文章编号:1671-4598(2021)03-0252-06 DOI:10.16526/j.cnki.11—4762/tp.2021.03.050 中图分类号:TP242.2 文献标识码:A

基于区块链的智能机器人多传感信息加密控制研究

丁 璇
(陕西警官职业学院，西安 710021)

摘要：由于现有智能机器人多传感信息加密控制方法多传感信息加密效率较高，导致安全时间较短；为了解决上述问题，基于区块链技术，研究了一种新的智能机器人多传感信息加密控制方法；通过信息位置源备份设置陷阱、信息路径伪装、网络匿名和信息通信控制实现位置传感信息加密，应用封装处理和二次验证加密数据传感信息；设置定位传感器结构控制位置传感信息，利用区块链技术获得加密有效区域，针对智能机器人的眼睛、腕关节、胸部和手部进行控制；实验结果表明，基于区块链的智能机器人多传感信息加密控制方法能够有效提高多传感信息加密效率，安全时间更长。

关键词：区块链；智能机器人；多传感信息；加密控制

Research on Multi-sensor Information Encryption Control of Intelligent Robot Based on Blockchain

Ding Xuan
(Shaanxi Police Vocational College, Xi'an 710021, China)

Abstract: Due to the high efficiency of the existing multi-sensor information encryption control methods for intelligent robots, the security time is short. In order to solve the above problems, based on the blockchain technology, a new multi-sensor information encryption control method for intelligent robot is studied. The location sensing information is encrypted by setting traps for information location source backup, information path camouflage, network anonymity and information communication control. The positioning sensor structure is set to control the position sensing information, and the block chain technology is used to obtain the encrypted effective area to control the eyes, wrist, chest and hand of the intelligent robot. The experimental results show that the multi-sensor information encryption control method based on blockchain can effectively improve the efficiency of multi-sensor information encryption, and the security time is longer.

Keywords: blockchain; intelligent robot; multi-sensor information; encryption control

0 引言

机器人在学术界和工业界取得了长足的发展，尽管在这方面已取得了许多进展，但机器人的实际应用还是相当有限[1-2]。针对智能机器人在应用过程中易受外部环境限制的特点，相关学者提出了设计稳定、可长期使用的自动化装置以解决上述问题，包括传感器的选择、配置、算法及实现。在智能机器人多传感信息管理这一问题中，加密控制属于难点问题，屠袁飞等人[3]提出一种基于CP-ABE的可撤销属性加密访问控制算法，通过CP-ABE完成访问控制的初始构建和密钥生成，为提高可撤销属性加密访问控制算法的访问控制效果，在加密算法以及解密算法中写入新文件创建，新用户授权，吊销用户，文件访问等方面过程的设计，该方法访问控制时耗时缩短，控制效果较好，但是无法保障加密信息的真实性和合法性。杜远志等人[4]提出一种基于属性加密的信息流控制机制，将基于属性的加密技术与信息流控制技术相结合，通过对用户私钥和访问树的生成方法重新设计，在减少用户制定访问策略工作的同时，使得该机制能够对云中数据进行有效的信息流控制，从而消除安全隐患，该机制能够抵抗基于共享内存的侧通道攻击，保护静态虚拟域中敏感数据安全性，但是该方法多传感信息加密效率较高，导致安全时间较短。

区块链是一个可以共享的数据存储库，区块链数据库中的数据都具有真实性和唯一性，这一特点对于信息加密控制尤为重要。一旦数据库内的信息失去真实性和可靠性，再高级的加密方法也无效，因此采用区块链的智能机器人多传感信息加密控制，可以保证驱动智能机器人行为的加密信息的可靠性和真实性，提高加密信息加密效率[5]。

综上所述，基于区块链研究一种新的智能机器人多传感信息加密控制方法，将加密后的信息进行区块链技术的封装，封装完成后根据信息的应用领域和需求，完成最终

收稿日期:2020-12-29； **修回日期**:2020-01-22。
作者简介:丁 璇(1977-)，女，湖南醴陵人，工程硕士，讲师，主要从事计算机应用方向的研究。
引用格式:丁 璇. 基于区块链的智能机器人多传感信息加密控制研究[J]. 计算机测量与控制，2021，29(3)：252-257.

的信息加密控制。

1　智能机器人多传感信息加密

应用的智能机器人如图 1 所示。

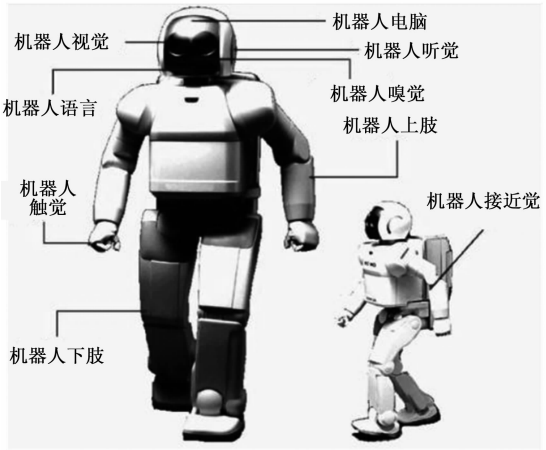

图 1　智能机器人示意图

根据图 1 可知，智能机器人共分为机器人视觉、机器人电脑、机器人听觉、机器人嗅觉、机器人触觉、机器人上肢、机器人下肢和机器人接近觉几部分[5]。其中，机器人电脑是核心设备，对机器人内部各个设备进行控制。机器人视觉、机器人听觉、机器人嗅觉、机器人触觉属于数据传感信息，机器人上肢、机器人下肢属于位置传感信息。针对位置传感信息和数据传感信息进行加密。

1.1　位置传感信息加密

针对智能机器人的位置信息进行加密，位置信息加密对于确保机器人智能行走有重要意义。通过位置信息加密来提高机器人的自主定位、建图、路径规划及避障等能力。位置信息加密包括的内容如图 2 所示。

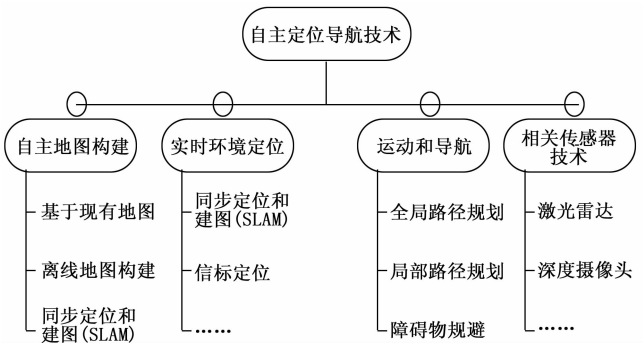

图 2　位置信息加密内容

信息同时存在的附属属性很多，比如信息的存储位置、信息大小、信息的目的地址、信息创建时间等，这些属性可以暴露信息源[6-7]。为了提高多传感信息加密的加密级别，对信息的位置属性进行加密处理，信息位置加密目的是阻止外界恶意窃取信号源和攻击手段。位置加密方法的原理是通过监测信息位置节点状态，一旦发现状态异常，立即增加多传感信息的防御程度，模拟一个虚假信息源迷惑攻击者，并切断恶意信号源，保证网络位置信息安全。信息位置加密的特点是实时性和灵敏性，根据信息的类别，多传感信息加密方法分为数据源位置加密方法、sink 位置加密算法[8]。为了达到多传感信息全局加密效果，以信息加密程度最大化为目的，因此选择数据源位置加密方法进行加密，数据源位置加密方法主要分为信息位置源备份设置陷阱、信息路径伪装、网络匿名和信息通信控制 4 个步骤。

加密过程如图 3 所示。

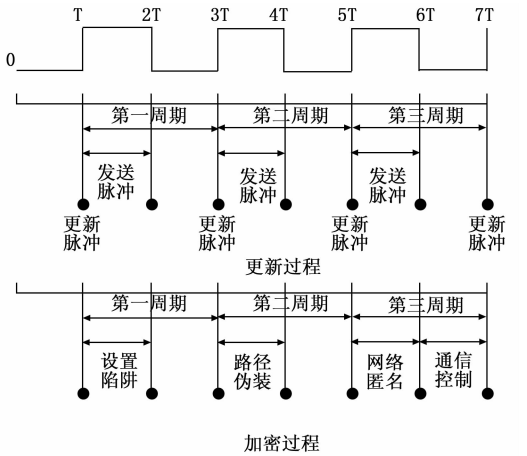

图 3　位置信息加密过程

根据图 3 可知，信息位置源备份、设置陷阱指的是智能机器人监测信息状态时，传感机器人一旦识别到信息存在恶意攻击行为或者信号时，立即随机模拟一个信息的信号源（其信号源不可以与其他真正的信号源重复）用来迷惑攻击者，误导攻击者认为他已经找到了真实的数据源信息，攻击者在重复确认信息源位置时，数据源位置加密方法对攻击者进行无防备的消灭处理。路径伪装是信号源备份的进一步体现，如果信息源备份时没有全部清除攻击者，那么在位置信息转发过程中，数据源节点不通过最短路径策略进行数据转发，而在预先设计的多条伪装路径中随机选择某一条作为数据传输链路，使攻击者攻击错误路径，延长正常位置信息的转发周期，在消灭攻击者时可以连带路径全部消除，简化防御策略[9]。网络匿名指的是通过对位置信息的 IP 地址进行加密。位置信息通信控制指的是在各个安全位置的信息交互过程中，更改位置信息交互模式，对位置信息节点信息进行加密[10]。

1.2　数据传感信息加密

数据传感信息包括感知数据信息、认知数据信息和行为数据信息。数据信息加密指的是合法网络对加密数据的信息查询、数据聚集以及数据被访问过程中进行过程加密，防止攻击者窃取数据信息[11-12]。

设定传感器加密机器人内部数据信息，传感器标定工作台如图 4 所示。

如图 4，在传感器标定工作台上对数据传感信息进行加

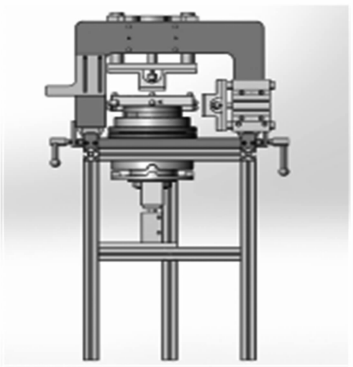

图 4 传感器标定工作台

密。数据信息加密方法主要采用数据隐私保护法完成智能机器人的行为驱动，对于数据信息的查询加密方法主要防止传感网络攻击者攻击数据信息的存储节点和 IP 地址节点。数据信息聚集操作是多传感信息中关键数据节点连接外界节点的方式，一旦数据聚集操作加密性低，被攻破，信息就会大量流失。因此对于数据聚集节点加密方法增加一项封装处理，信息数据处于聚集行为时，数据信息连通时进行二次验证，并且通信的数据必须在信息库内进行转码，才可以还原数据信息，因此攻击者攻击到初步加密后的数据信息，也不能得到数据信息[13]。

2 智能机器人多传感信息加密控制

区块链技术的工作原理是在区块链数据库内按照信息封装方式对需要加密区域的数据进行分块，然后在数据库内进行共享，使新的加密数据信息被原有的区块链数据库认可，共同形成一个全新的区块链数据库。区块链数据库为了避免出现人为误操作导致的信息丢失或者其他问题，设置区域链的数据库信息管理不依赖于管理人员，内部信息实时更新。区块链数据库的管理依靠于数据库的各个网络节点、工作算法以及 TCP 协议，每个节点之间按照协议规则相互监督，依赖算法完成区块链数据库的逻辑循环操作，一旦对接出现异常时，发出警报，进行处理[14]。

区块链技术概括示意图如图 5 所示。

图 5 区块链技术概括示意图

引入区块链技术对智能机器人多传感信息进行加密控制，智能机器人内部结构如图 6 所示。

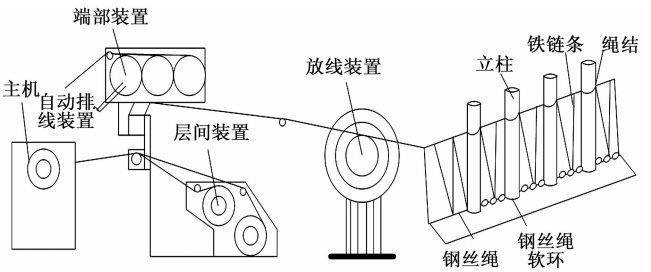

图 6 智能机器人内部结构

基于区块链的智能机器人多传感信息加密控制具体流程如图 7 所示。

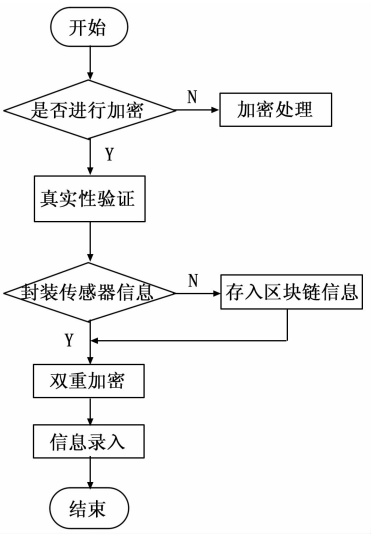

图 7 智能机器人多传感信息加密控制具体流程

(1) 首先对需要加密的传感信息进行真实性验证，验证通过后，区块链数据库赋予每一条数据信息一个数字签名、信息私有地址和公有地址，为接下来加密多传感信息加密操作和调用操作提供基础；

(2) 然后智能机器人对上传的传感信息进行封装，通过对信息进行位置加密和数据加密处理，初步加密完成后，将封装好的加密信息传到区块链数据库内，与初次加密后的信息进行对比，查看是否与区块链数据库内信息重复，确定加密信息的合法性和真实性。如果不重复那么对传感信息进行数字签名加密；

(3) 多传感信息双重加密后，将信息传输到智能机器人的区块链数据库内，数据库在收取信息时，验证每一条信息的数字签名，因为数字签名具有不可伪造性和鉴定性。最后，将多传感加密信息录入成功后，通过随机路由控制算法将加密信息转化为时间戳的格式，驱动智能机器人的合法行为。

引用传感器控制位置传感信息，位置传感信息控制引入的传感器结构如图 8 所示。

由图 8 可知，机器人位置感知信息控制的实现主要包

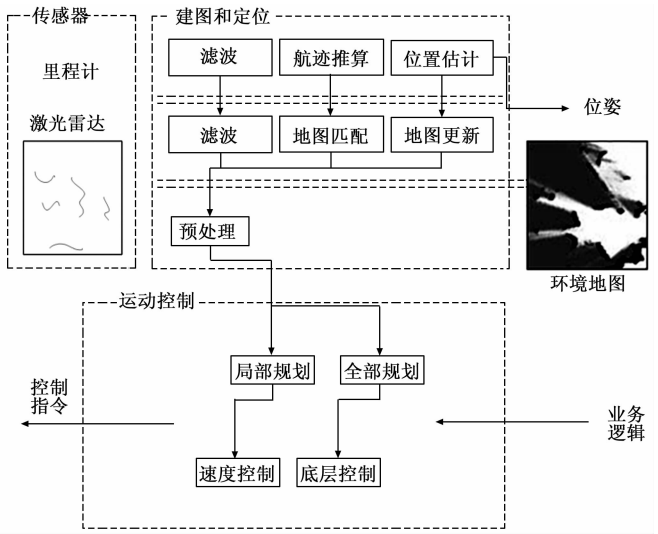

图 8　定位传感器结构

括激光冲击和视觉冲击。多采用 2D 或 3D 激光雷达，其在机器人上的主要应用是 2D 激光雷达，它能实时采集周围目标的环境信息，并形成角度和距离精确的散点云图，对所采集的目标信息进行处理。利用激光 SLAM 系统，实现了两个不同时间点的点云数据匹配与比较。通过对目标相对运动距离和姿态的计算，实现了对机器人自身的定位。以单眼和鱼眼相机为基础，主要采用多帧图像估计自身姿态变化，通过累计姿态变化来计算目标与目标之间的距离，建立定位图[15]。

构建基于多传感器融合技术的社会服务机器人开发平台，能够提供更为全面、可靠的信息，准确地反映被测对象的特征，使机器人行走更加智能化。内建于 SLAMWARE 的高性能自主定位导航系统，不仅为机器人提供最基本的自主行走能力，还支持虚拟墙和虚拟轨迹，自主反馈，第三方应用扩展和楼层绘制导航，自动电梯控制等功能。

数据传感信息控制主要针对智能机器人的眼睛、腕关节、胸部和手部进行控制，传感器混合机构如图 9 所示。

利用对称的 3 RRR 机构定位摄像机，并通过底座 R 关节驱动旋转电机控制图 8 中的敏捷眼可以有效控制视觉传感信息。因为所有的联轴器必须在一个中心点相交，所以敏捷眼的制造和组装都需要很高的精度。在底座和平台之间，只有一个轴承安装在远端 R 接头上，因此该机构的 3 RRR 机构加入了驱动器。在敏捷手腕中，设计了一个 3 RRP 体系结构来实现持续的旋转。在关节轴与旋转中心不能精确相交的情况下，增加被动活动关节可防止机构过远而不交叉。

同时引入随机路由控制算法实现提高数据传感信息的控制精度，随机路由控制算法的控制原理是通过智能机器人申请的行为驱动请求，区块链数据库按照请求查询相应驱动命令的多传感信息时间戳，转发进行行为驱动。加密

图 9　传感器混合机构

信息转发的同时立即启动随机路由控制算法，对加密信息驱动的行为进行控制，一旦行为出错，立即终止。

随机路由控制算法首先对区块链数据库内的加密信息进行识别备份，核实并得出加密数据控制的区域，并对需要控制的加密数据信息进行随机分组，每组筛选出一个随机整数，作为控制的关键信息节点。以加密信息的源节点作为坐标原点建立相对直角坐标系 XOY，通过公式计算出加密数据信息波及范围的半径值，根据半径值确定加密数据的有效驱动行为的有效区域。加密有效区域如图 10 所示。

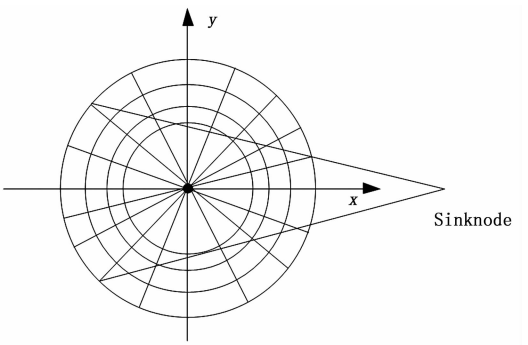

图 10　加密有效区域

具体公式如下所示：

$$R_{\text{phantom}} = R_{\min} + ((rand0\%\ 3) + I) \tag{1}$$

$$R_{\text{phantom}} - 1 = \sqrt{(x_i - x)^2 + (y_i - y)^2} \tag{2}$$

其中：R_{phantom} 表示区块链待选区域外层半径；$[R_{\text{phantom}} - 1, R_{\text{phantom}}]$ 表示待选区域范围；I 表示选取控制系数；x 表示每个数据信息的节点区域横坐标；y 表示每个数据信息的节点区域横坐标。

初次完成信息加密数据使用区域的划分后，继续对可用待选区域 $[R_{\text{phantom}} - 1, R_{\text{phantom}}]$ 进行二次划分，精确控制加密数据的使用范围，具体二次划分计算公式如下所示：

$$\int_{\text{relative}}^{\text{soueceNode}(x,y)} 0 < i < \text{nodeNum} \tag{3}$$

其中：soueceNode（x，y）表示多传感信息的原节点坐标；nodeNum 表示多传感信息的数量。

3 实验研究

为了验证提出的基于区块链的智能机器人多传感信息加密控制方法的有效性。设定实验参数如表 1 所示。

表 1 实验参数表

项目	参数
网络规模	400 m * 400 m
内部节点部署方式	随机部署
内部节点数量	500 个
节点初始能量	100 J
发射功率	50 mW
接收功率	20 mW

根据表 1 参数，选用方法和传统方法进行对比实验，通过能量模型和信息分析，提取网络内部的能量消耗，分析网络生存时间数据。首先对采集的信息进行预处理，去除冗余信息，预处理过程如图 11 所示。

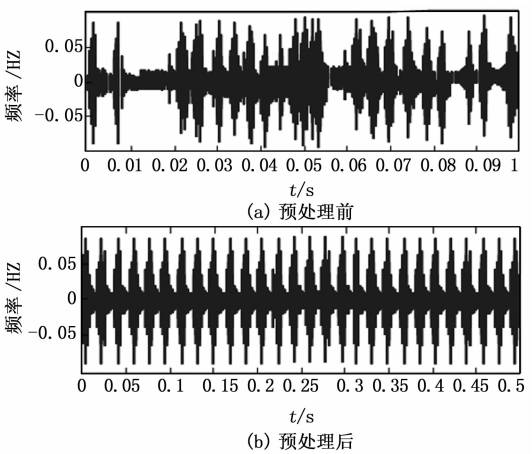

图 11 数据预处理效果图

如图 11 可知，经过预处理后，多传感线信息更加稳定，便于对其进行实验。

在此基础上，对多传感信息加密效率进行实验，实验结果如图 12 所示。

根据图 12 可知，随着迭代次数的增加，不同控制方法的多传感信息加密效率也在不断增加，但是所提方法多传感信息加密效率要始终高于传统方法的多传感信息加密效率。提出的方法在对数据进行加密时，以综合的角度分析节点数量，进行数据传输，由能耗模型原理可知，因此所提方法效率最高。所提方法在选取节点过程中，根据邻近节点的信息表分析出距离目标节点的最近节点，从而得到能量阈值，确保可以在最短时间内转发数据。

在此基础上，以安全时间为测试指标，进行实验测试，并统计结果，如图 13 可知。

从图中可以得出，在所提方法和传统加密控制方法之

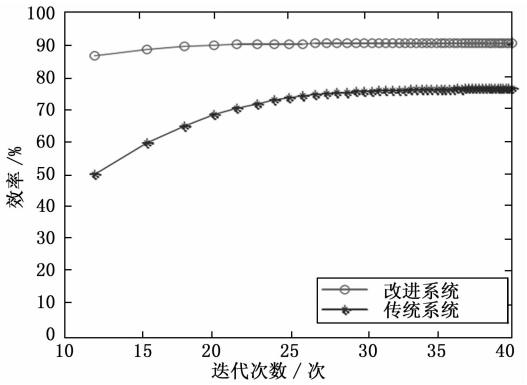

图 12 多传感信息加密效率实验结果

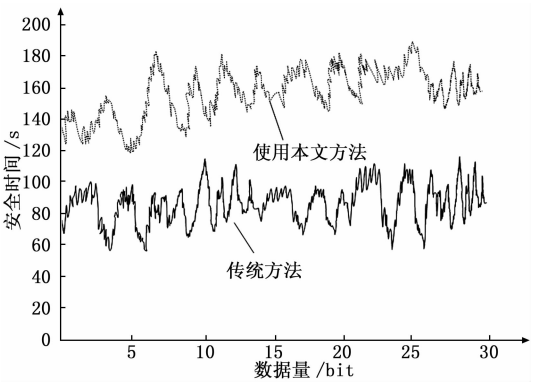

图 13 安全时间实验结果

间的安全时间差距较大，而随着数据量的增加，所提方法安全时间仍然高于传统方法。应用触觉传感器进行传感信息加密，触觉传感器在 MIS 应用中的设计要求（也称为约束条件）与传感器的物理特性和功能特性密切相关。触觉传感器相当灵敏，线性，低时滞，能测量 0～5 N 范围内的接触力，分辨率为 0.01 N，能够更好地传输数据，保证数据传输过程引入的路径多样性，从而提高加密过程的隐私保护能力。

4 结束语

综上所述，以信息位置加密、信息数据加密、区块链存储数据库规则原理以及随机路由控制算法作为研究的基础，完成多传感信息的加密、封装和控制操作，达到研究的目的。相信通过以上的研究分析，可以提高智能机器人的多传感信息的加密程度，规范智能机器人的行为。

参考文献：

[1] 李高峰，胡国强. 基于区块链技术实现智能档案协查 DAO [J]. 山西档案，2019 (4)：85－91.

[2] 许继平，孙鹏程，张 新，等. 基于区块链的粮油食品全供应链信息安全管理原型系统 [J]. 农业机械学报，2020，51 (2)：348－356.

[3] 屠袁飞，高振宇，李荣雨. 基于 CP－ABE 的可撤销属性加密访问控制算法 [J]. 计算机科学，2018，45 (11)：176－179.

[4] 杜远志，杜学绘，杨　智. 云计算环境下基于属性加密的信息流控制及实现 [J]. 计算机工程，2018，44 (3)：27 - 36.
[5] 潘吉飞，黄德才. 区块链技术对人工智能的影响 [J]. 计算机科学，2018，45 (z2)：53 - 57.
[6] 丁庆洋，王秀利，朱建明，等. 基于区块链的信息物理融合系统的信息安全保护框架 [J]. 计算机科学，2018，45 (2)：32 - 39.
[7] 丁晓蔚，苏新宁. 基于区块链可信大数据人工智能的金融安全情报分析 [J]. 情报学报，2019，38 (12)：1297 - 1309.
[8] 柴　洪. 基于区块链“去中心化”企业智能管理系统研究 [J]. 武汉理工大学学报（信息与管理工程版），2019，41 (1)：61 - 66.
[9] 樊建峰，李　轶，吴文渊，等. 基于双区块链的基站动环信息监控系统 [J]. 计算机科学，2019，46 (12)：155 - 164.
[10] 杨　栩，谭　琦. 基于区块链技术的高端装备制造企业智能化运营研究 [J]. 商业研究，2018，499 (11)：12 - 17.
[11] 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)：152 - 158.
[12] 罗以洪. 大数据人工智能区块链等 ICT 促进数字经济高质量发展机理探析 [J]. 贵州社会科学，2019 (12)：122 - 132.
[13] 周万锴，龙　敏. 基于区块链的环境监测数据安全传输方案 [J]. 计算机科学，2020，47 (1)：315 - 320.
[14] 张　省，董　盈. 基于区块链技术的数字版权保护研究 [J]. 科技管理研究，2020，40 (1)：132 - 136.
[15] 刘庆松，樊　哲，赛鹏新，等. 基于区块链的物联网控制总线 [J]. 福建茶叶，2020，42 (3)：308.

（上接第 242 页）

图 14　断路测试结果

三小时。经过多次反复实验，都没有出现数据错误或丢失现象，表明了模块具有长时间工作的能力。

所有的测试可以表明本文设计的四通道隔离 CAN 总线通讯模块可以实现 CAN 2.0B 规范所规定的数据收发功能，并具有良好的性能指标和一定的错误处理能力。

5　结束语

本文从实际应用需求出发，针对单通道 CAN 总线通讯系统的不足完成了 CPCI 四通道隔离 CAN 总线通讯模块的设计，并进行了相关的功能测试来验证设计的正确性，测试结果表明本文设计的模块满足设计要求，具备良好的性能指标以及四通道 CAN 总线数据传输的能力。

参考文献：

[1] Goyal U，Khurana G. Implementing MOD bus and CAN bus Protocol Conversion Interface [J]. International Journal of Engineering Trends & Technology，2013，4 (4)：630 - 635.
[2] Janschek K，Braune A. Application of industrial CAN bus technology for LEO－satellites [J]. Acta Astronautica，2000，46 (2 - 6)：313 - 317.
[3] 何立仁，王　义. 无触点控制的汽车 CAN 总线灯光系统研究设计 [J]. 电子设计工程，2012，20 (22)：23 - 26.
[4] Gurram S K，Conrad J M. Implementation of CAN bus in an autonomous all－terrain vehicle [A]. Southeastcon，2011 Proceedings of IEEE [C]. IEEE，2011.
[5] 刘承智，丁国良，原　亮，等. 改进型 CAN 总线协议的实时性研究 [J]. 计算机技术与发展，2012，22 (7)：81 - 84.
[6] Sebastian M，Ernst R. Reliability Analysis of Single Bus Communication with Real－Time Requirements [A]. Dependable Computing，2009. PRDC'09. 15th IEEE Pacific Rim International Symposium on [C]. IEEE，2009.
[7] 邱瑞阳，方　方，周　伟，等. 基于 CAN/USB 总线的测氡仪多通道数据采集系统 [J]. 核电子学与探测技术，2012，32 (5)：595 - 598.
[8] 方亚南，郑国光，李怀祖. 高效的冗余多通道电子支付模型的构建 [J]. 西安交通大学学报（社会科学版），2006 (4)：22 - 26.
[9] Takimoto E，Kondo Y，Itaya S，et al. Evaluation of Multi－Channel Flooding for Inter－Vehicle Communication [A]. 22nd International Conference on Advanced Information Networking and Applications，AINA 2008，Workshops Proceedings，GinoWan，Okinawa，Japan，March 25 - 28，2008 [C]. IEEE Computer Society，2008.
[10] CAN Protocol Controller [EB/OL]. https://opencores.org/projects.
[11] Han J，Fu P，Qiao J. UVM－Based CAN IP Verification [Z]. Advances in Intelligent Information Hiding and Multimedia Signal Processing. 2020.
[12] Xiaosong G，Xingjie P，Chuanqiang Y，et al. Design of a CAN Bus Testing and Control System Based on Fault Tolerant Redundancy [A]. 国际电子测量与仪器学术会议 [C]. 2007.
[13] 周　颖. 四通道 CAN 总线模块研制 [D]. 哈尔滨：哈尔滨工业大学，2017.
[14] 杜　洋. 基于微机监测的故障信号研究与应用 [D]. 北京：北京交通大学，2015.
[15] 张　英，张仁杰. 基于 CAN 总线的汽车远程故障诊断系统研究 [J]. 信息技术，2014 (10)：86 - 90.
[16] 王　聪，魏文娟，王　超. 基于 CANScope 的 CAN 总线故障诊断及改进设计 [J]. 中国测试，2018，44 (S1)：166 - 171.