车联网中可证安全的匿名可追溯快速组认证协议

张海波[1,2]，黄宏武[1,2]，刘开健[1,2]，贺晓帆[3]

（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 移动通信技术重庆市重点实验室，重庆 400065；
3. 武汉大学电子信息学院，湖北 武汉 430072）

摘 要：身份认证是车辆接入车联网（IoV）的第一道防线。然而现有方案还不能满足 IoV 的高效认证需求，也不能实现快速的匿名追溯。鉴于此，提出了一种 IoV 中双向匿名可追溯组认证协议。该协议先将多个路侧单元（RSU）进行快速动态的分组，并对进入 RSU 组的车辆利用切比雪夫混沌映射的单向陷门性和半群特性进行接入认证，当车辆在组内的 RSU 之间切换时采用反向哈希链进行快速切换认证。另外，组内 RSU 可以对恶意车辆进行身份的匿名追溯，并利用区块链对其身份进行快速撤销，还可以对泄露真实身份的用户进行 ID 的自由变更。同时运用随机预言机模型证明了协议的语义安全性。最后，通过仿真验证了该方案具有良好的安全性和有效性。

关键词：车联网；匿名追溯；混沌映射；组认证；反向哈希链；区块链

中图分类号：TN915.08

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021073

Verifiably secure fast group authentication protocol with anonymous traceability for Internet of vehicles

ZHANG Haibo[1,2], HUANG Hongwu[1,2], LIU Kaijian[1,2], HE Xiaofan[3]

1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. Chongqing Key Laboratory of Mobile Communication Technology, Chongqing 400065, China
3. School of Electronic Information, Wuhan University, Wuhan 430072, China

Abstract: Identity authentication is the first line of defense for vehicles to access IoV (Internet of vehicles). However, the existing schemes cannot meet the requirements of efficient authentication of IoV well, nor can they realize fast anonymous traceability. In view of this, a bidirectional anonymous traceability group authentication protocol was proposed in IoV. In this protocol, a number of RSU (road side unit) were grouped quickly and dynamically. And the vehicles entering the RSU group were authenticated with the one-way trap gating property and semi-group property of Chebyshev chaotic map. When the vehicle switched between the RSU within a group, the reverse hash chain was used for fast handover authentication. In addition, the RSU within a group can trace anonymously and revoke the identity of malicious vehicles quickly by using blockchain, and can also freely change the ID of users who reveal their real identity. At the same time, the semantic security of the proposed protocol is proved by using the random predictor model. Finally, simulation results show the proposed scheme has good security and effectiveness.

Keywords: IoV, anonymous traceability, chaotic mapping, group authentication, reverse Hash chain, blockchain

---

收稿日期：2020−12−17；**修回日期：**2021−03−03

基金项目：国家自然科学基金资助项目（No.61801065）；长江学者和创新团队发展计划基金资助项目（No.IRT16R72）；重庆市留创计划创新类基金资助项目（No.cx2020059）；重庆市基础与前沿基金资助项目（No.cstc2018jcyjAX0463）

Foundation Items: The National Natural Science Foundation of China (No.61801065), The Program for Changjiang Scholars and Innovative Research Team in University (No.IRT16R72), Chongqing Innovation and Entrepreneurship Project for Returned Overseas Chinese Scholars (No.cx2020059), The General Project on Foundation and Cutting-edge Research Plan of Chongqing (No.cstc2018jcyjAX0463)

1 引言

近年来，无线通信技术、云计算、自动驾驶技术、万物互联等技术[1]的发展大大促进了车联网（IoV, Internet of vehicles）的发展。IoV 具有动态拓扑结构、网络规模庞大、节点分布不均匀、节点移动性强、移动轨迹可预测等特点，使其更易遭受如仿冒攻击、重放攻击、中间人攻击等，因此隐私与安全问题成为制约 IoV 发展的关键[2]。接入认证是在车辆接入 IoV 之前确认其身份的合法性，阻止非法车辆进入 IoV[3-4]。安全、高效的接入认证方案是解决隐私安全问题的有效手段之一。

由于 IoV 的特点，使车辆的接入认证协议需要具备多重安全属性。匿名性是其中一个重要属性，然而由于车辆用户量巨大，假名的存储与管理显得格外重要。车路协同是智慧交通中的一个重要概念，它需要车辆与路侧单元（RSU, road side unit）之间不断交换信息，因此在实现接入认证的同时生成会话密钥是必要的。车辆以合法身份完成接入认证，仍然存在非法行为的可能，因此需要认证后的身份可追溯性以及身份撤销来保证车辆的实时安全性。车辆的高速移动性使车辆频繁地在多个 RSU 之间快速切换，因此低时延的接入认证与快速的切换认证是 IoV 认证协议的必然要求。

针对车辆的假名问题，已有一些学者对其展开了研究[5-7]。Freudiger 等[5]为了增强车辆的位置隐私，提出在车辆网络（VN, vehicle network）的适当位置创建混合区，然而该方案需要预存大量匿名证书，占用大量内存。Lu 等[6]在假设车与 RSU 能主动协作的前提下，提出通过运行两轮协议，使车向 RSU 申请一个短时间的匿名证书来克服预存大量证书的问题。然而，Zhang 等[7]指出由于车辆需要频繁变更假名，车与 RSU 的频繁交互会影响 IoV 的效率，并在此基础上提出了一种分散式组认证协议，用每个 RSU 维护其通信范围内的一个组，车辆加入组前对其身份进行认证，如果组内成员发现其他成员的非法行为，还可对其真实身份进行追溯。然而文献[7]中并没有提出追溯身份的具体方案，而且使用的是耗时的双线性映射运算。

针对 IoV 认证中的效率与安全问题，也有一些学者对其展开了研究[8-14]。Jiang 等[8]通过二进制认证树实现了消息签名的批量验证，然而该方案依赖于半可信的 RSU。Yao 等[9]指出 IoV 通信中，通信双方的 MAC 地址容易泄露，造成车辆易被追踪，基于此，提出了一种数据链路层生物特征加密的匿名认证方案，然而利用生物特征加密的方案本来就存在如生物特征难以提取、设备成本高等诸多问题。Jiang 等[10]为了克服检查证书撤销列表（CRL, certificate revocation list）的诸多缺点，提出用哈希验证码（HMAC, Hash message authentication code）来代替 CRL，然而该方案依赖于公钥基础设施（PKI, public key infrastructure）。Ying 等[11]利用哈希函数快速计算的特点设计了一种轻量级的认证方案，实现了车载单元（OBU, on broad unit）、RSU 与可信机构（TA, trusted authority）三者间的相互认证，然而该方案无法抵御重放攻击和修改攻击，也无法实现身份追溯。Liu 等[12]利用 k-双线性 DH 反演（k-BDHI, k-bilinear Diffie-Hellman inversion）的困难性问题设计了一种 OBU 与 RSU 的无证书短签名认证方案，该方案可实现两者间的高效认证与匿名追溯功能，然而该方案需要引入追溯机构（TBA, trace back authority）。Zhao 等[13]针对传统认证方案容易受到仿冒攻击和内部攻击等问题，提出了一种新的匿名认证方案，该方案满足多重安全属性，然而由于进行了多次非对称加解密，其认证时延较大。Cui 等[14]利用低时延的混沌映射设计了一种基于雾的认证方案，该方案用雾头代替 RSU 来实现 OBU 与 TA 间的认证，然而该方案同样无法实现匿名追溯。针对切换认证也有许多研究[15-16]，然而它们都存在计算时延较大的问题。

区块链源于中本聪 2008 年发表的论文“比特币：一个点对点的电子现金系统”[17]，它是一种按照时间顺序将生成的数据区块顺序连接的数据结构，本质上是一个不可篡改的分布式账本。区块链技术是处理车辆管理和数据传输方面的有效技术，通过合理构建车辆区块链可以有效解决 IoV 中的广播冲突避免、资源调度和隐私保护等诸多问题[18]。促进区块链技术与 IoV 的深度融合是 IoV 发展的必然趋势。

综上所述，现有的认证协议大多缺乏低时延的匿名可追溯性。基于此，本文在区块链架构下，提出了一种适用于 IoV 的快速匿名可追溯组认证方案。该方案可以实现 OBU 的安全接入、RSU 的动态分组、恶意车辆的快速撤销以及用户 ID 的自由变更。此外，考虑到车辆的高速移动性，本文还设计了一种高效的切换认证协议。然后，本文利用随

机预言机模型对协议的语义安全性进行了证明。最后的仿真结果验证了本文协议在效率和安全性能方面的优越性。

2　系统模型与安全需求

2.1　系统模型

当车辆需要获取 IoV 服务时，必须先进行接入认证。考虑到 RSU 是半可信的，用单个 RSU 维护车辆信息容易造成隐私泄露，因此本文动态地将多个 RSU 分成一组共同维护车辆信息。系统模型如图 1 所示，涉及 3 个实体，分别是 TA、RSU、OBU。

TA。TA 是车辆注册和认证的机构，可通过区块链查询撤销 ID，拥有最高的安全性、足够的计算资源和内存，是绝对可信的。

RSU。RSU 是区块链节点，可收集道路信息并与车辆实现数据交互，引导车辆安全行驶，是车路协同、智慧交通的关键设施，是半可信的。

OBU。OBU 是车辆与 RSU 或车辆之间进行通信的设备，可信程度最低。

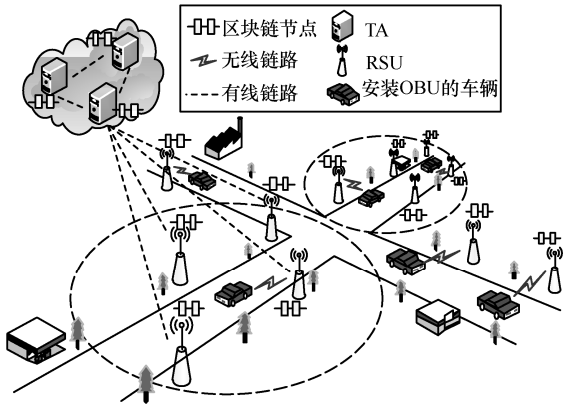


图 1　系统框架

2.2　安全需求

为确保 IoV 的通信安全，认证协议应该满足完整性、身份认证、保密性、不可否认性、可用性、可扩展性、时间约束、前向安全、后向安全[19]。本文将其总结为以下安全属性。

1) 双向认证。由于 IoV 使用开放链路进行通信，容易遭受各种攻击，因此需要 OBU 与 TA 之间实现双向认证。

2) 匿名性。车辆隐藏真实 ID，不断变更假名进行通信，可以有效减少被追踪的可能性。因此需要具备匿名性。

3) 可追溯性。车辆能以合法身份完成认证，但是当合法车辆做出非法行为时，需要追溯出匿名车辆的真实 ID。

4) 快速撤销。在 3)中得出真实 ID 后，需要将其加入撤销列表，以便后续查询。

5) 会话密钥安全。由于 OBU 与 RSU 需要经常交换信息，因此协议应该生成具有前向安全和后向安全的会话密钥。

6) 用户 ID 的自由变更。当真实 ID 泄露后，用户应具有自由变更 ID 的权利。

双向认证的协议流程保证了完整性、身份认证和时间约束。匿名性保证了协议的保密性。可追溯性和快速撤销保证了协议的不可否认性。会话密钥的前向安全和后向安全保证了数据的前向安全和后向安全。

3　基于 IoV 的认证协议

为满足 IoV 的安全需求，该方案分为 5 个阶段，分别是系统初始化阶段、注册阶段、接入认证与切换认证阶段、匿名追溯与身份撤销阶段、用户 ID 变更阶段。方案涉及的参数及含义如表 1 所示。

表 1　　方案涉及的参数及含义

参数	含义
p	一个大素数
h_0, h_1, h_2	哈希函数
$f(u)$	掩蔽函数
$\mathrm{sd}_1, \mathrm{sd}_2$	哈希函数的初始值
L', L	RSU 组的组长
OBU_i	车辆 V_i 对应的 OBU
RSU_i	RSU 组的第 i 个 RSU
$\mathrm{GID}_V{}^i$	第 i 个 RSU 组内的车辆组标识
$\mathrm{PID}_V{}^i$	RSU_i 范围内 OBU_i 的假名
$\oplus$	异或运算
$\|\|$	连接符
RID	RSU 的身份标识
ID_{V_i}	OBU_i 的身份标识
$T_{n_j}(x) (\mathrm{mod}\ p)$	切比雪夫混沌映射[20]
E / D	加密/解密
$T_{V_i^n}, T_{R_i^n}$	时间戳

3.1　系统初始化阶段

在车辆进行认证之前，需要先进行系统初始化。首先定义 $h_0^n(x) = h_0(h_0^{n-1}(x)), n \in Z_q^*$ 且

$h_0^0(x)=x$，然后定义运算

$$\sum_{j=1}^{j=L_0}\oplus T_{n_j}(x)(\mathrm{mod}\ p)=T_{n_1}(x)(\mathrm{mod}\ p)\oplus T_{n_2}(x)(\mathrm{mod}\ p)\oplus\cdots\oplus T_{n_{L_0}}(x)(\mathrm{mod}\ p), j\in N^* \tag{1}$$

TA 负责系统初始化。TA 确定 3 个哈希函数 $h_0,h_1,h_2:\{0,1\}^*\to\{0,1\}^l$，其中 l 为哈希函数的位宽。随机选择 $\mathrm{sd}_1,\mathrm{sd}_2\in Z_q^*$ 作为 h_1,h_2 的哈希种子，接下来，存在 2 种情况。

1) 组长由 L' 变为 L，计算 $h_1^L=h_1^L(\mathrm{sd}_1)$，选择 L 个随机数 $\{n_j\mid j\in[1,L],\ j\in Z_q^*\}$，将其通过安全通道发送给车辆预测轨迹上的 L 个 RSU，计算式(2)和式(3)。

$$T_{n_j}=\sum_{j=1}^{L}\oplus T_{n_j}(x)(\mathrm{mod}\ p) \tag{2}$$

$$f(u)=\mathrm{sd}_2+\prod_{j=1}^{L}(u-n_j) \tag{3}$$

2) 连续多个组的组长 L 保持不变，则 TA 在第 k 组计算 $h_1^L=h_1^L(\mathrm{sd}_1)$、式(4)和式(5)，其中 $L',L,k\in Z_q^*$。

$$T_{h_{n_j}}=\sum_{j=1}^{j=L}\oplus T_{h_0^{k-1}(n_j)}(x) \tag{4}$$

$$f(u)=\mathrm{sd}_2+\prod_{j=1}^{L}(u-h_0^{k-1}(n_j)) \tag{5}$$

TA 公布系统参数 $\{x,T(*),f(u),h_0,h_1,h_2\}$。

3.2 注册阶段

在此阶段，OBU_i、RSU_i 在 TA 上完成 ID 注册。

OBU_i 的注册。OBU_i 将要注册的 ID_{V_i} 通过安全通道发送给 TA，TA 收到后随机选择 $r\in Z_q^*$，计算 $T_r=T_r(x)(\mathrm{mod}\ p)$，$\mathrm{GID}_V{}^0=\mathrm{ID}_{V_i}\oplus T_{h_{n_j}}$，保存 $(\mathrm{GID}_V{}^0,\mathrm{ID}_{V_i},T_r)$，后续车辆 V_i 每进入一个新的 RSU 组就更新一次 GID。然后将 $<\mathrm{GID}_V{}^0,\mathrm{ID}_{V_i},T_r>$ 通过安全通道发回 OBU_i。OBU_i 保存收到的 $\mathrm{GID}_V{}^0$ 和 T_r。

RSU_i 的注册。RSU_i 将要注册的 RID 通过安全通道发送给 TA，TA 收到后计算并保存 $h_R=h_0(\mathrm{RID})$，产生一个由 h_R 构成的列表。

3.3 接入认证与切换认证阶段

车辆在进入 RSU 的范围时需要首先完成身份认证。具体可分为接入认证和切换认证 2 个阶段。接入认证和切换认证流程分别如图 2 和图 3 所示，具体步骤如下。

阶段 1 车辆加入 RSU 组的接入认证。在此阶段，OBU、RSU 与 TA 完成相互认证。

步骤 1 OBU_i 随机选择 $s,\gamma_i\in Z_q^*$，计算 $T_{sr}=T_s(T_r)(\mathrm{mod}\ p)$，$\mathrm{OA}=h_0(T_{sr}\|\gamma_i)$，$T_s=T_s(x)(\mathrm{mod}\ p)$，$W_1=h_0(\mathrm{GID}_V{}^{i-1}\|\mathrm{OA}\|T_s\|\gamma_i\|T_{V_i}\|T_r)$，发送 $<\mathrm{GID}_V{}^{i-1},\mathrm{OA},T_s,\gamma_i,T_{V_i},W_1>$ 给 RSU_1。

步骤 2 RSU_1 验证 $T_0-T_{V_i}<\Delta t$ 是否成立，其中 T_0 为系统当前时间，Δt 为预设的一个有效时间间隔，若成立则计算 $\mathrm{RA}=h_0(\mathrm{RID})\oplus\mathrm{OA}$，发送 $<\mathrm{GID}_V{}^{i-1},\mathrm{OA},T_s,\gamma_i,\mathrm{RA},T_{V_i},T_{R_i},W_1>$ 给 TA。

步骤 3 TA 验证 $T_1-T_{R_i}<\Delta t$ 是否成立，成立则计算 $W_1^*=h_0(\mathrm{GID}_V{}^{i-1}\|\mathrm{OA}\|T_s\|\gamma_i\|T_{V_i}\|T_r)$，验证 $W_1^*\overset{?}{=}W_1$，若相等则计算 $h_0^*(\mathrm{RID})=\mathrm{RA}\oplus\mathrm{OA}$，判断 $h_R\overset{?}{=}h_0^*(\mathrm{RID})$，如果相等则继续计算 $T_{rs}=T_r(T_s)(\mathrm{mod}\ p)$，$\mathrm{OA}^*=h_0(T_{rs}\|\gamma_i)$，判断 $\mathrm{OA}^*\overset{?}{=}\mathrm{OA}$，相等则计算 $\mathrm{sd}_1^*=h_0(T_{rs})\oplus\mathrm{sd}_1$，组长 L 不变时计算 $\mathrm{GID}_V{}^i=\mathrm{ID}_{V_i}\oplus T_{n_j}$，组长由 L' 变更为 L 时计算 $\mathrm{GID}_V{}^i=\mathrm{ID}_{V_i}\oplus T_{h_{n_j}}$，将 OBU_i 的信息更新为 $(\mathrm{GID}_V{}^i,\mathrm{ID}_{V_i},T_r)$，最后计算 $W_2=h_0(\mathrm{GID}_V{}^i\|\mathrm{sd}_1^*\|\ h_1^L\|T_{R_i^1}\|T_r)$，发送 $<\mathrm{GID}_V{}^i,\mathrm{sd}_1^*,h_1^L,T_{R_i^1},W_2>$ 给 RSU_1。

步骤 4 RSU_1 验证 $T_2-T_{R_i^1}<\Delta t$ 是否成立，成立则计算 $\mathrm{sd}_2=f(n_1)$，$h_2^L=h_2^L(\mathrm{sd}_2)$，随机选择 $z_1\in Z_q^*$，计算 $T_{z_1}=T_{z_1}(x)(\mathrm{mod}\ p)$，$T_{z_1s}=T_{z_1}(T_s)(\mathrm{mod}\ p)$，发送 $<\mathrm{GID}_V{}^i,\mathrm{sd}_1^*,h_1^L,h_2^L,T_{z_1},T_{R_i^1},T_{V_i^1},W_2>$ 给 OBU_i。并将 $<\mathrm{GID}_V{}^i,T_s,T_{z_1s},h_1^L,h_2^L>$ 通过安全通道发送给 RSU_2 以完成后续的切换认证。

步骤 5 OBU_i 验证 $T_3-T_{V_i^1}<\Delta t$ 是否成立，成立则计算 $W_2^*=h_0(\mathrm{GID}_V{}^i\|\mathrm{sd}_1^*\|h_1^L\|T_{R_i^1}\|T_r)$，判断 $W_2^*\overset{?}{=}W_2$，如果相等则计算 $\mathrm{sd}_1=h_0(T_{\mathrm{sr}})\oplus\mathrm{sd}_1^*$，$(h_1^L)^*=h_1^L(\mathrm{sd}_1)$，判断 $(h_1^L)^*\overset{?}{=}h_1^L$，如果相等则计算 $T_{sz_1}=T_s(T_{z_1})(\mathrm{mod}\ p)$，$h_{sz_1}=h_0(T_{sz_1})$，发送 $<\mathrm{GID}_V{}^i,h_{sz_1},T_{V_i^2}>$ 给 RSU_1。

步骤 6 RSU_1 验证 $T_4-T_{V_i^2}<\Delta t$ 是否成立，成立则判断 $h_{sz_1}\overset{?}{=}h_0(T_{z_1s})$，如果相等则认证通过。会话

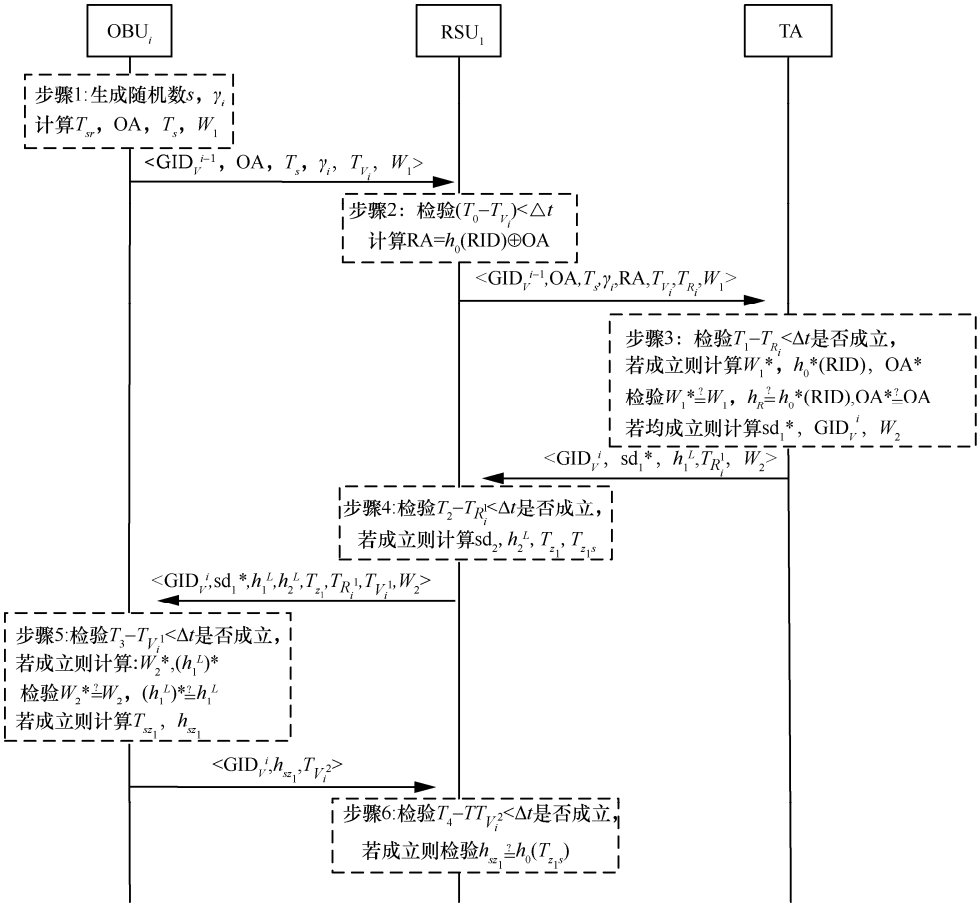


图 2　接入认证流程

密钥为 T_{sz_1}。

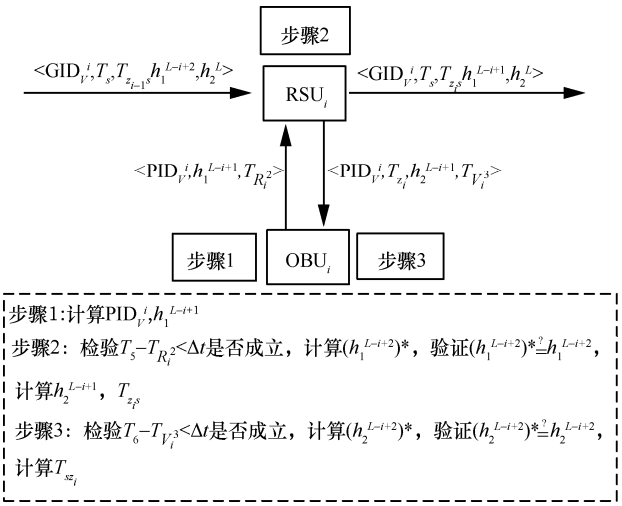


图 3　切换协议流程

阶段 2　车辆在组内的切换认证。

当车辆在组内的 RSU 之间切换时需要进行快速的切换认证。RSU$_i$ 利用 h_2 计算出 L，继续计算 $(\mathrm{PID}_V{}^i)^* = h_0(\mathrm{GID}_V{}^i \| h_1^{L-i+2} \| T_{sz_{i-1}})$，保存 $(\mathrm{GID}_V{}^i, (\mathrm{PID}_V{}^i)^*, T_s, L, h_1^{L-i+2}, h_2^L)$ 到表 Γ_p。

定义反向哈希链为 $h_0^{\lambda}(x) \leftarrow h_0^{\lambda-1}(x) \leftarrow \cdots \leftarrow h_0^1(x) \leftarrow h_0^0(x), \lambda \in N$。RSU 与 OBU 通过反向哈希链并利用图 4 的原理完成切换认证。由于 L 可能改变，因此切换认证存在 2 种情况。当 L 改变时，具体过程如下。

步骤 1　OBU$_i$ 计算 RSU$_i$ 处的临时假名 $\mathrm{PID}_V{}^i = h_0(\mathrm{GID}_V{}^i \| h_1^{L-i+2} \| T_{sz_{i-1}})$，继续计算 $h_1^{L-i+1} = h_1^{L-i+1}(\mathrm{sd}_1)$，发送 $<\mathrm{PID}_V{}^i, h_1^{L-i+1}, T_{R_i^2}>$ 给 RSU$_i$。

步骤 2　RSU$_i$ 检验 $T_5 - T_{R_i^2} < \Delta t$ 是否成立，如果成立则在表 Γ_p 中查找与 $\mathrm{PID}_V{}^i$ 相等的 $(\mathrm{PID}_V{}^i)^*$，继续计算 $(h_1^{L-i+2})^* = h_1(h_1^{L-i+1})$，判断 $(h_1^{L-i+2})^* \stackrel{?}{=} h_1^{L-i+2}$，若成立则计算 $h_2^{L-i+1} = h_2^{L-i+1}(\mathrm{sd}_2)$，随机选择 $z_i \in Z_q^*$，并计算 $T_{z_i} = T_{z_i}(x) (\mathrm{mod}\, p)$，$T_{z_i s} = T_{z_i}(T_s) (\mathrm{mod}\, p)$，发送 $<\mathrm{PID}_V{}^i, T_{z_i}, h_2^{L-i+1}, T_{V_i^3}>$ 给 OBU$_i$，并通过安全通道发送 $<\mathrm{GID}_V{}^i, T_s, T_{z_i s}, h_1^{L-i+1}, h_2^L>$ 给 RSU$_{i+1}$。

步骤 3　RSU$_i$ 检验 $T_6 - T_{V_i^3} < \Delta t$ 是否成立，如

果成立则计算 $(h_2^{L-i+2})^*=h_2(h_2^{L-i+1})$，判断 $(h_2^{L-i+2})^* \stackrel{?}{=} h_2^{L-i+2}$，相等则认证通过，计算会话密钥 $T_{sz_i}=T_s(T_{z_i}) \pmod p$。

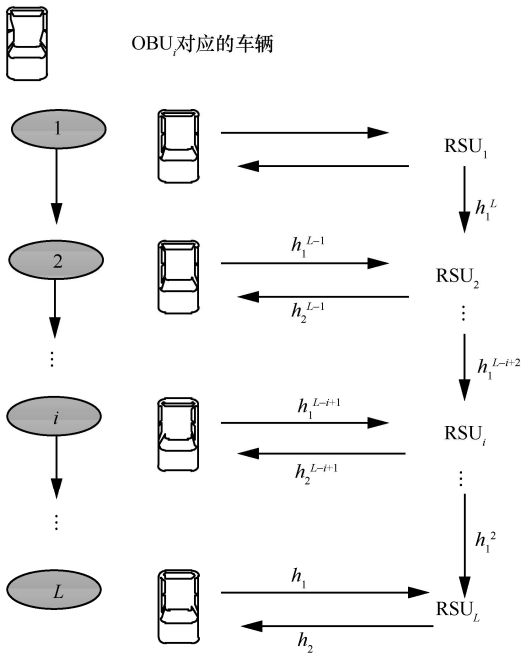


图 4 切换认证原理

当连续多个组的组长保持为 L 不变时，第 $k-1$ 组的 RSU$_i$ 完成切换认证后计算 $h_0^{k-1}(n_i)=h_0(h_0^{k-2}(n_i))$，通过安全通道将其发送给 k 组的 RSU$_{L+i}$，RSU$_{L+i}$ 将其代入式(5)计算 sd_2，然后利用其他哈希函数构成的反向哈希链和上述切换认证的方法进行认证。

3.4 匿名追溯与身份撤销阶段

在此阶段，RSU 组成员可以追溯恶意车辆的真实 ID，并将其加入撤销区块链。

1) 匿名追溯。RSU$_i$ 检测到 OBU$_i$ 存在恶意行为，在组长为 L 的组内广播追溯其真实身份的请求，其他组成员验证无误后计算 $T_{h_0^{k-1}(n_j)}(x)$，然后分别将其发送给 RSU$_i$，RSU$_i$ 计算式(6)恢复 OBU$_i$ 的真实 ID。

$$\mathrm{ID}=\mathrm{GID}_V{}^i \oplus \sum_{j=1}^{j=L} \oplus T_{h_0^{k-1}(n_j)}(x) \tag{6}$$

其中，$k=1$ 对应组长改变的初始化阶段。

2) 身份撤销。匿名追溯完成后，系统需要将恶意车辆 ID 更新到区块链。撤销区块链更新流程如图 5 所示，具体方法如下。

RSU$_i$ 发现恶意车辆 OBU$_i$，RSU 组成员利用前文的匿名追溯方法恢复真实 ID。RSU$_i$ 将恢复出的 ID 加入自己的待撤销列表并广播撤销 ID，其他节点验证无误后，将其加入自己的待撤销列表。然后通过共识算法选择节点将待撤销列表打包成区块上传到区块链，RSU 和 TA 节点均可以通过查询区块链检查车辆 ID 是否被撤销。

上述过程中的共识算法可采用改进的 PBFT 算法。原算法的核心思想是通过 3 轮广播使系统节点

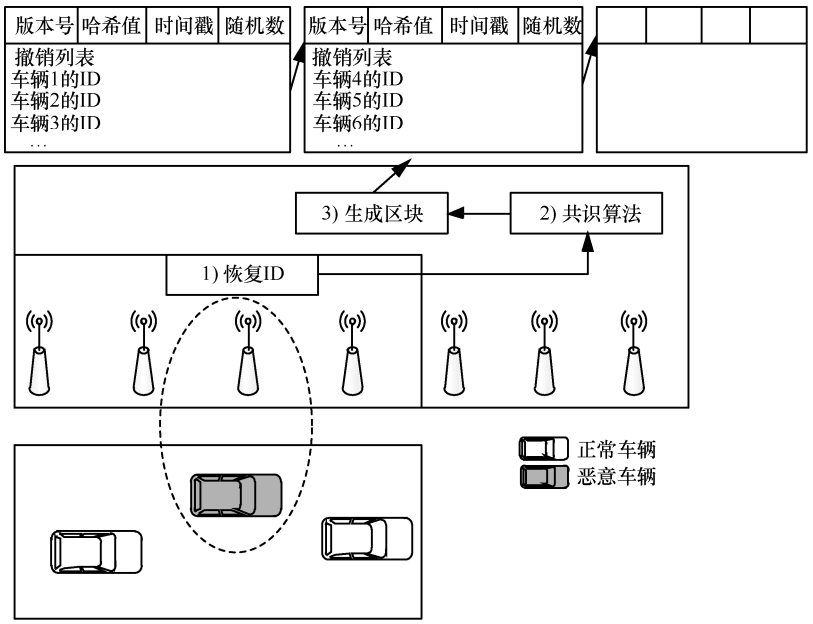


图 5 撤销区块链更新流程

对请求数据达成一致，其一致性结果为多数节点的响应结果。该算法主要由一致性协议、视图切换协议和检查点协议构成[21]。PBFT 算法具有出块时间短、吞吐量大的优点，其性能瓶颈在于随着节点数量的增加，共识效率会显著下降。文献[22-23]对 PBFT 算法进行了改进，使其具有更好的拓展性，更加适用于 IoV。目前，主流的共识算法还有 PoW、PoS、DPoS，然而 PoW 通过算力竞争选举记账节点，严重浪费电力；PoS 虽然克服了 PoW 的问题，但该机制的“无利害关系”问题尚待解决，且吞吐量不如 PBFT；DPoS 选择固定数量的超级节点轮流获得记账权，其竞选规则的去中心化存在争议[24]。

3.5　用户 ID 变更阶段

在此阶段，用户可以自由变更自己注册的 ID。方法如下。

步骤 1　OBU_i 随机选择 $s'\in Z_q^*$，计算 $T_{s'}=T_{s'}(x)(\mathrm{mod}\,p)$，$T_{s'r}=T_{s'}(T_r)(\mathrm{mod}\,p)$，$h_{V_i}=h_0(\mathrm{ID}_{V_i}\|T_{s'r})$，$E_{V_i}=E_{T_{s'r}}(h_{V_i},\mathrm{ID}_{V_i}^*)$，$W_1'=h_0(\mathrm{GID}_V{}^{i-1}\|T_{s'}\|E_{V_i}\|T_{V_i^4}\|T_r)$，发送 $<\mathrm{GID}_V{}^i,T_{s'},E_{V_i},T_{V_i^4},W_1'>$ 给 RSU_i。

步骤 2　RSU_i 检验 $T_7-T_{V_i^4}<\Delta t$ 是否成立，若成立则计算 $\mathrm{RA}'=h_0(\mathrm{RID})\oplus E_{V_i}$，发送 $<\mathrm{GID}_V{}^i,T_{s'},E_{V_i},\mathrm{RA}',T_{R_i^3},W_1'>$ 给 TA。

步骤 3　TA 检验 $T_8-T_{R_i^3}<\Delta t$ 是否成立，若成立则计算 $(W_1')^*=h_0(\mathrm{GID}_V{}^{i-1}\|T_{s'}\|E_{V_i}\|T_{V_i^4}\|T_r)$，判断 $(W_1')^*\overset{?}{=}W_1'$，相等则计算 $h_0(\mathrm{RID})=\mathrm{RA}'\oplus E_{V_i}$，判断 $h_R\overset{?}{=}h_0(\mathrm{RID})$，相等则计算 $T_{rs'}=T_r(T_{s'})(\mathrm{mod}\,p)$，$D_{T_{rs'}}(E_{V_i})=(h_{V_i},\mathrm{ID}_{V_i}{}^*)$，$h_{V_i}{}^*=h_0(\mathrm{ID}_{V_i}\|T_{rs'})$，判断 $h_{V_i}{}^*\overset{?}{=}h_{V_i}$，相等则在下一组认证时用 $\mathrm{ID}_{V_i}{}^*$ 代替 ID_{V_i}。

4　安全性分析

4.1　安全模型

本文使用文献[25]中提出的安全模型。定义 3 个实体 U^i、R^j、T^k。I 可以代表其中任意一个实体。

攻击者 $\mathcal{A}$ 可执行以下 4 种询问。

1) 发送询问 $\mathrm{send}(I,M_i)$。$\mathcal{A}$ 发送消息给 I 后，会收到对应的响应消息。

2) 执行询问 $(U^i,R^j)(R^j,T^k)$。在发送询问后由各实体执行。如 $(\mathrm{GID}_V{}^{i-1},\mathrm{OA},T_s,\gamma_i,T_{V_i},W_1)\leftarrow\mathrm{send}(U^i,\mathrm{start})$，$(\mathrm{GID}_V{}^{i-1},\mathrm{OA},T_s,\gamma_i,\mathrm{RA},T_{R_i},W_1)\leftarrow\mathrm{send}(R^j,(\mathrm{GID}_V{}^{i-1},\mathrm{OA},T_s,\gamma_i,T_{V_i},W_1))$。

3) 揭秘询问 $\mathrm{reveal}(I)$。由 $I(U^i$或$R^j)$ 返回会话密钥。

4) 测试询问 $\mathrm{test}(I)$。随机选择 $b=\{0,1\}$，$b=1$ 时返回会话密钥 sk，$b=0$ 时返回随机数 $\{0,1\}^{l_{\mathrm{sk}}}$，$l_{\mathrm{sk}}$ 为 sk 的位宽。

定义以下事件。

1) 成功事件 (Suc_n)。询问结束后，$\mathcal{A}$ 给出的测试询问结果 b' 和协议执行结果 b 相等表示此事件发生。

2) 认证事件 (Auth_n)。$\mathcal{A}$ 发送 (sd_1^*,h_1^L) 被 OBU 验证并接受表示此事件发生。

3) 询问事件 (AskH_n)。$\mathcal{A}$ 在 h_0 上询问 $T_{sr}\|\gamma_i$ 表示此事件发生。

4.2　形式化的安全性证明

引理 1　存在 $T_n(x),n\in[1,q-1]$，且 $\mathcal{A}$ 最多进行 q_s 次发送询问，q_p 次窃听询问及 q_h 次哈希询问的情况下，其破坏本文协议 p 的语义安全性的优势为

$$Adv_p^{\mathrm{sec}}(\mathcal{A})\leqslant 2\chi_1+2\chi_2+6q_h\,\mathrm{Suc}_p^{\mathrm{cdh}}(t') \tag{7}$$

其中，$\chi_1=\dfrac{(q_s+q_p)^2+2q_h+q_s}{2(q-1)}$，$\chi_2=\dfrac{{q_h}^2+4q_s}{2^{l+1}}$，$t'=t+(q_s+q_p+1)t_p$，$t_p$ 表示一次混沌映射的运算时间。由于 χ_1、χ_2 和 $\mathrm{Suc}_p^{\mathrm{cdh}}(t')$ 均是多项式时间内可忽略的概率，因此协议 p 是安全的。

证明　利用随机预言机模型定义以下规则。

对于哈希询问 $h_i(q)$，如果 (i,q,r) 在表 Γ_H 中，将 r 返回，否则执行 h_i，随机选择 $r\in\{0,1\}^{l_i}$，其中 l_i 为 h_i 的输出位宽，返回 (i,q,r) 并将其保存到表 Γ_H，$\mathcal{A}$ 将其保存到表 $\Gamma_{\mathcal{A}}$。

S 模拟 OBU 对 $\mathcal{A}$ 的询问做出回答，$\mathcal{A}$ 发送询问 (U^i,start)，S 执行 $U_1^{(1)}$，随机选择 $\alpha\in[1,q-1]$，计算 $T_{\alpha r}=T_\alpha(T_r)(\mathrm{mod}\,p)$，$\mathrm{OA}=h_0(T_{\alpha r}\|\gamma_i)$，$T_\alpha=T_\alpha(x)\,(\mathrm{mod}\,p)$，$W_1=h_0(\mathrm{GID}_V{}^{i-1}\|\mathrm{OA}\|T_\alpha\|\gamma_i\|T_{V_i}\|T_r)$，返回 $(\mathrm{GID}_V{}^{i-1},\mathrm{OA},T_s,\gamma_i,T_{V_i},V_1)$，S 进入 OBU 的下一状态。

当 S 处于正确状态，对于 $\mathcal{A}$ 的询问 $\mathrm{send}(U^i,(\mathrm{GID}_V{}^i,\mathrm{sd}_1^*,h_1^L,h_2^L,T_z,T_{R_i^1},T_{V_i^1},V_2))$，S 执行 $U_2^{(1)}$，验证 W_2，错误则拒绝认证，否则继续计算

$\mathrm{sd}_1 = h_0(T_{\alpha r}) \oplus \mathrm{sd}_1^*$，验证 $(h_1^L)^* = h_1^L(\mathrm{sd}_1)$，不相等则拒绝认证。相等则计算 $T_{\alpha\beta} = T_\alpha(T_\beta) (\mathrm{mod}\, p)$，$h_{\alpha\beta} = h_0(T_{\alpha\beta})$，返回 $(\mathrm{GID}_V{}^i, h_{\alpha\beta}, T_{V_i^2})$。

S 模拟 RSU 对 $\mathcal{A}$ 的询问做出回答，对于 $\mathcal{A}$ 的询问 $\mathrm{send}(R^j, (\mathrm{GID}_V{}^{i-1}, \mathrm{OA}, T_\alpha, \gamma_i, T_{V_i}, W_1))$，S 执行 $R_1^{(1)}$，随机选择 $\delta \in \{0,1\}^{l_R}$，其中 l_R 为 RID 的位宽，计算 $\mathrm{RA} = h_0(\delta) \oplus \mathrm{OA}$，返回 $(\mathrm{GID}_V{}^{i-1}, \mathrm{OA}, T_\alpha, \gamma_i, \mathrm{RA}, T_{V_i}, T_{R_i}, W_1)$，S 进入 RSU 的下一状态。

对于 $\mathcal{A}$ 的询问 $\mathrm{send}(R^j, (\mathrm{GID}_V{}^i, \mathrm{sd}_1^*, h_1^L, T_{R_i^1}, W_2))$，S 执行 $R_2^{(1)}$，随机选择 $\beta \in Z_q^*$，计算 $\mathrm{sd}_2 = f(n_1)$，$h_2^L = h_2^L(\mathrm{sd}_2)$，$T_\beta = T_\beta(x) (\mathrm{mod}\, p)$，$T_{\beta\alpha} = T_\beta(T_\alpha) \ (\mathrm{mod}\, p)$，返回 $(\mathrm{GID}_V{}^i, \mathrm{sd}_1^*, h_1^L, h_2^L, T_\beta, T_{R_i^1}, T_{V_i^1}, W_2)$，S 进入 RSU 的下一状态。

对于 $\mathcal{A}$ 的询问 $(R^j, (\mathrm{GID}_V{}^i, h_{\alpha\beta}, T_{V_i^2}))$，S 执行 $R_3^{(1)}$，判断 $h_{\alpha\beta} \stackrel{?}{=} h_0(T_{\beta\alpha})$，不相等则拒绝认证。S 停止游戏。

S 模拟 TA 对 $\mathcal{A}$ 的询问进行回答，对于 $\mathcal{A}$ 的询问 $\mathrm{send}(\mathrm{TA}^k, (\mathrm{GID}_V{}^{i-1}, \mathrm{OA}, T_\alpha, \gamma_i, \mathrm{RA}, T_{R_i}, W_1))$，S 执行 $T_1^{(1)}$，验证 W_1，失败则拒绝认证，否则计算 $h_0^*(\delta) = \mathrm{RA} \oplus \mathrm{OA}$，判断 $h_R \stackrel{?}{=} h_0^*(\delta)$，不相等则拒绝认证，否则执行 $T_2^{(1)}$，计算 $T_{r\alpha} = T_r(T_\alpha) (\mathrm{mod}\, p)$，$\mathrm{OA}^* = h_0(T_{r\alpha} \| \gamma_i)$，判断 $\mathrm{OA}^* \stackrel{?}{=} \mathrm{OA}$，不相等则拒绝认证，否则计算 $\mathrm{sd}_1^* = h_0(T_{r\alpha}) \oplus \mathrm{sd}_1$，$\mathrm{GID}_V{}^i = \mathrm{ID}_{V_i} \oplus T_{n_j}$ 或 $\mathrm{GID}_V{}^i = \mathrm{ID}_{V_i} \oplus T_{h_{n_j}}$，$W_2 = h_0(\mathrm{GID}_V{}^i \| \mathrm{sd}_1^* \| h_1^L \| T_{R_i^1} \| T_r)$，返回 $(\mathrm{GID}_V{}^i, \mathrm{sd}_1^*, h_1^L, T_{R_i^1}, W_2)$，将 $(\mathrm{GID}_V{}^{i-1}, \mathrm{GID}_V{}^i, \mathrm{OA}, \mathrm{RA}, T_r, T_\alpha, T_\beta, T_{\alpha\beta}, h_1^L, h_2^L, h_{\alpha\beta}, \mathrm{sd}_1^*)$ 存入表 Γ_ψ。

将协议的证明过程定义为以下游戏。

G_0。定义 $\mathcal{A}$ 在本文协议 p 中的安全优势为

$$\mathrm{Adv}_p^{\mathrm{sec}}(\mathcal{A}) \leqslant 2\Pr[\mathrm{Suc}_0] - 1 \tag{8}$$

G_1。用私人神谕 h_3、h_4、h_5 代替 h_0、h_1、h_2（在 G_7 中用 h_3、h_4 替换 h_0、h_1）。G_1 与 G_0 的可区分概率为

$$|\Pr[\mathrm{Suc}_1] - \Pr[\mathrm{Suc}_0]| = 0 \tag{9}$$

G_2。当以下矛盾发生时，终止游戏。

1) 在 h_i 中随机选择 $t \in \{0,1\}^{l_i}$，返回 $(i,*,t)$，存在 $(i,*,t) \in \Gamma_{\mathcal{A}}$。

2) 对于发送询问 $(U^i,*)$、$(R^j,*)$、$(T^k,*)$，存在 S 的响应 $M_i \in \Gamma_{\mathcal{A}}$。

G_2 与 G_1 的可区分概率为

$$|\Pr[\mathrm{Suc}_2] - \Pr[\mathrm{Suc}_1]| \leqslant \frac{(q_s + q_p)^2}{2(q-1)} + \frac{q_h^2}{2^{l_i+1}} \tag{10}$$

G_3。当 $\mathcal{A}$ 猜出 OA 并仿冒成 OBU 发送给 TA，则终止游戏。通过修改以下规则来实现此目标。

$T_2^{(3)}$。计算 $T_{r\alpha} = T_r(T_\alpha) (\mathrm{mod}\, p)$，$\mathrm{OA}^* = h_0(T_{r\alpha} \| \gamma_i)$，判断 $\mathrm{OA}^* \stackrel{?}{=} \mathrm{OA}$，如果不相等则拒绝认证，否则在表 Γ_H 中查找 $(0, T_{\alpha r}, \mathrm{OA})$，在表 $\Gamma_{\mathcal{A}}$ 中查找 $(0, T_{\alpha r}, \mathrm{OA})$，均存在则终止游戏。

G_3 与 G_2 的可区分概率为

$$\left|\Pr[\mathrm{Suc}_3] - \Pr[\mathrm{Suc}_2]\right| \leqslant \frac{q_s}{2^{l_0}} \tag{11}$$

G_4。当 $\mathcal{A}$ 猜出 RA 并发送给 TA 则终止游戏。通过修改以下规则实现此目标。

$T_1^{(4)}$。计算 $h_0^*(\delta) = \mathrm{RA} \oplus \mathrm{OA}$，验证 $h_R = h_0^*(\delta)$，不相等则拒绝认证，否则在表 Γ_ψ 中查找 RA，在表 $\Gamma_{\mathcal{A}}$ 中查找 $(0, \delta, h_R)$，如果均存在则终止游戏。

G_4 与 G_3 的可区分概率为

$$\left|\Pr[\mathrm{Suc}_4] - \Pr[\mathrm{Suc}_3]\right| \leqslant \frac{q_s}{2^{l_0}} \tag{12}$$

G_5。$\mathcal{A}$ 猜出 T_r 并仿冒成 OBU 发送认证向量给 TA 则终止游戏。通过修改以下规则来实现此目标。

$T_2^{(5)}$。计算 $T_{r\alpha} = T_r(T_\alpha) (\mathrm{mod}\, p)$，$\mathrm{OA}^* = h_0(T_{r\alpha} \| \gamma_i)$，判断 $\mathrm{OA}^* \stackrel{?}{=} \mathrm{OA}$，如果不相等则拒绝认证，否则在表 Γ_ψ 中查找 T_r，存在则终止游戏。

G_5 与 G_4 的可区分概率为

$$\left|\Pr[\mathrm{Suc}_5] - \Pr[\mathrm{Suc}_4]\right| \leqslant \frac{q_h}{q-1} \tag{13}$$

G_6。$\mathcal{A}$ 计算出 $T_{\alpha\beta}$ 并成功发送 $h_{\alpha\beta}$ 则终止游戏。通过修改以下规则实现此目标。

$R_3^{(6)}$。判断 $h_{\alpha\beta} \stackrel{?}{=} h_0(T_{\beta\alpha})$，若相等则在表 Γ_ψ 中查找 $T_{\beta\alpha}$，若存在则终止游戏。

G_6 与 G_5 的可区分概率为

$$\left|\Pr[\mathrm{Suc}_6] - \Pr[\mathrm{Suc}_5]\right| \leqslant q_h \mathrm{Suc}_p^{\mathrm{cdh}}(t') \tag{14}$$

其中，$t' = t + (q_s + q_p + 1)t_p$，$\mathrm{Suc}_p^{\mathrm{cdh}}(t') \geqslant \varepsilon$，$\varepsilon$ 是一个不可忽略的概率。

G_7。当 $\mathcal{A}$ 窃听得到 T_r 并仿冒成 TA 发送 (sd_1^*, h_1^L) 给 OBU 时终止游戏。通过修改以下规则实现此目标。

$U_2^{(7)}$。检查 $(\mathrm{sd}_1^*, h_1^L) \in \Gamma_\psi$，如果不存在，则拒绝认证；如果存在，则检查 $(0, T_{r\alpha}, r) \in \Gamma_{\mathcal{A}}$，若同样存在，则终止游戏。显然，当事件 Auth_n 发生时，G_7 与 G_6 是可区分概率的。

$$\left|\Pr[\mathrm{Suc}_7] - \Pr[\mathrm{Suc}_6]\right| \leqslant \Pr[\mathrm{Auth}_7] \tag{15}$$

G_8。用私人神谕 h_3、h_4 替换 G_7 中的 h_0、h_1，这样 sd_1^*、h_1^L 将独立于 h_0、h_1。当 $\mathcal{A}$ 在 h_0 上询问 $T_{sr} \| \gamma_i$ 时，G_8 与 G_7 是可区分的。

$$\left|\Pr[\mathrm{Suc}_8] - \Pr[\mathrm{Suc}_7]\right| \leqslant \Pr[\mathrm{AskH}_8] \tag{16}$$

$$\left|\Pr[\mathrm{Auth}_8] - \Pr[\mathrm{Auth}_7]\right| \leqslant \Pr[\mathrm{AskH}_8] \tag{17}$$

其中，$\Pr[\mathrm{Auth}_8] \leqslant \dfrac{q_s}{2(q-1)}$，$\Pr[\mathrm{AskH}_8] \leqslant q_h \mathrm{Suc}_p^{\mathrm{cdh}}(t')$，证明过程如下。

证明　对于给定实体 (Q_1, Q_2)，用 Diffie-Hellman 问题的随机自约性来模拟混沌映射的 CDH[26]问题。

U_1。随机选择 $\phi \in Z_q^*$，计算 $T_\phi = T_\phi(Q_1) \cdot (\mathrm{mod}\, p)$，将 (ϕ, T_ϕ) 加入表 $\Gamma_{\mathcal{A}}$。

T_1。随机选择 $\varphi \in Z_q^*$，计算 $T_\varphi = T_\varphi(Q_2) (\mathrm{mod}\, p)$，将 (φ, T_φ) 加入表 $\Gamma_{\mathcal{A}}$。

在表 $\Gamma_{\mathcal{A}}$ 中随机选择三元组 $(\phi, \varphi, T_{\phi\varphi}) = \mathrm{CDH}(Q_1, Q_2)$，其值相对应的概率为 $1/q_h$。因此，有

$$\mathrm{AskH}_7 \leqslant q_h \mathrm{Suc}_p^{\mathrm{cdh}}(t') \tag{18}$$

其中，$t' = t + (q_s + q_p + 1)t_p$，$\mathrm{Suc}_p^{\mathrm{cdh}}(t') \geqslant \varepsilon$，$\varepsilon$ 是一个不可忽略的概率。

设所有哈希输出均为 l 位，则由式(9)~式(17)可得

$$\left|\Pr[\mathrm{Suc}_8] - \Pr[\mathrm{Suc}_0]\right| \leqslant \chi_1 + \chi_2 + 3q_h \mathrm{Suc}_p^{\mathrm{cdh}}(t') \tag{19}$$

其中，$\chi_1 = \dfrac{(q_s + q_p)^2 + 2q_h + q_s}{2(q-1)}$，$\chi_2 = \dfrac{q_h^2 + 4q_s}{2^{l+1}}$。由式(8)得 $\mathrm{Adv}_p^{\mathrm{sec}}(\mathcal{A}) \leqslant 2\chi_1 + 2\chi_2 + 6q_h \mathrm{Suc}_p^{\mathrm{cdh}}(t')$。证毕。

4.3　其他安全性讨论

除从前述角度对安全性进行分析外，本节将从更多角度对协议性能进行更加详细的分析与讨论。

1) 双向认证。由于只有生成了 r 的 TA 和产生随机数 s 的 OBU 可以利用混沌映射的半群特性对认证向量 OA 和 (sd_1^*, h_1^L) 进行验证。因此，本文协议可以实现 OBU 与 TA 的双向认证。

2) 可以抵御 OBU、RSU、TA 的仿冒攻击。首先，由于攻击者无法得知 T_r，因此无法计算出有效认证向量 OA，也就无法仿冒成 OBU。其次，由于攻击者无法得知 RSU 注册的 RID，因此无法计算出有效的认证向量 RA，也就无法仿冒成 RSU。最后，由于攻击者无法得知 TA 产生的 r，因此无法利用 T_s 计算出有效的认证向量 (sd_1^*, h_1^L)，也就无法仿冒成 TA。

3) OBU 的匿名性。OBU 的身份信息包含在 $\mathrm{GID}_V{}^i$ 和 $\mathrm{PID}_V{}^i$ 中，一方面由 $\mathrm{GID}_V{}^i$ 求真实 ID 需要 L 个 RSU 的联合，攻击者很难在短时间内同时控制多个 RSU；另一方面临时假名 $\mathrm{PID}_V{}^i$ 在不同 RSU 范围内是不同的，可以满足 OBU 匿名身份的频繁变更。所以本文协议可以满足 OBU 的匿名需求。

4) 可以抵御中间人攻击。当攻击者希望在 OBU 与 TA 之间进行中间人攻击时，需要仿冒成 OBU 向 TA 发送认证向量，同时仿冒成 TA 向 OBU 发送认证向量。由 2)的分析可知，攻击者无法成功。另外，由于哈希摘要的存在，使攻击者只能截获和转发消息，而无法修改和获得额外信息。

5) 可以抵御重放攻击。假设攻击者成功修改时间戳并重新发送 OBU 过去的认证消息，本文协议使攻击者只能通过 T_s 求解随机数 s，由于拓展 DLP[26]，攻击者无法成功求出 s，从而无法正确计算 h_{sz_1} 以完成认证。因此，可以抵御重放攻击。

6) 会话密钥的前向和后向安全性。在同一 RSU 组内，不同 RSU 范围内的会话密钥为 T_{sz_i}，由于 z_i 是一个临时生成的随机数，因此 T_{sz_i} 也是随机变化的。攻击者无法从当前的 T_{sz_i} 推测出 $T_{sz_{i-1}}$ 或 $T_{sz_{i+1}}$，所以满足前向和后向安全性。

7) 可拓展性。本文通过 RSU 的动态分组，使车辆在组内只需进行快速的切换认证，而不需要与远端的 TA 频繁认证，可缓解车辆节点增加带来的网络损耗，使系统具有更强的可拓展性。

5　仿真与性能对比分析

5.1　基本功能对比

为了有效分析本文协议的性能，本节对本文协议与 Zhao 方案[13]、Cui 方案[14]进行了功能对比，其中 Zhao 方案拥有良好的安全性能，Cui 方案拥有

较低的计算时延，结果如表 2 所示。由表 2 可知，Zhao 方案满足大多数常见的安全属性，但是忽略了可追溯性、可撤销性以及灵活的用户 ID 变更功能，Cui 方案则忽略了双向认证及 TA 仿冒攻击等重要问题，显然，本文协议满足更多的安全属性。

表 2 功能对比

安全需求	Zhao 方案	Cui 方案	本文协议
用户匿名性	√	√	√
双向认证	√	×	√
抵御重放攻击	√	√	√
抵御中间人攻击	√	√	√
抵御 OBU/MU 仿冒攻击	√	√	√
抵御 RSU/FA/Fog 仿冒攻击	√	√	√
抵御 TA/HA 仿冒攻击	√	×	√
生成会话密钥	√	√	√
前向/后向安全性	√	√	√
可追溯性	×	×	√
可撤销性	×	×	√
用户 ID 自由变更	×	×	√

5.2 时延性能分析

相比于其他物联网，IoV 对时延有着更高的要求。所以本节将把本文协议的认证时延与 Zhao 方案、Cui 方案的认证时延进行对比。定义 T_{h}、T_{se}、T_{sd}、T_{ase}、T_{asd}、T_{mul}、T_{chev} 分别表示单次的哈希运算、对称加密、对称解密、非对称加密、非对称解密、椭圆曲线中的点乘运算、切比雪夫映射的计算时间。本文使用 Intel(R) Core(TM) i5-9500，2.00 GB 的 RAM，在 VS-2010 中使用密码库 OpenSSL-1.1.1h 进行 10^6 次运算，测得数据如表 3 所示。因此 $T_{\mathrm{h}} \approx 0.008\,0$ ms，$T_{\mathrm{se}} \approx 0.018\,3$ ms，$T_{\mathrm{sd}} \approx 0.018\,2$ ms，$T_{\mathrm{ase}} \approx 0.037\,6$ ms，$T_{\mathrm{asd}} \approx 1.097\,7$ ms，$T_{\mathrm{mul}} \approx 0.051\,4$ ms，$T_{\mathrm{chev}} \approx 0.033\,6$ ms。

5.2.1 认证时延对比

通过实验测得的数据，可以计算 3 种方案中涉及的各个实体的计算时延。由于异或操作时间很短，因此忽略异或运算时延，结果如表 4 所示。可见，Zhao 方案的较高计算时延主要在于服务器端的对称加解密和非对称签名。Cui 方案是 3 种方案中计算时延最低的，但是它缺乏一些重要的安全属性。本文协议计算时延不是一个定值，而是随组长 L 的增大而增大。

表 3 密码学操作时间

密码学操作	运算时间/ms
SHA256	8 128
MD5	7 831
DES/E	18 252
DES/D	18 205
RSA/E	37 597
RSA/D	1 097 717
ECC 点乘	51 449
切比雪夫映射	33 622

本文在不进行分组的情况下（L=1），3 种方案的计算时延如图 6 所示，L 值对计算时延的影响如图 7 所示，车辆数量与认证时延的关系如图 8 所示。图 7 和图 8 表明，当 L 值合适时，随着车辆数量的增加，系统的计算时延是一个 IoV 中可以容忍的时延，这证明了系统的可用性。

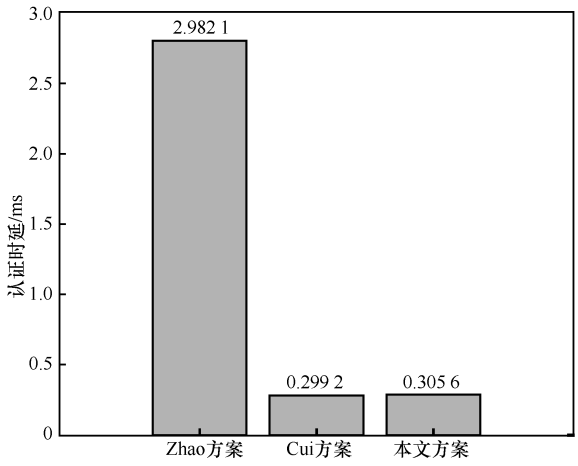


图 6 认证时延对比

表 4 认证时延对比

方案	OBU/MU	RSU/FA/Fog	TA/HA
Zhao 方案	$T_{\mathrm{sd}} + 3T_{\mathrm{mul}} + 8T_{\mathrm{h}} \approx 0.172\,4$ ms	$2T_{\mathrm{se}} + T_{\mathrm{sd}} + T_{\mathrm{ase}} + T_{\mathrm{asd}} + 3T_{\mathrm{mul}} + 4T_{\mathrm{h}} \approx 1.376\,3$ ms	$T_{\mathrm{se}} + T_{\mathrm{sd}} + T_{\mathrm{ase}} + T_{\mathrm{asd}} + 4T_{\mathrm{mul}} + 7T_{\mathrm{h}} \approx 1.433\,4$ ms
Cui 方案	$4T_{\mathrm{chev}} + 3T_{\mathrm{h}} \approx 0.158\,4$ ms	$3T_{\mathrm{chev}} + 2T_{\mathrm{h}} \approx 0.116\,8$ ms	$3T_{\mathrm{h}} \approx 0.024\,0$ ms
本文方案	$3T_{\mathrm{chev}} + (L+5)T_{\mathrm{h}} \approx (0.140\,8 + 0.008L)$ ms	$2T_{\mathrm{chev}} + (L+2)T_{\mathrm{h}} \approx (0.083\,2 + 0.008L)$ ms	$T_{\mathrm{chev}} + 4T_{\mathrm{h}} \approx 0.065\,6$ ms

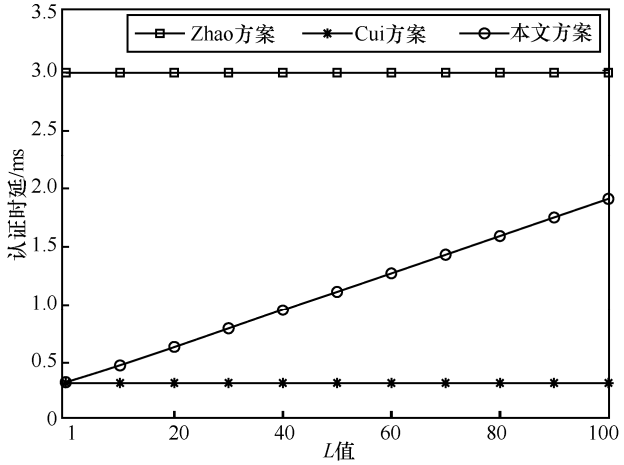


图 7　L 值对认证时延的影响

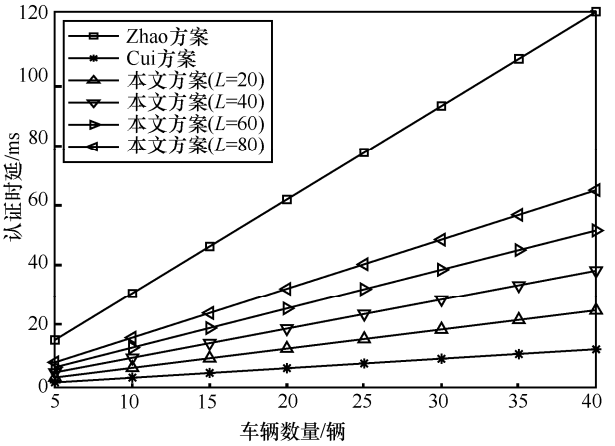


图 8　不同 L 值的认证时延

相比于 Zhao 方案，本文协议最短计算时延减少了约89.75% 。相比于 Cui 方案，本文协议牺牲少量时延换来了更完善的抵御仿冒攻击的性能、更灵活的分组认证方式及匿名可追溯性。这些性能可以更好地增强 IoV 的安全性。因此本文协议更适用于 IoV。

5.2.2　切换时延对比

本节对 Zhao 方案、Cui 方案与本文方案的切换认证时延进行了对比。表 5 列出了 3 种方案中各实体的具体计算时延。由于本文方案的切换时延与组长 L 及 RSU 在组中的位置 i 有关，因此具有不确定性。为了便于比较，本文分别取 $L=10$ 、 $L=20$ 、 $L=30$ 时的时延与 Zhao 方案和 Cui 方案进行比较，$i=L/2$ ，这是因为组内首尾 RSU 哈希运算次数的互补对称性。

图 9 为本文方案取最短切换时延时（ L=2 ）3 种方案的时延比较。相比于 Cui 方案，本文方案切换时延减少了约82.30% 。

图 10 为 L 值对切换时延的影响，显然本文方案时延曲线上升十分平缓，这表明 L 值对时延影响较小。

表 5　　切换时延对比

方案	UE/OBU	OBU_m/AP/RSU
Zhao 方案	$T_{mul}+2T_h$ ≈ 0.067 4 ms	$T_{mul}+2T_h$ ≈ 0.067 4 ms
Cui 方案	$T_{se}+8T_{chev}+8T_h$ ≈ 0.3511 ms	$2T_{se}+10T_{chev}+9T_h$ ≈ 0.444 6 ms
本文方案	$T_{chev}+(L-i+2)T_h \approx$ (0.049 6+0.008(L−i)) ms	$2T_{chev}+(L-i+1)T_h \approx$ (0.075 2+0.008(L−i)) ms

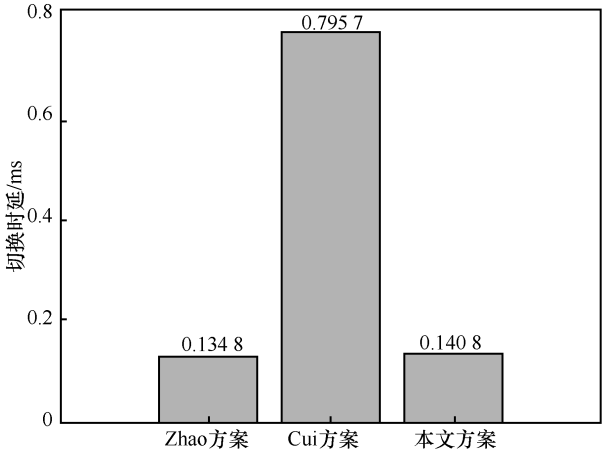


图 9　切换时延对比

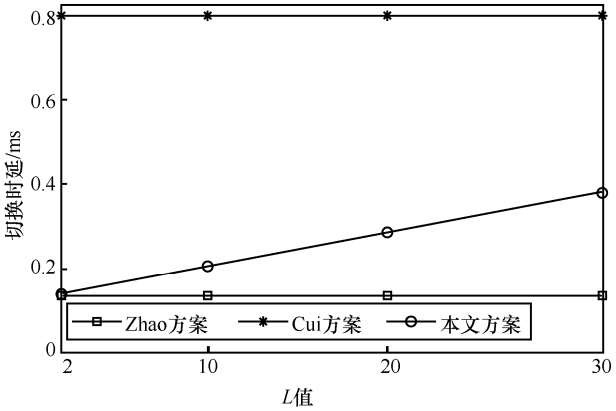


图 10　L 值对切换时延的影响

图 11 为车辆数量与切换时延的关系，可见当待切换的车辆数量增加时，其切换时延仍是 IoV 中可容忍的时延。

5.3　通信开销对比分析

表 6 列出了 Zhao 方案、Cui 方案与本文方案在接入认证和切换认证过程中的通信开销。为了便于比较，本文假设 ID 为 160 bit，时间戳为 32 bit，哈

希摘要为 160 bit，随机数为 128 bit，椭圆曲线点乘为 320 bit，切比雪夫映射为 480 bit，非对称加密输出为 1 024 bit，对称密钥为 256 bit，对称加密输出为 128 bit，并分别用 B_{ID}、B_t、B_h、B_R、B_{mul}、B_{chev}、B_{ase}、B_{sk}、B_{se} 表示。

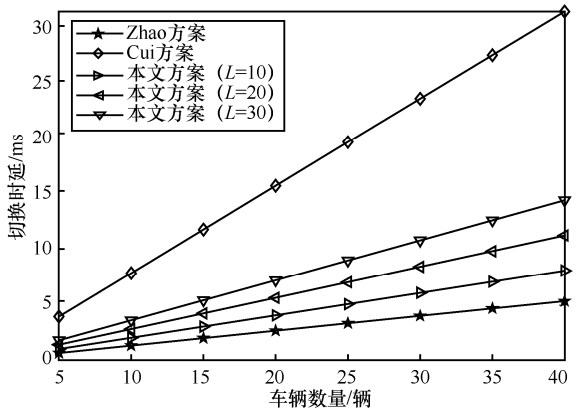


图 11　不同 L 值的切换时延

表 6　　通信开销对比

方案	接入认证	切换认证
Zhao 方案	$2B_{ID}+2B_h+4B_{mul}+3B_{se}+2B_{ase}=4\,352$ bit	$B_h+2B_{mul}=800$ bit
Cui 方案	$3B_{ID}+4B_t+3B_h+4B_{chev}=3\,008$ bit	$4B_h+3B_{chev}+B_{se}+B_{sk}=2\,464$ bit
本文方案	$5B_{ID}+7B_t+13B_h+2B_R+3B_{chev}=4\,800$ bit	$2B_{ID}+2B_t+2B_h+B_{chev}=1\,184$ bit

各方案接入认证和切换认证的通信成本比较结果分别如图 12 和图 13 所示。可见，本文方案在接入认证阶段的通信成本略高于 Zhao 方案和 Cui 方案，这主要是由于本文方案进行了更多次的哈希运算用于保证数据传输的安全。在切换认证阶段，本文方案的通信成本比 Cui 方案减少了约 51.95%，其原因在于本文方案仅需发送一次切比雪夫映射值，而 Cui 方案需要传输 3 次切比雪夫映射值。

6　结束语

本文利用切比雪夫混沌映射的单向陷门性和半群特性设计了一种适用于 IoV 的组认证协议，利用反向哈希链设计了快速切换认证协议，通过构建撤销区块链实现了恶意车辆的及时撤销，利用随机预言机的证明和仿真数据说明本文协议相比于现有的协议具有一定的优越性。

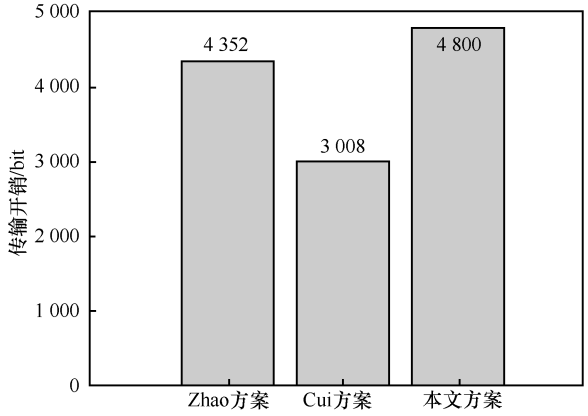


图 12　接入认证的通信成本

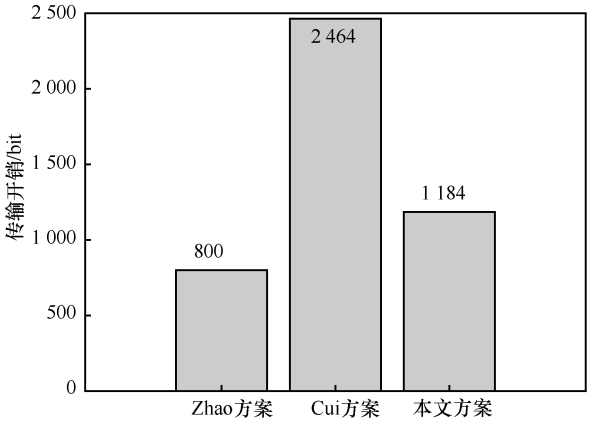


图 13　切换认证的通信成本

参考文献：

[1] VASUDEV H, DAS D. Work-in-progress: SAFE: secure authentication for future entities using Internet of vehicles[C]//2019 IEEE Real-Time Systems Symposium. Piscataway: IEEE Press, 2019: 560-563.

[2] SUN Y C, WU L, WU S Z, et al. Security and privacy in the Internet of vehicles[C]//2015 International Conference on Identification, Information, and Knowledge in the Internet of Things. Piscataway: IEEE Press, 2015: 116-121.

[3] TULADHAR K M, LIM K. Efficient and scalable certificate revocation list distribution in hierarchical VANETs[C]//2018 IEEE International Conference on Electro/Information Technology. Piscataway: IEEE Press, 2018: 620-625.

[4] SUN G, SUN S Y, SUN J, et al. Security and privacy preservation in fog-based crowd sensing on the Internet of vehicles[J]. Journal of Network and Computer Applications, 2019, 134: 89-99.

[5] FREUDIGER J, RAYA M, FELEGHHAZI M. Mix zones for location privacy in vehicular networks[C]//ACM Workshop on Wireless Networking for Intelligent Transportation Systems. New York: ACM Press, 2007:1-7.

[6] LU R, LIN X, ZHU H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[C]//IEEE INFOCOM 2008-The 27th Conference on Computer Communications. Piscataway: IEEE Press, 2008: 1229-1237.

[7] ZHANG L, WU Q H, SOLANAS A, et al. A scalable robust authentication protocol for secure vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2010, 59(4): 1606-1617.

[8] JIANG Y X, SHI M H, SHEN X M, et al. BAT: a robust signature scheme for vehicular networks using binary authentication tree[J]. IEEE Transactions on Wireless Communications, 2009, 8(4): 1974-1983.

[9] YAO L, LIN C, DENG J, et al. Biometrics-based data link layer anonymous authentication in VANETs[C]//2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Piscataway: IEEE Press, 2013: 182-187.

[10] JIANG S R, ZHU X Y, WANG L M. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.

[11] YING B D, NAYAK A. Anonymous and lightweight authentication for secure vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 10626-10636.

[12] LIU J W, LI Q Q, SUN R, et al. An efficient anonymous authentication scheme for Internet of vehicles[C]//2018 IEEE International Conference on Communications. Piscataway: IEEE Press, 2018: 1-6.

[13] ZHAO D W, PENG H P, LI L X, et al. A secure and effective anonymous authentication scheme for roaming service in global mobility networks[J]. Wireless Personal Communications, 2014, 78(1): 247-269.

[14] CUI J, WANG Y L, ZHANG J, et al. Full session key agreement scheme based on chaotic map in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 8914-8924.

[15] LI G S, JIANG Q, WEI F S, et al. A new privacy-aware handover authentication scheme for wireless networks[J]. Wireless Personal Communications, 2015, 80(2): 581-589.

[16] ZENG Y B, GUANG H, LI G S. Attribute-based anonymous handover authentication protocol for wireless networks[J]. Security and Communication Networks, 2018, 2018: 1-9.

[17] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Cryptography Mailing, 2008.

[18] SHARMA V. An energy-efficient transaction model for the blockchain-enabled Internet of vehicles (IoV)[J]. IEEE Communications Letters, 2019, 23(2): 246-249.

[19] BAGGA P, DAS A K, WAZID M, et al. Authentication protocols in Internet of vehicles: taxonomy, analysis, and challenges[J]. IEEE Access, 2020, 8: 54314-54344.

[20] YANG J L, WANG D H. Applying extended chebyshev polynomials to construct a trap-door one-way function in real field[C]//2009 First International Conference on Information Science and Engineering. Piscataway: IEEE Press, 2009: 1680-1682.

[21] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation. New York: ACM Press, 1999: 173-186.

[22] CHEN Z L, CHEN S Z, XU H, et al. A security authentication scheme of 5G ultra-dense network based on block chain[J]. IEEE Access, 2018, 6: 55372-55379.

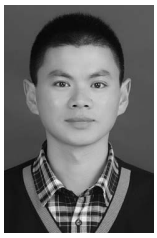
[23] HU W, HU Y W, YAO W H, et al. A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles[J]. IEEE Access, 2019, 7: 139703-139711.

[24] 郑敏, 王虹, 刘洪, 等. 区块链共识算法研究综述[J]. 信息网络安全, 2019(7): 8-24.
ZHENG M, WANG H, LIU H, et al. Survey on consensus algorithms of blockchain[J]. Netinfo Security, 2019(7): 8-24.

[25] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Security proofs for an efficient password-based key exchange[C]//Proceedings of the 10th ACM Conference on Computer and Communication Security. New York: ACM Press, 2003: 241-250.

[26] 屈娟, 冯玉明, 李艳平, 等. 可证明安全的面向无线传感器网络的三因素认证及密钥协商方案[J]. 通信学报, 2018, 39(S2): 189-197.
QU J, FENG Y M, LI Y P, et al. Provably secure three-factor authentication and key agreement scheme for wireless sensor network[J]. Journal on Communications, 2018, 39(S2): 189-197.

[作者简介]



张海波（1979− ），男，重庆人，博士，重庆邮电大学副教授、硕士生导师，主要研究方向为车联网、区块链、安全认证等。

黄宏武（1994− ），男，湖北孝感人，重庆邮电大学硕士生，主要研究方向为车联网、区块链、认证协议。

刘开健（1981− ），女，重庆人，重庆邮电大学讲师，主要研究方向为区块链、安全认证等。

贺晓帆（1985− ），男，河北保定人，博士，武汉大学教授，主要研究方向为资源优化、安全认证等。