文献标识码：B 文章编号：1003-0492（2020）09-078-04 中图分类号：TP309.7

短报文加密技术在铁路北斗通信中的应用研究

Research on the Application of Short Message Encryption Technology in Beidou Communications of Locomotives

★胡杏（北京鼎合信安科技有限公司，北京 100194）
★龚利，王庆武（中国铁道科学研究院集团有限公司，北京 100084）
★陈志国（北京鼎合信安科技有限公司，北京 100194）

摘要：对北斗短报文通信中所涉及的敏感数据进行加密是确保应用数据安全的必要措施。北斗短报文因自身的传输特点，对其进行加密需要采取特殊的数据加密方法。本文详细阐述了在铁路机车北斗加密通信项目中所采用的短报文加密技术，并论述了该技术方案的科学性和有效性，为类似的工程应用提供了经验参考。

关键词：加密通信；北斗短报文；铁路信息化

Abstract: Encrypting of sensitive data involved in Beidou short message communications is a necessary measure ensuring application system data security. Taking the unique characteristics of Beidou shout message transmission, encrypting short messages requires special data encryption methods. The paper elaborates the short message encryption technologies in Beidou encryption communications programs for locomotives and expounds the scientific nature and effectiveness of this technical scheme so as to provide experience reference for similar engineering applications.

Key words: Encrypted communication; Beidou short message; Railway informatization

1 引言

近年来随着北斗卫星导航系统的快速发展，并即将全面建成全球导航系统，其应用的广度和深度也在不断拓展。北斗短报文通信作为北斗卫星导航系统的重要组成部分，也在各领域得到了广泛应用。北斗短报文通信利用北斗卫星实现天地通信，不受时间、空间的约束，具备全天候、不受自然灾害影响的特点。将北斗短报文通信应用于铁路机车的车地通信，能够充分发挥其自身技术优势，同时也解决了机车远程通信可靠性要求高，网络建设难度大等一系列难题。

但采用北斗短报文实现铁路机车远程通信也存在着数据通信安全问题。因为民用北斗短报文通信采用的是明文数据传输，在机车与地面传输敏感数据过程中，可能会造成数据泄露，严重情况下可能会威胁到列车运行安全。因此，对短报文数据进行加密十分必要，能够有效避免数据安全事故。本文结合中国机车远程监测与诊断系统（CMD系统）中北斗短报文的加密传输应用实践，对短报文的加密和解密方法、密钥管理、加密传输等技术进行了充分研究，并全面总结了相关工程应用经验，对其他类似的北斗短报文通信应用具有较高的参考和借鉴价值。

2 铁路机车北斗短报文通信

2.1 北斗短报文通信方案

CMD系统中机车车载装备实时采集机车位置坐标和运行状态信息，并通过北斗短报文通信，经由卫星通信链路、地面专线传输等通信链路，最终送达CMD系统地面通信服务器，如图1所示。

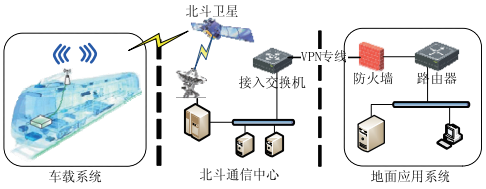

图1 北斗短报文通信方案

通信链路从车载终端开始，机车数据由终端北斗设备发射至北斗卫星；北斗卫星收到短报文后，将数据发送至地面北斗通信中心；北斗通信中心根据短报文发送方进行信息分发，通过用户VPN专线，将机车上传的短报文推送至CMD系统通信服务器。

2.2 方案技术特点

（1）数据实时性要求高

CMD系统根据机车上传的位置和运行状态数据，实现对机车运行情况的远程监测。机车各项运行参数具有较高的时效性，地面监控人员需根据机车的实时参数，分析机车当前的运行状态是否良好，对于异常情况必须立即采取应急处置措施。数据的实时性要求决定了通信链路应该具备较高的传输速率，通信链路中各节点应优化数据处理方案，尽量降低数据处理和传输延时。

（2）通信链路长

机车上传北斗短报文经车载北斗终端发出，到地面通信服务器，须途经四条数据链路传递。首先短报文从北斗终端发送至北斗卫星，再由北斗卫星到北斗地面接收站，由地面接收站经VPN专线到铁路外网DMZ区，再经安全通道发送至位于铁路内网的应用系统通信服务器。整个北斗短报文的通信链路较长，数据转手次数较多，这对于数据传输的时效性和安全性而言，是较大的不利因素。因此短报文的数据封装方式和数据加密方法，都需充分考虑短报文传输的这一特点，以避免因通信链路过长而造成的不利影响。

（3）通信带宽受限

长度限制：民用北斗短报文通信服务规定，单条报文的最大传输字节数为78个半字节。这就极大地限制了机车每次上传报文的信息量，对报文封装格式需进行严格设计，尽量减少不必要字节，提高报文有效信息的占比。

发送频率限制：民用北斗短报文通信服务，一般可用的服务频率为每分钟发送一条。

2.3 短报文加密的主要难点

（1）不变长加密

目前常用对称商用密码算法在对明文加密处理后，密文数据长度会发生变化，以3DES算法为例，即明文长度不是整8字节的情况下，加密后密文长度必须以整8字节的长度出现，也就是L（密文）≥L（明文）。对于北斗短报文通信而言（民用长度78个半字节），若采用3DES算法，则实际使用时，明文数据长度就不能超过72个字节。这将极大限制北斗短报文通信的应用效能。

（2）密钥索引传递

一般对称加密算法需要加解密双方以安全的方式交换密钥，常用的方式是以加密卡ID作为索引。在北斗短报文通信过程中交换密钥有两种方式，要么在短报文中增加密钥索引字段，要么占用一次服务频度来交换密钥索引，两种方式都会占用北斗短报文通信的数据带宽。所以无论采用哪种方式，都会制约北斗短报文通信的应用。

（3）加密北斗终端

现有车载北斗终端是按北斗系统技术标准进行设计生产的，具备北斗RN定位和RD服务功能。要对现有北斗终端进行改造，增加短报文加密功能，需要对终端进行硬件和软件改造。改造不能影响现有北斗应用功能，并能较好地实现短报文加密功能，整体升级难度较大。

3 短报文加密方案

3.1 总体加密方案

机车北斗短报文加密方案是对CMD系统现有北斗通信进行升级改造，通过在车载端和地面应用系统端增加加密方案，实现短报文的加密传输。通过加密改造，实现了北斗短报文的密文传输，确保了机车数据的传输安全。

机车车载端北斗加密模组使用加密卡，将机车实时运行数据加密成密文，通过北斗短报文方式传回地面。数据密钥存储在安全加密卡中，数据明文也由加密卡提供的加密算法进行加密，密钥和加密过程都封装在加密卡中，具备极高的安全等级。如图2所示。

加密，密钥和加密过程都封装在加密卡中，具备极高的安全等级。如图2所示。

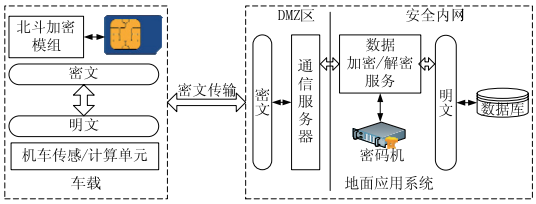

图 2 总体加密方案 图2 总体加密方案

地面应用系统网络根据安全等级划分为DMZ区和安全内网，两区之间通过安全网闸进行隔离。系统通信服务器位于DMZ区负责接收北斗短报文密文，并通过安全传输通道发送至内网。数据加密/解密服务运行在安全内网，解密服务通过网络接口，将密文数据发送至密码机进行解密，并将返回的明文发送给应用系统最终存库。服务器端数据密钥和加解密算法均封装在安全密码机中，能够有效保护密码和加密方法的安全。

3.2 加解密算法

算法以商用加密算法为基础，重新设计算法计算步骤，实现加解密后不改变数据长度。能够满足北斗短报文通信对数据长度的严格要求，有效解决了短报文加密的技术难题。

（1）加密方法

· 检测待加密明文数据P的数据位长度L（P）；如果L（P）＜Dbit，则进行第四步，否则进行第二、三步；

· 将明文数据P划分成若干Dbit的数据块，分别标记为P_1、P_2、…P_{n-1}、P_n，即$P=P_1P_2\cdots P_n$；

· 采用对称加密算法对P_1、$P_2\cdots P_{n-1}$数据块分别进行加密，得到对应的密文C_1、$C_2\cdots C_{n-2}$、C_{n-1}。如果L（P_n）=Dbit，则采用对称加密算法对P_n数据块进行加密得到密文C_n；如果L（P_n）≠Dbit，则从数据块Ci的设定位置a处截取D-L（P_n）bit的加密数据P'i补在数据块P_n的位置b处组成Dbit的新数据P'n，截取后的Ci记为C'_i。然后采用对称加密算法对P'_n数据块进行加密得到密文C_n，最后得到该明文数据P的密文$C=C_1C_2\cdots C'_i\cdots C_n$；$i=_1,2\cdots_{n-1}$，D为对称加密算法的分组长度；

从明文数据P最低位后面开始依次补1位bit“1”和若干位bit“0”，直至补足Dbit，生成新的明文数据P'，即L（P'_1）=Dbit；然后对P'1取反，生成P'_2=!P'_1；最后采用对称加密算法对P'_1、P'_2加密，得到该明文数据P的密文C。

进一步的，第二步中，将明文数据P按从高位至低位或从低位到高位划分成若干Dbit的数据块。

进一步的，该设定位置a为数据块Ci的最低位开始的连续或设定间隔的D-L（Pn）bit数据。

进一步的，该设定位置a为数据块C_i的最高位开始的连续或设定间隔的D-L（P_n）bit数据。

进一步的，该设定位置a为数据块Ci中连续或设定间隔的D-L（P_n）bit数据。

进一步的，该位置b为数据块P_n的高位或低位或中间设定位置。

（2）解密方法

· 检测待解密密文C的数据位长度L（C），如果L（C）=2Dbit，则进行第四步，否则进行第二、三步；

· 将密文C划分成若干Dbit的数据块，分别标记为C_1、C_2、…C_{n-1}、C_n，即$C=C_1C_2\cdots C_n$；

· 如果L（C_n）=Dbit，将采用对称解密算法对C_1、$C_2\cdots C_n$数据块进行解密，得到明文数据$P=P_1P_2\cdots P_n$；如果L（C_n）≠Dbit，则从数据块C_i中的设定位置a处截取D-L（C_n）bit的加密数据C'_i补在数据块C_n的位置b处组成Dbit的新数据C'_n，截取后的Ci记为C''_i，然后采用对称解密算法对C'_n解密得到明文P''_n，从数据块P"n的位置b处截取D-L（C_n）bit的明文数据P'_n补在数据块C''_i的设定位置a处，组成新的Dbit密文数据C_i，截取后的数据块P'' $_n$记为P_n；采用对称解密算法对C_1、$C_2\cdots C_{n-1}$数据块进行解密，得到明文数据$P=P_1P_2\cdots P_{n-1}$，最后得到明文数据$P=P_1P_2\cdots P_{n-1}P_n$；其中，i=1,2…n-1，D为对称解密算法的分组长度；

· 将密文C划分为Dbit的两数据块C_1、C_2；然后采用对称解密算法对C_1、C_2解密分别得到对应的明文P_1、P_2，将P2取反，生成P'_2=!P_2，如果$P_1=P'_2$，则从P1最低位依次向高位判断，直至出现bit”1”为止，该bit”1”之前至最高位为明文P，否则解密后的明文$P=P_1P_2$。

进一步的，将密文C按从高位至低位或从低位到高位划分成若干Dbit的数据块。

进一步的，该设定位置a为数据块最低位开始的连续或设定间隔的D-L（P_n）bit数据；或者该设定位置a为数据块最高位开始的连续或设定间隔的D-L（P_n）bit数据；或者该设定位置a为数据块中连续或设定间隔的D-L（P_n）bit数据。

进一步的，该位置b为数据块的高位D-L（P_n）bit数据或低位D-L（P_n）bit数据或中间设定位置的D-L（P_n）bit数据。

3.3 密钥管理

短报文加密方案采用对称加密算法，密钥体系分主级密钥、应用密钥和终端密钥三级密钥。主级密钥为企业级密钥，由企业两位主管领导分别在密码机中输入一组密钥分量生成。应用密钥为应用系统核心密钥，由企业级密钥衍生生成。终端密钥是终端设备使用的一组密钥，终端密钥由应用密钥根据密钥索引生成。主级密钥和应用密钥存储在安全密码机中，密码机提供数据加密和解密、密钥衍生计算等接口，外部不能直接访问存储的密钥。

北斗加密模组终端密钥以北斗卡号为密钥索引，采用不同的衍生算法生成主控密钥、主服务密钥、实时数据加密密钥和基本信息维护密钥。终端密钥采用SAM加密卡进行存储和运输，北斗加密模组利用加密卡进行短报文加密和解密计算。

4 方案实施过程分析

短报文加密方案在项目应用中，所遇到的项目可能是新建项目或者是加密改造项目，而一般对已有项目进行

加密升级改造的项目居多。针对不同的项目类型，短报文加密方案在实施过程中会面临不同的技术和管理问题。

4.1 项目实施步骤

（1）启动与规划

项目管理者拟定项目愿景和目标，并根据项目的实际情况进行可行性研究。项目启动后各软硬件子系统负责人研究子系统与加密通信的关系，给出子系统改造的技术方案。项目管理者需要协调各方的技术方案和改造任务，并最终完成改造项目的整体规划，确定各阶段的任务目标及完成时间。

（2）产品研制

软件及硬件产品设计与研制是整个加密改造项目的关键阶段，产品设计应以现有系统为基础，尽量降低对运行系统的影响。

车载终端部分将以北斗加密模组替代现有北斗模组，北斗加密模组保留原有的设备软硬件接口，原有车载终端无需改动。增加加密卡作为加密模组的加密单元，既确保了加密的安全性，又保证了新增功能的独立性。

地面应用系统部分在原有数据链路中，插入数据加密/解密服务，与原有数据链路保持了无缝连接。在密文数据接入端，直接处理通信服务器接收的密文数据并解密为明文提供给后续应用。密码机则选用成熟的商用密码机，并通过网络接口提供服务。

（3）试运行与正式上线

在系统加密改造完成实验室研制及测试阶段后，首先需要进行上车试运行阶段，以验证加密设备的设计和生产质量是否满足要求。试运行期间根据实验计划，需选择一定数量的机车，安装经加密改造的车载终端。地面应用部分搭建一套经加密改造的试运行系统，试运行系统具备完整的系统功能，在试运行期间需对所有功能进行功能和性能测试。

正式上线阶段首先需完成地面应用系统的切换，应用系统加/解密服务采用了多服务互为备份机制，能够在不停机情况下进行升级，从而保证了系统在运行期间顺利更新到加密通信版本。施工方安装短报文加密通信车载终端，系统人员对机车运行数据进行跟踪。

4.2 成功实施的关键因素

短报文加密通信的实际应用有自身的特点和实施难度，能否在项目中成功实施短报文加密由项目相关方人员、技术条件和管理因素决定。成功实施的关键因素主要有以下几个方面：

（1）项目管理者决心：项目管理者的主观意志决定了项目能够获取的资源，对短报文加密改造起着决定性的推动作用。

（2）降低对现有系统的变动：短报文加密改造内容应该以现有项目为基础，充分利用现有系统接口，最大限度降低对现有系统的改动。

（3）加密设备可用性：加密设备应该选用成熟可靠的技术和设备，对设计的实用性进行充分论证，产品生产过程中应确保产品质量的可靠性。

5 结束语

北斗短报文通信已经应用到国内很多重要的生产生活领域，涉及到很多行业的重要敏感数据。短报文通信数据的安全性，也应该引起数据管理者的足够重视。推动短报文通信的数据加密，有利于北斗短报文应用的进一步发展，避免造成严重的生产安全事故。AP

作者简介：

胡　杏（1983-），男，湖北黄冈人，工程师，硕士，现任北京鼎合信安科技有限公司技术部技术总监，研究方向为信息管理与信息系统。

龚　利（1975-），男，北京人，高级工程师，博士，现就职于中国铁道科学研究院集团有限公司电子计算技术研究所，研究方向为机务信息化与机务安全监测。

王庆武（1963-），男，北京人，正高工，现任中国铁道科学研究院集团有限公司货运事业部总经理，研究方向为铁路信息化。

陈志国（1969-），男，北京人，学士，现任北京鼎合信安科技有限公司总经理，研究方向为工业电气自动化。

参考文献：

[1] 申瑞源, 龚利. 中国机车远程监测与诊断系统（CMD系统）总体方案研究[J]. 中国铁路, 2017, (3) : 9 - 15.

[2] 刘晗. 基于北斗全球卫星的短报文通信业务[C]. 第十五届卫星通信学术年会论文集, 2019.

[3] 陈志国. 一种短报文通信的加解密方法: 中国, ZL 2016 1 0322745.9[P]. 2019 - 04 - 30.

[4] 王亚民. 北斗卫星导航系统在铁路同步网的应用[J]. 中国铁路, 2013, (4) : 4 - 7.