DOI：10.13890/j.issn.1000-128X.2024.01.100

面向列车通信网络的轻量化加密方案

唐　军，葛强华，邹智荣，陈　勃，唐　品
（中车株洲电力机车研究所有限公司，湖南 株洲 412001）

摘　要：随着无线通信技术的广泛应用，列车通信网络面临的网络安全风险随之增加。数据加密是应对网络安全风险的重要手段，但也需要额外消耗处理器的计算资源。列车通信网络主机都是由嵌入式设备组成，计算资源有限。文章提出了一种面向列车通信网络的轻量化加密方案，该加密方案在传统通信加密方案上提出了一种密钥协商流程，大幅降低密钥管理硬件要求和计算量，达到在列车通信网络轻量化加密，满足通信数据真实性、完整性、保密性要求。经过试验验证，该方案的密钥协商用时约为传统SM2+SM3+SM4通信加密方案的31.9%，设备CPU负荷约为其35.8%。

关键词：列车通信网络；数据加密；轻量化；密钥协商

中图分类号：TP311.1；TP393　　**文献标识码：**A　　**文章编号：**1000-128X（2024）01-0122-07

0　引言

随着信息技术飞速发展，数字化、信息化和智能化已成为轨道交通领域发展的大趋势。伴随着无线通信技术的广泛应用，轨道交通车载设备的信息安全问题也日趋复杂和严峻，一旦有不法分子入侵，就有可能对列车数据进行窃听、阻断、篡改等攻击，从而对列车行车安全造成极大影响[1]。采用数据加密技术可以有效保证列车数据的安全性和可靠性，在通信数据加密场景，通常采用基于PKI体系[2]的传统通信加密方案，使用到的密码算法主要包括高级加密标准[3]（简称AES）、Rivest-Shamir-Adleman密码系统[4]（简称RSA）、安全散列算法[5]（简称SHA）等，这些算法主要由国外的科研机构提出。随着网络安全上升到国家安全战略，近年来国密算法得到大量研究和应用，包括SM2椭圆曲线公钥密码算法[6]（简称SM2）、SM3杂凑算法[7]（简称SM3）、SM4分组密码算法[8]（简称SM4）等。

为减少轨道交通列车数据面临的网络安全攻击风险，提高列车运行安全性，本文提出一种面向列车通信网络的轻量化加密方案。

1　列车通信网络架构

列车通信网络（Train Communication Network, TCN）主要实现车辆控制、故障诊断、数据采集记录、状态显示和通信管理等功能，被誉为列车的“大脑和神经系统”。当前TCN主要采用列车骨干网络(Ethernet Train Backbone, ETB)和编组网络(Ethernet Consist Network, ECN)架构[9]，如图1所示。

TCN主要由通信设备和终端设备组成。其中通信设备包括骨干网交换机、编组网交换机以及车地通信网关(Mobile Communication Gateway, MCG)。ECN通过MCG实现列车与地面数据的传输，非法设备可能通过MCG入侵列车通信网络，导致列车内部网络传输的数据面临泄露、伪造风险。

列车通信网络的终端设备主要包括列车主控单元(Central Control Unit, CCU)、牵引控制单元(Traction Control Unit, TCU)以及人机交互单元(Human-Machine Interface, HMI)等[10]。这些终端设备采用嵌入式软硬件设计，具备很强的实时性要求，根据指令的类别，通

通信作者：葛强华（1999—），男，主要从事列车网络安全加密技术方面的研究；E-mail: geqh@csrzic.com
引用格式：唐军, 葛强华, 邹智荣, 等. 面向列车通信网络的轻量化加密方案[J]. 机车电传动, 2024(1): 122-128.DOI:10.13890/j.issn.1000-128X.2024.01.100.
Citation：TANG Jun, GE Qianghua, ZOU Zhirong, et al. Lightweight encryption scheme for train communication network[J]. Electric drive for locomotives, 2024(1): 122-128.DOI:10.13890/j.issn.1000-128X.2024.01.100.

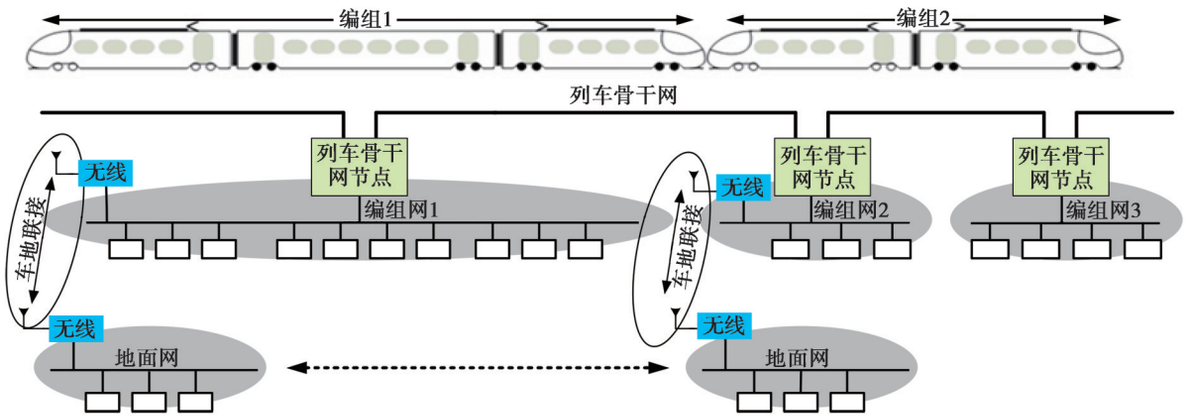


图1　ETB/ECN架构

Fig. 1　ETB/ECN framework

常需要在10~100 ms内完成控制指令的传达和执行。正常情况下列车设备上电启动需要在30 s内完成。

列车通信网络强调稳定性和可靠性，终端设备使用嵌入式系统CPU，由于功耗和运行环境限制，计算能力有限，见表1。因此，在加密算法的选取上需要重点考虑设备实的时性和计算资源消耗。

表1　嵌入式系统CPU计算性能

Table 1　CPU computing performance for embedded systems

CPU型号	MPC5200	MPC5125	MPC8349	P1011
主频/MHz	132	596	333	800

2　传统通信加密方案分析

2.1　加密算法分析

加密算法主要包括对称加密、非对称加密和散列3类[11]。

对称加密采用单一密钥系统进行数据加密，该密钥同时具备加密和解密功能，通信双方共同持有该密钥，数据安全性完全取决于密钥安全性。对称加密具有计算简单高效，密钥长度短，适合多次加密大批量数据等优点，但存在密钥安全管理难度大的问题。在进行安全通信前，预先通过信道共享密钥，需要保证传输过程密钥保密、真实、完整。在某些场景下，很难保证甚至无法保证信道安全，往往需要与其他加密策略组合使用，这大幅增加了系统负担和通信难度。

非对称加密使用公钥、私钥两种密钥，通信双方各自拥有一对公私钥对，其中公钥向外界公开，私钥由自身秘密存储。在通信过程中，双方仅需要将公钥进行传输，验证公钥来源是否正确，无须将私钥进行传输。非对称加密算法相较而言，具有密钥安全性高，密钥管理简单，可实现数据签名和数字证书多种需求的优点。由于非对称加密算法通常采用数字证书方式实现公钥共享，公钥证书的安全性决定于通信双方身份是否真实可靠，往往配套使用公钥基础设施（Public-key infrastructure, PKI）确保公钥证书的合法性和真实性，PKI涉及诸多组件，如证书认证中心（Certification Authority,CA）、注册机构（Registration Authority,RA）、密钥管理系统（Key Management System,KMS）等[12]。

散列算法具有正向快速、逆向困难、输入敏感、冲突避免四大特性[13]。正向快速指给定明文和散列算法，在有限时间和资源内能计算出散列值；逆向困难指给定散列值，在有限时间内基本不可能逆推出明文；输入敏感指原始输入信息即使只修改1位，输出的散列值也大为不同；冲突避免指不同内容的明文很难计算出同一散列值。通信时使用散列算法计算出通信数据散列值，通过比较接收的散列值与计算数据得到的散列值，可以保证通信数据的完整性。表2为常见的对称

表2　常用对称、非对称、散列算法特点

Table 2　Characteristics of common symmetric, asymmetric, and hash algorithms

对比项目	对称加密算法		非对称加密算法		散列算法	
	AES	SM4	RSA	SM2	SHA256	SM3
密钥长度/bit	128/192/256	128	1 024/2 048/3 072	160/224/256	无	无
实现难度	较难，加解密算法不同	较易，加解密算法一致	容易，加解密算法不同，原理简单	难，加解密算法不同，原理复杂	简单	简单
密钥安全强度/bit	128/192/256	128	1 024/2 048/3 072	160/224/256，单位强度远高于RSA	256位散列值	256位散列值
算法安全性	能够抵抗目前已知的攻击	能够抵抗目前已知的攻击	能够抵抗目前已知的攻击	能够抵抗目前已知的攻击	能够抵抗目前已知的攻击	能够抵抗目前已知的攻击
计算速度	快	快	慢	较慢	快	快

加密、非对称加密、散列算法列表。

2.2 应用场景分析

传统通信加密方案结合了以上3种算法，通信双方向PKI设施申请、注册证书等，使用非对称加密算法将用于通信数据加密的对称密钥通过密钥协商过程安全传输到对方，然后通信双方使用对称加密算法将通信数据进行加解密，使用散列算法计算通信数据散列值，通过散列值验证通信数据是否真实合法，达到通信数据的真实性、完整性、保密性要求，具体方案步骤如下[14]：

①通信双方各自生成一组公私钥对，并向CA申请公钥证书。

②通信时，由用户A向用户B请求进行密钥协商，用户A提交自己的公钥证书，请求用户B的公钥证书。

③用户B检查用户A的公钥证书中的公钥、有效期、CA数字签名等信息的有效性，保存用户A的公钥pk_A，发送自身公钥证书到用户A。

④用户A接收到用户B的公钥证书后，检查证书有效性，获得用户B的公钥pk_B，生成一个随机数r_1、pk_B和r_1经过非对称加密算法F生成密文$m_A=F(pk_B,r_1)$，并将其发送到用户B。

⑤用户B用自己的私钥rk_B解密密文m_A，获得随机数r_1，生成新随机数r_2，使用两个随机数和规定加密方式计算生成会话密钥k_E，使用加密计算组件加密值$m_B=F(pk_A,r_2)$并将其发送到用户A。

⑥用户A接收到m_B后使用私钥rk_A解密，获得随机数r_2，将两个随机数加密生成会话密钥k_E。

⑦用户A和用户B使用对称加密密钥k_E进行通信数据加密传输。

在上述方案中，为保证公钥pk_A和pk_B的有效性，需要经过较复杂的运算以及额外的证书认证服务器，对于列车通信网络环境而言，大幅增加系统资源消耗，对系统改造较大，可能带来额外的安全隐患和风险。

3 面向列车通信网络的轻量化加密方案

3.1 方案设计

根据前面1、2章内容，可以发现在TCN上实施传统通信加密方案需要面临诸多困难。因此，本文提出了一种面向列车通信网络的轻量化加密方案。该方案在传统通信加密方案基础上，使用一个随机密钥和初始密钥生成对称加密密钥，随机密钥的作用是用于动态修改加密密钥，提高对称加密密钥可变性，减少入侵者收集大量明密文对进行统计学攻击的可能性，初始密钥的作用是提供通信双方可在未进行通信的情况下计算出同一初始密钥。方案结构如图2所示。

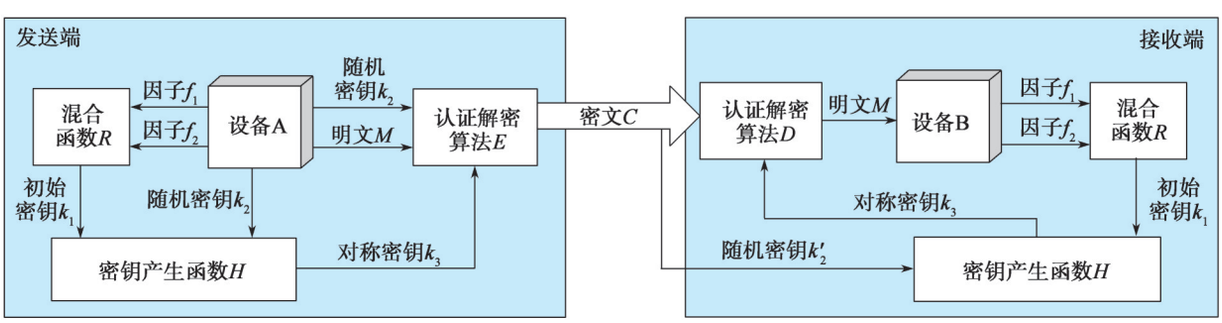


图2 轻量化实时加密方案结构

Fig. 2 Structure of lightweight real-time encryption solution

上述方案中，初始密钥k_1可预先生成，随机密钥k_2可根据通信需要进行动态变化，设备A、B通信需确定混合函数R、密钥产生函数H、认证加密算法E、认证解密算法D，该方案具体步骤如下：

① 设备A、B输入因子f_1和f_2到混合函数R中，生成初始密钥k_1；

② 设备A生成随机密钥k_2，k_2和初始密钥k_1一起进入密钥产生函数H，生成对称密钥$k_3=H(k_1,k_2)$；

③ 设备A使用对称密钥k_3通过认证加密算法E加密明文M和随机密钥k_2，生成密文$C=E(k_2||M,k_3)$，并将随机密钥k_2和密文C拼接生成新密文$C=C||k_2$；

④ 设备B接收密文C，将密文C分离出随机密钥k'_2，k'_2和初始密钥k_1一起输入到密钥产生函数H，生成对称密钥$k_3=H(k_1,k'_2)$，通过认证解密算法D解密密文C，得到明文M和随机密钥k_2，即$(k_2,M)=D(C,k_3)$；

⑤ 设备B将随机密钥k_2与随机密钥k'_2进行校验，若$k_2=k'_2$，则密钥正确，设备B保存明文M，若$k_2\neq k'_2$，则密钥错误，丢弃密文C。

上述方案中，随机密钥k_2与初始密钥k_1之间无任何关系，即密钥k_2任意取值，均不会影响密钥k_1取值，也无法通过任何方法由密钥k_2推算出密钥k_1，反之亦然；因子f_1、f_2为仅在设备A、B之间共同具备的信息，推算f_1、f_2难度极大；密钥产生函数H对输入数据变化极其敏感，任何微小的变化会导致输出结果差别巨大。

3.2 方案安全性及性能分析

从安全性角度分析，本方案使用了3种密钥，仅随机密钥k_2需要通过信道传输，而k_2为动态生成，可抵

抗对k_2的统计学分析攻击，在传输过程中，增加了对k_2的检验，可抵抗对k_2的伪造、篡改攻击。初始密钥k_1与随机密钥k_2无关，且因子f_1、f_2不可推算，因此k_1是安全的，无法仅通过k_2推算出对称密钥k_3，因此k_3也是安全的。由于密钥产生函数H对输入数据变化极其敏感，k_2的微小变化也会导致k_3变化巨大，收集大量密文进行统计学分析k_3也是极为困难的。若每次发送明文均选择一个随机密钥k_2，即k_3每次加密时均不同，则本方案可近似看作“一次一密”加密方案，“一次一密”加密方案中每一个密文与明文对应关系相等，获取到密文不会增加“知识”[15]，安全性是绝对安全的；若仅在第一次发送明文选择一个随机密钥k_2，即第一次验证双方k_2一致后，保存k_3，之后只用传输密文C，则本方案可近似看作传统通信加密方案，此时方案安全性与传统通信加密方案一致。

从性能角度分析，k_2的保密性不影响k_1和k_3，f_1、f_2、k_1、k_3存储在设备内部，不用传输，因此f_1、f_2、k_1、k_3秘密管理是容易的，无须额外增加密钥管理、认证等设备。通过选择合适的混合函数R、密钥产生函数H、认证加密算法E及认证解密算法D即可实现通信数据安全加密。此外，由于本方案未使用到非对称加密算法，本方案验证对称密钥k_3真实性、可用性、保密性所需时间远远短于传统通信加密方案，认证加解密数据所需时间两者基本一致。

综上所述，本方案相较于传统通信加密方案，减少了额外设备开销，降低了密钥管理难度，可根据实际需求选择合适算法提高方案性能，并在传统通信加密方案基础上提高了加密、解密过程整体安全性。

4　试验验证及分析

为验证上述方案的可行性和有效性，对轻量化加密方案和传统通信加密方案分别进行试验。其中，轻量化加密方案中混合函数R为异或运算，密钥产生函数H选择散列算法SM3，满足单向性和散列性要求，认证加密算法E选择SM4算法和基于SM4和SM3的消息认证算法，认证解密算法D与认证加密算法E算法一致。传统通信加密方案选择SM2+SM3+SM4加密算法组合，满足通信数据保密性、完整性、真实性要求。

4.1　试验环境

参照TCN环境，使用两台设备通信，发送端设备为CCU，接收端设备为TCU，设备参数见表3。

表3　列车控制设备CCU和TCU参数

Table 3　CCU and TCU parameters for train control equipment

参数项目	CCU	TCU
CPU型号	MPC5125	MPC8349
CPU主频/MHz	596	333
操作系统版本	VxWorks6.8	VxWorks6.8

4.2　试验结果及分析

试验测试了在不同数据加密需求场景下，CCU和TCU分别采用轻量化加密方案和传统通信加密方案完成密钥协商功能的平均用时以及设备CPU占用率。图3为轻量化加密方案发送端、接收端功能测试结果，图4为轻量化加密方案加解密及验证功能测试结果。

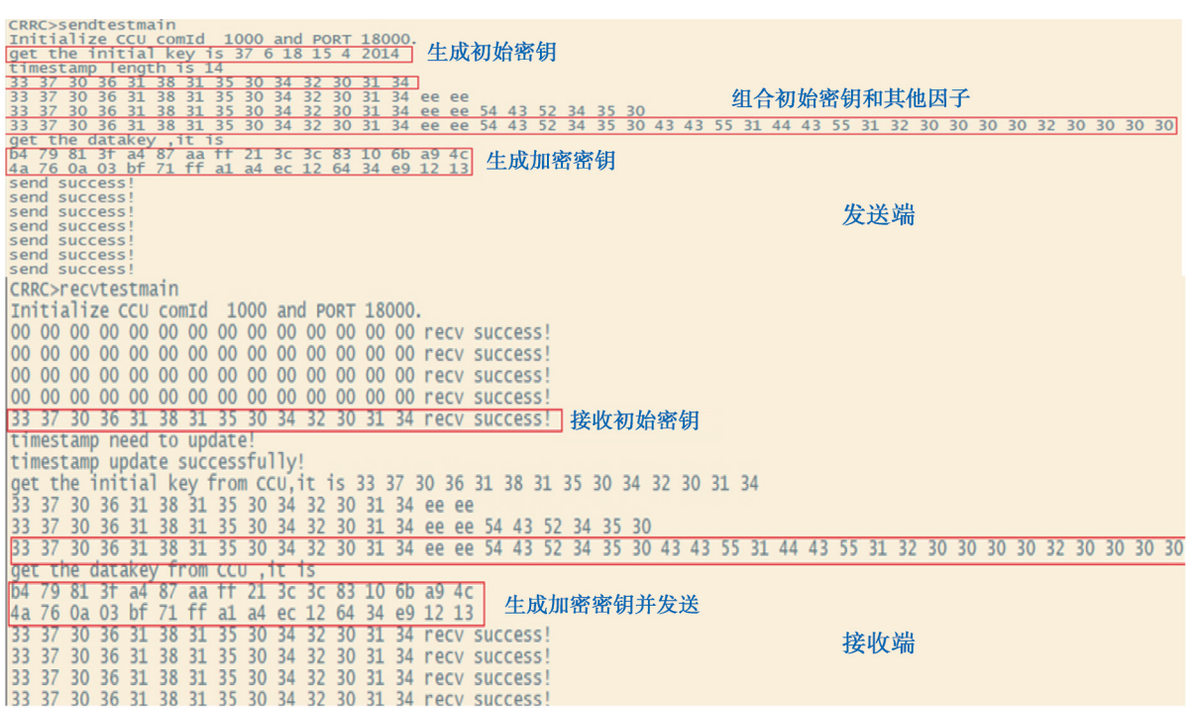


图3　发送端和接收端功能测试结果

Fig. 3　Test results of functions at sending and receiving ends

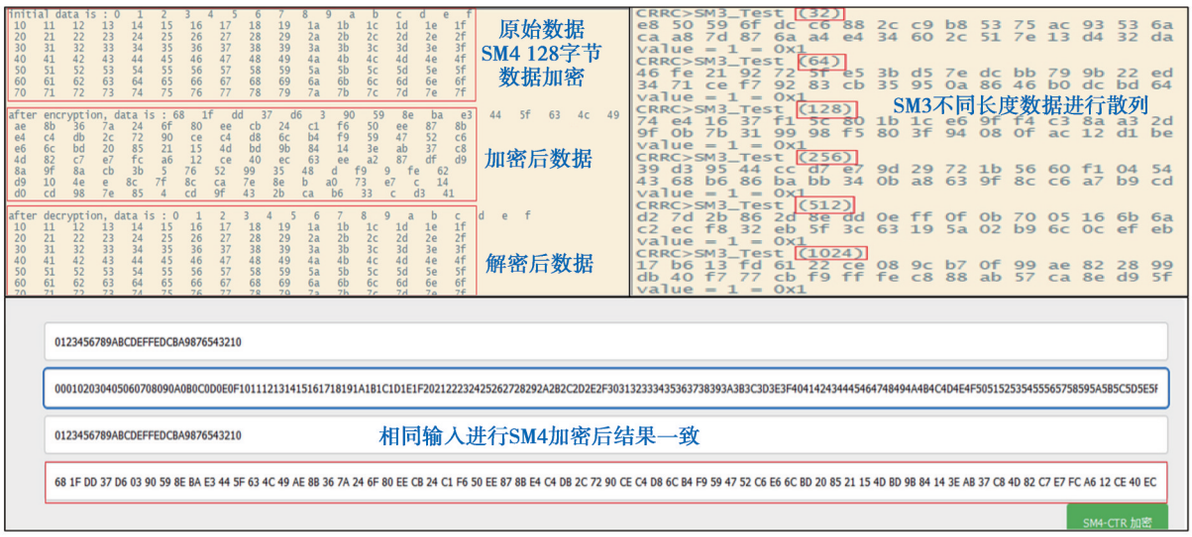


图4　认证加解密功能测试结果

Fig. 4　Test results of authenticated and decryption functions

为验证不同种类的加密方案对TCN设备上电初始化影响，分别测试两种方案完成100轮密钥协商过程平均所用时间。其中，轻量化加密方案密钥协商流程平均用时为304.94 ms，传统通信加密方案平均用时为956.65 ms。

为测试加密方案对TCN控制设备资源占用的影响，分别测试开启1/5/10个通信端口及32/64/128/256/512字节数据周期性执行不加密通信、轻量化加密通信、传统通信加密程序，测试3种场景下发送端和接收端CPU平均占用率，见表4。

表4　CPU负荷测试结果

Table 4　Test results of CPU load

测试类型		不加密通信		轻量化加密通信		SM2+SM3+SM4传统通信加密	
加密字节数	通信端口数	总CPU占用率（发送端）	总CPU占用率（接收端）	总CPU占用率（发送端）	总CPU占用率（接收端）	总CPU占用率（发送端）	总CPU占用率（接收端）
32	1	1%	4%	2%	4%	5%	6%
	5	5%	6%	6%	7%	13%	16%
	10	7%	11%	12%	16%	27%	29%
64	1	3%	0%	3%	3%	5%	5%
	5	3%	2%	9%	10%	16%	18%
	10	7%	4%	17%	19%	34%	35%
128	1	3%	1%	3%	4%	6%	5%
	5	5%	4%	12%	10%	21%	22%
	10	7%	6%	21%	22%	41%	44%
256	1	0%	1%	4%	4%	6%	7%
	5	4%	7%	15%	15%	26%	28%
	10	8%	6%	26%	29%	53%	55%
512	1	0%	1%	4%	5%	7%	7%
	5	5%	5%	21%	24%	30%	35%
	10	8%	9%	36%	39%	65%	67%

为测试轻量化加密方案对设备通信用时的影响，测试轻量化加密方案分别进行100/1 000/10 000轮认证加解密32/64/128/256/512/1 024字节数据的总用时，测试结果取平均值。认证加解密数据的平均用时见表5。

通过分析试验测试结果可以看出，两台TCN设备间通信使用本方案完成单次密钥协商流程用时约为传统通信加密方案的31.9%，单次密钥协商的方案比传统通信加密方案减少651.71 ms，结合TCN网络设备实际

表5　认证加解密平均用时

Table 5　Average time consumption for authenticated encryption and decryption　ms

次数	32字节	64字节	128字节	256字节	512字节	1 024字节
100	6	9	21	39	69	138
1 000	63	106	192	396	701	1 376
10 000	631	1 071	1 903	3 946	6 999	1 378

的节点数为20~30，采用本方案比采用传统通信加密方案用时减少约13~20 s，可满足设备启动时间要求。采用本方案设备CPU占用率平均约为采用传统通信加密方案的35.8%。同时，本方案认证加解密数据1 024字节仅增加1.38 ms用时，能够满足列车数据实时性要求。

5　结束语

本文提出了一种面向列车通信网络的轻量化加密方案，并依据该方案提供了一种具体实施方案。相较于传统通信加密方案需要额外部署众多管理设施，完整加密流程复杂，该方案通过将通信密钥由动态随机密钥与预协同初始密钥共同生成的方式，解决了TCN管理密钥困难和传统通信密钥单一、改变难度大的问题，并通过理论分析及试验证明该方案的安全性不弱于传统通信加密方案，对设备的实时性和CPU占用影响小于传统通信加密方案。

参考文献：

[1] 刘晓溪. 信息安全助力深圳地铁数字化转型稳步推进[J]. 城市轨道交通, 2021(8): 34-36.
LIU Xiaoxi. Information security helps Shenzhen metro digital transformation advance steadily[J]. China metros, 2021 (8): 34-36.

[2] 全国信息安全标准化技术委员会(SAC/TC 260). 信息安全技术 公钥基础设施 PKI系统安全技术要求: GB/T 21053—2023[S]. 北京: 中国标准出版社, 2023.
National Information Security Standardization Technical Committee(SAC/TC 260). Information security techniques-public key infrastructure-security technology requirement for PKI system: GB/T 21053—2023[S]. Beijing: Standards Press of China, 2023.

[3] Information Technology Laboratory, National Institute of Standards and Technology. Advanced encryption standard (AES): FIPS 197[S]. Gaithersburg: National Institute of Standards and Technology, 2023.

[4] 潘晓中, 张薇, 徐晓军, 等. 数据加密技术分析[J]. 系统工程与电子技术, 2003, 25(2): 236-238.
PAN Xiaozhong, ZHANG Wei, XU Xiaojun, et al. Analysis of data encryption techniques[J]. Systems engineering and electronics, 2003, 25(2): 236-238.

[5] Information Technology Laboratory, National Institute of Standards and Technology. Secure Hash Standard (SHS): FIPS PUB 180-4[S]. Gaithersburg: National Institute of Standards and Technology, 2015.

[6] 全国信息安全标准化技术委员会(SAC/TC 260). 信息安全技术SM2椭圆曲线公钥密码算法 第1部分: 总则: GB/T 32918.1—2016[S]. 北京: 中国标准出版社, 2017.
National Information Security Standardization Technical Committee(SAC/TC 260). Information security technology-public key cryptographic algorithm SM2 based on elliptic curves-part 1: general: GB/T 32918.1—2016[S]. Beijing: Standards Press of China, 2017.

[7] 全国信息安全标准化技术委员会(SAC/TC 260). 信息安全技术 SM3密码杂凑算法: GB/T 32905—2016[S]. 北京: 中国标准出版社, 2017.
National Information Security Standardization Technical Committee(SAC/TC 260). Information security techniques-SM3 cryptographic hash algorithm: GB/T 32905—2016[S]. Beijing: Standards Press of China, 2017.

[8] 全国信息安全标准化技术委员会(SAC/TC 260). 信息安全技术SM4分组密码算法: GB/T 32907—2016[S]. 北京: 中国标准出版社, 2017.
National Information Security Standardization Technical Committee(SAC/TC 260). Information security technology-SM4 block cipher algorithm: GB/T 32907—2016[S]. Beijing: Standards Press of China, 2017.

[9] 高枫, 余博, 李元轩. 城轨车辆列车网络控制系统技术方案及发展方向[J]. 铁路技术创新, 2015(4): 57-62.
GAO Feng, YU Bo, LI Yuanxuan. Technical scheme and development direction of train network control system for urban rail vechicles[J]. Railway technical innovation, 2015 (4): 57-62.

[10] 张顺广, 王隆龙, 袁涛. 动车组统型PTU服务软件的设计与实现[J]. 铁道机车车辆, 2019, 39(4): 6-10.
ZHANG Shunguang, WANG Longlong, YUAN Tao. Design and implementation of EMU's integrated PTU service software[J]. Railway locomotive & car, 2019, 39(4): 6-10.

[11] SCHNEIER B. 应用密码学: 协议、算法与C源程序[M]. 吴世忠, 祝世雄, 张文政, 等译. 北京: 机械工业出版社, 2014: 20-23.
SCHNEIER B. Applied cryptography: protocols, algorithms, and source code in C[M]. Translated by WU Shizhong, ZHU Shixiong, ZHANG Wenzheng, et al. Beijing: China Machine Press, 2014: 20-23.

[12] 刘远航. PKI实现与应用中的一些问题[D]. 长春: 吉林大学, 2004.
LIU Yuanhang. Some issues in implementing and applying a PKI[D]. Changchun: Jilin University, 2004.

[13] 杨波. 现代密码学[M]. 5版. 北京: 清华大学出版社, 2022: 161-163.
YANG Bo. Modern cryptography[M]. 5th ed. Beijing: Tsinghua University Press, 2022: 161-163.

[14] 刘洪强. 基于SSL协议的VPN技术研究与实现[D]. 济南: 山东大学, 2008.
LIU Hongqiang. Research and implementation of SSL-

based VPN[D]. Jinan: Shandong University, 2008.
[15] SHANNON C E. Communication theory of secrecy systems [J]. The bell system technical journal, 1949, 28(4): 656-715.

Lightweight encryption solution for train communication network

TANG Jun, GE Qianghua, ZOU Zhirong, CHEN Bo, TANG Pin

(CRRC Zhuzhou Institute Co., Ltd., Zhuzhou, Hunan 412001, China)

Abstract: The wide application of wireless communication technology has brought about an increase in network security risks for train communication networks. To mitigate these risks, data encryption has emerged as an important means, albeit with additional demand on CPU computing resources. However, train communication network hosts predominantly rely on embedded devices with limited computing resources. This paper proposes a lightweight encryption solution for train communication networks. This solution employs a key negotiation process based on traditional communication encryption scheme, aiming to achieve lightweight encryption in train communication networks and compliance with the authenticity, integrity, and confidentiality requirements of communication data, while greatly reducing hardware demands and computational burdens associated with key management. Experimental verification using the proposed solution yielded a key negotiation time consumption of about 31.9% and reduced the CPU load on devices to about 35.8% when compared to the traditional SM2+SM3+SM4 communication encryption method.

Keywords: train communication network; data encryption; lightweight; key negotiation

收稿日期：2023-08-25