(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111882704 B
(45)授权公告日 2021.02.12

(21)申请号 202010662731.8
(22)申请日 2020.07.10
(65)同一申请的已公布的文献号
申请公布号 CN 111882704 A
(43)申请公布日 2020.11.03
(73)专利权人 安安(深圳)智能电子有限公司
地址 518000 广东省深圳市宝安区西乡街道劳动社区西乡大道宝源华丰总部经济大厦C栋3层325号
(72)发明人 徐传清
(74)专利代理机构 深圳市道勤知酷知识产权代理事务所(普通合伙) 44439
代理人 何兵 饶盛添
(51)Int.Cl.
G07C 9/00(2020.01)
G07C 9/27(2020.01)
H04L 29/08(2006.01)

(56)对比文件
CN 207115538 U,2018.03.16
CN 207115538 U,2018.03.16
CN 104952128 A,2015.09.30
CN 101765995 A,2010.06.30
CN 110572843 A,2019.12.13
CN 201993826 U,2011.09.28
CN 202650103 U,2013.01.02
CN 109191630 A,2019.01.11
JP 4600096 B2,2010.12.15

审查员 周红静

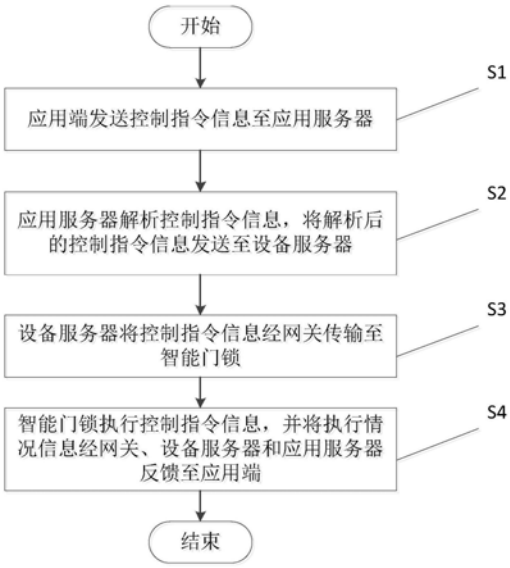
权利要求书2页 说明书10页 附图2页

(54)发明名称

一种智能门锁系统的控制方法以及智能门锁管理系统

(57)摘要

本发明揭示了一种智能门锁系统的控制方法以及智能门锁管理系统,所述方法应用于智能门锁管理系统,智能门锁管理系统包括应用端、应用服务器、设备服务器、网关和智能门锁;应用端发送控制指令信息至应用服务器;应用服务器解析控制指令信息,将解析后的控制指令信息发送至设备服务器;设备服务器将控制指令信息经网关传输至智能门锁;智能门锁执行控制指令信息,并将执行状态信息经网关、设备管理服务器、应用服务器反馈至应用端。通过本方案,管理者通过应用端即可给予用户使用智能门锁的权限,实现了门锁集中式可视化的系统管理;开门记录及电量信息都上传到系统,门锁状态可通过应用端设置,极大的方便了大批量智能门锁的有序化的集中管理。



CN 111882704 B

1.一种智能门锁系统的控制方法,其特征在于,所述方法应用于智能门锁管理系统,所述智能门锁管理系统包括应用端、应用服务器、设备服务器、网关和智能门锁;

所述应用端发送控制指令信息至所述应用服务器;

所述应用服务器解析所述控制指令信息,将解析后的所述控制指令信息发送至所述设备服务器;

所述设备服务器将控制指令信息经所述网关传输至所述智能门锁;

所述智能门锁执行所述控制指令信息,并将执行状态信息经所述网关、所述设备服务器和所述应用服务器反馈至所述应用端;

其中,所述智能门锁系统通过智控卡进行安装调试,所述应用端发送控制指令信息至所述应用服务器的步骤之后包括:

所述智能门锁是否读取到所述智控卡;

若是,则所述智能门锁获取所述智控卡物理身份ID,并生成第一门锁身份信息,其中,所述第一门锁身份信息为临时身份标识MAC;

所述智能门锁根据所述智控卡物理身份ID和所述第一门锁身份信息,生成注册包;

所述智能门锁通过所述网关将所述注册包发送至所述设备服务器;

所述设备服务器校验所述注册包信息,判断所述注册包信息是否有效;

若是,则所述设备服务器获取数据库生成的第二门锁身份信息并根据所述注册包信息、所述第二门锁身份信息以及当前系统时间生成调试反馈数据包,经所述网关发送至所述智能门锁,其中,所述调试反馈数据包包括所述第二门锁身份信息,第三门锁身份信息,网关身份信息和系统当前时间信息,其中所述第三门锁身份信息与所述第一门锁身份信息内容相同,第二门锁身份信息为所述智能门锁的真实身份标识MAC;

所述智能门锁解析所述调试反馈数据包,比对所述智能门锁本地的所述第一门锁身份信息与所述调试反馈数据包中的所述第三门锁身份信息是否一致;

若是,则所述智能门锁从所述调试反馈数据包中读取所述第二门锁身份信息,并将所述智能门锁本地临时的所述第一门锁身份信息替换成所述第二门锁身份信息并存储相应的网关身份唯一标识信息,校正本地时间,校正本地时间,完成调试,其中,所述网关身份唯一标识信息用于初步判断数据的合法性。

2.根据权利要求1所述的智能门锁系统的控制方法,其特征在于,所述智能门锁执行所述控制指令信息的步骤,包括:

判断所述控制指令信息的数据是否有效;

若是,则解析所述控制指令信息的数据,并再次判断解析后的所述控制指令信息的数据是否有效;

若是,则读取当前所述控制指令信息对应的传输序列号,判断所述传输序列号的数值是否大于前一传输序列号数值,其中,所述传输序列号包含于所述控制指令信息中,所述前一传输序列号存储于所述智能门锁中;

若是,则判定当前所述控制指令信息为可执行命令,执行所述控制指令信息。

3.根据权利要求2所述的智能门锁系统的控制方法,其特征在于,所述智能门锁执行所述控制指令信息,并将执行状态信息经所述网关、所述设备服务器和所述应用服务器反馈至所述应用端的步骤,包括:

所述智能门锁执行所述控制指令信息后生成反馈报文，其中，所述反馈报文包含所述执行状态信息；

所述智能门锁对所述反馈报文根据预先定义的加密种子进行加密，生成加密数据包，进入发送模式；

所述智能门锁将所述加密数据包发送至所述设备服务器。

4.根据权利要求1所述的智能门锁系统的控制方法，其特征在于，所述设备服务器将控制指令信息经所述网关传输至所述智能门锁的步骤之后，包括：

以所述设备服务器发送控制指令信息至所述网关的时刻为第一起点时刻，判断第一预设时间段内是否接收到所述网关反馈的所述执行状态信息；

若否，则所述设备服务器将控制指令信息放到重发数据队列中等待重发至所述网关。

5.根据权利要求4所述的智能门锁系统的控制方法，其特征在于，所述若否，则所述设备服务器将控制指令信息放到重发数据队列中等待重发至所述网关步骤之后，包括：

以所述设备服务器重新发送控制指令信息至所述网关的时刻为第二起点时刻，判断第二预设时间段内是否接受到所述网关反馈的所述执行状态信息；

若否，则判定所述智能门锁异常，门锁控制指令执行异常信息推送。

6.根据权利要求1至5任意一项所述的智能门锁系统的控制方法，其特征在于，所述所述设备服务器将控制指令信息经所述网关传输至所述智能门锁的步骤，包括：

所述网关采用双频率双通道收发机制，发送数据时使用频率为434MHz的频段，接收数据时使用频率为471MHz的频段。

7.根据权利要求1所述的智能门锁系统的控制方法，其特征在于，所述应用服务器解析所述控制指令信息，将解析后的所述控制指令信息发送至所述设备服务器的步骤，包括：

所述设备服务器判断所述应用服务器是否授权；

若是，则所述设备服务器允许所述应用服务器的访问，并执行所述应用端传输的控制指令信息。

8.根据权利要求1所述的智能门锁系统的控制方法，其特征在于，所述设备服务器将控制指令信息经所述网关传输至所述智能门锁的步骤之前，包括：

所述智能门锁唤醒后进入初始化，经过初始化后进入CAD模式；

所述智能门锁通过CAD方式嗅探，判断是否接收到预设频段的前导码数据；

若否，则所述智能门锁进入休眠状态。

9.一种智能门锁管理系统，应用于权利要求1至8任意一项所述的智能门锁系统的控制方法，其特征在于，包括：

应用端，用于用户发送控制指令信息以及查看智能门锁管理系统的状态信息；

应用服务器，用于所述应用端信息的发送与接收；

设备服务器，用于所述智能门锁、网关的管理，以及对传输数据进行加密、解密、校验和访问控制；

智能门锁，用于开关门，并将所述控制指令信息的执行状态反馈至所述应用端；

网关，用于绑定所述智能门锁身份，以及传输数据。

一种智能门锁系统的控制方法以及智能门锁管理系统

技术领域

[0001] 本发明涉及到物联网领域，特别是涉及到一种智能门锁系统的控制方法以及智能门锁管理系统。

背景技术

[0002] 随着信息技术的不断发展，伴随这传感器技术和自动化控制技术的进步，人们不再满足于有线的信息传递方式，追求无线、高速且更加安全的信息传输方式，物联网应运而生。

[0003] 目前，常用的门锁主要由机械锁和智能电子门锁。机械锁需要人们随身携带机械钥匙，机械钥匙非常不便且容易丢失，像学校、公寓、酒店、办公室、宿舍等管理员，对于房间和门锁钥匙的管理越来越难以及钥匙配送麻烦。常见的智能电子门锁有密码、指纹识别、刷卡等智能门锁，在锁上输入密码、刷卡或者识别指纹进行开锁，带来了极大的便利，但不能远程对人员权限和门锁进行管理。

[0004] 对于学校、公寓、酒店、办公等场景而言，需要与人员、房卡、房间等信息以及人员权限管理相融合，现有的智能电子门锁明显无法满足需求。

发明内容

[0005] 本发明的主要目的为提供一种智能门锁系统的控制方法，旨在解决传统智能门锁系统无法实现大批量门锁和人员的精细化管理的技术问题。

[0006] 一种智能门锁系统的控制方法，所述方法应用于智能门锁管理系统，智能门锁管理系统包括应用端、应用服务器、设备服务器、网关和智能门锁；

[0007] 应用端发送控制指令信息至应用服务器；

[0008] 应用服务器解析控制指令信息，将解析后的控制指令信息发送至设备服务器；

[0009] 设备服务器将控制指令信息经网关传输至智能门锁；

[0010] 智能门锁执行控制指令信息，并将执行情况信息经网关、设备服务器和应用服务器反馈至应用端。

[0011] 优选的，智能门锁执行控制指令信息的步骤，包括：

[0012] 判断控制指令信息的数据是否有效

[0013] 若是，则解析控制指令信息的数据，并再次判断解析后的控制指令信息的数据是否有效；

[0014] 若是，则读取当前控制指令信息对应的传输序列号，判断传输序列号的数值是否大于前一传输序列号数值，其中，传输序列号包含于控制指令信息中，前一传输序列号存储于智能门锁中；

[0015] 若是，则判定当前控制指令信息为可执行命令，执行控制指令信息。

[0016] 优选的，智能门锁执行控制指令信息，并将执行情况信息经网关、设备服务器和应用服务器反馈至应用端的步骤，包括：

[0017] 智能门锁执行控制指令信息后生成反馈报文,其中,反馈报文包含执行状态信息、本次通信传输序列号等信息;

[0018] 智能门锁对反馈报文根据预先定义的加密种子进行加密,生成加密数据包,进入发送模式;

[0019] 智能门锁将加密数据包发送至设备服务器。

[0020] 优选的,智能门锁系统通过智控卡进行安装调试,应用端发送控制指令信息至应用服务器的步骤之后包括:

[0021] 智能门锁是否读取到智控卡;

[0022] 若是,则智能门锁获取智控卡物理身份ID,并生成第一门锁身份信息,其中,第一门锁身份信息为临时身份标识MAC;

[0023] 智能门锁根据智控卡物理身份ID和第一门锁身份信息,生成注册包;

[0024] 智能门锁通过网关将注册包发送至设备服务器;

[0025] 设备服务器校验注册包信息,判断注册包信息是否有效;

[0026] 若是,则设备服务器获取数据库生成的第二门锁身份信息并根据注册包信息、第二门锁身份信息以及当前时间生成调试反馈数据包,经网关发送至智能门锁,其中,调试反馈数据包包括第二门锁身份信息,第三门锁身份信息,网关身份信息和系统当前时间信息,其中第三门锁身份信息与第一门锁身份信息内容相同,第二门锁身份信息为智能门锁的真实身份标识MAC;

[0027] 智能门锁解析调试反馈数据包,比对智能门锁本地的第一门锁身份信息与调试反馈数据包中的第三门锁身份信息是否一致;

[0028] 若是,则智能门锁从调试反馈数据包中读取第二门锁身份信息,并将智能门锁本地临时的第一门锁身份信息替换成第二门锁身份信息并存储相应的网关身份唯一标识信息,校正本地时间,完成调试,其中,网关身份唯一标识信息用于初步判断数据的合法性。

[0029] 优选的,设备服务器将控制指令信息经网关传输至智能门锁的步骤之后,包括:

[0030] 以设备服务器发送控制指令信息至网关的时刻为第一起点时刻,判断第一预设时间段内是否接收到网关反馈的执行情况信息;

[0031] 若否,则设备服务器将控制指令信息放到重发数据队列中等待重发至网关。

[0032] 优选的,若否,则设备服务器将控制指令信息放到重发数据队列中等待重发至网关步骤之后,包括:

[0033] 以设备服务器重新发送控制指令信息至网关的时刻为第二起点时刻,判断第二预设时间段内是否接受到网关反馈的执行状态信息;

[0034] 若否,则判定智能门锁异常,门锁控制指令执行异常信息推送。

[0035] 优选的,设备服务器将控制指令信息经网关传输至智能门锁的步骤,包括:

[0036] 网关采用双频率双通道收发机制,发送数据时使用频率为434MHz的频段,接收数据时使用频率为471MHz的频段。

[0037] 优选的,应用服务器解析控制指令信息,将解析后的控制指令信息发送至设备服务器的步骤,包括:

[0038] 设备服务器判断应用服务器是否授权;

[0039] 若是,则设备服务器允许应用服务器的访问,并执行应用端传输的控制指令信息。

[0040] 优选的，设备服务器将控制指令信息经网关传输至智能门锁的步骤之前，包括：

[0041] 智能门锁唤醒后进入初始化，经过初始化后进入CAD模式；

[0042] 智能门锁通过CAD方式嗅探，判断是否接收到预设频段的前导码数据；

[0043] 若否，则智能门锁进入休眠状态。

[0044] 本发明还提供一种智能门锁管理系统，应用于上述的智能门锁系统的控制方法，包括：

[0045] 应用端，用于用户发送控制指令信息以及查看智能门锁管理系统的状态信息；

[0046] 应用服务器，用于应用端信息的发送与接收；

[0047] 设备服务器，用于智能门锁、网关的管理，以及对传输数据进行加密、解密、校验和访问控制；

[0048] 智能门锁，用于开关门，并将控制指令信息的执行情况反馈至应用端；

[0049] 网关，用于绑定智能门锁身份，以及传输数据。

[0050] 本发明的有益效果在于：通过本方案，管理者可通过设备服务器远程授权的方式给予用户使用智能门锁的权限，避免了传统方式的现场交接的繁琐；此外，用户使用智能门锁的记录都存储在系统中，方便管理者查看各用户的情况，实现大批量智能门锁的有序化的集中管理。管理者通过应用端即可给予用户使用智能门锁的权限，实现了门锁集中式可视化的系统管理；此外，开门记录及电量信息都上传到系统，门锁状态可通过应用端设置，极大的方便了大批量智能门锁的有序化的集中管理。

附图说明

[0051] 图1为本发明一种智能门锁系统的控制方法的第一实施例的流程示意图；

[0052] 图2为本发明一种智能门锁管理系统的结构示意图；

[0053] 图3为本发明一种智能门锁系统的控制方法的调试过程示意图。

[0054] 标号说明：

[0055] 1、应用端；2、应用服务器；3、设备服务器；4、网关；5、智能门锁。

[0056] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0057] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0058] 参照图1和图2，本发明提供一种智能门锁系统的控制方法，所述方法应用于智能门锁管理系统，智能门锁管理系统包括应用端1、应用服务器2、设备服务器3、网关4和智能门锁5；

[0059] S1：应用端1发送控制指令信息至应用服务器2；

[0060] S2：应用服务器2解析控制指令信息，将解析后的控制指令信息发送至设备服务器3；

[0061] S3：设备服务器3将控制指令信息经网关4传输至智能门锁5；

[0062] S4：智能门锁5执行控制指令信息，并将执行情况信息经网关4、设备服务器3和应用服务器2反馈至应用端1。

[0063] 在本发明实施例中，应用端1包括电脑端和移动终端(如智能手机和平板电脑等)，

一个网关4可对接多个智能门锁5。举例的，以“远程开门”为例。用户经过应用端1发送“远程开门”指令至应用服务器2，应用服务器2解析该指令，将指令传输至设备服务器3，其中，开门指令信息包括房间号、设备类型、控制命令、访问权限的token、控制信息等。设备服务器3对控制指令进行数据来源校验、解析等动作，判断控制指令有效后加密该指令，将加密后的指令传输至网关4通过SPI3通信接口将控制指令传输至智能门锁5。智能门锁5在判断控制指令有效后，执行控制指令，完成开锁，并将开锁情况（如开锁成功，或失败）反馈至应用端1。除此之外，本智能门锁管理系统还可实时远程开门、清除用户开门信息、获取日志、绑定、解绑、本地授权、时间同步等动作，实现联网门锁的远程控制和集中管理。通过上述设置，管理者可通过设备服务器3远程授权的方式给予用户使用智能门锁5的权限，避免了传统方式的现场交接的繁琐；此外，用户使用智能门锁5的记录都存储在系统中，方便管理者查看各用户的情况，实现大批量智能门锁5的有序化的集中管理。综上，通过本方法还能实现实时远程开门、远程密码授权、远程IC卡授权、远程门锁长开长关设置、清除用户开门信息、获取日志、安装调试、解绑、本地授权、时间同步、信号测试等功能，实现联网门锁的远程控制和集中管理；将人员、房间、房卡、租金、水电费等信息的管理相融合，实现智能门锁5精细化管理，提高管理效率，降低运营成本。通过本方案，管理者通过应用端1即可给予用户使用智能门锁5的权限，实现了门锁集中式可视化的系统管理；此外，开门记录及电量信息都上传到系统，门锁状态可通过应用端设置，极大的方便了大批量智能门锁的有序化的集中管理。

[0064] 进一步地，智能门锁5执行控制指令信息的步骤S4，包括：

[0065] S41：判断控制指令信息的数据是否有效；

[0066] S42：若是，则解析控制指令信息的数据，并再次判断解析后的控制指令信息的数据是否有效；

[0067] S43：若是，则读取当前控制指令信息对应的传输序列号，判断传输序列号的数值是否大于前一传输序列号数值，其中，传输序列号包含于控制指令信息中，前一传输序列号存储于智能门锁5中；

[0068] S44：若是，则判定当前控制指令信息为可执行命令，执行控制指令信息。

[0069] 在本发明实施例中，控制指令信息发到智能门锁5后，智能门锁5根据网关身份唯一标识信息和门锁身份唯一标识信息，判断所述控制指令信息的数据是否有效。若是，则智能门锁5的处理器判断控制指令信息的数据的包头、校验、和结束位信息是否均对等。若是，则初步判定控制指令信息的数据有效，将数据进行层层解析，还需再次判断数据的包头、校验、和结束位信息是否对等。如果对等，即再次判定控制指令信息有效。智能门锁5读取控制指令信息中的传输序列号，此外，智能门锁5内部存储有以往控制指令信息存储下来的传输序列号，即序列号记录，其中，网关4每次传输控制指令信息到智能门锁5对应的传输序列号都会更新。智能门锁5判断当前序列号的数值是否大于前一传输序列号数值。若是，则证明控制指令信息为可执行命令，并更新由网关4传输控制指令信息到智能门锁5对应的传输序列号至本地内存中，智能门锁5执行控制指令信息。通过上述设置，智能门锁5在接收数据时会判断数据是否有效，特别是通过判断传输序列号的机制，防止他人空中监听截取数据，即使他人空中拦截控制指令信息，待智能门锁5执行完当前控制指令信息后，他人再将拦截的控制指令信息发送至智能门锁5，智能门锁5判断出控制指令信息中的传输序列号是历史值，故不会执行拦截的控制指令信息，从而提高了系统的安全性。

[0070] 在本发明其它实施例中，智能门锁5接收到控制指令信息时会解析，获取数据包的加密ID。然后，通过加密ID获取真正的解密密匙，经过解密函数的处理，得到解密后的数据。再通过私有协议层层解析，获取到具体数据，比对身份ID以及传输序列号的合法性，执行相关控制指令，比如开门。举例的，智能门锁5接收到的数据包(即控制指令)为“7C 0C D2 D6 66 15 6D BA 20 CC CD C3 CB CC CC CC D6 4C 89 68 72 EC C9 EC D4 F9 EE 36 27 FF”。经过解析后，得到获取的加密ID为8。再通过加密ID获取真正的解密密匙，经过解密函数的处理，得到解密后的数据，如下所述，“C0 EE 1E 11 AA 09 21 06 EC 00 01 0F 07 00 00 00 10 80 45 A4 0E 20 05 20 18 35 22 FA 27 FF”，最终得到具体数据。通过上述设置，通过解析数据包获取加密ID、通过加密ID获取解密密匙，再经过解密函数，才能对数据包解密，该环节层层设置，一层不符合，则数据包解密失败，智能门锁5无法执行控制指令，加大他人破解系统的难度，极大的提高了系统的安全性。

[0071] 进一步地，智能门锁5执行控制指令信息，将执行情况信息经网关4、设备服务器3和应用服务器2反馈至应用端1的步骤S4，包括：

[0072] S4a：智能门锁5执行控制指令信息后产生反馈报文，其中，反馈报文包含执行状态信息；

[0073] S4b：智能门锁5对反馈报文根据预先定义的加密种子进行加密，生成加密数据包，进入发送模式；

[0074] S4c：智能门锁5将加密数据包发送至设备服务器3。

[0075] 在本发明实施例中，智能门锁5执行控制指令信息后产生反馈报文，举例的，反馈报文为十六进制数据，具体为“E0 A0 1F BA AA 7F DF 01 4D 85 0C 01 10 60 20 92 73 20 05 20 18 40 14 96 3C FF”，这是原始数据，不能暴露，因此需要进一步进行加密。智能门锁5对反馈报文根据预先定义的加密种子进行加密，生成加密数据包。经过加密种子加密后，得到数据为“A3 D3 09 09 B9 6C CC 12 5E 96 1F 12 03 13 13 11 60 33 16 33 0B 53 07 85 2F FF”。智能门锁5将加密数据包发送至设备服务器3。本套加密方法的优点在于结合自身协议及智能门锁资源设计，严格筛选加密种子，大大增加解密的难度；加密与解密后数据长度不会发生改变，提高数据传输的可靠性；加密与解密占用资源少，速度快，极大降低智能门锁能耗。此外，通过上述设置，防止别人窃取数据后，破解私有协议，随意控制智能门锁5，且防止别人监听，获取数据二次使用以达到控制智能门锁5目的。具体的，本方案的加密方法包括：预先严格筛选解密的难度大的加密种子，分别存储在智能门锁5和服务程序中，并不存储在服务器或者智能门锁5的内存中，防止直接破解获取内存中的加密种子；服务器和智能门锁5具备相同的加密和解密算法，提供程序在收到或者发送数据时，进行加密和解密获取正确的数据；为进一步加强破解的难度，在加密处理函数中定义了一个特殊的种子以及通过Unix时间作为种子，随机函数获取种子ID，增加加密数据的不确定性；加密所需要为种子ID、需要加密的数据、特殊种子经过特定的算法，得到加密后的数据，数据解密与加密是一个可逆的过程，通过解密函数做相同的处理就可以得到原始的数据。

[0076] 参照图3，智能门锁系统通过智控卡进行安装调试，应用端1发送控制指令信息至应用服务器3的步骤S1之后，包括：

[0077] S1a：智能门锁5是否读取到智控卡；

[0078] S1b：若是，则智能门锁5获取智控卡物理身份ID，并生成第一门锁身份信息，其中，

第一门锁身份信息为临时身份标识MAC；

[0079] S1c：智能门锁5根据智控卡物理身份ID和第一门锁身份信息，生成注册包；

[0080] S1d：智能门锁5通过网关4将注册包发送至设备服务器3；

[0081] S1f：设备服务器3校验注册包信息，判断注册包信息是否有效；

[0082] S1g：若是，则设备服务器3获取数据库生成的第二门锁身份信息并根据注册包信息、第二门锁身份信息以及当前时间生成调试反馈数据包，经网关4发送至智能门锁5，其中，调试反馈数据包包括第二门锁身份信息，第三门锁身份信息，网关4身份信息和系统当前时间信息，其中第三门锁身份信息与第一门锁身份信息内容相同，第二门锁身份信息为智能门锁5的真实身份标识MAC；

[0083] S1h:智能门锁5解析调试反馈数据包，比对智能门锁5本地的第一门锁身份信息与调试反馈数据包中的第三门锁身份信息是否一致；

[0084] S1i:若是，则智能门锁5从调试反馈数据包中读取第二门锁身份信息，并将智能门锁5本地临时的第一门锁身份信息替换成第二门锁身份信息并存储相应的网关4身份唯一标识信息，校正本地时间，完成调试，其中，网关4身份唯一标识信息用于初步判断数据的合法性。

[0085] 在本发明实施例中，管理人员在应用端1点击“安装调试”按钮，应用服务器2将房间号和请求参数向设备服务器3发送。管理人员通过智能门锁5刷智控卡，开启注册调试，触发智能门锁5发起注册请求。若管理人员已刷智控卡，则智能门锁5获取智控卡的ID信息，且生成第一门锁身份信息，即第一临时MAC地址。设备服务器3接收到调试指令信息后，在设备服务器3的数据库(MySQL书库)生成第二门锁身份信息，即数据库MAC地址。智能门锁根据智控卡ID信息和第一临时MAC地址，生成注册包，其中，注册包为数据包。智能门锁5通过广播的形式向周围所有网关4发送注册包，所有接收到注册包的网关4都向设备服务器3发送注册包。设备服务器3接收到数据后解析相关参数、校验、判别进入相应的处理程序，通过解析后的相关参数在MySQL数据库中查询智能门锁5的身份信息，即数据库MAC地址，设备服务器3收到智能门锁5反馈的注册包中状态为成功时，将房间信息、智能门锁5和网关4三者进行绑定，将绑定结果推送到应用服务器2或者第三方。设备服务器3成功校验注册包数据后，生成调试反馈数据包，经网关4以点对点形式发送至智能门锁5，其中，调试反馈数据包包括第二门锁身份信息(数据库MAC地址)，第三门锁身份信息(第二临时MAC地址)，网关身份信息(网关MAC地址)和时间校正包。智能门锁5解析调试反馈数据包，判断智能门锁5本地的第一门锁身份信息(即第一临时MAC地址)与调试反馈数据包中的第三门锁身份信息(即第二临时MAC地址)。若一致，则证明该智能门锁5为正在进行安装调试的智能门锁5。该智能门锁5的第一门锁身份信息(第一临时MAC地址)被替换成第二门锁身份信息(即数据库MAC地址)，完成智能门锁5的注册。在本发明其它实施例中，智能门锁5通过时间校正包，调整好智能门锁5的工作时间，保证智能门锁5的正常运行。在本发明其它实施例中，从触发“安装调试”按钮为起点时刻，智能门锁5需在预设时间段内(如30秒)接触智控卡，调试成功后，智能门锁5响起四声，提醒管理人员完成安装调试。超过预设时间段，则用户需要重新在应用端1点击“安装调试”按钮。通过上述设置，避免智能门锁5长期处于待注册状态，影响该账号无法再进行安装调试。此外，在本发明其它实施例中，通过输入密码的形式代替刷智控卡，触发智能门锁5的注册。通过该设置，实现智能门锁5多元化注册。综上，相比于传统门锁系统安装

调试过程，需要使用多种卡，比如功能卡、校准卡和数据卡完成安装调试的各个环节，调试过程相当复杂。本方案仅需一张智控卡即可完成门锁系统的安装调试，大幅降低安装调试过程中繁琐复杂的操作，提高智能门锁系统的安装调试的工作效率。

[0086] 进一步地，设备服务器3将控制指令信息经网关4传输至智能门锁5的步骤S3之后，包括：

[0087] S31：以设备服务器3发送控制指令信息至网关4的时刻为第一起点时刻，判断第一预设时间段内是否接收到网关4反馈的执行情况信息；

[0088] S32：若否，则设备服务器3将控制指令信息放到重发数据队列中等待重发至网关4。

[0089] 在本发明实施例中，用户通过应用端1发送控制指令信息，设备服务器3收到后，通过解析和封装，将封装好的数据加入到数据队列中，通过数据中包含的网关身份信息通知相应的网关4将控制指令信息发送至智能门锁5。由于无线通信受环境影响因素较大，为保证系统的可靠性，以设备服务器3发送控制指令信息至网关4的时刻为第一起点时刻，判断第一预设时间段内是否接收到网关4反馈的执行情况信息。若没有，则设备服务器3重新发送控制指令信息放到重发数据队列中等待重发至至网关4，减少环境因素对系统可靠性的影响。

[0090] 进一步地，设备服务器3将控制指令信息放到重发数据队列中等待重发至网关4的步骤S32之后，包括：

[0091] S33：以设备服务器3重新发送控制指令信息至网关4的时刻为第二起点时刻，判断第二预设时间段内是否接受到网关4反馈的执行情况信息；

[0092] S34：若否，则判定智能门锁5异常，执行异常信息推送。

[0093] 在本发明实施例中，以设备服务器3重新发送控制指令信息至网关4的时刻为第二起点时刻，判断第二预设时间段内是否接受到网关4反馈的执行情况信息。若设备服务器3在规定时间内再次没收到网关4的反馈信息，则设备服务器3判定智能门锁5异常，无法接收数据包。设备服务器3将智能门锁5的异常信息推送至应用端1。通过上述设置，系统异常时，提醒用户和管理人员及时维修。

[0094] 在本发明其它实施例中，当设备服务器3在规定时间内收到网关4反馈的信息后。设备服务器3获取反馈信息中的命令序列号，通过所述命令序列号在数据队列和缓存队列中查找对应的原始数据，删除数据队列和缓存队列中的原始数据，向应用端1推送执行命令成功的结果。通过删除数据队列和缓存队列中的原始数据，避免设备服务器3重复发送相同命令，导致智能门锁5多次执行同一控制指令，占用系统资源。在本发明又一实施例中，设备服务器3无法找到命令序列号时，证明该数据包是非法数据包，丢弃该数据包。设备服务器3将不执行数据推送，继续下发下一个数据包，同时清除超时数据包。

[0095] 进一步地，设备服务器3将控制指令信息经网关4传输至智能门锁5的步骤S3，包括：

[0096] S3A：网关4采用双频率双通道收发机制，发送数据时使用频率为434MHz的频段，接收数据时使用频率为471MHz的频段。

[0097] 在本发明实施例中，网关4采用双频率单通道收发机制，发送数据时使用频率为434MHz的频段，接收数据时使用频率为471MHz的频段。这样可以有效避免数据发送碰撞，从

而提高数据发送成功率,保证通信链路的可靠性,稳定性。

[0098] 进一步地,应用服务器2解析控制指令信息,将解析后的控制指令信息发送至设备服务器3的步骤S2之前,包括:

[0099] S21:设备服务器3判断应用服务器2是否授权;

[0100] S22:若是,则设备服务器3允许应用服务器2的访问,并执行应用端1传输的控制指令信息。

[0101] 在本发明实施例中,应用端1根据账号appid和密码secret,获取设备服务器3的访问凭证token。设备服务器3判断应用端1是否授权,即设备服务器3判断redis中是否存在该token。若存在,设备服务器3允许应用端1的访问,并执行应用端1传输的控制指令信息。通过上述设置,只有获取访问凭证的应用端1才允许访问设备服务器3,从而保证系统的安全性。

[0102] 在本发明其它实施例中,以安装调试为例。若“安装调试”的请求是合法的,则设备服务器3进一步判断传进的数据的正确性。通过查询数据库比对房间号、appid和设备类型的正确性,检测到的错误反馈给调用者,比如房间号不存在,返回房间号不存在的提示给管理人员。

[0103] 进一步地,设备服务器3将控制指令信息经网关4传输至智能门锁5的步骤S3之前,包括:

[0104] S3A1:智能门锁5唤醒后进入初始化,经过初始化后进入CAD模式;

[0105] S3A2:智能门锁5通过CAD方式嗅探,判断是否接收到预设频段的前导码数据;

[0106] S3A3:若否,则智能门锁5进入休眠状态。

[0107] 在本发明实施例中,智能门锁5唤醒后进入初始化,智能门锁5的射频模块里的控制芯片进行CAD初始化。经过初始化后进入CAD模式。智能门锁5通过CAD方式嗅探,判断是否接收到预设频段的前导码数据,其中,预设频段为471MHz。如果智能门锁5嗅探后没收到前导码数据,则智能门锁5进入休眠状态,使得智能门锁5无需实时处于工作状态,降低它的功耗。此外,本方案结合自身通信距离有限的特点,通过调优LORA通信主要的技术参数,为提高智能门锁信号的稳定性和持续续航的能力。具体包括:通过调节发射功率和功耗之间是比例关系,使之恰好适合智能门锁的通信距离特性要求,从而大大降低功耗,延长智能门锁5续航能力;增加信号带宽,可以提高有效数据速率以缩短传输时间,通过真实的应用环境和多种距离测试,调优出智能门锁信号带宽最优值,缩短了通信时同时降低了智能门锁5的耗电量和提高了用户的体验感;此外,为进一步降低智能门锁5的功耗,根据实际应用场景及以往的经验,通过设置LORA的前导码的长短,适应智能门锁具体的应用环境,减少LORA模块的唤醒次数,增长智能门锁的睡眠时间,延长智能门锁正常运行的时间;由于智能门锁会安装在复杂多变的环境中,提高LORA通信的抗干扰性是很有必要的,通过调整扩频因子(SF)和纠错率(CR)这两种设计变量,从而在带宽占用、数据速率、链路预算改善以及抗干扰性之间达到更好的平衡,

[0108] 在本发明其它实施例中,若智能门锁5接收到前导码数据,则智能门锁5进入工作状态,处理任务。

[0109] 参照图2,本发明提供一种智能门锁管理系统,应用于上述的智能门锁系统的控制方法,包括:

[0110] 应用端1,用于用户发送控制指令信息以及查看智能门锁管理系统的状态信息;

[0111] 应用服务器2,用于应用端1信息的发送与接收;

[0112] 设备服务器3,用于智能门锁、网关的管理,以及对传输数据进行加密、解密和校验和访问控制;

[0113] 智能门锁5,用于开关门,并将控制指令信息的执行情况反馈至应用端1;

[0114] 网关4,用于绑定智能门锁5的身份,以及传输数据。

[0115] 在本发明实施例中,应用端1主要由java后台、web页面和微信公众号组成,能够满足移动端和pc端客户的需求,不需要复杂的安装过程,打开页面即可使用。

[0116] 应用端1是管理员对联网门锁的日常管理工具,为了方便管理员的管理工作,结合用户的使用需求,为客户提供楼宇人员、房间、房卡、记录详情、门锁状态等信息的融合远程管理功能,分别为:业务办理模块、查询报表、基础信息设置、门禁管理、系统设置模块。业务办理模块主要用于人员信息登记、人员信息审核、房卡信息、开门权限设置、清除数据、获取门锁日志、远程开门、历史用户记录等功能。查询报表具备开门日志查询和操作日志查询功能,可以根据具体时间进行查询和追踪所有开门记录和系统操作记录。

[0117] 基础信息设置是用于设置账号的一些基本信息;网关设置是用于网关4从相关操作,包括设备的增加、删除、修改、查看具体信息、指控卡的更改等功能;房间设置是用于楼栋、房间的分配,联网锁的安装调试、解绑、信号测试、电量情况等功能;管理员卡管理是指特定的卡可以设置特定网关4所管理的联网锁的开门权限,可根据需要任意设定;写卡器管理是将要使用的写卡器序列号添加进来,在使用时写卡器软件将数据与服务器同步,在相应的房间显示相关用户信息;房卡设置主要用于添加要使用的卡到服务器,方便管理员在登记人员信息或设置开门权限提供选择;

[0118] 门禁设置管理是用于门禁设备从相关操作,包括设备的增加、删除、修改、查看具体信息、门禁状态、设置门禁、远程开门、日志查询;用户详情是指该门禁具体有哪些人在使用;门禁开门日志查询和门禁操作日志查询功能,可以根据具体时间进行查询和追踪所有开门记录和系统操作记录

[0119] 管理员账号管理是可以为该账号分配一个子账号。

[0120] 设备服务器3是智能门锁管理系统的核心,为保证服务端的功能稳定性,该远程服务端基于golang语言开发,语言本身从底层原生支持高并发,无须第三方库以及线程轻量级,可以很轻松解决使用cpu资源问题,为更多设备接入提供便利。设备服务器3采用beego框架设计,为应用端1提供HTTP请求,采用TCP/IP通信协议与网关4建立连接,实现相互通信。为了维持应用端1的连接,与网关4建立了心跳机制,防止异常情况下导致网关4与设备服务器3的连接断开,服务端无法检测和推送通知用户网关4的在线状态,为正常通信提供实时监控数据。

[0121] 设备服务器3主要设备提供服务,功能包括设备的添加、删除、修改、绑定、解除绑定、随机产生控制中心与智能门锁5通信时使用MAC地址、为第三方提供HTTP协议接口控制智能门锁5以及开门记录、控制命令是否成功的推送。其中HTTP协议接口包括远程开门、发卡/密码、设备复位、设置长开长关、信号测试、电量状态、获取日志、增删改设备、安装调试、解绑、房间同步等接口,极大方便第三方将门锁管理功能植入他们自己系统。

[0122] 网关4管理的智能门锁5的数据,是设备服务器3与智能门锁5进行通信的桥梁。网

关4与设备服务器3建立的连接是基于传输控制协议(TCP/IP),网络中两个不同程序通过建立一个双向的通讯连接实现数据交换,这个双向链路的一端称为Socket,其中发起连接的一端称为应用端,被连接的一端称为服务端。

[0123] 由于网关4与设备服务器3一直保持连接,才能保证门锁指令正常收发,在实际环境中一些特殊情况或其他因素导致连接断开,如网络异常、程序跑飞等情况,这就需要异常处理机制,当网络情况异常时,网关4尝试连接设备服务器3,直至网络恢复正常。程序跑飞也可以通过看门狗检测出来,重启程序恢复正常。这些异常情况都可以通过网关指示灯获悉。

[0124] 网关4可以进入路由管理界面,设置网关对应的设备服务器ip地址、端口、动静态获取ip地址等功能。设备服务器IP地址和端口时是该网关4要接入目标设备服务器公网ip地址和端口;动静态获取ip地址时指由本地路由随机或者指定分配ip给控制中心使用。

[0125] 每一个网关4都有一个唯一产品序列号,该序列号用于网关4接入设备服务器使用身份凭证。

[0126] 设备服务器3能够正常使用的前提条件是,管理员在对应账号应用端添加网关4,输入网关4的产品序列号和名称并提交后,应用端1向设备服务器3发送添加网关4的相关参数请求,设备服务器3对请求方身份权限进行认证识别、产品序列号唯一性判别,经设备服务器3一系列检验正确后,响应应用端1的请求,返回成功状态表示该请求正确执行。

[0127] 接下来设备服务器3继续执行网关4添加的任务,为新添加的控网关4产生LORA通信唯一身份识别MAC,将控制中心的产品序列号和身份识别MAC在MySQL数据库中插入新的数据。

[0128] 每一个网关4通电后,与设备服务器3建立tcp连接时,首要的任务组织数据报文、加密、校验数据、封装发起注册请求,设备服务器3收到该控制中心数据包后,对该数据包进行解析、解密、检验并执行相关处理程序。

[0129] 相关处理程序任务包括查找该控制中心LORA通信唯一身份识别的MAC、建立控制中心Socket管理结构体初始化、在Redis中存储该控制中心与设备服务器ip对应关系、推送网关4在线状态到应用端1和第三方用户、获取当前时间,组织数据报文、加密、校验数据、封装将相关注册信息下发到该网关4,将解密后数据用于网关4的初始化,初始化成功后,网关4正面上方指示灯为呼吸状态,可以正常使用。

[0130] 相反,该网关4在注册的时候,设备服务器3在数据库中查找不到对应的产品序列号,设备服务器3既不响应网关4的请求也不会推送在线状态到应用端1和第三方用户。网关4一直处于未注册状态,导致无法正常使用网关4。

[0131] 网关4是设备服务器3与智能门锁通信转换器,由有线连接转换成无线的方式,网关4与设备服务器3之间的连接通过tcp建立通信链路,而网关4与智能门锁5之间的通信是通过LORA无线扩频技术,进行数据交换的。目前技术无线通信无法避免信号碰撞的问题,为尽可能避免这一缺陷,网关4在设计时搭载了两个LORA模块,采用双频率双通道收发机制,尽可能减少信号碰撞,提高数据传送的可靠性和成功率。

[0132] 以上所述仅为本发明的优选实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

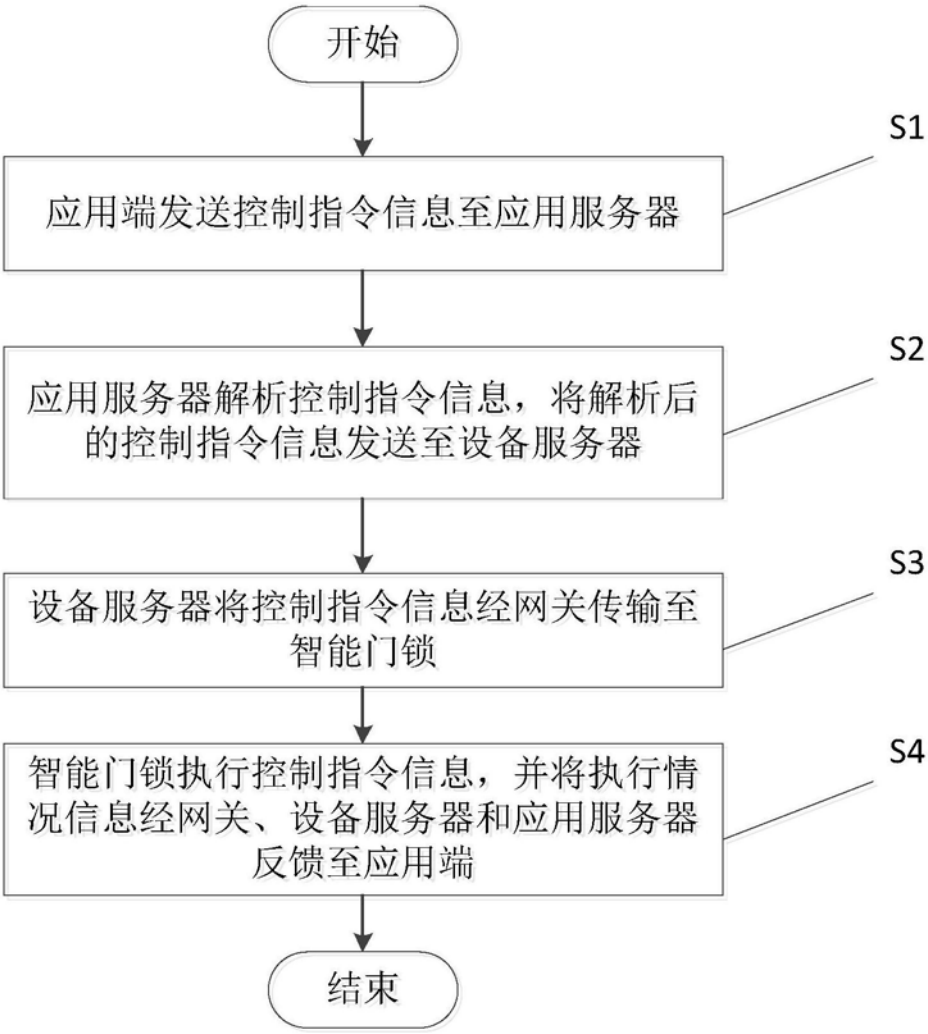

开始
S1
应用端发送控制指令信息至应用服务器
S2
应用服务器解析控制指令信息，将解析后的控制指令信息发送至设备服务器
S3
设备服务器将控制指令信息经网关传输至智能门锁
S4
智能门锁执行控制指令信息，并将执行情况信息经网关、设备服务器和应用服务器反馈至应用端
结束

图1

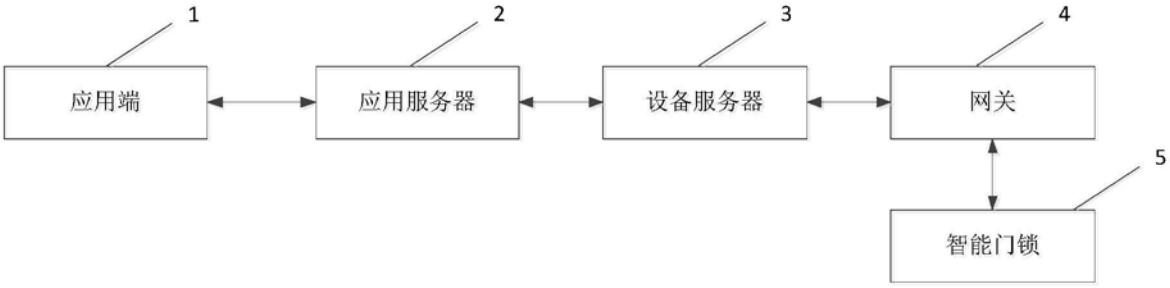

1
应用端
2
应用服务器
3
设备服务器
4
网关
5
智能门锁

图2

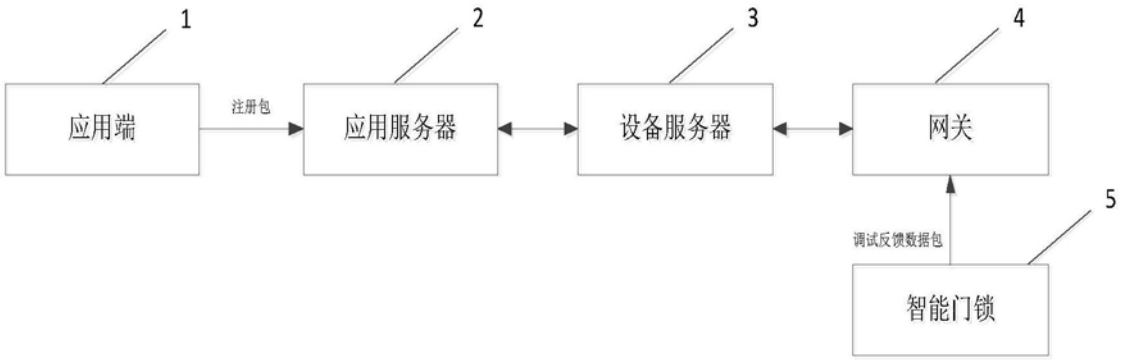


图3