文章编号:1671-4598(2022)04-0161-04 DOI:10.16526/j.cnki.11—4762/tp.2022.04.027 中图分类号:TP311 文献标识码:A

# 基于区块链技术的工控数据安全传输系统设计

薛中伟
(中国人民解放军92941部队,辽宁 葫芦岛 125000)

**摘要**:目前工控数据存在安全传输系统加密速率较低,导致加密过程稳定性较差;为了解决上述问题,基于区块链技术设计了一种新的工控数据安全传输系统;系统硬件采用嵌入式的麒麟990处理器,处理器由单片机、内存器以及扩展电路组成,采用双频JJSH-9传输器代替传统的传输器;传输器两端设置双频的GPS接收天线,完成工控数据的发送和接收工作,配置PLC多路导轨式控制器;利用非对称加密算法,对需要传输的工控数据进行加密,保证数据的安全性;非对称加密算法由数据加密和解密两部分组成,算法通过密钥空间序列自动生成密钥对,可以生成解密密钥,完成解密;实验结果表明,基于区块链技术的系统传输速率在15~20 kbps范围内,传输速率波动平稳;传输效率在95%~99%之间,能够保证加密速率和数据传输的稳定性。

**关键词**:区块链技术;工控数据;数据安全传输;传输系统

# Design of Industrial Control Data Security Transmission System Based on Blockchain Technology

XUE Zhongwei
(PLA 92941 Unit, Huludao 125000, China)

**Abstract**: Data secure transmission systemfor current industrial control existslow encryption rate, whichresults in poorstability of encryption process. In order to solve the above problems, a new industrial control data secure transmission system is designed based on blockchain technology. The system hardware adopts the embedded Kirin 990 processor, which is composed of single-chip microcomputer, memory and expansion circuit, anddual-frequency JJSH-9 transmitter is adopted to replace the traditional transmitter. The two ends of transmitter are equipped with dual-frequency GPS receiving antennas to complete the transmission and reception of industrial control data, and configure a PLC multi-channel guide rail controller. An asymmetric encryption algorithm is used to encrypt the industrial control data that needs to be transmitted to ensure data security. The asymmetric encryption algorithm is composed of two parts: data encryption and decryption. The algorithm automatically generates a key pair through the key space sequence, and the decryption key is generated to complete the decryption. The experimental results show that the systemtransmission ratebased on blockchain technology is within the range of 15~20 kbps, and the transmission ratefluctuatessmoothly; the transmission efficiency is between 95%~99%, which can ensurethe stability ofencryption rate and data transmission.

**Keywords**: blockchain technology; industrial control data; data secure transmission; transmission system

## 0 引言

目前,随着互联网技术的快速发展,工控网络和通信网络不断地融合,使得传统的工控内部传输模式更改成内外交互的传输模式,工控系统传输模式的改变虽然为工控系统带来翻倍的利润,与此同时,也为工控系统带来了数据传输安全威胁[1-2]。工控领域就此现象提出了工控数据安全传输系统加以维护,传统的系统利用一些数据加密技术,对工控数据进行加密,但是此操作也在一定程度上增加了工控传输数据的负载量,降低数据传输的时效性和稳定性[3-4]。

为了解决以上问题,本文提出了基于区块链技术的光口数据安全传输系统,提高系统的稳定性和数据传输加密性,在根本上消灭数据安全攻击。

## 1 基于区块链技术的工控数据安全传输系统设计

### 硬件设计

基于区块链技术的工控数据安全传输系统硬件结构如图1所示。

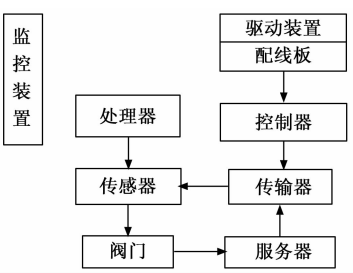


图1 基于区块链技术的工控数据安全传输系统硬件结构

**收稿日期**:2021-08-13; **修回日期**:2021-09-24。

**作者简介**:薛中伟(1983-),男,辽宁葫芦岛人,硕士,工程师,主要从事信息安全、通信新技术应用、网络通信方向的研究。

**引用格式**:薛中伟.基于区块链技术的工控数据安全传输系统设计[J].计算机测量与控制,2022,30(4):161-164.

分析图 1 可知，工控数据安全传输系统硬件结构主要由处理器、传输器及控制器组成。处理器负责驱动系统各个器件和通信协议的开启，控制器接收系统内部数据并判断其传输状态，控制工控数据的读取及传输，并将安全数据通过传输器传输至系统服务器，实现工控数据安全传输。下面对上述硬件模块进行具体介绍。

### 1.1 处理器设计

系统硬件区域处理器的主要工作是驱动系统各个器件和通信协议的开启，并维持系统的稳定运行，处理运行小错误，对于基于区块链技术的工控数据安全传输系统，对于处理器的配置要求极其严格，为了使处理器的性能达到设计要求，本文采用嵌入式的麒麟 990 处理器，处理器的工作频率为 50～100 MHz 范围内，超过设定的高强度运行持续时间后，处理器会立即调用散热器，降低处理器的工作负载，提高处理器的运行速率，并降低处理器的物理损耗。处理器配置 DOC 256M 的内置存储器，具有 32M 的缓存空间，与其他器件通过 BISO 接口和 PC104 串口进行连接，提高传输性能，处理器可以预测系统的运行网络攻击，驱动解决方案[5-6]。处理器串口端的连接方法结构如图 2 所示。

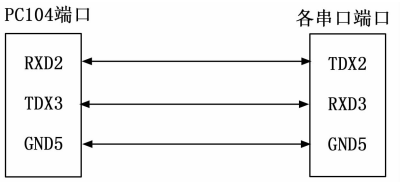


图 2 处理器串口电路结构示意图

### 1.2 传输器设计

传输器是基于区块链技术的工控数据安全传输系统硬件区域的主要器件，传输器是工控数据安全传输的凭借，传输器的传输性能直接影响到工控数据安全传输的消耗，本文连接的接口是 SRS232 串口，此传输器采用并行传输模型，传输器可以保证内部数据的传输速率为 19.2 kbps，并且传输完成率为 100%，不会出现数据丢包的情况。双频 JJSH-9 传输器支持 FTP 文件共享服务模式和 socket 数据交互模式，具有较强的适应性，传输器完成传输会向发送端发送一个通知，并且将指示灯的颜色由红色转变为绿色。数据传输器支持 HAMI1.4 信号，兼容 DHCP 1.4 通信协议，内部线缆采用非屏蔽五类线缆和六类线缆。传输器电路如图 3 所示。

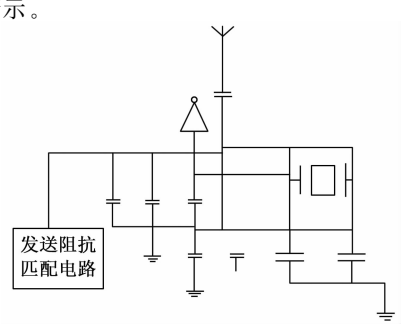


图 3 传输器电路图

### 1.3 控制器设计

控制器的工作任务是监测系统内部数据传输的状态，一旦监测到数据攻击，立即将系统实时的数据进行锁定，使工控数据处于不可获取、不可读取修改的属性，保证系统内工控数据传输的安全，控制器一直运行在系统的后台。本文为硬件区域控制器的电源为 24 V，具有独立供电形状，内置 PID 模糊算法，保证控制器指令的执行，控制器具有全部参数可读写功能，对于任意工控数据都设定一个控制起始位，2 个控制结束位，以及就校验流程。控制器的有效电阻信号为 0～500 Ω，标准的毫伏信号为 0～100 mV，控制周期为 0.5 s，控制指令的执行触点容量为 250 V/0.8 A，采用线性电流输出，默认为 1～5 V[7-9]。

### 1.4 电源设计

电源虽然是一个配件，但是对于系统内部任意一个器件的有效使用周期都存在关系，为了降低系统内部设备电磁的辐射量，基于区块链技术的工控数据安全传输系统硬件区域采用高性能的华硕 TUF 突击手额定电源模块完成硬件区域的配置[10-12]。电源电路如图 4 所示。

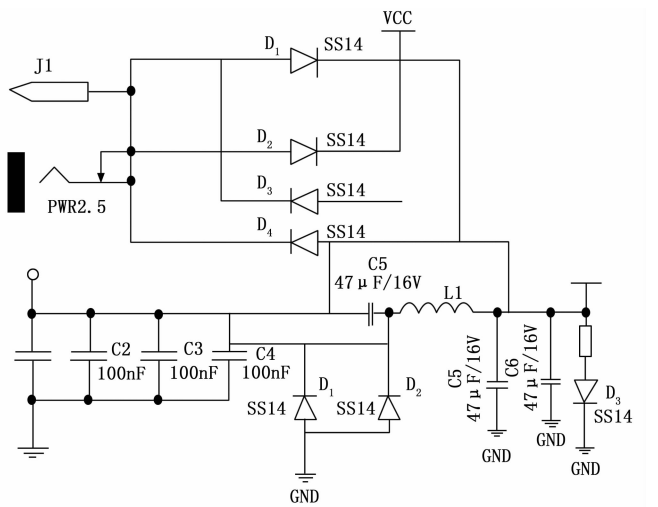


图 4 电源电路图

此电源模块内部设计了双滚珠轴承风扇，此风扇的性能高于磁浮轴风扇，可以定期清理系统内部的灰尘，提高系统器件的使用周期。电源配置 ROG 显卡，保证电源持续输出电能的同时，0 dB 噪音的产生。电源的转换效率通过 80 plus认证，有效输出电压为 100～240 Vac，输出电流为 25 A、20 A、45 A、3 A 共 4 个等级，对应的有效额度功率为 120 W、549 W、9.6 W、15 W[13]。

## 2 基于区块链技术的工控数据安全传输系统设计软件设计

区块链的本质是一个共享数据库，共享数据库内部的所有数据具有不可伪造性、可以追溯性、公开透明性、不可篡改性，并具有独特的身份验证机制。对于本文分析的工控数据安全传输系统来说，区块链技术是最合适的数据传输备份、存储技术，本文采用公有链形式，主要调用区块链技术的数据不可篡改功能和身份验证功能[14-15]。区块链技术可以

作为数据传输的保护层，辅助需要传输的工控数据进行传输，在接收端数据录入前会进行身份验证，保证传输的准确性。区块链技术执行的过程是发送端向区块链技术发送接收端的地址信息和通信信号频段，然后区块链技术在工控数据头增加一个时间戳字节，可以根据此字节序列对工控数据传输的信息进行查询，最后区块链技术与系统传输技术共同完成数据的传输。传输端通过区块时间戳字节的长度和信息，检验工控数据是否被拷贝和篡改[16-18]。具体的工控数据利用区块链技术传输文件流程如图 5 所示。

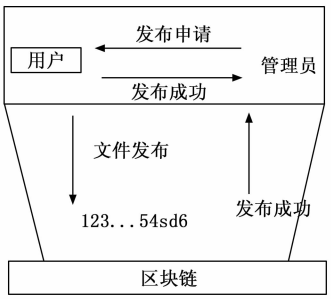


图 5　工控数据利用区块链技术传输文件流程示意图

为了达到工控数据安全传输系统的设计要求，采用非对称加密算法对工控数据进行加密设计，实现数据上链，具体非对称加密算法的加密原理如图 6 所示。

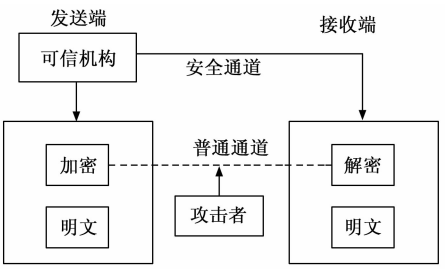


图 6　非对称加密算法的加密原理示意图

算法的工作流程如下：

首先调用非对称加密算法，算法依据工控数据标题自动生成一个密钥对，发送到数据接收端和数据发送端进行备份，作为解密数据的密文。数据接收端利用密钥才可以接收工控数据，以此保证数据传输的加密性和安全性。

对需要传输的工控数据进行安全加密后，本文利用多输入输出模型对需要传输的工控数据完成传输操作。多输入输出模型的加密传输机制结构如图 7 所示。

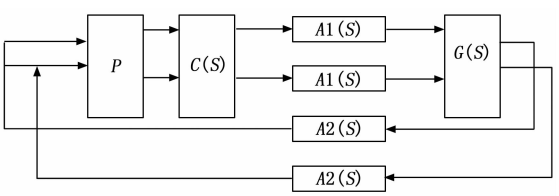


图 7　多输入输出模型的加密传输机制结构图

多输入输出模型是一款具备加密性质的传输模型，在数据传输过程中利用有理传递函数矩阵将数据接收端和数据发送端进行配对，数据传递通道的传递函数如下所示：

$$y(t)=\mathrm{diag}\{(e^{-t^{\tau}},e^{-\tau 2^{\tau}}\cdots\cdots.e^{-\tau 3^{\tau}})*u\}+det(j(s)+g(s)) \tag{1}$$

其中：$j(s)$、$g(s)$ 分别表示多输入输出模型传递数据的输入端向量和输出端向量；$\tau$ 表示传输通道的总延时；$u$ 表示反馈通道的总延时；$y(t)$ 表示传输模型的传输特征方程。

根据以上公式计算出需要传输工控数据的传输特征量，选择工控数据传输的最佳通信信道，完成工控数据的安全传输。

## 3　实验分析

通过以上对工控数据安全传输系统硬件器件性能和软件技术的分析，完成了基于区块链技术的工控数据安全传输系统的设计，为了检验此系统的数据安全传输加密性、稳定性和时效性，本文接下来借助基于非对称加密算法的工控数据安全传输系统（传统系统 1）和基于数据隔离的工控数据安全传输系统（传统系统 2），共同完成对比试验，得出测试结果，完成系统性能的检验。

### 3.1　实验步骤

实验前将 3 个系统嵌入到 3 台工控系统内的计算机内，试验测试分别准备 3 份相同的工控数据测试样本，每份测试样本都包括 3 组 500 字节的工控数据，3 组 1 000 字节的工控数据、3 组 3 000 字节的工控数据。系统嵌入的计算机会记录试验测试过程中的所有试验数据，作为试验分析数据，测试样本在测试开始时全部发送到 3 个系统内，为了降低试验误差，将数据接收端设置为一个 ip 地址，因为每个系统发送数据的 ip 地址不同，根据不同的 ip 地址就可以分辨出每个系统传输的对应结果。试验通过对比 3 个系统完成工控数据安全传输的时间、传输稳定性以及数据安全传输效率，得出试验结论。当接收端全部接收到控制中心发布的工控数据包后，结束试验，将系统在工控系统内部计算机内删除，整理试验数据，绘制试验数据结果图，进行试验数据的分析。

### 3.2　实验结果与分析

具体工控数据加密长度执行时间实验结果如图 8 所示。

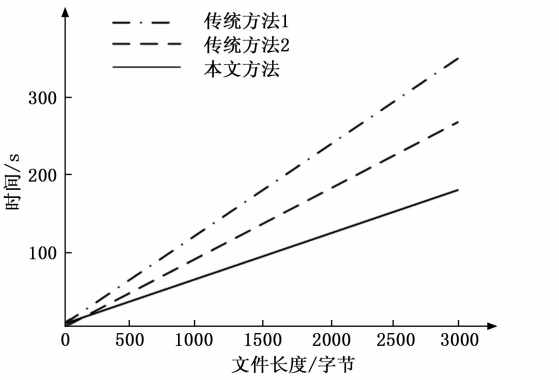


图 8　不同系统对于工控数据加密长度执行时间结果图

观察图试验结果图可以了解到 3 个系统在工控数据字节长度不断增加的变量控制下，数据安全加密执行时间不断地增加，并且两个变量的关系成正比，3 个由试验数据总

结绘制的试验线段的倾斜度表示，基于区块链技术的工控数据安全传输系统的斜率最小，传统系统 2 的线段斜率最大线段的斜率越小表示工控数据字节长度变量和加密时间变量的关系度强，因此可以得到本文设计系统的安全加密性能对于工控数据字节的影响波动最小。

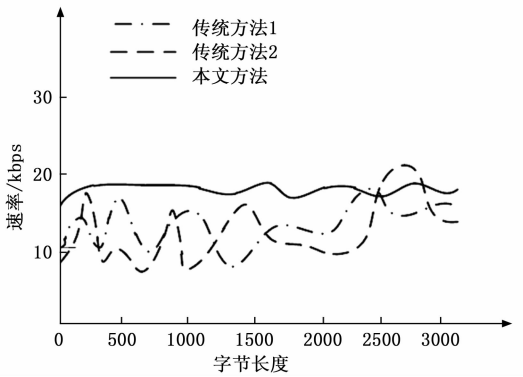


图 9 不同系统在数据传输过程中稳定性示意图

观察图 9，可以了解到 3 个系统在数据传输过程中，工控数据传输的速率波动图，其中基于区块链技术的工控数据安全数据系统每组数据传输过程中速率都保证在 15～20 kbps范围内，没有太大的速率波动。传统系统 1 在每组工控数据传输中的速率波动较大，最低速率达到 8 kbps，最高速率达到 17 kbps；传统系统 2 在每组工控数据传输中的速率波动较大，最低速率达到 6 kbps，最高速率达到 22 kbps；因此可以证明基于区块链技术的工控数据安全传输系统具有传输稳定性。

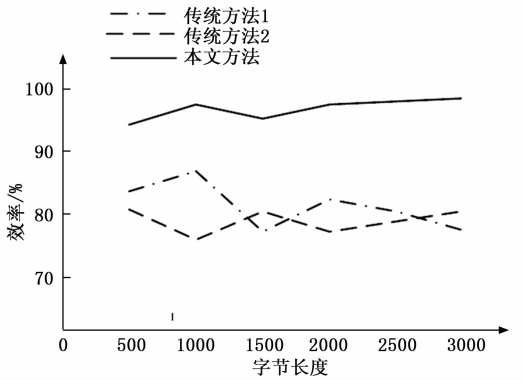


图 10 不同系统对于工控数据传输效率示意图

观察图 10，可以直观地了解到，无论需要传输工控数据的字节多大，系统的传输效率对比其他两种传统系统来说都是最高的，并且传输效率始终在 95%～99%之间，达到了本文设计的系统性能标准。得到这一试验数据的关键在于，本文调用了区块链技术和工控数据加密传输框架，在传输前根据传输内容，合理调用传输信道，节省数据传输的时间和缩短数据安全传输的流程，保证系统的传输效率。最后对接收端数据包的检验，检验工控数据的完整性，试验结果图中虚线表示每组工控数据传输数据包字节的完整的，观察上图，可以证明本文设计系统数据安全传输的安全性。

综上所述，本文设计的基于区块链技术的工控数据安全传输系统具有稳定性和较高的传输效率，并且可以保证工控数据传输的安全性。

## 4 结束语

在互联网技术的映射下，工控数据安全数据技术的研究正处于起步阶段，本文针对工控数据安全数据的威胁，利用区块链技术分析需要传输工控数据的字节特征，保证数据传输的时效性和稳定性，提出基于区块链技术的工控数据安全传输加密方法。实验结果表明，该方法能够保证工控数据传输速率在 15～20 kbps 范围内，且传输效率在 95%～99%之间，体现了区块链技术的高效性及安全加密性能。

**参考文献：**

[1] 谭朋柳，王雪娇，唐伟强，等. 基于区块链的 MCPS 数据安全架构设计 [J]. 计算机工程与设计，2020，41 (12)：47－53.
[2] 段 平. 基于区块链及分层加密技术的数据传输控制系统设计 [J]. 计算机测量与控制，2020，28 (10)：81－85.
[3] 艾学瑛. 基于区块链和 5G 物联网的溯源及异常数据预警系统 [J]. 电子设计工程，2020，28 (10)：108－112.
[4] 朱凤霞. 基于区块链技术的交易数据库加密技术 [J]. 电子设计工程，2020，28 (3)：93－97.
[5] 韩菊茹，纪兆轩，李一鸣，等. 基于区块链的可信日志存储与验证系统 [J]. 计算机工程，2019，45 (5)：19－23.
[6] 李孟特，顾春华，温 蜜. 基于区块链的充电交易数据安全存储平台设计 [J]. 计算机工程与应用，2020，56 (21)：85－90.
[7] 朱 曦，吴 浩. 基于区块链技术的云身份管理信任模型设计 [J]. 山东科学，2020，33 (3)：100－108.
[8] 隋新玉，王云清. 基于区块链的电商数据分发技术研究 [J]. 电子设计工程，2020，28 (7)：69－73.
[9] 屈 阳，钱蓓力，张呈宇，等. 一种基于区块链技术的智能运维系统的设计与实现 [J]. 电信科学，2020，36 (5)：156－162.
[10] 葛 琳，季新生，江 涛，等. 基于区块链技术的物联网信息共享安全机制 [J]. 计算机应用，2019，39 (2)：458－463.
[11] 王英资，侯 珏，张 越. 基于区块链技术的数据管理 [J]. 电子设计工程，2019，27 (6)：87－90，95.
[12] 朱凤霞. 基于区块链技术的交易数据库加密技术 [J]. 电子设计工程，2020，48 (3)：99－103.
[13] 谷昱君，黄永章，付文启，等. MGP 系统参与新能源电网调频的实验研究 [J]. 大电机技术，2020 (1)：38－42.
[14] 韩宇龙，韩海庭，王政宏，等. 基于区块链和安全终端的物联卡交易管理系统设计与实现 [J]. 电子设计工程，2019，27 (21)：32－35.
[15] 梁作放，潘 华，朱兆顺，等. 泛在电力物联网的技术架构与关键技术研究 [J]. 内蒙古电力技术，2020，38 (1)：27－30.
[16] 陈瑞滢，陈泽茂，王 浩. 工业控制系统安全监控协议的设计与优化研究 [J]. 信息网络安全，2019，218 (2)：60－69.
[17] 徐元清，卓 蔚. 区块链技术在烟草系统工控安全中的应用 [J]. 微型电脑应用，2019，35 (3)：113－116.
[18] 徐海洲，周纯杰. 基于 SDN 的工控信息安全防护系统设计及实现 [J]. 制造业自动化，2019，41 (4)：164－168.