国产加密技术在轨道交通信号系统中的应用

钱 蔚 徐 烨

（卡斯柯信号有限公司，200071，上海//第一作者，高级工程师）

摘 要 城市轨道交通信号系统的车地无线通信，其传输的物理介质存在于开放的空间范围内，具有一定的非授权接入风险，需符合 EN 50159-2—2001 中所规定的要求。目前车地无线的通信层普遍采用的加密算法，属于国际标准加密算法；而在车地无线通信中传输的应用信息都是与列车运行控制相关的信息，目前尚未应用密码技术。国产加密技术符合我国在重点行业中采用国产密码算法的趋势，有利于保护轨道交通数据安全，尤其在无人驾驶轨道交通系统中，可实现车地无线通信的高安全性和高可靠性。

关键词 轨道交通；信号系统；车地通信；信息安全；国产加密技术

中图分类号 U231.7

DOI：10.16037/j.1007-869x.2019.10.034

Application of Chinese Encryption Technology in Urban Rail Transit Signal System

QIAN Wei, XU Ye

Abstract The train-to-track wireless communication of urban rail transit signal system faces with unauthorized access risks, because the physical medium of signal transmission exists in the open space, that is required by the specified clauses in EN 50159-2—2001. At present, the encryption algorithm commonly used on the train-to-track wireless communication level belongs to the international standard encryption algorithm, and the application messages transmitted are all the information related to train running control, but no cryptography technology has been adopted yet. The Chinese encryption technology discussed in this paper is in line with the trend of encryption algorithm application in key Chinese industries, which is conducive to rail transit data security protection, especially applicable to the driverless system with high security and high reliability in train-to-track wireless communication.

Key words rail transit; signaling; train-track communication; security; Chinese encryption

Author's address CASCO Signal Ltd., 200071, Shanghai, China

2017 年 6 月 1 日起开始实施的《网络安全法》中，交通领域已被列为关键信息基础设施，在网络安全等级保护制度基础上，予以重点保护。城市轨道交通系统的运营安全、运行速度、运送能力和运行效率都与其信号系统密切相关。信号系统车地传输的数据，如列车信息、车辆信息、控制指令等，在信息传输过程中容易被有目的地拦截和窃取。特别是在轨道交通无人驾驶线路中，如果车地通信数据被不法分子所利用，后果将不堪设想。因而，利用密码技术来保证轨道交通信号系统车地无线通信的安全性尤为重要。

1 信号系统网络安全风险分析

在城市轨道交通基于通信的列车控制（CBTC）系统中，安全通信需求存在于地面安全网络和车地无线安全网络中。

信号系统的地面安全网络因接入的设备均为有限数量的已知安全设备，且通信介质和拓扑结构固定，不存在非授权接入情况，属于封闭式网络，其安全通信标准符合 EN 50159-1—2001 中第 6 章“安全规程要求”所规定的内容。

信号系统的车地无线安全网络因其传输的物理介质存在于开放的空间范围内，具有一定的非授权接入风险，因此属于开放式网络，其安全通信标准符合 EN 50159-2—2001 中第 6 章“防护要求”所规定的内容。

对于车地无线通信，信号系统在应用层采用的安全通信协议（如 RSSP-I 和 RSSP-II 标准协议）设置了多种防护措施，用以抵御重复、删除、插入、重排序、损坏、延时的出现，确保功能安全，使信号系统达到安全完整性等级 4 级（SIL4）的要求。

在轨道交通无人驾驶系统中，列车上不配备司机，其运行控制信息和指令都由列车与轨旁通过车地双向无线通信传递，主要内容包括：列车移动授权、列车位置信息、列车运行命令、临时限速命令

等。在开放网络中如出现恶意攻击,特别是当不法分子通过使用网络抓包工具长期嗅探或相关行业人员获知信号系统的既有安全通信协议格式时,则可以通过伪装的方式给列车发送错误的运行控制信息和指令,从而产生难以预计的后果。

在 EN 50159-2—2001 中,对于轨道交通网络中伪装的威胁,其评价定义为威胁可被忽略,推荐了经典的且经过良好测试的算法,采用密码技术对伪装进行有效防护,但这些算法在工程上并无实际应用。在车地无线通信网络层面,无论是采用 2.4 G 无线(Wi-Fi)还是以 LTE(长期演进)技术标准,所使用的加密方式主要有有线等效保密(WEP)协议、临时密钥完整性协议(TKIP)、高级加密标准(AES)等。密码算法是保障信息安全的核心技术,其核心领域长期以来都是沿用国际通用的密码算法体系及相关标准,并不属于自主可控的算法。

随着密码破译技术的发展和计算机运算水平的提高,一些国际算法已经无法满足当今数据加密安全性的要求,比如 WEP 加密,用来产生密钥的方法具有可预测性,即使是一个中等技术水平的无线黑客也可以在 2~3 min 内迅速地破解;56 位的 DES 算法在枚举破解下的安全性也变得十分脆弱。

2　国产密码算法介绍

国产密码算法是我国自主研制实现的密码算法,具有较高的安全性,得到国家密码管理局认可并予以推广。在国家重点行业中采用国产密码算法已逐渐成为一种趋势。这对于维护国家主权安全、维护客户利益、保护数据安全、防止各种高科技犯罪,以及推动我国信息安全产业的发展等方面,均具有十分重要的意义。

2.1　祖冲之算法

祖冲之算法集是我国自主设计的加密和完整性算法,包括祖冲之算法、加密算法 128-EEA3 和完整性算法 128-EIA3,已经被国际组织推荐为第 4 代移动通信技术(4G)无线通信的第三套国际加密和完整性标准的候选算法。祖冲之密码算法为流密码,其密钥长度不小于 128 bit,其初始化向量的长度不小于 128 bit。祖冲之密码算法的安全强度不低于国际同类密码算法标准,能够抵抗常见的各种密码学攻击,特别是代数攻击、快速相关攻击等。

2.2　商密 1 号(SM1)算法

SM1 算法是由国家密码管理局编制的一种商用密码分组标准对称算法。该算法是国家密码管理部门审批的 SM1 分组密码算法 ,分组长度和密钥长度都为 128 bit,算法安全保密强度及相关软硬件实现性能与 AES 相当。该算法不公开,仅封装在芯片中,目前已广泛应用于我国电子政务、电子商务及国民经济等各个重要领域。

2.3　商密 2 号(SM2)算法

SM2 算法是国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法。该算法采用椭圆曲线密码机制,但在签名、密钥交换方面有别于其他国际标准,采取了更为安全的机制。

2.4　商密 3 号(SM3)算法

SM3 密码杂凑(哈希、散列)算法给出了杂凑函数算法的计算方法和计算步骤,并给出了运算示例。此算法适用于商用密码应用中的数字签名和验证,消息认证码的生成、验证,以及随机数的生成,可满足多种密码应用的安全需求。

3　国产加密技术在轨道交通中的应用

如图 1 所示,目前主流的城市轨道交通信号系统大多采用 CBTC 信号系统,涉及车地无线通信的应用层设备由车载子系统、区域控制器(ZC)和线路控制器(LC)子系统、列车自动监控(ATS)子系统组成,网络通信层设备为数据通信(DCS)子系统。本文所述的应用方案是:在既有 CBTC 信号系统架构基础上,增加公钥基础设施(PKI)/证书颁发机构(CA)服务器(含信息安全认证管理系统)和硬件加密机;在应用层设备上增加国产加密安全芯片。

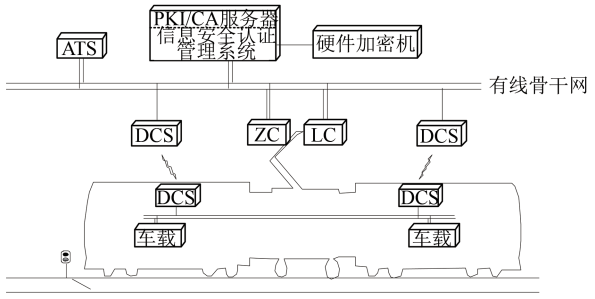

图 1　应用了国产加密技术的 CBTC 系统结构

具体分析如下:

1) PKI/CA 服务器。是身份认证和数字证书的基础,包含 CA 认证中心、数字证书(RA)注册中心,支持 SM2 算法,支持 X.509V3 证书格式;主要提供用户信息注册、证书签发、证书更新、证书恢复、证书废除、证书重发、证书吊销列表(CRL)及

CA 证书下载等功能。

2）信息安全认证管理系统。包括证书管理、认证和应用接口，为国密安全芯片提供证书灌装的应用接口；配合 CA 实现证书注销列表（CRL 列表）的更新；为信息安全接入系统提供 CRL 列表的在线和离线认证；通过加密卡认证身份实现不同用户间的分权管理。

3）硬件加密机。用来生成随机数。采用硬件噪声源所生成的随机数是真随机，不存在重复的可能性。

4）应用设备。即信息安全接入系统，基于国密安全芯片，支持 SM1、SM2、SM3 等商用密码算法；实现通信双方的双向认证；建立安全通信链路，保证信息传输的机密性、完整性和不可抵赖性。

3.1 在网络层的技术应用

以 LTE 网络通信为例，通过在现有 LTE 网络架构和硬件产品上进行升级和配置，采用国密的祖冲之算法在 LTE 网络上针对控制数据和用户数据分别实施加密和完整性保护，把原有的 LTE 网络加密核心算法——欧洲发布的改进型流序列算法（SNOW 3G）或美国国家标准技术研究所发布的高级加密标准算法（AES）替换为祖冲之算法。

1）针对车载终端与控制中心核心网之间的控制数据，采用加密算法 128-EEA3 进行加密处理，采用完整性算法 128-EIA3 实现完整性保护。具体部署位置在车载终端上和控制中心的核心网上。

2）针对车载终端与车站基带单元之间的用户数据，采用加密算法 128-EEA3 进行加密处理。具体部署位置在车载终端上和车站的基带单元上。

通过上述多层次、多阶段的加密和完整性保护，可以实现控制数据和用户数据的信息安全可靠传输。

如图 2 所示，对比开放系统互联（OSI）网络参考模型，LTE 网络通信应用了祖冲之算法后，对 OSI1 至 OSI4 四个层级的数据通信进行了加密，保护车载应用设备与轨旁应用设备之间通过无线传输的数据安全。

3.2 在应用层的技术应用

在网络层 LTE 加密的基础上，对应用层设备 ZC/LC、车载和 ATS 设备上集成国产加密安全芯片，实现 ZC 与车载、LC 与车载、ATS 与车载之间的应用层数据加密，进一步增强数据通信的安全性。此外，可使用国密 SM2 算法实现身份认证和会话密钥协商，使用国密 SM1 算法对数据报文进行加密，使用国密 SM3 算法实现数据的完整性校验。

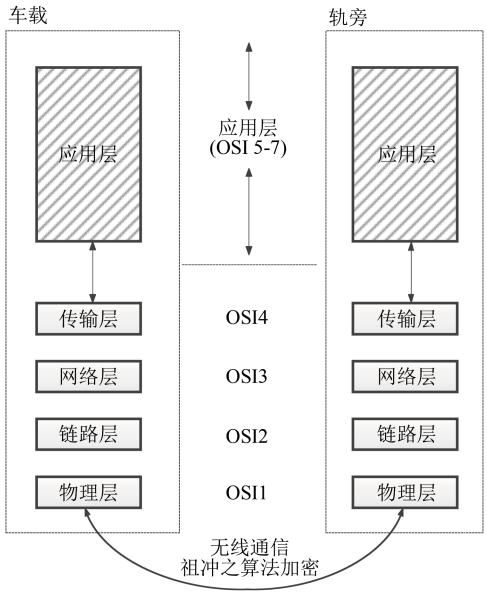

图 2　轨道交通信号系统车地通信网络层加密示意图

整个通信过程分为证书灌装阶段、身份认证阶段、会话密钥协商阶段和数据通信阶段。应用层加密和解密流程如图 3 所示。其中，会话密钥存储于国密安全芯片中，可以根据应用需要定期更新会话密钥。

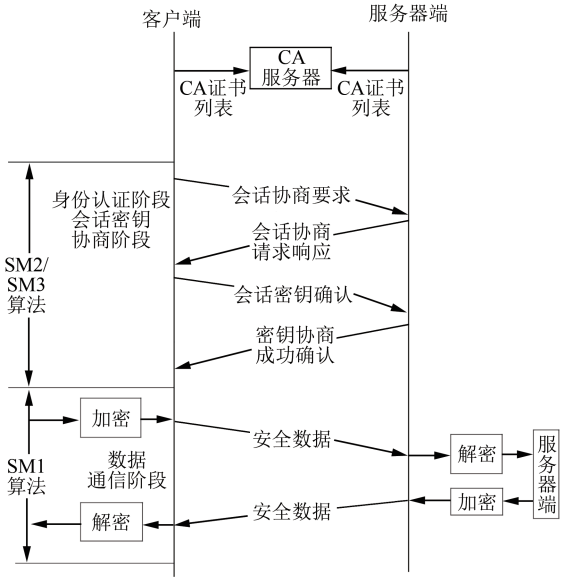

图 3　轨道交通信号系统应用层加密和解密流程示意图

如图 4 所示，对比 OSI 网络参考模型，加密层位于应用层的最底层，包含应用数据逻辑层、安全层、信号层和冗余层在内的全部数据在车地传输时都将采用 SM1 算法进行数据加密，保证应用层数据的

机密性。数据加密的会话密钥通过 SM2 算法协商获得，采用 SM3 算法保证数据的完整性。

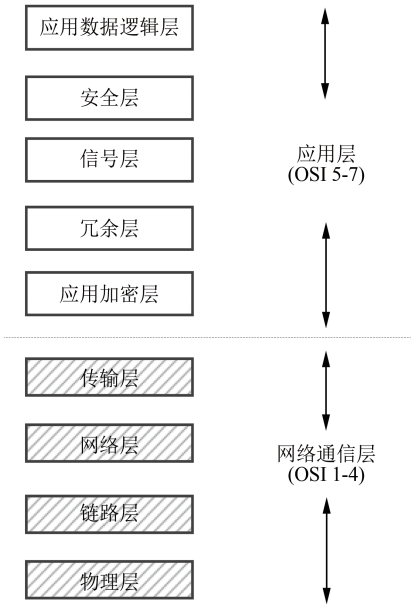

图 4　轨道交通信号系统车地通信应用层加密示意图

在没有应用加密技术前，可以在应用层设备上通过网络抓包工具获得明文数据。如图 5 所示，通过对数据格式的解析，能获得列车位置报告，包含列车运行的方向以及列车在线路上的位置等信息。

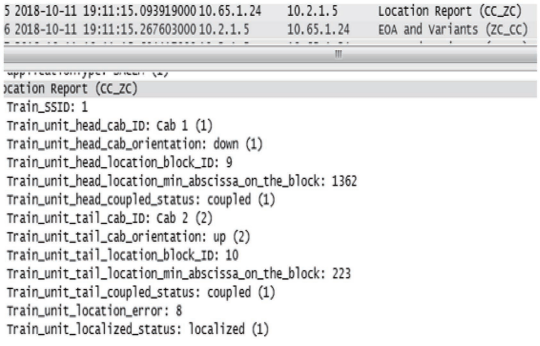

图 5　应用数据-加密前信息截图

如图 6 所示，应用了加密技术后，抓包获得的应用数据为密文，此数据无法进行识别。入侵者即使截获数据也无法读取有价值的信息。由于入侵者无法获得会话密钥，所以无法对数据包进行解密、篡改等操作，从而保护了车地无线通信的数据安全。

4　结语

本文将国产加密技术应用到轨道交通信号系统中，具有如下优点：

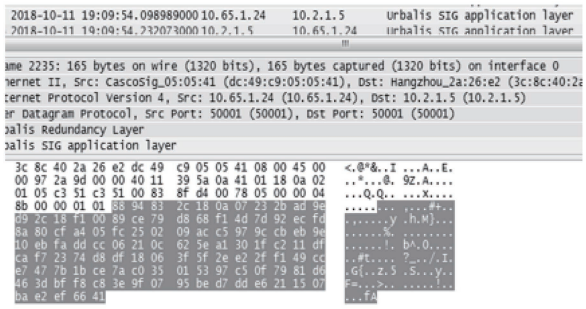

图 6　应用数据-加密后信息截图

1）在信号系统车地无线通信的端到端应用层设备中应用数据加密技术，可提升车地无线通信的信息安全水平，保障信号系统的安全性。

2）基于可信计算技术原理和国产安全芯片、国产密码算法支撑，可充分应用 SM1/SM2/SM3 算法。

3）应用层方案包括证书签发、身份认证、密钥管理、数据加解密、信息完整性一体化等。

4）采用密钥动态协商机制，提高了信息的安全性，避免设备的单点故障，在 PKI/CA 服务器故障情况下不影响信号系统的正常运行。

5）最大限度地保持了轨道交通信号系统的既有架构，其系统功能和功能安全等级也未受影响。

国产密码算法的推出和应用推广，不仅符合国际密码算法的发展趋势，也有助于实现核心技术的自主可控。国产密码算法的公开，有助于国产密码算法及相关产品的国际化。

参考文献

[1] 王绍杰，柯皓仁，卢凯.CTCS-3 级列车控制系统信息安全防护策略浅析[J].信息网络安全，2016(增刊 1)：1.

[2] 王斯梁.列控系统密码应用研究[J].信息安全与通信保密，2016(4)：84.

[3] 陈登科.城市轨道交通信号系统网络安全分析[J].铁路通信信号工程技术，2012，9(5)：41.

[4] 魏珊珊，韩庆敏，郭肖旺，等.基于国密算法的 PKI 在工控系统中的应用研究[J].计算机与现代化，2018(11)：1.

[5] 石军.城市轨道交通信号系统网络传输安全加密机制讨论[J].科技信息，2013(6)：296.

[6] 陈嘉怡，燕飞.城市轨道交通信号系统信息安全风险辨识[J].都市快轨交通，2018，31(2)：119.

（收稿日期：2019-06-07）