面向车载自组网的无证书聚合签名方案的安全性分析与改进

杨小东* 麻婷春 陈春霖 王晋利 王彩芬

(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：2018年，王大星和滕济凯提出了一种适用于车载自组织网络的无证书聚合签名方案，并在随机模型下证明该方案是存在不可伪造的。针对该方案的安全性，给出了3类伪造攻击："honest-but-curious"的KGC攻击、恶意的KGC与RSU的联合攻击、内部签名者的联合攻击。分析结果表明，王大星等人设计的无证书聚合签名方案在这3类攻击下均是不安全的。为了抵抗这些攻击，进一步提出了一个改进的无证书聚合签名方案。所提方案不仅在自适应性选择消息攻击下满足存在不可伪造性，还能有效抵抗联合攻击。

关键词：车载自组织网络；无证书聚合签名；联合攻击；不可伪造性

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)05-1265-06

DOI: 10.11999/JEIT180571

Security Analysis and Improvement of Certificateless Aggregate Signature Scheme for Vehicular Ad Hoc Networks

YANG Xiaodong MA Tingchun CHEN Chunlin WANG Jinli WANG Caifen

(*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: In 2018, Wang Daxing and Teng Jikai proposed a certificateless aggregate signature scheme for vehicular ad-hoc networks, and proved that their scheme was existentially unforgeable in the random oracle model. To analyze the security of this scheme, three types of forgery attacks are given: "honest-but-curious" KGC attacks, malicious KGC and RSU coalition attacks, and internal signers' coalition attacks. The analysis results show that the certificateless aggregate signature scheme designed by Wang Daxing and Teng Jikai is insecure against these three types of attacks. To resist these attacks, an improved certificateless aggregate signature scheme is further proposed. The new scheme not only satisfies existential unforgeability under adaptive chosen-message attacks, but also resists effectively coalition attacks.

Key words: Vehicular ad-hoc networks; Certificateless aggregate signature; Coalition attack; Unforgeability

1 引言

车载自组织网络(Vehicular Ad hoc NETworks, VANETs)是一种高速移动的无线自组织网络，已成为智能交通的重要基础[1,2]。VANETs通过车辆与路边基础设施(RoadSide Units, RSU)、车与车之间的通信，能最大限度地减少或避免交通事故，提升交通效率，改善乘车环境。然而，VANETs为驾驶员和乘客的出行带来安全和提供各种娱乐信息服务的同时，也面临诸多的信息安全挑战[3,4]。由于无线网络自身的开放性和脆弱性，使得VANETs中传输的消息很容易受到伪造或篡改等各类攻击。此外，VANETs中的车辆高速移动，并且通信的带宽非常有限，这就要求VANETs中的消息认证必须具有较低的通信开销。因此，如何确保VANETs中消息的完整性、真实性和实时性已成为近年来智能交通领域的一个研究热点。

无证书聚合签名是一类重要的密码体制，不仅能提供消息的可认证性和完整性、用户行为的不可否认性等安全服务，还可解决传统的公钥证书管理问题和基于身份密码方案中的密钥托管问题。无证书聚合签名能将来自多个用户的不同签名压缩成一个短的聚合签名，只需验证聚合签名的正确性便可实现对所有参与聚合的单个签名的有效性验证。因此，无证书聚合签名是一种非常重要的数据聚合技

收稿日期：2018-06-11；改回日期：2018-12-11；网络出版：2018-12-17
*通信作者： 杨小东 y200888@163.com
基金项目：国家自然科学基金(61662069, 61562077)，中国博士后科学基金(2017M610817)，兰州市科技计划项目(2013-4-22)，西北师范大学青年教师科研能力提升计划(NWNU-LKQN-14-7)

Foundation Items: The National Natural Science Foundation of China (61662069, 61562077), The China Postdoctoral Science Foundation (2017M610817), The Science and Technology Project of Lanzhou City (2013-4-22), The Foundation of Northwest Normal University (NWNU-LKQN-14-7)

术，能减少数据的通信带宽和签名验证开销，非常适用于带宽受限的VANETs。自从Boneh等人[5]提出第1个聚合签名方案后，研究者设计了一系列无证书聚合签名方案[6−8]。然而，大多数方案无法抵抗现实中的联合攻击[9,10]。在这类攻击中，攻击者企图利用非法的单个签名生成合法的聚合签名。如果联合攻击成功，则聚合签名的合法性无法确保生成聚合签名的所有单个签名的合法性，但这与无证书聚合签名的安全目标相违背。因此，研究抗联合攻击的无证书聚合签名方案具有重要的现实意义和理论价值。

近年来，面向VANETs的无证书聚合签名方案颇受研究者的关注[11−13]。在无证书聚合签名方案中，一个半可信的密钥生成中心(Key Generation Center, KGC)负责生成每个用户的部分私钥，用户自己生成秘密值和对应的公钥。由于用户的最终私钥是由部分私钥和秘密值2部分组成，因此KGC无法获取用户的签名私钥。Malhi等人[14]为VANETs设计了一个高效的无证书聚合签名方案，但Kumar等人[15]发现该方案不能抵抗honest-but-curious的KGC攻击。为了阻止这类攻击，Kumar等人[15]也提出了一个改进的无证书聚合签名方案，但没有考虑联合攻击。2018年，王大星等人[16]提出了一种新的适用于VANETs的无证书聚合签名方案(简称王方案)，并在随机预言模型中证明了该方案的安全性。然而，本文通过3类具体的攻击对王方案进行了安全性分析，发现该方案针对honest-but-curious的KGC攻击和联合攻击均是不安全的。为了解决王方案中存在的安全缺陷，进一步提出了一个改进的无证书聚合签名方案，其安全性依赖于Computational Diffie-Hellman(CDH)假设。新方案不仅能抵抗联合攻击，并具有身份的匿名性和可追踪性。

2 准备知识

假设G_1和G_2是2个阶为素数p的乘法循环群，g是G_1的一个生成元。如果一个可有效计算的映射$\hat{e}: G_1 \times G_1 \to G_2$满足以下性质，则称$\hat{e}$是一个双线性映射[17]。(1)双线性：对于任意的$a, b \in Z_p^*$，有$\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$。(2)非退化性：$\hat{e}(g, g) \neq 1_{G_2}$，这里$1_{G_2}$表示$G_2$中的单位元。给定$(g, g^a, g^b) \in G_1^3$，其中未知的$a, b \in Z_p^*$, CDH问题是计算$g^{ab}$。

定义 1 如果不存在任何一个多项式时间算法能以不可忽略的概率求解CDH问题，则称CDH假设成立[17]。

3 王方案的回顾

王大星等人[16]设计了一种面向VANETs的无证书聚合签名方案，具体描述如下：

(1) Setup：给定安全参数$\lambda \in Z$, KGC首先选择2个阶为素数p的循环群G_1和G_2，一个G_1的生成元和一个双线性映射$\hat{e}: G_1 \times G_1 \to G_2$；然后选择3个哈希函数$H_1: \{0,1\}^* \to G_1$和$H_2, H_3: \{0,1\}^* \to Z_p^*$。KGC随机选择$s \in Z_p^*$，计算$P_K = g^s$。每个路边单元(RSU)随机选择$y_i \in Z_p^*$作为自己的秘密值，并计算公钥$\bar{P}_i = g^{y_i}$。最后，KGC秘密保存主密钥msk=$s$，公开系统参数$\mathrm{sp} = \{\mathrm{G_1}, \mathrm{G_2}, \hat{\mathrm{e}}, \mathrm{p}, \mathrm{g}, \mathrm{P_K}, \bar{\mathrm{P}}_\mathrm{i}, H_1, H_2, H_3\}$。

(2) PartialKeyGen：对于一个车辆用户的身份ID_i, KGC计算$Q_i = H_1(\mathrm{ID}_i)$和$\mathrm{psk}_i = (Q_i)^s$，然后在用户注册表中保存$\{\mathrm{ID}_i, Q_i\}$，通过一个安全信道将部分私钥psk_i发送给用户。

(3) UserKeyGen：车辆用户随机选择$x_i \in Z_p^*$作为自己的秘密值usk_i，计算对应的公钥$\mathrm{pk}_i = g^{x_i}$。身份为ID_i的签名私钥为$\mathrm{sk}_i = (\mathrm{usk}_i, \mathrm{psk}_i) = (x_i, Q_i^s)$。

(4) PseudonymGen：RSU收到车辆用户发送的身份信息$Q_i = H_1(ID_i)$后，首先随机选择$a_i \in Z_p^*$，然后计算$F1_i = (Q_i)^{a_i}$, $w_i = H_2(F1_i)$和$F2_i = a_i w_i$，最后将假名$(F1_i, F2_i)$发送给用户，并在假名登记表中保存记录$\{(Q_i, (F1_i, F2_i)\}$。

(5) Sign：对于一个消息m_i，车辆用户随机选择$r_i \in Z_p^*$，计算$U_i = g^{r_i}$；然后利用自己的私钥sk_i和邻近RSU的公钥$\bar{P}_i$计算$h_i = H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$和$V_i = (\mathrm{psk}_i)^{F2_i}(P_K)^{h_i r_i}(\bar{P}_i)^{h_i x_i}$，最后输出$m_i$的单个签名$\sigma_i = (U_i, V_i)$。

(6) Verify：对于车辆用户的部分假名$F1_i$和公钥pk_i，RSU的公钥$\bar{P}_i$及消息m_i的单个签名$\sigma_i = (U_i, V_i)$，验证者计算$h_i = H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$和$w_i = H_2(F1_i)$。如果$\hat{e}(V_i, g) = \hat{e}(F1_i^{w_i} U_i^{h_i}, P_K) \cdot \hat{e}(\mathrm{pk}_i^{h_i}, \bar{P}_i)$，则接受$\sigma_i$是一个合法的单个签名；否则，拒绝$\sigma_i$。

(7) Aggregate：对于来自n个用户的消息/签名对$(m_i, \sigma_i = (U_i, V_i))$，其中$i = 1, 2, \cdots, n$，聚合器计算$V = \prod_{i=1}^{n} V_i$，并生成关于$\{m_1, m_2, \cdots, m_n\}$的聚合签名$\sigma = (U_1, U_2, \cdots, U_n, V)$。

(8) AggVerify：给定n个用户的部分假名$\{F1_1, F1_2, \cdots, F1_n\}$和公钥$\{\mathrm{pk}_1, \mathrm{pk}_2, \cdots, \mathrm{pk}_n\}$, RSU的公钥$\bar{P}_i$及一个关于$\{m_1, m_2, \cdots, m_n\}$的聚合签名$\sigma = (U_1, U_2, \cdots, U_n, V)$，验证者计算$h_i = H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$和$w_i = H_2(F1_i)$，其中$i = 1, 2, \cdots, n$。如果$\hat{e}(V, g) = \hat{e}\left(\prod_{i=1}^{n} F1_i^{w_i} U_i^{h_i}, P_K\right) \hat{e}\left(\prod_{i=1}^{n} pk_i^{h_i}, \bar{P}_i\right)$，接受$\sigma$是一个合法的聚合签名；否则，拒绝$\sigma$。

4　王方案的安全性分析

下面通过3类具体的攻击来说明王大星等人[16]提出的无证书聚合签名方案是不安全的。第1类攻击是普通的伪造攻击，另外2个攻击是基于合谋的联合攻击。

4.1 “honest-but-curious”的KGC攻击

假定$\mathcal{A}_1$是一个“honest-but-curious”的KGC，则$\mathcal{A}_1$执行如下的步骤能成功伪造一个合法的聚合签名。

(1) $\mathcal{A}_1$随机选择一个签名者：不失一般性，假设$\mathcal{A}_1$选择身份ID_1和消息m_1'。$\mathcal{A}_1$从RSU处获取ID_1的假名$(F1_1, F2_1)$，然后发起关于(ID_1, m_1')的签名询问并获得一个相应的签名$\sigma_1' = (U_1', V_1')$。

(2) $\mathcal{A}_1$计算$h_{1'} = H_3(m_{1'}, F1_1, \mathrm{pk}_i, U_{1'})$：因为$\sigma_1' = (U_1', V_1')$是$m_1'$的合法签名，所以$\sigma_1'$必须满足下面的等式$V_{1'} = (\mathrm{psk}_1)^{F2_1}(P_K)^{h_{1'}r_{1'}}(\bar{P}_i)^{h_{1'}x_1}$。由于$(P_K)^{h_1'r_1'} = (g^s)^{h_1'r_1'} = (g^{r_1'})^{h_1's} = (U_1')^{h_1's}$，KGC知道主密钥$s$和$ID_1$的部分私钥$\mathrm{psk}_1$，因此$\mathcal{A}_1$能计算出$\mathrm{RSK}_{i,1} = (\bar{P}_i)^{x_1} = \left(V_1'/((\mathrm{psk}_1)^{F2_1}(U_1')^{h_1's})\right)^{(h_1')^{-1}}$。

(3) $\mathcal{A}_1$随机选择$r_1 \in Z_p^*$和一个待签名的消息m_1，然后计算$U_1 = g^{r_1}$, $h_1 = H_3(m_1, F1_1, \mathrm{pk}_1, U_1)$和$V_1 = (\mathrm{psk}_1)^{F2_1}(P_K)^{h_1r_1}(\mathrm{RSK}_{i,1})^{h_1}$，最后输出$m_1$的单个签名$\sigma_1 = (U_1, V_1)$。很容易验证$\sigma_1 = (U_1, V_1)$是一个合法的单个签名，但$\sigma_1$不是签名询问的输出。由于秘密值$x_1$对$\mathcal{A}_1$是未知的，因此$\mathcal{A}_1$成功伪造了单个签名$\sigma_1$。

(4) $\mathcal{A}_1$发起关于(ID_i, m_i)的签名询问，并获得对应的单个签名$\sigma_i = (U_i, V_i)$，其中，$i = 2, 3, \cdots, n$。

(5) $\mathcal{A}_1$计算$V^* = \prod_{i=1}^{n} V_i$，输出一个关于$\{m_1, m_2, \cdots, m_n\}$的聚合签名$\sigma^* = (U_1, U_2, \cdots, U_n, V^*)$。由于$\sigma_1 = (U_1, V_1)$是$\mathcal{A}_1$伪造的合法签名，$\sigma_i = (U_i, V_i)$ $(i = 2, 3, \cdots, n)$是签名询问的返回值，所以$\mathcal{A}_1$成功伪造了一个合法的聚合签名$\sigma^* = (U_1, U_2, \cdots, U_n, V^*)$。这表明王方案无法抵抗来自“honest-but-curious”的KGC攻击，即王方案[16]在第1类攻击$\mathcal{A}_1$下是不安全的。

4.2 恶意的KGC与RSU的联合攻击

令$\mathcal{A}_3$表示一个恶意的KGC，$\{m_1, m_2, \cdots, m_n\}$，$\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$和$\{\mathrm{pk}_1, \mathrm{pk}_2, \cdots, \mathrm{pk}_n\}$分别表示$n$个消息、$n$个用户的身份和对应的公钥。$\mathcal{A}_3$联合RSU能伪造任意消息的单个签名和聚合签名，具体步骤如下。

(1) $\mathcal{A}_3$计算$Q_i = H_1(\mathrm{ID}_i)$和$\mathrm{psk}_i = (Q_i)^s$，其中$i = 1, 2, \cdots, n$；然后将$\{Q_1, Q_2, \cdots, Q_n\}$和$\{\mathrm{pk}_1, \mathrm{pk}_2, \cdots, \mathrm{pk}_n\}$发送给RSU。

(2) RSU随机选择$a_i \in Z_p^*$，计算$F1_i = (Q_i)^{a_i}$，$w_i = H_2(F1_i)$和$F2_i = a_iw_i$，并利用私钥y_i计算$(\mathrm{pk}_i)^{y_i}$，其中，$i = 1, 2, \cdots, n$；然后发送$\{(\mathrm{pk}_1)^{y_i}, (\mathrm{pk}_2)^{y_i}, \cdots, (\mathrm{pk}_n)^{y_i}\}$和假名集合$\{(F1_1, F2_1), (F1_2, F2_2), \cdots, (F1_n, F2_n)\}$给$\mathcal{A}_3$。

(3) $\mathcal{A}_3$随机选择$r_1, r_2, \cdots, r_n \in Z_p^*$，计算$U_i = g^{r_i}$，$h_i = H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$和$V_i = (\mathrm{psk}_i)^{F2_i}(P_K)^{h_ir_i}(\mathrm{pk}_i^{y_i})^{h_i}$；然后生成$\mathrm{ID}_i$和$\mathrm{pk}_i$关于消息$m_i$的单个签名$\sigma_i = (U_i, V_i)$，其中，$i = 1, 2, \cdots, n$。

(4) $\mathcal{A}_3$计算$V = \prod_{i=1}^{n} V_i$，输出关于$\{m_1, m_2, \cdots, m_n\}$的聚合签名$\sigma = (U_1, U_2, \cdots, U_n, V)$。由于$(\mathrm{pk}_i)^{y_i} = (g^{x_i})^{y_i} = (g^{y_i})^{x_i} = (\bar{P}_i)^{x_i}$，因此$V_i = (\mathrm{psk}_i)^{F2_i}(P_K)^{h_ir_i}(\mathrm{pk}_i^{y_i})^{h_i} = (\mathrm{psk}_i)^{F2_i}(P_K)^{h_ir_i}(\bar{P}_i)^{h_ix_i}$。很容易验证$\mathcal{A}_3$联合RSU生成的单个签名$\sigma_i = (U_i, V_i)(i = 1, 2, \cdots, n)$和聚合签名$\sigma = (U_1, U_2, \cdots, U_n, V)$均是合法的。这说明王方案[16]无法抵抗来自恶意的KGC与RSU的联合攻击。

4.3 内部签名者的联合攻击

不失一般性，假定用户1和用户2是两个任意的签名者，它们的身份、假名和公钥分别是$\{\mathrm{ID}_1, \mathrm{ID}_2\}$，$\{(F1_1, F2_1), (F1_2, F2_2)\}$和$\{\mathrm{pk}_1, \mathrm{pk}_2\}$，邻近RSU的公钥为$\bar{P}_i$。如果用户1和用户2分别签名两个消息$m_1$和$m_2$，则用户1与用户2执行如下的步骤能生成非法的单个签名σ_1和σ_2，但关于m_1和m_2的聚合签名σ是合法的。

(1) 用户1随机选择$r_1 \in Z_p^*$，计算$U_1 = g^{r_1}$和$h_1 = H_3(m_1, F1_1, \mathrm{pk}_1, U_1)$，发送$(P_K)^{h_1r_1}$给用户2。

(2) 用户2随机选择$r_2 \in Z_p^*$，计算$U_2 = g^{r_2}$和$h_2 = H_3(m_2, F1_2, \mathrm{pk}_2, U_2)$，发送$(P_K)^{h_2r_2}$给用户1。

(3) 用户1计算$V_1 = (\mathrm{psk}_1)^{F2_1}(P_K)^{h_2r_2}(\bar{P}_i)^{h_1x_1}$，输出$m_1$的单个签名$\sigma_1 = (U_1, V_1)$。

(4) 用户2计算$V_2 = (\mathrm{psk}_2)^{F2_2}(P_K)^{h_1r_1}(\bar{P}_i)^{h_2x_2}$，输出$m_2$的单个签名$\sigma_2 = (U_2, V_2)$。

(5) 输出关于m_1和m_2的聚合签名$\sigma = (U_1, U_2, V)$，这里$V = V_1V_2$。

由于$\hat{e}(V_1, g) = \hat{e}((\mathrm{psk}_1)^{F2_1}(P_K)^{h_2r_2}(\bar{P}_i)^{h_1x_1}, g) = \hat{e}((\mathrm{psk}_1)^{F2_1}, g)\hat{e}((P_K)^{h_2r_2}, g)\hat{e}((\bar{P}_i)^{h_1x_1}, g) = \hat{e}(F1^{w_1}, P_K)\hat{e}(U_2^{h_2}, P_K)\hat{e}((\mathrm{pk}_1)^{h_1}, \bar{P}_i) \neq \hat{e}(F1^{w_1}, P_K)\hat{e}(U_1^{h_1}, P_K)\cdot\hat{e}((\mathrm{pk}_1)^{h_1}, \bar{P}_i)$，因此$\sigma_1 = (U_1, V_1)$不满足单个签名的验证等式，即$\sigma_1$不是一个关于$m_1$的合法签名。类似地，可以验证$\sigma_2 = (U_2, V_2)$也不是一个关于$m_2$的合法签名。但聚合签名$\sigma = (U_1, U_2, V)$满足下面的签名验证等式：$\hat{e}(V, g) = \hat{e}(V_1V_2, g) = \hat{e}((\mathrm{psk}_1)^{F2_1}\cdot(P_K)^{h_2r_2}(\bar{P}_i)^{h_1x_1}\cdot(\mathrm{psk}_2)^{F2_2}(P_K)^{h_1r_1}(\bar{P}_i)^{h_2x_2}, g) = \hat{e}((\mathrm{psk}_1)^{F2_1}(P_K)^{h_1r_1}(\bar{P}_i)^{h_1x_1}\cdot(\mathrm{psk}_2)^{F2_2}(P_K)^{h_2r_2}(\bar{P}_i)^{h_2x_2}, g)$

$=\hat{e}(\prod_{i=1}^{2} F1_i^{w_i} U_i^{h_i}, P_K)\hat{e}(\prod_{i=1}^{2} \mathrm{pk}_i^{h_i}, \bar{P}_i)$。即聚合签名$\sigma=(U_1, U_2, V)$关于$m_1$和$m_2$是合法的。这说明用户1和用户2利用非法的单个签名能生成合法的聚合签名，因此王方案[16]对于来自内部签名者的联合攻击也是不安全的。

5 改进的无证书聚合签名方案

基于王方案[16]，本节提出了一个改进的无证书聚合签名方案。具体描述如下：

(1) Setup：与王方案中的Setup算法相同，但需要增加2个抗碰撞的哈希函数$H_4:\{0,1\}^*\rightarrow G_1$和$H:\{0,1\}^*\rightarrow\{0,1\}^l$，其中$l\in Z$是哈希函数$H$输出的固定长度。

(2) PartialKeyGen: PartialKeyGen, UserKeyGen和PseudonymGen与王方案中的算法相同。

(3) Sign：对于一个消息m_i，车辆用户执行下面的步骤生成m_i的单个签名：

(a) 随机选择$r_i\in Z_p^*$，计算$U_i=g^{r_i}$和$h_i=H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$；

(b) 对于邻近RSU的公钥$\bar{P}_i$，计算$\Delta=H_4(\bar{P}_i)$；

(c) 利用自己的私钥$\mathrm{sk}_i=(\mathrm{usk}_i, \mathrm{psk}_i)=(x_i, Q_i^s)$和假名$(F1_i, F2_i)$，计算$V_i=(\mathrm{psk}_i)^{F2_i}(P_K)^{h_i r_i}\Delta^{h_i x_i+r_i}$；

(d) 输出m_i的单个签名$\sigma_i=(U_i, V_i)$。

(4) Verify：对于车辆用户的部分假名$F1_i$和公钥pk_i，RSU的公钥$\bar{P}_i$及消息m_i的单个签名$\sigma_i=(U_i, V_i)$，验证者计算$h_i=H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$，$\Delta=H_4(\bar{P}_i)$和$w_i=H_2(F1_i)$。如果$\hat{e}(V_i, g)=\hat{e}(F1_i^{w_i}U_i^{h_i}, P_K)\hat{e}(\mathrm{pk}_i^{h_i}U_i, \Delta)$，则接受$\sigma_i$是一个合法的单个签名；否则，拒绝$\sigma_i$。

(5) Aggregate：对于来自n个用户的消息/签名对$(m_i, \sigma_i=(U_i, V_i))$，其中$i=1, 2, \cdots, n$，聚合器首先计算$V=H(\hat{e}(V_1, g), \hat{e}(V_2, g), \cdots, \hat{e}(V_n, g))$，然后输出关于$\{m_1, m_2, \cdots, m_n\}$的聚合签名$\sigma=(U_1, U_2, \cdots, U_n, V)$。

(6) AggVerify：给定n个用户的部分假名$\{F1_1, F1_2, \cdots, F1_n\}$和公钥$\{\mathrm{pk}_1, \mathrm{pk}_2, \cdots, \mathrm{pk}_n\}$，RSU的公钥$\bar{P}_i$及一个关于$\{m_1, m_2, \cdots, m_n\}$的聚合签名$\sigma=(U_1, U_2, \cdots, U_n, V)$，验证者计算$\Delta=H_4(\bar{P}_i)$，$h_i=H_3(m_i, F1_i, \mathrm{pk}_i, U_i)$和$w_i=H_2(F1_i)$，其中$i=1, 2, \cdots, n$。如果$V=H(\hat{e}(F1_1^{w_1}U_1^{h_1}, P_K)\hat{e}(\mathrm{pk}_1^{h_1}U_1, \Delta), \cdots, \hat{e}(F1_n^{w_n}U_n^{h_n}, P_K)\hat{e}(\mathrm{pk}_n^{h_n}U_n, \Delta))$，则接受$\sigma$是一个合法的聚合签名；否则，拒绝$\sigma$。

6 安全性证明

定理 1 如果第1类攻击者$\mathcal{A}_1$在多项式时间内最多进行了$q_i(i=1, 2, 3, 4)$次H_i的哈希询问、q_{psk}次部分私钥询问、q_{pk}次公钥询问、q_{usk}次秘密值询问、q_{rep}次公钥替换询问和q_s次签名询问后，能以不可忽略的概率ε_1伪造一个改进方案的合法签名，则存在一个算法C能以不可忽略的概率ε_1'解决CDH问题。

定理 2 如果第2类攻击者$\mathcal{A}_2$在多项式时间内最多进行了$q_i(i=1, 2, 3, 4)$次H_i的哈希询问、q_{pk}次公钥询问、q_{usk}次秘密值询问和q_s次签名询问后，能以ε_2的概率伪造一个改进方案的合法签名，则存在一个算法C能以$\varepsilon_2'\geq(1-1/q_4)^{q_{\mathrm{usk}}}(1-(1-1/q_4)^n)\cdot(1-q_1/p)(1-q_2/p)(1-q_3/p)\varepsilon_2$的概率解决CDH问题。

以上2个定理的证明过程与文献[16]中的定理1与定理2基本相同，因此不再赘述。结合定理1和定理2，很容易推导出如下的定理。

定理 3 如果哈希函数H是抗碰撞的，则本文提出的无证书聚合签名方案在联合攻击下是安全的。

证明 如果参与生成聚合签名的单个聚合签名是合法的，则$\hat{e}(V_i, g)=\hat{e}(F1_i^{w_i}U_i^{h_i}, P_K)\hat{e}(\mathrm{pk}_i^{h_i}U_i, \Delta)$，$i=1, 2, \cdots, n$。于是有$V=H(\hat{e}(V_1, g), \hat{e}(V_2, g), \cdots, \hat{e}(V_n, g))=H(\hat{e}(F1_1^{w_1}U_1^{h_1}, P_K)\hat{e}(\mathrm{pk}_1^{h_1}U_1, \Delta), \hat{e}(F1_2^{w_2}U_2^{h_2}, P_K)\cdot\hat{e}(\mathrm{pk}_2^{h_2}U_2, \Delta), \cdots, \hat{e}(F1_n^{w_1}U_n^{h_n}, P_K)\hat{e}(\mathrm{pk}_n^{h_n}U_n, \Delta))$。即$\sigma=(U_1, U_2, \cdots, U_n, V)$是一个合法的聚合签名。

另一方面，如果聚合签名$\sigma=(U_1, U_2, \cdots, U_n, V)$是合法的，则下面的等式成立：$V=H(\hat{e}(F1_1^{w_1}U_1^{h_1}, P_K)\cdot\hat{e}(\mathrm{pk}_1^{h_1}U_1, \Delta), \hat{e}(F1_2^{w_2}U_2^{h_2}, P_K)\hat{e}(\mathrm{pk}_2^{h_2}U_2, \Delta), \cdots, \hat{e}(F1_n^{w_n}U_n^{h_n}, P_K)\hat{e}(\mathrm{pk}_n^{h_n}U_n, \Delta))=H(\hat{e}(V_1, g), \hat{e}(V_2, g), \cdots, \hat{e}(V_n, g))$。由哈希函数$H$的抗碰撞性可知$\hat{e}(V_i, g)=\hat{e}(F1_i^{w_i}U_i^{h_i}, P_K)\hat{e}(\mathrm{pk}_i^{h_i}U_i, \Delta)$，$i=1, 2, \cdots, n$，因此单个签名$\sigma_i=(U_i, V_i)$也是合法的。

上面的分析表明，一个聚合签名是合法的当且仅当参与聚合的所有单个签名是合法的。因此，本文提出的改进方案能抵抗联合攻击。 证毕

定理 4 本文提出的无证书聚合签名满足匿名性和可追踪性。

证明 车辆用户身份ID_i在KGC处申请部分私钥时，KGC计算$Q_i=H_1(\mathrm{ID}_i)$，并在用户注册表中保存记录$\{\mathrm{ID}_i, Q_i\}$。车辆用户从临近RSU申请假名时，车辆用户提交的身份信息是Q_i，而哈希函数H_1的抗碰撞性使得RSU无法从$Q_i=H_1(\mathrm{ID}_i)$中计算出真实的身份ID_i。RSU选取随机数$a_i\in Z_p^*$生成ID_i的假名，并在假名登记表中保存$\{Q_i, (F1_i, F2_i)\}$。除了RSU外，任何人无法将Q_i与假名$(F1_i, F2_i)$关联起来。因此，本文提出的无证书聚合签名方案具有身份的匿名性。

如果车辆用户发布了违规消息，则RSU通过签名中的$F1_i$在假名登记表中查找$\{Q_i,(F1_i,F2_i)\}$，并将违规消息的签名和$\{Q_i,(F1_i,F2_i)\}$提交给KGC。随后，KGC通过Q_i在用户注册表中查找$\{\mathrm{ID}_i,Q_i\}$，进而追踪到发布虚假消息的车辆真实身份ID_i。因此，本文提出的改进方案具有身份的可追踪性。

证毕

7　有效性分析

下面对本文提出的改进方案进行性能分析，主要考虑比较耗时的双线性对操作和幂运算。为了便于表述，令P和E分别表示一次双线性对运算和一次幂运算，$|G_1|$表示G_1中一个元素的长度，n表示参与聚合的签名者个数。表1给出了几种适用于VANETs的无证书聚合签名方案[14−16]的性能比较。

表 1　几类无证书聚合签名方案的性能比较

方案	聚合签名长度	单个签名生成	聚合签名验证	抗联合攻击
文献[14]	$(n+1)\|G_1\|$	$4E$	$3P+3nE$	否
文献[15]	$(n+1)\|G_1\|$	$4E$	$3P+3nE$	否
文献[16]	$(n+1)\|G_1\|$	$4E$	$3P+3nE$	否
本文方案	$(n+1)\|G_1\|$	$3E$	$2nP+3nE$	是

在无证书聚合签名方案中，用户的签名私钥由2部分组成：部分私钥和秘密值。由一个半可信的第三方KGC生成用户的部分私钥，而用户独立生成自己的秘密值和对应的公钥。因为KGC无法获得用户的秘密值，所以无证书聚合签名方案能解决基于身份签名方案中的密钥托管问题。此外，用户的公钥无需证书来认证其合法性，因此无证书聚合签名方案避免了证书的生成、分发、撤销等管理操作。王方案[16]和本文提出的改进方案均是普通的无证书聚合签名方案，只需用户的公开身份和公钥来验证签名的有效性，因而有效降低了证书维护成本的复杂度，同时解决了密钥托管问题。

表1说明以上4种面向VANETs的无证书聚合签名方案[14−16]具有相同的聚合签名长度，生成单个签名所需要的计算开销也基本相同。然而，在聚合签名的验证开销方面，本文提出的改进方案高于其它3个方案；但车辆具有较强的计算能力，因此本文提出的改进方案完全适用于VANETs。更重要的是，只有本文提出的无证书聚合签名方案能抵抗联合攻击，其它3个方案均存在安全缺陷。

下面对本文提出的改进方案进行了聚合签名验证时间开销的实验分析，结果如图1所示。仿真实验的硬件环境：i7-6500的处理器和8G的内存；软件环境为Windows 10 64位操作系统及PBC-0.47-VC软件包。

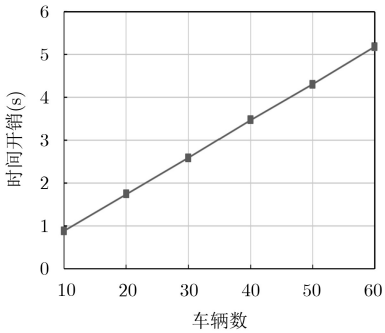

图 1 车辆密度与聚合签名的验证开销

GPS时钟已广泛应用于通信、电子商务、工业控制等领域，能为网络设备提供高精度、低成本、安全、可靠的时钟同步服务。每个车辆通过车载终端设备获取GPS卫星上的标准时间信号，确保车辆签名消息的时钟同步。从图1可知，改进的方案同时验证60辆车发送消息的有效性时，所需的时间约为5.2 s。为了保证并行车辆的通信，假定车辆通信的距离为60 m。如果只有一辆车通行时，签名的验证时间为0.104298 s，此时车辆的最大速度为575.27 m/s。如果同一时间段有60辆车同时通行时，签名的验证时间为5.180794 s，此时车辆的最大速度平均为11.58 m/s。因此，本文的改进方案满足高速移动环境下的车载通信。

8　结束语

本文分析了王方案[16]的安全性，发现该方案无法抵抗3类伪造攻击。因此，王方案[16]并不满足无证书聚合签名方案的存在不可伪造性的安全需求。为了克服这些安全缺陷，进一步提出了一个改进的无证书聚合签名方案，并在随机预言模型下证明了新方案在第1类攻击者和第2类攻击者下是存在不可伪造的。分析结果表明，新方案能有效抵抗联合攻击，实现了有条件的隐私保护。然而，新方案的签名验证开销比较大，下一步的研究任务是设计更加高效的适用于VANETs的无证书聚合签名方案。

参 考 文 献

[1] VIJAYAKUMAR P, CHANG V, DEBORAH L J, *et al*. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks[J]. *Future Generation Computer Systems*, 2018, 78(3): 943–955. doi: 10.1016/j.future.2016.11.024.

[2] REN Mengying, ZHANG Jun, KHOUKHI L, *et al*. A unified framework of clustering approach in vehicular ad

hoc networks[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2018, 19(5): 1401–1414. doi: 10.1109/TITS.2017.2727226.

[3] ARIF M and AHMAD S. Security issues in vehicular ad hoc network: a critical survey[C]. Intelligent Communication, Control and Devices, Singapore, 2018: 527–536. doi: 10.1007/978-981-10-5903-2_53.

[4] LOGESHWARI K and LAKSHMANAN L. Authenticated anonymous secure on demand routing protocol in VANET[C]. IEEE Information Communication and Embedded Systems, Chennai, India, 2017: 1–7. doi: 10.1109/ICICES.2017.8070730.

[5] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003: 416–432. doi: 10.1007/3-540-39200-9_26.

[6] XIONG Hu, GUAN Zhi, CHEN Zhong, *et al*. An efficient certificateless aggregate signature with constant pairing computations[J]. *Information Sciences*, 2013, 219(10): 225–235. doi: 10.1016/j.ins.2012.07.004.

[7] LI Jiguo, YUAN Hong, and ZHANG Yichen. Cryptanalysis and improvement for certificateless aggregate signature[J]. *Fundamenta Informaticae*, 2018, 157(1/2): 111–123. doi: 10.3233/FI-2018-1620.

[8] CHENG Lin, WEN Qiaoyan, JIN Zhengping, *et al*. Cryptanalysis and improvement of a certificateless aggregate signature scheme[J]. *Information Sciences*, 2015, 295(2): 337–346. doi: 10.1016/j.ins.2014.09.065.

[9] ZHANG Futai, SHEN Limin, and WU Ge. Notes on the security of certificateless aggregate signature schemes[J]. *Information Sciences*, 2014, 287(10): 32–37. doi: 10.1016/j.ins.2014.07.019.

[10] SHEN Limin, MA Jianfeng, LIU Ximeng, *et al*. A secure and efficient id-based aggregate signature scheme for wireless sensor networks[J]. *IEEE Internet of Things Journal*, 2017, 4(2): 546–554. doi: 10.1109/JIOT.2016.2557487.

[11] CUI Jie, ZHANG Jing, ZHONG Hong, *et al*. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. *Information Sciences*, 2018, 451(7): 1–15. doi: 10.1016/j.ins.2018.03.060.

[12] MING Yang and SHEN Xiaoqin. PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks[J]. *Sensors*, 2018, 18(5): 1573–1596. doi: 10.3390/s18051573.

[13] AZEES M, VIJAYAKUMAR P, and DEBOARH L J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2017, 18(9): 2467–2476. doi: 10.1109/TITS.2016.2634623.

[14] MALHI A K and BATRA S. An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks[J]. *Discrete Mathematics and Theoretical Computer Science*, 2015, 17(1): 317–338. doi: 10.1109/hal-01196850.

[15] KUMAR P and SHARMA V. On the security of certificateless aggregate signature scheme in vehicular ad hoc networks[C]. Soft Computing: Theories and Applications, Singapore, 2018: 715–722. doi: 10.1007/978-981-10-5687-1_63.

[16] 王大星, 滕济凯. 车载网中可证安全的无证书聚合签名算法[J]. 电子与信息学报, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

WANG Daxing and TENG Jikai. Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc network[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

[17] 俞惠芳, 杨波. 可证安全的无证书混合签密[J]. 计算机学报, 2015, 38(4): 804–813.

YU Huifang and YANG Bo. Provably secure certificateless hybrid signcryption[J]. *Chinese Journal of Computers*, 2015, 38(4): 804–813.

杨小东：男，1981年生，博士后，副教授，研究方向为应用密码学与信息安全.

麻婷春：女，1992年生，硕士生，研究方向为物联网安全.

陈春霖：女，1995年生，硕士生，研究方向为应用密码学.

王晋利：女，1993年生，硕士生，研究方向为大数据安全.

王彩芬：女，1963年生，博士，教授，研究方向为信息安全协议与网络安全.