**专利名称：一种支持****位置隐私保护的访问控制方案**

**申请人 ：南京邮电大学**

**发明人：柯昌博、王帅**

**第一发明人身份证号：**

本发明公开了位置隐私保护的访问控制方案，解决了车辆网环境中身份安全和位置隐私泄露的问题。首先，利用虚拟机隔离特征构建位置服务共享隐私保护模型, 根据虚拟机与用户之间的映射关系，对虚拟机的访问策略以及服务分发策略进行建模. 其次，Handle标识替换传统的MAC或IP地址来防止用户身份被篡改；再次，基于属性访问控制策略和信息流模型的动态访问控制算法扩展的SDN网关来保护用户存储在LBS服务虚拟机中的隐私数据，并实现细粒度的数据操作。



1.一种支持位置隐私保护的访问控制方案，包括以下步骤：

步骤 1）系统初始化，本发明通过第三方可信中心TC来管理和引导整个系统的运行，在进行访问控制之前，系统中每个车辆()需要自己唯一的Handle标识以及访问控制策略在可信中心TC进行注册，注册成功后，车辆能获得自身的属性向量以及秘密值。本文提出的基于属性和信息流模型方案，需要同时满足上述定义的三个规则，生成每个车辆的属性向量。

步骤 2）设备注册，每个车辆都会向信任中心 （TC）进行登记注册，只有经过注册的车辆才被认为是可信的安全车辆。如果车辆注册成功，说明车辆的Handle标识在系统中都是唯一且真实存在的。在可信中心TC系统内部分别维护了车辆信息表管理所有车辆的注册信息。

步骤 3）车辆的身份认证，在我们的方案中,由于每个车辆()都申请了Handle标识。可以利用Handle标识唯一性确定车辆在系统中的真实身份。在我们的系统中，在注册阶段可信中心会对车辆具有的属性与车辆的Handle标识的hash值进行异或操作即,将异或操作得到的结果返回给车辆。车辆可以根据自身的Handle标识对结果进行异或操作，车辆获得自身的属性集。即使属性集被系统中某一车辆盗取，由于车辆的Handle标识唯一且在我们系统中我们认为Handle标识不会被攻击者盗取。因此攻击者即使得到了TC中心发给车辆的信息，也不会得到车辆的属性信息。

步骤 4）基于属性的访问控制，为保护用户的位置隐私安全，在对系统中每个车辆进行身份认证后，我们需要在申请访问车辆()中筛选出满足服务提供者()访问策略车辆。只有满足服务提供者访问策略的车辆，服务使用者才被允许访问到相应的虚拟机。辆在向对应的虚拟机发出访问请求时，车辆会携带由信任中心分配的属性向量。由SND控制器分析处理服务使用者是否满足服务提供者规定的访问策略并做出允许访问or拒绝访问决定。

步骤 5）基于信息流模型实现细粒度的数据操作，通过上述基于属性的访问控制后，我们可以确定系统中每个车辆的真实身份，并允许满足服务提供者访问策略的车辆访问相应的虚拟机，拒绝非法用户或恶意用户的访问。我们将位置服务分发策略转化为信息流模型规定每个授权车辆可以访问到哪些服务以及访问的时间，实现细粒度的数据操作，保护隐私数据的安全。

其中所述步骤1）具体如下：

步骤11）首先选取一个用于认证的秘密值s以及e-1个随机整数即，，其中k是一个安全参数，是一个常数。

步骤 12）选择一个安全的加密哈希函数Hash：，随机数作为主密钥。

所述步骤 2）具体如下：

步骤21）首先，系统中每个车辆将自己的Handle标识发送至可信中心TC，可信中心根据每个车辆注册的Handle标识和车辆信息表确定注册车辆是否为系统中唯一存在的真实车辆。同时每个服务提供者()将自己的访问控制策略发送至可信中心。

步骤 22）TC根据系统中注册成功服务提供者的访问控制策略与本文定义的规则生成访问策略矩阵，具体规则如下所示：

在我们访问控制方案中，我们需要将访问策略转换为一个分发矩阵M，矩阵M可以被下面三个规则表示。我们定义是一个单条目矩阵，即.存在矩阵表示访问策略.用表示居正的第一列，用表示矩阵除去第一列的剩余列。

规则1：

访问策略中的每个变量都可以用矩阵表示。

规则2：

对于任意的或结构（OR）即.访问策略和对应的矩阵分别为和，故访问策略P的矩阵可以通过如下方式构造。

规则3：

对于任意的与结构（AND）即. 访问策略和对应的矩阵分别为和，故访问策略P的矩阵可以通过如下方式构造。

根据可信中心选取的秘密值s以及e-1个随机整数即。可信中心计算，并将秘密值返回给系统中的服务提供者。同时计算,返回给注册成功的相应车辆，其中为车辆具有的某一属性，为异或操作，对车辆的Handle标识进行hash操作。

所述步骤 4）具体如下：

步骤 41) 请求流在OVS交换机流表中匹配成功，说明车辆的访问请求已经被处理过并且还在上次处理结果的周期中，因此OVS交换机根据流表规定的动作决定这个流如何处理。如果规定的动作为forward表示此访问车辆满足服务提供者定义的访问策略，若规定的动作为block表示访问车辆为服务提供者定义的恶意用户。

步骤 42）请求流在OVS交换机流表中未能匹配成功，交换机将此信息流作为可疑流发送至控制器，控制器根据访问车辆请求时携带的属性向量判断是否满足服务提供者定义的访问策略。SDN控制器收到OVS交换机发送的可疑流后，从流中获取访问车辆的属性向量 。对于任意一个访问用户具有的属性满足服务提供者定义的访问策略，则存在一个重构向量，使得。因此我们可以根据如下等式得到重构向量：

其中为服务使用者属性向量矩阵，为重构向量，为目标向量。控制器根据计算得到的重构出秘密值s，即

步骤 43）SDN将计算得到的秘密值s发送到服务提供者进行比较。若验证成功则说明此访问车辆满足当前用户定义的访问策略，SDN控制器在根据服务提供者定义的隐私策略规定访问车辆此次授权访问的时间，根据访问车辆的MAC地址和虚拟机的IP地址作为流表项的源MAC地址、目的IP地址和目的MAC地址、源IP地址。下发流表项到OVS交换机允许此次车辆的访问请求。若验证失败，表示访问车辆的属性不满足用户定义的访问策略(非法用户)，控制器将丢弃该信息流拒绝其访问请求。

所述步骤 5）具体如下所示：

步骤 51）我们需要将位置服务分发策略(SRM)转化为信息流模型

其中表示一个信息流规则。

其中是信息流规则的创造者，是系统中车辆的Handle标识，Time表示服务使用者可以访问的时间，,表示管理员创造了这个此信息流规则，表示普通用户创造了此信息流规则，我们默认当有两个规则发生冲突时管理员角色的优先级大于普通用户，即按照管理员创造的信息流规则执行。

步骤 52）访问用户根据信息流规则在规定的时间内访问规定的哪些服务。当访问时间超出规定的时间后，访问用户需要进行重新的身份认证以及查看是否满足数据拥有者的访问策略。满足访问用户定义的访问策略则可以继续访问，否则拒绝其访问请求。

**一种****支持位置隐私保护的访问控制方案**

**技术领域**

本发明提出一种在车辆网环境下支持保护车辆位置隐私服务安全共享的访问控制方案，属于隐私保护、访问控制和身份认证等交叉技术领域。

**背景技术**

近十年来,车对车(V2V)和车对基础设施(V2I)通信技术的迅速发展，车载adhoc网络(VANETs)受到了广泛的关注。现代车辆的发展趋势是配备车载单元(OBU)和路边单元(RSU)。车辆自组织网络(VANET)是智能交通系统(ITS)的关键技术，具有提高安全性和便捷性等优点。然而，它成功的最大挑战之一是位置隐私。随着无线通信、定位技术和智能移动终端的迅速发展，基于地理信息系统(GIS)平台的位置服务(Location-Based Service，LBS)使车辆能够随时获取与空间位置相关的各种信息，车辆的地理位置被用来提供信息和娱乐服务，因为车辆的位置通常表示其上下文信息。车辆可以很容易地获取诸如附近的餐馆、加油站、休息区等信息。用户的位置可能会泄露用户的敏感隐私信息，如兴趣、习惯和健康状况，尤其是当这些隐私信息被对手获取时，会对用户的隐私与安全带来威胁。当VANET和基于位置的服务集成在一起时，LBS服务提供商可以提供很多基于位置的共享服务，如好友位置查询、好友旅行轨迹查询、当前位置实时共享等。然而，在享受LBS便利的服务同时，也有一些挑战需要解决。位置信息是用户最敏感的隐私信息之一，因此具有重要的价值。例如，攻击者窃取用户合法好友的身份,请求用户的位置服务信息，可以从位置信息中推断出许多敏感信息。例如，攻击者可以从医院数据推断出用户的身体状况。此外，攻击者根据用户的旅行规划,很容易得到用户生活行为隐私。这些对用户都造成了极大的安全隐患，防止恶意攻击者获取敏感位置信息非常重要。

目前国内外研究者对数据共享方案有基于属性加密(ABE)和基于身份认证的访问控制，其中基于属性加密，它允许人们根据适用于数据的访问控制策略来加密每个数据项。然而，除了密钥托管问题外，ABE还存在吊销问题,因为只要用户被吊销，就应该更新提供给现有用户的私钥。我们希望可以实现动态保护每个用户的隐私数据，当一个非授权用户变为授权用户时，我们要求能够动态检测到访问用户权限变化，并拒绝非授权用户的访问请求。同时基于ABE加密的文件一旦被一个用户解密，这个用户就可以对这个文件做任何操作，然而我们希望有些数据不能被复制或下载。基于身份验证的访问控制有基于角色的访问控制(RBAC)或基于身份的访问控制(IBAC)在VANET中，在面临身份盗窃时易受攻击，即如果合法用户的身份（私钥）被攻击者破解，则攻击者将相应地获得所有合法授权对用户的隐私造成很大的威胁。

基于上述的研究成果本发明将采用不同以往的方案，在车辆自组织网络中我们将Handle标识、线性整数密钥共享与软件定义网络(SDN)相结合保护用户位置服务隐私数据。在我们的方案中，每个用户在LBS服务提供商有一个专用的虚拟机保存自己的位置服务隐私数据。每一个虚拟机都提供一组服务只有满足自己定义访问策略以及服务分发策略的合法用户才能访问，并且每个用户可以定义自己的访问策略，指定哪些用户可以访问自己的哪些服务，拒绝其他非授权的用户则访问。由于虚拟机是一个封闭的系统,因此只有每个虚拟机专属的用户能够访问到存储在虚拟机中的数据，其他人都不能访问.为了能够验证每个用户真实的身份，我们引入了Handle标识唯一确定每个用户的真实身份，同时我们设计一个SDN网关保护每个用户的存储在LBS服务提供商虚拟机中的数据，在SDN网关中我们嵌入了基于属性和信息流模型的动态访问控制算法满足动态环境下对每个用户隐私数据保护，SDN网关根据用户定义的访问策略筛选出满足属性要求的授权用户，根据用户定义的服务分发策略规定每个授权用户可以访问到哪些服务以及访问时间，对非授权的用户网关会阻止他们的访问。

**发明内容**

**技术问题：**发明所要解决的技术问题是设计一种支持位置隐私保护的访问控制方案

，以有效地降低车辆网环境下用户位置隐私数据泄露的风险。

**技术方案：**本发明的一种支持位置隐私保护访问控制方案包括以下步骤：

步骤 1）系统初始化，本发明通过第三方可信中心TC来管理和引导整个系统的运行，在进行访问控制之前，系统中每个车辆()需要自己唯一的Handle标识以及访问控制策略在可信中心TC进行注册，注册成功后，车辆能获得自身的属性向量以及秘密值。本文提出的基于属性和信息流模型方案，需要同时满足上述定义的三个规则，生成每个车辆的属性向量。

步骤 2）设备注册，每个车辆都会向信任中心 （TC）进行登记注册，只有经过注册的车辆才被认为是可信的安全车辆。如果车辆注册成功，说明车辆的Handle标识在系统中都是唯一且真实存在的。在可信中心TC系统内部分别维护了车辆信息表管理所有车辆的注册信息。

步骤 3）车辆的身份认证，在我们的方案中,由于每个车辆()都申请了Handle标识。可以利用Handle标识唯一性确定车辆在系统中的真实身份。在我们的系统中，在注册阶段可信中心会对车辆具有的属性与车辆的Handle标识的hash值进行异或操作即,将异或操作得到的结果返回给车辆。车辆可以根据自身的Handle标识对结果进行异或操作，车辆获得自身的属性集。即使属性集被系统中某一车辆盗取，由于车辆的Handle标识唯一且在我们系统中我们认为Handle标识不会被攻击者盗取。因此攻击者即使得到了TC中心发给车辆的信息，也不会得到车辆的属性信息。

步骤 4）基于属性的访问控制，为保护用户的位置隐私安全，在对系统中每个车辆进行身份认证后，我们需要在申请访问车辆()中筛选出满足服务提供者()访问策略车辆。只有满足服务提供者访问策略的车辆，服务使用者才被允许访问到相应的虚拟机。辆在向对应的虚拟机发出访问请求时，车辆会携带由信任中心分配的属性向量。由SND控制器分析处理服务使用者是否满足服务提供者规定的访问策略并做出允许访问or拒绝访问决定。

步骤 5）基于信息流模型实现细粒度的数据操作，通过上述基于属性的访问控制后，我们可以确定系统中每个车辆的真实身份，并允许满足服务提供者访问策略的车辆访问相应的虚拟机，拒绝非法用户或恶意用户的访问。我们将位置服务分发策略转化为信息流模型规定每个授权车辆可以访问到哪些服务以及访问的时间，实现细粒度的数据操作，保护隐私数据的安全。

其中所述步骤1）具体如下：

步骤11）首先选取一个用于认证的秘密值s以及e-1个随机整数即，，其中k是一个安全参数，是一个常数。

步骤 12）选择一个安全的加密哈希函数Hash：，随机数作为主密钥。

所述步骤 2）具体如下：

步骤21）首先，系统中每个车辆将自己的Handle标识发送至可信中心TC，可信中心根据每个车辆注册的Handle标识和车辆信息表确定注册车辆是否为系统中唯一存在的真实车辆。同时每个服务提供者()将自己的访问控制策略发送至可信中心。

步骤 22）TC根据系统中注册成功服务提供者的访问控制策略与本文定义的规则生成访问策略矩阵，具体规则如下所示：

在我们访问控制方案中，我们需要将访问策略转换为一个分发矩阵M，矩阵M可以被下面三个规则表示。我们定义是一个单条目矩阵，即.存在矩阵表示访问策略.用表示居正的第一列，用表示矩阵除去第一列的剩余列。

规则1：

访问策略中的每个变量都可以用矩阵表示。

规则2：

对于任意的或结构（OR）即.访问策略和对应的矩阵分别为和，故访问策略P的矩阵可以通过如下方式构造。

规则3：

对于任意的与结构（AND）即. 访问策略和对应的矩阵分别为和，故访问策略P的矩阵可以通过如下方式构造。

根据可信中心选取的秘密值s以及e-1个随机整数即。可信中心计算，并将秘密值返回给系统中的服务提供者。同时计算,返回给注册成功的相应车辆，其中为车辆具有的某一属性，为异或操作，对车辆的Handle标识进行hash操作。

所述步骤 4）具体如下：

步骤 41) 请求流在OVS交换机流表中匹配成功，说明车辆的访问请求已经被处理过并且还在上次处理结果的周期中，因此OVS交换机根据流表规定的动作决定这个流如何处理。如果规定的动作为forward表示此访问车辆满足服务提供者定义的访问策略，若规定的动作为block表示访问车辆为服务提供者定义的恶意用户。

步骤 42）请求流在OVS交换机流表中未能匹配成功，交换机将此信息流作为可疑流发送至控制器，控制器根据访问车辆请求时携带的属性向量判断是否满足服务提供者定义的访问策略。SDN控制器收到OVS交换机发送的可疑流后，从流中获取访问车辆的属性向量。对于任意一个访问用户具有的属性满足服务提供者定义的访问策略，则存在一个重构向量，使得。因此我们可以根据如下等式得到重构向量：

其中为服务使用者属性向量矩阵，为重构向量，为目标向量。控制器根据计算得到的重构出秘密值s，即

步骤 43）SDN将计算得到的秘密值s发送到服务提供者进行比较。若验证成功则说明此访问车辆满足当前用户定义的访问策略，SDN控制器在根据服务提供者定义的隐私策略规定访问车辆此次授权访问的时间，根据访问车辆的MAC地址和虚拟机的IP地址作为流表项的源MAC地址、目的IP地址和目的MAC地址、源IP地址。下发流表项到OVS交换机允许此次车辆的访问请求。若验证失败，表示访问车辆的属性不满足用户定义的访问策略(非法用户)，控制器将丢弃该信息流拒绝其访问请求。

所述步骤 5）具体如下所示：

步骤 51）我们需要将位置服务分发策略(SRM)转化为信息流模型

其中表示一个信息流规则。

其中是信息流规则的创造者，是系统中车辆的Handle标识，Time表示服务使用者可以访问的时间，,表示管理员创造了这个此信息流规则，表示普通用户创造了此信息流规则，我们默认当有两个规则发生冲突时管理员角色的优先级大于普通用户，即按照管理员创造的信息流规则执行。

步骤 52）访问用户根据信息流规则在规定的时间内访问规定的哪些服务。当访问时间超出规定的时间后，访问用户需要进行重新的身份认证以及查看是否满足数据拥有者的访问策略。满足访问用户定义的访问策略则可以继续访问，否则拒绝其访问请求。

**有益效果：**本发明采用的以上技术方案与现有技术相比，具有以下技术效果：

本发明在兼顾对访问用户进行真实身份验证的同时还支持了位置隐私的保护，具体来说：

1. 本发明利用Handle技术唯一性确定车辆在系统中的真实身份，同时利用Handle标识替换传统的MAC或IP地址来防止用户身份被篡改。
2. 本发明利用可信中心TC统一对访问用户的属性信息分发，降低了访问用户终端的资源消耗。
3. 本发明通过基于属性和信息流模型的动态访问控制算法保证只有满足访问策略的用户才能访问到相应虚拟机中的哪些服务，保证位置数据的安全共享。

**附图说明**

图1是本认证方案所运用的实际场景。

图2是访问车辆具体的访问流程。

### 具体实施方式

下面结合附图对本发明的技术方案做进一步的详细说明：

在具体实施中，图1是本认证方案所运用的实际场景。在车联网领域中，用户在向第三方服务提供商请求服务的同时，也会将自身的位置隐私数据保存在第三方服务提供商。LBS服务提供商可以提供很多基于位置的共享服务，如好友位置查询、好友旅行轨迹查询、当前位置实时共享等。然后一旦用户的隐私数据被恶意用户获取，可能会对数据拥有者造成了极大的安全隐患。在该情况下，每个访问用户在访问数据前都需要通过网关的筛选，只有满足数据拥有者定义的访问策略才能通过网关访问到相应虚拟机，拒绝不满足访问策略的用户访问，保证数据隐私安全。与此同时利用信息流模型保证哪些用户可以访问到哪些服务，实现细粒度的数据操作。因此用户需要通过基于属性和信息流模型的动态访问控制算法才能访问相应虚拟机中的数据，保证数据隐私安全。

图2是本专利的访问流程图，假设车辆将自己的位置服务存在第三方服务提供商虚拟机中，车辆根据自己的隐私需求制定自己的访问控制策略P，并将访问策略P发送到可信中心，可信中心根据用户的访问控制策略以及随机数生成访问控制矩阵，同时将秘密值发送给车辆。在身份确认阶段，由于每个车辆()都申请了Handle标识。可以利用Handle标识唯一性确定车辆在系统中的真实身份。在我们的系统中，在注册阶段可信中心会对车辆具有的属性与车辆的Handle标识的hash值进行异或操作即,将异或操作得到的结果返回给车辆。车辆可以根据自身的Handle标识对结果进行异或操作，车辆获得自身的属性集。在访问控制阶段，请求流在OVS交换机流表中匹配成功，说明车辆的访问请求已经被处理过并且还在上次处理结果的周期中，因此OVS交换机根据流表规定的动作决定这个流如何处理。如果规定的动作为forward表示此访问车辆满足服务提供者定义的访问策略，若规定的动作为block表示访问车辆为服务提供者定义的恶意用户。

请求流在OVS交换机流表中未能匹配成功，交换机将此信息流作为可疑流发送至控制器，控制器根据访问车辆请求时携带的属性向量判断是否满足服务提供者定义的访问策略。SDN控制器收到OVS交换机发送的可疑流后，从流中获取访问车辆的属性向量, 因此我们可以根据等式，得到重构向量。其中为服务使用者属性向量矩阵，为重构向量，为目标向量。控制器根据计算得到的以及等式重构出秘密值s。SDN将计算得到的秘密值s发送到服务提供者进行比较。若验证成功则说明此访问车辆满足当前用户定义的访问策略，SDN控制器在根据服务提供者定义的隐私策略规定访问车辆此次授权访问的时间，根据访问车辆的MAC地址和虚拟机的IP地址作为流表项的源MAC地址、目的IP地址和目的MAC地址、源IP地址。下发流表项到OVS交换机允许此次车辆的访问请求。若验证失败，表示访问车辆的属性不满足用户定义的访问策略(非法用户)，控制器将丢弃该信息流拒绝其访问请求。最后根据信息流模型在规定的访问时间内访问虚拟机中具体哪些服务。

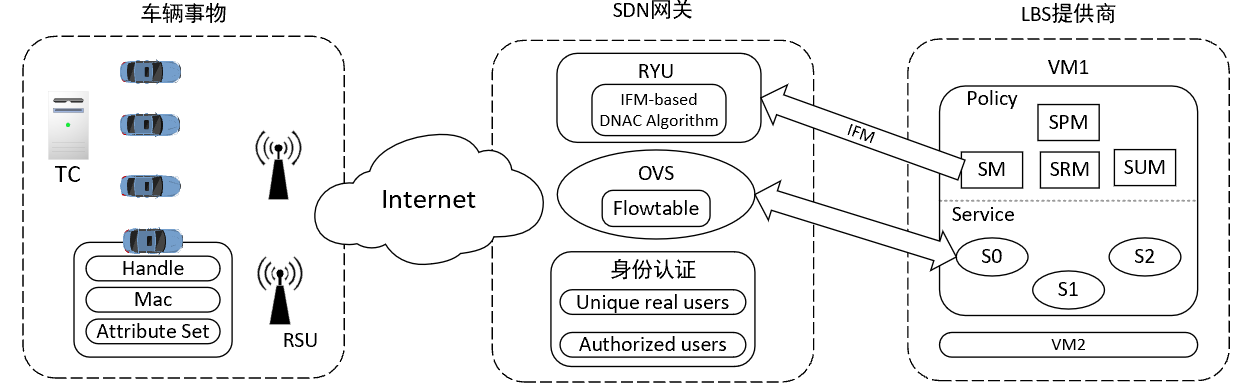


图1 实际场景

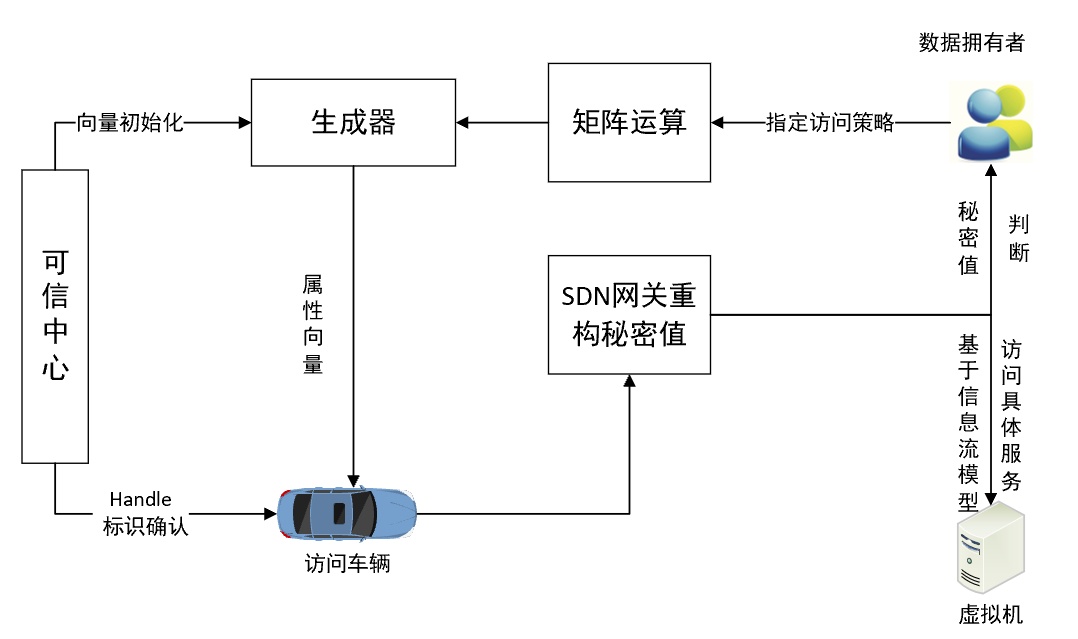


图2 访问车辆具体的访问流程