智能车载自组织网络中匿名在线注册与安全认证协议

张晓均*① 王文琛① 付 红① 牟黎明② 许春香③

①(西南石油大学计算机科学学院网络空间安全研究中心 成都 610500)

②(神州绿盟成都科技有限公司 成都 610213)

③(电子科技大学计算机科学与工程学院 成都 611731)

摘 要：随着智能交通系统(ITS)的建立，车载自组织网络(VANETs)在提高交通安全和效率方面发挥着重要的作用。由于车载自组织网络具有开放性和脆弱性特点，容易遭受各种安全威胁与攻击，这将阻碍其广泛应用。针对当前车载自组织网络传输中数据的认证性与完整性，以及车辆身份的隐私保护需求，该文提出一种智能车载自组织网络中的匿名在线注册与安全认证协议。协议让智能车辆在公开信道以匿名的方式向交通系统可信中心(TA)在线注册。可信中心证实智能车辆的真实身份后，无需搭建安全信道，在开放网络中颁发用于安全认证的签名私钥。车辆可以匿名发送实时交通信息到附近路边基站单元(RSU)，并得到有效认证与完整性检测。该协议使得可信中心可以有效追踪因发送伪造信息引起交通事故的匿名车辆。协议可以让路边基站单元同时对多个匿名车辆发送的交通信息进行批量认证。该协议做了详细的安全性分析和性能分析。性能比较结果表明，该协议在智能车辆端的计算开销以及在路边基站单元端的通信开销都具有明显优势，而且无需搭建安全信道就能够实现匿名在线注册，因此可以安全高效地部署在智能车载自组织网络环境。

关键词：车载自组织网络；匿名在线注册；安全认证；身份追踪；批量认证

中图分类号：TN918; TN309.7 **文献标识码**：A **文章编号**：1009-5896(2022)10-3618-09

DOI: 10.11999/JEIT210882

Anonymous Online Registration and Secure Authentication Protocol in Intelligent Vehicular Ad-hoc Networks

ZHANG Xiaojun① WANG Wenchen① FU Hong①

MU Liming② XU Chunxiang③

①(*Research Center for Cyber Security, School of Computer Science, Southwest Petroleum University, Chengdu* 610500, *China*)

②(*NSFOCUS Information Chengdu Technology Co., LTD, Chengdu* 610213, *China*)

③(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu* 611731, *China*)

Abstract: With the establishment of the Intelligent Transportation Systems (ITS), Vehicular Ad-hoc NETworks (VANETs) play great roles in improving traffic safety and efficiency. However, due to the openness and fragility of VANETs, they are vulnerable to various network threats and attacks, and thereby hindering the wide applications of VANETs. To address the requirements for authentication and integrity of transmitted data, identity privacy-preservation, an anonymous online registration and secure authentication protocol is proposed in intelligent VANETs. The protocol enables a vehicle to execute anonymous online registration in transportation systems Trusted Authority (TA) via a public channel. Once validating the real identity, TA can return the private key to the vehicle for subsequent secure authentication via public channel. Thus, the vehicle can generate an authenticated traffic message to a nearby RoadSide Unit (RSU) in real time, so that RSU

收稿日期：2021-08-27；改回日期：2022-03-04；网络出版：2022-04-08

*通信作者： 张晓均 zhangxjdzkd2012@163.com

基金项目：国家重点研发计划(2017YFB0802000)，国家自然科学基金(61902327, 61872060)，中国博士后科学基金(2020M681316)，成都市科技局重点研发项目(2021-YF05-00965-SN)

Foundation Items: The National Key R&D Program of China (2017YFB0802000), The National Natural Science Foundation of China (61902327, 61872060), China Postdoctoral Science Foundation (2020M681316), Chengdu Key R&D Project (2021-YF05-00965-SN)

performs the authentication and integrity verification. This protocol supports anonymous identity traceability, thus TA can revoke the real identity of a malicious vehicle, which has generated some forged messages and caused traffic jams or accidents. In addition, this protocol supports batch authentication and verification of those transmitted traffic messages from different anonymous vehicles. The detailed security analysis and performance evaluation have been conducted. The results demonstrate that the protocol has outstanding advantages on the computational costs of each vehicle and the communication overhead of RSU, and can realize anonymous online registration without establishing secure channel. Therefore, the protocol could be securely and efficiently deployed in intelligent VANETs.

Key words: Vehicular Ad-hoc NETworks (VANETs); Anonymous online registration; Secure authentication; Identity traceability; Batch authentication and verification

1　引言

智能交通系统(Intelligent Transportation Systems, ITS)通过应用现代信息和通信技术来缓解传统交通运输系统的压力。ITS把行人、车辆和道路进行了综合考虑，可通过约束各实体的交通行为使其更为规范。因此，ITS可以提高交通管理部门决策水准，减少驾驶人员失误，进而提高道路系统运输效率和可靠性[1]。

如今，移动通信技术已进入5G时代，5G具有超高速率、超低时延、高可靠性的特性，还具有庞大的网络容量，可实现海量连接[2–4]。随着5G的快速发展，车载自组织网络在智能交通系统中必将成为重要的应用。智能汽车嵌入车载通信单元OBUs (On-Board Units)，通过车载自组织网络可以实现特殊车辆避让、碰撞预警等功能来帮助缓解交通压力，减少交通事故，提高交通运输效率和道路安全性。在车载自组织网络中，道路上的所有车辆之间都始终保持着相互通信的状态，称为V2V (Vehicle-to-Vehicle)通信。此外，在行驶途中也和道路两侧基础设施保持V2I (Vehicle-to-Infrastructure)通信。

尽管车载自组织网络在智能交通系统中有着巨大的应用优势，但是要实现其大规模的部署仍然存在着一些挑战：需要保证服务质量、高连接性和带宽以及车辆和个人隐私安全性等问题[5–7]。在智能车联网中，给用户提供一定的服务质量保证，就需要做到数据传输的延迟最小，重传次数少以及能长时间保持网络连接等。由于车载自组织网络的开放性，各个节点之间传递的信息很容易遭受到主动攻击。比如，攻击者还可以通过篡改、替换、重放攻击等来引发重大的交通事故，由此，确保传输消息的完整性和可认证性是十分重要的[8–10]。一个安全的车联网，需要保证一些重要信息只能在指定的节点传输，而无法被其他节点获取；也要保证恶意攻击者无法通过伪造成合法车辆进入车联网；还需要保证车联网可以抵御常见的网络攻击等。在如今的网络时代中，每天都有大量隐私信息泄露，身份隐私保护显得尤为重要[11–13]。为保护驾驶员的隐私，需要在车载自组织网络可信中心以匿名的方式进行注册，在传输的交通信息时会以匿名的方式与周围的车辆或路边基础设施进行身份认证。此外，车辆间通信及车内敏感数据保存等都依赖密钥，因此密钥管理也极其重要。针对上述安全问题，设计出适用于车载自组织网络环境的高效、安全的匿名注册与安全认证协议是非常重要的。

为确保交通信息传输的可认证性和完整性，Jiang等人[14]提出了一种基于组密钥的车载自组织网络中的认证方案。Azees等人[15]提出了一种有效的匿名身份验证和VANET的条件隐私保护方案，该方案提供了一种条件跟踪机制来跟踪恶意肇事者，但其效率并不是很高。文献[16]提出了一种有效的针对VANET的隐私保护匿名身份验证方案，该方案不仅支持批量身份验证，而且还提供了一种条件跟踪机制来跟踪行为异常的车辆或RSU。Xiong等人[17]提出了一种支持车载自组织网络中车辆能进行批量验证的条件隐私保护方案，该方案可以为主私钥和车辆私钥提供双重保险，即使这两个私钥中的一个在侧信道攻击下被攻破，恶意实体仍然无法伪造有效的认证消息。2018年，Cui等人[18]提出了无双线性对的基于无证书的批量验证方案，该方案能够有效地抗密钥泄露。文献[19]提出了一种无证书的批量认证方案，并且对该方案进行了严格的安全性证明。为了满足车载网中车辆计算能力弱和低延时通信的需求，Liu等人[20]提出了基于无证书短签名的方案，该方案最大的优势就是将匿名认证以区域管理的方法结合车联网的环境实现。Cui等人[21]提出了一种将伪身份预加载到车辆的可信任平台模组方案，该方案能够有效减少车辆计算开销。文献[22]给出了一种消息认证码和基于身份的签名方案，该方案能够解决证书撤销列表消耗资源过大问题，并且能够进行批量聚合认证。

本文提出一种智能车载自组织网络中基于身份的匿名在线注册与安全认证协议。现有的协议，大

多是智能车辆通过离线方式或安全信道在智能车载可信中心进行注册，这将造成资源的极大浪费，而且在增加新用户的时候，可能会导致信息泄露等问题。本文中，智能车辆通过对注册信息进行对称加密，并通过公开信道进行在线注册，增加了安全性。车辆的消息利用匿名身份进行传输，路边基站单元能够正确地判断消息的完整性和消息来源。当发生事故时，可信中心能够对消息发送者的真实身份进行追踪。此外，协议可以让路边基站单元同时对多个匿名车辆发送的交通信息进行有效认证与完整性检测，极大地提高了效率。最后，给出本文设计的协议的安全性分析与性能评估，结果表明该协议在智能车载自组织网络中安全部署具有很好的安全与性能优势。

2 基础知识

2.1 椭圆曲线密码系统中的困难问题

在有限域GF(p)中选取椭圆曲线$E_p(a,b)$：$y^2=x^3+ax+b(\mathrm{mod}p)$，满足$4a^3+27b^2\neq 0(\mathrm{mod}p)$。设置基于椭圆曲线的$q$阶加法循环群$G\subset E_p(a,b)$，$P$是$G$的一个生成元。基于椭圆曲线的密码困难问题定义如下：

定义1(DL困难问题) 给定$P,Q\in G$，满足$Q=xP$，其中$x\in Z_q^*$，在多项式时间内求解x，是计算不可行的。

定义2(CDH困难问题) 对于两个未知的$y,z\in Z_q^*$，给定yP,zP，在多项式时间内求解yzP，是计算不可行的。

2.2 系统模型

系统模型包含3类通信实体：Vehicles, RSU和TA (Trusted Authority)，如图1所示。

Vehicles：智能车辆都配置了一个车载通信单元(OBU)。OBU包含一个支持DRSC(Dedicated Short Range Communication)协议的防篡改装置TPD(Tamper Proof Device)。TPD通常用于存储机密数据，攻击者几乎不可能获取TPD之中的数据。车辆之间以及车辆与RSU之间是通过无线网络进行通信的。

RSU(RoadSide Unit)：路边基站单元，固定在道路两旁的基础设施，是个半可信的实体，主要负责消息的认证和转发，能够与车辆进行实时通信。

TA：可信中心，充当身份密码系统中密钥生成中心PKG(Private Key Generator)的角色，是一个完全可信任的第三方机构，具有高存储量和高计算能力，能够为系统生成和公布公开参数，为智能车辆提供在线匿名注册，以及签名私钥生成服务。

3 智能车载自组织网络中匿名在线注册与安全认证协议

3.1 协议具体内容

智能车载自组织网络中匿名在线注册与安全认证协议主要包括系统初始化阶段、在线匿名注册阶段、签名私钥产生阶段、匿名认证阶段、匿名认证信息验证阶段5个阶段，具体协议描述如下。

系统初始化阶段：由完全可信任的TA执行。TA按照以下步骤产生系统公开参数，主公钥和主私钥。

(1) TA基于有限域GF(p)选取椭圆曲线$E_p(a,b)$：$y^2=x^3+ax+b(\mathrm{mod}p)$，满足$4a^3+27b^2\neq 0(\mathrm{mod}p)$。TA选取基于椭圆曲线的$q$阶加法循环群$G\subset E_p(a,b)$，$P$是$G$的一个生成元。

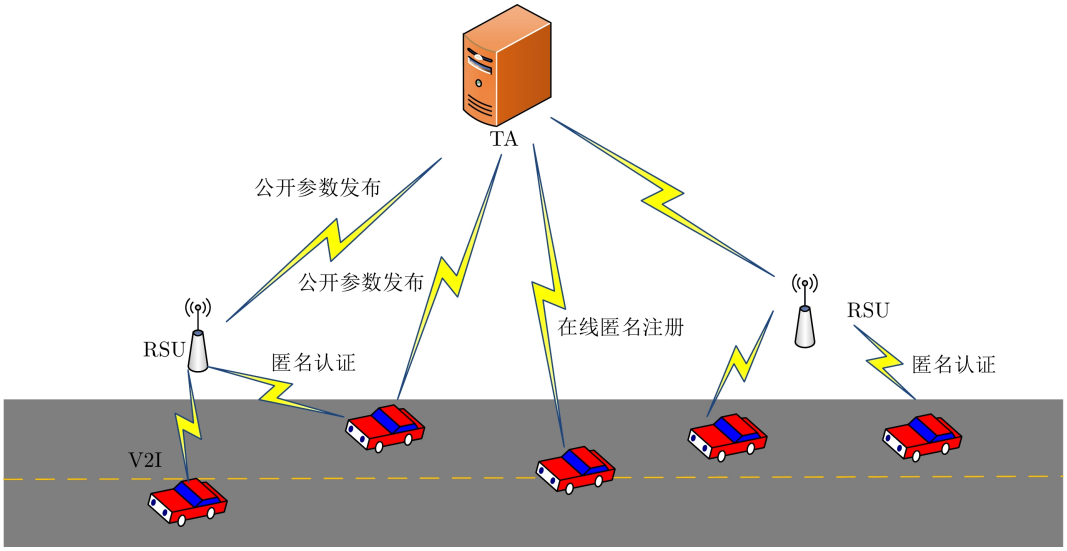

图 1 智能车载自组织网络通信模型

(2) TA随机选取$s \leftarrow Z_q^*$，作为其主私钥，并计算相应的主公钥$\mathrm{PK_{TA}} = sP$。

(3) TA选取5个抗碰撞的哈希函数$H_i : \{0,1\}^* \rightarrow Z_q^*$，$i = 1,2,3,4,5$；TA选取一个轻量级对称加密算法Enc。最后，TA公布系统公开参数$\{E_p(a,b), , P, \mathrm{PK_{TA}}, q, H_1, H_2, H_3, H_4, H_5, \mathrm{Enc}\}$，并且秘密保存主私钥$s$。

在线匿名注册阶段：由智能车辆产生合法匿名身份，并可以在公开信道在线向可信中心TA进行注册，具体流程见表1。

(1) 用户输入个人身份UID_i和用于登录验证的口令PWD_i，计算$\mathrm{UPW}_i = H_1(\mathrm{UID_i}||\mathrm{PWD}_i)$。

(2) 智能车辆V_i(真实身份是RID_i)选择随机数$s_i \leftarrow Z_q^*$，计算$Q_i = H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)P$，$Q_i^* = H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)\mathrm{PK_{TA}}$，以及匿名身份$\mathrm{PSID}_i = \mathrm{Enc}_{Q_{i,y}^*}(\mathrm{RID}_i||\mathrm{PK_{TA}}||T_i||\mathrm{request})$，其中$\mathrm{time}_i$是时间戳，request表明此智能车辆$V_i$请求具体区域匿名认证的服务内容，$T_i$是此匿名身份$\mathrm{PSID}_i$的使用期，$Q_{i,y}^*$是椭圆曲线上点$Q_i^*$的纵坐标。

(3) 智能车辆V_i计算认证值$\mathrm{Auth}_i = H_3(\mathrm{PSID}_i||Q_i||\mathrm{time}_i||T_i||\mathrm{RID}_i)$。将注册信息$\mathrm{Reg}_i = \{\mathrm{PSID}_i, Q_i, \mathrm{time}_i, \mathrm{Auth}_i\}$通过公开信道以匿名的方式发送给TA。可信中心TA接收到来自匿名车辆V_i的注册信息Reg_i之后，执行如下操作：

(4) TA首先判断当前的时间戳time_j，是否满足$\mathrm{time}_j - \mathrm{time}_i \le \Delta\mathrm{time}$，如果不符合要求，则拒绝此次注册请求。如果符合，则TA计算$Q_i^* = sQ_i$，利用Q_i^*的纵坐标进行解密PSID_i，得到相应的RID_i,T_i。

表 1　车辆匿名在线注册流程

(1) 计算$\mathrm{UPW}_i = \mathrm{H_1(UID_i||PWD_i)}$;

(2) 随机选取$s_i \leftarrow Z_q^*$，计算$Q_i = H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)P$;

(3) 计算$Q_i^* = H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)\mathrm{PK_{TA}}$,

$\mathrm{PSID}_i = \mathrm{Enc}_{Q_{i,y}^*}(\mathrm{RID}_i||\mathrm{PK_{TA}}||T_i||\mathrm{request})$;

(4)计算$\mathrm{Auth}_i = H_3(\mathrm{PSID}_i||Q_i||\mathrm{time}_i||T_i||\mathrm{RID}_i)$;

Vehicles $\xrightarrow{\mathrm{Reg}_i = \{\mathrm{PSID}_i, Q_i, \mathrm{time}_i, \mathrm{Auth}_i\}}$ TA

(a) 判断时间戳是否满足time_j - $\mathrm{time}_i \le \Delta\mathrm{time}$;

(b) 计算$Q_i^* = sQ_i$，解密得到RID_i, T_i;

(c) 计算$\mathrm{Auth}_i' = H_3(\mathrm{PSID}_i||Q_i||\mathrm{time}_i||T_i||\mathrm{RID}_i)$;

(d) 判断$\mathrm{Auth}_i' = \mathrm{Auth}$是否相等;

(e) 选择$t_i \leftarrow Z_q^*$，计算$R_i = t_iP$，
$\mathrm{sk}_i = t_i + s\mathrm{H_4(PSID}_i||R_i)$;

(f) $F_i = \mathrm{Enc}_{Q_{i,y}^*}(\mathrm{sk}_i||T_i||\mathrm{request})$。

$\xleftarrow{\{F_i, R_i\}}$

(5) TA计算$\mathrm{Auth}_i' = H_3(\mathrm{PSID}_i||Q_i||\mathrm{time}_i||T_i||\mathrm{RID}_i)$并判断$\mathrm{Auth}_i'$与$\mathrm{Auth}_i$是否相等。如果相等，则TA安全保存智能车辆$V_i$的真实身份$\mathrm{RID}_i$及其注册信息。

签名私钥产生阶段　当TA获取到智能车辆V_i真实有效的身份之后，TA充当基于身份密码系统中的PKG角色，为此匿名智能车辆产生有效的签名私钥，为后续安全认证使用。

(1) TA随机选取$t_i \leftarrow Z_q^*$，并计算$R_i = t_iP$，并为注册成功的智能车辆V_i生成签名私钥$\mathrm{sk}_i = t_i + sH_4(\mathrm{PSID}_i||R_i)$;

(2) TA计算$F_i = \mathrm{Enc}_{Q_{i,y}^*}(\mathrm{sk}_i||T_i||\mathrm{request})$。最后，TA并将$F_i$和$R_i$返回给智能车辆$V_i$。

匿名认证阶段　当智能车辆V_i到达一个敏感区域时，V_i产生一个需要认证的信息M_i，并以匿名的方式发送给邻近的RSU请求与其通信。

(1) V_i随机选取$r_i \leftarrow Z_q^*$，计算$U_i = r_iP = (\xi_i, \zeta_i)$。

(2) V_i获取当前时间戳time_i'，计算$\eta_i = H_5(\mathrm{PSID_i}||M_i||\mathrm{time}_i')$。

(3) V_i计算η_i的数字签名:$\mu_i = \xi_i \mathrm{mod} q$，$\nu_i = (\mathrm{sk}_i + \mu_i r_i \eta_i)\mathrm{mod} q$。

最后，智能车辆V_i发送这个匿名认证信息$\mathrm{Msg}_i = (M_i, U_i, \nu_i, \mathrm{PSID}_i, \mathrm{time}_i', R_i)$给附近的RSU。

匿名认证信息验证阶段　当RSU收到来自智能车辆V_i发送的匿名认证信息Msg_i，RSU执行验证步骤，匿名认证与验证流程见表2。RSU首先判断当前的时间戳$\mathrm{time_j'}$，是否满足$\mathrm{time_j'} - \mathrm{time}_i' \le \Delta\mathrm{time}'$，如果不符合要求，则匿名认证不通过。如果符合要求，则计算$\eta_i = H_5(\mathrm{PSID}_i||M_i||\mathrm{time}_i')$，根据$U_i = (\xi_i, \zeta_i)$，计算$\mu_i = \xi_i \mathrm{mod} q$，并通过验证方程式$\nu_i P = \mu_i \eta_i U_i + R_i + H_4(\mathrm{PSID}_i||R_i)\mathrm{PK_{TA}}$来验证匿名认证信息的完整性：

表 2　匿名认证验证流程

Vehicle	RSU
(1)选择$t_i \leftarrow Z_q^*$，计算$U_i = r_iP = (\xi_i, \zeta_i)$;	
(2)计算$\eta_i = H_5(\mathrm{PSID}_i||M_i||\mathrm{time}_i')$;	
(3)进行签名$\mu_i = \xi_i \mathrm{mod} q$，$\nu_i = (\mathrm{sk}_i + \mu_i r_i \eta_i)\mathrm{mod} q$;	
	Vehicles $\xrightarrow{\mathrm{Msg}_i = (M_i, U_i, \nu_i, \mathrm{PSID}_i, \mathrm{time}_i', R_i)}$ RSU
	(a) 判断时间戳是否满足$\mathrm{time}_j' - \mathrm{time}_i' \le \Delta\mathrm{time}'$;
	(b) 计算$\eta_i = H_5(\mathrm{PSID}_i\|M_i\|\mathrm{time}_i')$，$\mu_i = \xi_i \mathrm{mod} q$;
	(c) 验证$\nu_i P = \mu_i \eta_i U_i + R_i + H_4(\mathrm{PSID}_i\|\|R_i)\mathrm{PK_{TA}}$是否相等。

3.2 批量匿名认证

本协议可支持RSU同时对多个匿名车辆信息进行批量认证。当收到n个智能车辆发来的认证信息$\mathrm{Msg}_i=(M_i,U_i,\nu_i,\mathrm{PSID}_i,\mathrm{time}_i',R_i)$，$i=1,2,\cdots,n$，RSU依次执行以下步骤：

(1) 根据时间戳$\mathrm{time}_i',i=1,2,\cdots,n$来判断当前的时间戳$\mathrm{time}_j'$，是否满足$\mathrm{time}_j'-\ \mathrm{time}_\mathrm{i}'\le\Delta\mathrm{time}'$，如果不符合要求，则匿名认证不通过。

(2) RSU随机选取$\vartheta=\{\vartheta_1,\vartheta_2,\cdots,\vartheta_n\}$，其中每一个$\vartheta_i$在$[1,2^\kappa]$中随机选取的，$\kappa$是一个非常小的整数。对于每一个$i=1,2,\cdots,n$，RSU计算$\eta_i=H_5(\mathrm{PSID}_i||M_i||\mathrm{time}_i')$，根据$U_i=(\xi_i,\zeta_i)$，计算$\mu_i=\xi_i\mathrm{mod}q$。

(3) RSU通过批量验证方程$\left(\sum_{i=1}^n\vartheta_iv_i\right)P=\sum_{i=1}^n\vartheta_i\mu_i\eta_iU_i+\sum_{i=1}^n\vartheta_i(R_i+\mathrm{PK}_\mathrm{TA}H_4(\mathrm{PSID}_i||R_i))$来确保$n$个匿名智能车辆发送认证信息的正确性。

4 正确性与安全性分析

4.1 正确性证明

(1)安全匿名注册的正确性。智能车辆V_i(真实身份是RID_i)能够通过公开信道以匿名方式在TA处进行在线注册，关键在于智能车辆发送的$\mathrm{Reg}_i=\{\mathrm{PSID}_i,Q_i,\mathrm{time}_i,\mathrm{Auth}_i\}$中，$\mathrm{PSID}_i=\mathrm{Enc}_{Q_{i,y}^*}(\mathrm{RID}_i||\mathrm{PK}_\mathrm{TA}||T_i||\mathrm{request})$是通过对称加密算法Enc产生的，这里对称密钥$Q_{i,y}^*$指的是椭圆曲线上点$Q_i^*$的纵坐标，而$Q_i^*=H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)\mathrm{PK}_\mathrm{TA}=H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)sP=\mathrm{s}Q_i$。当收到$\mathrm{Reg}_i=\{\mathrm{PSID}_{,},Q_i,\mathrm{time}_i,\mathrm{Auth}_i\}$，TA也可以有效计算$Q_i^*$，解密$\mathrm{PSID}_i$恢复智能车辆的真实有效身份，为其产生对应签名私钥$\mathrm{sk}_i$，同样用对称加密算法Enc，将通过公开信道返回加密的sk_i给智能车辆V_i。

(2)安全匿名认证的正确性。RSU通过验证方程$\nu_iP=\mu_i\eta_iU_i+R_i+H_4(\mathrm{PSID}_i||R_i)\mathrm{PK}_\mathrm{TA}$来验证智能车辆$V_i$发送的匿名认证信息的完整性。匿名认证方程正确性推导为

$$\begin{aligned}\nu_iP=&(\mu_ir_i\eta_i+\mathrm{sk_i})P\\=&\mu_i\eta_ir_iP+\mathrm{sk_i}P\\=&\mu_i\eta U_i+(sH_4(\mathrm{PSID_i}||R_i)+t_i)P\\=&\mu_i\eta_iU_i+R_i+H_4(\mathrm{PSID_i}||R_i)\mathrm{PK}_\mathrm{TA}\end{aligned}$$

(3)批量安全匿名认证的正确性。RSU通过批量验证方程$\left(\sum_{i=1}^n\vartheta_iv_i\right)P=\sum_{i=1}^n\vartheta_i\mu_i\eta_iU_i+\sum_{i=1}^n\vartheta_i(R_i+\mathrm{PK}_\mathrm{TA}H_4(\mathrm{PSID}_i||R_i))$来确保$n$个匿名智能车辆发送认证信息的正确性。批量匿名认证方程正确性推导为

$$\begin{aligned}&\left(\sum_{i=1}^n\vartheta_i\nu_i\right)P\\&=\left(\sum_{i=1}^n\vartheta_i(\mu_ir_i\eta_i+\mathrm{sk}_i)\right)P\\&=\left(\sum_{i=1}^n\vartheta_i(\mu_ir_i\eta_i+(sH_4(\mathrm{PSID}_i||R_i)+t_i)\right)P\\&=\sum_{i=1}^n\vartheta_i\mu_i\eta_ir_iP+\sum_{i=1}^n\vartheta_i(sH_4(\mathrm{PSID}_i||R_i)+t_i)P\\&=\sum_{i=1}^n\vartheta_i\mu_i\eta_iU_i+\sum_{i=1}^n\vartheta_i(R_i+\mathrm{PK}_\mathrm{TA}H_4(\mathrm{PSID}_i||R_i))\end{aligned}$$

4.2 安全性分析

本节将对本文所提出的协议进行安全性分析，具体包括：安全在线匿名注册，匿名认证信息的完整性，匿名身份的可追踪性。

定理1 该协议可确保智能车辆通过公开信道在可信中心TA处进行有效匿名注册。

证明 在协议中，用户输入自己的身份UID_i和口令PWD_i，同时计算$\mathrm{UPW}_i=H_1(\mathrm{UID}_i||\mathrm{PWD}_i)$，可以保证设备不会知道用户的身份和口令但却能进行登录验证。智能车辆V_i能够自己产生匿名身份，并且对其进行定期更新，以保证更加安全。匿名身份$\mathrm{PSID}_i=\mathrm{Enc}_{Q_{i,y}^*}(\mathrm{RID}_i||\mathrm{PK}_\mathrm{TA}||T_i||\mathrm{request})$，其中$\mathrm{PSID}_i$表示利用$Q_i^*$的纵坐标对真实身份信息$\mathrm{RID}_i$进行对称加密作为车辆的匿名身份。这里$Q_i^*=H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)\mathrm{PK}_\mathrm{TA}=sQ_i$，本质上是采用了Diffie-Hellman密钥交换技术实现车辆与TA的临时密钥协商。如果敌手截获了PSID_i，想要解密得到车辆真实身份RID_i，需要计算：$Q_i^*=sQ_i=H_2(\mathrm{UPW}_i||\mathrm{time}_i||s_i||T_i)sP$，因为$s$为可信中心TA的私钥，$\mathrm{UPW}_i$和$Q_i^*$也是敌手不能有效获取的，因此敌手如果想在多项式时间内计算得到Q_i^*等价于在多项式时间内可以求解基于椭圆曲线的CDH困难问题，这是计算上不可行的。因此智能车辆V_i对于外界来说是匿名的。此外，智能车辆V_i发送的注册阶段消息为$\mathrm{Reg}_i=\{\mathrm{PSID}_i,Q_i,\mathrm{time}_i,\mathrm{Auth}_i\}$，而消息认证值$\mathrm{Auth}_i=H_3(\mathrm{PSID}_i||Q_i||\mathrm{time}_i||T_i||\mathrm{RID}_i)$，根据哈希函数的抗碰撞性，因此即便敌手截获并篡改了PSID_i和Q_i，在TA端计算认证值Auth_i'也会发现与Auth_i不相等，认证不通过。这样保证了注册阶段消息Reg_i的完整性。从而确保了用户匿名身份信息的有效性，以及车辆与TA的正确密钥协商。 证毕

定理2 该协议可确保匿名认证阶段消息的可认证性和完整性。

证明 假设敌手截获消息$\mathrm{Msg}_i=(M_i,U_i,\nu_i,$

PSID_i, time_i', R_i)，其中$\nu_i = (\mu_i r_i H_5(\mathrm{PSID}_i || M_i || \mathrm{time}_j') + \mathrm{sk}_i) \mathrm{mod} q$是车辆利用自己的私钥$\mathrm{sk}_i$对消息$M_i$产生的数字签名，这个正确的匿名认证消息可以通过验证方程：$\nu_i P = \mu_i \eta_i U_i + R_i + H_4(\mathrm{PSID}_i ||R_i)\mathrm{PK}_{\mathrm{TA}}$。如果没有对应的正确私钥$\mathrm{sk}_i$，敌手在多项式时间内想要伪造$M_i$对应的签名$\nu_i^*$，并通过以下验证方程是不可行的：$\nu_i^* P = \mu_i \eta_i U_i + R_i + H_4(\mathrm{PSID}_i||R_i)\mathrm{PK}_{\mathrm{TA}}$。

如果敌手替换、篡改或者一个消息M_i^*，并且通过验证方程：$\nu_i P = \mu_i \eta_i^* U_i + R_i + H_4(\mathrm{PSID}_i||R_i)\mathrm{PK}_{\mathrm{TA}}$，其中$\eta_i^* = H_5(\mathrm{PSID}_i||M_i^*||\mathrm{time}_i')$是计算上不可行的。同样方法分析得知，在批量匿名认证阶段，没有掌握某个车辆的正确私钥，敌手要想在多项式时间内至少伪造其消息的数字签名，或者篡改消息，要想通过批量方程的验证也是计算上不可行的。因此，从以上分析得知，该协议可确保匿名认证阶段消息的可认证性和完整性。　　证毕

定理3　该协议可确保匿名身份的可追踪性。

证明　在此协议中，如果车联网中存在恶意车辆，或者否认自己发送的匿名认证消息，或者交通事故需要追责某些车辆，TA能够利用自己的主私钥s，计算出相应的$Q_i^* = sQ_i$，之后利用其纵坐标解密$\mathrm{PSID_i}$得到相应的真实身份$\mathrm{RID_i}$，实现匿名身份的可追踪性。　　证毕

5　性能分析

本节对本文所提的协议与具有相关功能的协议进行性能分析与比较，这些协议分别是：AAAS协议[14]、Shao协议[16]和Cui协议[18]。协议中所有的算法实现都运行在操作系统为Windows 10，处理器为Intel(R)Core(TM)I5-2320 3.00 GHz和内存为8.00 GB的主机上，所有算法的计算开销时间都使用C语言的版本号为5.6.2密码算法基础函数库MIRACL得出。为了后续可以更方便地进行计算开销分析，用符号Pair, Exp, Mult, mult, Hash, hash, Add, Inv分别表示双线性对运算时间、普通模指数运算时间、椭圆曲线中的倍点运算时间、普通模乘法运算时间、映射到循环群中的哈希运算时间、普通哈希运算时间、椭圆曲线上的加法运算时间、模逆运算时间，具体各密码模块运算时间实验参数见表3。

5.1　计算开销

首先，对本协议和AAAS协议、Shao协议以及Cui协议进行计算开销的分析和对比，主要涉及协议中的车辆(智能车载)和RSU(路边基站单元)的计算开销。

根据文献[14]所提出的AAAS协议分析得知，智能车辆需要执行1次倍点运算获得其与RSU的共享密钥，然后执行3次倍点运算、1次逆运算、1次椭圆曲线上的加法运算和1次哈希到循环群上的运算得到签名信息，并最终发送给RSU进行验证。因此，智能车辆的计算开销为4Mult + Inv + Add + Hash。当RSU接收到车辆发送的信息后，需要执行1次哈希到循环群上的运算得到车辆的公钥，再执行3次双线性对运算、2次倍点运算、1次模乘法运算和1次哈希到循环群上的运算来验证车辆的签名是否合法。因此，RSU总的计算开销为3Pair + 2Mult + mult + Hash。根据文献[16]所提出的Shao协议，分析得知当智能车辆需要进入一个新的RSU通信范围内时，车辆需要发送请求信息给RSU以获得其公钥，再使用RSU的公钥对消息进行加密后将密文发送给RSU进行验证。然后，RSU再计算出群证书后发送给车辆进行验证，确保智能车辆能够加入群组，智能车辆的计算开销为2Exp + 3Pair + mult。而RSU在接收到其通信范围内的智能车辆发送的请求加入群组的消息密文后，需要执行2次双线性对运算、3次模指数运算和1次普通模乘法运算后获得即将为智能车辆颁发的群证书。因此，RSU总的计算开销为3Exp + 2Pair + mult。根据文献[18]提出的Cui协议分析得出，车辆需要执行1次椭圆曲线上的倍点运算、1次普通哈希运算和1次普通的乘法运算生成签名信息发送给RSU进行验证，智能车辆的总计算开销为Mult + hash + mult。当RSU收到车辆的信息后，需要进行3次椭圆曲线上的倍点运算、2次椭圆曲线上的加法运算和2次普通哈希运算来验证签名是否合法，RSU的总开销为3Mult + 2Add + 2hash。在本协议中，智能车辆需要执行1次倍点运算，1次哈希运算，2次乘法运算得到签名信息，并最终发给RSU进行验证，智能车辆的计算开销为Mult + hash + 2mult。当

表 3　密码模块运算时间实验参数

操作类型	符号表示	时间(ms)
双线性对运算	Pair	5.427
普通模指数运算	Exp	1.17
椭圆曲线倍点运算	Mult	2.1652
普通模乘法运算	mult	0.0009
映射到循环群的哈希运算	Hash	5.493
普通哈希运算	hash	0.0078
椭圆曲线上的加法运算	Add	0.0132
模逆运算	Inv	0.631

RSU收到车辆发送的信息之后，需要执行3次倍点运算、2次椭圆曲线上的加法运算和2次普通哈希运算来验证智能车辆签名是否合法。因此RSU的总计算开销为3Mult + 2Add + 2hash。所有协议中的车辆(智能车载)和RSU(路边基站单元)的具体计算开销如表4所示，相关性能实现结果如图2所示。结果表明本设计协议与Cui协议在智能车载和RSU端的计算开销相同，但比AAAS协议和Shao协议要高效得多。同时，由于本设计协议能够实现在线安全匿名注册，而Cui协议不具备这个功能。因此，整体上本协议在计算开销方面占有应用优势，且无需搭建安全信道。

5.2 通信开销

本节对本协议和AAAS协议、Shao协议以及Cui协议中对智能车辆和RSU进行认证时产生的通信开销进行分析与比较，考虑到路边基站单元(RSU)可能同时与多个智能车辆进行通信，其通信开销直接影响这个系统的性能，因此我们侧重对路边基站单元(RSU)的通信开销进行分析与比较。定义$|\mathbb{G}|=1024$ bit为循环群中的元素长度，符号$\xi=32$ bit表示序列号的长度，$|q|=160$ bit表示有限域Z_q中的元素长度，将时间戳和匿名身份有效期时间分别用$|\mathrm{ts}|=32$ bit和$|\mathrm{ex}|=32$ bit表示。

根据文献[14]所提出的AAAS协议分析得知，路边基站单元(RSU)从智能车辆获得的认证信息包括匿名身份信息、时间戳、匿名身份有效期、挑战序列值和数字签名，方案在RSU端的通信开销为$2|q|+2|\mathrm{ts}|+2|\mathrm{ex}|+2\xi+4|\mathbb{G}|$。根据文献[16]所提出的Shao协议，分析得知智能车辆在路边基站单元(RSU)管辖范围时，智能车辆发送加密请求信息给RSU的通信开销为$|\mathbb{G}|$，同时，RSU需要发送加密信息给车辆的通信开销为$|q|+3|\mathbb{G}|$，因此在该协议中，在RSU端总的通信开销为$4|\mathbb{G}|+|q|$。根据文献[18]提出的Cui协议分析得出，智能车辆发送认证消息给路边基站单元(RSU)进行认证，在RSU端的通信开销为$3|\mathbb{G}|+2|q|+|\mathrm{ts}|$。在本协议中，智能车辆发送匿名认证信息$\mathrm{Msg}_i=(M_i,U_i,\nu_i,\mathrm{PSID}_i,\mathrm{time}_i',R_i)$到路边基站单元(RSU)进行认证，通信开销为$2|\mathbb{G}|+3|q|+|\mathrm{ts}|$。所有协议中的智能车辆和RSU进行认证时，在路边基站单元(RSU)产生的通信开销如表5所示，相关性能实现结果如图3所示。结果表明，本协议在RSU端通信开销具有明显优势，同时

表 4 智能车载和RSU端计算开销比较

协议	智能车载通信模块	路边基站单元(RSU)
AAAS协议	4Mult + Inv + Add + Hash ≈ 14.78 ms	3Pair + 2Mult + mult + 2Hash ≈ 26.11 ms
Shao协议	2Exp + 3Pair + mult ≈ 18.63 ms	3Exp + 2Pair + mult ≈ 14.37 ms
Cui协议	Mult + hash + mult ≈ 2.17 ms	3Mult + 2Add + 2hash ≈ 6.54 ms
本协议	Mult + hash + 2mult ≈ 2.18 ms	3Mult + 2Add + 2hash ≈ 6.54 ms

表 5 通信开销比较

协议	单个智能车载认证	n个智能车载认证
AAAS协议	$2\|q\|+2\|\mathrm{ts}\|+2\|\mathrm{ex}\|+2\xi+4\|\mathbb{G}\|$	$2n\|q\|+2n\|\mathrm{ts}\|+2n\|\mathrm{ex}\|+2n\xi+4n\|\mathbb{G}\|$
Shao协议	$4\|\mathbb{G}\|+\|q\|$	$4n\|\mathbb{G}\|+n\|q\|$
Cui协议	$3\|\mathbb{G}\|+2\|q\|+\|\mathrm{ts}\|$	$3n\|\mathbb{G}\|+2n\|q\|+n\|\mathrm{ts}\|$
本协议	$2\|\mathbb{G}\|+3\|q\|+\|\mathrm{ts}\|$	$2n\|\mathbb{G}\|+3n\|q\|+n\|\mathrm{ts}\|$

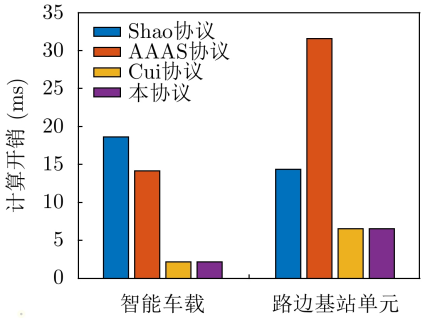

图 2 计算开销对比

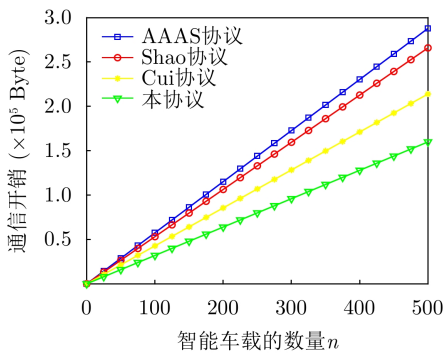

图 3 RSU端通信开销对比

只有本设计协议能够实现在线安全匿名注册，且无需搭建安全信道。

6　结束语

本文提出一种智能车载自组织网络中的匿名在线注册与安全认证协议，使得智能车辆可以在公开信道以匿名的方式远程向可信中心进行在线安全注册并获得认证的签名私钥，避免了搭建安全信道的成本。这样，智能车辆可以与智能交通系统部署的路边基站单元进行匿名认证。在必要的交通事故追责情况下，恶意车辆的真实身份可以被可信中心有效恢复。此外，该协议能够进行批量匿名验证，同一时间验证的消息数目越大，通信开销和计算开销效率优势越明显。

参 考 文 献

[1] ZHANG Lei, HU Chuanyan, WU Qianhong, *et al*. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response[J]. *IEEE Transactions on Computers*, 2016, 65(8): 2562–2574. doi: 10.1109/TC.2015.2485225.

[2] 李兴华, 钟成, 陈颖, 等. 车联网安全综述[J]. 信息安全学报, 2019, 4(3): 17–33. doi: 10.19363/J.cnki.cn10-1380/tn.2019.05.02.

LI Xinghua, ZHONG Cheng, CHEN Ying, *et al*. Survey of internet of vehicles security[J]. *Journal of Cyber Security*, 2019, 4(3): 17–33. doi: 10.19363/J.cnki.cn10-1380/tn.2019.05.02.

[3] 宋昊辰, 杨林, 徐华伟, 等. 智能网联汽车信息安全综述[J]. 信息安全与通信保密, 2020(7): 106–114. doi: 10.3969/j.issn.1009-8054.2020.07.013.

SONG Haochen, YANG Lin, XU Huawei, *et al*. Overview of the intelligent connected vehicles cyber security[J]. *Information Security and Communications Privacy*, 2020(7): 106–114. doi: 10.3969/j.issn.1009-8054.2020.07.013.

[4] WU Qianhong, DOMINGO-FERRER J, GONZALEZ-NICOLAS Ú, *et al*. Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications[J]. *IEEE Transactions on Vehicular Technology*, 2010, 59(2): 559–573. doi: 10.1109/TVT.2009.2034669.

[5] ZHANG Xiaojun, WANG Wenchen, MU Liming, *et al*. Efficient privacy-preserving anonymous authentication protocol for vehicular ad-hoc networks[J]. *Wireless Personal Communications*, 2021, 120(4): 3171–3187. doi: 10.1007/s11277-021-08605-x.

[6] QU Fengzhong, WU Zhihui, WANG Feiyue, *et al*. A security and privacy review of VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2015, 16(6): 2985–2996. doi: 10.1109/TITS.2015.2439292.

[7] LU Rongxing, LIN Xiaodong, LUAN T H, *et al*. Pseudonym changing at social spots: An effective strategy for location privacy in VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2012, 61(1): 86–96. doi: 10.1109/TVT.2011.2162864.

[8] MANVI S S and TANGADE S. A survey on authentication schemes in VANETs for secured communication[J]. *Vehicular Communications*, 2017, 9: 19–30. doi: 10.1016/j.vehcom.2017.02.001.

[9] ALFADHLI S A, LU Songfeng, CHEN Kai, *et al*. MFSPV: A Multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs[J]. *IEEE Access*, 2020, 8: 142858–142874. doi: 10.1109/ACCESS.2020.3014038.

[10] FOTOUHI M, BAYAT M, DAS A K, *et al*. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT[J]. *Computer Networks*, 2020, 177: 107333. doi: 10.1016/j.comnet.2020.107333.

[11] LI Jie, LU Huang, and GUIZANI M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(4): 938–948. doi: 10.1109/TPDS.2014.2308215.

[12] YING Bidi, MAKRAKIS D, and MOUFTAH H T. Privacy preserving broadcast message authentication protocol for VANETs[J]. *Journal of Network and Computer Applications*, 2013, 36(5): 1352–1364. doi: 10.1016/j.jnca.2012.05.013.

[13] WANG Yimin, ZHONG Hong, XU Yan, *et al*. Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs[J]. *Security and Communication Networks*, 2016, 9(18): 5460–5471. doi: 10.1002/sec.1710.

[14] JIANG Yanji, GE Shaocheng, and SHEN Xueli. AAAS: An anonymous authentication scheme based on group signature in VANETs[J]. *IEEE Access*, 2020, 8: 98986–98998. doi: 10.1109/ACCESS.2020.2997840.

[15] AZEES M, VIJAYAKUMAR P, and DEBOARH L J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2017, 18(9): 2467–2476. doi: 10.1109/TITS.2016.2634623.

[16] SHAO Jun, LIN Xiaodong, LU Rongxing, *et al*. A threshold anonymous authentication protocol for VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(3): 1711–1720. doi: 10.1109/TVT.2015.2405853.

[17] XIONG Wanjun, WANG Ruomei, WANG Yujue, *et al*. CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-Insurance in VANETs[J]. *IEEE Transactions on Vehicular Technology*,

2021, 70(4): 3456–3468. doi: 10.1109/TVT.2021.3064337.

[18] CUI Jie, ZHANG Jing, ZHONG Hong, *et al*. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. *Information Sciences*, 2018, 451–452: 1–15. doi: 10.1016/j.ins.2018.03.060.

[19] 曾萍, 郭瑞芳, 马英杰, 等. 车载自组网中可证明安全的无证书认证方案[J]. 电子与信息学报, 2020, 42(12): 2873–2881. doi: 10.11999/JEIT190883.

ZENG Ping, GUO Ruifang, MA Yingjie, *et al*. Provable security certificateless authentication scheme for vehicular Ad hoc network[J]. *Journal of Electronics & Information Technology*, 2020, 42(12): 2873–2881. doi: 10.11999/JEIT190883.

[20] LIU Jingwei, LI Qingqing, SUN Rong, *et al*. An efficient anonymous authentication scheme for internet of vehicles[C]. 2018 IEEE International Conference on Communications, Kansas City, USA, 2018: 1–6. doi: 10.1109/ICC.2018.8422447.

[21] CUI Jie, WU Di, ZHANG Jing, *et al*. An efficient authentication scheme based on semi-trusted authority in VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(3): 2972–2986. doi: 10.1109/TVT.2019.2896018.

[22] JIANG Shunrong, ZHU Xiaoyan, and WANG Liangmin. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2016, 17(8): 2193–2204. doi: 10.1109/TITS.2016.2517603.

张晓均：男，副教授，研究方向为密码学与信息安全、车联网安全、云计算安全.

王文琛：男，硕士生，研究方向为密码学与信息安全、车联网安全.

付　红：女，硕士生，研究方向为密码学与信息安全、车联网安全.

牟黎明：男，硕士生，研究方向为密码学与信息安全、车联网安全.

许春香：女，教授，研究方向为密码学与信息安全、车联网安全、云计算安全.

责任编辑：马秀强