VANET 系统中基于中国剩余定理的群内相互认证密钥协商协议

张海波[1,2]，陈舟[1,2]，黄宏武[1,2]，贺晓帆[3]

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

摘 要：针对车载自组网（VANET）系统中车辆在公开网络上相互通信容易受到恶意攻击的问题，提出一种 VANET 系统中群内相互认证密钥协商协议。利用中国剩余定理建立动态车辆群，以适应 VANET 拓扑的快速变化。通信双方利用签名信息快速认证消息发送方的身份，并通过切比雪夫混沌映射的半群性进行密钥协商。采用假名更新和私钥更新机制，保护车辆的身份隐私安全。对于恶意车辆的身份，利用签名信息进行准确追溯，并通过修改公钥信息实现快速撤销。此外，使用 BAN 逻辑模型证明了协议的语义安全。仿真结果表明，所提协议相较于现有同类方案，能有效降低通信消耗，并显著降低计算消耗。

关键词：车载自组网；认证密钥协商；中国剩余定理；切比雪夫映射

中图分类号：U495

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022002

Intra-group mutual authentication key agreement protocol based on Chinese remainder theorem in VANET system

ZHANG Haibo[1,2], CHEN Zhou[1,2], HUANG Hongwu[1,2], HE Xiaofan[3]

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

Abstract: Aiming at the problem that vehicles in the vehicular ad-hoc network (VANET) system were vulnerable to malicious attacks when communicating with each other on the public network, a mutual authentication key agreement protocol in the VANET was proposed. A dynamic vehicle group was established by the Chinese remainder theorem to adapt to the rapid changes in the VANET topology. Signature information was used by both parties in communication to quickly authenticate the identity of the message sender, and key agreement was conduct through the semigroup of Chebyshev chaotic mapping. The pseudonym update and private key update mechanism were adopted to protect the privacy and security of the vehicle's identity. The identities of malicious vehicles were tracked accurately by using signature information, and were revoked quickly by modifying the public key information. In addition, the semantic security of the protocol was proved by the BAN logic model. The simulation results show that the proposed protocol can effectively reduce the communication consumption and significantly reduce the computational consumption compared with the existing similar literature.

Keywords: VANET, authentication key agreement, Chinese remainder theorem, Chebyshev map

---

收稿日期：2021−09−12；**修回日期：**2021−12−09

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

Foundation Items: The National Natural Science Foundation of China (No.61801065), 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

无线通信和汽车技术的飞速发展，促进了智能交通系统（ITS, intelligent transportation system）的发展。VANET（vehicular ad-hoc network）系统作为 ITS 的重要组成部分，能够为车辆节点提供当前驾驶路面情况、交通拥塞状况和天气情况等辅助信息，使车辆驾驶员能够更加安全便捷地驾驶车辆[1]。VANET 系统主要包括 3 种实体：可信机构（TA, trusted authority）、路边单元（RSU, road side unit）和车载单元（OBU, on broad units）。TA 负责 RSU 以及 OBU 的注册，是一个完全可信的机构。RSU 是 TA 与车辆之间的桥梁，安装在道路的两侧，方便车辆的快速访问。OBU 负责车辆的计算任务和无线通信服务。

VANET 系统使用专用短程通信（DSRC, dedicated short range communication）协议进行通信[2]，DSRC 协议符合 IEEE 802.11p 标准。VANET 系统主要的通信方式分为 2 种：车辆与车辆（V2V, vehicle-to-vehicle）、车辆与基础设施（V2I, vehicle-to-infrastructure）。V2V 和 V2I 都是在公开的无线信道上进行通信的，所以在 VANET 系统中进行信息传输时很容易受到恶意者的攻击，例如窃听、仿冒、重放攻击等[3]。恶意者的攻击行为使 VANET 系统中的通信隐私安全受到威胁。同时，与其他静态的网络结构相比，VANET 系统具有车辆高速移动和快速的网络拓扑变化的特性，这使 VANET 系统的隐私安全更容易受到恶意者的破坏[4]。

认证密钥协商（AKA, authentication key agreement）协议能够使参与者在公开的网络上完成相互认证并建立安全的会话密钥，以保护通信双方的隐私安全。许多学者对 AKA 技术做了大量研究工作，并提出了很多有价值的方案。传统的基于公钥基础设施（PKI, public key infrastructure）方案[5-6]，以数字证书为媒介，结合对称与非对称加密技术，将用户的身份和公钥等信息捆绑在一起，从而确保消息的完整性、身份认证和不可否认性。但是该方案需要管理大量的匿名证书和撤销列表，存储开销非常大；且该方案的证书验证过程涉及的节点数量较多，比较烦琐，导致该方案认证效率比较低。为避免基于 PKI 技术带来的管理大量匿名证书和撤销列表的难题，Shamir[7]引入了基于身份基础设施的方案。身份基础设施由用户身份信息和一个可信的拥有用户密钥对的私钥生成中心（PKG, private key generator）组成，允许用户很容易地从自己的身份信息（例如电子邮箱、手机号码等）中获取公钥，再由 PKG 为用户颁发私钥，这样就减轻管理大量证书带来的开销。基于区块链[8-9]的密钥协商方案通过利用区块链的优势，如可审计的日志、分散的体系结构和拒绝服务（DoS, denial of service），在保护用户隐私的同时提供了用户间的相互认证和密钥协商。但是基于区块链的认证密钥协商方案很少考虑成员动态变化的因素，无法应对 VANET 拓扑快速变化的特性。无证书非对称的群密钥协商方案[10-11]提供了一个公开的加密密钥，每个群成员都可以计算一个对应的解密密钥，并且只有群成员才能正确解密通过公钥加密的信息。该方案可以实现成员间的相互认证和密钥协商。但是该方案没有考虑成员的身份可追溯性和可撤销性，无法处理群成员的恶意行为。

许多学者对中国剩余定理（CRT, Chinese remainder theorem）在身份认证和密钥协商中的应用也进行了大量研究。文献[12]基于 CRT 提出了 2 种群签名方案，可信机构利用群成员的部分签名生成群签名，方案的安全性依赖于整数难分解、离散对数和椭圆曲线离散对数难题。文献[13]提出了一种基于 CRT 的车载自组网中条件隐私保护认证方案，利用CRT的密钥管理方案为TA侧的每个车辆生成一个通用域密钥，降低了 TA 的计算复杂度。

混沌系统具有对初始条件、伪随机性和遍历性十分敏感的特性，并具有良好的扩散和混淆特性，这对密码学特别是密钥系统有重要意义[14]。Kocarev 等[15]提出了一种基于切比雪夫混沌映射的公钥加密协议，由于切比雪夫混沌映射的数学特性，在公钥密码体制中使用切比雪夫混沌映射是一种更加安全的方法。Cui 等[16]提出了一种车载自组网中基于混沌映射的全会话密钥协商方案，利用扩展的切比雪夫多项式建立公钥，实现了雾服务器和车辆群管理者之间的安全会话。

综上所述，现有文献提出的 VANET 系统中的认证密钥协商方案大多对车辆的匿名性、可追溯性和撤销性等安全问题考虑不全面，并且很少考虑 VANET 拓扑的动态变化。本文针对上述问题，结合中国剩余定理和切比雪夫混沌映射，提出了一种 VANET 系统中群内相互认证密钥协商协议。本文的主要贡献如下。

1) 提出了一种基于CRT的动态车辆群建立方案。TA 利用分配给车辆节点的素数信息和车辆节点返回的公钥信息，再结合 CRT 建立动态车辆群。新车辆节点加入时，群内成员不需要改变自己的私钥，只需要 TA 重新计算系统公钥。车辆离开车辆群或 TA 撤销车辆节点时，TA 将其对应的公钥信息修改即可。

2) 提出了一种基于切比雪夫混沌映射的密钥协商协议。密钥协商双方通过访问 RSU 获取对方的素数信息，并通过获取的素数认证对方的身份。密钥协商发起方利用切比雪夫映射产生密钥协商信息。接收方认证发起方对应的车辆身份后，利用切比雪夫混沌映射生成密钥协商回应信息。本文通过 BAN 逻辑模型证明了所提协议的语义安全性。

3) 安全分析结果表明，和现有的文献相比较，本文提出的认证密钥协商协议对车辆节点的身份认证性、身份隐私性和不可否认性等 VANET 系统中的通信安全问题考虑更加全面，还考虑了 VANET 拓扑动态变化的特性。仿真结果表明，本文所提协议能有效降低通信消耗，并且显著减少了计算开销。

1 预备知识

1.1 系统模型

本文提出的 AKA 协议的系统模型如图 1 所示。该模型中的 VANET 主要由 3 个实体组成，即 TA、RSU 和 OBU。

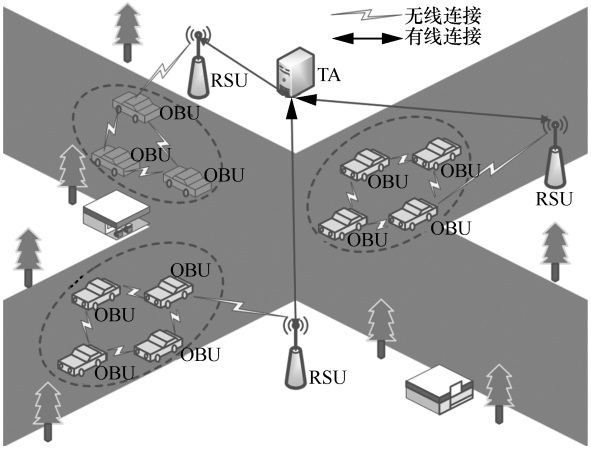


图 1 AKA 协议的系统模型

TA。TA 拥有强大的计算能力、存储能力，是一个完全可信的机构。在 VANET 系统中，合法的 RSU 和 OBU 都需要在 TA 进行注册，然后 TA 为注册实体分配参数。当有新的车辆节点加入车辆群或车辆节点离开车辆群使 VANET 拓扑发生改变时，TA 会实时更新系统公钥。当有注册车辆进行恶意行为时，TA 会对该车辆的身份进行追溯并撤销其合法身份。

RSU。RSU 安装在道路的两侧，连接车辆和可信中心。RSU 负责管理车辆假名和素数信息表；当车辆通过 RSU 的验证后，可以得到密钥协商对象的素数。相邻 RSU 之间也可以进行通信，当车辆群进行下一个 RSU 覆盖范围时，当前 RSU 将假名和素数信息表发送给下一个 RSU。

OBU。每一个车辆都配备一个 OBU，OBU 负责车辆的通信和计算任务。

1.2 安全性假设

本文提出的认证密钥协商协议的安全性基于 2 种难破解问题，即计算离散对数问题（CDLP, computational discrete logarithm problem）和 Zhang[17]提出的基于扩展切比雪夫混沌映射的计算 Diffie-Hellman 问题（CDHP, computational Diffie-Hellman problem）。

CDLP。给定一个 P 阶有限循环乘法群 $G=\langle g\rangle$，P 是一个大素数，$g_1,g_2,\cdots,g_n$ 是乘法群 G 的生成元。选定任意乘法群 G 的生成元 g 和 y，计算 x 满足 $y=g^x$，其中 $0\leqslant x\leqslant|G|$。

基于扩展切比雪夫混沌映射的 CDHP。给定 3 个参数 $x\in(-\infty,+\infty)$、$T_\alpha(x)\bmod n$ 和 $T_\beta(x)\bmod n$。其中 n 是一个大素数。计算 $T_{\alpha\beta}(x)\bmod P$。

通常情况下，想要在多项式时间内解决 CDLP 和基于扩展切比雪夫混沌映射的 CDHP 是非常困难的。这 2 种难破解问题在密码学中的应用十分广泛，例如数字签名技术、匿名认证技术和密钥协商等。

2 VANET 系统中的 AKA 协议

为满足 VANET 系统中车辆间安全通信的需求，本文提出的 AKA 协议包含 7 个阶段，即系统初始化阶段、注册阶段、相互认证和密钥协商阶段、VANET 拓扑变化阶段、私钥更新阶段、假名更新阶段、RSU 切换阶段。协议涉及的参数及定义如表 1 所示。

2.1 系统初始化阶段

TA 负责系统初始化，定义 2 个单向哈希函数 $H_0,H_1:\{0,1\}^*\to\{0,1\}^{l_i},i\in\{0,1\}$，$l_i$ 为哈希函数输出的位宽。对于切比雪夫混沌映射，TA 选择公共参数 x、大素数 n 和系统私钥 δ_{sk}。

表 1　协议涉及的参数及定义

参数	含义
n	一个大素数
H_0, H_1	哈希运算
δ_{sk}	系统私钥
V_i	车辆节点
OBU_i	车辆 V_i 的 OBU
RSU_i	第 i 个路边单元 RSU
IDV_i	车辆 V_i 的身份
IDR_i	路边单元 RSU_i 的身份
$SIDV_i$	车辆 V_i 假名
$SIDR_i$	路边单元 RSU_i 的假名
p_i	TA 分配给车辆 V_i 的大素数
y_i	车辆 V_i 对应的公钥
$x_{i,0}$	车辆 V_i 在第 0 个时间片段对应的私钥
SP_i	车辆 V_i 的假名和素数的哈希运算输出值
S_i^1, S_i^2	车辆 V_i 对密钥协商消息的签名
T_{vi}, T_{vj}	时间戳
sk	会话密钥

2.2　注册阶段

RSU_i 和车辆的 OBU_i 在 TA 完成注册后身份才合法。

1) OBU_i 的注册

假设现有一个车辆群，该群里现在有 k 个车辆成员 $\{V_1, V_2, \cdots, V_k\}$。车辆节点 V_i 在进行身份注册时，V_i 上的 OBU_i 将 V_i 的真实身份 IDV_i 通过安全信道发送给 TA。TA 收到消息后，计算 V_i 的假名 $SIDV_i = H_0(IDV_i \| \delta_{sk})$ 并公布在整个系统中。TA 选择一个大素数 $p_i (i = 1, 2, \cdots, k)$，满足 $i \neq j$ 时 $p_i \neq p_j$，且在 $p_i - 1$ 中有 2 个大素数。TA 选择系统公共参数 g，g 是指数运算的原根，也是所有乘法群 $Z_{p_i}^* (i = 1, 2, \cdots, k)$ 的生成元。TA 将 $\{SIDV_i, p_i\}$ 通过安全信道发送给 V_i。

V_i 收到 TA 发来的 $\{SIDV_i, p_i\}$ 后，随机选择自己初始密码 $x_{i,0} \in Z_{p_i}^*$，计算 V_i 的公钥 $y_i \equiv g^{x_{i,0}} \cdot \bmod p_i$。$V_i$ 将 $\{y_i\}$ 通过安全信道发送给 TA。TA 将车辆群内车辆的公钥的有效时间划分为 L 个时间片段，在 L 个时间片段内，车辆节点的公钥 y_i 保持不变。当 L 个时间片段用完时，V_i 会重新选择私钥 $x_{i,0}^{'}$ 并重新计算公钥 y_i，TA 也会更新系统公钥 c。

2) RSU_i 的注册

RSU_i 的注册过程和 OBU_i 的注册过程类似，将真实身份 IDR_i 通过安全信道发送给 TA，TA 计算 RSU_i 的假名 $SIDR_i = H_0(IDR_i \| \delta_{sk})$，并分配给 RSU_i 一个大素数 p_{k+1}。RSU_i 选择私钥 $x_{k+1,0} \in Z_{p_{k+1}}^*$，并计算对应公钥 y_{k+1} 返回给 TA。

3) TA 构建群组

TA 根据接收到的来自 k 个车辆节点的 $y_i (i = 1, 2, \cdots, k)$ 和来自 RSU_i 的 y_{k+1} 构建同余方程组。

$$\begin{cases} c \equiv y_1 (\bmod p_1) \\ c \equiv y_2 (\bmod p_2) \\ \quad \vdots \\ c \equiv y_k (\bmod p_k) \\ c \equiv y_{k+1} (\bmod p_{k+1}) \end{cases} \tag{1}$$

其中，c 为系统公钥，利用中国剩余定理可以计算该同余方程组为

$$c \equiv \sum_{i=1}^{k+1} y_i \frac{P}{p_i} \left[\left(\frac{P}{p_i} \right)^{-1} \right]_{p_i} (\bmod P) \tag{2}$$

其中，$P = p_1 p_2 \cdots p_{k+1}$，$\left[\left(\frac{P}{p_i} \right)^{-1} \right]_{p_i}$ 表示 $\frac{P}{p_i}$ 对 p_i 取模的逆。TA 计算 $SP_i = H_1(SIDV_i \| p_i)$，并将 $\{SIDV_i, p_i\}$ 发送给经过注册的 RSU_i。RSU_i 根据收到的 $\{SIDV_i, p_i\}$ 生成一个 V_i 假名和素数对应的列表 $\lambda_{SIDV,p}$。

根据上面的描述，系统公布的参数为 $\{x, n, g, SIDV_i, SIDR_i, c, P, SP_i\}$。

2.3　相互认证和密钥协商阶段

在该阶段，车辆节点 V_i 和 V_j 在公开网络上完成相互认证和密钥协商，流程如图 2 所示。具体步骤如下。

Step1　V_i 通过发送请求给 RSU_i 来获取 V_j 的素数 p_j。V_i 选择时间戳 T_{vi}，计算 $B_{vi} = H_1(SIDV_i \| p_i \| T_{vi})$、$AIDV_i = SIDV_i \oplus H_1(p_i \| T_{vi})$，然后发送 $\{B_{vi}, T_{vi}, AIDV_i, SIDV_j\}$ 给 RSU_i。

Step2　RSU_i 对接收到的消息进行验证。RSU_i 收到消息后，首先通过 $T_{Ri} - T_{vi} < \Delta t$ 检查 T_{vi} 的新鲜度。检验通过后，计算 $SIDV_i' = AIDV_i \oplus H_1(p_i \| T_{vi})$，通过判断等式 $B_{vi}' = H_1(SIDV_i' \| p_i \| T_{vi}) = B_{vi}$ 是否成立，判断消息请求方身份的合法性，只有群内成员

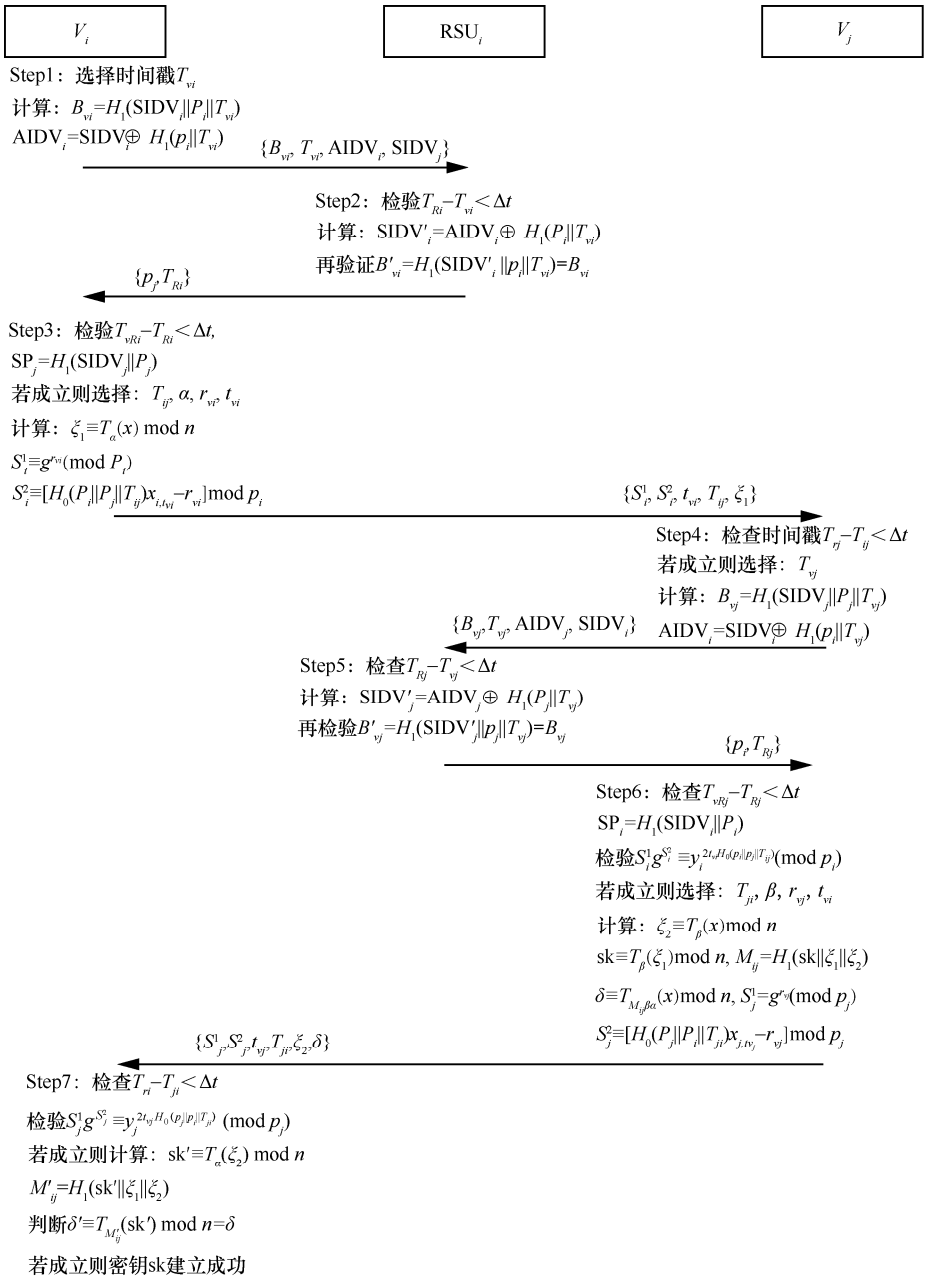


图 2　认证密钥协商流程

才能通过验证。如果等式不成立，拒绝请求消息；如果等式成立，RSU$_i$ 将$\{p_j, T_{Ri}\}$发送给V_i。

Step3　V_i验证来自RSU$_i$的消息，并发送密钥协商请求消息给V_j。V_i收到$\{p_j, T_{Ri}\}$后，首先由$T_{vRi}-T_{Ri}<\Delta t$检验时间戳T_{Ri}的新鲜度，T_{vRi}是系统当前时间戳。然后通过等式$\mathrm{SP}_j=H_1(\mathrm{SIDV}_j\|p_j)$是否成立来判断来自RSU$_i$消息的正确性。验证通过后，$V_i$选择当前时间戳$T_{ij}$，选择随机数$\alpha$，计算$\xi_1\equiv T_\alpha(x) \bmod n$。$V_i$对密钥协商请求进行签名，随机选择$r_{vi}\in Z_{p_i}^*$，确定时间片段$t_{vi}$，计算$S_i^1\equiv g^{r_{vi}} (\mathrm{mod}\ p_i)$和$S_i^2\equiv[H_0(p_i\|p_j\|T_{ij})x_{i,t_{vi}}-r_{vi}] \bmod p_i$。$V_i$将签名消息$\{S_i^1, S_i^2, t_{vi}, T_{ij}, \xi_1\}$发送给$V_j$。

Step4　V_j检查来自V_i消息的时间戳，然后向RSU$_i$访问V_i对应的素数p_i。V_j收到消息后，通过$T_{rj}-T_{ij}<\Delta t$检验T_{ij}的新鲜度，T_{rj}是系统当前时间戳。验证通过后，生成时间戳T_{vj}，计算$B_{vj}=H_1(\mathrm{SIDV}_j\|p_j\|T_{vj})$、$\mathrm{AIDV}_j=\mathrm{SIDV}_j\oplus H_1(p_j\|$

T_{vj})。V_j 发送素数请求消息 $\{B_{vj}, T_{vj}, \mathrm{AIDV}_j, \mathrm{SIDV}_i\}$ 给 RSU_i。

Step5　RSU_i 对接收到的消息进行验证。RSU_i 收到消息后，首先通过 $T_{Rj} - T_{vj} < \Delta t$ 检查时间戳 T_{vj} 的新鲜度，T_{Rj} 是系统当前时间戳。检验通过后，计算 $\mathrm{SIDV}_j' = \mathrm{AIDV}_j \oplus H_1(p_j \| T_{vj})$，通过等式 $B_{vj}' = H_1(\mathrm{SIDV}_j' \| p_j \| T_{vj}) = B_{vj}$ 是否成立判断消息请求方身份的合法性。如果等式不成立，拒绝请求消息；若成立，RSU_i 将 $\{p_i, T_{Rj}\}$ 发送给 V_j。

Step6　V_j 验证来自 RSU_i 的消息，然后对 V_i 的身份进行认证，最后发送密钥协商消息给 V_i。V_j 通过 $T_{vRj} - T_{Rj} < \Delta t$ 判断时间戳 T_{Rj} 的新鲜度，T_{Rj} 是系统当前时间戳。通过等式 $\mathrm{SP}_i = H_1(\mathrm{SIDV}_i \| p_i)$ 判断来自 RSU_i 素数的正确性。验证通过后，对 V_i 的身份信息进行认证，具体方法如下：计算 $y_i \equiv c(\mathrm{mod}\, p_i)$，判断等式 $S_i^1 g^{S_i^2} \equiv y_i^{2t_{vi}H_0(p_i \| p_j \| T_{ij})} \pmod{p_i}$ 是否成立。如果等式不成立，拒绝来自 V_i 的密钥协商请求。如果等式成立，V_j 随机选择 β 和时间戳 T_{ji}，计算 $\xi_2 \equiv T_\beta(x) \bmod n$，$\mathrm{sk} \equiv T_\beta(\xi_1) \bmod n$，$M_{ij} = H_1(\mathrm{sk} \| \xi_1 \| \xi_2)$，$\delta \equiv T_{M_{ij}\beta\alpha}(x) \bmod n$。然后，$V_j$ 对密钥协商消息进行签名，随机选择 $r_{vj} \in Z_{p_j}^*$，确定时间片段 t_{vj}，计算 $S_j^1 \equiv g^{r_{vj}} (\mathrm{mod}\, p_j)$ 和 $S_j^2 \equiv [H_0(p_j \| p_i \| T_{ji}) x_{j,t_{vj}} - r_{vj}] \bmod p_j$。$V_j$ 发送消息 $\{S_j^1, S_j^2, t_{vj}, T_{ji}, \xi_2, \delta\}$ 给 V_i。

Step7　V_i 检验 V_j 的密钥协商消息，检验通过后，会话密钥建立成功。V_i 首先通过 $T_{ri} - T_{ji} < \Delta t$ 对时间戳 T_{ji} 进行检验，T_{ri} 是系统当前时间戳。时间戳检验通过后，再认证 V_j 的身份，即判断 $S_j^1 g^{S_j^2} \equiv y_j^{2t_{vj}H_0(p_j \| p_i \| T_{ji})} (\mathrm{mod}\, p_j)$ 是否成立。认证通过后，计算 $\mathrm{sk}' \equiv T_\alpha(\xi_2) \bmod n$ 和 $M_{ij}' = H_1(\mathrm{sk}' \| \xi_1 \| \xi_2)$，判断等式 $\delta' \equiv T_{M_{ij}'}(\mathrm{sk}') \bmod n = \delta$ 成立。若成立 V_i, V_j 之间会话密钥协商成功，会话密钥即为 $\mathrm{sk} \equiv T_\alpha(T_\beta(x)) \bmod n = T_\beta(T_\alpha(x)) \bmod n$。

2.4　VANET 拓扑变化阶段

1) 车辆节点的加入

当新的车辆节点 V_{k+2} 想要成为车辆群的一员时，V_{k+2} 首先需要向 TA 发送加入请求。TA 接收到 V_{k+2} 的请求后，选择新的大素数 p_{k+2} 发送给 V_{k+2}，并确保 g 是 $Z_{p_{k+2}}^*$ 的生成元。V_{k+2} 接收到 p_{k+2} 后，随机选择初始密钥 $x_{k+2,0} \in Z_{p_{k+2}}^*$，计算公钥 $y_{k+2} \equiv g^{x_{k+2,0}} \cdot (\mathrm{mod}\, p_{k+2})$ 并发送给 TA。TA 收到 y_{k+2} 后对系统公钥 c 进行更新，并将 $\{\mathrm{SIDV}_{k+2}, p_{k+2}\}$ 发送给 RSU。此时 V_{k+2} 就成为车辆群的一员。

从 V_{k+2} 的加入过程可以发现，新的车辆节点的加入，不会导致原始群内车辆的密钥发生改变，TA 只需要重新计算 c。

2) 车辆节点的追溯与撤销

当经过注册的车辆节点 V_i 在车辆群内发布恶意消息时，TA 会对其合法身份进行追溯和撤销。V_i 在 RSU_i 覆盖范围内发布恶意消息时，RSU_i 首先获取 V_i 在发送恶意消息使用的 p_i，然后在假名和素数列表 $\lambda_{\mathrm{SIDV},p}$ 中找到 TA 为 V_i 生成的当前假名。得到 V_i 的当前假名 SIDV_i 后，发送假名 SIDV_i 和 p_i 给 TA。TA 通过等式 $H_0(\mathrm{IDV}_i \| \delta_{\mathrm{sk}}) = \mathrm{SIDV}_i$、$p_i$ 对应的 l 和假名更新种子 $\delta \mathrm{ID}_i$ 判断该假名对应车辆的真实身份。获取 V_i 的真实身份后，TA 将会对 V_i 在群内的合法身份进行撤销。此外，当经过注册的合法车辆节点 V_j 离开 TA 建立的车辆节点群时，TA 也会撤销 V_j 的身份。

TA 撤销群成员 V_i 在群内的合法身份，只需要将 V_i 对应的公钥信息 y_i 修改为另一个随机数 y_i'，其他车辆节点信息保持不变，然后更新系统公钥 c。此时 V_i 就被撤销了，其密钥将不能生成有效的密钥协商信息。

从撤销 V_i 的过程看，如果系统想要撤销一个车辆节点，TA 只需要改变 V_i 对应的公钥并重新计算 c。

2.5　私钥更新阶段

V_i 在第 t_{vi} 个时间片段的私钥为 $x_{i,t_{vi}}$，则在 $t_{vi}+1$ 个时间片段内 V_i 的私钥为 $x_{i,t_{vi}+1} \equiv x_{i,t_{vi}}^2 (\mathrm{mod}\, p_i)$。当 $t_{vi}+1$ 个时间片段对应的私钥生成后，OBU_i 会立刻将第 t_{vi} 个时间片段的私钥删除。若 $t_{vi} = L$，车辆节点 V_i 输出的第 $t_{vi}+1$ 个时间片段的密钥为空串。当 V_i 的时间片段用完时，V_i 重新选择私钥 $x_{i,0}'$ 并重新计算对应公钥 y_i，TA 也会更新系统公钥 c。

2.6　假名更新阶段

如果车辆自始至终都使用一个假名，这个假名就会被视为该车辆对应的真名。攻击者通过收集该车辆假名对应的信息，就可以对该车辆进行攻击。

为了解决使用固定假名导致的安全问题，本文采用假名更新方案对车辆对应假名进行更新。TA 给每一个注册车辆都分配一个假名更新种子 $\delta\mathrm{ID}_i$，当车辆节点 V_i 访问 V_j 当前假名 SIDV_j^l 对应的素数后，RSU 向 TA 发送假名更新请求，TA 计算 V_j 对应的下一个假名 $\mathrm{SIDV}_j^{l+1}=H_0(\mathrm{SIDV}_j^l \| \delta\mathrm{ID}_j)$ 并公布，记录对应的素数 p_j 和 l。然后将假名素数对应列表 $\{\mathrm{SIDV}_j^{l+1}, p_j\}$ 发送给 RSU。

2.7 RSU 切换阶段

本文协议中的车辆节点的假名和素数对应表 $\lambda_{\mathrm{SIDV},p}$ 由 RSU 直接存储和维护，车辆节点不需要通过访问 TA 获取 $\lambda_{\mathrm{SIDV},p}$，而是直接通过访问 RSU 获取。当车辆节点 V_i 从 RSU_i 覆盖的区域进入经过注册的 RSU_j 覆盖的区域后，V_i 向 RSU_j 发送获取 V_j 的素数的请求，$\lambda_{\mathrm{SIDV},p}$ 在 RSU 间的传递如图 3 所示。

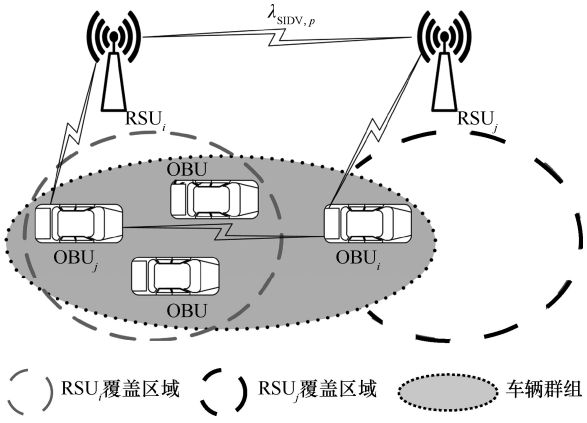


图 3 $\lambda_{\mathrm{SIDV},p}$ 在 RSU 间的传递

3 安全性证明与分析

3.1 协议安全的形式化证明

BAN 逻辑[18]由 Burrows、Abadi 和 Needham 提出，主要用于对认证协议的可靠性形式化证明，来确定信息交换面对任何恶意节点时是否安全。本节通过 BAN 逻辑对本文提出的认证密钥协商协议的安全性进行证明。

1) BAN 逻辑符号

在对本文协议安全证明过程中，使用的 BAN 逻辑符号如下。

① $P \models X$：P 相信消息 X 是真实可信的。

② $P \lhd X$：P 发现一条包含 X 的消息。

③ $P \mid\sim X$：P 在某个时间段发送过包含 X 的消息。

④ $P \mid\Rightarrow X$：P 拥有消息 X 的管辖权。

⑤ $\#(X)$：消息 X 是新鲜的。

⑥ (X,Y)：X 和 Y 是消息 (X,Y) 的一部分。

⑦ $\langle X\rangle_Y$：使用密钥 Y 加密消息 X。

⑧ $P \overset{K}{\longleftrightarrow} Q$：$K$ 是 P 和 Q 共享的密钥。

2) BAN 逻辑规则

本文使用 4 个 BAN 逻辑规则 R1～R4 对协议安全进行形式化证明。

① 信息含义（message-meaning）规则

R1：$\dfrac{P \models P \overset{K}{\longleftrightarrow} Q, P \lhd \langle X\rangle_K}{P \models Q \mid\sim X}$。R1 表示如果 P 相信 P 和 Q 之间共享的密钥 K，并发现 K 对消息 X 进行加密。P 就会相信 Q 曾经发送过 X。

② 随机数证明（nonce-verification）规则

R2：$\dfrac{P \models \#(X), P \models Q \mid\sim X}{P \models Q \models X}$。R2 表示如果 P 相信 X 是新鲜的，并且 P 相信 Q 曾经发送过 X。那么 P 相信 Q 是相信 X 的。

③ 管辖权（jurisdiction）规则

R3：$\dfrac{P \models Q \mid\Rightarrow X, P \models Q \models X}{P \models X}$。R3 表示如果 P 相信 Q 对 X 有管辖权，并且 P 相信 Q 是相信 X 的。那么 P 就会相信 X。

④ 新鲜度（freshness）规则

R4：$\dfrac{P \models \#(X)}{P \models \#(X,Y)}$。R4 表示如果 P 相信消息 (X,Y) 的一部分 (X) 是新鲜的，那么 P 相信 (X,Y) 也是新鲜的。

3) 建立 2 个协议安全证明目标

为了表明群内车辆节点相互认证密钥协商是安全的，需要实现 2 个协议安全证明目标 Goal1 和 Goal2。

Goal1：$V_j \models \xi_1$。V_j 相信 V_i 发来的密钥协商信息。

Goal2：$V_i \models \xi_2$。V_i 相信 V_j 发来的密钥协商信息。

4) 理想化协议形式

将 2.3 节认证和密钥协商协议流程的普遍形式转化为理想化形式。

① $\mathrm{RSU}_i \lhd \langle B_{vi}, T_{vi}, \mathrm{AIDV}_i, \mathrm{SIDV}_j\rangle_{p_i}$。

② $V_i \lhd \langle p_j, T_{Ri}\rangle_{\mathrm{SP}_j}$。

③ $\mathrm{RSU}_i \lhd \langle B_{vj}, T_{vj}, \mathrm{AIDV}_j, \mathrm{SIDV}_i\rangle_{p_j}$。

④ $V_j \triangleleft \langle p_i, T_{Rj} \rangle_{\mathrm{SP}_i}$。

⑤ $V_j \triangleleft \langle S_i^1, S_i^2, t_{vi}, T_{ij}, \xi_1 \rangle_{p_i, p_j}$。

⑥ $V_i \triangleleft \langle S_j^1, S_j^2, t_{vj}, T_{ji}, \xi_2, \delta \rangle_{p_i, p_j}$。

5) 前提假设

在对协议进行安全证明之前，需要对 BAN 逻辑做出如下假设。

P1：$\mathrm{RSU}_i \mid\equiv \mathrm{RSU}_i \xleftrightarrow{p_i} V_i$。

P2：$V_i \mid\equiv V_i \xleftrightarrow{\mathrm{SP}_j} \mathrm{RSU}_i$。

P3：$V_i \mid\equiv V_i \xleftrightarrow{p_i, p_j} V_j$。

P4：$V_j \mid\equiv V_i \xleftrightarrow{p_i, p_j} V_j$。

P5：$\mathrm{RSU}_i \mid\equiv \mathrm{RSU}_i \xleftrightarrow{p_j} V_j$。

P6：$V_j \mid\equiv V_j \xleftrightarrow{\mathrm{SP}_i} \mathrm{RSU}_i$。

P7：$\mathrm{RSU}_i \mid\equiv V_i \Rightarrow \{B_{vi}, \mathrm{AIDV}_i\}$。

P8：$V_i \mid\equiv \mathrm{RSU}_i \Rightarrow p_j$。

P9：$V_j \mid\equiv V_i \mid\Rightarrow \{S_i^1, S_i^2, \xi_1\}$。

P10：$\mathrm{RSU}_i \mid\equiv V_j \Rightarrow \{B_{vj}, \mathrm{AIDV}_j\}$。

P11：$V_j \mid\equiv \mathrm{RSU}_i \Rightarrow p_i$。

P12：$V_i \mid\equiv V_j \mid\Rightarrow \{S_j^1, S_j^2, \xi_2, \delta\}$。

6) 协议安全性证明

通过分析理想化协议形式的安全性，得到 2 个协议安全证明目标 Goal1 和 Goal2。

① $\mathrm{RSU}_i \triangleleft \langle B_{vi}, T_{vi}, \mathrm{AIDV}_i, \mathrm{SIDV}_j \rangle_{p_i}$。根据 P1：$\mathrm{RSU}_i \mid\equiv \mathrm{RSU}_i \xleftrightarrow{p_i} V_i$ 和 message-meaning 规则 R1：$\dfrac{P \mid\equiv P \xleftrightarrow{K} Q, P \triangleleft \langle X \rangle_K}{P \mid\equiv Q \mid\sim X}$，可以得到 $\mathrm{RSU}_i \mid\equiv V_i \mid\sim \{B_{vi}, \mathrm{AIDV}_i\}$。时间戳 T_{vi} 通过检验后，有 $\mathrm{RSU}_i \mid\equiv \#(T_{vi})$。再根据 freshness 规则 R4：$\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$ 和 nonce-verification 规则 R3：$\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$，可以得到 $\mathrm{RSU}_i \mid\equiv V_i \mid\equiv \{B_{vi}, \mathrm{AIDV}_i\}$。最后根据 jurisdiction 规则 R2：$\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$ 和 P7：$\mathrm{RSU}_i \mid\equiv V_i \Rightarrow \{B_{vi}, \mathrm{AIDV}_i\}$，可以得到 $\mathrm{RSU}_i \mid\equiv \{B_{vi}, \mathrm{AIDV}_i\}$。$B_{vi}$ 和 AIDV_i 通过检验后，RSU_i 将 SIDV_j 对应的素数 p_j 发送给 V_i。

② $V_i \triangleleft \langle p_j, T_{Ri} \rangle_{\mathrm{SP}_j}$。同理，根据 P2：$V_i \mid\equiv V_i \xleftrightarrow{\mathrm{SP}_j} \mathrm{RSU}_i$ 和 R1，可以得到 $V_i \mid\equiv \mathrm{RSU}_i \mid\sim p_j$。时间戳 T_{Ri} 通过检验后，便有 $V_i \mid\equiv \#(T_{Ri})$。根据 R3 和 R4，可以得到 $V_i \mid\equiv \mathrm{RSU}_i \mid\equiv p_j$。最后根据 R2 和 P8：$V_i \mid\equiv \mathrm{RSU}_i \Rightarrow p_j$，可以得到 $V_i \mid\equiv p_j$。当 V_i 得到 V_j 对应的素数后，便将签名认证密钥协商消息发送给 V_j。

③ $\mathrm{RSU}_i \triangleleft \langle B_{vj}, T_{vj}, \mathrm{AIDV}_j, \mathrm{SIDV}_i \rangle_{p_j}$。根据 P5：$\mathrm{RSU}_i \mid\equiv \mathrm{RSU}_i \xleftrightarrow{p_j} V_j$ 和 R1，可以得到 $\mathrm{RSU}_i \mid\equiv V_j \mid\sim \{B_{vj}, \mathrm{AIDV}_j\}$。时间戳 T_{vj} 通关检验后，便有 $\mathrm{RSU}_i \mid\equiv \#(T_{vj})$。再根据 R3 和 R4，可以得到 $\mathrm{RSU}_i \mid\equiv V_j \mid\equiv \{B_{vj}, \mathrm{AIDV}_j\}$。最后根据 R2 和 P10：$\mathrm{RSU}_i \mid\equiv V_j \Rightarrow \{B_{vj}, \mathrm{AIDV}_j\}$，可以得到 $\mathrm{RSU}_i \mid\equiv \{B_{vj}, \mathrm{AIDV}_j\}$。$B_{vj}$ 和 AIDV_j 通过检验后，RSU_i 将 SIDV_i 对应的素数 p_i 发送给 V_j。

④ $V_j \triangleleft \langle p_i, T_{Rj} \rangle_{\mathrm{SP}_i}$。根据 P6：$V_j \mid\equiv V_j \xleftrightarrow{\mathrm{SP}_i} \mathrm{RSU}_i$ 和 R1，可以得到 $V_j \mid\equiv \mathrm{RSU}_i \mid\sim p_i$。时间戳 T_{Rj} 通过检验后，便有 $V_j \mid\equiv \#(T_{Rj})$。根据 R3 和 R4，可以得到 $V_j \mid\equiv \mathrm{RSU}_i \mid\equiv p_i$。最后根据 R2 和 P11：$V_j \mid\equiv \mathrm{RSU}_i \Rightarrow p_i$，可以得到 $V_i \mid\equiv p_j$。当 V_j 得到 V_i 对应的素数后，便对来自 V_i 的签名信息进行验证，验证通过后就发送签名密钥协商消息给 V_i。

⑤ $V_j \triangleleft \langle S_i^1, S_i^2, t_{vi}, T_{ij}, \xi_1 \rangle_{p_i, p_j}$。根据 P4：$V_j \mid\equiv V_i \xleftrightarrow{p_i, p_j} V_j$ 和 R1，可以得到 $V_j \mid\equiv V_i \mid\sim \{S_i^1, S_i^2, \xi_1\}$。时间戳 T_{ij} 通过检验后，有 $V_j \mid\equiv \#(T_{ij})$。根据 R3 和 R4，可以得到 $V_j \mid\equiv V_i \mid\equiv \{S_i^1, S_i^2, \xi_1\}$。然后根据 R2 和 P9：$V_j \mid\equiv V_i \mid\Rightarrow \{S_i^1, S_i^2, \xi_1\}$，可以得到 $V_j \mid\equiv \{S_i^1, S_i^2, \xi_1\}$。当来自 V_i 的签名消息 S_i^1 和 S_i^2 通过检验后，协议就完成了 V_j 对 V_i 的认证，V_j 就会相信 V_i 的密钥协商消息 ξ_1，即 $V_j \mid\equiv \xi_1$。这样就完成了 Goal1。V_j 选择随机数 β，计算 $\xi_2 = T_\beta(x) \bmod n$ 和会话密钥 $\mathrm{sk} \equiv T_\beta(\xi_1) \bmod n \equiv T_{\beta\alpha}(x) \bmod n$。最后发送签名认证密钥协商消息给 V_i。

⑥ $V_i \triangleleft \langle S_j^1, S_j^2, t_{vj}, T_{ji}, \xi_2, \delta \rangle_{p_i, p_j}$。根据 P3：$V_i \mid\equiv V_i \xleftrightarrow{p_i, p_j} V_j$ 和 R1，可以得到 $V_i \mid\equiv V_j \mid\sim \{S_j^1, S_j^2, \xi_2, \delta\}$。时间戳 T_{ji} 被验证是新鲜的后，即 $V_i \mid \#(T_{ji})$。根据 R3 和 R4，可以得到 $V_i \mid\equiv V_j \mid\equiv \{S_j^1, S_j^2, \xi_2, \delta\}$。然后根据 R2 和 P12：$V_i \mid\equiv V_j \mid\Rightarrow \{S_j^1, S_j^2, \xi_2, \delta\}$，可以得到 $V_i \mid\equiv \{S_j^1, S_j^2, \xi_2, \delta\}$。当来自 V_j 的签名信息 S_j^1

和 S_j^2 通过检验，δ 也通过验证，V_i 便相信来自 V_j 的会话密钥消息 ξ_2，即 $V_i \models \xi_2$。这里便完成了 Goal2。最后 V_i 计算会话密钥 $\mathrm{sk} \equiv T_\alpha(\xi_2) \bmod n \equiv T_{\alpha\beta}(x) \bmod n$。

从 Goal1 和 Goal2 的证明过程可以看出，本文提出的协议能够有效地实现群内成员相互认证密钥协商的安全证明。

利用 BAN 逻辑模型，模拟了协议中涉及的所有消息，建立了 2 个协议安全证明目标。并通过合理的假设前提，完成了对消息来源的验证、消息新鲜度的验证和消息来源可信度的验证。最后根据模型规则证明了预先设定的 2 个目标，完成了对协议的形式化证明。任何认证密钥协商协议都必须满足形式化安全证明的要求，否则提出的协议很可能存在安全漏洞。

3.2 安全性分析

为了在 VANET 系统中安全通信，认证密钥协商协议除了需要对协议的语义安全进行形式化证明，还需要满足 VANET 系统中一些基本安全需求[19]，如身份认证性、身份隐私性、消息不可否认性、前向和后向安全性。同时协议还需要能够抵御各种恶意攻击，如女巫攻击、OBU 和 RSU 仿冒攻击、重放攻击。

1) 身份认证性。本文提出的认证密钥协商协议中，V_j 通过检验 V_i 对密钥协商消息的签名来认证 V_i 的身份，即判断 $S_i^1 g^{S_i^2} \equiv y_i^{2t_{\mathrm{wi}} H_0(p_i \| p_j \| T_{ij})} (\bmod p_i)$ 是否成立。所有签名只有经过注册的群成员使用私钥才能生成。攻击者只有破解了 CDLP 和基于扩展的切比雪夫混沌映射的 CDHP 才能生成正确的签名信息。通过对签名信息的检验，车辆能够对接收消息的身份进行验证和消息完整性检验。所以该密钥协商协议可以实现 V_i 和 V_j 的相互身份认证。

2) 身份隐私性。整个密钥协商过程中，V_i 和 V_j 都使用假名进行通信，只有 TA 知道它们的真实身份。如果攻击者想要通过车辆节点的假名 $\mathrm{SIDV}_i = H_0(\mathrm{IDV}_i \| \delta_{\mathrm{sk}})$ 知道车辆的真实身份，就必须破解单向哈希函数难题并获取系统私钥。因为单向哈希函数难题解决的困难性和系统私钥的隐私性，车辆假名可以有效保护车辆的真实身份，实现车辆节点在认证密钥协商过程中的隐私性。

3) 消息不可否认性。当车辆 V_a 在 RSU_i 覆盖范围内发布恶意消息时，如果 V_a 不是合法的车辆群内成员，其他车辆群内成员可以直接拒接 V_a 发布的消息；如果 V_a 是车辆群内成员，RSU_i 通过检查 V_a 的发布信息使用的素数 p_a，在 $\lambda_{\mathrm{SIDV},p}$ 找到 p_a 对应的假名 SIDV_a，再将假名和对应素数 p_a 发给 TA。TA 通过 $H_0(\mathrm{IDV}_a \| \delta_{\mathrm{sk}}) = \mathrm{SIDV}_a^0$、$p_a$ 对应的 l 和假名更新种子 $\delta \mathrm{ID}_a$ 就找到 V_a 的真实身份，完成了对车辆身份的追溯，确保车辆发送消息的不可否认性。

4) 前向和后向安全性。V_i 选择随机数 α，计算出 $\xi_1 \equiv T_\alpha(x) \bmod n$。$V_j$ 选择随机数 β，计算出 $\xi_2 \equiv T_\beta(x) \bmod n$。会话密钥 $\mathrm{sk}_t \equiv T_{\alpha\beta}(x) \bmod n$。$V_i$ 和 V_j 都是通过选择随机数计算当前会话密钥，攻击者无法通过 sk_t 推导出 sk_{t-1} 或者 sk_{t+1}。所以该方案的会话密钥具有前向和后向安全性。

5) 抵御女巫攻击。攻击者创建大量假名车辆身份发送错误信息，以获得对对等网络的控制。在本文提出的认证密钥协商协议中，会话双方都可以通过访问 RSU 对接收消息中假名对应的素数进行访问，如果没有获取到该假名对应的素数，可以直接拒绝接收的信息；如果获取到对应的素数，就可以利用该素数对消息的签名进行验证。在这个过程中，会话车辆并不关注其他车辆对该接收消息的信任度，而是通过素数对签名消息进行验证。所以本文提出的协议能够有效抵御女巫攻击。

6) 抵御 OBU 和 RSU 仿冒攻击。对于 OBU 仿冒攻击，攻击者 $\mathcal{A}$ 想要仿冒 OBU_i 或 OBU_j 来完成会话密钥协商。如果 $\mathcal{A}$ 不是合法的群成员，就无法通过 RSU_i 的检验。RSU_i 根据 $\mathcal{A}$ 发来的消息计算 $\mathrm{SIDV}_j^{'} = \mathrm{AIDV}_j \oplus H_1(p_j \| T_{vj})$，并判断等式 $B_{vj}^{'} = H_1(\mathrm{SIDV}_j^{'} \| p_j \| T_{vj}) = B_{vj}$ 是否成立，如果等式不成立，RSU_i 将会拒绝 $\mathcal{A}$ 的素数请求。如果 $\mathcal{A}$ 是经过注册的群成员，那么 $\mathcal{A}$ 就能成功的获取密钥协商的发起方和接收方对应的素数；但是密钥协商双方通过访问 RSU_i 都知道对方对应的素数 p_i，然后计算 $y_i \equiv c(\bmod p_i)$，对对方生成的签名进行检验 $S_i^1 g^{S_i^2} \equiv y_i^{H_0(p_i \| p_j \| T_{ij})} (\bmod p_i)$；攻击者没有密钥协商双方的密钥 $x_{i,t}, x_{j,t}$，就无法生成有效的签名。所以无论 $\mathcal{A}$ 是不是群成员都无法仿冒 OBU_i 或 OBU_j，本文协议可以抵御仿冒攻击，对于 RSU 仿冒攻击，当车辆节点 V_i 向 RSU 发送素数请求后，得到 RSU 的回答。V_i 通过 $\mathrm{SP}_j = H_1(\mathrm{SIDV}_j \| p_j)$ 检验来自

RSU 的信息，$\lambda_{\mathrm{SIDV},p}$ 只有进过注册的合法的 RSU 才能获取，其他 RSU 无法获取。所以本文协议可以有效抵御 RSU 仿冒攻击。

7) 抵御重放攻击。在车辆进行认证和密钥协商协商过程中，恶意车辆监听车辆节点和 RSU_i 之间的通信，并在当前会话中重放身份验证消息，以模拟该车辆。为避免这种情况，RSU_i 验证由车辆节点生成的时间戳，由于时间戳是新鲜的，因此重放攻击消息无法通过验证。同样，车辆节点双方进行消息的传输的过程中，都使用时间戳来保证消息的新鲜度。此外，每个会话都使用不同的时间戳，这增加了对重放攻击的抵抗力。所以本文协议可以有效抵御重放攻击。

4　仿真与性能评估分析

VANET 系统具有车辆快速移动和网络拓扑快速变化的特性，所以 VANET 系统对通信性能要求比较高。下面将从安全性、计算开销和通信开销这几个角度对本文协议进行分析，并和 Cui[16]方案、Bagga[20]方案和 Ying[21]方案进行比较。

4.1　安全性分析

安全是 VANET 系统中车辆间进行通信最基本的需求。本文对几种 VANET 系统中认证和密钥协商方案的安全性进行了对比，具体如表 2 所示。Cui 方案、Bagga 方案和 Ying 方案都忽略了车辆认证密钥协商的不可否认性、身份可撤销性和群组动态性的安全需求。Cui 方案无法完成身份的双向认证，Bagga 方案无法保证会话密钥的前向和后向安全性，Ying 方案也忽略了车辆身份双向认证性且不可以抵御 RSU / Fog 仿冒攻击。本文协议满足所有安全需求，有较高的安全性。

4.2　计算开销分析

本文使用 OpenSSL-1.0.1 密码学库，在配置为 Intel（R）Core（TM）i5-8500、RAM 为 2 GB 的 Windows 10 系统及 Visual Studio 2017 的编译环境下对几种方案涉及的密码学操作进行了模拟，密码学运算的平均执行时间如表 3 所示。其中 T_{h}、T_{c}、T_{exp}、T_{ecm}、T_{eca}、T_{sym}、T_{asy} 分别表示进行一次哈希运算、切比雪夫映射、模指数运算、椭圆曲线中的点乘运算、椭圆曲线中点的加法运算、对称加密/解密运算、非对称加密/解密运算的执行时间。

表 2　安全性对比

安全性	Cui 方案	Bagga 方案	Ying 方案	本文协议
身份认证性	×	√	×	√
身份隐私性	√	√	√	√
不可否认性	×	×	×	√
身份可撤销性	×	×	×	√
前向和后向安全性	√	×	√	√
群组动态性	×	×	×	√
抵御重放攻击	√	√	√	√
抵御女巫攻击	×	√	√	√
抵御 OBU 仿冒攻击	√	√	√	√
抵御 RSU / Fog 仿冒攻击	√	√	×	√

表 3　密码学运算的平均执行时间

密码学运算	平均执行时间/ms
T_{h}	0.44
T_{c}	18.47
T_{exp}	26.35
T_{ecm}	23.47
T_{eca}	6.04
T_{sym}	7.64
T_{asy}	107.35

表 4 给出了各方案在认证密钥协商过程中，在密钥协商发起方 V_i、密钥协商接收方 V_j 和 RSU 处需要执行的密钥学运算次数和总的计算开销。Cui 方案需要执行 17 次单向哈希运算、18 次切比雪夫映射和 3 次对称加密运算。所以 Cui 方案总的计算开销为 $17T_{\mathrm{h}}+18T_{\mathrm{c}}+3T_{\mathrm{sym}}\approx 362.86$ ms。Bagga 方案需要执行 10 次单向哈希运算、12 次椭圆曲线乘法运算和 4 次椭圆曲线加法运算。所以 Bagga 方案总的计算开销为 $10T_{\mathrm{h}}+12T_{\mathrm{ecm}}+4T_{\mathrm{eca}}\approx 310.19$ ms。Ying 方案需要执行 22 次单向哈希运算、4 次模指数运算和 4 次非对称加密/解密运算。所以 Ying 方案总的计算开销为 $22T_{\mathrm{h}}+4T_{\mathrm{exp}}+4T_{\mathrm{asy}}\approx 272.23$ ms。本文协议需要执行 16 次单向哈希函数、6 次切比雪夫映射和 4 次模指数运算，所以总的计算开销为 $16T_{\mathrm{h}}+6T_{\mathrm{c}}+4T_{\mathrm{exp}}\approx 223.25$ ms。

各方案计算开销对比如图 4 所示。从图 4 可以看出，Cui 方案的计算开销最大，本文协议的计算开销明显低于其他方案。与 Cui 方案相比，本文协议的计算开销减少了约 38%。计算开销所

表 4 各方案在认证密钥协商过程中的计算开销

方案	V_i / ms	RSU / ms	V_j / ms	总的计算开销 /ms
Cui 方案	$T_{\text{sym}}+8T_{\text{c}}+8T_{\text{h}}\approx 158.92$	—	$2T_{\text{sym}}+10T_{\text{c}}+9T_{\text{h}}\approx 203.94$	$17T_{\text{h}}+18T_{\text{c}}+3T_{\text{sym}}\approx 362.86$
Bagga 方案	$4T_{\text{h}}+6T_{\text{ecm}}+2T_{\text{eca}}\approx 154.66$	—	$6T_{\text{h}}+6T_{\text{ecm}}+2T_{\text{eca}}\approx 155.54$	$10T_{\text{h}}+12T_{\text{ecm}}+4T_{\text{eca}}\approx 310.2$
Ying 方案	$4T_{\text{h}}+T_{\text{exp}}\approx 28.11$	$14T_{\text{h}}+2T_{\text{exp}}+4T_{\text{asy}}\approx 292.26$	$4T_{\text{h}}+T_{\text{exp}}\approx 28.11$	$22T_{\text{h}}+4T_{\text{exp}}+4T_{\text{asy}}\approx 348.48$
本文协议	$6T_{\text{h}}+3T_{\text{c}}+2T_{\text{exp}}\approx 110.75$	$4T_{\text{h}}\approx 1.76$	$6T_{\text{h}}+3T_{\text{c}}+2T_{\text{exp}}\approx 110.75$	$16T_{\text{h}}+6T_{\text{c}}+4T_{\text{exp}}\approx 223.26$

导致就是通信时延。VANET 系统对通信时延特别敏感，因为只有低的通信时延才能满足 VANET 拓扑快速变化的需求。所以相较于其他认证和密钥协商方案，本文协议拥有低通信时延的属性。

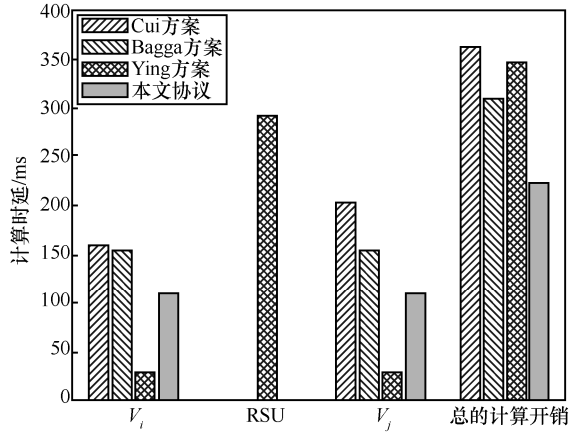


图 4 各方案计算开销对比

4.3 通信开销分析

本文假设哈希摘要为 160 bit，时间戳为 32 bit，ID 为 160 bit，椭圆曲线点乘为 320 bit，切比雪夫映射为 480 bit，非对称加密为 1024 bit，对称加密为 256 bit。各方案在密钥协商过程中需要发送的消息数量和总的通信开销如表 5 所示。Cui 方案在密钥协商过程中需要发送 4 条消息，分别是 $\{h(k_i),y_i\}$、$\{\text{sid}_i,z_i,C_i,\text{MAC}_i\}$、$M_i^3=\{k_i\oplus t_i^R,T_i\}$ 和 $\{D_i\}$，总的通信开销为 2 464 bit。Bagga 方案在密钥协商过程中需要发送 3 条消息，分别是 $\{\text{RID}_{V_i},X_{V_i},P_{V_i},\text{Sig}_x,t_1\}$、$\{\text{RID}_{V_m},P_{V_m},Z_{V_m},\text{Sig}_{\text{SK}},t_2\}$ 和 $\{\text{ACK}_{V_i},V_m,t_3\}$，总的通信开销为 2 176 bit。Ying 方案在密钥协商过程中需要发送 4 条消息，分别是 $\{\text{DIDV}_{i,j},\text{CV}_i,n_j,T_{V_i}\}$、$\{\text{DIDR}_i,\text{CV}_i,n_j,T_{R_i}\}$、$\{C_3,M_i,T_{R_i}^{'}\}$ 和 $\{C_3,M_i,T_{v_i}^{'}\}$，总的通信开销为 3 392 bit。本文协议在密钥协商过程中需要发送 6 条消息，分别是 $\{B_{vi},T_{vi},\text{AIDV}_i,\text{SIDV}_j\}$、$\{p_j,T_{Ri}\}$、$\{S_i^1,S_i^2,t_{vi},T_{ij},\xi_1\}$、$\{B_{vj},T_{vj},\text{AIDV}_j,\text{SIDV}_i\}$、$\{p_i,T_{Rj}\}$ 和 $\{S_j^1,S_j^2,t_{vj},T_{ji},\xi_2,\delta\}$，总的通信开销为 3 232 bit。

表 5 各方案在密钥协商过程中需要发送的消息数量和总的通信开销

方案	消息数量/条	总的通信开销/bit
Cui 方案	4	2 464
Bagga 方案	3	2 176
Ying 方案	4	3 392
本文协议	6	3 232

各方案通信开销对比如图 5 所示。从图 5 可以看出，Ying 方案通信开销最大，因为方案中使用了非对称加密解密运算。Bagga 方案通信开销最小。本文协议的通信开销比 Ying 方案低但高于 Cui 方案和 Bagga 方案，主要是本文利用了签名机制验证群成员身份并使用了切比雪夫映射进行密钥协商，在认证和密钥协商过程中都保证了车辆节点通信的安全。从 4.1 节的分析也可以看出，相较于 Cui 方案和 Bagga 方案，本文协议对 VANET 系统中认证密钥协商的安全性考虑更加全面。

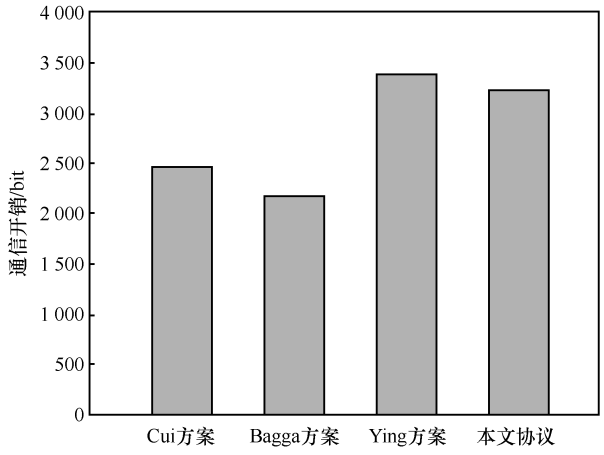


图 5 各方案通信开销对比

5　结束语

本文提出了一种 VANET 系统中的基于中国剩余定理的群内相互认证密钥协商协议。利用中国剩余定理建立动态车辆群，以适应 VANET 拓扑变化。群内成员利用签名机制实现相互身份认证，并利用切比雪夫混沌映射实现车辆间的密钥协商。采用假名更新和私钥更新机制，保护通信双方隐私安全。通过 BAN 逻辑模型证明了该协议的语义安全。最后，仿真结果表明，相较于现有方案，所提协议对 VANET 系统中通信的安全性考虑更加全面，能有效降低通信消耗，并且显著减少了计算开销。

参考文献：

[1] CHENG J J, CHENG J L, ZHOU M C, et al. Routing in Internet of vehicles: a review[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(5): 2339-2352.

[2] JIANG D, TALIWAL V, MEIER A, et al. Design of 5.9 GHz DSRC-based vehicular safety communication[J]. IEEE Wireless Communications, 2006, 13(5): 36-43.

[3] LAI C Z, ZHANG K, 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.

[4] LAI C Z, ZHANG M, CHENG N, et al. SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(6): 1559-1574.

[5] CHEN Z M, ZHAO J G, HUANG B Y. Optimizing PKI for 3GPP authentication and key agreement[C]//Proceedings of 2012 Fourth International Conference on Multimedia Information Networking and Security. Piscataway: IEEE Press, 2012: 79-82.

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

[7] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Advances in Cryptology. Berlin: Springer, 1985: 47-53.

[8] HOJJATI M, SHAFIEINEJAD A, YANIKOMEROGLU H. A blockchain-based authentication and key agreement (AKA) protocol for 5G networks[J]. IEEE Access, 2020, 8: 216461-216476.

[9] XU J B, MENG X W, LIANG W, et al. A secure mutual authentication scheme of blockchain-based in WBANs[J]. China Communications, 2020, 17(9): 34-49.

[10] 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.
CHEN R X, CHEN J, ZHANG Y Y, et al. Certificateless asymmetric group key agreement[J]. Journal of Cryptologic Research, 2016, 3(4): 382-398.

[11] 杜红珍, 温巧燕. 无证书强指定验证者多重签名[J]. 通信学报, 2016, 37(6): 20-28.
DU H Z, WEN Q Y. Certificateless strong designated verifier multi-signature[J]. Journal on Communications, 2016, 37(6): 20-28.

[12] PORKODI C, ARUMUGANATHAN R. Group-oriented signature schemes based on Chinese remainder theorem[C]//Proceedings of 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC). Piscataway: IEEE Press, 2009: 1661-1664.

[13] 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.

[14] YOON E J, JEON I S. An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(6): 2383-2389.

[15] KOCAREV L, TASEV Z. Public-key encryption based on Chebyshev maps[C]//Proceedings of the 2003 International Symposium on Circuits and Systems. Piscataway: IEEE Press, 2003: 28-31.

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

[17] ZHANG L H. Cryptanalysis of the public key encryption based on multiple chaotic systems[J]. Chaos, Solitons & Fractals, 2008, 37(3): 669-674.

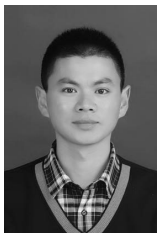
[18] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[19] MATHEW N, UMA V. VANET security-analysis and survey[C]// Proceedings of 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT). Piscataway: IEEE Press, 2018: 100-106.

[20] BAGGA P, DAS A K, WAZID M, et al. On the design of mutual authentication and key agreement protocol in Internet of vehicles-enabled intelligent transportation system[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1736-1751.

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

[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。

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、安全认证、密钥协商。

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

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