

基于区块链的轻量级车载自组网条件隐私保护认证

周岳霖, 钟伯成, 王瑞

(上海工程技术大学电子电气工程学院, 上海 201620)

摘要: 条件隐私保护认证(CPPA)是一种车载自组网(VANET)中支持安全通信的有效途径。针对 VANET 中消息认证低效以及数据隐私存在敌手威胁的问题,提出基于区块链的轻量级 CPPA 方案。该方案在消息验证过程中采用改进的基于椭圆曲线加密的非交互式 Schnorr 签名算法,避免使用耗时的密码学操作;采用实体自行生成的短假名进行匿名通信,系统架构引入联盟区块链,在消息验证过程中利用智能合约技术自动验证发送者身份,减少了方案的通信开销。安全性分析结果表明,在随机预言模型(ROM)中,提出的方案在自适应选择消息攻击下具有抗伪造的安全性,且满足条件隐私保护要求。通过 MIRACL 密码学库测量了提出的方案和现有 CPPA 方案使用密码学操作的执行时间,并运用 Hyperledger Caliper 评估了区块链测试网络的交易延迟和吞吐量。实验结果表明,提出方案在签名生成和单条消息验证阶段的计算开销和通信开销均达到轻量级,且有效支持批量消息验证。

关键词: 车载自组网;条件隐私保护;联盟区块链;Schnorr 签名;随机预言模型

中图分类号: TP309

文献标志码: A

DOI: 10.19678/j.issn.1000-3428.0069973

Lightweight Vehicular Ad-Hoc Network Conditional Privacy-Preserving Authentication Based on Blockchain

ZHOU Yuelin, ZHONG Bocheng, WANG Rui

(School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

【Abstract】 Conditional Privacy-Preserving Authentication (CPPA) effectively supports secure communication in Vehicular Ad-hoc Network (VANET). To address the issues of inefficient message authentication and adversarial threats to data privacy in VANETs, a lightweight blockchain-based CPPA scheme is proposed. The proposed scheme utilizes an improved noninteractive Schnorr signature algorithm based on elliptic curve cryptography in the message verification phase, which avoids time-consuming cryptographic operations. The scheme employs entity-generated short pseudonyms for anonymous communication and introduces a consortium blockchain into the system architecture. The sender's identity is automatically verified during the message verification process using smart contract technology, thereby reducing the communication overhead of the scheme. Security analysis shows that the proposed scheme is secure against forgery under an adaptive chosen-message attack in the Random Oracle Model (ROM) while satisfying the requirements of conditional privacy preservation. Performance analysis measures the execution time of the proposed scheme and the existing CPPA scheme using cryptographic operations with the MIRACL cryptographic library. A Hyperledger Caliper is used to evaluate the transaction latency and throughput of the blockchain test network. The results demonstrate that the proposed scheme achieves lightweight computation and communication overhead in the signature generation and single-message verification phases and effectively supports batch message verification.

【Key words】 Vehicular Ad-hoc Network (VANET); conditional privacy-preserving; consortium blockchain; Schnorr signature; Random Oracle Model (ROM)

0 引言

智能交通系统旨在改善道路交通问题^[1]。新的汽车电信公司和制造商已经提出,无线工具将成为每辆车的一个组成部分,使车辆能够与其他车辆和道路基础设施进行通信。随着无线通信技术的快速

发展^[2-4]以及云计算、雾计算^[5-6]等计算模式的提出,车辆可以借助车载单元(OBU)和道路基础设施组建车载自组网(VANET)。

VANET 是移动自组网在智能交通领域的一种新型应用形态^[7],它能提供综合的智能交通服务^[8],有助于减少交通事故^[9]。利用 VANET 对各类交

基金项目: 国家自然科学基金(62102241)。

作者简介: 周岳霖,男,硕士研究生,主研方向为车联网安全;钟伯成(通信作者),教授;王瑞,硕士研究生。

收稿日期: 2024-06-06

修回日期: 2024-07-30

E-mail: bczhong@sues.edu.cn

通消息进行广播以提升交通效率已成为研究热点之一。VANET 节点数量众多且高速移动,其网络拓扑结构变化快,无线信道质量不稳定^[10],通信易受路边障碍物影响^[11]。

公共、开放的无线通信使 VANET 容易受到各种攻击^[12-13]。一方面,敌手可以通过监控无线信道轻松获取车辆的位置、速度、驾驶员身份和其他隐私。如果车辆直接使用真实身份在无线网络中进行通信,那么车辆的位置信息和移动轨迹将被直接暴露^[14]。另一方面,敌手通过监控无线信道并拦截、修改或删除传输的消息^[15],从而欺骗交通控制中心发出错误的指令,进而导致交通拥堵,甚至导致致命交通事故。因此,需要设计消息认证机制来保证消息的完整性^[16-17],以避免假冒或恶意修改。

匿名认证是车辆隐私保护的一般解决方案^[18],但是通过这种方式,车辆通信中敌手的身份隐私也得到了保护。为了缓解上述不足,同时提供匿名认证和可追溯性,条件隐私保护认证(CPPA)方案被认为是一种合适的方法。条件隐私保护意味着车辆对大多数实体保持匿名,受信任的实体可以提取车辆的真实身份,也可以追踪违规车辆并给予适当的处罚。

目前,有研究人员基于 VANET 提出了 CPPA 方案,部分方案的系统流程易受敌手攻击,还有部分方案的计算与通信开销过大,无法应用于真实 VANET 环境。为了使 CPPA 方案的安全性和性能实现更好的权衡,本文采用联盟区块链和改进的基于椭圆曲线密码学(ECC)的非交互式 Schnorr 签名技术,基于 VANET 提出了一种无证书条件隐私保护方案。

1 提出的方案

1.1 系统架构设计

本文提出的系统架构包含 4 类实体,即可信机构(TA)、装有车载单元(OBU)的车辆、路侧单元(RSU)和联盟区块链网络。系统架构涉及的 4 类实体如下:

1)TA:TA 是智能交通服务提供商,包含管理员,主要负责广播初始化区块链网络、车辆或 RSU 注册和追踪车辆真实身份。TA 利用智能合约提交已注册实体的假名和公钥信息。提出的方案假设 TA 为完全可信的实体,拥有 VANET 中存储空间和计算能力,也是唯一可以追踪车辆真实身份和撤销恶意车辆的实体。

2)车辆:车辆嵌有全球定位系统、嵌入式系统和其他传感器,能获取准确的时间信息。由于提出的

方案假设车辆为不可信实体,车辆传输消息需要验证环节。车辆的密钥对和假名均由车辆自行生成,车辆中的 OBU 配有防篡改设备,用来存储车辆密钥、假名等其他敏感信息,这些敏感信息将在消息发送后或年检期间更新。另外,车辆是 VANET 中拥有存储空间和计算能力最少的实体。

3)RSU:该实体位于路边或十字路口处,充当 VANET 的无线基站,并参与区块链共识过程。RSU 利用无线通信技术与管理范围内车辆通信,通过安全信道与 TA 进行 Internet 通信,并验证接收到的消息签名元组的有效性。RSU 可自行生成密钥对和假名。另外,提出的方案假设 RSU 为诚实且好奇的实体,且 VANET 中只有少数 RSU 会被敌手入侵。

4)联盟区块链网络:联盟区块链提供去中心化、不可篡改的数据存储,VANET 实体可调用自动化智能合约。该网络用于存储和管理已注册实体的假名和相应公钥,区块数据对 VANET 实体透明。RSU 和 TA 节点与区块链保持高频交互,并合作维护联盟区块链网络,但智能合约中提交与撤销操作只能由 TA 完成。此外,联盟区块链网络中的节点应用 PBFT 共识算法。

1.2 系统流程

系统流程使用的符号和相应定义描述如表 1 所示。

表 1 符号定义

Table 1 Definitions of symbols

符号	描述
$\mathbb{F}_p$	素数 p 的有限域
$E(\mathbb{F}_p)$	有限域 $\mathbb{F}_p$ 的椭圆曲线
G	加法循环群
q	加法循环群的阶数
P_{pub}	系统主公钥(TA 的公钥)
s	系统主私钥(TA 的私钥)
H_1, H_2	单向散列函数
P	加法循环群 G 的生成元
p_{pub}	系统公共参数
I_i	实体 i 的真实身份
A_i	实体 i 的假名
r_i	实体 i 的秘密值
K_i	实体 i 的公钥
k_i	实体 i 的私钥
σ_i	实体 i 对消息的数字签名
c	密文
$\text{Enc}_{K_i}(\cdot)$	用公钥 K_i 加密
$\text{Dec}_{k_i}(\cdot)$	用私钥 k_i 解密

本文提出的系统流程如图 1 所示。其中,车辆间通信以及车辆与 RSU 通信属于无线通信。提出的方案系统流程主要包含系统设置、智能合约部署、RSU 注册、车辆注册、消息签名生成、单条消息验证、批量消息

验证、追踪和撤销、密钥与假名更新 9 个部分。车辆和 RSU 均可充当消息的发送方或接收方。方案根据时间戳生成随机数种子,并使用 SHA-256 安全散列函数,另外,方案中联盟区块链采用 Hyperledger Fabric 平台。

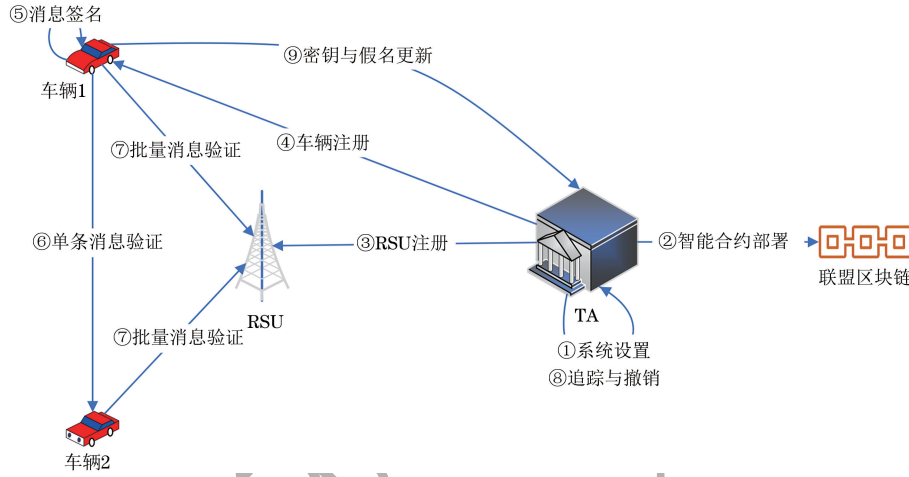


图 1 系统流程

Fig.1 System procedure

1.2.1 系统设置

TA 选定有限域 $\mathbb{F}_p$ 的非奇异椭圆曲线 $E(\mathbb{F}_p)$: $y^2 \equiv x^3 + ax + b \pmod{p}$, 其中, $a, b \in \mathbb{Z}_q^* = \{1, 2, \dots, q-1\}$, $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, p 为大素数, 并确定 $E(\mathbb{F}_p)$ 相应的加法循环群 G 、阶数 q 和生成元 P 。之后, TA 选择随机数 $s \in \mathbb{Z}_q^*$ 作为系统主私钥, $P_{\text{pub}} = s \cdot P$ 作为系统主公钥, 选择单向散列函数 $H_1: G \rightarrow \mathbb{Z}_q^*$, $H_2: \{0, 1\}^* \times \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ 。最后, TA 向 VANET 中的 RSU 和车辆节点发布公共参数 $p_{\text{pub}} = \{a, b, p, G, q, P, P_{\text{pub}}, H_1, H_2\}$, 并通过维护配置文件来建立联盟区块链。

1.2.2 智能合约部署

TA 将智能合约 PIDList 部署到联盟区块链中, 获得智能合约标识, 注意构造函数只执行一次。PIDList 主要为所有 VANET 实体提供假名记录的管理, 内含 Submit、Search 和 Revoke 三个函数, Submit 和 Revoke 只能由 TA 操作, 分别用于提交假名和撤销恶意实体的假名。智能合约标识将发布给 VANET 范围内所有车辆和 RSU, 用于后续调用智能合约 PIDList。智能合约 PIDList 的伪代码如下算法 1 所示。

算法 1 智能合约 PIDList

输入 函数名, 调用参数

输出 设置的函数

1. address manager; %管理员的地址
2. function PIDList()
%构造函数, 在智能合约部署期间自动执行
3. manager = msg.sender; %定义部署者为 TA

```

4. struct sPID
5. {
6.     PID; %uint256, 实体的假名
7.     PK; %uint256[2], 实体的公钥
8. }
9. mapping(uint256 → sPID) pid; %PID 的映射
10. function Submit(uint256 A, uint256[2] K) public
returns (address addr)
    %由管理员调用, 提交一条假名记录
11.     require(msg.sender == manager);
    %只有管理员可以成功调用该函数
12.     pid.PID = A;
13.     pid.PK = K;
14.     return msg.sender;
15. function Search(uint256 A) view returns (uint256[2])
    K)
    %任何实体均可调用, 获取假名对应的公钥
16.     if pid.PID == A then
17.         return pid.PK;
18.     return NULL;
19. function Revoke(uint256 A, uint256[2] K) public
returns (bool)
    %由管理员调用, 撤销某条假名记录
20.     require(msg.sender == manager);
    %只有管理员可以成功调用该函数
21.     if pid.PID == A || pid.PK == K then
22.         pid.PID = NULL;
23.         pid.PK = NULL;
24.         return 1;
25.     return 0;

```

1.2.3 RSU 注册

第 w 个路侧单元(RSU_w)收到公共参数 p_{pub} 后, RSU_w 随机选择 $k_w \in \mathbb{Z}_q^*$ 作为 RSU_w 的私钥,并计算 $K_w = k_w \cdot P$ 作为 RSU_w 的公钥。 RSU_w 之后选取身份 I_w ,并计算 A_w 作为 RSU_w 的假名,如式(1)所示:

$$A_w = I_w \oplus H_1(k_w \cdot P_{pub}) \quad (1)$$

然后 RSU_w 将 $\langle K_w, A_w \rangle$ 通过安全信道发送给 TA,TA 收到 $\langle K_w, A_w \rangle$ 后调用智能合约的 Submit 函数提交该假名记录至联盟区块链存储。注册完成后, RSU_w 向其区域内的车辆广播 $\langle K_w, A_w \rangle$ 。 RSU_w 管理范围的车辆将存储 K_w 在 OBU 中。

1.2.4 车辆注册

当第 i 辆车辆 V_i 收到公共参数 p_{pub} 后, V_i 选择随机数 $k_i \in \mathbb{Z}_q^*$ 作为车辆的私钥,并计算 $K_i = k_i \cdot P$ 作为 V_i 的公钥。 V_i 使用车辆识别符作为真实身份 I_i ,然后计算车辆 V_i 的假名,如式(2)所示:

$$A_i = I_i \oplus H_1(k_i \cdot P_{pub}) \quad (2)$$

然后 V_i 将 $\langle K_i, A_i \rangle$ 通过安全信道发送给 TA,TA 收到 $\langle K_i, A_i \rangle$ 后调用智能合约的 Submit 函数提交该假名记录至联盟区块链存储,注册过程中 K_i, k_i 和 A_i 存储在 V_i 的 OBU 中。

1.2.5 消息签名生成

假设车辆 V_i 作为消息 m_i 的发送方,则 V_i 先随机选择秘密值 $r_i \in \mathbb{Z}_q^*$,并计算 $R_i = r_i \cdot P$,然后 V_i 生成时间戳 t_i ,并利用其私钥 k_i 计算 $S_i = r_i + H_2(m_i \parallel A_i \parallel K_i \parallel t_i) \cdot k_i \pmod{q}$, m_i 的数字签名记为 $\sigma_i = \{R_i, S_i\}$ 。最后, V_i 将 $\langle m_i, \sigma_i, t_i, A_i \rangle$ 发送给验证方。

1.2.6 单条消息验证

对于消息签名元组 $\langle m_i, \sigma_i, t_i, A_i \rangle$,验证方首先检查时间戳 t_i 的新鲜度,记 t_{cur} 表示验证方收到消息签名元组生成的时间戳, Δt 表示最大有效时间间隔,则验证方验证 $|t_{cur} - t_i| \leq \Delta t$ 是否成立,若无效则丢弃该消息签名元组。之后调用智能合约的 Search 函数,验证 A_i 是否有效,若有效,则验证方可获得假名相应公钥 K_i ,并验证式(3)是否成立,若成立,则验证方接收该消息签名元组。

$$S_i \cdot P = R_i + H_2(m_i \parallel A_i \parallel K_i \parallel t_i) \cdot K_i \quad (3)$$

1.2.7 批量消息验证

对于接收到的 n 个消息签名元组: $\langle m_1, \sigma_1, t_1, A_1 \rangle, \langle m_2, \sigma_2, t_2, A_2 \rangle, \dots, \langle m_n, \sigma_n, t_n, A_n \rangle$,验证者先验证时间戳的新鲜度和假名的有效性(借助智能合约),然后验证式(4)是否成立,若式(4)成立,则验证方接收这 n 个消息签名元组。

$$\sum_{j=1}^n S_j \cdot P = \sum_{j=1}^n R_j + \sum_{j=1}^n (H_2(m_j \parallel A_j \parallel K_j \parallel t_j) \cdot K_j) \quad (4)$$

1.2.8 追踪和撤销

根据 VANET 中其他节点的举报,TA 获取 $\langle m_o, \sigma_o, t_o, A_o \rangle$ 中恶意车辆 V_o 的假名 A_o ,之后 TA 利用主私钥 s 计算 I_o 来揭露 V_o 的真实身份,如式(5)所示:

$$I_o = A_o \oplus H_1(s \cdot K_o) \quad (5)$$

然后 TA 调用智能合约的 Revoke 函数来完成 V_o 的撤销操作,被撤销的车辆无法再次加入 VANET。

1.2.9 密钥与假名更新

为防止敌手链接同一车辆发送的不同消息,车辆 V_i 在发送完消息后,或在长期未使用 OBU 存储数据的情况下,均需更新存储在 OBU 上的密钥和假名。 V_i 选择新随机数 $k_{i_new} \in \mathbb{Z}_q^*$ 作为车辆的新私钥,并计算 $K_{i_new} = k_{i_new} \cdot P$ 作为车辆的新公钥。然后, V_i 计算新假名 $A_{i_new} = I_i \oplus H_1(k_{i_new} \cdot P_{pub})$ 。假设 V_i 收到附近 RSU_w 的公钥 K_w , V_i 使用 K_w 对公钥与假名进行加密得到密文 $c = \text{Enc}_{K_w}(K_{i_new} \parallel A_{i_new})$ (可使用 ECC 加密、ElGamal 加密等公钥加密算法),并将密文 c 传输给 RSU_w ,然后, RSU_w 使用其私钥 k_w 解密得 $(K_{i_new} \parallel A_{i_new}) = \text{Dec}_{k_w}(c)$,并将 $\langle K_{i_new}, A_{i_new} \rangle$ 通过安全信道发送给 TA。最后 TA 根据假名生成等式[即式(1)或式(2)]计算 I_i ,如式(6)所示:

$$I_i = A_{i_new} \oplus H_1(s \cdot K_{i_new}) \quad (6)$$

确认 I_i 是否代表已注册实体,若 I_i 代表的实体已注册,则 TA 调用智能合约 Submit 函数,将 $\langle K_{i_new}, A_{i_new} \rangle$ 提交至联盟区块链存储。

2 安全性分析

2.1 安全模型

根据敌手的能力,提出的方案考虑到敌手 Adv 扮演不诚实的签名者角色,包含恶意车辆和恶意 RSU,但敌手 Adv 无法替换目标用户的公钥^[19]。挑战者 C 与敌手 Adv 的博弈(Game)是在针对自适应选择消息攻击的存在不可伪造性模型下进行的。敌手 Adv 可以通过以下由 C 执行的预言(Oracle)进行查询^[19]:

1) Setup($\bullet$)-Oracle:该预言以安全参数 λ 作为输入,系统主私钥 s 和公共参数 p_{pub} 作为输出。C 将系统主私钥 s 秘密保存,并将公共参数 p_{pub} 转发

给 Adv。

2) $H_1(\cdot)$ -Oracle: 该预言以 α 作为输入, 以对应散列值作为输出, C 将对应散列值转发给 Adv, 并在散列值列表中插入相应元组。

3) $H_2(\cdot)$ -Oracle: 该预言以消息 m_i 、假名 A_i 、公钥 K_i 和时间戳 t_i 作为输入, 以对应散列值作为输出, C 将对应散列值转发给 Adv, 并在散列值列表中插入相应元组。

4) KeyExtract($\cdot$)-Oracle: 该预言将假名 A_i 作为输入, 并将输出的密钥转发给 Adv。

5) Corruption($\cdot$)-Oracle: 该预言用于获取目标用户的私钥。在检查 KeyExtract($\cdot$)-Oracle 的输出后, C 将用户的私钥转发给 Adv。

6) Sign($\cdot$)-Oracle: 该预言用于获取消息签名。C 将签名转发给 Adv, 同时进行记录。

根据敌手 Adv 的定义, 本文定义了博弈 Game_1 。

Game_1 : Adv 为消息 $\langle m_i, A_i \rangle$ 输出伪造签名 σ_{Adv} 。如果满足以下要求, 那么 Adv 赢得了博弈。

- 1) σ_{Adv} 是消息 m_i 的有效签名。
- 2) A_i 在 Corruption($\cdot$)-Oracle 期间不被查询。
- 3) $\langle m_i, A_i \rangle$ 在 Sign($\cdot$)-Oracle 期间不被查询。

定义 1 对于自适应选择的消息攻击安全模型, 如果在进行 q_M 次签名查询后, 不存在能够在 T 时间内以不可忽略的优势 ϵ 赢得 Game_1 的 Adv, 则签名方案在存在不可伪造性下 (T, q_M, ϵ) 是安全的。

基于椭圆曲线密码学, 提出的方案使用如下的假设。

定义 2 椭圆曲线离散对数问题(ECDLP) 已知元组 $\langle P, Q = sP \in G \rangle$, 任何概率多项式时间(PPT), 敌手计算密钥 s 的概率忽略不计。

2.2 形式化安全性证明

引理 1 对于敌手 Adv, 提出的方案在 Game_1 中是不可伪造的。假设 $S_{\text{Adv}}^{\text{Succ}}$ 表示 Adv 在 Game_1 成功的概率, 如果 ECDLP 假设在 G 中成立, 那么 Adv 求解 ECDLP 的概率为:

$$S_{\text{Adv}}^{\text{Succ}} \geq \frac{1}{q_M} \left(1 - \frac{1}{q_M}\right)^{q_M} \epsilon \quad (7)$$

式中: ϵ 表示提出方案被破解的概率; q_M 表示所有查询的最大次数。

证明: Adv 以概率 ϵ 赢得 Game_1 。C 是一个挑战者, 旨在以不可忽略的概率求解 ECDLP, 即 $K_j = k_j \cdot P$, 其中, $K_j, P \in G, k_j \in \mathbb{Z}_q^*$ 。C 在各种列表中维护所有查询的输出。C 首先初始化 1 个密钥对列

表 List_{key} 、1 个签名列表 $\text{List}_{\text{sign}}$ 、2 个安全散列值列表 List_{H_1} 和 List_{H_2} 为空。

下面是查询及其输出:

1) Setup($\cdot$): C 以安全参数 λ 作为输入来运行 Setup($\cdot$)-Oracle, 然后随机选择 $s \in \mathbb{Z}_q^*$ 作为系统主私钥, 并设 $P_{\text{pub}} = s \cdot P$ 作为系统主公钥, 将 $p_{\text{pub}} = \{P_{\text{pub}}, P, q, H_1, H_2\}$ 作为系统公共参数。C 随机选择一个满足 $1 \leq L \leq M_{H_2}$ 的索引 L , 其中 M_{H_2} 为 $H_2(\cdot)$ -Oracle 请求的个数。

2) KeyExtract($\cdot$)-query: 接收到 Adv 使用用户的 A_j ($1 \leq j \leq M_{\text{key}}, M_{\text{key}}$ 为密钥查询次数) 进行 KeyExtract($\cdot$) 查询之后, C 首先在 List_{key} 中查找元组 $\langle A_j, K_j, k_j \rangle$ 是否存在, 如果存在, 则 C 将 K_j 返回给 Adv。否则, 它的响应如下:

- (1) 若 $j \neq L$, C 选择私钥 $k_j \in \mathbb{Z}_q^*$, 并设公钥 $K_j = k_j \cdot P$ 。
- (2) 若 $j = L$, 则 C 设公钥 $K_j = P_{\text{pub}}$ 。
- (3) C 将元组 $\langle A_j, K_j, k_j \rangle$ 添加到 List_{key} 中, 并返回 K_j 给 Adv。

3) $H_1(\cdot)$ -query: C 接收到 Adv 用 α 进行 $H_1(\cdot)$ 查询时, 其中 $\alpha = s \cdot K_j$ 或 $\alpha = k_j \cdot P_{\text{pub}}$, C 查找 List_{H_1} 中是否存在元组 $\langle \alpha, L_{j_1} \rangle$, 其中 $L_{j_1} = H_1(\alpha)$ 。如果存在, 那么 C 返回 L_{j_1} 给 Adv。否则, C 随机选择 $L_{j_1} \in \mathbb{Z}_q^*$ 并计算 $L_{j_1} = H_1(\alpha)$ 。最后, C 将元组 $\langle \alpha, L_{j_1} \rangle$ 添加到 List_{H_1} 中, 并将 L_{j_1} 返回给 Adv。

4) $H_2(\cdot)$ -query: 当 C 接收到 Adv 用元组 $\langle m_j, A_j, K_j, t_j \rangle$ 进行 $H_2(\cdot)$ 查询时, C 查找 List_{H_2} 中是否存在元组 $\langle m_j, A_j, K_j, t_j, L_{j_2} \rangle$, 其中 $L_{j_2} = H_2(m_j \parallel A_j \parallel K_j \parallel t_j)$ 。如果存在, 那么 C 将 L_{j_2} 返回给 Adv。否则, C 随机选择 $L_{j_2} \in \mathbb{Z}_q^*$ 并计算 $L_{j_2} = H_2(m_j \parallel A_j \parallel K_j \parallel t_j)$ 。最后, C 将元组 $\langle m_j, A_j, K_j, t_j, L_{j_2} \rangle$ 添加到 List_{H_2} 中, 并将 L_{j_2} 返回给 Adv。

5) Corruption($\cdot$)-query: 收到 Adv 的查询后, C 采取以下步骤:

- (1) 若 $j \neq L$, C 检查 List_{key} 中是否存在元组 $\langle A_j, K_j, k_j \rangle$, 如果是, 则 C 返回 k_j 给 Adv; 否则, C 随机选择 $k_j \in \mathbb{Z}_q^*$ 并设 $K_j = k_j \cdot P$ 。然后, C 返回 k_j 给 Adv 并更新 List_{key} 。
- (2) 若 $j = L$, C 返回 $\perp$ 。

6) Sign($\cdot$)-query: 收到 Adv 的查询后, C 采取以下步骤:

- (1) 若 $j \neq L$, C 执行签名算法 Sign($\cdot$), 并将签

(Peer)节点,用户类型包含管理员(Admin)。性能评估采用 Hyperledger Caliper V0.5.0 评估套件,并使用键值(Key-Value)数据库 leveldb 来存储状

态数据。本评估所涉及的依赖包括 Docker V26.0.0、Docker Compose V1.29.2、go V1.18、Node.js V16.20.2 和 npm V8.19.4。测试网络建立了一个名为 mychannel 的通道,并在其中部署了智能合约 PIDList(即算法 1)。

3.2 计算开销分析

对于计算开销,表 3 显示了本文涉及到的密码学操作的执行时间,实验所涉及到的密码学操作执行 1 000 次,取执行时间的平均值作为密码学操作执行时间。

表 3 密码学操作的执行时间

Table 3 Execution time of cryptographic operations

符号	描述	单位:ms
T_h	SHA-256 函数执行时间	0.000 7
T_{sm}	加法循环群 G 的标量乘法运算时间	0.473 7
T_{ssm}	加法循环群 G 的小指数标量乘法运算时间	0.041 2
T_{sa}	加法循环群 G 的点加法运算时间	0.002 1

需要注意的是,由于一些运算执行时间极短(即执行时间比 SHA-256 函数执行时间更短),本文中大整数的加减法、乘法及异或运算和 $\mathbb{Z}_q^*$ 上的模量乘法、模量加法运算的执行时间忽略不计。由表 3 可知, G 的标量乘法运算(即 T_{sm})是这 4 类运算中最耗时的。

另外,消息签名生成与验证过程的实际总耗时会略高于方案的计算开销。原因是整个签名与验证过程包括消息传输的延迟,该延迟一般随车辆密度增加而增加,而计算开销分析不考虑消息传输延迟。

本文分析了提出的方案和其他方案在消息签名生成、单条消息验证和批量消息验证 3 个系统阶段的计算开销,并与 6 个现有的 CPPA 方案进行比较。表 4 给出了提出的方案与比较方案在消息签名生成阶段的计算开销。

表 4 签名生成阶段的计算开销比较

Table 4 Comparison of computational overhead of the signature generation phase

方案	计算开销	单位:ms
文献[22]方案	$T_{sm} + 2T_h \approx 0.475 1$	
文献[23]方案	$T_{sm} + T_h \approx 0.474 4$	
文献[24]方案	$T_{sm} + T_h \approx 0.474 4$	
文献[25]方案	$T_{sm} + T_{sa} + T_h \approx 0.476 5$	
文献[26]方案	$T_{sm} + T_{sa} + T_h \approx 0.476 5$	
文献[27]方案	$3T_{sm} + T_{sa} + T_h \approx 1.423 9$	
提出的方案	$T_{sm} + T_h \approx 0.474 4$	

在提出的方案中,消息签名生成阶段需要 1 次 G 的标量乘法运算和 1 次 SHA-256 函数运算,该阶段计算开销为 $T_{sm} + T_h \approx 0.474 4$ ms。在消息签名生成阶段中,文献[22]方案需要 1 次 G 的标量乘法运算和 2 次 SHA-256 函数运算,文献[23-24]方案均需要 1 次 G 的标量乘法运算和 1 次 SHA-256 函数运算,文献[25-26]方案均需要 1 次 G 的标量乘法运算、1 次 G 的点加法运算和 1 次 SHA-256 函数运算,文献[27]方案需要 3 次 G 的标量乘法运算、1 次 G 的点加法运算和 1 次 SHA-256 函数运算。由表 4 可知,提出的方案以及文献[23-24]方案拥有最低的计算开销。

表 5 给出了提出的方案与比较方案在单条消息验证阶段的计算开销。在提出的方案中,单条消息验证阶段需要 2 次 G 的标量乘法运算、1 次 G 的点加法运算和 1 次 SHA-256 函数运算,该阶段计算开销为 $2T_{sm} + T_{sa} + T_h \approx 0.950 2$ ms。

表 5 单条消息验证阶段的计算开销比较

Table 5 Comparison of computational overhead of single message verification phase

方案	计算开销	单位:ms
文献[22]方案	$2T_{sm} + T_{sa} + T_h \approx 0.950 2$	
文献[23]方案	$2T_{sm} + T_{sa} + T_h \approx 0.950 2$	
文献[24]方案	$3T_{sm} + 2T_{sa} + 2T_h \approx 1.426 7$	
文献[25]方案	$3T_{sm} + 2T_{sa} + 2T_h \approx 1.426 7$	
文献[26]方案	$2T_{sm} + 2T_{sa} + T_h \approx 0.952 3$	
文献[27]方案	$3T_{sm} + 4T_{sa} + T_h \approx 1.430 2$	
提出的方案	$2T_{sm} + T_{sa} + T_h \approx 0.950 2$	

在单条消息验证阶段中,文献[22-23]方案均需要 2 次 G 的标量乘法运算、1 次 G 的点加法运算和 1 次 SHA-256 函数运算,文献[24-25]方案均需要 3 次 G 的标量乘法运算、2 次 G 的点加法运算和 2 次 SHA-256 函数运算,文献[26]方案需要 2 次 G 的标量乘法运算、2 次 G 的点加法运算和 1 次 SHA-256 函数运算,文献[27]方案需要 3 次 G 的标量乘法运算、4 次 G 的点加法运算和 1 次 SHA-256 函数运算。由表 5 可知,提出的方案与文献[22-23]方案在单条消息验证阶段拥有最低的计算开销。

根据表 4 和表 5 的结果可知,提出的方案和文献[23]方案能在 299.166 ms 时间内完成 210 条消息的签名生成和单条消息验证操作。

表 6 给出了提出的方案和比较方案在批量消息验证阶段的计算开销。图 2 用折线图直观地展示了各方案在批量消息验证阶段的计算开销。假设批量消息验证中消息数为 n ,那么提出的方案在批量消

息验证阶段需要 $n+1$ 次 G 的标量乘法运算、 $2n$ 次 G 的点加法运算和 n 次 SHA-256 函数运算,该阶段

计算开销为 $(n+1)T_{sm}+2nT_{sa}+nT_h \approx 0.4786n+0.4737$ ms。

表 6 批量消息验证阶段的计算开销比较

Table 6 Comparison of computational overhead of batch message verification phase

单位:ms

方案	n 条消息批量验证阶段计算开销
文献[22]方案	$2T_{sm}+2nT_{ssm}+(n+1)T_{sa}+nT_h \approx 0.0852n+0.9495$
文献[23]方案	$2T_{sm}+nT_{ssm}+nT_{sa}+nT_h \approx 0.044n+0.9474$
文献[24]方案	$(n+2)T_{sm}+2nT_{ssm}+2nT_{sa}+2nT_h \approx 0.5617n+0.9474$
文献[25]方案	$(n+2)T_{sm}+2nT_{ssm}+2nT_{sa}+2nT_h \approx 0.5617n+0.9474$
文献[26]方案	$2nT_{sm}+2nT_{ssm}+nT_h \approx 0.9523n$
文献[27]方案	$(2n+2)T_{sm}+4nT_{sa}+nT_h \approx 0.9565n+0.9474$
提出的方案	$(n+1)T_{sm}+2nT_{sa}+nT_h \approx 0.4786n+0.4737$

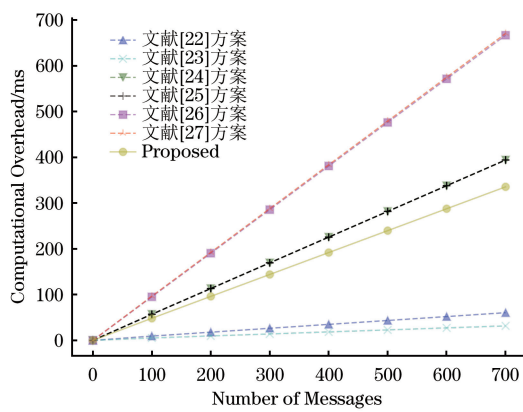


图 2 不同方案批量消息验证阶段的计算开销

Fig.2 The computational overhead of the batch message verification phase in different schemes

对于 n 条消息的批量验证,文献[22]方案需要 2 次 G 的标量乘法运算、 $2n$ 次 G 的小指数标量乘法运算、 $n+1$ 次 G 的点加法运算和 n 次 SHA-256 函数运算,文献[23]方案需要 2 次 G 的标量乘法运算、 n 次 G 的小指数标量乘法运算、 n 次 G 的点加法运算和 n 次 SHA-256 函数运算,文献[24-25]方案均需要 $n+2$ 次 G 的标量乘法运算、 $2n$ 次 G 的小指数标量乘法运算、 $2n$ 次 G 的点加法运算和 $2n$ 次 SHA-256 函数运算,文献[26]方案需要 $2n$ 次 G 的标量乘法运算、 $2n$ 次 G 的点加法运算和 n 次 SHA-256 函数运算,文献[27]方案需要 $2n+2$ 次 G 的标量乘法运算、 $4n$ 次 G 的点加法运算和 n 次 SHA-256 函数运算。

根据表 4 和表 6 的结果可知,提出的方案能在 299.7157 ms 的时间内完成 314 条消息签名生成和批量消息验证操作。

根据表 6 可知,虽然提出的方案的批量消息验证阶段时间开销低于文献[24-27]方案,但是高于文献[22-23]方案。根据安全性分析可知,提出的方案可以抵御窃取验证表攻击和密钥泄露攻击,而文

献[22-23]方案无法抵御这些攻击。在文献[22-23]方案中,消息发送方与验证方采用签名密钥,而不是提出的方案使用的实体公私钥。尽管签名密钥在批量消息验证阶段能让验证方执行标量乘法的次数达到常量级,以达到更小的计算开销,但这些方案中签名密钥易遭受密钥泄露攻击。另外,根据通信开销分析可知,文献[22-23]方案的通信开销比提出的方案更高。因此,提出的方案实现了更好的安全性与性能的权衡,其批量消息验证计算开销是可接受的,且具有良好的可扩展性。

3.3 通信开销分析

对于通信开销,表 7 显示了本文传输数据中的数据类别和大小,其中,根据 IEEE 1609.2 标准^[21], $|m|$ 的大小设为 67 Byte。

表 7 传输数据类别与大小

Table 7 Transmission data types and sizes 单位:Byte

符号	描述	数据大小
$ G $	加法循环群 G 元素大小	64
$ \mathbb{Z}_q^* $	有限域 $\mathbb{Z}_q^*$ 元素大小	32
$ t $	时间戳所占用的空间	8
$ m $	传输消息所占用的空间	67

为了公平比较,本文假设比较方案中各类数据大小与提出方案一致,且只将传输的消息签名元组所占空间大小作为方案的通信开销。

表 8 给出了提出的方案和比较方案的通信开销。在提出的方案中,发送方传输消息签名元组 $\langle m_i, \sigma_i, t_i, A_i \rangle$,其中 $\sigma_i = \{R_i, S_i\}$, $R_i \in G$, $S_i \in \mathbb{Z}_q^*$, $A_i \in \mathbb{Z}_q^*$, m_i 为消息, t_i 为时间戳。因此,对于单条消息,提出的方案的通信开销为 $|G| + 2|\mathbb{Z}_q^*| + |m| + |ts| = 64 + 2 \times 32 + 32 + 8 = 203$ Byte,其中签名长度为 $|G| + |\mathbb{Z}_q^*| = 64 + 32 = 96$ Byte。对于 n 条消息,提出的方案相应的通信开销为 $203n$ Byte。其他方案的通信开销可按上述方

法进行计算。

表 8 不同方案的通信开销比较

Table 8 Comparison of communication overhead of different schemes

单位:Byte

方案	通信开销
文献[22]方案	$ G + 3 Z_q^* + m + 2 t = 243$
文献[23]方案	$ G + 3 Z_q^* + m + t = 235$
文献[24]方案	$2 G + 2 Z_q^* + m + t = 267$
文献[25]方案	$2 G + 2 Z_q^* + m + t = 267$
文献[26]方案	$ G + 2 Z_q^* + m + t = 203$
文献[27]方案	$4 G + 3 Z_q^* + m + t = 427$
提出的方案	$ G + 2 Z_q^* + m + t = 203$

根据表 8 可知,提出的方案和文献[26]方案的通信开销是最小的,相比于其他方案,提出的方案在

表 9 Caliper 评估结果

Table 9 Caliper benchmark results

函数名	成功次数/次	失败次数/次	传输速率/(transaction·s ⁻¹)	最大延迟/s	最小延迟/s	平均延迟/s	吞吐量/(transaction·s ⁻¹)
Submit	500	0	22.4	2.02	0.02	0.23	20.5
Search	500	0	526.9	0.02	0.00	0.00	524.7
Revoke	500	0	540.0	0.01	0.00	0.00	538.2

4 结束语

本文提出一种采用联盟区块链和 Schnorr 签名且适用于 VANET 的轻量级 CPPA 方案。安全性及性能分析结果表明,提出的方案满足了条件隐私保护要求,在签名生成和单条消息验证阶段的计算与通信开销达到轻量级,有效支持批量消息验证,与现有的方案相比处于低开销水平。未来将在真实的 VANET 环境中测试消息签名与验证算法,并进一步评估 VANET 消息认证全过程中实际的计算开销。

参考文献

[1] LIU Y, WANG C X, HUANG J, et al. Novel 3-D nonstationary MmWave massive MIMO channel models for 5G high-speed train wireless communications [J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2077-2086.

[2] AGIWAL M, ROY A, SAXENA N. Next generation 5G wireless networks: a comprehensive survey [J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 1617-1655.

[3] JI M, CAIRE G, MOLISCH A F, et al. Wireless device-to-device caching networks: basic principles and system performance [J]. IEEE Journal on Selected Areas in Communications, 2016, 34(1): 176-189.

[4] SIMSEK M, AIJAZ A, DOHLER M, et al. 5G-enabled tactile Internet [J]. IEEE Journal on Selected Areas in Communications, 2016, 34(3): 460-473.

[5] WANG T, ZHOU J Y, CHEN X L, et al. A three-layer

传输消息签名元组的过程中不需要传输公钥,且假名的长度更短,更适用于通信带宽受限的 VANET 环境中。

3.4 区块链性能评估

为保证结果的准确性,本文对智能合约每个算法在随机输入样本上使用 Hyperledger Caliper 运行 500 次测试,评估结果如表 9 所示。由表 9 可知,智能合约所有函数的 500 次测试均成功执行。Submit 函数是可以定期预执行的,其平均延迟为 0.23 s,Search 和 Revoke 函数的延迟均小于等于 0.02 s。另外,智能合约所有函数的吞吐量完成率(即吞吐量除以传输速率)均在 91.5%以上。综上,提出的方案的区块链性能满足 VANET 应用需求,具有良好的可扩展性。

privacy preserving cloud storage scheme based on computational intelligence in fog computing [J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 3-12.

[6] HOU X, LI Y, CHEN M, et al. Vehicular fog computing: a viewpoint of vehicles as the infrastructures [J]. IEEE Transactions on Vehicular Technology, 2016, 65(6): 3860-3873.

[7] 宋彩霞, 谭国真, 丁男, 等. 面向应用的车载自组织网络跨层多信道 MAC 协议[J]. 通信学报, 2016, 37(5): 95-105.

SONG C X, TAN G Z, DING N, et al. Application oriented cross-layer multi-channel MAC protocol for VANET [J]. Journal on Communications, 2016, 37(5): 95-105. (in Chinese)

[8] ZHANG F S, LIU H, LEUNG Y W, et al. CBS: community-based bus system as routing backbone for vehicular ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2017, 16(8): 2132-2146.

[9] AUNG N, ZHANG W D, DHELMIS S, et al. Accident prediction system based on hidden Markov model for vehicular ad-hoc network in urban environments [J]. Information, 2018, 9(12): 311.

[10] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.

[11] EZE E C, ZHANG S J, LIU E J, et al. Advances in vehicular ad-hoc networks: challenges and road-map for future development[J]. International Journal of Automation and Computing, 2016, 13(1): 1-18.

[12] 杨小东, 李沐紫, 马国祖, 等. 车联网中支持非法签名定位的无证书匿名认证方案[J]. 计算机工程, 2024, 50(6): 157-165.

YANG X D, LI M Z, MA G Z, et al. Certificateless anonymous authentication scheme supporting illegal signatures localization for internet of vehicles[J]. Computer Engineering, 2024, 50(6): 157-165. (in Chinese)

- [13] LAI C Z, LU R X, ZHENG D, et al. Security and privacy challenges in 5G-enabled vehicular networks [J]. *IEEE Network*, 2020, 34(2): 37-45.
- [14] PALANISWAMY B, CAMTEPE S, FOO E, et al. An efficient authentication scheme for intra-vehicular controller area network [J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 3107-3122.
- [15] ISAAC J T, ZEADALLY S, CÁMARA J S. Security attacks and solutions for vehicular ad hoc networks [J]. *IET Communications*, 2010, 4(7): 894-903.
- [16] LIN X D, LI X. Achieving efficient cooperative message authentication in vehicular ad hoc networks [J]. *IEEE Transactions on Vehicular Technology*, 2013, 62(7): 3339-3348.
- [17] ZHANG J, CUI J, ZHONG H, et al. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks [J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(2): 722-735.
- [18] VIJAYAKUMAR P, AZEES M, KOZLOV S A, et al. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs [J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(2): 1630-1638.
- [19] 陈蕾. 车联网中基于雾计算的安全高效认证方法研究 [D]. 合肥: 安徽大学, 2023.
CHEN L. Research on secure and efficient authentication method based on fog computing for vehicular ad hoc network [D]. Hefei: Anhui University, 2023: (in Chinese)
- [20] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures [J]. *Journal of Cryptology*, 2000, 13(3): 361-396.
- [21] IEEE standard for wireless access in vehicular environments—security services for applications and management messages: IEEE 1609.2-2016 [S]. New York, USA: Institute of Electrical and Electronics Engineers, 2016.
- [22] AL-SHAREEDA M A, ANBAR M, MANICKAM S, et al. A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks [J]. *Sensors*, 2022, 22(5): 1696.
- [23] ALSHUDUKHI J S, MOHAMMED B A, AL-MEKHLAFI Z G. An efficient conditional privacy-preserving authentication scheme for the prevention of side-channel attacks in vehicular ad hoc networks [J]. *IEEE Access*, 2020, 8: 226624-226636.
- [24] SHEN L Y, WANG L L, ZHANG K, et al. An efficient conditional privacy-preserving authentication scheme with scalable revocation for VANETs [J]. *Journal of Systems Architecture*, 2022, 133: 102764.
- [25] ZHONG H, CHEN L, CUI J, et al. Secure and lightweight conditional privacy-preserving authentication for fog-based vehicular ad hoc networks [J]. *IEEE Internet of Things Journal*, 2022, 9(11): 8485-8497.
- [26] ZHOU X T, HE D B, KHAN M K, et al. An efficient blockchain-based conditional privacy-preserving authentication protocol for VANETs [J]. *IEEE Transactions on Vehicular Technology*, 2023, 72(1): 81-92.
- [27] LIN C, HUANG X Y, HE D B. EBCPA: efficient blockchain-based conditional privacy-preserving authentication for VANETs [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023, 20(3): 1818-1832.

文字编辑 索书志
栏目编辑 赖玉玲