DOI:10.20033/j.1003-7241.(2025)01-0154-05.

电力设备场景智能锁具状态远程授权控制技术研究

黄湛华，阳 浩，徐启源，何 明
（深圳供电局有限公司，广东 深圳 518000）

摘 要：在智能锁具远程授权控制过程中，受到授权模型的影响，易出现授权效率较低的问题，无法满足电力设备运行需求。因此，研究电力设备场景智能锁具状态远程授权控制技术。采用SimpliciTI网络协议，实现智能锁具远程监控和通信。根据无线网络通信协议数据，利用PCA算法识别用户信息。构建电力设备场景智能授权模型，结合Hash函数实现密钥协商，达到智能锁具状态远程授权的目的。实验结果表明：与已有技术相比，文中所设计的控制技术授权效率得到了大幅度的提升。

关键词：电力设备；智能锁具；远程授权；控制；网络协议；识别算法
中图分类号：TP273^{+}.5 文献标识码：A 文章编号：1003−7241(2025)01−0154−05

Research on Remote Authorization Control Technology of Intelligent Lock State in Power Equipment Scene

HUANG Zhan-hua, YANG Hao, XU Qi-yuan, HE Ming
(Shenzhen Power Supply Bureau Co., Ltd., Shenzhen 518000 China)

Abstract: In the process of remote authorization control of intelligent locks, the authorization efficiency is easy to be low due to the influence of the authorization model, and the operation requirements of power equipment cannot be met. Therefore, the remote authorization control technology of intelligent lock state in power equipment scene is studied. Using SimpliciTI network protocol, the remote monitoring and communication of intelligent lock are realized. Based on wireless network communication protocol data, PCA algorithm is used to identify user information. The intelligent authorization model of power equipment scenario is built, and the Hash function is combined to realize key negotiation, so as to achieve the purpose of remote authorization of intelligent lock status. The experimental results show that compared with the existing technologies, the authorization efficiency of the control technology designed in this paper is greatly improved.

Keywords: power equipment; intelligent lock; remote authorization; control; network protocol; recognition algorithm

0 引言

由于电力设备的种类繁多，使得变电站的锁具和钥匙数量较多[1]。在变电站工作过程中，如何实现开锁和钥匙管理已经成为电力系统智能化发展的难点。智能锁具的应用一定程度上解决了这一问题，既避免了寻找钥匙的巨大工作量，又对变电站安全产生了保障。智能化的发展使得当前智能锁具状态具有远程授权功能，无法满足当前电力设备场景工作需求[2]。

为了避免非准许人员进入变电站，增强电网运行安全性，同时有效增强工作效率，授权控制技术备受关注。当前，有学者提出相关研究方法。文献[3]以多级属性加密作为核心内容，设计了信任度授权控制方法。综合员工信息、属性加密算法，以及多级访问控制策略等技术，将信任度计算模型融入授权控制技术中心，保证电力设备场景安全，但是该方法的通用性较差。文献[4]应用区块链技术，设计了基于云环境的授权控制方案。在授权控制中融合区块链技术，保证所有授权机构合理分发私钥。通过多层次算法判断用户是否满足授权需求，对满足需求的用户进行授权。研究显示，该授权控制方案具有较好的安全性，可以较好地抵抗恶意攻击，但该方法执行效率较低。文献[5]进一步分析电力配电场景，建立模型实现智能锁授权。在多个部门的合作下，依靠密钥协商协议达到为智能锁具授权的目的。该方法可以在多种配电场景下均有可行性，但是授权失误率较高。

文中深入电力设备场景智能锁具状态，提出一种远程授权控制技术。通过SimpliciTI网络协议和PCA算法识别申请者信息。应用授权模型和Hash函数设计具体授权方案，从而实现远程授权效率提升，在保证配电房安全的基础上，降低了运维人员的工作难度。

1 智能锁具状态远程授权控制设计

1.1 设计SimpliciTI网络协议

收稿日期：2023-03-13

智能锁具远程授权控制技术设计，需监控门锁状态。文中以终端节点的数据采集和传输为基础，设计SimpliciTI网络协议[6]。利用图1所示的低功耗网络模块、加密模块、扩展节点模块跳频模块、访问节点模块和网络管理模块等六个功能模块实现获取智能锁具数据信息。

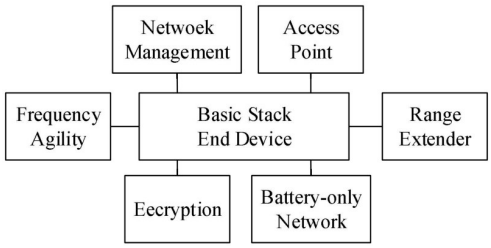

图1 SimpliciTI网络协议各功能模块

SimpliciTI网络协议应用时，通过网络通信节点，实现终端信息访问。网络协议中主要由射频层、板级支持包层实现通信。通过射频层收发数据，经过板级支持包的传递，将该数据传输至网络层。

网络层主要负责频段管理、调制方式和数据传输速率等多种基本功能的参数设置，实现网络连接和数据传输[7]。网络层在端口号的作用下获取目标地址信息，并完成目标设备信息向后台的传递和接收。为了区分无线传感器网络中的节点，将端口号的范围设置为0x01～0x3F，将接口号和节点地址相连接，建立数据连接。SimpliciTI网络协议工作中将其网络结构设置为星型网络，基于可利用范围将结构向外扩展，逐渐形成串型网络。利用上述网络结构分析接收到的终端智能锁具信息，以满足智能锁具远程授权的通讯监控需求

1.2 识别用户身份信息

根据SimpliciTI网络协议传递的数据信息，识别用户身份信息，以保证电力设备场景的安全。文中采用PCA算法[8-9]，将获取的终端智能锁具获取的数据降维处理，并从中提取出数据中的主元部分。为了简化计算复杂度，提升远程授权控制工作效率，在降维过程中忽略冗余维数，将数据信息简化。由于原始图像数据是一种高维向量，其中每个元素都有其对应的像素点。利用PCA算法提取出信息中的特征点，形成特征空间呈现用户人脸图像。最后，汇总变电站所有工作人员的人脸信息构成数据库，用于识别用户身份信息。

基于K-L变换的PCA算法，是一种最优正交变换识别技术。对于一个n维中随机选取的变量A，通过该维度的基向量加权计算，得出：

$$A=\sum_{n}\alpha\varphi \tag{1}$$

式中，随机变量加权计算结果受到加权系数a和基向量的φ影响当所有的基向量形式均为正交，那么可以形成正交矩阵β。

为了提升识别准确率，需要确保正交矩阵内应用的向量，相互之间不具有相关性，针对正交向量集E，计算随机向量的自相关矩阵：

$$R=E\left[\varphi\beta\beta^{T}\varphi^{T}\right] \tag{2}$$

式中，T表示权值，为了满足正交矩阵的各向量之间不相关，需要满足：

$$E\left[\beta_j\beta_k\right]=\begin{cases}\lambda_j, j=k\\0, j\neq k\end{cases} \tag{3}$$

式中，j表示向量特征值，k表示阈值。因为矩阵R具有正定的实对称特点，因此计算结果为非负数。在考虑到基向量的自身特点后，将K-L变换公式表示为：

$$\beta=\varphi^{T}A \tag{4}$$

PCA识别算法的应用，本质上是通过新坐标的建立，按照物体的特征矢量旋转主轴进行变换操作，经过变换后将原数据的相关性大大降低，加强用户身份信息识别效果。

计算过程中，将所有的人脸信息放置在低维空间内，完成不同人脸的区分处理。通过K-L变换算法，将区分后的人脸数据库进行高维空间对角化计算，获取新的正交基。通过正交基汇总特征信息，以低维特征空间的形式体现出人脸信息。SimpliciTI网络协议传输过来的数据，划分为训练和测试两部分。在将测试图像X、平均差值δ向特征空间投影后，获取图像特征向量W计算公式：

$$W=\delta^{T}(X-\omega) \tag{5}$$

式中，ω是投影后图像，针对待检测图像、训练集内图像的特征向量进行计算，获取特征向量距离。在分析各种计算方法后，文中采用欧几里得距离计算方法，得出下列计算公式：

$$L(x,y)=\|x-y\|=\sqrt{\sum(x-y)^{2}} \tag{6}$$

式中，L表示欧几里得距离，x，y分别表示待检测图像和训练集图像的特征向量。通过欧几里得距离构建相似度计算标准，计算当前图像与数据库中图像的可信度，将可信度值与设定阈值相比，若大于阈值表明用户身份识别完成，反之则需要重新计算。通过上述识别方法，提升电力设备场景智能锁具状态授权的准确度。

1.3 构建智能授权模型

由于远程授权技术需要通过后台的处理，因此构建智能授权模型，将与智能锁具状态远程授权控制相关的多个部门统一管理，构成图2。

在电力设备场景中，基于用户身份信息识别结果，采用单片机控制智能锁具授权。将单片机操作融合到后台编程中，硬件设备放置在智能锁具终端内。当收到异常

警告时开启闭锁模式，确保开关分合处理功能暂停。根据网络协议提供的数据，在后台实现用户身份识别，运维人员依据识别结果发送智能授权信息。确定用户身份后下达解锁指令，在单片机的作用下不再闭锁。需要注意的是，远程授权过程中需要保证智能锁具每隔1分钟重新自动关闭，达到合理控制电力设备场景智能锁具的目的，提升配电工作场景安全性。

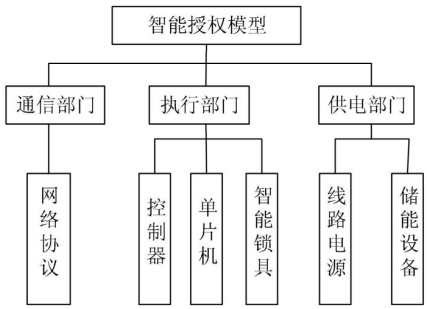

图2 智能授权模型

在智能锁具授权模型中，处于核心位置的是执行部门，该部门包括控制器、单片机，以及智能锁具，对多种场景下的远程授权结果产生关键性影响。实际工作中，执行部门获取授权指令后，旋转单片机将锁栓拨动到开锁位置，使得智能锁具可以开启。关锁时需要保证单片机处于初始位置，依靠弹簧弹力拨动锁栓，确保智能锁具的关闭。

1.4 智能锁具远程授权的实现

根据上述智能授权模型实现电力设备场景的智能锁具关闭控制，为实现远程授权的合理化，设计授权模型的初始化任务。应用Hash函数设计一个临时密钥，在新无线节点引入后，再根据新节点共同计算，获取共享密钥。为了保证远程授权准确率更高，授权效率满足电力场景工作需求，添加散列函数HMAC。在加密服务器、随机无线节点之间展开密钥协商计算，得到新的、符合二者要求的新密钥。最后，依据不同密钥的一致性计算结果，对共享密钥进行刷新，解决当前远程授权中存在的适配场景单一的缺陷。

电力配电场景中的智能锁具作为一个沟通载体，将后台远程授权结果传递至锁具终端。因此在密钥协商时，主要考虑加密服务器Z、随机无线节点B二者的建议。实际应用中首先在加密服务器非指定模式$b\in S$下，结合运算密钥协商因子H_Z，以及无线节点密钥G_B，形成如下公式：

$$N_Z = T_2(H_Z, G_B) \tag{7}$$

式中，加密服务器的认证码N_Z，根据Hash函数T进行计算。

获取公式(7)的可行性验证结果，若可行性满足要求。则对随机无线节点非指定模式$c\in S$进行计算，可以得出以下计算公式：

$$N_B = T_2(H_B, L_B, G_B) \tag{8}$$

式中，N_B表示随机无线节点模式下认证码，H_B表示节点密钥协商因子，L_B表示节点中出现的HMAC认证码，G_B表示节点共享密钥，并将运算结果传递至加密服务器中。加密服务器接收到传递信息后判断可用性。可用性判断结果符合远程授权需求，进行下一步工作，相反则需要重新建立会话密钥协商在经过节点和加密服务器测试后，二者均可以通过以下运算得到新的会话密钥G_Z、G_B。

$$\begin{cases} P_B = T_1(L_B) \\ G_Z = d(P_B, H_B, m) \end{cases} \tag{9}$$

$$\begin{cases} P_B = T_1(L_B) \\ G_B = d(P_Z, H_Z, m) \end{cases} \tag{10}$$

式中，d表示映射系数，P_B、P_Z表示节点和加密服务器的Hash函数与认证码相乘的相关性。之后，对新的会话密钥一致性进行判断，当消息认证码验证完成后，确认节点和加密服务器密钥相同，则表示会话密钥协商成立。以散列函数HMAC为基础，认证密钥协商协议中的身份信息，实现智能锁具远程授权。

2 实验及分析

针对文中设计的智能锁具状态远程授权控制技术，展开实验测试。通过分析智能锁具工作原理，构建硬件电路，并对其正常进行状态检测，基于硬件分析授权结果，获取远程授权控制技术的应用性能。

为了保证实验测试效果，通过对电力设备场景的智能锁具工作原理分析，设计智能锁具硬件电路。将管理控制电路和BC95通信电路相结合，形成总体硬件电路。其中，管理控制电路由单层板构成，在仿真器的作用下，利用排针调试接口，将电路与PC端连接，实现智能锁具电路的调试。而管理控制电路的右侧排针接口连接通信电路，并在BC95通信电路的稳压芯片上连接电源供电口。通过BC95通信电路中两个UART0_RXD串口，放置一个微控制器MSP430。除此之外，硬件电路板中显示的序号1和2分别连接电池、电机。最上方排针中的UART1_RXD串口连接转换模块，达到与PC机通信的目的。另一个主要硬件为锁具电机，本研究中的锁具电机为直流推拉式电磁阀，从而实现电路的简化。在完成硬件实物设计后，将整体的硬件电路板与MSP430仿真器相连，通过PC机实现对智能锁具状态检测。

针对调试过后的电路板，测试智能锁具的状态。应用一次性亚硫酰氯电池，将定时检测的状态信息上传至数据中心。利用PC端发送智能锁具状态控制指令，通过控制微控制器保证直流推拉式电磁阀平稳供电，执行授权开锁的命令。在完成远程授权控制后，电路呈现出高

电压状态，用lock_flag 1表示此时的锁标志位，而该情况下的智能锁具开启，用LockState 0表示锁的状态。之后，利用PC机发送lock命令，在微控制器的作用下关闭直流推拉式电磁阀的供电，实现智能锁具关闭。该状态下的锁标志位表示为lock_flag 0，采用LockState 1表示电力设备场景智能锁具关闭状态。

实验进行过程中，除了对智能锁具开关状态检测外，还需要在供电线路中串联万用表，完成智能锁具状态授权控制过程中电流变化测量。电流测量过程如图3所示。



图3 电流测量

通过多次测量结果的汇总，形成表1所示的智能锁具各种状态平均电流。

表1 智能锁具各种状态平均电流

工作状态	电流/mA
通信模块激活状态	323.25
通信模块通信状态	48.21
通信模块空闲状态	3.19
电机驱动	173.10
切断供电开关MSP430激活状态	301.21
切断供电开关MSP430休眠状态	9.01

根据数次测量的均值，明确实验过程中正常变化范围。将电流测量应用的电信卡设置为APN，当数据信息得到上传后，可以激活通信模块，此时智能锁具的电流为323.25 mA。当智能锁具通信进行时，智能锁具处于监听状态，此时的平均电流约为48.21 mA。而当智能锁具在较长时间内没有数据交互后，通信模块开始呈现出空闲状态，也就会变成类似休眠的情况，此时平均电流为3.19 mA。除此之外，电机驱动状态下智能锁具平均电流为173.10 mA。在供电开关电路截止后，微控制器激活与休眠状态下智能锁具的平均电流分别为301.21 mA、9.01 mA。以上述检测结果作为正常标准，在实验过程中随时对锁具电流信息进行抽查，确保电流信息处于正常状态，以保证实验结果的准确性。

为了测试本文模型的应用性能，在上述硬件环境中采用文中设计的远程授权控制技术进行测试，并采用文献[3]、文献[4]提出的技术完成同样操作。通过授权结果对比，分析文中设计授权技术的应用性能。分别选取低压配电、多电源供电、三相供电、临时供电、正式用电五个电力设备工作场景，测试远程授权控制技术的应用效果。对智能锁授权时的授权响应耗时进行计算，以此测试3种模型的授权效率，结果如图4所示。

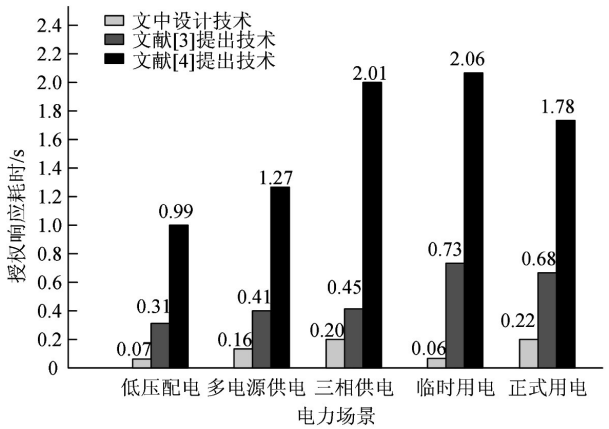

图4 三种授权控制技术的授权效率对比

通过图4所示的三种方法的授权效率对比结果可知，在不同的电力设备工作场景下，文中所设计远程授权控制技术的响应耗时远远低于两篇文献提出的技术。通过计算得出，文中设计远程授权技术的平均响应耗时为0.14 s。文献[3]所提出的授权技术，授权响应的平均时间约为0.58 s。而授权效率最低的是文献[4]所提出的授权控制技术，根据实验结果可知，该技术的授权响应平均时间达到了1.62 s。由此可见，文中设计的远程授权控制技术与文献[3]、文献[4]提出的技术相比，使得授权效率提升了75.8%、91.3%。综上所述，文中设计授权技术有效提高工作效率。

3 结束语

文中针对电力设备场景智能锁具状态进行研究，提出远程授权控制技术。实验结果显示，文中设计的技术具有可行性，在各种电力设备场景中平均授权响应时间仅有0.14 s，有效提升了工作效率。这种高效率的智能锁具状态远程授权控制技术的应用，满足了电力设备场景工作需求。但是由于时间的限制，研究仍然存在部分缺陷。未来将对该技术进一步优化，分析授权访问部门的职责，提升授权协议的细粒度，融合计算机技术全面挖掘配电工作，更好地控制智能锁具远程授权。

参考文献：

[1] 胡绍谦，李力，朱晓彤，等.基于检修态切换的智能变电站保护设备检修辅助安全措施[J].电力系统自动化，2019，43(1)：242-247.

[2] 牛荣泽，张凯，谢芮芮，等.基于随机森林的电缆管网综合监测系统研究[J].电测与仪表，2024，61(10)：74-81.

(下转第172页)