车上无司机时,则需要救援。这严重影响了列车运营。

2 互联互通的 FAO 系统车地安全通信协议

2.1 标准要求

欧洲标准 EN 50159:2010^[6]将现有铁路信号系统中的传输系统划分为 3 类,其中 FAO 系统车地间的传输系统为第 3 类开放式传输系统,其推荐的安全通信系统架构如图 1 所示。

其中,根据欧洲标准 EN 50129:2003^[7]的要求,安全相关应用和安全相关传输功能应使用安全相关的设备、安全相关的加密技术,而非安全相关传输系统应使用安全相关的设备,或使用通过安全相关的技术检查的非安全相关的设备。

2.2 RSSP- I 和 RSSP- II 对比分析

我国铁道部参照欧洲标准并结合国内铁路信号系统实际情况,制定了分别适用于封闭式传输系统的安全通信协议 RSSP- I 和封闭式/开放式传输系统的安全通信协议 RSSP- II^[3,8]。

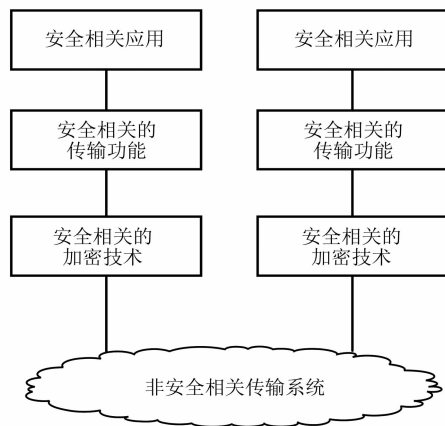


图 1 EN 50159—2010 推荐的安全通信系统参考架构
Fig. 1 Reference architecture for secured communication system recommended by EN 50159—2010

RSSP- I 的制定是基于欧洲标准 Subset-037 的子集。其通信功能模块中,各层都选取了标准协议,而在安全功能模块上增加了自定义的 ER (欧洲无线),用于车载设备和地面设备之间进行无线通信的安全协议;而 RSSP- II 则是基于欧洲标准 Subset-098 的子集。其开始用于地面设备之间的通信安全协议,即设计之初用于有线通信服务,因此是基于分组交换的 TCP/IP。因标准化需求,RSSP- II 借用 Subset-037 中的欧洲无线安全层,同时增加了一个 SAI 层。其中 SAI 层是对欧洲无线通信安全层的补充,预防了 RSSP- I 未防护的伪装威胁。总体上讲,RSSP- II 的 5 种防护措施基本覆盖了防御 EN 50159:2003 中的 7 种威胁。

RSSP- I 的安全层和通信驱动层是独立的,底层数据的传输方式可以是串口 (RS422、RS232 等),也可以是网络 (TCP、UDP (用户数据协议) 等);RSSP- II 的安全功能模块 (SFM) 则依赖通信功能模块 (CFM) 的网络适配层,是基于 TCP/IP 的。RSSP- I 可以有效地防御封闭式传输系统中的威胁,但对外部入侵如恶意伪造消息等威胁则没有防御手段。RSSP- I 和 RSSP- II 对开放系统的威胁项/防御技术对比见表 1。

假定车载设备和地面设备的通信周期均为 200 ms,根据文献[9],在不考虑祖冲之序列密码算法延时的情况下,RSSP- I 和 RSSP- II 的通信时延对比见表 2。

由于 RSSP- II 的加密认证算法和建链处理的复杂度高于 RSSP- I 的,因此 RSSP- II 的时延高于 RSSP- I 的时延,尤其是建链时延及重传时延。

表 1 RSSP- I 和 RSSP- II 对开放系统的威胁项/防御技术对比

Tab. 1 Comparison of threat items/defense technology RSSP- I and RSSP- II on open system

威胁项	防御技术	
	RSSP- I	RSSP- II
重复	序列号与时间戳	序列号
删除	序列号与时间戳	序列号
插入	序列号与时间戳、源标识、反馈报文	源和目的地标识符
重排序	序列号与时间戳	序列号
损坏	双重校验	加密技术
延时	序列号与时间戳、时间戳、超时	TTS 或 EC
伪装		加密技术

注：TTS 为三重时间戳；EC 为执行周期。

表 2 RSSP- I 和 RSSP- II 的通信时延对比

Tab. 2 RSSP-I and RSSP-II communication time delay comparison

对比项	通信时延及相关时间/ms	
	RSSP- I	RSSP- II
发送端处理时延	4.58	7.69
发送时延	0.12	0.13
接收时延	0.12	0.13
接收端处理时延	4.58	7.69
消息传输时间	6.67×10^{-4}	6.67×10^{-4}
安全连接建立时间	0	805.00
安全连接释放时间	0	200.00
重传时间	406.00	800.00

3 基于 RSSP- I 的互联互通 FAO 系统车地安全通信方案

城市轨道交通车地无线通信需要承载的业务主要有 7 项：列车控制业务数据（优先级：2）、集群调度语音业务（优先级：2）、列车运行状态信息（优先级：4）、紧急信息文本下发（优先级：4）、视频监控（优先级：6）、PIS（乘客信息系统）流媒体业务（优先级：6）、集群调度视频业务（优先级：7）。根据《城市轨道交通全自动运行系统技术规范 第 2 部分：接口规范》的要求，信号系统与数据网络子系统的无线通信应采用 LTE-M 或 Wi-Fi（无线网络）等方案。因此，通过无线网络的加密认证算法为系统提供外部威胁的防御，可以弥补 RSSP- I 的不足。

与 WLAN（无限局域网）相比，LTE（长期演进）工作在专用频段，不易受外界干扰，覆盖能力强，且支持精细的资源调度颗粒度，可从时间、频率的维度区分用户，以保证业务 QoS（服务质量）需求^[10-11]。LTE-M 是针对城市轨道交通综合业务承载需求的 LTE 系统，弥补了使用 WLAN 承载车地无线通信业务的种种劣势，为保障城市轨道交通安

全运营提供技术支撑。祖冲之序列密码算法是中国自主设计的流密码算法，现已被 3GPP（第三代移动通信合作伙伴计划）LTE 采纳为国际加密标准^[12-13]，祖冲之序列密码算法见文献^[14]。

要满足 3GPP 对 LTE 网络访问部分的安全需求，只需将加密算法实施于 LTE 网络的服务层及传输层的相关部分，即可保障数据传输的保密性和完整性。因此，本文提出基于 LTE-M 和 RSSP- I，采用祖冲之加密算法，构建互联互通 FAO 系统车地安全通信方案，如图 2 所示。

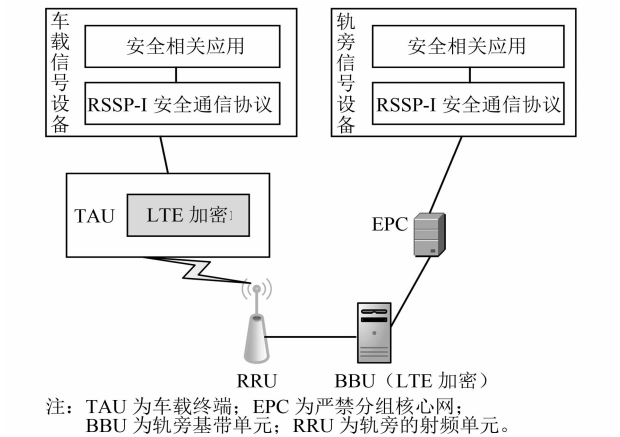


图 2 互联互通 FAO 系统车地安全通信方案架构

Fig. 2 Vehicle-wayside secured communication scheme architecture of interoperation FAO system

车载信号设备至轨旁信号设备的数据传输过程为：①车载信号设备将需要与轨旁信号设备交互的数据经 RSSP- I 安全通信模块处理后，发送至 TAU；②TAU 采用 128 位祖冲之序列密码算法对接收数据在 PDCP（分组数据汇聚）层加密后，通过空口发送至 BBU、RRU；③BBU 对接收到的数据用相同的 128 位祖冲之序列密码算法在 PDCP 层解密后，获取到车载至轨旁的 RSSP- I 处理后的数据，通过 EPC 传输至轨旁信号设备；④轨旁信号设备收到数据后，经 RSSP- I 安全通信模块解析、校验后，获取到车载至轨旁的应用数据，交由相关应用处理。

轨旁信号设备至车载信号设备的数据传输过程为：①轨旁信号设备将需要与车载信号设备交互的数据经 RSSP- I 安全通信模块处理后，经 EPC 传输至 BBU；②BBU 对接收到的数据用 128 位祖冲之序列密码算法在 PDCP 层加密后，通过 RRU 和空口发送至 LTE 的 TAU；③TAU 采用相同的 128 位祖冲之序列密码算法对接收的数据在 PDCP 层解密后，获取到轨旁至车载的 RSSP- I 处理后的数据；④

车载信号设备收到数据后,经 RSSP- I 安全通信模块解析、校验后,获取到轨旁至车载的应用数据,交由安全相关应用处理。

4 结语

互联互通 FAO 车地通信系统属于第3类开放式传输系统,除 RSSP- I 可防御的封闭式传输系统的威胁(重复、删除、插入、重排序、损坏、延时)外,还存在伪装威胁。本方案在基于 RSSP- I 的基础上,在 LTE-M 无线通信系统中,在 TAU 和 BBU 的 PDCP 层部署祖冲之加密算法对传输消息进行加密处理。

相较于现有的互联互通 CBTC 系统采用的《RSSP- II 安全通信协议》,本方案采用基于 UDP/IP 的 RSSP- I ,不仅降低了实现互联互通车地通信的复杂程度,而且通过在 LTE 的设备上增加加密算法以有效防御外部伪装威胁。该通信系统架构更有利于不同信号设备厂商之间实现互联互通,可满足开放式通信系统的安全性要求。

参考文献

- [1] 李晶. 城轨全自动驾驶信号系统方案设计及运营场景分析[J]. 铁道通信信号,2016(2):48.
LI Jing. Scheme design and operation scenario analysis of urban rail transit FAO signaling system[J]. Railway Signalling & Communication,2016(2):48.
- [2] 乔珂. 城市轨道交通网络化运营特征及列车运行调整研究[D]. 北京:北京交通大学,2015.
QIAO Ke. Research on urban rail transit network operation characteristics and train regulation[D]. Beijing:Beijing Jiaotong University,2015.
- [3] 铁道部运输局. RSSP- II 铁路信号安全通信协议(V1.0)[S]. 北京:铁道部运输局,2010.
Ministry of Railways of the People's Republic of China. RSSP- II railway signal safety communication protocol (V1.0)[S]. Beijing:Transport Bureau of the Ministry of Railways,2010.
- [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(12):142.
XU Guoping, LYU Xinjun. Analysis of train/ground safety communication solution in the interoperable CBTC system based on LTE and "RSSP- I railway signal safety protocol"[J]. Urban Mass Transit,2018(12):142.
- [5] 任军,杨剑. RSSP- II 安全通信协议参数配置问题的分析

- [J]. 铁路通信信号工程技术. 2013(增刊1):259.
REN Jun, YANG Jian. Analysis of RSSP- II safety communication protocol parameter configuration[J]. Railway Signalling & Communication Engineering,2013(S1):259.
- [6] CENELEC. Railway applications-communication, signalling and processing systems-safety-related communication in transmission systems:BS EN 50159:2010[S]. Brussels:European Committee for Electrotechnical Standardization,2012.
- [7] CENELEC. Railway applications-communication, signalling and processing systems-safety related electronic systems for signalling:BS EN 50129:2003[S]. Brussels:European Committee for Electrotechnical Standardization,2003.
- [8] 铁道部运输局. RSSP- I 铁路信号安全通信协议(V1.0)[S]. 北京:铁道部运输局,2010.
Ministry of Railways of the People's Republic of China. RSSP- I railway signal safety communication protocol (V1.0)[S]. Beijing:Transport Bureau of the Ministry of Railways,2010.
- [9] 南迪. RSSP- II 安全通信协议 CBTC 的应用研究[D]. 北京:北京交通大学,2015.
NAN Di. Application of RSSP- II safety communication protocol in CBTC[D]. Beijing:Beijing Jiaotong University,2015.
- [10] 朱东飞,洪婷. 城市轨道交通车地通信综合承载系统(LTE-M)性能测试与分析[J]. 城市轨道交通研究,2017(5):171.
ZHU Dongfei, HONG Ting. Test and analysis of integrated service capacity for train-ground communication based on metro LTE-M system[J]. Urban Mass Transit,2017(5):171.
- [11] 顾蔡君. LTE 技术在中国城市轨道交通车地通信中的应用[J]. 铁路通信信号工程技术,2018(3):51.
GU Caijun. Application of LTE technology in train-ground communication for urban rail transit[J]. Railway Signalling & Communication Engineering,2018(3):51.
- [12] 冯秀涛. 3GPP LTE 国际加密标准 ZUC 算法[J]. 信息安全与通信保密,2011(12):45.
FENG Xiutao. ZUC algorithm:3GPP LTE international encryption standard[J]. Information Security and Communication Privacy,2011(12):45.
- [13] 冯秀涛. 祖冲之序列密码算法[J]. 信息安全研究,2016(11):1028.
FENG Xiutao. The ZUC stream cipher algorithm[J]. Journal of Information Security Research,2016(11):1028.
- [14] 国家密码管理局. 信息安全技术 祖冲之序列密码算法第1部分:算法描述:GB/T 33133.1—2016[S]. 北京:中国标准出版社,2016.
State Cryptography Administration. Information security technology-ZUC stream cipher algorithm—Part 1:algorithm description:GB/T 33133.1—2016[S]. Beijing:China Standard Press,2016.

(收稿日期:2020-03-16)