针对车联网认证方案CPAV和ABV的安全分析

王青龙 乔 瑞 段宗涛
(长安大学信息工程学院 西安 710064)

摘 要 为了实现车联网中车辆身份的隐私保护,近年来人们提出了很多不同的匿名认证方案。Vijayakumar等于2018年提出了针对车联网的计算有效的隐私保留匿名交互认证(CPAV)及批量认证(ABV)方案,该方案可以实现车辆与RSU之间的匿名互认证以及RSU对车辆的匿名批量认证,能够抵抗假冒攻击、伪造攻击以及关联攻击,并且在必要时TA(Trusted Agency)能够追踪出已注册车辆的真实身份。文中对CPAV和ABV方案的安全性进行了深入分析,在CPAV方案中外部攻击者完全能够成功实施假冒攻击和伪造攻击,进而证明该方案不满足不可否认性,也不能实现对车辆的条件追踪。另外,因为该方案中使用的匿名身份是唯一的,导致该方案不能抵抗关联攻击,这表明该方案也不具有所谓的不可连接性。此外,还证明了批量认证方案也不能抵抗伪造攻击。

关键词 车联网,匿名认证,隐私保护,假冒攻击,伪造攻击,关联攻击,条件追踪

中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.04.028

Security Analysis on VANETs Authentication Schemes:CPAV and ABV

WANG Qing-long QIAO Rui DUAN Zong-tao
(School of Information Engineering,Chang'an University,Xi'an 710064,China)

Abstract Recently,many different anonymous authentication schemes have been proposed for privacy protection of vehicles in vehicular ad hoc networks (VANETs). In 2018,Vijayakumar et al. proposed a computationally efficient privacy preserving anonymous authentication scheme for VANETs (CPAV) and anonymous batch authentication scheme for VANETs (ABV). The schemes can achieve anonymous mutual authentication between the vehicle and the road side unit (RSU),as well as anonymous batch authentication of vehicle by the RSU,and resist bogus attacks,forgery attack,and associated attacks. TA (Trusted Agency) can track the true identity of registered vehicles when necessary. This paper deeply analyzed the security of CPAV and ABV. In CPAV scheme,the external attackers are fully able to successfully conduct bogus attack and forgery attack,which proves that this scheme does not satisfy non-repudiation,nor can it conduct conditional tracking for vehicles. In addition,because the anonymous identity used in the scheme is unique,the scheme cannot resist the associated attacks,which indicates that this scheme doesn't possess the so-called unlinkability. At last,it's also proved that the anonymous batch authentication (ABV) scheme can't resist forgery attack.

Keywords Vehicular ad hoc networks (VANETs),Anonymous authentication,Privacy preserving,Bogus attack,Forgery attack,Associated attack,Conditional tracking

1 引言

作为移动自组网技术在交通领域的应用,车联网已成为未来智能交通系统的重要组成部分[1]。利用车联网技术,可以改善道路通行状况,减少车辆事故,并且可以提供定制性娱乐服务,使得行车更安全、便捷、舒适[2]。典型的车联网系统通常包括3个不同的实体。其中,TA(Trusted Agency)为系统的建立者与管理者;OBU(On Board Unit)为车载智能设备,具有一定的存储、计算和通信能力;RSU(Road Side Unit)为安装在道路旁边的固定基础设施。在车联网中,通过OBU以及相应的DSRC(Dedicated Short Range Communication)无线通信协议[3],车辆能够实现Vehicle-to-Vehicle(V2V)和Vehicle-to-RSU(V2R)两种方式的通信,而RSU与TA之间通过有线方式进行通信[4]。由于存在很多类型的网络安全攻击,车联网自身存在广泛安全需求,如消息的可认证性和完整性、隐私保护和保密性、可用性、不可连接性、可追踪性等,因此

到稿日期:2018-02-26 返修日期:2018-05-24 本文受陕西省重点科技创新团队项目(2017KCT-29),陕西省重点研发计划项目(2017GY-072,2018GY-136,2018GY-022 ,2018GY-032),陕西省国际科技合作计划项目(2017KW-015),陕西省工业科技攻关项目(2015GY002)资助。

王青龙(1970—),男,博士,副教授,主要研究方向为公钥密码学及应用,E-mail:qlwang@chd.edu.cn(通信作者);**乔 瑞**(1994—),女,硕士生,主要研究方向为车联网信息安全;**段宗涛**(1977—),男,博士,教授,主要研究方向为可信交通信息服务。

要保护车辆系统中的隐私。常见的隐私保护主要包括:车辆身份的隐私、服务提供商数据的隐私和车辆位置信息的隐私[5]。

根据 IEEE802.11P 标准,车辆以 100～300ms 为间隔,周期性地对外广播信息,这些信息既包括天气条件、拥塞状况等交通信息,也包括车辆位置、行驶速度等信息。为了保障这些信息的真实性和可靠性,接收者需要对广播信息的车辆身份进行认证,保证接收的信息来自于合法授权车辆。另外,对车联网中很多应用而言,车辆也需要将自己的身份以明文形式发送给 RSU 或其他车辆。但是,车辆身份属于高度敏感信息,与司机的隐私密切相关[5]。例如,攻击者利用消息中包含的身份信息可以关联同一个车辆发送的不同消息(称为关联攻击),利用这些消息的位置信息很容易重构出车辆的行驶轨迹,进而推断出司机的家庭地址、工作场所以及出行习惯等个人隐私,通过对这些隐私信息进行进一步分析,攻击者也容易确定用户的真实身份。隐私信息如果得不到很好的保护,车联网就不可能被大规模应用。因此,车联网在实际应用中必须考虑如何保护车辆的身份信息,现有的大多方法中车辆除拥有一个真实身份外,另有大量的匿名身份,每次需要时车辆只需出示匿名身份而不是真实身份,从而达到对身份信息的保护。但是,另一方面,有些车辆可能恶意利用匿名身份,有目的地提供虚假的道路信息来误导其他车辆,以使自己获得更多的道路资源。为了阻止这种情况的发生,恶意行为车辆的真实身份在必要时能够被追踪揭示,也就是车辆的真实身份应具有可追踪性。事实上,关于车辆身份认证与隐私保护的研究仍是车联网研究的一个热点问题,此处的挑战是如何有效地解决好(隐私)匿名性与可追踪性之间的矛盾。

在 PPA(隐私保留认证)的实现上主要有几种不同的方式。

1)采用环签名机制。这类方案的主要问题是 TA 需要参与环签名的全部成员协助才能完成对恶意车辆的追踪,实践中难以实现[6-7]。

2)采用群签名机制。利用群签名自身具有的匿名性与可追踪性实现对车辆身份隐私的保护[8-9],但是这类方案存在签名长度大和验证时间长的不足,同时车辆的快速移动性使得群主难以对群成员进行有效的动态管理。

3)基于身份的公钥密码机制。文献[10]提出了一种基于身份的 PPA 方案,该方案的主要思想是将系统主密钥存储在车辆的 TPD 中,利用存储的系统主密钥,每个车辆都可以自己生成足够的匿名证书,从而避免复杂的证书管理问题。该方案的不足是对 TPD 的安全性假设太强,其假设攻击者不能够从 TPD 处获得任何存储信息。但实际上,利用旁路攻击,攻击者有可能从 TPD 处得到大量的信息[11]。2011 年,Zhang 等[12]采用基于身份的聚合签名技术和秘密共享技术提出了一个 PPA 方案,与文献[10]一样,通过存放在 TPD 中的系统主密钥,车辆能够自己生成需要的匿名证书。2017 年,Zhang 等[13]提出了另一种改进的方案,该改进方案不再把系统主密钥存储在 TPD 中,但 RSU 对车辆首次进行认证时需要 TA 的参与才能完成,可能导致 TA 成为认证过程中的瓶颈。

2014 年,Zhu 等[14]提出了一种高效的 PPA 方案,该方案没有使用匿名证书,其保护身份隐私的思路是 RSU 对新进入的车辆进行认证,认证通过则发送当前群密钥给车辆,车辆利用该群密钥计算所发送消息的 *HMAC* 值。对于拥有同样群密钥的其他车辆,车辆能够通过该 *HMAC* 值验证消息的完整性以及发送者的可靠性。但是方案中 RSU 需要通过车辆的真实身份对车辆进行认证,因为 RSU 并不是可信实体,真实身份的泄露会对用户的隐私带来如前所述的潜在威胁;另外,作者声称 RSU 能够追踪出恶意车辆的真实身份,但并没有描述具体的追踪过程。2016 年,文献[15-16]分别提出了两种 PPA 方案,为了实现身份隐私保护,两种方案都假设车辆事先从 TA 处获得了需要的匿名证书,因此都存在与下述基于 PKI 的方案类似的不足。

4)基于 PKI(Public Key Infrastructure)机制[17-19]。这类方案中,TA 需要为每个车辆颁发多个匿名证书,匿名证书不包含与车辆真实身份有关的任何信息,为了防止关联追踪导致隐私泄露,每个匿名证书只能少量并且有限次被使用,因此车辆需要定期或不定期获得新的匿名证书。为了追踪车辆的真实身份,TA 需要存储车辆当前拥有的全部匿名证书,同时为了阻止恶意车辆继续使用拥有的匿名证书发布信息,TA 需将这些匿名证书公布到系统的证书撤销列表中以供其他车辆查询。该类方案的关键是如何实现匿名证书的高效更新过程以及对证书撤销列表的高效查询与维护。

Vijayakumar 等[20]在 *Future Generation Computer Systems* 上发表了一篇针对车联网计算有效的隐私保留匿名交互认证(CPAV)及批量认证方案(ABV)的文章,他们的方案中存在多个 TA,每个 TA 负责一个区域,车辆需要使用自己的真实身份向本地 TA 进行注册。方案中车辆的匿名证书由车辆自己生成,并利用该匿名证书完成对消息的签名。车辆进入一个区域时,需要激活 TPD 来得到自己的私钥和公钥,从而进行匿名交流。与其他方案不同的是,该方案既不需要在 TPD 中存储系统主密钥,非本地车辆的认证也不需要车辆注册地 TA 的参与。同时,该方案还支持对 RSU 隐私的保护,也就是 RSU 也能够使用自己生成的匿名证书向车辆证明自己的身份,而不是使用 RSU 的真实身份,这一点在已有 PPA 方案中鲜有考虑。作者在安全分析部分给出了 7 个特性:特性 1 证明 CPAV 方案在信息传输过程中可以保障信息的完整性和信息来源的可靠性;特性 2 证明 CPAV 方案可以实现车辆的条件隐私保护;特性 3 证明 CPAV 方案可以实现车辆真实身份的匿名性;特性 4 证明 CPAV 方案可以消息的不可连接性;特性 5 表明 CPAV 方案可以实现不可否认性;特性 6 表明 CPAV 方案可以实现抵抗假冒消息攻击;特性 7 表明 CPAV 方案可以实现不可伪造性。但是仔细分析后发现这些特性都是不成立的,表明他们的方案是完全不安全的。

本文对文献[20]的安全性进行了深入分析,证明该方案存在严重的安全漏洞。1)文献[20]假设车辆只有通过注册才能得到有效的假名,但本文证明了攻击者完全能够伪造有效的假名,而不需要向本地 TA 注册以获得必要的消息,利用该假名,攻击者可以发送任何消息,且消息能够通过其他车辆和

RSU 的正常验证，即攻击者能够成功实施伪造攻击。由于车辆没有进行注册，TA 没有关于车辆的任何消息，因此攻击者能够逃避 TA 的追踪。2)作者假设攻击者只有得到车辆的私钥($upuk_j$)和 TA 的秘密值(m,n)才能成功假冒车辆的真实身份以进行假冒攻击，但我们证明攻击者只要得到车辆广播的任何一个消息，就可以从该消息中获得车辆的假名，并以假名发送任何消息，从而成功实施假冒攻击。

针对文献[20]提出的相关方案，本文第 2 节对 CPAV 方案进行简单介绍；第 3 节对 CPAV 方案的安全性进行详细分析；第 4 节介绍 ABV 方案并对其安全性进行分析；最后总结全文。

2　CPVA 方案介绍

本文的安全性分析仅针对车辆之间的匿名认证，因此只介绍文献[20]的 CPAV 方案中与车辆相关的部分内容，其余内容可以参考原文。

2.1　系统初始化

该方案是基于双线性对运算的操作方案，TA 从双线性对运算参数(G_1,G_2,G_T,e,q)中产生系统参数。其中 G_1,G_2,G_T 是 3 个阶数都为 q 的乘法循环群，g_1 是 G_1 的生成元，g_2 是 G_2 的生成元，ϕ 是从 G_2 到 G_1 的同构，使得 $\phi(g_2)=g_1$。双线性映射 $e:G_1\times G_2=G_T$。TA 首先选择两个随机数 m，$n\in Z_q^*$和主私钥 $prk\in Z_q^*$，计算出相应的公钥 $puk=g_1^{prk+n}$。同时，TA 选择一个安全的哈希函数：$H:\{0,1\}^*\rightarrow Z_q^*$。最后，TA 公布系统参数 $param=(q,G_1,G_2,G_T,e,g_1,g_2,puk,H)$。

2.2　注册

1)在注册阶段，TA 首先选择一个随机数 $uprk_j\in Z_q^*$ 作为车辆的私钥，同时计算产生相应的公钥 $upuk_j=g_1^{uprk_j+a}$(其中，a 为随机数且 $a\in Z_q^*$)。然后，每个车辆需要在 TA 上注册自己的防篡改设备 TPD(Tamper Proof Device)。在注册 TPD 的过程中，TA 首先要分配一个密钥 $pw_j=g_1^{m+n}$ 并且计算出激活密钥 $s=g_1^{uprk_j+m+n+prk}$，其中密钥 pw_j 和密钥 s 被用来激活 TPD 以便得到私钥 $uprk_j$ 和公钥 $upuk_j$。最后，TA 计算出一个重加密密钥 $REK_j=pw_j*upuk_j$，该密钥被用来提取激活密钥 s。车辆得到激活密钥后就能够使用它的 pw_j 和 s 来激活 TPD。

2)TA 生成相应车辆的许可证 VL_{V_j}，$VL_{V_j}=upuk_j^m*g_1^m$，用于追踪车辆的真实身份。

3)TA 在车辆注册时分配原始身份 $ID-V_j$，然后生成每个车辆的伪身份 DID_{V_j}，其中 $DID_{V_j}=g_1^{d_1+prk+n}\bmod q$($d_1$ 为随机数且 $d_1\in Z_q^*$)。伪身份用于保护车辆的真实身份不被泄露。TA 将(DID_{V_j}，$ID-V_j$，$upuk_j^{m*n}$)保存在追踪列表中用于后续的条件追踪。

4)TA 在车辆的 TPD 中提前下载 $uprk_j$ 和 $upuk_j$，并且在成功完成注册后将 DID_{V_j}，pw_j，VL_{V_j}，REK 和 F_j 提供给车辆($F_j=g_1^{-d_1}\bmod q$)。

2.3　安全激活密钥分发

在 VANET 系统中，车辆 V_j 需要激活 TPD 以得到 $uprk_j$ 和 $upuk_j$，具体过程如下：

1)V_j 使用 TA 的公钥 puk 来加密它的许可证 VL_{V_j}(即 $E_{puk}(VL_{V_j})$)，并通过首次遇到的 RSU 将 $E_{puk}(VL_{V_j})$ 发送给 TA。TA 接收到该加密值后使用自己的私钥 prk 进行解密得到 VL_{V_j}，并且计算出私钥消息 $SM=s*pw_j*upuk_j$。

2)TA 通过 R_j 将 $E_{pw_j}(SM)$发送给 V_j，在接收该值之后，V_j 通过解密 $E_{pw_j}(SM)$得到 SM，最后从下列等式中提取 TPD 的激活密钥：

$$\text{激活密钥}=\frac{SM}{REK_j}=\frac{s*pw_j*upuk_j}{pw_j*upuk_j}=s$$

2.4　V2V 匿名多方认证

V2V 匿名多方认证指的是一个车辆 V_i 给另一个车辆 V_j 发送消息时的认证情形。例如，V_1 需要进入 V_2 的区域时，它通过临时的匿名密钥进行认证，一旦 V_1 离开 V_2 的区域进入到另一个车辆所在的区域时便需要进行新的认证。具体的认证过程如下：

1)车辆 V_j 首先从 Z_N^* 中选取一个随机数 x_j 并将其作为临时密钥，同时计算出相应的公钥 $y_j=g_1^{x_j+uprk_j}$。

2)车辆生成自己的临时匿名证书，随机选择 $h_1\in Z_q^*$，并且计算 $s_1=g_1^{uprk_j}$，$s_2=g_1^{uprk_j}+h_1$。

①计算出挑战值：$C=H(puk\parallel DID_{V_j}\parallel y_j\parallel s_1\parallel s_2)$。

②生成临时匿名证书：$cer_j=\{F_j\parallel DID_{V_j}\parallel y_j\parallel s_1'\parallel s_2'\parallel C\}$。其中，$s_1'=g_1^{x_j-h_1}$，$s_2'=\frac{1}{g_1^{x_j}}$。

3)车辆使用临时的 x_j，y_j 和 cer_j 进行匿名认证，为了保护消息 M 的完整性，车辆计算出签名 $\delta_j=g_2^{\frac{1}{x_j+uprk_j+H(M)}}$，并且将 $msg=(M\parallel\delta_j\parallel y_j\parallel cer_j\parallel VL_{V_j})$广播给其他所有车辆。

4)当接收到消息 M 后，接收者首先计算 $N_j=F_j\times DID_{V_j}$，$s_a=y_j\times s_2'$，$s_b=\frac{y_j}{s_1'}$；然后计算 $C'=H(N_j\parallel DID_{V_j}\parallel y_j\parallel s_a\parallel s_b)$。由原文证明可知：

$$N_j=F_j\times DID_{V_j}=puk \tag{1}$$

$$s_a=y_j\times s_2'=s_1 \tag{2}$$

$$s_b=\frac{y_j}{s_1'}=s_2 \tag{3}$$

这意味着：

$$C'=C \tag{4}$$

5)当证书通过验证后，接收者再通过下列等式来验证消息 M 的完整性：

$$e(y_j\cdot g_1^{H(M)},\delta_j)=e(g_1,g_2) \tag{5}$$

由式(4)和式(5)可知该消息能够通过验证。

6)条件追踪。如果基于许可证 VL_{V_j} 的消息 M 有误，TA 计算：

$$\frac{(VL_{V_j})^n}{g_1^{m*n}}=\frac{(upuk_j^m*g_1^m)^n}{g_1^{m*n}}$$

$$=\frac{upuk_j^{m*n} * g_1^{m*n}}{g_1^{m*n}}$$

$$=upuk_j^{m*n} \tag{6}$$

根据式(6)的结果,TA 在追踪列表中查找与 $upuk_j^{m*n}$ 对应的记录($ID-V_j$,$upuk_j^{m*n}$),从而追踪出消息发送者的真实身份为 $ID-V_j$。

3 对 CPAV 方案的攻击

3.1 假冒消息攻击

文献[20]声称他们的方案能够抵抗假冒消息攻击,也就是攻击者不能够假冒任何一个合法车辆发送消息,但我们发现攻击者能够利用截获的合法车辆发送的消息成功假冒该车辆并且能够发送任意的合法消息,具体攻击过程如下。

步骤 1 假设攻击者首先截获的合法消息为 $msg=(M \| \delta_j \| y_j \| cer_j \| VL_{V_j})$,则从中提取出 cer_j 和 VL_{V_j},然后从 $cer_j=\{F_j \| DID_{V_j} \| y_j \| s_1' \| s_2' \| C\}$中获得 F_j 和 DID_{V_j}。

步骤 2 攻击者随机选取 $\lambda,\alpha_1 \in Z_q^*$,$\gamma_j \in Z_N^*$,并将 γ_j 作为临时私钥。计算 $s_1=g_1^{\lambda}$,$s_2=g_1^{\lambda+\alpha_1}$,$y_j=g_1^{\gamma_j+\lambda}$。

步骤 3 计算出挑战值 $C_1=H(puk \| DID_{V_j} \| y_j \| s_1 \| s_2)$。

步骤 4 生成匿名证书 $cer=\{F_j \| DID_{V_j} \| y_j \| s_1' \| s_2' \| C_1\}$,其中 $s_1'=g_1^{\gamma_j-\alpha_1}$,$s_2'=\frac{1}{g_1^{\gamma_j}}$。

步骤 5 计算出任意消息 M_j 的签名 $\delta_j=g_2^{\frac{1}{\gamma_j+\lambda+H(M)}}$,并广播 $Msg=(M_j \| \alpha_j \| y_j \| cer \| VL_{V_j})$。

消息 Msg 被广播出来之后,接收者将通过以下步骤进行验证。

步骤 1 计算 $N_j=F_j \times DID_{V_j}$,$s_a=y_j \times s_2'$,$s_b=\frac{y_j}{s_1'}$。

步骤 2 计算 $C_1'=H(N_j \| DID_{V_j} \| y_j \| s_a \| s_b)$。由于

$$s_a=y_j \times s_2'=g_1^{\gamma_j+\lambda} \times \frac{1}{g_1^{\gamma_j}}=g_1^{\lambda}=s_1 \tag{7}$$

$$s_b=\frac{y_j}{s_1'}=\frac{g_1^{\gamma_j+\lambda}}{g_1^{\gamma_j-\alpha_1}}=g_1^{\lambda+\alpha_1}=s_2 \tag{8}$$

F_j 和 DID_{V_j} 是从合法车辆的匿名证书 $cer_j=\{F_j \| DID_{V_j} \| y_j \| s_1' \| s_2' \| C\}$中提取的,因此显然有:

$$N_j=F_j \times DID_{V_j}=puk \tag{9}$$

综合式(7)-式(9)可得:

$$C_1=C_1' \tag{10}$$

步骤 3 当证书 cer 通过检验后,再通过验证 $e(y_j \cdot g_1^{H(M)},\delta_j)=e(g_1,g_2)$是否成立来检验消息 M 的完整性,显然有:

$$\begin{aligned} e(y_j \cdot g_1^{H(M)},\delta_j)&=e(g_1^{\gamma_j+\lambda} \cdot g_1^{H(M)},g_2^{\frac{1}{\gamma_j+\lambda+H(M)}}) \\ &=e(g_1^{\gamma_j+\lambda+H(M)} \cdot g_2^{\frac{1}{\gamma_j+\lambda+H(M)}}) \\ &=e(g_1,g_2) \end{aligned} \tag{11}$$

由式(10)和式(11)可得假冒消息能够通过正常验证。

步骤 4 TA 对攻击者发送的假冒消息进行追踪时,从假冒消息中获得 VL_{V_j},显然有:

$$\frac{(VL_{V_j})^n}{g_1^{m*n}}=upuk_j^{m*n} \tag{12}$$

最后根据式(12)的结果在追踪列表中查找与 $upuk_j^{m*n}$ 对应的记录($ID-V_j$,$upuk_j^{m*n}$),从而认为假冒消息的发送者为合法车辆 $ID-V_j$。

从上述验证过程中可知攻击者能够成功冒充一个合法车辆发布任意消息。

3.2 伪造消息攻击

文献[20]声称他们的方案能够抵抗伪造消息攻击,也就是攻击者无法生成有效的匿名身份并发送合法消息,但是我们发现攻击者只需要利用公开的系统参数就能够实施伪造消息攻击,并且能够成功逃避 TA 的追踪。

步骤 1 攻击者利用系统公钥 puk 计算 $DID_{V_t}=g_1^{x_1} \cdot puk$,$F_t=g_1^{-x_1} \bmod q$(其中 x_1 为随机数且 $x_1 \in Z_q^*$)。攻击者再选取随机数 $\eta_1 \in Z_q^*$,并令 $VL_{V_t}=\eta_1$。

步骤 2 随机选取 $\lambda_t,\alpha_t \in Z_q^*$,$\gamma_t \in Z_N^*$(其中 γ_t 作为临时私钥),计算 $s_{1t}=g_1^{\lambda_t}$,$s_{2t}=g_1^{\lambda_t+\alpha_t}$,$y_t=g_1^{\gamma_t+\lambda_t}$。

步骤 3 计算出挑战值 $C_t=H(puk \| DID_{V_t} \| y_t \| s_{1t} \| s_{2t})$,然后计算 $s_{1t}'=g_1^{\gamma_t-\alpha_t}{}_1$,$s_{2t}'=\frac{1}{g_1^{\gamma_t}}$。

步骤 4 生成匿名证书 $cer_t=\{F_t \| DID_{V_t} \| y_t \| s_{1t}' \| s_{2t}' \| C_t\}$。

步骤 5 计算出任意消息 M 的签名 $\delta_t=g_2^{\frac{1}{\gamma_t+\lambda_t+H(M)}}$,并广播出 $MSG=(M_t \| \delta_t \| y_t \| cer_t \| VL_{V_t})$。

消息 MSG 被广播出来之后,接收者将通过以下步骤对其进行验证:

步骤 1 计算 $N_t=F_t \times DID_{V_t}$,$s_{at}=y_t \times s_{2t}'$,$s_{bt}=\frac{y_t}{s_{1t}'}$。

步骤 2 计算 $C_t'=H(N_t \| DID_{V_t} \| y_t \| s_{at} \| s_{bt})$。由于

$$s_{at}=y_t \times s_{2t}'=g_1^{\gamma_t+\lambda_t} \times \frac{1}{g_1^{\gamma_t}}=g_1^{\lambda_t}=s_{1t} \tag{13}$$

$$s_{bt}=\frac{y_t}{s_{1t}'}=\frac{g_1^{\gamma_t+\lambda_t}}{g_1^{\gamma_t-\alpha_t}}=g_1^{\gamma_t+\alpha_t}=s_{2t} \tag{14}$$

$$N_t=F_t \times DID_{V_t}=g_1^{-x_1} \cdot g_1^{x_1} \cdot puk=puk \tag{15}$$

因此可得出:

$$C_t=C_t' \tag{16}$$

步骤 3 当证书 cer_t 通过检验后,再通过验证 $e(y_t \cdot g_1^{H(M)},\delta_t)=e(g_1,g_2)$是否成立来检验消息 M_t 的完整性,显然有:

$$\begin{aligned} &e(y_t \cdot g_1^{H(M)},\delta_t) \\ &=e(g_1^{\gamma_t+\lambda_t} \cdot g_1^{H(M)},g_2^{\frac{1}{\gamma_t+\lambda_t+H(M)}}) \\ &=e(g_1^{\gamma_t+\lambda_t+H(M)} \cdot g_2^{\frac{1}{\gamma_t+\lambda_t+H(M)}}) \\ &=e(g_1,g_2) \end{aligned} \tag{17}$$

由式(16)和式(17)可知,伪造消息能够通过验证。

步骤 4 TA 需要追踪上述消息发送者的真实身份时,计算:

$$\frac{(VL_{V_t})^n}{g_1^{m*n}}=\frac{(\eta_1)^n}{g_1^{m*n}} \tag{18}$$

由于攻击者并没有进行注册，η_2 的值并未存储在追踪列表中，因此 TA 查找不到与 $\frac{(\eta_1)^n}{g_1^{m**n}}$ 相对应的追踪记录，从而无法追踪攻击者的真实身份，也就是攻击者能够逃避 TA 的追踪。

以上攻击过程表明：CPAV 方案不能抵抗伪造消息攻击。

由于 3.1 节和 3.2 节的假冒攻击和伪造攻击不成立，因此原方案声称的不可伪造性和不可否认性也都不成立。

3.3 关联攻击

文献[20]中提出由于 δ_j 和证书 $cert_j$ 的计算都是基于随机选择的临时私钥计算得到的，因此攻击者很难确定两个消息是否由同一个车辆发送，但是我们可以证明该结论是错误的。

从车辆广播的证书 $cer_j=\{F_j \parallel DID_{V_j} \parallel y_j \parallel s_1' \parallel s_2' \parallel C\}$ 中可以看出车辆的伪身份 DID_{V_j} 是唯一的，并且可以从发送的公开消息中获得，攻击者利用伪身份的唯一性能够关联同一合法车辆发送的不同消息，从而可以实施关联攻击，因此可以得出文献[20]中的不可连接性是不成立的。通过关联攻击，攻击者能够重构出车辆的行驶轨迹，进而推断出司机的家庭住址、工作场所以及出行习惯等个人隐私，进而容易确定车辆的真实身份。

4 对车辆批认证方案的介绍及攻击

4.1 ABV 方案

文献[20]中车辆的 ABV(匿名批量用户认证)方案与 CPAV 方案存在差别。在 ABV 方案中能够对批量车辆同时进行认证，具体认证过程如下：

1)车辆 V_j 注册时，TA 为 V_j 生成用于批量认证的密钥 VBK_j($VBK_j=g_1^{prk+n+uprk_j}$)以及相应的追踪密钥 BTK_j($BTK_j=g_1^{-prk-n}$)。TA 也为每个 RSU 生成批量密钥 RBK_j($RBK_j=g_1^{prk+n}=puk$)。

2)进行批量认证时，车辆 V_j 选择一个随机数 d_j($d_j\in Z_N^*$)作为临时私钥，分别计算公钥 $c_j=g_1^{d_j}$，$M_j=g_1^{-uprk_j+d_j}$ 和 $Z_j=VBK_jM_j$。

3)车辆 V_j 计算 $L_j=H(c_j \parallel Z_j)$。

4)Z_j 计算完成后，车辆 V_j 生成一个元组$\{Z_j,c_j,L_j\}$。

5)假设 $V_1,V_2,\cdots,V_b$ 为批量认证的车辆，则每个车辆分别发送$\{Z_1,c_1,L_1,BTK_1\}$，$\{Z_2,c_2,L_2,BTK_2\}$，…，$\{Z_b,c_b,L_b,BTK_b\}$给 RSU。

6)收到 b 个批量认证消息$\{Z_i,c_i,L_i,BTK_i\}$($i=1,2,\cdots,b$)后，RSU 首先验证每个元组中 $L_j=H(c_j \parallel Z_j)$是否成立。

7)若验证通过，RSU 计算 $Z=\prod_{i=1}^{b}Z_b$ 和 $c=\prod_{i=1}^{b}c_b$，并验证 $(RBK_j)^b=Z/c$ 是否成立。若成立，则批量认证成功；否则终止通信。

8)条件追踪。为了防止在批量认证过程中出现由于单个车辆行为不当而造成 RSUs 无法获得$(RBK_j)^b$ 的情况，RSU 需要分别检查等式 $c_j=Z_j\cdot BTK_j$ 是否成立。若等式成立，则该车辆被视为合法的；否则该车辆将从 VANET 系统中被移除。

4.2 ABV(批量车辆认证)方案的伪造攻击

1)攻击者 V_t 首先选择一个随机数 $r_t\in Z_N^*$ 作为临时私钥，然后计算出相应的公钥 $c_t=g_1^{r_t}$ 和 $M_t=g_1^{-\lambda_t+r_t}$(其中 λ_t 是一个随机数且 $\lambda_t\in Z_q^*$)。攻击者生成自己的追踪密钥 BTK_t($BTK_t=puk^{-1}=g^{-(prk+n)}$)和用于批量认证的密钥 VBK_t($VBK_t=puk\cdot g_1^{\lambda_t}$)。

2)攻击者 V_t 计算 $Z_t=VBK_tM_t$。

3)攻击者 V_t 计算：

$$L_t=H(c_t \parallel Z_t) \tag{19}$$

4)生成元组$\{Z_t,c_t,L_t\}$。

5)对于包含攻击车辆 V_t 在内的批量认证车辆 V_1，V_2，…，V_b，分别发送$\{Z_1,c_1,L_1,BTK_1\}$，$\{Z_2,c_2,L_2,BTK_2\}$，…，$\{Z_b,c_b,L_b,BTK_b\}$给 RSU。

6)RSU 首先验证 $L_t=H(c_t \parallel Z_t)$是否成立，由式(19)可知攻击者发送的元组显然能够通过批量验证。

7)R_j 计算 $Z=\prod_{i=1}^{b}Z_b$ 和 $c=\prod_{i=1}^{b}c_b$。

8)R_j 检验$(RBK_j)^b=Z/c$ 是否成立，可得：

$$\begin{aligned}RHS&=\frac{\prod_{i=1}^{b}Z_b}{\prod_{i=1}^{b}c_b}=\frac{VBK_1\cdot M_1\cdot VBK_2\cdot M_2\cdot\cdots\cdot VBK_b\cdot M_b}{c_1c_2\cdots c_b}\\&=\frac{puk\cdot g_1^{\lambda_1}\cdot g_1^{-\lambda_1+r_1}\cdot puk\cdot g_1^{\lambda_2}\cdot g_1^{-\lambda_2+r_2}\cdot\cdots\cdot puk\cdot g_1^{\lambda_b}\cdot g_1^{-\lambda_b+r_b}}{g_1^{r_1}\cdot g_1^{r_2}\cdot\cdots\cdot g_1^{r_b}}\\&=puk^b=(RBK_j)^b=LHS\end{aligned} \tag{20}$$

式(20)表明包含攻击车辆在内的批量认证能成功通过验证。

9)条件追踪。当 RSU 进行条件追踪时，有：

$$\begin{aligned}c_t&=Z_t\cdot BTK_t\\&=VBK_t\cdot M_t\cdot BTK_t\\&=puk\cdot g_1^{\lambda_t}\cdot g_1^{-\lambda_t+r_t}\cdot puk^{-1}\\&=g_1^{r_t}=c_t\end{aligned} \tag{21}$$

由式(21)可知攻击者可以通过 RSU 的追踪检验，即攻击者被视为合法车辆。

上述攻击过程表明攻击者能够成功伪造成合法车辆并通过批量认证，因此文献[20]中批量车辆认证过程也是不安全的。

结束语　本文对最近发表的车联网匿名认证方案[20]的安全性进行了全面分析，结果表明该方案中的 CPAV 不能抵抗假冒攻击、伪造攻击和关联攻击，因此其声称的不可连接性、不可否认性及条件追踪都是不正确的；同时方案中针对车辆的 ABV(批量认证方案)也不能够抵抗伪造攻击，表明其关于车辆的批量认证也是不安全的。

参 考 文 献

[1] AZIMI R, BHATIA G, RAJKUMAR R, et al. Vehicular networks for collision avoidance at intersections[C]// SAE world congress & exhibition. Carnegie Mellon University: Priyantha Mudalige, 2011: 406-416.

[2] TANGADE S S, MANVI S S. A survey on attacks, security and trust management solutions in VANETs[C]// 4th IEEE International Conference on Computing, Communications nad Networking Technologies. Tiruchengode: IEEE Computer Society, 2013: 105-112.

[3] JIANG S R, ZHU X Y, WANG L M. An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs [J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2205.

[4] AI-SULTAN S M, AI-DOORI M H, AI-BAYATTI A, et al. A comprehensive survey on vehicular ad hoc network[J]. Journal of Network and Computer Applications, 2014, 37(1): 380-392.

[5] QU F Z, WU Z H, WANG F Y, et al. A security and privacy review of VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(6): 2985-2996.

[6] ZENG S K, HUANG Y, LIU X W. Privacy-preserving Communication for VANETs with Conditionally Anonymous Ring Signature[J]. International Journal of Network Security, 2015, 9(12): 135-141.

[7] JIANG Y C, JI Y, LIU T H. An Anonymous Communication Scheme based on Ring Signature in VANETs[OL]. https://arxiv.org/pdf/1410.1639.pdf.

[8] 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.

[9] ZHANG L, WU Q, SOLANS A, et al. A scalable robust authentication protocol for secure vehicular communications[J]. IEEE Transactions On Vehicular Technology, 2009, 59(4): 1606-1617.

[10] ZHANG C X, LU R X, LIN X D, et al. An efficient identity based batch verification scheme for vehicular sensor networks [C]// International Conference on Computer Communications-2008. Phoenix: IEEE Press, 2008: 816-824.

[11] KILTZ E, PIETRZAK K. Leakage resilient elgamalencryption [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer: Computer Science, 2010: 595-612.

[12] ZHANG L, WU Q H, QIN B, et al. APPA: Aggregate privacy-preserving authentication in vehicular ad hoc networks[C]// International Conference on Information Security. Springer: Computer Science, 2011: 293-308.

[13] ZHANG L, WU Q H, DOMINGO-FERRER J, et al. Distributed Aggregate Privacy-Preserving Authentication in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(3): 516-526.

[14] ZHU X Y, JIANG S R, WANG L G, et al. Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks[J]. IEEE Transactions on Vehicular Technology, 2014, 63(2): 907-918.

[15] JIANG S R, ZHU X Y, WANG L M. An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs [J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.

[16] LO N W, TSAI J L. An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5): 1319-1328.

[17] LU R, LIN X, ZHU H, et al. ECPP: Efficient conditional privacy-preservation protocol for secure vehicular communications [C]// IEEE Conference on Computer Communications INFOCOM 2008. Phoenix: IEEE Press, 2008: 1229-1237.

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

[19] STUDER A, SHI E, BAI F, et al. Tacking together Efficient Authentication, Revocation, and Privacy in VANETs[C]// Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON 2009). Rome: IEEE Press, 2009: 22-26.

[20] VIJAYAKUMAR P, CHANG V, JEGATHA DEBORAH L, et al. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks[J]. Future Generation Computer System, 2018, 78(3): 943-995.