(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112272377 B
(45)授权公告日 2022.06.14

(21)申请号 202011203441.3

(22)申请日 2020.11.02

(65)同一申请的已公布的文献号
申请公布号 CN 112272377 A

(43)申请公布日 2021.01.26

(73)专利权人 桂林电子科技大学
地址 541004 广西壮族自治区桂林市七星区金鸡路1号

(72)发明人 臧美美 朱英 蓝如师 刘忆宁 罗笑南 赵文婷

(74)专利代理机构 桂林市华杰专利商标事务所有限责任公司 45112
专利代理师 杨雪梅

(51)Int.Cl.
H04W 12/069(2021.01)
H04W 12/02(2009.01)
H04W 4/46(2018.01)
H04W 4/44(2018.01)
H04W 4/06(2009.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)
G06F 16/27(2019.01)

(56)对比文件
CN 109194610 A,2019.01.11
CN 110430061 A,2019.11.08

审查员 刘珍

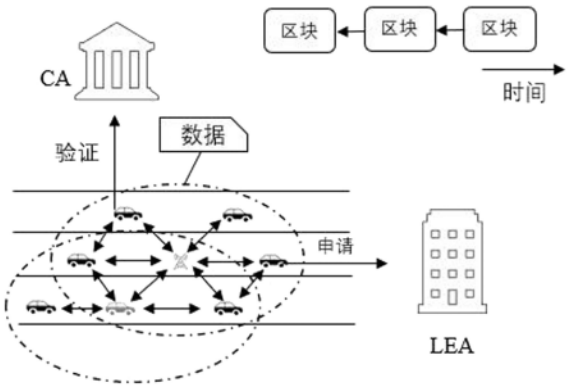
权利要求书2页 说明书6页 附图4页

(54)发明名称

一种基于区块链的车辆安全通信方法

(57)摘要

本发明公开了一种基于区块链的车辆安全通信方法，包括以下步骤：(1)车联网系统初始化，建立系统所需的参数，车辆进入时，向LEA发送证明自己身份的信息，系统中的验证节点对其身份进行验证；(2)通过验证的车辆，由LEA向其颁发证书并记录车辆的身份信息，最后并上传至区块链，车辆和车辆、车辆和路边单元RSU通信，通信方式采取多边形网络组播方式；(3)参数更新，系统中的参数在参数有效性到期或者可能被攻击，保密性受到威胁时进行参数的更新。本发明能够有效地解决车辆在车联网中通信的安全和隐私保护问题。相比传统车联网，本发明使用区块链技术取代可信的第三方，解决了单节点失败问题，实现车辆之间数据的安全交换。



CN 112272377 B

1.一种基于区块链的车辆安全通信方法,其特征在于,包括以下步骤:

(1)车联网系统初始化,建立系统所需的参数,车辆进入时,向LEA发送证明自己身份的信息,系统中的验证节点对其身份进行验证;

(2)通过验证的车辆,由LEA向其颁发证书并记录车辆的身份信息,最后并上传至区块链,车辆和车辆、车辆和路边单元RSU通信,通信方式采取多边形网络组播方式;

所述的多边形网络组播的通信方式包括:

车辆与车辆之间的通信,车辆与路边单元RSU的通信,共同构成多边形网络组播通信模型,模型包括两种通信类型:

第一种,以一个车辆为中心,与其相邻的车辆和距离中心车辆最近的路边单元RSU构成多个三角形组成的多边形,这种情况下,中心车辆为主节点,RSU和其他车辆为从节点;

第二种,以一个RSU为中心,与其相邻的车辆构成多个三角形组成的多边形,这种情况下,RSU为主节点,周围的车辆为从节点;在其通信范围内最多6辆车,中心节点RSU将收集到的信息加密并签名发送给通信范围内的从节点,因为从RSU发送出的消息都是经过验证的,所以从节点车辆收到后消息解密即可得到路况交通信息;

(3)参数更新,系统中的参数在参数有效性到期或者可能被攻击,保密性受到威胁时进行参数的更新。

2.如权利要求1所述的基于区块链的车辆安全通信方法,其特征在于,步骤(1)所述系统初始化的过程包括:

定义有限域$F_p=\{0,1,2,3\cdots p-1\}$,p为质数;

选取椭圆曲线$E:y^2=x^3+ax+b$,其中$a,b\in F_p$,满足条件$4a^3+27b^2\neq 0(\mathrm{mod}\ p)$;

定义q阶循环加法群G,G包含E中有限域内所有的点;

基点P为椭圆曲线的生成元,$P\in G$;

定义哈希函数:$H:\{0,1\}\rightarrow Z_q^*$;

随机选择系统私钥$SK_s\in Z_q^*$,$PK_s=SK_s\cdot P$作为系统的公钥;

CA公布系统参数$\{p,q,E,PK_s,H\}$。

3.如权利要求1所述的基于区块链的车辆安全通信方法,其特征在于,

步骤(1)所述车辆身份验证的过程如下:

车辆进入系统时,向LEA发送能够证明自己身份的信息和公钥,例如车辆V向LEA发送身份ID_v和公钥PK_v,表示为$V\rightarrow LEA:S_(ID_v||PK_v)$,S_是发送函数;收到申请信息后,系统中的验证节点对车辆身份进行验证,并对合格的车辆进行签名,车辆收集不少于51%的验证节点的签名,作为诚实节点加入系统,LEA颁发电子通信证书给诚实车辆,记录其信息后上传至区块链中。

4.如权利要求1所述的基于区块链的车辆安全通信方法,其特征在于:

步骤(2)在第一种以车辆为中心的通信类型中,中心车辆是主节点,相邻车辆和距离中心车辆最近的路边单元RSU是从节点,每个主节点在其通信范围内最多5个从节点辆车,加上1个最近的RSU从节点构成多个三角形组成的多边形网络的从节点进行分组转发;

主节点首先向从节点RSU发送消息,计算参数Q、R、z和v,然后,车辆发送$M_1=\{z,v,PID_v,m_1,T_s,R\}$到从节点RSU;

$Q=H(PK_{rsu}\cdot SK_v||PID_v||m_1||T_s)$;

$R=H(PK_{rsu}\cdot SK_s||PK_{rsu}||T_s)$；

$z=Q\cdot SK_v$；

$v=R\cdot PK_{rsu}$；

上述公式中，M_1中的参数是RSU计算验证消息所需要的参数，m_1表示要发送的消息，T_s表示时间戳，PID_v代表车辆的匿名，R为随机参数；

PK_{rsu}是路边单元RSU的公钥，SK_v为车辆的私钥，H是哈希函数；

SK_s为系统的私钥；

在计算Q、R时，先使用连接符将系统参数和消息m_1连接起来，然后对其进行哈希运算；RSU收到M_1后，计算参数：

$Q^*=H(SK_{rsu}\cdot PK_v||PID_v||m_1||T_s)$；

$R^*=H(PK_s\cdot SK_{rsu}||PK_{rsu}||T_s)$；

$z^*=Q\cdot PK_v$；

$v^*=R\cdot SK_{rsu}$

因为$PK_v=SK_v\cdot P$，$PK_{rsu}=SK_{rsu}\cdot P$，所以通过验证等式$z\cdot P+v=z^*+v^*\cdot P$是否成立来验证消息的可靠性；

若等式$z\cdot P+v=z^*+v^*\cdot P$成立，$m_1$通过RSU的验证，然后，中心车辆将共享信息加密并签名发送给5个从节点车辆。

5.如权利要求1所述的基于区块链的车辆安全通信方法，其特征在于，步骤(3)所述系统参数更新是对车辆通信时所用的相关参数应进行定时更新，如果密钥的有效性失效或者节点被攻击导致保密性降低，应对密钥进行更新；

系统密钥更新：当系统私钥SK_s和公钥PK_s的有效性到期，不能继续使用时，系统重新选取私钥SK'_s和公钥PK'_s，CA使用系统公钥PK_s，对新私钥SK'_s和公钥PK'_s进行加密，然后将加密后的参数上传至区块链网络，系统中的节点从区块链网络下载后使用原密钥解密就可以得到新的系统密钥；

更新车辆匿名PID_v：当车辆的假名有效性过期时，车辆从Z_q^*中随机选择参数r，计算$R=r\cdot P$，$U_{PIDv}=H(R,PK_s\cdot r,T_s,m)$，m是请求更新假名的信息；车辆使用$U_{PIDv}$加密假名$PID_v$和时间戳$T_s$得到$C_{PIDv}$，发送$M_u=\{C_{PIDv},R,T_s,m4\}$给LEA，LEA收到$M_u$后检验时间戳，若有效，则计算$U_{PIDv}=H(R,SK_s\cdot R,T_i,m)$，解密$C_{PIDv}$得到$PID_v$，如果$PID_v$是诚实节点，LEA为车辆形成新的假名$PID_v'$，将新的假名加密并签名发送给车辆；

车辆密钥更新：车辆密钥在以下情况下会申请更新，

第一，车辆的密钥已过期，需要更换新的密钥；

第二，车辆的密钥具有有效性，但车辆密钥的安全性受到威胁，可能已不具有保密性了；

车辆密钥更新具体步骤如下：

Step1：车辆生成新的密钥对$\{SK'_v,PK'_v\}$；

Step2：车辆向LEA发送密钥更新请求，加密请求内容并签名，请求包括车辆当前的公钥PK_v，新形成的公钥PK'_v；

Step3：LEA收到信息后，解密得到申请更换密钥的信息并验证；

Step4：验证通过，车辆更新密钥，将新的密钥对上传至区块链，替换原来的密钥对。

一种基于区块链的车辆安全通信方法

技术领域

[0001] 本发明涉及区块链技术领域，具体是一种基于区块链的车辆安全通信方法。

背景技术

[0002] 随着无线网络的快速发展，智能交通也取得了很大的进展，车联网开始受到广泛关注。车联网中车辆之间通过共享交通、路况等信息，能够提高车辆行驶效率，保护人们的生命和财产安全。安全和隐私保护是车联网必须首要解决的问题，传统车联网基于中心化，依靠一个可信赖的第三方。但是，中心化的系统存在单节点失败问题，目前除了通过法律手段，现有的技术无法确保存储在第三方数据库的数据安全。区块链是一个分布式的账本，它使用密码学和哈希函数将数据存储在块中，具有去中心化、不可篡改、匿名性、可追溯等优势。区块链的这些特点能够有效地保证车联网车辆的安全和隐私问题。基于区块链的车联网系统能够有效的解决系统数据的存储和通信的安全问题。只要系统中攻击者的计算力的总和不超过51％，系统就是安全的。

发明内容

[0003] 针对车联网车辆数据交换的安全和车辆隐私保护问题，本发明提出了一种能够有效地实现车联网中车辆安全通信的方法。相比传统车联网，本发明使用区块链技术取代可信的第三方，解决了单节点失败问题，实现车辆之间数据的安全交换。

[0004] 本发明一种基于区块链的车辆安全通信办法，包括以下步骤：

[0005] (1)车联网系统初始化，建立系统所需的参数，车辆进入时，向LEA发送证明自己身份的信息，系统中的验证节点对其身份进行验证；

[0006] (2)通过验证的车辆，由LEA向其颁发证书并记录车辆的身份信息，最后并上传至区块链，车辆和车辆、车辆和路边单元RSU通信，通信方式采取多边形网络组播方式；

[0007] (3)参数更新，系统中的参数在参数有效性到期或者可能被攻击，保密性受到威胁时进行参数的更新。

[0008] 步骤(1)所述系统初始化的过程包括：

[0009] 定义有限域$F_p=\{0,1,2,3\cdots p-1\}$，p为质数；

[0010] 选取椭圆曲线$E:y^2=x^3+ax+b$，其中$a,b\in F_p$，满足条件$4a^3+27b^2\neq 0(\mathrm{mod}\ p)$；

[0011] 定义q阶循环加法群G，G包含E中有限域内所有的点；

[0012] 基点P为椭圆曲线的生成元，$P\in G$；

[0013] 定义哈希函数：$H:\{0,1\}\rightarrow Z_q^*$；

[0014] 随机选择系统私钥$SK_s\in Z_q^*$，$PK_s=SK_s\cdot P$作为系统的公钥；

[0015] CA公布系统参数$\{p,q,E,PK_s,H\}$。

[0016] 步骤(1)所述车辆身份验证的过程如下：

[0017] 车辆进入系统时，向LEA发送能够证明自己身份的信息和公钥，例如车辆V向LEA发送身份ID_v和公钥PK_v，表示为$V\rightarrow LEA:S_(ID_v||PK_v)$，S_是发送函数；

[0018] 收到申请信息后，系统中的验证节点对车辆身份进行验证，并对合格的车辆进行签名，车辆收集不少于51％的验证节点的签名，作为诚实节点加入系统，LEA颁发电子通信证书给诚实车辆，记录其信息后上传至区块链中。

[0019] 步骤(2)所述的采取多边形网络组播的通信方式包括：

[0020] 车辆与车辆之间的通信，车辆与路边单元RSU的通信，共同构成多边形网络组播通信模型，模型包括两种通信类型：

[0021] 第一种，以一个车辆为中心，与其相邻的车辆和距离中心车辆最近的路边单元RSU构成多个三角形组成的多边形，这种情况下，中心车辆为主节点，RSU和其他车辆为从节点；

[0022] 第二种，以一个RSU为中心，与其相邻的车辆构成多个三角形组成的多边形，这种情况下，RSU为主节点，周围的车辆为从节点。

[0023] 在以车辆为中心的通信类型中，中心车辆是主节点，相邻车辆和距离中心车辆最近的路边单元RSU是从节点，每个主节点在其通信范围内最多5个从节点辆车，加上1个最近的RSU从节点构成多个三角形组成的多边形网络的从节点进行分组转发；

[0024] 主节点首先向从节点RSU发送消息，计算参数Q、R、z和v，然后，车辆发送$M_1=\{z,v,PID_v,m_1,T_s,R\}$到从节点RSU；

[0025] $Q=H(PK_{rsu}\cdot SK_v||PID_v||m_1||T_s)$；

[0026] $R=H(PK_{rsu}\cdot SK_s||PK_{rsu}||T_s)$；

[0027] $z=Q\cdot SK_v$；

[0028] $v=R\cdot PK_{rsu}$；

[0029] 上述公式中，M_1中的参数是RSU计算验证消息所需要的参数，m_1表示要发送的消息，T_s表示时间戳，PID_v代表车辆的匿名，R为随机参数；

[0030] PK_{rsu}是路边单元RSU的公钥，SK_v为车辆的私钥，H是哈希函数；

[0031] SK_s为系统的私钥；

[0032] 在计算Q、R时，先使用连接符将系统参数和消息m_1连接起来，然后对其进行哈希运算；RSU收到M_1后，计算参数：

[0033] $Q^*=H(SK_{rsu}\cdot PK_v||PID_v||m_1||T_s)$；

[0034] $R^*=H(PK_s\cdot SK_{rsu}||PK_{rsu}||T_s)$；

[0035] $z^*=Q\cdot PK_v$；

[0036] $v^*=R\cdot SK_{rsu}$

[0037] 因为$PK_v=SK_v\cdot P$，$PK_{rsu}=SK_{rsu}\cdot P$，所以通过验证等式$z\cdot P+v=z^*+v^*\cdot P$是否成立来验证消息的可靠性；

[0038] 若等式$z\cdot P+v=z^*+v^*\cdot P$成立，$m_1$通过RSU的验证，然后，中心车辆将共享信息加密并签名发送给5个从节点车辆。

[0039] 以RSU为中心的通信类型中，RSU为主节点，在其通信范围内最多6辆车，中心节点RSU将收集到的信息加密并签名发送给通信范围内的从节点，因为从RSU发送出的消息都是经过验证的，所以从节点车辆收到后消息解密即可得到路况交通信息。

[0040] 步骤(3)所述系统参数更新是对车辆通信时所用的相关参数应进行定时更新，如果密钥的有效性失效或者节点被攻击导致保密性降低，应对密钥进行更新；

[0041] 系统密钥更新：当系统私钥SK_s和公钥PK_s的有效性到期，不能继续使用时，系统重

新选取私钥SK'_s和公钥PK'_s，CA使用系统公钥PK_s，对新私钥SK'_s和公钥PK'_s进行加密，然后将加密后的参数上传至区块链网络，系统中的节点从区块链网络下载后使用原密钥解密就可以得到新的系统密钥；

[0042] 更新车辆匿名PID_v：当车辆的假名有效性过期时，车辆从Z_q^*中随机选择参数r，计算$R=r\cdot P$，$U_{PIDv}=H(R,PK_s\cdot r,T_s,m)$，m是请求更新假名的信息；车辆使用$U_{PIDv}$加密假名$PID_v$和时间戳$T_s$得到$C_{PIDv}$，发送$M_u=\{C_{PIDv},R,T_s,m4\}$给LEA，LEA收到$M_u$后检验时间戳，若有效，则计算$U_{PIDv}=H(R,SK_s\cdot R,T_i,m)$，解密$C_{PIDv}$得到$PID_v$，如果$PID_v$是诚实节点，LEA为车辆形成新的假名$PID_v'$，将新的假名加密并签名发送给车辆；

[0043] 车辆密钥更新：车辆密钥在以下情况下会申请更新，

[0044] 第一，车辆的密钥已过期，需要更换新的密钥；

[0045] 第二，车辆的密钥具有有效性，但车辆密钥的安全性受到威胁，可能已不具有保密性了；

[0046] 车辆密钥更新具体步骤如下：

[0047] Step1：车辆生成新的密钥对$\{SK'_v,PK'_v\}$；

[0048] Step2：车辆向LEA发送密钥更新请求，加密请求内容并签名，请求包括车辆当前的公钥PK_v，新形成的公钥PK'_v；

[0049] Step3：LEA收到信息后，解密得到申请更换密钥的信息并验证；

[0050] Step4：验证通过，车辆更新密钥，将新的密钥对上传至区块链，替换原来的密钥对。

[0051] 目前，车联网系统，系统参数的选取和通信加密采用双线性配对方法，双线性配对计算成本较高，本发明采用椭圆曲线加密算法，该算法安全性高并且计算成本较低。

[0052] 本发明的有益效果为：

[0053] 本发明通过验证节点对车辆身份信息验证，只有收到不少于51％验证节点的签名才能作为诚实节点进入通信网络，能够有效的阻止恶意车辆进入系统，除了LEA，网络的任何实体都不知道车辆的真实身份信息，保证了系统的安全和车辆的隐私。

[0054] 本发明使用多三角形构成的多边形组播通信方式。多边形通信网络中同时存在两种通信方式，分别是以车为主节点，相邻车辆和最近的RSU为从节点的通信类型和以路边单元RSU为主节点，相邻车辆为从节点的通信类型。通过多边形分组传播方式，系统中的车辆能够快速、便捷、准确的进行信息共享和信息同步。

[0055] 系统中产生的数据都保存在区块链中，相比传统的中心实体，不存在单节点失败的问题，而且数据存储在区块中，是不可篡改、不可否认的，信息的真实性和溯源性得到了有效的保障。

附图说明

[0056] 图1本发明的系统模型图。

[0057] 图2为本发明车辆身份认证的示意图。

[0058] 图3为本发明方法中以车辆为主节点的多三角形网络通信示意图。

[0059] 图4为本发明方法中以路边单元RSU为主节点的多三角形网络通信示意图。

[0060] 图5为本发明方法中由多个三角形构成的多边形系统通信网络示意图。

具体实施方式

[0061] 下面结合附图对本发明内容作进一步的详细说明，但不是对本发明的限定。

[0062] 本发明基于区块链的车辆安全通信系统模型图，如图1所示，系统主要包括LEA负责管理系统车辆的信息、授权CA向车辆颁发证书、密钥的更新。CA协助LEA向车辆颁发证书，负责系统密钥的更新，也是系统的验证节点。RSU路边单元，系统的验证节点，在车辆数据交换过程中与车辆交互，保证信息的准确性。

[0063] 本发明基于区块链的车辆安全通信方法，第一步，车联网系统初始化，建立系统所需的参数，车辆进入时，向LEA发送证明自己身份的信息，系统中的验证节点对其身份进行验证；

[0064] 系统初始化的过程包括：

[0065] 定义有限域$F_p=\{0,1,2,3\cdots p-1\}$，p为质数；

[0066] 选取椭圆曲线$E:y^2=x^3+ax+b$，其中$a,b\in F_p$，满足条件$4a^3+27b^2\neq 0(\mathrm{mod}\ p)$；

[0067] 定义q阶循环加法群G，G包含E中有限域内所有的点；

[0068] 基点P为椭圆曲线的生成元，$P\in G$；

[0069] 定义哈希函数：$H:\{0,1\}\rightarrow Z_q^*$；

[0070] 随机选择系统私钥$SK_s\in Z_q^*$，$PK_s=SK_s\cdot P$作为系统的公钥；

[0071] CA(Certificate Authority)公布系统参数$\{q,E,PK_s,H\}$。

[0072] 参照图2，车辆申请进入系统时，进行身份认证的结构图。该过程包括几个阶段：车辆申请、验证节点验证、收集签名、进入系统。车辆进入系统时，向LEA发送能够证明自己身份的信息和公钥，例如车辆V向LEA发送身份ID_v和公钥PK_v，表示为$V\rightarrow LEA:S_(ID_v||PK_v)$，S_是发送函数；

[0073] 收到申请信息后，系统中的验证节点对车辆身份进行验证，并对合格的车辆进行签名，车辆收集不少于51％的验证节点的签名，作为诚实节点加入系统，LEA颁发电子通信证书给诚实车辆，记录其信息后上传至区块链中。

[0074] 本发明基于区块链的车辆安全通信方法，第二步，通过验证的车辆，由LEA向其颁发证书并记录车辆的身份信息，最后并上传至区块链，车辆和车辆、车辆和路边单元RSU通信，通信方式采取多边形网络组播方式；

[0075] 车辆与车辆之间的通信，车辆与路边单元RSU的通信，共同构成多边形网络组播通信模型，模型包括两种通信类型：

[0076] 第一种，以一个车辆为中心，与其相邻的车辆和距离中心车辆最近的路边单元RSU构成多个三角形组成的多边形，这种情况下，中心车辆为主节点，RSU和其他车辆为从节点；

[0077] 第二种，以一个RSU为中心，与其相邻的车辆构成多个三角形组成的多边形，这种情况下，RSU为主节点，周围的车辆为从节点。

[0078] 参照图3，以车辆为中心的多三角通信模型图，在通信时，中心车辆是主节点，相邻车辆和距离中心车辆最近的路边单元RSU是从节点，每个主节点在其通信范围内最多最多5个从节点辆车，加上1个最近的RSU从节点构成多个三角形组成的多边形网络的从节点进行分组转发；

[0079] 主节点首先向从节点RSU发送消息，计算参数Q、R、z和v，然后，车辆发送$M_1=\{z,v,PID_v,m_1,T_s,R\}$到从节点RSU；

[0080] $Q=H(PK_{rsu}\cdot SK_v||PID_v||m_1||T_s)$；

[0081] $R=H(PK_{rsu}\cdot SK_s||PK_{rsu}||T_s)$；

[0082] $z=Q\cdot SK_v$；

[0083] $v=R\cdot PK_{rsu}$；

[0084] 上述公式中，M_1中的参数是RSU计算验证消息所需要的参数，m_1表示要发送的消息，T_s表示时间戳，PID_v代表车辆的匿名，R为随机参数；

[0085] PK_{rsu}是路边单元RSU的公钥，SK_v为车辆的私钥，H是哈希函数；

[0086] SK_s为系统的私钥；

[0087] 在计算Q、R时，先使用连接符将系统参数和消息m_1连接起来，然后对其进行哈希运算；RSU收到M_1后，计算参数：

[0088] $Q^*=H(SK_{rsu}\cdot PK_v||PID_v||m_1||T_s)$；

[0089] $R^*=H(PK_s\cdot SK_{rsu}||PK_{rsu}||T_s)$；

[0090] $z^*=Q\cdot PK_v$；

[0091] $v^*=R\cdot SK_{rsu}$

[0092] 因为$PK_v=SK_v\cdot P$，$PK_{rsu}=SK_{rsu}\cdot P$，所以通过验证等式$z\cdot P+v=z^*+v^*\cdot P$是否成立来验证消息的可靠性；

[0093] 若等式$z\cdot P+v=z^*+v^*\cdot P$成立，$m_1$通过RSU的验证，然后，中心车辆将共享信息加密并签名发送给5个从节点车辆。

[0094] 以路边单元RSU为中心的多三角通信模型，如图4所示。路边单元将收集到的信息传送给附近的车辆，RSU将信息加密并签名发送到相邻的从节点车辆。从节点车辆收到信息后，解密即可得到附近的路况、位置等交通信息。

[0095] 上述的两种通信方式在系统通信网络同时存在，如图5所示。图3作为主节点的车辆可能是另一组节点通信的从节点，而作为从节点的路边单元RSU也可能是另一组的主节点。

[0096] 本发明基于区块链的车辆安全通信方法，第三步，参数更新，系统中的参数在参数有效性到期或者可能被攻击，保密性受到威胁时进行参数的更新；

[0097] 系统参数更新是对车辆通信时所用的相关参数应进行定时更新，如果密钥的有效性失效或者节点被攻击导致保密性降低，应对密钥进行更新；

[0098] 系统密钥更新：当系统私钥SK_s和公钥PK_s的有效性到期，不能继续使用时，系统重新选取私钥SK'_s和公钥PK'_s，CA使用系统公钥PK_s，对新私钥SK'_s和公钥PK'_s进行加密，然后将加密后的参数上传至区块链网络，系统中的节点从区块链网络下载后使用原密钥解密就可以得到新的系统密钥；

[0099] 更新车辆匿名PID_v：当车辆的假名有效性过期时，车辆从Z_q^*中随机选择参数r，计算$R=r\cdot P$，$U_{PIDv}=H(R,PK_s\cdot r,T_s,m)$，m是请求更新假名的信息；车辆使用$U_{PIDv}$加密假名$PID_v$和时间戳$T_s$得到$C_{PIDv}$，发送$M_u=\{C_{PIDv},R,T_s,m4\}$给LEA，LEA收到$M_u$后检验时间戳，若有效，则计算$U_{PIDv}=H(R,SK_s\cdot R,T_i,m)$，解密$C_{PIDv}$得到$PID_v$，如果$PID_v$是诚实节点，LEA为车辆形成新的假名$PID_v'$，将新的假名加密并签名发送给车辆；

[0100] 车辆密钥更新：车辆密钥在以下情况下会申请更新，

[0101] 第一，车辆的密钥已过期，需要更换新的密钥；

[0102] 第二,车辆的密钥具有有效性,但车辆密钥的安全性受到威胁,可能已不具有保密性了;

[0103] 车辆密钥更新具体步骤如下:

[0104] Step1:车辆生成新的密钥对$\{SK'_v, PK'_v\}$;

[0105] Step2:车辆向LEA发送密钥更新请求,加密请求内容并签名,请求包括车辆当前的公钥PK_v,新形成的公钥PK'_v;

[0106] Step3:LEA收到信息后,解密得到申请更换密钥的信息并验证;

[0107] Step4:验证通过,车辆更新密钥,将新的密钥对上传至区块链,替换原来的密钥对。

[0108] 本发明在车辆通信时使用的系统密钥、车辆密钥和车辆假名,系统会设置一个有效期,到期要进行更新,才能继续使用。密钥和假名的动态更新,可以增强系统的安全性,降低被攻击的风险。车辆的密钥动态生成,使得车辆之间的数据交换过程变的更安全。

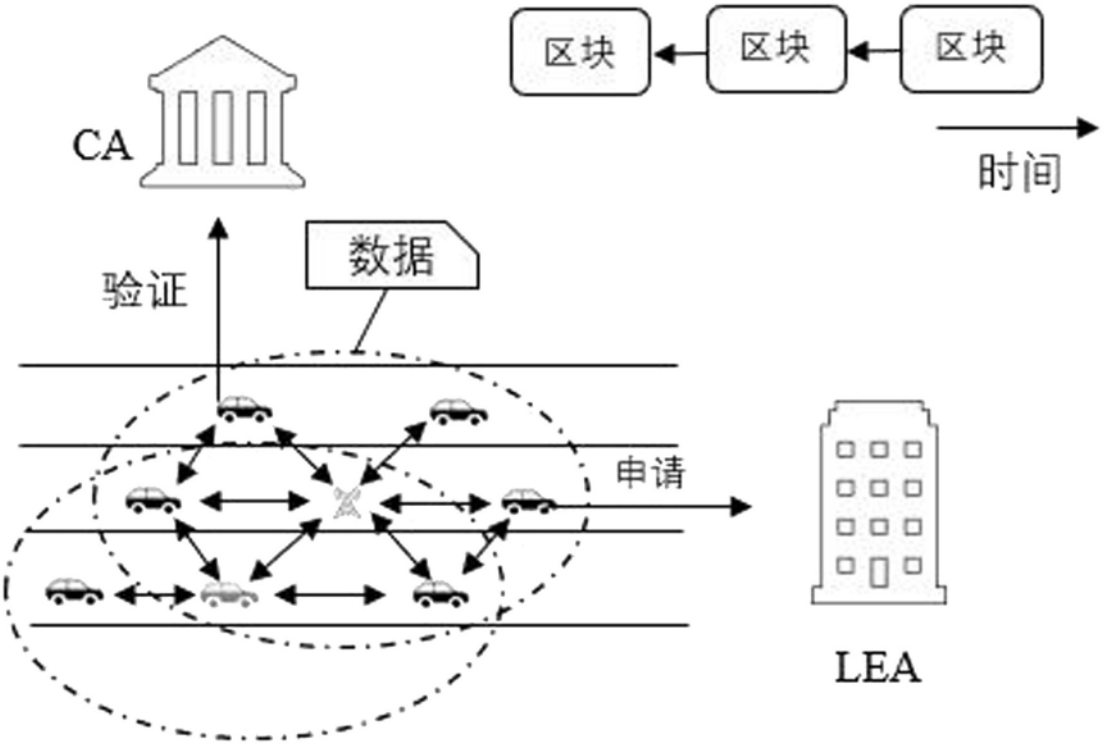


图1

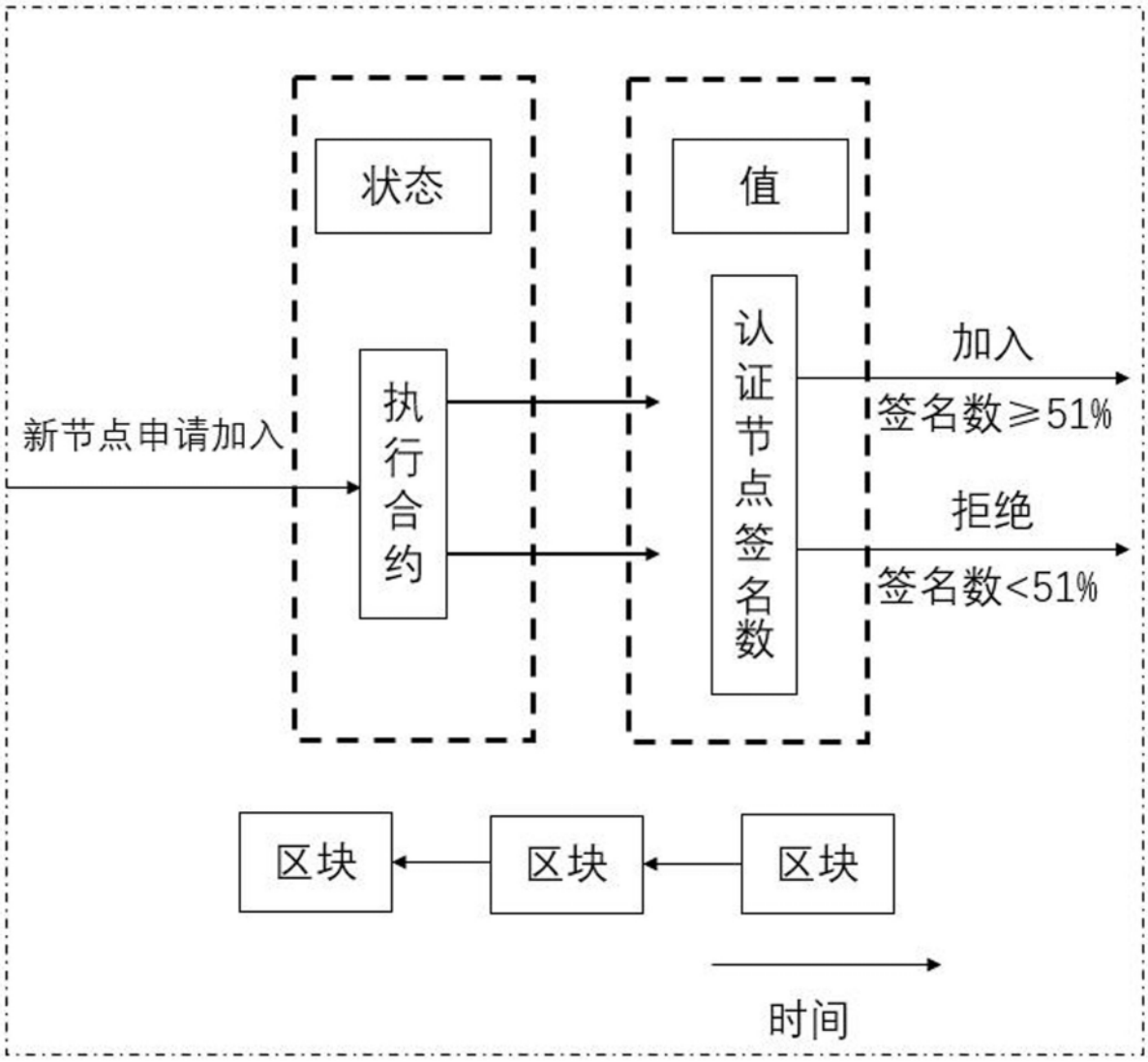


图2

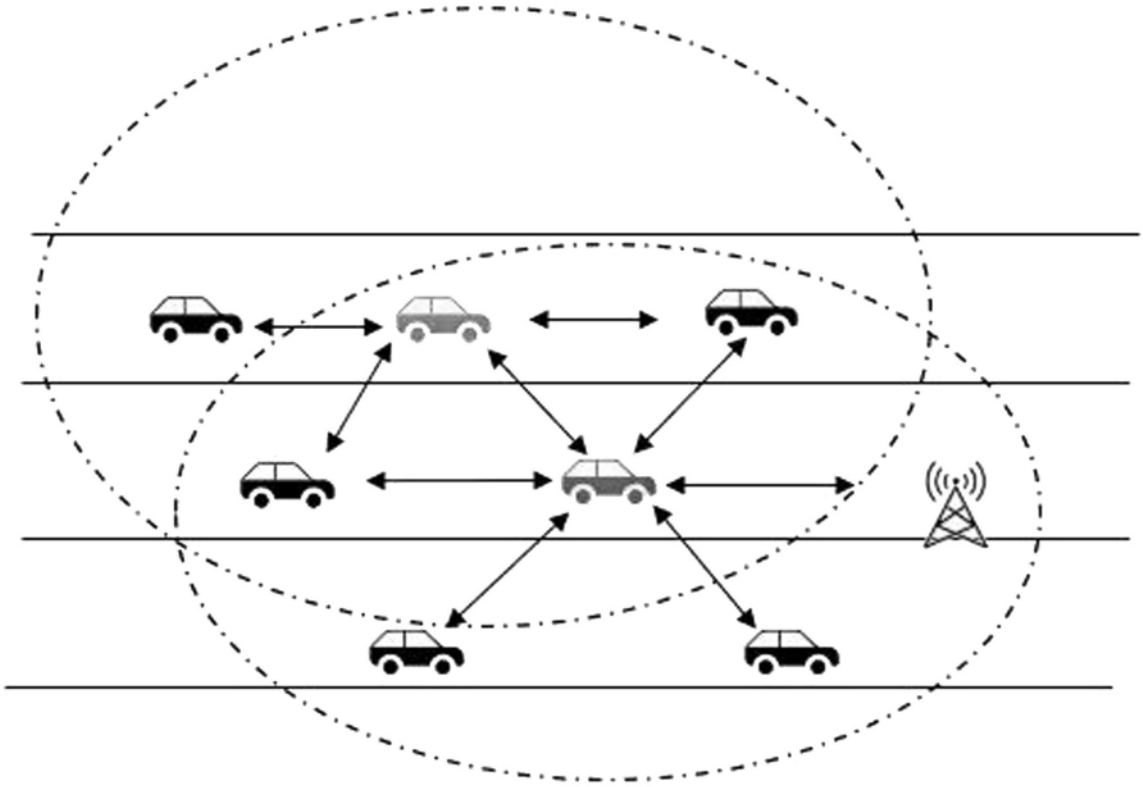


图3

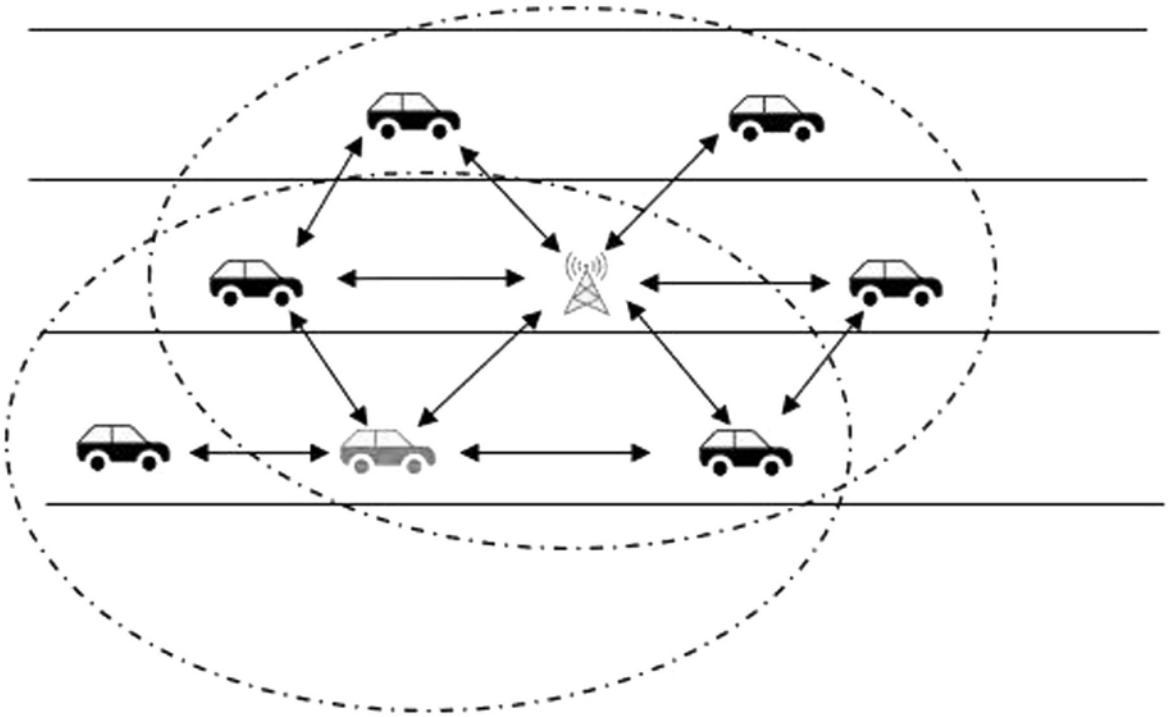


图4

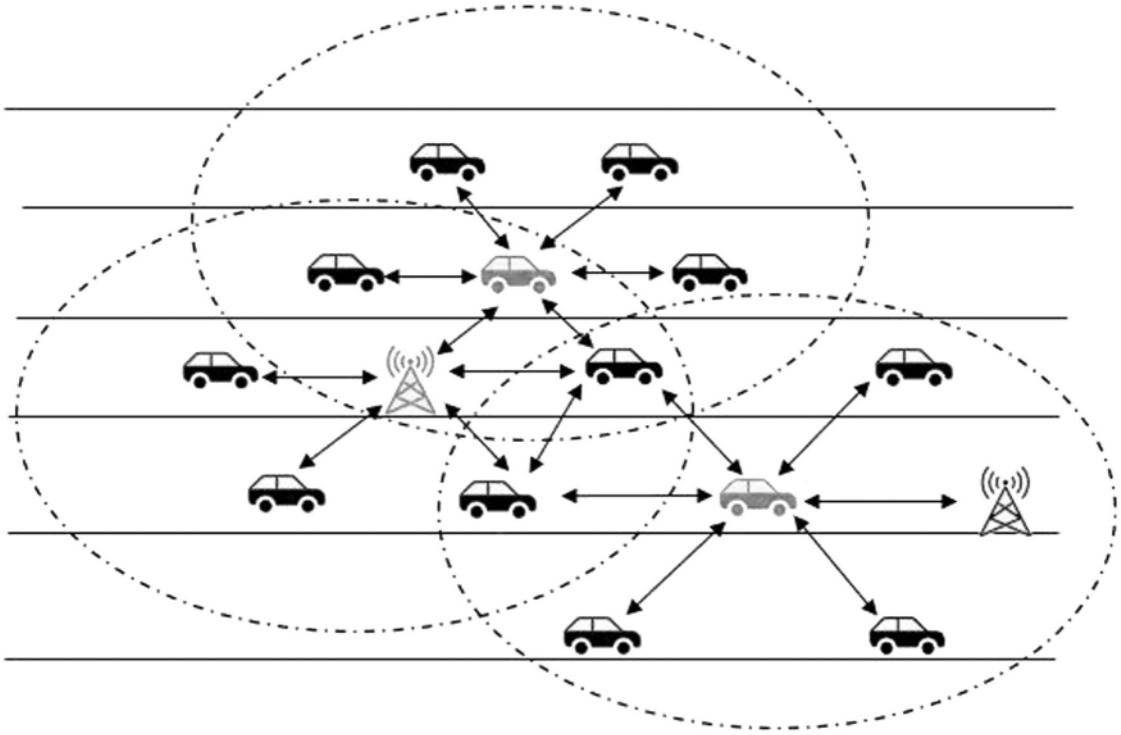


图5