计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(10):140−145 [doi: 10.15888/j.cnki.csa.006598]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

高铁传感器系统数据安全传输协议①

左黎明, 陈兰兰, 周　庆

(华东交通大学 理学院, 南昌 330013)
(华东交通大学 系统工程与密码学研究所, 南昌 330013)
通讯作者: 左黎明, E-mail: limingzuo@126.com

摘　要: 随着高速铁路的快速发展, 以云计算和实时在线分析为基础的高铁数据安全传输研究成为一个热门课题. 针对高铁数据传输过程中存在的数据安全认证问题, 设计了一种基于国密 SM2 签名算法的高铁传感器系统数据安全传输协议. 以 SM2 签名算法为核心, 基于安全协议将传感器网络收集的行车状态数据传输到云服务平台, 实现了高铁行车记录仪和云服务平台之间的安全交互, 提高了数据传输的可靠性和完整性. 最后对安全传输协议进行实验与仿真, 实验结果表明协议在高铁数据传输过程中具有较高的效率和安全性.

关键词: SM2 签名算法; 数据安全传输协议; 传感器网络; 高铁行车记录仪; 安全交互

引用格式: 左黎明,陈兰兰,周庆.高铁传感器系统数据安全传输协议.计算机系统应用,2018,27(10):140–145. http://www.c-s-a.org.cn/1003-3254/6598.html

Data Secure Transmission Protocol of High-Speed Rail Sensor System

ZUO Li-Ming, CHEN Lan-Lan, ZHOU Qing

(School of Science, East China Jiaotong University, Nanchang 330013, China)
(SEC Institute, East China Jiaotong University, Nanchang 330013, China)

Abstract: With the rapid development of high-speed railway, the research of the data secure transmission of high-speed railway based on cloud computing and real-time online analysis have become the hot topics. Aiming at the problem of the data secure authentication in the process of the data transmission at high-speed rail, a data secure transmission protocol for high-speed rail sensor system based on SM2 signature algorithm is designed. The traffic state data collected by the sensor network are transmitted to the cloud service platform by the security protocol based on SM2 signature algorithm, and the secure interaction between the high-speed rail traveling data recorder and the cloud service platform is realized. Therefore, the reliability and integrity of data transmission are improved. Finally, the experiment and simulation of secure transmission protocol are carried out, and the result shows that the protocol has high efficiency and security in the process of high-speed railway data transmission.

Key words: SM2 signature algorithm; data secure transmission protocol; sensor network; high-speed rail traveling data recorder; secure interaction

随着高速铁路的快速发展, 人流、物流、资金流、信息流的流动加快, 给人们的生活带来了便利, 然而随之而来的数据传输安全问题也越来越重视. 近年来, 铁路交通事故层出不穷, 2016 年郑州铁路局

① 基金项目: 国家自然科学基金 (11361024); 江西省自然科学基金 (20171BAB201009); 江西省教育厅科技项目 (GJJ170386)
Foundation item: National Natural Science Foundation of China (11361024); Natural Science Foundation of Jiangxi Province (20171BAB201009); Technology Project of Education Department of Jiangxi Province (GJJ170386)
收稿时间: 2018-03-18; 修改时间: 2018-04-10; 采用时间: 2018-04-17; csa 在线出版时间: 2018-09-28

“12•10”事故, 现场安全防护失效导致 6 人死亡[1]; 2017 年印度北方邦火车脱轨事故, 造成至少 23 人死亡、70 多人受伤[2]. 上述铁路交通事故大部分是缺乏铁路安全方面监测, 为实现对铁路行车状态进行监测, 高铁行车记录仪的研究具有重要意义. 目前, 许多国内外专家、学者对车载行车记录仪和飞行记录仪进行了研究, 2008 年 Tomer Toledo 等[3]介绍了车载行车记录仪系统作为监测和反馈司机在道路上行为的工具在各种商业和研究应用中的潜力. 2011 年 Chang Youli 等[4]设计了飞行记录仪断带处理的计算机信息系统, 同年姜列为等[5]提出了基于 CAN 总线的汽车黑匣子的总体设计方案. 2013 年白雅伟[6]提出基于 ARM 的新型行车记录仪的研究与设计, 对新型行车记录仪的硬件设计及软件开发进行了深入分析和研究. 2013 年董文扬[7]提出行车记录仪中 GIS 的设计与实现, 实现了在行车记录仪管理系统中嵌入 GIS 功能, 对采集到的车辆信息, 实现行车信息的高效查询、计算、分析及辅助决策. 2014 年 Xu Dong 等[8]研究基于飞行记录仪的直升机寿命可靠性, 同年 Yun Huzhang 等[9]采用 ARM 处理器设计了一种基于危险判断的车辆行车记录仪. 2015 年 Ruhul Amin Rana 等[10]研究飞行记录仪的热生存, 为飞行记录仪的热设计提供了确定尺寸和材料选择的一般指导. 2016 年 Yair Wiseman[11]研究了飞行记录仪存储器的扩展性和安全性, 实现了飞行记录仪嵌入式设备的无限制存储容量, 从而可以存储更多的信息. 2017 年党改慧等[12]提出一种多功能汽车行车记录仪设计与实现, 解决现有产品功能单一, 且记录数据依赖人工进行数据提取的不足. 但在上述研究中, 没有考虑到行车和飞行过程中的数据传输安全问题, 而高铁运行过程中也存在类似的问题, 因此为提高高铁信息交互的安全性, 提出高铁传感器[13]系统数据安全传输协议, 并将此协议运用于高铁行车记录仪中, 对提供一个安全的高铁行车环境具有重要意义.

目前高铁行车记录仪用于列车运行安全防护和运行状态记录, 但现有数据保护机制对传输过程中数据保护尚有欠缺. 因此通过遍布车厢的传感器网络收集行车状态数据, 利用基于 SM2 签名算法[14]的高铁传感器系统数据安全传输协议对传输的数据进行实时保护, 再通过数据挖掘和分析监测列车的行进状态并采用神经网络算法[15]进行预测和评估, 提前发现列车中的潜在危险并作出预警, 从而降低恶性事件发生的概率, 最大程度地提高乘坐高铁的安全性.

1 系统设计

1.1 系统总计架构

系统整体结构如图 1 所示, 主要由高铁行车记录仪、云服务平台组成, 基于 C/S 架构, 高铁行车记录仪作为客户端, 云服务平台作为服务端. 高铁行车记录仪主要由 Raspberry Pi 3 Model B ARMv8(树莓派) 主板和传感器数据收集模块组成, 其中树莓派包括 GPRS 模块、信息处理模块和签名模块, 传感器数据收集模块通过遍布车厢的多种传感器网络采集行车数据, 主要包括速度传感器、加速度传感器、位置传感器、轴温传感器、TR 系列振动速度传感器、噪声传感器和压力传感器. 云服务平台主要由信息处理模块、身份认证模块、数据分析模块和云数据库组成, 其中身份认证模块用于对传输数据的用户进行身份认证, 数据分析模块再对认证通过的信息进行实时分析.

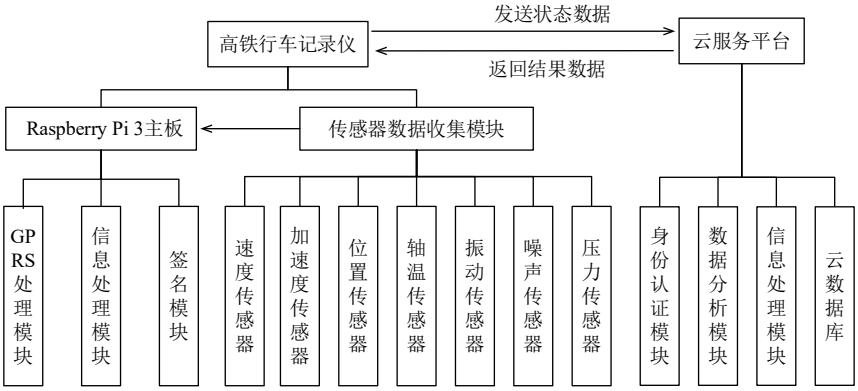

图 1 系统整体结构示意图

在该系统中, 高铁行车记录仪通过传感器数据收集模块每隔一段时间采集高铁行车过程中速度、加速度、位置、轴温、振动、噪声、压力等状态数据, 并将数据记录在树莓派的存储模块中, 然后通过树莓派的签名模块对行车数据进行签名, 再将行车数据与签名信息以封包的形式发送给云服务平台. 云服务平台的身份认证模块对接收的封包进行解析并验证签名, 对验证通过的数据利用数据挖掘和神经网络等算法进行实时分析, 同时将状态数据分析结果记录到云数据库中.

1.2 系统硬件设计

系统中客户端是高铁行车记录仪, 整体呈扁盒状, 其结构如图 2 所示, 主要包括信息采集模块、树莓派. 信息采集模块包含电源, USB 接口和传感器接口等, 其中电源用于对行车记录仪提供电量支持, 传感器接口用于连接遍布车厢的传感器. 高铁行车记录仪内部设置散热模块用于树莓派运行时散热, 树莓派包括签名模块、信息处理模块和 GPRS 模块, GPRS 模块用于将数据发送至云服务平台.

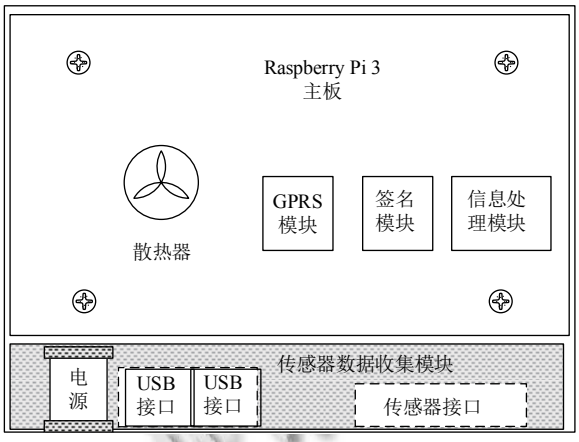

图 2 高铁行车记录仪结构示意图

1.3 信息处理模块设计

信息的处理包括组装数据封包和解析数据封包. 本系统中接收信息、返回信息都以统一标准的封包来实现, 一个完整封包包括: 协议序列号$protocolID$、行车记录仪编号$userID$、行车状态数据$data$、时间戳T、签名数据$Sign(protocolID, userID, data, T)$, 具体封包参数如表 1 所示, 规定封包以协议保留字“#”连接, 以便处理时分割并重新对象化, 其中$data$为编号为$userID$的行车记录仪中传感器收集的行车状态数据, $Sign(protocolID, userID, data, T)$表示以“#”连接协议序列号$protocolID$、行车记录仪编号$userID$、时间戳$T$和业务数据$data$后的签名数据.

表 1 封包参数表

参数名	说明
$protocolID$	协议序列号
$userID$	行车记录仪编号
$data$	行车状态数据
T	时间戳
$Sign(protocolID, userID, data, T)$	签名数据

2 基于 SM2 的签名算法

高铁传感器系统传输协议基于 SM2 签名算法[14], 采用 SM2 签名算法对高铁行车状态数据进行签名并在云服务平台验证签名, 具体算法描述如下:

系统参数: 有限域F_q上的q, 椭圆曲线方程$E(F_q)$上的元素 a、$b \in F_q$, $E(F_q)$上的点$K=(x_K, y_K)(K \neq O)$, 其中椭圆曲线方程$E(F_q)$是指方程$y^3=x^3+ax+b$, $x_K, y_K \in F_q$, K 的阶为 n, 及其它可选参数.

密钥对生成: 设高铁行车记录仪客户端用户为U, 其密钥对为$(priKey_U, pubKey_U)$, 其生成算法满足$pubKey=[priKey]K=(x_U, y_U)$.

其他信息: 用户U唯一的标识ID_U长度为len_U, 设LEN_U为len_U由整数转换而成的两个字节, 本方案用户U的杂凑值Z_U需要签名者或验证者通过密码杂凑函数求得, 计算方法为:

$$Z_U = H_{256}(LEN_U \| ID_U \| a \| b \| x_K \| y_K \| x_U \| y_U)$$

签名生成: 设待签名消息为Msg, 先令$\overline{Msg}=Z_U \| Msg$, 计算$e=H_{256}(\overline{Msg})$, 然后生成随机数$k \in [1, n-1]$, 计算椭圆曲线上点$(x_1, y_1)=[k]K$, 再计算$r=(e+x_1) \bmod n$ 和$s=((1+pri_U)^{-1} \cdot (k-r \cdot pri_U)) \bmod n$. 最后将 r、s 的数据类型转换为字符串, 签名者高铁行车记录仪用户U获得消息Msg的签名为 $Sign(Msg)=(r, s)$.

签名验证: 云服务平台身份验证模块对签名$M'=Sign(Msg)$进行验证$Verify(M')$, 首先验证$r' \in [1, n-1]$和$s' \in [1, n-1]$是否成立, 若不成立则验证不通过, 然后令$\overline{M'}=Z_A \| M'$, 计算$e'=H_{256}(\overline{M'})$, 接着计算$t=(r'+s') \bmod n$, 若$t=0$, 则验证不通过, 再计算椭圆曲线点$(x'_1, y'_1)=[s']K+[t]pubKey_U$, 最后计算$R=(e'+x'_1) \bmod n$, 检验$R=r'$是否成立, 若成立则验证通过; 否则验证不通过.

3 协议交互流程与安全性分析

3.1 协议交互流程

如图 3 所示, 为高铁行车记录仪与云服务平台之间进行协议交互的时序图, 包括以下流程:

(1) 传感器数据收集模块→信息处理模块: 传感器数据收集模块中遍布车厢的传感器将每隔一定时间采集的行车状态数据*data*发送到信息处理模块.

(2) 信息处理模块→签名模块: 信息处理模块将协议序列号 *protocolID*、行车记录仪编号 *userID*、行车状态数据 *data* 和时间戳 *T* 组成封包 *protocolID#userID#data#T*, 并将组装的封包发送到签名模块.

(3) 签名模块→信息处理模块: 签名模块对接收到的包含行车状态数据 *data* 的封包进行签名, 签名信息为 *Sign*(*protocolID, userID, data, T*), 再将签名信息发送到信息处理模块.

(4) 高铁行车记录仪→云服务平台: 高铁行车记录仪信息处理模块接收签名信息后, 组装签名封包 *protocolID#userID#data#T#Sign*(*protocolID#userID#data#T*), 并通过 GRPS 模块发送给云服务平台.

(5) 信息处理模块→身份认证模块: 云服务平台的信息处理模块对接收到的封包数据进行解析, 将解析的签名信息 *Sign*(*protocolID, userID, data, T*) 发送到云服务平台的身份认证模块. 身份认证模块采用 SM2 签名算法验证签名 *Verify*(*Sign*(*protocolID, userID, data, T*)), 若验证成功, 则将数据发送到数据分析模块进行实时分析, 并将结果保存至云数据库中; 否则, 将此行车记录仪编号对应的数据设置身份验证失败标识.

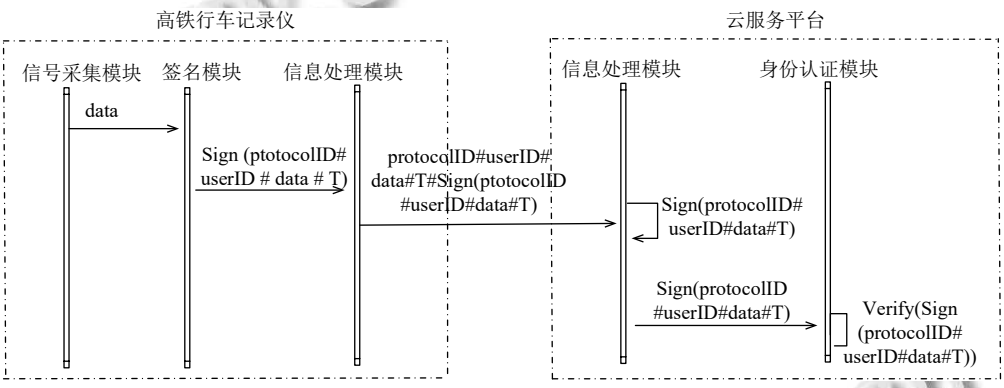

图 3 高铁行车记录仪与云服务平台之间的交互

3.2 协议安全性分析

本协议采用基于椭圆曲线离散对数问题的 SM2 (Elliptic Curve Cryptography, ECC)[16]是国家密码管理局发布的椭圆曲线公钥密码算法, 目前只存在指数级计算复杂度的求解方法, 与大数分解问题相比求解难度大得多, 具有更高的安全性. 基于此安全签名算法, 本协议实现了高铁行车记录仪向云服务平台传输行车状态数据, 为保证传输数据的有效性和新鲜性, 本协议采用时戳机制, 高铁行车记录仪信息处理模块将当前时间合成到待签名数据中, 云服务平台在身份认证模块验证签名时, 把得到的时间与本地时间进行比较, 若比较结果所显示的时差足够小, 则认为传输的数据是新鲜的, 若数据新鲜且验证签名通过, 则验证成功, 否则验证失败. 采用时戳机制避免了重放攻击, 从而大大提高协议的安全性.

4 实验与仿真

4.1 高铁行车记录仪签名模拟

高铁行车记录仪对状态数据签名, 并把签名和状态数据组成封包的核心代码如下, 具体数据信息如图 4 所示.

```
//高铁传感器装置采集的行车状态数据
string data="[速度:350 km/h;加速度:0.16 m/s^2]";
string str=string.Format(
"高铁传感器装置采集的行车状态数据为:\n{0}",data);
string protocolID = "1";
//1. 高铁行车记录仪信息初始化阶段
//初始化高铁行车记录仪内 MicroSD 卡信息
MicroSDCardInform MicroSDcardIn = MicroSDCardInform.Init();
```

```
//一个 MicroSD 卡对应一个高铁行车记录仪
MobileTerminal MobileTerminal = new testusbkeyCsharp.
MobileTerminal(MicroSDcardIn);
//2. 对待签名数据进行封包处理
string uid = MicroSDcardIn.CardID;
string T = DateTime.Now.ToString();
string msg = protocolID + "#" + uid + "#" + data + "#" + T;
//3. 签名阶段
//根据 MicroSD 卡存入的私钥
//对待签名数据进行国密 SM2 签名
string Signmessage = MobileTerminal.SM2Sign
(msg, MicroSDcardIn.PrivateKey);
//4.组成数据封包:将“协议序列号、行车记录仪编//号、行车状态数据、时间戳、签名数据”组成签//名数据包
string Signaturestr = MobileTerminal
.AssemblyPackage(protocolID, uid,
data, T, Signmessage);
SignPacket SignPacket = MobileTerminal
.StringToPacket(Signaturestr);
```

图 4 高铁行车记录仪产生的基本信息

4.2 云服务平台验证签名模拟

云服务平台接收到签名数据包后, 对签名进行验证的核心代码如下, 具体数据信息如图 5 所示.

```
//1. 初始化服务端
WebServer websever = new WebServer();
//2. 服务端获取签名数据包
SignPacket.PacketToString();
//3. 服务端接收到并解析签名数据包
string SignaturePacket = SignPacket.PacketStr;
//4. 对签名数据进行验证
string result = websever.VerifySign(SignPacket);
```

图 5 云服务平台身份认证产生的基本信息

4.3 效率分析

如图 6 所示, 高铁行车记录仪信息处理耗时为 0.152 8893 秒, 云服务平台信息处理耗时为 0.045 6867 秒, 系统信息处理耗时总计 0.198 576 秒, 因此, 系统各终端在信息处理方面效率很高.

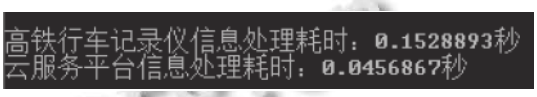

图 6 终端信息处理耗时

5 结论

本文针对传统高铁数据交互系统存在信息传输的安全性问题, 提出了一种基于 SM2 签名算法的高铁传感器系统数据安全传输协议, 以 SM2 签名算法为核心, 通过高铁行车记录仪和云服务平台之间的安全交互, 实现高铁行车数据传输的有效性和完整性. 通过实验仿真, 表明本交互协议在实际应用中具有较高的安全性和高效性. 在高铁逐渐普及的今天, 安全可靠的行车环境也越来越重要, 因此本安全协议具有良好的应用前景. 基于此协议, 通过云服务平台的数据分析模块对传感器网络收集的行车数据进行实时分析, 利用神经网络等数据挖掘算法进行预测和评估是以后的研究方向.

参考文献

1 财新网. 郑州铁路局“12•10”事故初步调查结论 现场安全防护失效. http://companies.caixin.com/2016-12-11/101025776.html. [2016-12-11].

2 央视网. 央视记者探访印度北方邦火车脱轨事故现场: 车厢变形成一堆废铁. http://m.news.cctv.com/2017/08/21/ARTIfgfRlmTmGGvPS9iXc5av170821.shtml, [2017-08-21].

3 Toledo T, Musicant O, Lotan T. In-vehicle data recorders for monitoring and feedback on drivers' behavior. Transportation Research Part C: Emerging Technologies, 2008, 16(3): 320–331. [doi: 10.1016/j.trc.2008.01.001]

4 Li CY, Li HZ. Information processing of the broken tape of flight data recorder. Applied Mechanics and Materials, 2011, 58–60: 2402–2406. [doi: 10.4028/www.scientific.net/AMM.58-60.2402]

5 姜列为, 余春暄. 基于 CAN 总线的汽车黑匣子的设计与实现. 计算机测量与控制, 2011, 19(1): 131–132, 135. [doi: 10.16526/j.cnki.11-4762/tp.2011.01.007]

6 白雅伟. 基于 ARM 的新型行车记录仪的研究与设计[硕士学位论文]. 武汉: 武汉理工大学, 2013.

7 董文扬. 行车记录仪中 GIS 的设计与实现[硕士学位论文]. 石家庄: 河北科技大学, 2013.

8 Li XD, Yang XH. The research on the reliability of helicopter life based on analysis of the data of flight data recorder. In: Wang JS, ed. Proceedings of the First Symposium on Aviation Maintenance and Management-Volume II. Berlin, Heidelberg: Springer. 2014. 157–164. [doi: 10.1007/978-3-642-54233-6_17]

9 Zhang YH, Zhang C, Zhu YZ. Vehicle traveling data recorder design based on judgment of danger. Applied Mechanics and Materials, 2014, 488–489: 1108–1111. [doi: 10.4028/www.scientific.net/AMM.488-489.1108]

10 Rana RA, Li R. Thermal protection from a finite period of heat exposure – heat survival of flight data recorders. Applied Thermal Engineering, 2015, 75: 748–755. [doi: 10.1016/j.applthermaleng.2014.09.077]

11 Wiseman Y. Unlimited and protected memory for flight data recorders. Aircraft Engineering and Aerospace Technology, 2016, 88(6): 866–872. [doi: 10.1108/AEAT-06-2015-0152]

12 党改慧, 王雅红. 一种多功能汽车行车记录仪设计与实现. 机械制造与自动化, 2017, 46(1): 213–214, 233. [doi: 10.19344/j.cnki.issn1671-5276.2017.01.057]

13 晋泽炎, 吕伟杰, 刘丽萍. 基于洋流模型的水下传感器网络实时定位算法. 传感器与微系统, 2017, 36(12): 149–152, 156. [doi: 10.13873/J.1000-9787(2017)12-0149-04]

14 国家密码管理局. SM2 椭圆曲线公钥密码算法 第 1 部分：总则. http://www.sca.gov.cn/sca/xwdt/2010-12/17/1002386/files/b791a9f908bb4803875ab6aeeb7b4e03.pdf. [2010-12-01].

15 Petlíková K, Jarský Č. Modeling of the time structure of construction processes using neural networks. Organization, Technology and Management in Construction, 2017, 9(1): 1559–1564. [doi: 10.1515/otmcj-2016-0018]

16 汪朝晖, 张振峰. SM2 椭圆曲线公钥密码算法综述. 信息安全研究, 2016, 2(11): 972–982.