车联网中基于环的匿名高效批量认证与组密钥协商协议

张海波[1,2]，兰凯[1,2]，陈舟[1,2]，王汝言[1,2]，邹灿[3]，王明月[1,4]

（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 先进网络与智能互联技术重庆市高校重点实验室，重庆 400065；
3. 三六零数字安全科技集团有限公司，北京 100015；4. 丹麦奥尔堡大学，奥尔堡 9220）

摘 要：针对当前批量认证与密钥协商协议依赖于半可信路边单元（RSU）且不适用于大规模车联网（IoV）场景下密钥更新的问题，提出了 IoV 中基于环的匿名高效批量认证与组密钥协商协议。通过假名机制确保匿名性，利用混沌映射安全构建认证密钥对，并通过少量双线性映射快速完成对大批车辆的批量认证。充分考虑大规模 IoV 场景下车辆加入与离开情况，利用混沌映射半群性高效构建环状会话组，设计了适用于大规模车辆的组密钥建立与更新机制。此外，该协议设定了假名更新与匿名追溯机制确保更安全的会话过程，同时利用 BAN 逻辑模型证明了协议语义安全性。安全性分析与仿真结果表明，所提协议具备多重安全属性且拥有一定的效率优势。

关键词：车联网；批量认证；组密钥协商；混沌映射；密钥更新机制

中图分类号：TN915.08

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023055

Ring-based efficient batch authentication and group key agreement protocol with anonymity in Internet of vehicles

ZHANG Haibo[1,2], LAN Kai[1,2], CHEN Zhou[1,2], WANG Ruyan[1,2], ZOU Can[3], WANG Mingyue[1,4]

1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. Advanced Network and Intelligent Connection Technology Key Laboratory of Chongqing Education Commission of China, Chongqing 400065, China
3. 360 Digital Security Technology Group Co., Ltd., Beijing 100015, China
4. Aalborg University, Aalborg 9220, Denmark

Abstract: Aiming at the problem that the current batch authentication and key agreement protocol were relied on semi-trusted road side unit (RSU) and were not suitable for key update in large-scale Internet of vehicles (IoV), a ring-based efficient batch authentication and group key agreement protocol with anonymity in IoV was proposed. The anonymity was ensured by the pseudonym mechanism. The authentication key pairs were constructed by the chaotic map, and the batch authentication for many vehicles was quickly completed by a small number of bilinear maps. The joining and leaving of vehicles in large-scale IoV scenario were fully considered, a ring session group was efficiently constructed by using the semi-group property of chaotic maps, and a group key establishment and update mechanism suitable for large-scale vehicles was designed. In addition, a pseudonym update mechanism and an anonymous tracing mechanism were designed to ensure a more secure session process. At the same time, the BAN logic model was used to prove the semantic security of the protocol. The security analysis and simulation results show that the proposed protocol has multiple security attributes and certain efficiency advantages.

Keywords: IoV, batch authentication, group key agreement, chaotic mapping, key update mechanism

收稿日期：2022−11−28；**修回日期：**2023−02−06

基金项目：国家自然科学基金资助项目（No.61901071，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）

Foundation Items: The National Natural Science Foundation of China (No.61901071, No.61801065), The Program for Changjiang Scholars and Innovative Research Team in University (No.IRT16R72), Chongqing Innovation and Entrepreneurship Program for the Returned Overseas Chinese Scholars (No.cx2020059)

0 引言

信息与通信技术的飞速发展，使车联网（IoV, Internet of vehicles）的能力随着车辆与基础设施、行人系统以及云服务商之间的合作通信得到了有效提升[1]。IoV 使智能车辆（IV, intelligent vehicles）能够感知、处理和执行许多新型应用[2]，为用户带来了更多快捷便利的服务。然而，IoV 建立在传统无线通信网络的基础之上，继承了无线通信网络开放性的特点，加上车辆的高度动态性，使 IoV 极易遭受各种攻击[3-4]，致使用户的个人隐私信息泄露与生命财产安全受到严重威胁，因此解决 IoV 中的安全与隐私问题已然成为研究关键。

批量认证与密钥协商（BAKA, batch authentication and key agreement）是解决 IoV 安全与隐私问题的有效手段。通过批量认证使大批合法注册车辆快速接入 IoV，同时拒绝非法恶意车辆的访问；通过密钥协商建立安全会话密钥加密实体间的通信信息，以此保障会话内容不被窃取。IoV 的特性要求 BAKA 协议应当具备多重安全属性与低开销、高效率等特点，然而现有对 BAKA 协议的研究仍然存在一些问题。

关于批量认证，已有学者开展了相关研究[5-9]。Jiang 等[5]提出了车载自组网（VANET, vehicular ad-hoc network）中的高效匿名批量认证方案，该方案通过可信中心（TA, trusted authority）确保车辆生成的假名具有匿名性，利用路边单元（RSU, road side unit）完成对车辆的批量验证，然而该方案依赖于 TA 为 RSU 颁布的证书，存在复杂证书管理问题。Sutrala 等[6]针对上述问题，提出了 IoV 中的无证书条件隐私保护批量认证方案，该方案通过 RSU 为车辆生成假名并基于椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm）完成对大批车辆的同时验证，然而该方案依赖于密钥生成中心（KGC, key generation center），无法解决密钥托管问题。Tzeng 等[7]指出现有批量验证方案存在一定的安全风险，提出了基于身份的隐私保护批量认证方案，该方案以 TA、应用服务器（AS, application server）、RSU 和车载单元（OBU, on-board unit）共同组成的双层网络架构为基础，在 RSU 认证前预先通过防篡改设备（TPD, tamper-proof device）检验车辆真实身份和密码，但方案限制在 TA 与 RSU 通过安全信道进行通信的条件下。Vijayakumar 等[8]提出了 VANET 中基于双线性配对的匿名批量认证协议，该协议只需车辆与 RSU 间通过少许步骤即可完成身份验证，有效降低了通信开销，然而协议在对消息完整性进行检验时频繁使用较复杂的双线性配对，产生了较大的计算负担，同时协议没有进行安全性证明且不能抵御重放攻击，缺乏一定的安全属性。Gayathri 等[9]针对双线性配对与证书的复杂性问题提出了 VANET 中无证书无配对的高效批量认证方案，该方案以椭圆曲线点乘操作代替双线性对来减少 RSU 批量验证中产生的计算开销，同时以为车辆设置部分私钥代替完整私钥的方式确保了更安全的认证过程。由此可见，上述方案均依赖于 RSU 完成对车辆的批量验证，但实际上 RSU 属于半可信实体，在开放环境中容易遭受攻击，因此直接利用 RSU 进行批量认证存在一定安全隐患。

关于密钥协商，文献[10-15]进行了相关研究。Huang 等[10]为减小密钥协商过程中的验证时延和传输开销，基于 ECDSA 提出了车辆与服务提供商（SP, service provider）之间的密钥协商协议。Zhang 等[11]指出现有方案侧重单车与单 SP 之间的信息交互，提出了 IoV 中支持多车多 SP 间协商会话密钥的方案。Liu 等[12]基于双线性配对和可信计算提出了一种安全高效的隐私保护密钥协商方案，该方案以车辆历史交互行为来评估车辆信誉度，符合要求的车辆间能够安全协商会话密钥，但方案中大量使用双线性配对操作，因而产生了较大的计算开销。Xu 等[13]针对基于双线性配对的方案太过复杂的问题，提出了一种新的基于双线性映射的组密钥协商方案，该方案利用 TA 负责组密钥的生成、加密与传输，有效降低了计算开销与密钥存储负担，然而方案只利用了 RSU 生成的随机数充当组密钥核心部分，存在较高的密钥泄露风险。上述方案均没有考虑到车辆高速移动的特性，协议并不具备密钥更新机制。Kim 等[14]提出了基于树的组密钥协商协议，协议考虑到车辆的动态变化因素，支持密钥的建立和更新，同时利用模指数运算代替双线性对运算表现出了显著的效率优势。Wei 等[15]指出 Kim 方案的密钥更新发起方会在不受信任的不同车辆间变化，具有较高的安全隐患，因此提出了一种改进的基于树的组密钥协商协议，该协议在密钥更新过程中并不改变原树的结构，并且密钥建立（或更新）由固定的 RSU 节点负责，拥有较高安全性，然而该协议并不适用于大规模 IoV 通信环境，当有多辆车同时加入会话组时协议会产生较高的计算开销与排队时延。

综上所述，现有批量认证协议大多依赖于半可信的 RSU，而密钥协商协议很少考虑到 IoV 网络拓扑

的高速动态变化，且不适用于大规模通信场景。针对上述问题，本文设计了 IoV 中基于环的匿名高效批量认证与组密钥协商（BAGKA, batch authentication and group key agreement）协议。本文主要贡献如下。

1) 提出了一种基于切比雪夫混沌映射与双线性映射的高效匿名批量认证协议。利用混沌映射安全构建认证密钥对，通过 TA 为车辆设置假名确保匿名性，并利用少量双线性映射完成对大批同时涌入车辆的高效批量认证。通过设置长期会话密钥确保车辆和 RSU 能够与 TA 进行安全通信。

2) 设计了一种基于环的分布式快速组密钥协商协议。利用混沌映射半群性快速构建环状会话组，通过 RSU 利用单向哈希函数与对称加密技术完成组密钥的建立与加密传输。组内所有车辆与 RSU 均提供了部分私密值参与完整组密钥的生成，同时协议支持大规模 IoV 场景下的高效密钥更新。

3) 本文所提协议能够实现车辆的假名更新和匿名追溯，同时协议通过 BAN 逻辑模型进行了语义安全性证明。安全性分析与仿真结果表明，本文所提协议具备多重安全属性，且较传统协议有一定的效率优势。

1　预备知识

1.1　系统模型

本文所提协议的系统模型包含 3 个实体，即 TA、RSU 和车辆。系统模型如图 1 所示。

TA：IoV 系统中完全受信任的实体，拥有强大的计算与存储能力，主要负责为车辆与 RSU 提供注册与批量认证服务。

RSU：IoV 系统中的半可信实体，主要部署在路边，负责与车辆和 TA 进行信息交互。

车辆：IoV 系统中的不受信任实体，每辆车都配备有 OBU，负责简单计算与通信任务。

1.2　双线性对与复杂性假设

设 G,G_T 为乘性循环群，其对应素数阶均为 q，令 $g_1,g_2\in G$ 为 G 的 2 个生成元，定义一个双线性映射 $e:G\times G\to G_T$ 满足以下 3 个条件。

1) 双线性：$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$，$\forall a,b\in Z_q^*$，$Z_q^*\in\{1,2,\cdots,q-1\}$。

2) 非退化性：$e(g_1,g_2)\neq 1$。

3) 可计算性：对于 $e:G\times G\to G_T$，在有效概率多项式时间内能够计算出该结果。

基于扩展切比雪夫混沌映射计算离散对数问题（CDLP, computational discrete logarithm problem）：给定参数 $x\in(-\infty,+\infty),n$，计算 $y=T_\theta(x)\bmod n$，n 为一个大素数，在已知 y,x,n 的条件下，在概率多项式时间内成功求解出 θ 值的概率可以忽略不计。

基于扩展切比雪夫混沌映射计算迪菲–赫尔曼问题（CDHP, computational Diffie-Hellman problem）：对于 $y_1=T_\alpha(x)\bmod n,y_2=T_\beta(x)\bmod n$，在已知 y_1,y_2,x,n 的条件下成功计算 $T_{\alpha\beta}=T_{\alpha\beta}(x)\bmod n$ 是困难的。

2　IoV 中的 BAGKA 协议

为了实现 IoV 中车辆、RSU 与 TA 之间的安全通信，本文所提 BAGKA 协议包含 6 个阶段，分别为系统初始化、车辆与 RSU 注册、匿名批量认证、

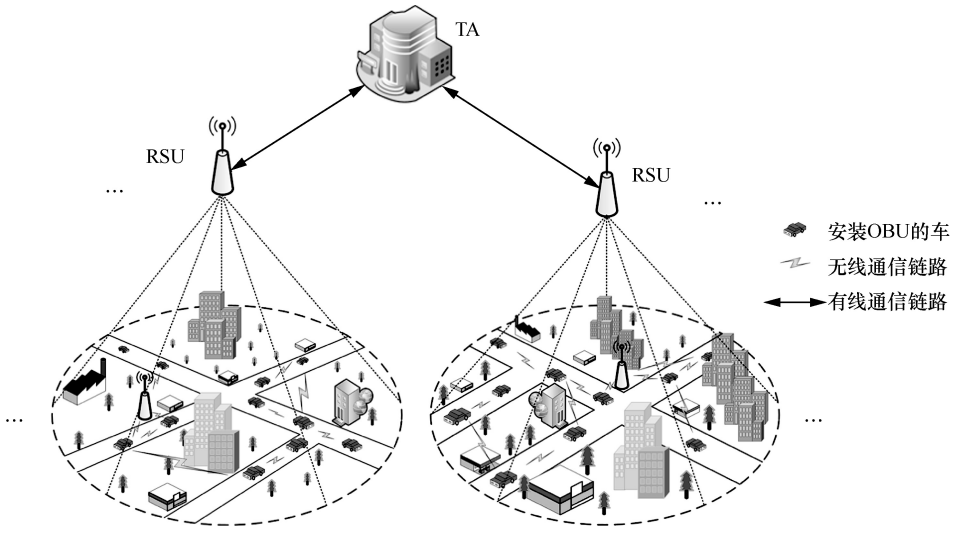


图 1　系统模型

组密钥协商、假名更新以及匿名追溯阶段。协议所涉及的系统参数及其含义如表 1 所示。

表 1 系统参数及其含义

参数	含义
n	大素数
h	哈希运算
s	系统私钥
V_i	车辆节点
RSU_j	第 j 个 RSU
$\mathrm{FID}_{V_i},\mathrm{FID}_{R_j}$	V_i 与 RSU_j 的假名
$\mathrm{SK}_{V_i},\mathrm{SK}_{R_j}$	V_i 与 RSU_j 的长期会话密钥
B_i,D_j	V_i 与 RSU_j 的公钥
T_i,t_i	时间戳
E_k,D_k	使用密钥 k 进行对称加密/解密
$\oplus$	异或加密
SK_z	组密钥

2.1 系统初始化阶段

TA 选择系统公共参数 x,n（n 为一个随机的大素数），确定素数阶为 q 的循环群 G,G_T 与其生成元 g_1,g_2，并选择一个随机数 $s\in Z_q^*\in\{1,2,\cdots,q-1\}$ 作为系统私钥，然后计算对应的系统公钥 $\mathrm{PK}_{\mathrm{TA}}=T_s(x)\bmod n$，确定一个单向抗冲突哈希函数 $h:\{0,1\}^*\to\{0,1\}^{l_i}$，其中，$l_i$ 为位长，计算 $e(g_1,g_2)=F$。TA 在系统中广播公共参数 $\{G,h,q,n,x,g_1,g_2,\mathrm{PK}_{\mathrm{TA}}\}$。

2.2 车辆与 RSU 注册阶段

1) 车辆注册

车辆 V_i 通过安全信道上传其真实身份 ID_{V_i} 到 TA，TA 收到后计算 $\mathrm{FID}_{V_i}=h(\mathrm{ID}_{V_i}\|s)$ 作为 V_i 的假名，然后继续计算 $\mathrm{SK}_{V_i}=T_{\mathrm{FID}_{V_i},s}(x)\bmod n$ 作为 V_i 与 TA 之间的长期会话密钥。之后 TA 选择一个随机 $b_i\in Z_q^*$ 作为 V_i 的私钥，并计算对应公钥 $B_i=g_1^{s+b_i}$，$\mathrm{RK}_{V_i}=g_1^{-b_i}$ 作为一个再加密密钥，最后 TA 通过安全信道返回参数 $\{B_i,\mathrm{FID}_{V_i},\mathrm{SK}_{V_i}\}$ 给 V_i。

2) RSU 注册

RSU_j 选择一个随机数 $d_j\in Z_q^*$ 作为其私钥，并计算对应公钥 $D_j=T_{d_j}(x)\bmod n$，之后 RSU_j 通过安全信道上传真实身份 ID_{R_j} 与 D_j 到 TA。TA 接收到消息后计算 $\mathrm{SK}_{R_j}=h\left(\mathrm{ID}_{R_j}\|s\right)$，将 SK_{R_j} 作为 RSU_j 与 TA 之间的长期会话密钥，最后 TA 将 SK_{R_j} 通过安全信道返回给 RSU_j。

2.3 匿名批量认证阶段

在进行组密钥协商之前，需要对车辆和 RSU 进行认证。本文设计了通过 TA 对大批同时涌入车辆进行快速匿名批量认证的协议，同时 TA 也完成了对覆盖这些车辆的 RSU 的认证，只有经过身份验证的车辆与 RSU 才能参与后续的组密钥协商过程，整个匿名批量认证协议通过以下 5 个步骤完成（这些步骤均在公共不安全信道中进行），该阶段实体间的信息交互如图 2 所示。

步骤 1 车辆 V_i 选择随机数 $x_i\in Z_q^*$ 作为其密钥协商的部分私钥，并计算对应的部分公钥 $y_i=T_{x_i}(x)\bmod n$，之后计算 $\varepsilon_i=g_1^{\mathrm{SK}_{V_i}}$，$\beta_i=B_i\varepsilon_i$。获取当前时间戳 T_{V_i}，计算 $\delta_i=h\left(y_i\|T_{x_i}(\mathrm{PK}_{\mathrm{TA}})\|T_{V_i}\right)$，最后 V_i 上传消息 $M_i=\{y_i,\mathrm{FID}_{V_i},T_{V_i},\beta_i,\delta_i\}$，$(i=1,2,\cdots,k)$ 到 RSU_j。

步骤 2 RSU_j 收到来自 k 辆车的认证请求消息后，首先检验时间戳的有效性，记录当前系统时间为 T_{cur}，检验 $|T_{\mathrm{cur}}-T_{V_i}|\leqslant\Delta T$ 是否成立（其中，ΔT 为最大合法时间间隔，本文接下来的步骤均采用此种检验机制），若不成立则拒绝此次请求，若成立则存储消息 M_i。然后 RSU_j 选择一个随机数 $x_j\in Z_q^*(j\neq i)$ 作为其用于密钥协商的部分私钥，计算对应部分公钥 $y_j=T_{x_j}(x)\bmod n$，获取当前时间戳 T_{R_j}，然后计算 RSU_j 对应的假名 $\mathrm{FID}_{R_j}=\mathrm{ID}_{R_j}\oplus h\left(T_{d_j}(\mathrm{PK}_{\mathrm{TA}})\|T_{R_j}\right)$，再计算 RSU_j 对应的签名 $\mu_j=h\left(\mathrm{ID}_{R_j}\|T_{R_j}\|\mathrm{SK}_{R_j}\|y_j\right)$，最后 RSU_j 发送消息 $m_1=\{\mu_j,\mathrm{FID}_{R_j},T_{R_j},\mathrm{FID}_{V_i},T_{V_i},\beta_i,y_i,y_j,\delta_i\}$ 到 TA。

步骤 3 TA 收到消息后先检验时间戳 T_{R_j} 的有效性，如果时间戳有效则 TA 计算 $\mathrm{ID}_{R_j'}=\mathrm{FID}_{R_j}\oplus h\left(T_s(D_j)\|T_{R_j}\right)$，$\mathrm{SK}_{R_j}'=h\left(\mathrm{ID}_{R'_j}\|s\right)$，$\mu_j'=h\left(\mathrm{ID}_{R_j'}\|T_{R_j}\|\mathrm{SK}_{R_j}'\|y_j\right)$，验证 $\mu_j=\mu_j'$ 是否成立，若等式不成立则拒绝此次请求，若成立则计算 $\delta_i'=h\left(y_i\|T_s(y_i)\|T_{V_i}\right)$，再判断等式 $\delta_i'=\delta_i$ 是否成

图 2　匿名批量认证阶段实体间的信息交互

立，若等式成立则继续计算 $\mathrm{SK}_{V_i}' = T_{\mathrm{FID}_{V_{i,s}}}(x) \bmod n$，$\mathrm{RK}_{V_i}' = \mathrm{RK}_{V_i} g_1^{-\mathrm{SK}_{V_i}'}$，最后判断等式 $e\left(\prod_{i=1}^{n} \beta_i \prod_{i=1}^{n} \mathrm{RK}_{V_i}', g_2^{\frac{1}{ns}}\right) = F$ 是否成立，若成立则 TA 完成了对此 k 辆车的一次批量认证，若不成立则拒绝访问。为了使车辆和 RSU$_j$ 相互验证其关键参数，TA 继续计算 $\gamma_{\mathrm{TA}} = h\left(T_{\mathrm{TA}} \| \mathrm{FID}_{V_i} \| \beta_i \| y_i \| \mathrm{SK}_{R_j}\right)$，$\phi_{\mathrm{TA}}^{V_i} = h\left(T_{\mathrm{TA}} \| \mathrm{FID}_{R_j} \| y_j \| \mathrm{SK}_{V_i} \| D_j\right), (i = 1, 2, \cdots, k)$，其中，$T_{\mathrm{TA}}$ 为当前时间戳，D_j 为 RSU$_j$ 注册时上传给 TA 的公钥，最后 TA 将消息 $m_2 = \left\{T_{\mathrm{TA}}, \gamma_{\mathrm{TA}}, \phi_{\mathrm{TA}}^{V_i}\right\}$ 发送给 RSU$_j$。

步骤 4　RSU$_j$ 收到消息 m_2 后首先检验时间戳 T_{TA} 是否有效，若有效则 RSU$_j$ 计算 $\gamma_{\mathrm{TA}}' = h\left(T_{\mathrm{TA}} \| \mathrm{FID}_{V_i} \| \beta_i \| y_i \| \mathrm{SK}_{R_j}\right)$，判断 $\gamma_{\mathrm{TA}}' = \gamma_{\mathrm{TA}}$ 是否成立，若成立则 RSU$_j$ 接收参数 $\{\mathrm{FID}_{V_i}, y_i\}$，若不成立则拒绝本次请求。最后 RSU$_j$ 广播消息 $m_3 = \left\{T_{\mathrm{TA}}, \phi_{\mathrm{TA}}^{V_i}, \mathrm{FID}_{R_j}, D_j, y_j\right\}$ 给之前发送认证请求的所有车辆。

步骤 5 车辆 V_i 接收到消息 m_3 后，同样先检验时间戳 T_{TA} 的有效性，若有效则 V_i 计算 $\phi'^{V_i}_{\mathrm{TA}}=h\left(T_{\mathrm{TA}}\|\mathrm{FID}_{R_j}\|y_j\|\mathrm{SK}_{V_i}\|D_j\right)$，判断等式 $\phi'^{V_i}_{\mathrm{TA}}=\phi^{V_i}_{\mathrm{TA}}$ 是否成立，若成立则 V_i 接收参数 $\left\{\mathrm{FID}_{R_j},y_j,D_j\right\}$，若不成立则中止此过程。

2.4 组密钥协商阶段

对于成功认证后发起会话请求的车辆，由 RSU 负责对其范围内的请求车辆进行组密钥协商。考虑到 IoV 网络拓扑的高速动态变化问题，本文针对车辆加入与离开 RSU 会话组 2 种场景，设计了基于环的组密钥协商算法，相邻车辆间通过混沌映射快速构建关键参数，参数之间的关联性使它们与 RSU 间形成了环状。通过本文所提协议，将加入车辆按请求时间先后顺序依次编号（便于协议描述），环内所有车辆与 RSU 共同参与计算并生成组内公共会话密钥。

2.4.1 新车加入会话组的组密钥协商过程

当 RSU 组内存在 k 辆车（若组内不存在已加入车辆，则 $k=0$）并在接下来有 m 辆车想要加入组内时，按照下述步骤协商组密钥，场景示意如图 3 所示。

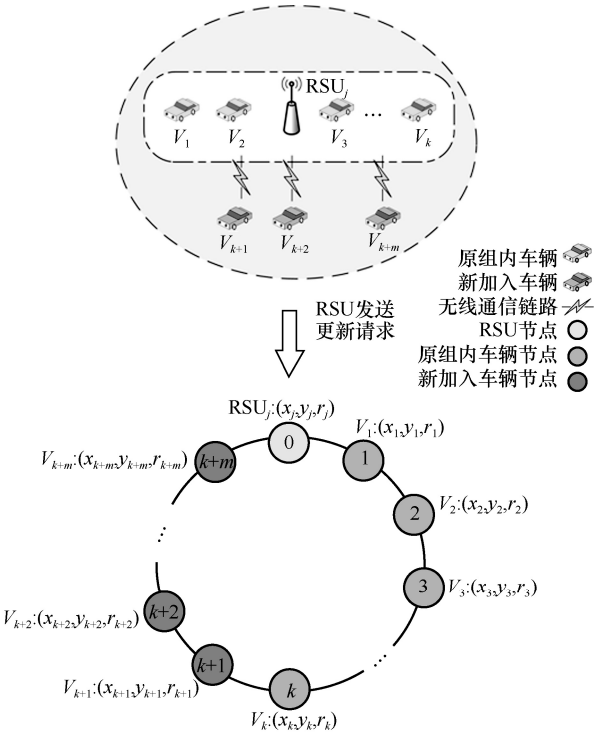


图 3 新车加入组内的组密钥协商过程

步骤 1 组外的 m 辆新车向 RSU$_j$ 发送加入请求，RSU$_j$ 获取当前时间戳 t_{R_j} 并计算 $\eta_i=h(T_{d_j}(y_i)\|y_1\|y_2\|\cdots\|y_{k+m}\|t_{R_j}),(i=1,2,\cdots,k+m)$，之后 RSU$_j$ 向附近所有车辆 $V_i(i=1,2,\cdots,k+m)$ 广播消息 $\mathrm{Mg}_1=\{y_1,y_2,\cdots,y_{k+m},\eta_i,t_{R_j}\}$。

步骤 2 车辆 V_i 接收到消息 Mg_1 后，首先检验时间戳 t_{R_j} 的新鲜度，通过后计算 $\eta'_i=h(T_{x_i}(D_j)\|y_1\|y_2\|\cdots\|y_{k+m}\|t_{R_j})$，判断 $\eta'_i=\eta_i$ 是否成立，若成立则 V_i 存储消息 Mg_1，若不成立则拒绝此次请求。确认消息合法之后 $V_i(i=k+1,k+2,\cdots,k+m)$ 选择一个随机二进制数 $r_i\in\{0,1\}^r$，其中 r 为二进制数的位长，获取系统当前时间戳 t_{V_i} 并计算 $\nu_i=h(r_i\|t_{V_i}),k_i^L=h(T_{x_i}(y_{i-1})),k_i^R=h(T_{x_i}(y_{i+1})),K_i=k_i^L\oplus k_i^R,\alpha_i=k_i^R\oplus r_i$。$V_k$ 更新 k_k^R,K_k 的值（若组内不存在已加入车辆则忽略此步）。最后 V_i 将消息 $\mathrm{mg}_i=\{K_i,t_{V_i},\nu_i,\alpha_i\}$ 发送到 RSU$_j$。

步骤 3 RSU$_j$ 收到消息 mg_i 后，首先检验 t_{V_i} 的有效性，若有效则 RSU$_j$ 计算 $k_j^L=h(T_{x_j}(y_{k+m})),k_j^R=h(T_{x_j}(y_1)),K_j=k_j^L\oplus k_j^R$，验证 $K_j\oplus K_1\oplus\cdots\oplus K_k=0$ 是否成立，若成立则从消息 α_i 中解密出 r'_i 并计算 $\nu'_i=h(r'_i\|t_{V_i}),(i=k+1,k+2,\cdots,k+m)$，验证等式 $\nu'_i=\nu_i$ 是否成立，成立则确定了 V_i 所传消息的合法性，不成立则拒绝本次请求。确认合法性之后 RSU$_j$ 选择一个随机二进制数 $r_j\in\{0,1\}^r$，计算组密钥 $\mathrm{SK}_z^t=h\left((r'_1,y_1)\|(r'_2,y_2)\|\cdots\|(r'_{k+m},y_{k+m})\|(r'_j,y_j)\right)$，之后 RSU$_j$ 对 SK_z^t 进行对称加密 $\mathrm{SK}_{z_i}^{*,t}=E_{\omega_i}(\mathrm{SK}_z^t),(i=1,2,\cdots,k+m)$，其中 ω_i 表示一个安全的对称加密密钥且 $\omega_i=T_{d_j}(y_i)$，获取当前时间戳 t'_{R_j} 并计算相应签名 $\tau_i=h\left(\mathrm{SK}_{z_i}^{*,t}\|t'_{R_j}\|\omega_i\right)$，最后 RSU$_j$ 广播消息 $\mathrm{Mg}_2=\{\mathrm{SK}_{z_i}^{*,t},\tau_i,t'_{R_j}\},i=(1,2,\cdots,k+m)$ 到附近车辆。

步骤 4 车辆 V_i 收到消息 Mg_2 后同样先检验时间戳 t'_{R_j} 的新鲜度，判定有效后继续计算 $\tau'_i=h\left(\mathrm{SK}_{z_i}^{*,t}\|t'_{R_j}\|\omega_i\right)$，其中 $\omega_i=T_{x_i}\left(D_j\right)$，然后判断等式 $\tau'_i=\tau_i$ 是否成立，若等式成立则 V_i 进行对称解密操作并计算出组内公共会话密钥 $\mathrm{SK}_z^t=D_{\omega_i}(\mathrm{SK}_{z_i}^{*,t})$，若不成立则拒绝本次请求。至此，组内所有车辆 V_i 与 RSU$_j$ 完成了一次组密钥协商，

它们之间共享公共会话密钥SK_z^t。

2.4.2 旧车离开会话组的组密钥更新过程

RSU 组内已经存在 k 辆车并在接下来有 m 辆车离开组，该场景下的组密钥更新过程如图 4 所示。

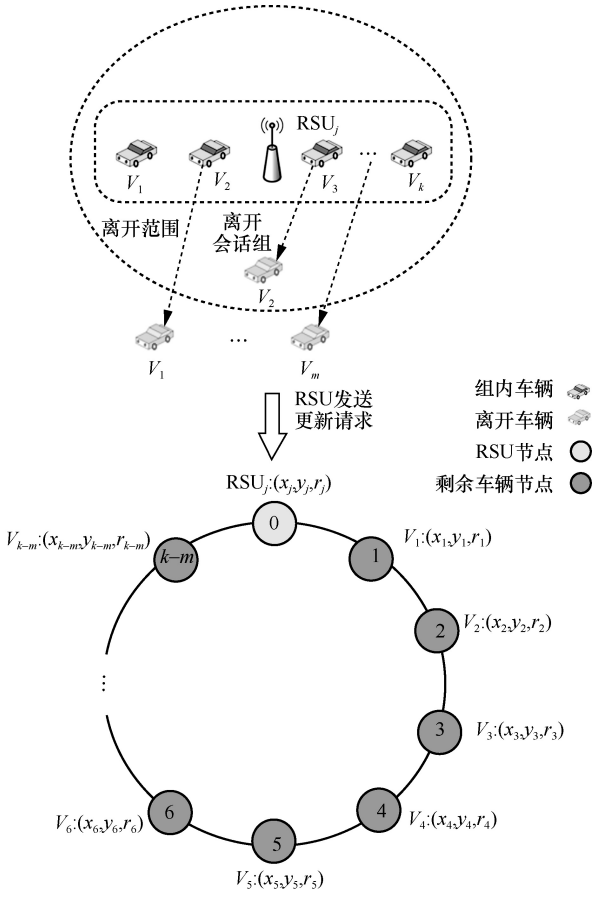


图 4　旧车离开组内的组密钥更新过程

步骤 1　当有 m 辆车离开会话组后，RSU_j 会更新组内剩余车辆的下标并向组内剩余车辆发送组密钥更新消息。RSU_j 重新选择一个随机的 r_j'，然后利用剩余车辆的 r_i', y_i 更新组密钥 $\mathrm{SK}_z^{t+1}=h\left((r_1',y_1)\|(r_2',y_2)\|\cdots\|(r_{k-m}',y_{k-m})\|(r_j',y_j)\right)$ 并进行相应的对称加密操作与签名，$\mathrm{SK}_{z_i}^{*,t+1}=E_{\omega_i}(\mathrm{SK}_z^{t+1}),(i=1,2,\cdots,k-m),\tau_i'=h(\mathrm{SK}_{z_i}^{*,t+1}\|t_{R_j}''\|\omega_i)$，最后向组内剩余车辆广播消息 $\{\mathrm{SK}_{z_i}^{*,t+1},\tau_i',t_{R_j}''\},i=(1,2,\cdots,k-m)$。

步骤 2　组内车辆在接收到更新消息后同样需要先检验时间戳，检验通过后解密出更新后的组密钥 SK_z^{t+1}。至此，组内剩余车辆与 RSU_j 之间完成了一次组密钥更新过程。

2.5 假名更新阶段

若车辆与 RSU 在系统中反复使用同一个假名发送相关消息，那么敌手可以将该假名作为真名发动攻击。因此本文设定了相应假名更新方式以应对敌手追踪。对于车辆而言，TA 给每辆车进行注册时都会为其分配一个假名更新种子 $\delta\mathrm{ID}_{V_i}$，当认证阶段结束后会更新一次假名，更新方式为 $\mathrm{FID}_{V_i}^1=h(\mathrm{FID}_{V_i}\|\delta\mathrm{ID}_{V_i})$。然后 TA 通过安全信道将更新后的假名返回给注册车辆，车辆在下次认证时会使用新的假名来发送消息；对于 RSU 而言，本文为其设定的假名生成方式包含了时间戳，因此 RSU 在不同时间段发送消息所携带的假名是不同的。

2.6 匿名追溯阶段

当经过合法注册的车辆在系统内散布恶意消息时，TA 将对车辆的合法身份进行匿名追溯与撤销。若车辆节点 V_i 在 RSU_j 的覆盖范围内散布恶意消息，RSU_j 则将 V_i 所对应的当前假名发送给 TA，TA 在收到消息后通过等式 $\mathrm{FID}_{V_i}=h(\mathrm{ID}_{V_i}\|s)$ 和假名更新种子 $\delta\mathrm{ID}_{V_i}$ 追溯出 V_i 的真实身份 ID_{V_i}，并对此真实身份进行撤销。

3 安全性证明与分析

3.1 形式化安全性证明

BAN 逻辑[16]是一种可靠的用于认证协议进行安全性证明的逻辑，由 Burrows、Abadi 和 Needham 提出。IoV 系统中所设计的认证协议需要进行形式化的证明才能够确定协议交互过程中面对敌手时是否能够保证安全性。本节将基于 BAN 逻辑对所提批量认证与组密钥协商协议进行形式化安全性证明。

3.1.1 BAN 逻辑符号定义

① P,Q：认证主体，K：共享密钥。

② (X,Y)：X 和 Y 的连接，表示消息 X 和消息 Y 一起组成了整体消息 (X,Y)。

③ $P|\equiv X$：P 认为消息 X 是真实可信的。

④ $P|\sim X$：P 曾经在某时刻发送过包含 X 的消息。

⑤ $P\lhd X$：P 发现了一条由其他主体所发送的包含 X 的消息。

⑥ $P|\Rightarrow X$：P 拥有对消息 X 的仲裁权。

⑦ $\#(X)$：消息 X 是新鲜的。

⑧ $\langle X\rangle_K$：利用密钥 K 加密消息 X。

⑨ $P \xleftrightarrow{K} Q$：P,Q 拥有共享的密钥 K。

3.1.2 BAN 逻辑推理规则

① 消息含义规则

$$\text{L1}:\frac{P\mid\equiv P\xleftrightarrow{K}Q, P\lhd\langle X\rangle_K}{P\mid\equiv Q\mid\sim X}$$。消息含义规则表示若 P 相信 P 与 Q 之间的共享密钥 K，且 P 发现了一条由 K 加密的消息 X，则 P 相信 Q 曾经发送过消息 X。

② 新鲜度规则

$$\text{L2}:\frac{P\mid\equiv \#(X)}{P\mid\equiv \#(X,Y)}$$。新鲜度规则表示若 P 相信消息 X 是新鲜的，则 P 会相信消息 (X,Y) 也是新鲜的。

③ 临时值验证规则

$$\text{L3}:\frac{P\mid\equiv \#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$$。临时值验证规则表示若 P 相信消息 X 是新鲜的，且 P 相信 Q 曾经发送过消息 X，则 P 会相信 Q 是相信 X 的。

④ 仲裁规则

$$\text{L4}:\frac{P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$$。仲裁规则表示若 P 相信 Q 有对消息 X 的仲裁权，且 P 相信 Q 是相信 X 的，那么 P 就会相信消息 X。

3.1.3 协议的理想化

为了将 BAN 逻辑规则与所提协议的具体步骤关联起来，需要由原协议导出理想化协议，即将所提协议中的消息转换为对应的 BAN 逻辑语言。

对于匿名批量认证阶段，协议的理想化形式如下。

① $\text{RSU}_j \lhd\langle y_i,\text{FID}_{V_i},T_{V_i},\beta_i,\delta_i\rangle_{\text{SK}_{V_i}}$。

② $\text{TA}\lhd\langle\mu_j,\text{FID}_{R_j},T_{R_j},\text{FID}_{V_i},T_{V_i},\beta_i,y_i,y_j,\delta_i\rangle_{\text{SK}_{V_i},\text{SK}_{R_j}}$。

③ $\text{RSU}_j \lhd\langle T_{\text{TA}},\gamma_{\text{TA}},\phi_{\text{TA}}^{V_i}\rangle_{\text{SK}_{R_j},\text{SK}_{V_i}}$。

④ $V_i \lhd\langle T_{\text{TA}},\phi_{\text{TA}}^{V_i},\text{FID}_{R_j},D_j,y_j\rangle_{\text{SK}_{V_i}}$。

对于环状组密钥协商阶段，协议的理想化形式如下。

① $V_i \lhd\langle y_1,y_2,\cdots,y_n,\eta_i,t_{R_j}\rangle_{D_j}$。

② $\text{RSU}_j \lhd\langle K_i,t_{V_i},\nu_i,\alpha_i\rangle_{y_i}$。

③ $V_i \lhd\langle\text{SK}_{z_i}^{*,t},\tau_i,t_{R_j}^{'}\rangle_{\omega_i}$。

3.1.4 确定协议初始假设

正式进行协议的安全证明之前，需要先对协议设定初始假设条件，主要分为 2 个部分，一个是实体之间的信任假设（2 个实体事先约定好的某个密钥或者共享的公钥）；另一个是状态假设，主要指实体对某消息的仲裁权。

$\text{P1}:\text{TA}\mid\equiv\text{TA}\xleftrightarrow{\text{SK}_{R_j}}\text{RSU}_j$

$\text{P2}:\text{TA}\mid\equiv\text{TA}\xleftrightarrow{\text{SK}_{V_i}}V_i$

$\text{P3}:\text{RSU}_j\mid\equiv\text{RSU}_j\xleftrightarrow{\text{SK}_{R_j}}\text{TA}$

$\text{P4}:V_i\mid\equiv V_i\xleftrightarrow{\text{SK}_{V_i}}\text{TA}$

$\text{P5}:V_i\mid\equiv V_i\xleftrightarrow{D_j}\text{RSU}_j$

$\text{P6}:\text{RSU}_j\mid\equiv\text{RSU}_j\xleftrightarrow{y_i}V_i$

$\text{P7}:V_i\mid\equiv V_i\xleftrightarrow{\omega_i}\text{RSU}_j$

$\text{P8}:\text{TA}\mid\equiv\text{RSU}_j\mid\Rightarrow\{\mu_j,\text{FID}_{R_j},y_j\}$

$\text{P9}:\text{TA}\mid\equiv V_i\mid\Rightarrow\{\text{FID}_{V_i},\beta_i,y_i,\delta_i\}$

$\text{P10}:\text{RSU}_j\mid\equiv\text{TA}\mid\Rightarrow\{\gamma_{\text{TA}}\}$

$\text{P11}:V_i\mid\equiv\text{RSU}_j\mid\Rightarrow\{\phi_{\text{TA}}^{V_i},\text{FID}_{R_j},D_j,y_j\}$

$\text{P12}:V_i\mid\equiv\text{RSU}_j\mid\Rightarrow\{y_1,y_2,\cdots,y_n,\eta_i\}$

$\text{P13}:\text{RSU}_j\mid\equiv V_i\mid\Rightarrow\{K_i,\nu_i,\alpha_i\}$

$\text{P14}:V_i\mid\equiv\text{RSU}_j\mid\Rightarrow\{\text{SK}_{z_i}^{*,t},\tau_i\}$

3.1.5 为协议设定安全证明目的

为了证明本文所提协议的语义是安全的，对协议的 2 个部分分别引入 2 个安全证明目的 agoal1,agoal2和kgoal1,kgoal2。经过形式化安全证明之后，需要实现此 4 个目的。

agoal1：$\text{RSU}_j\mid\equiv\gamma_{\text{TA}}$。$\text{RSU}_j$ 相信 TA 所发送的认证确认消息 γ_{TA}。

agoal2：$V_i\mid\equiv\phi_{\text{TA}}^{V_i}$。$V_i$ 相信 TA 所发送的认证确认消息 $\phi_{\text{TA}}^{V_i}$。

kgoal1：$\text{RSU}_j\mid\equiv\alpha_i$。$\text{RSU}_j$ 相信 V_i 所发送的密钥协商消息 α_i。

kgoal2：$V_i\mid\equiv\text{SK}_{z_i}^{*,t}$。$V_i$ 相信 RSU_j 所发送的密钥协商消息 $\text{SK}_{z_i}^{*,t}$。

3.1.6 协议的安全性证明

根据前述条件，可分别对本文所提协议的 2 个阶段进行相应的安全性证明，得到预期的安全证明目的。

1) 匿名批量认证阶段

① $\text{RSU}_j \lhd\langle y_i,\text{FID}_{V_i},T_{V_i},\beta_i,\delta_i\rangle_{\text{SK}_{V_i}}$。由于此阶段 RSU_j 对 V_i 所发送的消息只起到一个转发作用，此时 RSU_j 并不关心 V_i 所发送消息的可信度，因此该步骤不需要进行安全性证明（对于 V_i 所发送消息

的真实性，RSU_j 会在后续步骤中进行检验）。

② $\mathrm{TA}\lhd\langle\mu_j,\mathrm{FID}_{R_j},T_{R_j},\mathrm{FID}_{V_i},T_{V_i},\beta_i,y_i,y_j,\delta_i\rangle_{\mathrm{SK}_{V_i},\mathrm{SK}_{R_j}}$。此部分可分为 2 个阶段进行证明，首先是 TA 对 RSU_j 的检验，根据 P1：$\mathrm{TA}\mid\equiv\ \mathrm{TA}\xleftrightarrow{\mathrm{SK}_{R_j}}\mathrm{RSU}_j$ 和 L1：$\dfrac{P\mid\equiv P\xleftrightarrow{K}Q,P\lhd\langle X\rangle_K}{P\mid\equiv Q\mid\sim X}$ 可以得到 $\mathrm{TA}\mid\equiv\mathrm{RSU}_j\mid\sim\{\mu_j,\mathrm{FIDR}_j,y_j\}$；当时间戳 T_{R_j} 通过检验后可以得到 $\mathrm{TA}\mid\equiv\#(T_{R_j})$；再根据 L2：$\dfrac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$ 和 L3：$\dfrac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$ 得到 $\mathrm{TA}\mid\equiv\mathrm{RSU}_j\mid\equiv\{\mu_j,\mathrm{FID}_{R_j},y_j\}$；最后根据 L4：$\dfrac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$ 和 P8：$\mathrm{TA}\mid\equiv\mathrm{RSU}_j\mid\Rightarrow\{\mu_j,\mathrm{FID}_{R_j},y_j\}$ 得到 $\mathrm{TA}\mid\equiv\{\mu_j,\mathrm{FID}_{R_j},y_j\}$。然后是 TA 对 V_i 的检验，首先同样根据 L1 和 P2：$\mathrm{TA}\mid\equiv\ \mathrm{TA}\xleftrightarrow{\mathrm{SK}_{V_i}}V_i$ 可以得到 $\mathrm{TA}\mid\equiv V_i\mid\sim\{\mathrm{FID}_{V_i},\beta_i,y_i,\delta_i\}$；再根据 L2 和 L3 得到 $\mathrm{TA}\mid\equiv\ V_i\mid\equiv\{\mathrm{FID}_{V_i},\beta_i,y_i,\delta_i\}$；最后根据 L4 和 P9：$\mathrm{TA}\mid\equiv V_i\mid\Rightarrow\{\mathrm{FID}_{V_i},\beta_i,y_i,\delta_i\}$得到 $\mathrm{TA}\mid\equiv\{\mathrm{FID}_{V_i},\beta_i,y_i,\delta_i\}$。当 TA 完成对 RSU_j 和 V_i 的检验后，TA 继续生成认证确认参数 $\gamma_{\mathrm{TA}},\phi_{\mathrm{TA}}^{V_i}$ 并发送给 RSU_j。

③ $\mathrm{RSU}_j\lhd\langle T_{\mathrm{TA}},\gamma_{\mathrm{TA}},\phi_{\mathrm{TA}}^{V_i}\rangle_{\mathrm{SK}_{R_j},\mathrm{SK}_{V_i}}$。首先根据 L1 和 P3：$\mathrm{RSU}_j\mid\equiv\mathrm{RSU}_j\xleftrightarrow{\mathrm{SK}_{R_j}}\mathrm{TA}$ 可以得到 $\mathrm{RSU}_j\mid\equiv\mathrm{TA}\mid\sim\{\gamma_{\mathrm{TA}}\}$；成功检验时间戳 T_{TA} 后有 $\mathrm{RSU}_j\mid\equiv\#(T_{\mathrm{TA}})$；再根据 L2 和 L3 得出 $\mathrm{RSU}_j\mid\equiv\mathrm{TA}\mid\equiv\{\gamma_{\mathrm{TA}}\}$；最后通过 L4 和 P10：$\mathrm{RSU}_j\mid\equiv\mathrm{TA}\mid\Rightarrow\{\gamma_{\mathrm{TA}}\}$ 可以得到 $\mathrm{RSU}_j\mid\equiv\{\gamma_{\mathrm{TA}}\}$。至此，便实现了最初设定的认证目的 agoal1，即 RSU_j 完成了对 TA 和 V_i 的验证，RSU_j 接收合法化的车辆假名 FID_{V_i} 与公钥 y_i，最后 RSU_j 将自己的公钥、假名以及 $\phi_{\mathrm{TA}}^{V_i}$ 广播给发送认证请求的所有车辆。

④ $V_i\lhd\langle T_{\mathrm{TA}},\phi_{\mathrm{TA}}^{V_i},\mathrm{FID}_{R_j},D_j,y_j\rangle_{\mathrm{SK}_{V_i}}$。根据 L1 和 P4：$V_i\mid\equiv V_i\xleftrightarrow{\mathrm{SK}_{V_i}}\mathrm{TA}$得到 $V_i\mid\equiv\mathrm{RSU}_j\mid\sim\{\phi_{\mathrm{TA}}^{V_i},\mathrm{FID}_{R_j},D_j,y_j\}$；时间戳 T_{TA} 通过验证后得到 $V_i\mid\equiv\#(T_{\mathrm{TA}})$；然后通过 L2 和 L3 得到 $V_i\mid\equiv\mathrm{RSU}_j\mid\equiv\{\phi_{\mathrm{TA}}^{V_i},\mathrm{FID}_{R_j},D_j,y_j\}$；最后根据 L4 和 P11：$V_i\mid\equiv\mathrm{RSU}_j\mid\Rightarrow\{\phi_{\mathrm{TA}}^{V_i},\mathrm{FID}_{R_j},D_j,y_j\}$ 得到 $V_i\mid\equiv\{\phi_{\mathrm{TA}}^{V_i},\ \mathrm{FID}_{R_j},D_j,y_j\}$。至此，便达到了认证目的 agoal2，即 V_i 完成了对 TA 和 RSU_j 的检验，V_i 接收合法化的 RSU_j 假名与公钥，车辆成功完成认证之后则有资格进入组密钥协商阶段。

2) 环状组密钥协商阶段

① $V_i\lhd\langle y_1,y_2,\cdots,y_n,\eta_i,t_{R_j}\rangle_{D_j}$。根据 L1 和 P5：$V_i\mid\equiv V_i\xleftrightarrow{D_j}\mathrm{RSU}_j$得到 $V_i\mid\equiv\mathrm{RSU}_j\mid\sim\{y_1,y_2,\cdots,y_n,\eta_i\}$；在时间戳 t_{R_j} 通过检验后得到 $V_i\mid\equiv\#(t_{R_j})$；再根据 L2 和 L3 得到 $V_i\mid\equiv\mathrm{RSU}_j\mid\equiv\{y_1,y_2,\cdots,y_n,\eta_i\}$；最后通过 L4 和 P12：$V_i\mid\equiv\mathrm{RSU}_j\mid\Rightarrow\{y_1,y_2,\cdots,y_n,\eta_i\}$ 得到 $V_i\mid\equiv\{y_1,y_2,\cdots,y_n,\eta_i\}$。当 V_i 相信了消息 $\{y_1,y_2,\cdots,y_n,\eta_i\}$ 的真实性后，会继续生成用于组密钥协商的相关消息，然后将组密钥协商消息 m_i 发送给 RSU_j。

② $\mathrm{RSU}_j\lhd\langle K_i,t_{V_i},\nu_i,\alpha_i\rangle_{y_i}$。根据 L1 和 P6：$\mathrm{RSU}_j\mid\equiv\mathrm{RSU}_j\xleftrightarrow{y_i}V_i$得到$\mathrm{RSU}_j\mid\equiv V_i\mid\sim\{K_i,\nu_i,\alpha_i\}$；成功验证时间戳 t_{V_i} 后得到 $\mathrm{RSU}_j\mid\equiv\#(t_{V_i})$；再通过 L2 和 L3 得到 $\mathrm{RSU}_j\mid\equiv V_i\mid\equiv\{K_i,\nu_i,\alpha_i\}$；最后根据 L4 和 P13：$\mathrm{RSU}_j\mid\equiv V_i\mid\Rightarrow\{K_i,\nu_i,\alpha_i\}$ 得到 $\mathrm{RSU}_j\mid\equiv\{K_i,\nu_i,\alpha_i\}$。当 RSU_j 认可了接收消息的真实性后，即 $\mathrm{RSU}_j\mid\equiv\alpha_i$，此时便完成了组密钥协商目的 kgoal1，之后 RSU_j 利用合法化的 r_i,y_i 的值生成组密钥 SK_z，然后将组密钥协商确认消息广播给 V_i。

③ $V_i\lhd\langle\mathrm{SK}_{z_i}^{*,t},\tau_i,t'_{R_j}\rangle_{\omega_i}$。根据 L1 和 P7：$V_i\mid\equiv V_i\xleftrightarrow{\omega_i}\mathrm{RSU}_j$得到$V_i\mid\equiv\mathrm{RSU}_j\mid\sim\{\mathrm{SK}_{z_i}^{*,t},\tau_i\}$；成功验证时间戳 t'_{R_j} 后得到 $V_i\mid\equiv\#(t'_{R_j})$；再通过 L2 和 L3 得到 $V_i\mid\equiv\mathrm{RSU}_j\mid\equiv\{\mathrm{SK}_{z_i}^{*,t},\tau_i\}$；最后根据 L4 和 P14：$V_i\mid\equiv\mathrm{RSU}_j\mid\Rightarrow\{\mathrm{SK}_{z_i}^{*,t},\tau_i\}$ 得到 $V_i\mid\equiv\{\mathrm{SK}_{z_i}^{*,t},\tau_i\}$。当 V_i 确认所收到消息合法时，即 $V_i\mid\equiv\mathrm{SK}_{z_i}^{*,t}$，便完成了组密钥协商目的 kgoal2，最后 V_i 解密出合法的组密钥 SK_z，至此，一个安全的会话组便成功建立，组内所有车辆 V_i 与 RSU_j 共享公共会话密钥。

3.2　安全性分析

IoV 系统要求所设计的认证密钥协商协议除了需要进行形式化安全证明外，还需要满足系统中的一些基本安全需求[17-18]，并且应当能够抵御常见恶意攻击[19]。下面分析本文所提协议的安全性。

1) 身份隐私性。身份隐私性表明在整个认证与密钥协商过程中，车辆节点均是以匿名的形式发送消息，只有 TA 有权限揭示出它们的真名。本文所

提协议中，车辆节点 V_i 所发送的每条消息均由假名 FID_{V_i} 进行标识，该假名由系统私钥与单向哈希函数保护，若敌手想要从假名 $\mathrm{FID}_{V_i}=h(\mathrm{ID}_{V_i}\|s)$ 中分析出车辆的真实身份，就必须破解单向哈希函数难题，同时还需要获取 TA 的私钥，然而这种假设成功的概率是可以忽略不计的。因此本文所提协议能够保证身份隐私性。

2) 身份认证性。身份认证性表明消息的接收方能够检验所收到消息的完整性与发送方身份的有效性。在本文所提协议的匿名批量认证阶段，每条消息均由接收方通过哈希值的比对来进行验证，只有通过了的消息才会被接收。需要注意的是，单纯的哈希函数并不能保证消息身份检验，本文所提协议中通过长期会话密钥和安全哈希函数来保证消息中所包含的内容均不能被修改，若敌手想要成功修改消息且不被检测到，那么就要破解基于扩展切比雪夫混沌映射的 DLP 与 CDHP 才能够令接收方完成相关签名验证，事实上敌手破解的概率是忽略不计的。因此本文所提协议具有身份认证性。

3) 消息的不可否认性。当车辆节点 V_i 在系统内发布恶意消息时，若其不在当前 RSU 的会话组内，则组内的其他车辆节点直接拒绝 V_i 所发布的消息；若 V_i 是当前会话组内的合法成员，RSU 查询其所对应的假名 FID_{V_i} 并将其发送给 TA，TA 通过 $\mathrm{FID}_{V_i}=h(\mathrm{ID}_{V_i}\|s)$ 与假名更新种子 $\delta\mathrm{ID}_{V_i}$ 可以追溯出恶意车辆的真实身份 ID_{V_i}，以此来确保所发送消息的不可否认性。

4) 前向与后向安全保密性。在本文所提协议的组密钥协商阶段，只有经过身份认证的车辆才能够参与并成功计算出组内公共会话密钥，未经身份认证的车辆或者敌手均无法计算公共会话密钥。此外，本文的组密钥生成方式为每个车辆与 RSU 所提供的私密值共同参与计算生成，组密钥 $\mathrm{SK}_z^t=h\left((r_1',y_1)\|(r_2',y_2)\|\cdots\|(r_k',y_k)\|(r_j',y_j)\right)$，每当有新车辆加入或者旧车辆离开时，RSU 都会更新自己的私密值然后更新组密钥，任何新加入的车辆、离开的车辆或者敌手都无法通过当前会话密钥 SK_z^t 来推断出 SK_z^{t-1} 或者 SK_z^{t+1}。因此本文所提协议具有前向与后向安全保密性。

5) 抵御重放攻击。重放攻击指敌手通过截获有效消息并对此消息进行重放来使该条消息再次生效，然而实际上这是一条虚假消息。本文所提协议通过设置时间戳检验机制来抵御重放攻击，发送方发送消息时均附带了当前系统时间戳，接收方可以通过检验接收时间是否超过了最大合法时间间隔 ΔT 来判断时间戳的新鲜度。此外，为了应对敌手成功修改时间戳并重放的问题，本文所提协议还额外在哈希签名中加入了时间戳，以此来检验时间戳本身是否受到篡改。因此，本文所提协议除了能够抵御常规重放攻击外，还能够抵御敌手成功修改时间戳的重放攻击。

6) 抵御中间人攻击。中间人攻击指敌手伪造发送方所发送的有效消息，进而与接收方正常通信。本文所提协议中车辆与 RSU 发送消息由假名标识，任何敌手都不可能使用该假名来伪造消息，因为如果想要伪造消息，则敌手必须知道车辆与 RSU 的真实身份以及其与 TA 之间的长期会话密钥，但其是无法破解的，并且长期会话密钥始终处于保密状态，不会泄露给敌手。因此，本文所提协议能够有效抵御中间人攻击。

7) 抵御女巫攻击。女巫攻击指敌手通过创建大量车辆假名身份来发送伪造消息，以此来影响网络的正常运作。在本文所提协议中，车辆在成功完成认证之后其所对应的假名均在 RSU 处得到了合法化，而没有经过认证的车辆假名均不会得到 RSU 的认可，因此当敌手创建大量假名并发送大批伪造消息时，RSU 并不会关注消息本身的可信度，而是直接检验对应假名是否合法，若假名不合法则直接拒绝发送的消息。因此本文所提协议能够有效抵御女巫攻击。

4 仿真与性能对比分析

4.1 计算开销对比分析

本节对本文所提协议在 2 个不同场景下完成批量认证与建立或更新组密钥所需要的计算开销进行分析。在配置为 Intel(R) Core(TM) i5-9500、RAM 为 2.00 GB 的 Win10 环境下，于 VS2010 中使用密码学库 OpenSSL-1.1.1h 对本文所使用的密码学操作进行了模拟，计算得出各项密码学运算平均执行时间，如表 2 所示（本文只考虑了对协议有重要影响的操作，异或运算的时延忽略不计）。其中，T_{h}、T_{se}、T_{sd}、T_{ecc}、T_{cm}、T_{bm}、T_{mo} 分别表示进行一次哈希运算、对称加密、对称解密、椭圆曲线点乘运算、切比雪夫映射、双线性映射、模指数运算所需要的时间。

表 2　　加密操作执行时间

密码学运算	执行时间/ms
T_h(SHA256)	0.008 0
T_{se}(DES/E)	0.018 3
T_{sd}(DES/D)	0.018 2
T_{ecc}	0.051 4
T_{cm}	0.033 6
T_{bm}	1.254 1
T_{mo}	0.173 2

4.1.1　场景 1 下的计算开销对比

场景 1 表示有 k 辆车进入 RSU 的覆盖范围并成功通过认证与密钥协商阶段，最终建立会话密钥。本节对文献[8]、文献[12]、文献[15]和本文所提协议进行了对比，得出了各协议下多辆车完成认证与密钥协商所需要的计算开销，相应的各部分实体与总计算开销如表 3 所示。图 5 展示了存在 10 辆车成功通过各协议的认证与密钥协商阶段后各实体分别需要的计算开销，图 6 显示了不同车辆数下各协议所需的计算开销。

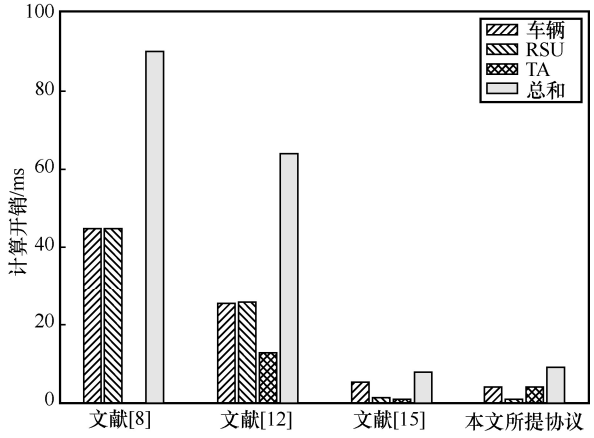


图 5　各协议下的计算开销

从图 5 中可以看到，文献[8]和文献[12]协议所需开销较大，这是因为 2 种协议均频繁使用计算更复杂的双线性对操作来进行签名与验签，浪费了额外的计算资源。本文所提协议与文献[15]协议在车辆数较少时计算开销接近，其中本文所提协议在车辆与 RSU 侧的计算压力更小，而文献[15]协议的优势体现在 TA 的低复杂度。

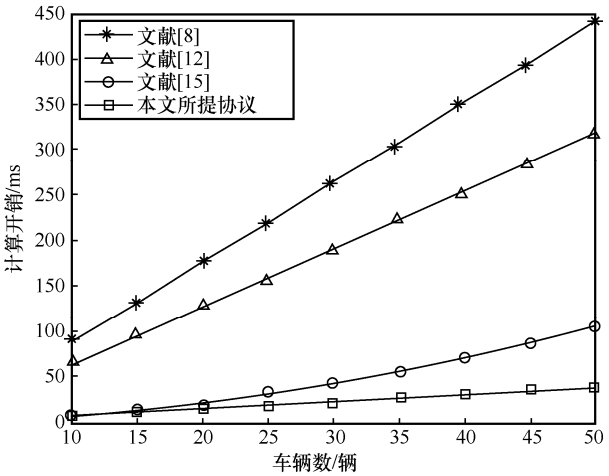


图 6　不同车辆数下各协议所需的计算开销

从图 6 可以看到，本文所提协议在车辆数逐渐增大的过程中与文献[15]协议的计算开销对比产生了明显优势，这是由于本文所提协议更加适合大批车辆同时涌入的情况（环形结构的优势），更符合实际车联网场景，而文献[15]协议仅支持单车辆加入的情况（二叉树的特性所导致），且每当有一辆车加入组内时，所有车辆与 RSU 均要重复计算，因而产生了更大的计算开销。

4.1.2　场景 2 下的计算开销对比

场景 2 为已经成功建立公共会话密钥的车辆离开会话组。本节对文献[15]协议与本文所提协议车辆离开后组密钥更新过程中所产生的计算开销进

表 3　　场景 1 中各协议下的计算开销对比

协议	V_i / ms	RSU/ms	TA/ms	总计算开销/ms
文献[8]	$3kT_{bm}+5kT_h+4kT_{mo}\approx 4.495\,1k$	$(k+3)T_{bm}+(k+5)T_h+(k+5)T_{mo}\approx 4.321\,9k$	—	$8.817\,0k$
文献[12]	$2kT_{bm}+2kT_h+kT_{se}\approx 2.542\,5k$	$2kT_{bm}+2kT_h+kT_{se}+kT_{sd}\approx 2.560\,7k$	$kT_{bm}+3kT_h+kT_{sd}\approx 1.296\,3k$	$6.399\,5k$
文献[15]	$(3.5k+0.5k^2)T_{ecc}+(4k+k^2)T_h\approx 0.211\,9k+0.033\,7k^2$	$4kT_h+(2k+1)T_{ecc}\approx 0.134\,8k+0.051\,4$	$kT_{ecc}+7kT_h\approx 0.107\,4k$	$0.033\,7k^2+0.454\,1k+0.051\,4$
本文所提协议	$5kT_{cm}+7kT_h+kT_{mo}+kT_{sd}\approx 0.415\,4k$	$(k+4)T_{cm}+(6+3k)T_h+kT_{se}\approx 0.075\,9k+0.182\,4$	$(4+2k)T_h+(2k+1)T_{cm}+(k+1)\cdot T_{mo}+T_{bm}\approx 0.256\,4k+1.492\,9$	$0.747\,7k+1.675\,3$

行了对比（由于文献[8]和文献[12]协议并没有考虑密钥更新过程，因此不参与本节的密钥更新开销对比），结果分别如图 7 和图 8 所示。其中，图 7 表示当组内剩余 35 辆车时 2 种协议所需的密钥更新开销，图 8 表示组内剩余车辆数不同时 2 种协议的密钥更新开销。

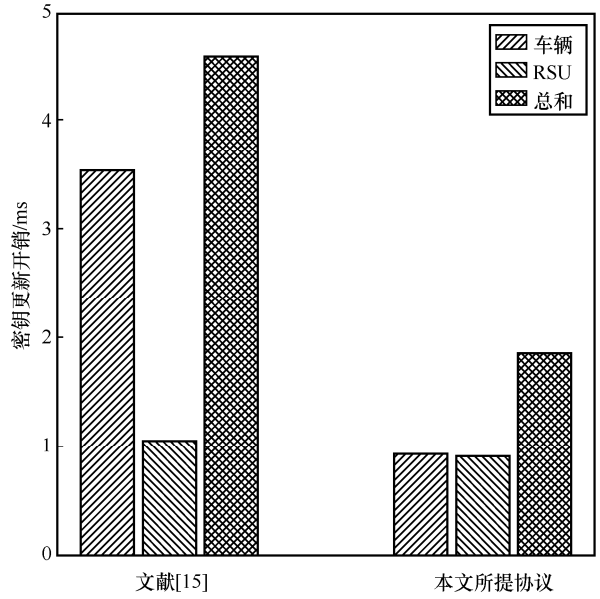


图 7 当组内剩余 35 辆车时 2 种协议所需的密钥更新开销

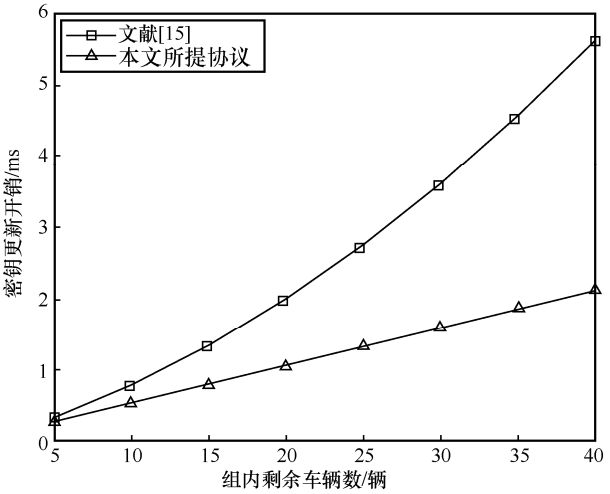


图 8 组内剩余车辆数不同时 2 种协议的密钥更新开销

在文献[15]协议的组密钥更新过程中，考虑在最坏情况下，车辆所需要的最大总密钥更新开销为 $(k-1)T_{ecc}+(1.5k+0.5k^2-1)T_h \approx 0.063\,4k+0.004\,0k^2-0.059\,4$（其中 k 为组内剩余车辆数）；RSU 的最大总密钥更新开销为 $kT_{ecc}+kT_h \approx 0.059\,4k$，而文献[15]协议在最好情况下的开销可以忽略不计，因此车辆的平均更新开销为 $0.031\,7k+0.002\,0k^2-0.029\,7$；RSU 的平均更新开销为 $0.029\,7k$。在本文所提协议中并不区分最好与最差情况，组内剩余车辆总更新开销为 $kT_h+kT_{se} \approx 0.026\,3k$；RSU 总更新开销为 $(k+1)T_h+kT_{se} \approx 0.026\,3k+0.008\,0$。

从图 7 可以看到，本文所提协议拥有更低的密钥更新开销，且主要体现在车辆的更新开销上，这是因为在密钥更新过程中，本文只需要车辆进行较少次数的简单哈希与对称解密运算，而文献[15]协议则需要车辆进行较复杂的椭圆曲线点乘运算与指数次的哈希运算。从图 8 可以看出，本文的密钥更新开销会随着组内剩余车辆数的增长与文献[15]协议产生更大的差距，理由同 4.1.1 节所述。因此，综合场景 1 与场景 2 下的计算开销对比结果，本文所提协议拥有更低的认证与密钥协商计算开销。

4.2 通信开销对比分析

本节对场景 1 下的上述 4 种协议完成会话密钥的建立所需要的通信开销进行了对比，定义 W_h、W_{bm}、W_{mo}、W_{ecc}、W_{ID}、W_T、W_R、W_{cm}、W_{se} 分别表示哈希函数、双线性映射、模指运算、椭圆曲线点乘、用户 ID、时间戳、随机数、切比雪夫映射和对称加密的输出位宽。根据文献[20]，本文假设 $|W_h|$=256 bit，$|W_{bm}|$=1 024 bit，$|W_{mo}|$=512 bit，$|W_{ecc}|$=320 bit，$|W_{ID}|$=256 bit，$|W_T|$=32 bit，$|W_R|$=128 bit，$|W_{cm}|$=480 bit，$|W_{se}|$=128 bit。对比结果如表 4 所示。

表 4 各协议下的通信开销

协议	通信开销/bit
文献[8]	4 416 k
文献[12]	9 504 k
文献[15]	5 568 k
本文所提协议	5 376 k + 2 624

从表 4 可以看出，在文献[8]协议的认证与密钥协商阶段，车辆和 RSU 的通信开销分别为 $(4W_{mo}+W_h+W_R+W_T)k=2\,464k$ 和 $(3W_{mo}+W_h+W_R+W_T)\cdot k=1\,952\,k$。在文献[12]协议的认证与密钥协商阶段，车辆、RSU 和 TA 的通信开销分别为 $(3W_{bm}+2W_R+2W_T)k=3\,392k$、$(3W_{bm}+5W_R++2W_T)k=3\,776k$ 和 $(2W_{bm}+2W_R+W_T)k=2\,336k$。在文献[15]协议的认证与密钥协商阶段，车辆、RSU 和 TA 的通信开销分别为 $(2W_h+2W_{ecc}+W_T)k=1\,184k$、$(2W_{ID}+5W_h+6W_{ecc}+4W_T)\ k=3\,840k$ 和 $(2W_h+W_T)k=544k$。在本

文所提协议的认证与密钥协商阶段，车辆、RSU 和 TA 的通信开销分别为 $(W_{mo}+4W_h+W_{cm}+2W_T+W_R)k=2\,208k$、$(W_{mo}+5W_h+2W_{cm}+W_T+W_{se})k+3W_h+3W_{cm}+4W_T=2\,912k+2\,336$和$(k+1)W_h+W_T=288+256k$。

图 9 给出了存在 10 辆车成功通过认证与密钥协商阶段后各协议所需的通信开销。从图 9 可以看出，文献[12]协议所需通信开销最大，这是因为文献[12]协议在消息发送过程中频繁输出位宽更大的双线性映射结果；文献[8]协议拥有最低的通信开销，因为其 TA 只负责车辆与 RSU 的注册，并不直接参与认证与密钥协商过程，所以开销为 0，但仅由半可信的 RSU 负责车辆认证显然具有更大的安全隐患。本文所提协议与文献[15]协议产生的通信开销接近，这是因为本文所提协议利用切比雪夫映射保障了更快速的认证与密钥协商过程，而切比雪夫映射的输出位宽高于椭圆曲线点乘。相较于文献[15]协议，本文所提协议在 RSU 与 TA 侧的通信开销更具优势，而文献[15]协议则是在车辆侧具有更低的通信开销。

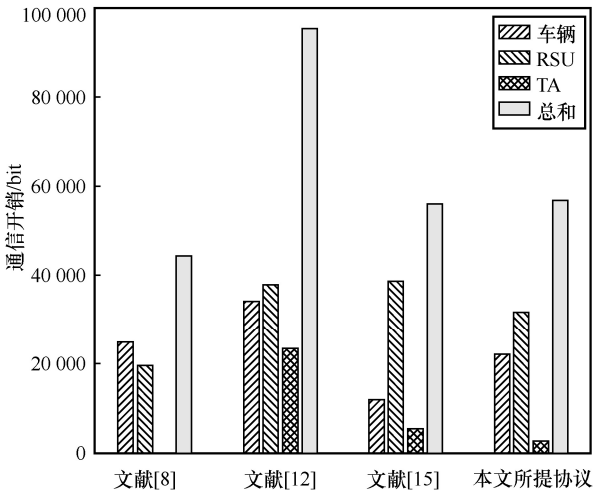


图 9　各协议所需的通信开销

图 10 显示了不同车辆数下各协议所需的通信开销。从图 10 可以看到，本文所提协议与文献[15]协议在车辆数较少时所需通信开销接近，但随着车辆数的增多对比逐渐明显，即本文所提协议在车辆数越大时较文献[15]协议拥有更低的通信开销，这是因为本文所提协议支持多车辆同时加入，因而部分消息不需要重复发送，有效减小了大规模场景下的通信负担。

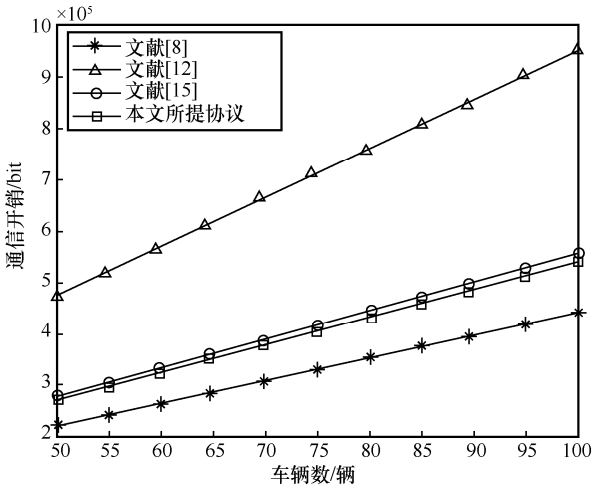


图 10　不同车辆数下各协议所需的通信开销

5　结束语

本文提出了 IoV 中基于环的匿名高效批量认证与组密钥协商协议。利用混沌映射安全构建认证密钥对，通过少许双线性映射快速完成大批车辆的批量验证。环状会话组的设计实现了大规模车辆通信环境下的高效组密钥建立与更新。假名更新与匿名追溯机制确保了车辆间更安全的通信过程。通过 BAN 逻辑模型证明了协议的语义安全性，仿真结果表明，本文所提协议相较于传统协议具有一定的优势。

参考文献：

[1] SHARMA S, KAUSHIK B. A survey on Internet of vehicles: applications, security issues & solutions[J]. Vehicular Communications, 2019, 20: 100182.

[2] JAN M A, KHAN F, MASTORAKIS S, et al. LightIoT: lightweight and secure communication for energy-efficient IoT in health informatics[J]. IEEE Transactions on Green Communications and Networking, 2021, 5(3): 1202-1211.

[3] KHAN F, REHMAN A U, ZHANG Y L, et al. A secured and reliable continuous transmission scheme in cognitive HARQ-aided Internet of things[J]. IEEE Internet of Things Journal, 2021, 8(19): 14835-14844.

[4] ZOU Y L, ZHU J, WANG X B, et al. A survey on wireless security: technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[5] 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.

[6] SUTRALA A K, BAGGA P, DAS A K, et al. On the design of conditional privacy preserving batch verification-based authentication

scheme for Internet of vehicles deployment[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5535-5548.

[7] TZENG S F, HORNG S J, LI T R, et al. Enhancing security and privacy for identity-based batch verification scheme in VANETs[J]. IEEE Transactions on Vehicular Technology, 2017, 66(4): 3235-3248.

[8] 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.

[9] GAYATHRI N B, THUMBUR G, REDDY P V, et al. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks[J]. IEEE Access, 2018, 6: 31808-31819.

[10] HUANG J L, YEH L Y, CHIEN H Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1): 248-262.

[11] ZHANG J, ZHONG H, CUI J, et al. SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 1810-1824.

[12] 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.

[13] XU G Q, LI X T, JIAO L T, et al. BAGKD: a batch authentication and group key distribution protocol for VANETs[J]. IEEE Communications Magazine, 2020, 58(7): 35-41.

[14] KIM Y, PERRIG A, TSUDIK G. Tree-based group key agreement[J]. ACM Transactions on Information and System Security, 2004, 7(1): 60-96.

[15] WEI L, CUI J, ZHONG H, et al. Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs[J]. IEEE Transactions on Mobile Computing, 2022, 21(9): 3280-3297.

[16] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

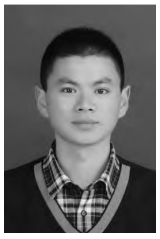
[17] BAGGA P, DAS A K, WAZID M, et al. Authentication protocols in Internet of vehicles: taxonomy, analysis, and challenges[J]. IEEE Access, 2020, 8: 54314-54344.

[18] 杨小东, 陈春霖, 杨平, 等. 可证安全的部分盲代理重签名方案[J]. 通信学报, 2018, 39(2): 65-72.
YANG X D, CHEN C L, YANG P, et al. Partially blind proxy re-signature scheme with proven security[J]. Journal on Communications, 2018, 39(2): 65-72.

[19] LAI C Z, ZHANG M, CAO J, et al. SPIR: a secure and privacy-preserving incentive scheme for reliable real-time map updates[J]. IEEE Internet of Things Journal, 2020, 7(1): 416-428.

[20] JIA X Y, HE D B, KUMAR N, et al. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing[J]. IEEE Systems Journal, 2020, 14(1): 560-571.

[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、安全认证、密钥协商等。

兰凯（1998– ），男，重庆人，重庆邮电大学硕士生，主要研究方向为车联网、安全认证、密钥协商。

陈舟（1999– ），男，四川遂宁人，重庆邮电大学硕士生，主要研究方向为车联网、认证协议、密钥协商。

王汝言（1969– ），男，湖北浠水人，博士，重庆邮电大学教授、博士生导师，主要研究方向为泛在网络、多媒体信息处理等。

邹灿（1982– ），男，重庆人，三六零数字安全科技集团有限公司工程师，主要研究方向为大数据、信息安全、数字经济。

王明月（1990– ），女，重庆人，重庆邮电大学博士生，主要研究方向为移动通信安全技术。