(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 112017341 B
(45)授权公告日 2021.08.17

(21)申请号 202010695846.7

(22)申请日 2020.07.17

(65)同一申请的已公布的文献号
申请公布号 CN 112017341 A

(43)申请公布日 2020.12.01

(73)专利权人 北京大学
地址 100871 北京市海淀区颐和园路5号

(72)发明人 许辰人 徐燮阳

(74)专利代理机构 北京海虹嘉诚知识产权代理有限公司 11129
代理人 何志欣

(51)Int.Cl.
G07C 9/22(2020.01)
G07C 9/27(2020.01)
H04W 4/70(2018.01)
H04W 4/80(2018.01)
H04B 10/116(2013.01)

(56)对比文件
CN 102222378 A,2011.10.19
CN 101151642 A,2008.03.26
CN 1504626 A,2004.06.16
CN 101156177 A,2008.04.02
CN 104601236 A,2015.05.06
EP 0166087 A1,1986.01.02
CN 104408501 B,2017.10.27
CN 103942857 A,2014.07.23
CN 104408501 B,2017.10.27
CN 104408501 A,2015.03.11
Guojun Chen、Purui Wang,Lilei Feng, Yue Wu, Xieyang Xu,Yang Shen.Demo Abstract: Long Range Retroreflective V2X Communication with Polarization-based Differential Reception.《SenSys ″18: Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems November 2018 Pages 381》.2018,
Xieyang Xu、Yang Shen,Junrui Yang, Chenren Xu,Guobin Shen, Guoj.PassiveVLC: Enabling Practical Visible Light Backscatter Communication for Battery-free IoT Applications.《MobiCom ″17: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking October 2017》.2017,

审查员 周红静

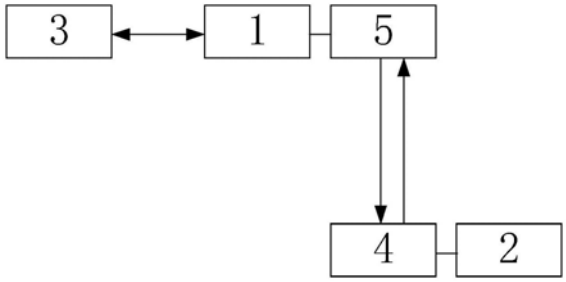
权利要求书2页 说明书13页 附图3页

(54)发明名称

一种基于逆反射可见光通信的物联网门禁系统

(57)摘要

本发明涉及一种基于逆反射可见光通信的物联网门禁系统，至少包括移动端、门禁端，所述移动端或门禁端设置有可配置的逆反射单元，其中，所述移动端和/或门禁端通过所述逆反射单元被动接收光信号且以逆反射的方式将光信号返回而处于被动通信状态，其中，所述光信号能够为所述移动端和/或门禁端提供能量。通过该设置方式，使得需要配置的一端能够无需供电也无需单独建立通信链接就始终处于被动无源工作之中，并且能够实现针对特定对象的可配置性，尤其适用于一方不便于获得供电但又应得到单独配置的权限管理场景。



CN 112017341 B

1.一种基于逆反射可见光通信的物联网门禁系统,至少包括:移动端(1)和门禁端(2),其特征在于,

所述移动端(1)或所述门禁端(2)设置有可配置的逆反射单元(4),其中,

所述移动端(1)或门禁端(2)通过所述逆反射单元(4)被动接收光信号且以逆反射的方式将光信号返回而处于被动通信状态,其中,

所述光信号能够为所述移动端(1)或门禁端(2)提供能量,其中,

所述逆反射单元(4)至少包括调制模块(41)、第一控制器(42)、第一光学传感器(43)以及储能装置(45),其中,

所述逆反射单元(4)配置为:基于脉冲序列通过第一控制器(42)控制第一光学传感器(43)分别与储能装置(45)和调制模块(41)的连接状态,从而实现能量收集状态与信号检测状态的彼此隔离和高频切换。

2.根据权利要求1所述的物联网门禁系统,其特征在于,所述逆反射单元(4)至少包括调制模块(41)、与所述调制模块(41)连接的第一控制器(42)、与所述第一控制器(42)连接的第一光学传感器(43)以及分别与所述第一光学传感器(43)、所述第一控制器(42)和所述调制模块(41)连接的储能装置(45),其中,

所述第一光学传感器(43)用于收集能量和接收带有信息的光信号,并将收集的能量传输至所述储能装置(45)和将光信号传输至所述第一控制器(42),

所述第一控制器(42)配置为基于带有信息的光信号生成反馈信息,并基于反馈信息生成驱动所述调制模块(41)的驱动信号,

所述调制模块(41)的一侧设置有逆反射光信号的逆反射层(44),使得所述调制模块(41)能够基于所述驱动信号以控制所述逆反射层(44)逆反射的光信号的明暗变化的方式将所述反馈信息调制在该逆反射的光信号上。

3.根据权利要求1或2所述的物联网门禁系统,其特征在于,在所述逆反射单元(4)接收光信号的情况下,所述光信号分别进入所述第一光学传感器(43)和调制模块(41),所述第一控制器(42)配置为:监测所述第一光学传感器(43)接收的光信号,并在识别带有信息的光信号的情况下,控制所述第一光学传感器(43)断开与所述储能装置(45)的连接以退出收集能量的状态,并且通过所述第一光学传感器(43)接收所述带有信息的光信号。

4.根据权利要求2所述的物联网门禁系统,其特征在于,所述调制模块(41)至少包括第一偏振器件(411)和第二偏振器件(412),其中,

所述逆反射层(44)与所述第一偏振器件(411)可拆卸地连接,

所述第二偏振器件(412)配置为设置于所述第一偏振器件(411)的出光一侧,并且其偏振方向能够随所述第一控制器(42)生成的驱动信号发生变化从而实现光信号的明暗变化。

5.根据权利要求1所述的物联网门禁系统,其特征在于,所述移动端(1)或所述门禁端(2)还设置有发射光信号和接收光信号的读写单元(5),其中,

所述读写单元(5)配置为主动向所述逆反射单元(4)发送至少包括身份验证信息的光信号,并接收由所述逆反射单元(4)调制反射回的逆反射光信号,从而实现所述移动端(1)与所述门禁端(2)之间的信息交互。

6.根据权利要求5所述的物联网门禁系统,其特征在于,所述读写单元(5)至少包括依次电连接的发光装置(51)、第二控制器(52)以及第二光学传感器(53),其中,

所述第二控制器(52)基于身份验证信息驱动所述发光装置(51),并通过调节光明暗变化的方式将身份验证信息调制于光信号上。

7.根据权利要求1所述的物联网门禁系统,其特征在于,在所述移动端(1)设置有读写单元(5)的情况下,所述逆反射单元(4)设置在所述门禁端(2),其中,

所述移动端(1)配置为与服务器(3)连接以获取相应身份验证信息,并将身份验证信息以光信号的形式主动发送至所述门禁端(2);

所述门禁端(2)配置为:

通过所述逆反射单元(4)接收光信号;

基于预先存储的信息验证所述光信号承载的身份验证信息以生成至少包括本地信息的反馈信息,从而基于所述反馈信息打开或关闭门禁,并将所述反馈信息通过所述逆反射单元(4)调制于反射至所述移动端(1)的逆反射光信号上。

8.根据权利要求1所述的物联网门禁系统,其特征在于,在所述移动端(1)设置有所述逆反射单元(4)的情况下,读写单元(5)设置在所述门禁端(2),其中,

所述门禁端(2)配置为:通过与服务器(3)连接以获取相应身份验证信息,并将身份验证信息以光信号的形式主动发送至所述移动端(1);

所述移动端(1)配置为通过所述逆反射单元(4)接收光信号;

基于预先存储的信息验证所述光信号承载的身份验证信息以生成至少包括本地信息的反馈信息,并将所述反馈信息通过所述逆反射单元(4)调制于反射至所述移动端(1)的所述逆反射光信号上;其中,

在所述门禁端(2)接收到所述逆反射光信号的情况下,所述门禁端(2)配置为:

通过所述读写单元(5)获取所述反馈信息,并发送至所述服务器(3)以使得所述服务器(3)完成身份验证逻辑生成确认信息;

接收所述服务器(3)返回的确认信息以打开或关闭门禁。

9.一种基于逆反射可见光通信的物联网门禁方法,其特征在于,所述方法包括:

移动端(1)或门禁端(2)通过其设置的可配置的逆反射单元(4)被动接收光信号且以逆反射的方式将光信号返回而处于被动通信状态,其中,

所述光信号能够为所述移动端(1)或门禁端(2)提供能量;

所述逆反射单元(4)通过在收集光信号能量的状态和检测光信号的状态之间进行切换的方式实现在收集光信号能量的过程中识别带有信息的光信号。

一种基于逆反射可见光通信的物联网门禁系统

技术领域

[0001] 本发明涉及可见光通信领域的应用，例如将可见光通信应用于物联网门禁系统。

背景技术

[0002] 门禁系统是在智能建筑领域，意为Access Control System，指“门”的禁止权限，是对“门”的戒备防范。这里的“门”指的是能够通行的各种通道，包括人通行的门、车辆通行的门、物品存储的门等。主要实现的出入口门禁的权限管理。随着通信、计算机、互联网技术的飞速发展，现代门禁技术集微机自动识别技术和现代安全管理措施为一体，涉及电子、机械、光学、计算机技术、通信技术、生物技术等诸多新技术，门禁系统是解决重要部门出入口实现安全防范管理的有效措施，适用于各种应用场景，例如银行、宾馆、车场管理、机房、军械库、机要室、办公间、智能小区、工厂等。

[0003] 现有门禁系统主要有密码门禁系统、刷卡门禁系统和生物识别门禁系统等。密码门禁系统由于其本身的安全性弱和便捷性差已经面临淘汰。生物识别门禁系统是根据人体生物特征的不同而识别身份的门禁系统。常见的有指纹门禁系统、虹膜门禁系统、面部识别门禁系统等。生物识别门禁系统的缺点是成本高不易进行广泛部署、对比速度慢以及不适用于人员较多的场合。刷卡门禁系统分为接触式门禁系统和非接触式门禁系统。接触式门禁系统包括接触式集成电路卡(Integrated Circuit Card，IC)、磁条卡、条码卡等。由于接触卡容易磨损，导致使用次数有限，而且容易被复制，安全性低，限制了其使用范围。

[0004] 非接触式门禁系统包括无线射频识别技术(Radio Frequency Identification，RFID)以及感应式IC卡等。由于传感器技术、无线射频识别技术、嵌入式技术的飞速发展，非接触式门禁系统能够与物联网技术相结合从而满足现代门禁技术的实际需求。例如，文献[1]杨柄均.基于物联网的门禁系统研究[D].天津大学.将物联网技术与门禁系统相结合，构建基于物联网技术的新型门禁系统，通过引入物联网技术中的传感器技术，能够对门禁现场的物理状态进行感知，可以在远程测控端了解和处理现场的实时状况，如使用红外感应器、激光扫描器等获取身份信息，或使用摄像头让用户获取直观的监控画面；通过引入物联网中的嵌入式技术，能够增加门禁系统的集成程度和稳定性，减小安装体积，缩减安装成本和供电需求，延长生命周期等。通过引入物联网中的RFID技术，可以有效认证持卡人、持卡车辆等人或物的身份，防止陌生身份的人或物进入。但是基于物联网技术的无线射频信息容易被干扰和破解，从而容易被截获复制，造成信息泄露及财产损失。以上所述内容均构成物联网无线组网技术的本领域公知常识。为避免重复，本发明将其参引于此，使得这些文献构成本发明公开的一部分。

[0005] 以上现有的门禁系统大多存在安全性和系统成本之间难以两全的问题，即由于门禁系统的验证方式是基于传统的无线方式，导致传输方式不可控和保密性差。然而可见光通信技术(Visible Light Communication，VLC)天然具有传输可控性强、安全保密性高的天然优势，能够有效克服现有门禁系统对比效率低和安全性差的问题。

[0006] 例如，文献[2]郭燕青.基于可见光通信的物联网门禁系统设计与实现[D].2016.

南京邮电大学.公开了一种基于可见光通信的物联网门禁系统,将可见光通信技术与无线网门禁技术相结合,实现用户能够以可见光的方式完成门禁系统的个人信息验证,并通过物联网无线组网技术组成CS模式,实现用户门禁权限的在线匹配和门禁监控。该门禁系统包括光秘钥、光门禁以及后台服务器三大部分。光秘钥单元负责对秘钥信息进行加密和发送处理,以可见光为载波发送至光门禁控制单元,光门禁单元接收到加载加密秘钥信息的可见光载波进行光电转换和秘钥解密处理,然后通过光门禁单元的无线信息收发模块将门禁的请求信息和状态信息发送给后台监管单元进行权限的验证和状态记录,后台监管单元反馈门禁使能信息给光门禁控制单元。其中,该文献使用光秘钥单元来替代无线磁卡、RFID、接触式IC卡、电子密码、指纹识别、虹膜识别、人脸识别等等,利用LED发射光的亮度的变化实现信息的调制,并传输至光门禁单元。光秘钥单元采用两种实现方案,一种是基于嵌入芯片的便携式光秘钥,另外一种是与智能手机Micro USB接口连接的光秘钥。基本技术方案都是将信息进行处理,例如编码等,并将信息传递至LED的驱动电路,从而驱动LED灯发出明暗变化的可见光,即将信息加载至可见光上;光门禁单元接收到可见光并解调获取信息。其中,光门禁控制单元对可见光的检测原理如下:

[0007] 光门禁控制单元设置有光学传感器,例如光电二极管(Photodiode,PD),能够对周围环境的光信号进行感应,从而实现光电转换。由于周围其他环境光的强烈干扰,例如照明的荧光灯,使得光秘钥单元发送的可见光和环境光混叠在一起,而且PD中产生的电子噪声,例如热噪声、散粒噪声、暗电流噪声等也会对光信号的转换产生干扰,因此需要对接收到的可见光信号进行噪声隔离,提高信噪比。然后对该信号进行放大处理。一般采用两级放大,其中第一级放大主要是提高信号的信噪比,第二级放大则是将信号放大后续恢复电路所需要的信号量级。但运算放大器也会同时放大噪声,并且运算放大器本身也会产生噪声,主要是来自芯片内部所产生,因此需要信号滤波来滤除,以保证输出信号的信噪比。放大之后进行信号恢复。信号恢复的原理是按照数字通信对电信号的要求,对模拟信号进行采样和判决,进而恢复成对应对码率的数字信号,起到模数转换的功能。按照可见光调制的规则解码恢复电信号,然后根据系统为模块定义的串口通信协议,形成光门禁控制单元可识别的数据帧。

[0008] 例如,公开号为CN106296896A的中国专利文献公开一种基于LED可见光通信的门禁系统,该门禁系统的智能手持设备通过无线网络与门禁网络服务器进行通信,获取门禁通行码,经过编码后的通行码利用移动设备自带的LED闪光灯进行信息的发送;门禁网络服务器,通过编程设计在PC端搭建门禁数据服务系统,作为门禁管理系统,对请求登录服务器的用户进行身份的确认,通过无线网络向登录成功的智能手持设备传送登录通行码;支持与PC端通信的可见光接收控制单元,通过在接收电路上搭载单片机,实现传输信息的解码、串口通信、控制门禁系统的开关功能。

[0009] 例如,公开号为CN108734823A的中国专利文献公开了一种基于紫外光通信的门禁认证方法、钥匙装置及门禁装置,该门禁认证方法包括:钥匙端发送包含随机位验证码信息;门禁端判断该随机位验证码信息的位数L是否处于预设位数范围内;门禁端判断排列序号是否与存储的排列序号M相一致;门禁端判断该随机验证码信息是否准确;开启门禁,并将M+L作为新的排列序号进行存储。该发明的门禁认证方法需要依次对随机位验证码的位数、随机位验证码在验证序列信息中的位置和随机验证码信息本身进行验证,安全性更高,

紫外光近距离传输及可部分穿透障碍物的特性，验证过程不易被干扰，交互信息不易被复制或破解。

[0010] 例如，公开号为CN107492175A的中国专利文献公开了一种可见光安全门锁、系统及开锁方法，所述可见光安全门锁包括电子门锁机构、LED背光板、光电检测器及处理器，其中，光电检测器用于接收可见光信号，LED背光板用于发送可见光信号，处理器与电子门锁机构、LED背光板及光电检测器电连接，处理器保存有对应的地址码；使用时，处理器收到激活码后，将地址码进行发送，并根据地址码运用RSA加密算法计算得到一个校验码；处理器在收到开锁码后，对比校验码与开锁码，对比一致后控制电子门锁机构开锁。该发明通过采用移动终端代替门禁卡以及采用双重计算验证开锁，解决了门禁卡可复制性的弊端，使用户仅仅通过移动终端即可开锁，进而提高了门禁系统的安全性与便捷性。

[0011] 以上文献公开的基于可见光通信的门禁系统，采用的是移动端主动发射光信号，门禁端接收光信号并验证该光信号包含的身份信息，或通过物联网或互联网与服务器连接以验证身份信息，然后打开或关闭门禁；或者是移动端通过互联网与服务器连接，获取相应的秘钥信息以可见光的形式发送至门禁终端，门禁终端根据收到的光信号进行解调并生成相应的校验信息，然后发送至移动端，移动端解调获取相应的校验信息与服务器发送秘钥信息进行验证，当验证通过后再一次向门禁端发送开锁信息，门禁终端根据开锁信息与本地信息对比进行验证，验证成功后开锁。因此，上述基于可见光通信的门禁系统无论采用单向通信还是双向通信，都是主动发射可见光以进行信息的传递。但是通用的LED或者其他普通的发光器件的发光范围以及相应的接收光学信号的传感器对光敏感的角度范围都是有限的，这就要求移动端和门禁端需要完全对准才能实现双向通信，这对任何一个设备的移动性(Mobility)和一对多通信、多对多通信的可扩展性(Scalability)提出了严峻的挑战，很难实际应用于人流量较大的应用场景。其次，从设计理念、经济成本、运行维护以及广泛部署使用的角度来说，相应的设备应该是小型化、低功耗甚至是无源的。但是基于LED的通信发射能耗通常在几百毫瓦，而通常物联网设备大小的太阳能电池能转换的有效电能仅在几百微瓦，导致可移动性差，成本高。再其次，这种主动发射—接收的可见光模式，不仅容易被周围的环境光干扰，抗干扰能力差，而且容易被截获，安全性存疑。最后，上述文献公开的基于可见光通信的门禁系统为了提高安全性，不仅需要移动端和门禁端通过互联网与相应的服务器或者后台管理系统连接，而且验证程序繁复复杂，需要移动端、门禁端以及服务器彼此双向通信多次才能完成身份的验证。

[0012] 此外，一方面由于对本领域技术人员的理解存在差异；另一方面由于发明人做出本发明时研究了大量文献和专利，但篇幅所限并未详细罗列所有的细节与内容，然而这绝非本发明不具备这些现有技术的特征，相反本发明已经具备现有技术的所有特征，而且申请人保留在背景技术中增加相关现有技术之权利。

发明内容

[0013] 针对现有技术不足，本发明提供一种基于逆反射可见光通信的物联网门禁系统，至少包括移动端、门禁端以及通过物联网无线组网技术与所述移动端或门禁端建立连接的服务器。所述移动端能够与门禁端建立可见光通信链接以传递身份验证信息，使得所述身份验证信息经由所述服务器完成认证以打开或关闭所述门禁端。所述移动端或门禁端设置

有可配置的逆反射单元。所述移动端和/或门禁端通过所述逆反射单元被动接收光信号且以逆反射的方式将光信号返回而处于被动通信状态。所述光信号能够为所述移动端和/或门禁端提供能量。在双向通信管理权限的过程中，带有逆反射单元的一端通常为需要配置的一端，而配置涉及信号传输处理与供电这两个重要的方面。在本发明中，由于可配置的逆反射单元利用被动接收光信号来实现可配置性且以逆反射的方式将光信号返回，即本发明的逆反射单元除了能够利用逆反射光信号的方式大幅度降低能量消耗之外，还同时具备收集能量和处理光信号的能力，使得需要配置的一端能够无需供电也无需单独建立通信链接就始终处于被动无源工作之中，并且能够实现针对特定对象的可配置性，尤其适用于一方不便于获得供电但又应得到单独配置的权限管理场景。而且得益于逆反射单元采用逆反射的方式建立光通信链接，使得移动端和门禁端之间的光通信链路既具有良好的方向响应特性，又保证了反射方向的集中。此外，采用逆反射的方式建立光通信链路具有高度的空间定向特性，能够保证通讯信息不被截获，进一步增加了门禁系统的安全性。

[0014] 根据一个优选实施方式，所述逆反射单元至少包括调制模块、与所述调制模块连接的第一控制器、与所述第一控制器连接的第一光学传感器以及分别与所述第一光学传感器、所述第一控制器和所述调制模块连接的储能装置。所述第一光学传感器用于收集能量和接收带有信息的光信号，并将收集的能量传输至所述储能装置和将光信号传输至所述第一控制器。所述第一控制器配置为基于带有信息的光信号生成反馈信息，并基于反馈信息生成驱动所述调制模块的驱动信号。所述调制模块的一侧设置有逆反射光信号的逆反射层，使得所述调制模块能够基于所述驱动信号以控制所述逆反射层逆反射的光信号的明暗变化的方式将所述反馈信息调制在该逆反射的光信号上。

[0015] 所述逆反射单元还配置为：基于脉冲序列通过所述第一控制器控制所述第一光学传感器分别与所述储能装置和所述调制模块的连接状态，从而实现能量收集状态与信号检测状态的彼此隔离和高频切换。尽管现有技术可以通过减小尺寸或者采用低功耗的方式减少逆反射单元的能耗，但仍然需要额外的装置来为逆反射单元供电。此外，尽管可以采用类似太阳能电池的光学传感器来收集能量获取信号，例如公开号为CN106529645B的中国专利公开了一种基于可见光通信的自动识别无源标签，其公开了采用太阳能电池将光能转化为电能输入到无源标签的电源管理系统。该专利文献公开的利用太阳能电池获取信号的原理是：太阳能电池将光信号转化成电信号输入至电容，由于电容具有去直通交的特性，可以通过合理的选取电容以获得太阳能电池输出中的交流信号，并将其输入到光接收机中，实现可见光信号到电信号的转换。但是，太阳能电池输出的并不是交流信号。事实上太阳能电池接收的光信号包括环境光信号和读写单元发送的光信号，其中环境光信号大部分时间处于幅值缓慢变化的连续状态，而读写单元发送的具有间隔状态的离散光信号。环境光信号的存在极可能会淹没读写单元发送的光信号，可见太阳能电池输出的电信号由于环境光信号的存在而不会输出具有部分间断特性的交流信号，因而使用电容的去直通交的特性来获取读写单元发送的光信号，显然是不可靠的。尽管能够通过多种电气器件构建相应的电路来检测得到读写单元发送的光信号，但这无疑会增加逆反射单元的功率和体积，导致太阳能电池提供的能量无法维持逆反射单元的能量消耗，因此该专利公开的技术方案无法在太阳能电池收集能量的同时可靠地检测信号。本发明通过将能量的收集状态和光信号的检测状态彼此隔离，即逆反射单元不会在收集能量的状态下同时检测读写单元发送的光信号，从

而能够实现光信号的可靠检测。本发明通过第一控制器控制所述第一光学传感器分别与所述储能装置和所述调制模块的连接，能够在物理上将能量收集状态和信号检测状态隔离，即当第一光学传感器与储能装置连接的情况下，逆反射单元处于能量收集状态；当第一光学传感器与调制模块连接的情况下，逆反射单元处于信号检测状态。此外，逆反射单元需要在能量收集的状态下及时可靠地识别移动端或者门禁端发射的光信号，意味着逆反射单元需要花费一定的时间来检测信号，虽然花费更多的时间检测信号能够避免逆反射单元错过移动端或门禁端发射的光信号，但是可能导致能量收集时间减少，即充电时间减少导致充电功率小于逆反射单元消耗的功率，从而逆反射单元无法正常工作，因此本发明基于脉冲序列通过所述第一控制器来实现能量收集状态和信号检测状态隔离和高频切换。高频切换指的是通过脉冲序列的占空比来控制第一光学传感器分别与储能装置和调制模块的连接，即定时短间隔地采集第一光学传感器获得的波形，使得能量收集状态和检测信号状态交替变换，在尽可能短的时间内来检测信号，其余的时间用来实现能量的收集。事实上，根据奈奎斯特采样定理，当采样频率大于门禁端或移动端发送的光信号的频率的两倍时，第一控制器仍然能够识别该信号。优选地，在逆反射单元识别出门禁端或移动端发送的光信号后，逆反射单元直接接入调制状态，即第一控制器解调该光信号，并生成反馈信息。直到逆反射单元将反馈信息调制在逆反射的光信号上之后重新进入收集能量状态与检测信号状态的高频切换。而且，在类似门禁的权限管理场景下，逆反射单元的大部分时间是处于休眠状态，即处于能量收集状态，通过以上设置能够使得逆反射单元获得足够的能量。而且采用逆反射光信号的方式来发送光信号使得逆反射单元只需要为低功耗的第一控制器和调制模块供电，使得逆反射单元的功耗极小，从而在应得到单独配置的权限管理场景中，例如需要配置与服务器连接以后台验证信息权限的场景，或者需要配置与本地存储系统连接验证信息权限的场景，不需要采用额外的供电装置来进行供电。

[0016] 根据一个优选实施方式，在所述逆反射单元接收光信号的情况下，所述光信号分别进入所述第一光学传感器和调制模块。所述第一控制器配置为：监测所述第一光学传感器接收的光信号，并在识别带有信息的光信号的情况下，控制所述第一光学传感器断开与所述储能装置的连接以退出收集能量的状态，并且通过所述第一光学传感器接收所述带有信息的光信号。

[0017] 根据一个优选实施方式，所述调制模块至少包括第一偏振器件和第二偏振器件。所述逆反射层与所述第一偏振器件可拆卸地连接。所述第二偏振器件配置为设置于所述第一偏振器件的出光一侧，并且其偏振方向能够随所述第一控制器生成的驱动信号发生变化从而实现光信号的明暗变化。。

[0018] 根据一个优选实施方式，所述移动端或所述门禁端还设置有发射光信号和接收光信号的读写单元。所述读写单元配置为主动向所述逆反射单元发送至少包括身份验证信息的光信号，并接收由所述逆反射单元调制反射回的逆反射光信号，从而实现所述移动端与所述门禁端之间的信息交互。

[0019] 根据一个优选实施方式，所述读写单元至少包括依次电连接的发光装置、第二控制器以及第二光学传感器。所述第二控制器基于身份验证信息驱动所述发光装置，并通过调节光明暗变化的方式将身份验证信息调制于光信号上。所述第二光学传感器在其进光路径上设置有至少一个第一偏振器件。

[0020] 根据一个优选实施方式，在所述移动端设置有所述读写单元的情况下，所述逆反射单元设置在所述门禁端。所述移动端配置为与服务器连接以获取相应身份验证信息，并将身份验证信息以光信号的形式主动发送至所述门禁端。所述门禁端配置为通过所述逆反射单元接收光信号。所述门禁端基于预先存储的信息验证所述光信号承载的身份验证信息以生成至少包括本地信息的反馈信息，从而基于所述反馈信息打开或关闭门禁。所述门禁端将所述反馈信息通过所述逆反射单元调制于反射至所述移动端的逆反射光信号上。

[0021] 根据一个优选实施方式，在所述移动端设置有所述逆反射单元的情况下，所述读写单元设置在所述门禁端。所述门禁端配置为通过与服务器连接以获取相应身份验证信息，并将身份验证信息以光信号的形式主动发送至所述移动端。所述移动端配置为通过所述逆反射单元接收光信号。所述移动端基于预先存储的信息验证所述光信号承载的身份验证信息以生成至少包括本地信息的反馈信息，并将所述反馈信息通过所述逆反射单元调制于反射至所述移动端的所述逆反射光信号上。在所述门禁端接收到所述逆反射光信号的情况下，所述门禁端配置为：通过所述读写单元获取所述反馈信息，并发送至所述服务器以使得所述服务器完成身份验证逻辑生成确认信息；接收所述服务器返回的确认信息以打开或关闭门禁。

[0022] 本发明还提供一种基于逆反射可见光通信的物联网门禁方法，所述方法包括：通过移动端与门禁端建立可见光通信链接以传递身份验证信息，使得所述身份验证信息经由服务器完成认证以打开或关闭所述门禁端。所述移动端或门禁端通过其设置的可配置的逆反射单元被动接收光信号且以逆反射的方式将光信号返回而处于被动通信状态。所述光信号能够为所述移动端和/或门禁端提供能量。

[0023] 根据一个优选实施方式，所述方法还包括：所述逆反射单元通过在收集光信号能量的状态和检测光信号的状态之间进行切换的方式实现在收集光信号能量的过程中识别带有信息的光信号。

附图说明

[0024] 图1是本发明的一个优选实施方式的模块示意图；

[0025] 图2是本发明的另一个优选实施方式的模块示意图；

[0026] 图3是本发明的一个优选的逆反射光通信示意图；

[0027] 图4是本发明的一个优选的调制模块的结构示意图；

[0028] 图5是本发明的另一个优选的调制模块的结构示意图；

[0029] 图6是本发明的一个优选地读写单元的结构示意图；和

[0030] 图7是本发明的一个优选的逆反射单元的结构示意图。

[0031] 附图标记列表

[0032] 1：移动端 2：门禁端

[0033] 3：服务器 4：逆反射单元

[0034] 5：读写单元 6：环境光信号

[0035] 7：带有信息的光信号 41：调制模块

[0036] 42：第一控制器 43：第一光学传感器

[0037] 44：逆反射层 45：储能装置

[0038] 46:开关 47:检测电路

[0039] 48:DC-DC转换器 51:发光装置

[0040] 52:第二控制机器 53:第二光学传感器

[0041] 411:第一偏振器件 412:第二偏振器件

具体实施方式

[0042] 下面结合附图1至7进行详细说明。

[0043] 实施例1

[0044] 本实施例公开了一种门禁系统,可以是一种物联网门禁系统,也可以是一种基于可见光通信的门禁系统,也可以是一种基于可见光通信的物联网门禁系统,该系统可以由本发明的系统和/或其他可替代的零部件实现。比如,通过使用本发明的系统中的各个零部件实现本实施例公开的方法。在不造成冲突或者矛盾的情况下,其他实施例的优选实施方式的整体和/或部分内容可以作为本实施例的补充。

[0045] 优选地,现有的基于可见光通信的门禁技术需要用户在移动终端上与网络互联,来获得对应的激活码,并利用LED闪光发出激活码,采用这种可见光通信技术的门禁系统,成本和功耗较高,容易被恶性代码攻击,导致安全性较低,并且使用过程不够便捷。具体而言,现有技术的基于可见光通信的门禁系统无论采用单向通信还是双向通信,都是主动发射可见光以进行信息的传递。但是通用的LED或者其他普通的发光器件的发光范围以及相应的接收光学信号的传感器对光敏感的角度范围都是有限的,这就要求移动端1和门禁端2需要完全对准才能实现双向通信,不仅导致移动端1和门禁端2的移动性有限,而且在一对多通信或者多对多通信的应用场景下提出了严峻的挑战,很难实际应用于人流量较大的应用场景,例如,地铁闸机的门禁系统、火车站的门禁系统、汽车站的门禁系统以及飞机场的门禁系统。其次,从设计理念、经济成本、运行维护以及广泛部署使用的角度来说,现有基于可见光通信的门禁设备不够小型化,也不具备低功耗的特点。例如,基于LED的通信发射能耗通常在几百毫瓦,而通常物联网设备大小的太阳能电池能转换的有效电能仅在几百微瓦,导致可移动性差,成本高。再其次,这种主动发射—接收的可见光通信模式,不仅容易被周围的环境光干扰,抗干扰能力差,而且容易被截获,安全性存疑。最后,现有基于可见光通信的门禁系统为了提高安全性,不仅需要移动端1和门禁端2通过互联网与相应的服务器3或者后台管理系统连接,而且验证程序繁复复杂,例如通过复杂的加密算法来保证身份验证的安全性,使得移动端1或者门禁端2本身需要具有较强的计算能力,导致设备的硬件功耗、成本以及验证的时间成倍的增加。而且需要移动端1、门禁端2以及服务器3彼此双向通信多次才能完成身份的验证,进一步增加了验证时间的开销。基于以上原因,本实施例提供一种基于可见光通信的物联网门禁系统,采用一端主动发射,另一端被动反射的方式建立双向可见光通信链接,从而减少设备的复杂度、功耗以及体积,增加设备的可移动性,减少部署难度。

[0046] 针对现有技术不足,本发明提供一种基于逆反射可见光通信的物联网门禁系统,至少包括移动端1、门禁端2以及通过物联网无线组网技术与移动端1或门禁端2建立连接的服务器3。优选地,移动端1指的是人、车辆等需要验证身份信息的客体所使用的能够验证身份的设备。例如,工作人员、住户等携带能够验证身份的移动终端(例如手机、平板电脑等),

或者携带能够验证身份的IC卡、RFID卡等。门禁端2的作用是验证移动终端1的发射的光信号所携带的验证信息，需要门禁端2能够与移动端1建立可见光通信链接以传递身份验证信息。门禁端2还包括门锁机构、驱动门锁机构开或关的门禁驱动以及控制模块。控制模块至少包括处理器和存储器。存储器用于存储指令。处理器被配置为通过执行存储器存储的指令。处理器可以是中央处理器(Central Processing Unit,CPU)，通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application-Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field Programmable Gate Array,FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。优选地，在不同的实施方式下，移动端1或门禁端2还需要无线模块(RF Wireless Module)来实现与服务器3的网络连接。无线模块可以是Wi-Fi模块、LTE模块、蓝牙模块、Zigbee模块等。优选地，移动端1或者门禁端2还包括供电模块以及门锁检测模块。门锁检测模块用于检测门锁机构的运行状态，在门锁出现问题的情况下及时发现问题并做出警报处理，能够主动的进行安全监控。优选地，门锁检测模块可以采用红外无线探测、视频监控、声音监控、动作检测等。优选地，服务器3用于记录、验证以及管理当前的门禁系统相关的出入信息、身份信息等。优选地，身份验证信息经由服务器3完成认证以打开或关闭门禁端2。

[0047] 优选地，移动端1或门禁端2设置有可配置的逆反射单元4。逆反射单元4被动接收光信号且以逆反射的方式将光信号返回，使得移动端1或门禁端2处于被动通信状态。优选地，所述光信号能够为所述移动端1和/或门禁端2提供能量。优选地，逆反射单元4可以设置在移动端1，相应的门禁端2设置有读写单元5。优选地，逆反射单元4可以设置在门禁端2，相应的移动端1设置有读写单元5。优选地，读写单元5发射光信号和接收光信号。如图1至图3所示，读写单元5配置为主动向逆反射单元4发送至少包括身份验证信息的光信号，并接收由逆反射单元4调制并反射回的逆反射光信号，从而实现移动端1与门禁端2之间的信息交互。优选地，逆反射是指光线照射到逆反射材料的表面后反射回到光源方向。当入射光线的方向在较大范围内变化时，仍能保持这种性质。优选地，逆反射单元4的可配置可以是为服务器3的连接无线模块提供电能，从而实现身份验证信息的在线匹配。通过该设置方式，本实施例的有益效果是：

[0048] 1、由于逆反射单元4采用被动逆反射光信号的方式实现移动端1和门禁端2之间的可见光通信，因此移动端1和门禁端2不需要全部配置光发射器，例如不需要配置LED、LED驱动电路等，显著地降低了功耗和成本，便于设备的微型化，提高了移动性，便于实际的部署。例如，由于逆反射单元4的低功耗和微型化，能够容易地集成于移动端，例如集成于用户的手机、平板电脑等。而且由于逆反射单元4本身不需要发射光信号，并且接收到的光信号也能够部分转换为电能，因此逆反射单元4不需要额外的供电模块，具有较强的移动性以及可携带性，从而能够直接替代现有的IC卡、RFID卡等。甚至在逆反射单元4部署于门禁端2的情况下能够设置面积较大的第一光学传感器42，从而更多的能量为门禁端2的其他的电气器件供电。

[0049] 2、得益于逆反射单元4采用逆反射的方式建立光通信链接，使得移动端1和门禁端2之间的光通信链路既具有良好的方向响应，又保证了反射方向的集中，即光线的出射方向与光线的入射角无关，使得移动端1和门禁端2之间能够宽角度双向通信。此外，采用逆反射的方式建立光通信链路具有高度的空间定向特性，能够保证通信信息不被截获，进一步增

加了门禁系统的安全性。

[0050] 3、具有良好的扩展性，尤其适用于一对多通信或者多对多通信场景。得益于逆反射的高度空间定向特性以及宽角度双向通信，能够实现多个移动端1与门禁端2连接，或者移动端1能够与多个门禁端2连接，或者多个移动端1能够与多个门禁端2连接，在人流量较大的应用场景下，能够保证人流快速通过，实现门禁无缝体验功能。

[0051] 4、设置有逆反射单元4的移动端1或者门禁端2能够在不与服务器3交互的情况下实现身份信息的验证，从而不仅能够极大地减低成本和功耗，还能够避免被恶意程序攻击，进一步提高门禁系统的安全性。此外，也能够避免复杂的、需要移动端1和门禁端2多次信息交互的身份验证方法，不仅能够降低验证时间的开销，还能够避免不必要的计算开销，从而降低本地设备的复杂度。

[0052] 优选地，设置有逆反射单元4的移动端1或者门禁端2不需要与服务器3交互的优选实施方式如下：

[0053] 根据一个优选实施方式，在移动端1设置有读写单元5的情况下，逆反射单元4设置在门禁端2，如图1所示。优选地，移动端1配置为与服务器3连接以获取相应身份验证信息，并将身份验证信息以光信号的形式主动发送至门禁端2。优选地，如图1所示，门禁端2配置为通过逆反射单元4接收光信号。门禁端2基于预先存储的信息验证光信号承载的身份验证信息以生成至少包括本地信息的反馈信息。优选地，预先存储的信息是之前存储关于身份验证的信息。优选地，逆反射单元4也可以通过读写单元5发送的信息来更新存储的信息。优选地，本地信息至少包括通行人员的时间信息、身份信息、门禁的状态信息等。门禁的状态信息至少包括开启状态、关闭状态、离线状态、警报状态等。从而门禁端2能够根据基于反馈信息打开或关闭门禁。优选地，门禁端2将反馈信息通过逆反射单元4调制于反射至移动端1的逆反射光信号上，从而能够把信息传递至移动端1。移动端1获得相应的本地信息。优选地，另一种实施方式可以采用如下方式验证。优选地，移动端1配置为与服务器3连接以获取相应身份验证信息，并以光信号的形式主动发送至门禁端2。门禁端2配置为通过逆反射单元4接收光信号，基于预先存储的信息验证光信号承载的身份验证信息以生成至少包括本地信息的反馈信息，从而将反馈信息通过逆反射单元4调制于反射至移动端1的逆反射光信号。在移动端1接收到逆反射光信号的情况下，移动端1配置为基于逆反射光信号获取反馈信息，并发送至服务器3以完成身份验证逻辑，从而生成确认信息。移动端1通过读写单元5将该确认信息发送至门禁端2，从而门禁端2基于确认信息打开或关闭门禁。

[0054] 根据一个优选实施方式，在移动端1设置有逆反射单元4的情况下，读写单元5设置在门禁端2，如图2所示。门禁端2配置为通过与服务器3连接以获取相应身份验证信息，并将身份验证信息以光信号的形式主动发送至移动端1。移动端1配置为通过逆反射单元4接收光信号。移动端1基于预先存储的信息验证光信号承载的身份验证信息以生成至少包括本地信息的反馈信息，并将反馈信息通过逆反射单元4调制于反射至移动端1的逆反射光信号上。在门禁端2接收到逆反射光信号的情况下，门禁端2配置为：通过读写单元5获取反馈信息，并发送至服务器3以使得服务器3完成身份验证逻辑生成确认信息；接收服务器3返回的确认信息以打开或关闭门禁。

[0055] 优选地，逆反射单元4至少包括调制模块41、第一控制器42、第一光学传感器43以及储能装置45。第一控制器42与调制模块41连接。第一光学传感器43与第一控制器42连接。

储能装置45分别与第一光学传感器43、第一控制器42和调制模块41连接。第一光学传感器43用于收集能量和接收带有信息的光信号7，并将收集的能量传输至储能装置45和将光信号传输至第一控制器42。第一控制器42配置为基于带有信息的光信号7生成反馈信息，并基于反馈信息生成驱动调制模块41的驱动信号。调制模块41的一侧设置有逆反射光信号的逆反射层44，使得调制模块41能够基于驱动信号以控制逆反射层44逆反射的光信号的明暗变化的方式将反馈信息调制在该逆反射的光信号上。

[0056] 优选第一控制器42至少包括解码器、电源管理以及传输和编码逻辑器。第一控制器42可以选择型号为MSP430G2403的微程序控制芯片，该芯片包括解码器、电源管理以及传输和编码逻辑器。第一光学传感器43可以是太阳能电池或太阳能板。优选地，逆反射单元4还包括设置在调制模块41与第一控制器42之间的驱动电路。优选地，逆反射单元4还包括检测电路47。检测电路47至少包括比较器和放大器，其中放大器用于放大从第一光学传感器43接收到的电信号，比较器用于实现信号的数字化。优选地，储能装置45可以是超级电容。优选地，调制模块41至少包括第一偏振器件411和第二偏振器件412。第二偏振器件412与第一控制器42连接。优选地，第一偏振器件411能够实现光的偏振。第一偏振器件411可以是偏振方向确定的偏振器件。例如偏振滤光片、偏振滤光镜等。优选地，第二偏振器件412其偏振方向能够随第一控制器42生成的驱动信号发生变化从而实现光信号的明暗变化。优选地，第二偏振器件412可以是液晶材料。液晶材料在其两端电压变化的情况下会改变经过的光的偏振方向。第二偏振器件412配置为设置于第一偏振器件411的出光一侧。当第二偏振器件412与第一偏振器件411的偏振方向相同时，光信号能够全部通过，光信号的亮度较大。当第一偏振器件411和第二偏振器件412的偏振方向不同时，光信号无法全部通过，光信号的亮度较暗。当第一偏振器件411和第二偏振器件412的偏振方向正交的情况下，光信号无法通过。通过该设置方式能够实现光信号的明暗变化控制，进而实现信息的调制。优选地，第二偏振器件412与第一控制器42可连接。优选地，逆反射层44与第一偏振器件411可拆卸地连接。优选地，逆反射层44采用逆反射材料制作，例如玻璃珠型或棱镜型的反光材料。优选地，可拆卸连接的方式可以是粘接、螺纹连接等。

[0057] 优选地，逆反射单元4还配置为：基于脉冲序列通过第一控制器42控制第一光学传感器43分别与储能装置45和调制模块41的连接状态，从而实现能量收集状态与信号检测状态的彼此隔离和高频切换。事实上第一光学传感器43为太阳能电池的情况下，其接收的光信号包括环境光信号6和读写单元5发送的带有信息的光信号7，如图7所示。环境光信号6大部分时间处于幅值缓慢变化的连续状态，而读写单元5发送的带有信息的光信号7为具有间隔状态的离散光信号。环境光信号6的存在极可能会淹没读写单元5发送的带有信息的光信号7，可见太阳能电池输出的电信号由于环境光信号的存在而不会输出具有明显间断特性的信号，因而简单的使用电容的去直通交的特性来获取读写单元5发送的光信号，显然是不可靠的。尽管能够通过多种电气器件构建相应的电路来检测得到读写单元5发送的光信号，但这无疑会增加逆反射单元4的功率和体积，导致太阳能电池提供的能量无法维持逆反射单元4的能量消耗。因此，本发明通过将能量的收集状态和光信号的检测状态彼此隔离，即逆反射单元4不会在收集能量的状态下同时检测读写单元5发送的光信号，从而能够实现光信号的可靠检测。优选地，在逆反射单元4接收光信号的情况下，光信号分别进入第一光学传感器43和调制模块41。第一控制器42配置为：监测第一光学传感器43接收的光信号，并在

识别带有信息的光信号7的情况下，控制第一光学传感器43断开与储能装置45的连接以退出收集能量的状态，并且通过第一光学传感器43接收带有信息的光信号7。本发明通过第一控制器42控制第一光学传感器43分别与储能装置45和调制模块41的连接，能够在物理上将能量收集状态和信号检测状态隔离，即当第一光学传感器43与储能装置45连接的情况下，逆反射单元4处于能量收集状态。当第一光学传感器43与调制模块41连接的情况下，逆反射单元4处于信号检测状态。由于超级电容，即储能装置45可能会滤除部分带有信息的光信号7，因此第一光学传感器43通过开关46分别与储能装置45和检测电路47连接。开关46可以是低功耗的单刀双掷开关。储能装置45通过DC-DC转换器48为调制模块41、第一控制器42、开关46、检测电路47提供稳定的直流电能，如图7所示。优选地，逆反射单元4需要在能量收集的状态下及时可靠地识别移动端1或者门禁端2发射的光信号，意味着逆反射单元4需要花费一定的时间来检测信号，虽然花费更多的时间检测信号能够避免逆反射单元4错过移动端1或门禁端2发射的光信号，但是可能导致能量收集时间减少，即充电时间减少导致充电功率小于逆反射单元4消耗的功率，从而逆反射单元4无法正常工作，因此本发明基于脉冲序列通过第一控制器42来实现能量收集状态和信号检测状态隔离和高频切换。高频切换指的是通过脉冲序列的占空比来控制第一光学传感器43分别与储能装置45和调制模块41的连接，即定时短间隔地采集第一光学传感器43获得的波形，使得能量收集状态和检测信号状态交替变换，在尽可能短的时间内来检测信号，其余的时间用来实现能量的收集。事实上，根据奈奎斯特采样定理，当采样频率大于门禁端2或移动端1发送的光信号的频率的两倍时，第一控制器42仍然能够识别该信号。优选地，基于脉冲序列的占空比来控制能量收集状态和检测信号状态的切换的方式是：基于带有信息的光信号7的频率和所采用的寄生电容和阻抗来设计脉冲序列的占空比；脉冲序列的逻辑值包括“0”和“1”，当脉冲序列处于逻辑值为“0”时，第一控制器42控制开关46使得第一光学传感器43与储能装置45连接，从而使得逆反射单元4处于能量收集状态；当脉冲序列处于逻辑值为“1”时，第一控制器42控制开关46使得第一光学传感器43与检测电路47连接，从而使得逆反射单元4处于检测信号状态。优选地，占空比可以是保持逻辑值“1”的时间与周期之间的比值。占空比的取值小于1。优选地，占空比的值为可以设置在0.2～0.5之间。优选地，在逆反射单元4识别出门禁端2或移动端1发送的光信号后，逆反射单元4直接接入调制状态，即第一控制器42解调该光信号，并生成反馈信息。直到逆反射单元4将反馈信息调制在逆反射的光信号上之后重新进入收集能量状态与检测信号状态的高频切换。而且，在类似门禁的权限管理场景下，逆反射单元4的大部分时间是处于休眠状态，即处于能量收集状态，通过以上设置能够使得逆反射单元4获得足够的能量。而且采用逆反射光信号的方式来发送光信号使得逆反射单元4只需要为低功耗的第一控制器42和调制模块41供电，使得逆反射单元4的功耗极小，从而在应得到单独配置的权限管理场景中，例如需要配置与服务器3连接以后台验证信息权限的场景，或者需要配置与本地存储系统连接验证信息权限的场景，不需要采用额外的供电装置来进行供电。通过以上设置方式，使得逆反射单元4能够根据读写单元5发射的光信号获取身份验证信息，并根据身份验证信息将验证后的反馈信息返回至读写单元5，从而使得门禁端2能够基于该信息以打开和关闭门锁机构。

[0058] 优选地，如图4，第二偏振器件412位于两个第一偏振器件411之间。优选地，光信号经过第一偏振器件411后起偏，成为偏振光。通过控制第二片偏振器件412的电压变化实现

控制经过第二偏振器件412的光信号的偏振方向，因此当逆反射的光信号经过第二偏振器件412后其偏振方向改变，当改变后的偏振的方向与第一偏振器件411的偏振方向同时，逆反射的光信号的光强变弱。只有当改变后的偏振方向与第一偏振器件411的偏振方向相同的情况下，逆反射的光信号的光强不变。通过以上设置方式，能够实现对光信号的调制。

[0059] 根据一个优选实施方式，读写单元5至少包括依次电连接的发光装置51、第二控制器52以及第二光学传感器53。优选地，发光装置可以是LED、或者手机的闪光灯、汽车的前照灯等。优选地，第二控制器52可以与第一控制器51相同。优选地，第二光学传感器53与第一光学传感器43相同，可以是光电检测器。优选地，第二控制器52基于身份验证信息驱动发光装置51，并通过调节光明暗变化的方式将身份验证信息调制于光信号上。。优选地，读写单元5设置有相应的驱动发光装置51的驱动电路，从而使得第二控制器53能够驱动发光装置51。

[0060] 实施例2

[0061] 本实施例是对实施例1进一步的改进，重复的内容不再赘述。优选地，逆反射单元4的结构如图5所示，与实施例1的逆反射单元4的结构不同，第二偏振器件412不是位于两个第一偏振器件411之间，而是仅在第二偏振器件412和逆反射层44之间设置至少一个第一个偏振器件。通过该设置方式，使得移动端1与门禁端2之间的可见光通信是无闪烁的。

[0062] 优选地，逆反射单元4设有仅在进光时起偏的至少一个第一偏振器件411。优选地，第一偏振器件411可以是偏振滤光片、偏振滤光镜等。通过该设置方式，使得逆反射单元4接收的光信号是偏振光信号，便于后续逆反射单元4利用第二偏振器件412调制光信号的偏振状态。优选地，逆反射单元4采用后置偏振的方式调制读写单元5发射的光信号。后置偏振是指逆反射单元4的光信号开或关的状态是后置在读写单元5上发生的，从而读写单元5与逆反射单元4之间的光信号是以在时间上和/或空间上连续的方式传输的。优选地，如图6所示，第二光学传感器53在其进光路径上设置有至少一个第一偏振器件411，从而读写单元5可以通过第一偏振器件411或其他能够感知偏振变化的装置来实现光信号的开/关或明暗变化。优选地，现有技术基本采用OOK调制或者其他振幅相关的调制方式，使得逆反射单元4调制后的光信号处于明暗交替变化的状态，从而出现光闪烁的问题。光闪烁问题是指由于人类视觉对运动的物体以及闪烁的物体非常敏感，闪烁的逆反射单元4很可能会分散移动端1处人员的注意力，尤其是在移动端1为交通工具的情况下，不仅会分散驾驶员的注意力，还会导致驾驶人员头晕和头痛。事实上，一方面可以采用其他不会引起闪烁的调制技术，但这些调制技术不仅功耗较大并且成本较高。另一方面，可以通过提高开/关键控(OOK)的调制频率使得人眼无法感知光的闪烁，但是这种方法需要提高驱动器的响应速度，因此需要高昂的代价来构建和维护VLBC系统，不符合物联网门禁系统低功耗、低成本以及大规模部署的设计理念。本发明通过后置偏振，使的逆反射单元4采用OOK调制或者其他振幅相关的调制方式导致的光的明暗交替变化后置在读写单元5上发生，而逆反射单元4只需要通过第二偏振器件412调制光信号的偏振方向即可将信息调制到光信号即可，因此逆反射单元4传输至读写单元5的光信号是在时间和/或空间上连续的。在时间和/或空间上连续指的是逆反射单元4反射的光信号的强度或幅度没有被调制，即不产生规律、连续的变化，因此光信号在一定的时间范围内，其空间上的幅度或光强度随时间连续变化，而且其变化幅度较小，可近似为不变。通过该设置方式，由于人眼无法感知光的偏振方向，因此强度不变的光不会

产生闪烁，由于读写单元5和逆反射单元4分别设置在移动端1和门禁端，因此能够实现移动端1与门禁端2之间的无闪烁可见光通信。

[0063] 实施例3

[0064] 本实施例公开了一种门禁方法，可以是一种基于物联网的门禁方法，也可以是一种基于可见光通信的门禁方法，也可以是一种基于可见光通信的物联网方法，该方法可以由本发明的系统和/或其他可替代的零部件实现。比如，通过使用本发明的系统中的各个零部件实现本实施例公开的方法。在不造成冲突或者矛盾的情况下，其他实施例的优选实施方式的整体和/或部分内容可以作为本实施例的补充。

[0065] 本发明还提供一种基于逆反射可见光通信的物联网门禁方法，方法包括：通过移动端1与门禁端2建立可见光通信链接以传递身份验证信息，使得身份验证信息经由服务器3完成认证以打开或关闭门禁端2。优选地，方法还包括移动端1或门禁端2通过其设置的可配置的逆反射单元4被动接收光信号且以逆反射的方式将光信号返回而处于被动通信状态，并且光信号能够为移动端1和/或门禁端2提供能量。根据一个优选实施方式，方法还包括：逆反射单元4通过在收集光信号能量的状态和检测光信号的状态之间进行切换的方式实现在收集光信号能量的过程中识别带有信息的光信号7，从而为逆反射单元4的可配置提供能源。优选地，本实施例提供的物联网门禁方法采用实施例1和实施例2所公开的移动端1、门禁端2以及逆反射单元4，重复的内容不再赘述。

[0066] 需要注意的是，上述具体实施例是示例性的，本领域技术人员可以在本发明公开内容的启发下想出各种解决方案，而这些解决方案也都属于本发明的公开范围并落入本发明的保护范围之内。本领域技术人员应该明白，本发明说明书及其附图均为说明性而并非构成对权利要求的限制。本发明的保护范围由权利要求及其等同物限定。

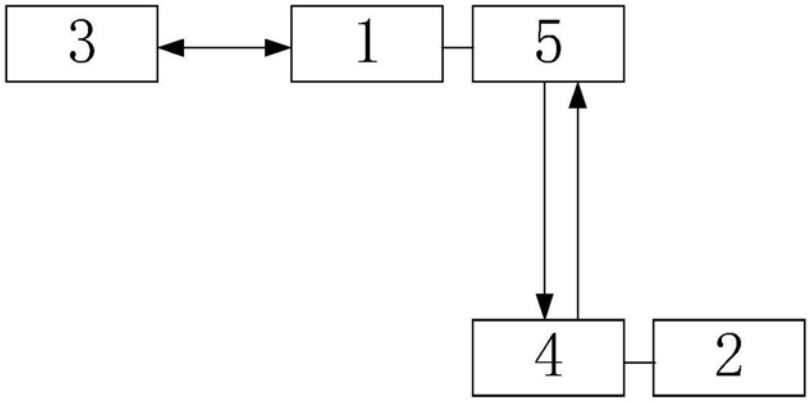


图1

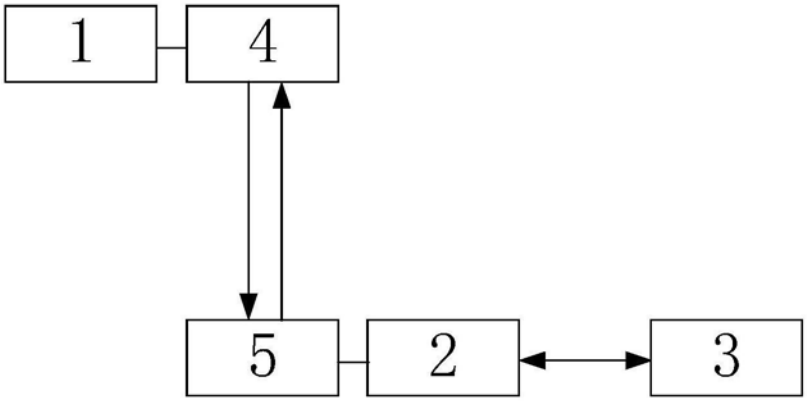


图2

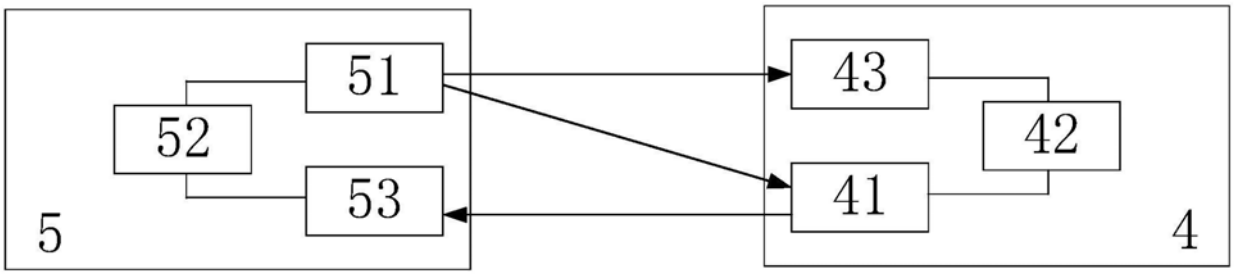


图3

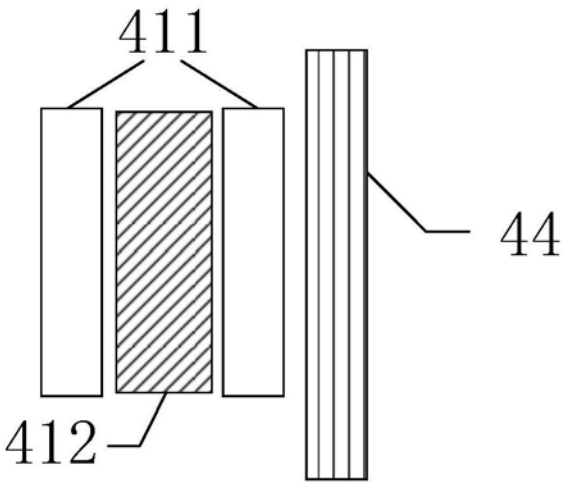


图4

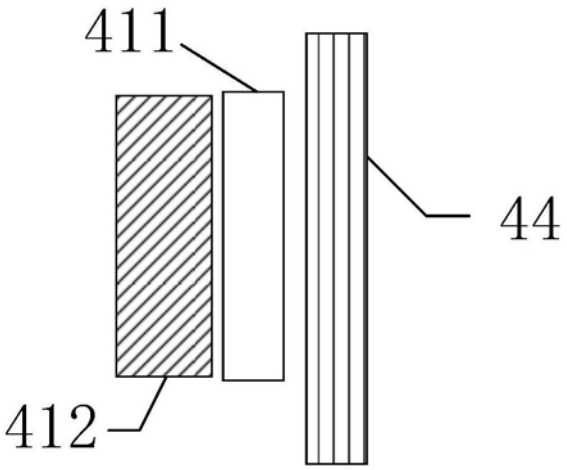


图5

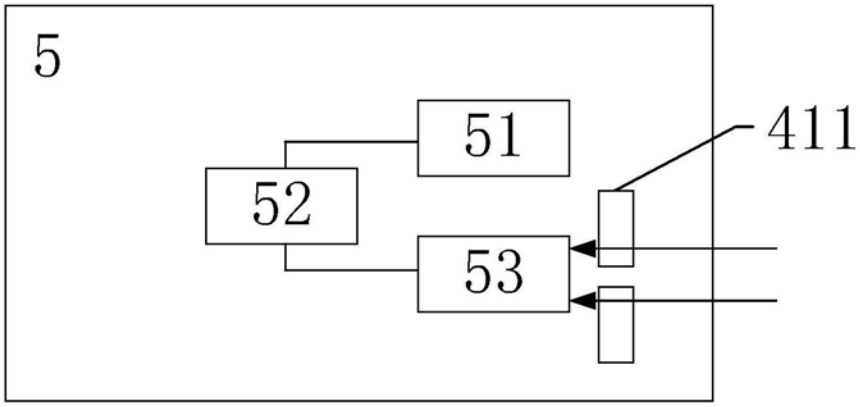


图6

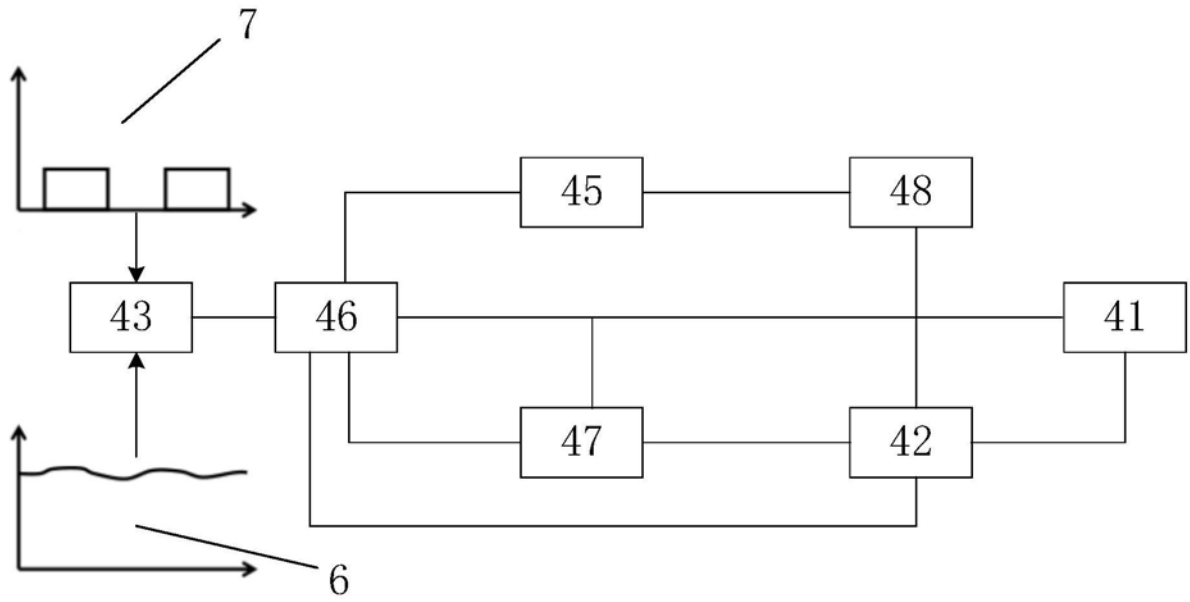


图7