车载网中可抵制合谋攻击的批量认证方案

陆 杰 宋香梅 韩 牟 周从华
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 由于无线网络本身的脆弱性和开放性,车载网很容易受到各种攻击和破坏,面临着信息伪造、篡改攻击与重放攻击等安全威胁。消息认证是保障车载网安全的有效技术之一,但是车载网规模较大、涉及的通信实体数量多且移动速度非常快的特点要求消息能够被快速认证。目前,b-SPECS+是公认的最好的消息批量认证的方案,具有基于软件、通信开销小、安全性高、批量认证的特点,但是该方案不能够抵制固定路边设备和车辆的合谋攻击。基于b-SPECS+提出了一个基于假名验证公钥的批量认证方案,并证明了该方案能够很好地抵制合谋攻击。性能分析结果表明,与b-SPECS+相比,所提方案不仅具有b-SPECS+的特点,而且在认证时延方面,认证的消息越多,其相对于其他方案的耗时越短。

关键词 RSU辅助认证,匿名认证,合谋抵制,车辆撤销
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.6.028

Batch Verification Scheme Defensing Collusive Attack in VANET

LU Jie SONG Xiang-mei HAN Mou ZHOU Cong-hua
(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract Owning to vulnerabilities and openness of the wireless networks, Vehicular ad-hoc networks (VANET) are vulnerable to attacks, such as the bogus information attack and the message replay attacks. Message authentication is one of the effective techniques to solve these problems. Obviously VANET consists of a huge number of fast moving vehicles, thus messages need to be verified rapidly. Recently, b-SPECS+ has became the best scheme on batch verification, which provids a software-based solution to satisfy the privacy requirement, gives lower message overhead and verifies message in batch. However, it suffers from the collusion attack executed by the roadside unit and the on-board unit. In this paper, we provided a pseudonymous verification public key based scheme that can solve collusion attack problem. Our solution has a higher rate than b-SPECS+ in the message verification.

Keywords RSU-aided verification, Anonymous verification, Collusion resistance, Revocability

1 引言

车载自组网(VehicularAd Hoc Networks, VANET)作为一种能够给车辆提供宽带通信的新型网络技术,将会给交通系统带来革命性的变化,它创造性地将自组网技术应用于车辆间通信,使得司机能够在超视距的范围内获得其它车辆的状况信息(如车速、转向、位置、刹车等)和实时路况信息。车载自组网的部署和实施将最大限度地减少或避免交通事故,而且可以提高道路通行效率,能够使司乘人员的旅行更加安全和舒适。由于其具有巨大的社会效益和潜在经济利益,这种网络近年来吸引了广泛的关注。日本、美国和欧盟的政府组织、汽车企业和研究机构等相继启动了一批大型的科研项目,如C-ITS[1],iTETRIS[2],COOPERS[3]等。在美国,联邦通信委会已经为车载自组网分配了75MHz的专用带宽,也称为专用短距离无通信协议(DSRC)[4,5];国际电子电气工程师协会(IEEE)专门为车载自组网定义了MAC层和物理层协议802.11p。

根据DSRC协议,每辆车要周期性地广播自己的常规车辆信息,包括当前行驶速度、车辆位置、方向、加速或减速、交通状况和交通事故等,以便在非正常情况下,比如出现了交通堵塞、交通事故和紧急刹车等,其它车辆在收到这些信息后能尽早采取行动。但由于无线网络本身的脆弱性和开放性,车载网也很容易受到攻击和破坏,面临着信息伪造、篡改攻击、重放攻击、女巫攻击和拒绝服务攻击等问题,因此车载自组网的部署和实施必须满足信息的可认证性、完整性和不可否认性等安全需求。就目前的信息安全技术而言,要达到这些安全需求,离不开消息的认证[6-9],同时较高的安全要求通常会导致认证效率低下。但是车载网中车辆移动速度较快,必须保证消息认证的效率,否则安全消息得不到及时的认证,丢包率将会上升,从而导致通信效率低下。消息的批量认证是目

到稿日期:2015-05-12 返修日期:2016-08-23 本文受国家自然科学基金(61300288,61300229),江苏省六大人才高峰项目(WLW-012)资助。
陆 杰(1990-),男,硕士生,主要研究方向为车载网隐私保护,E-mail:lujie112211@163.com;宋香梅(1979-),女,讲师,主要研究方向为信息安全、隐通道;韩 牟(1980-),女,副教授,主要研究方向为编码学、抗量子公钥密码学;周从华(1978-),男,副教授,主要研究方向为大数据分析与应用技术、数据与系统安全。

前提高认证效率的有效方法。

Zhang 等[10]提出了基于身份的批量验证(IBV)方案,该方案能够同时验证一批签名消息,很好地提高了系统性能,但该方案太依赖于防篡改装置,并且车辆可以伪装成其他车辆通信以避免被追责。该方案最重要的问题在于一个签名出错将会导致整个批量验证失效,验证效率大大降低。文献[11]中提出的提高安全和隐私的交流方案(SPECS)是一个基于软件的满足高安全要求和低通信开销的方案。SPECS 使用了二分搜索技术和布隆过滤器,使得批验证成功率大大提高,能够快速及时地处理移动自组网的消息,但是它不能抵挡伪装攻击,一个车辆可以通过收集它的签名消息,伪装成别的车辆来发送消息[12]。后来为了解决伪装攻击,文献[12]提出了新的方案 b-SPECS+,该方案不仅满足隐私保护要求,而且考虑到了相关的安全问题,如消息认证、完整性、合谋攻击。b-SPECS+中可信的权威机构能够从签名消息中恢复和撤销任意车辆的真实身份,所以达到了有条件的隐私保护,其验证延迟和传输开销都低于现有的其他方案。但是 b-SPECS+中不能很好地抵制合谋攻击,只要路边单元(RSU)和车辆合谋,攻击者就会拥有假名验证公钥和共享密钥,可以有效地伪造出合法的假名,如再拥有车辆提供的用于签名的主密钥,就可以伪造出一个有效的签名消息。

为了能够实现有条件的匿名认证和批量认证,并且能够很好地抵制合谋攻击,本文基于 b-SPECS+提出了一种新的签名方案,该方案使用基于假名验证的私钥进行签名。本文的主要贡献如下:1)能够有效地防止 RSU 与车辆合谋,伪造签名消息;2)在批量认证时,消息越多,与其他方案相比认证效率越高。

本文第 2 节介绍了相关的背景知识;第 3 节具体描述了所提方案;第 4 节针对安全性进行了分析,并进行了理论证明;第 5 节进行了性能评估;最后对全文进行总结,并给出展望。

2 背景知识

2.1 网络模型

在可认证的车载网络模型中,主要存在以下 3 个角色:一个可信的权威机构(TA)、多个分布在各地的固定路边设备(RSU)以及移动车载单元(OBU)。图 1 给出了车载网络模型。

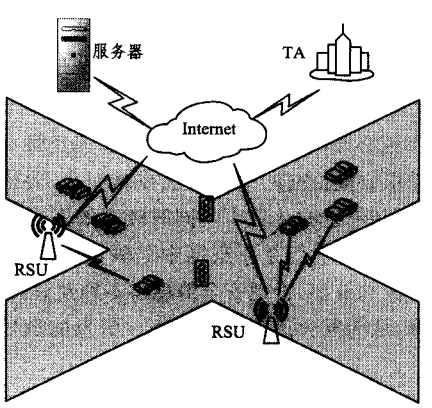

图 1 车载网络模型图

TA:TA 是系统中完全可信的角色,拥有最高的管理权限。TA 将所管理区域划分为若干子区域,区域划分属于公开信息,假定各个区域内部及区域交界处部署有 RSU。一般假设 TA 拥有足够大的存储能力,并且不会被任何敌手入侵。

RSU:RSU 是车载自组网的基础设施,与 TA 通过有线网络互联,为车辆认证消息。作为分散在路边的设施,RSU 存在着被攻击者破坏的可能。虽然有研究假设 TA 可以检测到侵害行为,并迅速恢复它,但储存在该 RSU 中的信息可能已经泄露了。

OBU:车辆对外发布信息,经过 RSU 认证后被接收,提高了驾驶体验。车辆经过新的 RSU 时,请求更换共享消息和认证公钥。

2.2 双线性对

双线性配对函数通常被用在密码分析中,通过使用配对函数可以将某些椭圆曲线上的离散对数问题约减到有限域上的离散对数问题。设 G_1 和 G_2 分别是阶为素数 q 的加法循环群和乘法循环群,P 是 G_1 的一个生成元。$\hat{e}:G_1\times G_2\rightarrow G_2$ 是一个双线性对,则满足如下性质:

(1)双线性:$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{a,b}=\hat{e}(Q,P)^{a,b}$ 对所有的 $P,Q\in G_1,a,b\in Z_{q^*}$。

(2)非退化:存在 $(P,Q)\in G_1\times G_1$,使得 $\hat{e}(P,Q)\neq 1$,其中,1 表示乘法群 G_2 中的单位元。

(3)可计算性:映射 $\hat{e}$ 是高效可计算的。

3 基于假名验证公钥的批量认证方案

本文提出一种基于假名验证公钥的批量认证方案。基本认证过程如下:首先车辆进入第一个 RSU 时,TA 验证其身份,并为它计算假名验证公钥以及基于验证公钥的私钥,然后选定一个与 RSU 共享的秘密用于后续交流认证;车辆可以根据该验证公钥和私钥以及共享秘密生成签名消息,RSU 接收到消息后可以进行批量认证并进行广播。

图 2 给出了车辆初次遇见 RSU 进行认证到发送签名消息的过程。

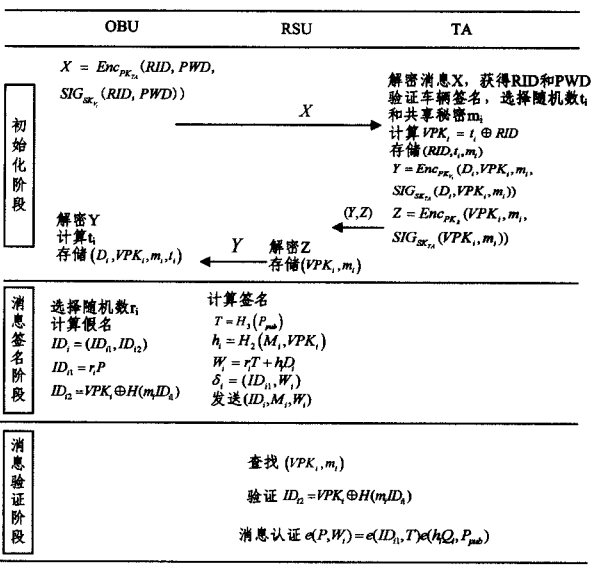

图 2 车辆初次认证到发送消息的过程

3.1 系统初始化

给定安全参数 λ,TA 运行 $\varsigma en(\lambda)$ 生成公共参数 (q,G_1,G_2,e,P)。然后 TA 选择一个随机参数 $s(s\in Z_q^*)$ 作为自己的

主秘钥，并且计算系统公钥 $P_{pub}=sP\in G_1$。TA 再选择 3 个密码学 Hash 函数 $H_1,H_3:\{0,1\}^*\rightarrow G_1,H_2:\{0,1\}^*\rightarrow Z_q^*$ 和一个安全的加密算法 $Enc_k()$。最后 TA 公布系统参数$(q,G_1,G_2,e,P,H_1,H_2,H_3,Enc_k())$。在车辆注册时，TA 给每一辆车分配一个真实身份 $RID\in G$ 和一个验证密码 PWD。表 1 给出了对应的名词概念。

表 1　对应的名词概念

名词符号	描述	名词符号	描述
TA	权威机构	$Enc_k(M)$	用秘钥 k 对消息 M 加密的函数
V_i	车辆 i	$SIG_k(M)$	用秘钥 k 对消息 M 签名的函数
RSU	路边单元	VPK_i	车辆的假名验证公钥
G_1	循环加法群	D_i	基于验证公钥生成的私钥
G_2	循环乘法群	ID_i	车辆 i 的假名
s	系统主秘钥	M_i	车辆 i 发送的消息
P_{pub}	系统公钥	H_i	隐射哈希函数
RID	车辆真实身份	$\oplus$	异或操作

3.2　初始化握手协议

具体过程如下。

(1)当车辆遇见第一个 RSU 时，它用自己的私钥 SK_{v_i} 签名 RID 和 PSW，然后用 TA 的公钥加密 RID，PSW 和 $SIG_{SK_{V_i}}(RID,PWD)$，并通过 RSU 发送 $X=Enc_{PK_{TA}}(RID,PWD,SIG_{SK_{V_i}}(RID,PWD))$给 TA。

(2) TA 接收到消息后解密得到 RID，PWD，$SIG_{SK_{V_i}}(RID,PWD)$，然后用车辆 V_i 的公钥 PK_{V_i} 验证签名。如果它们都是有效的，并且 RID 不在撤销链表中，TA 为车辆 V_i 选择一个随机数 $t_i(t_i\in Z_q^*)$，计算 V_i 的身份认证公钥 $VPK_i=t_i\oplus RID$和部分私钥 $D_i=sQ_i$，其中 $Q_i=H_1(VPK_i)$，再为 V_i 和 RSU 选择一个共享秘钥 m_i。最后 TA 发送消息 $Y=Enc_{PK_{V_i}}(D_i,VPK_i,m_i,SIG_{SK_{TA}}(D_i,VPK_i,m_i))$ 和 $Z=Enc_{PK_R}(VPK_i,m_i,SIG_{SK_{TA}}(VPK_i,m_i))$给 RSU。TA 将 (RID_i,t_i,m_i)存储在自己的存储空间中。

(3)RSU 接收到 Y,Z 后，解密 Z 得到 VPK_i,m_i，及 TA 对它们的签名。然后 RSU 验证 TA 的签名，如果验证成功，RSU 存储(VPK_i,m_i)在它的验证表里供随后的通信使用；随后将 Y 发送给 V_i。

(4)V_i 接收到 Y 后解密得到 VPK_i,m_i,D_i 和 TA 对它们的签名。然后 V_i 验证 TA 的签名，如果签名有效，V_i 计算 $t_i=VPK_i\oplus RID$，并将(t_i,VPK_i,m_i,D_i)存储在自己的存储空间里。

经过上述 4 步完成了初始握手阶段，随后如果车辆离开这个 RSU 的范围，进入到下一个 RSU，只需要一个简单的认证过程就可以得到 TA 为它和新的 RSU 生成的新的共享消息。

(5)当车辆 V_i 进入新的 RSU 时，V_i 选择一个随机数 r'，然后通过新的 RSU 将 $Enc_{PK_{TA}}(RID\parallel r')$发送给 TA。$r'$用来防止敌手收集信息，从而得到该车辆经过哪些 RSU。TA 解密消息，检查 RID 是否在撤销链表中，无需检查 PWD。如果车辆身份有效，TA 直接为车辆 V_i 生成新的 t_i,m_i,VPK_i 和 D_i，传送新的(Y',Z')给新的 RSU，其中 $Y'=Enc_{PK_{V_i}}(D_i,VPK_i,m_i,SIG_{SK_{TA}}(D_i,VPK_i,m_i))$ 和 $Z'=Enc_{PK_R}(VPK_i,m_i,SIG_{SK_{TA}}(VPK_i,m_i))$。TA 增加新的 t_i,m_i 到自己的存储空间中。RSU 首先存储(VPK_i,m_i)到自己的验证表里，随后将 Y'发送给 V_i。然后车辆用新的 t_i,m_i 通信。

3.3　消息签名

对每一个消息进行签名时，车辆都会生成一个假名，这样可以实现消息的匿名发送。

(1)车辆 V_i 选择一个随机数 r_i 用于生成假名。假名 ID_i 由两部分组成，$ID_i=(ID_{i1},ID_{i2})$，其中 $ID_{i1}=r_iP$，$ID_{i2}=VPK_i\oplus H(m_iID_{i1})$。

(2)对消息 M_i 的签名：首先计算 $h_i=H_2(M_i,VPK_i)$和 $T=H_3(P_{pub})$；然后计算 $W_i=r_iT+h_iD_i$；那么 $\delta_i=(ID_{i1},W_i)$就是车辆 V_i 对 M_i 的签名。由于假名中含有 ID_{i1}，签名中也含有 ID_{i1}，因此最后发送的消息格式为(ID_i,M_i,W_i)，签名 δ_i 可从中提取。

3.4　消息认证

对于给定消息签名(ID_i,M_i,W_i)，RSU 的验证如下：

(1)对于给定的 ID_i，通过检查存储的(VPK_i,m_i)，满足 $ID_{i2}=VPK_i\oplus H(m_iID_{i1})$。

(2)计算 $h_i=H_2(M_i,VPK_i)$。

(3)接受该签名当且仅当以下等式成立：

$$e(P,V_i)=e(ID_{i1},T)e(h_iQ_i,P_{pub}) \tag{1}$$

下面验证等式(1)的正确性。

证明：$e(ID_{i1},T)e(h_iQ_i,P_{pub})=e(r_iP,T)e(h_iQ_i,sP)=e(P,r_iT)e(h_isQ_i,P)=e(P,r_iT)e(h_iD_i,P)=e(P,r_iT+h_iD_i)=e(P,V_i)$。

(4)批量验证：计算 $ID=\sum_{i=1}^{n}ID_{i1}$ 和 $W=\sum_{i=1}^{n}W_i$。对于给定的 ID_i，通过检查存储的(VPK_i,m_i)，满足 $ID_{i2}=VPK_i\oplus H(m_iID_{i1})$，计算 $h_i=H_2(M_i,VPK_i)$，$1\leqslant i\leqslant n$，接受该签名当且仅当 $e(P,W)=e(ID,T)e(\sum_{i=1}^{n}h_iQ_i,P_{pub})$。

各个车辆的消息 $M_i(1\leqslant i\leqslant n)$发送经过 RSU 的认证广播给车辆。比如车辆 V_j 想要验证车辆 V_i 关于消息 M_i 的签名 δ_i，车辆 V_j 验证(ID_i,M_i,W_i)是否在 RSU 的广播消息中，如果在就接受，否则说明该消息还没有认证或者认证不成功，所以车辆 V_j 只能等待 RSU 的下一个广播消息。文中采用 SPECS[11]方案生成消息通知和处理失效的批认证以及从中提取出有效的签名而不是丢弃整个批认证。

RSU 将会存储假名来防止重放攻击，不同的车辆选用同样的假名的概率极低，如果收到的消息的假名是存储中已有的，那么将认为该签名无效，车辆就会选择新的假名重新签名。

3.5　真实身份的追踪和撤销

只有 TA 才有能力追踪车辆。当出现一个有争议的消息时，根据车辆 V_i 的假名 ID_i 和与 RSU 共享的消息 m_i，TA 从它的存储空间中搜索存储的(RID_i,t_i,m_i)，得到车辆 V_i 的真实身份 $ID_{i2}\oplus t_i\oplus H(m_iID_{i1})=RID_i$。其正确性证明：左边$=VPK_i\oplus H(m_iID_{i1})\oplus t_i\oplus H(m_iID_{i1})=t_i\oplus RID_i\oplus H(m_iID_{i1})\oplus t_i\oplus H(m_iID_{i1})=$右边。

除了 TA，没有人能够获得车辆 V_i 的真实身份，因为只有 TA 和 V_i 有 t_i。TA 一旦获得 RID_i，就可很容易地将其撤销。只要将 RID_i 加入撤销链表，V_i 将来就再也无法获得新的 VPK_i 和 m_i。

4 安全性分析

本节从下面4个方面分析该方案的安全性：消息完整性和认证、身份隐私的保护、车辆追踪和车辆撤销、合谋攻击。

4.1 消息完整性和认证

在车载网中，消息完整性和认证是最基本的安全要求。假设敌手是一个外部的攻击者，文中方案中 δ_i 是基于验证身份公钥 VPK_i 的一个签名，在不知道用户私钥或验证公钥 VPK_i 的情况下是不可能伪造一个有效的签名的。如果敌手是一个内部攻击者，假如是车辆 V_j，首先它不能计算一个新的假名，因为它不知道分享的秘密 m_i；其次在知道 m_i 和 VPK_i 时，签名也是不可伪造的。

定理 1 在随机预言机模型下，假设存在一个敌手 A 以 $(t,q,q_E,q_S,n,\varepsilon)$ 攻破该签名方案。记 A 询问 $H_i(i=1,2,3)$ 预言机，私钥解析预言机和签名预言机的次数分别为 $q_{H_i}(i=1,2,3)$，q_E 和 q_S，则存在一个算法 C，以优势 $\varepsilon' \geqslant \varepsilon\delta_1^{q_E}(1-\delta_2(1-\delta_1))^{q_S}(1-\delta_1(1-\delta_2))$ 在时间 $t'<t+(q_{H_1}+q_E+3q_S+2)t_{sm}$ 内解决 CDH 问题，其中 t_{sm} 是计算群上一个标量乘所用的时间。

证明：算法 C 调用 A 为子程序在一个概率多项式时间内解决 CDH 问题。设 (aP,bP) 是群 G_1 上 CDH 问题的任意一个实例，C 的目标是输出该 CDH 问题的解 abP。C 运行 Setup 算法，定义系统公钥 $P_{pub}=aP$，生成系统参数 $params:=\{k,e,G_1,G_2,P,P_{pub},H_1,H_2,H_3\}$，将其发给 A。A 执行以下询问：

(1) Hash 询问

为了模拟 Hash 询问，C 需要维护 3 张列表即 L_1,L_2,L_3，分别跟踪对 H_1,H_2,H_3 的询问，3 张表的起始设置为空。

(1.1) H_1-询问：若 A 以 $VPK_i(1\leqslant i\leqslant q_{H_1})$ 作为输入，C 调出列表 L_1。如果 L_1 中已有相应的记录 (VPK_i,Q_i,t_i,c)，则返回 Q_i；否则采用文献[18]的技巧，C 任选 $t_i\in Z_q^*$，抛掷一个偏心硬币 $c\in\{0,1\}(\Pr[c=0]=\delta_1,\Pr[c=1]=1-\delta_1)$，若 $c=0$，定义 $Q_i=t_iP$，否则 $Q_i=t_i(bP)$，添加 (VPK_i,Q_i,t_i,c) 到列表 L_1 中，返回 Q_i 给 A。

(1.2) H_2-询问：A 输入 (M_i,VPK_i)，C 调出列表 L_2。若 L_2 中已有相应的记录，返回以前定义的值；否则任选 $h_i\in Z_q^*$，添加 (M_i,VPK_i,h_i) 到列表 L_2 中，返回 h_i 给 A。

(1.3) H_3-询问：当 A 询问 P_{pub} 的 Hash 值时，C 任选 $l\in Z_q^*$，抛掷偏心硬币 $c^*\in\{0,1\}(\Pr[c^*=0]=\delta_2,\Pr[c^*=1]=1-\delta_2)$，若 $c^*=0$，定义 $T=lP$。否则 $T=lP_{pub}$，添加 (P_{pub},l,T,c^*) 到 L_3 中，返回 T。

(2) 私钥解析询问

C 维护一个列表 E^{list}，给定 VPK_i，C 从 L_1 中调出 (VPK_i,Q_i,t_i,c)，若 $c=1$，则停止模拟，输出“FAILURE”；否则，计算 $D_i=t_i(aP)$，添加 (VPK_i,D_i) 到 E^{list} 中，返回 D_i。

(3) 签名询问

当对 (M_i,VPK_i) 进行签名询问时，C 调出列表 L_1,L_3，找出 (VPK_i,Q_i,t_i,c) 和 (P_{pub},l,T,c^*) 进行以下操作：

(3.1) 如果 $c=0,c^*=0$，调出列表 L_2，找到对应的记录 (M_i,VPK_i,h_i)，任选一个元素 $W_i\in G_1$，计算 $ID_{i1}=l^{-1}(W_i-h_it_iP_{pub})$，返回 (ID_{i1},W_i) 作为对 A 的应答。

(3.2) 如果 $c=0,c^*=1$，C 任选 $\alpha\in Z_q^*$，计算 $W_i=\alpha P_{pub}$，$ID_{i1}=l^{-1}(\alpha P-h_it_iP)$，返回 (ID_{i1},W_i)。

(3.3) 如果 $c=1,c^*=1$，C 任选 $\beta\in Z_q^*$，计算 $W_i=\beta P_{pub}$，$ID_{i1}=l^{-1}(\beta P-h_it_ibP)$，返回 (ID_{i1},W_i)。

(3.4) 如果 $c=1,c^*=0$，C 停止模拟，输出“FAILURE”。

最后，A 停止询问，输出一个挑战验证公钥 VPK_i^* 的消息/签名对 (M_i^*,ID_{i1}^*,W_i^*)，C 调用列表 L_1，找出 (VPK_i,Q_i,t_i,c)，如果 $c=0$，则停止模拟，输出“FAILURE”；否则在列表 L_3 中找出记录 (P_{pub},l,T,c^*)，如果 $c^*=1$ 则输出“FAILURE”，否则有以下等式：$e(P,W_i^*)=e(ID_{i1}^*,T)e(h_i^*Q_i^*,P_{pub})$，即 $e(P,W_i^*)=e(ID_i^*,lP)e(h_i^*t_i^*bP,aP)$，$e(P,W_i^*-lID_{i1}^*)=e(h_i^*t_i^*abP,P)$，所以 C 可以计算出 $abP=(h_i^*t_i^*)^{-1}(W_i^*-lID_{i1}^*)$。

下面分析 C 成功的概率，定义 3 个独立事件 E_1,E_2,E_3。

E_1：C 回答私钥解析询问没有失败；

E_2：C 回答签名询问没有失败；

E_3：A 生成一个有效的签名，并且这个 VPK_i^* 在 L_1,L_3 中的记录分别对应 $c=0$ 和 $c^*=1$。

则 $\Pr[E_1\wedge E_2\wedge E_3]\geqslant\varepsilon\delta_1^{q_E}(1-\delta_2(1-\delta_1))^{q_S}(1-\delta_1(1-\delta_2))$，当 3 件事都发生时，$C$ 获胜，它的概率 $\varepsilon'\geqslant\varepsilon\delta_1^{q_E}(1-\delta_2(1-\delta_1))^{q_S}(1-\delta_1(1-\delta_2))$。$C$ 在游戏中用的时间 $t'<t+(q_{H_1}+q_E+3q_S+2)t_{sm}$，输出值 abP 作为对 CDH 问题的答案，从而解决了 CDH 问题的一个实例。

4.2 身份隐私保护

任意一辆车的真实身份都不应当被其他任意的车辆和第三方通过分析多个消息而知道。首先，车辆 V_i 的真实身份 RID_i 被 TA 转换成 VPK_i，并通过它的公钥 PK_{V_i} 加密后经过 RSU 发送给它，车辆通过解密 X 得到 VPK_i，生成假名 $ID_i=(ID_{i1},ID_{i2})$，其中 $ID_i=r_iP$，$ID_{i2}=VPK_i\oplus H(m_iID_{i1})$。对不同消息，根据随机数 r_i 的变换得到不同的假名，并且每个假名只使用一次，所以具有不可连接性，并且在 DDH 难题的假设下，假名生成算法在适应性选择明文攻击下是抗存在性伪造的[12]。

任意一个 RSU 也不能通过假名得到 V_i 的真实身份，因为它不能解密 TA 发送给 V_i 的消息 Y。所以在我们的方案中除了 TA 和车辆自己，没有任何人知道它的真实身份。除此之外，车辆在不同的 RSU 使用的是不相同的验证身份公钥，所以即使所有的 RSU 合谋也无法得到车辆的运行轨迹。

4.3 追踪和撤销

当发生消息争议时，只有 TA 才能追踪到车辆的真实身份。给定假名 $ID_i=(ID_{i1},ID_{i2})$，由 TA 存储的 (RID_i,t_i,m_i)，可以得到车辆的真实身份 $RID_i=ID_{i2}\oplus t_i\oplus H(m_iID_{i1})$，TA 也能根据真实身份撤销该车辆。

4.4 合谋抵制

无论多少车辆合谋，它们也不能生成一个有效的签名，因为敌手得不到车辆验证身份公钥 VPK_i，因此它们不能生成车辆的签名私钥，同样，无论多少 RSU 合谋它们也不能得到车辆的行驶轨迹。在 b-SPECS+[12] 方案中，车辆和 RSU 合谋时，就可以伪造一个合法的签名，因为攻击者既知道主秘钥，也知道与 RSU 的共享秘密和验证公钥，但我们的方案基于上述 CDH 难题，除了 TA 谁也计算不出 D_i，所以该方案是强抵抗合谋攻击的。

5 性能评估

5.1 认证延时

首先定义3个密码学的操作：T_{par}代表一个双线性对操作，T_{mul}代表一个点乘操作，T_{mtp}代表一个哈希映射操作，在这里采用i7 3.07GHz的处理器。在文献[16]的实验中，选择80比特安全的椭圆曲线[19]上159比特的循环子群，根据MIRACL[17]加密函数库的处理时间，得出T_{par}是3.21ms，T_{mul}是0.39ms，T_{mtp}是0.09ms。据此给出了文中所提方案与SPECS[11]，b-SPECS+[12]，BLS[13,14]和ECDSA[15]在签名认证时间上的比较，结果如表2所列。表2表明随着签名数量的增加，所提方案具有最短的签名时间。

表2 签名验证时间比较

方法	验证单个签名(ms)	验证n个签名(ms)
所提方案	$3T_{par}+T_{mul}+T_{mtp}\approx 10.03$	$3T_{par}+nT_{mul}+nT_{mtp}\approx 0.4n+9.63$
b-SPECS+	$2T_{par}+2T_{mul}+T_{mtp}\approx 7.29$	$2T_{par}+2nT_{mul}+nT_{mtp}\approx 0.87n+6.42$
SPECS	$2T_{par}+2T_{mul}+T_{mtp}\approx 7.29$	$2T_{par}+2nT_{mul}+nT_{mtp}\approx 0.87n+6.42$
BLS	$4T_{par}+2T_{mul}\approx 13.02$	$(2n+2)T_{par}+2T_{mul}\approx 6.6+6.42$
ECDSA	$4T_{mul}\approx 1.56$	$4nT_{mul}\approx 1.56n$

接下来，假设每个RSU覆盖范围内每个车辆周期性地发送消息，而消息密度代表在RSU范围内车辆发送的消息数量，给出所提方案与其他方案在消息密度变化时认证延时的比较，如图3所示。图3表明与现有方法相比，所提签名方案具有最小的认证延时。在消息数目达到30时，所提方案的消息延时只有SPECS和b-SPECS+的66.5%、BLS的10.6%、ECDSA的46.2%。

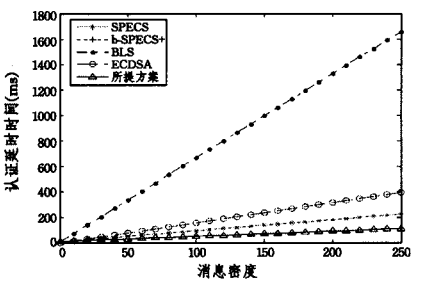

图3 消息密度与延时对比

图4说明所提方案拥有最小的认证时延率。

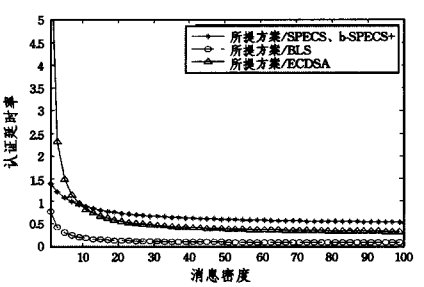

图4 消息密度与延时率对比

5.2 传输开销

将所提方案与SPECS，b-SPECS+，BLS和ESCDA方案进行了传输开销比较，文中方案中假名占42字节，签名也是42字节，但是由于签名与假名中有一部分相同，因此每个消息签名的开销是63字节；SPECS和b-SPECS+方案中假名占42字节，签名21字节；BLS方案中是21字节的签名加125字节的证书，证书采用IEEE 1609.2标准[15]；ECDSA方案中是42字节的签名加上125字节的证书。表3给出了具体的传输开销。

表3 传输开销比较

方案	发送单个消息(bytes)
所提方案	21+42
b-SPECS+	21+42
SPECS	21+42
BLS	21+125
ECDSA	42+125

图5描述了30s内传输开销随着RSU接收消息数量增长的关系。该图说明所提方案的传输开销与SPECS和b-SPECS+方案一样，但明显远远小于BLS和ECDSA方案。

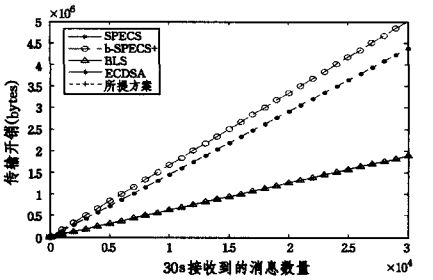

图5 30s接收到消息数量与传输开销对比

结束语 b-SPECS+方案中，只要RSU和车辆合谋就会拥有主密钥与RSU之间的共享秘密，进而伪造出合法的签名的缺陷，提出了基于假名验证公钥的RSU辅助批量认证方案。该方案基于CDH难题，除了车辆自身和TA，谁也计算不出签名私钥，已经被理论证明具有不可伪造性。性能评估结果表明，所提方案具有认证时延小、通信开销低的特点。文中方案需要TA一直在线和完全可信，并且需要RSU介入，在接下来的工作中，将会考虑如何构造半可信中心的系统，以及在TA离线，没有RSU介入的情况下，车辆如何进行批量认证。

参考文献

[1] European vehicle manufacturers working hand in hand on deployment of cooperative Intelligent Transport Systems and Services (C-ITS)[OL]. http://www.car-to-car.org

[2] CO-OPerative SystEms for Intelligent Road Safety [OL]. http://www.coopers-ip.eu

[3] An Integrated Wireless and Traffic Platform for Real-Time Road Traffic Management Solutions[EU-FP7]. http://www.ict-itetris.eu

[4] Dedicated short range communications (5.9 ghz dsrc)[OL]. http://www.leearmstrong.com/DSRC/DSRCHomeset.html

[5] Dedicated Short Range Communications (DSRC)[OL]. http://grouper.ieee.org/groups/scc32/dsrc/index.html

[6] Zhang C, Lin X, Lu R, et al. An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks [C]//IEEE Proceedings of the ICC 2008. 2008:1451-1457

[7] Raya M, Papadimitratos P, Hubaux J P. Securing vehicular communications[J]. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006, 13(5):8-15

[8] Hubaux J P, Capkun S, Luo J. The security and privacy of smart

vehicles[J]. IEEE Security and Privacy Magazine, 2004, 2(3): 49-55

[9] Lu R, Lin X, Zhu H, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications [C]// Proc. of the INFOCOM 2008. Phoenix, Arizona, USA, April 2008: 1229-1237

[10] Zhang C, Lu R, Lin X, et al. An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks[C]// IEEE Proceedings of the INFOCOM 2008. April 2008: 816-824

[11] Chim T W, Yiu S M, Hui L C K, et al. SPECS: Secure and privacy enhancing communications schemes for VANETs[J]. Ad Hoc Networks, 2011, 9(2): 189-203

[12] Horng S J, Tzeng S F, Pan Yi, et al. b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET[J]. IEEE Transaction on information and Security, 2013, 8(11): 1860-1875

[13] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing, Asiacrypt 01[J]. Journal of Cryptology, 2001, 17(4): 297-319

[14] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]// Procedings of Eurocrypt. 2003, 2656: 416-432

[15] IEEE Trial-Use Standard for Wireless Access in Vehicular Environment-Security Services for Applications and Management Message: IEEE Standard 1609. 2[S]. Jul. 2006

[16] Shim K A. CPAS: An efficient conditional privacy-preserving authenticationscheme for vehicular sensor networks [J]. IEEE Transaction on Vehicular Technolgy, 2012, 61(4): 1874-1883

[17] MIRACL Cryptographic Library: Multiprecision Integer and Rational Arithmetic C/C++ Library [OL]. http://indigo.ie/~mscott/

[18] Coron J. On the exact security of full domain hash[M]// Advanced in Cryptoloyg — Eurocrypt'2000, LNCS 1880. Berlin: Springer-Verlag, 2000: 229-235

[19] Nakabayashi M M, Takano S. New explicit conditions of elliptic curve traces for FR-reduction[J]. IEICE Trans. Fundamentals, 2001, E84-A(5): 1234-123

(上接第 115 页)

参 考 文 献

[1] Kuang Guang-tao, Wang Suo-gang, Ding Jia, et al. A system Design of a Hybrid BCI Based on the Dual characteristics[J]. Computer Simulation, 2014, 31(8): 222-225(in Chinese)
匡光涛, 王索刚, 丁佳, 等. 一种基于双特征的联合脑-机接口系统设计[J]. 计算机仿真, 2014, 31(8): 222-225

[2] Zhu Xiao-jun, Lv Shi-qin, Wang Yan-fei, et al. The Improved LMD Algorithm and Its Applocation in the EEG Feature Extraction[J]. Journal of Taiyuan University of Technology, 2012, 43(3): 339-343(in Chinese)
朱晓军, 吕士钦, 王延菲, 等. 改进的 LMD 算法及其在 EEG 信号特征提取中的应用[J]. 太原理工大学学报, 2012, 43(3): 339-343

[3] Huang N E, Shen Z, Long S R, et al. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis[J]. Proceeding of Royal Society Lond. A, 1998(454): 903-995

[4] Wu Z H, Huang N E. Ensemble empirical mode decomposition: a noise assisted data analysis method[J]. Advances in Adaptive Data Analysis, 2009, 1(1): 1-41

[5] Cheolsoo P, David L, Van Hulle Marc M. The complex local mean decomposition[J]. Neurocimputing, 2001, 74(6): 867-875

[6] Wang Ting. Research on EMD algorithm and its Application in signal denoising[D]. Harbin: Harbin Engineering University, 2010(in Chinese)
王婷. EMD 算法研究及其在信号去噪中的应用[D]. 哈尔滨: 哈尔滨工程大学, 2010

[7] Guo Qi, Liu Bu-yu, Shi Li-bo, et al. Experimental study and fault signal analysis of rotating machinery based on dual EEMD and wigner-ville distributinf[J]. Journal of Vibration and Shock, 2012, 31(13): 129-133, 153(in Chinese)
郭奇, 刘卜瑜, 史立波, 等. 基于二次 EEMD 的 Wigner-Ville 分布旋转机械故障信号分析及试验研究[J]. 振动与冲击, 2012, 31(13): 129-133, 153

[8] Ren Da-qian. Based on local mean decomposition of rotating machinery fault feature extraction method and system research [D]. Hangzhou: Zhejiang University, 2008(in Chinese)
任达千. 基于局部均值分解的旋转机械故障特性提取方法及系统研究[D]. 杭州: 浙江大学, 2008

[9] Ai Yan-ting, Feng Yan-yan, Zhou Hai-lun. Fault Diagnosis of Bearing Acoustic Emission Signals Based on Improved Wavelet Threshold Denoising and LMD[J]. Science Technology and Engineering, 2014, 14(33): 86-91(in Chinese)
艾延廷, 冯研研, 周海仑. LMD 和改进小波阈值去噪的轴承声发射信号故障诊断[J]. 科学技术与工程, 2014, 14(33): 86-91

[10] Zhu Xiao-jun, Fan Liu-juan, Lv Shi-qin, et al. Application Research of LMD Method in EEG Signal Processing[J]. Computer Science, 2012, 39(2): 273-275(in Chinese)
朱晓军, 樊刘娟, 吕士钦, 等. LMD 方法在脑电信号处理中的应用研究[J]. 计算机科学, 2012, 39(2): 273-275

[11] Hou Gao-yan, Lv Yong, Li You-rong, et al. LMD Morphology Compared with EEMD Morphology in the Fault Diagnosis[J]. Instrument Technique and Sensor, 2014(8): 107-110(in Chinese)
侯高雁, 吕勇, 李友荣, 等. LMD 形态学与 EEMD 形态学在故障诊断中的对比研究[J]. 仪表技术与传感器, 2014(8): 107-110

[12] Zhang Xiao-nan, Liu Jian-ping. LMD algorithm and time-frequency analysis of motor imagery signal[J]. Modern Electronics Technique, 2013, 36(17): 55-58(in Chinese)
张晓楠, 刘建平. LMD 算法与运动想象脑电信号的时频分析[J]. 现代电子技术, 2013, 36(17): 55-58

[13] Tao Ke, Zhu Jian-jun. A Hybrid Indicator for Determining the Best Decomposition Scale of Wavelet Denoising[J]. Acta Geodaetica et Cartographica Sinica, 2012, 41(5): 749-755

[14] Wu Fu-mei, Yang Yuan-xi. GPS/INS Integrated Navigation by Adaptive Filtering Based on Wavelet Threshold De-noise[J]. Acta Geodaetica et Cartographica Sinica, 2007, 36(2): 124-128

[15] Zhang Zhe-tao, Zhu Jian-jun, Kuang Cui-lin, et al. Multi-threshold Wavelet Packet De-noising Method and Its Application in Deformation Analysis[J]. Acta Geodaetica et Cartographica Sinica, 2014, 43(1): 13-20(in Chinese)
章浙涛, 朱建军, 匡翠林, 等. 小波多阈值去噪法及其在形变分析中的应用[J]. 测绘学报, 2014, 43(1): 13-20