(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106850671 A
(43)申请公布日 2017.06.13

(21)申请号 201710126870.7

(22)申请日 2017.02.27

(71)申请人 南京聚鲲物联网科技有限公司
地址 210000 江苏省南京市建邺区仁恒江湾城2期6栋204室

(72)发明人 徐伟达 李伟铭

(51)Int.Cl.
H04L 29/06(2006.01)
G08C 23/02(2006.01)

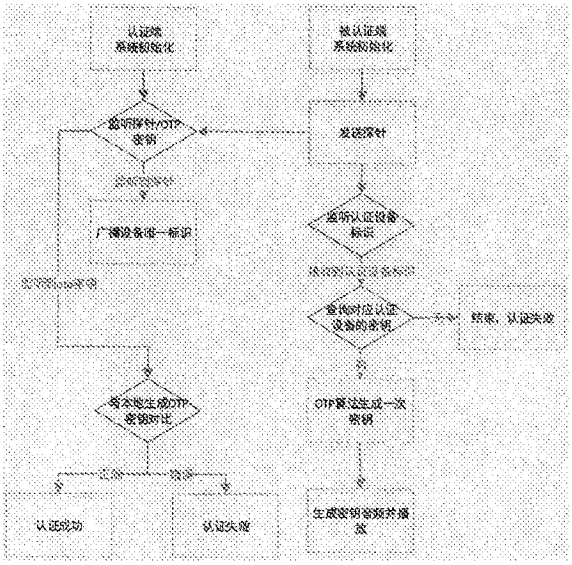
权利要求书3页 说明书4页 附图2页

(54)发明名称

一种利用声波通信的身份认证方法及其系统

(57)摘要

本发明提出一种声波认证方法以弥补现有技术的不足，该技术采用高频声波的编码，充分利用高频声波的传输能力，在设备端实时编码/解码包含一次性密钥编码信息的音频流，在无需安装额外通信设备的情况下，在认证设备之间实现数据的直接传递，快速准确安全地完成认证端和被认证端的双向认证。



CN 106850671 A

1.一种利用声波通信身份认证的方法，其特征在于，所述方法基于声波通信验证设备，包括如下步骤：

步骤10、系统初始化，认证双方约定认证算法初始参数；

步骤20、被认证方发送探针声波信息激活认证设备；

步骤30、认证设备播放包含其设备唯一标识号的音频信号；

步骤40、被认证方通过认证算法以及约定好的参数生成一次性密钥；

步骤50、被认证方将一次性密钥通过实时音频流进行编码；

步骤60、认证端接收实时音频信息，进行解码认证；

步骤70、认证端对认证结果进行处理。将认证结果实时音频编码，传递给被认证端；

步骤80、被认证方接受步骤7播放的认证结果音频流，进行解码并展示认证结果。

2.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤10包含如下步骤：

步骤11.认证方初始化认证算法参数，所述认证算法参数信息至少包含以下信息：认证方唯一标识号、对应认证方唯一标识号的共享密钥、以及准确的国际标准时间。

步骤12.被认证方初始化认证算法参数，所述认证算法参数信息至少包含以下信息：被认证方持有，经权限认证成功后的认证方的唯一标识号列表、及该唯一标识号对应的共享密钥列表、以及准确的国际标准时间。

3.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤20包含如下步骤：

步骤21、被认证方到达认证方设备附近，直径为0.1m～3m的球形的范围内，触发认证操作；

步骤22、被认证方设备发送音频探针信号激活认证方设备。

4.根据权利要求3所述的方法，其特征在于：步骤21所述被认证方持有移动终端设备、智能手机或平板电脑进行认证操作；步骤21所述认证方设备为移动终端设备、智能手机、平板电脑或其他带有麦克风和话筒的嵌入式设备。

5.根据权利要求3所述的方法，其特征在于：步骤21所述认证方设备一直处于音频监听状态。

6.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤30包含如下步骤：

步骤31.认证设备接收到探针信号后，播放包含自己设备唯一标识的编码音频信号。

7.根据权利要求6所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤31播放自己的设备唯一标识编码音频一段固定时间后停止播放，可以达到节能以及减少干扰的目的。

8.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤40包含如下步骤：

步骤41.被认证方设备正确接收到认证设备的唯一标示号后，检索本设备是否有该认证设备的共享密钥。若查询存在，则进入步骤42，否则认证失败。

步骤42.使用TOTP算法(Time-Based One-Time Password Algorithm)以及步骤10初始化的参数以及共享密钥，生成一次性认证密钥。TOTP算法为现有成熟认证算法，可参见RFC

(Request For Comments)文档RFC 6238。

9.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤50包含如下步骤：

步骤51.被认证设备将步骤42生成的一次性密钥进行音频实时流编码并进行音频循环播放。

10.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤60包含如下步骤：

步骤61.认证方设备处于音频监听状态，收到并校验步骤51播放的音频。

步骤62.认证方设备对正确接收到的51音频进行音频解码，解码后得到的被认证方发送的一次性密钥。

步骤63.认证方设备通过步骤10初始化的参数，使用TOTP算法，同时生成一次性认证密钥，并将该密钥与步骤62解码出来的密钥进行比对。

11.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤70包含如下步骤：

步骤71.若步骤63的比对结果一致，则认证成功。否则认证失败。

步骤72.认证方设备将认证结果进行实时音频流编码，并播放该音频流。

12.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述步骤80包含如下步骤：

步骤81.被认证方设备接受并解码步骤72播放的认证结果音频流，同时在显示设备上展示认证结果

步骤82.被认证方和认证方对认证结果进行日志记录，通过移动网络上传系统中央服务器备案。

13.根据权利要求1所述的一种利用声波通信身份认证的方法，其特征在于，所述声波通信验证设备包括：声波输入模块；声波输出模块；时间同步模块；声波编解码；认证算法处理器模块。

14.根据权利要求13所述的一种利用声波通信身份认证的方法，其特征在于：

所述声波输入模块，用于通过设备上的麦克风或其他声音采集设备，采集设备附近有限范围内的声音；

所述声波输出模块，用于通过设备上的扬声器或者其他声音播放设备，播放实时编码或预编码的音频流信息；

所述时间同步模块，实现多个设备之间的时间同步，确保认证算法能够正常准确工作。时间同步模块分为网络同步和离线同步两种模式；

所述声波编解码模块即包括了声波编码模块和声波解码模块，声波编码模块可以将文本信息编码进音频流中；声波解码模块可以将带有编码信息的音频流中携带的信息解码成文本信息；

所述认证算法处理器模块即使用OTP算法进行生成OTP密钥以及校验密钥的处理模块。

15.根据权利要求14所述的一种利用声波通信身份认证的方法，其特征在于，所述时间网络同步和离线同步模式为：

网络时间同步模块可以通过互联网，通过时间同步服务器实时同步UTC(Universal

Time Coordinated)来协调世界时。

离线时间同步模块使用实时时钟模块进行离线的时间计时，确保与UTC保持一致。

一种利用声波通信的身份认证方法及其系统

技术领域

[0001] 本发明涉及一种基于声波通信的低成本，高可靠的身份认证信息方法和系统。

背景技术

[0002] 目前常用的认证技术包括传统的密码输入，IC/ID卡刷卡或者生物特征(如指纹、人脸识别)等。然而这些技术均存在密码更换成本大，发卡流程冗长或者认证设备昂贵等问题。与此同时，随着智能手机的进一步普及，手机通信认证正越来越多地被应用在现有的认证系统中，主要的方式包含了二维码、蓝牙、NFC和WIFI等方式。但这些方式也存在操作繁琐，响应时间长等问题。在此背景下，本专利提出一种利用高频声波通信实现手机与设备间的认证。区别于现有音频编码控制方法采用对固定ID或者固定密钥进行音频编码的低安全性策略，本方案采用动态一次性密钥方案，音频内容即使被复制也不能通过认证，从而保证了认证的安全性。此外，由于该方案无需额外硬件设备，手机仅使用麦克风和话筒便可进行通信。因此，有潜力能够快速部署并推广。

发明内容

[0003] 本发明提出一种声波认证方法以弥补现有技术的不足，该技术采用高频声波的编码，充分利用高频声波的传输能力，在设备端实时编码/解码包含一次性密钥编码信息的音频流，在无需安装额外通信设备的情况下，在认证设备之间实现数据的直接传递，快速准确安全地完成认证端和被认证端的双向认证。

[0004] 为了满足传输要求，本发明通过以下技术方案解决其技术问题。该技术方案主要包含两个部分：一、基于声波通信的身份认证方法；二、实现基于声波通信的身份认证的系统设计。参考图1，一种利用声波通信身份认证的方法，其特征在于，所述方法基于声波通信验证设备的身份认证方法，包括如下步骤：

[0005] 步骤10、系统初始化，认证双方约定认证算法初始参数；

[0006] 步骤20、被认证方发送探针信息激活认证设备；

[0007] 步骤30、认证设备播放包含其设备唯一标识号的音频信号；

[0008] 步骤40、被认证方通过认证算法生成一次性密钥；

[0009] 步骤50、被认证方将一次性密钥通过实时音频流进行编码；

[0010] 步骤60、认证端接收实时音频信息，进行解码认证；

[0011] 步骤70、认证端对认证结果进行处理。将实时音频编码，传递给被认证端；

[0012] 步骤80、被认证方接受步骤7播放的认证结果音频流，进行解码并展示认证结果。

[0013] 进一步的，所述步骤10包含如下步骤：

[0014] 步骤11.认证方初始化认证算法参数，所述认证算法参数信息至少包含以下信息：认证方唯一标识号、以及对应认证方唯一标识号的共享密钥以及准确的国际标准时间。

[0015] 步骤12.被认证方初始化认证算法参数，所述认证算法参数信息至少包含一下信息：被认证方有权限认证成功的认证方唯一标识号列表、唯一标识号对应的共享密钥列表

以及准确的国际标准时间。

[0016] 进一步的，所述步骤20包含如下步骤：

[0017] 步骤21、被认证方到达认证方设备附近，直径为0.1m～2m的球形的范围内，触发认证操作；

[0018] 步骤22、被认证方设备发送音频探针信号激活认证方设备。

[0019] 进一步的，步骤21所述被认证方持有移动终端设备、智能手机或平板电脑进行认证操作；步骤21所述认证方设备为移动终端设备、智能手机、平板电脑或嵌入式设备。

[0020] 进一步的，步骤21所述认证方设备一直处于音频监听状态。

[0021] 进一步的，所述步骤30包含如下步骤：

[0022] 步骤31.认证设备接收到探针信号后，广播播放自己的设备唯一标识编码音频；

[0023] 进一步的，所述步骤31广播播放自己的设备唯一标识编码音频一段固定时间后停止播放，可以达到节能以及减少干扰的目的。

[0024] 进一步的，所述步骤40包含如下步骤：

[0025] 步骤41.被认证方设备正确接收到认证设备的唯一标示号，检索本设备是否有该认证设备的共享密钥。若查询存在，则进入步骤42，否则认证失败。

[0026] 步骤42.使用TOTP算法(Time-Based One-Time Password Algorithm)以及步骤10初始化的参数以及共享密钥，生成一次性认证密钥。TOTP算法为现有成熟认证算法，可参见RFC(Request For Comments)文档RFC 6238。

[0027] 所述声波通信验证设备包括：声波输入模块；声波输出模块；时间同步模块；声波编解码；认证算法处理器模块。

[0028] 进一步的，所述声波输入模块，用于通过设备上的麦克风或其他声音采集设备，采集设备附近有限范围内的声音；

[0029] 进一步的，所述声波输出模块，用于通过设备上的扬声器或者其他声音播放设备，播放编码或未编码的音频流信息；

[0030] 进一步的，所述时间同步模块，实现多个设备之间的时间同步，确保认证算法能够正常准确工作。时间同步模块分为网络同步和离线同步两种模式；

[0031] 进一步的，所述时间网络同步和离线同步模式为：

[0032] 网络时间同步模块可以通过互联网，通过时间同步服务器实时同步UTC(Universal Time Coordinated)来协调世界时。

[0033] 离线时间同步模块使用实时时钟模块进行离线的时间计时，确保与UTC保持一致。

[0034] 进一步的，所述声波编解码模块即包括了声波编码模块和声波解码模块，声波编码模块可以将文本信息编码进音频流中；声波解码模块可以将带有编码信息的音频流中携带的信息解码成文本信息；

[0035] 进一步的，所述认证算法处理器模块即使用OTP算法进行生成OTP密钥以及校验密钥的处理模块。

[0036] 本发明的优点在于：

[0037] (1)通过高频声波进行信息传递，用户端的现有设备无需改造或新加模块即可支持该类通讯方式。

[0038] (2)定义高频声波双向通信协议，实现认证方与被认证方的双工通信。

[0039] (3)音频流认证信息为实时编码的一次性密钥，即使音频流信息被复制，也无法进行多次认证，确保了认证的安全性。

[0040] (4)使用声波通信承载TOTP验证方式，安全性高，应用场景广。

[0041] (5)通信距离可通过调节音频播放分贝实现0.1m～2m的可调节通信距离。

附图说明

[0042] 图1是本发明的详细流程框图

[0043] 图2是本发明的功能模块设计图

[0044] 图3是本发明的认证机制设计图

具体实施方式

[0045] 如图1所示，本发明提供了一种基于声波双向通信的身份认证方法，由三个部分组成：认证双方(包括单不仅限于，手机端和声波门禁设备)，以及权限管理后台。

[0046] 参考图1，整个认证流程涉及认证方和被认证方，被认证方可以是智能手机上预装的应用程序；认证方可以既是智能手机的认证应用程序，也可以是包含各类模块的订制认证设备(参见图2)。

[0047] 以下具体实施场景，设定被认证方为手持智能手机的业主；认证方为支持声波通信认证的门禁控制器。具体实施方法详述如下：

[0048] 首先认证双方完整系统初始化，完成认证算法初始参数的设置。

[0049] 所述系统初始化为智能手机中预装的应用程序和认证设备处理器中烧录的编解码程序和认证程序均保持一致。

[0050] 初始参数中的时间参数：手机通过互联网采用实时时间同步模块进行时间同步；门禁控制器采取离线时间同步模块方式，保证与手机的时间同步。

[0051] 初始化权限信息所包含的算法密钥，手机APP通过网络从认证后台获取该用户被授权的设备的权限列表以及每个权限对应的种子密钥。

[0052] 当用户手持手机设备到达门禁控制器设备附近0.1m～2m范围内时可以手动触发认证操作。手动触发的动作可以是点击程序中的特定按钮，也可以是摇动手机触发。

[0053] 手机程序在收到触发指令后，通过手机扬声器播放经过编码的探针信号音频流以激活门禁控制设备。

[0054] 进一步的，编码的音频流的频段为17kHz～22kHz。

[0055] 门禁端一直处于监听状态，当其接收到探针信号后，立即播放包含其设备唯一标识编码的音频信号。

[0056] 如图3所示，手机正确接收到认证设备的唯一标识号后，检索本地数据权限列表中是否包含该门禁设备的权限授权以及对应的TOPT共享密钥。

[0057] 进一步的，其中本地的权限列表是通过网络下载的方式从远程权限管理系统服务器获取。用户与设备之间的权限关系可以通过权限管理服务器进行管理和修改。

[0058] 如果权限列表中包含该门禁设备的权限，则可根据TOTP算法结合共享密钥和当前时间生成一次性认证密钥。

[0059] 手机端将一次性密钥通过实时音频流进行编码。

[0060] 手机APP将生成的一次性密钥进行音频实时流编码并进行音频循环播放。

[0061] 门禁设备一直处于监听状态，接收并校验手机端播放的包含一次性密钥的编码音频流，然后对正确接收到的音频进行解码，解码后得到的手机APP传输给门禁设备的一次性密钥。

[0062] 门禁设备通过门禁设备本地存储的TOTP共享密钥参数，结合时间同步模块输出的时间，使用TOTP算法，生成TOTP一次性密钥，并将该密钥与解码后手机端发送的密钥进行比对，如果比对结果一致，则控制门锁打开，认证成功。若比对结果不一致，则无门锁动作，认证失败。

[0063] 门禁设备将认证结果进行实时音频流编码并播放。

[0064] 手机端接受门禁设备播放的认证结果音频流，进行解码并展示认证结果。

[0065] 手机APP正确接受步骤72播放的认证结果音频流后，进行解码，并且在显示设备上展示认证结果。

[0066] 手机APP对认证结果进行日志记录，并且在有网络的情况下上传系统中央服务器备案。

[0067] 认证场景在现实生活中有多处应用场景，如考勤、签到等等，不仅限于本发明中的门禁场景较佳实施例。

[0068] 以上所述仅为本发明的较佳实施例，并不用于限制本发明，凡依本发明申请专利范围所做的均等变化、修饰与改进等，均应在本发明的保护范围之内。

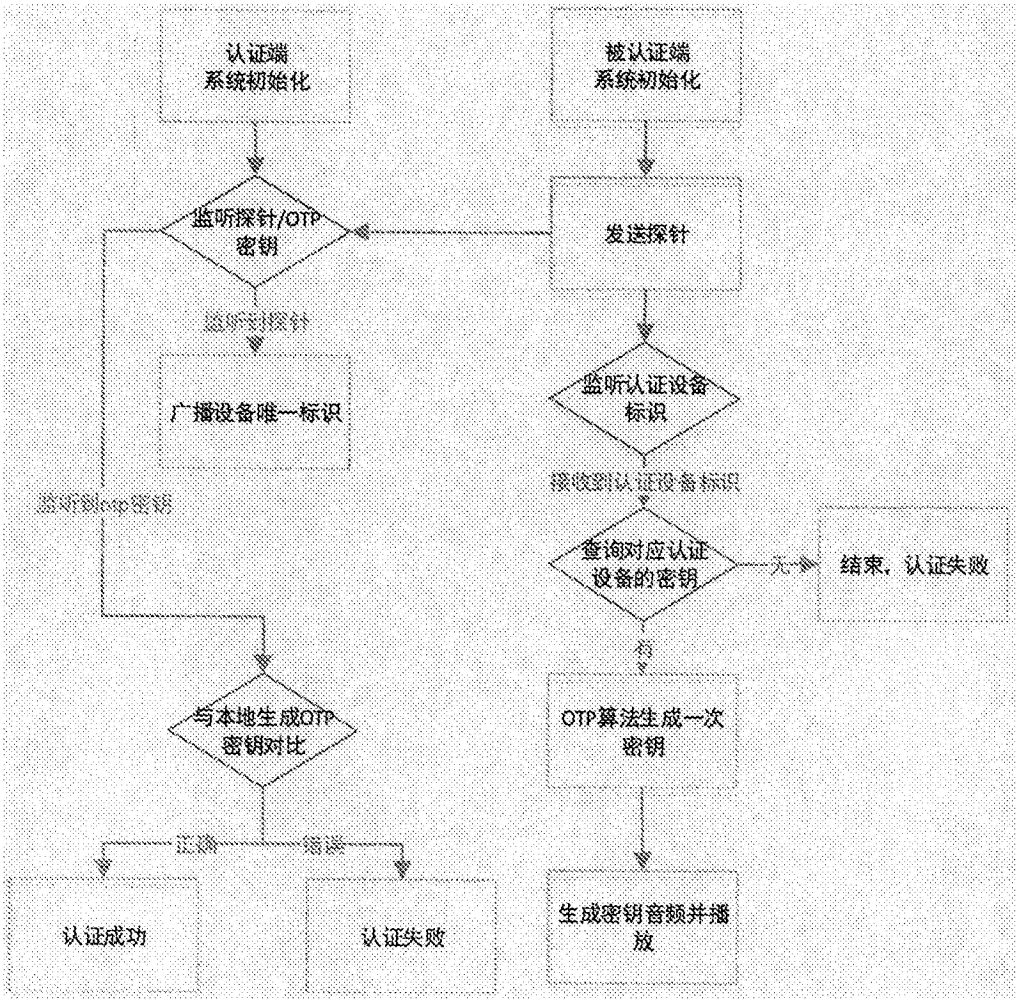

认证端
系统初始化
被认证端
系统初始化
监听探针/OTP
密钥
发送探针
监听到探针
广播设备唯一标识
监听认证设备
标识
接收到认证设备标识
查询对应认证
设备的密钥
无
结束，认证失败
有
监听到otp密钥
与本地生成OTP
密钥对比
OTP算法生成一次
密钥
匹配
不匹配
认证成功
认证失败
生成密钥音频并播
放

图1

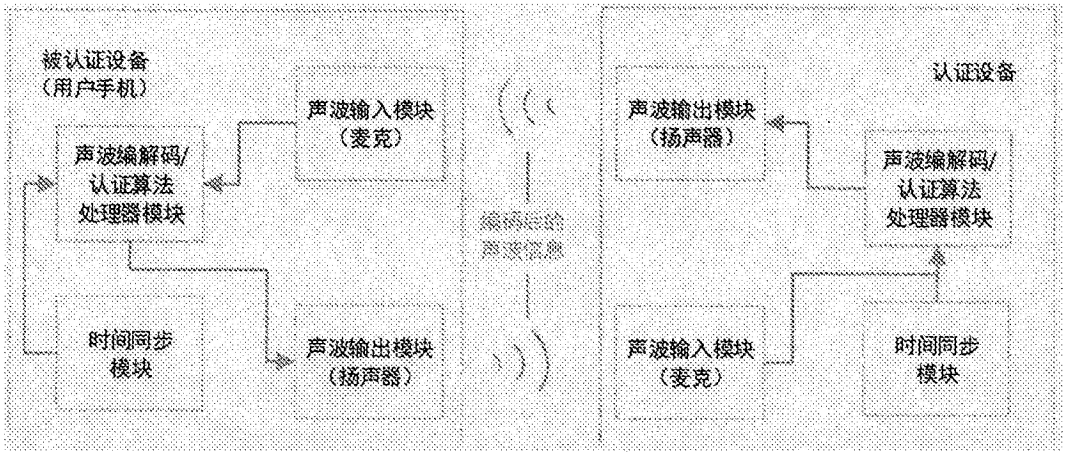

被认证设备
（用户手机）
声波输入模块
（麦克）
声波编解码/
认证算法
处理器模块
时间同步
模块
声波输出模块
（扬声器）
认证设备
声波输出模块
（扬声器）
声波编解码/
认证算法
处理器模块
声波输入模块
（麦克）
时间同步
模块

图2

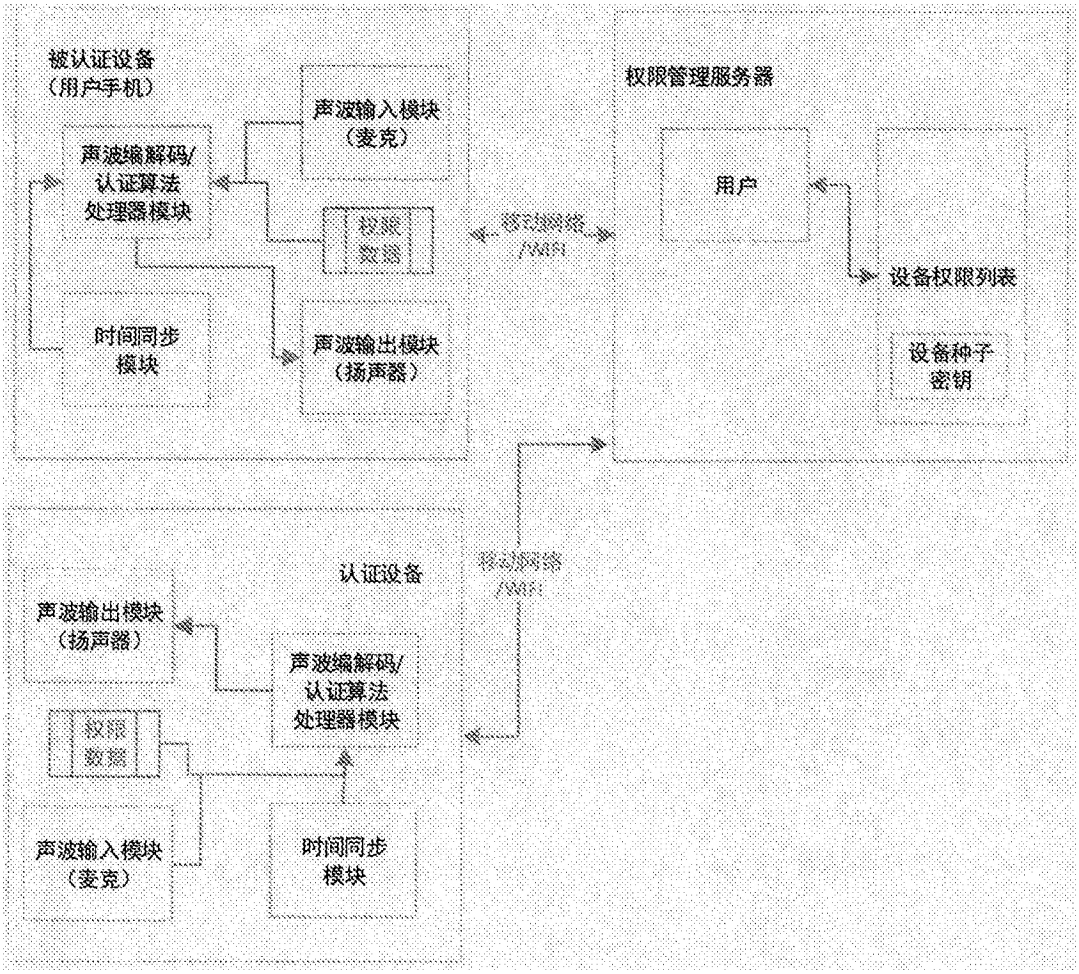

被认证设备
（用户手机）
声波输入模块
（麦克）
声波编解码/
认证算法
处理器模块
权限
数据
时间同步
模块
声波输出模块
（扬声器）
移动网络
/WiFi
权限管理服务器
用户
设备权限列表
设备种子
密钥
移动网络
/WiFi
认证设备
声波输出模块
（扬声器）
声波编解码/
认证算法
处理器模块
权限
数据
声波输入模块
（麦克）
时间同步
模块

图3