VANET 中基于不经意传输和群签名的强隐私保护方案*

朱晓玲[1]，陆 阳[1,2]，侯整风[1]，朱晓娟[1]
(1. 合肥工业大学 计算机与信息学院，合肥 230009；2. 安徽省矿山物联网与安全监控技术重点实验室，合肥 230088)

摘 要：隐私保护是部署 VANET 的重要需求，事故责任判定要求隐私可揭露，因此给出可追踪的 VANET 隐私保护方案。为解决已有方案中权威伪造签名和权威妥协后隐私泄露问题，采取不经意传输为车辆颁发私钥，基于秘密共享联合揭露身份。为确保高效的匿名通信，采用了群签名、批验证、撤销预处理方法。安全分析表明，方案在匿名性和健壮性方面优于已有方案；性能分析表明，方案通信和计算代价与已有方案相近，可有效应用于有强隐私保护需求的 VANET 安全通信。

关键词：车用自组网络；隐私保护；不经意传输；秘密共享
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2014)01-0226-05
doi:10.3969/j.issn.1001-3695.2014.01.053

Strong privacy protection scheme based on oblivious transfer and group signature in VANET

ZHU Xiao-ling[1], LU Yang[1,2], HOU Zheng-feng[1], ZHU Xiao-juan[1]
(1. *School of Computer & Information, Hefei University of Technology, Hefei* 230009, *China*; 2. *Anhui Provincial Key Laboratory of Mine IoT & Mine Safety Supervisory Control, Hefei* 230088, *China*)

Abstract: Privacy protection is an important requirement in vehicle networks. Meanwhile, privacy requires to be disclosed when a traffic accident happens. So the paper presented a traceable privacy protection scheme. In existing schemes the issues about authority forgery and authority leaks remained unresolved. So using the oblivious transfer protocol, the manage authority issued private keys. Based on secret sharing scheme, tracking authorities collaboratively revealed identities. It used the methods of group signature, batch verification and preprocessing revocation efficiently in anonymous communication. Security analysis shows that the scheme is superior to the existing schemes in terms of unforgeability and robustness. Performance analysis shows that the cost of communication and computation is similar to the existing schemes. So it will have effective applications in VANET.

Key words: VANET; privacy protection; oblivious transfer; secret sharing

0 引言

车用自组网络(vehicle Ad hoc network,VANET)通过车辆与车辆、车辆与路边单元(road-side unit,RSU)的无线通信，提高了车辆对周围环境的感知能力，从而在交通优化、路面安全、智能驾驶等方面具有广泛的应用前景。但是由于车辆的实时广播，导致了大量隐私数据泄露，因此研究 VANET 的隐私保护机制是重要的[1,2]。

2005 年，Raya 等人[3]分析了 VANET 特点及安全隐私需求，指出隐私保护在一定条件是可追踪的；权威为实现追踪，需要存储管辖区域内的所有车辆与匿名证书的关系，存储和搜索代价大。由于群签名[4]具有匿名和可追踪的特点，2007 年 Lin 等人[5]在文献[4]基础上提出基于群签名的车辆安全和隐私保护协议 GSIS，车辆作为群成员，交通管理部门作为群管理者。该协议无须匿名证书，通信和计算代价较低。Calandriello 等人[6,7]在文献[3,5]基础上，提出基于群签名的匿名证书自动生成方案 Hybrid，存储和搜索代价较文献[3]低。2010 年，Zhang 等人[8]提出可扩展认证协议，协议在秘密分发阶段采用签密的方法，解决了通信信道的安全性。2011 年，Hao 等人[9]建议分布式的密钥管理框架，在车辆撤销和系统维护方面具有优势。这些基于群签名的协议[5~9]都存在着安全漏洞：车辆的私钥由权威产生并颁发，权威可以冒充车辆发送签名消息，协议无法阻止权威欺骗。Schaub 等人[10]采取盲签名产生匿名证书，试图解决权威欺骗问题，但协议复杂，通信代价高。

基于不经意传输和秘密共享，本文提出 VANET 的强隐私保护方案，主要特点是：a) 车辆私钥虽由管理权威产生，但不经意传输协议保证了权威只能以较低的概率获得车辆私钥，避

收稿日期：2013-03-14；**修回日期**：2013-04-26 **基金项目**：国家自然科学基金资助项目(60873195)；国家“863”计划资助项目(2011AA060406)；安徽省自然科学基金项目(09041251)

作者简介：朱晓玲(1974-)，女，安徽合肥人，博士，主要研究方向为密码学、移动互联网(zhuxl@hfut.edu.cn)；陆阳(1967-)，男，教授，博导，主要研究方向为无线传感器网络、分布式控制技术；侯整风(1958-)，男，教授，主要研究方向为计算机网络、信息安全；朱晓娟(1978-)，女，博士研究生，主要研究方向为无线 Ad hoc 网络、可信网络.

免了在权威面前车辆无隐私的情况;b) 车辆的隐私与权威追踪是一对矛盾,方案采用秘密共享方案将单个权威扩展为 k 个权威,只要妥协权威的数量少于门限值 m,车辆的隐私都不会受到威胁;c) 在安全和隐私增强的情况下兼顾效率,采用批验证和撤销预处理减少验证和撤销检测的计算量。

1　隐私保护模型

模型中所有实体构成一个群,包括:

a) 车辆 V,所有车辆以群成员方式通过注册预装公共参数和成员私钥。车辆包含传感输入模块、无线通信模块、中央处理模块、硬件安全模块(hardware security module,HSM)。HSM 具有防窜改功能,负责敏感信息的存储和操作,如存储车辆私钥,并执行与私钥相关的数字签名操作等。

b) 群管理者,包括管理权威(manage authority,MA)和追踪权威(trace authority,TA)。MA 可能是交通管理机构,负责车辆注册与撤销等。TA 负责身份追踪,将单个权威扩展为 k 个权威形成追踪组 TA_s,$TA_s=\{TA_1,TA_2,\cdots,TA_k\}$,$TA_i(1\leqslant i\leqslant k)$ 可能是执法机构、法官、隐私保护机构等,其标志为 ID_i。

具有隐私保护的安全通信框架如图 1 所示。

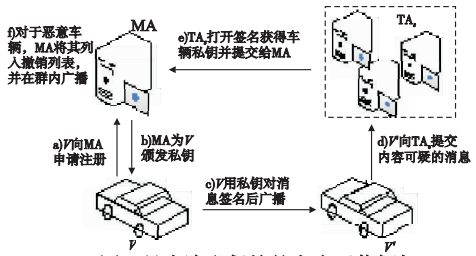

图1 具有隐私保护的安全通信框架

2　强隐私保护方案

方案由六部分组成:系统初始化、车辆注册、消息签名、批验证、联合追踪、车辆撤销。相互依存关系如图 2 所示,初始化和车辆注册协议是底层协议,为上层协议和算法提供基本参数。消息签名和批验证确保数据的真实性、完整性和不可抵赖性。当车辆行为可疑,则启动追踪协议,由追踪组打开签名获得车辆真实身份。当被追踪车辆确定为恶意车辆,则启动撤销协议,由管理权威将其列入撤销列表,其签名消息不再被群成员所接收。

图2 方案组成

2.1　系统初始化

Boneh 等人[4] 提出的短群签名具有签名短、节省通信带宽的特点,因此将 Boneh 短群签名作为本方案的密码学基础。

a) 系统选取双线性映射 $e:G_1\times G_2\rightarrow G_T$,其中 $G_1=\langle g_1\rangle$,$G_2=\langle g_2\rangle$,$|G_1|=|G_2|=p$,p 为素数,$\psi(g_2)=g_1$,ψ 为同态映射,构造 $H:\{0,1\}^*\rightarrow Z_p^*$。

b) 随机选取 $h\in G_1\backslash\{1_{G_1}\}$,$h_0\in G_2\backslash\{1_{G_2}\}$,$\zeta_1,\zeta_2\in Z_p^*$。其中 $\{1_{G_1}\}$、$\{1_{G_2}\}$ 分别为群 G_1、G_2 中的单位元。取 $u,v\in G_1$,使 $u^{\zeta_1}=v^{\zeta_2}=h$;取 $h_1,h_2\in G_2$,$h_1=h_0^{\zeta_1}$,$h_2=h_0^{\zeta_2}$。构造 $m-1$ 次多项式 $f(x)$ 和 $g(x)\in Z_p[x]$,使 $f(0)=\zeta_1$,$g(0)=\zeta_2$,计算 $\zeta_{1,i}=f(ID_i)$,$\zeta_{2,i}=g(ID_i)(1\leqslant i\leqslant k)$,将 $\zeta_{1,i}$、$\zeta_{2,i}$ 秘密分发给追踪组成员 TA_i 后,销毁 ζ_1、ζ_2。

c) MA 随机选取元素 $\gamma\in Z_p^*$,计算 $w=g_2^{\gamma}$,公开 w。

初始化产生公共参数 $param=(G_1,G_2,G_T,p,\psi,e,H)$,群公钥 $gpk=(g_1,g_2,u,v,w,h,h_0,h_1,h_2)$,MA 私钥 $gmsk=\gamma$,TA_i 私钥 $gtsk_i=(\zeta_{1,i},\zeta_{2,i})(1\leqslant i\leqslant k)$。步骤 b) 用秘密共享方案[11] 将 ζ_1、ζ_2 分割给 k 个管理者,恢复秘密的门限为 m。

2.2　车辆注册

不经意传输协议[12] 是设计密码学协议的有力工具,可应用于公平电子合同的签署、秘密信息检索、安全多方计算等,有 1-out-of-2、1-out-of-n、k-out-of-n 等情形。1-out-of-n 不经意传输是指发送者有 n 个秘密消息 $m_1,m_2,\cdots,m_n$,接收者能且只能够得到其中一个消息,而发送者不知道接收者得到的是哪个消息。Boneh 方案[4] 中,群成员私钥由群管理员产生并颁发,管理员拥有所有成员私钥,日后可冒充任意成员进行签名。为解决群成员在群管理员面前秘密完全暴露的问题,本文基于 1-out-of-n 不经意传输[13],给出车辆注册协议。

a) 车辆 V_i。随机选取 $x_i\in Z_p^*$ 作为其秘密,随机选 $r\in Z_p^*$,$k\in Z_n^*$,令 $m_k=x_i$,随机选 $n-1$ 个 $m_j\in Z_p^*(1\leqslant j\leqslant n,j\neq k)$,计算 $y=\hat{g}^r\hat{h}^k$,向 MA 发送 $(ID_{V_i},m_1,m_2,\ldots,m_n,y)$。其中 $\hat{g}$、$\hat{h}$ 为 G_1 的两个生成元,为车辆和管理权威共有。

b) MA 对 V_i 身份审核后,计算并发送 $a=\hat{g}^t$,$b_j=g_1^{\frac{1}{m_j+\gamma}}F((y/h^j)^t,j)(1\leqslant j\leqslant n,F$ 为 hash 函数)。

c) V_i:计算中的 $A_i=\dfrac{b_k}{F(a^r,k)}$,存储私钥 $gvsk_i=(A_i,x_i)$。

协议步骤 a) 中的 V_i 将 x_i 嵌入 n 个备选值,将选择的 k 嵌入 y,并发送给 MA;b) 中的 MA 用自己的私钥 γ 参与计算后返回;c) 中的 V_i 获得想要的秘密 $A_i=g_1^{\frac{1}{x_i+\gamma}}$。因为

$$\frac{b_k}{F(a^r,k)}=\frac{g_1^{\frac{1}{m_k+\gamma}}F((\hat{g}^r\hat{h}^k/\hat{h}^k)^t,k)}{F(a^r,k)}=\frac{g_1^{\frac{1}{x_i+\gamma}}F(a^r,k)}{F(a^r,k)}=g_1^{\frac{1}{x_i+\gamma}}。$$

在文献[4~6]中,MA 产生 x_i,计算 A_i,将 (x_i,A_i) 秘密发送给车辆;本文车辆和 MA 共同计算 $A_i=g_1^{\frac{1}{x_i+\gamma}}$,其中 x_i 由车辆提供,γ 由 MA 提供,通过不经意传输,车辆获得 A_i。当 n 较大,协议以较大概率保证秘密 x_i 和 A_i 被 V_i 唯一拥有,实现车辆在权威面前的隐私保护。

2.3　消息签名

签名消息的格式如图 3 所示。群 ID 字段用于识别车辆所属群;消息 ID 表明消息编号;数据净荷包含车辆位置、方向、速度、告警等;时戳用来防止重放攻击;签名存储签名结果;生命期可适时终止消息在 VANET 中传输。

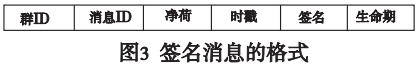

图3 签名消息的格式

采用 Boneh 群签名对消息 $M=\{$群 ID ‖ 消息 ID ‖ 净荷 ‖ 时戳$\}$ 签名。车辆随机选择 $\alpha,\beta,r_\alpha,r_\beta,r_{x_i},r_{\delta_1},r_{\delta_2}\in Z_p^*$,计算 $T_1=u^\alpha$,$T_2=v^\beta$,$T_3=A_ih^{\alpha+\beta}$,$\delta_1=x_i\alpha$,$\delta_2=x_i\beta$;计算 $R_1=u^{r_\alpha}$,$R_2=v^{r_\beta}$,$R_3=e(T_3,g_2)^{r_{x_i}}e(h,w)^{-r_\alpha-r_\beta}e(h,g_2)^{-r_{\delta_1}-r_{\delta_2}}$,$R_4=T_1^{r_{x_i}}u^{-r_{\delta_1}}$,$R_5=T_2^{r_{x_i}}v^{-r_{\delta_2}}$;计算 $c=H(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)\in Z_p^*$;计算 $S_\alpha=r_\alpha+c\alpha$,$S_\beta=r_\beta+c\beta$,$S_{x_i}=r_{x_i}+cx_i$,$S_{\delta_1}=$

$r_{\delta_1}+c\delta_1, S_{\delta_2}=r_{\delta_2}+c\delta_2$；将结果 $\sigma=(T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5,S_\alpha,S_\beta,S_{x_i},S_{\delta_1},S_{\delta_2})$ 填充到签名字段。

2.4 批验证

批验证方法能判断签名集合中是否包含无效签名，从而减少验证时间。文献[8,14,15]分别给出 Boneh 群签名和 XSGS 群签名的批验证 。基于以上方法，本文对 q 个消息 M_i 及签名 σ_i 进行批验证。设 $\sigma_i=(T_{i,1},T_{i,2},T_{i,3},R_{i,1},R_{i,2},R_{i,3},R_{i,4},R_{i,5},S_{i,\alpha},S_{i,\beta},S_{i,x_i},S_{i,\delta_1},S_{i,\delta_2})$：

a)计算

$c_i=H(M_i,T_{i,1},T_{i,2},T_{i,3},R_{i,1},R_{i,2},R_{i,3},R_{i,4},R_{i,5})(1\leqslant i\leqslant q)$

b)检测下面等式是否成立 $u^{S_{i,\alpha}}=R_{i,1}\cdot {T_{i,1}}^{c_i}, v^{S_{i,\beta}}=R_{i,2}\cdot {T_{i,2}}^{c_i}, {T_{i,1}}^{S_{i,x_i}}=R_{i,4}\cdot u^{S_{i,\delta_1}}, {T_{i,2}}^{S_{i,x_i}}=R_{i,5}\cdot v^{S_{i,\delta_2}}(1\leqslant i\leqslant q)$，如等式成立，则继续；否则返回 false。

c)随机选择 q 个比特长度为 b 的数 $\lambda_1,\lambda_2,\cdots,\lambda_q\in Z_p^*$，判断检测公式 $\prod_{i=1}^{q}{R_{i,3}}^{\lambda_i}=e(\prod_{i=1}^{q}(T_{i,3}{}^{S_{i,x_i}\lambda_i}h^{(-S_{i,\delta_1}-S_{i,\delta_2})\lambda_i}g_1{}^{-c_i\lambda_i}),g_2)e(\prod_{i=1}^{q}(h^{(-S_{i,\alpha}-S_{i,\beta})\lambda_i}T_{i,3}{}^{c_i\lambda_i}),w)$ 是否成立，如成立返回 true，否则返回 false。

步骤 b)是对每个签名的 $R_{i,1}$、$R_{i,2}$、$R_{i,4}$、$R_{i,5}$进行单独检测，步骤 c)是对签名集合的 $R_{i,3}$ 进行联合检测。当 $q=1,\lambda_1=1$ 时，批验证算法退化为单独验证算法，由文献[4]知，检测式成立。当 $q>1$ 时，q 个签名都为有效签名时，显然通过批验证；当 q 个签名中至少一个为无效签名时，由文献[14]知，批验证算法接受无效签名的概率为 2^{-b}，即算法以大概率返回签名集合无效。对于无效的签名集合，根据消息性质，可采取丢弃或对重要消息单独验证等方法作进一步处理。

通过比较发现，当批验证返回 true 时，本文与文献[8,14]批验证计算时间一样，配对运算数都降为 2 次。当返回 false 时，本文可能单独检测 $R_{i,1},R_{i,2},R_{i,4},R_{i,5}$ 时已发现无效签名，无须再检测 $R_{i,3}$，而计算 $R_{i,3}$ 需要两次较为耗时的配对运算，与文献[8,14]相比，本文计算时间略少。

2.5 联合追踪

a)某车辆向某追踪成员如 TA_1 举报违章车辆的签名消息，TA_1 检查时戳和签名 σ 是否有效。如检查通过，TA_1 向其他成员发送 req‖σ，其中 req 为联合追踪请求。当愿意参与追踪的成员数量达到 m，可进行追踪，不妨假设 m 个参与追踪成员 TA_i，其标志为 $ID_i(1\leqslant i\leqslant m)$。

b)$TA_i(2\leqslant i\leqslant m)$将 $T_1{}^{\zeta_{1,i}}\cdot T_2{}^{\zeta_{2,i}}$秘密发送给 TA_1。

c)TA_1 结合自己的份额计算 $A_i=\dfrac{T_3}{\prod_{i=1}^{m}(T_1{}^{\zeta_{1,i}}\cdot T_2{}^{\zeta_{2,i}})^{l_i(0)}}$，其中 $l_i(0)=\prod_{\substack{j=1\\j\neq i}}^{m}\dfrac{ID_j}{ID_j-ID_i}\bmod p$。

d)TA_1 向 MA 发送 A_i，MA 将其列入撤销列表 RL，并在群内广播。

如图 4，假设门限 $m=3$，参与追踪的小组成员为执法部门、法官和隐私保护机构。执法部门收到举报车辆 V_i 的消息，收集、整理并向法官和隐私保护机构提交 V_i 的违章证据等；法官和隐私保护机构审查证据同意受理后，返回与秘密恢复相关数据；执法机构把收到数据与自己计算结果合并得 A_i，将 A_i 交给交通管理部门。

3.6 车辆撤销

每个车辆在进行批验证前，需要判断消息是否来自于 RL，其计算量随着 RL 规模的增大而增加。为减少每个车辆计算量，本文 MA 对 RL 进行预处理，对 RL 中每项 A_i，计算 $P_i=e(A_i,h_0)$，将 RL 扩展为 $RL=\{A_i,P_i\}_{1\leqslant i\leqslant l}$，$l$ 为撤销列表的长度。

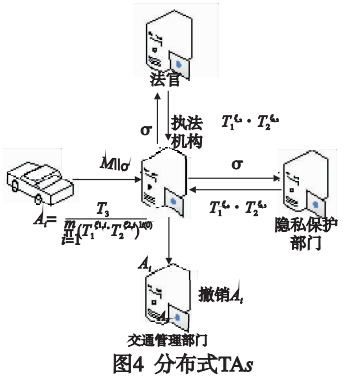

图4 分布式TA*s*

a)MA 在群内广播 $RL=\{A_i,P_i\}_{1\leqslant i\leqslant l}$。

b)车辆对接收到的消息 M 及签名 $\sigma=(T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5,S_\alpha,S_\beta,S_{x_i},S_{\delta_1},S_{\delta_2})$，计算 $Q=\dfrac{e(T_3,h_0)}{e(T_1,h_1)e(T_2,h_2)}$，遍历 RL 判断 $Q=P_i$，如等式成立，返回签名无效；否则进入批验证。检测式显然成立，因为

$$Q=\frac{e(A_i,h_0)e(h^\alpha,h_0)e(h^\beta,h_0)}{e(T_1,h_1)e(T_2,h_2)}=\frac{e(A_i,h_0)e(T_1,h_0{}^{\zeta_1})e(T_2,h_0{}^{\zeta_2})}{e(T_1,h_1)e(T_2,h_2)}=e(A_i,h_0)=P_i$$

与文献[5,8]相比，本文 MA 的预处理将每个车辆原先 $l+2$次配对运算减少为 3 次，提高了撤销性能。

3 安全性分析

1)DL 假设 不存在多项式时间概率算法，以不可忽略的概率解决 DL 问题(即已知 g、y，求 $\log_g^y$ 的问题，其中 $G=\langle g\rangle, y\in G$)。

2)CDH 假设 不存在多项式时间概率算法，以不可忽略的概率解决 CDH 问题(即已知 g、g^a、g^b，求 g^{ab} 的问题，其中 $G=\langle g\rangle, |G|=p, p$ 为素数，$a,b\in Z_p^*$)。

3)q-SDH 假设 不存在多项式时间概率算法，以不可忽略的概率解决 q-SDH 问题(即已知 $g_1,g_2,g_2^r,\cdots,g_2{}^{r^q},x$，求 $g_1^{\frac{1}{r+x}}$ 的问题，其中 $G_1=<g_1>, G_2=\langle g_2\rangle, |G_1|=|G_2|=p, p$ 为素数，$\psi(g_2)=g_1$，ψ 为同态映射，$x,r\in Z_p^*$)。

性质 1 不论 MA、TA_s，还是恶意车辆都不能假冒其他实体生成群签名，方案具有强不可伪造性。

针对 MA 诚实、半诚实、不诚实三种情形，讨论各实体(车辆、TA_s和 MA)的伪造签名情况。

情形 1 MA 诚实，即 MA 不参与欺骗，不透漏秘密。

如果 q-SDH 假设成立，恶意车辆在签名阶段无法伪造签名。

证明 设 A 为攻击者，与 A 交互的模拟器定义如下：

a)建立 $gpk=(g_1,g_2,u,v,w,h,h_0,h_1,h_2)$。

b)hash 询问。当 A 询问 $M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5$ 的 hash 值，如果该询问已在 H 表，则返回对应值；否则返回随机数 c，并添加至 H 表。

c) 签名询问。当 A 询问消息 M 的群成员签名，随机选取

$A^* \in G_1, \alpha, \beta \in Z_p^*$,计算 $T_1 = u^\alpha, T_2 = v^\beta, T_3 = A^* h^{\alpha+\beta}$,随机选取 $c, S_\alpha, S_\beta, S_{x_i}, S_{\delta_1}, S_{\delta_2} \in Z_p^*$,计算 $R_1 = u^{S_\alpha} T_1^{-c}, R_2 = v^{S_\beta} T_2^{-c}$, $R_3 = e(T_3, g_2)^{S_{x_i}} e(h, w)^{-S_\alpha - S_\beta} e(h, g_2)^{-S_{\delta_1} - S_{\delta_2}} \left(\frac{e(T_3, w)}{e(g_1, g_2)}\right)^c$, $R_4 = T_1^{S_{x_i}} u^{-S_{\delta_1}}, R_5 = T_2^{S_{x_i}} v^{-S_{\delta_2}}$。

设置 $M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5$ 的 hash 值为 c,如果发生碰撞,则失败退出;否则返回签名 $\sigma = (T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, S_\alpha, S_\beta, S_{x_i}, S_{\delta_1}, S_{\delta_2})$ 给 A。

d)输出伪造的签名 σ。

将上述模拟过程重新绕回到选取 c 前,选取不同的 c', $S_\alpha', S_\beta', S_{x_i}', S_{\delta_1}', S_{\delta_2}'$。令 $\Delta c = c - c'$,同样定义 $\Delta S_\alpha, \Delta S_\beta, \Delta S_{x_i}, \Delta S_{\delta_1}, \Delta S_{\delta_2}$,令 $\bar{\alpha} = \frac{\Delta S_\alpha}{\Delta c}, \bar{\beta} = \frac{\Delta S_\beta}{\Delta c}, \bar{x} = \frac{\Delta S_{xi}}{\Delta c}$,得 $\frac{e(g_1, g_2)}{e(T_3, w)} = e(T_3, g_2)^{\bar{x}} e(h, w)^{-\bar{\alpha}-\bar{\beta}} e(h, g_2)^{-\bar{x}(\bar{\alpha}+\bar{\beta})}$,因此 $e(g_1, g_2) = e(T_3 h^{-\bar{\alpha}-\bar{\beta}}, w g_2^{\bar{x}})$,令 $\bar{A} = T_3 h^{-\bar{\alpha}-\bar{\beta}}$,则 $e(\bar{A}, w g_2^{\bar{x}}) = e(g_1, g_2)$,所以 $(\bar{A}, \bar{x})$ 是 q-SDH 问题解,这与 q-SDH 假设矛盾。

情形 2　MA 半诚实。

a)如果 CDH 假设成立,恶意车辆在车辆注册阶段,从 MA 只能获得一个秘密。

证明　定义与 MA 交互的模拟器 M 如下:

(a)M 生成 $y = \hat{g}^r \hat{h}^k$,随机选取 $\{b_j\}_{1 \leqslant j \leqslant n}$,并发送给 MA。

(b)MA 计算并返回 $a = \hat{g}^t$。

(c)Hash 询问。当 M 询问 (z, j) 的 hash 值,如果 $z = \left(\frac{y}{\hat{h}^j}\right)^t$,MA 返回 $\frac{b_j}{g_1^{\frac{1}{m_j + \gamma}}}$,否则返回随机数。将结果记入 F 表。

(d)M 输出秘密 $g_1^{\frac{1}{m_j + \gamma}}$。

假设 M 获得了两个秘密,对应的 hash 询问不妨设为 z_1 和 z_2,则 $z_1 = \left(\frac{y}{\hat{h}^k}\right)^t, z_2 = \left(\frac{y}{\hat{h}^j}\right)^t (k \neq j)$,因此 $\hat{h}^t = \left(\frac{z_1}{z_2}\right)^{\frac{1}{j-k}}$,令 $\hat{h} = \hat{g}^s$,则 $\hat{h}^t = \hat{g}^{st}$,这意味着由 $\hat{g}^s$、$\hat{g}^t$,可求出 $\hat{g}^{st}$,与 CDH 假设矛盾。

b)如果 DL 假设成立,在车辆注册阶段,MA 无法确定车辆最终得到的是哪个秘密。

这是因为在车辆注册阶段,车辆随机选 r 和 k,生成 $y = \hat{g}^r \hat{h}^k$,并发送给 MA。在 DL 假设下,车辆选择的 k 对于 MA 是安全的。

c)如果 DL 假设成立,在车辆追踪阶段,即使 MA 和 TA_s 合谋,TA_s 也无法获得车辆的另一部分私钥 x_i。

虽然 TA_s 通过追踪协议获得了车辆的部分私钥 A_i, MA 和 TA_s 合谋并告之 γ,不妨假设 TA_s 能获得 x_i,这意味着由 A_i, $A_i^{x_i} \left(= \frac{g_1}{A_i^\gamma}\right)$,$TA_s$ 可求出 x_i,与 DL 假设矛盾。

情形 3　MA 不诚实,即 MA 直接欺骗,伪造车辆私钥。

车辆 V_i 用知识证明向仲裁者证明其拥有私钥 (A_i, x_i)。

a) 仲裁者随机选取 t,向车辆发送 g_2^t, w^t。

b) 车辆计算并发送 $e(A_i^{x_i}, g_2^t) e(A_i, w^t)$。

c) 仲裁者验证 $e(A_i^{x_i}, g_2^t) e(A_i, w^t) = e(g_1, g_2)^t$,如等式成立,则表明 MA 伪造私钥。

性质 2　除权威,其他实体根据群签名结果确定车辆身份,在计算上是不可行的,方案具有匿名性。

证明　除权威外的其他实体已知 u, v, h, h_0, h_1, h_2 及关系 $u^{\zeta_1} = v^{\zeta_2} = h, h_1 = h_0^{\zeta_1}, h_2 = h_0^{\zeta_2}$,在 DL 困难性假设下,$\zeta_1$ 和 ζ_2 是安全的。其他实体无法对车辆的身份进行追踪,方案具有匿名性。

性质 3　TA_s 中 m 个成员联合可以由签名恢复出车辆 V_i 的私钥 A_i,方案具有可追踪性和健壮性。

证明　由系统初始化协议和拉格朗日插值定理知

$$\zeta_1 = \sum_{i=1}^{m} \zeta_{1,i} l_i(0), \zeta_2 = \sum_{i=1}^{m} \zeta_{2,i} l_i(0)$$

故 $$\frac{T_3}{\prod_{i=1}^{m} (T_1^{\zeta_{1,i}} \cdot T_2^{\zeta_{2,i}})^{l_i(0)}} = \frac{T_3}{T_1^{\sum_{i=1}^{m} \zeta_{1,i} l_i(0)} T_2^{\sum_{i=1}^{m} \zeta_{2,i} l_i(0)}} = \frac{T_3}{T_1^{\zeta_1} T_2^{\zeta_2}} = \frac{A_i h^{\alpha+\beta}}{u^{\alpha\zeta_1} v^{\beta\zeta_2}} = \frac{A_i h^{\alpha+\beta}}{h^\alpha h^\beta} = A_i$$

因此 TA_s 中 m 个成员联合可计算出 A_i,将 A_i 交给 MA,MA 将其加入 RL,在群内广播,方案具有可追踪性。只要 TA_s 中妥协成员的数量不超过 $m-1$,则无法揭露车辆身份,方案具有健壮性。

本方案和 GSIS[5]、Signcryption[8] 的安全性比较如表 1 所示。三个方案都满足匿名、可追踪和可撤销性。GSIS 和 Signcryption 没有提供强不可伪造性,这是因为车辆的私钥完全由权威产生并颁发,权威可以伪造签名。由于本方案引入门限秘密共享,在隐私保护方面容忍部分权威妥协,提供了系统的健壮性。因此本方案在强不可伪造性、健壮性方面要优于已有方案。

表 1 安全性比较

方案	强不可伪造	匿名	追踪	健壮	撤销
GSIS[5]	×	√	√	×	√
Signcryption[8]	×	√	√	×	√
本文方案	√	√	√	√	√

4　性能分析

4.1　消息长度

为达到 $t = 80$ 安全水平,即相当于密钥长度为 1 024 bit 的 RSA 签名的安全强度,文献[16]指出 $|p| = 160, |G_1| = 161$,其中 $|p|$、$|G_1|$ 分别表示阶 p、G_1 中元素的比特长度。

1)注册消息长度

在注册协议 2 轮交互中,权威为车辆颁发秘密的消息较长,故比较三个方案中该消息的长度。GSIS[5] 直接将车辆的私钥 (x_i, A_i) 颁发给车辆,注册消息长度约为 40 Byte。Signcryption[8] 将私钥分组加密后颁发,如选择 AES 的 128 bit 分组,则长度为 48 Byte。本方案采用不经意传输协议将 a、$\{b_j\}_{1 \leqslant j \leqslant n}$ 发送给车辆,注册消息长度为 $20(n+1)$ Byte,通信代价增加,但由于消息传输发生注册阶段,对系统整体性能的影响有限。

2)签名消息长度

本方案签名消息格式如图 3 所示。由于 $|\sigma| = 8|G_1| + 5|p| = 2088\text{bit} = 261\text{Byte}$,消息总长度 $= 2 + 2 + 100 + 4 + 261 + 1 = 370\text{Byte}$。GSIS 签名约 180 Byte,消息总长度约 289 Byte。因为增添了批验证需要的数据项,本方案、Signcryption 比 GSIS 签名消息长,如表 2 所示。

表 2 消息长度比较　　/Byte

方案	注册	签名
GSIS[5]	40	289
Signcryption[8]	48	368
本文方案	$20(n+1)$	370

4.2 计算时间

由于 G_1 上乘法、hash、Z_p^* 上乘法等操作的运算量较小，因此将 G_1 上指数、双线性映射(配对)作为主要运算进行分析，用 $x \cdot G_1$ 表示 G_1 中 x 次指数运算，用 $x \cdot P$ 表示 x 次配对运算。在签名算法中，考虑到两个配对 $e(h,w)$ 和 $e(h,g_2)$ 可以预先计算好，签名计算量由 $12 \cdot G_1 + 3 \cdot P$ 减为 $12 \cdot G_1 + 1 \cdot P$。在验证算法中，q 个签名集合的验证只需两个配对运算，总计算量为 $14q \cdot G_1 + 2 \cdot P$，平均每个消息验证的计算量为 $14 \cdot G_1 + 2 \cdot P/q$。跟踪协议中，$m$ 个参与追踪的成员进行分布式计算，总计算量为 $3m \cdot G_1$，平均每个成员计算量为 $3 \cdot G_1$。撤销协议中，车辆对长为 l 的撤销列表计算量为 $3 \cdot P$。方案时间性能如表 3 所示，其中 n、m、l 和 q 分别表示不经意传输协议参数、秘密共享门限值、撤销列表长度、批验证消息数。

表 3 本方案的时间性能

操作	计算代价
注册	$3n \cdot G_1 + 4 \cdot G_1$
签名	$12 \cdot G_1 + 1 \cdot P$
验证	$14 \cdot G_1 + 2 \cdot P/q$
跟踪	$3 \cdot G_1$
撤销	$3 \cdot P$

在 Pentium 4 3.0 GHz 机器上(性能接近于 VANET 未来的车载设备系统)，当 $|p| = 160$，群 G_1 的一次指数运算时间约0.6 ms，配对运算时间 4.5 ms[16]。GSIS、Signcryption 和本方案时间性能比较如表 4 所示。

表 4 时间性能比较 /ms

方案	注册	签名	验证	跟踪	撤销
GSIS[5]	0.6	11.7	16.2	1.2	$9 + 4.5l$
Signcryption[8]	12	11.7	$8.4 + 9/q$	1.2	$9 + 4.5l$
本文方案	$1.8n + 2.4$	11.7	$\leqslant 8.4 + 9/q$	1.8	13.5

由表 4 可看出，三个方案在签名阶段的计算时间一样。在验证阶段，本方案和 Signcryption 的时间性能要优于 GSIS；当验证返回 true 时，本方案与 Signcryption 的计算时间一样；当返回 false 时，计算时间较 Signcryption 方案少。在撤销阶段，本方案使用预处理，时间性能最优。注册阶段，Signcryption 建立秘密分发的安全信道耗费了时间。本方案不经意传输中的消息嵌入、提取等操作，也增加计算时间。跟踪阶段，m 个参与追踪的成员分布式地计算，单个成员的计算时间略高于已有方案。

以上分析表明本方案的通信和计算代价大体与已有方案相近，批验证和撤销预处理减少了计算开销，但由于使用了不经意传输和协同追踪，使注册和跟踪协议的计算时间增加，这也是为了强化防止权威伪造签名或权威妥协方面的安全性能而增加的代价。而且，考虑这两个协议往往运行在车辆进入 VANET 前和车辆发生争议阶段，对 VANET 通信影响不大，因此方案是有效的。

5 结束语

本文给出基于不经意传输和群签名的 VANET 强隐私保护方案，解决了现有方案中未解决的权威伪造签名和部分权威妥协后车辆隐私泄露问题。方案由系统初始化、车辆注册、消息签名、批验证、联合追踪、车辆撤销六部分组成。安全性分析表明，方案具有强不可伪造性、匿名性、可追踪性、健壮性。性能分析表明，批验证和撤销预处理减少了签名消息验证和处理撤销列表时间，方案整体的通信和计算代价与已有方案相近。将本方案实际应用于 VANET 安全通信，满足车辆的隐私需求是笔者进一步的工作。

参考文献：

[1] The Sixth Framework Programme of the European Commission. SeVeCom[EB/OL]. (2009-09) [2011-03]. http://www.sevecom.org.

[2] ZEADALLY S, HUNT R, CHEN Y S, *et al*. Vehicular Ad hoc networks (VANETs): status, results, and challenges[J]. Telecommunication Systems, 2012, 50(4): 217-241.

[3] RAYA M, HUBAUX J. The security of vehicular Ad hoc networks [C] // Proc of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'05). New York: ACM Press, 2005: 11-21.

[4] BONEH D, BOYEN X, SHACHAM H. Short group signatures[C]// Proc of Advances in Cryptology (Crypto'04), LNCS, vol 3152. Berlin: Springer-Verlag, 2004: 41-55.

[5] LIN Xiao-dong, SUN Xiao-ting, HO P H, *et al*. GSIS: secure vehicular communications with privacy preserving [J]. IEEE Trans on Vehicular Technology, 2007, 56(6): 3442- 3456.

[6] CALANDRIELLO G, PAPADIMITRATOS P, HUBAUX J P, *et al*. Efficient and robust pseudonymous authentication in VANET[C] // Proc of the 4th ACM International Workshop on Vehicular Ad hoc Networks (VANET'07). New York: ACM Press, 2007: 19-28.

[7] CALANDRIELLO G, PAPADIMITRATOS P, HUBAUX J P, *et al*. On the performance of secure vehicular communication systems[J]. IEEE Trans on Dependable and Secure Computing, 2011, 8(6): 898-912.

[8] ZHANG Lei, WU Qian-hong, SOLANAS A. A scalable robust authentication protocol for secure vehicular communications[J]. IEEE Trans on Vehicular Technology, 2010, 59(4): 1606-1617.

[9] HAO Yong, CHENG Yu, ZHOU Chi, *et al*. A distributed key management framework with cooperative message authentication in VANETs[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(3): 616-629.

[10] SCHAUB F, KARGL F, MA Zhen-dong, *et al*. V-tokens for conditional pseudonymity in VANETS[C]//Proc of IEEE Wireless Communications & Networking Conference . [S. l.]: IEEE Press, 2010: 1-6.

[11] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1989, 22(11): 612-613.

[12] RABIN M O. How to exchange secrets by oblivious transfer, Technical report TR-81[R]. [S. l.]: Aiken Computation Laboratory, Harvard University, 1981.

[13] TZENG W. Efficient 1-out-of-*n* oblifvious transfer schemes with universally usable parameters[J]. IEEE Trans on Computers, 2004, 53(2): 232-240.

[14] FERRARA A, GREEN M, HOHENBERGER S, *et al*. On the practicality of short signature batch verification[C]//Proc of CT-RSA. 2009.

[15] KIM K, YIE I, LIM S, *et al*. Batch verification and finding invalid signatures in a group signature scheme[J]. International Journal of Network Security, 2011, 12(3): 229-238.

[16] SCOTT M. Efficient implementation of cryptographic pairings [EB/OL]. (2007-12-14) [2012-01-20]. ftp://ftp.disi.unige.it/pub/person/MoraF/CRYPTO/PARING/mscott-samos07.pdf.