文章编号:1671-4598(2021)06-0119-04 DOI:10.16526/j.cnki.11—4762/tp.2021.06.025 中图分类号:TP309 文献标识码:A

基于区块链技术的机器人数据加密传输控制系统设计

杨 亮
(陕西工业职业技术学院 航空工程学院,陕西 咸阳 712000)

摘要:针对传统方法机器人数据加密传输缺少信息交互步骤,信息置换过程出现失误,导致加密效果较差的问题,提出了基于区块链技术的机器人数据加密传输控制系统设计;设计机器人硬件结构,在Ts—210型号可信存储器、NoSQL数据库、X86服务器上完成信息存储、操作与分析;基于区块链技术进行机器人数据去中心化和抗篡改信息交互,分解机器人数据客户端传输信息,经信息编码处理后,可获取信息加密矩阵;以原始信息矩阵为依据,选择加密信息初始密钥,使用区块链技术设计机器人数据加密传输控制系统软件加密流程;引入信息签名验证机制,提取机器人上传加密信息,通过SHA—256哈希算法控制加密流程;由实验结果可知,该方法置乱结果与理想结果一致,数据吞吐量平均值为0.95 Gbps,为机器人高效率加密传输信息提供帮助。

关键词:区块链;智能机器人;多传感器信息;加密控制;哈希算法

Design of Robot Data Encrypted Transmission Control System Based on Blockchain Technology

Yang Liang
(Department of Aeronautical Engineering, Shaanxi Polytechnic Institute, Xianyang 712000, China)

Abstract: In view of the lack of information interaction steps in the traditional method of robot data encryption transmission, and the error in the information replacement process, resulting in poor encryption effect, the design of a robot data encryption transmission control system based on blockchain technology is proposed. Design the hardware structure of the robot, and complete the information storage, operation and analysis on the Ts—210 model trusted memory, NoSQL database, and X86 server. Based on the blockchain technology, the robot data decentralization and tamper—resistant information interaction are carried out, and the information transmitted by the robot data client is decomposed. After the information encoding process, the information encryption matrix can be obtained. Based on the original information matrix, select the initial key of encrypted information, and use blockchain technology to design the software encryption process of the robot data encryption transmission control system. Introduce the information signature verification mechanism, extract the encrypted information uploaded by the robot, and control the encryption process through the SHA—256 hash algorithm. It can be seen from the experimental results that the scrambling results of this method are consistent with the ideal results, and the average data throughput is 0.95 Gbps, which provides help for the efficient encrypted transmission of information by the robot.

Keywords: block chain; intelligent robots; multi—sensor information; encryption control; Hash algorithm

0 引言

机器人是由计算机控制的可编程自动化机器,根据环境和操作的需要,它具有某些环境感知能力(如视觉、力感、触觉、接触感等)、语言功能、逻辑思考、判断和决策功能等,以代替人在环境中操作[1]。由于有些机器人涉及现场监测的敏感数据,采集的传感器数据容易被人为篡改和破坏,因此在实际工作中需要保密[2]。随着机器人技术的发展,单靠传感器提供信息已不能满足现代移动机器人的需要,为此,相关学者对机器人数据加密传输控制系统作出了研究。有学者将多传感器融合技术引入了机器人应用领域。该方法中只有数字水印等传统数据保护技术通过中央数据库进行存储,数据和交易过程主要由第三方实施,存在很大安全风险,交易信息容易被篡改;采用微加密算法对采样报文的密钥内容进行加密,循环冗余校对验证码以保证解密报文的完整性。但是该系统的网络负载率很高,难以保证现场采样数据的真实性。

基于上述考虑,本文研究了基于区块链技术的机器人数据加密传输控制方法。利用区块链来保护机器人的整个生命周期以及采集到的敏感数据,从而达到机器人数据加密传输。

收稿日期:2021-01-12; **修回日期**:2021-03-24。

作者简介:杨 亮(1984-),男,陕西咸阳人,硕士,讲师,主要从事传感器技术和工业机器人技术等方向的研究。

引用格式:杨 亮.基于区块链技术的机器人数据加密传输控制系统设计[J].计算机测量与控制,2021,29(6):119-122,163.

1 基于区块链技术的机器人加密总体结构分析

机器人控制系统通过识别数据特征发出指令后，驱动机构根据指令信号做出相应的动作，具有实时监控、检测等功能，能将监控信息反馈给控制系统。通过与设置信息对比，可以调整执行器，以保证机器人动作符合预定要求[3]。通过远程视频服务，扩大了视频监控应用范围，能够准确地获取外部条件变化，及时调整机器动作，以适应外部环境变化，提高机器人移动准确性[4]。上位机通过局域网直接连接到服务器端，进行远程控制和播放，提高了信息反馈效率。机器人的每个模块都有一个或多个线程，可根据需要启动有用线程或阻塞无用线程，能够有效提高机器人系统执行效率[5]。除了远程控制、自动采样等业务功能外，传感器数据也被定期封装，通过非对称加密通信技术签名后发送给可信存储服务模块，以完成数据安全功能。基于区块链技术的机器人加密总体结构如图 1 所示。

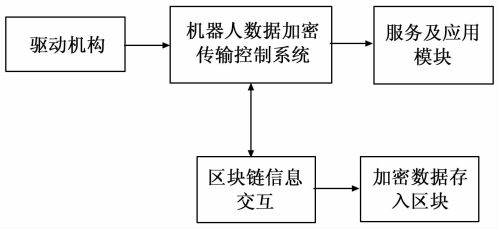

图 1 机器人加密总体结构示意图

2 基于区块链技术的机器人数据加密传输控制系统硬件设计

2.1 可信存储模块

可信存储主要模块是机器人数据加密传输控制系统硬件的重要组成部分，它的功能是存储指令和数据，可以被中央处理机直接随机存取[6]。存储模块面板包括各种状态指示器和 USB 接口，因为存储芯片容量有限，主存通常是由一定量芯片构成的比特扩充[7]。比特扩充指的是只在单位数（增加字长）上扩充，某些扩展接线方式链接地址线，每个芯片选择行和并行读写存储器芯片，而每个芯片的数据线都单独列在单词扩展表中[8]。单词扩展是指仅有的单词数量扩展，而比特数没有变化。字元扩展与芯片的地址线、数据线和读写控制线平行，而芯片选择信号以区别芯片字元扩展和字元扩展[9]。当形成大容量容器的时候，通常需要在字数和比特方向同时展开。

将机器人收到的传感器数据拆分并校验，检查数据源可靠性；将传感器数据存储在数据库中，通过 Hash 算法计算其加密情况，并将其存储在加密的数字货币区块链中以防止篡改[10]。

2.2 数据库

本文采用 NoSQL 数据库作为机器人加密数据存储数据库，其中 mysql、MS SQL server 和 mongodb 可用于机器人多传感实际操作，在采集利用机器人加密数据后，将数据存储在 NoSQL 数据库中，能够提升数据加密存储的可靠性。

2.3 服务及应用模块

在 X86 服务器上，使用 Intel 或其他与 X86 指令集和 windows 操作系统兼容的处理器芯片，即 PC 架构。服务及应用模块利用 PC 架构获取数据库数据，能够向用户提供采样数据分析服务，并提供数据显示等常用应用[11]。

2.4 区块链模块

该技术具有数据分散、数据库安全、可靠等特点。该技术的核心特征就是去中心化，去掉了第三方管理机构，数据存储直接由网络中的验证节点群集处理；一个可靠数据库意味着每个验证节点都有其完整的数据记录，所以，即使某些节点受到攻击或者数据丢失，整个系统仍然可以在不崩溃的情况下工作；安全可靠是指区块链技术利用加密技术对数据进行签名，使信息不会被篡改，从而使数据的存储更加可靠[12]。

图 2 中显示了区块链链接结构，链接主要取决于散列值。当区块内的数据被恶意篡改时，区块计算的散列值将更改。对比下一区块中存储的原始散列值，可以发现异常，有效地防止了数据被恶意篡改。

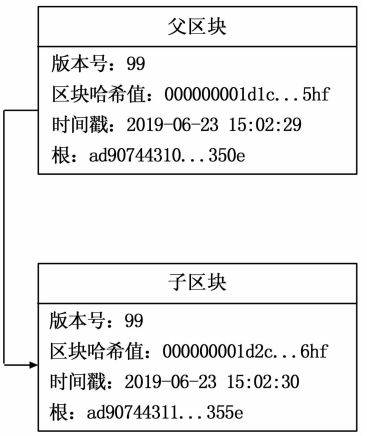

图 2 区块链链接结构示意图

3 基于区块链技术的机器人数据加密传输控制系统软件设计

在硬件模块设计的基础上，设计机器人数据加密传输控制系统软件流程。通过区块链信息交互实现数据的交互传输，对数据进行编码处理得到信息加密矩阵，通过信息签名验证机制将得到加密数据存入区块，实现机器人数据加密传输控制。

3.1 区块链信息交互

区块链上数据交互是指进入区块链记录的交互过程，其主要区别于区块链下信息交互过程，所有链上交互都属于去中心化和抗篡改的交互[13]。在机器人出厂部署前，硬件中包含公、私钥地址。在机器人部署上线时，机器人通过数据客户端远程调用接口，实现交互信息传输。

3.2　数据加密设计

将机器人数据客户端传输的信息分解成 m 组信息，将这些信息全部发送到待传输节点中[14]。在发送前，信息源点会产生 r 个 m 维向量，每个向量都含有 m 个分量，可表示为 $w_1,w_2,\cdots,w_r$。

经过信息编码处理后的 r 个 m 维向量，可得到 r 个数据包，可表示为 $b_1,b_2,\cdots,b_r$，计算公式为：

$$b_r = w_r(a_1a_2\cdots a_m)^t, i = 1,2,\cdots,r \tag{1}$$

信息源点全部完成编码处理后，统一打包 r 个 m 维向量，由此得到的 r 个数据包全部传输到目标节点之中[15]。该节点能够接收到较多信息，编码处理的向量是具有无线性的，由此完成的信息加密矩阵可表示为：

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{22} & \cdots & w_{21} \\ \vdots & \vdots & & \vdots \\ w_{r1} & w_{r2} & \cdots & w_{rm} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix} \tag{2}$$

以公式（2）原始信息矩阵为依据，选择加密信息初始密钥，该密钥是由 512 个字节组成的，对于信息存储来说是非常安全的。在该加密情况下，使用区块链技术设计加密流程：

Step1：机器人自主选择文件，获取相关文件信息；

Step2：数据分类与识别；

Step3：分类后的数据，在机器人中是否显示是第一次识别？如果是，则将机器人作为第一个识别模板；如果不是，则说明该信息异常，无法加密，需重新选择数据；

Step4：根据公式（2）得到信息加密矩阵；

Step5：判断是否删除异常文件，如果是，则机器人直接删除异常文件，由此完成加密处理。

3.3　控制方案设计

3.3.1　引入信息签名验证机制

在区块链技术中，各记账节点必须维护同一账本，因此，有必要引入信息签名验证机制[16]，以实现信息间的一致性处理。针对节点可能存在恶意操作，引入信息签名验证机制，如图 3 所示。

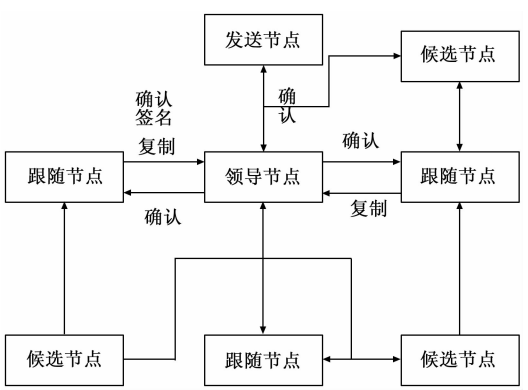

图 3　信息签名验证机制

由图 3 可知，确认发送节点是否正常，确认后发送给领导节点，领导节点经过复制与确认后，发送给跟随节点，待签名确认完成后，可将结果发送给候选节点。

3.3.2　控制流程

在信息签名验证机制支持下，设计控制流程，首先提取机器人上传加密信息，通过 SHA－256 哈希算法，得到定长短字符串[17]；然后发起区块链上数据交互，记录信息加密到区块链上。该控制过程如下所示：

Step1：设定信息发送方机器人为主公钥地址，接收方机器人为原始信息来源公钥地址；

Step2：检索公钥地址尚未完成的交互输出信息；

Step3：选择一个合适的交互信息输出项，将加密信息存入 OP _ RETURN 脚本中，OP _ RETURN 脚本存入区块链过程为：需先创建一个交互信息，完善 OP _ RETURN 脚本内容，实现交互数据封装签名。

为了说明该步骤，将以下机器人多传感数据作为例子：

2019－04－20 08:00:00 0001 62 83 74；

2019－04－20 08:00:30 0001 55 75 70；

2019－04－20 08:01:00 0001 50 80 82；

2019－04－20 08:01:30 0001 48 85 72；

2019－04－20 08:02:00 0001 60 91 73；

使用 SHA－256 哈希算法计算上述多传感数据的加密信息，得到定长加密结果。将该结果附加上前缀标识“robot－”，由此得到最终存入区块的加密数据[18]。使用该算法安全性高，将上述结果存入 OP _ RETURN 脚本中，并构造信息交互传输，得到其在区块链上的索引 ID，机器人随时查询验证，实现机器人数据加密传输控制。

4　实验结果

4.1　实验数据及方法

为了验证基于区块链技术的机器人数据加密传输控制系统的合理性，在机器人坐标系统模型下进行实验验证分析。实验仿真平台选用 Matlab 软件，在仿真软件中设计机器人坐标系统模型如图 4 所示。

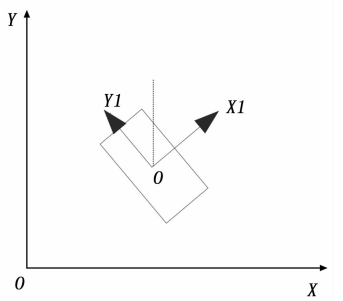

图 4　机器人坐标系统模型

由图 4 可知，该坐标系是一个直角坐标系，机器人位姿可用该坐标系表示。使用 6 个传感器采集机器人运动数据，分别为 W1、W2、W3、W4、W5、W6，测试数据传输过程中的置乱情况，在此基础上测试机器人吞吐量，测试

其信息加密情况。

4.2 置乱情况下加密效果分析

将 6 个传感器采集到的信息进行置乱处理，理想情况下得到的数据位置依次为：W1＝W6、W2＝W3、W3＝W2、W4＝W5、W5＝W4、W6＝W1。在置乱情况下，分别使用数字水印、微加密算法和所提基于区块链技术的机器人数据加密传输控制系统对数据加密传输情况进行对比分析，结果如图 5 所示。

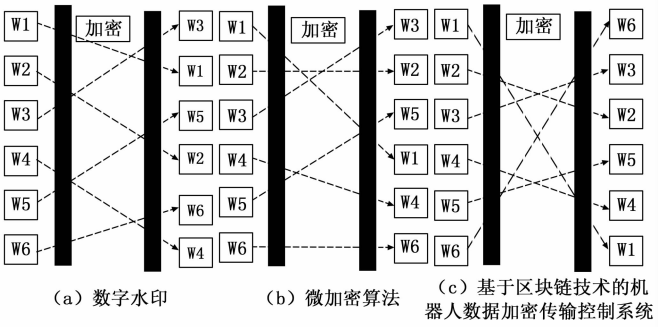

图 5 信息置乱情况下不同方法加密传输控制效果对比分析

由图 5 可知：信息置乱情况下不同方法加效果不同，详细分析内容为：

1）使用数字水印加密算法信息全部置乱，不会出现信息丢失现象，但置乱结果与理想结果不一致，数据位置依次为：W1＝W3、W2＝W1、W3＝W5、W4＝W2、W5＝W6、W6＝W4。说明使用该算法虽然对每个信息进行水印处理，但容易受到多个传感器信息采集混乱影响，导致加密效果较差。

2）使用微加密算法，信息无法全部置乱，会出现信息丢失现象，置乱结果与理想结果不一致，数据位置依次为：W1＝W3、W2＝W2、W3＝W5、W4＝W1、W6＝W6。说明使用该算法，加密力度不够，容易受到多个传感器信息采集混乱影响，导致加密效果较差。

3）使用基于区块链加密传输控制方法，信息全部置乱，不会出现信息丢失现象，置乱结果与理想结果一致，数据位置依次为：W1＝W6、W2＝W3、W3＝W2、W4＝W5、W5＝W4、W6＝W1。

4.3 不同数据量情况下加密效果分析

当数据在没有被外界黑客攻击情况下，机器人所能接收到的信息即为吞吐量，改变信息接收量来验证吞吐量对信息加密情况。

分别使用数字水印、微加密算法和基于区块链技术的机器人数据加密传输控制系统对信息吞吐量进行对比分析，设置数据接收量为 0～105 bit，测试不同方法的吞吐量，吞吐量越高则表明数据加密的压缩解压性能越好，数据加密效率越好。实验结果如图 6 所示。

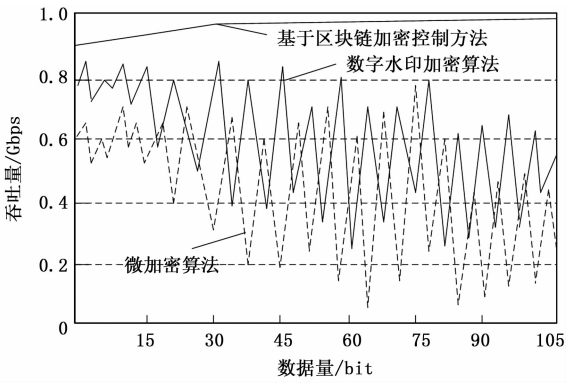

图 6 不同信息吞吐量情况下不同方法加密效果对比分析

由图 6 可知：使用数字水印加密算法，数据吞吐量平均值为 0.6 Gbps；使用微加密算法，数据吞吐量平均值为 0.6 Gbps；使用基于区块链技术的机器人数据加密传输控制系统，数据吞吐量平均值为 0.95 Gbps。通过上述分析结果可知，使用基于区块链技术的机器人数据加密传输控制系统的加密效率更好。

5 结束语

利用区块链技术对机器人数据进行加密传输控制，采用区块存储数据，通过区块链加密技术和协商机制实现数据加密传输，具有较好的安全性。此方案具有安全性高、实用性强、成本低的特点。该研究技术也可广泛应用于物联网设备数据交互、大数据隐私保护、电子证据保存与识别等技术领域。

参考文献：

[1] 李明飞. 基于区块链的自组织网络多信道访问控制仿真 [J]. 计算机仿真，2019，36 (5)：480－483.

[2] 杜瑞忠，谭艾伦，田俊峰. 基于区块链的公钥可搜索加密方案 [J]. 通信学报，2020，41 (4)：114－122.

[3] 徐 健，温 蜜，张 凯. 结合区块链技术的改进 K－匿名激励机制方案 [J]. 计算机工程与应用，2020，56 (6)：111－116.

[4] 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.

[5] 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.

[6] 霍延军，袁旭华. 基于 CARLA－PSO 组合模型的机器人步态控制系统设计 [J]. 计算机测量与控制，2020，28 (9)：249－253.

[7] 田有亮，杨科迪，王 缵，等. 基于属性加密的区块链数据溯源算法 [J]. 通信学报，2019，40 (11)：101－111.

[8] 卢勇威，黄良永. CAD/CAM 与机器人的轨迹映射及集成控制系统设计 [J]. 机械设计与制造，2019 (6)：162－165.

[9] 王 童，马文平，罗 维. 基于区块链的信息共享及安全多方计算模型 [J]. 计算机科学，2019，46 (9)：169－175.

[10] 庞党锋，宋亚杰，王春光，等. 基于工业机器人的数控加工控制系统设计 [J]. 机床与液压，2020，48 (21)：67－69.

(下转第 163 页)