文章编号:1005-0523(2019)05-0067-07

铁路物流中基于短签名的实时跟踪协议

左黎明[1,2],易传佳[1,2],陈艺琳[1]

(华东交通大学 1.理学院; 2.系统工程与密码学研究所,江西 南昌 330013)

摘要:随着铁路物流软硬件建设的快速发展,大数据和物联网技术在铁路物流中得到广泛应用,以云计算、人工智能和实时在线监控技术为基础的智慧铁路物流系统研究成为一个热门课题。针对当前一些铁路智慧物流系统和设计方案在信息交互过程中缺乏安全认证和数据完整性保护的缺点,提出了一个基于身份标识的高效短签名方案,进一步以此签名方案为基础,设计了一种适用于铁路实时物流跟踪协议。对签名方案进行了协议交互的实验仿真,结果表明签名方案计算量小,效率较高,协议交互次数少,可有效的解决实时物流信息数据完整性保护和可靠性认证问题。

关键词:智慧物流;短签名;安全协议;实时物流跟踪

中图分类号:TP309.2 **文献标志码**:A

近年来我国铁路事业发展很快[1],铁路货物运输已经是国内大宗运输[2]的主要方式之一。随着互联网技术的发展,铁路运输系统物联网化、智能化[3-5]是铁路运输发展的必然趋势。传统的智能运输系统研究集中在运单管理、调度[6]、库存、配送等[7]环节。随着物联网技术的发展,以物联网技术为核心实现物流实时监控、智慧感知的铁路物流智能系统[8]成为近年来研究的热点[9-11]。智慧物流技术推动铁路物流的发展,但大部分系统并未考虑对物联网采集的数据进行来源合法性认证,难以抵抗各种类型的网络攻击。本文提出了一个适用于低成本硬件窄带通讯的实时安全物流跟踪协议, 该协议核心为一个基于数据采集装置身份ID的短签名方案,协议中利用该签名方案对采集信息进行了数字签名,服务端验证签名,整个协议交互过程传输数据少、计算量小,可以保障铁路物流信息高效传输的同时实现信息来源的可靠性和安全性。

1 相关基础

1.1 物流跟踪系统数据采集装置

图1为设计的一种安全的铁路物流跟踪信息采集装置的物理架构。其分别由内嵌密码芯片的粘贴式易

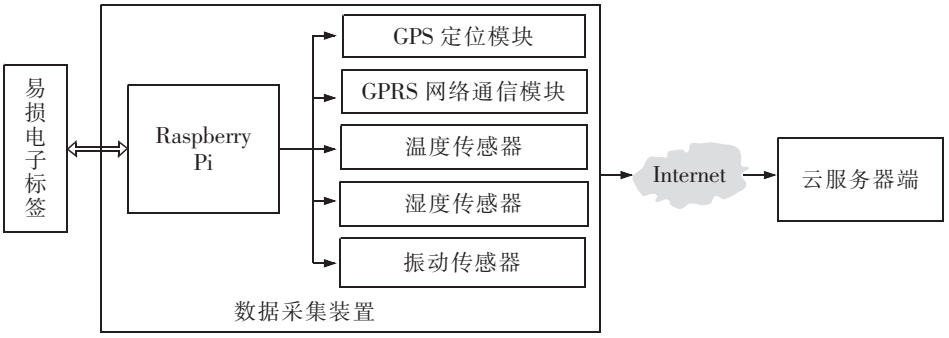

图1 整体架构图

Fig.1 Overall architecture

收稿日期:2018-12-21

基金项目:国家自然科学基金项目(11361024);江西省教育厅科技项目(GJJ170386);江西省科技厅科技项目(20192BBHL80004)

作者简介:左黎明(1981—),男,副教授,研究方向为信息安全、非线性系统。

损电子标签、数据采集装置和铁路物流跟踪信息系统云服务器端组成。

其中粘贴式易损电子标签用于封印货柜门，如图2所示，当货物装箱完成关闭集装箱门后，将易损电子标签粘贴在门中，同时连通了安装在集装箱侧门的数据采集装置，当粘贴式易损电子标签使用激活后，非授权的移除和撕毁均会引起数据采集装置向云服务器端发出报警信息报文。数据采集装置是以树莓派(Raspberry Pi 3B)为控制中心，通过GPS(VOGO-919)定位模块、温度传感器(MEACON-PT100 WZP)、湿度传感器(Risym DHT11)和振动传感器(TELESKY)收集实时信息，GPRS(SIM900)网络通信模块实现与云端的数据交互。

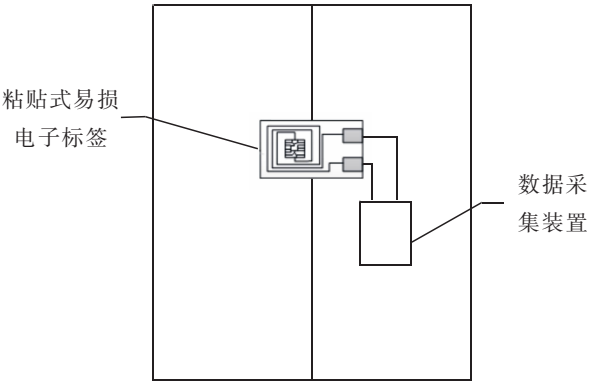

图2 粘贴式电子标签

Fig.2 Pasted electronic label

1.2 基于标识ID的短签名

云服务器端的物流追踪管理系统含密钥生成中心(key generator center，KGC)，每个数据采集装置端在系统内均有唯一的识别ID，实时物流跟踪协议使用基于数据采集装置端ID的数字签名方案的目的是利用ID作为每一个数据采集端的记录索引，可以实现高速的信息查询与检索。KGC利用ID生成数据采集装置端的签名私钥，可以在装置使用初始化的时候注入该私钥，使用短签名的主要原因是在实时环境下，通讯和计算能力受限，协议要尽可能使得封包数据长度短。为叙述方便，以下我们把每一个数据采集装置端称为一个装置或者签名者，云服务器端为验证者。

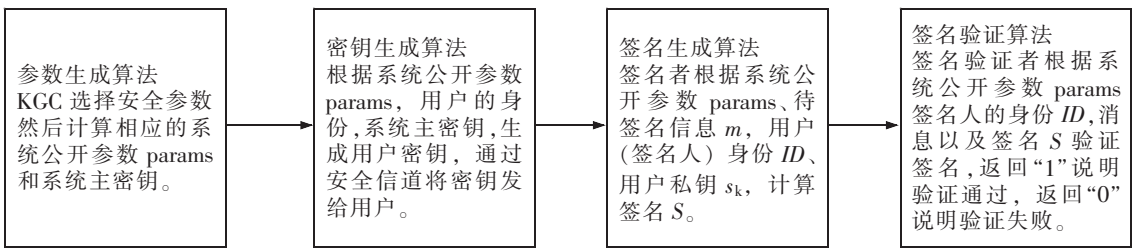

图3 算法流程图

Fig.3 Algorithm flow

如图3所示，本文提出的短签名方案由以下四个多项式算法构成：① 参数生成算法；② 密钥生成算法；③ 签名生成算法；④ 签名验证算法。

2 签名方案构造

1) 系统参数建立：给定安全参数k，系统密钥生成中心KGC选择两个阶都为安全素数的群G_1和G_2(其中G_1的生成元为g)，选择双线性映射$e:G_1\times G_1\rightarrow G_2$，选择安全哈希函数$H_1:\{0,1\}^*\rightarrow Z_q^*$，$H_2:\{0,1\}^*\rightarrow Z_q^*$。KGC随机选择$s_k\in Z_q^*$作为系统主私钥，计算系统公钥$P_k=s_kg$，公布系统参数$\{k,G_1,G_2,g,P_k,H_1,H_2\}$，保存私钥$s_k$。

2) 密钥生成：系统密钥生成中心KGC计算装置密钥$x_A=\dfrac{1}{H_1(ID_A,t,K)+s_k}g$，记录并公开装置$A$的公钥信息$(ID_A,t,K)$，然后通过安全信道将装置密钥$x_A$发送给(或者注入)装置$A$。其中参数$ID_A$为装置$A$的标识。参数$t$为时间戳，保证每次重新使用装置可以生成不同的密钥对，也便于服务器对装置相关信息的管理与索引。参数K为货物标识码，指示该密钥用于何种货物的跟踪，便于系统根据货物标识码对运输信息进行管

理与索引并进行密钥关联。

3）签名：对给定消息 $m\in(0,1)^*$ 进行如下签名：

① 计算 $h=H_2(m,ID_A)$；

② 计算 $S=hx_A$，则 S 为装置对消息 m 的签名。

4）签名验证：验证端获取(ID_A,t,K)，对给定消息/签名对(m,S)进行如下验证:

① 计算 $h=H_2(m,ID_A)$，$\hat{h}=H_1(ID_A,t,K)$；

② 令 $y_A=\hat{h}g+P_k$，y_A 作为装置公钥；

③ 验证等式：$e(S,y_A)=e(hg,g)$。

正确性验证如下：

$$e(S,y_A)=e(hx_A,\hat{h}g+P_k)$$

$$=e\left(h\frac{1}{H_1(ID_A,t,K)+s_k}g,\hat{h}g+P_k\right)$$

$$=e\left(h\frac{1}{H_1(ID_A,t,K)+s_k}g,H_1(ID_A,t,K)g+s_kg\right)$$

$$=e\left(h\frac{1}{H_1(ID_A,t,K)+s_k}g,(H_1(ID_A,t,K)+s_k)g\right)$$

$$=e(hg,g)$$

3　实时跟踪协议的设计与实现中的关键技术

3.1　实时跟踪协议与安全性分析

图 4 为实时物流跟踪协议交互原理图。具体步骤如下：

Step1:首先数据采集装置分别获取温度信息 T、湿度信息 H、经纬度信息 LD、振动信息 V 和当前时间 CT(作为时间戳，保证信息的新鲜性)。

Step2:数据采集装置将装置 ID_A 和采集到的数据以 $ID_A\#T\#H\#LD\#V\#CT$ 封包格式发送给易损电子标签。

Step3：易损电子标签接收消息封包后进行如下操作：

1）首先对消息封包$(ID_A\#T\#H\#LD\#V\#CT)$进行 $Hash$ 计算得到 h_m，$h_m=H_2(ID_A\#T\#H\#LD\#V\#CT)$；

2）调用签名算法对 h_m 进行签名处理得到签名结果 S。

Step4：易损电子标签将签名结果 S 返回给数据采集装置。

Step5：数据采集装置接收易损电子标签返回的签名结果后与采集到的数据结合，生成新的封包消息$(ID_A\#T\#H\#LD\#V\#CT\#S)$，并通过 GPRS 网络通信模块将该封包传输至云服务器端。

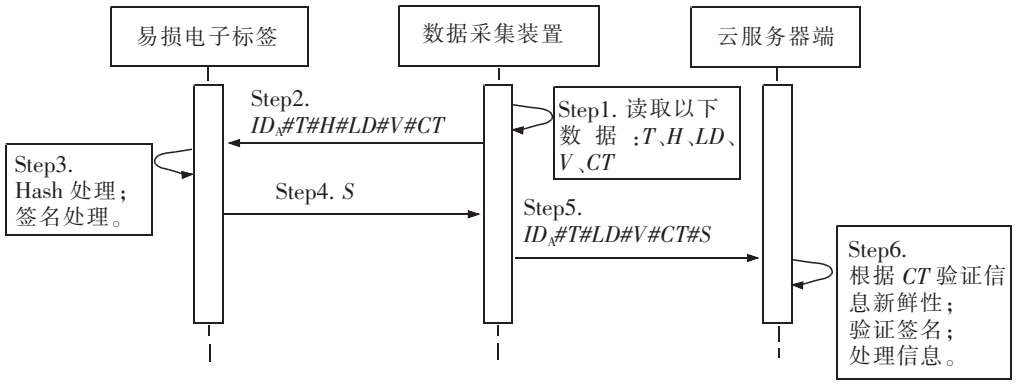

图 4　协议交互图

Fig.4　Protocol interaction

Step5:云服务器端接收到物流封包消息后进行如下操作:

1) 对封包消息进行拆包处理得到 ID 、T、H、LD、V、CT、S。

2) 根据 CT 验证消息的新鲜性,如果通过则进行下一步,否则丢弃该数据包并终止这一次数据交互协议。

3) 根据装置 ID 检索该装置对应公钥 y_A,根据 y_A,T、H、LD、V、CT 和 S 进行物流信息的签名验证,验证通过则记录该物流信息,否则云服务器端进行报警提示。

从以上协议交互过程中可知,数据封包通过网络传输过程只有一步,而且是单向的,可能的网络攻击只存在于该环节,协议的安全性可完全规约于短签名方案的安全性。

3.2 可粘贴式易损电子标签

本协议中使用的可粘贴式易损电子标签,内嵌了深圳华视微电子有限公司生产的 CVF1040D[12]智能安全芯片。芯片具有唯一 ID,注入了本方案的签名算法。在铁路货物运输过程中对数据采集装置采集到的实时数据进行签名处理。

3.3 相关传感器

数据采集装置中集成了温度传感器、湿度传感器、振动传感器和 GPS 模块,可以精确的采集铁路物流中的各类数据。

4 实验与仿真

本实验云服务器端的仿真平台环境为:浪潮英信 1U 服务器 NF5140M3 (处理器:E5-2420 3.0 GHz,内存:16.0 GB),操作系统为 Windows Server 2008R2。

4.1 数据采集端签名生成仿真

在数据采集端,数据采集装置首先将采集到的温度信息、湿度信息、经纬度为信息、振动信息和当前时间进行封包处理后,然后通过本文方案对封包消息进行签名处理,其部分核心代码如下:

```
strcat(m,ID);strcat(m,"#");
strcat(m,T);strcat(m,"#");
strcat(m,LD);strcat(m,"#");
strcat(m,H);strcat(m,"#");
strcat(m,V);strcat(m,"#");
strcat(m,CT);
element_init_Zr(h2,pairing);
element_from_hash(h2,m,strlen(m));
element_init_G1(S,pairing);
element_mul(S,h2,Xa)。
```

如图 5 所示,通过本方案对封包数据 m(B22-73218-12#37#115.89,28.68#0.5#80#20181220095216)先进行哈希处理,然后进行签名后得到签名信息 S,并且整个签名过程的耗时为 0.008 s。

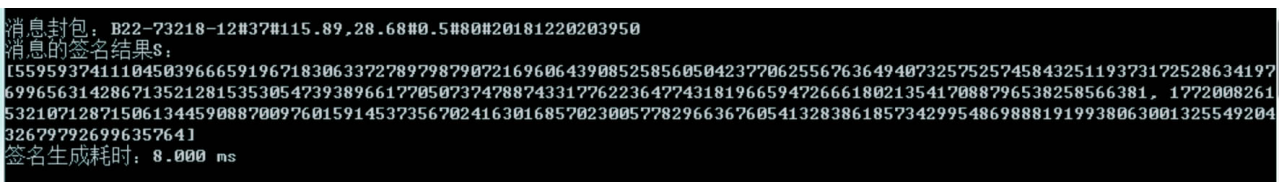

图 5 签名结果图

Fig.5 Signature result

4.2 云服务器端签名生成仿真

在云服务器端,对接收到的封包信息进行解析,然后根据时间戳验证物流信息新鲜性并根据本文方案的签名验证等式验证签名正确性,其部分代核心码如下:

```
        bool IsVerify;
    time_t currentTime;
    time(&currentTime);
    element_t left,right;
    if(difftime(ct,currentTime)<5)
    {
        element_init_GT(left,pairing);
        element_init_GT(right,pairing);
        element_init_Zr(data2,pairing);
        element_init_G1(ya,pairing);
        element_init_G1(temp3,pairing);
        element_add(data2,h1,Skgc);
        element_mul(ya,data2,g);
        element_pairing(left,S,ya);
        element_mul(temp3,h2,g);
        element_pairing(right,temp3,g);
        IsVerify=element_cmp(right, left);
    }
```

如图 6 所示,为云服务器端验证签名等式的结果和签名验证耗时(0.029 s)。本实验仿真表明云服务器端可以以较高的效率对数据采集端发送来的消息进行新鲜性验证和签名验证。并且整个实验仿真耗时为 0.092 s,所以在实际的物流信息实时跟踪中,具有较好的可行性。

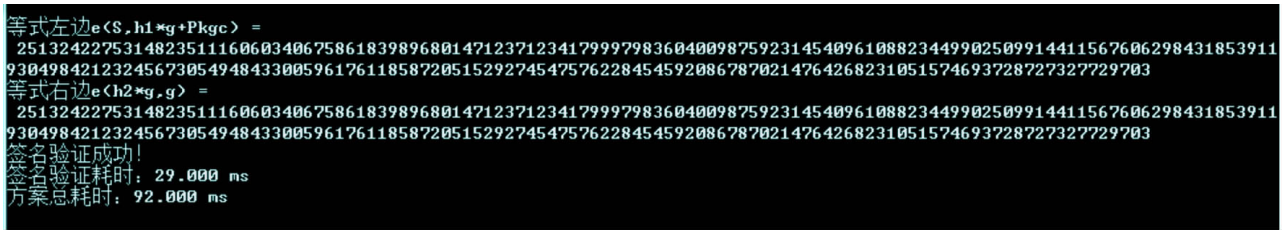

图 6　签名验证结果

Fig.6　Signature verification results

4.3　性能比较

表 1 给出了本文方案与几个经典短签名方案和近几年的基于身份签名方案的计算性能比较。其中 E 表示加法群上 G_1 的指数运算,Pr 表示双线性对运算,M 表示上 G_1 的一个标量乘,Sm 表示 G_1 上形如 $ag+bg$ 的同步标量乘,H 表示哈希运算,$|G_1|$表示 G_1 上元素的长度。

表 1　各签名方案的性能比较

Tab.1　Performance comparison of signature schemes

方案	签名算法	验证算法	签名长度
文献[13]	$1Sm+1E+1H$	$2Pr+2E+1H$	$2\|G_1\|$
文献[14]	$1E+1H$	$3Pr+1H$	$2\|G_1\|$
文献[15]	$1E+1Sm+1H$	$4H+4Pr+4M$	$2\|G_1\|$
文献[16]	$1M+2E+1H$	$2Pr+1M+1H$	$2\|G_1\|$
文献[17]	$1M+1H$	$2Pr+1H$	$\|G_1\|$
本文方案	$1M+1H$	$2Pr+1H$	$\|G_1\|$

5 结语

本文针对现有的部分铁路智慧物流系统和设计方案在信息交互过程中存在安全性认证和数据完整性保护问题,提出了一个高效短签名方案,并以此签名方案为基础,设计了一种适用于铁路实时物流跟踪协议。对签名方案进行了协议交互的实验仿真,签名过程平均耗时0.008 s,签名验证平均耗时0.029 s,整个方案平均耗时0.092 s,结果表明签名方案计算量小,效率较高,协议交互次数少,可有效的解决实时物流信息数据完整性保护和可靠性认证问题。

参考文献:

[1] 中华铁道网. 国务院:到2030年全国铁路营业里程达20万千米[EB/OL].(2017-02-06)[2018-5-24]. http://www.chnrailway.com/html/20170206/1554811.shtml。

[2] 中华人民共和国国家统计局. 中国统计年鉴[M]. 北京:中国统计出版社,2017.

[3] 沈江,周莉超,齐二石. 铁路物流的电子商务策略及其应用系统[J]. 计算机集成制造系统-CIMS,2001(7):58-61.

[4] 陶然,向静. 物流与信息流的辩证关系及其在铁路货物运输中的应用[J]. 中国铁道科学,2003(4):131-133.

[5] WANG G G,SHI T Y. Research actuality of railway intelligent transportation system technology[J]. Commu-nication & Transportation Systems Engineering & Information,2004,4(4):25-31.

[6] 魏臻,鲍红杰,陆阳,等. 企业铁路智能运输调度平台的关键流程[J]. 中国铁道科学,2006(4):101-105.

[7] 甘卫华,张婷婷,朱雨薇. 铁路物流中心的RFID技术应用[J]. 中国铁路,2010(9):33-36.

[8] GUO Z,ZHANG Z,LI W. Establishment of intelligent identification management platform in railway logistics system by means of the internet of things[J]. Procedia Engineering,2012,29(4):726-730.

[9] CHU X,LI W,ZHANG Z,et al. Design and implementation of electronic recognition system in internet of things for railway logistics[J]. Communications in Control Science and Engineering(CCSE),2014,2(1):78-81.

[10] LV H,WANG S,LIU Z. Application of wisdom logistics technology in railway transportation[C]// International Conference of Logistics Engineering and Management,Shanghai,2014:1321-1327.

[11] 张年,张诚,张志坚. 基于DEA的中西部地区铁路与公路物流协同发展研究[J]. 华东交通大学学报,2018,35(1):37-45.

[12] 深圳华视微电子有限公司. 双界面智能卡安全芯片CVF1040D [EB/OL].(2017-01-02)[2018-5-20].http://www.cvchip.com/china/cpsj/zn.

[13] JIA X,HE D,ZEADALLY S,et al. Efficient revocable ID-Based signature with cloud revocation server[J]. IEEE Access,2017,5(99):2945-2954.

[14] ZHANG Y,LIU J K,HUANG X,et al. Efficient escrow-free identity-based signature[C]// International Conference on Provable Security. Springer-Verlag,2012:161-174.

[15] AMARAPU R B,REDDY P V. Efficient identity-based parallel key-insulated signature scheme using pairings over elliptic curves[J]. Journal of Scientific & Industrial Research,2018,77(1):24-28.

[16] ZHANG L Y,HU Y,WU Q. New identity-based short signature without random oracles[J]. Procedia Engineering,2011,5:3445-3449.

[17] BONEH D,LYNN B,SHACHAM H. Short signatures from the weil pairing[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security:Advances in Cryptology. Berlin:Springer,2001:514-532.

Real-Time Tracking Protocol Based on Short Signature in Railway Logistics

Zuo Liming[1,2], Yi Chuanjia[1,2], Chen Yilin[1]

(1.School of Science, East China Jiaotong University , Nanchang 330013, China; 2.SEC Institute, Nanchang 330013, China)

Abstract: With the rapid development of software and hardware construction of railway logistics, big data and internet of things have been widely applied in railway logistics. The research of intelligent railway logistics system based on cloud computing, artificial intelligence and real-time online monitoring technology has become a hot topic. With the shortcomings of some railway intelligent logistics systems and design schemes, which is in lack of security authentication and data integrity protection in the process of information exchange, this paper proposed an efficient short signature scheme. Then, it designed a real-time logistics tracking protocol for railway based on the signature scheme. Finally, the protocol interaction of the signature scheme was simulated. The results show that the signature scheme has the advantages of less computation, higher efficiency and less protocol interaction, which can effectively solve the problems of data integrity protection and reliable authentication of real-time logistics information.

Key words: intelligent logistics; short signature; security protocol; real-time logistics tracking