



(12) 发明专利申请

(10) 申请公布号 CN 103873473 A

(43) 申请公布日 2014. 06. 18

(21) 申请号 201410102335. 4

(22) 申请日 2014. 03. 19

(71) 申请人 西安电子科技大学

地址 710071 陕西省西安市太白南路 2 号

(72) 发明人 陈杰 张跃宇 时俊萍 乔巧梅

李琪 王晓辉 刘珺峰

(74) 专利代理机构 陕西电子工业专利中心

61205

代理人 田文英 王品华

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 9/32 (2006. 01)

H02J 7/00 (2006. 01)

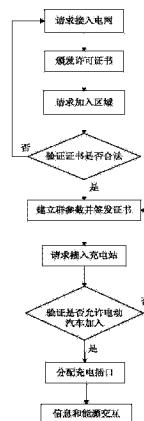
权利要求书3页 说明书6页 附图2页

(54) 发明名称

充电站对电动汽车匿名群组认证方法

(57) 摘要

本发明公开了一种充电站对电动汽车匿名群组认证方法,它涉及信息安全技术领域,包括如下步骤:1. 电动汽车请求接入电网;2. 中央聚合器为电动汽车颁发入网许可证书;3. 电动汽车请求加入某一区域的充电站;4. 本地聚合器验证电动汽车入网许可证书的合法性;5. 本地聚合器给电动汽车分配所属群并签发证书;6. 电动汽车请求接入充电站;7. 充电站验证是否允许电动汽车接入;8. 充电站给通过验证的电动汽车分配一个实际可用的充电插口;9. 电动汽车和充电站之间进行信息和能源的交互。本发明实现了充电站对车辆的匿名认证,能够对恶意用户进行追踪,并给予一定的处罚,同时提高了群组认证效率。



1. 充电站对电动汽车匿名群组认证方法,包括以下步骤:

(1) 请求接入电网:

(1a) 用户将用户的真实身份和拟入网电动汽车牌照的真实身份,分别发送给中央聚合器进行注册,中央聚合器为拟入网的电动汽车颁发身份证,并将身份证记录到中央聚合器的数据库中;

(1b) 拟入网的电动汽车将入网请求信息发给中央聚合器,请求接入充电站;

(2) 颁发许可证书:

中央聚合器查找其数据库是否存储该拟入网的电动汽车身份证,若存储,但尚未颁发入网许可证书,则中央聚合器利用自己的私钥将电动汽车的身份和公钥进行签名生成入网许可证书,将该许可证书颁发给该拟入网的电动汽车;若没有存储,则执行步骤(1);

(3) 请求加入区域:

电动汽车将拟加入区域的请求信息,发送给本地聚合器;

(4) 验证证书是否合法:

(4a) 本地聚合器利用中央聚合器公钥,验证入网许可证书是否合法,若入网许可证书不合法,则执行步骤(1);否则,执行步骤(4b);

(4b) 本地聚合器验证收到入网许可证书的时间是否在有效日期范围内,若超过了有效日期,则执行步骤(1),否则执行步骤(5);

(5) 建立群参数并签发证书:

(5a) 本地聚合器将电动汽车允许加入充电站所在群的消息发送给电动汽车;

(5b) 电动汽车按照编号生成方法,生成一个电动汽车编号,并将该电动汽车编号发给本地聚合器;

(5c) 本地聚合器接收到从电动汽车发来的电动汽车编号后,检查当前数据库中的记录表中是否包含该电动汽车编号,若包含,则执行步骤(5b);否则,给电动汽车分配一个充电位置和对应的充电位置标识符;

(5d) 本地聚合器将所属群的相关消息及接入充电站的签名证书发给电动汽车;

(5e) 电动汽车按照下式,生成群成员证书:

$$C = (I, X, \text{num}, \sigma)$$

其中,C表示群成员证书,I表示电动汽车充电位置标识符,X表示电动汽车的编号,num表示电动汽车的路径编码, σ 表示本地聚合器用结构保护型签名的系统私钥对电动汽车的编号和电动汽车的路径编码进行的结构保护型签名;

(6) 请求接入充电站:

电动汽车将拟接入充电站的请求消息,发送给充电站;

(7) 验证是否允许电动汽车接入:

(7a) 充电站用本地聚合器的公钥,验证电动汽车签名证书的合法性,若签名证书不合法,则执行步骤(5),否则执行步骤(7b);

(7b) 充电站验证收到签名证书的时间是否在签名证书的有效日期内,若超过有效日期,则执行步骤(5),否则执行步骤(8);

(8) 充电站给电动汽车分配一个实际可用的充电插口;

(9) 信息和能源交互:

- (9a) 电动汽车接入充电站后和充电站进行密钥协商,协商出一个会话密钥;
- (9b) 电动汽车分别通过子集划分方法和向量承诺方法,证明自己是合法的群成员;
- (9c) 电动汽车用群私钥,对自己的申请消息进行签名,并将签名结果发送给充电站;
- (9d) 充电站收到从电动汽车发来的消息后,用群公钥对签名进行验证,若验证通过,则充电站根据申请及电网需求,充电站和电动汽车进行能源及信息的交互;否则,执行步骤(9e);
- (9e) 充电站将电动汽车发来的群签名消息发给本地聚合器;
- (9f) 本地聚合器接收到从充电站发来的签名消息后,按照群成员追踪方法,对发送错误消息的电动汽车进行追踪。

2. 根据权利要求1所述的充电站对电动汽车匿名群组认证方法,其特征在于,步骤(4a)所述的验证入网许可证书是否合法,按如下步骤进行:

第一步,本地聚合器接收到电动汽车发来的请求消息后,用本地聚合器的私钥解密该请求消息,得到电动汽车的身份、电动汽车的公钥、中央聚合器的身份、电动汽车想要加入的充电站,中央聚合器给电动汽车颁发的入网许可证书;

第二步,本地聚合器根据中央聚合器的身份,查找公钥列表,得到该中央聚合器的公钥;

第三步,本地聚合器利用中央聚合器的公钥,验证中央聚合器的签名是否成立,若成立,则说明入网许可证书合法;否则,说明入网许可证不合法。

3. 根据权利要求1所述的充电站对电动汽车匿名群组认证方法,其特征在于,步骤(5b)所述的编号生成方法是指,按照下式得到电动汽车编号:

$$X=g^x$$

其中, X 表示电动汽车的编号, x 表示电动汽车的群私钥, g 表示群 G 的生成元。

4. 根据权利要求1所述的充电站对电动汽车的匿名群组认证方法,其特征在于,步骤(7a)所述的验证签名证书是否合法,按如下步骤进行:

第一步,充电站接收到电动汽车发来的请求消息后,用充电站的私钥解密该请求消息,得到电动汽车的编号、电动汽车的公钥、本地聚合器的身份、本地聚合器给电动汽车颁发的签发证书;

第二步,充电站根据本地聚合器的身份,查找公钥列表,得到该本地聚合器的公钥;

第三步,充电站利用本地聚合器的公钥,验证本地聚合器的签名是否成立,若成立,则说明签发证书合法;否则,说明签发证书不合法。

5. 根据权利要求1所述的充电站对电动汽车匿名群组认证方法,其特征在于,步骤(9b)所述的子集划分方法,按如下步骤进行:

第一步,本地聚合器将未撤销群成员划分为若干个不相交的集合;

第二步,本地聚合器将不相交的集合进行编码,得到未撤销群成员的路径编码。

6. 根据权利要求1所述的充电站对电动汽车匿名群组认证方法,其特征在于,步骤(9b)所述的向量承诺方法,按如下步骤进行:

第一步,电动汽车对可以证明自己是合法用户的消息向量做出承诺后,将承诺值发给充电站;

第二步,充电站利用向量承诺密钥打开承诺,获得消息向量。

7. 根据权利要求 1 所述的充电站对电动汽车匿名群组认证方法,其特征在于,步骤(9f)所述的群成员追踪方法,按如下步骤进行:

第一步,本地聚合器利用群签名打开私钥,得到一个电动汽车编号;

第二步,在本地聚合器的数据库中查阅存有该编号的电动汽车的相关信息记录,将该编号的电动汽车的相关信息发送给中央聚合器;

第三步,中央聚合器根据所接收的本地聚合器发送的电动汽车相关信息,在数据库中查出电动汽车的真实身份。

充电站对电动汽车匿名群组认证方法

技术领域

[0001] 本发明属于通信技术领域,更进一步涉及信息安全技术领域中的一种充电站对电动汽车匿名群组认证方法。本发明可用于电动汽车需要充电或供电接入电网场景时,实现充电站对车辆用户的匿名认证,从而保护车辆用户的隐私。

背景技术

[0002] 电动汽车接入电网(V2G)将电动汽车与智能电网相结合,既解决了电动汽车大规模发展带来的充电压力问题,又可将电动汽车作为移动的、分布式储能单元接入电网。然而电动汽车的流动性较强,频繁数据交换在满足实时管理的同时带来用户敏感信息泄露的风险。因此V2G的充电站(ST_i)需要设计匿名群组认证方案,同时支持成员的动态加入和小开销的身份吊销。

[0003] Binod Vaidya 等人在文章“Efficient Authentication Mechanism for PEV Charging Infrastructure”(In:Communications(ICC),2011IEEE International Conference on)中提出了一种对于电动汽车充电的综合的分散认证方法。该方法的具体实施步骤是:第一,初始化,充电站的服务器从注册机构获得一个证书;第二,用户注册,用户UD_i将自己的身份及登陆密码发给注册机构,注册机构计算合适的参数,将这些参数写入到智能卡中,并将该智能卡发给用户UD_i。第三,认证阶段,当用户UD_i想要接入充电设备时,用户UD_i必须将自己的身份和登陆密码输入智能卡,智能卡验证登陆密码是否成立,若不成立拒绝登陆请求,否则,智能卡生成一个证书,并将该证书发给充电站的服务器。服务器验证证书的合法性。第四,若用户UD_i想要更新登陆密码,就需要进行密码重置。第五,当用户的有效登记过期的时候,需要更新所有参数。虽然该方法具有相互认证功能,并且保护了用户的身份隐私。但是,该方法仍然存在的不足之处是:当有恶意用户扰乱电网秩序时,无法查证恶意用户的身份,从而不能对恶意用户进行处罚。

[0004] Huei-Ru Tseng等人在文章“A Secure and Privacy-Preserving Communication Protocol for V2G Networks”(In:Communitations,2012IEEE Wireless Communications and Networking Conference)中提出了电动汽车加入电网(Vehical-to-Grid,V2G)中一种安全的、具有隐私保护的通信方法。该方法的具体实施步骤是:第一,密钥中心初始化系统参数,为电动汽车、本地聚合器和中央聚合器分配公私钥。第二,电动汽车在加入电动汽车与电网构成的网络之前必须向中央聚合器进行注册,电动汽车将自己的身份和生成的参数发给中央聚合器,中央聚合器验证身份合法后,生成一个证书,并将该证书发给电动汽车。第三,当电动汽车接入电动汽车加入电网(Vehical-to-Grid,V2G)的时候,电动汽车将假名和证书一起发给本地聚合器,本地聚合器验证证书的合法性。第四,确定证书的合法性后,电动汽车将自己的状态信息发给本地聚合器,本地聚合器再将收到的所有的信息聚合,并将聚合结果发给中央聚合器。该方法采用假名实现了对用户身份的隐私保护。假名是由中央聚合器生成并分发给不同用户的,中央聚合器需要存储这些假名。每次电动汽车加入V2G网络时都需要使用不同假名,并且用户量也比较大。这样就给中央聚合器带来了假名的管

理和维护的问题。

[0005] 国家电网公司在其申请的专利“电动汽车与充换电站的安全数据交换方法及系统”(申请日:2010年10月15日,申请号:201010508362.3,公开号:CN102045340A)中提出了一种电动汽车与充换电站安全的数据交换方法。该方法的实施方法是:第一,电动汽车向充换电站发出经数字签名的自身的完整性信息,并获取对方的完整性信息来提交安全信息管理中心;第二,充换电站向安全信息管理中心提交电动汽车发送的完整性信息,并向电动汽车提交经数字签名的完整性信息;第三,安全信息管理中心对完整性信息进行认证,并反馈认证结果;第四,认证结果均符合时,电动汽车与充换电站间建立连接,进行数据交换。该专利申请虽然通过设备完整性信息验证,实现了对电动汽车和充换电站设备状态的安全性验证。但是,该方法仍然存在不足之处是:对于用户身份的合法性没有进行认证,当出现恶意用户时,无法对恶意用户进行追踪。

发明内容

[0006] 本发明的目的在于克服上述已有技术的不足,针对电动汽车加入电网提出了一种充电站对电动汽车匿名群组认证方法。本发明实现了充电站对电动汽车的匿名认证,同时能够对恶意用户进行追踪,并给予一定的处罚,很好地提高了电网系统的稳定性。

[0007] 为实现上述目的,本发明具体步骤如下:

[0008] 1. 充电站对电动汽车匿名群组认证方法,包括以下步骤:

[0009] (1) 请求接入电网:

[0010] (1a) 用户将用户的真实身份和拟入网电动汽车牌照的真实身份,分别发送给中央聚合器进行注册,中央聚合器为拟入网的电动汽车颁发身份证,并将身份证记录到中央聚合器的数据库中;

[0011] (1b) 拟入网的电动汽车将入网请求信息发给中央聚合器,请求接入充电站;

[0012] (2) 颁发许可证书:

[0013] 中央聚合器查找其数据库是否存储该拟入网的电动汽车身份证,若存储,但尚未颁发入网许可证书,则中央聚合器利用自己的私钥将电动汽车的身份和公钥进行签名生成入网许可证书,将该许可证书颁发给该拟入网的电动汽车;若没有存储,则执行步骤(1);

[0014] (3) 请求加入区域:

[0015] 电动汽车将拟加入区域的请求信息,发送给本地聚合器;

[0016] (4) 验证证书是否合法:

[0017] (4a) 本地聚合器利用中央聚合器公钥,验证入网许可证书是否合法,若入网许可证书不合法,则执行步骤(1);否则,执行步骤(4b);

[0018] (4b) 本地聚合器验证收到入网许可证书的时间是否在有效日期范围内,若超过了有效日期,则执行步骤(1),否则执行步骤(5);

[0019] (5) 建立群参数并签发证书:

[0020] (5a) 本地聚合器将电动汽车允许加入充电站所在群的消息发送给电动汽车;

[0021] (5b) 电动汽车按照编号生成方法,生成一个电动汽车编号,并将该电动汽车编号发给本地聚合器;

[0022] (5c) 本地聚合器接收到从电动汽车发来的电动汽车编号后,检查当前数据库中的

记录表中是否包含该电动汽车编号,若包含,则执行步骤(5b);否则,给电动汽车分配一个充电位置和对应的充电位置标识符;

[0023] (5d) 本地聚合器将所属群的相关消息及接入充电站的签名证书发给电动汽车;

[0024] (5e) 电动汽车按照下式,生成群成员证书:

[0025] $C = (I, X, \text{num}, \sigma)$

[0026] 其中, C 表示群成员证书, I 表示电动汽车充电位置标识符, X 表示电动汽车的编号, num 表示电动汽车的路径编码, σ 表示本地聚合器用结构保护型签名的系统私钥对电动汽车的编号和电动汽车的路径编码进行的结构保护型签名;

[0027] (6) 请求接入充电站;

[0028] 电动汽车将拟接入充电站的请求消息,发送给充电站;

[0029] (7) 验证是否允许电动汽车接入;

[0030] (7a) 充电站用本地聚合器的公钥,验证电动汽车签名证书的合法性,若签名证书不合法,则执行步骤(5),否则执行步骤(7b);

[0031] (7b) 充电站验证收到签名证书的时间是否在签名证书的有效日期内,若超过有效日期,则执行步骤(5),否则执行步骤(8);

[0032] (8) 充电站给电动汽车分配一个实际可用的充电插口;

[0033] (9) 信息和能源交互;

[0034] (9a) 电动汽车接入充电站后和充电站进行密钥协商,协商出一个会话密钥;

[0035] (9b) 电动汽车分别通过子集划分方法和向量承诺方法,证明自己是合法的群成员;

[0036] (9c) 电动汽车用群私钥,对自己的申请消息进行签名,并将签名结果发送给充电站;

[0037] (9d) 充电站收到从电动汽车发来的消息后,用群公钥对签名进行验证,若验证通过,则充电站根据申请及电网需求,充电站和电动汽车进行能源及信息的交互;否则,执行步骤(9e);

[0038] (9e) 充电站将电动汽车发来的群签名消息发给本地聚合器;

[0039] (9f) 本地聚合器接收到从充电站发来的签名消息后,按照群成员追踪方法,对发送错误消息的电动汽车进行追踪。

[0040] 本发明与现有技术相比具有以下优点:

[0041] 第一,由于本发明在电动汽车和充电站进行信息交互时,采用了可撤销群成员签名,克服了现有技术存在的对恶意用户不可追踪的缺点,使得本发明对恶意用户实现了可追踪,能够对恶意用户进行处罚,提高了电网系统的稳定性。

[0042] 第二,由于本发明在电动汽车向充电站匿名证明身份合法性时,采用子集划分方法和向量承诺方法,克服了现有技术中用假名实现匿名认证存在的管理和维护复杂度高的缺点,使得本发明实现了管理和维护的简单化。

[0043] 第三,由于本发明在群成员证书形成时,采用了结构保护型签名,克服了现有技术中更新成员状态列表时需要不断地更新群成员证书的缺点,使得本发明实现了在更新成员状态列表时不需要更新群成员证书,降低了计算开销,提高了群组认证效率。

附图说明

[0044] 图 1 为本发明流程图；

[0045] 图 2 为本发明中央聚合器、本地聚合器、充电站的关系与功能示意图。

具体实施方式

[0046] 下面结合附图对本发明做进一步的描述。

[0047] 参照附图 2, 本发明所涉及到的中央聚合器、本地聚合器、充电站的关系与功能如下：

[0048] 中央聚合器是电动汽车加入电网 (Vehical-to-Grid, V2G) 中最高层级的处理器, 由于中央聚合器计算和存储能力很强, 因此, 它主要负责电动汽车的入网注册, 为拟加入电网的电动汽车颁发入网许可证书, 并保存所有注册过的用户的详细身份信息, 包含多个本地聚合器。

[0049] 本地聚合器是中央聚合器下一级的处理器, 由于本地聚合器计算和存储能力比中央聚合器弱, 所以, 它主要负责为电动汽车分配所属群, 签发证书。

[0050] 充电站是本地聚合器的下一级, 作为电动汽车接入电网的接口。电动汽车和充电站之间进行信息和能源交互, 并且充电站和本地聚合器共同维持可撤销列表。

[0051] 参照附图 1, 本发明的实现步骤如下。

[0052] 步骤 1, 请求接入电网。

[0053] 用户将用户的真实身份和拟入网电动汽车牌照的真实身份, 分别发送给中央聚合器进行注册, 中央聚合器为拟入网的电动汽车颁发身份证, 并将身份证记录到中央聚合器的数据库中。

[0054] 拟入网的电动汽车将入网请求信息发给中央聚合器, 该请求信息是将电动汽车的身份证用中央聚合器的公钥加密的结果。

[0055] 步骤 2, 颁发许可证书。

[0056] 中央聚合器收到请求信息后, 用其私钥解密, 得到电动汽车的身份证。然后, 中央聚合器查找其数据库是否存储该拟入网的电动汽车身份证, 若存储, 但尚未颁发入网许可证书, 则中央聚合器利用自己的私钥将电动汽车的身份和公钥进行签名得到入网许可证书, 将该许可证书颁发给该拟入网的电动汽车; 若没有存储, 则执行步骤 1。

[0057] 步骤 3, 请求加入区域。

[0058] 电动汽车将拟加入区域的请求信息, 发送给本地聚合器, 此请求信息是将电动汽车的身份、电动汽车的公钥、中央聚合器的身份、电动汽车想要加入的充电站、中央聚合器给电动汽车颁发的入网许可证书用本地聚合器的公钥进行加密的结果。

[0059] 步骤 4, 验证证书是否合法。

[0060] 第一步, 本地聚合器利用中央聚合器公钥, 按照如下步骤, 验证入网许可证书是否合法, 若入网许可证书不合法, 则执行步骤 1; 否则, 执行步骤 4 的第一步。

[0061] 本地聚合器接收到电动汽车发来的请求消息后, 用本地聚合器的私钥解密该请求消息, 得到电动汽车的身份、电动汽车的公钥、中央聚合器的身份、电动汽车想要加入的充电站、中央聚合器给电动汽车颁发的入网许可证书。

[0062] 本地聚合器根据中央聚合器的身份, 查找公钥列表, 得到该中央聚合器的公钥。

[0063] 本地聚合器利用中央聚合器的公钥,验证中央聚合器的签名是否成立,若成立,则说明入网许可证书合法;否则,说明入网许可证书不合法。

[0064] 第二步,本地聚合器验证收到入网许可证书的时间是否在有效日期范围内,若超过了有效日期,则执行步骤 1,否则执行步骤 5。

[0065] 步骤 5,建立群参数并签发证书。

[0066] 第一步,本地聚合器根据电动汽车想要加入的充电站,为其分配所属群,并将所属群的相关消息发送给电动汽车。

[0067] 第二步,电动汽车按照下式,计算出一个电动汽车编号,并将该电动汽车编号发给本地聚合器:

[0068] $X = g^x$

[0069] 其中, X 表示电动汽车的编号, x 表示电动汽车的群私钥, g 表示群 G 的生成元。

[0070] 第三步,本地聚合器接收到从电动汽车发来的电动汽车编号后,检查当前数据库中的记录表中是否包含该电动汽车编号,若包含,则执行步骤 5 的第二步;若不包含,则给电动汽车分配一个充电位置 and 对应的充电位置标识符,并在其数据库中记录下该编号。

[0071] 第四步,本地聚合器用自己的私钥对电动汽车的编号和公钥进行签名得到电动汽车接入充电站的签名证书,并将该签名证书发给电动汽车,此签名证书有效期较短,一般为一天。

[0072] 第五步,电动汽车按照下式,得到群成员证书:

[0073] $C = (I, X, \text{num}, \sigma)$

[0074] 其中, C 表示群成员证书, I 表示电动汽车充电位置标识符, X 表示电动汽车的编号, num 表示电动汽车的路径编码, σ 表示本地聚合器用结构保护型签名的系统私钥对电动汽车的编号和电动汽车的路径编码进行的结构保护型签名。

[0075] 步骤 6,请求接入充电站。

[0076] 电动汽车将拟接入充电站的请求消息,发送给充电站,此请求消息是将电动汽车的编号、电动汽车的公钥、本地聚合器的身份、本地聚合器给电动汽车颁发的签发证书用充电站的私钥进行加密的结果。

[0077] 步骤 7,验证是否允许电动汽车接入。

[0078] 第一步,充电站用本地聚合器的公钥,按照如下步骤,验证电动汽车签名证书的合法性,若签名证书不合法,则执行步骤 5,否则执行步骤 7 的第二步。

[0079] 充电站接收到电动汽车发来的请求消息后,用充电站的私钥解密该请求消息,得到电动汽车的编号、电动汽车的公钥、本地聚合器的身份、本地聚合器给电动汽车颁发的签发证书。

[0080] 充电站根据本地聚合器的身份,查找公钥列表,得到该本地聚合器的公钥。

[0081] 充电站利用本地聚合器的公钥,验证本地聚合器的签名是否成立,若成立,则说明签发证书合法;否则,说明签发证书不合法。

[0082] 第二步,充电站验证收到签名证书的时间是否在签名证书的有效日期内,若超过有效日期,则执行步骤 5,否则执行步骤 8。

[0083] 步骤 8,分配充电插口。

[0084] 充电站给电动汽车分配一个实际可用的充电插口。

[0085] 步骤 9, 信息和能源交互。

[0086] 第一步, 电动汽车接入充电站后和充电站进行密钥协商, 协商出一个会话密钥。

[0087] 第二步, 分别采用子集划分方法和向量承诺方法, 电动汽车向充电站匿名地证明自己是合法的群成员。

[0088] 第三步, 电动汽车用群私钥, 对自己的充电申请消息进行签名, 并将签名结果发送给充电站, 这里使用的签名方法是可撤销的群签名。

[0089] 第四步, 充电站收到从电动汽车发来的消息后, 用群公钥对签名进行验证, 若验证通过, 则充电站根据申请及电网需求, 充电站和电动汽车进行能源及信息的交互; 否则, 执行步骤 9 的第五步。

[0090] 第五步, 充电站将电动汽车发来的群签名消息发给本地聚合器。

[0091] 第六步, 本地聚合器接收到从充电站发来的签名消息后, 采用群成员追踪方法, 按照如下步骤, 对发送错误消息的电动汽车进行追踪, 并给予一定的处罚。

[0092] 本地聚合器利用群签名打开私钥, 得到一个电动汽车编号。

[0093] 在本地聚合器的数据库中查阅存有该编号的电动汽车的相关信息记录, 将该编号的电动汽车的相关信息发送给中央聚合器。

[0094] 中央聚合器根据所接收的本地聚合器发送的电动汽车相关信息, 在数据库中查出电动汽车的真实身份, 并给予一定的处罚。

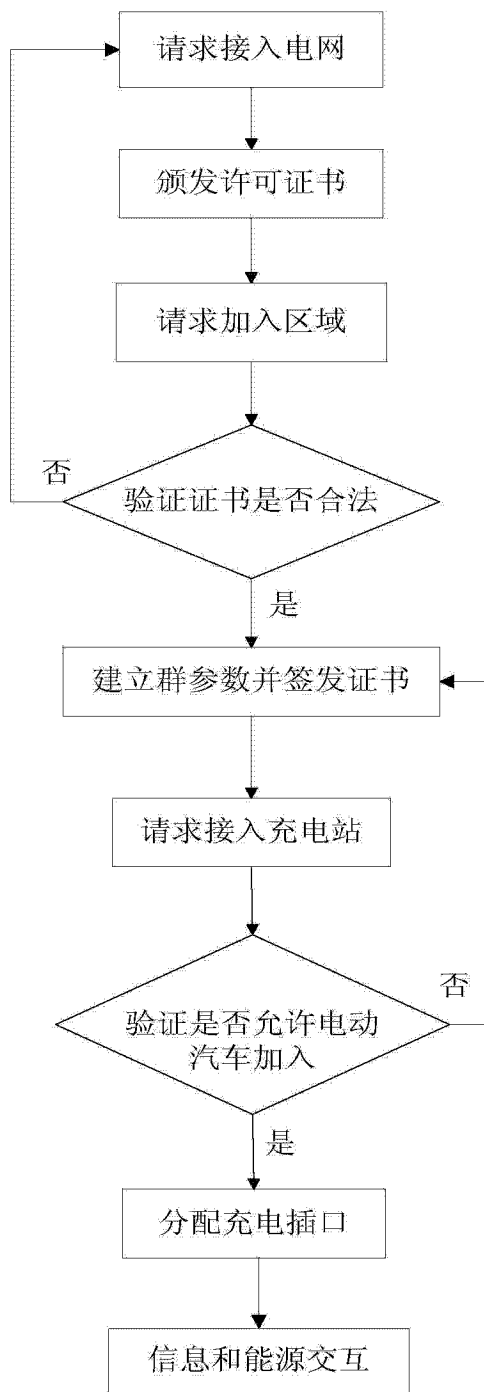


图 1

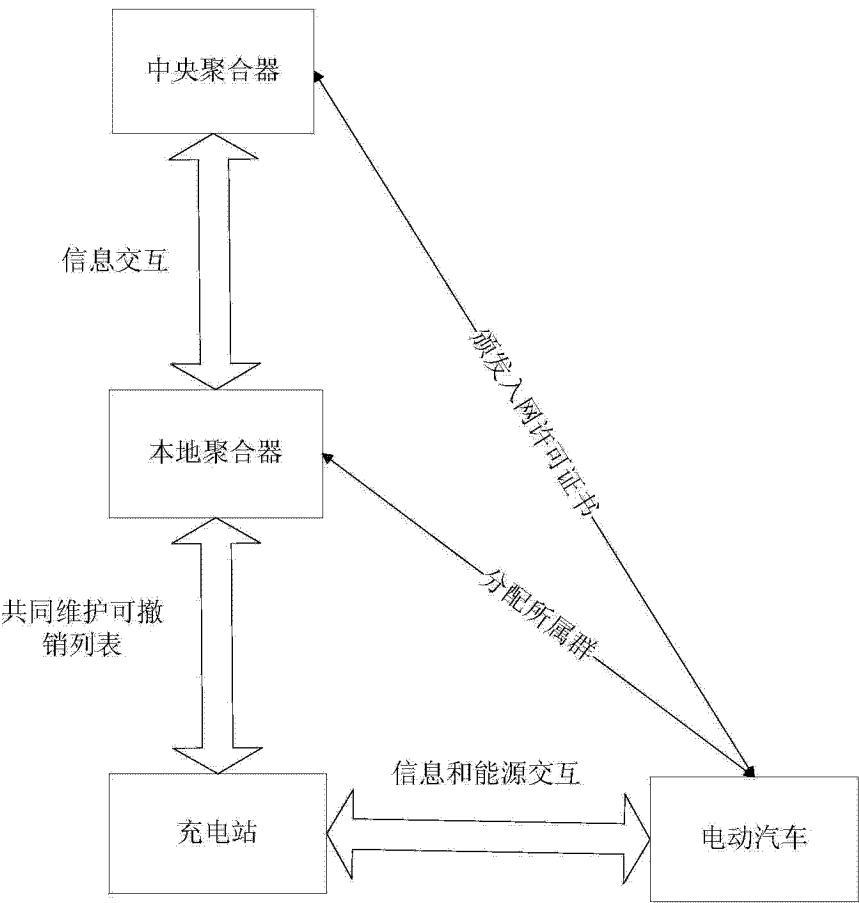


图 2