文章编号:1671-4598(2024)10-0139-07 DOI:10.16526/j.cnki.11-4762/tp.2024.10.020 中图分类号:TP242 文献标识码:A

基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计

张西霞[1], 王 欢[1], 于 浪[2]
(1. 西安思源学院 理工学院, 西安 710038; 2. 西安长天长软件股份有限公司, 西安 710065)

摘要: 在嵌入式机器人中, 包含大量重要的运行数据, 这些数据需要连接到网络上进行通信和传输, 使其容易受到多种网络攻击; 如果这些数据被篡改则会导致机器人无法正确执行任务, 造成安全隐患; 因此, 为了确保数据的完整性和安全性, 设计基于区块链的嵌入式机器人运行数据防篡改传输控制系统; 在嵌入式主控板电路的配合下, 协调机器人运行数据解算模块、传输数据矫正模块、控制系统微处理器之间的实时连接关系, 完成传输控制系统硬件部分设计; 设计控制系统环境和角色对象, 并根据不同角色身份, 确定运行数据在区块链 RBAC 组织中的访问能力, 基于区块链中的哈希值实现对运行数据防篡改链码的恢复处理, 完成基于区块链的嵌入式机器人运行数据防篡改方案的设计; 提取运行数据中的关键嵌入部分, 建立防篡改要求下的机器人运行数据聚集索引, 计算篡改率数值, 并实施针对性控制, 完成基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计; 实验结果表明, 经过上述系统的防篡改控制作用后, 数据传输效率明显提高, 非关联信息难以入侵嵌入式机器人运行系统, 也无法篡改关键传输数据, 有助于保障机器人运行数据的安全性。

关键词: 区块链; 嵌入式机器人; 运行数据; 哈希值; 链码恢复; 聚集索引

Design of Embedded Robot Operation Data Tamper-Proof Transmission Control System Based on Blockchain

ZHANG Xixia[1], WANG Huan[1], YU Lang[2]
(1. Institute of Technology, Xi'an SiYuan University, Xi'an 710038, China;
2. Xi'an Jointsky Software Co., Ltd., Xi'an 710065, China)

Abstract: In embedded robots, there is a large amount of important operational data, which needs to be connected to the network for communication and transmission, making them vulnerable to various network attacks. If these data are distorted, it will cause robots to be unable to correctly perform tasks, resulting in security risks. Therefore, in order to ensure the integrity and security of data, an embedded robot operation data transmission control system based on blockchain is designed to prevent tampering. With the coordination of the embedded main control board circuit, the real-time connection relationship between the robot operation data calculation module, transmission data correction module, and control system microprocessor is coordinated to complete the hardware design of the transmission control system. Design the control system environment and role objects, and determine the access capability of running data in blockchain RBAC organization based on different role identities. Based on the Hash value in blockchain, implement the recovery processing of anti tampering chain codes for running data, and complete the design of the embedded machine's anti tampering data scheme based on blockchain. Extract the key embedded parts from the running data, establish the robot running data aggregation index under anti tampering requirements, calculate the tampering rate value, implement the targeted control, and complete the design of the embedded robot running data anti tampering transmission control system based on blockchain. Experimental results show that after the anti tampering control effect of the above system, the data transmission efficiency is significantly improved. It is difficult for non associated information to invade the embedded robot operating system, it cannot be tampered with critical transmission data, which helps to ensure the security of robot operating data.

Keywords: blockchain; embedded robots; operating data; hash value; chain code recovery; clustered index

0 引言

嵌入式机器人是一种将计算机硬件和软件集成到机器系统中, 以实现自动化和智能化的机器人技术[1]。这种机器人通常具有嵌入式处理器、传感器、执行器和其他电子设备, 可以执行各种任务。嵌入式机器人的主要特点是具有高度集成化和智能化性能, 由于其内部集成了计算机硬件和软件, 因此可以自主地感知、决策和执行任务, 且无需人工干预。此外, 嵌入式机器人还可以通过无线通信与外部设备进行连接, 实现远程控制和监控。机器人运行数

收稿日期:2024-03-06; **修回日期**:2024-05-06。
作者简介:张西霞(1985-),女,硕士,讲师。
引用格式:张西霞,王 欢,于 浪.基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计[J].计算机测量与控制,2024,32(10):139-145,153.

据包括传感器数据、控制数据、故障诊断数据等多种表现形式，对于这类数据的防篡改处理，是为了保障数据的完整性与真实性，主要采用加密数字签名的方式，一旦数据被篡改，数字签名就会发生变化，导致安全隐患。为此，需要研究一种数据防篡改传输控制系统。

在实际应用过程中，文献［2］设计一种新的操作日志篡改保护系统，以解决系统管理员的不受限制导致的安全威胁，提高 dbms 操作日志系统的安全性。文献［3］针对现有加密系统存储开销大、稳定性差的问题，设计一种结合变动数据捕获机制和消息摘要的防篡改控制系统，有效识别篡改行为。然而上述方法存在单点故障的风险，一旦攻击者成功入侵或破坏系统的某个关键节点，则会导致整个系统的数据受到威胁。文献［4］设计基于嵌入式 S3C6410 的机器人控制系统，首先在机器人自动导航框架的基础上，搭建嵌入式的硬件平台结构；然后联合相关运动学数据，建立机器人导航行为模型；最后设计基于模糊控制的调向控制策略，以实现对 S3C6410 机器人运行数据的传输与控制。但由于该系统没有明确说明运行数据之间的实时占位情况，所以控制指令的执行并不能有效避免数据篡改行为的出现。文献［5］设计基于空间视觉的机器人柔性控制系统，设计了一种 IBP-PID 的数据信息控制方法，可以在有效控制柔性机器人运行数据传输行为的同时，避免信息文本之间出现相互覆盖的行为，又通过核准检验的方式，对系统进行了校正处理。特定情况下，运行数据可能会受到入侵信息的干扰，从而出现缓慢传输行为，若不能及时制止该问题，极有可能使目标传输数据受到攻击性威胁，从而面临被篡改的风险。

区块链是一种去中心化的分布式账本技术，它结合了分布式存储、点对点传输、共识机制、密码学等技术手段，通过不断增长的数据块链记录交易和信息，以确保数据的安全和透明性。每个数据块都连接到前一个块的哈希值，形成连续的链，保障了交易历史的完整性。为此，将区块链技术应用到计算机网络、智能化平台等多个领域之中，能够在保障信息完整性的同时，避免不安全数据传输行为的出现，从而最大化满足网络体系对于数据样本独立性与真实性的需求。在区块链技术的基础上，设计一种新型的嵌入式机器人运行数据防篡改传输控制系统，并通过对比实验的方式，突出说明该系统与嵌入式 S3C6410 控制系统、空间视觉控制系统间的应用差异性。

1 传输控制系统硬件设计

嵌入式机器人运行数据防篡改传输控制系统硬件包括主控板电路、机器人运行数据解算模块、传输数据矫正模块、微处理器，本章节针对各个部件结构具体设计方法展开研究。

1.1 嵌入式主控板电路

主控板电路以内插嵌入的形式连接于机器人运行数据防篡改传输控制系统中，提供了系统运行所需的全部电量信号，由 STM32F407ZGT6 主控芯片、以太网通讯模块、SD 卡存储模块、RS232 通讯模块、RS422 通讯模块、电源电路模块几部分共同组成。STM32F407ZGT6 主控芯片内配有独立的数据访问控制器，支持机器人运行数据的单独响应行为。以太网通讯模块负责建立嵌入式主控板电路与机器人运行数据解算模块之间的连接关系，由于模块与模块之间保持对应连接关系，所以入侵信息很难进入系统运行环境中，对当前传输数据进行篡改。SD 卡存储模块具有一定的识别能力，可以根据区块链体系所要求的数据防篡改要求，对机器人运行数据进行取样处理，再将符合要求的数据样本存储于模块体系之中。RS232 通讯模块、RS422 通讯模块的连接等级与以太网通讯模块相同，可以按照机器人运行数据的传输需求，对嵌入式主控板中信息参量的存储形式进行重新定义[6]。电源电路模块与＋VCC 高压端相连，具有一定的变电与电量转换能力，可将交流谐波转化为可供下级部件结构直接应用的直流谐波。具体的嵌入式主控板电路连接结构如图 1 所示。

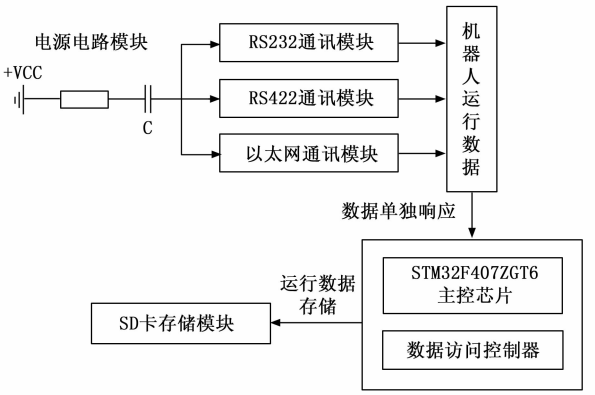


图 1 嵌入式主控板电路结构图

嵌入式主控板电路的设计需要考虑各种因素，如功耗、稳定性、可靠性及安全性等；同时，还需要根据具体的应用需求选择合适的芯片和器件，以满足系统的性能和功能要求。

1.2 机器人运行数据解算模块

机器人运行数据解算模块是用于处理和分析机器人运行数据的模块单元，其主要功能涉及数据采集、预处理、特征提取、数据分析、结果呈现等多个行为流程。数据采集就是指从机器人传感器和其他相关设备中收集具体的运行数据，包括位置、速度、姿态、温度及压力等。预处理需要对采集到的原始数据进行必要的处理，如滤波、去噪、归一化等，以提高数据的准确性和可靠性。特征提取是从预处理后的数据中提取出与机器人运动和性能相关的特征，如姿态信息、行进角、轨迹偏差等[7]。数据分析则是根据具体的应用需求，对提取的特征进行进一步的分析和处理，如模式识别、运动学建模、动力学分析等，且该项指令行为遵循区块链组织所定义的数据防篡改要求。结果呈现是将分析结果以直观的方式呈现出来，如图形、图表、报告等，以便主机元件更好地了解机器人的运行状态和性能[8]。

完整的机器人运行数据解算模块逻辑如图 2 所示。

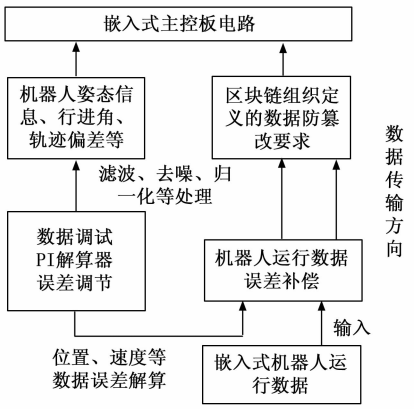


图 2　机器人运行数据解算模块的逻辑框图

作为嵌入式主控板电路的下级附属结构，机器人运行数据解算模块中所有输入的运行数据样本只具有单向传输的能力，且经过 PI 解算器的运算处理后，机器人姿态信息、行进角、轨迹偏差等数据参量中不再存在具有明显滤波特性的信息样本。因此，对于该模块来说，PI 解算器的运行能力决定了所输出数据样本的具体程度。

1.3　传输数据矫正模块

传输数据矫正模块是用于对嵌入式机器人运行数据进行矫正的模块单元。由于机器人在实际运行过程中可能会受到各种干扰和误差的影响，导致运行数据存在偏差和不准确性。因此，传输数据矫正模块需要对数据进行必要的处理和调整，以恢复数据的真实性和准确性。传输数据矫正模块通常包括数据滤波、误差补偿、坐标变换等执行功能[9]。数据滤波用于消除数据中的噪声和干扰，提高数据的准确性。误差补偿用于对机器人运动中产生的偏离和误差进行补偿处理，以保证数据的准确性。坐标变换用于将机器人坐标系中的数据转换为目标坐标系中的数据，以避免在防篡改过程中，运行数据的传输会出现二次偏离行为。此外，该模块还需要对矫正后的数据进行必要的验证和测试，以确保数据矫正行为的执行准确性与可靠性。详细的传输数据矫正模块连接结构如图 3 所示。

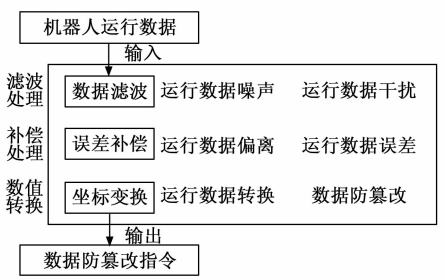


图 3　传输数据矫正模块连接结构图

传输控制系统通过对机器人运行数据的矫正与校准处理，可以获取机器人的各项参数和误差，从而使得区块链体系能够准确掌握机器人行进状态，以便于系统主机对其进行针对性控制[10]。从功能性角度来看，传输数据矫正模块还可以通过建立机器人的运动学模型，将关节角度等与运动行为相关的运行数据转化为实际的姿态或位姿信息。对于传输控制系统而言，实体信息防篡改比抽象运行数据防篡改更易完成。

1.4　控制系统微处理器

控制系统微处理器是一种单芯片 CPU，是装配在单颗芯片上的一个完整的计算引擎。微处理器能完成读取指令、执行指令，以及与外界存储器和逻辑部件交换信息等操作，是微型计算机的运算控制部分。微处理器结构中的 IP 是指令指针，内部标志寄存器也是暂时存放数据的寄存器，指令队列是把预先取来的机器人运行数据存放起来[11]。此外，微处理器还具有强大的中断功能，但通常需要外部元件的配合。而微控制器在片上集成了所有处理中断必需的处理单元，可以快速进行数据信息的切换，挂起一个进程去执行另一个进程以响应一个“防篡改执行指令”。在嵌入式机器人运行数据防篡改传输控制系统中，微处理器结构相当于一个通用的数字计算机中央处理单元，凭借通用寄存器、专用寄存器对运行数据进行总线控制，将指令寄存、指令译码、控制逻辑等多项控制条件集成在一起，从而在嵌入式主控板电路的驱动作用下，在区块链组织中建立一个完整的微型计算机体系[12]。图 4 为控制系统微处理器基础结构的具体连接形式。

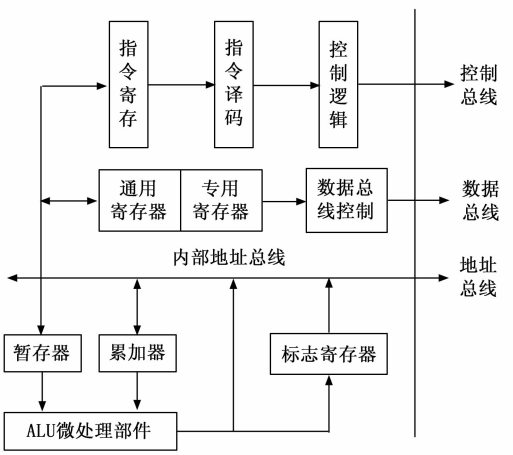


图 4　控制系统微处理器基础结构

在微处理器结构中，内部地址总线同时负载暂存器、累加器、标志寄存器的连接，当 ALU 微处理部件向外输出运行数据时，总线另一端所负载的通用寄存器、专用寄存器同时进入运行状态，此时数据总线端所生成的防篡改执行指令可供区块链体系的直接调取与利用。

2　基于区块链的嵌入式机器人运行数据防篡改方案设计

区块链中每个区块均包含前一个区块的哈希值，确保数据的不可篡改性。一旦数据被存储在区块链上，任何尝试篡改数据的行为都会破坏整个区块链的连续性，从而保

护数据的完整性。为此，采用区块链设计嵌入式机器人运行数据防篡改方案，具体内容如下：

2.1 控制系统环境和角色设计

嵌入式机器人运行数据防篡改传输控制系统所要求的访问控制和数据安全存储服务完全由区块链组织所提供，且这些服务指令可被机器人运行数据解算模块、传输数据矫正模块、控制系统微处理器的直接调取，因此在完善控制系统环境时，应注意数据样本与模块组织之间的实时配合关系。在传输控制系统中对于运行环境的完善与定义如图 5 所示。

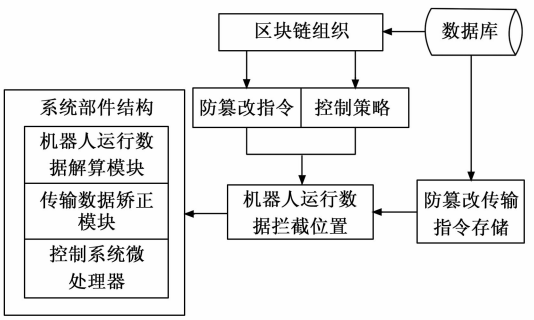


图 5 传输控制系统的环境模型

区块链组织针对嵌入式机器人运行数据防篡改传输控制系统所设定的角色，以数据解算模块（l_1）、传输数据矫正模块（l_2）、控制系统微处理器（l_3）3 类部件结构作为服务对象。由于不同设定角色所享有的服务权限不同，所以区块链组织必须具有按需分配运行数据样本的能力[13-14]。规定 ΔL 表示嵌入式机器人运行数据的单位传输量，δ_1、δ_2 和 δ_3 分别表示数据解算模块、传输数据矫正模块和控制系统微处理器内的哈希值，联立上述物理量，可将传输控制系统中不同部件结构的角色定义式表示为：

$$\begin{cases} l_1 = \dfrac{\delta_1(|\Delta L|^2-1)}{2} \\ l_2 = \delta_2 \cdot |\Delta L|^{-1} \\ l_3 = \dfrac{(1-\delta_3)}{|\Delta L|^2} \end{cases} \tag{1}$$

在角色设计方面，需要明确机器人在控制系统中的角色和功能，以及与其他组件或系统的交互方式。根据机器人的任务和性能要求，为系统部件结构分配不同的角色，以便系统主机对嵌入式机器人运行数据进行合理规划，以避免数据篡改行为的出现。

2.2 嵌入式机器人运行数据的区块链 RBAC 访问

RBAC 是基于角色对象的权限访问控制条件。在嵌入式机器人运行数据防篡改传输控制系统中，RBAC 访问行为依附于区块链组织而存在，且随着角色对象定义数量的增多，RBAC 访问行为所受到的限制性作用也会不断增强。针对嵌入式机器人运行数据所设定的区块链 RBAC 访问条件，应注重角色管理、权限管理、访问控制等多项执行指令之间的关联作用[15]。对于区块链 RBAC 访问条件的设定参考如下标准。

1）角色管理：定义多种不同的系统角色，并为每个角色分配相应的权限。这些权限可以包括对特定机器人的控制权、数据访问权等。

2）权限管理：为每个角色分配具体的权限。例如，管理员有权修改机器人的配置，而操作员只能执行预定义的数据防篡改控制操作。

3）访问控制：根据角色的权限，控制服务器对机器人数据的访问，只有具有相应权限的角色才能在防篡改控制的过程中访问或修改运行数据。

4）区块链集成：利用区块链的不可篡改和可追溯的特性，确保机器人运行数据的完整性和安全性。所有的操作和权限更改都会被记录在区块链上，从而形成一个公开透明的数据管理环境[16]。

设 χ 表示系统角色定义项，k_χ 表示角色管理阈值，β 表示当前角色的权限管理参数，$\vec{j}$ 表示嵌入式机器人运行数据的访问控制向量，α 表示区块链集成系数，联立公式（1），推导嵌入式机器人运行数据的区块链 RBAC 访问机制表达式如下：

$$J = \beta\vec{j}\,\frac{(\chi-1)^2 k_\chi}{|l_1 l_2 l_3|^\alpha} + \overline{H}^2 \tag{2}$$

$\overline{H}$ 表示嵌入式机器人运行数据在区块链体系中的单位累积量。由于区块链组织的特殊性，利用机器人运行数据定义 RBAC 访问链接时，应保证每一个信息参量都得到系统服务器的记录，以避免在实施防篡改修复时，主机元件中出现数据错选或漏选行为。

2.3 区块链网络内的运行数据防篡改链码恢复

区块链具有去中心化、不可篡改、透明、安全和可编程性的特点。在区块链网络中，RBAC 访问机制虽然对嵌入式机器人运行数据提供了不同等级的安全保护策略，但是这些保护策略并不绝对安全，恶意传输文件依然可以通过非法手段入侵区块链组织，并篡改其中的机器人运行数据，而一旦数据遭到篡改，传输控制系统的安全性就会受到严重威胁。因此，在机器人运行数据上传到区块链之前，应对防篡改链码进行恢复处理[17]。此外，防篡改链码所对应的数据文本应该存储在安全的环境中，以防止未经授权的访问和篡改。在区块链 RBAC 访问机制中，运行数据防篡改链码的定义遵循零知识证明原则，它可以单独验证一个数据样本是否为真，而不泄露任何关于该数据本身的编码信息[18]。通过使用这种技术，可以最大化避免数据篡改行为的出现，从而保证了数据的真实性与完整性。

设 ε 表示数据防篡改链码在区块链网络中的连接系数，$\dot{g}$ 为防篡改链码编译特征，φ 为区块链网络内的机器人运行数据码源参数，$\boldsymbol{s}$ 为零知识证明向量，φ 为链码连接的恢复运算门限值。在上述物理量的支持下，联立公式（2），可将区块链网络内的运行数据防篡改链码恢复处理运算式表示为：

$$G = \sum_{\varepsilon=1}^{+\infty} \frac{(\varphi g \cdot J)^{-1}}{\varphi \cdot \boldsymbol{s}} \tag{3}$$

为了确保区块链网络内的运行数据防篡改链码恢复，需要采取一系列的安全措施和技术手段，除了要防止黑客攻击和未经授权的访问行为外，还可以通过使用强大的加密算法、安全协议和防火墙来实现恢复链码的处理需求。

3　机器人运行数据防篡改与传输控制

通过整合区块链技术、RBAC 访问控制和数据恢复处理等多种方法，在嵌入式机器人运行数据防篡改传输控制系统中建立了一套完备的安全管理框架，从环境定义到数据权限控制，再到数据恢复处理，形成了一套系统的安全保障机制。结合哈希值和零知识证明原则，在数据上传到区块链前进行验证，确保数据的完整性。对于嵌入式机器人运行数据的防篡改与传输控制，应针对对运行数据中的关键嵌入部分进行提取，再根据防篡改要求下所定义的机器人运行数据聚集索引标准，完成对篡改率统计运算与实时控制。

3.1　运行数据中的嵌入部分提取

关键嵌入部分就是机器人运行数据中最能够反映出机器人行进状态的信息参量，在区块链网络中，入侵信息的核心攻击对象就是关键嵌入部分，如若这些信息被篡改，则会使网络服务器错误认证数据样本，从而造成严重的数据错传问题。而针对运行数据中的关键嵌入部分的提取，就是利用区块链机制，将必要的数据样本筛选处理，再根据防篡改链码定义标准，将这些信息参量整合成数据样本集合，以便于控制系统可在嵌入式机器人运行数据防篡改传输过程中，对信息参量进行针对性提取[19]。设 $\tilde{d}$ 表示机器人运行数据中的核心嵌入信息，其定义式如下：

$$\tilde{d}=\sqrt{\frac{(\gamma-1)F_0}{\hat{\boldsymbol{D}}}} \tag{4}$$

γ 为区块链机制中的机器人运行数据筛选系数，F_0 为核心嵌入数据的认证标准值，$\hat{\boldsymbol{D}}$ 为基于数据防篡改标准所定义的机器人运行数据认证向量。

由于机器人运行数据具有高维度时序特征，所以在针对关键嵌入部分进行提取时，还应对系统主机所采集到的数据样本进行降维处理，以确保核心防篡改信息参量能够得以保留[20]。联立公式（3）（4），可将运行数据中关键嵌入部分的提取运算式表示为：

$$A=\int_{a=1}^{+\infty}\frac{1}{f}G\cdot\left|\frac{a}{Q}\right|\Big|_{w^2-1}^{e} \tag{5}$$

其中：a 为运行数据降维系数，f 为核心防篡改信息预留项，Q 为关键信息取样系数，w 为机器人运行数据的时序标记特征，e 为区块链网络中的核心嵌入数据取样权限。取样所得的运行数据核心嵌入部分需要适应多种不同的机器人运动场景，所以定义取样条件时，还应判断攻击性信息所面对的目标篡改对象是否存在于当前信息传输区域之中。

3.2　防篡改要求下的机器人运行数据聚集索引建立

在区块链网络中，防篡改要求下的机器人运行数据聚集索引条件是以核心嵌入部分信息为模板定义的搜索标准。聚集索引的作用就是使机器人运行数据中某一项信息的实际存储顺序与区块链网络所规定的防篡改要求顺序保持一致[21]。对于嵌入式机器人运行数据防篡改传输控制系统而言，聚集索引实际上就是按照特定顺序对区块链组织所认证的数据样本进行存储，索引页面内包含系统主机所要求的核心防篡改信息对象。当系统主机在索引页的区块节点上找到所要标记的数据对象后，就说明已经完成了一次防篡改搜索。聚集索引的次级页面不只存储了数据样本的索引键值，还存储了与防篡改运行指令相关的其他数据信息[22]。以 ι 作为嵌入式机器人运行数据的初始索引地址，κ 表示目标索引地址，λ 表示区块链网络中的数据样本聚集程度，联立公式（5），推导防篡改要求下的机器人运行数据聚集索引表达式如下：

$$R=\tilde{Y}[\frac{\lambda}{A}(y_k-y_t)^2]-(\eta\dot{I})^2 \tag{6}$$

为基于数据防篡改要求所定义的机器人运行数据索引向量，y_t 为基于参数 ι 的信息索引对象，y_κ 为基于参数 κ 的信息索引对象，η 为机器人运行数据在区块链网络中的传输效率，$\dot{I}$ 为运行数据聚集索引序列。在防篡改要求下建立机器人运行数据的聚集索引需要采取一系列的安全措施和技术手段，以确保防篡改执行指令的机密性、完整性和可信性。

3.3　篡改率的统计与控制

对于区块链网络而言，篡改率可以理解为攻击信息对嵌入式机器人运行数据的篡改能力，其取值越大，就表示在传输控制系统中，必须频繁执行防篡改指令才能够避免数据篡改行为的出现。为保证篡改率统计结果的准确性，应在同一聚集索引标准下，完成对传输数据的取样，一方面避免控制系统中出现信息交叉传输的情况，另一方面也使得防篡改指令得以顺利执行[23-24]。设 i 为区块链网络所评估的机器人运行数据篡改项，P_i 为基于参数 i 的数据篡改行为可能性计量值，c_i 表示与之相关的控制项系数，P_0 为数据篡改行为可能性计量参数的标准值，c_0 表示与之相关的控制项系数，μ 为阈值参量，联立公式（6），可将篡改率计算式表示为：

$$O=\frac{1}{\mu^2}\times R\times\sum_{i\to\infty}\frac{P_i}{P_0}\cdot\frac{c_i}{c_0} \tag{7}$$

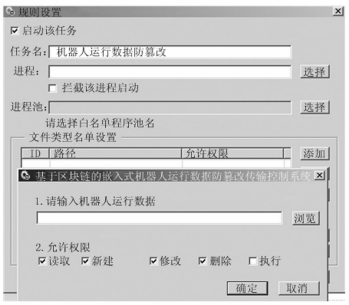
基于区块链的嵌入式机器人运行数据防篡改传输控制系统的运行目的是避免数据传输过程中，出现信息参量被篡改的情况，所以在求解篡改率指标的过程中，应对该项物理量的计算结果进行有效控制。

4　实验分析与研究

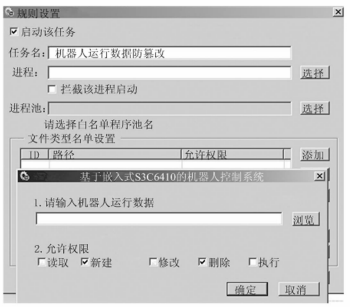
4.1　实验准备

本次实验设置 3 种不同的对比系统，分别为设计系统（第一组）、文献［2］系统（第二组）和文献［3］系统（第三组），在实施运行数据防篡改传输控制的过程中，该系统允许数据读取、新建、修改、删除权限；支持基于嵌入式 S3C6410 的机器人控制系统规则的实验系统为第二组，

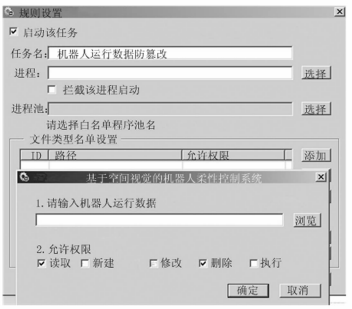
在实施运行数据防篡改传输控制的过程中，该系统允许数据新建与删除权限；支持基于空间视觉的机器人柔性控制系统规则的实验系统为第三组，在实施运行数据防篡改传输控制的过程中，该系统允许数据读取与删除权限。对于各组实验系统的设置如图 6 所示。



（a）第一组



（b）第二组



（c）第三组

图 6 系统设置

针对嵌入式机器人运行数据的防篡改处理，是为了提高数据传输效率，从而在保障数据安全性的同时，避免篡改行为的出现。因此，在将机器人运行数据输入不同实验系统之后，只需要根据数据样本的实时传输效率，就可以判断出不同系统在防篡改控制方面的应用能力。数据篡改是指入侵信息对系统原传输信息进行的修改，由于码源模板的不同，所以修改指令的执行也需要一定的时间，而这一行为会严重影响机器人运行数据的传输，也就造成了数据传输效率下降的问题。对于本次实验而言，在不考虑其他干扰条件的情况下，机器人运行数据在实验系统作用下的传输效率越快，就表示当前系统运行过程中，发生数据篡改问题的可能性越低，即该系统的防篡改控制能力越强。本次采用 1 000 条嵌入式机器人运行数据进行实验测试，区块链集成系数为 0.95，链码连接的恢复运算门限值为 5，设置管理员角色拥有修改机器人配置和数据访问权限，而操作员角色：只能执行预定义的数据防篡改控制操作。控制系统的结构如图 7 所示。

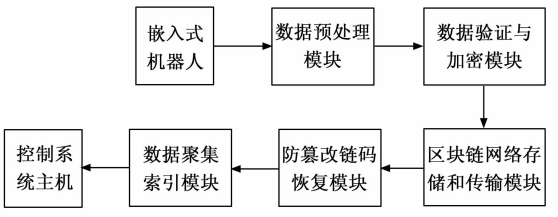


图 7 嵌入式机器人传输控制系统结构

图 7 中，作为数据源，嵌入式机器人负责收集并生成运行数据，传输至数据预处理模块进行必要的预处理，利用哈希值和零知识证明原则对预处理后的数据样本进行验证，确保数据的完整性和真实性。区块链网络作为数据存储和传输的核心，负责存储经过验证和加密的机器人运行数据，确保只有授权用户才能访问和修改数据。通过防篡改链码恢复模块确保链码的正确性和有效性，从而增强数据的防篡改能力。基于数据聚集索引模块对存储在区块链上的机器人运行数据建立聚集索引，便于后续的数据检索和验证。控制系统主机是整个系统的中央控制器，负责协调各个模块的工作。它接收来自嵌入式机器人的运行数据，通过数据预处理、验证、加密等步骤后，将数据存储到区块链网络中，并管理数据的访问和修改权限。同时，控制系统主机还可以根据需要对数据进行查询、分析和控制操作。由此，实现基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计。

4.2 实验结果与分析

4.2.1 数据传输效率测试

不同系统作用下，机器人运行数据实时传输效率的具体实验情况如图 8 所示。

整个实验过程中，第一组、第二组、第三组机器人运行数据实时传输效率的最大值分别为 326、281、259 bps。从均值角度来看，第一组数据传输效率主要集中在 150～250 bps 的数值区间之内，第二组数据传输效率主要集中在 100～200 bps 的数值区间之内，第三组数据传输效率的主要集中效率与第二组相似，但在 10 和 50 min 左右时，数据传输效率的数值水平均出现了明显下降，明显第一组数值水平更高。

不同系统下，机器人运行数据逆序传输速率的实验情况如图 9 所示。

相较于机器人运行数据顺序传输速率，逆序传输速率的平均数值水平较低。就图 9 来看，第一组逆序传输速率相对较高，其最大值接近 100 bps，明显大于第二组最大值 61 bps 与第三组最大值 35 bps，数据传输效果更好。

4.2.2 数据防篡改能力测试

根据系统的安全需求，设定一个可接受的篡改率阈值。

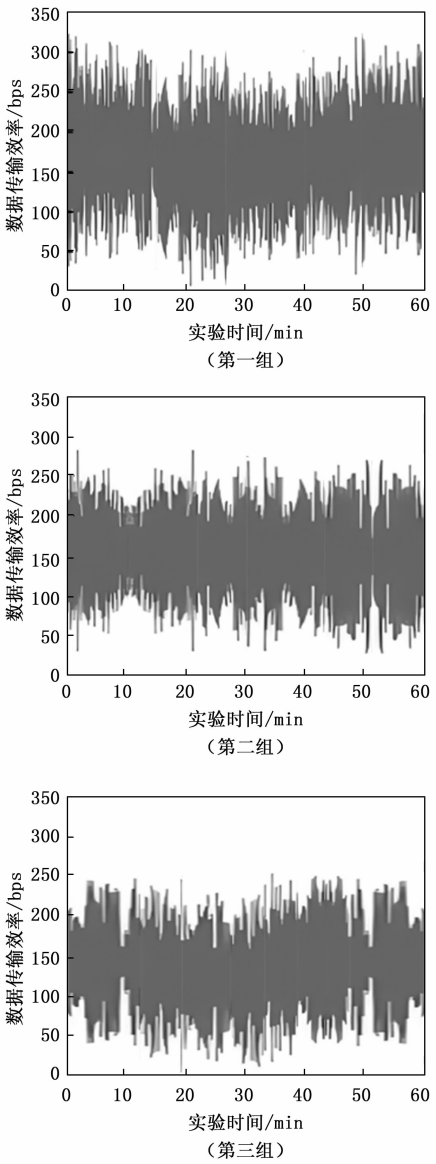


图 8　机器人运行数据传输效率

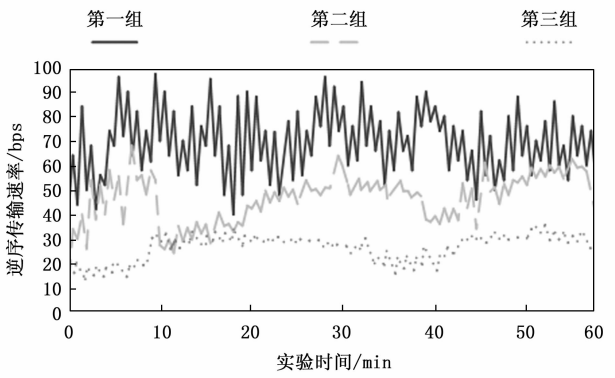


图 9　机器人运行数据逆序传输速率

例如，设定阈值为 0.1%，表示在 1 000 个数据事件中，允许有 1 个数据事件被篡改。当监测到的篡改率接近或达到设定的阈值时，系统应发出警告，并通知管理员或相关人员。根据篡改率的严重程度，系统可以采取不同的数据传输调整策略，以提高数据的可靠性；当篡改率持续升高并超过某个严重级别时，系统可以暂停数据传输，以防止更多的数据被篡改。在机器人运行数据样本量相同情况下，不同系统的防篡改防护率如图 10 所示。

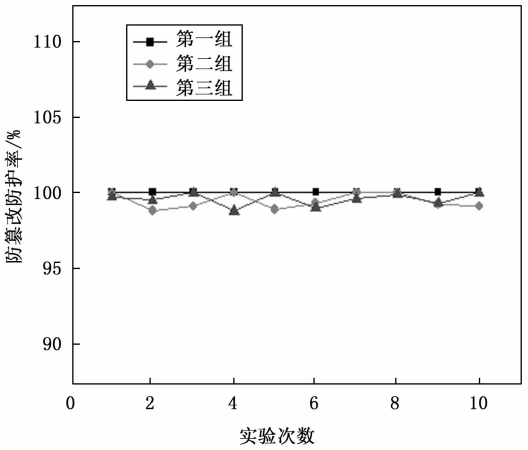


图 10　防篡改防护效果

分析图 10 可知，在机器人运行数据样本量相同的情况下，第二组、第三组均存在数据篡改威胁，而第一组在 10 次实验过程中的防护率达到 100%，由此证明了设计系统的数据防篡改传输控制能力最好。这主要是因为设计系统采用了区块链技术，该技术中多个区块按照时间顺序连接而成，每个区块包含了前一个区块的哈希值，使其形成一个不可逆的链条，提高系统的防篡改能力。

综上可以得出结论：基于区块链的嵌入式机器人运行数据防篡改传输控制系统的应用，起到了提升机器人运行数据传输效率的作用，相较于对比系统，该系统在数据防篡改控制方面的应用能力更强。

5　结束语

基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计是一项复杂且具有挑战性的任务。在设计和实施过程中，需要综合考虑数据的安全性、完整性和可信性，同时确保系统的可靠性和可扩展性。通过利用区块链技术的不可篡改和去中心化特性，可以有效保障机器人运行数据的真实性和可信度。与此同时，通过篡改率统计与控制的方法，可以及时发现和处理数据篡改问题，降低潜在的风险和影响。在未来的研究和应用中，相关组织机构可以进一步探索和完善相关技术和方法，以提高系统的性能和可靠性，并适应不断变化的应用需求和技术环境。总之，基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计是一个重要的研究方向和实践领域。通过不断地研究和创新，有望为机器人的智能化和安全可信的发展提供重要的支持和保障。

（下转第 153 页）