

具有隐私保护的动态高效车载云管理方案

肖敏¹, 姚涛², 刘媛妮¹, 黄永洪¹

(1. 重庆邮电大学网络空间与信息法学院, 重庆 400065; 2. 重庆邮电大学计算机科学与技术学院, 重庆 400065)

摘要: 由车辆自主形成的车载云用于交通传感数据的本地化处理和消耗, 实现高时效性的智能交通管理。针对车载云的高度动态性、自组织性和高时效性特点及其车联网中用户身份和位置隐私保护需求带来的车载云管理挑战, 设计了基于非对称群密钥协商协议的动态自组织车载云管理方案, 通过车辆自组织的群密钥协商自动形成车载云, 利用群密钥控制车载云服务提供与访问, 利用群密钥更新动态管理车载云。该方案使用可追踪的一次性假名技术实现车辆的匿名认证和条件隐私保护, 并在群密钥协商阶段只使用一次双线性, 使运算实现了更高的效率; 密钥协商和更新过程利用支持批量验证的轻量级签名实现高效的消息源认证和完整性认证, 在确保效率的前提下保证自组织环境下车载云通信的安全性; 密钥协商协议的动态密钥更新机制实现车载云中车辆的动态加入或退出, 适应车载云的动态性特点。在随机预言机模型和求逆计算 Diffie-Hellman (ICDH) 问题困难假设下, 证明了非对称群密钥协商方案满足选择明文安全性。安全性分析显示所提方案能够保护车辆用户的身份和位置隐私, 能够实现恶意车辆的合法追踪, 保证通信的保密性、完整性和防假冒以及车载云动态管理的前向安全性。性能对比分析证明所提方案在实现相同功能和满足相同安全性的情况下具有一定的通信和计算效率优势。

关键词: 车载云; 非对称群密钥协商; 隐私保护; 匿名认证

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022083

Dynamic and efficient vehicular cloud management scheme with privacy protection

XIAO Min¹, YAO Tao², LIU Yuanni¹, HUANG Yonghong¹

1. School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

2. School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: The vehicular cloud (VC) formed by vehicles is used for localization processing and consumption of traffic sensing data to achieve timely intelligent traffic management. The vehicle cloud is highly dynamic, self-organizing and timely, in which the identity and location privacy of vehicle users need to be protected as this

收稿日期: 2022-01-20; 修回日期: 2022-09-12

通信作者: 肖敏, xiaomin@cqupt.edu.cn

基金项目: 四川省重点研发计划(2020YFG0292)

Foundation Item: The Key Research and Development Project of Sichuan Province(2020YFG0292)

引用格式: 肖敏, 姚涛, 刘媛妮, 等. 具有隐私保护的动态高效车载云管理方案[J]. 网络与信息安全学报, 2022, 8(6): 70-83.

Citation Format: XIAO M, YAO T, LIU Y N, et al. Dynamic and efficient vehicular cloud management scheme with privacy protection[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 70-83.

poses challenges to the vehicular cloud management. A dynamic and self-organizing vehicle cloud management scheme based on the asymmetric group key agreement protocol was designed, where the vehicle cloud is automatically formed through the self-organized group key agreement of vehicles. The group key was used to control the provision and access of vehicle cloud services, and the dynamic management of the vehicle cloud was implemented through group key update. The scheme used traceable one-time pseudonym technology to achieve anonymous authentication and conditional privacy protection of vehicle users, and the group key agreement stage only included one bilinear pair operation to achieve high efficiency. In addition, the key negotiation and update process used lightweight signatures, supporting batch verification, to achieve efficient message source authentication and integrity authentication. Then the security and efficiency of vehicle cloud communications in the self-organizing environment can be ensured. The dynamic key update mechanism of the key agreement protocol realized the dynamic joining or exiting of vehicles in the vehicle cloud, adapting to the dynamic characteristics of the vehicle cloud. Under the random oracle model and the difficult assumption of the inverse computational Diffie Hellman (ICDH) problem, it was proved that the asymmetric group key agreement scheme satisfied the selective-plaintext security. The security analysis shows that the scheme can protect the identity and location privacy of vehicle users, realize the legal tracking of malicious vehicles, and ensure the confidentiality, integrity and anti-counterfeiting of communications, as well as the forward security of vehicle cloud dynamic management. The performance comparison analysis shows that this scheme has certain advantages in communication and computing efficiency under the condition of the same function and security level.

Keywords: vehicular cloud, asymmetric group key agreement, privacy protection, anonymous authentication

0 引言

随着车载自组网 (VANET, vehicular ad-hoc network) 以及自动驾驶汽车技术的发展, 汽车正在成为一个集成的信息系统^[1,2]。大量数据由嵌入式传感器收集, 通过车与车 (V2V, vehicle to vehicle) 或车与基础设施 (V2I, vehicle to infrastructure) 通信实现相邻车辆以及路边单元 (RSU, road side unit) 实时交换交通安全消息, 提高道路交通的效率和增强安全性。大量数据的处理和共享可能超出单个车辆的计算和存储能力, 任务外包是有效的解决方案。但是, 车载网数据具有较强的时空有效性 (即局部有效性、局部兴趣和短的生存期), 只在特定的时间和特定的范围内有效, 传统的集中式云计算^[3,4]模式会造成高的时延和成本。车云计算 (VCC, vehicular cloud computing)^[5-7]充分利用车辆和路边基础设施的存储、通信和计算能力, 实现数据本地化处理, 局部区域内的车辆和传感器生成的数据 (速度、位置、道路状况、事故报告等) 在附近存储, 并在其生命周期内由邻近车辆处理和消耗, 保证车辆决策的实时性和有效性, 实现智能交通管理。

VCC 由 Olariu 等^[8]学者率先提出, 其总体思想是车辆自主地将多余的计算与存储资源集合起来构成临时云, 为经过授权的车辆用户提供低成本的计算和存储资源, 以确保实时服务, 实现智能交通系统、智能电网等。VCC 和传统的云计算结合是主要的 VCC 架构^[9-13]。文献[9-11]使用三层云结构: 车辆形成的云、路边基础设施形成的云和传统的云计算中心。云计算中心有足够的云资源, 但是端到端的通信时延较高, 与之相反, 路边基础设施云和车辆形成的云的云资源有限, 但是通信时延较低。因此, 云计算中心适合非实时性的大容量数据存储和高速计算。相比车辆形成的云, 路边 (或路边基础设施) 云利用路边固定基础设施或静止车辆提供服务, 更为稳定, 覆盖范围更大, 适合于提供稳定实时的公共服务, 车辆形成的云具有高度动态性和短的生命周期, 比较适合高时效性的临时任务。该架构需要高效的云资源管理策略, 实现 3 个层次的云资源的有效配置和整体最优^[12]。

车载网中的实体在进行无线通信时, 其实体可能会受到各种类型的攻击, 如拒绝服务 (DoS) 攻击、重放攻击、女巫攻击等。因此, 车载网通

信过程中需要保证不可否认性、隐私性（即匿名性和不可链接性）和可追踪性。而车载云环境不仅需要满足车载网通信的安全需求，还要保证高移动性车辆的身份认证以及由于车辆动态加入和离开导致参与者之间建立信任的复杂性等。针对车载云的安全和隐私问题，有很多相关研究^[14-24]。

文献[14-16]中使用的 VCC 架构是利用传统的云计算中心。文献[14]提出了一个安全的令牌奖励系统，以鼓励车辆共享它们的资源，该方案中车辆通过 RSU 向云服务提供商管理器贡献自己的资源，以此来获得奖励代币。当车辆需要使用云服务时，向云服务提供商管理器请求服务。尽管考虑了车辆的隐私问题以及车辆之间交换消息的完整性和真实性，但是并没有给出具体的方案。随后在文献[15]中给出了具体的方案，使用数字签名和公钥加密来确保消息的完整性和真实性，使用假名机制保护了车辆的身份隐私。文献[16]提出一种新的面向多云环境的车载网络架构，由可信权威管理的云代理选择合适的云服务提供商，实现了车辆与多个云服务提供商之间快速高效的认证，减轻了车辆与云服务提供商密钥托管的负担。该方案实现了匿名性、可追踪性、不可链接性以及密钥的前向安全性，并且能够抵抗重放攻击和假冒攻击。该方案是对车辆使用传统云进行扩展的多个云服务提供商环境下的车载网认证方案，其根本还是利用传统的集中式云计算来解决单一车辆资源有限的问题。

文献[17-20]中使用的 VCC 架构是路边云，利用 RSU 或静止车辆提供服务。文献[17]提出了一种安全的数据转发方案，车载云是由停车场内的空闲车辆自主形成的。方案利用 (t, n) 门限信用奖励机制有效促进了贡献资源意愿低的车辆间的协作，同时保护了车辆用户个人隐私，可以抵抗车辆泄露攻击和共谋攻击。但是方案中需要 RSU 是完全可信的，对 RSU 的安全性要求过高。文献[18]中提出了一种安全且保护车辆隐私的方案，该方案中任务管理器负责选择一个领导车辆，由领导车辆发布任务并分配任务给周边车辆。利用群签名技术实现了领导车辆和潜在成员之间有条件的隐私保护认证，并且服务器可以根据车辆的签名来揭示其身份。文献[19]利用基于身份的签密和

短群签名方案设计了一种车载云的安全认证和隐私保护机制。该方案中，任务管理器通过发布资源获取任务来招募动态移动的车载资源，RSU 负责将任务管理器需要传递的消息传递给车辆。这些方案中任务管理器如何选择一个领导车辆是需要解决的问题，同时领导车辆需要发布任务、分配任务并在任务完成后汇总结果，容易产生单点故障问题。文献[20]提出了一种分布式 VCC 系统，这些 VCC 是由停车场中的空闲车辆组成的，然后通过一个管理器来管理这些 VCC。该方案利用基于密文策略的属性加密提出了一种安全有效的访问控制架构，并且引入区块链来减少可信机构和每个 VCC 之间的通信成本。但是车辆和 VCC 之间的传输时延较高，并且没有考虑到属性动态变化的情况。

文献[21,22]中使用的 VCC 架构是车辆自组织形成的车载云。文献[21]首次提出了 VCC 的建立和数据传播的方案，并且实现了条件隐私保护，该方案中的实体只有可信权威和车辆。在 VCC 形成过程中，不需要 RSU 的帮助，也不需要任务管理器选择领导车辆，利用群密钥协商协议实现了车辆之间的相互认证并形成 VCC，同时该方案允许车辆动态地加入和离开。然而方案中涉及大量映射到点的哈希运算，且在生成群密钥时涉及过多的双线性对运算，计算成本较大。文献[22]中提出了一种在给定的道路交叉口车辆形成 VCC 的架构，这种架构要求路口的车辆数量达到某个阈值，才能形成一个可用的 VCC，在车辆较少的情况下，该方案的实现较困难，并且方案中没有涉及车辆的隐私保护，不能抵抗一系列的攻击。

软件定义网络（SDN, software defined networking）被用来解决 VCC 中的资源管理问题，利用 SDN 中控制层可以掌握全局网络信息的优势，可以更好地管理 VCC 中的资源分配。文献[23]提出了一种基于 SDN 的 RSU 云，由 RSU 和专用的微型数据中心组成，RSU 云负责托管服务，满足车辆的需求，利用 SDN 的灵活性提高 VCC 中的资源利用率。文献[24]利用 SDN 来增强 VCC 中管理的灵活性，集中控制器负责管理车辆资源的全局信息，并利用这些信息实现了一种最优的资源调度策略；利用 SDN 扩展假名管理的灵活

性，以分层的方式快速调度和管理假名，提高假名资源的利用率，并通过提高车辆的熵有效提高车辆的位置隐私性，但是 SDN 通常需要一个控制器来集中管理资源，以提高资源的利用率，集中管理对用户的隐私保护带来威胁，同时更容易产生单点故障问题。

与传统具有固定的云服务供应商和基础设施的云计算不同，车辆高速移动且由车主自主确定是否贡献资源参与云计算，因此，车载云具有高度的动态性和自组织性，这给车载云的管理带来挑战。与传统的车载网安全一样，在整个车载云计算过程中，都需要保护车辆的身份和位置隐私，但车载网的主要任务是安全交互交通信息并验证消息的完整性和真实性，多为群体验证，不需要提前建立信任，所以具有不可链接的假名机制能较好地实现匿名认证和隐私保护^[25-29]。在 VCC 情景中，不仅需要安全机制在参与云计算的车辆之间建立基本的信任关系，形成车载云的基本服务团体，而且需要进行实时的成员动态管理和云服务的提供与获取管理。传统的车载网的认证和隐私保护机制难以直接应用于 VCC 环境。安全和隐私保护的管理机制是确保 VCC 有效的基础。

本文使用车辆自组织形成车载云的架构，在文献[30]的基础上使用假名技术实现了条件隐私保护，在群加密密钥生成阶段只使用一次双线性对运算，与文献[30]相比实现了更高的效率；基于此非对称群密钥协商协议和一个支持批量验证的轻量级签名构建具有隐私保护的动态高效车载云管理方案，保证了车辆身份匿名和车载云通信的安全性。在随机预言机模型下，基于 ICDH 问题困难性假设，证明了本文方案满足选择明文安全。通过与其他方案的性能分析对比显示，本文方案有更高的通信成本和计算成本，满足动态车载云的高时效性要求。

1 系统模型和安全模型

1.1 系统模型

本文方案的系统模型如图 1 所示，主要包含以下实体。

1) 可信权威 (TA, trusted authority): TA 是一个被广泛认可的、安全可靠的实体，负责生成

系统的公共参数和车辆的登记注册。它是唯一可以追踪车辆真实身份的实体。

2) 车辆：每个车辆都配有一个车载单元 (OBU, on board unit) 和一个安全的防篡改设备 (TPD, tamper proof device)。OBU 具有计算、存储和通信资源，TPD 负责存储安全参数，生成伪身份。每次车载云形成过程中有一个车辆担任云管理员。

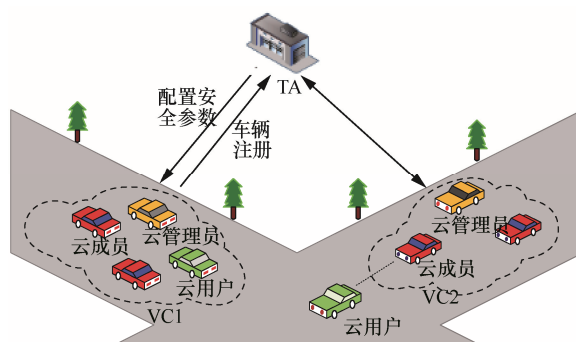


图 1 系统模型
Figure 1 The system model

1.2 安全模型

1.2.1 无证书可认证非对称群密钥协商的安全模型

本文提出的群密钥协商协议利用了文献[31]给出的无证书可认证非对称密钥协商 (CL-AAGKA) 安全模型进行安全证明。

(1) 参与者和符号说明

假设 $U = (u_1, u_2, \dots, u_n)$ 是一组参与群密钥协商的用户，定义参与者的一个实例为 $\Pi_{u_i}^\pi = (\text{Pid}_{u_i}^\pi, \text{sid}_{u_i}^\pi, \text{ms}_{u_i}^\pi, \text{ek}_{u_i}^\pi, \text{dk}_{u_i}^\pi, N_{j,i}, \text{state}_{u_i}^\pi)$ ，其中各参数的意义如表 1 所示。

表 1 参与者 u_i 有关的变量符号
Table 1 The variable symbol associated with actor u_i

符号	符号说明
$\Pi_{u_i}^\pi$	参与者 u_i 的一个实例
$\text{pid}_{u_i}^\pi$	与 u_i 一起参与协议的参与者实例的身份信息集合
$\text{sid}_{u_i}^\pi$	与 u_i 一起参与协议的参与者实例的会话身份信息
$\text{ms}_{u_i}^\pi$	$\Pi_{u_i}^\pi$ 在执行协议时发送和接收的消息集合
$\text{ek}_{u_i}^\pi$	实例 $\Pi_{u_i}^\pi$ 中的加密密钥
$\text{dk}_{u_i}^\pi$	实例 $\Pi_{u_i}^\pi$ 中的解密密钥
$N_{j,i}$	实例 $\Pi_{u_i}^\pi$ 中的密钥因子
$\text{state}_{u_i}^\pi$	实例 $\Pi_{u_i}^\pi$ 当前的内部状态

如果完成接收和发送消息, 则实例 $\Pi_{u_i}^\pi$ 终止, 如果一个实例 $\Pi_{u_i}^\pi$ 被 CL-AAGKA 方案接受, 则这个实例同时有了 $ek_{u_i}^\pi (\neq \text{null})$ 、 $dk_{u_i}^\pi (\neq \text{null})$, $pid_{u_i}^\pi$ 、 $sid_{u_i}^\pi$ 。

定义 1 (合作): 定义实例 $\Pi_{u_i}^\pi$ 和实例 $\Pi_{u_j}^\pi (i \neq j)$ 是合作的关系, 当且仅当满足如下 3 点:

- ① 它们都被方案接受; ② $pid_{u_i}^\pi = pid_{u_j}^\pi$; ③ $sid_{u_i}^\pi = sid_{u_j}^\pi$ 。

(2) 攻击者模型

本文只考虑被动攻击者, 可以替换任何用户的公钥。CL-AAGKA 方案的安全模型被定义为在挑战者 C 和攻击者 A 之间进行的三阶段游戏, 描述如下。

初始化: 挑战者 C 选择安全参数 λ , 进行系统初始化操作, 生成系统公共参数, 然后将系统公共参数发送给攻击者。

攻击过程: 攻击者 A 通过挑战者 C 访问预言机。

Send($\Pi_{u_i}^\pi, \Lambda$): 发送一个消息 Λ 给实例 $\Pi_{u_i}^\pi$, 通过这个实例的输出生成回复。如果 Λ 是不正确的, 则回复 null 。当 $\Lambda = (\text{sid}, \text{pid})$ 时, 则认为是正确的, 生成如表 2 所示的回复。

表 2 回复消息的符号说明

Table 2 The symbol description of reply message

符号	符号说明
$SK(u_i)$	输出参与者 u_i 的私钥
$PK(u_i)$	输出参与者 u_i 的公钥
$\text{Replace}(u_i, P_i')$	把参与者 u_i 的公钥替换为 P_i'
$\text{KF.Reveal}(\Pi_{u_i}^\pi)$	输出密钥因子 $N_{j,i}$
$\text{EK.Reveal}(\Pi_{u_i}^\pi)$	输出加密密钥 $ek_{u_i}^\pi$
$\text{DK.Reveal}(\Pi_{u_i}^\pi)$	输出解密密钥 $dk_{u_i}^\pi$

Test($\Pi_{u_i}^\pi$): A 返回两个消息 (message_0 , message_1) ($|\text{message}_0| = |\text{message}_1|$) 和一个新鲜的实例 $\Pi_{u_i}^\pi$ 。挑战者 C 随机选择 $b \in \{0, 1\}$, 生成用 $ek_{u_i}^\pi$ 加密 message_b 的密文 c 返回给攻击者 A。

猜测: 攻击者 A 提交猜测 $b' \in \{0, 1\}$, 如果 $b = b'$, 则称攻击者 A 赢得游戏。

A 的优势定义为 $\text{Adv}(\Lambda) = |2P_i[b = b'] - 1|$ 。

定义 2 (新鲜性): 如果在攻击者 A 回答 Test

预言机前, 实例 $\Pi_{u_i}^\pi$ 和它的合作实例都没有收到 $\text{DK.Reveal}(\Pi_{u_i}^\pi)$ 询问, 则实例 $\Pi_{u_i}^\pi$ 是新鲜的。

定义 3 (CL-AAGKA 的安全性): 上述模型中, 如果攻击者 A 在多项式时间内赢得游戏的优势 $\text{Adv}(\Lambda) = |2P_i[b = b'] - 1|$ 是可忽略的, 则 CL-AAGKA 方案满足选择明文安全性。

1.2.2 安全需求

1) 有条件的隐私保护: 参与 VCC 的车辆, 用户的身份和位置隐私应当受到保护。包括身份匿名和不可链接性, 即攻击者无法判断一个车辆是否参与多个 VCC, 从而保证车辆的位置隐私。但是, 车载云中可能存在恶意车辆 (如向云用户发送虚假信息), 一旦车辆出现不当的行为, TA 应该能够揭露车辆的真实身份。

2) 基本的安全通信保障, 如消息源认证、消息完整性和消息保密性等。

3) 前向安全性: 前向安全是指车辆新加入车载云, 新加入的车辆不能获知车载云以前的密钥。

2 本文方案

本文提出的方案主要由 6 个部分组成: 系统初始化、车载系统初始化、车载云密钥协商、车载云服务、车载云动态管理和身份追踪。

2.1 系统初始化

输入一个安全参数 λ , TA 执行如下步骤。

(1) 选择具有素数阶 q 的加法循环群 G_1 和乘法循环群 G_2 , 使得离散对数是困难的。 P 是 G_1 的生成元。在这两个群上定义如下双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 。

(2) 选取哈希函数: $H_1, H_2, H_3, H_4: \{0, 1\}^* \rightarrow Z_q^*$ 。

(3) 选择随机数 $s \in Z_q^*$ 作为系统私钥, $PK_{\text{pub}} = s \cdot P$ 作为系统公钥。

2.2 车载系统初始化

2.2.1 车辆注册

每个合法车辆必须向 TA 完成注册, 注册过程中, TA 通过安全的信道给车辆分配一个唯一的 $ID \in Z_q^*$, 并且预先加载 $\{ID, PWD, s\}$ 到车辆的防篡改设备 TPD 中。其中, PWD 是车辆登录 TPD 的口令。当系统私钥 s 更新后, TPD 需要重新加载。

2.2.2 车辆假名和密钥生成

为保护车辆用户的身份和位置隐私, 通信时

由车辆的 TPD 生成车辆的假名及其对应的公私钥对，具体步骤如下。

1) 车辆 u_i 输入真实身份 ID_{u_i} 和 PWD_{u_i} 登录 TPD，登录成功后，TPD 选择一个随机数 $\omega_i \in Z_q^*$ ，计算车辆 u_i 的假名 $PID_{u_i} = (PID_{u_i,1}, PID_{u_i,2})$ ，其中 $PID_{u_i,1} = \omega_i \cdot P \in G_1$ ， $PID_{u_i,2} = ID_{u_i} \oplus H_1(\omega_i PK_{pub}) \in Z_q^*$ 。

2) TPD 根据车辆 u_i 的假名和系统私钥 s 计算 u_i 的假名对应的公私钥。首先计算 $\alpha_i = H_2(PID_{u_i})$ ，然后计算 $SK_{PID_{u_i}} = (\omega_i + \alpha_i \cdot s) \bmod q \in Z_q^*$ ， $PK_{PID_{u_i}} = SK_{PID_{u_i}} \cdot P \in G_1$ ，TPD 将 $\{PID_{u_i}, SK_{PID_{u_i}}, PK_{PID_{u_i}}\}$ 发送给车辆。

2.2.3 消息签名方案

为了验证消息源和消息的完整性，VCC 中的车辆 u_i 在发送消息 M_i 时，发送的内容为 $\{M_i, PID_{u_i}, PK_{PID_{u_i}}, \tau_i\}$ ，其中 τ_i 是对发送的所有消息内容的签名。签名方案参考文献[32]中的方案，利用 Schnorr 算法构建了一个轻量级的安全的认证方法，无须双线性对运算，降低了运算时间，同时提供了批量验证签名方法。具体的签名和验证过程如下。

(1) 消息签名

选择一个随机数，计算 $R_i = r_i \cdot P \in G_1$ 和消息 M_i 的摘要 $\beta_i = H_3(M_i, PID_{u_i}, PK_{PID_{u_i}}, R_i)$ ，然后计算 $\sigma_i = (SK_{PID_{u_i}} + \beta_i \cdot r_i) \bmod q$ ，得到消息 M_i 的签名为 $\tau_i = \{R_i, \sigma_i\}$ 。签名者会公开信息 $\{M_i, PID_{u_i}, PK_{PID_{u_i}}, \tau_i\}$ ，便于接收者进行验证。

(2) 消息验证

① 单一验证

消息接收者接收到消息 $\{M_i, PID_{u_i}, PK_{PID_{u_i}}, \tau_i\}$ 后，计算 $\beta_i = H_3(M_i, PID_{u_i}, PK_{PID_{u_i}}, R_i)$ ，然后验证等式 $\sigma_i \cdot P = PK_{PID_{u_i}} + \beta_i \cdot R_i$ ，确定签名是否有效。

② 批量验证

假设消息接收者收到需要验证的 n 个不同消息 $\{M_1, PID_{u_1}, PK_{PID_{u_1}}, \tau_1\} \{M_2, PID_{u_2}, PK_{PID_{u_2}}, \tau_2\} \dots \{M_n, PID_{u_n}, PK_{PID_{u_n}}, \tau_n\}$ ，统一计算式(1)中各项，判断等式是否成立，同时验证这 n 个签名是否有效。

$$\left(\sum_{i=1}^n \sigma_i \right) \cdot P = \sum_{i=1}^n PK_{PID_{u_i}} + \left(\sum_{i=1}^n \beta_i \cdot R_i \right) \quad (1)$$

2.3 车载云密钥协商

本文改进了文献[30]的群密钥协商协议，使用假名技术实现了车辆的身份隐私保护，并在群加密密钥生成阶段只使用一次双线性对运算，实现了更高的效率，满足车载云的高时效性要求。

假设车辆 u_m 为车载云的发起者，密钥协商过程如图2所示，包括如下步骤。

1) u_m 对构建车载云的请求消息 M_m (请求消息中包含该云所需的资源种类、数量等描述) 用 2.2.3 节签名方案进行签名，然后广播 $\{M_m, PID_{u_m}, PK_{PID_{u_m}}, \tau_m\}$ 给周边车辆。

2) 有意愿参与 VCC 的周边车辆 u_x 收到消息

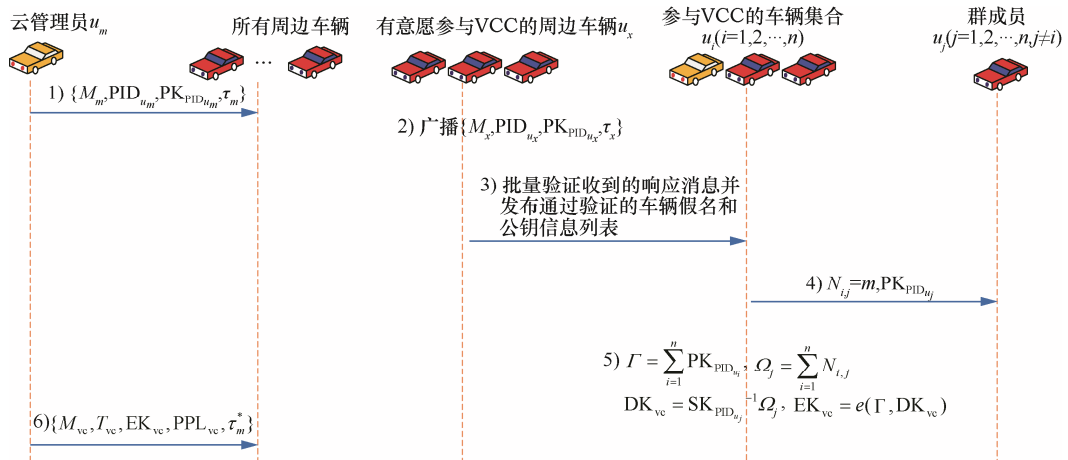


图2 车载云密钥协商过程

Figure 2 Process of vehicular cloud key agreement

$\{M_m, \text{PID}_{u_m}, \text{PK}_{\text{PID}_{u_m}}, \tau_m\}$ 后, 验证消息并生成响应消息 M_x (响应消息包括愿意提供的资源种类和数量等), 签名后广播 $\{M_x, \text{PID}_{u_x}, \text{PK}_{\text{PID}_{u_x}}, \tau_x\}$ 给其他周边车辆。

3) 周边的每一个有意愿参与 VCC 的车辆可以批量验证收到的响应消息并发布通过验证的车辆假名和公钥信息列表, 所有列表的交集为参与 VCC 的车辆集合, 设为 $\{u_i, i=1, 2, \dots, n\}$, 其中 u_m 为管理员。

4) $u_i (i=1, 2, \dots, n)$ 选择一个随机数 $m_i \in Z_q^*$, 计算 $N_{i,j} = m_i \cdot \text{PK}_{\text{PID}_{u_j}}$, 然后发送 $N_{i,j} (j=1, 2, \dots, n, j \neq i)$ 给群中成员 u_j 。

5) 群成员 u_j 收到其他成员发送给自己的 $\{N_{1,j}, \dots, N_{j-1,j}, N_{j+1,j}, \dots, N_{n,j}\}$ 后, 计算 $\Gamma = \sum_{i=1}^n \text{PK}_{\text{PID}_{u_i}}$, $\Omega_j = \sum_{i=1}^n N_{i,j}$, 然后计算群解密密钥 $\text{DK}_{\text{vc}} = \text{SK}_{\text{PID}_{u_j}}^{-1} \Omega_j$ 和群加密密钥 $\text{EK}_{\text{vc}} = e(\Gamma, \text{DK}_{\text{vc}})$, 其中, 群解密密钥由云成员安全保存, 群加密密钥由群管理员 u_m 广播出去。

6) 云管理员 u_m 生成一个云描述信息 $\{M_{\text{vc}}, T_{\text{vc}}, \text{EK}_{\text{vc}}, \text{PPL}_{\text{vc}}, \tau_m^*\}$ 并广播给周边车辆, 其中 M_{vc} 包括该车载云能够提供的资源集合, PPL_{vc} 是车载云中提供服务的所有车辆 $u_i (i=1, 2, \dots, n)$ 的假名和公钥对列表, 即 $\text{PPL}_{\text{vc}} = \{(\text{PID}_{u_i}, \text{PK}_{\text{PID}_{u_i}}) | i=1, \dots, n\}$ 。 T_{vc} 是时间戳, 指车载云开始提供服务的时间, τ_m^* 是对 $\beta_{\text{vc}} = H_3(M_{\text{vc}}, T_{\text{vc}}, \text{EK}_{\text{vc}}, \text{PPL}_{\text{vc}})$ 的签名, 签名算法和 2.2.3 中的方案一致。

2.4 车载云服务

假设车辆 u_{user} 想请求云服务, 且服务需求为 $M_{\text{user}} \in Z_q^*$, 其选择随机数 $t \in Z_q^*$, 然后计算 $U = t \sum_{i=1}^n \text{PK}_{\text{PID}_{u_i}} = t \cdot \Gamma$, $V = M_{\text{user}} \oplus H_4(\text{EK}_{\text{vc}}')$ 得到密文 (U, V) 。 u_{user} 广播 $\{(U, V), \text{PID}_{u_{\text{user}}}, \text{PK}_{\text{PID}_{u_{\text{user}}}}, \tau_{\text{user}}\}$ 给车载云成员。

车载云成员 $u_j (1 \leq j \leq n)$ 收到消息后, 验证消息的签名, 通过后, 用群解密密钥解密密文

(U, V) 得到消息 M_{user} 。解密过程为 $M_{\text{user}} = V \oplus H_4(e(U, \text{DK}_{\text{vc}}))$ 。

2.5 车载云动态管理

2.5.1 车辆加入

假设新成员 u_{join} 想要加入车载云作为云成员, 群密钥更新步骤如下。

1) u_{join} 选择一个随机数 $m_{\text{join}} \in Z_q^*$, 并计算 $N_{\text{join},j} = m_{\text{join}} \cdot \text{PK}_{\text{PID}_{u_j}} (j=1, 2, \dots, n)$, 然后广播 $\{M_{\text{join}}, \text{PID}_{u_{\text{join}}}, \text{PK}_{\text{PID}_{u_{\text{join}}}}, N_{\text{join},j}, \tau_{\text{join}}\}$ 给所有的云成员, 其中 τ_{join} 是对整个消息的签名。

2) 云管理员 u_m 可以验证接收到的消息, 验证成功后, u_m 选择一个随机数 $m'_m \in Z_q^*$, 并计算 $N'_{m,j} = m'_m \text{PK}_{\text{PID}_{u_j}}$, 然后发送 $N'_{m,j} (j=1, 2, \dots, n, j \neq m)$ 给车载云中成员 u_j , 并声明有一个新成员加入。

3) 群成员 u_j 收到云管理员发给自己的 $N'_{m,j}$ 后, 计算 $\delta'_j = \text{SK}_{\text{PID}_{u_j}}^{-1} N'_{m,j}$, $\theta_j = \delta'_j + \text{DK}_{\text{vc}}$ 。

4) u_m 选择一个随机数 $\lambda \in Z_q^*$, 计算 $\theta_m = \text{SK}_{\text{PID}_{u_m}}^{-1} N'_{m,m} + \text{DK}_{\text{vc}}$, $\chi_m = \theta_m + \lambda \cdot P$, $\mu_m = \lambda \text{PK}_{\text{PID}_{u_{\text{join}}}}$, 然后发送 (χ_m, μ_m) 给新成员 u_{join} 。

5) 原云成员计算新的群解密密钥 $\text{DK}'_{\text{vc}} = \theta_j + \text{SK}_{\text{PID}_{u_j}}^{-1} N_{\text{join},j}$ 。新加入的成员 u_{join} 计算 $S_{u_{\text{join}}} = \text{SK}_{\text{PID}_{u_{\text{join}}}}^{-1} \cdot \mu_m$, 然后计算群解密密钥 $\text{DK}'_{\text{vc}} = \chi_m - S_{u_{\text{join}}} + m_{\text{join}} \cdot P$ 。

6) 原云成员和新加入的成员 u_{join} 计算 $\Gamma' = \Gamma + \text{PK}_{\text{PID}_{u_{\text{join}}}}$, 然后计算群加密密钥 $\text{EK}'_{\text{vc}} = e(\Gamma', \text{DK}'_{\text{vc}})$ 。

2.5.2 车辆离开

假设车载云中成员 u_{leave} 想要离开, 群密钥更新步骤如下。

1) u_{leave} 通过群加密密钥 EK_{vc} 加密消息 Leave 发送给群成员, Leave 消息中包含 u_{leave} 声明离开 VCC 的消息。

2) 群管理员 u_m 通过群解密密钥 DK_{vc} 解密得到消息 Leave 后, 选择一个随机数 $m''_m \in Z_q^*$, 计算 $N''_{m,j} = m''_m \text{PK}_{\text{PID}_{u_j}} (j=0, 1, \dots, n, j \neq \text{leave})$, 然后

发送 $N_{m,j}''$ 给对应的成员 u_j ，并声明更新群密钥。

3) 群成员 u_j 收到 u_m 和 u_{leave} 发送的消息后，计算 $\Omega_j'' = \Omega_j - N_{\text{leave},j}$ ， $\Gamma'' = \Gamma - \text{PK}_{\text{PID}_{u_{\text{leave}}}}$ ，然后计算群解密密钥 $\text{DK}_{\text{vc}}'' = \text{SK}_{\text{PID}_{u_j}}^{-1}(\Omega_j'' + N_{m,j}'')$ 和群加密密钥 $\text{EK}_{\text{vc}}'' = e(\Gamma'', \text{DK}_{\text{vc}}'')$ 。

2.6 身份追踪

如果检测到车辆的恶意行为，TA 可以根据车辆的假名追踪到车辆的真实身份。

假设车辆的一次性使用假名为 $\text{PID}_{u_i} = (\text{PID}_{u_i,1}, \text{PID}_{u_i,2})$ ，TA 可以利用系统私钥 s 和车辆的假名 PID_{u_i} 计算出车辆的真实身份 $\text{ID}_{u_i} = \text{PID}_{u_i,2} \oplus H_1(s \cdot \text{PID}_{u_i,1})$ 。

2.7 方案安全性证明

根据 1.2.1 节定义的安全模型证明本文的群密钥协商协议的安全性。

定理 在随机预言机模型下，假设攻击者 A 可以以一定的优势攻破群密钥协商协议，则可以构造一个算法以一定的优势解决 ICDH 问题。

证明 假设存在一个多项式时间的攻击者 A 能够以不可忽略的概率攻破系统，这意味着挑战者 C 可以通过攻击者 A 的查询以不可忽略的概率解决 ICDH 问题。

对于 ICDH 问题的实例 $(G_1, G_2, q, P, aP, abP)$ ，挑战者 C 的任务是计算出 b 的值。

初始化：挑战者 C 首先设置安全参数 λ ，然后选择 $s \in Z_q^*$ ，并计算 $\text{PK}_{\text{pub}} = s \cdot P$ ；接着将系统公共参数 $\text{params} = \{G_1, G_2, q, P, e, \text{PK}_{\text{pub}}, H_1, H_2, H_3, H_4\}$ 发送给攻击者 A。

攻击过程：C 作为挑战者来回答攻击者 A 的询问。

H_2 预言机模拟：列表 L_{H_2} 的格式是 $(\text{PID}_{u_i}, \alpha_i)$ ，当 A 对 H_2 进行询问时，C 先查询列表中是否存在相同的值 PID_{u_i} ，如果存在，则回复对应的 α_i 给 A；如果不存在，则选择随机值 $\alpha_i \in Z_q^*$ 。最后 C 把 α_i 返回给 A，并把 $(\text{PID}_{u_i}, \alpha_i)$ 加入列表 L_{H_2} 。

H_3 预言机模拟：列表 L_{H_3} 的格式是 $(M_i, \text{PID}_{u_i}, \text{PK}_{\text{PID}_{u_i}}, R_i, \beta_i)$ ，当 A 对 H_3 进行询问时，C 先查询列表中是否存在相同的值

$(M_i, \text{PID}_{u_i}, \text{PK}_{\text{PID}_{u_i}}, R_i)$ ，如果存在，则回复对应的 β_i 给 A；如果不存在，则选择随机值 $\beta_i \in Z_q^*$ 。最后 C 把 β_i 返回给 A，并把 $(M_i, \text{PID}_{u_i}, \text{PK}_{\text{PID}_{u_i}}, R_i, \beta_i)$ 加入列表 L_{H_3} 。

私钥查询：挑战者 C 维护一个形如 $(\text{PID}_{u_i}, \text{SK}_{\text{PID}_{u_i}}, \text{PK}_{\text{PID}_{u_i}}, \omega_i)$ 的列表 L_1 ，初始化为空。当收到攻击者 A 关于私钥的查询时，挑战者 C 首先检查列表 L_1 中是否存在相同的值 PID_{u_i} ，如果已经存在，挑战者返回 $\text{SK}_{\text{PID}_{u_i}}$ 给攻击者 A；如果不存在则 C 查询列表 L_{H_2} 中是否存在相同的值 PID_{u_i} ，如果不存在，则先进行 H_2 询问，得到 α_i ，如果存在，则直接计算 $\text{SK}_{\text{PID}_{u_i}} = (\omega_i + \alpha_i \cdot s) \bmod q \in Z_q^*$ ， $\text{PK}_{\text{PID}_{u_i}} = \text{SK}_{\text{PID}_{u_i}} \cdot P \in G_1$ 。最后将 $\text{SK}_{\text{PID}_{u_i}}$ 返回给 A，并更新列表。

公钥查询：当 A 对 PID_{u_i} 的公钥进行询问时，C 先查询列表 L_1 中是否存在相同的值 PID_{u_i} ，如果存在，则把对应的 $\text{PK}_{\text{PID}_{u_i}}$ 发送给 A；如果不存在，则 C 进行一次私钥查询。

公钥替换询问：当 A 用 (PID_{u_i}, P'_i) 对 C 进行公钥替换询问时，先查询列表中是否存在相同的值 PID_{u_i} ，若没有，则进行公钥询问。最后，C 返回 P'_i 给 A，并更新列表。

方案执行：C 创建一个空的列表 L_2 ，方案的用户集合是 $U = (u_1, u_2, \dots, u_n)$ ，用 PID_{u_i} 进行公钥查询得到 $\text{PK}_{\text{PID}_{u_i}}$ 。

① 选择随机数 $m_j \in Z_q^*$ ，对于 $(1 \leq j \leq n)$ 计算 $N_{j,i} = m_j \cdot \text{PK}_{\text{PID}_{u_i}} \in G_1$ ；

② 把 $(\text{PID}_{u_i}, m_j, N_{i,i})$ 加入列表 L_2 ，广播消息 $(\text{PID}_{u_i}, \text{PK}_{\text{PID}_{u_i}}, N_{1,i}, N_{2,i}, \dots, N_{n,i} (i \neq j))$ 。

群解密密钥查询：A 用一个实例 $\Pi_{u_i}^\pi$ 来进行群解密密钥查询，挑战者 C 从列表 L_1 获得 $\text{SK}_{\text{PID}_{u_i}}$ ，从列表 L_2 获得 $N_{i,i}$ ，计算密钥参数 $\Omega_i = \sum_{j=1}^n N_{j,i}$ ，然后计算群解密密钥 $\text{DK}_{\text{vc}} = \text{SK}_{\text{PID}_{u_i}}^{-1} \Omega_i$ ，返回 DK_{vc} 给攻击者 A。

群加密密钥查询：A 用一个实例 $\Pi_{u_i}^\pi$ 来进行

群加密密钥询问, 挑战者 C 从列表 L_1 获得 $SK_{PID_{u_i}}$, 从列表 L_2 获得 $N_{i,i}$, 计算密钥参数 $\Omega_i = \sum_{j=1}^n N_{j,i}$, $DK_{vc} = SK_{PID_{u_i}}^{-1} \Omega_i$, 然后计算群加密密钥 $EK_{vc} = e(\Gamma, DK_{vc})$, 返回 EK_{vc} 给 A。

测试: A 返回给 C 两个消息 ($message_0, message_1$) ($|message_0| = |message_1|$) 和一个新鲜的实例 $\Pi_{u_i}^*$, 此实例中合作者集合为 $U^* = (u_1^*, u_2^*, \dots, u_m^*)$ 。挑战者 C 在列表 L_1 中搜索用户的相关公私钥信息, 并进行群加密密钥查询, 得到群加密密钥 EK_{vc}^* , 选择 $t^* \in Z_q^*$, 计算 $U^* = t^* \sum_{i=1}^n PK_{PID_{u_i}}$, $V^* = message_b \oplus H_4(EK_{vc}^*, t^*)$, 其中 $b \in \{0, 1\}$, 返回密文 $c^* = \langle U^*, V^* \rangle$ 给攻击者 A。

猜测阶段: 攻击者 A 返回一个比特值 b' , 如果有 $b' = b$, 则认为 A 攻击成功。

通过上面的分析可知, 如果 A 攻击成功, 则意味着攻击者 A 可以从列表 L_2 获取 $N_{i,i}$, 并计算出 $\Omega_i = \sum_{j=1}^n N_{j,i}$, $DK_{vc} = SK_{PID_{u_i}}^{-1} \Omega_i$, 攻击者 A 有优势获得 $message_b = V^* \oplus H_5(e(U^*, DK_{vc}))$ 。根据攻击者 A 的方法, 挑战者 C 可以解决 ICDH 问题。因为设置 $abP = \Omega_i = SK_{PID_{u_i}} \cdot \sum_{j=1}^n m_j \cdot P$, $aP = PK_{PID_{u_i}} = SK_{PID_{u_i}} \cdot P$, 根据 (P, aP, abP) , $DK_{vc} = SK_{PID_{u_i}}^{-1} \Omega_i = \sum_{i=1}^n m_i P$, C 可以计算出 $bP = (ab/a)P$ 。

3 性能分析

3.1 安全性能分析

(1) 条件隐私保护

身份匿名: 车辆的真实身份仅包含在假名 $PID_{u_i} = (PID_{u_i,1}, PID_{u_i,2})$ 中, 其中 $PID_{u_i,1} = \omega_i \cdot P \in G_1$, $PID_{u_i,2} = ID_{u_i} \oplus H_1(\omega_i \cdot PK_{pub}) \in Z_q^*$, 且 $PK_{pub} = s \cdot P$ 。攻击者 A 要想知道车辆的真实身份, 必须计算出 $H_1(\omega_i \cdot PK_{pub}) = H_1(\omega_i \cdot s \cdot P)$, 但是在不知道 ω_i 和 s 的情况下, 如果 ECDH 问题是困难的, 任何攻击者在多项式时间内计算出 $\omega_i \cdot s \cdot P$ 是不可能的。

位置隐私: 在本文方案中, 车辆的假名只在一次车载云形成过程中使用, 在使用过一次后被丢弃, 所以任何车辆多次参与车载云的过程不能被链接, 从而保证位置隐私。

合法追踪: 要揭露车辆 u_i 的真实身份时, 除了 u_i 本身, 只有 TA 可以利用系统私钥 s 计算 $s \cdot PID_{u_i,1} = s \cdot \omega_i \cdot P = \omega_i \cdot PK_{pub}$, 得到车辆的真实身份 $ID_{u_i} = PID_{u_i,2} \oplus H_1(\omega_i \cdot PK_{pub})$ 。本文方案可以实现有条件的隐私保护。

(2) 基本的安全通信保障

消息源认证和完整性认证: 车载云计算过程中, 车辆对发送的所有消息都利用 2.2.3 节中介绍的签名方案进行了签名, 文献[32]证明了该签名方案的安全性, 保证了通信消息源的真实性和消息在传输过程中的完整性。

消息保密性: 所有云用户的请求会利用协商的群加密密钥进行加密, 群密钥协商协议的安全证明保证了消息的保密性。

(3) 密钥前向安全

本文方案中允许成员变动, 在车辆加入或离开时, 对群加密密钥和群解密密钥进行了更新, 当有新车辆加入时, 新成员只能解密加入之后收到的消息。因为新加入的车辆 u_{join} 只能收到群管理员 u_m 发送的 (χ_m, μ_m) , 其中 $\chi_m = \theta_m + \lambda \cdot P = m'_m \cdot P + DK_{vc} + \lambda \cdot P$, $\mu_m = \lambda \cdot PK_{PID_{u_{join}}}$ 。 u_{join} 想要计算出 DK_{vc} , 必须要知道整数 λ , 如果 ECDL 问题是困难的, 任何知道 $PK_{PID_{u_{join}}}$ 的攻击者在多项式时间内计算出整数 λ 是不可能的。

(4) 抵抗假冒攻击

车辆使用其真实身份在 TA 处获取 TPD 登录口令, 并且 TPD 是不可被破坏的, 因此攻击者无法生成 PID 对应的私钥。在车载云密钥协商过程中, 攻击者想要冒充合法车辆, 则必须构造合法的签名 $\tau_i = \{R_i, \sigma_i\}$, 满足方程式 $\sigma_i \cdot P = PK_{PID_{u_i}} + \beta_i \cdot R_i$, 以通过其他车辆的认证。根据文献[32]对该签名方案的安全证明可知, 在多项式时间内敌手无法构造有效的签名并通过验证。

3.2 通信和计算成本分析

为了更好地分析本文方案的通信和计算成本, 与文献[21]和文献[33]方案进行对比分析。本

文使用文献[34]中提出的计算评价方案，使用 JPBC 密码库来计算密码学操作在硬件平台上的执行时间，硬件平台包含 8 GB 内存，使用 Intel i5-8265U 处理器，安装的是 Windows10 操作系统。

(1) 通信成本

不同数据类型的大小如表 3 所示，考虑消息交换期间系统中各种数据类型的通信成本，使用这些度量，可以计算出两种方案的通信成本。

表 3 不同数据类型的大小
Table 3 The size of different data types

符号	数据类型	大小/byte
L_{G_1}	群 G_1 中的元素	40
L_{G_2}	群 G_2 中的元素	128
$L_{Z_q^*}$	Z_q^* 中的元素	4
L_{ID}	身份	4
L_{PID}	伪身份	44
L_m	消息	20
L_{TS}	时间戳	4
L_{sig}	一个基于身份的签名	80
L_K	AES-128 的密钥	16
L_H	单向哈希函数	20
L_{sid}	唯一标识	4
$L_{RSA1024}$	RSA1024 密钥长度	128
L_{JT}	加入的令牌	128

文献[21]方案中，在车载云初始化阶段，车辆 u_i 发送的签名为 $\sigma_i = (p_{i,1}, tp_i, a_i, b_i, \{y_{i,j}\})$ ， $j \in \{1, \dots, n\}, j \neq i$ ，云管理员发送的云信息为 $(\sigma, p_{t(n+1)}, E, \Theta, sid, info)$ ， $(a_i, b_i, \{y_{i,j}\}_{j \in \{1, \dots, n\}, j \neq i})$ 是群 G_1 中的元素， $p_{i,1}$ 是车辆 u_i 的假名， tp_i 是时间戳， σ 是采用基于身份的签名对 $(E, \Theta, sid, info)$ 在 $p_{t(n+1)}$ 下的签名， $p_{t(n+1)}$ 是云管理员的假名， (E, Θ) 是群加密密钥， sid 是唯一标识， $info$ 包括车载云的一些信息，可以得到其初始化阶段车辆 u_i 通信成本为 $(n+1)L_{G_1} + 1L_{PID} + 1L_{TS} = (40n+88)$ byte。

云管理员需要公布群成员的假名和公钥列表以及云信息，因此云管理员需要的额外通信成本为 $(n+1)L_{PID} + (n+1)L_{G_1} + L_{sig} + L_{G_2} + L_{sid} = (84n+296)$ byte。密文为 $C = C_1 \parallel C_2$ ，其中 $C_2 = (A_1, A_2, A_3)$ ， A_1, A_2 为

群 G_1 中的元素， A_3 为 AES-128 的密钥大小， C_1 为消息 m 和使用基于身份的签名算法对消息 m 的签名，密文大小为 $2L_{G_1} + 1L_K + 1L_m + 1L_{sig} = 196$ byte。

文献[33]方案中，在构建车载云阶段即本文方案的车载云密钥协商阶段，车辆 u_i 需要发送加入的令牌 JT_i 给 RSU，此令牌是 TA 对车辆注册请求的 RSA 签名，并且需要生成公钥 pk_i 发给 RSU，因此车辆 u_i 需要的通信成本为 $L_{JT} + L_{RSA1024} = 256$ byte。RSU 需要给每个车辆 u_i 颁发参数 $(g_i, p_i, q_i, p_i^{v_j}, q_i^{v_j})$ ，其中 v_j 是 RSU_j 的私钥， g_i, p_i, q_i 的大小等于 RSA1024 算法的密钥长度， p_i, q_i 是 RSA1024 算法中选取的两个素数，通常各取 64 byte，并且 RSU 需要发布组成员的公钥列表以及云信息 (g_j, m_j, u_j, c) ，其中 m_j, u_j 是其公钥， c 是利用组成员公钥计算出来的群密钥，因此 RSU 需要的通信成本为 $(5n+4)L_{RSA1024} = (640n+512)$ byte。该方案中不涉及云管理员角色。

本文方案中，在车载云初始化阶段即车载云密文协商阶段，车辆发送的消息包括 $\{M_m, PID_{u_m}, PK_{PID_{u_m}}, \tau_m\}$ 和车辆 u_i 发送的 $N_{i,j} (j = 1, 2, \dots, n, j \neq i)$ ，得到初始化阶段通信成本为 $(n+1)L_{G_1} + 1L_{PID} + 2L_{Z_q^*} = (40n+108)$ byte。而云管理员需要发布群成员的假名公钥列表以及云信息 $\{M_{vc}, T_{vc}, EK_{vc}, PPL_{vc}, \tau_m^*\}$ ，因此云管理员额外的通信成本为 $(n+1)L_{G_1} + nL_{PID} + L_{Z_q^*} + L_{G_2} + L_{TS} + L_m = (84n+154)$ byte。车载云服务生成的密文为 (U, V) ，其密文通信成本为 $L_{G_1} + L_{Z_q^*} = 44$ byte。

从表 4 可以看出，在车载云密钥协商阶段，车辆 u_i 的通信成本本文方案略高于文献[21]方案，且文献[33]方案远低于本文方案和文献[21]方案，这是因为文献[33]方案中是由 RSU 负责验证车辆身份是否合法以及计算对称群密钥，而本文方案和文献[21]方案的系统模型中不涉及 RSU，车辆的身份验证和非对称群密钥都是由车辆自己来完成的，因此车辆 u_i 的通信成本高于文献[33]方案，而文献[33]方案中 RSU 的通信成本很高，因为其用的是 RSA1024 算法，该算法密钥长度为 1024 bit，成本比较大。本文方案中云管理

表 4 通信成本对比
Table 4 Communication cost comparison

阶段	文献[21]	文献[33]	本文方案
初始化车辆	$(n+1)L_{G_1} + 1L_{PID} + 1L_{TS} =$ (40n+88) byte	$L_{JT} + L_{RSA1024} = 256$ byte	$(n+1)L_{G_1} + 1L_{PID} + 2L_{Z_q^*} =$ (40n+108) byte
初始化云管理员额外成本	$(n+1)L_{PID} + (n+1)L_{G_1} + L_{sig} +$ $L_{G_2} + L_{sid} = (84n+296)$ byte	—	$(n+1)L_{G_1} + nL_{PID} + L_{Z_q^*} + L_{G_2} +$ $L_{TS} + L_m = (84n+154)$ byte
RSU	—	$(5n+4)L_{RSA1024} = (640n+512)$ byte	—
密文	$2L_{G_1} + 1L_K + 1L_m +$ $1L_{sig} = 196$ byte	—	$L_{G_1} + L_{Z_q^*} = 44$ byte

员的通信成本和密文的通信成本均低于文献[21]方案，而文献[33]方案没有云管理员角色，并且只介绍了计算密文时用对称加密算法，尚未给出具体方案，因此文献[33]方案的密文成本是未知的。

(2) 计算成本

表 5 描述了密码算法中基础操作的时间和传输时延的测量，以此来分析各方案的计算成本。密码算法基础操作时间是使用 JPBC 密码库进行测量的。传输时延是使用交通仿真软件 Sumo、基于事件的网络模拟器 Omnet++ 和运行车联网网络仿真的框架 Veins 组合测量出来的。其中，仿真实验中的模拟参数如表 6 所示，仿真实验的时长为 100 s，模拟区域大小为 $2\,500 \times 2\,500 \text{ m}^2$ ，车辆的数据传输功率大小为 6 Mbit/s，车辆数量固定设置为 55 辆，车辆的速度最小设置为 10 m/s，最大设置为 35m/s。

在本文方案中，计算成本主要体现在车载云密钥协商、车辆的加入、加密密钥和解密密钥生成以及加解密阶段，如表 7 所示，在初始化阶段，文献[21]方案的计算成本为 $(n+4)T_{G_1\text{bpm}} + (n+1) \cdot T_{\text{mp}} + 3T_{\text{trans}}^{\text{oo}}$ ，文献[33]方案的计算成本为 $nT_{\text{TokenVer}} + 3nT_{G_1\text{bpm}} + T_{\text{trans}}^{\text{ot}} + 3T_{\text{trans}}^{\text{or}} + T_{\text{trans}}^{\text{rt}}$ ，本文方案在此阶段的计算成本为 $(5n+2)T_{\text{bpa}} + (2n+5)T_{G_1\text{bpm}} + (2n-1)T_h + 3T_{\text{trans}}^{\text{oo}}$ 。如图 3 所示，本文方案在车载云初始化阶段的计算成本低于文献[21]方案和文献[33]方案。文献[21]方案在车辆加入阶段需要的执行时间同初始化操作，本文车辆加入阶段需要的计算成本为 $(n+6)T_{G_1\text{bpm}} + 4T_{\text{bpa}} + 2T_h + 3T_{\text{trans}}^{\text{oo}}$ ，文献[33]方案不支持新车辆加入操作。如图 4 所示，在车辆加入阶

表 5 密码学操作和传输时延的测量
Table 5 Measurement of cryptographic operations and transmission delay

符号	含义	时间/ms
T_{bp}	双线性配对操作	5.627
$T_{G_1\text{bpm}}$	G_1 上的标量乘运算	0.724
$T_{G_2\text{bpm}}$	G_2 上的标量乘运算	0.687
T_{bpa}	点加运算	0.002
T_{mp}	映射到点的哈希运算	1.443
T_h	单向哈希运算	0.011
T_{RSAEnc}	RSA-1024 加密	0.625
T_{RSADec}	RSA-1024 解密	1.69
T_{SigGen}	RSA-1024 签名生成	1.644
T_{SigVer}	RSA-1024 签名验证	0.775
T_{TokenVer}	令牌验证	4.182
$T_{\text{trans}}^{\text{or}}$	车辆和 RSU 之间的通信时延	≤ 15
$T_{\text{trans}}^{\text{ot}}$	车辆和 TA 之间的通信时延	≤ 20
$T_{\text{trans}}^{\text{rt}}$	RSU 和 TA 之间的通信时延	≤ 15
$T_{\text{trans}}^{\text{oo}}$	车辆和车辆之间的通信时延	≤ 15

表 6 仿真实验中的模拟参数
Table 6 Simulation parameters in simulation experiments

参数	值
模拟区域	$2500 \times 2500 \text{ m}^2$
数据传输功率	6 Mbit/s
车辆数量	55
车辆速度	10~35 m/s
MAC 层协议	802.11p
网络层协议	Aodv
仿真时间	100 s

表7 计算成本对比
Table 7 Computational cost comparison

阶段	文献[21]	文献[33]	本文方案
初始化	$(n+4)T_{G_{ibpm}} + (n+1)T_{ntp} + 3T_{trans}^{oo}$	$nT_{TokenVer} + 3nT_{G_{ibpm}} + T_{trans}^{ot} + 3T_{trans}^{or} + T_{trans}^{rt}$	$(5n+2)T_{bpa} + (2n+5)T_{G_{ibpm}} + (2n-1)T_h + 3T_{trans}^{oo}$
加入	$(n+4)T_{G_{ibpm}} + (n+1)T_{ntp} + 3T_{trans}^{oo}$	—	$(n+6)T_{G_{ibpm}} + 4T_{bpa} + 2T_h + 3T_{trans}^{oo}$
加密密钥生成	$2T_{bp} + 1T_{G_{ibpm}} = 11.978 \text{ ms}$	—	$T_{bp} = 5.267 \text{ ms}$
解密密钥生成	$2T_{bp} = 11.254 \text{ ms}$	—	$T_{G_{ibpm}} = 0.724 \text{ ms}$
对称群密钥生成	—	$(n+3)T_{bpa} = (0.002n + 0.006) \text{ ms}$	—
加密	$3T_{G_{ibpm}} = 2.172 \text{ ms}$	—	$T_{G_{ibpm}} + T_{G_{ibpm}} + T_h = 1.422 \text{ ms}$
解密	$2T_{bp} + 1T_{G_{ibpm}} = 11.978 \text{ ms}$	—	$T_{bp} + T_h = 5.638 \text{ ms}$

段的计算成本远低于文献[21]方案。表7表明在其他阶段,本文方案的计算成本均低于文献[21]方案,而文献[33]方案生成的是对称群密钥且不支持车辆的加入和离开操作,没有给出具体的对称加密算法,因此在车载云服务的加解密阶段计算成本未知。

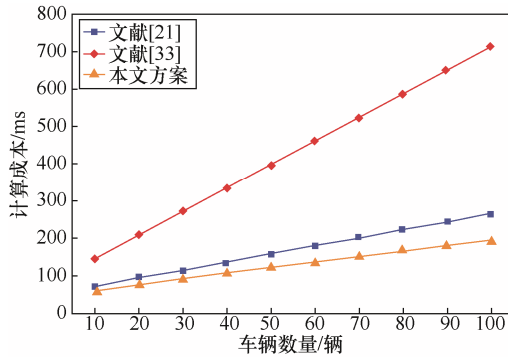


图3 车载云初始化阶段的计算成本
Figure 3 Computing overhead during the VC initialization phase

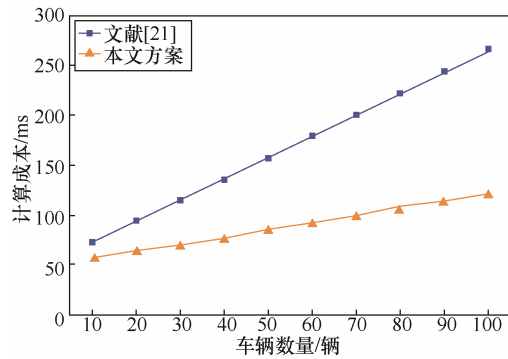


图4 车辆加入阶段的计算成本
Figure 4 Computing overhead during vehicle joining phase

3.3 丢包率和吞吐量分析

(1) 丢包率

式(2)定义了丢包率 P_L , 其中 $\text{Avg}(\cdot)$ 表示平均

值函数, Num_l^i 表示丢失的消息个数, Num_r^i 表示从车辆端接收到的消息个数。图5给出了本文方案中丢包率与车辆速度之间的关系,从图5中可以看出,随着车辆速度的增加,丢包率不断增加,这是因为车辆速度越快,节点间的网络拓扑变化越快,即会频繁发生网络断开,使得网络水平切换频率增加,不利于保持车辆之间的稳定通信连接,从而导致丢包率增加。

$$P_L = \text{Avg}\left(\sum_{i=1}^n \frac{\text{Num}_l^i}{\text{Num}_l^i + \text{Num}_r^i}\right) \quad (2)$$

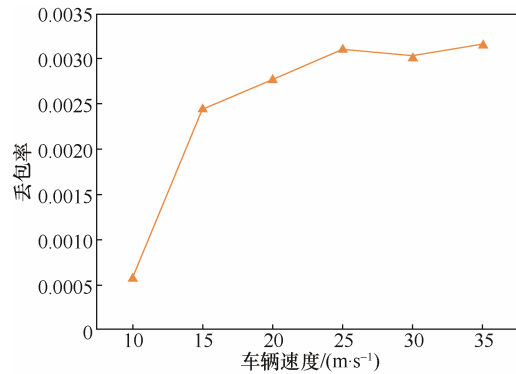


图5 丢包率与车辆速度之间的关系
Figure 5 The relationship of packet loss rate and vehicle speed

(2) 吞吐量

通常情况下,吞吐量是随着车辆数量的增加而增加的,因为车辆数量增加,发送的数据包数量相应增加。图6显示了吞吐量与仿真时间之间的关系,通过使用50辆、100辆、150辆汽车来评估吞吐量性能。随着仿真时间的增加,吞吐量值也会增加,因为这期间可能存在车辆的加入或退出,车辆会发送相应数据包,吞吐量会增加。

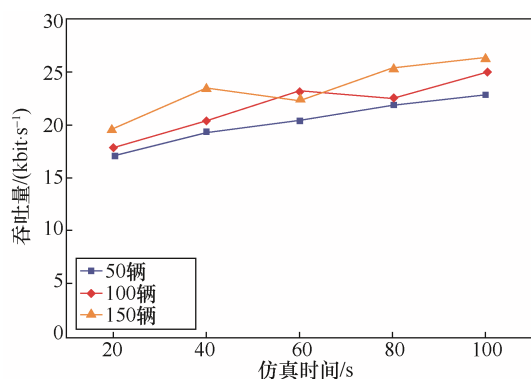


图 6 吞吐量与仿真时间之间的关系

Figure 6 The relationship between handling capacity and simulation time

4 结束语

本文针对 VCC 的安全、隐私和效率需求,设计了一个动态群密钥协商协议,用于在参与 VCC 的车辆之间建立基本的信任并保证 VCC 服务的安全性,而且该协议支持匿名认证,能保护车辆的身份隐私,支持 VCC 成员的动态加入和退出,保证群密钥的前向安全性。另外,为保证 VCC 通信的安全性,一个轻量级的支持批量验证的签名方案被用于保护所有通信消息的来源真实性和完整性。安全分析表明,本文方案满足 VCC 和 VANET 对车辆安全和隐私需求,分析显示本文方案具有一定的性能优势,满足 VCC 的高时效性要求。

参考文献:

- [1] HAMDI M M, AI-DOSARY O A R, ALRAWI O A S, et al. An overview of challenges for data dissemination and routing protocols in VANETs[C]//2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2021: 1-6.
- [2] PAVITHRA T, NAGABHUSHANA B S. A survey on security in VANETs[C]//2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA). 2020: 881-889.
- [3] SASUBILLI M K, VENKATESWARLU R. Cloud computing security challenges, threats and vulnerabilities[C]//2021 6th International Conference on Inventive Computation Technologies (ICICT). 2021: 476-480.
- [4] KANWAL I, SHAFI H, MEMON S, et al. Cloud computing security challenges: a review[C]//Cybersecurity, Privacy and Freedom Protection in the Connected World. 2021: 459-469.
- [5] OLARIU S, HRISTOV T, YAN G J. The next paradigm shift: from vehicular networks to vehicular clouds[C]//Mobile ad Hoc networking: Cutting Edge Directions. 2013: 645-700.
- [6] GOUMIDI H, ALIOUAT Z, HAROUS S. Vehicular cloud computing security: a survey[J]. Arabian Journal for Science and Engineering, 2020, 45(4): 2473-2499.
- [7] SHEIKH M S, LIANG J, WANG W S. Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey[J]. Wireless Communications and Mobile Computing, 2020, 2020(3): 1-25.
- [8] OLARIU S, KHALIL I, ABUELELA M. Taking VANET to the clouds[J]. International Journal of Pervasive Computing and Communications, 2010, 7(1): 7-21.
- [9] HUSSAIN R, SON J, EUN H, et al. Rethinking vehicular communications: Merging VANET with cloud computing[C]//4th IEEE International Conference on Cloud Computing Technology and Science Proceedings. 2012: 606-609.
- [10] YU R, ZHANG Y, GJESSING S, et al. Toward cloud-based vehicular networks with efficient resource management[J]. IEEE Network, 2013, 27(5): 48-55.
- [11] AHMAD F, KAZIM M, ADNANE A, et al. Vehicular cloud networks: architecture, applications and security issues[C]//2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC). 2015: 571-576.
- [12] ZHENG K, MENG H L, CHATZIMISIOS P, et al. An SMDP-based resource allocation in vehicular cloud computing systems[J]. IEEE Transactions on Industrial Electronics, 2015, 62(12): 7920-7928.
- [13] SHARMA S, KAUL A. VANETs cloud: architecture, applications, challenges, and issues[J]. Archives of Computational Methods in Engineering, 2021, 28: 2081-2102.
- [14] LIM K, ABUMUHFOUZ I M. STORS: secure token reward system for vehicular clouds[C]//SoutheastCon 2015. 2015: 1-2.
- [15] LIM K, ABUMUHFOUZ I M, MANIVANNAN D. Secure incentive-based architecture for vehicular cloud[C]//International Conference on Ad-Hoc Networks and Wireless. 2015: 361-374.
- [16] CUI J, ZHANG X Y, ZHONG H, et al. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 1654-1667.
- [17] ZHOU J, DONG X L, CAO Z F, et al. Secure and privacy preserving protocol for cloud-based vehicular DTNs[J]. IEEE Transactions on Information Forensics and Security, 2017, 10(6): 1299-1314.
- [18] KONG Q L, LU R X, ZHU H, et al. A secure and privacy-preserving incentive framework for vehicular cloud on the road[C]//2016 IEEE Global Communications Conference (GLOBECOM), 2016: 1-6.
- [19] 张瑾瑜. 基于车载云的安全认证和隐私保护机制研究[D]. 北京: 北京交通大学, 2018.
- [19] ZHANG J Y. Research on security authentication and privacy protection mechanism of vehicular cloud computing[D]. Beijing: Beijing Jiaotong University, 2018.
- [20] YAO Y Y, CHANG X L, MIŠIĆ J, et al. Lightweight and privacy-preserving ID-as-a-service provisioning in vehicular cloud computing[J]. IEEE Transactions on Vehicular Technology, 2019, 69(2): 2185-2194.
- [21] ZHANG L, MENG X Y, CHOO K K R, et al. Privacy-preserving cloud establishment and data dissemination scheme for vehicular

- cloud[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 17(3): 634-647.
- [22] SUN P, SAMAAN N. A novel VANET-assisted traffic control for supporting vehicular cloud computing[J]. IEEE Transactions on Intelligent Transportation Systems, 2020.
- [23] SALAHUDDIN M A, AL-FUQAHA A, GUIZANI M. Software-defined networking for rsu clouds in support of the internet of vehicles[J]. IEEE Internet of Things Journal, 2014, 2(2): 133-144.
- [24] HUANG X M, YU R, KANG J W, et al. Software defined networking with pseudonym systems for secure vehicular clouds[J]. IEEE Access, 2016, 4: 3522-3534.
- [25] WANG Q L, OU M, YANG Y, et al. Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks[J]. IEEE Access, 2020, 8: 217592-217602.
- [26] CAI Y, ZHANG H, FANG Y G. A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2020, 8(1): 647-656.
- [27] GUPTA M, GERA P, MISHRA B. CPAAS: an efficient conditional privacy-preservation anonymous authentication scheme using signcryption in VANET[J]. International Journal of Vehicle Information and Communication Systems, 2021, 6(1): 88-105.
- [28] CUI J, ZHANG J, ZHONG H, et al. SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 10283-10295.
- [29] 宋成, 张明月, 彭维平, 等. 基于双线性对的车联网批量匿名认证方案研究[J]. 通信学报, 2017, 38(6): 49-57.
- SONG C, ZHANG M Y, PENG W P, et al. Research on batch anonymous authentication scheme for VANET based on bilinear pairing[J]. Journal on Communications, 2017, 38(6): 49-57.
- [30] ZHANG Q K, GAN Y, ZHANG Q X, et al. A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application[J]. IEEE Access, 2018, 6: 24064-24074.
- [31] 陈若昕, 陈杰, 张跃宇, 等. 无证书非对称群密钥协商协议[J]. 密码学报, 2016, 3(4): 382-398.
- CHENG R X, CHENG J, ZHANG Y Y, et al. Certificateless asymmetric group key agreement[J]. Journal of Cryptologic Research, 2016, 3(4): 382-398.
- [32] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的信息认证方案[J]. 通信学报, 2016, 37(11): 1-10.
- WU L B, XIE Y, ZHANG Y B. Efficient and secure message authentication scheme for VANET[J]. Journal on Communications, 2016, 37(11): 1-10.
- [33] 姚英英. 面向车载云雾服务的信任协商[D]. 北京: 北京交通大学, 2021.
- YAO Y Y. Trust negotiation in vehicular cloud and fog services[D]. Beijing: Beijing Jiaotong University, 2021.
- [34] LIU Y B, WANG Y H, CHANG G H. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(10): 2740-2749

[作者简介]



肖敏(1971-), 女, 湖北宜昌人, 重庆邮电大学教授、博士生导师, 主要研究方向为现代密码学理论与应用、车联网安全、量子密码。



姚涛(1997-), 男, 安徽安庆人, 重庆邮电大学硕士生, 主要研究方向为现代密码学理论与应用、车联网安全。



刘媛妮(1978-), 女, 河南邓州人, 重庆邮电大学副教授, 主要研究方向为移动群智能感知网络、云计算安全。



黄永洪(1974-), 男, 重庆人, 重庆邮电大学讲师, 主要研究方向为安全操作系统、人工智能安全。