一种后向撤销隐私安全的车载自组织网络快速匿名消息认证协议

刘雪峰 张玉清* 王 鹤 张光华
(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

摘 要：该文提出适用于车载自组织网络的快速匿名消息认证协议。通过使用基于身份的签密技术，车辆行驶至某区域后，与该区域中心相互认证，获取其所维护的周期性群签名系统密钥材料。之后，该车辆能够使用获取的密钥材料对向网络中广播的携带有群签名的消息，实现消息的匿名认证。网络中的车辆收到其它车辆广播消息之后，仅需验证群签名的合法性，避免验证消息的签发者是否是撤销用户。此外，所采用的群签名算法支持批验证运算，能够快速处理短期内收到的多个消息。除了避免撤销验证特性之外，与已有的文献相比，文中的方案能够完善地保护撤销用户的后向隐私安全性。

关键词：密码学；车辆网络；认证；匿名性；后向撤销隐私安全
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1009-5896(2014)01-0094-07
DOI: 10.3724/SP.J.1146.2013.00342

An Efficient Anonymity Message Authentication with Backward Secure Revocation for Vehicular Ad Hoc Networks

Liu Xue-feng Zhang Yu-qing Wang He Zhang Guang-hua
(*National Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: This paper presents an efficient anonymous message authentication scheme for vehicular ad hoc networks. By using identity-based sign-encryption technique, a vehicular user can first authenticate with a region center to obtain a group signature key material, where the group is managed by the region center. Then, the user can employ the key material to sign a message and broadcast it into the network. Other vehicular users can directly check the signature without revocation verification. In addition, the used group signature supports batch verification, which significantly reduces the verification overhead. Compared with the existing schemes, the proposed scheme can achieve backward secure revocation.

Key words: Cryptography; Vehicular networks; Message authentication; Privacy-preserving; Backward secure revocation

1 引言

车载自组织网络能够提供有效的道路交通信息，为车辆驾驶员提供更为安全的驾驶环境以及便捷的多种网络服务[1,2]。典型的车辆自组织网络是由路边单元与车辆共同构成的，其中路边单元通过有线相互连接方式构成骨干网。车载自组织网络主要包括两种通信方式[3]：(1)车辆与路边单元的通信；(2)车辆与车辆之间的通信。网络中的车辆通过其装载的通信设备，向网络中发出其感知的信息(如位置、速度、紧急事宜等)，为道路上的驾驶员提供及时、准确的路况信息，以提高整个道路行驶的安全性。然而，在车辆自组织网络部署之前，急需解决以下安全问题。

(1)消息认证性：车辆在收到网络中消息时，要能够验证该消息的发送者是否是合法用户，以避免攻击者向网络中注入虚假、恶意的信息；(2)不可否认性：车辆在向网络中广播消息之后，不能对该消息否认；(3)车辆匿名性：侦听者以及网络中的车辆不能通过检测到的广播消息，来识别发送者其真实身份，否则车辆网络对用户便失去吸引力[4,5]；(4)可追踪性：在出现有争议或纠纷广播信息时，网络的管理者能够有效地识别出消息的发出者真实身份；(5)撤销车辆后向隐私安全性：车辆被撤销之后，全局侦听者不能根据其侦听的全网历史信息确定出该撤销用户的签发消息，进而保护该撤销用户的历史移动轨迹隐私；(6)高效撤销验证性：在验证收到的信息时，车辆能够确定出该消息的发送者是否是已撤销用户。在实际应用中，车辆网络的规模通常是比较大的，如截止2011年2月，我国现有机动车辆已达2.11亿辆[6]。如何迅速验证消息签名者是否是已撤销用户，依然是个棘手的问题。

根据采用的基础密码特性，现有解决车辆自组

2013-03-15收到，2013-07-27改回
国家自然科学基金(61272481)资助课题
*通信作者：张玉清 zhangyq@ucas.ac.cn

织网络的消息匿名认证问题的文献[7–15]可分为两类：多个匿名证书(或身份)类[7–12]与特殊签名类[13–15]。文献[7]提出每个车辆配置有多个公私钥对，随机使用其中一对公私钥对消息签名。然而，文献[8]指出，在实际应用中每个车辆需要部署至少2500 个公私钥对才能实现完善的身份隐私。文献[9]提出分布式的证书管理办法，来降低整个系统管理的复杂度。上述方案存在的主要问题是，系统的撤销列表随着撤销成员数目的增多而迅速增加，并且撤销列表需要以无线传输的方式在车辆网络中传输，以使得所有车辆获取最新的撤销列表。举个例子来说，假设有 1 万个用户撤销，则需要撤销 2.5 千万个证书。假设用户的身份是 4 byte，则撤销列表中包含的撤销身份信息是 100 MB。一方面，使得所有车辆均获取最新的撤销列表会严重地增加网络的通信负荷，降低网络的性能。另一方面，查询消息的签发者是否属于 2.5 千万个撤销群体依然会引入较大的延迟。文献[10]提出采用路边单元与车辆相互认证而后为车辆签发新的匿名证书来降低撤销验证开销。为了减少撤销列表的大小，文献[11]采用双向哈希链技术，来构造用户的多个不同身份。在撤销用户时，仅需公布两条链的哈希种子来降低撤销列表规模。文献[7–11]存在撤销车辆后向隐私安全隐患，即，用户一旦被撤销，其所有的证书以及身分将被公开。那么全网侦听者可通过监听到的历史信息，来确定出撤销用户所发出的消息，进而恢复出该撤销车辆的历史移动轨迹。

为了实现快速撤销验证，文献[12]提出合法车辆通过与路边单元认证，获取其所在区域的共享密钥，而后利用带有密钥的哈希认证码来实现消息认证。然而，系统中的任意一车辆泄露了该共享密钥，则整个系统不再安全。文献[13]提出采用群签名机制实现匿名消息认证，即车辆向网络发出携带群签名的消息来隐藏自己的身份。文献[14]采用 K 次匿名认证技术来保护车辆的隐私。文献[15]采用环签名机制来保护签发者的隐私。文献[13–15]存在的问题是撤销验证计算开销随着撤销车辆数目增加而线性增加，并且撤销用户后向隐私缺乏有效保护。

针对上述问题，本文提出一种适用于车载自组织网络的快速匿名消息认证方案。文中的方案仅需区域中心与车辆进行一次有效以及撤销性验证。之后，网络中的车辆在收到其它车辆发出的广播信息时，仅验证消息附带的签名是否正确，无需再验证签名者是否已被撤销。另外，文中的方案能够保护撤销用户的后向隐私安全，并且支持车辆对短期内收到的多个消息进行批验证操作以提高验证效率。

2　协议设计

2.1 系统模型

图 1 所示为常用的车载网络通信模型，主要有授权中心、区域中心、路边单元以及车辆 4 个部分构成。下面分别阐述它们的主要功能。

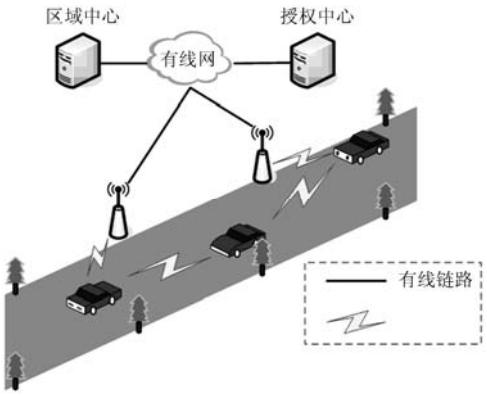

图 1 系统模型

(1)授权中心(trust authority)：是由完全可信的第三方担当该角色，如政府交通管理部门。其主要任务是给区域中心与车辆分发签密密钥[16]。

(2)区域中心(region center)：也被认为是完全可信的。区域中心维护群签名密码系统，其该系统密钥材料周期性地更新，如每天更新一次。主要职责是，与驶入其区域的车辆相互认证，并对合法且未撤销的车辆颁发群签名密钥材料[17]。

(3)路边单元 (roadside unit)：是车辆网络通信的主要基础实施，通过有线网络与其它路边单元以及区域中心实现网络互连。主要功能是，作为骨干网参与网络信息通信。

(4)车辆(vehicular)：主要向网络中广播周边的路况信息，为附近用户提供更好的驾驶环境以及对异常事情(如交通事故)做提早预判。

2.2 方案总体设计

车载网络中的消息快速认证，关键在于用户撤销验证的有效性。具体来说，网络中的车辆在收到其他用户发出的信息之后，首先验证消息的真伪性，即通过签名算法来验证消息以及其携带签名的正确性。之后，用户在排除签名者是已撤销用户后才能认定消息的合法性。

为了克服车辆每收到一个消息均进行撤销验证，本文提出的方案只需路边单元验证一次车辆的撤销性，网络中的车辆在收到其它用户广播信息之后，仅验证消息的携带签名是否正确，无需再验证签名者是否已撤销。方案的主要思想可以概括为以下 3 点：(1)区域中心维护群签名密码系统，该密码

系统周期性地更新，如每天更新一次；(2)车辆进入某区域之后，与区域管理中心相互认证。在验证车辆的有效以及未被撤销之后，该中心为用户分发群签名私钥；(3)撤销用户无法通过与路边单元的认证，因而无法获取群签名密钥。车辆在收到其他用户的广播消息之后，直接验证群签名的有效性，而无需再对签名者进行撤销验证。

2.3 安全模型

如上所述，本文提出的方案 P 分为两部分(1) P_{auth} 为匿名认证协议以获得群密钥材料；(2) P_{gs} 为群签名实现消息认证以及匿名性保护。接着，将给出两部分的形式化安全模型的细致描述。

2.3.1 匿名认证安全模型 在所设计的车辆与区域中心认证协议 P_{auth} 中，C 表示区域中心，V 表示一个车辆，C^i 表示区域中心执行的实例 i，V^j 表示车辆执行的实例 j。从本质上来看，P 是 C^i 与 V^j 之间执行的交互式认证协议，保护 V^j 的匿名性并且协商出 C^i 与 V^j 之间的会话密钥。在协议 P 的执行过程中，攻击者可以询问以下几种预言机，来模拟现实中的攻击能力。

(1) $\text{Send}(C^i/V^j,m)$：发送消息 m 给实例 C^i (或 V^j)，而后实例根据协议的执行返回信息。该预言机用来模拟实际中的主动攻击，例如插入伪造的消息、消息篡改以及终止现有的消息流等。另外，攻击者也可以监听全网通信；(2) $\text{Reveal}(C^i/V^j)$：预言机回馈 C^i (或 V^j)的会话密钥，用来模拟密钥滥用攻击；(3) $\text{RevealID}(V^j)$：返回实例 V^j 的真实身份，用来模拟身份滥用攻击；(4) $\text{Test}(C^i/V^j)$：该询问仅能执行一次，用来定义生成会话密钥的语义安全性。根据掷硬币的结果 b，若 $b=1$，返回给攻击者 C^i 与 V^j 协商出的真实会话密钥；若 $b=0$，返回给攻击者与会话密钥等长的随机数；(5) $\text{TestAnon}(V^j, \text{ID}_0, \text{ID}_1)$：该询问仅能执行一次，用来定义用户的匿名性。根据掷硬币的结果 b，若 $b=1$，返回给攻击者 V^j 的真实身份 ID_1；若 $b=0$，返回给攻击者与真实身份等长的伪身份 ID_0。

定义 1 AKE 安全性 在这个实验中，攻击者可以访问 $\text{Send}(C^i/V^j,m)$，$\text{Reveal}(C^i/V^j)$，$\text{Test}(C^i/V^j)$。最后，攻击者输出 b' 来判断 $\text{Test}(C^i/V^j)$ 给出的挑战是真实密钥还是一个随机数。$\text{Succ}(A)$ 表示攻击者赢取这个游戏，也就是说，$b'=b$，其中 b 是 $\text{Test}(C^i/V^j)$ 选择的。那么，攻击者 A 赢取协议 P 的语义安全性优势定义为：$\text{ADV}_P^{\text{ake}}(A)=2\Pr[\text{Succ}(A)]-1$。若对于任意攻击者 A 在多项式时间 t 内所赢得游戏的优势 $\text{ADV}_P^{\text{ake}}(A)$ 是可忽略的，则称协议 P 是语义安全性的。

定义 2 用户匿名性 攻击者可以询问 $\text{Send}(C^i/V^j,m)$，$\text{Reveal}(C^i/V^j)$，$\text{RevealID}(V^j)$ 以及 $\text{TestAnon}(V^j, \text{ID}_0, \text{ID}_1)$。最后，攻击者输出 b' 来判断 $\text{TestAnon}(V^j, \text{ID}_0, \text{ID}_1)$ 给出的挑战是真实密钥还是一个随机数。$\text{Succ}^{\text{anon}}(A)$ 表示攻击者赢取这个游戏，也就是说，$b'=b$，其中 b 是 $\text{TestAnon}(V^j, \text{ID}_0, \text{ID}_1)$ 选择的。则攻击者 A 赢取协议 P_{auth} 的用户匿名性优势定义为：$\text{ADV}_P^{\text{anon}}(A)=2\Pr[\text{Succ}^{\text{anon}}(A)]-1$。若对于任意攻击者 A 在多项式时间 t 内所赢得游戏的优势 $\text{ADV}_P^{\text{anon}}(A)$ 是可忽略的，则称协议 P 是具有匿名保护性。

2.3.2 群签名安全模型 在协议所使用的群签名中，将系统公开参数给具有适应性选择消息攻击能力的敌手 A，另外敌手 A 能够访问注册用户(即执行完认证协议获取群密钥材料的注册车辆 $\{V_1, V_2, \cdots\}$)的密钥生成预言机 O_k 以及签名预言机 O_s。

定义 3 完全匿名性 攻击者首先访问数次密钥生成预言机 O_k 以及签名预言机 O_s，而后输出 (V_i, V_j, m)。根据掷硬币的结果 b，若 $b=1$，返回给攻击者与 V_i 的密钥计算出的关于消息 m 的签名；若 $b=0$，则返回给攻击者与 V_j 的密钥计算出的关于消息 m 的签名。而后攻击者输出猜测 b'，$\text{Succ}^{\text{gs-anon}}(A)$ 表示攻击者赢取这个游戏(即，$b'=b$)，则攻击者 A 赢取协议 P_{gs} 的完全匿名性优势定义为：$\text{ADV}_P^{\text{gs-anon}}(A)=\Pr[\text{Succ}^{\text{gs-anon}}(A)]$ 若对于任意攻击者 A 在多项式时间 t 内所赢得游戏的优势 $\text{ADV}_P^{\text{gs-anon}}(A)$ 是可忽略的，则称协议 P_{gs} 是具有完全匿名保护性。

定义 4 自适应消息攻击下不可伪造性(ef-cma) 攻击者首先访问数次密钥生成预言机 O_k 以及签名预言机 O_s，而后输出一个有效的 V_i 关于消息 m 的签名，限制条件是：攻击者未访问过预言机 O_k 关于 V_i 的密钥以及未访问过预言机 O_s 关于 (V_i, m) 的签名。$\text{Succ}^{\text{ef-cma}}(A)$ 表示攻击者伪造一个有效群签名的优势，那么攻击者 A 赢取协议 P_{gs} 不可伪造性的优势定义为：$\text{ADV}_P^{\text{ef-cma}}(A)=\Pr[\text{Succ}^{\text{ef-cma}}(A)]$。若对于任意攻击者 A 在多项式时间 t 内所赢得游戏的优势 $\text{ADV}_P^{\text{ef-cma}}(A)$ 是可忽略的，则称协议 P_{gs} 是自适应消息攻击下不可伪造的。

3 方案描述

3.1 初始化

在车载网络部署之前，授权中心完成整个协议的初始化，包括生成系统参数、为区域中心以及车辆分配密钥，具体包括以下 3 点。

3.1.1 系统参数生成以及注册 授权中心维护签密

密码系统[16]，首先生成双线性对系统 $(e:G_1\times G_2\to G_T,g_1,g_2,g,q,\varphi())$，$G_1,G_2,G_T$ 是阶为 q 的乘法循环群，g_1,g_2 分别为 G_1,G_2 的生成元且满足 $\varphi(g_2)=g_1$，$g=e(g_1,g_2)$。授权中心选取随机数 $s\in Z_q^*$ 作为系统的主密钥，则对应的系统公钥为 $\mathrm{pw}=g_2^s$。此外，选取 3 个哈希函数 $H_1:\{0,1\}^*\to Z_q^*$，$H_2:\{0,1\}^*\times G_T\to Z_q^*$ 与 $H_3:G_T\to\{0,1\}^n$，以及消息认证码 $\mathrm{HMAC}_k()$，授权中心公开双线性对参数、哈希函数以及消息认证码。

设区域中心所在区域位置名称为 L_i，则授权中心为该区域中心分配的私钥是：$\mathrm{sk}_{L_i}=g_2^{\frac{1}{H_1(L_i)+s}}\in G_2$。设车辆的身份为 ID_i，在向授权中心注册之后，车辆获取私钥为：$\mathrm{sk}_{\mathrm{ID}_i}=g_2^{\frac{1}{H_1(\mathrm{ID}_i)+s}}\in G_2$。

3.1.2 区域群签名系统初始化　群签名密钥系统[17,18]的初始化是由区域中心执行，具体分为以下两个步骤：

(1)选择随机数 $h\in G_1$ 和 $r_1,r_2\in Z_q^*$，设置 u,v 满足 $u^{r_1}=v^{r_2}=h$；

(2)选择随机数 $x\in Z_q^*$ 并计算 $w=g_2^x$。

该区域的群签密系统公开参数为 $\{g_1,g_2,h,u,v,w,H_1()\}$，主密钥为 $\mathrm{gsk}=(x,r_1,r_2)$。

3.2 车辆与区域中心认证

任意一路边单元周期性地广播包含其所属区域信息 L_i 信标帧，当车辆行驶至路边单元通信范围之内，通过路边单元的路由转发，实现与该区域中心的相互认证并获取该区域的群签名密钥材料，具体过程如下：

$$\left.\begin{aligned}&V_i\to L_i:L_i,c,S,T\\&L_i\to V_i:\mathrm{PID}_i,L_i,g_1^b,t_L,\{\mathrm{gsk}_{\mathrm{ID}_i}\}_{g_1^{ab}},\\&\qquad\mathrm{HMAC}_{g_1^{ab}}(L_i,g_1^b,\{\mathrm{gsk}_{\mathrm{ID}_i}\}_{g_1^{ab}},t_L)\end{aligned}\right\}\quad(1)$$

步骤 1　车辆选取一个 l 位的随机数 k 作为会话密钥，采用路边单元的公钥 L_i 以及自己的私钥 $\mathrm{sk}_{\mathrm{ID}_i}$ 对自己的身份、随机数以及时戳 (ID_i,k,t_V) 做如下的签密运算：

(1)选取随机数 $t,a\in Z_q^*$，计算 $r=g^t$，g_1^a 以及 $c=(\mathrm{ID}_i\,||\,\mathrm{PID}_i\,||\,g_1^a\,||\,t_V)\oplus H_3(r)\in\{0,1\}^n$。其中 $||$ 是连接符，将两个字符串连接起来；PID_i 是用户自己选择的临时身份；

(2)计算 $h=H_2(g_1^a\,||\,\mathrm{ID}_i\,||\,k\,||\,t_V,r)\in Z_q^*$，$S=\varphi(S_{\mathrm{ID}_i})^{(t+h)}$ 以及 $T=(g_1^{H_1(L_i)}\varphi(\mathrm{pw}))^t$。

步骤 2　路边单元在收到消息 L_i,c,S,T 之后将消息转发给区域中心。而后区域中心执行以下几个步骤：

(1)使用其私钥 sk_{L_i} 计算 $r'=e(T,\mathrm{sk}_{L_i})=r$，该等式成立的推导过程如等式(2)所示。

$$\begin{aligned}r'=e(T,\mathrm{sk}_{L_i})&=e\left((g_1^{H_1(L_i)}\varphi(\mathrm{pw}))^t,g_2^{\frac{1}{H_1(L_i)+s}}\right)\\&=e\left((g_1^{H_1(L_i)}g_1^s)^t,g_2^{\frac{1}{H_1(L_i)+s}}\right)=e(g_1,g_2)^t=r\end{aligned}\quad(2)$$

(2)通过 $c\oplus H_3(r)$ 恢复 $\mathrm{ID}_i\,||\,\mathrm{PID}_i\,||\,k\,||\,t_V$，并验证时戳 t_V 的新鲜性。

(3)计算 $h=H_2(g_1^a\,||\,\mathrm{ID}_i\,||\,k\,||\,t_V,r)\in Z_q^*$，验证 $r'=e(S,g_2^{H_1(\mathrm{ID}_i)}\mathrm{pw})g^{-h}$ 是否成立，若成立则认为消息是合法的，否则终止该协议，上述等式成立的推导过程如等式(3)所示。

$$\begin{aligned}&e(S,g_2^{H_1(\mathrm{ID}_i)}\mathrm{pw})g^{-h}\\&=e\left(\varphi(S_{\mathrm{ID}_i})^{(t+h)},g_2^{H_1(\mathrm{ID}_i)+s}\right)g^{-h}\\&=e\left(g_1^{\frac{t+h}{H_1(\mathrm{ID}_i)+s}},g_2^{H_1(\mathrm{ID}_i)+s}\right)g^{-h}=e(g_1,g_2)^t=r\end{aligned}\quad(3)$$

(4)选择随机数 $b\in Z_q^*$ 计算 g_1^b,g_1^{ab} 以及 $\mathrm{gsk}_{\mathrm{ID}_i}=g_1^{\frac{1}{x+H_1(\mathrm{ID}_i)}}$，采用 g_1^{ab} 作为会话密钥加密 $\mathrm{gsk}_{\mathrm{ID}_i}$，并发送消息 $\mathrm{PID}_i,L_i,g_1^b,t_L,\{\mathrm{gsk}_{\mathrm{ID}_i}\}_{abP},\mathrm{HMAC}_{g_1^{ab}}(L_i,g_1^b,\{\mathrm{gsk}_{\mathrm{ID}_i}\}_{g_1^{ab}},t_L)$ 发送给该车辆，t_L 为区域中心当前的时戳。此外，区域中心将 $(\mathrm{gsk}_{\mathrm{ID}_i},\mathrm{ID}_i)$ 添加到用户列表之中，以备后续的纠纷处理。

步骤 3　在收到消息之后，车辆验证时戳 t_L 的新鲜性并且计算 g_1^{ab} 来验证 $\mathrm{HMAC}_k(L_i,g_1^b,\{\mathrm{gsk}_{\mathrm{ID}_i}\}_{g_1^{ab}},t_L)$ 来验证消息的真伪性。而后，解密以恢复出群签名密钥 $\mathrm{gsk}_{\mathrm{ID}_i}$。

3.3 车辆广播消息认证

在广播消息之前，车辆需要对该消息做签名，以证明该消息的有效性。假设车辆待广播的消息为 m，则通过群签名私钥组合成表 1 所示的消息格式之后再向网络之中广播，具体过程如下：

表 1 广播消息格式

消息标示符	消息负载	时戳	群签名
ID_m	m	T_i	$\mathrm{gsig}(m,T_i)$

(1)选择随机数 $\alpha,\beta,r_\alpha,r_\beta,r_x,r_{\gamma_1},r_{\gamma_2}\in Z_q^*$ 并计算 $T_1=u^\alpha,T_2=v^\beta,T_3=\mathrm{gsk}_{\mathrm{ID}_i}\cdot h^{\alpha+\beta}$；

(2)计算 $\gamma_1=\alpha H_1(\mathrm{ID}_i),\gamma_2=\beta H_1(\mathrm{ID}_i)$，$R_1=u^{r_\alpha}$，$R_2=v^{r_\beta},R_3=e(T_3,g_2)^{r_x}e(h,w)^{-r_\alpha-r_\beta}e(h,g_2)^{-r_{\gamma_1}-r_{\gamma_2}},R_4=T_1^{r_x}\cdot u^{-r_{\gamma_1}},R_5=T_2^{r_x}\cdot v^{-r_{\gamma_2}}$；

(3)计算 $\delta=H_1(\mathrm{ID}_m\,||\,m\,||\,T_i,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$；

(4) 计算 $s_\alpha = r_\alpha + \delta\cdot\alpha,\ s_\beta = r_\beta + \delta\cdot\beta,\ s_x = r_x + \delta\cdot H_1(\mathrm{ID}_i), s_{\gamma_1} = r_{\gamma_1} + \delta\cdot\gamma_1,\ s_{\gamma_2} = r_{\gamma_2} + \delta\cdot\gamma_2$；

(5) 构成群签名 $\mathrm{gsig}(m,T_i) = (T_1,T_2,T_3,R_3,\delta,s_\alpha, s_\beta,s_x,s_{\gamma_1},s_{\gamma_2})$。

在收到表 1 所示的消息之后，网络中的其它车辆首先验证时戳 T_i 的新鲜性。而后做以下处理：

(1) 计算 $R_1' = u^{s_\alpha}\cdot T_1^{-\delta} = u^{r_\alpha+\delta\cdot\alpha-\delta\cdot\alpha}=R_1, R_2'=v^{s_\beta}\cdot T_2^{-\delta} = v^{r_\beta+\delta\cdot\beta-\delta\cdot\beta} = R_2, R_4' = T_1^{s_x}\cdot u^{-s_{\gamma 1}} = T_1^{r_x+\delta\cdot H_1(\mathrm{ID}_i)}\cdot u^{-r_{\gamma_1}-\delta\cdot\gamma_1} = R_4$ 以及 $R_5' = T_2^{s_x}\cdot v^{-s_{\gamma_2}} = T_1^{r_x+\delta\cdot H_1(\mathrm{ID}_i)}\cdot v^{-r_{\gamma_2}-\delta\cdot\gamma_2} = R_5$；

(2)验证 $e(T_3^{s_x}\cdot h^{-s_{\gamma_1}-s_{\gamma_2}}\cdot g_1^{-\delta}, g_2)\cdot e(h^{-s_\alpha-s_\beta}\cdot T_3^{\delta}, w) = R_3$ 是否成立，其正确性由式(4)推出；

(3)验证 $\delta = H_1(\mathrm{ID}_m \,||\, m \,||\, T_i, T_1, T_2, T_3, R_1', R_2', R_3', R_4', R_5')$ 是否成立，若成立则接受该签名；否则，拒绝。

$$\begin{aligned} &e(T_3^{s_x}\cdot h^{-s_{\gamma_1}-s_{\gamma_2}}\cdot g_1^{-\delta}, g_2)\cdot e(h^{-s_\alpha-s_\beta}\cdot T_3^{\delta}, w)\\ &= e(T_3,g_2)^{s_x} e(h,w)^{-s_\alpha-s_\beta} e(h,g_2)^{-s_{\gamma_1}-s_{\gamma_2}}\\ &\quad\cdot (e(T_3,w)e(g_1,g_2)^{-1})^{\delta}\\ &= R_3\cdot e(T_3,g_2)^{\delta H_1(\mathrm{ID}_i)+x\delta} e(h,g_2)^{-\delta x(\alpha+\beta)}\\ &\quad\cdot e(h,g_2)^{-\delta(\gamma_1+\gamma_2)} e(g_1,g_2)^{-\delta}\\ &= R_3\cdot e\left(g_1^{\frac{1}{x+H_1(\mathrm{ID}_i)}} h^{\alpha+\beta}, g_2\right)^{\delta H_1(\mathrm{ID}_i)+x\delta}\\ &\quad\cdot e(h,g_2)^{-\delta x(\alpha+\beta)-\delta(\gamma_1+\gamma_2)} e(g_1,g_2)^{-\delta} = R_3 \end{aligned} \tag{4}$$

在上面的群签名验证过程中，可以看出验证者需要计算 13 个幂运算以及 2 个双线性对运算。验证者的计算开销随着群签名的个数增加而线性增加。为了加速验证过程，车辆可以对收到的群签名做批验证处理。假设车辆收到 n 个群签名，$\mathrm{gsig}_j(M_j) = (T_{j,1},T_{j,2},T_{j,3},R_{j,3}\delta,s_{j,\alpha},s_{j,\beta},s_{j,x},s_{j,\gamma_1},s_{j,\gamma_2})$ 表示某车辆对消息 $M_j = \mathrm{ID}_{j,m} \,||\, m_j \,||\, T_j$ 的签名。对于 $1\le j\le n$，验证者做以下处理：

(1) 计算 $R_{j,1} = u^{s_{j,\alpha}}\cdot T_{j,1}^{-\delta_j}$，$R_{j,2} = v^{s_{j,\beta}}\cdot T_2^{-\delta_j}$，$R_{j,4} = T_{j,1}^{s_{j,x}}\cdot u^{-s_{j,\gamma_1}}$ 和 $R_{j,5} = T_{j,2}^{s_{j,x}}\cdot v^{-s_{j,\gamma_2}}$；

(2) 验证 $\delta_j = H_1(M_j, T_{j,1}, T_{j,2}, T_{j,3}, R_{j,1}, R_{j,2}, R_{j,3}, R_{j,4}, R_{j,5})$ 是否成立；

(3)验证等式(5)是否成立，其中 θ_j 是 l_b 位的随机数。

$$\begin{aligned} &e\left(\prod_{j=1}^{n}(T_{j,3}^{s_{j,x}}\cdot h^{-s_{j\gamma_1}-s_{j,\gamma_2}}\cdot g_1^{-\delta_j})^{\theta_j}, g_2\right)\\ &\quad\cdot e\left(\prod_{j=1}^{n}(T_{j,3}^{\delta_j}\cdot h^{-s_{j,\alpha}-s_{j,\beta}})^{\theta_j}, w\right) = \prod_{j=1}^{n} R_{j,3}^{\theta_j} \end{aligned} \tag{5}$$

在批验证过程中，验证者仅需花费 2 个双线性对运算以及 $13n$ 个幂运算完成 n 个群签名验证。而在逐个群签名验证中，验证 n 个群签名，则需要花费 $2n$ 个双线性对以及 $13n$ 个幂运算。

3.4 追踪性

当出现纠纷或者有异议的消息时，区域中心可通过等式 $T_3\cdot T_1^{-\gamma_1}\cdot T_2^{-\gamma_2} = \mathrm{gsk}_{\mathrm{ID}_i}\cdot h^{\alpha+\beta}\cdot h^{-\alpha-\beta} = \mathrm{gsk}_{\mathrm{ID}_i}$ 计算出签名者的群签名私钥。而后再查询用户列表，获取用户的真实身份。

4 安全性证明

定理 1 P_{auth} 为所提出的认证协议，攻击者 A 在多项式时间 t 内询问了至多 q_s 次会话，则攻击者赢取协议的优势为可忽略的，即

$$\begin{aligned} \mathrm{ADV}_P^{\mathrm{ake}} = \xi \le\ & 2q_s\mathrm{ADV}_{\mathrm{IBSC}}^{\text{IND-CCA}} + 2q_s\mathrm{ADV}_{\mathrm{IBSC}}^{\text{ESUF-CMA}}\\ &+ 2q_s\mathrm{ADV}^{\mathrm{HMAC}} + 2q_s\mathrm{ADV}_{G_1}^{\mathrm{CDH}} \end{aligned} \tag{6}$$

证明 通过一系列游戏来完成定理 1 的证明。对于每个游戏 Game_i，Succ_i 表示攻击者 A 猜中 $\mathrm{Test}(C^i/V^j)$ 所选择的 b。

(1) Game_0：这是随机预言机模型下的真实协议，因而有 $\mathrm{ADV}_P^{\mathrm{ake}} = 2\Pr[\mathrm{Succ}_0]-1$。

(2) Game_1：在这个游戏中，我们模拟执行 Game_0 所有实例，若攻击者 A 能攻破所使用签密算法的消息机密性以及不可伪造特性，则终止该协议。而所使用的签密方案被证明是自适应选择密文安全以及本质不可伪造的。因而，Game_1 与 Game_0 是完善不可区分的，即 $\Pr[\mathrm{Succ}_1]-\Pr[\mathrm{Succ}_0]\le q_s\mathrm{ADV}_{\mathrm{IBSC}}^{\text{IND-CCA}} + q_s\mathrm{ADV}_{\mathrm{IBSC}}^{\text{ESUF-CMA}}$。

(3) Game_2：在这个游戏中，我们像 Game_1 一样模拟协议只是加入一个 CDH 问题到协议中，若 CDH 假设成立及 HMAC 是安全的，则 Game_2 和 Game_1 是不可区分的。若攻击者 A 可以 Test 询问所返回的数是随机数还是真实的会话密钥 $\mathrm{gsk}_{\mathrm{ID}_i}$ 的话从而进一步区分 Game_2 和 Game_1，我们则可以利用攻击者 A 来破解 CDH 问题。具体来讲，我们将一对随机的二元组 (g_1^m, g_1^n) 嵌入到协议中来代替协议中原有的二元组 (g_1^a, g_1^b)。从游戏 Game_1 中我们可以看出，因为所使用的签密算法是安全的，因此攻击者不可能冒充车辆自己选取一个 V_i 并将其加密从而伪造出一个正确的签密信息 $\{L_i, c, S, T\}$。同样，在 HAMC 算法安全的前提下，攻击者 A 也不可能冒充区域中心自己选取一个 $g_1^{b'}$ 从而产生一个正确的 HMAC 信息。这意味着攻击者只是是被动的窃听诚实用户的通信消息。这样当我们嵌入二元组 (g_1^m, g_1^n) 嵌入到协议 P 中来代替协议中原有的二元组 (g_1^a, g_1^b) 后，如敌手可以获得 $\mathrm{gsk}_{\mathrm{ID}_i}$，这说明敌手已经破解了 CDH 问题，因为此时的 $\mathrm{gsk}_{\mathrm{ID}_i}$ 是被 $g_1^{mn} = \mathrm{CDH}(g_1^m, g_1^n)$ 所加密的消息。因为所采用的加密算法

是安全的，因此攻击者比如获取了加密密钥即获得了 $g_1^{mn}=\mathrm{CDH}(g_1^m,g_1^n)$，即破解了 CDH 问题。因而，$\mathrm{Game}_1$ 与 Game_2 是完善不可区分的，即 $\Pr[\mathrm{Succ}_2]-\Pr[\mathrm{Succ}_1]\le q_s\mathrm{ADV}^{\mathrm{HMAC}}+q_s\mathrm{ADV}_{G_1}^{\mathrm{CDH}}$。

从攻击者 A 的角度来看，判断协议输出的是真正的密钥还是与密钥等长的随机数，则为判断 (g_1^m, g_1^n, c) 是否是有效的 DDH 元素组。因而有 $\Pr[\mathrm{Succ}_2]=1/2$。综上所述，得出公式(6)。　　证毕

定理 2　P_{auth} 为所提出的认证协议，攻击者 A 在多项式时间 t 内询问了至多 q_s 次会话，则攻击者赢取协议的优势为可忽略的，即

$$\mathrm{ADV}_P^{\mathrm{anon}}(A)=2q_s\mathrm{ADV}_{\mathrm{IBSC}}^{\mathrm{IND\text{-}CCA}} \tag{7}$$

证明　该定理的证明与定理 1 的证明类似，首先定义真实的攻击游戏 Game_0，而后基于 Game_0 修改获得新游戏 Game_1，区别是：当且仅当攻击者 A 能攻破所使用签密算法的消息机密性时，Game_1 停止并退出。签密算法的消息机密性被证明是选择密文安全的，因而 Game_0 与 Game_1 不可区分。从攻击者 A 的观点来看，由于 V_i 的真实身份有签密算法加密保护，则猜测出真实身份的概率是 $1/2$，进而得证。

定理 3　gs 为协议中所采用的群签名方案，则攻击者 A 在多项式时间 t 内赢取协议的完全匿名性以及在选择消息攻击下伪造签名的优势均为可忽略的，即：$\mathrm{ADV}_P^{\text{ef-cma}}(A)=\mathrm{ADV}_{\mathrm{gs}}^{\text{ef-cma}}$ 以及 $\mathrm{ADV}_P^{\text{gs-anon}}(A)=\mathrm{ADV}_{\mathrm{gs}}^{\mathrm{anon}}$。

证明　协议中所使用的群签名算法[17]是群签名算法[18]的一种变形，密码系统公开参数、用户密钥以及签名计算方法均相同，区别在于文中所采用方案签名的形式为 $(T_1,T_2,T_3,R_3,\delta,s_\alpha,s_\beta,s_x,s_{\gamma_1},s_{\gamma_2})$，而在原始群签名方案中签名的消息为 $(T_1,T_2,T_3,\delta,s_\alpha,s_\beta,s_x,s_{\gamma_1},s_{\gamma_2})$。这样处理的优点是：变换后的方案能够支持批验证，降低签名验证效率。其中，$R_3=e(T_3^{s_x}\cdot h^{-s_{\gamma_1}-s_{\gamma_2}}\cdot g_1,g_2)\cdot e(h^{-s_\alpha-s_\beta}\cdot T_3,w)$ 是暗含在原始签名方案之中，因而文中所采用群签名方案的不可伪造性以及匿名性安全性证明只需将文献[18]中 5.3 节中的签名预言机以 $(T_1,T_2,T_3,R_3,\delta,s_\alpha,s_\beta,s_x,s_{\gamma_1},s_{\gamma_2})$ 形式回答，其中 $R_3=e(T_3^{s_x}\cdot h^{-s_{\gamma_1}-s_{\gamma_2}}\cdot g_1,g_2)\cdot e(h^{-s_\alpha-s_\beta}\cdot T_3,w)$ 即可。　　证毕

通过定理 1，定理 2 以及定理 3，可以看出文中所设计的方案能够实现具有匿名保护的相互身份认证，消息认证性以匿名性。群签名密码系统是周期性更新，只有合法车辆才能获得最新的签名密钥，因而避免了撤销验证并且实现后向撤销安全。

5　性能分析

在衡量协议的计算开销，仅考虑运算复杂度较高的如幂运算以及线性对运算，而不考虑计算量较低的哈希、乘法、加法以及对称加密解密运算。在 Pentium 4 CPU 3.0 GHz、内存为 1 G 计算机上，使用 PBC 大数库[19]测试的阶 q 为 160 bit 位 MNT 曲线上一次幂运算 $T_{\exp}=0.4\,\mathrm{ms}$ 以及一次线性对运算 $T_{\mathrm{pair}}=4.3\,\mathrm{ms}$。

5.1　车辆与区域中心认证开销

在认证过程之中，车辆仅需 5 次幂运算计算 $g_1^t,g_1^a,g_1^{ab},S=\varphi(S_{\mathrm{ID}_i})^{(t+h)}$ 以及 $T=(g_1^{H_1(L_i)}\varphi(\mathrm{pw}))^t$。区域中心需要花费 5 次幂运算和两次线性对运算来计算 $g_1^b,g_1^{ab},e(T,sk_{L_i})$ 和 $e(S,g_2^{H_1(\mathrm{ID}_i)}\mathrm{pw})g^{-h}$。鉴于上述分析，认证过程总的计算开销为 $10\cdot T_{\exp}+2\cdot T_{\mathrm{pair}}=12.6\,\mathrm{ms}$。

车辆需要发送 L_i,c,S,T，其中 $c=(\mathrm{ID}_i\,||\,\mathrm{PID}_i\,||\,k\,||\,t_V)\oplus H_3(r)$, $S=\varphi(S_{\mathrm{ID}_i})^{(t+h)}\in G_1$ 和 $T=(g_1^{H_1(L_i)}\varphi(\mathrm{pw}))^t\in G_1$。其中假设身份与时戳均为 32 bit、密钥 k 长度为 128 bit，G_1 中的元素为 161 位。车辆在认证过程中的发送信息总长度是 578 bit。另一方面，区域中心需要发送 $\mathrm{PID}_i,L_i,\{\mathrm{gsk}_{\mathrm{ID}_i},t_L\}_k$，长度为 257 bit。

5.2　车辆广播消息开销

车辆广播消息的格式如表 1 所示，需要附加消息标示符 ID_m，时戳 T_i 以及群签名 $\mathrm{gsig}(m,T_i)$，其中消息标示符、时戳均为 4 byte，群签名的长度是 309 byte。因而，车辆广播消息的通信开销是 349 byte。

广播消息的计算开销即为群签名的计算量，$12T_{\exp}+3T_{\mathrm{pair}}=18\,\mathrm{ms}$。本文所提出的协议，在验证广播签名的有效性时，不再需要撤销验证，即验证开销是常量，与撤销成员个数无关。反之，直接采用群签名的验证开销是与群众撤销成员数目线性相关。图 2 给出本文所采用的方案与直接采用群签名方案验证开销，随群中撤销车辆个数的对比。另外，本文的方案支持批验证，即短时间段内收到多个广播消息。假设收到 n 广播消息，则批验证的计算开销为 $13n\cdot T_{\exp}+2\cdot T_{\mathrm{pair}}=8.6+5.2\cdot n$。图 3 给出批验证与单个验证的计算开销对比。

6　结论

本文结合基于身份签密技术与群签名方案，提出一种适用于车辆网络的高效消息认证方案。相对于历史文献来说，该方案能够支持后向撤销隐私安全，避免车辆在撤销之后，其历史路径信息被恢复出来，有效地保护了车辆用户的位置隐私。此外，用户在验证其它车辆广播消息时，不再需要对签名者进行撤销验证，即用户在验证网络中的广播消息的计算开销是常量，与撤销车辆的数目无关。最后，本文的方案能够支持同时验证多个广播消息的合法性，与逐个签名验证相比，极大程度地降低了计算开销。

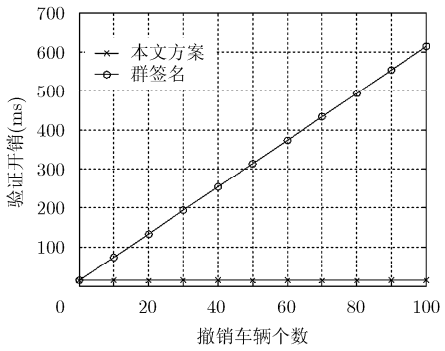

图 2 验证开销与撤销车辆个数关系图

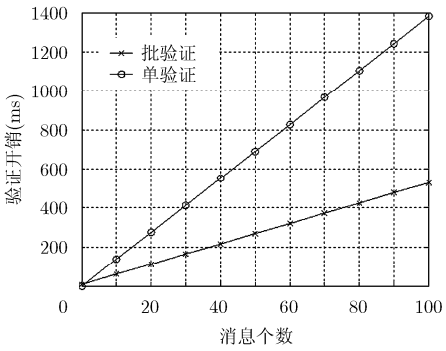

图 3 验证开销与消息个数关系图

参 考 文 献

[1] Chen M, Chen J, and Chang T. Android/OSGi-based vehicular network management system[J]. *Computer Communications*, 2011, 34(2): 169–183.

[2] Lu R, Lin X, Liang X, *et al.*. A dynamic privacy-preserving key management scheme for location based services in VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2012, 13(1): 127–139.

[3] Zhang W, Chen Y, Yang Y, *et al.*. Multi-hop connectivity probability in infrastructure-based vehicular networks[J]. *IEEE Journal on Selected Areas in Communications*, 2012, 30(4): 740–747.

[4] Liu X, Zhang Y, Wang B, *et al.*. Mona: secure multi-owner data sharing for dynamic groups in the Cloud[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2013, 24(6): 1182–1191.

[5] Liu X and Zhang Y. A privacy-preserving acceleration authentication protocol for mobile pay-TV systems[J]. *Security and Communication Networks*, 2013, 6(3): 361–372.

[6] 汤一亮. 截至 2 月底: 我机动车保有量达 2.11 亿辆[OL]. http:// news.xinhuanet.com/auto/2011-03/18/c_121201772.htm, 2011. 03. 18.

[7] Raya M and Hubaux J. Securing vehicular ad hoc networks[J]. *Journal of Computer Security*, 2007, 15(1): 39–68.

[8] Haas J, Hu Y, and Laberteaux K. Design and analysis of a lightweight certificate revocation mechanism for VANET[C]. Proceedings of 6th ACM international workshop on VehiculAr InterNETworking, New York, 2009: 89–98.

[9] Wasef A, Jiang Y, and Shen X. DCS: an efficient distributed certificate service scheme for vehicular networks[J]. *IEEE Transactions on Vehicular Technology*, 2010, 59(2): 533–549.

[10] Lu R, Lin X, Zhu H, *et al.*. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[C]. Proceedings of 27th Conference on Computer Communications, Arizona, 2008: 1229–1237.

[11] Sun Y, Lu R, Lin X, *et al.*. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications[J]. *IEEE Transactions on Vehicular Technology*, 2010, 59(7): 3589–3603.

[12] Wasef A and Shen X. EMAP: Expedite message authentication protocol for vehicular ad hoc networks[J]. *IEEE Transactions on Mobile Computing*, 2013, 12(1): 78–89.

[13] Lin X, Sun X, Ho P, *et al.*. GSIS: a secure and privacy-preserving protocol for vehicular communications[J]. *IEEE Transactions on Vehicular Technology*, 2007, 56(6): 3442–3456.

[14] Sun J, Zhang C, Zhang Y, *et al.*. An identity-based security system for user privacy in vehicular Ad hoc networks[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2010, 21(9): 1227–1239.

[15] Xiong H, Beznosov K, Qin Z, *et al.*. Efficient and spontaneous privacy-preserving protocol for secure vehicular communication[C]. Proceedings of International Conference on Communications, Cape Town, 2010: 1–6.

[16] Barreto P, Libert B, McCullagh N, *et al.*. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]. Proceedings of the 24th Annual International Cryptology Conference on Advances in Cryptology, Chennai, 2005: 515–532.

[17] Ferrara A, Green M, and Hohenberger S. Practical short signature batch verification[C]. Proceedings of the 9th Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology, San Francisco, 2009: 309–324.

[18] Boneh D, Boyen X, and Shacham H. Short Group Signatures[C]. Proceedings of the 23th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, 2004: 41–55.

[19] Lynn B. The pairing-based cryptography library[OL]. http:// crypto.stanford.edu/pbc/, 2013. 05.

刘雪峰： 男，1985 年生，博士生，研究方向为应用密码学、车辆网络安全、云计算安全、无线网络安全等.

张玉清： 男，1966 年生，博士生导师，研究方向为漏洞挖掘、应用密码学、量子密码理论.

王 鹤： 女，1987 年生，博士生，研究方向为应用密码学、量子密码理论.