基于信息备份技术提升城市轨道交通数据单向传输可靠性的设计方法*

许子恒[1]　李王睿[2]　张立东[3]　张菁博[3]

（1. 上海应用技术大学轨道交通学院，201418，上海；2. 华东师范大学软件工程学院，200241，上海；
3. 上海申通地铁集团有限公司技术中心，200233，上海）

摘　要　[目的]为了应对城市轨道交通系统各个子系统间复杂接入带来的潜在安全威胁，中国城市轨道交通协会提出安全生产网和外部服务网间应实施物理安全隔离。既有传输方式下，数据单向传输过程中经常发生丢包、误码等问题，需要寻求新的方法，以提高城市轨道交通数据单向传输的可靠性。[方法]阐述了单向安全隔离系统的传输原理及存在问题，以及单向安全网关内的代理、会话配置的情况。分析了传输异常 3 种类型（代理次序混乱、会话次序混乱及传输超时）的判断方式。提出了基于信息备份的数据传输方法，设定了备份信息的首部格式，制定了基于信息备份技术的数据传输方法检查传输异常的技术流程，并对该方法进行了试验验证。[结果及结论]该方法能够有效解决城市轨道交通数据单向传输可靠性低的问题。

关键词　城市轨道交通；信号系统；数据单向传输；传输可靠性；信息备份

中图分类号　U231.7

DOI：10.16037/j.1007－869x.2024.09.040

A Design Method for Improving the Reliability of Urban Rail Transit One-way Data Transmission Based on Information Backup Technology

XU Ziheng[1], LI Wangrui[2], ZHANG Lidong[3], ZHANG Jingbo[3]

(1. School of Rail Transit, Shanghai Institute of Technology, 201418, Shanghai, China; 2. School of Software Engineering, East China Normal University, 200241, Shanghai, China; 3. Technology Center of Shanghai Shentong Metro Group Co., Ltd., 200233, Shanghai, China)

Abstract　[Objective] In order to deal with the potential security threats caused by the complex connections between various subsystems in urban rail transit system, China Urban Rail Transit Association proposes that physical security isolation should be implemented between the safety production network and the external service network. Under the existing transmission method, problems such as packet loss and bit error often occur during one-way data transmission, and new methods need to be sought to improve the reliability of one-way data transmission in urban rail transit. [Method] The transmission principle and existing problems of the one-way security isolation system, as well as the proxy and session configuration in the one-way security gateway are described. The judgment methods of three types of transmission anomalies (proxy order disorder, session order confusion and transmission timeout) are analyzed. A data transmission method based on information backup is proposed, and the header format of backup information is built. The technical process of checking transmission anomalies by the data transmission method based on information backup technology is formulated, which is verified by experiments. [Result & Conclusion] This method can effectively solve the problem of low reliability of one-way data transmission of urban rail transit.

Key words　urban rail transit; signal system; one-way data transmission; transmission reliability; information backup

为了应对城市轨道交通系统各子系统间复杂接入带来的潜在威胁，GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》第 8.5.2.1 条规定："工业控制系统与企业其他系统之间应划分为 2 个区域，区域间应采用单向隔离技术手段。"为此，中国城市轨道交通协会提出，安全生产网和外部服务网间应实施物理安全隔离。

通常而言，单向安全隔离系统能够防止高性能的网络攻击。单向安全隔离系统只能单向连接，反向连接从物理上被阻断。基于单向安全隔离系统的数据传输方式，限制了 2 台计算机之间沿网络连接的通信，使数据只能沿 1 个方向传输。在数据单

* 上海市科学技术委员会项目（20511106400）

向传输中，由于不能从接收端向发送端发送 ACK（报文到达确认），发送方无法获知数据传输是否成功[1]，因此，数据的传输可靠性是一个大问题。

由于城市轨道交通业务系统的特殊性，安全生产网的数据需要安全、可靠送至服务管理网，服务管理网才能及时执行对应操作，此外，数据应通过会话送至服务管理网域内相应子系统中。为此，部分关键数据的丢包或误码，是数据传输过程中很大的安全隐患。为了解决城市轨道交通业务系统安全生产网和服务管理网之间单向数据传输的可靠性问题，本文提出了一种基于信息备份技术提升城市轨道交通数据单向传输可靠性的设计方法。

1 设计方法

1.1 单向安全隔离系统

图 1 为单向安全隔离系统示意图。单向通信模块由 1 个仅用于发送数据的单向安全网关和 1 个仅用于接收数据的单向安全网关组成。因此，传输双方通常使用 UDP（用户数据包协议）通信，不能使用端到端协议（如 TCP（传输控制协议）等）。然而，UDP 通信并不能保证数据的可靠接收，也无法确保传输的可靠性。

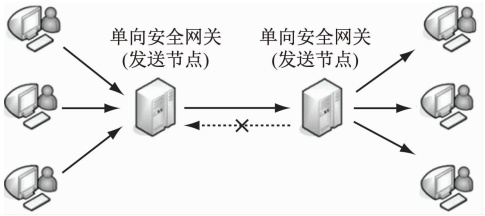


图 1 单向安全隔离系统示意图

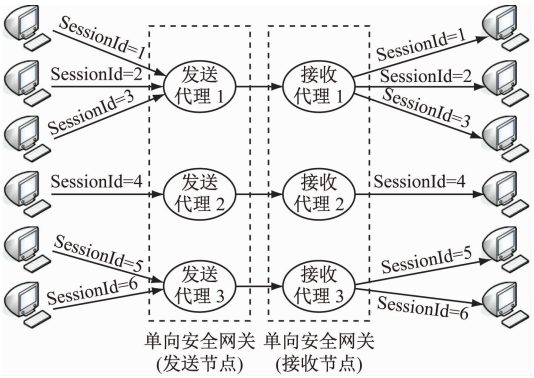
Fig. 1 Schematic diagram of the one-way security isolation system

提高 UDP 通信可靠性，主要有 2 个方法：

1）采取同一个数据包多次传输的方式。只要其中 1 个数据包成功发送至接收方，则此次数据传输是成功的。然而，该方法占用了实际数据信息的数倍带宽。由于大部分数据在传输时不会丢失，该方法会导致大量的网络资源被浪费，很难应用在需要传输大量数据的场景中。

2）采用 FEC（前向纠错）技术。FEC 是一种用于不可靠或嘈杂的通信信道上的数据传输差错控制技术，其中心思想是发送方节点使用预定算法，为即将发送的数据信息添加冗余信息，冗余信息位的值往往可通过原始数据信息位经函数运算后得到。当数据发送错误时，接收节点可以对数据包进行 FEC 解码，通过冗余信息计算出该数据包的真实值。该方法存在的问题是，过多的冗余数据导致发送节点编码和接收节点解码操作时需要占用较多的 CPU（中央处理器）资源，且无法解决流量突发和数据连续丢包等问题。

图 2 为单向安全网关内的代理和会话配置截图。单向安全网关内运行了多个代理。代理是一种中介各种协议的程序，由于城市轨道交通存在各类不同业务的子系统，各子系统运行的协议不尽相同，因此，可能存在如 TCP、UDP、FTP（文件传输协议）和 OPC（工业控制系统通用接口标准）等不同协议的代理。每个代理有一些会话，用于代理和使用同一个协议的不同接收方之间进行数据传输。



注：SessionId—会话 ID（标识号）。

图 2 单向安全网关内的代理和会话配置截图

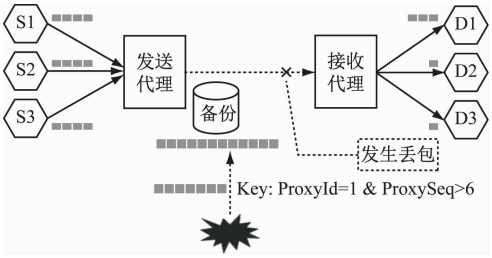
Fig. 2 Screenshot of proxy and session configuration within the one-way security gateway

1.2 传输异常的 3 种情况

接收节点处的代理可以检测到数据传输异常。潜在的传输异常主要分为 3 种情况：代理次序混乱（以下简称“代理失序”）、会话次序混乱（以下简称“会话失序”）和传输超时。一旦发现异常，代理会通过带外通道发出通知。发送节点的管理员终端收到通知后，管理员可能会要求对应的代理执行重传数据报文的请求。

1.2.1 代理失序

接收代理通常会通过代理 ID 和代理序列号来判断是否发生代理失序。图 3 为代理失序判断流程截图，接收代理期待收到代理 ID 号 ProxyId 为 1、代理序列号 ProxySeq 为 6 的数据包，因为前 5 个数据包已正确到达。若此时接收代理收到数据包的 ProxySeq 大于 6，则认为发生了代理失序。



注:S1、S2、S3 为会话发起方;D1、D2、D3 为会话接收方;Key 为判断依据。

图 3　代理失序判断流程截图

Fig. 3　Screenshot of the proxy out-of-order judgment process

1.2.2　会话失序

接收代理通常会通过会话 ID 和会话序列号来判断是否发生会话失序。图 4 为会话失序判断流程截图,接收代理期待收到会话 ID 号 SessionId 为 2、会话序列号 SessionSeq 为 2 的数据包,因为前 1 个数据包已正确到达。若此时接收代理接收到 SessionSeq 大于 2 的数据包,即认为发生了会话失序。

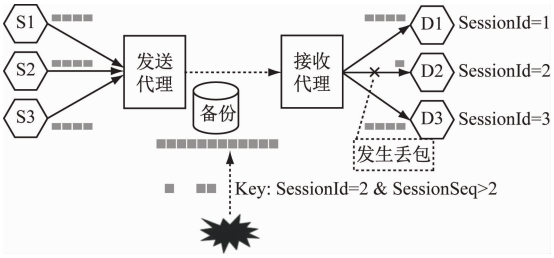


图 4　会话失序判断流程截图

Fig. 4　Screenshot of the session out-of-order judgment process

1.2.3　传输超时

接收代理会通过前 1 个数据包的时间戳(Timestamp)来判断是否发生传输超时。图 5 为传输超时判断流程截图,若接收代理在设定的重传时间内没有收到数据包,即认为发生了传输超时。

1.3　数据重新传输的方案设计

1.3.1　备份信息的首部格式

为了保证单向数据传输的可靠性,本文提出了基于信息备份技术的数据传输方法,并在收到重传请求时进行重传。为了检测上述异常并进行重传,所有数据包均需额外添加具有规定首部格式(见图 6)的备份信息。发送代理通过会话获取原始数据报文,经解析处理后得到数据内容,然后根据单向隔离私有协议将其封装为传输数据报文并存放至备份数据库。备份信息除 Data(数据)、CRC(循环冗余校验)码外,每个代理会被分配 1 个唯一的 ID,备份信息将记录该传输数据报文对应的代理 ID 号(ProxyId),并向每个代理的处理消息按顺序分配代理序列号(ProxySeq)。另外,代理处理消息的时间会被写入时间戳(Timestamp)。在每个代理中,可以有多个会话,用于识别数据源和目的地,每个会话会分配得到 1 个唯一的 ID(SessionId)。会话序列号被分配给通过每个会话的消息(SessionSeq)。

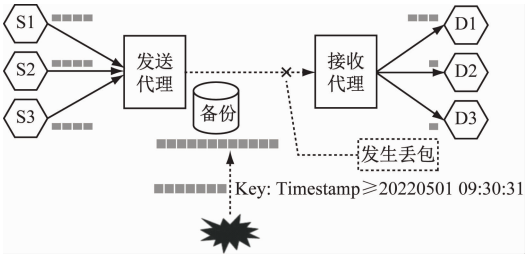


图 5　传输超时判断流程截图

Fig. 5　Screenshot of the transmission timeout judgment process

图 6　备份信息的首部格式

Fig. 6　Header format of backup information

在单向数据传输场景下,发送代理会将相应 ID 值分配给传输信息并进行备份。一旦发生传输错误,发送代理将通过密钥值提取对应的数据并重新传输。

1.3.2　检查数据传输异常的技术流程

图 7 为基于信息备份的数据传输方法检查传输异常的流程。通过 ProxySeq 来检测是否丢包或通过 CRC 来检测数据是否出错。如果数据丢失或出错,则从已收到的信息中提取 ProxyId 和 ProxySeq,并请求重传。如果某个子系统的会话传输失败(即出现数据丢包或出错),则从已收到的信息中提取 SessionId 和 SessionSeq,并请求重传。

传输超时异常并未在图 7 中体现,原因是传输超时的设定场景为没有接收到数据包。该场景下,在接收代理处设定计时器,接收代理每接收到 1 个非末尾数据包,均会启动计时器,传输时间一旦超出限定值,接收代理将自动发出重传请求。

由于数据通路是单向且仅用于传输数据,因此需要引入 1 条额外的数据链路,用于接收端向发送端发送重传请求。为此,本文在发送节点和接收节点处额外引入 1 条旁路的带外通道,并对其配置了本文提出的自动请求重传方案。

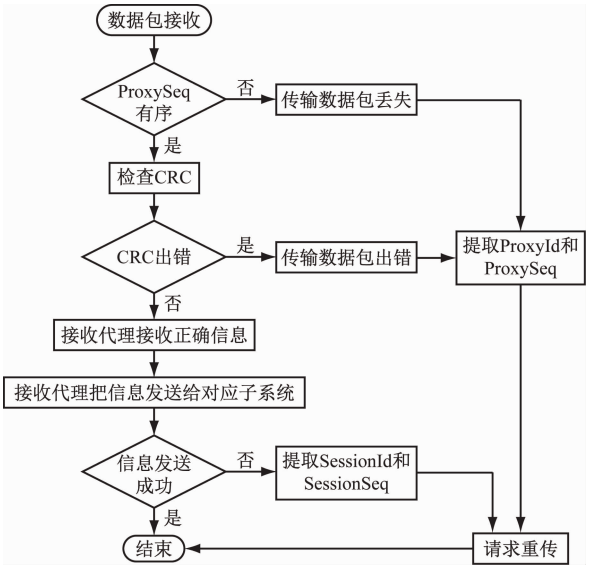


图 7　基于信息备份的数据传输方法检查传输异常的技术流程

Fig. 7　Technical process of checking transmission anomalies using data transmission methods based on information backup

当发送节点接收到 1 个重传请求后，将会检查该请求报文中携带的 ID 信息，以确认提取哪个备份数据包进行重传。如果 ID 信息在备份库中为空，则认为该重传请求出错。

2　试验验证

对上述方法进行试验验证，试验的软硬件配置如下：操作系统为 CentOS 6.8，内核版本为 4.4.43，CPU 型号为 Intel i5-2400，内存为 4 GiB，硬盘型号为 Seagate（内存为 500 GiB），主板为研祥工控主板。传输采用光闸进行数据单向传输。测试数据为 40 万个小文件，每个小文件约为 2 ~ 3 KiB。

由发送节点接收城市轨道交通系统安全生产网域数据，基于 UDP 协议进行传输，并按照上文所述方法对数据包首部格式进行额外封装，通过光闸传输数据。服务管理网接收节点接收光闸传输的数据，按照上文所述方法进行数据校验和重传。

光闸系统分光器的误码率按普通光纤误码率（10^{-11}）计算，传输速率按照峰值传输速率（800 Mibit/s）计算，即：在峰值传输情况下平均 1 000 s 出现 1 个错误码。为了验证本文所提方案的数据传输可靠性，选定传输速度和传输失败次数 2 个指标，分别对常规 UDP 协议、本文所提方法进行对比测试，测试结果如表 1 所示。由表 1 可知：2 种传输方法的传输速度差异不大；使用 UDP 协议进行传输时，容易发生丢包，传输失败次数较多；采用本文所提方法进行传输时，可以通过重传机制保证数据的可靠性，传输失败次数为 0。

表 1　常规 UDP 协议、本文所提方法下传输速度及传输失败次数的对比

Tab. 1　Comparison of transmission speed and number of transmission failures under the conventional UDP protocol and the method proposed in this paper

传输方法	传输次数	传输速度/（Mibit/s）	传输失败次数
常规 UDP 协议	5 000	62.8	21
本文所提方法	5 000	60.9	0

3　结语

本文提出了一种基于信息备份技术提升城市轨道交通数据单向传输可靠性的设计方法。试验表明，该方法能够有效解决既有传输方式下数据单向传输时出现的丢包、误码等问题，显著提高数据传输的成功率。可以应用该方法解决城市轨道交通的安全生产网和服务管理网数据单向传输可靠性低的问题。

参考文献

[1]　邵旭东，蒋海平，张菡. 基于光纤通信技术的数据单向传输可靠性研究[J]. 信息网络安全，2016(10)：76.
SHAO Xudong，JIANG Haiping，ZHANG Han. Research of data one-way transfer reliability based on fiber optic communication technology[J]. Netinfo Security，2016(10)：76.

[2]　蒋梦浩. 基于光纤通信技术的数据单向传输可靠性研究[J]. 数字技术与应用，2018，36(10)：53.
JIANG Menghao. Research on reliability of data one-way transmission based on optical fiber communication technology[J]. Digital Technology & Application，2018，36(10)：53.

[3]　GOPE P，DAS A K，KUMAR N，et al. Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks[J]. IEEE Transactions on Industrial Informatics，2019，15(9)：4957.

· 收稿日期：2022-05-10　修回日期：2022-06-17　出版日期：2024-09-10
Received：2022-05-10　Revised：2022-06-17　Published：2024-09-10
· 通信作者：许子恒，助理工程师，820498977@qq.com