



无实时网络下约定式运算的控制研究和应用

张正峰

(广东电网有限责任公司电力调度控制中心, 广东 广州 510600)

摘要: 在研究无网络状态下的定时约定机制和镜像同步运算获得密钥的基础上, 提出了基于密码控制、非实时虚拟通信和按约定计算密钥的逻辑控制方法, 能够很好地适用于智能锁或开关在无实时通信网覆盖下的动态认证以及开关工作。利用具有约定运算能力的智能终端, 建立了一种无实时通信网络下的“密控网”, 既可作为物联网技术在无通信覆盖情况下的有益补充, 也可作为固定地点的远端物件按计算次序移交管理权或使用权。通过采用终端的运算能力代替对远端的通信能力, 而无须构建后台通信网络以及等候期的通信费用支出。

关键词: 远端非联网; 加密算法; 约定; 约时

中图分类号: TN915.85

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020019

Control research and application of conventional operations without real-time networks

ZHANG Zhengfeng

Power Dispatching and Controlling Center of Guangdong Power Grid Co., Ltd., Guangzhou 510600, China

Abstract: On the basis of researching the timing agreement mechanism and mirror synchronization operation to obtain keys under the condition of no network, a logic control method was proposed based on cryptography control, non-real-time virtual communication and computing keys according to agreement, which could be well applied to dynamic authentication and switch operation of intelligent locks or switches without real-time communication network coverage. By using the intelligent terminal with the ability of agreed operation, a kind of “control network of cryptography” without real-time communication network was established, which could be used as a useful supplement to the IoT technology without communication coverage, as well as a remote object in a fixed location to transfer the right of management or use according to the order of calculation. By using the computing power of the terminal instead of the communication power of the remote end, without the need to build a backstage communication network and the communication expenses during the waiting period.

Key words: remote non-network, encryption algorithm, convention, agreed time

1 引言

物联网 (internet of things, IoT) 是通过射频

识别、红外感应器、全球定位系统、激光扫描仪等设备, 按约定的协议, 把任何物品与互联网连接起来进行信息交换和通信, 以实现智能化识别、



定位、跟踪、监控和管理的一种网络^[1]。目前，人们对现有的远端物件的开启使用和退出使用，都需要该远端物件具备接入互联网和受远程控制的功能，既要求业主方与租赁方都在通信网或互联网的网络上，也要求远端物件接入通信网或互联网，才能实现远端物件的管理权移交。如果一个远端物体是长期固定位置的，远端物体无须自己把定位信息告知业主方与租赁方，可以通过业主方通知租赁方。如果在边远山区、无信号的地下停车场中，远端物件无后台联网，即便有移动信号覆盖，也还需要业主到场进行交接，这限制了物联网的覆盖范围。所以，被联网管理的物品的后台通信和定位的需要与否都值得研究，对不同的“物”是否可进行有区分的按通信需求联网和“对话”。

2 物联网中的密码传递

对一件物件的开启使用和退出使用，有两种方式：一种是业主方到场将钥匙实物交给租赁方，并在使用完毕后收回钥匙；另一种是业主方通过通信手段告知租赁方控制密码，在租赁方使用完毕后的某时，业主方到场重新设置密码。在第二种方式中，如果远端物件已接入互联网，还可采取远程重置密码方式。无论是现场重新设置密码还是远程重置密码，都是为了防止刚使用完的租赁方在解除租约后仍采用未曾改动的密码继续使用远端物件。

目前，对远端物件开关装置进行控制的技术方案有：酒店客房钥匙管理、公共自行车租赁技术方案、商场临时存包柜、联网自助售货机，通过对现存技术方案的分析，可发现有以下缺点：现有对远端物件的开启使用和退出使用，都需要具有互联网接入和远程控制，既要求业主方与租赁方都在网络上，也要求远端物件接入互联网，才能实现业主方对远端物件有效的管理。

公共自行车的租赁的两种方式：一种就是使

用固定桩控制自行车，该固定桩带有网络和锁具，公共自行车固定在锁具上；另一种就是无固定桩的随借随还方式。无固定桩的“随借随还”方式，其关键技术在于移动车体上的锁具，该锁具内置 SIM 卡可以直接和服务器通信，通过网络服务器进行管理使用的开关装置开启步骤如下：手机扫码获取车子的编号，手机向服务器发送开锁指令，含带车子的编号；服务器收到开锁指令，与相应编号的车子通信，发送开锁指令；车子接收到服务器的开锁指令进行开锁。无固定桩的随借随还方式的公共自行车租赁运作示意图如图 1 所示。

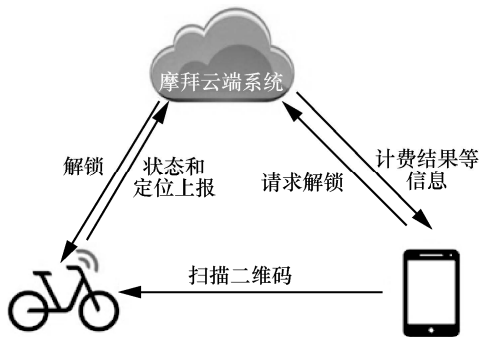


图 1 无固定桩的随借随还方式的公共自行车租赁运作示意图

酒店对门锁的管理需要后台通信网络；联网自助售货机同样需要接入通信网络才能对所有售货进行实时管理，相当于每个货物的出售开关都受售货机的统一管理。不动物件的共享方式运作示意图如图 2 所示。

另外，业主对远程房屋物业的出租使用，要求业主方与远端物件和租赁方三方在网的远程控制，需要对远程物业的房门部署电信网或互联网，才能有效地进行租赁物业的房门开合控制。如果该物业的房门是普通房门，或在网络不可达的情况下，就需要业主方与租赁方到场的钥匙交接。总之，目前这些案例都存在同一个问题：远端物件必须纳入互联网的网络部署或网络基础建设，远端物件必须随时在线以便接受业主方的控制。

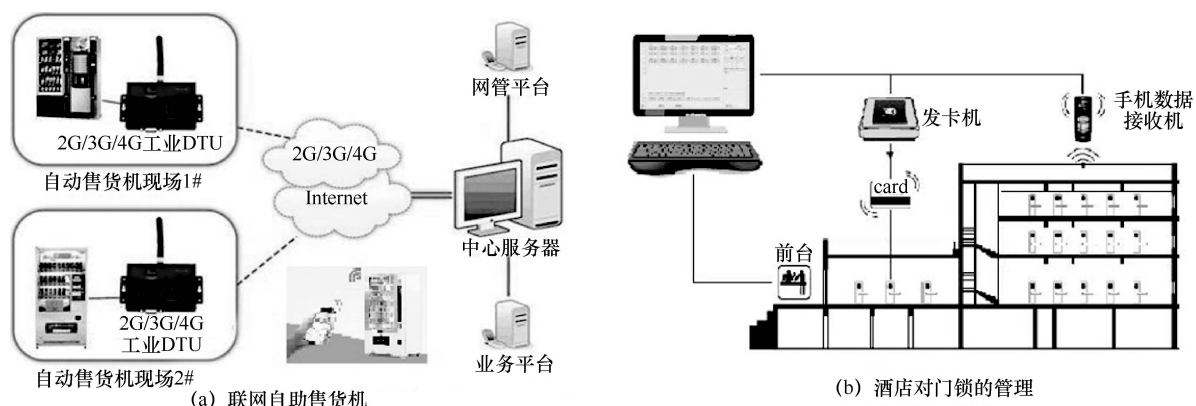


图 2 不动物件的共享方式运作示意

3 远端物件的管理权移交

远端物件必须接入互联网才能受控于业主方,这是目前远端物件的使用权转移的必要途径,因此限制了远端物件的应用范围。物联网是在互联网基础上的延伸和扩展的网络,是通过识别技术和感应器,按规定协议,将任何物品通过有线与无线方式与互联网连接,进行通信和信息交换,而远端物件的使用权转移可以说是物联网应用里最底层的管理权转移。

远端物件分为不动物件和移动物件。不动物件的管理权移交共享过程,其定位、跟踪功能都可以忽略;而对于可移动物件定位、跟踪也存在其受质疑的地方。如无固定桩随借随还的公共自行车租赁技术方案,虽然该方案所述的是无固定桩随借随还方式,但事实上该移动物件需一直在互联网上受到远端业主的控制,或者是使用的开始和结束时必须在网,否则将无法完成业主多物件的使用权临时转移和回收功能,所以无固定桩随借随还的自行车内置 GPS 定位功能,虽然方便业主方定位远端物件,但也暴露了租用人在使用过程中的移动路线和隐私。远端物件使用过程中由于有后台通信很容易在其未知的情况下被定位和跟踪,如何确保标签物的所有者个人隐私不受侵犯就成为物联网推广中的关键问题之一^[2]。一些固定地点的远端物件,例如房屋、充电桩、售

卖机、快递暂存机,其位置是固定不变的,交易次数可以按事件发生次数进行记录,需不需要建设后台通信网络以及支出等候期的通信费用,这都值得去研究。

4 约定式运算的智能终端

本文提出的技术方案主要是聚焦于非联网的具有电控开关、位置固定的远端物件,上述案例中描述的房屋、充电桩、售卖机、快递暂存机都是具有电子锁或电开关的。

4.1 核心思路和方法

首先,本方案设定远端物件没有接入通信网络或安装通信 SIM 卡,因此它接受允许启动或关闭的密码信息必须由租赁方中转,它必须有输入界面或接近式信息通信,如键盘、显示屏、蓝牙或红外通信;第二,远端物件必须要有运算解密和控制开关的能力;第三,本方案设定业主方具有一把与远端物件运算解密方法一致的虚拟锁,并且,制密运算方式是约定的、同步的多个加密算法约定,预设加密循环机制的循环起始位置和预设解密循环机制的循环起始位置相同;第四,业主方与远端物件交流的、由租赁方中转的信息是可读可写、可由输入界面输入的文字或图案;第五,远端物件具有获取时间信息和计时的能力;第六,租赁方的固定信息和预计使用信息都需要告知远端物件和业主方的虚拟锁,按既定的制密



运算方式运算出下一位租赁人使用的密码存储于各自本地。

物联网智能卡具有良好的人机界面、强大的读写能力、足够的安全性和及时性、大容量的存储能力和方便携带性。上述的思路方法，就好比是智能卡在经长距通信再进行接近式延伸通信，允许启动或关闭的密码信息由租赁方中转时，就好比在通信中间点做了一张智能卡去接触远端物件，而远端物件的开关装置具有识读器和运算、计时和存储功能。

该方案的核心思想就是，在远端物件无网络状态下，采用定时约定机制和业主手中的虚拟锁镜像同步运算获得相同的密匙用于远端物件的开启关闭。约定时间内正常结束或逾期不正常结束已使用过的密匙都为过期，同步跳到下一个加解密算法和密匙核对。提供输入的文字或图案是含有密匙和租约的必要信息，提供关闭时的输入的租约信息错误的话也得不到正确的关闭密码，远端物件和业主手中的虚拟锁所知租约信息内容作为下一个制密原料通过镜像同步的加密算法制作出只有两者所知密匙。由于具有加密算法约定的约时开关装置自带计时，应允许有计时误差，按目前的时钟的计时误差在此类固定远端物件租赁中亦是是可以忍受的。

4.2 具有加密算法约定的约时开关装置

远端物件具有加密算法约定的约时开关装置

是根据与控制端的约定相同的规则与双方都取得的其他信息进行各自运算出相同的下次使用密码，本端该次密码将通知下一未知的租赁使用者，而远端记录该密码将在下一对未知的租赁使用者核对后开启。

一种远端非联网加密算法约定的约时开关装置，包括本端密码运算器和远端非联网开关装置。一种远端非联网加密算法约定的约时开关装置结构如图3所示。

本端密码运算器包括本端微控制器及分别与本端微控制器电连接的本端键盘、本端显示屏和本端存储器；本端微控制器用于根据业主通过本端键盘输入的含有约时信息的明文生成开启加密字符串，并控制本端显示屏进行显示。

远端非联网开关装置包括远端微控制器及分别与远端微控制器电连接的远端键盘、远端显示屏、远端存储器、继电器组及连接在继电器组输出端的电控锁件；远端微控制器用于对共享资源临时使用人通过远端键盘输入的开启加密字符串进行解密，并通过继电器组开启电控锁件或共享资源物件，还用于在租赁约定截止时间或租赁实际结束时间，通过继电器组关闭电控锁件或共享资源物件。

远端非联网开关装置还包括闭合传感器、状态检测器和凭条打印机；闭合传感器用于检测电控锁件的闭合状态并通过状态检测器发送给远端

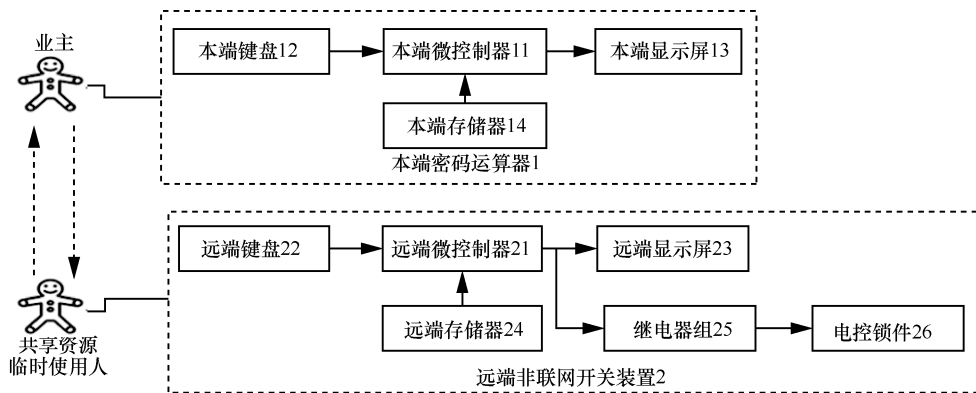


图3 一种远端非联网加密算法约定的约时开关装置结构

微控制器,以使远端微控制器在电控锁件闭合时,控制凭条打印机打印凭条。打印凭条上记载有租赁约定使用时间、租赁实际结束时间及租赁实际结束时间所对应的电控锁件闭合状态。

本端微控制器还用于根据业主输入的租赁实际结束时间和结算金额生成关闭加密字符串;远端微控制器还用于根据共享资源临时使用人通过远端键盘输入的关闭加密字符串,解密出结算金额,并根据共享资源临时使用人通过远端键盘输入的待开发票抬头信息和发票正文信息,控制发票打印机打印发票。

本端密码运算器还包括与本端微控制器电连接的本端二维码扫描器和本端蓝牙模块,二维码扫描器用于扫描由共享资源临时使用人提供给业主的,包含有租赁实际结束时间的二维码并发送给本端微控制器。本端蓝牙模块无线连接有本端智能移动设备,本端智能移动设备用于将业主输入的明文或者租赁实际结束时间,通过本端蓝牙模块发送给本端微控制器,并接收本端蓝牙模块发送的开启加密字符串或关闭加密字符串。

远端非联网开关装置还包括与远端微控制器电连接的远端二维码扫描器和远端蓝牙模块,远端二维码扫描器用于扫描由业主提供给共享资源临时使用人的,包含开启加密字符串或关闭加密字符串的二维码并发送给远端微控制器。远端蓝牙模块无线连接有远端智能移动设备,远端智能移动设备用于将共享资源临时使用人输入的开启加密字符串或关闭加密字符串,通过远端蓝牙模块发送给远端微控制器。

本端密码运算器还包括与本端微控制器电连接的本端密码循环控制器;远端非联网开关装置还包括与远端微控制器电连接的远端密码循环控制器。

远端密码循环控制器和本端密码循环控制器皆包括写入式存储器或可固封的拨动开关阵列。其中,写入式存储器用于存储用户设定的加密算

法或与加密算法相配套的解密算法;可固封的拨动开关阵列用于设定加密算法或解密算法的循环周期和起始位置。可固封的拨动开关阵列好比弹子锁的长短不一的弹子组合阵列,而密码循环控制器就是形成每次不同弹子组合阵列和相匹配的钥匙。

远端装置可级联应用,多个开关可串联控制。远端非联网开关装置有多个,多个远端非联网开关装置开启或关闭的优先级存储在每个远端非联网开关装置的远端存储器中。任一远端非联网开关装置还包括与远端微控制器电连接的级联状态输入模块和级联状态输出模块,级联状态输入模块与上一级远端非联网开关装置的级联状态输出模块电连接,级联状态输出模块与下一级远端非联网开关装置的级联状态输入模块电连接。

远端装置可延伸应用,以中继密码箱的方式保存原控制钥匙的使用权交接。电控锁件还包括安装在电子密码箱内的实体钥匙检测器和电控锁,其中,电子密码箱用于存放实体钥匙,实体钥匙检测器用于检测实体钥匙是否存放在电子密码箱中,电控锁用于控制电子密码箱的启闭;电子密码箱固定在出租车中或出租房门口位置处。

4.3 流程及控制方法

一种远端非联网加密算法约定的约时开关装置,其特征就是一种受密码控制开启使用和结束使用的控制电源开合的装置,密码的加密算法和循环机制只由业主和该种远端非联网加密算法约定的约时开关装置私密设定,受密码控制开启使用和结束使用,是指业主方与租赁方建立通信后,采用明文传递、各自解密和受授权转移的一种信息沟通控制流程。一种远端非联网加密算法约定的约时开关装置策划的逻辑时序的信息沟通控制流程如图4所示。

根据图4可知,远端非联网开关装置是不需要电信网或互联网部署的一种电子控制开关装置,无需以业主方为服务中心与远端物件和租赁方都有联网的远程通信,只需利用业主方与租赁

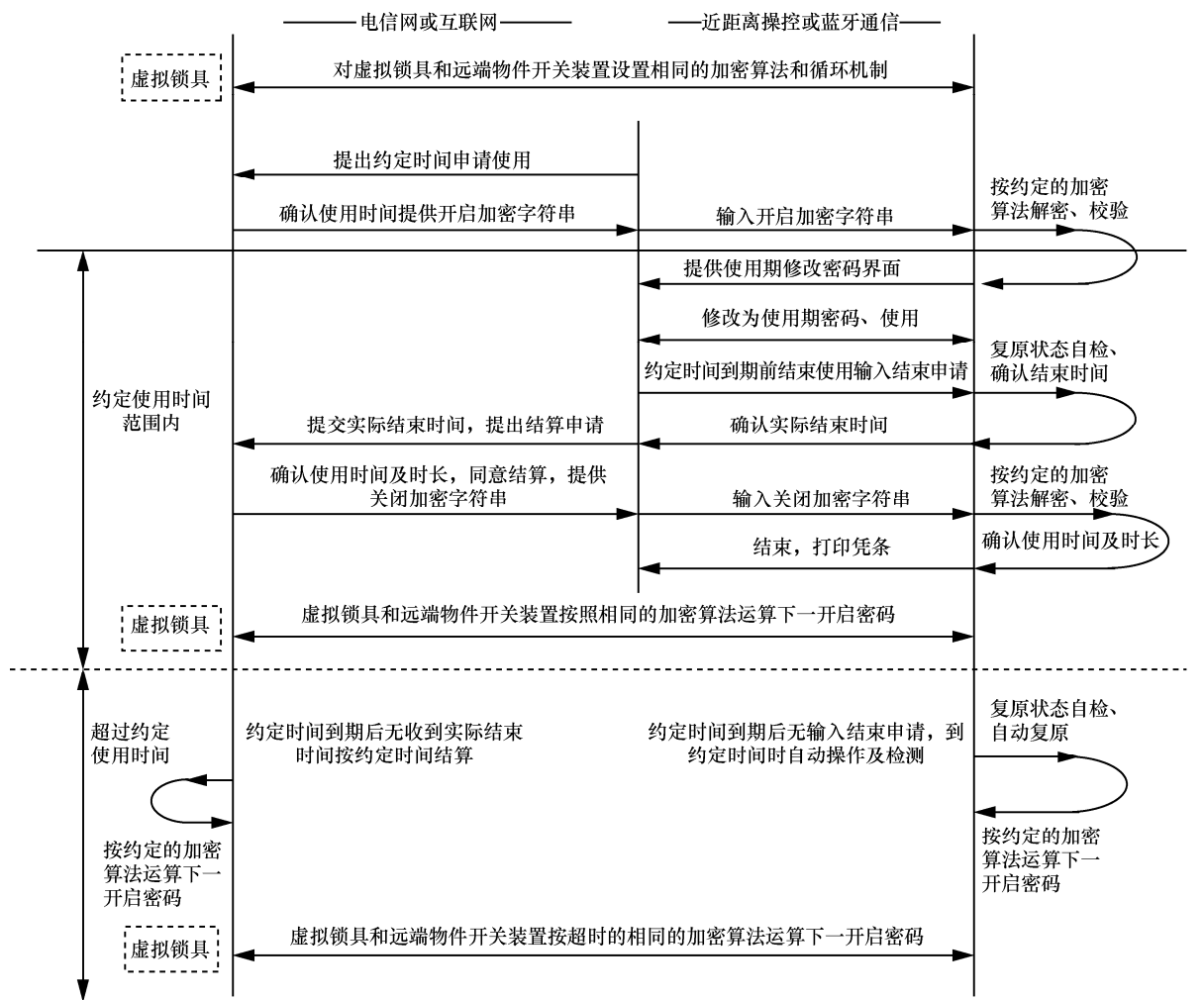


图4 一种远端非联网加密算法约定的约时开关装置的信息沟通控制流程

方建立的远程通信进行密码的传递，密码是可读可输入的字符串，所述的远程通信甚至涵盖传统的书信方式。一种远端非联网加密算法约定的约时开关装置的步骤方法如图5所示。

其中，本端密码运算器的预设加密循环机制选择和预设加密算法与远端非联网开关装置的预设解密循环机制和预设解密算法相匹配，预设加密循环机制的循环起始位置和预设解密循环机制的循环起始位置相同。

5 终端智能技术前景

通过在物体中植入智能系统，可以使物体有一定的智能性，能够主动或被动地实现与用户的

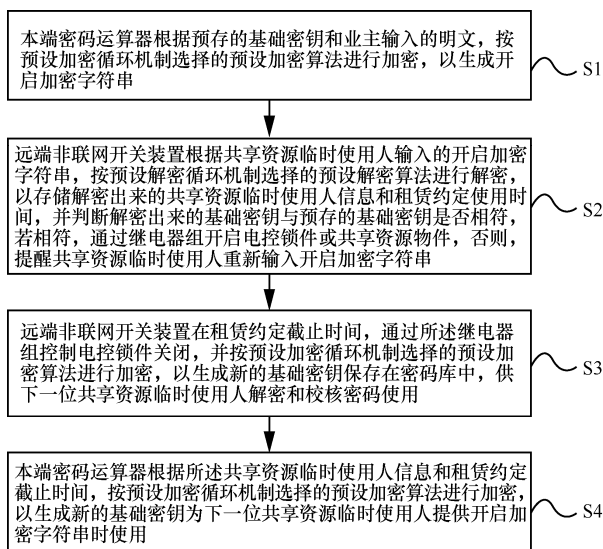


图5 一种远端非联网加密算法约定的约时开关装置的步骤方法

沟通,也是物联网的关键技术之一^[3]。具有加密算法约定的约时开关装置是在普通开关上植入了识读器和运算、计时和存储功能,与现有技术相比,无需以业主方为中心与远端物件和租赁方都有联网的远程通信;无需远端租赁物纳入互联网的网络部署和网络基础建设中;无需远端租赁物移动到有网络覆盖的地方才能完成使用权和退出使用的交接;对多数电器都可以使用文中提供的技术方案实现电器的应用控制,使电器类的设备灵活地受业主方控制;这种远端非联网加密算法约定的约时开关装置,只利用了业主与租赁户两者的通信,建立了一种“密控网”,是物联网技术的一个有益补充;只有本端密码运算器才有与远端非联网开关装置相同的加密算法,内置的不同加密算法根据本端密码运算器与远端非联网开关装置中才有的加密循环机制自动选择,密码自动运算出来,其他人无法破解。此前,绝大部分的人工智能都依赖云端实现;现在,部署在终端侧的人工智能正在开辟更为广阔的市场^[4]。依靠云端实现的人工智能存在一些弊端:首先,个人数据上传到云端不利于隐私保护;其次,云端人工智能需要较高的带宽支持,功耗较高;最后,云端人工智能会有较高的时延性,很多实时物联网场景无法应用。而利用远端非联网加密算法约定的解决方案,通过采用终端的运算能力代替对远端的通信能力,更能适应智能终端与云端无远程实时通信网络情况下的物联终端的应用体验,也就是说,植入了智能技术的终端能构建更大范围的物联网应用生态。

6 结束语

本文阐述的远端非联网加密算法约定的约时开关装置解决了远端物件的使用权在无网络环境下的转移问题;揭示了对不同的“物”是可以进行有区分的按需联网和“对话”,可以采用靠近物件的租赁方的长距通信延伸为接近通信进行远端

物件与业主方进行虚拟通信和对话;解决了现有技术中用户端需要接入互联网或通信网才能对远端可共享资源物件实现远程控制的问题,建立了一种无实时通信网络下的“密控网”,既作为物联网技术在无通信覆盖情况下的有益补充,也可以作为固定地点的远端物件按计算次序移交管理权或使用权,而无须建设后台通信网络以及等候期的通信费用支出。该技术方案特别适合偏僻地区的远端租赁物使用控制权的临时转移,例如偏僻地区的充电桩的收费使用控制、共享单车及共享汽车在无网络覆盖地区的使用。解决了在互联网覆盖未到达的地方,也能部署所有人的远端物件,并对该远端物件的加密算法约定的约时外租使用,扩大共享覆盖范围。

参考文献:

- [1] 田景熙. 物联网概论[M]. 南京: 东南大学出版社, 2010.
TIAN J X. Introduction to internet of things[M]. Nanjing: Southeast University Press, 2010.
- [2] 朱晓荣, 齐丽娜, 孙君. 物联网与泛在通信技术[M]. 北京: 人民邮电出版社, 2010.
ZHU X R, QI L N, SUN J. Internet of things ubiquitous communication technologies[M]. Beijing: Posts & Telecom Press, 2010.
- [3] 郭念, 张勇, 孙俊, 等. 浅谈电力物联网的应用与发展[J]. 工程技术, 2017(12): 114-115.
GUO N, ZHANG Y, SUN J, et al. Application and development of power internet of things[J]. Engineering Technology, 2017(12): 114-115.
- [4] 王旨, 张兴, 王文博. 无线边缘智能助力智慧社会[J]. 电信科学, 2019, 35(3): 54-61
WANG Z, ZHANG X, WANG W B. Wireless edge intelligence empowers smart society[J]. Telecommunications Science, 2019, 35(3): 54-61.

[作者简介]



张正峰(1971—),男,广东电网有限责任公司电力调度控制中心高级工程师,主要从事电力系统通信网络运行维护和规划工作,主要研究方向为电力通信资源管理系统。