doi:10.11959/j.issn.1000-436x.2016211

面向车联网高效安全的消息认证方案

吴黎兵[1]，谢永[1,2]，张宇波[1,3]
（1. 武汉大学计算机学院，湖北 武汉 430072；2. 景德镇陶瓷大学信息工程学院，江西 景德镇 333403；
3. 武汉大学软件工程国家重点实验室，湖北 武汉 430072）

摘 要：提出一种新型高效的基于身份的消息认证方案，该方案采用椭圆曲线密码构建了轻量级的安全认证协议，无需双线性对运算，降低了签名与认证过程的运算复杂性，同时提供了条件隐私保护的功能，安全分析验证了该方案可以满足 VANET 的安全需求。性能分析表明，与最近的相关方案相比，该方案不仅减少了签名与验证的计算开销，同时也降低了通信开销。

关键词：车联网；认证方案；椭圆曲线密码；效率；条件隐私保护
中图分类号：TP393 **文献标识码**：A

Efficient and secure message authentication scheme for VANET

WU Li-bing[1], XIE Yong[1,2], ZHANG Yu-bo[1,3]
(1. School of Computer Science, Wuhan University, Wuhan 430072, China;
2. School of Information and Engineering, Jingdezhen Ceramic Institute, Jingdezhen 333403, China;
3. State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China)

Abstract: A new efficient identity-based message authentication scheme for VANET was proposed. The proposed scheme decreased the complexity of cryptographic operations on signature by using elliptic curve cryptosystem (ECC) to construct authentication protocol without bilinear pairing and provided the function of conditional privacy-preserving. Security analysis demonstrated that the proposed scheme satisfies all security and privacy requirements for VANET. Performance analysis show that compared with the most recent proposed schemes the proposed scheme decreases the computation cost and communication cost.

Key words: VANET, authentication scheme, ECC, efficiency, conditional privacy preserving

1 引言

随着汽车工业的发展与经济水平的提高，汽车保有量持续快速增长，一方面造成了交通拥堵严重、交通事故频发等问题，另一方面使汽车进一步成为人们不可或缺的工具。因而，人们对行车安全、驾驶舒适的需求越来越急迫。车联网(VANET, vehicular ad hoc network)应运而生，并成为了政府、研究机构与车辆制造企业共同关注的研究热点[1]。VANET 是一种新型的多跳移动无线通信网络，通过多跳无线通信实现车辆相关的众多应用，如安全应用、内容下载与位置服务等应用[2]。VANET 一般包括 4 个主体：装配车载单元(OBU, onboard unit)的车辆、路边设施单元(RSU, roadside unit)、可信机构(TA, trusted authority)以及应用服务器(AS, application server)。其中，车辆 OBU 与其他车辆的 OBU 或 RSU 通过专用短距离通信(DSRC, dedicated short range communication)协议进行通信。在众多车载应用中，安全应用(如协同驾驶、碰撞避免、车道变更告警、拥塞避免等)是 VANET 中最受关注与最重要

收稿日期：2015-09-06；**修回日期**：2016-09-30
通信作者：吴黎兵，wu@whu.edu.cn
基金项目：国家自然科学基金资助项目（No.61272112, No.61472287）；湖北省科技支撑计划基金资助项目（No.2013BAA004）
Foundation Items: The National Natural Science Foundation of China (No.61272112, No.61472287), Hubei Science and Technology Support Program (No.2013BAA004)

的应用之一。为了能够实施这一应用，交通相关的实时信息需要及时收集与处理。依据 DSRC 协议[3]，车辆在行驶过程中每 100~300 ms 广播自身的交通状态信息，如速度、方向、道路状况等。利用这类信息，车辆、RSU 与交通控制应用中心就能实现碰撞避免与道路优化等，进而提高道路安全与交通效率。

由于 VANET 采用无线通信方式，消息在传送过程中很容易遭受恶意的探测、拦截、修改与重放等攻击[4,5]。一个提供错误信息的 VANET 消息，很可能会引发交通事件，甚至有可能造成严重的交通事故。为了保证消息的完整性与可靠性，避免 VANET 受到各种类型的安全攻击，研究者将消息签名与认证技术引入到 VANET 中。车辆或 RSU 在发送消息时需要对消息进行签名，接收者通过验证签名来确定是否接受所收到的消息。面向 VANET 的认证方案需要解决 3 个关键问题。首先，认证方案要满足 VANET 的各种安全需求，抵御各种安全攻击，确保消息来源于可靠实体(注册用户或可信 RSU)。其次，认证方案需要提供高效的签名算法与验证算法：一方面，交通相关的消息数量庞大，特别是汽车保有量持续快速的增长使消息数量直线上升，一个 RSU 或一辆车辆的 OBU 可能同时要验证几百个甚至上千个消息，RSU 或 OBU 因自身有限的计算能力而无法及时完成这些消息的验证[6]，而且面向 VANET 的交通安全相关的消息具有很强的时效性，必须被及时有效地处理，否则可能因处理延误造成交通事故；另一方面，车联网通信具有瞬时性特征，要保证车间通信的可靠性，需提高消息的响应效率，其中，签名效率与验证效率是重要组成部分。因此，VANET 需要高效率的认证方案。最后，认证方案需要提供条件隐私保护：人们对隐私保护的意识越来越强烈，同样希望 VANET 的消息具有匿名性，不能泄露自身真实身份、位置以及其他个人隐私信息；然而，匿名特性是一个双刃剑，恶意注册者可能利用匿名特性，发送虚假消息方式攻击 VANET，此时，认证方案必须能够追踪消息发送者的真实身份，因而条件隐私保护也成了 VANET 另一个需要解决的关键问题。为了解决 VANET 的消息认证方案的这 3 个关键问题，近些年，许多研究者提出各有特色的认证方案[4,6~15]。

利用公共密钥基础设施(PKI, public key infrastructure)密码系统，文献[7~9]分别提出给车辆分配大量证书的匿名认证方案。但这些方案需要车辆事先装配大量的匿名证书，从而产生一个匿名证书的存储与管理的复杂问题[16]，造成这些方案并不适合 VANET。文献[10]提出一种基于群签名的临时匿名证书的认证方案。但该方案因车辆频繁更换认证群造成效率低下的问题。文献[17]提出了一种自持证书的匿名认证算法来减少单个节点的证书存储问题，但证书管理依然是个难解的问题。证书的存储与管理问题成为了制约基于 PKI 的认证方案发展的瓶颈。为了克服签名证书所带来的问题，一些研究者将基于身份的公钥密码系统引入到了 VANET，并提出了一些基于身份公钥密码系统的认证方案[4,6,12~15,18]。基于身份的公钥密码系统是由 Miller 在 1984 年首次提出[19]。在该密码系统中，用户的公钥是由用户的身份信息（如身份标识、E-mail 或其他特征信息）计算得来的，用户的私钥则由可信密钥生成中心生成。基于身份的密码系统可以避免基于 PKI 公钥系统中的证书管理所带来的管理成本高，证书链处理复杂与更换频繁等问题。文献[11]提出了一个面向 VANET 的基于身份的批量认证方案。该方案无须在车辆上存储证书，并提供同时认证多个消息的批量认证方法，大幅度提高了消息的验证效率。然而，文献[12]指出文献[11]方案不能抵抗重放攻击与假扮攻击，并提出一种面向 V2I(vehicle-to-infrastructure)通信的批量认证方案，但是该方案易受到篡改攻击[14]。文献[5]也在文献[11]方案基础上提出了改进方案，为 VANET 用户提供了匿名性且有着更低的计算开销，但该方案不能有效抵抗假扮攻击。2013 年，文献[14]提出了另一种改进方案，并声称可抵抗重放攻击与假扮攻击。但文献[15]指出文献[14]方案不能抵抗重放攻击，并且无法实现追踪消息发送者的真实身份，然后提出一个可实现匿名与身份追踪的认证方案。2015 年，文献[4]提出另一种改进方案，弥补文献[14]方案的不足，具有较好的安全性能。

基于身份的认证方案有效地解决了证书存储与管理的问题，体现了较好的安全性与效率。特别是在近两年，文献[4,14,15]的方案是目前面向 VANET 的认证方案中安全性与计算效率较好的方案。这些方案都采用了双线性对运算。然而，双线性对运算是现代密码学中计算复杂的密码运算之一。相比传统移动传感网络(MANET, mobile ad hoc

network)，VANET 中的 OBU 或 RSU 虽然无需考虑能量问题，但计算能力还是相对有限，这些双线性对运算时效率低下，不满足 VANET 瞬时性对签名与验证效率的苛刻要求。另外，随着车辆保有量的增加，车辆或 RSU 往往同时有大量的 VANET 消息需要认证，特别是面向安全应用的消息更需要及时认证与快速处理，否则很可能造成安全事故。因此，设计一个面向 VANET 的，能同时解决安全性、效率与条件隐私保护 3 个关键问题的认证方案依然是个艰巨的挑战。

为了能解决这些问题，本文提出了一种新型高效的基于身份的消息认证方案。该方案在满足 VANET 的安全需求同时有着更优越的计算与通信性能。本文主要贡献有以下几点。

1) 提出了一个新型的基于身份的认证方案。本方案利用椭圆曲线密码（Schnorr 算法[20]）构建了轻量级的安全认证协议，无需任何双线性对运算，降低了运算的复杂性。本文方案设计了随机假名方法来保护用户隐私，但 TA 可追踪消息的真实身份，实现了条件隐私保护功能。本文方案还提供了同时认证多个签名的批量认证方法。

2) 在随机预言机模型下给出了本文方案的安全性证明，证明了本文方案满足 VANET 的安全需求。

3) 性能分析表明，相比文献[4,14]的方案，本文方案在签名、消息验证中的计算开销分别减少了 82%与 90%，通信开销降低 55%。

2　网络模型与安全需求

2.1　网络模型

VANET 的网络模型主要由 OBU（装配在车辆上）、RSU、TA 以及应用服务器(AS)组成[5,11]，如图 1 所示。在 VANET 中，车辆的 OBU 依据 DSRC 协议与 RSU 或其他车辆的 OBU 进行通信；RSU 装备可信模块，依据 DSRC 协议与车辆的 OBU 进行通信，通过有线网络与 TA、AS 进行通信；TA 具有最高级别的安全防护，是完全可信实体，不可能泄露任何机密信息[11]。TA 为注册的车辆分配一个防篡改装置(TPD，tamper-proof device)。TPD 为车辆提供消息签名时所需要的假名与对应的密钥对，TPD 同时具有高强度的安全特性，可以阻止各类环境下的信息泄露攻击，即攻击无法从该装置上获得所存储的数据[13]。AS 是一些与车辆相关的应用服务，如交通管理应用、娱乐应用等，是 VANET 发展重要内容之一。

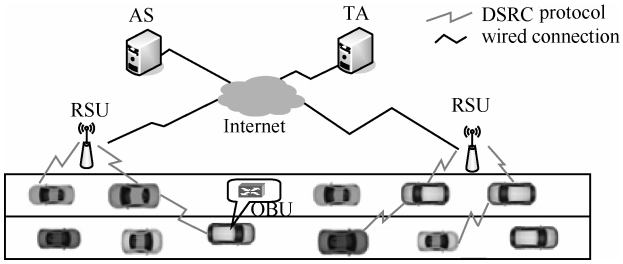


图 1　网络模型

2.2　威胁模型

依据文献[5,11]的定义，网络模型假定了注册的车辆与 RSU 是理性实体，能够诚实地执行既定协议，不会在无利益或明知能被追踪情况下攻击系统，但可能会通过分析已有数据获取其车辆的信息。因此认证方案主要遭受到 3 类安全威胁。1) 不诚实的或自私的车辆或 RSU 节点可能为了个人利益而发送虚假消息；2) 车辆节点的隐私信息在开放通信环境中可能被泄露或被恶意攻击者利用；3) 恶意攻击者会实施各类安全攻击，如窃听、篡改、发布虚假消息，伪造签名以及拒绝服务攻击。

2.3　安全需求

1) 认证性与完整性。在 VANET 中，消息验证者首先要确定消息发送者是否为可靠实体，即注册用户或可信 RSU 等，同时，要确定所收到消息是否为发送者所发送的原始消息，是否被他人修改过。

2) 隐私保护。随着人们隐私保护意识的增强，VANET 必须提供匿名性等隐私保护措施，以保护车辆用户的个人身份、会话记录以及位置等个人隐私信息，确保攻击者不能从截获的消息中获得任何个人隐私信息。

3) 可追踪性。恶意注册者利用匿名性，通过发送虚假消息等方式攻击 VANET；因此，当出现引发争议事件的消息时，认证方案必须能够追踪消息发送者的真实身份，以约束注册者合理使用匿名性。

4) 可抵抗各类安全攻击。VANET 易遭受到各类安全攻击，如假扮攻击与重放攻击等，因此，认证方案需要能抵抗各类安全攻击，以确保认证方案的安全性与可靠性。

3 预备知识

3.1 群概念

定义 1 群：设集合 G 和二元运算为·，若满足以下条件，则称为群 $(G,\cdot)$，常用 G 表示。

1) 封闭性：对任意 $a,b\in G$，有 $(a\cdot b)\in G$。

2) 结合律：对任意 $a,b,c\in G$，有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)\in G$。

3) 单位元：存在单位元 e，使对任意 $a\in G$，都有 $a\cdot e=e\cdot a=a$。

4) 逆元：对任意 $a\in G$，都有逆元 $a^{-1}\in G$，使 $a^{-1}\cdot a=a\cdot a^{-1}\in G$。

3.2 椭圆曲线密码

1984 年，Miller 首次将椭圆曲线应用到密码学中[19]，当 Kobilitz 利用椭圆曲线离散对数问题(ECDLP, elliptic curve discrete logarithm problem)构建了椭圆曲线密码系统(ECC, elliptic curve cryptosystem)[21]后，ECC 就开始被广泛地应用于加密、协议等安全相关领域。

设 F_p 表示阶为大素数 P 的有限域，一个椭圆曲线 E 定义为：$y^2=x^3+ax+b \bmod p$，其中，$a,b\in F_p$。群 G_p 是定义在 E 上的阶为 q、生成元为 P 的点的集合，其中，包含一个无穷远点 $\mathcal{O}$。则 G_p 有如下性质。

1) 加法(+/−)。设 P 与 Q 为 G_p 上的 2 个点，若 $P\neq Q$，则有 $R=P+Q$，R 是 E 与连接 P、Q 两点直线的交点。若 $P=Q$，则有 $R=P+Q$，R 是 E 与 $P(Q)$ 点切线的交点。若 $Q=-P$，则有 $P+Q=P-P=\mathcal{O}$。

2) 标量乘法$(\cdot)$。设 $P\in G_p$，$m\in Z_q^*$，则在 G_p 域上的标量乘法为 $m\cdot P=P+P+\cdots+P$ (共 m 次)。

定义 2 椭圆曲线离散对数问题(ECDLP)：设 G 为椭圆曲线上阶为大素数 q 的有限循环群，P 为群 G 的生成元，设 Q 是 G 上的随机点，求能满足 $Q=x\cdot P$ 的解 x，$x\in Z_q^*$。

如果没有能在运算时间 t 内以不可忽略的概率 ε 解决群 G 上 ECDLP 问题的算法，则称 ECDLP 问题在群 G 中是困难的。

4 新的认证方案

本节提出一种面向车联网高效的基于身份的认证方案。该方案包含 4 个部分：系统建立、假名生成与签名、签名验证和身份追踪。

4.1 系统建立

设 F_p 表示阶为大素数 p 的有限域，TA 定义一个椭圆曲线 E：$y^2=x^3+ax+b \bmod p$，其中，$a,b\in Z_q^*$。从 E 上选择一个阶为 q、生成元为 P 的群 G_p。TA 随机选择 $s_1,s_2\in Z_q^*$ 作为系统的 2 个私钥，并计算出系统的 2 个公钥 $P_{\text{pub}_1}=s_1P$，$P_{\text{pub}_2}=s_2P$。TA 选择 4 个散列函数：$h_1:G\to Z_q$，$h_2:G\times\{0,1\}^*\times\ \{0,1\}^*\to Z_q$，$h_3:G\times\{0,1\}^*\times\{0,1\}^*\to Z_q$，$h_4:\{0,1\}^*\times\{0,1\}^*\times G\times G\times\{0,1\}^*\to Z_q$。最后，TA 公布系统参数 $Paras=\{p,q,a,b,P_{\text{pub}_1},P_{\text{pub}_2},h_1,h_2,h_3,h_4\}$。

当合法车辆向 TA 注册时，提交代表自己唯一身份的 RID 与密码 PWD。TA 则为该车辆装备一个 TPD，TPD 中存储了访问本地 TPD 的 RID 与 PWD，以及系统私钥 s_1、s_2 与系统参数 $Paras$。

4.2 假名生成与签名

车辆在发送消息过程中，利用 TPD 提供假名与密钥对消息进行签名，然后将消息发送给接收者，具体步骤如下。

1) 车辆 V_i 在 TPD 中输入正确的 RID_i 与 PWD_i，然后 TPD 检验输入的 RID_i 与 PWD_i 是否与存储中的一致，若不一致则中止操作，否则继续执行后续步骤。

2) TPD 产生 2 个随机数 $r_i,u_i\in {}_RZ_q^*$ 与时间戳 T_i，然后计算 $R_i=r_i\cdot P$，$U_i=u_i\cdot P$，$PID_i=RID_i\oplus h_1(r_i\cdot P_{\text{pub}_1})$，$h_{r_i}=h_2(PID_i,T_i,R_i)$，$h_{u_i}=h_3(PID_i,T_i,U_i)$，$SK_i^1=s_1\cdot h_{r_i}+r_i \bmod q$，$SK_i^2=s_2\cdot h_{u_i}+u_i \bmod q$，最后将 $\{PID_i,R_i,U_i,SK_i^1,SK_i^2,T_i\}$ 发送给车辆 V_i 的 OBU。

3) 车辆 V_i 的 OBU 利用收到的 $\{PID_i,R_i,U_i,SK_i^1,SK_i^2,T_i\}$ 对消息 M_i 进行签名，计算消息的摘要 $h_i=h_4(M_i,PID_i,T_i,R_i,U_i)$，然后计算出消息的签名 $\delta_i=SK_i^1+h_iSK_i^2 \bmod q$。此时，车辆 V_i 是以假名 PID_i 发送消息 M_i，对应的签名信息为 $\tau_i=\{U_i,R_i,\delta_i\}$。

4) 车辆 V_i 广播消息及签名 $\{M_i,PID_i,T_i,\tau_i\}$。

其中，为了更符合实际应用需求，可以设置步骤 1)在一个使用期间内只需要执行一次。然后，在这期间内，本阶段签名就直接从步骤 2)执行。TPD 工作状态如图 2 所示。

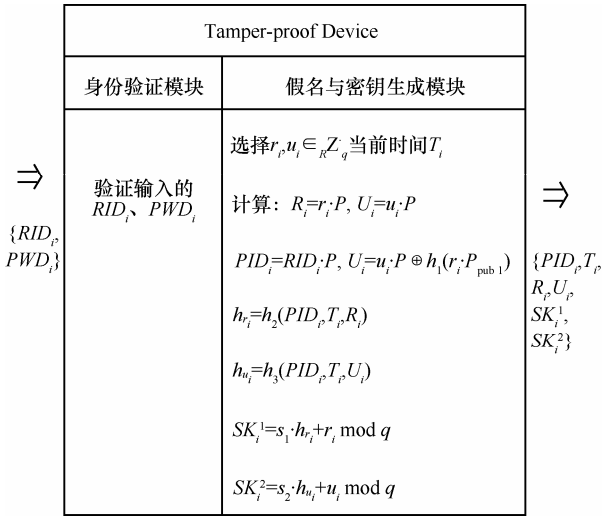


图 2　TPD 工作状态

4.3　消息验证

一旦收到消息$\{M_i, PID_i, T_i, \tau_i\}$，验证者对消息进行验证。消息验证方法可采用单一消息认证或批量消息认证。

1) 单一消息验证。验证者首先验证消息的T_i是否新鲜。若不新鲜，丢弃该消息；否则，计算$h_{r_i}=h_2(PID_i, T_i, R_i)$，$h_{u_i}=h_3(PID_i, T_i, U_i)$，$h_i=h_4(M_i, PID_i, T_i, R_i, U_i)$，然后验证单一消息验证式(1)是否成立。

$$\delta_i \cdot P = h_{r_i} \cdot P_{\text{pub}_1} + h_i \cdot h_{u_i} \cdot P_{\text{pub}_2} + h_i \cdot U_i + R_i \quad (1)$$

如果成立，说明该消息的签名有效，验证者接受该消息；否则，说明该消息的签名无效，丢弃该消息。

2) 批量消息验证。为了提高验证效率，本文方案还提供一种同时处理多个消息的批量认证方法。设验证者当前需要验证 n 个不同的消息$\{M_1, PID_1, T_1, \tau_1\}$、$\{M_2, PID_2, T_2, \tau_2\}$、…、$\{M_i, PID_i, T_i, \tau_i\}$、…、$\{M_n, PID_n, T_n, \tau_n\}$。验证者首先验证这些消息的时间 T 是否新鲜，若是，则将该消息加入批量认证队列，否则丢弃该消息。然后，为了防止敌手攻击批量求和，本文引入随机小因子测试技术[22]，选取较小的整数序列$\lambda=\{\lambda_1, \lambda_2, \cdots, \lambda_i, \cdots, \lambda_n\}$作为随机小因子，其中，$\lambda_i \in [1, 2^{\zeta}]$，$\zeta$ 是随机小因子的安全参数。最后验证批量消息验证式(2)是否成立。

$$\left(\sum_{i=1}^{n} \lambda_i \cdot \delta_i\right) \cdot P = \left(\sum_{i=1}^{n} \lambda_i \cdot h_{r_i}\right) \cdot P_{\text{pub}_1} + \left(\sum_{i=1}^{n} \lambda_i \cdot h_{u_i} \cdot h_i\right) \cdot P_{\text{pub}_2} + \left(\sum_{i=1}^{n} \lambda_i \cdot h_i \cdot U_i\right) + \left(\sum_{i=1}^{n} \lambda_i \cdot R_i\right) \quad (2)$$

若成立，则证明这些消息签名都是有效的，验证者接受这些消息。否则，说明这些消息中至少有一个消息的签名是无效的，验证者可以通过无效签名查找算法[6]进行验证，详情请参见文献[6]，本文不再详述。

4.4　身份追踪

当一个有效签名$\{M_i, PID_i, T_i, \tau_i\}$因争议事件需要追踪车辆的真实身份 RID_i 时，TA 通过 $RID_i = PID_i \oplus h_1(s_1 \cdot R_i)$ 获取消息发送者真实身份。由系统设置可知，只有 TA 拥有系统私钥s_1，因此仅有 TA 可以提取出消息签名者的真实身份。

5　安全性分析

5.1　正确性分析

定理 1　(正确性)　本文方案满足正确性。

证明　认证方案的正确性体现在签名验证过程中验证等式的正确性。依据本文方案在系统建立与签名阶段中的参数设计可得：$P_{\text{pub}_1}=s_1P$，$P_{\text{pub}_2}=s_2P$，$R_i=r_i \cdot P$，$U_i=u_i \cdot P$，$SK_i^1=s_1 \cdot h_{r_i}+r_i \bmod p$，$SK_i^2=s_2 \cdot h_{u_i}+u_i \bmod p$，$\delta_i=SK_i^1+h_i \cdot SK_i^2 \bmod q$。因而，由单一消息验证式(1)可得到

$$\begin{aligned}\delta_i \cdot P &= (SK_i^1 + h_i \cdot SK_i^2) \cdot P \\ &= (s_1 \cdot h_{r_i} + r_i + h_i(s_2 \cdot h_{u_i} + u_i)) \cdot P \\ &= h_{r_i} \cdot P_{\text{pub}_1} + h_i \cdot h_{u_i} \cdot P_{\text{pub}_2} + h_i \cdot U_i + R_i\end{aligned}$$

即式(1)成立，证毕。

由批量消息验证式(2)可以得到

$$\begin{aligned}&\left(\sum_{i=1}^{n} \lambda_i \cdot \delta_i\right) \cdot P = \left(\sum_{i=1}^{n} \lambda_i \cdot (SK_i^1 + h_i \cdot SK_i^2)\right) \cdot P \\ &= \left(\sum_{i=1}^{n} \lambda_i \cdot (s_1 \cdot h_{r_i} + r_i + h_i(s_2 \cdot h_{u_i} + u_i))\right) \cdot P \\ &= \sum_{i=1}^{n} \lambda_i \cdot (s_1 \cdot h_{r_i} \cdot P + r_i \cdot P + h_i \cdot s_2 \cdot h_{u_i} \cdot P + h_i \cdot u_i \cdot P) \\ &= \sum_{i=1}^{n} \lambda_i \cdot (h_{r_i} \cdot P_{\text{pub}_1} + R_i + h_i \cdot h_{u_i} \cdot P_{\text{pub}_2} + h_i \cdot U_i) \\ &= \sum_{i=1}^{n} \lambda_i \cdot (h_{r_i} \cdot P_{\text{pub}_1} + R_i + h_i \cdot h_{u_i} \cdot P_{\text{pub}_2} + h_i \cdot U_i) \\ &= \left(\sum_{i=1}^{n} \lambda_i \cdot h_i\right) \cdot P_{\text{pub}_1} + \left(\sum_{i=1}^{n} \lambda_i \cdot h_i \cdot h_{u_i}\right) \cdot P_{\text{pub}_2} + \left(\sum_{i=1}^{n} \lambda_i \cdot h_i \cdot U_i\right) + \left(\sum_{i=1}^{n} \lambda_i \cdot R_i\right)\end{aligned}$$

即式(2)成立，证毕。

5.2 安全性证明

在随机预言机模型下，利用文献[22]提出安全模型证明本文方案的安全性。

定理 2 (不可伪造性) 在ECDLP问题是困难的情况下，本文方案能够抵抗自适应性选择消息伪造攻击。

证明 假定存在一个攻击者 A 能够在多项式时间内以 ε 的优势伪造一个消息的签名 $\{M_i, PID_i, T_i, \tau_i\}$。给定一个 ECDLP 问题的实例 $(P, Q=xP)$，其中，$P, Q\in G, x\in Z_q^*$。假定一个挑战者 C 充当解决 ECDLP 问题的游戏挑战者，A 利用 C 作为子程序，可以在多项式时间内解决 ECDLP 问题。

挑战者 C 运行系统初始化，定义系统公钥 $P_{\text{pub}_1}=x\cdot P$，$P_{\text{pub}_1}=\varphi\cdot P_{\text{pub}_1}$，秘密保存主密钥 x。然后，C 生成系统参数 $Paras=\{p, q, a, b, P_{\text{pub}_1}, P_{\text{pub}_2}, h_1, h_2, h_3, h_4\}$，同时为 A 维护 Query-Oracle 列表 ℓ_1、ℓ_2、ℓ_3、ℓ_4、ℓ_{sk}，分别用于跟踪 A 对预言机 h_1、h_2、h_3、h_4 以及用户私钥预言机的查询。初始时，这些 Query-Oracle 列表为空。然后将系统参数 *Paras* 发送给 A。挑战游戏开始后，A 将执行如下询问。

1) h_1 预言机查询。列表 ℓ_1 的格式为 $<\theta, \tau_{h_1}>$，当 A 以消息 $\{\theta\}$ 查询时，C 查询列表 ℓ_1。若 ℓ_1 中存在相应的记录 $\{\theta, \tau_{h_1}\}$，则将 τ_{h_1} 发送给 A。否则，C 随机产生 $\tau_{h1}\in Z_q^*$，并将 $\{\theta, \tau_{h_1}\}$ 插入到列表 ℓ_1，并把 τ_{h1} 发送给 A。

2) h_2 预言机查询。列表 ℓ_2 的格式为 $<PID_i, T_i, R_i, \tau_{h_2}>$，当 A 以消息 $\{PID_i, T_i, R_i\}$ 进行查询时，C 查询列表 ℓ_2。若 ℓ_2 中存在相应的记录 $\{PID_i, T_i, R_i, \tau_{h_2}\}$，则把相应的 τ_{h_2} 发送给 A。否则，C 随机产生 $\tau_{h_2}\in Z_q^*$，将 $\{PID_i, T_i, R_i, \tau_{h_2}\}$ 插入到列表 ℓ_2 中，并把 τ_{h_2} 发送给 A。

3) h_3 预言机查询。列表 ℓ_3 的格式为 $<PID_i, T_i, U_i, \tau_{h_3}>$，当 A 以消息 $\{PID_i, T_i, U_i\}$ 进行查询时，C 查询列表 ℓ_3。若 ℓ_3 中存在相应的记录 $\{PID_i, T_i, U_i, \tau_{h_3}\}$，则把相应的 τ_{h_3} 发送给 A。否则，C 随机产生 $\tau_{h_3}\in Z_q^*$，将 $\{PID_i, T_i, U_i, \tau_{h_3}\}$ 插入到列表 ℓ_3 中，并把 τ_{h_3} 发送给 A。

4) h_4 预言机查询。列表 ℓ_4 的格式为 $<M_i, PID_i, R_i, T_i, \tau_{h_i}>$，当 A 以 $\{M_i, PID_i, R_i, T_i\}$ 进行查询时，C 查询列表 ℓ_4。若 ℓ_4 中存在相应的记录 $\{M_i, PID_i, R_i, T_i, \tau_{h_i}\}$，则把相应的 τ_{h_i} 发送给 A。否则，C 随机产生 $\tau_{h_i}\in Z_q^*$，将 $\{M_i, PID_i, R_i, T_i, \tau_{h_i}\}$ 插入到列表 ℓ_4 中，并把 τ_{h_i} 发送给 A。

5) 私钥的查询。C 维护一个私钥列表 $\ell_{sk}=<PID_i, T_i, SK_i^1, SK_i^2>$，A 对给定身份 PID_i 查询私钥时，有如下情况。

① 当 $PID_i=PID_I$ 时，C 停止模拟，输出“⊥”(终止)。

② 当 $PID_i\neq PID_I$ 时，C 随机产生 $h_{r_i}, h_{u_i}, r_i, u_i\in Z_q^*$，计算 $SK_i^1=xh_{r_i}+r_i \bmod q$，$SK_i^2=x\zeta h_{u_i}+u_i \bmod q$，将 $\{PID_I, T_i, SK_i^1, SK_i^2\}$ 添加到列表 ℓ_{sk} 中，同时将 SK_i^1、SK_i^2 发给 A。

6) 签名预言机查询：当 A 以 $sign(M_i, PID_i, T_i)$ 查询时，C 随机产生 $\delta_i, h_{r_i}, h_i\in Z_q^*$，并随机选择 $PID_i, U_i\in G$，则 $h_{u_i}=h_3(PID_i.T_i, U_i)$，C 将 $\{PID_i, T_i, U_i, h_{u_i}\}$ 加入到 ℓ_3 中。再令 $R_i=\delta_i\cdot P-h_{r_i}\cdot P_{\text{pub}_1}-h_i\cdot h_{u_i}\cdot\varphi\cdot P_{\text{pub}_1}-h_i\cdot U_i$，并将 $\{PID_i, T_i, R_i, h_{r_i}\}$ 插入到列表 ℓ_2 中。最后 C 将消息 $\{M_i, PID_i, T_i, R_i, U_i, \delta_i\}$ 发送给 A。

敌手 A 收到消息 $\{M_i, PID_i, T_i, R_i, U_i, \delta_i\}$ 后保存该消息。依据分叉引理[23]，A 以选择不同的 $h_{r_i}^{'}$ 在多项式时间内重新构造消息的另一个有效的签名 $\{M_i, PID_i, T_i, R_i, U_i, \delta_i^{'}\}$。A 所构建的 2 个签名中的 h_i 是相同的，此时 2 个签名分别满足

$$\delta_i\cdot P=h_{r_i}\cdot P_{\text{pub}_1}+h_i\cdot h_{u_i}\cdot\varphi\cdot P_{\text{pub}_1}+h_i\cdot U_i+R_i \quad (3)$$

$$\delta_i^{'}\cdot P=h_{r_i}^{'}\cdot P_{\text{pub}_1}+h_i\cdot h_{u_i}\cdot\varphi\cdot P_{\text{pub}_1}+h_i\cdot U_i+R_i \quad (4)$$

通过式(3)和式(4)可得

$$(\delta_i-\delta_i^{'})\cdot P=(h_{ri}-h_{ri}^{'})\cdot x\cdot P \quad (5)$$

因此，A 可得到 $x=\dfrac{\delta_i-\delta_i^{'}}{h_{r_i}-h_{r_i}^{'}} \bmod q$ 作为 x 解，但求解 x 是一个 ECDLP 问题，由定义 2 可知，一个敌手不可能在一个多项式时间内解决一个 ECDLP 问题。因此，假设不成立，命题得证。

定理 3 （条件隐私保护）在随机预言模型下，本文方案可以同时实现隐私保护与身份可追踪性。

证明　车辆在发送消息时采用了随机假名 PID_i 与随机密钥，假名是由随机数与真实的 RID_i 共同组成，$PID_i = RID_i \oplus h_1(r_i \cdot P_{\text{pub}_1})$，其中，$R_i = r_i \cdot P$。密钥由 2 部分组成，$SK_i^1 = s_1 \cdot h_{r_i} + r_i \bmod q$，$SK_i^2 = s_2 \cdot h_{u_i} + u_i \bmod q$，其中，$r_i, u_i \in Z_q^*$，$T_i$ 为时间戳，$h_{r_i} = h_2(PID_i, T_i, R_i)$，$h_{u_i} = h_3(PID_i, T_i, U_i)$。因此，车辆即使对同一消息进行签名时，由于时间 T_i、随机数据 r_i 和 u_i 每一次都不相同，会产生毫无关联的假名与不同的签名。因此，敌手 A 若要从假名 $PID_i = RID_i \oplus h_1(r_i \cdot P_{\text{pub}_1}) = RID_i \oplus h_1(s_1 \cdot R_i)$ 中进行身份信息攻击，则必须得求解出 $r_i \cdot P_{\text{pub}_1}$ 或 $s_1 \cdot R_i$，依据 ECDLP 问题假设可知，在随机预言模型与未知 r_i、s_1 的情况下求解 $r_i \cdot P_{\text{pub}_1}$ 或 $s_1 \cdot R_i$，在多项式时间内是不可能完成的。因此，本文方案提供身份隐私保护。

本文方案的每一个有效签名 $\{M_i, PID_i, T_i, \tau_i\}$ 都包含了车辆的真实身份 RID_i。当需要追踪消息发送者的真正身份时，可以依据方案中的身份追溯算法进行真实身份，即 TA 通过 $RID_i = PID_i \oplus h_1(s_1 \cdot R_i)$ 计算出消息发送者真实身份。因此，本文方案可以实现身份的可追踪性。

引理 1　本文方案可以抵抗假扮攻击、篡改攻击与重放攻击等安全攻击。

证明　在本文方案中，敌手 A 假扮一个注册车辆 V_i 发送消息 $\{M_i, PID_i, T_i, \tau_i\}$ 时，必须满足验证方程 $\delta_i \cdot P = h_{r_i} \cdot P_{\text{pub}_1} + h_i \cdot h_{u_i} \cdot P_{\text{pub}_2} + h_i \cdot U_i + R_i$。依据定理 2 可知，在随机预言机模型下，敌手要伪造一个签名需要求解一个 ECDLP 问题，但在多项式时间内无法求解出此问题。

敌手 A 将消息 $\{M_i, PID_i, T_i\}$ 的签名 $\tau_i = \{U_i, R_i, \delta_i\}$ 篡改为 $\tau_i' = \{U_i', R_i', \delta_i'\}$。篡改后的签名 τ_i' 需要满足验证方程式。在随机预言机模型下，在不知道系统私钥 s_1 与 s_2 情况下，敌手 A 无法计算出正确的 TPD 产生的 SK_i^1 与 SK_i^2，即无法计算出正确的 δ_i' 满足验证方程 $\delta_i' = SK_i^1 + h_i' \cdot SK_i^2 \bmod q$，最终无法满足验证方程。因此，本文方案可以抵制篡改攻击。

由于本文方案增加了时间戳 T_i，验证者在验证签名时先验证 T_i 是否新鲜。若 T_i 已不新鲜，即可丢弃该消息。因此，本文方案可抵抗重放攻击。

5.3　安全性比较

最近，文献[14]与文献[4]分别提出了基于双线性对的认证方案。文献[14]方案不能抵抗重放攻击，并且无法实现消息发送者真实身份的追踪，文献[4]方案可抵抗各类安全攻击。表 1 列出了文献[14]、文献[4]的方案与本文方案在安全性能方面的对比结果。显然，本文方案与文献[4]方案能满足各种 VANET 的安全需求。

表 1　安全性能对比

性能	文献[14]方案	文献[4]方案	本文方案
可认证性	√	√	√
匿名性	√	√	√
条件追踪	×	√	√
抗伪造攻击	√	√	√
抗篡改攻击	√	√	√
抗重放攻击	×	√	√

说明：√表示满足要求，×表示不满足要求。

6　性能分析

VANET 车间通信具有瞬时性特征，因而通信过程中的计算开销、通信开销、消息丢失率以及延迟是认证协议设计时最重要的评价指标。本节将对本文方案进行性能分析。

6.1　计算开销分析

文献[14]和文献[4]的认证方案采用了双线性对密码，而本文方案采用椭圆曲线密码。为此，本文分别构建了安全级别为 80 bit 不同的 2 个密码运算方案。安全级别为 80 bit 双线性对密码运算方案设置如下：$e: G_1 \times G_1 \to G_2$，其中，加法群 G_1 是由生成元 $\overline{P}$ 生成的阶为 $\overline{q}$ 的加法群，其中，$\overline{P}$ 是度为 2 的超奇异曲线 $\overline{E}: y^2 = x^3 + ax + b \bmod \overline{p}$ 上的点，$\overline{p}$ 是一个 512 bit 的素数，$\overline{q} = 2^{159} + 2^{17} + 1$ 为一个 160 bit 的素数。椭圆曲线密码运算方案设置如下：加法群 G 是由生成元 P 生成的阶为 q 的加法群，P 为非超奇异椭圆曲线 $E: y^2 = x^3 + ax + b \bmod p$ 上的点。其中，p, q 为 160 bit 的素数，$a, b \in Z_p^*$。利用 MIRACL 库[25]，在操作系统为 Win7 系统，CPU 主频为 2.4 GHz，内存为 4 GB 的环境下，本文实现了 2 种密码运算方案中的密码运算，并记录了各个密码运算的执行时间。表 2 给出了密码运算以及对应缩写、执行时间。

表 2 密码运算的执行时间

运算操作名称		缩写	执行时间/ms
双线性对	双线性对运算, $e(P, Q)$	T_b	6.416 4
	标量乘法运算, $x\cdot P$	T_{bm}	2.643 9
	小因子乘法运算, $\lambda_i P$	T_{bsm}	0.826 6
	加法运算, $P+Q$	T_{ba}	0.014 6
椭圆曲线	标量乘法运算, $x\cdot P$	T_{em}	0.735 8
	小因子乘法运算, $\lambda_i P$	T_{esm}	0.042 8
	加法运算，$S+T$	T_{ea}	0.004 0
MapToPoint 散列函数运算		T_H	1.327 7
单向散列函数运算		T_h	0.000 2

在文献[14]方案中，签名过程主要包含了 4 个双线性对密码的标量乘法运算 T_{bm}、1 个双线性对密码的加法运算 T_{ba}、2 个 Map-to-Point 运算 T_H 和 1 个 one-way 的散列运算 T_h，此阶段的总计算开销为 $4T_{bm}+1T_{ba}+2T_H+1T_h$；单一认证过程主要包含 3 个双线性对运算 T_b、1 个双线性对密码的标量乘法运算 T_{bm}、1 个 Map-to-Point 运算 T_H 和 1 个单向的散列运算 T_h，此阶段的计算开销为 $3T_b+1T_{bm}+1T_H+1T_h$；批量认证 n 个签名主要包括了 3 个双线性对运算 T_b、n 个双线性对密码的标量乘法运算 T_{bm}、$3(n-1)$个双线性对密码的加法运算 T_{ba}、n 个 Map-to-Point 运算 T_H 和 n 个单向散列运算 T_h，总和为 $3T_b+nT_{bm}+3(n-1)T_{ba}+nT_H+nT_h$。同样方法可计算出文献[4]方案的计算开销，这里不再列出。

在本文方案中，签名过程中，主要包含了 3 个 ECC 的标量乘法运算 T_{em} 和 4 个单向散列运算，此阶段的总计算开销为 $3T_{em}+4T_h$；单一消息验证过程主要包含 3 个 ECC 的标量乘法运算 T_{em}、3 个 ECC 的标量加法运算 T_{ea} 和 3 个单向散列运算 T_h，此阶段的计算总开销为 $3T_{em}+3T_{ea}+3T_h$；批量消息验证 n 个签名主要包括了 n+3 个 ECC 的标量乘法 T_{em}、n 个 ECC 的小因子标量乘法运算 T_{esm}、$2n$+1 个 ECC 的加法运算 T_{ea} 和 $3n$ 个单向散列运算 T_h，总和为 $(n+3)T_{em}+nT_{esm}+(2n+1)T_{ea}+3nT_h$。

结合表 2 的密码运算的实验数据，3 种认证方案在签名过程、单一消息验证与批量消息验证过程中所需要的计算开销如表 3 所示。从表 3 的结果可以看出：在签名阶段，相比文献[14]方案和文献[4]方案，本文方案在计算开销方面分别节省了约 82%与 84%；在单一认证阶段，相比文献[14]方案和文献[4]方案，本文方案在计算开销方面节省了约 90%。在批量认证阶段，各个方案认证时所需要的计算开销随着消息的数量增加呈线性增长。本文方案 n 的系数为 0.805，而文献[14]方案为 4.015，文献[4]方案是 2.198。因而本文方案在批量认证过程，随着消息数量的增加，认证所增加的计算开销增速要小于文献[14]和文献[4]。图 3 给出了 3 种认证方案在批量认证中计算开销与消息数量之间的线性关系。

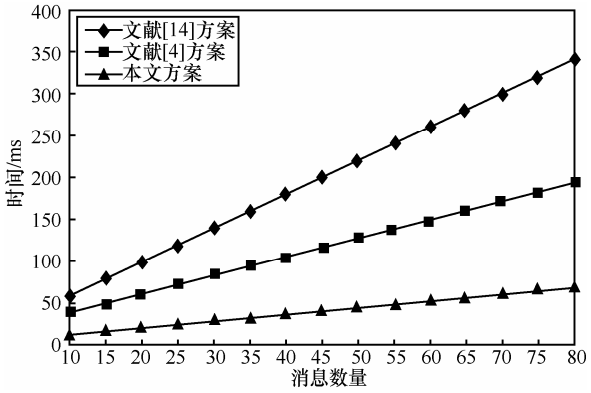


图 3 各类方案批量认证的时间与消息数量的关系

因此，计算开销分析表明本文方案在计算开销方面有着较大的优势，更好地满足了 VANET 对高效的验证算法的需求。

6.2 通信开销分析

由 5.1 节的分析可知，$\overline{p}$ 与 p 所占字节分别是 64 byte 与 20 byte，因此，群 G_1 与群 G 中的元素所占的字节数分别为 128 byte 与 40 byte。假定车联网

表 3 认证协议的计算开销

方案	签名过程	单一认证	批量认证
文献[14]方案	$T_{bm}+1T_{ba}+2T_H+1T_h\approx$13.245 ms	$3T_b+1T_{bm}+1T_H+1T_h\approx$23.220 ms	$3T_b+nT_{bm}+3(n-1)T_{ba}+nT_H+nT_h\approx(4.015n+19.205)$ ms
文献[4]方案	$5T_{bm}+1T_{ba}+1T_H+2T_h\approx$14.562 ms	$3T_b+1T_{bm}+1T_H+1T_h\approx$23.220 ms	$3T_b+nT_{bsm}+3(n-1)T_{ba}+nT_H+nT_h\approx(2.198n+19.205)$ ms
本文方案	$3T_{em}+4T_h\approx$2.262 ms	$3T_{em}+3T_{ea}+3T_h\approx$2.274 ms	$(n+3)T_{em}+nT_{esm}+(2n+1)T_{ea}+3nT_h\approx(0.805n+2.265)$ ms

中消息的时间 T 所占字节数为 4 byte，真实身份的 RID 所占字节数为 20 byte，单向散列函数的值所占字节数 20 byte。

如表 4 所示，在文献[14]方案中，消息由 $\{M_i, ID_i^1, ID_i^2, \delta_i\}$ 组成，其中，$ID_i^1, \delta_i \in G_1$，ID_i^2 ($ID_i^2 = RID_i \oplus h(r \cdot P_{pub_1})$ 为 20 byte)是为签名所增加的通信开销，增加的通信开销总量为 128×2+20= 276 byte；在文献[4]方案中，消息由 $\{M_i, AID_i^1, AID_i^2, T_i, \delta_i\}$ 组成，其中，$AID_i^1, \delta_i \in G_1$，$AID_i^2$ ($AID_i^2 = RID_i \oplus h(r \cdot P_{pub_1})$ 为 20 byte)以及 T_i 是为签名所增加的通信开销，增加的通信开销总量为 128×2+20+4=280 byte；在本文方案中，消息由 $\{M_i, PID_i, T_i, R_i, U_i, \delta_i\}$ 组成，其中，U_i，$R_i \in G$，$\delta_i, PID_i \in Z_q^*$，(其中，$PID_i = RID_i \oplus h_1(r_i P_{pub_1})$，20 byte) 以及 T_i 为签名所增加的通信开销，因此，所增加的通信开销总量为 40×2+20+20+4=124 byte。由此可见，相比文献[4]与文献[14]，本文方案减少了约 55% 的通信开销。因此，本文方案更符合 VANET 的通信需求。

表 4　　通信开销比较

方案	消息组成	增加的通信开销/byte
文献[14]方案	$\{M_i, ID_i^1, ID_i^2, \delta_i\}$	276
文献[4]方案	$\{M_i, AID_i^1, AID_i^2, T_i, \delta_i\}$	280
本文方案	$\{M_i, PID_i, T_i, R_i, U_i, \delta_i\}$	124

6.3　仿真实验

为了验证本文方案在消息丢失率与延迟上的优势，本文利用 OMNeT++仿真平台[25]构建仿真场景。仿真场景的参数设置如下：道路设为总长 12 km 的双向 4 车道公路，每 3 km 部署一个 RSU，每一个 RSU 的通信范围为 800 m，车辆的通信半径为 250 m，且车辆每 300 ms 广播一个消息。车辆的带宽设为 200 kbit/s。车辆的速度由系统在 40~90 km/h 之中随机产生，且车辆速度变化率符合正态分布。车流密度为 5~35 辆/100 m。

图 4 是 3 种方案在仿真实验中消息丢失率与车流密度之间的关系。车流密度越大，则整个系统的通信量越大。从图 4 可以看出，随着车流密度的上升，3 种方案的消息丢失率都在上升。文献[14]方案与文献[4]方案的消息丢失率都增速较快，而本文方案的丢失率增速较慢，且值最低。这主要是因为本文方案减少了消息认证时间，提高消息的接收与处理速度。

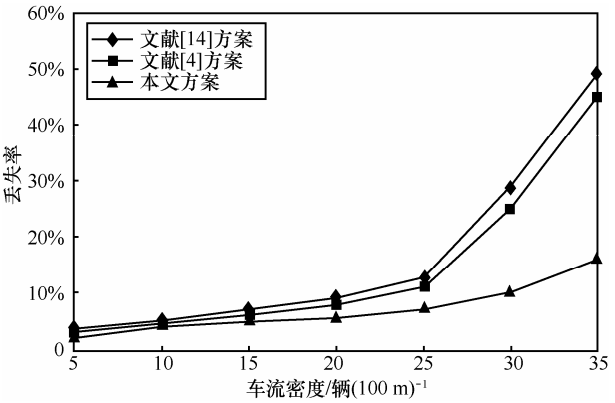


图 4　消息丢失率与车流密度关系

图 5 是 3 种方案在仿真实验中消息延迟与车流密度之间的关系。随着车流密度增加，本文方案的消息延迟有所上升，但增速相比文献[14]与文献[4]的方案小一些。仿真结果进一步验证了本文方案能够减少消息的延迟，提高系统的性能。

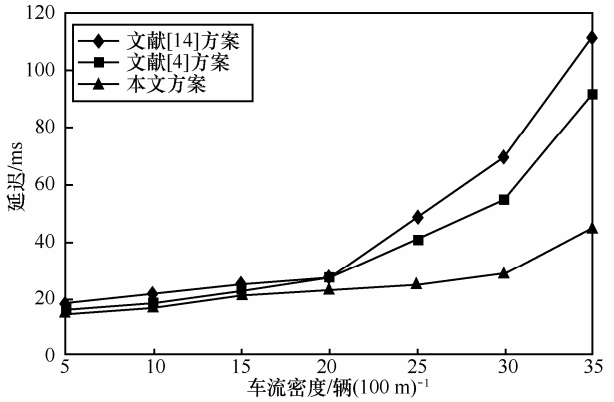


图 5　消息延迟与车流密度的关系

7　结束语

VANET 通信的瞬时性特征对消息签名与认证的效率提出了苛刻要求。为此，本文提出了一种新型高效的条件隐私保护的消息认证方案。本文方案采用椭圆曲线密码构建了轻量级的安全认证协议，无需任何双线性对运算，降低了运算的复杂性。本文方案还提供了批量认证方法，可以同时认证多个签名，进一步提高了签名的认证效率。安全分析证明了本文方案满足 VANET 的各种安全需求。性能分析表明，与其他认证方案相比，本文方案在消息

签名、单一消息验证以及批量消息认证方面都降低了计算开销，同时也减少了通信开销。仿真结果进一步验证了本文方案在消息的丢失率与延迟方面的优势。消息认证技术是 VANET 应用的关键技术之一，还有很多问题有待进一步解决。

参考文献：

[1] KAKKASAGERI M S, MANVI S S. Information management in vehicular ad hoc networks: a review[J]. Journal of Network and Computer Applications, 2014, 39(1): 334-350.

[2] BITAM S, MELLOUK A, ZEADALLY S. VANET-cloud: a generic cloud computing model for vehicular ad hoc networks[J]. IEEE Wireless Communications, 2015, 22(1): 96-102.

[3] IEEE. IEEE standard for WAVE security services for applications and management messages[S]. IEEE. 2013: 1-289.

[4] BAYAT M, BARMSHOORY M, RAHIMI M, et al A secure authentication scheme for VANETs with batch verification[J]. Wireless Networks, 2015, 21(5): 1733-1743.

[5] CHIM T, YIU S, HUI L, et al. SPECS: secure and privacy enhancing communications schemes for VANETs[J]. Ad Hoc Networks, 2011, 9(2): 189-203.

[6] 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.

[7] RAYA M, HUBAUX J P. The security of vehicular ad hoc networks[C]//The 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. 2005:11-21.

[8] FREUDIGER J, RAYA M, FE´LEGYHA Z, et al. Mix-zones for location privacy in vehicular networks[C]//ACM Workshop on Wireless Networking for Intelligent Transportation Systems. 2007.

[9] ZHANG C, LIN X, LU R, et al. RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks[C]// ICC'08, 2008: 1451-1457.

[10] LU R, LIN X, ZHU H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[J]. IEEE INFOCOM Proceedings, 2008: 1229-1237.

[11] ZHANG C, LU R, LIN X, et al. An efficient identity-based batch verification scheme for vehicular sensor networks[J]. Proceedings IEEE INFOCOM'08, 2008:246-250.

[12] SHIM K. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.

[13] LIU J K, YUEN T H, AU M H, et al. Improvements on an authentication scheme for vehicular sensor networks[J]. Expert Systems with Applications, 2014, 41(5): 2559-2564.

[14] LEE C C, LAI Y M. Toward a secure batch verification with group testing for VANET[J]. Wireless Networks, 2013, 19(6): 1441-1449.

[15] ZHANG J, XU M, LIU L. On the security of a secure batch verification with group testing for VANET[J]. International Journal of Network Security,2014, 16(5): 355-362.

[16] SHIM K. An ID-based aggregate signature scheme with constant pairng computations[J]. Journal of Systems and Software, 2010, 83(10):1873-1880.

[17] 李晋国, 林亚平, 李睿, 等. 车载自组织网络中基于椭圆曲线零知识证明的匿名安全认证机制[J]. 通信学报, 2013, 34(5): 52-61.
LI J G, LIN Y P, LI R, et al. Secure anonymous authentication scheme based on elliptic curve and zero-knowledge proof in VANET[J]. Journal on Communications, 2013, 34(5): 52-61.

[18] HORNG S J, TZENG S F ,PAN Y, et al. B-SPECS+: batch verification for secure pseudonymous authentication iv VANET[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1860-1875.

[19] MILLER V S. Use of elliptic curves in cryptography[C]//CRYPTO'85 Proceedings. 1985: 417-426.

[20] SCHNORR C P. Efficient identification and signatures for smart cards[M]// Advances in Cryptology — EUROCRYPT '89. Springer Berlin Heidelberg. 1989: 688-689.

[21] KOBLITZ N. Elliptic curve cryptosystem[J]. Journal of Mathematics of Computation, 1987, 48(1): 203-209.

[22] YUAN Y, LI D, TIAN L, et al. Certificateless signature scheme without random oracles[C]//Information Security and Assurance. Springer Berlin Heidelberg, 2009: 31-40.

[23] POINTCHEVAL D, STERN J. Security proofs for signature schemes[C]//EUROCRYPT'96. 1996: 387-398.

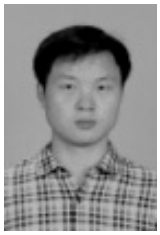
[24] MIRACL library on Certivox.com[EB/OL]. https://www.certivox.com/miracl.

[25] 谢永, 吴黎兵, 何炎祥, 等. 无间隙的车联网协助下载方法[J]. 通信学报, 2016, 37(1): 180-190.
XIE Y, WU L B, HE Y X, et al. Non-intermittent cooperative downloading approach for VANET[J]. Journal on Communications, 2016, 37(1) :180-190.

作者简介：

吴黎兵（1972-），男，湖北黄梅人，武汉大学教授、博士生导师，主要研究方向为分布式计算、网络性能与服务质量、可信软件。

谢永（1978-），男，湖南郴州人，武汉大学博士生，景德镇陶瓷大学副教授，主要研究方向为车联网、下一代网络与网络安全。



张宇波（1988-），男，湖北武穴人，武汉大学博士生，主要研究方向为密码学、协议安全分析。