(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 108569250 A
(43)申请公布日 2018.09.25

(21)申请号 201810293027.2

(22)申请日 2018.03.30

(71)申请人 上海汽车集团股份有限公司
地址 200438 上海市杨浦区军工路2500号

(72)发明人 章彪

(74)专利代理机构 上海科琪专利代理有限责任公司 31117
代理人 郑明辉

(51)Int.Cl.
B60R 25/24(2013.01)
G07C 9/00(2006.01)

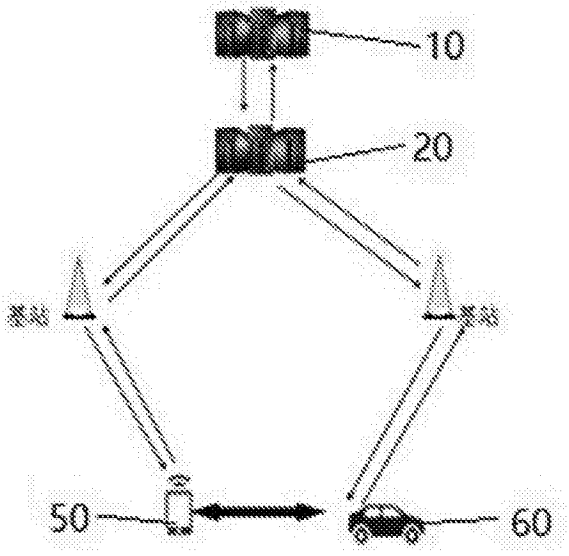
权利要求书2页 说明书7页 附图2页

(54)发明名称

基于共享汽车的蓝牙钥匙的自动授权方法

(57)摘要

本发明公开了一种基于共享汽车的蓝牙钥匙的自动授权方法，包括数据信息平台(10)、车辆(60)及业务处理授权平台(20)；业务处理授权平台与数据信息平台、移动终端设备(50)和车辆连接；车辆作为车载通讯设备(70)和车身控制部件及执行单元(80)的载体，车载通讯设备与车身控制部件及执行单元连接；控制方法包括：步骤1：用户通过移动终端设备进行注册，业务处理授权平台一对一绑定用户信息；步骤2：用户通过移动终端设备登陆；步骤3：通过业务处理授权平台自动授权；本发明能以更加安全和方便的形式授权蓝牙钥匙到移动终端设备，供共享汽车用户使用。



CN 108569250 A

1.一种基于共享汽车的蓝牙钥匙的自动授权方法，其特征是：包括：

数据信息平台(10)，是拥有驾驶员身份信息和驾驶资格信息及两种信息的一致性匹配的平台；

车辆(60)，作为车载通讯设备(70)和车身控制部件及执行单元(80)的载体，车载通讯设备(70)与车身控制部件及执行单元(80)连接；

及业务处理授权平台(20)，分别与数据信息平台(10)、移动终端设备(50)和车辆(60)双向通信连接；

其控制方法如下：

步骤1：用户通过移动终端设备(50)进行注册，业务处理授权平台(20)一对一绑定用户信息；

步骤2：用户通过移动终端设备(50)登陆；

步骤3：登陆完成后通过业务处理授权平台(20)进行自动授权；

步骤3.1：业务处理授权平台(20)基于用户的实时位置在移动终端设备(50)上的显示周围能被授权的车辆(60)，移动终端设备(50)发送授权请求；

步骤3.2：业务处理授权平台(20)收到授权请求后判断登陆口令是否有效来验证是否是合法用户，如果是合法用户，则执行步骤3.3，如果登陆口令无效，则拒绝并通知移动终端设备(50)；

步骤3.3：判断关联的驾驶员信息是否有效，若驾驶员信息有效，则实时查询车辆(60)的状态，车载通讯设备(70)反馈车辆(60)状态，若驾驶员信息无效，返回错误代码到移动终端设备(50)，授权流程终止；

步骤3.4：如果车辆(60)无故障，业务处理授权平台(20)产生授权信息并且先后下发到车载通讯设备(70)和移动终端设备(50)；

步骤3.5：车载通讯设备(70)通过比较接收到来自移动终端设备(50)的蓝牙钥匙和自己接受到的蓝牙密钥是否一致来判断移动终端设备(50)是否是合法的钥匙拥有者，如果一致，根据同步到车载通讯设备(70)中的用户权限来判断用户的操作权限是否合法，如果合法，予以响应，如果不合法，不予以响应；如果不一致，该用户为非法钥匙拥有者，不予以响应。

2.根据权利要求1所述的基于共享汽车的蓝牙钥匙的自动授权方法，其特征是：在所述的步骤1中，还包括如下分步骤：

步骤1.1，用户使用移动终端设备(50)提交用户信息到业务处理授权平台(20)；

步骤1.2，业务处理授权平台(20)接收到用户请求后，验证是否包含用户的驾驶信息，如果包含，则用户的驾驶信息被转发到数据信息平台(10)；如果不包含，返回步骤1.1；

步骤1.3，数据信息平台(10)负责验证驾驶信息的真实性以及数据一致性，并将结果反馈到业务处理授权平台(20)，如果信息真实且一致，则执行步骤1.4，若驾驶信息无效或者用户没有提供该信息，则执行步骤1.5；

步骤1.4，业务处理授权平台(20)将驾驶员信息和用户信息做一对一的绑定关系，并且存储用户名和密码以及绑定关系；

步骤1.5，业务处理授权平台(20)存储用户名和密码，并且标识为非绑定关系。

3.根据权利要求2所述的基于共享汽车的蓝牙钥匙的自动授权方法，其特征是：在所述

的步骤1.4中，同一个驾驶员信息只能绑定一个用户名，如果业务处理授权平台(20)检测到不同的用户名试图绑定已经被绑定的驾驶员信息，那么该行为将会被拒绝。

4.根据权利要求1所述的基于共享汽车的蓝牙钥匙的自动授权方法，其特征是：在所述的步骤2中，还包括如下分步骤：

步骤2.1：用户通过移动终端设备(50)发起第一次登陆请求，其中只包含用户名，业务处理授权平台(20)为该次登陆生成一个密钥对，并将公钥下发到移动终端设备(50)，自己持有私钥；

步骤2.2：移动终端设备(50)将用户名和利用公钥加密后的密码传递到业务处理授权平台(20)，业务处理授权平台(20)利用私钥将密码解密，并验证数据中的用户名和密码信息是否匹配，若匹配，则执行步骤2.3，若不匹配，则无法登陆；

步骤2.3：基于用户非敏感信息生成一个口令，以后移动终端设备(50)的每次请求将携带该口令；

步骤2.4：业务处理授权平台(20)根据对应的密钥和用户信息，验证口令的有效性，并确定不是伪造的请求，并且每次请求时该口令以密文形式传输。

5.根据权利要求1所述的基于共享汽车的蓝牙钥匙的自动授权方法，其特征是：在所述的步骤3.4中，只有在成功下发授权信息到车载通讯设备(70)后，才能下发授权信息到移动终端设备(50)；如果成功下发授权信息到车载通讯设备(70)，且下发授权信息到移动终端设备(50)失败，需要通知车载通讯设备(70)，车载通讯设备(70)将已经获取的蓝牙密钥置为无效；如果下发授权信息到车载通讯设备(70)失败或下发到移动终端设备(50)失败，那么授权终止并且由用户业务处理授权平台(20)通知移动终端设备(50)。

6.根据权利要求1所述的基于共享汽车的蓝牙钥匙的自动授权方法，其特征是：步骤3所述的授权无时间限制，由用户通过移动终端设备(50)发起终止授权，业务处理授权平台(20)实时向车载通讯设备(70)查询车辆状态，如果车辆状态正常，那么同意终止授权，并通知移动终端设备(50)和车载通讯设备(70)。

基于共享汽车的蓝牙钥匙的自动授权方法

技术领域

[0001] 本发明涉及一种共享汽车的钥匙授权方式，尤其涉及一种基于共享汽车的蓝牙钥匙的自动授权方法。

背景技术

[0002] 伴随着城市化的进程带来的是城市人口的激增和城市道路的拥塞，道路拥塞极大地阻碍了社会经济活动的正常进展，造成社会资源和能源的巨大浪费和日常生活的极大不便，伴随着自动驾驶研发的进步和共享经济模式的逐步推广，共享汽车必然成为一种人们可以接受的出行方式，它可以降低汽车持有总量，但是提高了单车使用频率和减少汽车占用的城市道路以及土地资源，丰富和方便了人们的出行，也有助于解决交通拥堵的顽疾。

[0003] 但是如何方便地使用共享汽车，尤其是如何安全地共享汽车的车辆钥匙，鲜有专利详细论及这个问题。

[0004] 中国专利号CN105490996A的专利公开了一种车辆蓝牙钥匙的授权系统和方法，所述系统包括：车辆的信息站、被授权移动终端、授权移动终端和服务器，信息站用于将车辆的识别信息发送至服务器；服务器用于接收被授权移动终端发送的申请信息，并根据车辆的识别信息将申请信息发送至授权移动终端，以及接收授权移动终端发送的授权信息，并将授权信息发送至被授权移动终端；授权移动终端用于在验证申请信息合法后，生成授权信息，并将授权信息发送至服务器；被授权移动终端用于根据自身的识别码和标识信息以及车辆的车牌号生成申请信息，并将申请信息发送至服务器，以及根据授权信息控制车辆。

[0005] 以上专利实现了蓝牙钥匙的一套安全授权方法，但是安全的应用场景应该被限定在授权者和被授权者社会属性的可信任关系的范围，而且授权中的关键的身份验证需要依赖其它手段例如其它通讯软件工具的安全通信和身份可靠的基础上。在安全性上仍然有缺失和使用上的不够便捷性。

[0006] 安全上的缺失表现在：

(A)授权者的用户名和密码被传递到被授权者，对于授权者拥有大批量车辆的情况已经严重不适用，并且会危及其它车辆的安全状态，如果被授权的移动通信设备安全状态不佳，可能造成授权移动设备用户名和密码的泄露。

[0007] (B)授予请求者权限的验证过程是基于对车辆本身信息和移动设备本身的身份信息的共享，而非请求者本身的身份，但是车辆信息(例如VIN码)和移动设备标识信息(例如手机号)都是容易获得数据。

[0008] (C)授予的权限除了时间上的差异，没有表现出权限本身的差异细分。

[0009] 便捷性上的缺失表现在：

(A)授权请求者需要输入车辆信息编码串，十分不便。

[0010] (B)授权审批者需要人工审批，这对于大规模并发的多时域用车授权请求显然不适用。

发明内容

[0011] 本发明的目的在于提供一种基于共享汽车的蓝牙钥匙的自动授权方法，能以更加安全和方便的形式授权蓝牙钥匙到移动终端设备，供共享汽车用户使用。

[0012] 本发明是这样实现的：

一种基于共享汽车的蓝牙钥匙的自动授权方法，包括：

数据信息平台，是拥有驾驶员身份信息和驾驶资格信息及两种信息的一致性匹配的平台；

车辆，作为车载通讯设备和车身控制部件及执行单元的载体，车载通讯设备与车身控制部件及执行单元连接；

及业务处理授权平台，分别与数据信息平台、移动终端设备和车辆双向通信连接；

其控制方法如下：

步骤1：用户通过移动终端设备进行注册，业务处理授权平台一对一绑定用户信息；

步骤2：用户通过移动终端设备登陆；

步骤3：登陆完成后通过业务处理授权平台进行自动授权；

步骤3.1：业务处理授权平台基于用户的实时位置在移动终端设备上的显示周围能被授权的车辆，移动终端设备发送授权请求；

步骤3.2：业务处理授权平台收到授权请求后判断登陆口令是否有效来验证是否是合法用户，如果是合法用户，则执行步骤3.3，如果登陆口令无效，则拒绝并通知移动终端设备；

步骤3.3：判断关联的驾驶员信息是否有效，若驾驶员信息有效，则实时查询车辆的状态，车载通讯设备反馈车辆状态；若驾驶员信息无效，返回错误代码到移动终端设备，授权流程终止；

步骤3.4：如果车辆无故障，业务处理授权平台产生授权信息并且先后下发到车载通讯设备和移动终端设备；

步骤3.5：车载通讯设备通过比较接收到来自移动终端设备的蓝牙钥匙和自己接受到的蓝牙密钥是否一致来判断移动终端设备是否是合法的钥匙拥有者，如果一致，根据同步到车载通讯设备中的用户权限来判断用户的操作权限是否合法，如果合法，予以响应，如果不合法，不予以响应；如果不一致，该用户为非法钥匙拥有者，不予以响应。

[0013] 在所述的步骤1中，还包括如下分步骤：

步骤1.1，用户使用移动终端设备提交用户信息到业务处理授权平台；

步骤1.2，业务处理授权平台接收到用户请求后，验证是否包含用户的驾驶信息，如果包含，则用户的驾驶信息被转发到数据信息平台；如果不包含，返回步骤1.1；

步骤1.3，数据信息平台负责验证驾驶信息的真实性以及数据一致性，并将结果反馈到业务处理授权平台，如果信息真实且一致，则执行步骤1.4，若驾驶信息无效或者用户没有提供该信息，则执行步骤1.5；

步骤1.4，业务处理授权平台将驾驶员信息和用户信息做一对一的绑定关系，并且存储用户名和密码以及绑定关系；

步骤1.5，业务处理授权平台存储用户名和密码，并且标识为非绑定关系。

[0014] 在所述的步骤1.4中，同一个驾驶员信息只能绑定一个用户名，如果业务处理授权平台检测到不同的用户名试图绑定已经被绑定的驾驶员信息，那么该行为将会被拒绝。

[0015] 在所述的步骤2中，还包括如下分步骤：

步骤2.1：用户通过移动终端设备发起第一次登陆请求，其中只包含用户名，业务处理授权平台为该次登陆生成一个密钥对，并将公钥下发到移动终端设备，自己持有私钥；

步骤2.2：移动终端设备将用户名和利用公钥加密后的密码传递到业务处理授权平台，业务处理授权平台利用私钥将密码解密，并验证数据中的用户名和密码信息是否匹配，若匹配，则执行步骤2.3，若不匹配，则无法登陆；

步骤2.3：基于用户非敏感信息生成一个口令，以后移动终端设备的每次请求将携带该口令；

步骤2.4：业务处理授权平台根据对应的密钥和用户信息，验证口令的有效性，并确定不是伪造的请求，并且每次请求时该口令以密文形式传输。

[0016] 在所述的步骤3.4中，只有在成功下发授权信息到车载通讯设备后，才能下发授权信息到移动终端设备；如果成功下发授权信息到车载通讯设备，且下发授权信息到移动终端设备失败，需要通知车载通讯设备，车载通讯设备将已经获取的蓝牙密钥置为无效；如果下发授权信息到车载通讯设备失败或下发到移动终端设备失败，那么授权终止并且由用户业务处理授权平台通知移动终端设备。

[0017] 步骤3所述的授权无时间限制，由用户通过移动终端设备发起终止授权，业务处理授权平台实时向车载通讯设备查询车辆状态，如果车辆状态正常，那么同意终止授权，并通知移动终端设备和车载通讯设备。

[0018] 本发明在授权时候基于用户身份的可靠性进行授权，而用户身份(用户名、密码及包括驾驶员身份和驾驶资格的驾驶员信息)的可靠性，在用户注册和登陆时候进行验证；授权请求者可以请求不同的权限，例如将权限集合分成车门的开锁上锁，车门的开锁上锁车辆启动两个权限集合，授予不同的权限确保了车辆的不同安全状态；授予请求者的密钥是一次性的，授权终止后密钥无效，且下一次授权密钥不同与上次授权密钥。本发明基于用户身份的合法性验证后采用自动授权，无需人工审批；申请授权过程无需与实际物理车辆接触，仅仅需要基于在移动终端设备上选择的车辆，发起授权即可。本发明确保了用户使用车辆的便捷性和车辆的安全性，为用户共享出行方案提供了可行性蓝牙钥匙授权方案。

[0019] 本发明能以更加安全和方便的形式授权蓝牙钥匙到移动终端设备，供共享汽车用户使用。

附图说明

[0020] 图1是本发明基于共享汽车的蓝牙钥匙的自动授权方法的系统拓扑图；

图2是本发明基于共享汽车的蓝牙钥匙的自动授权方法的注册流程图；

图3是本发明基于共享汽车的蓝牙钥匙的自动授权方法的授权流程图；

图4是本发明基于共享汽车的蓝牙钥匙的自动授权方法的授权后车辆使用流程图。

[0021] 图中，10数据信息平台，20业务处理授权平台，50移动终端设备，60车辆，70车载通讯设备，80车身控制部件及执行单元。

具体实施方式

[0022] 下面结合附图和具体实施例对本发明作进一步说明。

[0023] 请参见附图1，一种基于共享汽车的蓝牙钥匙的自动授权方法，包括：

数据信息平台10，是拥有驾驶员身份信息和驾驶资格信息及两种信息的一致性匹配的平台；

业务处理授权平台20，分别与数据信息平台10、移动终端设备50和车辆60双向通信连接，数据信息平台10、移动终端设备50和车辆60在业务处理授权平台20上进行交互，它具有一定的存储能力，需要存储用户信息包括用户名和密码以及驾驶员信息ID(通过该ID可以关联到驾驶员数据信息平台10中的驾驶员信息)，驾驶员信息是否有效等信息；此外业务处理授权平台20还存储车辆信息<主要包括车辆ID、车辆的配置(例如动力配置、车身颜色)和车辆身份信息(例如VIN码)>、车载通讯设备70上报的动态车辆位置、车载通讯设备70监控到的车辆状态(例如车辆是否存在故障)以及车辆的授权状态(如果处于授权状态还包括授予的权限)。业务处理授权平台20与数据信息平台10之间可通过移动通信数据网络(3G/4G)连接或物理线缆的连接；移动终端设备50和车辆60之间可通过蓝牙无线连接；

及车辆60，作为车载通讯设备70和车身控制部件及执行单元80的载体，车载通讯设备70与车身控制部件及执行单元80连接；车载通讯设备70指具有移动数据通信能力，连接到车辆总线并且具有蓝牙通信能力的设备，身控制部件以及执行单元80指车身控制单元(例如BCM<body control module>)以及具体执行单元(例如车辆门锁控制器)；其控制方法如下：

请参见附图2，步骤1：用户通过移动终端设备50进行注册，业务处理授权平台20一对一绑定用户信息。

[0024] 步骤1.1，用户使用移动终端设备50提交用户的信息到业务处理授权平台20；

步骤1.2，业务处理授权平台20接收到用户请求后，验证是否包含用户的驾驶信息，如果包含，则用户的驾驶信息(包括驾驶员身份信息以及驾驶资格)被转发到数据信息平台10；如果不包含，返回步骤1.1；

步骤1.3，数据信息平台10平台负责验证驾驶信息的真实性以及数据一致性，并将结果反馈到业务处理授权平台20，如果信息真实且一致，则执行步骤1.4，若驾驶信息无效或者用户没有提供该信息，则执行步骤1.5；

步骤1.4，业务处理授权平台20将该驾驶员信息和用户信息(用户名和密码)做一对一的绑定关系(有效的驾驶员信息ID)，并且存储用户名和密码以及绑定关系(有效的驾驶员信息ID)；

步骤1.5，业务处理授权平台20存储用户名和密码，并且标识为非绑定关系。

[0025] 在所述的步骤1.1中，用户的信息包括用户名、密码及用户的驾驶信息(包括驾驶员身份信息和驾驶资格)。

[0026] 在所述的步骤1.4中，同一个驾驶员信息(包括驾驶员身份信息和驾驶资格)只能绑定一个用户名，如果检测到不同的用户名试图绑定已经被绑定的驾驶员信息，那么该行为将会被拒绝。

[0027] 用户提供真实有效的身份信息(例如身份证和驾驶证)后，以及绑定了支付软件账

号，通过多重身份标志以及身份标识的一致性确认了用户信息的安全有效性。

[0028] 步骤2：用户通过移动终端设备50登陆。

[0029] 步骤2.1：用户通过移动终端设备50发起第一次登陆请求，其中只包含用户名，业务处理授权平台20基于RSA算法为该次登陆生成一个密钥对，并将公钥下发到移动终端设备50，自己持有私钥；RSA算法是一种非对称加密算法，在公开密钥加密和电子商业中RSA算法被广泛使用。

[0030] 步骤2.2：移动终端设备50将用户名和利用公钥加密后的密码传递到业务处理授权平台20，业务处理授权平台20利用私钥将其密码解密，并验证数据中的用户名和密码信息是否匹配，若匹配，则执行步骤2.3，若不匹配，则无法登陆；

步骤2.3：利用HMACSHA256算法基于用户非敏感信息生成一个口令，以后移动终端设备50的每次请求将携带该口令；HMAC是密钥相关的哈希运算消息认证码，HMAC运算利用哈希算法，以一个密钥和一个消息为输入，生成一个消息摘要作为输出。哈希值用作表示大量数据的固定大小的唯一值。数据的少量更改会在哈希值中产生不可预知的大量更改。SHA256算法的哈希值大小为 256 位。

[0031] 步骤2.4：业务处理授权平台20根据对应的密钥和用户信息，验证口令的有效性，并确定不是伪造的请求的，并且每次请求时该口令以密文形式传输；

在所述的步骤2.3中，所述的口令包含两部分，一部分为用户非敏感信息，另一部分为基于用户非敏感信息和该用户对应的一个密钥串基于HMACSHA256算法生成的签名信息。

[0032] 请参见附图3，步骤3：登陆完成后将通过业务处理授权平台20进行自动授权。

[0033] 步骤3.1：登陆后业务处理授权平台20基于移动终端设备50提交的用户实时位置，在移动终端设备50上的显示用户周围的可以被授权给用户的车辆60，移动终端设备50基于车辆60的显示发送授权请求。为了专注于授权本身，假定显示给用户的所有车辆60，都是无故障状态，并且动力能源充足，也没有被授权到其他用户使用；

步骤3.2：业务处理授权平台20接收到用户的授权请求后判断登陆口令是否有效，来验证是否是合法用户，如果是合法用户，则执行步骤3.3，如果无效，则直接予以拒绝并通知到移动终端设备50；

步骤3.3：判断关联的驾驶员信息是否有效，若驾驶员信息有效，则实时查询车辆60的状态(是否有车辆故障)，并且由车载通讯设备70对车辆60的状态进行反馈，车辆60无故障，执行步骤3.4；若驾驶员信息无效，返回错误代码到移动终端设备50，授权流程终止。这里车载通讯设备70本身按照一定时间间隔向业务处理授权平台20提交车辆60状态信息(主要指是否有故障)，但是实时性不够或者不排除因为网络延迟故障信息还没有上传到业务处理授权平台20；

步骤3.4：业务处理授权平台20产生授权信息，并且将其先后下发到车载通讯设备70和移动终端设备50；

请参见附图4，步骤3.5：车载通讯设备70通过比较接收到来自移动终端设备50的蓝牙钥匙和自己接受到的蓝牙密钥是否一致，来判断移动终端设备50是否是合法的钥匙拥有者，如果一致，再根据同步到车载通讯设备70中的用户权限来判断用户的操作权限是否合法，如果合法，予以响应，如果不合法，不予以响应；如果不一致，该用户为非法钥匙拥有者，不予以响应，具体地由车载通讯设备70通过汽车总线向车身控制部件及执行单元80发出指

令，并接收执行结果，反馈给移动终端设备50。

[0034] 在所述的步骤3.1中，授权请求包含车辆ID、请求的权限子集合及登陆口令。

[0035] 在所述的步骤3.4中，只有在成功下发授权信息到车载通讯设备70后，才能下发授权信息到移动终端设备50；如果成功下发授权信息到车载通讯设备70，且下发授权信息到移动终端设备50失败(例如下发信息超时)，那么需要通知车载通讯设备70，车载通讯设备70将已经获取的蓝牙密钥(用于操作车辆)置为无效；如果下发授权信息到车载通讯设备70失败或下发到移动终端设备50失败，那么授权终止并且由用户业务处理授权平台20通知移动终端设备50。

[0036] 在所述的步骤3.4中，下发到移动终端设备50和车载通讯设备70的授权信息都包括蓝牙密钥(用于操作车辆)和授予的权限子集。

[0037] 步骤3所述的授权一般无时间限制，由用户来终止授权，终止授权请求包括车辆ID，终止授权请求由移动终端设备50发起，业务处理授权平台20实时向车载通讯设备70查询车辆状态(例如动力是否熄火并且是否停放在安全位置)，如果车辆状态正常，那么同意终止授权，并通知移动终端设备50和车载通讯设备70。

[0038] 在某些情况下为了提高车辆使用率，如果检测到车辆的特定状态(例如已经熄火并且锁车)超过一定时间，并且车辆处于被授权状态，会自动终止该车辆对该用户的授权。

[0039] 在授权的操作中，无论授权时间长短，必然产生一个不同的授权密钥，确保了即使一次使用中密钥泄露，也不会影响下次的安全使用；如果移动终端设备丢失，可以通过验证用户身份后接受置授权密钥无效的请求，避免造成损失；授权的权限有进一步的细分，确保了不同授权状态下车辆的安全状态。

[0040] 在本发明的操作流程中，用户注册认证以后，无需每次借用不同车辆，都需要输入车辆信息，例如VIN码和车牌号。授权的过程由服务器根据用户的认证信息及账户状态(例如信用等)和请求授权车辆的状态，判断是否进行授权，无需人工审核是否进行授权；请求授权无需与实际物理车辆接触，更进一步地讲，无需扫码形式，在使用过程中基于车辆在地图上的位置显示来确定使用车辆；请求授权时支持车辆预定和预览，基于用户的个性化需求和驾驶习惯来进行请求授权。

[0041] 在本发明中，请求授权无需扫码获取车辆密钥，更进一步地讲，在使用过程中基于车辆在地图上的位置显示来确定使用车辆。车辆60可使用高精度GPS，定位精度30cm以下，基于车辆60 400cm x 150cm的长和宽可以近距离在现场基于移动终端设备50上车辆60相对位置和车辆60的本身信息(车身颜色、汽车共享品牌等)准确关联现场车辆。而扫码容易受天气(例如雨天水滴覆盖扫描条码)和光线影响，并且条码的人为破坏会造成无法获取扫码密钥。

[0042] 在请求授权时支持车辆60的预定和预览，基于用户的个性化需求和驾驶习惯，对于车辆60有不同配置(例如车身颜色、动力配置、内饰等)，在用户移动终端设备50上可以展示车辆信息可以以文字或者示意图形式展示，选中示意车辆60后可以进行预定。

[0043] 授权请求者可以请求不同的权限，例如将权限集合分成车门的开锁上锁，车门的开锁上锁车辆启动两个权限集合，在某些情况下，车辆使用者刚刚终止了授权，但是有私人物品遗落在车辆60上，并且车辆此时未授权其他使用者，此时车辆使用者只需要车门的上锁和解锁权限即可，这种授权进一步限定车辆本身的安全状态和用户可能需要支付的成

本。

[0044] 以上仅为本发明的较佳实施例而已，并非用于限定发明的保护范围，因此，凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

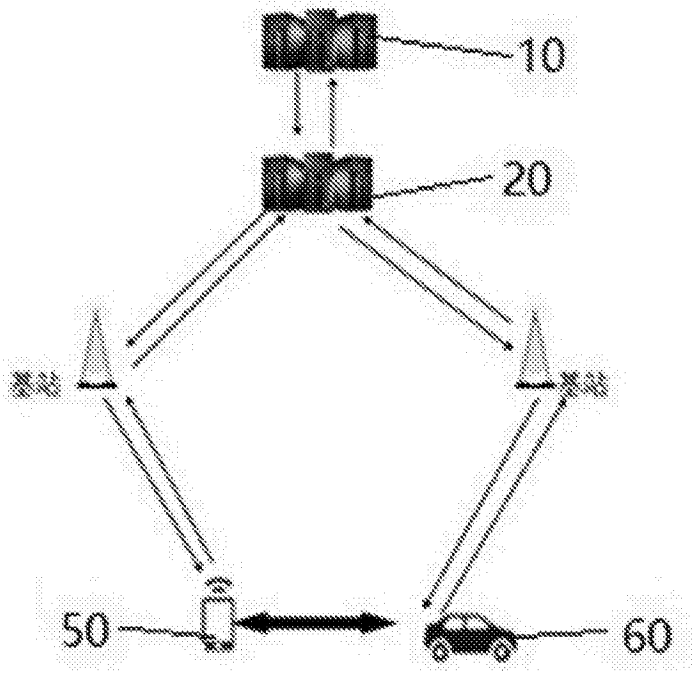


图1

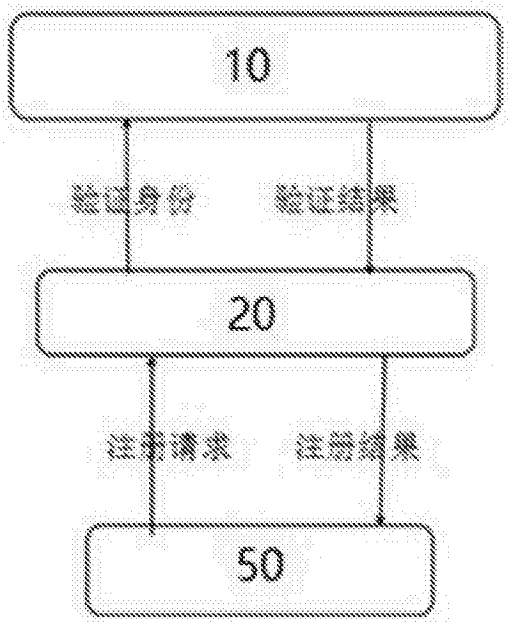


图2

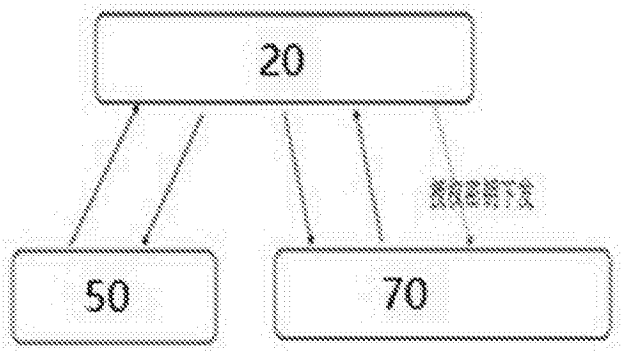


图3

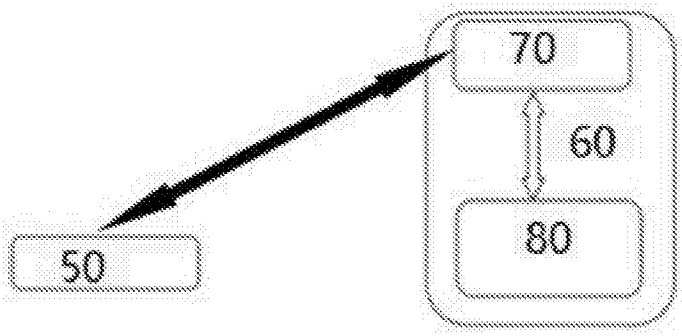


图4