隐私保护的 VANET 警告消息发布协议

刘辉[1,2]，刘鑫衍[1]，许艳[1]，仲红[1]，王梦[1]
（1. 安徽大学计算机科学与技术学院，安徽 合肥 230601；2. 安徽大学电子信息与工程学院，安徽 合肥 230601）

摘 要：针对交管部门向车辆发布违章消息的问题，提出了一种隐私保护的警告消息发布协议。在该协议中，交通管理部门可以根据车辆的真实身份获取车辆假名，并通过车辆假名向 VANET 中的车辆发布警告消息。所提协议采用椭圆曲线密码体制，构造了轻量级的警告消息发布和接收过程。此外，所提协议实现了条件隐私保护，能够有效保护警告消息接收车辆的身份隐私。最后，安全性分析表明，所提协议可以满足 VANET 的安全要求。性能分析表明，所提协议有着较低的计算开销和通信开销。

关键词：车载自组织网络；警告消息发布；条件隐私保护；椭圆曲线密码体制
中图分类号：TP309
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021135

Privacy protection of warning message publishing protocol in VANET

LIU Hui[1,2], LIU Xinyan[1], XU Yan[1], ZHONG Hong[1], WANG Meng[1]
1. School of Computer Science and Technology, Anhui University, Hefei 230601, China
2. School of Electronics and Information Engineering, Anhui University, Hefei 230601, China

Abstract: Aiming at the problem that the traffic control department publishes violation messages to vehicles, a privacy protection warning message publishing protocol was proposed, where transportation manage department could obtain vehicle's pseudonym according to its real identity and send warning message to vehicles based on its pseudonym in VANET. Elliptic curve cryptography was used to construct a lightweight warning message publishing and receiving process. Furthermore, the conditional privacy protection was realized, which could effectively protect the identity privacy of the receiving vehicle. Security analysis shows that the proposed protocol can meet the security requirements of VANET. Performance analysis shows that the protocol protocol has lower computational overhead and communication overhead.

Keywords: VANET, warning message publishing, conditional privacy protection, elliptic curve cryptography

1 引言

车载自组织网络（VANET, vehicle ad-hoc network）是智能交通系统（ITS, intelligent traffic system）的核心组成部分[1]，可帮助驾乘人员和交通管理人员获得实时全面的交通信息，减少交通事故的发生。为了实现交通信息的交互，VANET 包含 2 类通信节点：部署在车辆中的车载单元（OBU, on-board unit）和固定于路边的基础设施单元（RSU, road side unit）。OBU 和 RSU 使用专用短程通信（DSRC, dedicated short range communication）协议[2]，实现车车通信（V2V, vehicle-to-vehicle）、车辆与 RSU 通信（V2I, vehicle-to-infrastructure）、RSU 与车辆通信（I2V, infrastructure-to-vehicle）。

然而，DSRC 协议是无线通信协议，传输的数据容易被监听、修改和伪造[3]。车辆或 RSU 在接收

收稿日期：2021−03−22；修回日期：2021−06−22
通信作者：许艳，xuyan@ahu.edu.cn
基金项目：国家自然科学基金资助项目（No.61702005）
Foundation Item: The National Natural Science Foundation of China (No.61702005)

消息时需确认消息来源的合法性以及消息的完整性。此外，车辆身份关乎驾乘人员的生命财产安全，除了需要确认消息来源的合法性以及消息的完整性，VANET 还需保护车辆的身份隐私。同时，当车辆发生交通事故或产生违规行为时，还需要对恶意车辆进行追责。这种能够保护车辆的身份隐私，但在必要时又可追踪车辆真实身份的行为被称为条件隐私保护。2007 年，Raya 等[4]提出了一种基于公钥基础设施（PKI, public-key infrastructure）的条件隐私保护认证方案来实现车辆身份和消息完整性的验证。随后，学者提出 VANET 条件隐私保护协议，以实现安全的 V2V 或 V2I 认证。

已有的 VANET 条件隐私保护协议多考虑对车辆发布的消息进行验证[4-13]。然而，在 VANET 中也需要考虑对 RSU 发布的消息进行认证，因为交通管理部门（TMD, transportation manage department）可通过 RSU 向车辆发布与车辆相关的交通信号、路况信息或者车辆的违章信息等。此外，在车辆行驶过程中 TMD 捕获到的是道路上行驶车辆的真实身份，如车牌号码等。随后，TMD 经由 RSU 给车辆发送的警告信息，包含的也是车辆的真实身份。而在 VANET 中，为了保护身份隐私，车辆往往使用假名进行通信。所以 TMD 在经由 RSU 向车辆发布警告消息之前需要根据车辆的真实身份获取车辆的假名。但是，在 VANET 中车辆的真实身份和假名应是难以相互推导的。已有的 VANET 条件保护隐私协议，往往研究的是可信第三方可以根据假名追踪出车辆的真实身份。而如何由真实身份推导出车辆的假名，目前的研究较少。

本文提出隐私保护的 VANET 警告消息发布协议，TMD 在发布违章消息之前能够根据车辆的真实身份及时获取车辆假名，从而经由 RSU 给车辆发送警告消息。

本文的主要贡献如下。

1) 提出条件隐私保护的警告消息发布协议，该协议可以根据车辆的真实身份及时获取车辆假名。此外，TMD 也可以通过车辆假名追踪到车辆的真实身份，实现条件隐私保护。

2) 采用签密技术实现 I2V 认证，在实现车辆对 RSU 身份认证的同时保护警告消息涉及车辆的身份隐私。

3) 采用椭圆曲线密码体制（ECC, elliptic curve cryptography）实现车辆执行的验证过程，不依赖于双线性对，有较高的计算效率。实验分析表明，所提协议有较低的计算开销和通信开销。

2　相关工作

2008 年，Lu 等[5]提出了一个高效的条件隐私保护协议，实现了可追踪的匿名认证。该协议能够在 OBU 和 RSU 之间生成实时的临时匿名密钥，最小化存储临时匿名密钥所需的存储空间。但是在该协议中，车辆需要频繁地向 RSU 申请匿名证书，导致 RSU 需要维护庞大的证书列表。同年，Zhang 等[6]采用假名技术来为车辆假名生成私钥。该协议不需要向 RSU 申请证书，减轻了 RSU 的负担。2011 年，Zhang 等[7]提出带有群测试的支持批验证的 VANET 条件隐私保护协议。Lee 等[8]指出文献[7]提出的协议不能抵抗重放攻击，并提出一个新的基于身份的批验证协议。文献[9-11]指出 Lee 等[8]方案也存在安全缺陷，即恶意车辆能够伪造其他车辆的合法签名。但是，文献[9-11]采用耗时的双线性对操作。为了减少计算开销，文献[12-13]提出无双线性配对的面向车联网高效安全的消息认证方案，这些方案基于 ECC，具有较高的计算效率。然而，上述协议虽然保护了车辆的身份隐私、消息的完整性和消息来源的合法性，但没有考虑到消息的机密性，未授权的车辆可能会获取敏感的违章信息[5-13]。

为实现传输消息的机密性，Rabieh 等[14]使用同态加密技术构造了隐私保护的交通信息上报协议，但是加密后再进行签名会造成很大的时延。为减少对消息加密和签名的总计算开销和通信开销，Zheng[15]提出了签密的概念，实现了在一个步骤内同时完成加密和签名操作。2017 年，Basudan 等[16]将签密技术于应用于路况监测。2019 年，Wang 等[17]提出基于源认证的隐私保护云路况监测方案，将路况信息以密文形式上报给云服务器，云服务器需要在路况信息是密文的情况下验证消息来源，但该方案无法追踪恶意车辆的真实身份。为解决文献[17]无法追踪恶意车辆真实身份的问题，韩牟等[18]提出一种 VANET 高效群密钥协商协议，但该协议使用了较耗时的双线性对操作。2020 年，为提高计算效率，Xu 等[19]构造了车辆的身份可追踪的路况检测协议，该方案无双线性对操作。2021 年，Elkhali 等[20]提出一种适用于车联网异构系统的高效签密方案，但该方案未考虑车辆的匿名性。Ali 等[21]提

出一种异构车联网中条件保密的混合签密方案，解决了文献[20]中车辆的匿名性问题。

3 预备知识

3.1 系统模型

本文采用的系统模型包括 4 个参与者：可信中心（TA, trusted authority）、TMD、车辆和 RSU。如图 1 所示，系统模型的上层由 TA 和 TMD 组成，底层由 RSU 和若干车辆组成。TA、TMD 和 RSU 可以通过安全套接字层（SSL, secure socket layer）协议进行安全通信。RSU 与车辆、车辆与车辆之间可以通过 DSRC 协议进行通信。这些参与者的详细情况介绍如下。

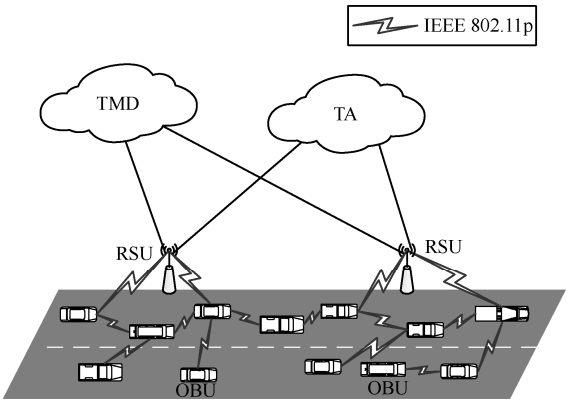

图 1 系统模型

TA 是可信第三方，具有较强的计算能力。负责生成系统参数，并为 TMD、车辆等参与者进行注册。

TMD 是高度可信的交通管理部门，可以捕获车辆违章消息，并经由 RSU 给车辆发送警告消息，是唯一能够追踪车辆真实身份的参与者。

RSU 是半可信的，诚实遵守协议但对车辆的隐私好奇。RSU 能够使用 DSRC 协议与车辆通信，验证车辆发送的消息的有效性。TA、TMD 与车辆的通信通过 RSU 进行消息传递。

车辆配备了支持 DSRC 协议的 OBU。车辆通过 OBU 与 RSU 进行无线通信。此外，车辆配有防篡改设备（TPD, temper-proof device）。

3.2 安全需求

安全和隐私对 VANET 通信都相当重要。基于 VANET 安全和隐私研究的相关文献[12-17,19], 本文提出的 VANET 警告消息发布协议应满足以下安全要求：消息认证、身份隐私保护、可追溯性、保密性和抗攻击性。

1) 消息认证。车辆能够认证 RSU 发送消息的有效性。此外，车辆能够确认接收消息是否被修改，即车辆可以对收到消息的来源以及消息的完整性进行认证。

2) 身份隐私保护。RSU 与其他车辆无法获得其他车辆的真实身份，即除 TMD 外的任何第三方都无法通过分析截获的信息获得车辆的真实身份。

3) 可追溯性。TMD 可以在必要时追踪车辆的真实身份。例如，当恶意车辆发送错误消息来误导他人时，TMD 可以追踪恶意车辆的真实身份。

4) 保密性。TMD 发送给车辆的消息是保密的，任何其他车辆都无法获取 TMD 发送给指定车辆的消息内容。

5) 抗攻击性。本文提出的协议能够抵御各种常见的攻击，如伪造攻击、修改攻击以及重放攻击。

3.3 困难问题

本文主要用到椭圆曲线密码学中的 2 个困难问题，分别是椭圆曲线离散对数问题（ECDLP, elliptic curve discrete logarithm problem）和椭圆曲线 Diffie-Hellman 问题（ECDHP, elliptic curve Diffie-Hellman problem）。

1) ECDLP。设 G 是阶为 q 的椭圆曲线，存在 $P,Q\in G$，$a\in Z_q^*$，$Q=aP$，$0\leqslant a\leqslant q-1$，若 P 和 Q 是已知的，则计算出整数 a 属于 ECDLP。

2) ECDHP。P 是阶为 q 的群的生成元，对于任意 $a,b\in Z_q^*$，若 P,aP,bP 已知，则计算出 abP 属于 ECDHP。

3.4 安全模型

本节给出“攻击−挑战”游戏的形式化定义，该模型可用于证明协议的不可伪造性和保密性。

3.4.1 不可伪造性

游戏由系统初始化、询问和伪造 3 个阶段组成，参与者为敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$，具体步骤如下。

1) 系统初始化。$\mathcal{C}$ 生成系统私钥 x 和公开参数 params，然后将 params 发送给 $\mathcal{A}$，并维护查询队列记录预言机询问及密钥生成询问的数据。

2) 询问。$\mathcal{A}$ 向 $\mathcal{C}$ 发起 $h_i(i=1,2,3)$ 询问，当 $\mathcal{A}$ 调用 h_i 并且使用参数 m 查询时，$\mathcal{C}$ 选取 $h\in_R Z_q$，将 (m,h) 插入查询队列 L_h，并将 h_i 返回给 $\mathcal{A}$。以上询问是自适应的，即执行每一次询问时都可以根据前一次询问的结果进行调整。

3) 伪造。$\mathcal{A}$ 输出元组 $(\sigma^*,\mathrm{ID}_{\mathrm{TMD}},\mathrm{AID}_i)$ 作为对

签名的伪造，$\mathcal{C}$ 将上述元组提交给预言机进行询问。预言机将 σ^* 的验证结果返回给 $\mathcal{C}$，如果 σ^* 不是由询问产生，AID_i 未执行过询问，且验证成功，则 $\mathcal{A}$ 赢得游戏。$\mathcal{A}$ 赢得游戏的优势定义为 $\mathrm{Adv}(\mathcal{A})=\Pr[\mathrm{Succ}(\mathcal{A})]$。

定义 1　对于任意敌手 $\mathcal{A}$，在多项式时间均不能以不可忽略的优势赢得上述游戏，则称协议在适应性选择明文攻击下具有不可伪造性（EUF-CMA, existentially unforgeable against chosen-message insider attack）。

3.4.2　保密性

游戏由系统初始化、询问、挑战和猜测 4 个阶段组成，参与者为敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$，具体步骤如下。

1) 系统初始化。$\mathcal{C}$ 生成系统私钥 x 和公开参数 params，然后将 params 发送给 TMD，并维护各个查询队列记录预言机询问及密钥生成询问的数据。

2) 询问。$\mathcal{A}$ 向 $\mathcal{C}$ 发起如下询问。

① 密钥生成询问。$\mathcal{A}$ 输入身份 $\mathrm{ID}_{\mathrm{TMD}_i}$，$\mathcal{C}$ 查询私钥列表，产生私钥 x_j 发送给 $\mathcal{A}$。

② 签密询问。$\mathcal{A}$ 输入发送者和接收者身份 $\mathrm{ID}_{\mathrm{TMD}}$、$\mathrm{AID}_i$、明文 m_i，$\mathcal{C}$ 查找发送者的私钥 x_j，并向预言机进行签密询问，最后将询问结果 σ 返回给 $\mathcal{A}$。

③ 解签密询问。$\mathcal{A}$ 以 $\mathrm{ID}_{\mathrm{TMD}}$、$\mathrm{AID}_i$ 和 σ 进行询问，$\mathcal{C}$ 计算接收者秘密值 v_i，并以相同的输入向预言机进行解签密询问，预言机将 m_i 返回给 $\mathcal{C}$，$\mathcal{C}$ 再发送给 $\mathcal{A}$。

以上询问是自适应的，即执行每次询问都可以根据前一次询问结果调整。

3) 挑战。

① $\mathcal{A}$ 选择消息 m_0、m_1 和挑战的身份 $\mathrm{ID}_{\mathrm{TMD1}}$、$\mathrm{AID}_{i1}$，其中 $\mathrm{ID}_{\mathrm{TMD1}}$ 和 AID_{i1} 未进行过密钥生成询问。

② $\mathcal{C}$ 随选择 $b\in_R 0,1$，并将 m_b、$\mathrm{ID}_{\mathrm{TMD1}}$、$\mathrm{AID}_{i1}$ 及 x_j、params 作为预言机的输入进行签密询问，预言机返回询问结果 σ^*，并发送给 $\mathcal{A}$。

③ $\mathcal{A}$ 可以进行多项式次询问，但不能对 $\mathrm{ID}_{\mathrm{TMD1}}$ 和 AID_{i1} 进行密钥生成询问，也不可以对 σ^* 进行解签密询问。

4) 猜测。$\mathcal{A}$ 输出 $b\in_R 0,1$ 作为对 b 的猜测，$\mathcal{A}$ 赢得游戏的优势为 $\mathrm{Adv}(\mathcal{A})=|\Pr[b'=b]-1/2|$。等式 $b'=b$ 成立的概率即为 $\mathcal{A}$ 赢得游戏的概率。

定义 2　对于任意敌手 $\mathcal{A}$，在多项式时间内不能以不可忽略的优势赢得上述游戏，则称该协议是抗选择密文内部攻击安全（SC-IND-CCA, semantically secure against chosen ciphertext insider attack）。

4　提出的协议

本文提出隐私保护的 VANET 警告消息发布协议包括 5 个阶段：系统设置、TMD 注册、车辆注册、警告消息发布、警告消息接收。车辆在 VANET 中使用的身份是其假名，而 TMD 发布警告消息之前已经知道车辆的真实身份（如车牌号码）。本文协议实现了通过车辆的真实身份获取车辆的假名。

4.1　系统设置

TA 在此阶段执行以下步骤。

1) 设 F_p 是一个有限域，p 是素数，TA 定义椭圆曲线 $E: y^2=x^3+ax+b \bmod p$，其中 $a,b\in Z_q^*$。

2) TA 从 E 上选择一个阶为 q、生成元为 p 的加法循环群 G，它由椭圆曲线 E 和无穷远点 O 组成。假设 G 中的每个元素都可以用 l 位长的二进制字符串表示。TA 选择随机数 $x\in Z_q^*$ 作为系统的私钥，并计算系统公钥 $P_{\mathrm{pub}}=xP$。

3) TA 选择 3 个安全的哈希函数 $h_1:\{0,1\}\to Z_q^*, h_2:\{0,1\}^n\times G^3\to Z_q^*, h_3: G^3\to\{0,1\}^n+2l$，其中 n 表示明文的长度，并且是 k 的多项式。

4) TA 为每个车辆分配一个真实身份 RID 和一个密码 PWD，并 $\{\mathrm{RID},\mathrm{PWD},x\}$ 预加载到其 TPD 中。

5) TA 将系统参数 $\mathrm{parmas}=\{p,q,a,b,P,P_{\mathrm{pub}},h_1,h_2,h_3\}$ 发送给 TMD、RSU 和车辆。

4.2　TMD 注册

TMD 使用其真实身份 $\mathrm{ID}_{\mathrm{TMD}}$ 向 TA 注册。

1) TA 生成一个随机数 $u_j\in Z_q^*$，并计算 $U_j=u_jP$，$\alpha_j=h_1(\mathrm{ID}_{\mathrm{TMP}}\|\mathrm{VP}_i)$，$x_j=u_j+a_jx \bmod q$，其中 VP_i 是有效期，x_j 作为 TMD 的私钥。

2) TA 通过安全信道将 u_j 和 x_j 发送到 TMD。同时，TMD 通过 RSU 广播 U_j 和 α_j。TMD 定时生成有效期 VP_i，通过安全信道将 VP_i 发送给车辆。

4.3　车辆注册

1) 车辆将真实身份 RID（如车牌号码）和密码 PWD 输入 OBU。OBU 检查 RID 和 PWD 是否等于存储的 RID 和 PWD。如果其中之一与相应存储的不相等，则 OBU 将要求所有者再次输入正确的身

份和密码。

2) OBU 计算 $v_i=h_1(\mathrm{RID}\|\mathrm{VP}_i)$，$V_i=v_iP$，$\mathrm{AID}_i=E_{\mathrm{ID_{TMD}}}[\mathrm{RID}\oplus v_iU_j]$。OBU 经由 RSU 将 V_i 发送给 TMD。

4.4 警告信息发布

TMD 将违章消息发送给目标车辆 RID。TMD 在发布违章消息前需要根据车辆的真实身份（如车牌号码）计算出车辆假名。此阶段 TMD 执行以下步骤。

1) TMD 使用 RID、V_i、u_j 和 x_j 计算得到车辆的匿名身份 $\mathrm{AID}_i=E_{\mathrm{ID_{TMD}}}[\mathrm{RID}\oplus v_iU_j]$。

2) TMD 选择一个随机的 $r_j\in Z_q^*$，计算 $R_j=r_jP$，并在 RSU 的帮助下将 R_j 发送给车辆。

3) TMD 计算 $V=x_j+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)r_j \bmod q$，$Z=\left(m_i\left\|\mathrm{ID_{TMP}}\right\|V\right)\oplus h_3\left(R_j,\mathrm{AID}_i,r_jV_i\right)$。签密文为 $\sigma=\left(\mathrm{AID}_i,R_j,Z\right)$，并且 $\sigma=\left(\mathrm{AID}_i,R_j,Z\right)$ 通过 RSU 在其通信范围内广播。

4.5 警告信息接收

当车辆收到密文 $\sigma=(\mathrm{AID}_i,\ R_j,Z)$ 时，车辆执行以下步骤。

1) 计算 $D_i=v_iR_j$。

2) 计算 $(m_i\|\mathrm{ID_{TMD}}\|V)=Z\oplus h_3(R_j,\mathrm{AID}_i,D_i)$。

3) 如果 $\mathrm{ID_{TMD}}$ 不属于 G，则输出拒绝。否则，对于消息签名对 $<m_i,(R_j,\mathrm{AID}_i,D_i,V,\alpha_j,U_j)>$，使 $(P,U_j+\alpha_j,h,V,R_j)$ 验证式(1)是否成立。若式(1)成立，则输出 $<m_i,(R_j,\mathrm{AID}_i,D_i,V,\alpha_j,U_j)>$；否则，输出拒绝。

$$VP=U_j+\alpha_jP_{\mathrm{pub}}+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j \tag{1}$$

这是因为 $P_{\mathrm{pub}}=xP$，$R_j=r_jP$，$U_j=u_jP$，$x_j=u_j+\alpha_jx \bmod q$，$V=x_j+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)\cdot r_j \bmod q$，$V=x_j+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j$，因而可得到

$$VP=(x_j+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)r_j)\ P=$$
$$x_jP+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)r_jP=$$
$$(u_j+\alpha_jx)P+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)r_jP=$$
$$(u_jP+\alpha_jP_{\mathrm{pub}})+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)r_jP$$

5 安全性证明与分析

5.1 安全性证明

本节将证明在随机预言机模型下本文提出的警告消息发布协议具有不可伪造性和保密性。

定理 1 不可伪造性。基于 ECDLP 问题的困难性，本文提出的警告消息发布协议能够抵抗自适应选择消息伪造攻击。

证明 假设存在挑战者 $\mathcal{C}$ 能够在多项式时间内以不可忽略的优势伪造签名 σ，那么对给定的 ECDLP 问题 $(P,Q=xP)$，其中 $P,Q\in G$，$x\in Z_q^*$，$\mathcal{A}$ 可以利用 $\mathcal{C}$ 作为子程序，在多项式时间内解决 ECDLP 问题。

1) 系统初始化

$\mathcal{C}$ 运行系统初始化算法：定义系统公钥 $P_{\mathrm{pub}}=xP$，保密 x 作为系统私钥，然后选择 $a,b\in Z_q^*$，发送系统参数 $\mathrm{params}=\{p,q,a,b,P\}$ 给 $\mathcal{A}$。维护预言机 h_1,h_2,h_3 的查询列表 L_{h_1},L_{h_2},L_{h_3}，L_{h_1},L_{h_2},L_{h_3} 初始时为空。

2) 询问

挑战游戏开始后，$\mathcal{A}$ 执行如下询问。

h_1 查询。列表 L_{h_1} 的格式为 $<\theta,\tau>$。$\mathcal{A}$ 的查询消息为 $\{\theta\}$，若 L_{h_1} 中存在 $\{\theta,\tau_{h_1}\}$，$\mathcal{C}$ 将 τ_{h_1} 发送给 $\mathcal{A}$；否则，$\mathcal{C}$ 随机产生 $\tau_{h_1}\in Z_q$ 发送给 $\mathcal{A}$，并将 $\{\theta,\tau_{h_1}\}$ 插入列表 L_{h_1}。

h_2 查询。列表 L_{h_2} 的格式为 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$。$\mathcal{A}$ 的查询消息为 $<m_i,R_j,\mathrm{AID}_i,D_i>$，若 L_{h_2} 中存在相应的记录 $<m_j,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$，$\mathcal{C}$ 将 τ_{h_2} 发送给 $\mathcal{A}$；否则，$\mathcal{C}$ 随机产生 $\tau_{h_2}\in Z_q$ 发送给 $\mathcal{A}$，并将 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$ 插入列表 L_{h_2} 中。

h_3 查询。列表 L_{h_3} 的格式为 $\{R_j,\mathrm{AID}_i,D_i,\tau_{h_i}\}$。$\mathcal{A}$ 的查询消息为 $\{R_j,\mathrm{AID}_i,D_i,\tau_{h_3}\}$，若 L_{h_3} 中存在相应的记录 $\{R_j,\mathrm{AID}_i,D_i,\tau_{h_3}\}$，$\mathcal{C}$ 将 τ_{h_3} 发送给 $\mathcal{A}$；否则，$\mathcal{C}$ 随机产生 $\tau_{h_3}\in Z_q$ 发送给 $\mathcal{A}$，并将 $\{R_j,\mathrm{AID}_i,D_i,\tau_{h_3}\}$ 插入列表 L_{h_3} 中。

3) 伪造

假设要伪造签名的消息为 m_i，$\mathcal{C}$ 随机产生 $r_j\in Z_q$，$u_j,v_j\in Z_q^*$，其中 $v_i=h_1(\mathrm{RID}\|\mathrm{VP}_i)$，$\mathrm{AID}_i=E_{\mathrm{ID_{TMD}}}[\mathrm{RID}\oplus v_iU_j,v_iU_j]$，并将 $<m_i,R_j,\mathrm{AID}_i,D_i,r_j>$ 添加到列表 L_{h_2} 中。最后 $\mathcal{C}$ 将消息 $<m_i,(R_j,\mathrm{AID}_i,D_i,V,\alpha_j,U_j)>$ 发送给 $\mathcal{A}$。

$\mathcal{A}$ 收到消息 $<m_i,(R_j,\mathrm{AID}_i,D_i,V,\alpha_j,U_j)>$ 后保存。根据分叉引理[22]，$\mathcal{A}$ 选择不同的 α_j 在多项式时间内

重新构建消息的另一个有效的签名 $<m_i,(R_j,\mathrm{AID}_i,D_i,V',\alpha_j',U_j)>$。此时，2 个签名分别满足

$$VP=U_j+\alpha_j P_{\mathrm{pub}}+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j \quad (2)$$

$$VP=U_j'+\alpha_j' P_{\mathrm{pub}}+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j \quad (3)$$

通过式(2)和式(3)可得

$$(V-V')P=(\alpha_j-\alpha_j')xP \quad (4)$$

因此，$\mathcal{A}$ 可得到 $x=(\alpha_j-\alpha_j')^{-1}(V-V')$。但求解 x 是 ECDLP 问题，而敌手不可能在多项式时间内解决 ECDLP 问题。因此，假设不成立，定理 1 得证。

定理 2　保密性。设 k 为安全参数，在随机预言模型下，如果存在一种多项式时间算法攻破加密方案的 SC-IND-CCA 安全优势是 $\rho(k)$，那么存在一种多项式时间算法求解 ECDHP 问题的概率至少是 $2(1-\rho 2^{-\mathrm{poly}(k)})\rho(k)$，其中 poly(·) 是多项式，$p$ 是 SC-IND-CCA 安全模型中最大的解签密查询次数。

证明　首先假设存在敌手 $\mathcal{A}$ 能以不可忽略的优势在定义 2 给出的游戏中获胜。下面，将构造算法 $\mathcal{C}$ 求解 ECDHP 问题。

假设给定 $\mathcal{C}$ 一个 ECDHP 问题：P 是 q 阶群 G 的生成元，给定 $a,b\in Z_q^*$，已知 P,aP,bP，$\mathcal{C}$ 将利用 $\mathcal{A}$ 作为子程序计算 abP，以求解 ECDHP 问题。$\mathcal{C}$ 与 $\mathcal{A}$ 的交互过程如下。

h_1 查询。列表 L_{h_1} 的格式为 $<\theta,h>$，当 $\mathcal{A}$ 以消息 $\{\theta\}$ 从查询列表 L_{h_1} 查询时。若 L_{h_1} 中存在相应的记录 $\{\theta,\tau_{h_1}\}$，则将 τ_{h_1} 发送给 $\mathcal{A}$。如果不存在，但 $\tau_{h_1}=h_1(\theta)$ 成立，并且 $\{\theta,\perp\}$ 在列表中，其中 $\perp$ 是特殊标志，然后挑战者 $\mathcal{C}$ 用 τ_{h_1} 取代列表中的 $\perp$，并返回 τ_{h_1}。对于其他情况，挑战者 $\mathcal{C}$ 选择随机数 $\tau_{h_1}'\in Z_q^*$ 发送给 $\mathcal{A}$。

h_2 查询。列表 L_{h_2} 的格式为 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$，当 $\mathcal{A}$ 以消息 $<m_i,R_j,\mathrm{AID}_i,D_i>$ 进行查询时，$\mathcal{C}$ 查询列表 L_{h_2}。若 h_2 中存在相应的记录 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$，则把相应的 τ_{h_2} 发送给 $\mathcal{A}$。如果不存在，但 $\tau_{h_2}=h_2(m_i,R_j,\mathrm{AID}_i,D_i)$ 成立，并且 $<m_i,R_j,\mathrm{AID}_i,D_i,\perp>$ 在列表中，然后挑战者 $\mathcal{C}$ 用 τ_{h_2} 取代列表中的 $\perp$，并返回 τ_{h_3}。对于其他情况，挑战者 $\mathcal{C}$ 选择随机数 $\tau_{h_2}'\in Z_q^*$ 发送给 $\mathcal{A}$。

h_3 查询。列表 L_{h_3} 的格式为 $\{R_j,\mathrm{AID}_i,D_i,\tau_{h_3}\}$，当 $\mathcal{A}$ 以 $\{R_j,\mathrm{AID}_i,D_i\}$ 进行查询时，$\mathcal{C}$ 查询列表 L_{h_3}。若 $\mathcal{C}$ 中存在相应的记录 $\{R_j,\mathrm{AID}_i,D_i,\tau_{h_3}\}$，则把相应的 τ_{h_3} 发送给 $\mathcal{A}$。如果不存在，但 $\tau_{h_3}=h_3(R_j,\mathrm{AID}_i,D_i)$ 成立，并且 $<R_j,\mathrm{AID}_i,D_i,\perp>$ 在列表中，然后挑战者 $\mathcal{C}$ 用 τ_{h_3} 取代列表中的 $\perp$，并返回 τ_{h_3}。对于其他情况，挑战者 $\mathcal{C}$ 选择随机数 $\tau_{h_3}'\in Z_q^*$ 发送给 $\mathcal{A}$。

密钥生成询问。当接收到对身份 $\mathrm{ID}_{\mathrm{TMD}}$ 的私钥询问时，$\mathcal{C}$ 查询列表 L_{SK}，若存在对应项，则返回 x_j；否则选择任意随机数 $x_j'\in Z_q^*$ 发送给 $\mathcal{A}$，并将该项添加到 L_{SK} 中。

签密询问。假设签密过程中签密者的身份为 $\mathrm{ID}_{\mathrm{TMD}}$，接收者身份为 AID_i，明文为 m_i，进行签密询问。$\mathcal{C}$ 随机选择 $r_j\in Z_q^*$，通过调用 h_3 查询得到 $\tau_{h_3}=h_3(R_j,\mathrm{AID}_i,r_jV_i)$，通过调用 h_2 查询得到 $\tau_{h_2}=h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)$，计算得 $V=x_j+h_2(m_i,R_j,\mathrm{AID}_i,r_jV_i)r_j \bmod q$，$Z=(m_i\|\mathrm{ID}_{\mathrm{TMD}}\|V)\oplus h_3(R_j,\mathrm{AID}_i,r_jV_i)$ 最终签密文为 $\sigma=(\mathrm{AID}_i,R_j,Z)$。

解签密询问。在 $\sigma=(\mathrm{AID}_i,R_j,Z)$ 上的解签密如下。

1) 列表 L_{h_3} 中是否存在 $<R_j,\mathrm{AID}_i,D_i,\perp>$ 使 $\tau_{h_3}=h_3(R_j,\mathrm{AID}_i,r_jV_i)$ 成立或者 $\tau_{h_3}=\perp$。

① 如果 L_{h_3} 中不存在 $<R_j,\mathrm{AID}_i,D_i,\tau_{h_3}>$，$\mathcal{C}$ 将 $<R_j,\mathrm{AID}_i,D_i,\perp>$ 添加到 L_{h_3} 中作为访问元组。

② 如果 L_{h_3} 中已存在 $<R_j,\mathrm{AID}_i,D_i,\tau_{h_3}>$，则现存结果将用作 $h_3(R_j,\mathrm{AID}_i,\mathrm{D}_i)$ 的值。

2) $\mathcal{C}$ 计算 $Z=(m_i\|\mathrm{ID}_{\mathrm{TMD}}\|V)\oplus h_3(R_j,\mathrm{AID}_i,D_i)$，列表 L_{h_2} 中是否在 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$ 使 $\tau_{h_2}=h_2(m_i,R_j,\mathrm{AID}_i,D_i)$ 或者 $\tau_{h_2}=\perp$。

① 如果列表 L_{h_2} 中不存在元组 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$，$\mathcal{C}$ 将 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$ 添加到列表 L_{h_2} 中作为访问元组。

② 如果列表 L_{h_2} 中存在元组 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$，则现存结果将用作 $h_2(m_i,R_j,\mathrm{AID}_i,D_i)$ 的值。

3) $\mathcal{C}$ 检查等式 $VP=U_j+\alpha_j P_{\mathrm{pub}}+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j$ 是否成立。

① 如果等式成立，返回 $<m_i,(R_j,\mathrm{AID}_i,D_i,$

$V,\alpha_j,U_j)>$。

② 如果等式不成立，则终止。

在完成游戏的第一阶段后，$\mathcal{A}$ 选择 2 个 n bit 的消息 m_0 和 m_1，以及发送者的私钥 x_j，并要求 $\mathcal{C}$ 在接受者的挑战身份之下建立挑战密文。

$\mathcal{C}$ 设置挑战密文为 $\sigma^*=(\mathrm{AID}_i,R_j,Z^*)$，$\mathcal{C}$ 随机选择 $b\leftarrow 0/1$，同时通过添加 $<m_b,R_j,\mathrm{AID}_i,r_jV_i,\tau_{h_2}>$ 至列表 L_{h_2}。注意，只有这个元组不存在列表 L_{h_2} 中才会被添加。列表 L_{h_3} 也会被新的元组 $<R_j,\mathrm{AID}_i,D_i,\tau_{h_i}>$ 更新，$h_3(R_j,\mathrm{AID}_i,r_jV_i)$ 的值为 $(m_i\|\mathrm{ID}_{\mathrm{TMD}}\|V)\oplus Z^*$。

之后，$\mathcal{C}$ 返回 $\mathcal{A}$ 的查询。如果 $\mathcal{A}$ 查询 h_1、h_2、h_3，$\mathcal{C}$ 输出对应的哈希值并停止。如果 $\mathcal{A}$ 没有访问，$\mathcal{C}$ 会输出随机的一个点并停止。

为了确保模拟游戏在计算上与真实游戏没有区别，h_1、h_2、h_3 查询，签密查询都能得到模拟。对于解签密查询，除了以下情况外，也能被模拟。

在上述解签密查询模拟的步骤 3)：当元组 $<m_i,R_j,\mathrm{AID}_i,D_i,\perp>$ 在列表 L_{h_2} 中，元组 $<m_i,R_j,\mathrm{AID}_i,D_i,\perp>$ 已存在列表 L_{h_3} 中。$VP=U_j+\alpha_jP_{\mathrm{pub}}+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j$，$(m_i\|\mathrm{ID}_{\mathrm{TMD}}\|V)=Z\oplus h_3(R_j,\mathrm{AID}_i,r_jV_i)=Z\oplus h_3$ $(R_j,\mathrm{AID}_i,R_jv_i)$ 这种情况意味着 $\mathcal{A}$ 没有查询 h_2 元组 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_2}>$，也没有查询 h_3 元组 $<m_i,R_j,\mathrm{AID}_i,D_i,\tau_{h_i}>$。注意，解签密查询没有泄露 $h_3(R_j,\mathrm{AID}_i,R_jv_i)$ 的任何信息。因此，本文可以得到挑战者赢得游戏的概率至少是 $(1-\rho 2^{-\mathrm{poly}(k)})\rho(k)$，这一事件为 h_2 或者 h_3 被查询。注意，此时 $\mathcal{C}$ 求解了 ECDHP 问题的实例。

对于事件 $\overline{E}$（$\overline{E}$ 表示不会被查询的事件），本文声称 $\mathcal{A}$ 在随机猜测中没有任何优势赢得比赛。令 $v_{\bar{b}}=x_j^*+h_2(m_{\bar{b}},R_j,\mathrm{AID}_i,r_jV_i)\mathrm{mod}q$，如果 $(m_{\bar{b}}\|\mathrm{ID}_{\mathrm{TMD}}\|V)=Z^*\oplus h_3(R_j,\mathrm{AID}_i,D_i)$ 成立，$\sigma=(\mathrm{AID}_i,R_j,Z)$ 是 $m_{\bar{b}}$ 的签密文。如果关注于 $h_3(R_j,\mathrm{AID}_i,D_i)$ 的输出部分，在事件 $\overline{E}$ 中，即使元组 $<m_{\bar{b}},R_j,\mathrm{AID}_i,D_i,\perp>$ 在列表 L_{h_2} 中，元组 $<R_j,\mathrm{AID}_i,D_i,\perp>$ 早已经存在于列表 L_{h_3} 中。正如上述所说，$\mathcal{C}$ 没有泄露这些值的任何信息给 $\mathcal{A}$。由于 h_2 与 h_3 的随机性，$\mathcal{A}$ 没有任何优势决定 $h_2(m_{\bar{b}},R_j,\mathrm{AID}_i,r_jV_i)$ 与 $h_3(R_j,\mathrm{AID}_i,D_i)$ 的返回值。因此 $\Pr[\mathrm{Succ}(\mathcal{A})]=1/2+\rho(k)\leqslant\Pr[E]+1/2(1-\Pr[E])$，其中 ρ 在定理 2 中定义，k 是系统参数。此时，$\mathcal{A}$ 以不可以忽略的优势赢得该游戏，即 $\Pr[E]\geqslant 2\rho(k)$，则可以得到 $\Pr[\mathrm{Succ}(E\wedge C)]\geqslant 2(1-\rho 2^{-\mathrm{poly}(k)})\rho(k)$。即存在多项式时间算法求解 ECDHP 问题，该算法成功的概率至少是 $2(1-\rho 2^{-\mathrm{poly}(k)})\rho(k)$。

5.2 安全性分析

本节将分析证明提出的警告消息发布协议可以满足 3.2 节提出的安全需求。

1) 消息认证。根据定理 1 可知，没有敌手能在多项式时间内解决 ECDLP 问题，因此，验证者可以通过验证等式 $VP=U_j+\alpha_jP_{\mathrm{pub}}+h_2(m_i,R_j,\mathrm{AID}_i,D_i)R_j$ 是否成立来确认消息 $<m_i,(R_j,\mathrm{AID}_i,D_i,V,\alpha_j,U_j)>$ 是否具有合法性和完整性。因此，该协议具有消息认证功能。

2) 身份隐私保护。车辆在发送消息时使用假名 $\mathrm{AID}_i=E_{\mathrm{ID}_{\mathrm{TMD}}}[\mathrm{RID}\oplus v_iU_j,\ v_iU_j]$，$\mathrm{AID}_i$ 由随机数和真实的身份 RID 生成，其中 $U_j=u_jP,u_j\in Z_q^*$。由于 u_j 和 v_i 的随机性，会产生毫无关联的假名。因此，敌手 $\mathcal{A}$ 想要从假名 $\mathrm{AID}_i=E_{\mathrm{ID}_{\mathrm{TMD}}}[\mathrm{RID}\oplus v_i\cdot U_j,v_iU_j]$ 中进行身份信息攻击，就必须得求出 u_jP。依据 ECDLP 问题假设可知，在随机预言模型与未知 u_j 和 v_i 的情况下求解 v_iU_j，在多项式时间内是不可行的。因此，该协议具有身份隐私保护功能。

3) 可追踪性。该协议的有效签名 $<m_i,(R_j,\mathrm{AID}_i,D_i,V,\alpha_j,U_j)>$ 包含车辆的真实身份 RID，当 TMD 需要追踪消息发送者的真实身份时，可以通过 $\mathrm{AID}_i=E_{\mathrm{ID}_{\mathrm{TMD}}}[\mathrm{RID}\oplus v_iU_j,v_iU_j]$ 计算出消息发送者的真实身份。因此，该协议具有车辆身份可追踪性。

4) 保密性。TMD 计算 $Z=(m_i\|\mathrm{ID}_{\mathrm{TMD}}\|V)\oplus h_3(R_j,\mathrm{AID}_i,r_jV_i)$ 对消息进行保密，其中 $D_i=V_iR_j$，$v_i=h_1(\mathrm{RID}\|\mathrm{VP}_i)$，$V_i=v_iP$。根据定理 2，如果不知道 v_i 与 r_j，则计算 v_ir_jP 不可行，即不能计算得到 $h_3(R_j,\mathrm{AID}_i,r_jV_i)$。所以除了消息的发送者 TMD 和接收者 AID_i，其他任何车辆都不能得到消息明文。因此，该协议实现了警告信息的保密性。

5) 抗攻击性。由定理 1 可知，没有任何一方可以伪造出 TMD 的签密消息，因此该协议可以抵抗

伪造攻击。而且任何中间人对消息的修改都可以被验证出，因此该协议可以抵抗修改攻击。此外，在 TMD 每次发送警告信息都会附带有时间戳，所以该协议可以抵抗重放攻击。

6　性能分析

6.1　计算开销

安全级别为 80 bit 的基于双线性对的方案设置如下：$e:G_1\times G_1\to G_2$，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 $E:y^2=x^3+ax+b \bmod \overline{p}$ 上的点，$\overline{p}$ 是 512 bit 的素数，$\overline{q}$ 是 160 bit 的素数。椭圆曲线密码运算方案如下：G 是由生成元 P 生成的阶为 q 的加法群，P 为非奇异椭圆曲线 $E:y^2=x^3+ax\ \ +b \bmod p$ 上的点，其中 p,q 为 160 bit 的素数，$a,b\in F_p$。表 1 给出了密码运算及其对应的缩写和执行时间。

表 1　密码运算及其对应的缩写和执行时间

运算范围	运算名称	缩写	执行时间/ms
双线性配对	双线性配对运算 $e(P,Q)$	T_{b}	6.416 4
	标量乘法运算 xP	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
	幂运算 P^a	T_{exp}	2.145 6
椭圆曲线	标量乘法运算 xP	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
哈希函数	MapToPoint 哈希函数运算	T_{H}	1.327 7
	单向哈希函数运算	T_{h}	0.000 2

在文献[16]中，消息生成过程包含 7 个双线性对标量乘法运算 T_{bm}、3 个双线性对加法运算 T_{ba}、一个单向哈希函数运算 T_{h} 和 2 个 MapToPoint 哈希函数运算 T_{H}，此阶段的总开销为 $T_h+2T_{\mathrm{H}}+3T_{\mathrm{ba}}+7T_{\mathrm{bm}}$；解密和验证过程包含 4 个双线性配对运算 T_{b}、3 个双线性对的标量乘法运算 T_{bm}、一个双线性对加法运算 T_{ba}、2 个 MapToPoint 哈希函数运算 T_{H} 和一个单向哈希函数运算 T_{h}，此阶段的总开销为 $4T_{\mathrm{b}}+3T_{\mathrm{bm}}+T_{\mathrm{h}}+2T_{\mathrm{H}}+T_{\mathrm{ba}}$。在文献[17]中，消息生成的过程中主要包含 4 个双线性对上的幂运算 T_{exp}、一个 MapToPoint 哈希函数运算 T_{H} 和 2 个单向哈希函数运算 T_{h}，此阶段的总计算开销为 $2T_{\mathrm{h}}+4T_{\mathrm{exp}}+T_{\mathrm{H}}$；解签名、解密和验证过程主要包含 4 个双线性对上的幂运算 T_{exp}、4 个双线性配对运算 T_{b}、一个 MapToPoint 哈希函数运算 T_{H} 和 4 个单向哈希函数运算 T_{h}，此阶段的总开销为 $4T_{\mathrm{exp}}+4T_{\mathrm{b}}+4T_{\mathrm{h}}$。在文献[19]中，消息生成过程主要进行 3 个椭圆曲线标量乘法运算 T_{em} 和 7 个单向哈希函数运算 T_{h}，此阶段总计算开销为 $3T_{\mathrm{em}}+7T_{\mathrm{h}}$；解密和验证过程包含 5 个椭圆曲线标量乘法运算 T_{em}，2 个椭圆曲线加法运算 T_{ea} 和 9 个单向哈希函数运算 T_{h}，此阶段总计算开销为 $5T_{\mathrm{em}}+2T_{\mathrm{ea}}+9T_{\mathrm{h}}$。在本文协议中，消息生成过程中包含 3 个椭圆曲线的标量乘法运算 T_{em} 和 2 个单向哈希函数运算 T_{h}，此阶段的总开销为 $2T_{\mathrm{h}}+3T_{\mathrm{em}}$；解密过程包括验证，该过程包含 2 个椭圆曲线的加法运算 T_{ea}、4 个椭圆曲线的标量乘法运算 T_{em} 和 2 个单向哈希函数运算 T_{h}，此阶段的总开销为 $2T_{\mathrm{ea}}+2T_{\mathrm{h}}+4T_{\mathrm{em}}$。因此，如表 2 所示，本文协议有着较低的计算开销。

表 2　计算开销对比

协议	消息生成/ms	解密和验证/ms
文献[16]	$T_{\mathrm{h}}+2T_{\mathrm{H}}+3T_{\mathrm{ba}}+7T_{\mathrm{bm}}\approx$ 21.206 7	$4T_{\mathrm{b}}+3T_{\mathrm{bm}}+T_{\mathrm{h}}+2T_{\mathrm{H}}+T_{\mathrm{ba}}\approx$ 36.267 5
文献[17]	$2T_{\mathrm{h}}+4T_{\mathrm{exp}}+T_{\mathrm{H}}\approx$ 9.910 5	$4T_{\mathrm{exp}}+4T_{\mathrm{b}}+4T_{\mathrm{h}}+T_{\mathrm{H}}\approx$ 35.576 5
文献[19]	$3T_{\mathrm{em}}+7T_{\mathrm{h}}\approx$ 2.208 8	$5T_{\mathrm{em}}+2T_{\mathrm{ea}}+9T_{\mathrm{h}}\approx$ 3.688 8
本文协议	$2T_{\mathrm{h}}+3T_{\mathrm{em}}\approx$ 2.207 8	$2T_{\mathrm{ea}}+2T_{\mathrm{h}}+4T_{\mathrm{em}}\approx$ 2.951 6

6.2　通信开销

由安全性分析可知，$\overline{p}$ 与 p 分别为 64 B 与 20 B，因此，群 G_1 与群 G 中的元素的字节数分别为 128 B 与 40 B。假定 VANET 中消息的时间戳 T 为 4 B，真实身份 RID 为 20 B，单向哈希函数值为 20 B。

文献[16-17,19]与本文协议的通信开销对比如图 2 所示。在文献[16]中，消息为聚合的密文 $\mathrm{SRER}_{\mathrm{agg}}=((Q_j)_{j=1}^{n},T_1,\cdots,T_n,K_1,\cdots,K_n,\mathrm{sig}_{\mathrm{agg}})$，单个消息为 $<Q_j,(T_i,K_i,\alpha_i)>$，其中 $Q_j=H_1(\mathrm{Sen}_j)$，$\alpha_j,T_i\in G_1$，Q_j 属于单向哈希函数值。因此，所增加的通信开销为 128×2+20=276 B。在文献[17]中，消息由 $<U,W>$ 组成，其中 $U=(u_1,u_2,u_3,u_4)$，$W=(\mathrm{SA}_i\ \ ,\mathrm{SA}_l,V_j,\ \mathrm{vsk}_{j,1},\mathrm{vsk}_{j,2},t_l,t_j,T_d,\theta_t,\mathrm{Time})$，

$\theta_l=\{\theta_{l,1},\theta_{l,2}\}$，$u_1,u_3$，$\mathrm{vsk}_{j,1},\mathrm{vsk}_{j,2},\theta_{l,1}\in G_1$，$u_4,\mathrm{SA}_i$，$\mathrm{SA}_j,V_j,\theta_{l,2},T_d\in Z_q^*$。因此，所增加的通信开销为128×5+64×6+ 3×4=1036 B。在文献[19]中，消息由$<\mathrm{AID}_i, C_i, T_i, \delta_i>$组成，其中$\mathrm{AID}_i=\{\mathrm{AID}_{i,1}, \mathrm{AID}_{i,2}\}$，$C_i=\{C_{i,1},C_{i,2},C_{i,3}\}$，$\delta_i$和$\mathrm{AID}_{i,2}$是单向哈希函数值，$C_{i,3},\mathrm{AID}_{i,2},\delta_i\in Z_q^*$，$C_{i,1},\mathrm{AID}_{i,2}\in G$。因此，在文献[19]中单个消息所增加的通信开销为 20×3+40×3+4=184 B。在本文协议中，消息由$<\mathrm{AID}_i,R_j,Z>$组成，$Z=(m_i\|\mathrm{ID}_{\mathrm{TMD}}\|V)\oplus h_3(\mathrm{AID}_i, r_j,V_i)$，其中$R_j\in G$，$V\in Z_q^*$，$\mathrm{ID}_{\mathrm{TMD}}$长度为 20 B，$\mathrm{AID}_i=E_{\mathrm{ID}_{\mathrm{TMD}}}[\mathrm{RID}\oplus v_iU_j]$（20 B），因此，在本文提出的协议中单个消息所增加的通信开销为40+20+20×2=100 B。通过对比，本文协议有较低的通信开销，可满足 VANET 的通信需求。

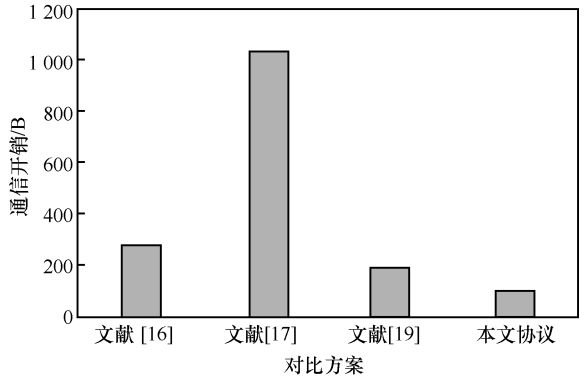

图 2 各方案的通信开销对比

7 结束语

本文提出 VANET 中保护隐私的警告消息发布协议，其中 TMD 可以根据车辆的真实身份获取车辆的假名，必要时又可以通过车辆假名追踪车辆的真实身份。所提协议采用椭圆曲线密码体制，不依赖于双线性对，具有较小的计算开销和通信开销。安全性分析和性能分析表明，所提协议可用于 VANET 实现保护隐私的警告消息发布。

参考文献：

[1] 宋成, 张明月, 彭维平, 等. 基于双线性对的车联网批量匿名认证方案研究[J]. 通信学报, 2017, 38(6): 49-57.
SONG C, ZHANG M Y, PENG W P, et al. Research on batch anonymous authentication scheme for VANET based on bilinear pairing[J]. Journal on Communications, 2017, 38(6): 49-57.

[2] LIU Y L, WANG L M, CHEN H H. Message authentication using proxy vehicles in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(8): 3697-3710.

[3] CHENG X, WANG C X, LAURENSON D I, et al. An adaptive geometry-based stochastic model for non-isotropic MIMO mobile-to-mobile channels[J]. IEEE Transactions on Wireless Communications, 2009, 8(9): 4824-4835.

[4] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.

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

[6] ZHANG C, LU R, LIN X, et al. An efficient identity-based batch verification scheme for vehicular sensor networks[C]//The 27th Conference on Computer Communications. Piscataway: IEEE Press, 2008: 246-250.

[7] ZHANG C X, HO P H, TAPOLCAI J. On batch verification with group testing for vehicular communications[J]. Wireless Networks, 2011, 17(8): 1851-1865.

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

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

[10] JIANHONG Z, MIN X, LIYING 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.

[11] 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.

[12] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的消息认证方案[J]. 通信学报, 2016, 37(11): 1-10.
WU L B, XIE Y, ZHANG Y B. Efficient and secure message authentication scheme for VANET[J]. Journal on Communications, 2016, 37(11): 1-10.

[13] HE D B, ZEADALLY S, XU B W, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[14] RABIEH K, MAHMOUD M M E A, YOUNIS M. Privacy-preserving route reporting scheme for traffic management in VANETs[C]//2015 IEEE International Conference on Communications. Piscataway: IEEE Press, 2015: 7286-7291.

[15] ZHENG Y L. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)[C]//Advances in Cryptology—CRYPTO'97. Berlin: Springer, 1997: 165-179.

[16] BASUDAN S, LIN X D, SANKARANARAYANAN K. A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing[J]. IEEE Internet of Things Journal, 2017, 4(3): 772-782.

[17] WANG Y J, DING Y, WU Q H, et al. Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(7): 1779-1790.

[18] 韩牟, 华蕾, 王良民, 等. 车载自组网中高效的群组协商通信协议[J]. 通信学报, 2018, 39(1): 34-45.
HAN M, HUA L, WANG L M, et al. Efficient communication protocol of group negotiation in VANET[J]. Journal on Communications, 2018, 39(1): 34-45.

[19] XU Y, WANG M, CUI J, et al. LPE-RCM: lightweight privacy-preserving edge-based road condition monitoring for VANETs[C]// Wireless Algorithms, Systems, and Applications. [S.n.:s.l.], 2020: 78-86.

[20] ELKHALIL A, ZHANG J S, ELHABOB R, et al. An efficient signcryption of heterogeneous systems for Internet of Vehicles[J]. Journal of Systems Architecture, 2021, 113: 101885.

[21] ALI I, LAWRENCE T, OMALA A A, et al. An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10): 11266-11280.

[22] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[作者简介]

刘辉（1981− ），男，安徽合肥人，安徽大学实验师，主要研究方向为数字签名、车联网安全通信等。

刘鑫衍（1998− ），女，山东济南人，安徽大学硕士生，主要研究方向为数字签名、车联网安全、车联网隐私保护等。

许艳（1982− ），女，江苏泗洪人，博士，安徽大学副教授，主要研究方向为云计算安全、车联网安全和隐私保护等。

仲红（1965− ），女，安徽固镇人，博士，安徽大学教授，主要研究方向为物联网、车联网、软件定义网络、大数据隐私保护、云安全、边缘计算等。

王梦（1994− ），女，安徽亳州人，安徽大学硕士生，主要研究方向为车联网安全与隐私保护。