基于群签名的前向安全 VANET 匿名认证协议

岳笑含 惠明亨 王溪波
(沈阳工业大学信息科学与工程学院 沈阳 110870)

摘 要 车载自组织网络在提高交通安全和效率方面得到广泛应用。然而,其中仍然存在着通信信任和用户隐私保护问题。许多现有认证协议都需要验证者从远程机构下载最新的撤销列表,这大大增加了远程中心的负担。为了解决这些问题,基于群签名方案,利用分散群模型和完全子树方法提出了新的认证协议。提出的协议在验证阶段无需获取最新的撤销列表,只需获取最新的时间即能验证,具有前向安全性、撤销高效性、匿名性、不可伪造性、不可诬陷性、可追踪性等特点。

关键词 群签名,车载自组织网络,匿名认证,前向安全,可追踪
中图法分类号 TP309.07 **文献标识码** A

Forward Security Anonymous Authentication Protocol Based on Group Signature for Vehicular Ad Hoc Network

YUE Xiao-han HUI Ming-heng WANG Xi-bo
(School of Information Science and Engineering, Shenyang University of Technology, Shenyang 110870, China)

Abstract Vehicular Ad Hoc network is widely used in improving traffic safety and efficiency. However, there is still a problem of communication trust and user privacy protection. Many existing authentication protocols require that certifiers download up-to-date revocation lists from remote center, which greatly increase the remote center's workload. In this paper, in order to solve these problems, a new authentication protocol based on group signature scheme was proposed by combining the decentralized group model and the complete sub-tree method. In this protocol, the verifier can verify a signature by getting the latest time, without having to obtain the latest revocation list, with forward security, effective revocation, anonymity, unforgeability, non-frameability and traceability.

Keywords Group signature, Vehicular ad hoc network, Anonymous authentication, Forward security, Traceability

1 引言

车载自组织网络(Vehicular Ad Hoc Network, VANET)可以给人们提供更安全、高效、舒适的驾驶体验,近年来备受学术界和行业的广泛关注[1-5]。具体来说,VANET 使得车辆通过车上安装的车载单元(OBU)通讯设备来与其他车辆通信,即车对车(V-2-V)通信;或车辆与路边单元(RSU)通信,即车载到基础设施(V-2-I)通信。这种混合通信方式(包括 V-2-V 和 V-2-I)使得 VANET 能够提供许多舒适和安全服务,例如接收交通和天气信息,以及对突发事件和交通违规行为进行警告[6]等,如图 1 所示。

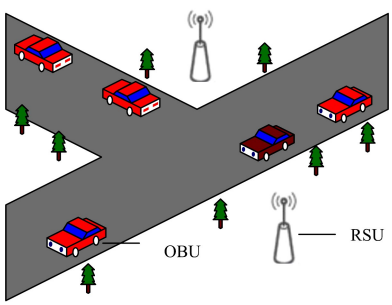

图 1 VANET 模型

尽管 VANET 具有广泛的应用前景,但在现实生活中应用 VANET 时仍有通讯安全和隐私保护问题需要解决,否则将带来许多问题。例如,如果在 VANET 中广播的消息未被认证,则 OBU 不能根据接收到的消息来评估路况;如果使用基础的认证方法来验证车辆的真实身份,则车辆的隐私信息会被暴露。

近年来,安全认证和隐私保护成为 VANET 中的一个重要研究方向。许多学者提出了基于传统数字鉴名技术来验证消息的 VANET 匿名认证方案[7-9],这需要公钥基础设施 PKI 的参与。

Raya 等[10]提出了一个基于 PKI 的方案,其中每辆车预装大量的公钥/私钥对和相应的公钥证书,车辆随机选择其中一个签名。密钥和证书被定期更换,以保护车辆的隐私。该方法能够保证消息的完整性和发送者的隐私,但是也存在一些缺点。首先,当车辆的私钥被撤销时,系统需要经常更新证书,这是一个耗时的任务;其次,每辆车需要存储大量的匿名公钥/私钥对,这就需要大量的存储空间。

Zhang 等[11]提出了一种基于身份的批量验证(IBV)方案用于车辆和 RSU 之间的通信。IBV 方案通过一次性基于身份的签名实现了条件隐私保护,但严重依赖于防篡改设备,这些设备会预先装置系统的秘密参数,一旦设备受到攻击,整

本文受辽宁省教育厅高等学校优秀人才支持计划(LJQ2015081),辽宁省科技厅博士科研启动基金(201601166)资助。
岳笑含(1982-),男,博士,讲师,主要研究方向为密码学、可信计算、信息安全等;**惠明亨**(1994-),男,硕士,主要研究方向为信息安全,E-mail:huimh034@163.com(通信作者);**王溪波**(1964-),男,博士,教授,主要研究方向为计算机检测、控制、管理信息系统设计、实时及嵌入式系统。

个系统的安全性都将受到威胁。IBV 的另一个缺点是可以追踪到车辆的真实身份，不符合隐私要求。

宋成等[12]提出了基于双线性对的匿名认证方案用于车辆和 RSU 之间的通信，但在撤销时需要更新群公钥。

通过使用群签名技术，Lin 等[13]提出了一种基于群签名技术和基于身份签名技术的匿名认证协议。由于每个群成员都可以代表群进行签名，而只有群管理员才能揭示签名者的身份，故该协议可以解决用户的匿名问题。但是，当某个违法用户需要被撤销时，会更新所有其他用户的公钥，较为低效。

此外，使用群签名技术的大多数 VANET 的现有匿名认证协议要从远程机构下载最新的撤销列表。这种本地验证撤销群签名方案 RL 包含每个撤销用户的令牌，验证算法必须验证签名每个令牌[16]，且验证成本与撤销用户的数量必然呈线性关系。

针对现有方案的不足，本文在分散管理的群模型中将整个 VANET 系统分为几个群组，每个群组由一个对应的 RSU 控制，而不是集中控制。在成员管理中，使用广播加密的完全子树方法来实现成员撤销。

然而，这两种技术不能简单地整合，在分散管理的群模型中进行认证有以下要求：

1）快速的验证，OBU 无需下载撤销列表即可验证签名的有效性；

2）高效的追踪性，要求能够以小的常数级计算和通信成本揭示任何签名的签名者的身份；

3）有效的撤销，管理器可对违法成员做出撤销，同时不改变群公钥及群成员私钥。

另外，为实现高效的前向安全性，即用户被撤销后所产生的签名不再有效，本文采用了完全子树方法对群成员证书撤销列表进行周期性更新，而无需更新整个群的公私密钥信息，进而达到高效的前向安全性。

为了达到上述要求，本文将介绍一种新的匿名认证协议，通过使用这种新的认证协议，可以很好地结合分散管理的群模型和群签名方案。具体来说，本文的主要贡献有 3 个方面：

1）所提出的协议基于群签名方案进行构建，并利用完全子树方法实现高效的前向安全性，且具备匿名认证和撤销高效性。

2）所提出的协议采用分散管理模式，将可信任的权力中心从生成 OBU 群证书的沉重工作负担中解放出来，并令 RSU 从可信任的权力中心中获取撤销列表，OBU 无需下载撤销列表即可验证签名的有效性。

3）该群签名方案支持高效追踪。追踪管理器仅需要做双线性群的 3 个指数运算，即两个乘法运算和一个除法运算，就可以追踪任何一个群签名的签名者的身份。

本文第 2 节形式化定义系统和安全模型，并确定设计目标；第 3 节介绍一些与匿名认证协议有关的基础知识；第 4 节提出了匿名身份验证协议及其基础群签名方案；第 5 节进行安全性分析；第 6 节进行性能评估；最后总结全文。

2　系统模型和设计目标

本节形式化定义系统模型和安全模型，并确定设计目标。

2.1　系统模型

该系统模型由追踪管理器（TM）、多个 RSU 和多个 OBU 组成，如图 2 所示。TM 负责认证 RSU 和 OBU 的公钥。验证后，TM 将发送相应的公钥证书。TM 还能够追踪在网络中广播非法消息的发送者的真实身份。RSU 沿着道路密集分布，管理其通信范围内的一组 OBU。具体来说，每个 RSU 将在其通信范围内发出与 OBU 的私钥一起使用的群证书中的每个 OBU 来对相应组中的广播消息进行签名。每个车辆配备了一个 OBU，OBU 可以向 RSU 请求群证书，并根据专用的短距离通信协议相互通信[17]。值得注意的是，RSU 不会向由 TM 管理的撤销列表中已存在的 OBU 发出群证书。

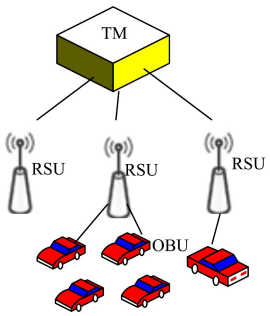

图 2　系统模型

2.2　安全模型

假设 TM 是完全可信任的，而 RSU 是诚实的。也就是说，RSU 将忠实地遵循所提议的协议，但可以发起被动攻击以尽可能获得秘密信息。具体来说，RSU 将尝试通过勾结恶意 OBU 来获取广播消息的签名者的踪迹或真实身份，但不会修改其中的通信数据和 OBU，也不会与其他 RSU 串通。除了 TM，广播消息的签名者不会被揭露。为了获得道路的非法权限，恶意的 OBU 可能会尝试广播虚假消息，而不会被检测到。

2.3　设计目标

该方案的设计目标是为 VANET 开发一个有效的匿名认证协议。该协议应具有以下性质。

1）快速验证：OBU 无需下载撤销列表即可验证签名的有效性。

2）有效撤销：TM 能够以常数级的计算和通信成本揭示任何一个签名的签名者的身份。此外，OBU 不需要从远程 TM 检索最新的撤销列表。

3）不可伪造性：只有持有来自一个 RSU 的组证书的 OBU 可以代表由 RSU 维护的组生成有效的签名。

4）匿名性：只有 TM 才能揭示签名者的身份。换句话说，如果 OBU 不在自己的通信范围内，即使 RSU 也不能显示任何 OBU 的位置。

5）可追溯性：任何 OBU 都无法生成跟踪到其他 OBU 的任何有效的签名。

6）前向安全性：保证在当前密钥泄露时对之前的签名不会造成危害。

3　预备知识

本节将回顾一些与匿名认证协议有关的基本知识，包括群签名、双线性群和数学难题假设、BBS＋签名、完全子树方法。

3.1　群签名的定义

群签名是一种特殊的数字签名，存在 3 种实体：群管理者、追踪者和一些群成员。它允许群成员代表群签署消息，除

了追踪者之外，其他人不能揭示签名者的身份。群签名方案由以下 5 种算法组成：SETUP，CERTGEN，SIGN，VERIFY 和 OPEN。算法 SETUP 采用安全参数作为输入，并输出系统中每个实体（群管理者，追踪者和群成员）的公钥/私钥对。算法 CERTGEN 将群管理员的私钥、群成员和追踪者的公钥作为输入，并输出与输入群成员的公钥相对应的群证书。算法 SIGN 将群证书、群成员公钥和消息 M 作为输入，输出相应的签名。算法 VERIFY 验证消息和消息签名的有效性，如果签名有效则输出 1，否则输出 0。OPEN 算法由追踪者运行，将追踪者的私钥、消息和有效签名作为输入，并输出生成签名的群成员。另一方面，群签名方案也应该满足以下 3 种安全属性：不可伪造性、匿名性和可追踪性。第一个安全属性确保只有群成员可以代表群生成签名。第二个安全属性确保除了追踪者外没有人能揭露其签名者的身份。第三个安全属性确保所有有效的签名，追踪者可以追踪签名者的身份。

3.2 双线性群

设 G_1 和 G_2 是生成元分别为 g 和 h 的两个 p（p 为素数）阶加法循环群。又设 G_T 是具有相同阶数的乘法循环群，其单位元记为 1。双线性对 $e(G_1,G_2)\rightarrow G_T$ 是满足以下性质的一个映射：对于任意的 $m,n\in Z_p$，$P_1\in G_1$，$P_2\in G_2$，有 $e(P_1^m,P_2^n)=e(P_1,P_2)^{mn}$ 成立；将上述生成的结果记为 (p,G_1,G_2,G_T,e,g,h)。

对于 (p,G,g)，令 $x\xleftarrow{R}Z_p$，$y:=g^x$。离散对数（DL）问题为：给定 (g,y,p,G)，求出 $x=\log_g y$。

概率多项式时间算法 A 解决 DL 问题的优势记为 $Adv_A^{DL}(\lambda)=\Pr[A(g,y,p,G)=x\mid y=g^x]$。

定义 1 对于任意的概率多项式时间算法 A，解决 DL 问题的优势 $Adv_A^{DL}(\lambda)$ 是可忽略的。

对于 $(p,G_1,G_2,G_T,e,g,h),u,v,h\leftarrow G_1,\alpha,\beta,r\leftarrow Z_p$，令 $g1:=u^\alpha$，$g2:=v^\beta$。判定线性难题（DLIN）如下：给定一组 $(u,v,h,u^\alpha,v^\beta,z)$，如果 $z=h^{\alpha+\beta}$，输出 1；否则 $z=h^r$，输出 0。概率多项式时间算法 A 解决 DLIN 问题的优势记为 $Adv_A^{DLIN}(\lambda)=\Pr[A(u,v,h,u^\alpha,v^\beta,z)=1\mid z=h^{\alpha+\beta}]-\Pr[A(u,v,h,u^\alpha,v^\beta,z)=1\mid z=h^\gamma]$。

定义 2 对于任意的概率多项式时间算法 A，解决 DLIN 问题的优势 $Adv_A^{DLIN}(\lambda)$ 是可忽略的。

对于 $(p,G_1,G_2,G_T,e,g,h),r\leftarrow Z_p,A_i:=g^{\gamma^i}$，$i=0,\cdots,q$。q-SDH 难题如下：给定一组 $(g,(A_i)_{i\in[0,q]},h,h^\gamma)$，输出 $(c,g^{1/(\gamma+c)})$，其中 $c\in z_p^*$。概率多项式时间算法 A 解决 q-SDH 问题的优势记为 $Adv_A^{q\text{-}SDH}(\lambda)=\Pr[A(g,(A_i)_{i\in[0,q]},h,h^\gamma)=(c,g^{1/(\gamma+c)})]$。

定义 3 对于任意的概率多项式时间算法 A，解决 q-SDH 问题的优势 $Adv_A^{q\text{-}SDH}(\lambda)$ 是可忽略的。

3.3 BBS+ 签名

BBS+ 签名[17] 如下：给定 $(p,G_1,G_2,G_T,e),g_0,g_1,\cdots,g_L,g_{L+1}$ 为 G_1 的生成元，h 为 G_2 的生成元。

密钥生成：随机选择 $\gamma\xleftarrow{R}Z_p$，令 $w=h^\gamma$，则签名密钥为 $sk=\gamma$，验证密钥为 $vk=w$。

签名：对于要签名的消息 $(m_1,\cdots,m_L)$，随机选择 $\eta,\zeta\xleftarrow{R}Z_p$，计算 $A=(g_0g_1^\zeta g_2^{m_1}g_{L+1}^{m_L})^{1/(\eta+\gamma)}$。签名值 $\sigma=(A,\eta,\zeta)$。

验证：对于收到的签名 $\sigma=(A,\eta,\zeta)$ 和消息 $(m_1,\cdots,m_L)$，检验下面等式是否成立：$e(A,h^\eta w)=e(g_0g_1^\zeta g_2^{m_1}\cdots g_{L+1}^{m_L},h)$

该签名算法在 q-SDH 难题假设下具有不可伪造性[18]。

3.4 完全子树方法

Naor，Naor 和 Lotspiech（NNL）[19] 提出的子集覆盖框架是一种用于成员撤销和违法成员追踪的通用技术，该技术可用于构造广播加密。这个框架有两种方法实现：子集差（SD）和完全子树（CS）方法。

使用完全子树方法，给二叉树的每个节点分配一个密钥，并将每个用户分配给二叉树的一个叶节点，使 $\{u_0,u_1,\cdots,u_l\}$ 是从根节点到叶节点的路径。用户获得的密钥是与每个 $u_i\in\{u_0,u_1,\cdots,u_l\}$ 相关联的。密文由该方法定义的节点的密钥计算。令 $\{u_0',u_1',\cdots,u_l'\}$ 是一组节点，它们对应的密钥用于加密。如果一个用户的路径为 $\{u_0',u_1',\cdots,u_l'\}$，其被指示为被授权的接收方，则存在一个节点 u，使得 $u\in\{u_0,u_1,\cdots,u_l\}\cap\{u_0',u_1',\cdots,u_l'\}$。因此，用户可以使用与节点 u 对应的密钥来解密密文。

4 VANET 匿名身份验证协议

本节介绍一个群签名方案，为车载自组织网络匿名认证协议提供基础。表 1 中给出一些符号及其含义。

表 1 符号说明

符号	含义
TM	追踪管理器
RSU	路边单元
OBU	车载单元
G_1,G_2,G_T	椭圆曲线上的循环群
Z_p	p 阶加法群
$cert_{rsu}$	RSU 的证书
$cert_{obu}$	OBU 的证书
RL_t	t 时刻撤销列表
gpk	群公钥
sk_{OA}	开启密钥
sec_i	OBU_i 的私钥
M	消息
σ	签名值

4.1 群签名方案

（1）系统建立

Setup(λ，N)：由安全参数 λ 生成参数 (p,G_1,G_2,G_T,e,g,h)。随机选取 $f_1,f_2,f_3,h_0,h_1,h_2\xleftarrow{R}G_1$，随机选取 $\gamma_0,\gamma_1\xleftarrow{R}Z_p$，则群管理者密钥对为 $(sk_0,vk_0)=(\gamma_0,h^{\gamma_0})$，$(sk_1,vk_1)=(\gamma_1,h^{\gamma_1})$。然后，随机选择 $\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3'\xleftarrow{R}Z_p$，计算：$g_1=f_1^{\varepsilon_1}f_3^{\varepsilon_3}$，$g_2=f_2^{\varepsilon_2}f_3^{\varepsilon_3}$，$g_1'=f_1^{\varepsilon_1'}f_3^{\varepsilon_3'}$，$g_2'=f_2^{\varepsilon_2'}f_3^{\varepsilon_3'}$。选用一个哈希函数 $H:\{0,1\}^*\rightarrow Z_p$。

1）开启密钥为 $sk_{OA}=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3')$；

2）群管理者密钥为 $sk_{GM}=(sk_0,sk_1)=(\gamma_0,\gamma_1)$；

3）群公钥 $(p,G_1,G_2,G_T,e,g,h,f_1,f_2,f_3,h_0,h_1,h_2,g_1,g_2,g_1',g_2',vk_0,vk_1,H)$；

4）存储器 $St=(St_{user},St_{trans})$（初始状态为空）。

（2）成员加入

Join：用户 i 随机选取 $x\leftarrow Z_p$ 计算 $X=h_2^x$。对 X 进行一个签名 sig_i，用以向管理者证明自己的身份，将 (X,sig_i) 发送给群管理者。群管理者 GM 给用户 i 分配一个二叉树的叶子节点 u_l。根节点到叶节点的路径为 $u_0,u_1,\cdots,u_l$。对于每个 $j=0,1,\cdots,l$，群管理者随机选取 $\eta_j,\zeta_j\xleftarrow{R}Z_p$，计算：$A_j=(gh_0^{\zeta_j}h_1^{u_j}X)^{1/(\gamma_0+\eta_j)}$。向用户发送 $\{\theta_j=(A_j,\eta_j,\zeta_j)\}_{j=0}^l$ 和

$\langle v_i\rangle:=(u_0,u_1,\cdots,u_l)$。

1)用户成员资格证书为 $cert_i=(\langle v_i\rangle,\{A_j\}_{j=0}^{l},X)$,私钥 $sec_i=x$;

2)群管理者将用户 i 和副本 $transcript_i=(X,\{A_j\}_{j=0}^{l},sig_i)$添加进存储器。

(3)成员撤销

Revoke(gpk,sk_{GM},t,R_t):使用完全子树方法确定代表所有未撤销用户的节点集合$\{u_0',u_1',\cdots,u'_{num}\}$。对于每个 $i=0,1,\cdots,num$,群管理者随机选取 $\eta_i',\zeta_i'\xleftarrow{R}Z_p$,计算:$B_{i,t}=(gh_0^{\zeta_i'}h_1^{u_i}h_2^{t})^{1/(\gamma_1+\eta_i')}$。令$\{\Theta=(B_{i,t},\eta_i',\zeta_i')\}_{i=0}^{num}$,则 t 时刻的撤销列表为 $RL_t=(t,R_t,\Theta)$。

(4)签名算法

Sign($gpk,t,RL_t,cert_i,sec_i,M$):若 $i\in R_t$,则不能进行签名。否则做如下运算:由于 i 没有被撤销,则存在一个节点 u_j 同时满足以下等式:

$$A_j=(gh_0^{\zeta_j'}h_1^{u_j}X)^{1/(\gamma_0+\eta_j)} \tag{1}$$

$$B_{j,t}=(gh_0^{\zeta_j'}h_1^{u_j}h_2^{t})^{1/(\gamma_0+\eta_j')} \tag{2}$$

然后随机选取 $\alpha,\beta\leftarrow Z_p$,计算:

$$\psi_1=f_1^{\alpha},\psi_2=f_2^{\beta},\psi_3=f_3^{\alpha+\beta},\psi_4=g_1^{\alpha}g_2^{\beta}A_j,\psi_5=g_1'^{\alpha}g_2'^{\beta}B_{j,t}) \tag{3}$$

接着签名者构建一个非交互零知识证明:随机选取 $r_\alpha,r_\beta,r_\eta,r_\zeta,r_{\eta'},r_{\zeta'},r_{\alpha\eta},r_{\beta\eta},r_{\alpha\eta'},r_{\beta\eta'},r_{u_j},r_x\xleftarrow{R}Z_p$,计算 $R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'}$,如下:

$R_\alpha\leftarrow f_1^{r_\alpha},R_\beta\leftarrow f_2^{r_\alpha},R_{\alpha+\beta}\leftarrow f_3^{r_\alpha+r_\beta}$

$R_A\leftarrow e(\psi_4,h)^{r_\eta}e(g_1,h)^{-r_{\alpha\eta}}e(g_1,vk_0)^{-r_\alpha}\cdot e(g_2,h)^{-r_{\beta\eta}}e(g_2,vk_0)^{-r_\beta}e(h_0,h)^{-r_\zeta}\cdot e(h_1,h)^{-r_{u_j}}e(h_2,h)^{-r_x}$

$R_{\alpha\eta}\leftarrow\psi_1^{r_\eta}f_1^{-r_{\alpha\eta}},R_{\beta\eta}\leftarrow\psi_2^{r_\eta}f_2^{-r_{\beta\eta}}$

$R_B\leftarrow e(\psi_5,h)^{r_{\eta'}})e(g_1',h)^{-r_{\eta'}}e(g_1',vk_0)^{-r_\alpha}\cdot e(g_2',h)^{-r_{\beta\eta'}}e(g_2',vk_0)^{-r_\beta}\cdot e(h_0,h)^{-r_{\zeta'}}\cdot e(h_1,h)^{-r_{u_j}}$

$R_{\alpha\eta'}\leftarrow\psi_1^{r_{\eta'}}f_1^{-r_{\alpha\eta'}},R_{\beta\eta'}\leftarrow\psi_2^{r_{\eta'}}f_2^{-r_{\beta\eta'}}$ (4)

最后使用上述计算结果,用哈希函数 H 计算:$c\leftarrow H(M,\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'})$,计算以下值:

$s_\alpha\leftarrow r_\alpha+c\alpha,s_\beta\leftarrow r_\beta+c\beta,s_\eta\leftarrow r_\eta+c\eta$

$s_\zeta\leftarrow r_\zeta+c\zeta,s_{\eta'}\leftarrow r_{\eta'}+c\eta',s_{\zeta'}\leftarrow r_{\zeta'}+c\zeta'$

$s_{\alpha\eta}\leftarrow r_{\alpha\eta}+c\alpha\eta,s_{\alpha\eta'}\leftarrow r_{\alpha\eta'}+c\alpha\eta'$

$s_{\beta\eta}\leftarrow r_{\beta\eta}+c\beta\eta,s_{\beta\eta'}\leftarrow r_{\beta\eta'}+c\beta\eta'$

$s_{u_j}\leftarrow r_{u_j}+cu_j,s_x\leftarrow r_x+cx$ (5)

证据 π 为:$(c,s_\alpha,s_\beta,s_\eta,s_\zeta,s_{\eta'},s_{\zeta'},s_{\alpha\eta},s_{\alpha\eta'},s_{\beta\eta},s_{\beta\eta'},s_{u_j},s_x)$,签名者将签名$(\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,\pi)$发送给接收者。

(5)验证算法

Verify(σ,M,t,gpk):接收者收到群签名 $\sigma=(\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,\pi)$后,计算如下值:

$R_\alpha'\leftarrow f_1^{s_\alpha}\psi_1^{-c},R_\beta'\leftarrow f_2^{s_\alpha}\psi_2^{-c},R'_{\alpha+\beta}\leftarrow f_3^{s_\alpha+s_\beta}\psi_3^{-c}$

$R_A'\leftarrow e(\psi_4,h)^{s_\eta}e(g_1,h)^{-s_{\alpha\eta}}e(g_1,vk_0)^{-s_\alpha}\cdot e(g_2,h)^{-s_{\beta\eta}}e(g_2,vk_0)^{-s_\beta}e(h_0,h)^{-s_\zeta}e(h_1,h)^{-s_{u_j}}\cdot e(h_2,h)^{-s_x}(e(g,h)/e(\psi_4,vk_0))^{-c}$

$R'_{\alpha\eta}\leftarrow\psi_4^{s_\eta}f_1^{-s_{\alpha\eta}},R'_{\beta\eta}\leftarrow\psi_2^{s_\eta}f_2^{-s_{\beta\eta}}$

$R_B'\leftarrow e(\psi_5,h)^{s_{\eta'}}e(g_1',h)^{s_{\eta'}}e(g_1',vk_0)^{-s_\alpha}\cdot e(g_2',h)^{-s_{\beta\eta'}}e(g_2',vk_0)^{-s_\beta}e(h_0,h)^{-s_{\zeta'}}e(h_1,h)^{-s_{u_j}}\cdot(e(g,h)e(h_2,h)^{t}/e(\psi_5,vk_1))^{-c}$

$R'_{\alpha\eta}\leftarrow\psi_1^{s_{\eta'}}f_1^{-s_{\alpha\eta'}},R_{\beta\eta}'\leftarrow\psi_2^{s_{\eta'}}f_2^{-s_{\beta\eta'}}$ (6)

如果 $c=H(M,\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'})$,则验证通过,否则验证不通过。

(6)开启算法

Open($M,t,RL_t,\sigma,sk_{OA},gpk,S_t$):计算 $A'=\psi_4/\psi_1^{\xi_1}\psi_2^{\xi_2}\psi_3^{\xi_3}$,存在一个用户 i,有 $transcript_i=(X,A',sig_i)$,验证 sig_i 对应的用户 i。

4.2　车载自组织网络匿名认证协议

基于上述群签名方案,VANET 匿名认证协议由 7 个部分组成:系统初始化(Setup)、成员注册(Registration)、OBU 加入(Join)、消息签名(Sign)、消息认证(Verify)、身份追踪(Open)和 OBU 撤销(Revoke)。

(1)初始化阶段

在这个阶段,TM 生成整个系统的参数以及自身的密钥。此外,TM,RSU 和 OBU 也生成自己的个人密钥对。

TM 执行以下步骤:

由安全参数 λ 生成参数 (p,G_1,G_2,G_T,e,g,h)。其中,G_1,G_2,G_T 为 p 阶,g 为 G_1 生成元,h 为 G_2 生成元。随机选取 $f_1,f_2,f_3,h_0,h_1,h_2\xleftarrow{R}G_1$。选用一个哈希函数 $H:\{0,1\}^{*}\rightarrow Z_p$。

随机选取 $\gamma_1\xleftarrow{R}Z_p$,则$(sk_1,vk_1)=(\gamma_1,h^{\gamma_1})$。TM 随机选择 $\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3'\xleftarrow{R}Z_p$,计算:

$$g_1=f_1^{\varepsilon_1}f_3^{\varepsilon_3},g_2=f_2^{\varepsilon_2}f_3^{\varepsilon_3},g_1'=f_1^{\varepsilon_1'}f_3^{\varepsilon_3'},g_2'=f_2^{\varepsilon_2'}f_3^{\varepsilon_3'}$$

其中,$sk_{OA}=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3')$作为 TM 的开启密钥。公布系统参数$(p,G_1,G_2,G_T,e,g,h,f_1,f_2,f_3,h_0,h_1,h_2,g_1,g_2,g_1',g_2',vk_1,H)$。

每个 RSU 随机选取 $\gamma_0\xleftarrow{R}Z_p$,计算$(sk_0,vk_0)=(\gamma_0,h^{\gamma_0})$,$vk_0$ 作为 RSU 的群公钥,sk_0 作为其私钥。

每个 OBU 随机选取 $x\leftarrow Z_p$,计算 $X=h_2^{x}$。x 作为其私钥。

(2)成员注册阶段

每个 RSU 要从 TM 获取公钥证书,每个 RSU 应通过使用一些零知识证明相应的密钥的知识协议,如文献[22]中的 Shamir 零知识证明。之后,TM 发送 RSU 的公钥证书 $certg_{rsu}$。

每个 OBU 要从 TM 获取公钥证书,每个 OBU 应使用一些零知识来证明相应的密钥的知识,如文献[22]中的协议。OBU 向 TM 发送 X,然后 TM 为 OBU 分配一个二叉树叶节点,其路径为$\langle u_0,u_1,\cdots,u_l\rangle$。之后,TM 发送 OBU 的公钥证书 $cert_{obu}=\{u_l,X\}$。

TM 使用完全子树方法确定代表所有未撤销用户的节点集合$\{u_0',u_1',\cdots,u'_{num}\}$。对于每个 $i=0,1,\cdots,num$,群管理者随机选取 $\eta_{i'},\zeta_{i'}\xleftarrow{R}Z_p$,计算 $B_{i,t}=(gh_0^{\zeta_{i'}}h_1^{u_{i'}}h_2^{t})^{1/(\gamma_1+\eta_{i'})}$。令$\{\Theta=(B_{i,t},\eta_{i'},\zeta_{i'})\}_{i=0}^{num}$,$t$ 时刻的撤销列表为 $RL_t=(t,R_t,\Theta)$。假定 RSU 能获取到最新的二叉树和撤销列表为 RL_t。

(3)OBU 加入

当一个 OBU 行驶到一个新的 RSU 的通信范围内时,OBU 加入,它是 OBU 和 RSU 之间的交互式阶段。

当 OBU 进入新的 RSU 的通信范围时,OBU 将发出请求消息以获取 RSU 的公钥。

RSU 收到请求消息后，广播自己的群公钥和证书 $cert_{rsu}$。

OBU 接收到 RSU 的群公钥和证书 $cert_{rsu}$，检验其有效性，若无效，则再次发出请求；若有效，OBU 则将自己的个人证书 $cert_{obu}$ 用 RSU 的公钥加密，再将结果 C_{obu} 发送给 RSU。

RSU 收到 C_{obu} 后，对其进行解密，然后检验 $cert_{obu}$ 的有效性。若 $cert_{obu}$ 无效或已被撤销，则终止；若有效，RSU 则检验 OBU_i 二叉树的叶子节点 u_t，根节点到叶节点的路径为 u_0，u_1，…，u_l。$\{u_0,u_1,\cdots,u_l\}$ 与节点集合 $\{u_0',u_1',\cdots,u_{num}'\}$ 的交点为 u_j，计算：$A_j=(gh_0^{\xi_j}h_1^{u_j}X)^{1/(\gamma_0+\eta_j)}$。RSU 再查看撤销列表 RL_t，得到 u_j 对应的 $B_{j,t}$。向 OBU_i 发送 $\theta_j=(A_j,\eta_j,\zeta_j)$，$\theta_j'=(B_{j,t},\eta_j',\zeta_j')$。$OBU_i$ 的私钥 $sec_i=x$。

最后，RSU 将 OBU 的副本 $transcript_i=(X,A_j)$ 发送给 TM，TM 将其添加进存储器。

(4)签名阶段

图 3 给出消息的格式。其中，消息 ID 表示消息类型；有效载荷部分包含与执行 OBU 的车辆相关的信息，例如位置、交通事件和事件时间；TTL 部分是“生存时间”，确定在 VANET 中允许转发的次数；群 ID 部分用于标识哪个 RSU 向 OBU 发出群证书；签名部分是前四部分的 OBU 签名。

消息 ID	有效载荷	TTL	群 ID	签名

图 3 消息格式

在输入消息 $M\in\{0,1\}^*$ 时，OBU 使用群签名方案的算法 SIGN 对消息进行签名，并与消息 M 一起广播签名。具体如下：

随机选取 $\alpha,\beta\leftarrow Z_p$，计算：

$$\psi_1=f_1^{\alpha},\psi_2=f_2^{\beta},\psi_3=f_3^{\alpha+\beta},\psi_4=g_1^{\alpha}g_2^{\beta}A_j,\psi_5=g_1'^{\alpha}g_2'^{\beta}B_{j,t} \tag{7}$$

随机选取 $r_\alpha,r_\beta,r_\eta,r_\zeta,r_{\eta'},r_{\zeta'},r_{\alpha\eta},r_{\beta\eta},r_{\alpha\eta'},r_{\beta\eta'},r_{u_j},r_x\overset{R}{\leftarrow}Z_p$，计算 $R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'}$，如下：

$R_\alpha\leftarrow f_1^{r_\alpha},R_\beta\leftarrow f_2^{r_\alpha},R_{\alpha+\beta}\leftarrow f_3^{r_\alpha+r_\beta}$

$R_A\leftarrow e(\psi_4,h)^{r_\eta}e(g_1,h)^{-r_{\alpha\eta}}e(g_1,vk_0)^{-r_\alpha}\cdot e(g_2,h)^{-r_{\beta\eta}}e(g_2,vk_0)^{-r_\beta}e(h_0,h)^{-r_\zeta}\cdot e(h_1,h)^{-r_{u_j}}e(h_2,h)^{-r_x}$

$R_{\alpha\eta}\leftarrow\psi_1^{r_\eta}f_1^{r_{\alpha\eta}},R_{\beta\eta}\leftarrow\psi_2^{r_\eta}f_2^{-r_{\beta\eta}}$

$R_B\leftarrow e(\psi_5,h)^{r_{\eta'}}e(g_1',h)^{-r_{\eta'}}e(g_1',vk_0)^{-r_\alpha}\cdot e(g_2',h)^{-r_{\beta\eta'}}e(g_2',vk_0)^{-r_\beta}e(h_0,h)^{r_{\zeta'}}\cdot e(h_1,h)^{-r_{u_j}}$

$R_{\alpha\eta'}\leftarrow\psi_1'^{r_{\eta'}}f_1^{-r_{\alpha\eta'}},R_{\beta\eta'}\leftarrow\psi_2'^{r_{\eta'}}f_2^{r_{\beta\eta'}}$ (8)

然后使用上述计算结果，用哈希函数 H 计算：$c\leftarrow H(M,\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'})$，进而计算以下值：

$s_\alpha\leftarrow r_\alpha+c\alpha,s_\beta\leftarrow r_\beta+c\beta,s_\eta\leftarrow r_\eta+c\eta$

$s_\zeta\leftarrow r_\zeta+c\zeta,s_{\eta'}\leftarrow r_{\eta'}+c\eta',s_{\zeta'}\leftarrow r_{\zeta'}+c\zeta'$

$s_{\alpha\eta}\leftarrow r_{\alpha\eta}+c\alpha\eta,s_{\alpha\eta'}\leftarrow r_{\alpha\eta'}+c\alpha\eta'$

$s_{\beta\eta}\leftarrow r_{\beta\eta}+c\beta\eta,s_{\beta\eta'}\leftarrow r_{\beta\eta'}+c\beta\eta'$

$s_{u_j}\leftarrow r_{u_j}+cu_j,s_x\leftarrow r_x+cx$ (9)

证据 π 为 $(c,s_\alpha,s_\beta,s_\eta,s_\zeta,s_{\eta'},s_{\zeta'},s_{\alpha\eta},s_{\alpha\eta'},s_{\beta\eta},s_{\beta\eta'},s_{u_j},s_x)$，OBU 签名 $\sigma=(\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,\pi)$，广播 (M,σ)。

(5)验证阶段

在该阶段，OBU 运行验证算法来检验收到的消息 (M,σ) 的有效性，计算如下值：

$R_\alpha'\leftarrow f_1^{s_\alpha}\psi^{-c},R_\beta'\leftarrow f_2^{s_\alpha}\psi_2^{-c},R_{\alpha+\beta}'\leftarrow f_3^{s_\alpha+s_\beta}\psi_3^{-c}$

$R_A'\leftarrow e(\psi_4,h)^{s_\eta}e(g_1,h)^{-s_{\alpha\eta}}e(g_1,vk_0)^{-s_\alpha}\cdot e(g_2,h)^{-s_{\beta\eta}}e(g_2,vk_0)^{-s_\beta}e(h_0,h)^{-s_\zeta}e(h_1,h)^{-s_{u_j}}\cdot e(h_2,h)^{-s_x}(e(g,h)/e(\psi_4,vk_0))^{-c}$

$R_{\alpha\eta}'\leftarrow\psi_1^{s_\eta}f_1^{-s_{\alpha\eta}},R_{\beta\eta}'\leftarrow\psi_2^{s_\eta}f_1^{-s_{\beta\eta}}$

$R_B'\leftarrow e(\psi_5,h)^{s_{\eta'}}e(g_1',h)^{-s_{\eta'}}e(g_1',vk_0)^{-s_\alpha}\cdot e(g_2',h)^{-s_{\beta\eta'}}e(g_2',vk_0)^{-s_\beta}e(h_0,h)^{-s_\zeta}e(h_1,h)^{-s_{u_j}}\cdot(e(g,h)e(h_2,h)^t/e(\psi_5,vk_1))^{-c}$

$R_{\alpha\eta}'\leftarrow\psi_1^{s_{\eta'}}f_1^{-s_{\alpha\eta'}},R_{\beta\eta}'\leftarrow\psi_2^{s_{\eta'}}f_2^{-s_{\beta\eta'}}$ (10)

如果 $c=H(M,\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'})$，则验证通过，否则验证不通过。验证通过后，OBU 接受该消息。

(6)追踪阶段

在该阶段，对于要追踪的消息 (M,σ)，TM 计算 $A'=\psi_4/\psi_1^{\xi_1}\psi_2^{\xi_2}\psi_3^{\xi_3}$，存在一个 OBU_i，有 $transcript_i=(X,A')$，验证 X 对应的 OBU_i。

(7)撤销阶段

TM 使用完全子树方法更新代表所有未撤销用户的节点集合 $\{u_0,u_1,\cdots,u_{num}\}$。对于每个 $i=0,1,\cdots,num$，随机选取 $\eta_{i'},\zeta_{i'}\overset{R}{\leftarrow}Z_p$，计算：

$$B_{i,t}=(gh_0^{\zeta'}h_1^{u_i}h_2^t)^{1/(\gamma_1+\eta_{i'})} \tag{11}$$

令 $\{\Theta=(B_{i,t},\eta_{i'},\zeta_i)\}_{i=0}^{num}$，更新 t 时刻的撤销列表为 $RL_t=(t,R_t,\Theta)$。

5 安全性分析

定理 1 所提出的方案基于 DLIN 难题假设在随机预言模型中具有匿名性。

证明：匿名性意味着没有开启者的私钥就不能识别出签名者，因此攻击者对匿名性 $(\psi_1,\psi_2,\psi_3,\psi_4,\psi_5)$ 的攻击等于对密文的攻击，即该方案的匿名性为降低到线性加密方案的 CCA 安全性。

具体证明如下：首先，我们定义一系列 Game 序列，用 S_i 表示在 $Game_i$ 中，敌手成功猜出了挑战者挑选的 bit。

Game 0 最初的游戏与匿名定义中定义的游戏相同。首先，假定挑战者响应哈希咨询。为此，挑战者维护一个哈希列表，其中包含形式为 $(M,\psi_1,\psi_2,\psi_3,\psi_4,\psi_5,R_\alpha,R_\beta,R_{\alpha+\beta},R_A,R_B,R_{\alpha\eta},R_{\beta\eta},R_{\alpha\eta'},R_{\beta\eta'},c)$ 的元组，用函数 H 表示。

Game 1 在这个游戏中，使用一个模拟证明代替挑战签名的零知识证明。当敌手通过输入 (i_0,i_1,M) 询问挑战签名 $(\psi_1^*,\psi_5^*,c^*,R_\alpha^*,\cdots,R_{\beta\eta'}^*)$ 时，挑战者做如下计算：挑战者随机选取比特 $b\in\{0,1\}$，使用签名密钥 $(cert_{ib},sec_{ib})$ 计算 (ψ_1^*,ψ_5^*)，随机生成：

$c,s_\alpha,s_\beta,s_\eta,s_\zeta,s_{\eta'},s_{\zeta'},s_{\alpha\eta},s_{\alpha\eta'},s_{\beta\eta},s_{\beta\eta'}\leftarrow Z_p$

计算：

$R_\alpha'\leftarrow f_1^{s_\alpha}\psi_1^{-c},R_\beta'\leftarrow f_2^{s_\alpha}\psi_2^{-c},R_{\alpha+\beta}'\leftarrow f_3^{s_\alpha+s_\beta}\psi_3^{-c}$

$R_A'\leftarrow e(\psi_4,h)^{s_\eta}e(g_1,h)^{-s_{\alpha\eta}}e(g_1,vk_0)^{-s_\alpha}\cdot e(g_2,h)^{-s_{\beta\eta}}e(g_2,vk_0)^{-s_\beta}e(h_0,h)^{-s_\zeta}e(h_1,h)^{-s_{u_j}}\cdot(h_2,h)^{-s_x}(e(g,h)/e(\psi_4,vk_0))^{-c}$

$R_{\alpha\eta'}\leftarrow\psi_1^{s_\eta}f_1^{-s_{\alpha\eta}}$

$R_B'\leftarrow e(\psi_5,h)^{s_{\eta'}}e(g_1',h)^{s_{\eta'}}e(g_1',vk_0)^{-s_\alpha}\cdot e(g_2',h)^{s_{\beta\eta'}}e(g_2',vk_0)^{-s_\beta}e(h_0,h)^{-s_{\zeta'}}e(h_1,h)^{-s_{u_j}}\cdot(e(g,h)e(h_2,h)^t/e(\psi_5,vk_1))^{-c}$

$R_{\alpha\eta'}'\leftarrow\psi_1^{s_{\eta'}}f_1^{s_{\alpha\eta'}},R_{\beta\eta}'\leftarrow\psi_2^{s_{\eta'}}f_2^{-s_{\beta\eta'}}$ (12)

挑战者将元组 $(M,\psi_1^*,\cdots,\psi_5^*,c^*,R_\alpha^*,\cdots,R_{\beta\eta'}^*)$ 添加到

H 的哈希列表中。如果此时挑战者的哈希函数 H 的列表已经包含了一些形式为 $(M,\psi_1^*,\cdots,\psi_5^*,c^*,R_\alpha^*,\cdots,R_{\beta\eta'}^*)$ 的元组,那么挑战者输出 $\perp$ 并中止;否则挑战者将发送 $(\psi_1^*,\cdots,\psi_5^*,c^*,s_\alpha^*,\cdots,s_{\beta\eta'}^*)$ 给对手作为挑战签名。这个改变对敌手获胜概率的影响是可忽略的。

Game 2　在这个游戏中,我们将挑战中的线性加密修改为一般形式。具体来说,为了计算挑战 $(\psi_1^*,\cdots,\psi_5^*,c^*,s_\alpha^*,\cdots,s_{\beta\eta'}^*)$,挑战者选择随机整数 $\alpha,\beta,\tau\in z_p$,其中 $\tau\neq\alpha+\beta$,计算:

$$\psi_1^*=f_1^\alpha,\psi_2^*=f_2^\beta,\psi_3^*=f_3^\tau,\psi_4^*=(\psi_1^*)^{\varepsilon_1}(\psi_2^*)^{\varepsilon_2}(\psi_3^*)^{\varepsilon_3}A_{ib},$$
$$\psi_5^*=(\psi_1^*)^{\varepsilon_1'}(\psi_2^*)^{\varepsilon_2'}(\psi_3^*)^{\varepsilon_3'}B_{ib} \tag{13}$$

其中,f_1,f_2,f_3 是群公钥 gpk 的一部分,b 是在 $\{0,1\}$ 中随机选取的,A_{ib} 是成员 i_b 的群成员证书的一部分,B_{ib} 是在撤销列表 RL_t^* 中与成员 i_b 对应的签名。挑战者使用开启密钥 sk_{OA} (即 $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3')$)来计算挑战值。其余的挑战值计算与 Game 1 中一样。基于 DLIN 假设,这个改变对敌手获胜概率的影响是可忽略的。

Game 3　在这个游戏中,如果签名包含的线性加密分量 (ψ_1,ψ_2,ψ_3) 不构成线性元组,则开启预言机会拒绝敌手进行访问。即,当 $\psi_1=f_1^a,\psi_2=f_2^\beta,\psi_1=f_3^v$,且 $\alpha+b\neq v$ 时,挑战者拒绝查询访问。因为敌手可以伪造出可以通过验证的有效证据的这种查询只有微不足道的概率,这个改变对敌手获胜概率的影响是可忽略的。

下面证明不可区分性,即 $(\psi_1^*)^{\varepsilon_1}(\psi_2^*)^{\varepsilon_2}(\psi_3^*)^{\varepsilon_3}$ 和 $(\psi_1^*)^{\varepsilon_1'}(\psi_2^*)^{\varepsilon_2'}(\psi_3^*)^{\varepsilon_3'}$ 的值是随机均匀分布的,且这些值不会增加敌手知道的信息。因为 $(\psi_1^*)^{\varepsilon_1}(\psi_2^*)^{\varepsilon_2}(\psi_3^*)^{\varepsilon_3}=(f_1^\alpha)^{\varepsilon_1}(f_2^\beta)^{\varepsilon_2}(f_3^{\alpha+\beta})^{\varepsilon_3}=(f_1^{\varepsilon_1}f_3^{\varepsilon_3})^\alpha(f_2^{\varepsilon_2}f_3^{\varepsilon_3})^\beta=g_1^\alpha g_2^\beta$,同样计算出 $(\psi_1^*)^{\varepsilon_1'}(\psi_2^*)^{\varepsilon_2'}(\psi_3^*)^{\varepsilon_3'}=g_1'^\alpha g_2'^\beta$。而 g_1,g_2,g_1',g_2' 均为已知的信息。它们的具体关系如下:

$$\begin{pmatrix}\\ \log_g g_1\\ \\ \log_g g_2\\ \\ \log_g(\psi_1^*)^{\varepsilon_1}(\psi_2^*)^{\varepsilon_1}(\psi_3^*)^{\varepsilon_3}\end{pmatrix}=\begin{pmatrix}\log_g f_1 & 0 & \log_g f_3\\ 0 & \log_g f_2 & \log_g f_3\\ \alpha\cdot\log_g f_1 & \beta\cdot\log_g f_2 & \tau\cdot\log_g f_3\end{pmatrix}\begin{pmatrix}\varepsilon_1\\ \varepsilon_2\\ \varepsilon_3\end{pmatrix}$$

因此,$(\psi_1^*)^{\varepsilon_1}(\psi_2^*)^{\varepsilon_2}(\psi_3^*)^{\varepsilon_3}$ 的值随机均匀分布的,也就是说挑战签名值是与 A_{ib} 无关的,即敌手猜测出 $b\in\{0,1\}$ 值的概率为 1/2。

定理 2　所提出的方案基于 DL 难题假设在随机预言模型中具有不可诬陷性。

证明:成员证书中 X 的离散对数 x 是只有签名者知道的秘密信息,签名者在签名中给出了 x 的 NIZK 证明。因此,没有 x 就不能伪造签名。在针对 DL 问题的攻击者的模拟中,x 的提取器可以利用敌手最终伪造的群签名来构造(基于分叉引理[20])。因此,方案的不可诬陷性被规约为 DL 问题。

敌手 A 构建一个签名 (M^*,σ^*),其开启结果为某个诚实的群成员 i。模拟器 B 生成 $f_1,f_2,f_3,h_0,h_1,h_2\leftarrow G_1,h\leftarrow G_2,\gamma_0,\gamma_1,\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3'\overset{R}{\leftarrow}Z_p$,计算 $(sk_0,vk_0)=(\gamma_0,h^{\gamma_0})$,$(sk_1,vk_1)=(\gamma_1,h^{\gamma_1})$,$g_1=f_1^{\varepsilon_1}f_3^{\varepsilon_3}$,$g_2=f_2^{\varepsilon_2}f_3^{\varepsilon_3}$,$g_1'=f_1^{\varepsilon_1'}f_3^{\varepsilon_3'}$,$g_2'=f_2^{\varepsilon_2'}f_3^{\varepsilon_3'}$。记 $sk_{OA}=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3')$;$sk_{GM}=(sk_0,sk_1)=(\gamma_0,\gamma_1)$;$gpk=(p,G_1,G_2,G_T,e,g,h,f_1,f_2,f_3,h_0,h_1,h_2,g_1,g_2,g_1',g_2',vk_0,vk_1,H)$。敌手 A 和模拟器 B 做如下的交互:包括 $O_{gpk},O_{GM},O_{OA},O_{revoke},O_{sig}$ 咨询。然后,敌手 A 输出一个对消息 M^* 的签名值 $\sigma^*=(\psi_1^*,\cdots,\psi_5^*,c^*,s_\alpha^*,\cdots,s_{\beta\eta'}^*)$,其开启结果为某个未对消息 M^* 做出签名的用户 i^*。B 计算 $A_{i^*}=\psi_4/\psi_1^{\varepsilon_1}\psi_2^{\varepsilon_2}\psi_3^{\varepsilon_3}$,输出 $X=g^x$,否则输出 $\perp$ 并中止。将敌手 A 解决该问题的概率记为 $Adv_A^{frame}(\lambda)$,模拟器 B 解决 DL 问题的概率记为 $Adv_B^{DL}(\lambda)$,根据分叉定理,有:

$$Adv_A^{frame}(\lambda)\cdot\left(\frac{Adv_A^{frame}(\lambda)-\frac{1}{p}}{q_{sig}}-\frac{1}{p}\right)>\frac{Adv_A^{frame}(\lambda)^2}{q_{sig}}-\frac{1+\frac{1}{q_{sig}}}{p}$$

即:

$$\frac{Adv_A^{frame}(\lambda)^2}{q_{sig}}-\frac{1+\frac{1}{q_{sig}}}{p}\leqslant q_{join}\cdot Adv_B^{DL}(\lambda)$$

因此,若 $Adv_B^{DL}(\lambda)$ 是可忽略的,则 $Adv_A^{frame}(\lambda)$ 也是可忽略的。

定理 3　所提出的方案基于 q-SDH 难题假设在随机预言模型中具有不可伪造性。

证明:对不可伪造性的攻击也就是伪造一个 BBS +签名作为成员证书。因此,可以将不可伪造性攻击的安全性简化为 BBS+签名方案的不可伪造性,文献[18]证明了这一点。考虑两种伪造:(1)伪造属于该群的证书;(2)伪造未撤销用户的证书。基于破解 BBS +签名方案的不可伪造性,可以构造一个破解 q-SDH 假设的算法,因此该定理成立。

敌手 A 构建一个签名 (M^*,σ^*),其开启结果不是某个诚实的群成员 i。模拟器 B 生成 $f_1,f_2,f_3,h_0,h_1,h_2\leftarrow G_1,h\leftarrow G_2,\gamma_0,\gamma_1,\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3'\overset{R}{\leftarrow}Z_p$,两种伪造情况分别为:

(1)令 $vk_0=w$,计算 $(sk_1,vk_1)=(\gamma_1,h^{\gamma_1})$;

(2)令 $vk_1=w$,计算 $(sk_0,vk_0)=(\gamma_0,h^{\gamma_0})$。

$g_1=f_1^{\varepsilon_1}f_3^{\varepsilon_3}$,$g_2=f_2^{\varepsilon_2}f_3^{\varepsilon_3}$,$g_1'=f_1^{\varepsilon_1'}f_3^{\varepsilon_3'}$,$g_2'=f_2^{\varepsilon_2'}f_3^{\varepsilon_3'}$。记 $sk_{OA}=(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_1',\varepsilon_2',\varepsilon_3')$;$sk_{GM}=(sk_0,sk_1)=(\gamma_0,\gamma_1)$;$gpk=(p,G_1,G_2,G_T,e,g,h,f_1,f_2,f_3,h_0,h_1,h_2,g_1,g_2,g_1',g_2',vk_0,vk_1,H)$。对敌手 A 和模拟器 B 做如下交互:包括 $O_{gpk},O_{join},O_{revoke}$ 咨询。然后敌手 A 输出一个对消息 M^* 的一个签名值 $\sigma^*=(\psi_1^*,\cdots,\psi_5^*,c^*,s_\alpha^*,\cdots,s_{\beta\eta'}^*)$,其开启结果不是某个诚实的群成员 i^*。B 解密 ψ_4^* 获得 A_{i^*}(情况 1),或解密 ψ_5^* 获得 B_{i,t^*}(情况 1),B 输出解密的证书作为伪造签名,分别将伪造(1)和伪造(2)成功伪造签名记为 F_1,F_2。敌手 A 伪造成功的概率记为 $Adv_A^{mis}(\lambda)$,通过上面的交互,如果 A 赢得不可伪造性游戏,那么 B 就可以伪造 BBS+签名。因此,$Adv_A^{mis}(\lambda)\leqslant\Pr[F_1]+\Pr[F_2]$。由于 BBS+签名在 q-SDH 假设下具有不可伪造性,因此概率 $\Pr[F_1]$ 和 $\Pr[F_2]$ 在 q-SDH 假设下是可以忽略的。因此,若 q-SDH 假设成立,则 $Adv_A^{mis}(\lambda)$ 是可忽略的。

此外,所提出的方案具有前向安全性。由式(10)中 $R_B'\leftarrow e(\psi_5,h)^{s_{\gamma'}}e(g_1',h)^{-s_{\eta'}}e(g_1',vk_0)^{-s_\alpha}\cdot e(g_2',h)^{-s_{\beta\eta'}}e(g_2',vk_0)^{-s_\beta}e(h_0,h)^{-s_{\nu'}}e(h_1,h)^{-s_{u_t}}\cdot(e(g,h)e(h_2,h)^t/e(\psi_5,vk_1))^{-c}$ 可以看出,验证阶段根据一个时刻 t 来进行计算,在时刻 t 更新(即有用户被撤销)后,之前的签名验证等式则不会成立,这样即可以保证前向安全性。

6 性能评估

本节在个人电脑中模拟提出的协议。选用 Intel i7 3.07 GHz 的处理器，使用基于椭圆曲线配对的密码库[21] Type A 曲线(安全参数 80bit)来实现所提出的协议。

实验结果如表 2－表 4 所列，其中 T_{exp} 表示一次指数运算，T_{par} 表示一次配对运算。

表 2 TM 的计算开销

TM	初始化	注册	追踪
理论值	$7T_{exp}$	$4T_{exp}$	$3T_{exp}$
实验值/ms	336	289	185

表 3 RSU 的计算开销

RSU	初始化	注册	加入
理论值	$1T_{exp}$	$1T_{exp}+1T_{par}$	$3T_{exp}$
实验值/ms	112	156	195

表 4 OBU 的计算开销

OBU	初始化	注册	加入	签名	验证
理论值	$1T_{exp}$	$1T_{exp}$	$1T_{par}$	$15T_{par}+25T_{exp}$	$20T_{par}+30T_{exp}$
实验值/ms	120	94	137	769	812

另外，本方案所提出的协议中 OBU 无需下载撤销列表即可验证签名的有效性，验证开销不随撤销用户的增加而改变。

在实现方案的安全需求性能方面，本方案有较高的安全性。表 5 给出一些方案在某些主要安全需求性能方面的比较。

表 5 安全性比较

	匿名性	不可抵赖	不可诬陷	不可伪造	可撤销	前向安全
文献[13]方案	√	√	√	√	√	
文献[14]方案	√	√		√	√	
文献[15]方案	√	√		√		
本文方案	√	√	√	√	√	√

此外，文献[13]中撤销用户会更改群公钥，这无疑增加了额外的负担。本方案中撤销用户后公钥和私钥均保持不变。

结束语 本文针对车联网隐私保护过程中匿名认证安全与效率较低的问题，基于椭圆曲线上双线对的性质提出了一种有效的匿名认证协议。该匿名认证协议的特点是集成分散的群模型和完全子树方法来实现，具有高效撤销、不可伪造性、匿名性和 VANET 的可追溯性，还保证了前向安全性，方案的安全性得到明显加强。今后的工作将进一步提高其效率。

参 考 文 献

[1] ZHANG D,CHEN M. Mobility prediction in telecom cloudusing mobile calls[J]. IEEE Wireless Communications,2014,21(1):26-32.

[2] KUMARI S V,PARAMASIVAN B. Defense against Sybil attacks and authentication for anonymous location-based routing in MANET[J]. Wireless Networks,2016,23(2):1-12.

[3] YAO L,LIN C,WU G,et al. An anonymous authentication scheme indata-link layer for VANETs[J]. International Journal of Ad Hoc &Ubiquitous Computing,2016,22(1):1-13.

[4] ZHANG D,ZHANG D,XIONG H,et al. BASA:building mobile adhoc social networks on top of Android[J]. IEEE Network,2014,28(1):4-9.

[5] LIN X,LI X. Achieving efficient cooperative message authenticationin vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology,2013,62(7):3339-3348.

[6] JIANG S,ZHU X,WANG L. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems,2016,17(8):2193-2204.

[7] BLUM J,ESKANDARIAN A. The threat of intelligent collisions[J]. It Professional,2004,6(1):24-29.

[8] ZHANG J,SUN Z,LIU S,et al. On the security of a threshold anonymous authentication protocol for VANETs [C]// Proceedings of Security,Privacy,and Anonymity in Computation,Communication,and Storage. Berlin:Springer,2016:145-155.

[9] HUBAUX J P,CAPKUN S,LUO J. The security and privacy of smart vehicles[J]. IEEE Security & Privacy,2004,2(3):49-55.

[10] RAYA M,HUBAUX J P. Securing vehicular ad hoc networks [J]. Comput Secur Spec Issue Secur Ad Hoc Sens Network,2007,15(1):39-68.

[11] ZHANG C,LU R,LIN X,et al. An efficient identity-based batch verification scheme for vehicular sensor networks[C]// IEEE INFOCOM. 2008:816-824.

[12] 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)：50-57.

[13] LIN X,SUN X,HO P H,et al. GSIS:A Secure and Privacy-Preserving Protocol for Vehicular Communications [J]. IEEE Transactions on Vehicular Technology,2007,56(6):3442-3456.

[14] SHAO J,LIN X,LU R,et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology,2016,65(3):1711-1720.

[15] LIU Y,HE Z,ZHAO S,et al. An efficient anonymous authentication protocol using batch operations for VANETs[J]. Multimedia Tools & Applications,2016,75(24):1-21.

[16] LIBERT B,VERGNAUD D. Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard-Model [C]// Proceedings of 8th International Conference on CANS'09. Springer,2009:498-517.

[17] FURUKAWA J,IMAI H. An Efficient Group Signature Scheme from Bilinear Maps[J]. IEICE Transactions,2006,89(25):1328-1338.

[18] AU M H,SUSILO W,MU Y,et al. Constant-size dynamic k-times anonymous authentication[J]. IEEE Systems Journal,2013,7(2):249-261.

[19] NAOR D, NAOR M, LOTSPIECH J. Revocation and Tracing Schemes for Stateless Receivers[M]// Proceedings of Advances in Cryptology—CRYPTO. Berlin,Springer, 2001:41-62.

[20] POINTCHEVAL D,STERN J. Security Proofs for Signatur chemes [M]// Proceedings of Advances in Cryptology-Eurocrypt. Berlin,Springer,1996:387-398.

[21] LYNN B. The pairing-based cryptography library[OL]. http://crypto. stanford. edu/pbc.

[22] ATENIESE G,CAMENISCH J,JOYE M,et al. A Practicaland Provably Secure Coalition-Resistant Group Signature Scheme [M]// Proceedings of 20th CRYPTO. Berlin: Springer, 2000:255-270.