·计算机与信息技术·

车载自组网中基于密钥协商的条件隐私保护认证方案

龚　成,牛宪华*,熊　玲,王杨鹏
(西华大学计算机与软件工程学院,四川 成都 610039)

摘　要: 车载自组网作为智慧交通的重要组成部分,其安全和隐私一直是被关注的 2 个难题。特别是在计算资源和存储资源向边沿端移动的去中心化趋势下,分布式的认证集群开始取代单一的认证中心,而现有的认证方案中较少考虑到认证服务集群的稳定性。为此,文章提出一种车载自组网中基于密钥协商的条件隐私保护认证方案。该方案利用树实现密钥协商协议中的密钥生成和更新,以保证认证服务集群中各个服务节点之间的信息同步;同时,结合匿名认证技术和分布式认证集群共同保障车辆、认证服务集群、可信权威之间的认证过程的隐私和安全。该方案不仅可保护车载自组网中的安全和隐私,还可维护认证集群的健壮性。

关键词: 车载自组网;树;密钥协商;条件隐私保护

中图分类号: TP309　　**文献标志码:** A　　**文章编号:** 1673–159X(2022)05 − 0073 − 11

doi:10.12198/j.issn.1673 − 159X.4359

Conditional Privacy-Preserving Authentication Scheme Based on Key Agreement for Vehicle Ad Hoc Networks

GONG Cheng, NIU Xianhua*, XIONG Ling, WANG Yangpeng
(*School of Computer and Software Engineering, Xihua University, Chengdu* 610039 *China*)

Abstract: Vehicular ad hoc network is an important part of intelligent transportation, and the security and privacy of vehicular ad hoc network are two challenging issues which concerned by academia and industry. Especially in the decentralized trend of computing resources and storage resources moving to the edge, distributed authentication clusters begin to replace a single authentication center, but the stability of authentication service clusters is seldom considered in the existing authentication schemes. This paper proposes a conditional privacy protection authentication scheme based on key agreement for vehicular ad hoc networks. This scheme uses the tree to realize the key generation and update in the key agreement protocol, and ensures the information synchronization between each service node in the authentication service cluster. At the same time, anonymous authentication technology and distributed authentication cluster are combined to ensure the privacy and security of the authentication process among vehicles, authentication ser-

收稿日期:2022 − 03 − 24
基金项目:四川省科技厅项目 (2020JDRC0100);西华大学研究生创新基金 (YCJJ2020019)。
* **通信作者:**牛宪华(1983—),女,教授,博士,硕士生导师,主要研究方向为信息安全、保密序列设计。
ORCID:0000 − 0003 − 0980 − 08770　　E-mail:rurustef1212@gmail.com

引用格式:龚成,牛宪华,熊玲,等. 车载自组网中基于密钥协商的条件隐私保护认证方案[J]. 西华大学学报(自然科学版),2022,41(5):73 − 83.
GONG Cheng, NIU Xianhua, XIONG Ling, et al. Conditional Privacy-Preserving Authentication Scheme Based on Key Agreement for Vehicle Ad Hoc Networks[J]. Journal of Xihua University(Natural Science Edition), 2022, 41(5): 73 − 83.

vice clusters and trusted authorities. This scheme not only protects the security and privacy in vehicular ad hoc networks, but also maintains the robustness of authentication clusters.

Keywords: VANETs；tree；key agreement；conditional privacy-preserve

车载自组网 (vehicular ad hoc networks, VANETs) 作为移动自组网 (mobile ad hoc network, MANET) 的子集，是通过路边单元 (roadside unit, RSU) 与车辆间的无线通信实现的。每辆车上的车载单元 (on-board unit, OBU) 负责广播实时交通信息给周围的车辆和 RSU[1]。通常而言，这些通信被划分为车辆与车辆的通信 (vehicle-to-vehicle, V2V) 和车辆与路边单元的通信 (vehicle-to-roadside unit, V2R)，它们都遵守专用短程通信协议 (dedicated short range communication, DSRC)[2]。而且，这些通信都依赖于云计算服务 (cloud computing services, CCS) 所提供的计算和存储资源[3]。在实际应用中，VANETs 较多采用低延迟的车辆雾服务 (vehicular fog services, VFS)[4]。

在开放的网络环境中，敌手可能会截获传输中的消息，因此对消息合法性的验证是不可或缺的[5]。一旦车辆的真实身份被敌手揭露[6]，敌手就能追踪车主的住址、行踪等，进而造成人身和财产的损失。车辆的隐私信息，例如认证过程中的车辆真实身份，不能被任一敌手所揭露[7]。此外，可能存在恶意的参与者为了自身的利益而广播虚假的交通信息。针对这种情况，系统中应该有一个可信的第三方机构能够追踪恶意参与者[8]。

近年来，许多认证方案被提出[9]。这些方案普遍采用的技术包含对称加密、公钥基础设施、基于身份的签名、无证书签名、群签名等[10]，它们均保证了车载自组网环境中的安全和隐私，并且它们的共同趋势是取代单一认证中心，实现去中心化。这些方案往往采用多个独立的服务节点组成认证服务集群。但在认证服务集群中，不仅需要保证各个服务节点之间的信息同步[11－15]，还需要考虑集群的健壮性。认证服务节点作为半可信的实体，在遭受攻击后，如何在集群内部快速移除瘫痪的节点，以及如何快速添加备用节点是保证集群稳定性和健壮性的关键。因此，设计一个既能满足安全性和隐私性，又能保证认证服务集群健壮性的认证方案是具有现实意义的。

本文的主要贡献如下。

1）实现了不可链接性，用于保护车辆的隐私。敌手无法关联同一辆车的不同假名。

2）实现了认证服务节点之间的认证信息同步。车辆在进入另一个服务节点的管理区域时，可以实现跨域认证。

3）实现了认证服务集群中各服务节点的快速添加和删除，保障了认证服务集群的健壮性、可维护性。

1 相关工作

近几年来，许多研究者开始关注车联网环境下的安全和隐私问题。这些方案分为：基于公钥基础设施 (public key infrastructure, PKI) 的、基于身份加密 (ID-based cryptography, IDC) 的和基于认证密钥协商 (authenticated key agreement, AKA) 的。在基于 PKI 的方案中，Raya 等[16] 系统地考虑了 VANET 中的安全问题，提出了一种基于 PKI 的安全协议，但该方案仅考虑了 V2V，没有考虑 V2R。随着 RSU 的完善，Wang 等[17] 提出了一种基于 PKI 证书和身份签名的混合条件隐私保护认证协议，该方案充分地考虑了 V2V 和 V2R。

在基于 PKI 的认证方案中，证书分发、管理和撤销所需的计算开销较大。为了解决计算开销问题，基于身份加密的认证方案被提出。Vijayakumar 等[18] 提出了基于身份划分的二重认证和密钥管理机制，但该方案的密钥管理开销仍然较大。Ying 等[19] 介绍了一种基于智能卡协议的轻量级匿名身份验证方案，但该方案没有考虑跨域认证的问题，即车辆出现通信对象的切换时，不同域的服务提供者需能认证车辆先前的假名。为了实现跨域认证，Liu 等[20] 利用基于身份加密和基于短生存期的证书构造了一个分布式条件隐私保护认证方案。类似地，Deng 等[21] 采用假名技术来保护隐私，并通过组密钥加密来改变假名。

除了 PKI 认证方案和 IDC 认证方案的密钥分发,另一种确保通信安全的方法是使用密钥协商获得安全的通信信道。Can 等[22] 指出,可以将满足会话密钥安全的密钥交换协议和认证算法结合起来,获得安全的通信信道,保证通信安全。Huang 等[23] 提出了一种 AKA 协议,一个基于椭圆曲线密码 (elliptic curve cryptography, ECC) 的签名算法被用来避免双线性对的高计算开销。Mejri 等[24] 考虑了 VANETs 中的组密钥生成问题,在传统的 Diffie-Hellman 密钥交换算法的基础上构建组密钥。

在满足安全和隐私的基础上,学术界开始研究认证方案的去中心化。文献 [25] 提出了一种动态的、跨域认证的非对称组密钥协议,该协议避免了密钥托管的风险和证书管理的复杂性,但该方案使用双线性映射,计算开销大。此外,去中心化也对基于 IDC 的认证方案提出了新挑战。为此,He 等[26] 设计了一个基于分层身份密码的匿名认证方案框架。Xiong 等[27] 利用自认证公钥密码和中国剩余定理 (chinese remainder theorem, CRT) 为移动云计算 (mobile cloud computing, MCC) 环境构建了一个完整的认证和分层访问控制方案。随着区块链技术的广泛应用,越来越多的去中心化方案开始使用区块链来实现认证集群间的信息同步。Wang 等[28] 采用联盟区块链技术,构建了一个分散的网络作为认证集群。Yao 等[29] 提出了一种基于区块链的跨区域认证方案。但上述基于区块链的认证方案都缺乏对不可链接性的保护,且没有考虑认证集群的健壮性。

2　背景知识

2.1　困难问题

本文方案的安全性主要依赖于椭圆曲线密码学中的 2 个困难问题[10]。

定义 1　椭圆曲线 Diffie-Hellman 难题 (elliptic curve diffie-hellman problem, ECDHP)。设 G 是由椭圆曲线上的点组成的循环加群,它的阶是素数 q,P 是 G 的生成元。给定 $xP, yP \in G(x,y \in \mathbf{Z}_q^*)$,计算 xyP 是困难的。

定义 2　椭圆曲线离散对数难题 (elliptic curve discrete logarithm problem, ECDLP)。设 G 是由椭圆曲线上的点组成的循环加群,它的阶是素数 q,P 是 G 的生成元。给定 $xP \in G(x \in \mathbf{Z}_q^*)$,计算 x 是困难的。

2.2　系统模型

本文的参与者有 4 种,系统模型如图 1 所示。

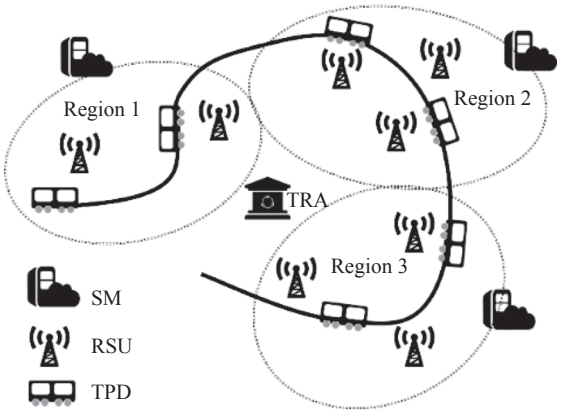

图 1　系统模型

1) 权威部门 (trusted authority, TA)。TA 是整个系统中唯一的可信第三方,负责车辆和服务节点的注册。同时,它还会参与群密钥协商。

2) 防篡改装置 (tamper-proof device, TPD)。TPD 是车辆上的安全设备。在 TA 注册后,TPD 负责秘密地存储车辆的假名和相应的密钥对。

3) 服务管理节点 (service manager, SM)。SM 是认证集群中的一个服务节点。在认证集群建成之前,它需要在 TA 注册。SM 提供多种服务,例如:验证车辆的认证请求;生成区域假名和相应密钥对;负责参与群密钥协商,生成会话密钥,维护集群内的公共账本等。

4) 路边单元 (roadside unit, RSU)。RSU 作为 SM 的下属,比 SM 分布更加广泛。此外,RSU 还负责认证消息的转发。

本文可能出现的符号,如表 1 所示。

2.3　安全需求

本文预期实现的安全目标如下。

1) 完整性。敌手不能篡改传输中的信息。

2) 匿名性。在认证过程中,敌手无法追踪车辆的真实身份。

3) 不可链接性。每个交通消息所使用的区域假名都是唯一的。即敌手无法分辨来自同一辆车的不同消息。

表 1 符号说明

符号	描述
TPD_i	V_i的防篡改设备
RID_{V_i}	车辆V_i的真实身份
PID_{V_i}	车辆V_i的假名
$(\mathrm{TVP}_i, \mathrm{NV}_i)$	PID_{V_i}对应的密钥
$\mathrm{RID}_{\mathrm{SM}_i}$	SM_i的真实身份
r_{SM_i}	SM_i的私钥
R_{SM_i}	SM_i的公钥
sk	TA的私钥
PK	TA的公钥
LPID_{V_i}	V_i的区域假名
LNV_i	LPID_{V_i}对应的私钥
LTVP_i	LPID_{V_i}对应的公钥
TSK_i	树私钥
TPK_i	树公钥
Sig	签名
L_t	有效期时间
T_1, T_2, T_3	时间戳
$X\|\|Y$	连接操作
$\oplus$	异或操作

4) 可追踪性。TA 可以追溯恶意车辆的真实身份。

5) 健壮性。集群内增删认证节点后,能够快速恢复集群内的信息同步。

3 群密钥协商协议

根据文献 [30] 提出的基于树的群密钥协商协议,本文实现了服务集群间的添加和删除操作。树的结构如图 2 所示,通用会话密钥的计算方法如下。

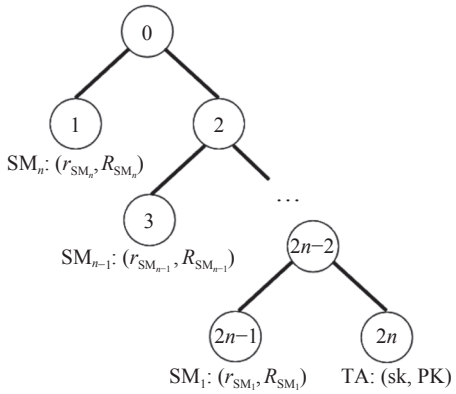

图 2 树的结构

1) 二叉树BT_n 满足 2 个特征。第一, BT_n的深度为n, 和已有 SM 数量一致。第二, BT_n是满二叉树, 且BT_n的根结点的右孩子为BT_{n-1}。

2) BT_n的每个节点通过数字$i(0 \leqslant i \leqslant 2n)$标记, 标记为奇数的节点是叶节点, 标记为偶数的节点($2n$除外) 是分支节点。每个节点都有自己的树私钥TSK_i和树公钥TPK_i, $\mathrm{TPK}_i = \mathrm{TSK}_i \cdot P$。其中, 标记为 $2n$的叶结点的树私钥为 TA 的私钥sk, $(\mathrm{sk} \in \mathbf{Z}_q^*)$, 标记为奇数的叶结点的树私钥为$\mathrm{SM}_j$的私钥$r_{\mathrm{SM}_j}(j = n-(i-1)/2)$。分支节点的私钥$\mathrm{TSK}_i$由等式(1)计算所得, 其中$h: \{0,1\}^* \to \mathbf{Z}_q^*$。

$$\mathrm{TSK}_i = h(\mathrm{TSK}_{i+1} \cdot \mathrm{TPK}_{i+2}) = h(\mathrm{TSK}_{i+2} \cdot \mathrm{TPK}_{i+1}) \tag{1}$$

3) 根节点的私钥TSK_0是集群间的会话密钥。

3.1 增加 SM

当集群出现无法继续提供服务的节点时, 需要新增备用节点。值得注意的是, 新增的 SM 设备也需要提前在 TA 进行注册。

为了描述群密钥协商协议中添加 SM 的情况, 假设已经加入群密钥协商进程的 SM, 按加入的时间顺序排序为$\{\mathrm{SM}_1, \mathrm{SM}_2, \cdots, \mathrm{SM}_{n-1}\}$。新增的 SM 为$\mathrm{SM}_n$。

1) 当需要新增SM_n到集群中时, SM_n向 TA 发起加入请求$\{\mathrm{RID}_{\mathrm{SM}_n}, \mathrm{Sig}_{r_{\mathrm{SM}_n}}(\mathrm{RID}_{\mathrm{SM}_n}), \mathrm{Join}\}$, Join 代表该消息是加入请求。

2) TA 在收到请求后, 根据$\mathrm{RID}_{\mathrm{SM}_n}$获取$\mathrm{SM}_n$的公钥$R_{\mathrm{SM}_n}$(TA 在$\mathrm{SM}_n$的注册阶段保存了$R_{\mathrm{SM}_n}$), 并对$\mathrm{Sig}_{r_{\mathrm{SM}_n}}(\mathrm{RID}_{\mathrm{SM}_n})$进行验证。若通过, 则更新二叉树, 将根节点作为新树的右孩子, 将SM_n作为新树的左孩子, 并计算新树的根节点的树私钥TSK_0和树公钥TPK_0。接着, TA 使用椭圆曲线数字签名算法(elliptic curve digital signature algorithm , ECDSA)对$h(\mathrm{TPK}_1, \mathrm{TPK}_2, n, T_3)$生成签名$\sigma$, 其中索引$n$用于协助各 SM 维护二叉树结构。最后, TA 广播$\{\mathrm{TPK}_1, \mathrm{TPK}_2, n, T_3, \sigma\}$给所有的 SM。

3) 在接收到$\{\mathrm{TPK}_1, \mathrm{TPK}_2, n, T_3, \sigma\}$后, $\mathrm{SM}_i(0 \leqslant 1 \leqslant n)$首先检查$T_3$的有效性, 然后根据 ECDSA 对$\sigma$和$h(\mathrm{TPK}_1, \mathrm{TPK}_2, n, T_3)$进行验证。若验证通过, SM_i计算TSK_0, 并将$\{\mathrm{TSK}_0, T_3\}$更新到自己的会话密钥列表。

为了具体地描述群密钥协商的添加操作, 以添加$\mathrm{SM}_1, \mathrm{SM}_2, \mathrm{SM}_3$为例, 如图 3 所示, 具体过程如下。

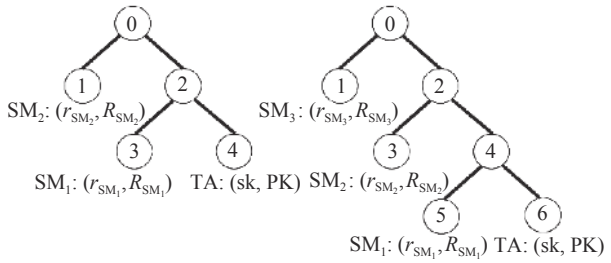

图 3　添加 SM

步骤 1, SM_1发送加入请求给 TA。TA 计算$TSK_0 = h(TSK_2 \cdot TPK_1) = h(sk \cdot R_{SM_1})$, $TPK_0 = TSK_0 \cdot P$, 并广播$\{TPK_1, TPK_2, 1, T_3, \sigma\}$给$SM_1$(TA 在 SM 注册阶段就已获悉$SM_1$的部分密钥$R_{SM_1}$)。在收到消息后, SM_1计算$TSK_0 = h(TSK_1 \cdot TPK_2) = h(r_{SM_1} \cdot PK)$。

步骤 2, SM_2发送加入请求给 TA。TA 计算 $TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_2})$, $TPK_0 = TSK_0 \cdot P$。其中, TSK_2就是步骤 1 中的TSK_0, TPK_2就是步骤 1 中的TPK_0。然后广播$\{TPK_1, TPK_2, 2, T_3, \sigma\}$给 SM_1、SM_2。对 SM_1而言, $TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_2})$。其中, TSK_2就是步骤 1 中的 TSK_0。对 SM_2而言, $TSK_0 = h(TSK_1 \cdot TPK_2) = h(r_{SM_2} \cdot TPK_2)$。

步骤 3, SM_3发送加入请求给 TA。TA 计算$TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_3})$, $TPK_2 = TSK_2 \cdot P$。其中, TSK_2就是步骤 2 中的TSK_0。然后广播$\{TPK_1, TPK_2, 3, T_3, \sigma\}$给 SM_1、SM_2、SM_3。对 SM_1和 SM_2而言, $TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_3})$, TSK_2就是步骤 2 中的TSK_0。对 SM_3而言, $TSK_0 = h(TSK_1 \cdot TPK_2) = h(r_{SM_3} \cdot TPK_2)$。

3.2　移除 SM

当服务节点出现故障无法继续提供服务时, 需要移除故障的节点。

为了描述群密钥协商协议中移除 SM 的情况, 假设集群中已经有n个服务节点, 而$SM_x(1 \leqslant x \leqslant n)$是需要被移除的节点。在移除操作中, 原来的$BT_n$变为$BT_{n-1}$, 标记为$2n-2x+1$的叶节点和标记为$2n-2x$的分支节点将会移除, 而$2n-2x+2$至$2n$的节点会上移一级。

步骤 1, SM_x主动发出移除请求$\{RID_{SM_x}, Sig_{r_{SM_x}}(RID_{SM_x}), Del\}$, Del 代表该消息为移除请求。

步骤 2, 在收到SM_x的移除请求后, TA 首先验证签名$Sig_{r_{SM_x}}(RID_{SM_x})$, 若通过, 则根据$RID_{SM_x}$检索$BT_n$。如果存在相应的树, 则更新树结构为$BT_{n-1}$, 并计算$BT_{n-1}$中所有需要更新的分支节点的树公钥和树私钥, 即标记为0至$2n-2x-2$的节点。然后, TA 使用 ECDSA 对$\{x, n, T_3, (2, TPK_2), \cdots, (2n-2x-2, TPK_{2n-2x-2})\}$进行签名。最后, 广播$\{x, n, T_3, (2, TPK_2), \cdots, (2n-2x-2, TPK_{2n-2x-2}), \eta\}$。

步骤 3, 在收到广播的消息后, 还存活的SM_i首先验证签名η, 然后根据x和n删除SM_x的叶节点和分支节点, 并根据更新后的分支节点的树公钥$\{TPK_2, \cdots, TPK_{2n-2x-2}\}$重构$BT_{n-1}$, 最后计算$TSK_0$。

为了更形象地描述上述操作中的群密钥协商过程, 以图 4 为例进行阐述。假设将SM_2从$\{SM_1, SM_2, SM_3, SM_4\}$组成的集群中移除, 并由剩余的$\{SM_1, SM_3, SM_4\}$协商出一个新的组密钥, 具体过程如下。

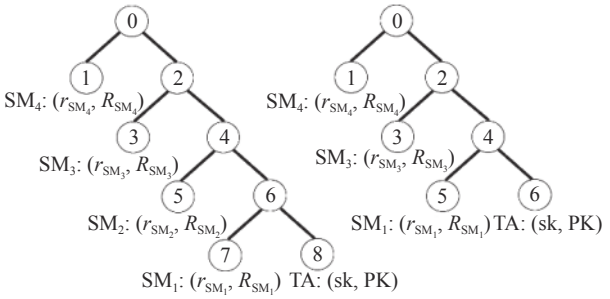

图 4　删除 SM

步骤 1, TA 将原来的树BT_4更新为新树BT_3, 将BT_4的TSK_6改为BT_3的TSK_4, 并计算$TSK_2 = h(TSK_4 \cdot TPK_3) = h(TSK_4 \cdot R_{SM_3})$, $TPK_2 = TSK_2 \cdot P$, $TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_4})$, $TPK_0 = TSK_0 \cdot P$。然后将$\{x = 2, TPK_2, TPK_4\}$发送给$\{SM_1, SM_3, SM_4\}$。

步骤 2, 对SM_1而言, 它先更新树的结构, 然后计算 $TSK_4 = h(r_{SM_1} \cdot PK)$, $TSK_2 = h(TSK_4 \cdot TPK_3) = h(TSK_4 \cdot R_{SM_3})$, $TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_4})$。

步骤 3, 对SM_3而言, 它先更新树的结构, 然后计算$TSK_2 = h(TSK_3 \cdot TPK_4) = h(r_{SM_3} \cdot TPK_4)$, $TSK_0 = h(TSK_2 \cdot TPK_1) = h(TSK_2 \cdot R_{SM_4})$。

步骤 4, 对SM_4而言, 它先更新树的结构, 然后计算$TSK_0 = h(TSK_1 \cdot TPK_2) = h(r_{SM_4} \cdot TPK_2)$。

4　认证方案

认证的一般流程, 如图 5 所示。在组网之前,

车辆和服务节点需提前注册,即车辆和服务器注册。在车辆加入自组网时,车辆从附近的节点获取区域假名,同时,服务节点间共享该区域假名,即认证及成员秘密生成阶段。加入组网后,车辆使用获取的区域假名签名交通消息,实现消息认证[31-33]。

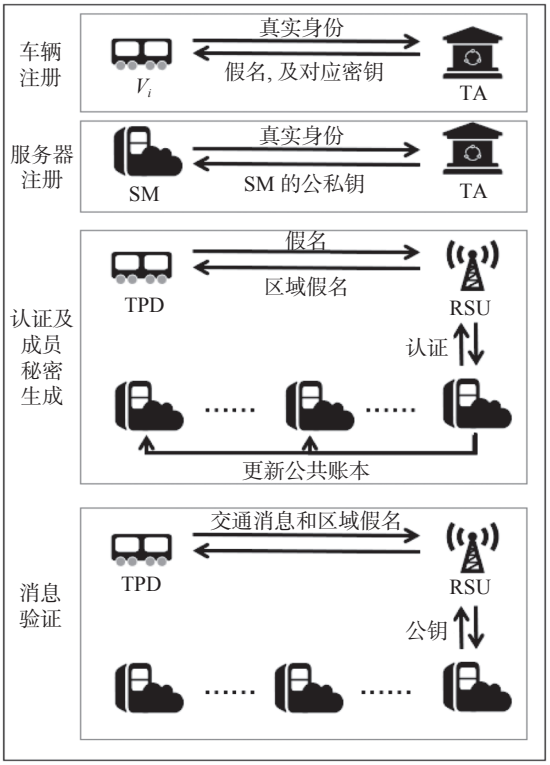

图 5 认证流程

4.1 初始阶段

在初始阶段,TA 首先选择一个由椭圆曲线上的点组成的加群G,G的阶为q,其生成元为P。然后,TA 生成系统私钥$\mathrm{sk}\in\mathbf{Z}_q^*$,并计算系统公钥$\mathrm{PK}=\mathrm{sk}\cdot P$。接着,TA 选择哈希函数$h:\{0,1\}^*\rightarrow\mathbf{Z}_q^*$。最后,TA 保留sk,并发布系统参数$\{G,P,\mathrm{PK},h\}$给所有的车辆和 SM。

4.2 车辆注册阶段

车辆在加入 VANETs 之前需要先在 TA 进行注册,在注册后,V_i 的 TPD 就获得了假名和对应的私钥。车辆注册的过程如下所述。

1)车辆V_i 通过专用信道提交它的真实身份RID_{V_i}给 TA。

2)收到请求后,TA 首先检查自己的车辆注册列表是否存在RID_{V_i}。若无,TA 生成一组随机数作为假名$\mathrm{PID}_{V_i}=\{\mathrm{PID}_{V_{i,0}},\mathrm{PID}_{V_{i,1}},\cdots,\mathrm{PID}_{V_{i,n-1}}\}$,以及一组$\mathrm{PID}_{V_i}$对应的私钥$(\mathrm{TVP}_i,\mathrm{NV}_i)=\{(\mathrm{TVP}_{i,0},\mathrm{NV}_{i,0}),\cdots,(\mathrm{TVP}_{i,n-1},\mathrm{NV}_{i,n-1})\}$,其中,$n$为每组元素的个数。首先,TA 产生$n$个随机数$(r_0,r_1,\cdots,r_{n-1})\in\mathbf{Z}_q^*$,并计算:

$$\begin{aligned}\mathrm{TVP}_{i,k}&=r_k\cdot P\\ \mathrm{NV}_{i,k}&=\mathrm{sk}+h(\mathrm{PID}_{V_{i,k}}\|\mathrm{TVP}_{i,k}\|L_t)\times r_k\end{aligned}\tag{2}$$

其中$0\leqslant k\leqslant n-1$。然后,TA 将$\{\mathrm{RID}_{V_i},\mathrm{PID}_{V_i},L_t\}$更新到车辆注册列表,并将$\{\mathrm{PID}_{V_i},(\mathrm{TVP}_i,\mathrm{NV}_i),L_t\}$通过专用信道返还给 TPD。

4.3 服务节点注册阶段

一个服务节点SM_i在被部署前,需要先在 TA 进行注册。服务节点注册过程如下所述。

1)服务节点SM_i通过专用信道提交它的真实身份$\mathrm{RID}_{\mathrm{SM}_i}$给 TA。

2)TA 在接收到$\mathrm{RID}_{\mathrm{SM}_i}$后,先检查自己的服务节点注册列表中是否存在$\mathrm{RID}_{\mathrm{SM}_i}$。若无,TA 生成$\mathrm{SM}_i$的私钥$r_{\mathrm{SM}_i}\in\mathbf{Z}_q^*$,并计算$R_{\mathrm{SM}_i}=r_{\mathrm{SM}_i}\cdot P$,$\mathrm{Sig}_{\mathrm{SM}_i}=\mathrm{Sig}_{\mathrm{sk}}(\mathrm{RID}_{\mathrm{SM}_i},R_{\mathrm{SM}_i})$,$\mathrm{Sig}_{\mathrm{SM}_i}$就是 TA 用系统私钥sk 对$(\mathrm{RID}_{\mathrm{SM}_i},R_{\mathrm{SM}_i})$的签名。然后,TA 将$\{\mathrm{RID}_{\mathrm{SM}_i},R_{\mathrm{SM}_i},L_t\}$更新到服务节点注册列表,并通过专用信道将$\{(r_{\mathrm{SM}_i},R_{\mathrm{SM}_i}),\mathrm{Sig}_{\mathrm{SM}_i},L_t\}$传给$\mathrm{SM}_i$。

4.4 认证及成员秘密生成阶段

当一个车辆V_i想要发送交通相关的消息时,会先检查是否还有未使用的区域假名。如果没有可用的区域假名,V_i的 TPD 需要向它所属的 SM 请求新的区域假名。这个阶段被称为认证及成员秘密生成阶段,细节如下。

1)V_i的TPD_i随机地选择一个从未使用过的假名$\mathrm{PID}_{V_{i,k}}$和$\mathrm{PID}_{V_{i,k}}$对应的私钥$(\mathrm{TVP}_{i,k},\mathrm{NV}_{i,k})$。随后,$\mathrm{TPD}_i$产生一个随机数$x\in\mathbf{Z}_q^*$,并计算:

$$\begin{aligned}X&=x\cdot P\\ V_1&=h(X\|\mathrm{PID}_{i,k}\|\mathrm{TVP}_{i,k}\|T_1)\times x+\mathrm{NV}_{i,k}\end{aligned}\tag{3}$$

其中T_1代表当前的时间戳。最后,TPD_{ti}将$\{X,\mathrm{PID}_{V_{i,k}},\mathrm{TVP}_{i,k},L_t,V_1,T_1\}$发送给附近的$R_j$。

2)当R_j收到消息后,会将该消息传递给它上级的服务节点,假设该节点为SM_i。

3)SM_i在收到认证消息后,首先查看时间戳T_1,检查是否在L_t的有效期内,然后,验证等式(4)是否成立。

$$\begin{aligned}V_1\cdot P=&h(X\|\mathrm{PID}_{V_{i,k}}\|\mathrm{TVP}_{i,k}\|T_1)\cdot X+\\ &\mathrm{PK}+h(\mathrm{PID}_{V_{i,k}}\|\mathrm{TVP}_{i,k}\|L_t)\cdot\mathrm{TVP}_{i,k}\end{aligned}\tag{4}$$

如果等式(4)成立,意味着TPD_i属于一个合法的车

辆。随后SM_i产生一组随机数作为V_i的区域假名,为

$$\mathrm{LPID}_{V_i}=\{\mathrm{LPID}_{V_{i,0}},\mathrm{LPID}_{V_{i,1}},\cdots,\mathrm{LPID}_{V_{i,m-1}}\}$$

以及一组区域假名对应的密钥对

$$(\mathrm{LTVP}_i,\mathrm{LNV}_i)=\{(\mathrm{LTVP}_{i,0},\mathrm{LNV}_{i,0}),\cdots,(\mathrm{LTVP}_{i,m-1},\mathrm{LNV}_{i,m-1})\}$$

其中m是每组元素的个数,并且$\mathrm{LTVP}_{i,l}=\mathrm{LNV}_{i,l}\cdot P,(0\leqslant l\leqslant m-1)$。接着$SM_i$获取当前时间戳$T_2$,计算:

$$\begin{aligned}\mathrm{CT}&=(\mathrm{LPID}_{V_i}\|\mathrm{LNV}_i)\oplus h(r_{\mathrm{SM}}\cdot X\|T_2)\\V_2&=h(\mathrm{LPID}_{V_i}||\mathrm{LTVP}_i||\mathrm{LNV}_i||T_2)\end{aligned}\tag{5}$$

并公开地将$\{\mathrm{CT},V_2,T_2\}$发送给TPD_i。同时,SM_i将$\{\mathrm{LPID}_{V_i},\mathrm{LTVP}_i\}$同步给集群内的其余节点。

4)TPD_i在接收到SM_i发送的消息后,会检查时间戳T_2的有效性,然后计算:

$$\begin{aligned}\mathrm{LPID}_{V_i}\|\mathrm{LNV}_i&=\mathrm{CT}\oplus h(x\cdot R_{\mathrm{SM}_i}\|T_2)\\\mathrm{LTVP}_i&=\mathrm{LNV}_i\cdot P\\V_2'&=h(\mathrm{LPID}_{V_i}||\mathrm{LTVP}_i||\mathrm{LNV}_i||T_2)\end{aligned}\tag{6}$$

并将计算出的V_2'和接收到的V_2比较,如果不相等,TPD_i结束这个会话,否则,TPD_i相信该消息来自合法的SM_i,并将$\{\mathrm{LPID}_{V_i},\mathrm{LTVP}_i,\mathrm{LNV}_i\}$存入内存。

4.5　信息同步阶段

在SM_i给车辆V_i返回消息$\{\mathrm{CT},V_2,T_2\}$的同时,它需要将区域假名相关的$\{\mathrm{LPID}_{V_i},\mathrm{LTVP}_i\}$通知给其余节点,用于实现集群的信息同步,细节如下。

1)假设由SM_i发起信息同步请求,首先,它会获取会话密钥列表中最新的会话密钥$\{\mathrm{TSK}_0,T_3\}$,检查时间戳T_3的有效性,然后计算$U_i=\mathrm{TSK}_0\oplus(\mathrm{LPID}_{V_i}\|\mathrm{LTVP}_i)$,并将$U_i$发送给其余$\mathrm{SM}_x,(x\neq i)$。

2)当其余 SM 收到U_i后,根据$(\mathrm{LPID}_{V_i}\|\mathrm{LTVP}_i)=\mathrm{TSK}_0\oplus U_i$计算出$\mathrm{LPID}_{V_i}$和$\mathrm{LTVP}_i$,然后保存。

4.6　消息验证阶段

消息验证应该是轻量级的,且满足条件隐私保护的。假设车辆V_i进入另一个地区,并且TPD_i的区域假名没有用完,消息验证的过程如下。

1)TPD_i随机地选择一个区域假名$\mathrm{LPID}_{V_{i,l}}$和相应的私钥$\mathrm{LNV}_{i,l}$,然后使用 ECDSA 对交通消息M_i生成一个签名$\mathrm{Sigma}_i=\mathrm{sig}_{\mathrm{LNV}_{i,l}}(\mathrm{LPID}_{V_{i,l}}\|M_i)$,接着$V_i$广播$\{\mathrm{LPID}_{V_{i,l}},\mathrm{Sig}_{M_i},M_i\}$给附近的车辆。

2)在接收到消息$\{\mathrm{LPID}_{V_{i,l}},\mathrm{Sig}_{M_i},M_i\}$后,车辆根据$\mathrm{LPID}_{V_{i,l}}$从集群获取$\mathrm{LTVP}_{i,l}$,并通过 ECDSA 验证签名$\mathrm{Sig}_{M_i}$是否合法。

5　安全分析

本章将对方案各阶段的安全性进行分析。其中,认证及成员秘密生成阶段的安全性将进行形式化分析,其余阶段的安全性将结合 2.3 节提出的安全需求进行非形式化分析。

5.1　形式化分析

根据文献 [30],该形式化分析被设计为一个包含敌手α和图灵机β的游戏。

α能够做出如下的问询。

1)初始询问。该询问模拟β初始化系统参数的功能,产生包括加群G和系统公私钥对$\{\mathrm{sk},\mathrm{PK}\}$在内的系统参数,最后,$\beta$将这些参数公布给$\alpha$。

2)车辆注册询问。该询问模拟α伪装成合法车辆进行注册的过程,最后,β返回PID_{V_i}给α。

3)车辆身份询问。该询问模拟β在收到PID_{V_i}后产生认证请求的过程。β会生成$\{X,\mathrm{PID}_{V_{i,k}},\mathrm{TVP}_{i,k},L_t,V_1,T_1\}$给$\alpha$。

4)SM 验证询问。这个询问模拟β在收到认证请求$\{X,\mathrm{PID}_{V_{i,k}},\mathrm{TVP}_{i,k},L_t,V_1,T_1\}$后,生成响应消息$\{\mathrm{CT},V_2,T_2\}$的过程。

敌手α是一个概率多项式时间攻击者,它有 3 个目标[31]。

1)伪造合法车辆V_i的认证请求消息。

2)模仿SM_i对V_i的认证过程。

3)伪造V_i的签名以获得其他合法车辆的信任。

定义 3　在公开信道中有 2 个参与者,分别为车辆V_i和服务节点SM_i。假设Π_Λ^s代表参与者Λ的实例s,$\Lambda\in\{V_i,\mathrm{SM}_i\}$。

定义 4　当满足如下关系时认为方案是安全的。

1)当它们是某次会话的通信双方时,Π_V^s和Π_{SM}^s接受彼此。

2)Π_V^s误认敌手α是Π_{SM}^s的可能性是可忽略不计的。

3)Π_{SM}^s误认敌手α是Π_V^s的可能性也是可忽略不计的。

5.1.1　安全的车辆认证

在方案中,如果h是理想的哈希函数,且Π_{SM}^s是被认可的,就不可能存在概率多项式时间攻击者能够伪造一个合法车辆的认证请求消息。

证明 假设在一个不可忽视的可能性ε下,敌手α能够伪造一个合法车辆的认证请求消息,那么β理应解决 ECDLP 难题。给定一个 ECDLP 实例$(\mathrm{TVP}_i = r \cdot P)$,$\beta$的任务就是计算$r$。此外,$\beta$会发布系统参数$\{G,P,\mathrm{PK},h\}$,并随机地选择一个真实的车辆身份$\mathrm{RID}_{\mathrm{VC}}$作为自己的挑战身份。$\alpha$的询问如下。

1)车辆注册问询。β维护一个身份列表L_{ID}。当α携带RID_{V_i}询问身份时,β在L_{ID}中查询是否存在该RID_{V_i}。如果存在,β返回对应的PID_{V_i}。否则,β进行如下操作。

a) 如果$\mathrm{RID}_{V_i} = \mathrm{RID}_{\mathrm{VC}}$,$\beta$产生 2 个随机的哈希数$r,c \in \mathbf{Z}_q^*$,计算$\mathrm{TVP}_i = r \cdot P$,并使$\mathrm{NV}_i = \perp$,$h(\mathrm{PID}_{V_i} \| \mathrm{TVP}_i \| L_t) = c$。然后将$\{\mathrm{PID}_{V_i}, r, \mathrm{TVP}_i, c, \mathrm{NV}_i, L_t\}$存入$L_{\mathrm{ID}}$,将$\{(\mathrm{PID}_{V_i} \| \mathrm{TVP}_i \| L_t), c\}$存入$L_h$。最后,$\beta$返回$\mathrm{PID}_{V_i}$给$\alpha$。

b) 如果$\mathrm{RID}_{V_i} \neq \mathrm{RID}_{\mathrm{VC}}$,$\beta$产生 2 个随机的哈希数$r,c \in \mathbf{Z}_q^*$,计算$\mathrm{TVP}_i = (r \cdot P - \mathrm{PK})/(c)$,并使$\mathrm{NV}_i = r$,$h(\mathrm{PID}_{V_i} \| \mathrm{TVP}_i \| L_t) = c$。然后将$\{\mathrm{PID}_{V_i}, r, \mathrm{TVP}_i, c, \mathrm{NV}_i, L_t\}$存入$L_{\mathrm{ID}}$,将$\{(\mathrm{PID}_{V_i} \| \mathrm{TVP}_i \| L_t), c\}$存入$L_h$。最后,$\beta$返回$\mathrm{PID}_{V_i}$给$\alpha$。

2)车辆身份询问。当β收到α包含有PID_{V_i}的问询后,β查看L_{ID}是否存在该PID_{V_i}。如果没有,β会再次运行车辆注册问询,产生新的$\{\mathrm{PID}_{V_i}, r, \mathrm{TVP}_i, c, \mathrm{NV}_i, L_t\}$并存入$L_{\mathrm{ID}}$。否则,$\beta$产生 2 个随机哈希数$\omega$,$\chi \in \mathbf{Z}_q^*$,计算$X = \chi \cdot P$,$V_1 = \chi \times \omega + r$,并使$h(X \| \mathrm{PID}_{V_i} \| \mathrm{TVP}_i \| T_1) = \omega$。然后将$\{(X \| \mathrm{PID}_{V_i} \| \mathrm{TVP}_i \| T_1), \omega\}$存入$L_h$。最后,$\beta$返回$\{\mathrm{PID}_{V_i}, \mathrm{TVP}_i, X, V_1, T_1\}$给$\alpha$。

3)SM 认证询问。β按照认证及成员秘密生成阶段进行操作,返回结果给α。

基于上述询问,α输出消息$\{\mathrm{PID}_{V_i}, \mathrm{TVP}_i, X, V_1, T_1\}$。$\beta$检查等式(7)是否成立。

$$V_1 \cdot P = \omega \cdot X + \mathrm{PK} + c' \cdot \mathrm{TVP}_i \tag{7}$$

如果等式 (7) 不成立,β结束该会话。如果α 能够伪造消息$\{\mathrm{PID}_{V_i}, \mathrm{TVP}_i, X, V_1', T_1\}$,$\alpha$将会被 SM 认可。根据文献 [32] 的引理 4 可得:

$$\begin{gathered}(V_1 - V_1') \cdot P = (c - c') \cdot \mathrm{TVP}_i = (c - c') \times r \cdot P \\ (V_1 - V_1') = (c - c') \times r\end{gathered} \tag{8}$$

因此,$(c - c')^{-1}(V_1 - V_1')$是 ECDLP 的解。而显然这是一个矛盾的假设。由此可得,不可能存在概率多项式时间攻击者能够伪造一个合法的车辆认证请求消息。

5.1.2 安全的 SM 认证

在方案中,如果h是安全的哈希函数,且Π_V^s是被认可的,就不可能存在概率多项式时间攻击者α能够伪造一个合法的 SM 响应消息。

证明 在一个不可忽视的可能性ε下,假设敌手α能够伪造一个合法 SM 响应消息,那么β在不可忽视的可能性下,理应能够解决 ECDHP 难题。给定一个 ECDHP 实例$(P, R_{\mathrm{SM}_i} = r_{\mathrm{SM}} \cdot P, X = x \cdot P)$,$\beta$的任务就是计算$r_{\mathrm{SM}} \cdot x \cdot P$。此外,$\beta$会发布系统参数$\{G,P,\mathrm{PK},h\}$和$R_{\mathrm{SM}_i}$。假设$\mathrm{RID}_{\mathrm{SC}}$是挑战身份,并且省略 5.1.1 节中重复的询问,β的询问如下。

1)车辆身份询问。β根据方案进行操作并返回$\{X, \mathrm{PID}_{V_i}, \mathrm{TVP}_i, L_t, V_1, T_1\}$。

2)SM 认证询问。β检查$\mathrm{RID}_{V_i} = \mathrm{RID}_{\mathrm{SC}}$是否成立。如果不成立,$\beta$按照认证及成员秘密生成阶段进行操作,返回$\{\mathrm{CT}, V_2, T_2\}$给$\alpha$。

基于上述询问,如果α能伪造消息$\{\mathrm{CT}, V_2, T_2\}$,车辆将认为$\alpha$是合法的 SM。但是,伪造$\{\mathrm{CT}, V_2, T_2\}$存在 2 个难点。

第一,α在没有r_{SM}的情况下无法推测出V_2。即推测成功的概率等于哈希碰撞的概率,概率为$1/2^{p/2}$,p是哈希数输出的比特长度。显然,这是可以忽略不计的。

第二,α即使获得了r_{SM},根据 ECDHP 难题,计算$r_{\mathrm{SM}} \cdot X$也是不可能的。

因此,不可能存在概率多项式时间攻击者能够伪造一个合法的 SM 响应消息。

5.2 非形式化分析

5.2.1 完整性

车辆注册阶段和服务节点注册阶段都由私有信道保证通信过程中的消息完整性。信息同步阶段因为使用会话密钥进行了加密,所以完整性也可以得到保障。最后,消息验证阶段的完整性由椭圆曲线数字签名算法 (ECDSA) 保证。

5.2.2 匿名性

因为集群处于封闭环境的缘故,所以本方案的匿名性主要体现在对车辆身份的保护上。即车辆和服务节点交互时的身份保护,以及车辆和其他车辆交流时的保护。在车辆和服务节点的交互中,它

使用的是假名PID_{V_i},无需提交真实的身份;在车辆和其他车辆交流时,它使用的是区域假名LPID_{V_i},而区域假名的分发过程对敌手是不可见的,所以敌手无法从区域假名逆推出车辆的假名,更无法获取车辆的真实身份。

5.2.3　不可链接性

因为每个区域假名只会被使用一次,所以对敌手而言,每条消息都是唯一的,即同一辆车的若干条消息之间是没有联系的,敌手无法逆推消息的来源。

5.2.4　可追溯性

当系统需要追溯恶意车辆的真实身份时,服务节点会从恶意消息中获取区域假名$\mathrm{LPID}_{i,l}$,并根据$\mathrm{LPID}_{V_{i,l}}$获取对应的假名信息$\mathrm{PID}_{V_{i,k}}$,然后将恶意车辆的假名信息$\mathrm{PID}_{V_{i,k}}$发送给 TA,由 TA 查阅车辆注册列表,找出真实身份。

5.2.5　健壮性

本方案的健壮性体现在认证集群中。当某个认证节点遭受攻击,无法正常提供服务时,集群内部需要快速删除瘫痪的服务节点,添加备用的服务节点,协商出新的会话密钥用于恢复各节点间的信息同步。本文方案的群密钥协商协议采用树状结构,协商密钥的速度快。添加操作只需要各节点在原会话密钥的基础上同步地计算一次;删除操作则根据被删除节点在树中所处深度的不同而有所不同,假设删除BT_n的节点的深度为m $(1<m\leqslant n+1)$,则深度大于m的各节点需要$m-2$次计算,而深度小于m的节点需要的次数为$x-1$ (x 为该节点的深度,即 1<x<m)。

6　性能分析

本章从计算开销、通信开销和安全性 3 个方面,将本文方案与文献 [20][29][30] 方案进行比较。计算开销主要取决于椭圆曲线点乘运算次数和 Hash 函数映射运算的执行次数。对于通信开销,根据车辆的请求消息的长度来评估[33]。在安全性方面,主要检查方案是否满足完整性、匿名性、不可链接性,以及方案是否实现集群模式等。在计算开销方面,测试的实验环境配置如表 2 所示,测得的各基础操作的计算开销如表 3 所示。

表 2　实验环境

项目	配置
CPU	Intel(R) Core(TM) i3-8 100 CPU at 3.60 GHz
RAM	4.00 GB
操作系统	Windows 10 Professional 64 bit version
运行环境	Java(TM) SE Runtime Environment (build 1.8.0_202-b08)

表 3　基础操作时间开销

符号	含义	时间/ ms
T_{hash}	一次hash函数运算时间	1
T_{mul}	一次椭圆曲线点乘运算时间	15

从表 4 可知,文献 [29] 基于属性加密,所以它的T_{mul}调用次数与 SM 的数量k相关,这导致该方案在 SM 数量较多时的计算效率较低。文献 [29] 还使用了区块链,它借助实用拜占庭容错算法来实现集群间的信息同步,故每轮的决策需要等待2/3k的节点进行响应。本文方案直接使用会话密钥发布消息,无需等待。

表 4　时间开销对比

方案	T_{hash}次数	T_{mul}次数	总开销/ms
文献[20]	5	3	50
文献[29]	5	k+3	15k+50
文献[30]	5	2	35
本文方案	5	2	35

表 5 为通信开销比较 。文献 [29] 的请求信息由$(V_1,V_2,\cdots,V_k,T,C)$组成,其中V是公钥的子秘密,长度为 128 bits,T是时间戳,长度为 13 bits,C为真实身份和随机数的签名,长度为 64 bits,故总长度为 (128k+77) bits。文献 [30] 的请求信息为$(\mathrm{ID}_j, T_j,\gamma_j,\mathrm{PID}_i,T_i,\alpha_i,K_i,R_i)$,其中$\gamma_j$为车辆身份信息的 Hash 签名 (SHA-256),α_i是 SM 对车辆身份的签名 (SHA-256),K_i为公钥长度为 128 bits,R_j为随机数,长度为 128 bits,ID_j和PID_i都是 13 bits,故总长度为 794 bits。文献 [20] 的请求信息为$\{X,\mathrm{CT}_1,V_1,T_1\}$,其中$X$为随机数,长度为 128 bits,$T_1$为时间戳,长度为 13 bits,$\mathrm{CT}_1$为签名,长度 128 bits,$V_1$为校验码,长度 128 bits,总长度为 397 bits。本文的请求消息为$\{X,\mathrm{PID}_{V_{i,k}},\mathrm{TVP}_{i,k},L_t,V_1,T_1\}$,其中$X$为随机数,长度为 128 bits,$T_1$为时间戳,长度为 13 bits,$\mathrm{TVP}_{i,k}$为

公钥, 长度 128 bits, V_1为校验码, 长度 128 bits, 总长度为 397 bits。

表 5 通信开销比较

方案	通信开销总长度/bits
文献[20]	397
文献[29]	128k+77
文献[30]	794
本文方案	397

在安全性方面: 文献 [20] 和 [30] 没有实现集群模式; 文献 [29] 虽然实现了集群, 但是没有考虑不可联接性的问题; 本文满足所有安全需求和场景假设。其比较内容如表 6 所示。

表 6 安全性比较

方案	完整性	匿名性	不可联接性	集群模式
文献[20]	√	√	√	×
文献[29]	√	√	×	√
文献[30]	√	√	×	×
本文方案	√	√	√	√

综上所述, 与文献 [20][29][30] 相比, 本文方案在计算开销和通信开销都更加优秀。在与文献 [30] 的性能持平的情况下, 本方案的应用场景更加丰富, 安全性也更强。

7 结束语

本文提出了一种车载自组网中基于密钥协商的条件隐私保护认证方案。其优势为: 1) 通过引入匿名认证技术使车辆发送的消息满足不可链接性, 即敌手无法关联来自同一辆车的不同区域假名; 2) 通过认证服务集群实现认证的去中心化, 并借助群密钥协商协议来保障集群的健壮性。

在未来的工作中, 笔者计划引入聚合技术来进一步降低 SM 的计算开销。此外, 设计另一种更高效的车联网认证方案也是努力的方向。

参 考 文 献

[1] LIN C, HE D, HUANG X, et al. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020(99): 1 − 13.

[2] KENNEY J B. Dedicated short-range communications (DSRC) standards in the United States[J]. Proceedings of the IEEE, 2011, 99(7): 1162 − 1182.

[3] ATLAM H F, ALENEZI A, ALHARTHI A , et al. Integration of cloud computing with internet of things: challenges and open issues[C]// 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). [S. l.] : IEEE, 2017: 670 − 675.

[4] HOU X, LI Y, CHEN M, et al. Vehicular fog computing: a viewpoint of vehicles as the infrastructures[J]. IEEE Transactions on Vehicular Technology, 2016: 3860 − 3873.

[5] LIU Y, WANG L, CHEN H H. Message authentication using proxy vehicles in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(8): 3697 − 3710.

[6] ALI H, SYED A A, WARIP M M, et al. Classification of security attacks in VANET: a review of requirements and perspectives[J]. MATEC Web of Conferences, 2018, 150: 06038.

[7] AZEES M, VIJAYAKUMAR P, 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.

[8] ZHENG D, JING C, GUO R, et al. A traceable blockchain-based access authentication system with privacy preservation in VANETs[J]. IEEE Access, 2019, 7: 117716 − 117726.

[9] LU Z, QU G, LIU Z. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2018: 1 − 17.

[10] 曾晟珂, 陈勇, 夏梅宸.车载自组网的隐私保护问题 [J].西华大学学报 (自然科学版), 2015, 34(4):1 − 7.

[11] CHEN Q, SHI S, LI X, et al. SDN-based privacy preserving cross domain routing[J]. IEEE Transactions on Dependable & Secure Computing, 2018, 16(6): 930 − 943.

[12] CUI J, ZHANG X, ZHONG H, et al. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment[J]. IEEE Transactions on Information Forensics and Security, 2019, 6: 1654 − 1667.

[13] HE D B, ZEADALLY S, KUMAR N, et al. Anonymous authentication for wireless body area networks

with provable security[J]. IEEE Systems Journal, 2017, 11(4): 2590 − 2601.

[14] HE D, KUMAR N, WANG H, et al. A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network[J]. IEEE Transactions on Dependable & Secure Computing, 2017, 15(4): 633 − 645.

[15] ZHANG Q K, GAN Y, ZHANG Q X, et al. A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application[J]. IEEE Access, 2018, 6: 24064 − 24074.

[16] RAYA M, HUBAUX J P. Securing Vehicular ad hoc networks[C]// Journal of Computer Security. [S. l.] : IOS Press, 2007: 39 − 68.

[17] WANG S, MAO K, ZHAN F, et al. Hybrid conditional privacy-preserving authentication scheme for VANETs[J]. Peer-to-Peer Networking and Applications, 2020, 13(12): 1600 − 1615.

[18] VIJAYAKUMAR P, AZEES M, KANNAN A, et al. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(4): 1 − 14.

[19] YING B, NAYAK A. Anonymous and lightweight authentication for secure vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 10626 − 10636.

[20] LIU Z C, XIONG L, PENG T, et al. A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Access, 2018, 6: 26307 − 26317.

[21] DENG X , XIN X , GAO T . A location privacy protection scheme based on random encryption period for VSNs[J]. Journal of Ambient Intelligence & Humanized Computing, 2019, 11(3):1351 – 1359.

[22] RAN C, KRAWCZYK H . Universally composable notions of key exchange and secure channels[C]// International Conference on the Theory & Applications of Cryptographic Techniques: Advances in Cryptology. Springer Berlin Heidelberg: Springer, 2002, 2332: 337 – 351.

[23] HUANG J L, YEH L Y, CHIEN H Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions On Vehicular Technology Vt, 2011, 60(1): 248 – 262.

[24] MEJRI M N, ACHIR N, HAMDI M. A new group diffie-Hellman key generation proposal for secure VANET communications[C]// 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC).[S.l.]: IEEE, 2016: 992 – 995.

[25] ZHANG Q K, GAN Y, ZHANG Q X, et al. A Dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application[J]. IEEE Access, 2018, 6:24064 – 24074.

[26] HE D, KUMAR N, WANG H, et al. A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network[J]. IEEE Transactions on Dependable & Secure Computing, 2017, 15(4):633 – 645.

[27] XIONG L, LI F, HE X M, et al. An efficient privacy-aware authentication scheme with hierarchical access control for mobile cloud computing services[J]. IEEE Transactions on Cloud Computing, 2020(9): 1 − 15.

[28] WANG W , NING H , XIN L . BlockCAM: A blockchain-based cross-domain authentication model[C]// 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC).[S.l.]: IEEE, 2018: 896 − 901.

[29] YAO Y, CHANG X, MISC J, et al. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775 − 3784.

[30] WEI L, CUI J, ZHONG H, et al. Proven secure tree-based authenticated key agreement for securing v2v and v2i communications in VANETs[J]. IEEE Transactions on Mobile Computing, 2021, 21(9): 3280 − 3297.

[31] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(12): 2681 − 2691.

[32] POINTCHEVAL, D STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361 − 396.

[33] LU R, LIN X, ZHU H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[C]//Infocom the Conference on Computer Communications IEEE. [S. l.] : IEEE, 2008: 1229 − 1237.

（编校：饶莉）