



(12)发明专利

(10)授权公告号 CN 105809777 B

(45)授权公告日 2019.06.18

(21)申请号 201410834401.7

(22)申请日 2014.12.29

(65)同一申请的已公布的文献号

申请公布号 CN 105809777 A

(43)申请公布日 2016.07.27

(73)专利权人 腾讯科技(深圳)有限公司

地址 518000 广东省深圳市福田区振兴路
赛格科技园2栋东403室

(72)发明人 何畅

(74)专利代理机构 深圳翼盛智成知识产权事务
所(普通合伙) 44300

代理人 黄威

(51)Int.Cl.

G07C 9/00(2006.01)

(56)对比文件

CN 103679883 A,2014.03.26,

CN 103679883 A,2014.03.26,

CN 102542649 A,2012.07.04,

CN 103546294 A,2014.01.29,

CN 103150798 A,2013.06.12,

US 2003014642 A1,2003.01.16,

审查员 梅潇

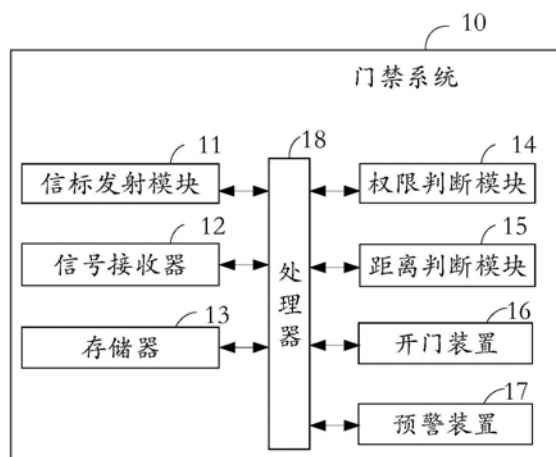
权利要求书3页 说明书10页 附图6页

(54)发明名称

门禁系统、客户端、及门禁的身份验证方法

(57)摘要

本发明公开一种门禁系统、客户端、及门禁的身份验证方法,包括:信号接收器用于接收近距离通信信号,包括信号内容与信号强度;存储器用于存储门禁权限列表,至少包括客户端识别信息、门禁权限;权限判断模块用于判断接收的近距离通信信号的内容与所述门禁权限列表是否匹配;距离判断模块用于根据所述匹配的近距离通信信号的信号强度来判断客户端与对应门禁的距离,并当距离小于第一距离阈值时,发送开启信号至开门装置;开门装置根据开启信号开启对应的门禁。本发明通过信号内容与信号强度的判断,实现了自动门禁的基本功能,同时还支持授权给用户更换手机时自主更新、以及多人考勤的记录,更安全、便携。



1. 一种门禁系统,其特征在于,包括:

信号接收器,用于接收来自客户端的近距离通信信号,包括信号内容与信号强度;

存储器,用于存储门禁权限列表,所述门禁权限列表至少包括客户端识别信息、以及门禁权限;

权限判断模块,用于判断所述接收的近距离通信信号的内容与所述门禁权限列表中的所述客户端识别信息与门禁权限是否皆匹配;

距离判断模块,用于根据所述所述客户端识别信息与门禁权限皆匹配的近距离通信信号的信号强度来判断所述客户端与对应门禁的距离,并当所述距离小于预置的第一距离阈值时,发送开启信号至开门装置;以及

开门装置,根据开启信号开启对应的门禁;

预警装置,连接于所述信号接收器、所述权限判断模块和所述距离判断模块;

所述预警装置,用于当与所述门禁权限列表不匹配的近距离通信信号靠近门禁时,进行预警,其中,所述不匹配包括:客户端识别信息不匹配和/或门禁权限不匹配;

所述距离判断模块还用于:

根据客户端识别信息不匹配的近距离通信信号的信号强度来判断其与对应门禁的距离,并当所述客户端识别信息不匹配的近距离通信信号与对应门禁的距离小于预置的第二距离阈值时,发送所述预警信号至所述预警装置;以及

根据门禁权限不匹配的近距离通信信号的信号强度来判断其与对应门禁的距离,并当所述门禁权限不匹配的近距离通信信号与对应门禁的距离小于预置的第三距离阈值时,发送所述预警信号至所述预警装置;

其中所述第一距离阈值大于所述第二距离阈值,所述第一距离阈值大于所述第三距离阈值。

2. 如权利要求1所述的门禁系统,其特征在于,还包括信标发射模块,用于发送信标广播,以便触发客户端发送所述近距离通信信号。

3. 如权利要求1所述的门禁系统,其特征在于,所述门禁权限列表中还包括注册账号,与所述客户端识别信息、以及所述门禁权限相对应;

所述权限判断模块,还用于在接收到用户发送的权限修改请求时,根据所述注册账号确认所述用户是否具有修改门禁权限列表中的客户端识别信息的权限。

4. 如权利要求1至3任一项所述的门禁系统,其特征在于,所述存储器还用于获取所述开门装置的开门记录,并根据所述开门记录生成考勤表或出入备案表。

5. 如权利要求1所述的门禁系统,其特征在于,所述预警装置包括如下模块中的一种或多种的组合:

摄像头,用于在预警的同时采集证据;

语音提示模块,安装于监控室,用于提醒监控人员注意辨别;或/和门禁处,用于提醒所述客户端不要误入;或

预警发送模块,用于向所述不匹配的客户端发送预警提示信息。

6. 一种门禁的身份验证方法,其特征在于,包括:

接收来自客户端的近距离通信信号,所述近距离通信信号包括信号内容与信号强度;

判断接收的近距离通信信号的信号内容与预置的门禁权限列表是否匹配,所述门禁权

限列表至少包括客户端识别信息、以及门禁权限；

若所述近距离通信信号的信号内容与所述预置的门禁权限列表匹配，则根据匹配的近距离通信信号的信号强度来判断所述近距离通信信号与对应门禁之间的距离；以及

当所述近距离通信信号与对应门禁的距离小于预置第一距离阈值时，开启对应的门禁；

当有不匹配的近距离通信信号靠近门禁时，通过预警装置进行预警；其中所述不匹配包括：客户端识别信息不匹配和/或门禁权限不匹配；

当有客户端识别信息不匹配的近距离通信信号靠近门禁时的判断步骤还包括：

根据客户端识别信息不匹配的近距离通信信号的信号强度，来判断所述近距离通信信号与对应门禁的距离；

当所述距离小于预置的第二距离阈值时，发送预警信号至所述预警装置；

根据门禁权限不匹配的近距离通信信号的信号强度，来判断所述门禁权限不匹配的近距离通信信号与对应门禁的距离；

并当所述距离小于预置的第三距离阈值时，发送预警信号至所述预警装置；

其中所述第一距离阈值大于所述第二距离阈值，所述第一距离阈值大于所述第三距离阈值。

7. 如权利要求6所述的身份验证方法，其特征在于，在接收来自客户端的近距离通信信号步骤之前，还包括：

获取各客户端的注册账号和客户端识别信息；

保存所述客户端的注册账号和客户端识别信息至所述门禁权限列表；以及

为所述注册账号赋予门禁权限，其中所述门禁权限是指开启的门禁系统中指定的部分或全部门禁的权限。

8. 如权利要求6所述的身份验证方法，其特征在于，还包括：

发送信标广播，以便触发所述客户端发送所述近距离通信信号。

9. 如权利要求6所述的身份验证方法，其特征在于，还包括：

获取各门禁的开门记录；以及

根据所述开门记录，生成考勤表或出入备案表。

10. 如权利要求6所述的身份验证方法，其特征在于，进行预警时的步骤还包括如下中的至少一步：

通过摄像头采集预警时对应门禁处的证据；

通过语音提示模块，提醒监控人员注意辨别、或/和提醒发送所述不匹配近距离通信信号的客户端不要误入；或

向所述发送所述不匹配近距离通信信号的客户端发送预警提示信息。

11. 一种客户端，其特征在于，包括：

门禁应用程序，包括登陆界面用于输入注册账号、及存储模块用于存储授权的信标ID以及所述注册账号；

接收模块，用于接收近距离通信信标，并检测所述信标中是否包含授权的信标ID；

发送模块，用于当检测到授权信标ID时，发送近距离通信信号；所述近距离通信信号包括信号内容与信号强度，以使得门禁系统判断所接收到的近距离通信信号的内容与门禁权

限列表中的客户端识别信息与门禁权限是否皆匹配；

根据所述客户端识别信息与门禁权限皆匹配的近距离通信信号的信号强度来判断所述客户端与对应门禁的距离，并当所述距离小于预置的第一距离阈值时，发送开启信号至开门装置，以使得开门装置根据开启信号开启对应的门禁；

根据客户端识别信息不匹配的近距离通信信号的信号强度，来判断所述近距离通信信号与对应门禁的距离；当所述距离小于预置的第二距离阈值时，发送预警信号至所述预警装置；

根据门禁权限不匹配的近距离通信信号的信号强度，来判断所述门禁权限不匹配的近距离通信信号与对应门禁的距离；并当所述距离小于预置的第三距离阈值时，发送预警信号至所述预警装置；

其中所述第一距离阈值大于所述第二距离阈值，所述第一距离阈值大于所述第三距离阈值。

12. 如权利要求11所述的客户端，其特征在于，还包括预警提示模块，用于接收预警提示信息，并以语言、提示框、或震动的方式之一或组合进行预警提示。

门禁系统、客户端、及门禁的身份验证方法

技术领域

[0001] 本发明属于门禁安全领域,尤其涉及一种门禁系统、客户端、及门禁的身份验证方法。

背景技术

[0002] 现在的门禁控制技术,大都采用传统的机械方式管理,人们需要随身携带钥匙,常常因为忘记带钥匙对生活造成诸多不便,而且随着信息技术发展,人们对智能化的追求也越来越高。

[0003] 指纹识别、面部识别等生物识别方式门禁系统虽然满足智能化的需求,然后在冬天干燥会受伤的情况下、以及妆容的浓淡都有可能影响到门禁系统识别的准确性,更为重要的是,生物识别方式很难在人员密集型企业当中推广,会导致上下班时间内大量员工等待在门禁处,即现有的门禁方案不仅识别率不高,而且处理效率较低。

发明内容

[0004] 有鉴于此,本发明的目的在于提供一种门禁系统、客户端、及门禁的身份验证方法,可以解决现有技术中识别率不高,且处理效率较低等问题。

[0005] 为解决上述技术问题,本发明实施例提供了一种门禁系统,包括:

[0006] 信号接收器,用于接收来自客户端的近距离通信信号,包括信号内容与信号强度;

[0007] 存储器,用于存储门禁权限列表,所述门禁权限列表至少包括客户端识别信息、以及门禁权限;

[0008] 权限判断模块,用于判断所述接收的近距离通信信号的内容与所述门禁权限列表中的所述客户端识别信息与门禁权限是否皆匹配;

[0009] 距离判断模块,用于根据所述所述客户端识别信息与门禁权限皆匹配的近距离通信信号的信号强度来判断所述客户端与对应门禁的距离,并当所述距离小于预置的第一距离阈值时,发送开启信号至开门装置;以及

[0010] 开门装置,根据开启信号开启对应的门禁。

[0011] 为解决上述技术问题,本发明实施例还提供一种门禁的身份验证方法,包括:

[0012] 接收来自客户端的近距离通信信号,所述近距离通信信号包括信号内容与信号强度;

[0013] 判断接收的近距离通信信号的信号内容与预置的门禁权限列表是否匹配,所述门禁权限列表至少包括客户端识别信息、以及门禁权限;

[0014] 若所述近距离通信信号的信号内容与所述预置的门禁权限列表匹配,则根据匹配的近距离通信信号的信号强度来判断所述近距离通信信号与对应门禁之间的距离;以及

[0015] 当所述近距离通信信号与对应门禁的距离小于预置第一距离阈值时,开启对应的门禁。

[0016] 为解决上述技术问题,本发明实施例又提供一种客户端,包括:

[0017] 门禁应用程序,包括登陆界面用于输入注册账号、及存储模块用于存储授权的信标ID以及所述注册账号;

[0018] 接收模块,用于接收近距离通信信标,并检测所述信标中是否包含授权的信标ID;

[0019] 发送模块,用于当检测到授权信标ID时,发送近距离通信信号。

[0020] 相对于现有技术,本发明中的门禁系统、客户端、及门禁的身份验证方法,通过对近距离通信信号的信号内容与信号的判断,实现了自动门禁的基本功能,不仅解决了现有技术中识别率不高,且处理效率较低等问题,还可以支持授权给用户更换手机时自主更新,更安全、便携。

附图说明

[0021] 图1是本发明实施例提供的门禁系统、客户端、及门禁的身份验证方法的应用环境示意图;

[0022] 图2是本发明实施例一提供的门禁系统的模块示意图;

[0023] 图3是本发明实施例二提供的门禁的身份验证方法的工作流程示意图;

[0024] 图4是本发明实施例三提供的门禁的身份验证方法的工作流程示意图;

[0025] 图5是本发明实施例四提供的客户端的模块示意图;

[0026] 图6是本发明实施例五提供的蓝牙门禁系统、蓝牙客户端、及蓝牙门禁的身份验证方法的时序示意图。

具体实施方式

[0027] 请参照附图中的图式,其中相同的组件符号代表相同的组件,本发明的原理是以实施在一适当的运算环境中来举例说明。以下的说明是基于所示例的本发明的具体实施例,其不应被视为限制本发明未在此详述的其它具体实施例。

[0028] 本发明原理以上述文字来说明,其并不代表为一种限制,本领域测试人员将可了解到以下所述的多种步骤及操作亦可实施在硬件当中。本发明的原理使用许多其它泛用性或特定目的运算、通信环境或组态来进行操作。

[0029] 请参阅图1,为本发明中提供的门禁系统及其实现方法的应用环境示意图。所述应用环境,包括门禁系统10、门禁服务器20、客户端30、用户40、通信网络50。

[0030] 其中,门禁系统10用于发送信标广播以唤醒客户端30,并接收客户端30发送的近距离通信信号,判断信号内容中是否包含授权信息。若包含授权信息,则根据信号强度来判断发送所述近距离通信信号的客户端与对应门禁的距离,并当其与对应门禁的距离小于第一距离阈值时,开启门禁。

[0031] 门禁服务器20,用于将所述授权信息存储为门禁权限列表,所述门禁权限列表中包括:注册账号、客户端识别信息、以及所述客户端对应的门禁权限。可以理解的是:所述门禁服务器20可以是云存储平台,也可以整合在门禁系统10中的存储模块。

[0032] 客户端30,包括授权客户端30a、和未授权客户端30b。可以理解的是:所述授权客户端30a与未授权客户端30b的区别在于其识别信息是否能与所述门禁权限列表中的客户端识别信息相匹配。

[0033] 用户40,亦包括授权用户40a、和未授权用户40b。可以理解的是:所述授权用户40a

与未授权用户40b的区别在于其是否拥有所述门禁权限列表中的注册账号。

[0034] 通信网络50,包括无线网络及有线网络。其中无线网络包括无线广域网、无线局域网、无线城域网、以及无线个人网中的一种或多种的组合。

[0035] 请参照以下实施例,其中,实施例一侧重于门禁系统,实施例二与实施例三分别侧重于门禁的身份验证方法的基本功能及扩展功能,实施例四侧重客户端;而实施例五以蓝牙技术为例概述门禁系统、客户端、及用户操作指令之间的工作时序。可以理解的是:虽然各实施例的侧重不同,但其设计思想是一致的。且,在某个实施例中沒有详述的部分,可以参见说明书全文的详细描述,不再赘述。

[0036] 实施例一

[0037] 请参阅图2,所示为本发明实施方式中门禁系统的模块示意图。所述门禁系统10,包括:信标发射模块11、信号接收器12、存储器13、权限判断模块14、距离判断模块15、开门装置16、预警装置17以及处理器18。

[0038] 信标发射模块11,用于发送信标广播,以唤醒客户端发送近距离通信信号。

[0039] 可以理解的是:信标广播中包含一信标ID,用于唤醒与所述信标ID相匹配的客户端。通常信标发射模块的广播范围在50米左右,会根据地理环境有所偏差,但足以支持本发明中的门禁功能。

[0040] 信号接收器12,用于接收客户端的近距离通信信号,包括信号内容与信号强度。其中,信号内容中包括客户端的识别信息,通常是独一无二的。

[0041] 可以理解的是:所述信号接收器12可以同时接受多个近距离通信信号,即可以支持多个客户端同时进出。

[0042] 存储器13,用于存储门禁权限列表,所述门禁权限列表包括注册账号、客户端识别信息、以及门禁权限。其中,客户端识别信息与门禁权限是必须的,加入注册账号后,可支持通过输入正确的注册账号后,对客户端识别信息进行修改。即,当用户更换手机后,可自行修改门禁权限后进入门禁系统10。

[0043] 此外,存储器13,既可以作为门禁系统10的一部分,也可以通过通信网络存储于云服务器上。

[0044] 表1 权限列表

[0045]

工号	姓名	手机号码	门禁权限	时间	时段
001	张一	137 1111 1111	公司门 01; 4 楼门 41; 4 楼三办公室 413	2011.01.11 至 2014.10.02	8:30 至 17:20
002	王二	158 1111 1112	公司门 01; 2 楼一办公室 211	2001.05.12 至今	全天

[0046] 以表1为例,其中注册账号由工号+姓名构成,客户端识别信息为手机号码,门禁权限由公司门、楼层门和专属办公室构成。

[0047] 所述门禁权限列表中,行的添加与列的修改权限一般由管理员统一管理。如下表1为权限列表的示例表,可以理解的是:不同行业中门禁的权限列表设置可能不同。

[0048] 其中,所述行的添加,通常是增加新员工时,为新员工的客户端注册,并赋予门禁权限。通常由指定的管理员完成。其中,所述员工离职时,通常不会删掉原纪录,而是在该员工对应列中存储其离职时间,以此撤销其进入门禁的权限。好处是可以作为记录保留,以支持人资部门的其他报表。当然,也可以直接删除。

[0049] 所述列的修改权限,包括两种:第一是员工的权限改变,如升职后可拥有更多权限或时段,支持由管理员进行修改;第二是员工因为带错手机、或变更手机号码时,仅修改手机号码单列,可以由管理员赋权给员工自行修改。

[0050] 其中,列中也可以增加部门,并对该部门门禁时段进行统一管理,比如销售部的全体员工在20:00之后禁入办公室。

[0051] 权限判断模块14,用于判断所述接收的近距离通信信号的信号内容与所述存储器13中权限列表中的客户端识别信息及门禁权限是否匹配,如果所述接收信号内容与权限列表中的客户端识别信息及门禁权限皆匹配,则通知所述距离判断模块15继续判断。

[0052] 可以理解的是:当客户端(其发送的近距离通信信号)靠近门禁系统10附近时,门禁系统10首先应判断客户端是否具有门禁权限,如果有门禁权限,则继续判断客户端与门禁系统10对应门禁的距离。一般设置在二者距离10米左右时,对门禁权限进行判断;在5米左右时,对距离进行判断,并确定是否需要开启对应门禁。当然,上述数字是可以调整的,仅为一般情形下较佳的示例,不作为对技术上的限定。

[0053] 距离判断模块15,用于根据匹配的近距离通信信号的信号强度来判断所述近距离通信信号与对应门禁的距离,并当上述距离小于第一距离阈值时,发送开启信号至开门装置16。

[0054] 可以理解的是:通常距离阈值为2米,即近距离通信信号与门禁系统中某一门禁的举例2米之内时,对应的门禁会自动开启,无需刷卡。

[0055] 开门装置16,根据开启信号开启对应的门禁。

[0056] 可以理解的是:如表1所示,用户可能会拥有办公楼内诸多门禁的权限,当其走到某一位置时,该位置的门禁会开启。

[0057] 以上为实现门禁管理的基本功能。此外,存储模块13还可以获取开门装置16的开门记录,并将所述开门记录生成为考勤表或出入备案表,通常包括:员工的工号、姓名、门禁号、进出时间,如表2所示。

[0058] 表2 出入备案表

[0059]

工号	姓名	手机号码	门禁权限	进出时间
003	李三	138 1111 1113	公司门 01	2014.11.11 08:02:29
			4 楼门 41	2014.11.11 08:04:32
			4 楼二办公室 412	2014.11.11 08:05:57
004	赵四	158 1111 1114	公司门 01	2014.11.11 08:02:29
			公司门 01	2011.01.11 20:05:39

[0060] 此外,所示门禁系统10还可以包括预警装置17,连接于所述信号接收器12、权限判断模块14、距离判断模块15。预警装置17用于当出现所述不匹配的近距离通信信号靠近门禁时进行预警。

[0061] 可以理解的是:所述预警的情形包括如下情形:

[0062] 1. 客户端识别信息不匹配:门禁系统10的信号接收器12接收到近距离通信信号,权限判断模块14判断该近距离通信信号的信号内容有无匹配的注册账号,距离判断模块14根据账号不匹配的近距离通信信号的信号强度来判断其与门禁系统的距离,并当上述距离小于第二距离阈值时,向预警装置17发送预警信号。通常预警阈值为1米或由管理员自行设定。

[0063] 2. 门禁权限不匹配:所述门禁系统10的信号接收器12接收到近距离通信信号,权限判断模块14判断该近距离通信信号的信号内容有无匹配的门禁权限,若无匹配的门禁权限后距离判断模块15判断根据门禁权限不匹配的近距离通信信号的信号强度来判断其与门禁的距离,并当上述距离小于第三距离阈值时,发送预警信号至所示预警装置17。通常预警阈值为0.2米左右。

[0064] 预警装置17,包括摄像头、语音提示模块、或预警发送模块中的一种或多种的组合。其中,摄像头,用于在预警的同时采集对应门禁处的证据;语音提示模块,安装于监控室用于提醒监控人员注意辨别、或/和门禁处用于提醒客户端不要误入;预警发送模块,用于向所述不匹配的客户端发送预警提示信息。

[0065] 本发明的门禁系统10,具有如下优点:

[0066] 1、通过近距离通信信号的信号内容和信号强度的判断,不仅实现了自动门禁的基本功能,还可以根据设定距离自动开启门禁;

[0067] 2、可以生成多人同时通过时的考勤,无需在门禁处排队等待;

[0068] 3、当不匹配的客户端靠近门禁系统时,提供多方位的预警,既可以警示误入者,又可以提醒监控室注意、以及及时保留证据。

[0069] 4、支持将客户端识别信息的修改权限授权给拥有注册账号的用户,使用户/员工在更换手机后,仍可便捷的进入,更安全、便携。

[0070] 实施例二

[0071] 请参阅图3,所示为本发明实施方式中,门禁的身份验证方法的流程示意图。简而言之,按功能划分包括两个部分:注册、门禁。

[0072] 注册部分,包括:

[0073] 在步骤S301中,将注册账号、客户端识别信息存储于门禁权限列表中,并为所述注册账号赋予门禁权限。

[0074] 可以理解的是:所述注册账号,用于确认是否具有修改门禁权限列表中客户端识别信息的权限,通常为员工工号+员工姓名、员工姓名+密码、或员工工号+密码中的一种或其他既包含员工信息又不是轻易试探即可得知的组合信息。

[0075] 所述门禁权限列表中,行的添加与列的修改权限由管理员进行管理。其中,所述行的添加,通常是增加新员工时,为新员工的客户端注册,并赋予门禁权限。通常由指定的管理员完成。所述列的修改权限,包括两种:第一是员工的权限改变,如升职后可拥有更多权限或时段,支持由管理员进行修改;第二是员工因为带错手机、或变更手机号码时,仅修改

客户端识别信息列,可以由管理员赋权给员工自行修改。

[0076] 所述门禁权限,是指用户可以进入对应门禁号的权限。比如员工A拥有进入公司门01、4楼门41、4楼一办公室411、4楼二办公室412号门禁的权限。

[0077] 门禁部分,包括:

[0078] 在步骤S302中,发送信标广播,以便触发所述客户端发送所述近距离通信信号。

[0079] 可以理解的是:信标广播中包含一信标ID,用于唤醒与所述信标ID相匹配的客户端。以蓝牙为例,通常蓝牙信标广播的广播范围在50米左右,会根据地理环境有所偏差,但足以支持本发明中的门禁的作用。

[0080] 在步骤S303中,接收来自于客户端的近距离通信信号,所述近距离通信信号包括信号内容和信号强度。

[0081] 可以理解的是:在本步骤中通过信号接收器可以同时接受多个近距离通信信号,即可支持多个客户端同时进出。

[0082] 在步骤S304中,判断接收的近距离通信信号的信号内容与所述权限列表中的客户端识别信息及门禁权限是否皆匹配?其中,若二者皆匹配,则执行步骤S305;若其一不匹配,则忽略所述近距离通信信号。

[0083] 可以理解的是:当客户端靠近门禁系统时,门禁系统首先应判断客户端是否具有门禁权限,如果有门禁权限,则继续判断客户端与对应门禁的距离。

[0084] 在步骤S305中,通过信号强度来判断近距离通信信号与对应门禁的距离,并当所述近距离通信信号与对应门禁的距离小于预置第一距离阈值时,发送开启信号至对应开门装置。

[0085] 可以理解的是:通常第一距离阈值为2米,即发送所述近距离通信信号的客户端距离门禁系统2米之内时,对应的门禁会自动开启,无需刷卡。

[0086] 在步骤S306中,开门装置根据开启信号开启对应的门禁。

[0087] 可以理解的是:客户端可能会拥有办公楼内诸多门禁的权限,当其走到某一位置时,该位置的门禁会开启。以上为实现门禁管理的基本功能。

[0088] 本发明的门禁的身份验证方法,具有如下优点:

[0089] 1、通过对近距离信号的信号内容和信号强度的判断,不仅实现了自动门禁的基本功能,还可以根据设定距离自动开启门禁;

[0090] 2、可以支持多人同时通过门禁系统时进行备案,而不用在门禁处排队等待;

[0091] 3、支持将客户端识别信息的修改权限授权给拥有注册账号的用户,使用户/员工在更换手机后,仍可便捷的进入,更安全、便携。

[0092] 实施例三

[0093] 请参阅图4,所示为本发明实施方式中,门禁系统的工作流程示意图。简而言之,按功能划分包括四个部分:注册、门禁、考勤、预警。

[0094] 注册部分,包括:

[0095] 在步骤S401中,将注册账号、客户端识别信息存储于门禁权限列表中,并为所述注册账号赋予门禁权限。

[0096] 可以理解的是:所述注册账号,用于确认是否具有修改门禁权限列表中客户端识别信息的权限,通常为员工工号+员工姓名、员工姓名+密码、或员工工号+密码中的一种或

其他既包含员工信息又不是轻易试探即可得知的组合信息。

[0097] 所述门禁权限列表中,行的添加与列的修改权限由管理员进行管理。其中,所述行的添加,通常是增加新员工时,为新员工的客户端注册,并赋予门禁权限。通常由指定的管理员完成。所述列的修改权限,包括两种:第一是员工的权限改变,如升职后可拥有更多权限或时段,支持由管理员进行修改;第二是员工因为带错手机、或变更手机号码时,仅修改客户端识别信息一列,可以由管理员赋权给员工自行修改。

[0098] 所述门禁权限,是指用户可以进入对应门禁号的权限。比如员工A拥有进入公司门01、4楼门41、4楼一办公室411、4楼二办公室412号门禁的权限。

[0099] 门禁部分,包括:

[0100] 在步骤S402中,发送信标广播,,以便触发所述客户端发送所述近距离通信信号。

[0101] 以蓝牙为例,通常蓝牙信标广播的广播范围在50米左右,会根据地理环境有所偏差,但足以支持本发明中的门禁的作用。

[0102] 在步骤S403中,接收来自于客户端的近距离通信信号,所述近距离通信信号包括信号内容和信号强度。

[0103] 可以理解的是:在本步骤中通过信号接收器可以同时接受多个近距离通信信号,以支持多个客户端同时进出。

[0104] 在步骤S404中,判断接收的近距离通信信号的信号内容与所述客户端识别信息是否匹配?其中,若近距离通信信号的信号内容与所述客户端识别信息匹配,则执行步骤S405;若不匹配,则忽略或执行步骤S410。

[0105] 可以理解的是:当发送近距离通信信号的客户端靠近门禁系统附近时,门禁系统首先应判断上述客户端是否具有门禁权限,如果有门禁权限,则继续判断上述客户端与门禁的距离。

[0106] 在步骤S405中,继续判断接收的近距离通信信号的信号内容与所述门禁权限是否匹配?其中,若所述信号内容与所述门禁权限匹配,则执行步骤S406;若不匹配,则忽略或执行步骤S411。

[0107] 在步骤S406中,通过对匹配的近距离通信信号的信号强度,来判断近距离通信信号与对应门禁的距离是否小于预置第一距离阈值。其中,若小于预置第一距离阈值则执行步骤S407,若大于等于预置第一距离阈值则执行步骤S413进行忽略或继续关注。

[0108] 可以理解的是:通常第一距离阈值为2米,即发送近距离通信信号的客户端距离门禁系统2米之内时,对应的门禁会自动开启,无需刷卡。

[0109] 在步骤S407中,当所述近距离通信信号与对应门禁的距离小于第一距离阈值时,发送开启信号至对应的开门装置。

[0110] 在步骤S408中,开门装置根据开启信号开启对应的门禁。

[0111] 可以理解的是:客户端可能会拥有办公楼内诸多门禁的权限,当其走到某一位置时,该位置的门禁会开启。以上为实现门禁管理的基本功能。

[0112] 考勤部分:

[0113] 在步骤S409中,获取各门禁处的开门记录,并根据开门记录生成考勤表或出入备案表。

[0114] 可以理解的是:出入备案表通常包括:员工的工号、姓名、门禁号、进出时间。而考

勤表则与出入备案表类似,选取出入备案表中的员工的工号、姓名、门禁号、以及当天的最早和最晚进出时间。

[0115] 预警部分,包括两种情况:

[0116] 第一种预警情形,有未授权用户靠近门禁系统,即客户端识别信息不匹配,具体包括:

[0117] 在步骤S404对客户端识别信息的匹配的判断步骤中,若接收的信号内容与客户端识别信息不匹配,则执行步骤S410;

[0118] 在步骤S410中,根据不匹配的近距离通信信号的信号强度,判断近距离通信信号与门禁系统的距离是否小于预置第二距离阈值;其中,当大于等于第二距离阈值时,忽略或继续关注,若小于所述第二距离阈值时,执行步骤S412。

[0119] 在步骤S412中,门禁系统进行预警。

[0120] 第二种预警情形,授权用户靠近未授权门禁,即门禁权限不匹配,具体包括:

[0121] 在步骤S405对门禁权限的判断步骤中,若接收的信号内容与门禁权限不匹配,则执行步骤S411;

[0122] 在步骤S411中,根据不匹配的近距离通信信号的信号强度,判断近距离通信信号与门禁系统的距离是否小于预置第三距离阈值;其中,当大于等于第三距离阈值时,忽略或继续关注;当小于第三距离阈值时,执行步骤S412,进行预警。

[0123] 所述进行预警的方式,包括如下中的至少一步:(1)通过摄像头采集预警时门禁处的现场证据;(2)通过语音提示模块,提醒监控人员注意辨别、或/和提醒发送不匹配的近距离通信信号的客户端不要误入;(3)向所述发送不匹配的近距离通信信号的客户端发送预警提示信息。

[0124] 本发明的门禁的身份验证方法,具有如下优点:

[0125] 1、通过近距离信号的信号内容和信号强度的判断,不仅实现了自动门禁的基本功能,还可以根据设定距离自动开启门禁;

[0126] 2、可以生成多人同时通过时的考勤,不用在门禁处排队,节省了用户的时间,而且不会出现随他人进门忘记打卡的情形;

[0127] 3、当不匹配的客户端靠近门禁系统时,提供多方位的预警,即提醒客户端和监控人员,还可以第一时间保留现场的证据。

[0128] 4、支持将客户端识别信息的修改权限授权给拥有注册账号的用户,使用户/住户/员工在更换手机后,仍可便捷的进入,并以此实现对人识别而非对物识别,更安全、便携。

[0129] 实施例四

[0130] 请参阅图5,所示为客户端的模块示意图。

[0131] 一种客户端,包括:门禁应用程序31、接收模块32、发送模块33、预警提示模块34、以及中央处理器35。

[0132] 门禁应用程序34,包括登陆界面用于输入注册账号、及存储模块用于存储授权的信标发射模块ID以及所述注册账号。

[0133] 可以理解的是:所述门禁应用程序31,在初次与所述门禁系统匹配时,由客户端进行下载。

[0134] 接收模块32,用于接收信标广播,并检测所述信标广播中是否包含授权的信标发

射模块ID。

[0135] 发送模块33,用于当检测到授权信标ID时,发送连接的近距离通信信号。

[0136] 可以理解的是:所述授权的信标发射模块ID可视为唤醒或触发发送模块进行近距离通信信号的发送。在未收到授权信标ID时,发送模块33可处于休眠状态以节省电源。

[0137] 预警提示模块34,用于接收预警信息,并以语音、提示框、或震动的方式之一或组合进行预警提示。

[0138] 本发明的客户端,具有如下优点:

[0139] 1、发送模块平时处于休眠状态,在接收到信标广播后被唤醒或触发,用于节省电能;

[0140] 2、发送的近距离通信信号相互之间干扰较小,支持生成多人同时通过时的考勤记录或出入备案表,不用在门禁处排队;

[0141] 3、当进入不匹配区域时,可接收到多类型的预警提示信息,以防误入。

[0142] 4、支持将客户端识别信息的修改权限授权给拥有注册账号的用户,使用户/住户/员工在更换手机后,仍可便捷的进入,并以此实现对人识别而非对物识别,更安全、便携。

[0143] 实施例五

[0144] 请参阅图6,所示为蓝牙门禁系统、蓝牙客户端、及蓝牙门禁的实现方法的时序示意图。可以理解的是:在本实施例中近距离通信技术采用的是蓝牙技术进行展示,所述蓝牙技术具有低功耗、抗干扰能力强等优点。

[0145] 本实施例的蓝牙门禁系统以小区中的门禁为例进行时序的展示,其中主体包括,管理员、用户、蓝牙客户端、蓝牙门禁系统、以及服务器。举例而言,管理员为物业人员,用户为住户,蓝牙客户端为手机等可收发蓝牙信号的设备,服务器既可以作为云服务平台,也可以是蓝牙门禁系统的存储模块,本实施例以云服务平台为例。包括如下步骤:

[0146] 在步骤A中,将蓝牙客户端的注册账号、蓝牙识别信息统一存储于服务器端的门禁权限列表中,并为所述注册账号赋予门禁权限;

[0147] 在步骤B中,由已注册账号的用户在蓝牙客户端中下载蓝牙门禁应用程序。可以理解的是,当用户由于个人原因更换手机时,可以在新的手机上重新下载应用程序,并通过进入注册账号,修改其蓝牙识别信息,已到达更换手机仍可使用门禁的作用。

[0148] 在步骤C中,由蓝牙门禁系统发送蓝牙广播,以唤醒蓝牙客户端;

[0149] 在步骤D中,由蓝牙客户端向蓝牙门禁系统发送蓝牙信号,包括蓝牙信号内容和信号强度;

[0150] 在步骤E中,蓝牙门禁系统将所述蓝牙信号中的信号内容与所述门禁权限列表中的蓝牙识别信息及门禁权限进行匹配;

[0151] 在步骤F中,若服务器判断所述蓝牙信号中的信号内容与所述门禁权限列表中的蓝牙识别信息及门禁权限皆匹配成功;

[0152] 在步骤G中,则由蓝牙门禁系统开启对应的门禁;

[0153] 在步骤H中,若所述蓝牙信号中的信号内容与所述门禁权限列表中的蓝牙识别信息及门禁权限之一匹配失败;

[0154] 在步骤I中,则由蓝牙门禁系统进行预警,预警方式包括通过摄像头、语音提示模块、或预警发送模块中的一种或多种的组合。

[0155] 在步骤J中,根据蓝牙门禁的开门记录,生成出入备案表。

[0156] 本发明的蓝牙门禁系统,具有如下优点:

[0157] 1、通过蓝牙信号内容和信号强度的判断,不仅实现了自动门禁的基本功能,还可以根据设定距离自动开启门禁;

[0158] 2、可以生成多人同时通过时的出入备案表,提高门禁系统的安全性、和备案记录的准确性;

[0159] 3、当不匹配的蓝牙客户端靠近蓝牙门禁系统时,提供多方位的预警。

[0160] 4、支持将客户端识别信息的修改权限授权给拥有注册账号的用户,使用户/员工在更换手机后,仍可便捷的进入,更安全、便携。。

[0161] 可以理解的是:本文所使用的词语“优选的”意指用作实例、示例或例证。奉文描述为“优选的”任意方面或设计不必被解释为比其他方面或设计更有利。相反,词语“优选的”的使用旨在以具体方式提出概念。如本申请中所使用的术语“或”旨在意指包含的“或”而非排除的“或”。即,除非另外指定或从上下文中清楚,“X使用A或B”意指自然包括排列的任意一个。即,如果X使用A;X使用B;或X使用A和B二者,则“X使用A或B”在前述任一示例中得到满足。

[0162] 而且,尽管已经相对于一个或多个实现方式示出并描述了本公开,但是本领域技术人员基于对本说明书和附图的阅读和理解将会想到等价变型和修改。本公开包括所有这样的修改和变型,并且仅由所附权利要求的范围限制。特别地关于由上述模块(例如元件、资源等)执行的各种功能,用于描述这样的模块的术语旨在对应于执行所述模块的指定功能(例如其在功能上是等价的)的任意模块(除非另外指示),即使在结构上与执行本文所示的本公开的示范性实现方式中的功能的公开结构不等同。此外,尽管本公开的特定特征已经相对于若干实现方式中的仅一个被公开,但是这种特征可以与如可以对给定或特定应用而言是期望和有利的其他实现方式的一个或多个其他特征组合。而且,就术语“包括”、“具有”、“含有”或其变形被用在具体实施方式或权利要求中而言,这样的术语旨在以与术语“包含”相似的方式包括。

[0163] 本文提供了实施例的各种操作。在一个实施例中,所述的一个或多个操作可以构成一个或多个计算机可读介质上存储的计算机可读指令,其在被服务器执行时将使得计算设备执行所述操作。描述一些或所有操作的顺序不应当被解释为暗示这些操作必需是顺序相关的。本领域技术人员将理解具有本说明书的益处的可替代的排序。

[0164] 本发明实施例提供的蓝牙门禁系统、蓝牙客户端、及蓝牙门禁的实现方法属于同一构思,其具体实现过程详见说明书全文,此处不再赘述。

[0165] 综上所述,虽然本发明已以优选实施例揭露如上,但上述优选实施例并非用以限制本发明,本领域的普通测试人员,在不脱离本发明的精神和范围内,均可作各种更动与润饰,因此本发明的保护范围以权利要求界定的范围为准。

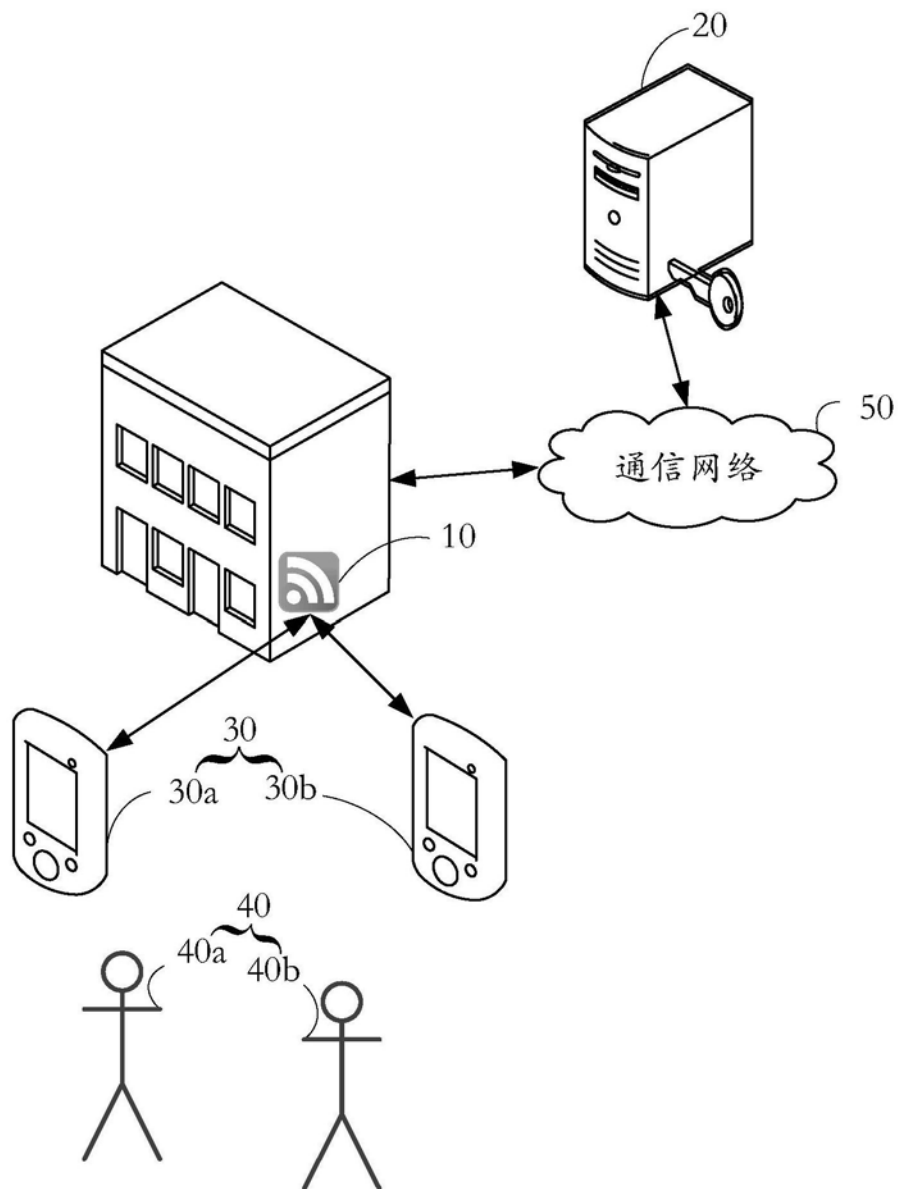


图1

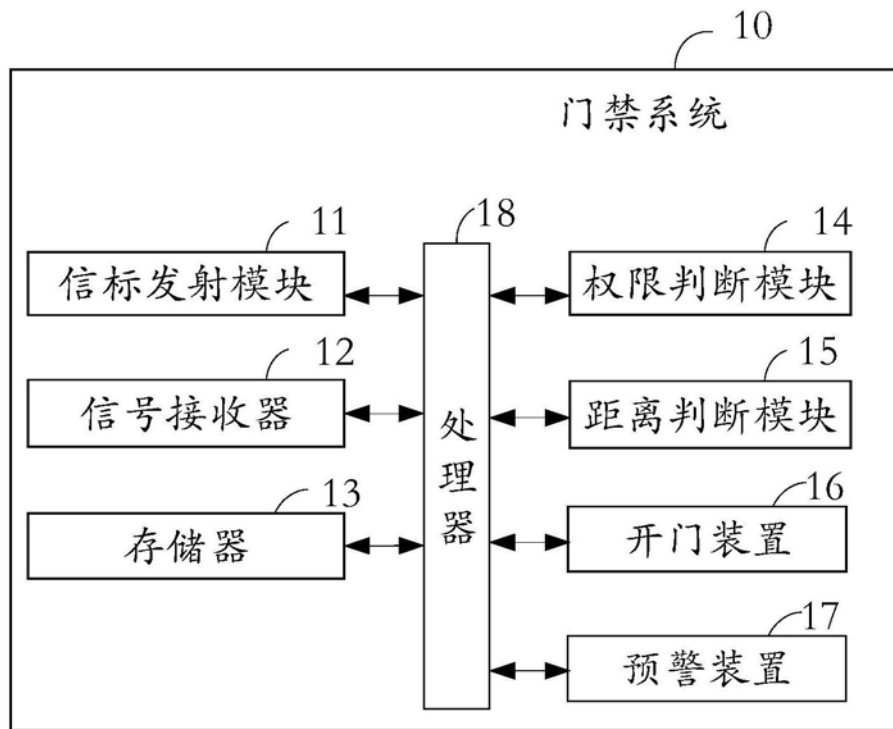


图2

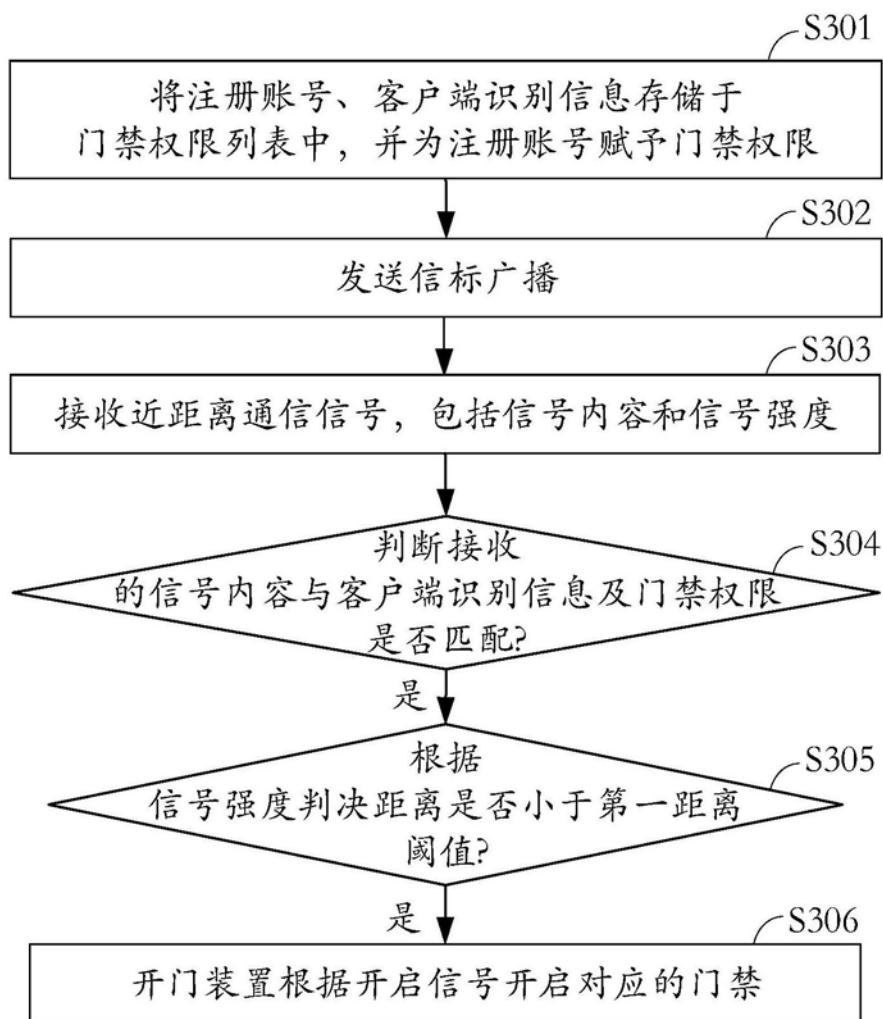


图3

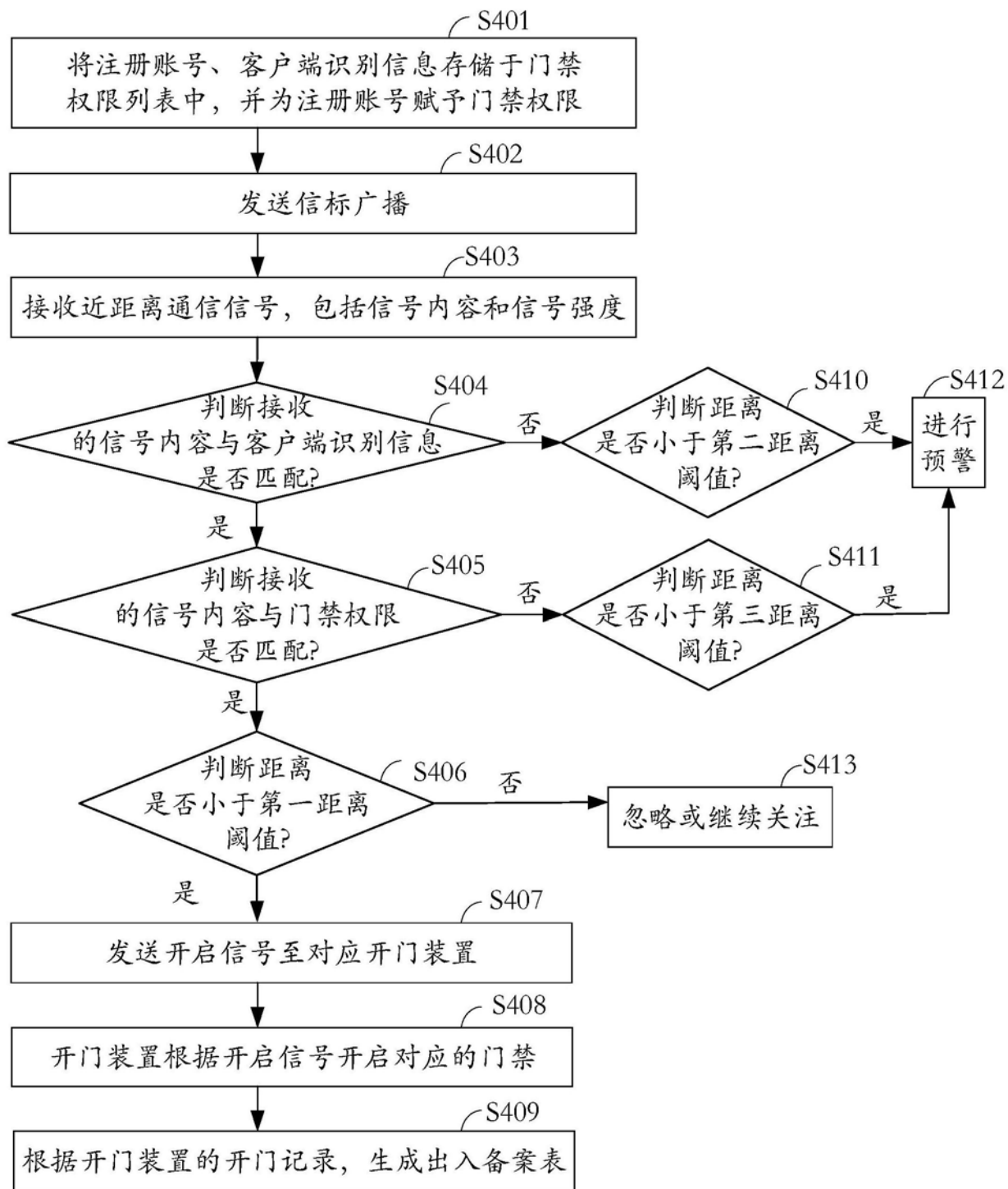


图4

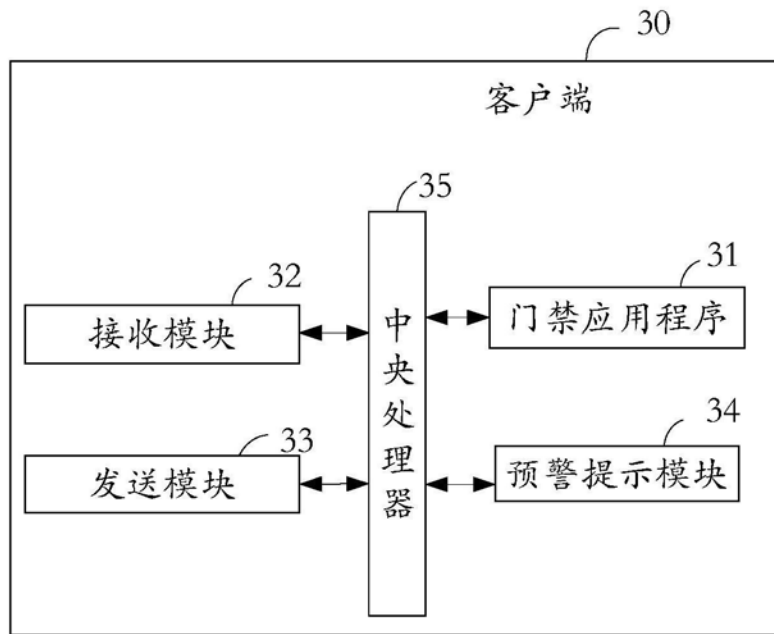


图5

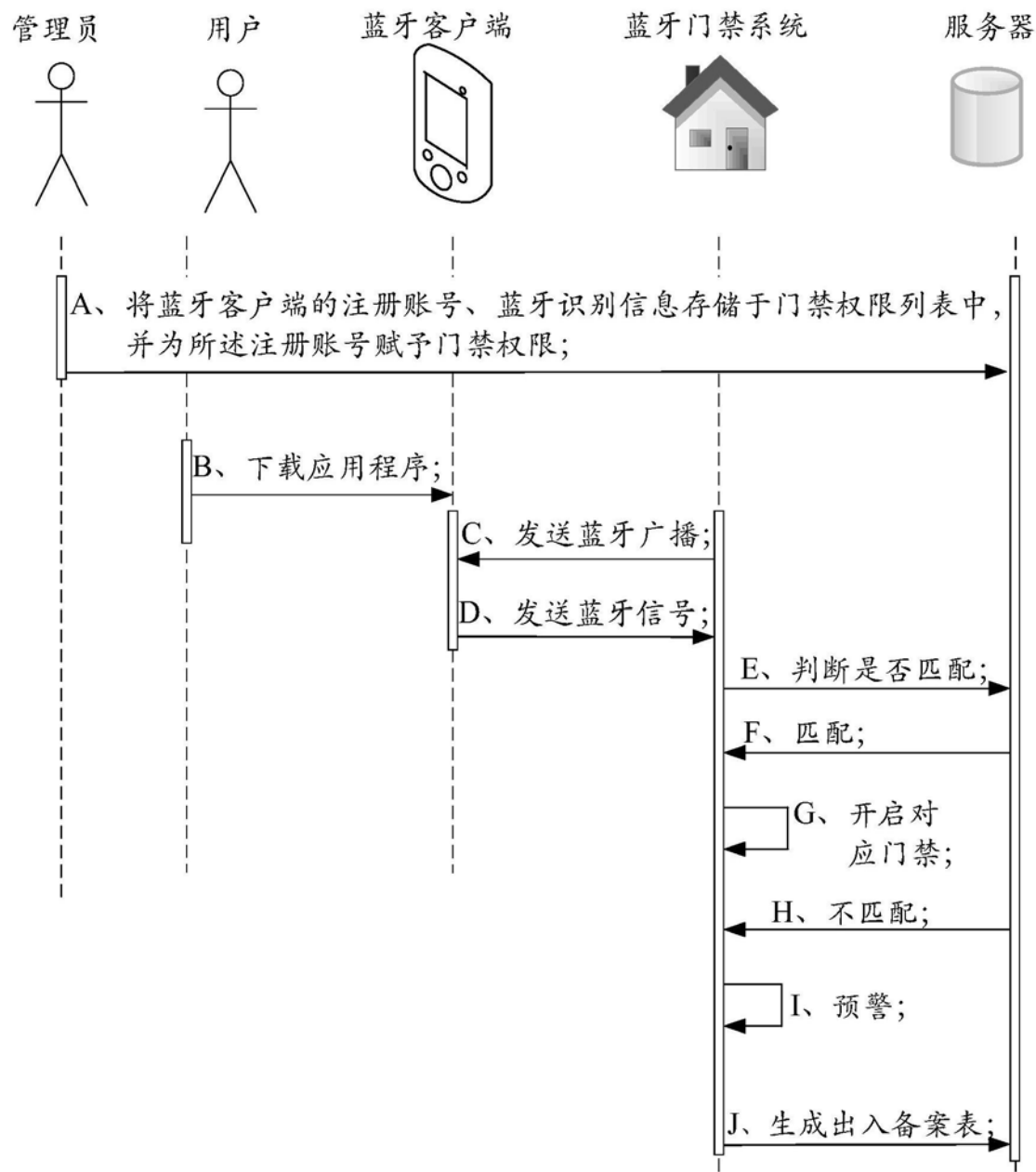


图6