车载网络中基于密钥驱动信任机制的身份认证协议

戴银飞[1],周秀贞[1],范子尧[1],刘镕源[2],刘志远[1],王绍强[1],杜 伟[1]

(1.长春大学 计算机科学技术学院,长春 130022;2.长春工业大学 计算机科学与工程学院,长春 130102)

摘 要:首先,针对车载自组网(VANET)中的安全和隐私问题,提出了一种基于密钥协商的身份认证和安全信任方案。其次,采用基于椭圆曲线密码体制生成签名,提出了一种低消耗的密钥分配方案,通信双方交换参数以相互验证并安全地生成会话密钥。最后,通过三向双路认证方式对通信实体进行身份认证。经安全性和性能分析,表明本文方案可提高身份认证效率,降低系统开销,具有较好的理论和应用价值,系统结合网络安全等级保护第三级要求标准进行部署,能够解决车载自组网中身份隐私保护和安全信任问题。

关键词:网络安全与通信安全;车联网;椭圆双曲线密码体制;密钥协商;身份认证

中图分类号:TP393.08 **文献标志码**:A **文章编号**:1671-5497(2025)05-1788-10

DOI:10.13229/j.cnki.jdxbgxb.20240599

Key-driven trust mechanisms for identity authentication in vehicular networks

DAI Yin-fei[1],ZHOU Xiu-zhen[1],FAN Zi-yao[1],LIU Rong-yuan[2],
LIU Zhi-yuan[1],WANG Shao-qiang[1],DU Wei[1]

(1. *College of Computer Science and Technology*, *Changchun University*, *Changchun* 130022, *China*; 2. *School of Computer Science and Engineering*, *Changchun University of Technology*, *Changchun* 130102, *China*)

Abstract: Firstly, a key negotiation based authentication and security trust scheme is proposed for security and privacy issues in vehicular ad-hoc network (VANET). Secondly, an elliptic curve cryptosystem based signature generation is used, and a low-consumption key distribution scheme is proposed, where the communicating parties exchange parameters to mutually authenticate and securely generate session keys. Finally, the communicating entities are authenticated by three-way two-way authentication. After security and performance analysis, it shows that the scheme can improve the efficiency of identity authentication and reduce the system overhead, which has good theoretical and application value, and the system is deployed in conjunction with the Network Security Level Protection level 3 requirements standard, which can solve the identity privacy protection and security trust problems in the in-vehicle self-organizing network.

收稿日期:2024-05-30.

基金项目:吉林省科技厅重点研发产业关键核心技术攻关项目(20220201154GX);吉林省教育厅科学技术研究项目(JJKH20240745KJ).

作者简介:戴银飞(1977-),女,教授,博士.研究方向:网络与信息安全,人工智能.E-mail:daiyf@ccu.edu.cn

通信作者:王绍强(1976-),男,教授,硕士.研究方向:网络与信息安全,人工智能.E-mail:xiu1232024@163.com

Key words: network security and communication security; vehicular ad hoc-network; elliptic hyperbolic signature; key agreement; identity authentication

0　引　言

智能交通系统(Intelligent transportation system, ITS)在其大规模使用与进步的历程里，车载自组网(Vehicular ad-hoc network, VANET)扮演了关键角色。路侧单元(Road side units, RSU)、车载单元(On board units, OBU)和可信管理局(Trusted authority, TA)是参与 VANET 的3个实体。为了保证系统的安全性和可靠性，TA 作为值得信赖的第三方，负责监督和验证每个机构的权威性和真实性。作为基础设施和汽车的代表，OBU 和 RSU 通过与 TA 的交互实现安全通信和身份识别，从而促进车联网系统的无缝运行[1]。

由于VANET，车辆可以各种方式协同工作和通信。但随着 VANET 的迅速发展，安全问题也引起了人们的关注。特别是在车辆之间的通信中，确保身份验证和安全信任的问题是一个至关重要的挑战。车对车(Vehicle-to-vehicle, V2V)和车对基础设施(Vehicle-to-infrastructure, V2I)是 VANET 系统通信机制的两大类[2]。然而，这两种通信形式都基于公共无线网络，而公共无线网络具有开放性和其他特性，使恶意用户可以瞄准任何车对车联网节点，从任何角度和位置入侵网络，并窃取车辆用户的个人数据，从而危及其安全。安全信任是车联网产业健康发展的前提。通过建立证书管理系统，采用数字证书、数字签名、数据加密等技术建立车路云之间的安全信任体系，除确保信息在传输过程中不被伪造、篡改或重放外，它还实现了对信息来源的认证，确保信息的合法性，防止反重放攻击，并维护终端实际身份和位置信息的机密性。另外，它还能防止用户隐私泄露[3]。

本文旨在提供一种基于密钥协商的安全信任机制，可用于车联网的身份验证。采用基于椭圆曲线密码体制生成签名；配合提出的一种无条件安全的密钥分配方案，通信双方交换参数以相互验证并安全地生成会话密钥；通过三向双路认证方式对通信实体进行身份认证。首先，对椭圆曲线密码与困难问题进行简单的介绍。其次，详细介绍基于密钥协商的身份验证安全信任方案的设计理念和过程。包括如何生成和分发安全认证密钥，以及如何保证通信的私密性和完整性。最后，通过测试验证了基于密钥协商的认证安全信任机制的有效性和性能。本文将评估该方案的安全性、计算复杂性和通信开销，以便进一步改进和增强。

1　相关工作

在使用数字签名方法验证信息时，人们会暴露自己的身份信息，传统算法无法满足保护车辆身份的要求。因此，匿名认证是常用技术之一，即车辆可使用假名与其他通信实体进行通信，满足身份隐私保护的可认证性和匿名性，同时，权威机构可根据车辆的一些行为，决定是否废除已颁发给其的假名证书，满足可撤销性[4]。

车联网身份认证方案是保证车辆网络连接安全的最重要技术之一。随着远程信息处理技术的发展，传统的基于密码学的身份认证系统虽然仍能满足车辆身份认证的基本需求，但是面对更加复杂的网络安全威胁，其功效正在逐渐丧失。因此，为了提高车辆联网的安全性和有效性，研究人员提出了许多创新和改进的认证方案。学术界对与车联网相关的隐私保护认证技术进行了大量的研究[5-8]。为了实现匿名通信，汽车和RSU可以使用自行生成的匿名证书。然而，这一方法需要预先存储大量的虚假身份，从而增加了存储负担。对此，Azees等[9]提出了一种名为高效匿名身份验证的条件隐私保护(EAAP)方案，旨在解决这一问题。2020年，杨晓东等[10]提出了一种基于身份聚合签名的信息认证技术。在该方案中，多条信息的验证被合并成一个简短的签名，通信双方只需验证合并签名，即可快速判断签名的有效性，有效缩短通信实体对通信消息的认证时间。

一种基于零知识识别(Feige-fiat-shamir, FFS)方案的改进身份认证方案被Han等[11]提出，该方案通过零一逆转和二对一验证方法解决了FFS无法有效抵抗猜测攻击的问题，并且在相同参数下，相比现有方案，能在6.1 ms内完成认证，减少了额外的认证延迟。此外，一种基于区块链技术的高效匿名认证方案也被陈葳葳等[12]提出，

利用区块链的防篡改和分布式特性来完成车辆临时身份的生成和存储,实现了高效的双向身份认证。Pournaghi等[13]提出一种新颖高效的条件隐私保护认证方案,称为NECPPA。NECPPA采用基于群签名的认证机制,允许车载单元匿名地进行通信和认证。同时引入了条件隐私保护机制,即在特殊情况下(如事故发生)可以撤销车载单元的匿名性,以支持事后溯源。该方案在安全性和性能方面都优于现有的VANET认证方案,具有较强的实用价值。Wang等[14]提出一种新型的条件隐私保护证书式聚合签名方案,该方案结合证书式密钥生成、条件隐私保护和聚合签名,在保护车载单元隐私的同时提高了通信效率,是一种创新的认证机制。其可以在标准模型下实现支持匿名认证、条件隐私保护和聚合签名等安全特性。文献[15]提出一种高效的证书式聚合签名方案,用于VANET中的安全路由。该方案结合证书式密钥生成和聚合签名,在确保VANET路由安全的同时提高了通信效率,是一种创新的认证机制,在安全性和性能方面都优于现有的VANET路由认证方案,具有较强的实用价值。文献[16]设计了一种无证书的批量密钥协商方案。基于ECDLP困难性假设设计了一种安全的密钥协商过程进行车辆节点的合法身份认证,能够对多辆车同时进入区域时进行批量处理。改善了传统密钥管理系统中身份认证过程计算复杂度高、通信开销大的问题,在保证安全性的前提下提高了通信效率,并减轻了车辆单元和路边单元的计算负担。

此外,还有基于SGX的车联网身份认证协议,该协议将身份认证过程中的主要计算工作从可信代理(TA)卸载到路边基站单元(RSU)内完成,实现了分布式计算,同时利用可信硬件存储主密钥,提高了安全性和实时性[17]。

基于上述相关研究发现,车联网可能会给基于密码学的传统认证技术带来一些挑战。例如,量子计算的脆弱性、管理和分发密钥的难度以及高昂的传输成本[18]。因此,基于密钥协商的身份验证安全信任系统作为解决这些问题的有用解决方案应运而生。

2 预备知识

椭圆曲线密码算法(Elliptic curve cryptography, ECC)是基于椭圆曲线数学的一种公钥密码算法,其安全性依赖于椭圆曲线离散对数问题(Elliptic curve discrete logarithm problem, ECDLP)的困难性[19]。

在为高效设计方案选择加密算法时,计算难度问题和相关安全参数是需要考虑的重要因素[20]。本文提出的方案中采用的国密SM2公钥密码算法是基于密码学中有限域上椭圆曲线有理点群上离散对数的困难问题。

定义:乘法群Z_p^*上的离散对数问题(Discrete logarithm problem, DLP)。

给定一个素数p,乘法群Z_p^*上的生成元g,以及Z_p^*上的随机选取的元素y,寻找整数x,$1\leqslant x\leqslant p-2$,使得$y=g^x \bmod p$。

困难问题:椭圆曲线离散对数难题。

设p为某个大素数,E是GF(P)上的椭圆曲线,设G是E的一个循环子群,P是G的一个生成元,$Q\in G$。已知P和Q,给定$nP=Q$,$0\leqslant n\leqslant \mathrm{ord}(P)-1$,计算$n$是困难的。

3 车载自组网消息认证方案

3.1 系统模型

车载自组网通信安全实体关系参考模型如图1所示,实线表示V2X (Vehicle to everything)设备之间的通信关系,虚线表示实体之间的授权关系。

本文针对车载自组网通信实体进行身份认证及消息传输过程中可能涉及的不安全问题,根据车载自组网自身特点,提出一种基于密钥协商的身份认证和安全信任方案。方案包括伪随机数的生成、消息签名、密钥协商算法及身份认证方法等阶段。方案的部分符号说明如表1所示。

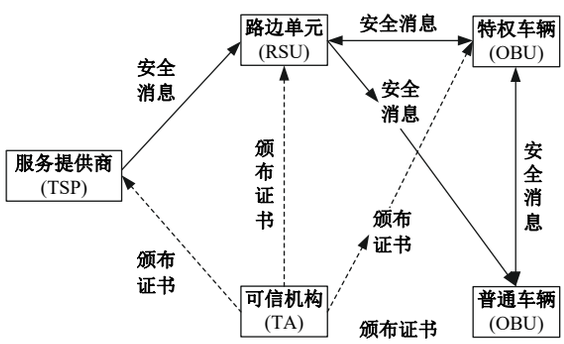

图1 车联网通信安全实体关系参考模型

Fig. 1 Reference model of entity relationship for vehicle network communication security

表 1 方案的部分符号说明

Table 1　Description of some of the symbols of the program

符号	含义
sk，Q	系统私钥及其对应公钥
G	基点
a，b	椭圆曲线方程的参数
UserId	签名者标识符
len	UserId的长度
AC	认证证书
SK	会话密钥
m	待签名的消息
$x\|\|y$	x与y的拼接，其中x、y可以是比特串或字节串
$[k]P$	椭圆曲线上点P的k倍点

3.2　身份认证方案

3.2.1　伪随机数的生成

RSU 在汽车网络中用于与其他汽车共享数据和通信。认证方案的伪随机数生成步骤用于保护车辆的身份和保证通信安全。在这一阶段，车辆（OBU）接收来自 RSU 的随机数形式的挑战。车辆收到挑战后，使用匹配的密钥和算法进行计算和加密，然后生成响应并将其传送回 RSU，RSU 使用预先共享的密钥和算法验证响应和车辆的身份。作为认证程序的一部分，RSU 在这一步骤中开始创建伪随机数。RSU 创建并发送挑战，同时确认车辆的回答，充当通信的控制方和可信方。这样做的目的是保护车辆身份、确保通信安全并阻止伪造。

系统实现真随机数通常需要生物特征或者其他物理方法，获取的随机数的随机性和精度不够，并且实现起来较为复杂，因此在实际中多采用伪随机数替代真随机数。采用 ANSI X9.17 伪随机生成器，使用一次 3DES 加密算法生成伪随机数，生成过程如图 2 所示。

首先，输入两个 64 位的随机数。$\mathrm{DateTime}_i$ 代表系统当前的日期和时间，每生成一个新的随机数 R_i 时，$\mathrm{DateTime}_i$ 都会更新。Seed_i 则是第 i 个随机数的生成种子，初始值可以任意设定，并且与 $\mathrm{DateTime}_i$ 一样，每次生成新的随机数时都会更新。在加密过程中，使用两个固定的 56 位密钥 K_1 和 K_2 进行三重加密。这两个密钥必须保持保密。最终，该过程生成两个数据：一个 64 位的伪随机数 R_i 和一个 64 位的新种子 Seed_{i+1}。加密操作 EDE_{K_1,K_2} 指的是使用固定的 56 位密钥 K_1 和 K_2 对输入数据进行加密。即

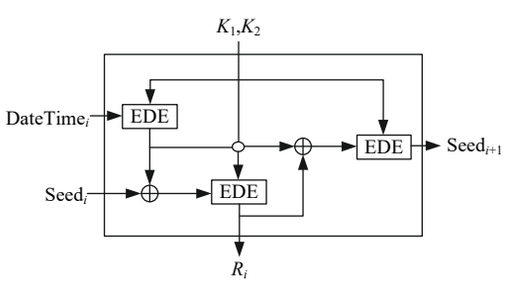

图 2　伪随机数生成过程图

Fig. 2　Pic pseudo-random number generation process

$$R_i = \mathrm{EDE}_{K_1,K_2}(\mathrm{EDE}_{K_1,K_2}(\mathrm{DateTime}_i) \oplus \mathrm{Seed}_i)$$

$$\mathrm{Seed}_{i+1} = \mathrm{EDE}_{K_1,K_2}(\mathrm{EDE}_{K_1,K_2}(\mathrm{DateTime}_i) \oplus R_i)$$

3.2.2　消息签名

基本安全消息（Basic safety message，BSM）的发送方需要首先执行证书一致性检查，通过检查证书撤销列表（Certificate revocation list，CRL）以确定签名证书是否被撤销，同时对签名证书的有效期、地域区域、权限描述等进行确认，然后利用 SM3 杂凑密码算法计算 BSM 的摘要值，并将消息连同摘要值的签名一同广播出去；签名验证方接收到包含数字签名和签名证书的消息后，将针对签名证书构建验证路径，并对验证路径上的每个证书进行证书一致性检查，未能通过检查的证书则不能用于验证消息签名操作。

消息签名及验证过程描述如下：

（1）参数设置

在初始化阶段，首先选择椭圆曲线 $E: y^2 = x^3 + ax + b$。设 $G_P(P)$ 为有限域，选择 E 上一点 $G \in E$，G 的阶为满足安全要求的素数 n，即 $nG = O$（O 为无穷远点）。选择随机正整数 sk，$sk \in [1, n-1]$，计算 Q，使 $Q = [sk] \cdot G$，则 Q 为公钥，sk 为私钥，长度为 32 字节。设待发送的消息为比特串。

（2）签名生成阶段

要传输数据，车辆必须以数据发送方的身份生成签名。签名生成阶段发生在车辆内部，OBU_i 对消息 m_i 进行签名。在签名生成阶段，车辆使用私人密钥为要传输的数据创建数字签名。为保持其匿名性，私钥通常保存在车内一个受保护的存储器中。原始数据和创建的数字签名会被传送给接收方，如路边设备或另一辆汽车。

设 UserId 为签名者的标识符；len 为 UserId 的长度；x_G、y_G 为椭圆曲线方程参数 G 的坐标；x_A、y_A 为 Q 的坐标。

① $m' = Z_A \| m$，$m \in M$，为待签名的消息，M 为消

息空间。其中 $Z_A=H(\text{len}\|\text{UserId}\|a\|b\|x_G\|y_G\|x_A\|y_A)$;$H$为SM3密码散列函数,产生固定长度256位哈希值;

②计算$h=H(m')$;

③用伪随机数发生器生成随机数R_i,$R_i\in[1,n-1]$,计算椭圆曲线点$(x_A,y_A)=[R_i]\cdot G$,进一步得$k=(h+x_A)\bmod n$;

④计算$S=\left((1+sk)^{-1}\cdot(R_i-k\cdot\text{sk})\right)\bmod n$。如果$k=0$或者$S=0$,则另生成随机数$R_i$,重新执行③~④。消息$m$的签名为$(k,S)$。

当车辆行驶入某一RSU的负责区域内时,将参数$\{Q,\text{UserId},Z_A,G,n,k,S\}$发送给RSU。

(3)验证签名

RSU接收到的消息为m'。RSU在接收到OBU传送的$\{Q,\text{UserId},Z_A,G,n,k,S\}$签名消息之后,RSU进行验证签名计算得到$K$值,将验证签名所得的$K$值与签名生成阶段所得到的$k$进行比较,若相等则通过验证,否则失败。详细过程如下:

①$m^*=Z_A\|m'$,$m\in M$,为待签名的消息,M为消息空间。

②计算$h'=H(m^*)$;

③$u=(k+S)\bmod n$,若$u=0$,则验证不通过;

④计算椭圆曲线点$(x_1,y_1)=[S]G+[u]Q$;

⑤将x_1的数据类型转换为整数,计算$K=(h+x_1)\bmod n$,检验$K=k$是否成立,若成立则验证通过,否则验证不通过。

3.2.3 密钥协商

在车联网中,车辆之间要进行密钥协商,以建立安全的通信链路。车辆之间可以是同一车队的车辆之间、相邻车辆之间,也可以是交通流中任何两辆车之间。

密钥协商是通信双方为防止通信信道不安全,共同合作生成同一个会话密钥的机制,即使中间传递过程中重要消息被截获,敌手也无法根据窃取的消息计算出会话密钥[21]。通常使用的密钥协商协议(Key agreement protocal, KAP)是Diffle-Hellman算法,可以实现会话密钥的保密性且可防止窃听,但该算法不支持认证,无法抵抗篡改及重放攻击。通常此算法会与另外的签名算法协议协同使用,如RSA、DSA算法,密钥的安全与密钥的长度有关。随着计算机运算能力的提高,要求安全密钥也越来越长,计算开销和通信开销也随之增加,同时RSA算法的加解密速度也限制了其无法有效地应用于计算能力受限的系统中。

为解决上述问题,本文中提出了一种轻量化的密钥分配方案。在此方案阶段包括3个步骤,通信双方交换参数以相互验证并安全地生成会话密钥。

(1)最初,l_i、m_i和n_i是由OBU_i节点生成的3个随机数,然后使用节点的私钥sk进行身份验证。不过,有时会混合使用随机数和私钥,以确保私钥的安全,并阻止攻击者伪造攻击。参数parameters_i就是这种组合的结果,计算公式如下:

$$\text{parameters}_i=H((\text{sk}*l_i)\|m_i)$$

接下来,将随机数n_i和基点进行标量相乘,得出参数T,这一步由OBU_i节点生成。除作为协议验证机制的有效参数外,该参数还用于生成会话密钥。通过上述计算还可生成身份验证证书AC,计算方法如下:

$$\text{AC}=H(\text{parameters}_i\|\text{UserId}\|\text{sk})$$

在生成参数T之后,必须制定一个方法来保证RSU_i节点S_i接收到的值的正确性,同时还要创建一个多重验证方法。为此,OBU_i节点按以下公式生成参数s_i:

$$s_i=H(\text{AC}\|\text{parameters}_i\|T)$$

使用公钥Q对参数s_i、T和parameters_i进行加密,并将它们发送到节点S_i中。

(2)本步骤中,节点S_i接收OBU_i节点加密后的消息,消息中携带参数parameters_i、s_i、T。

第一阶段验证OBU_i节点的身份及其提供的参数。节点S_i通过计算s_i'的值并将其与节点发送的参数s_i进行比较来完成验证。对参数的任何修改都会导致从OBU_i节点获得的值与S_i计算的参数之间出现差异,这种差异会导致通信实体中断。如果数值相等,S_i将继续执行协议流程,表明信息准确无误。S_i选择一个随机数x_i,并在确认信息后按以下公式生成会话密钥:

$$\text{SK}=H(\text{AC}\|s_i\|x_i\cdot T)$$

节点S_i计算出会话密钥后,生成R值来验证自身并验证OBU_i节点发送的参数。最后,它向节点发送一条使用密钥加密的消息。

$$R=H(s_i\|\text{SK}\|\text{AC})$$

(3)验证节点S_i及其提交的参数是密钥协商

程序的最后一个阶段。首先生成会话密钥节点，然后为这些操作生成会话密钥，并计算R'的值。参数的计算方法如下：

$$SK'=H\left(AC||s_i||R\|x_i\cdot n_i\cdot G\right)$$

$$R'=H\left(s_i||SK'||AC\right)$$

OBU_i节点利用节点S_i发送的自身拥有的参数生成会话密钥，然后生成R'参数。然后，通过检查R'和R这两个值来检查参数的准确性。如果这两个值相等，则意味着发送的信息是正确的，否则连接会丢失。最后，通过确认信息的准确性，选择生成的SK的值作为会话密钥。

3.2.4　身份认证

基于公钥密码的实体认证的优势在于可以利用数字签名提供抗抵赖性，不需要可信第三方[22]。车联网通信设备首先向注册CA申请认证并获得注册证书，然后利用注册证书向假名CA、应用CA等应用授权机构申请实际用于基本安全消息BSM的V2X通信证书。为保护车辆隐私，假名证书注册机构PRA接受车载单元OBU的假名证书申请，对OBU提供的假名证书种子密钥进行扩展，从链接机构LA获取对应的证书链接值后，基于扩展的密钥和链接值生成假名证书生成请求并发送给假名证书CA，从假名证书CA获取OBU的假名证书并发送给OBV。

X.509证书管理系统通过使用传输层安全(Transport layer security protocol, TLS)/传输层密码协议(Transport layer cryptography protocol, TLCP)等安全协议建立安全链路，保证车云平台之间传输消息的安全性和可追溯性。考虑到通信双方建立时钟同步比较困难，因此采用三路双向认证方案。在方案中采用基于随机数的挑战-应答方式[9]。协议中的参数$CERT_U$、PK_U、SK_U、E_{PKU}、K_{uv}、$SIGN_{SKU}$分别表示车辆OBU的公钥证书、公钥、私钥、会话密钥、加密算法、签名算法。过程如下：

$$A\rightarrow B:$$

$$SIGN_{SK_A}\{r_A,\ B,\ sighData,\ E_{PK_B}[K_{AB}]\},CERT_A$$

$$B\rightarrow A:$$

$$SIGN_{SK_B}\{r_B,\ A,\ sighData,\ E_{PK_A}[K_{BA}]\},CERT_B$$

$$A\rightarrow B:SIGN_{SK_A}\{r_B\}$$

(1)A→B代表车辆B从车辆A处收到附有公钥证书$CERT_A$的信息，向B证明了信息的完整性和新鲜度，以及A作为发送方和接收方B的身份。

A向B发送由A的私钥SK_A签署的消息，即A提交给B的凭证：

$$SIGN_{SK_A}\{r_A,\ B,\ sighData,\ E_{PK_B}[K_{AB}]\},CERT_A$$

消息由多个数据项组成：一次一生成随机数r_A、接收者B的标识，它包括信息的截止日期。在信息截止日期之前，接收者B只持有r_A，以便拒绝任何包含相同r_A的后续信息，可避免重放攻击。

如果A发给B的消息不单纯作为凭证，还可以包含其他信息sighData，将其作为A签署的数据项中，可以保证消息的真实性与完整性；数据项中还包括接收方B的公钥PK_B通过加密算法E加密的、经过密钥协商机制确定的会话密钥K_{AB}。

(2)B→A代表车辆B向车辆A做出应答：

$$SIGN_{SK_B}\{r_B,\ A,\ sighData,\ E_{PK_A}[K_{BA}]\},CERT_B$$

向A证明：应答消息是由A指定的具有公钥证书$CERT_B$的消息接收者B产生的，并在消息中指明期望接收者为A，以及消息的完整性和新鲜性。

应答信息中包含一个由A提供的用于验证应答信息有效性的一次性随机数(r_A)和一个由B发送的一次性随机数(r_B)，以及其他附加信息sighData和由A的公钥PK_A加密的会话密钥K_{AB}。

(3)A→B代表完成双向认证后，消息发送方A再将从接收方B发来的一次一生成的性随机数r_B进行数字签名后重新发送给B，即

$$SIGN_{SK_A}\{r_B\}$$

以完成三向认证。三向双路认证可以省去通信双方检查时间戳的过程，只需检查对方的一次性随机数即可检测出是否发生重放攻击。

4　性能分析

4.1　安全性分析

文中方案的安全性主要从机密性、完整性、不可抵赖性、抗重放攻击性、前向安全性和后向安全性进行分析。

4.1.1　机密性

(1)该方案使用ANSI X9.17伪随机发生器生成具有极高加密强度的伪随机数。它通过使用112位长的密钥和3DES加密算法(即系统当前的日期和时间以及上一个算法生成的新种子)来实现这一点。对手即使设法获得随机整数R_i，也无法推导出$Seed_{i+1}$，因为R_i经过了两次EDE加密，

以生成新的种子$Seed_{i+1}$。换句话说,密码保护了伪随机数发生器的内部状态。

(2)由ECDLP可得,已知P和Q,给定$nP=Q$, $0\leqslant n\leqslant \mathrm{ord}(P)-1$,计算$n$是困难的。

(3)方案所采用的密钥协商协议采用了s_i和R参数,这两个参数被用于认证的双方,通过对协议中其他相关参数的连接值进行哈希运算保证参数机密性与完整性。此外,AC作为认证证书参数,是每个认证节点独有的,用于生成认证参数和会话密钥。需要注意的是,在认证和密钥交换过程中,AC参数从未被发送到通道。考虑到用于认证的参数是点T和x_i,根据椭圆曲线离散对数难题可知,即使暴露了这些点,也无法获取会话密钥,以此保证只有经过认证和授权的实体才能正确计算会话密钥。

4.1.2 完整性

完整性是指各CA之间、CA内部各子系统之间通信时,系统具有防止消息被伪造、篡改的性质。方案利用X9.17伪随机生成器生成的种子作为私钥,一次一密,并且在签名之前对部分信息进行SM3散列计算,保证重要数据在传输过程中的完整性。

4.1.3 不可抵赖性

方案采用三路双向认证方案,保证了OBU、RSU和VSP接入CA系统过程中,支持数据源认证,确保数据来源的可靠性,防止伪造或篡改数据;同时工信部车联网安全信任根管理平台生成并发布可信根证书列表(TRCL),各安全证书管理系统获取TRCL并分发至路侧单元或车辆,由路侧单元或车辆从工信部车联网安全信任根管理平台获取TRCL,实现路侧设施与车辆直接的互信互认互通。

4.1.4 抗重放攻击

在身份认证过程,本方案采用基于随机数的“挑战-应答”方式,采用三路双向认证方式,获得对方的一次性随机数后,双方将各自返回对方。因此,OBU、RSU和VSP接入CA系统过程中,支持对消息的抗重放保护。另外,可在CA系统网络边界应部署边界防护设备,能够检测网络嗅探、DDoS攻击等行为。

4.1.5 前向安全性与后向安全性

为了防止外来车辆猜测RSU当前的密钥,前向安全要求RSU在车辆离开RSU服务区后生成一个新的随机数。与此相反,后向安全性要求RSU在车辆进入RSU服务区后更新系统密钥,以防止进入的车辆猜测之前在RSU中RSU的密钥。系统采用一次一密方式,结合动态时隙算法更新群密钥,当车辆发起加入服务网络请求时,通过与RSU进行双发身份认证后,等待RSU为其分发密钥随机数。RSU为单个车辆的等待时间设定最小阈值,以避免过长时间等待,并根据当前时段车流量决定是否更新密钥,在车辆密集进入和离开时批量更新密钥以减少通信和计算的开销。

4.2 开销分析

实验的硬件环境及运行环境:Intel(R) Xeon(R) CPU E3-1231 v3 @ 3.40GHz、16.0 GB,Java(TM) SE Runtime Environment(运行环境),使用JPBC库进行实验。方案采用ANSI X9.17伪随机生成器和SM3密码散列函数进行安全性相关的操作。实验中实现了基于椭圆曲线密码体制的身份认证协议,包括消息签名、密钥协商算法和身份认证方法,对提出的方案从安全性和性能两个角度进行评估,包括计算开销和通信开销的对比分析。

本节主要对提出的方案从计算开销和通信开销方面与文献[13]所提方案、文献[14]所提方案以及文献[15]所设计的方案进行对比和分析。

4.2.1 计算开销

计算开销主要取决于双线性配对运算(Tbp)、双线性配对中的标量乘(Tbpm)、映射到点的哈希运算次数(Tmtp)、椭圆曲线上标量乘运算(Teccm)、格基密码中的矩阵和向量乘、Hash求值运算(Th)的耗时,而计算量相对小的运算,如模加、模减、求逆运算的所耗时间忽略不计。参照文献[4]的研究方法,采用每种运算20次执行时间的平均值,如表2所示。

由表2可得:双线性配对中最耗时的3个操

表2 各种计算执行时间

Table 2 Various calculation execution times

运算类别	执行时间/ms
双线性对上的加法运算(Tbpa)	0.05
双线性配对运算(Tbp)	6.05
映射到点的哈希运算(Tmtp)	22.8
双线性配对中的标量乘(Tbpm)	9.85
椭圆曲线上标量乘(Teccm)	0.9
椭圆曲线上点加运算(Tecca)	0.002
哈希函数运算(Th)	0.001

作是标量乘法(Tbpm)、映射到点散列操作(Tmtp)和双线性配对操作(Tbp)，耗时分别为 9.85、22.8、6.05 ms。4 种方案各种运算的次数和计算开销如表 3 所示。

表 3　4 种方案的计算开销

Table 3　Calculation cost of four schemes

方案	运算次数	计算开销/ms
文献[13]	4Tbpm＋Tbpa＋2Th＋Tmtp	62.25
文献[14]	4Tbpm＋Th＋Tbpa	39.4
文献[15]	3Teccm＋Tecca＋2Tmtp	48.3
本文	10Teccm＋2Tecca＋13Th	9.02

对表 3 分析可得：文献[13][14][15]在执行过程中主要包含双线性配对中的标量乘运算、映射到点的哈希运算、双线性配对运算，这 3 种运算耗时较多；本文所提方案主要包括椭圆曲线标量乘运算和哈希运算，运算耗时少于文献[13][14][15]。

从图 3 可以看出，本文所提出的 DLS 方案在随着车辆数越来越多的情况下，其计算开销仍保持在一个较为良好的区间内，与文献[13][14][15]的方案进行比较，可以明显看出本方案有显著优势，更适用于车联网场景。

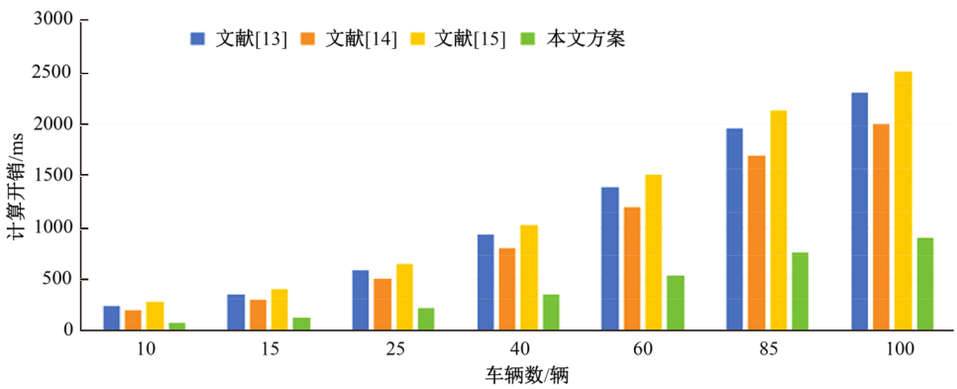

图 3　不同车辆数下各方案所需的计算开销

Fig. 3　Computational overhead required for each scenario with different numbers of vehicles

如图 4 所示，通过将 4 种方案的计算开销进行对比，得出结论：在同等安全环境下，与文献[13][14][15]的计算开销对比，本文所提方案计算开销最小。

4.2.2　通信开销

通信开销主要取决于根据车辆的请求消息长度。本文所提方案的请求消息由{PU, M, SIGNSKU, PV, CERTu}组成，PU 为消息请求方的假名，假名长度为 8 B，M 为经过加密的消息；SIGNSKU 为消息发送方的签名，签名长度为 71 B；PV 为消息接收方的假名，长度为 8 B；CERTu 为消息发送方证书，采用国密 SM2 算法，长度为 71 B；故总长度为 8＋71＋8＋71＝158 B。文献[13]请求消息长度为 296 B，文献[14]请求消息长度为 408 B，文献[15]请求消息长度为 469 B。将 4 种方案的通信开销进行对比，如表 4 所示。

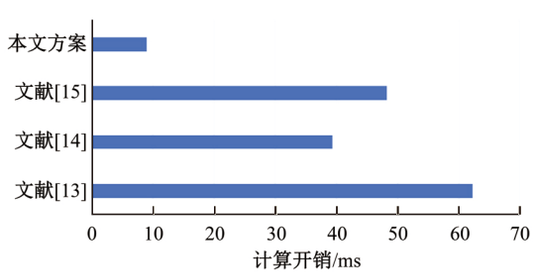

图 4　4 种方案计算开销对比图

Fig. 4　Comparison of computational costs for four schemes

根据表 4 与图 5 中 4 种方案的通信开销的数据对比结果，可知随着请求消息数量的增加，本文所提方案在通信开销中小于其他 3 种方案，在节点数量较多、实体间通信较频繁的车载自组网中占据优势。

综合上述对 4 种方案的性能进行对比和分析，可得结论：在同等安全性情况下，本文所提方

表 4　四种方案的请求消息长度对比

Table 4　Comparison of request information length for four schemes

方案	单条消息/B	n 条消息/B
文献[13]	296	296
文献[14]	408	408
文献[15]	469	469
本文	160	160

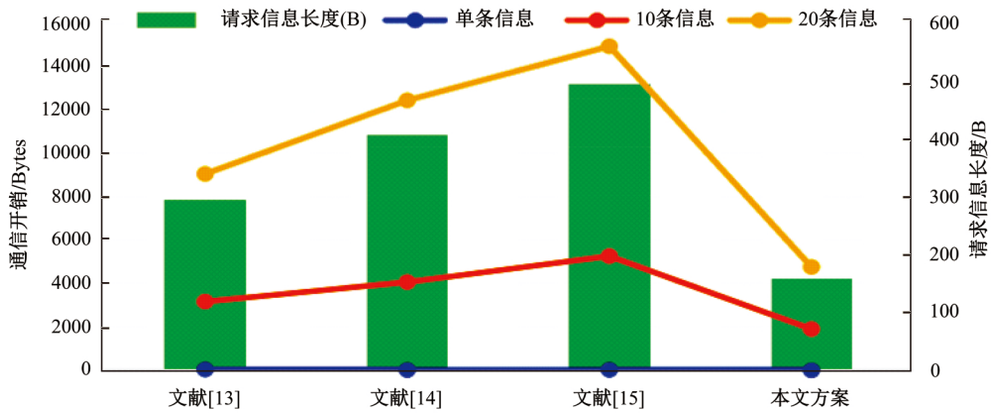

图5 4种方案通信开销对比图

Fig. 5 Comparison of communication costs among four schemes

案作为车载自组网身份认证和安全信任的方案在实际应用中更为合理。

5 结束语

在实验过程中,保证基于密钥驱动信任机制的认证方法在车载网络中的安全性和有效性至关重要。为了确保协议的保密性、完整性、不可抵赖性和防重放攻击,本文使用了一种安全性很高的伪随机数生成器、一种基于椭圆曲线密码系统的签名机制、一种一次性随机数挑战-响应方法和一种三向双向验证方案,这些措施共同构成了一个多层次的安全保护系统。考虑到联网汽车环境中计算资源有限的问题,本文优化了算法流程,最大限度地减少了双线性配对和散列操作的数量,以降低计算复杂度。这样,即使在资源有限的设备上也能有效执行安全协议。此外,本文将所提方案与现有文献中的方案进行对比分析,确保了实验结果的有效性。

通过上述措施,本文所提出的基于椭圆曲线密码体制方案由于其密钥短、存储空间小、计算速度快、对处理器速度要求低,因此适用于计算能力和存储空间有限、带宽受限和高速计算的情况。它提高了认证效率,并结合网络安全等级保护第三级要求,解决了车辆网中隐私保护和安全通信问题。

参考文献:

[1] Cheng T, Wu Z, Wang C, et al. Research on vehicle-to-cloud communication based on lightweight authentication and extended quantum key distribution [J]. IEEE Transactions on Vehicular Technology, 2024, 73(8): 12082-12095.

[2] Di X, Sun Y, Lu J, et al. Blockchain-based authentication scheme for vehicle network nodes[C]//2023 International Conference on Blockchain Technology and Information Security (ICBCTIS), Xi'an, China, 2023: 204-210.

[3] 叶卫明,常贺. 基于智能网联汽车的通信和信息安全研究[J]. 电信工程技术与标准化, 2022,35(1):93-97.
Ye Wei-ming, Chang He. Research on communication and information security based on intelligent connected vehicles[J]. Telecommunications Engineering Technology and Standardization, 2022, 35 (1): 93-97.

[4] 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.
Zeng Sheng-ke, Chen Yong, Xia Mei-chen. Privacy protection issues in vehicle ad hoc networks[J]. Journal of Xihua University (Natural Science Edition), 2015, 34 (4): 1-7.

[5] 邓雨康, 张磊, 李晶. 车联网隐私保护研究综述[J]. 计算机应用研究, 2022, 39 (10): 2891-2906.
Deng Yu-kang, Zhang Lei, Li Jing. A review of research on privacy protection in telematics[J]. Computer Application Research, 2022, 39 (10): 2891-2906.

[6] 朱栋, 殷新春, 宁建廷. 车联网中具有强隐私保护的无证书签名方案[J]. 计算机应用, 2022, 42(10): 3091-3101.
Zhu Dong, Yin Xin-chun, Ning Jian-ting. A certificate-less signature scheme with strong privacy preservation in telematics[J]. Computer Applications, 2022, 42(10): 3091-3101.

[7] Chen Y, Chen J. CPP-CLAS: efficient and conditional privacy preserving certificateless aggregate signature scheme for VANETs[J]. IEEE Internet of Things Journal, 2022, 9 (12): 10354-10365.

[8] Liang Y, Luo E, Liu Y. Physically secure and condi-

tional-privacy authenticated key agreement for VANETs[J]. IEEE Transactions on Vehicular Technology, 2023, 72 (6): 7914-7925.

[9] 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.

[10] 杨晓东, 裴喜祯, 安发英, 等. 基于身份聚合签名的车载自组网消息认证方案[J]. 计算机工程, 2020, 46 (2): 171-182.
Yang Xiao-dong, Pei Xi-zhen, An Fa-ying, et al. A message authentication scheme for vehicle ad hoc networks based on identity aggregation signature[J]. Computer Engineering, 2020,46 (2): 171-182.

[11] Han M, Yin Z K, Cheng P Z, et al. Zero-knowledge identity authentication for internet of vehicles: improvement and application[J]. PLoS ONE, 2020, 9: No. 0239043.

[12] 陈葳葳, 曹利, 邵长虹. 基于区块链技术的车联网高效匿名认证方案[J]. 计算机应用, 2020, 40(10): 2992-2999.
Chen Wei-wei, Cao Li, Shao Chang-hong. An efficient anonymous authentication scheme for Telematics based on blockchain technology[J]. Computer Applications, 2020, 40(10): 2992-2999.

[13] Pournaghi S M, Zahednejad B, Bayat M, et al. NECPPA: a novel and efficient conditional privacy-preserving authentication scheme for VANET[J]. Computer Networks, 2018, 134:78-92.

[14] Wang H, Wang L, Zhang K, et al. A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs[J]. IEEE Access, 2022, 10: 15605-15618.

[15] Xu Z Y, He D B, Kumar N, et al. Efficient certificateless aggregate signature scheme for performing secure routing in VANETs[J]. Security and Communication Networks,2020, 12(3): 53-68.

[16] 杨宜青. 车联网安全通信的密钥管理研究[D]. 成都: 成都电子科技大学信息通信与工程学院, 2021.
Yang Yi-qing. Research on key management for secure communication of internet of vehicles[D]. Chengdu: School of Information Communication and Engineering, Chengdu University of Electronic Science and Technology, 2021.

[17] 王冠, 张倩倩. 基于SGX的车联网身份认证方案研究[J]. 计算机技术与发展,2023,33(11):99-105.
Wang Guan, Zhang Qian-qian. Research on SGX-based identity authentication scheme for telematics [J]. Computer Technology and Development, 2023, 33(11):99-105.

[18] Jiang S, Zhu X, Wang L. An efficient anonymous batch authentication scheme based on hmac for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems,2016, 17(8):2193-2204.

[19] 陈虹, 刘雨朦, 肖成龙, 等. 基于椭圆曲线的改进RC4算法[J]. 计算机应用, 2019, 39(8):2339-2345.
Chen Hong, Liu Yu-meng, Xiao Cheng-long, et al. Improved RC4 algorithm based on elliptic curves[J]. Computer Applications, 2019, 39(8):2339-2345.

[20] 北京数字认证股份有限公司. 证书吊销列表分发方法、设备及存储介质、服务器、车联网设[P]. 中国: CN202111458608.5,2021-04-21.

[21] 张晓均, 唐浩宇, 张楠, 等. 分布式智能车载网联系统的匿名认证与密钥协商协议[J]. 电子与信息学报, 2024,46(4):1333-1342.
Zhang Xiao-jun, Tang Hao-yu, Zhang Nan, et al. An anonymous authentication and key negotiation protocol for distributed intelligent in-vehicle networked systems[J]. Journal of Electronics and Information, 2024,46(4):1333-1342.

[22] 于斌斌, 胡亮, 迟令. 可抵抗内外部攻击的无线传感器网络数字签名方案[J]. 吉林大学学报: 工学版, 2019, 49(5): 1666-1681.
Yu Bin-bin, Hu Liang, Chi Ling. A digital signature scheme for wireless sensor networks that can resist internal and external attacks[J]. Journal of Jilin University(Engineering and Technology Edition), 2019, 49 (5): 1666-1681.