(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 111542028 A
(43)申请公布日 2020.08.14

(21)申请号 202010303713.0

(22)申请日 2020.04.17

(71)申请人 软通动力信息技术(集团)有限公司
地址 100193 北京市海淀区西北旺东路10号院东区16号楼5层502

(72)发明人 陈佩雷 樊彦斌

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

(51)Int.Cl.
H04W 4/80(2018.01)
H04W 12/00(2009.01)
H04W 12/06(2009.01)

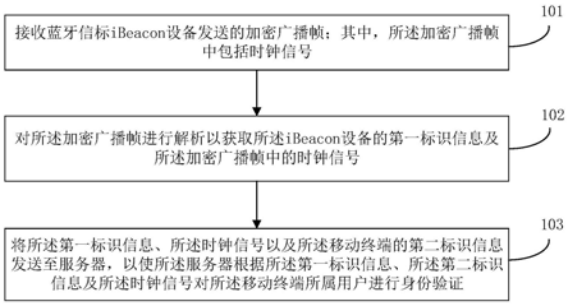
权利要求书2页 说明书8页 附图3页

(54)发明名称

身份验证方法、装置、存储介质、移动终端及服务器

(57)摘要

本发明实施例公开了一种身份验证方法、装置、存储介质、移动终端及服务器。所述方法包括:接收蓝牙信标iBeacon设备发送的加密广播帧;其中,所述加密广播帧中包括时钟信号;对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号;将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至服务器,以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证。通过采用上述技术方案,能够有效防止iBeacon信号被模拟,从而保证了身份验证的有效性和真实性。



CN 111542028 A

1.一种身份验证方法,其特征在于,应用于移动终端,包括:

接收蓝牙信标iBeacon设备发送的加密广播帧;其中,所述加密广播帧中包括时钟信号;

对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号;

将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至服务器,以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证。

2.根据权利要求1所述的方法,其特征在于,对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号,包括:

对所述加密广播帧进行解析以获取所述加密广播帧中的通用唯一识别码UUID及所述加密广播帧中的时钟信号,并将所述UUID作为所述iBeacon设备的第一标识信息。

3.根据权利要求2所述的方法,其特征在于,对所述加密广播帧进行解析以获取所述加密广播帧中的通用唯一识别码UUID及所述加密广播帧中的时钟信号,包括:

对所述加密广播帧进行解密操作生成解密广播帧;

从所述解密广播帧中提取UUID及时钟信号。

4.根据权利要求1所述的方法,其特征在于,所述加密广播帧中还包括时钟参考值和时钟信号调整频率,所述时钟信号为基于所述时钟参考值及所述时钟信号调整频率确定的信号。

5.一种身份验证方法,其特征在于,应用于服务器,包括:

接收移动终端发送的iBeacon设备的第一标识信息、所述移动终端的第二标识信息及时钟信号;其中,所述第一标识信息及所述时钟信号为所述移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取的信息;

根据所述第一标识信息、第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证。

6.根据权利要求5所述的方法,其特征在于,根据所述第一标识信息、第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证,包括:

获取iBeacon设备的标识信息与待进行身份验证用户的标识信息间的对应关系;

将所述第一标识信息及所述第二标识信息与所述对应关系进行匹配;

当所述第一标识信息及所述第二标识信息与所述对应关系匹配成功时,判断所述时钟信息与参考时钟信息的差值是否小于预设阈值,若是,则确定所述移动终端所属用户身份验证成功;其中,所数参考时钟信息为基于时钟参考值和时钟信号调整频率确定的信息。

7.一种身份验证装置,其特征在于,应用于移动终端,包括:

加密广播帧接收模块,用于接收iBeacon设备发送的加密广播帧;其中,所述加密广播帧中包括时钟信号;

加密广播帧解析模块,用于对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号;

信息发送模块,用于将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至服务器,以使所述服务器根据所述第一标识信息、所述第二标识信息及所述

时钟信号对所述移动终端所属用户进行身份验证。

8.一种身份验证装置,其特征在于,应用于服务器,包括:

信息接收模块,用于接收移动终端发送的iBeacon设备的第一标识信息、所述移动终端的第二标识信息及时钟信号;其中,所述第一标识信息及所述时钟信号为所述移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取的信息;

身份验证模块,用于根据所述第一标识信息、第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证。

9.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-4任一所述的身份验证方法。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求5-6任一所述的身份验证方法。

11.一种移动终端,其特征在于,包括存储器,处理器及存储在存储器上并可在处理器运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1-4任一所述的身份验证方法。

12.一种服务器,其特征在于,包括存储器,处理器及存储在存储器上并可在处理器运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求5-6任一所述的身份验证方法。

身份验证方法、装置、存储介质、移动终端及服务器

技术领域

[0001] 本发明实施例涉及通信技术领域，尤其涉及身份验证方法、装置、存储介 质、移动终端及服务器。

背景技术

[0002] 随着商家和企业的快速发展，越来越多的业务场景需要对用户身份进行验 证。比如，考勤、会议签到、车库停车或者其他商品或服务的消费需要用户亲 自在现场，为了方便用户进行身份验证，基于蓝牙信标的iBeacon的移动系统 (如移动考勤系统)应运而生。然而，如何保证身份验证的有效性和真实性变 得至关重要。

发明内容

[0003] 本发明实施例提供一种身份验证方法、装置、存储介质、移动终端及服务 器，以保证身份验证的有效性和真实性。

[0004] 第一方面，本发明实施例提供了一种身份验证方法，应用于移动终端，该 方法包括：

[0005] 接收蓝牙信标iBeacon设备发送的加密广播帧；其中，所述加密广播帧中 包括时钟信号；

[0006] 对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识信息及所 述加密广播帧中的时钟信号；

[0007] 将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发 送至服务器，以使所述服务器根据所述第一标识信息、所述第二标识信息及所 述时钟信号对所述移动终端所属用户进行身份验证。

[0008] 第二方面，本发明实施例提供了一种身份验证方法，应用于服务器，该方 法包括：

[0009] 接收移动终端发送的iBeacon设备的第一标识信息、所述移动终端的第二 标识信息及时钟信号；其中，所述第一标识信息及所述时钟信号为所述移动终 端对接收的iBeacon设备发送的加密广播帧进行解析获取的信息；

[0010] 根据所述第一标识信息、第二标识信息及所述时钟信号对所述移动终端所 属用户进行身份验证。

[0011] 第三方面，本发明实施例还提供了一种身份验证装置，应用于移动终端， 该装置包括：

[0012] 加密广播帧接收模块，用于接收iBeacon设备发送的加密广播帧；其中， 所述加密广播帧中包括时钟信号；

[0013] 加密广播帧解析模块，用于对所述加密广播帧进行解析以获取所述iBeacon 设备的第一标识信息及所述加密广播帧中的时钟信号；

[0014] 信息发送模块，用于将所述第一标识信息、所述时钟信号以及所述移动终 端的第二标识信息发送至服务器，以使所述服务器根据所述第一标识信息、所 述第二标识信息及

所述时钟信号对所述移动终端所属用户进行身份验证。

[0015] 第四方面，本发明实施例还提供了一种身份验证装置，应用于服务器，该 装置包括：

[0016] 信息接收模块，用于接收移动终端发送的iBeacon设备的第一标识信息、所述移动终端的第二标识信息及时钟信号；其中，所述第一标识信息及所述时 钟信号为所述移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取 的信息；

[0017] 身份验证模块，用于根据所述第一标识信息、第二标识信息及所述时钟信 号对所述移动终端所属用户进行身份验证。

[0018] 第五方面，本发明实施例提供了一种计算机可读存储介质，其上存储有计 算机程序，该程序被处理器执行时实现如本发明实施例第一方面提供的身份验 证方法。

[0019] 第六方面，本发明实施例提供了一种计算机可读存储介质，其上存储有计 算机程序，该程序被处理器执行时实现如本发明实施例第二方面提供的身份验 证方法。

[0020] 第七方面，本发明实施例提供了一种移动终端，包括存储器、处理器及存 储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机 程序时实现如本发明实施例第一方面提供的身份验证方法。

[0021] 第八方面，本发明实施例提供了一种服务器，包括存储器、处理器及存储 在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程 序时实现如本发明实施例第二方面提供的身份验证方法。

[0022] 本发明实施例中提供的身份验证方案，接收蓝牙信标iBeacon设备发送的 加密广播帧；其中，所述加密广播帧中包括时钟信号；对所述加密广播帧进行 解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号； 将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至 服务器，以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时 钟信号对所述移动终端所属用户进行身份验证。通过采用上述技术手段，能够 有效防止iBeacon信号被模拟，从而保证了身份验证的有效性和真实性。

附图说明

[0023] 图1为本发明实施例提供的一种身份验证方法的流程示意图；

[0024] 图2为本发明实施例提供的另一种身份验证方法的流程示意图；

[0025] 图3为本发明实施例提供的一种身份验证装置的结构框图；

[0026] 图4为本发明实施例提供的另一种身份验证装置的结构框图；

[0027] 图5为本发明实施例提供的一种移动终端的结构框图；

[0028] 图6为本发明实施例提供的一种服务器的结构框图。

具体实施方式

[0029] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此 处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需 要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结 构。

[0030] 图1为本发明实施例提供的一种身份验证方法的流程示意图，该方法可以 由身份

验证装置执行，其中该装置可由软件和/或硬件实现，一般可集成在移动 终端中。如图1所示，该方法包括：

[0031] 步骤101、接收蓝牙信标iBeacon设备发送的加密广播帧；其中，所述加密 广播帧中包括时钟信号。

[0032] 在本发明实施例中，iBeacon设备可以为一个也可以为多个，其中，iBeacon 设备的数量可以根据身份验证区域的大小进行设置，身份验证区域越大，设置 的iBeacon设备的数量可以越多；身份验证区域越小，设置的iBeacon设备的数 量可以越少。iBeacon设备可以以预设频率周期性地发送广播帧，在iBeacon设 备的信号范围内支持低功耗蓝牙的移动终端均可以接收到iBeacon设备发送的 广播帧。

[0033] 在本发明实施例中，iBeacon设备发送的广播帧为加密广播帧，在加密广播 帧中包含有时钟信号。示例性的，iBeacon设备上电后，时钟信号将按设置的时 钟基准值启动计数，将时钟基准值存放至广播帧中，并按照预设加密算法对广 播帧加密，生成加密广播帧，然后按预设的频率发送加密广播帧。可选的，所 述加密广播帧中还包括时钟参考值和时钟信号调整频率，所述时钟信号为基于 所述时钟参考值及所述时钟信号调整频率确定的信号。其中，时钟参考值可以 理解为时钟信号的初始值，时钟参考值按照时钟信号调整频率增加1，生成时 钟信号。对UUID、时钟信号、时钟参考值及时钟信号调整频率加密，可将加密结果分成两段分别存放至Major和Minor字段中，进而生成加密广播帧，并 将加密广播帧按照设定频率广播出去。其中，加密广播帧的格式如下所示：

[0034]

iBeacon prefix （9bytes）	Proximity UUID （16bytes）	Major （2bytes）	Minor （2bytes）	TX power （1bytes）

[0035] 步骤102、对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识 信息及所述加密广播帧中的时钟信号。

[0036] 在本发明实施例中，对加密广播帧进行解析，根据解析结果获取iBeacon 设备的标识信息及当前时钟信号，并将iBeacon设备的标识信息记作第一标识 信息。

[0037] 可选的，对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识 信息及所述加密广播帧中的时钟信号，包括：对所述加密广播帧进行解析以获 取所述加密广播帧中的通用唯一识别码UUID及所述加密广播帧中的时钟信号， 并将所述UUID作为所述iBeacon设备的第一标识信息。可选的，对所述加密 广播帧进行解析以获取所述加密广播帧中的通用唯一识别码UUID及所述加密 广播帧中的时钟信号，包括：对所述加密广播帧进行解密操作生成解密广播帧； 从所述解密广播帧中提取UUID及时钟信号。

[0038] 示例性的，对加密广播帧进行解密生成解密广播帧，并从解密广播帧中提 取UUID和时钟信号，其中，解密时可以先拼接Major和Minor字段，再输入 decode(param)函数得到当前时钟信号。

[0039] 步骤103、将所述第一标识信息、所述时钟信号以及所述移动终端的第二 标识信息发送至服务器，以使所述服务器根据所述第一标识信息、所述第二标 识信息及所述时钟信号对所述移动终端所属用户进行身份验证。

[0040] 在本发明实施例中，将iBeacon设备的标识信息(第一标识信息)、当前 时钟信号以及移动终端的标识信息(第二标识信息)发送至后台服务器，以使 后台服务器根据iBeacon设备的标识信息、当前时钟信号以及移动终端的标识 信息对移动终端所属用户进行身份验证。示例性的，移动终端的标识信息可以 为集成电路卡识别码(ICCID)。其中，在后台服务器中存储有iBeacon设备的 标识信息与待进行身份验证用户的标识信息间的对应关系，后台服务器将 iBeacon设备的第一标识信息以及移动终端的第二标识信息与上述对应关系进 行匹配，若匹配成功，则进一步计算当前时钟信号与参考时钟信号间的差值，当差值小于预设阈值，则表明移动终端所属用户身份验证成功。如在考勤领域， 如满足上述条件则表明用户打卡成功。

[0041] 其中，参考时钟信号为基于时钟参考值和时钟调整频率确定的信息。示例 性的，iBeacon设备上电后，管理员要在一分钟内通过其自己的移动终端采集初 始加密广播帧，并对初始加密广播帧解码后将时钟参考值和时钟调整频率上报 至后台服务器端，通知后台服务器该iBeacon设备已复位要求重新计数，后台 卡服务器保存时钟参考值和时钟调整频率，以方便在进行身份验证时根时钟参 考值和时钟调整频率得到参考时钟信号。

[0042] 需要说明的是，受iBeacon设备的广播周期的影响，移动终端解析得出的 当前时钟信号与服务器中的参考时钟信号(可以理解为时钟信号的真实计数值) 会有一定偏差，再加上网络传输时延，存在累计时间差，所以当当前时钟信号 与服务器中的参考时钟信号间的差值小于一定阈值时，在则可认为用户身份验 证成功。

[0043] 可以理解的是，在实际应用中，广播帧有可能被篡改或有可能被解析，从 而影响身份验证的真实性和有效性，而在本发明实施例中，对广播帧进行加密， 并且在加密广播帧中包含随着时间实时变化的时钟信号，使得广播帧不容易被 篡改或被解析，能够有效提供身份验证的真实性和有效性。

[0044] 本发明实施例中提供的身份验证方法，接收蓝牙信标iBeacon设备发送的 加密广播帧；其中，加密广播帧中包括时钟信号；对加密广播帧进行解析以获 取iBeacon设备的第一标识信息及加密广播帧中的时钟信号；将第一标识信息、时钟信号以及移动终端的第二标识信息发送至服务器，以使服务器根据第一标 识信息、第二标识信息及时钟信号对移动终端所属用户进行身份验证。通过采 用上述技术手段，能够有效防止iBeacon信号被模拟，从而保证了身份验证的 有效性和真实性。

[0045] 图2为本发明实施例提供的一种身份验证方法的流程示意图，该方法可以 由身份验证装置执行，其中该装置可由软件和/或硬件实现，一般可集成在服务 器中。如图2所示，该方法包括：

[0046] 步骤201、接收移动终端发送的iBeacon设备的第一标识信息、所述移动终 端的第二标识信息及时钟信号；其中，所述第一标识信息及所述时钟信号为所 述移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取的信息。

[0047] 在本发明实施例中，iBeacon设备可以为一个也可以为多个，其中，iBeacon 设备的数量可以根据身份验证区域的大小进行设置，身份验证区域越大，设置 的iBeacon设备的数量可以越多；身份验证区域越小，设置的iBeacon设备的数 量可以越少。iBeacon设备可以以预设频率周期性地发送广播帧，在iBeacon设 备的信号范围内支持低功耗蓝牙的移动终端均可以接收到iBeacon设备发送的 广播帧。

[0048] 在本发明实施例中，iBeacon设备发送的广播帧为加密广播帧，在加密广播 帧中包含有时钟信号。示例性的，iBeacon设备上电后，时钟信号将按设置的时 钟基准值启动计数，将时钟基准值存放至广播帧中，并按照预设加密算法对广 播帧加密，生成加密广播帧，然后按预设的频率发送加密广播帧。可选的，所 述加密广播帧中还包括时钟参考值和时钟信号调整频率，所述时钟信号为基于 所述时钟参考值及所述时钟信号调整频率确定的信号。其中，时钟参考值可以 理解为时钟信号的初始值，时钟参考值按照时钟信号调整频率增加1，生成时 钟信号。对UUID、时钟信号、时钟参考值及时钟信号调整频率加密，可将加密结果分成两段分别存放至Major和Minor字段中，进而生成加密广播帧，并 将加密广播帧按照设定频率广播出去。移动终端接收到加密广播帧后对加密广 播帧进行解析，根据解析结果获取iBeacon设备的标识信息及当前时钟信号， 并将iBeacon设备的标识信息记作第一标识信息。

[0049] 可选的，对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识 信息及所述加密广播帧中的时钟信号，包括：对所述加密广播帧进行解析以获 取所述加密广播帧中的通用唯一识别码UUID及所述加密广播帧中的时钟信号， 并将所述UUID作为所述iBeacon设备的第一标识信息。可选的，对所述加密 广播帧进行解析以获取所述加密广播帧中的通用唯一识别码UUID及所述加密 广播帧中的时钟信号，包括：对所述加密广播帧进行解密操作生成解密广播帧； 从所述解密广播帧中提取UUID及时钟信号。示例性的，对加密广播帧进行解 密生成解密广播帧，并从解密广播帧中提取UUID和时钟信号，其中，解密时 可以先拼接Major和Minor字段，再输入decode(param)函数得到当前时钟信号。 移动终端将解析获取的iBeacon设备的第一标识信息、时钟信号及移动终端的 第二标识信息发送至服务器，服务器接收移动终端发送的第一标识信息、第二 标识信息及时钟信号。

[0050] 步骤202、根据所述第一标识信息、第二标识信息及所述时钟信号对所述 移动终端所属用户进行身份验证。

[0051] 可选的，根据所述第一标识信息、第二标识信息及所述时钟信号对所述移 动终端所属用户进行身份验证，包括：获取iBeacon设备的标识信息与待进行 身份验证用户的标识信息间的对应关系；将所述第一标识信息及所述第二标识 信息与所述对应关系进行匹配；当所述第一标识信息及所述第二标识信息与所 述对应关系匹配成功时，判断所述时钟信息与参考时钟信息的差值是否小于预 设阈值，若是，则确定所述移动终端所属用户身份验证成功；其中，所数参考 时钟信息为基于时钟参考值和时钟信号调整频率确定的信息。

[0052] 示例性的，移动终端的标识信息可以为集成电路卡识别码(ICCID)。其 中，在后台服务器中存储有iBeacon设备的标识信息与待进行身份验证用户的 标识信息间的对应关系，后台服务器将iBeacon设备的第一标识信息以及移动 终端的第二标识信息与上述对应关系进行匹配，若匹配成功，则进一步计算当 前时钟信号与参考时钟信号间的差值，当差值小于预设阈值，则表明移动终端 所属用户身份验证成功。如在考勤领域，如满足上述条件则表明用户打卡成功。

[0053] 其中，参考时钟信号为基于时钟参考值和时钟调整频率确定的信息。示例 性的，iBeacon设备上电后，管理员要在一分钟内通过其自己的移动终端采集初 始加密广播帧，并对初始加密广播帧解码后将时钟参考值和时钟调整频率上报 至后台服务器端，通知后台服务器该iBeacon设备已复位要求重新计数，后台 卡服务器保存时钟参考值和时钟调整

频率,以方便在进行身份验证时根时钟参 考值和时钟调整频率得到参考时钟信号。

[0054] 需要说明的是,受iBeacon设备的广播周期的影响,移动终端解析得出的 当前时钟信号与服务器中的参考时钟信号(可以理解为时钟信号的真实计数值) 会有一定偏差,再加上网络传输时延,存在累计时间差,所以当当前时钟信号 与服务器中的参考时钟信号间的差值小于一定阈值时,在则可认为用户身份验 证成功。

[0055] 本发明实施例中提供的身份验证方法,接收移动终端发送的iBeacon设备 的第一标识信息、移动终端的第二标识信息及时钟信号;其中,第一标识信息 及时钟信号为移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取 的信息;根据第一标识信息、第二标识信息及时钟信号对移动终端所属用户进 行身份验证。通过采用上述技术手段,能够有效防止iBeacon信号被模拟,从 而保证了身份验证的有效性和真实性。

[0056] 图3为本发明实施例提供的一种身份验证装置的结构框图,该装置可由软 件和/或硬件实现,一般集成在移动终端中,可通过执行身份验证方法来进行身 份验证。如图3所示,该装置包括:

[0057] 加密广播帧接收模块301,用于接收iBeacon设备发送的加密广播帧;其中, 所述加密广播帧中包括时钟信号;

[0058] 加密广播帧解析模块302,用于对所述加密广播帧进行解析以获取所述 iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号;

[0059] 信息发送模块303,用于将所述第一标识信息、所述时钟信号以及所述移 动终端的第二标识信息发送至服务器,以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证。

[0060] 本发明实施例中提供的身份验证装置,接收蓝牙信标iBeacon设备发送的 加密广播帧;其中,所述加密广播帧中包括时钟信号;对所述加密广播帧进行 解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号; 将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至 服务器,以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时 钟信号对所述移动终端所属用户进行身份验证。通过采用上述技术手段,能够 有效防止iBeacon信号被模拟,从而保证了身份验证的有效性和真实性。

[0061] 可选的,所述加密广播帧解析模块,包括:

[0062] 加密广播帧解析单元,用于对所述加密广播帧进行解析以获取所述加密广 播帧中的通用唯一识别码UUID及所述加密广播帧中的时钟信号,并将所述 UUID作为所述iBeacon设备的第一标识信息。

[0063] 可选的,所述加密广播帧解析单元,用于:

[0064] 对所述加密广播帧进行解密操作生成解密广播帧;

[0065] 从所述解密广播帧中提取UUID及时钟信号。

[0066] 可选的,所述加密广播帧中还包括时钟参考值和时钟信号调整频率,所述 时钟信号为基于所述时钟参考值及所述时钟信号调整频率确定的信号。

[0067] 图4为本发明实施例提供的一种身份验证装置的结构框图,该装置可由软 件和/或硬件实现,一般集成在服务器中,可通过执行身份验证方法来进行身份 验证。如图4所示,该装置包括:

[0068] 信息接收模块401,用于接收移动终端发送的iBeacon设备的第一标识信息、所述移动终端的第二标识信息及时钟信号;其中,所述第一标识信息及所述时 钟信号为所述移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取 的信息;

[0069] 身份验证模块402,用于根据所述第一标识信息、第二标识信息及所述时 钟信号对所述移动终端所属用户进行身份验证。

[0070] 本发明实施例中提供的身份验证装置,接收移动终端发送的iBeacon设备 的第一标识信息、所述移动终端的第二标识信息及时钟信号;其中,所述第一 标识信息及所述时钟信号为所述移动终端对接收的iBeacon设备发送的加密广 播帧进行解析获取的信息;根据所述第一标识信息、第二标识信息及所述时钟 信号对所述移动终端所属用户进行身份验证。通过采用上述技术手段,能够有 效防止iBeacon信号被模拟,从而保证了身份验证的有效性和真实性。

[0071] 可选的,所述身份验证模块,用于:

[0072] 获取iBeacon设备的标识信息与待进行身份验证用户的标识信息间的对应 关系;

[0073] 将所述第一标识信息及所述第二标识信息与所述对应关系进行匹配;

[0074] 当所述第一标识信息及所述第二标识信息与所述对应关系匹配成功时,判 断所述时钟信息与参考时钟信息的差值是否小于预设阈值,若是,则确定所述 移动终端所属用户身份验证成功;其中,所数参考时钟信息为基于时钟参考值 和时钟信号调整频率确定的信息。

[0075] 本发明实施例还提供一种包含计算机可执行指令的存储介质,所述计算机 可执行指令在由计算机处理器执行时用于执行第一方面或第二方面提供的身份 验证方法。

[0076] 存储介质——任何的各种类型的存储器设备或存储设备。术语“存储介质”旨在包括:安装介质,例如CD-ROM、软盘或磁带装置;计算机系统存储器或 随机存取存储器,诸如DRAM、DDRRAM、SRAM、EDORAM,兰巴斯 (Rambus)RAM等;非易失性存储器,诸如闪存、磁介质(例如硬盘或光存储); 寄存器或其它相似类型的存储器元件等。存储介质可以还包括其它类型的存储 器或其组合。另外,存储介质可以位于程序在其中被执行的第一计算机系统中, 或者可以位于不同的第二计算机系统中,第二计算机系统通过网络(诸如因特网) 连接到第一计算机系统。第二计算机系统可以提供程序指令给第一计算机用于 执行。术语“存储介质”可以包括可以驻留在不同位置中(例如在通过网络连接的 不同计算机系统中)的两个或更多存储介质。存储介质可以存储可由一个或多个 处理器执行的程序指令(例如具体实现为计算机程序)。

[0077] 当然,本发明实施例所提供的一种包含计算机可执行指令的存储介质,其 计算机可执行指令不限于如上所述的身份验证操作,还可以执行本发明任意实 施例所提供的身份验证方法中的相关操作。

[0078] 本发明实施例提供了一种移动终端,该移动终端中可集成本发明实施例第 三方面提供的身份验证装置。图5为本发明实施例提供的一种移动终端的结构 框图。移动终端500可以包括:存储器501,处理器502及存储在存储器501 上并可在处理器运行的计算机程序,所述处理器502执行所述计算机程序时实 现如本发明实施例第一方面所述的身份验证方法。

[0079] 本发明实施例中提供的移动终端,接收蓝牙信标iBeacon设备发送的加密 广播

帧;其中,所述加密广播帧中包括时钟信号;对所述加密广播帧进行解析 以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号;将 所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至服 务器,以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时钟 信号对所述移动终端所属用户进行身份验证。通过采用上述技术手段,能够有 效防止iBeacon信号被模拟,从而保证了身份验证的有效性和真实性。

[0080] 本发明实施例提供了一种服务器,该服务器中可集成本发明实施例第四方 面提供的身份验证装置。图6为本发明实施例提供的一种服务器的结构框图。服务器600可以包括:存储器601,处理器602及存储在存储器601上并可在 处理器运行的计算机程序,所述处理器602执行所述计算机程序时实现如本发 明实施例第二方面所述的身份验证方法。

[0081] 本发明实施例中提供的服务器,接收移动终端发送的iBeacon设备的第一 标识信息、所述移动终端的第二标识信息及时钟信号;其中,所述第一标识信 息及所述时钟信号为所述移动终端对接收的iBeacon设备发送的加密广播帧进 行解析获取的信息;根据所述第一标识信息、第二标识信息及所述时钟信号对 所述移动终端所属用户进行身份验证。通过采用上述技术手段,能够有效防止 iBeacon信号被模拟,从而保证了身份验证的有效性和真实性。

[0082] 上述实施例中提供的身份验证装置、存储介质、移动终端及服务器可执行 本发明任意实施例所提供的身份验证方法,具备执行该方法相应的功能模块和 有益效果。未在上述实施例中详尽描述的技术细节,可参见本发明任意实施例 所提供的身份验证方法。

[0083] 注意,上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员 会理解,本发明不限于这里所述的特定实施例,对本领域技术人员来说能够进 行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此,虽 然通过以上实施例对本发明进行了较为详细的说明,但是本发明不仅仅限于以 上实施例,在不脱离本发明构思的情况下,还可以包括更多其他等效实施例, 而本发明的范围由所附的权利要求范围决定。

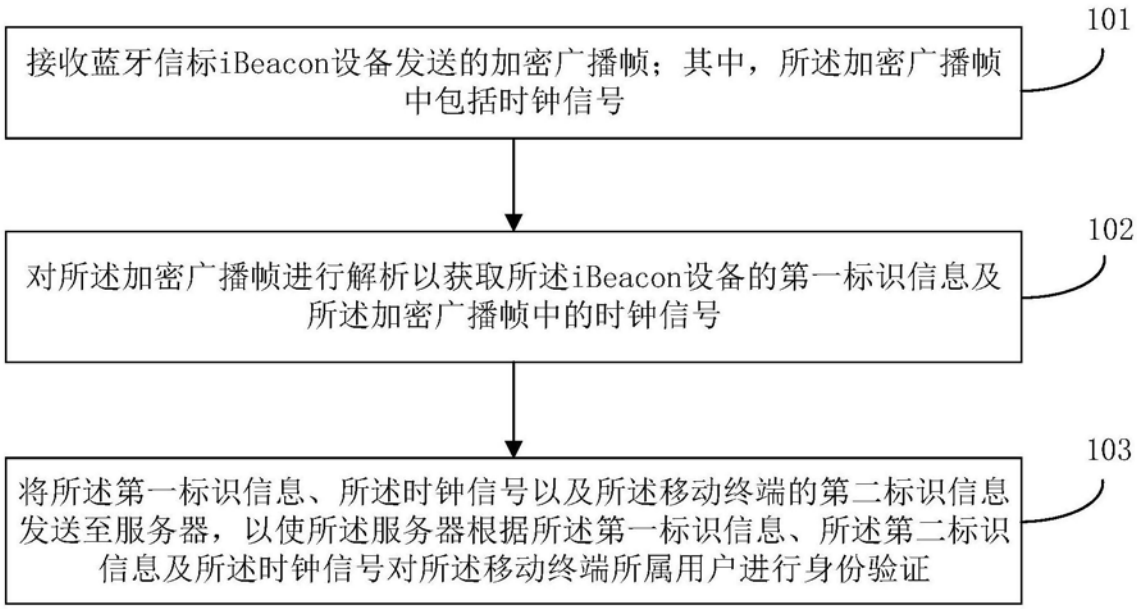

101
接收蓝牙信标iBeacon设备发送的加密广播帧；其中，所述加密广播帧中包括时钟信号
102
对所述加密广播帧进行解析以获取所述iBeacon设备的第一标识信息及所述加密广播帧中的时钟信号
103
将所述第一标识信息、所述时钟信号以及所述移动终端的第二标识信息发送至服务器，以使所述服务器根据所述第一标识信息、所述第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证

图1

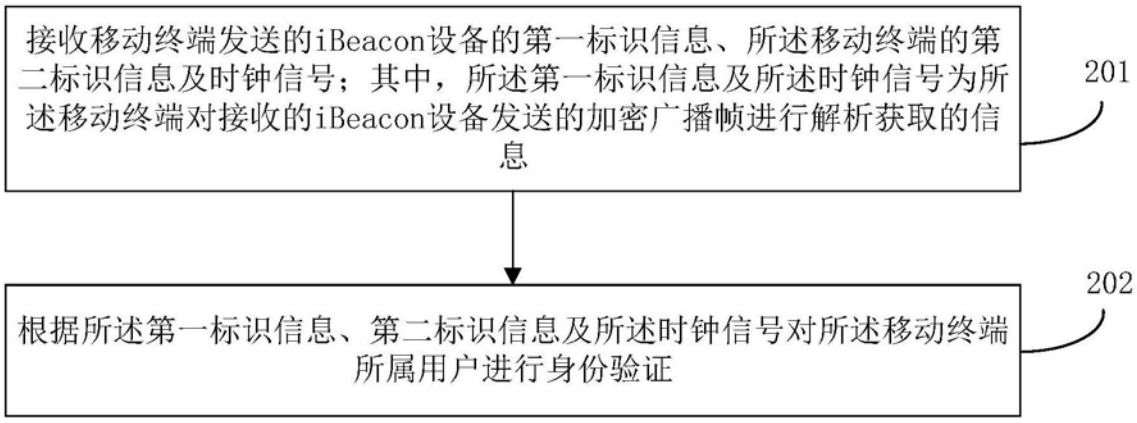

接收移动终端发送的iBeacon设备的第一标识信息、所述移动终端的第二标识信息及时钟信号；其中，所述第一标识信息及所述时钟信号为所述移动终端对接收的iBeacon设备发送的加密广播帧进行解析获取的信息
201
根据所述第一标识信息、第二标识信息及所述时钟信号对所述移动终端所属用户进行身份验证
202

图2

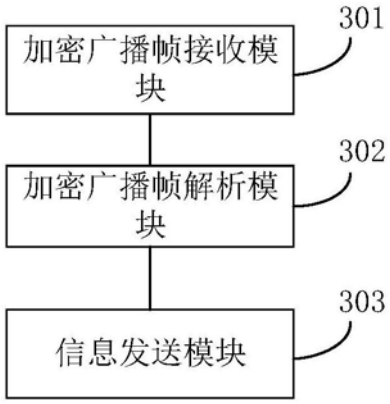

301
加密广播帧接收模块
302
加密广播帧解析模块
303
信息发送模块

图3

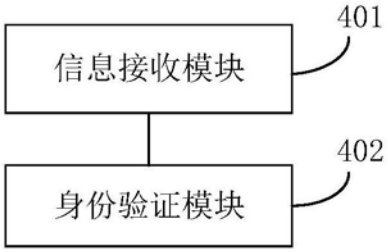

401
信息接收模块
402
身份验证模块

图4

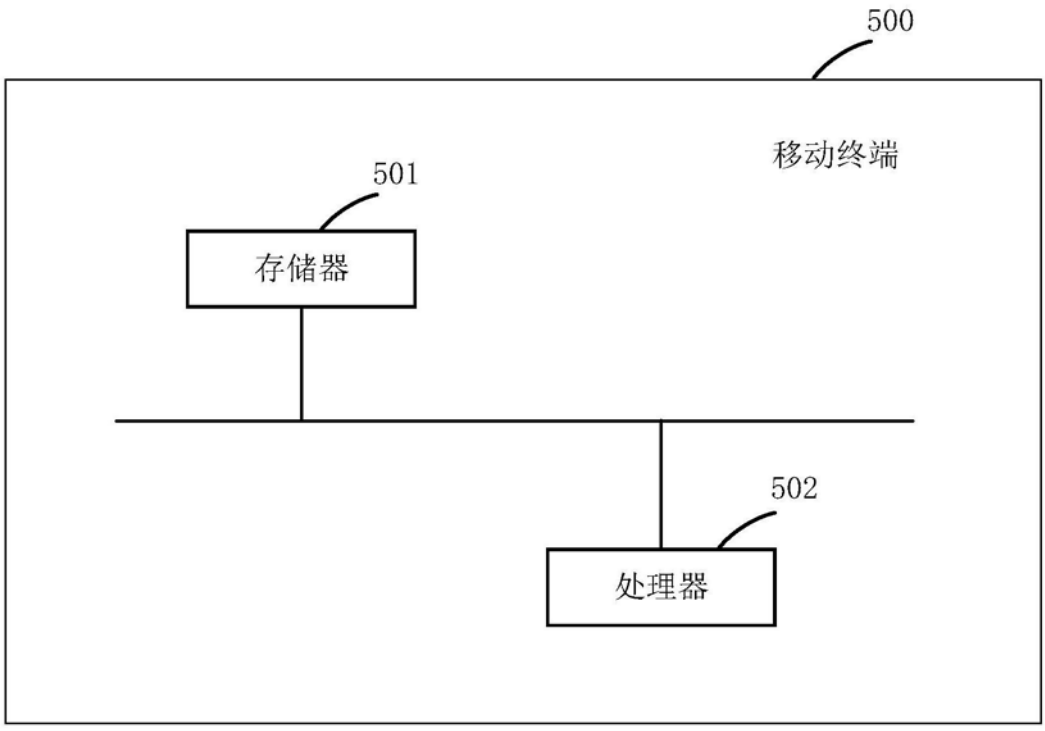

500
移动终端
501
存储器
502
处理器

图5

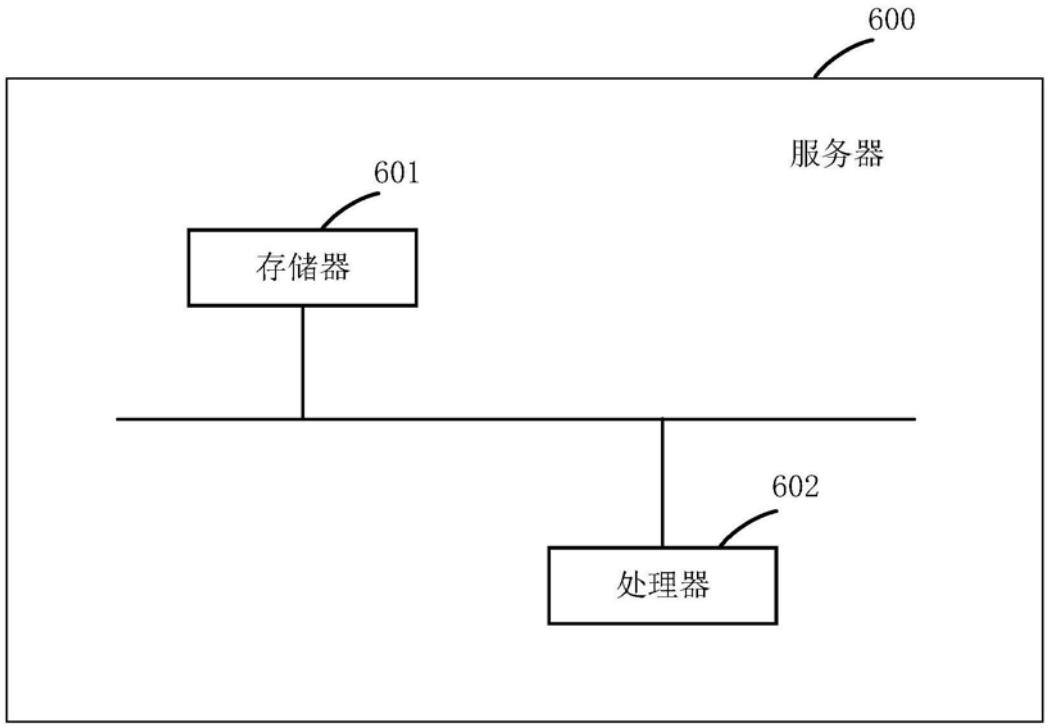


图6