基于CPN的车载网络无证书匿名认证和密钥协商方案研究

郑路[1]，冯涛[1]，苏春华[2]
（1.兰州理工大学计算机与通信学院，甘肃 兰州 730050；2.日本会津大学计算机科学系，福岛 会津若松 965-8580）

摘　要：为了解决现有车载网络的认证方案中普遍存在密钥托管带来的缺陷，以及没有考虑计算受限电子控制单元（ECU）轻量级部署和安全快速认证的问题，首先，针对计算不受限的ECU网络，提出了一种无双线性配对的轻量级无证书匿名认证和密钥协商方案，该方案通过椭圆曲线密码体制安全构建认证密钥对，通过哈希函数和异或等轻量级方法实现匿名认证和密钥协商。然后，针对计算受限的ECU网络，提出了一种无证书批量验证方案来降低认证成本。最后，提出了一种基于有色Petri网（CPN）和Dolev-Yao攻击者模型的安全验证方法，对整体方案进行形式化安全性评估。安全评估和性能分析表明，所提方案能有效抵抗重放、伪装、篡改、已知密钥、已知特定会话临时信息攻击等多种不同类型的攻击，在保证多重安全属性的同时有较小的计算与通信成本。

关键词：车载网络；安全协议；认证与密钥协商；有色Petri网；形式化验证
中图分类号：TN393.06
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024121

Research on certificateless anonymous authentication and key agreement scheme of vehicle network based on CPN

ZHENG Lu[1], FENG Tao[1], SU Chunhua[2]
1. School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China
2. Division of Computer Science, University of Aizu, Fukushima 965-8580, Japan

Abstract: To address the shortcomings of existing authentication schemes in vehicle networks, which commonly suffer from key escrow issues, as well as the lack of consideration for lightweight deployment and secure rapid authentication of compute-constrained electronic control unit (ECU), a lightweight certificateless anonymous authentication and key agreement scheme without bilinear pairings was proposed for compute-unconstrained ECU networks. The authentication key pair was securely constructed by elliptic curve cryptography, anonymous authentication and key agreement were realized by lightweight methods such as hash functions and XOR operation. Additionally, a certificateless batch verification scheme was proposed to reduce the authentication costs for compute-constrained ECU networks. Finally, a security verification method based on the colored Petri net (CPN) and Dolev-Yao attacker model was proposed to evaluate the formal security of the proposed scheme. The proposed scheme is proved through security evaluation and performance analysis to effectively resist various types of attacks such as replay, spoofing, tampering, known key, known specific session temporary information attack, etc., with multiple security attributes, small computation and communication cost.

Keywords: vehicle network, security protocol, authentication and key agreement, colored Petri net, formal analysis

收稿日期：2024–02–05；**修回日期：**2024–05–31
通信作者：冯涛，fengt@lut.edu.cn
基金项目：国家自然科学基金资助项目（No.62162039, No.61762060）；甘肃省重点研发基金资助项目（No.23YFGA0060）；甘肃省优秀博士生基金资助项目（No.23JRRA837）
Foundation Items: The National Natural Science Foundation of China (No.62162039, No.61762060), The Key Research and Development Program of Gansu Province (No.23YFGA0060), The Excellent Doctoral Program of Gansu Province (No.23JRRA837)

0 引言

工业互联网通过连接物流车辆的设备传感器，从生产调度到物料传输等方面实现物流运输过程的优化和管理，为工业制造业带来了更高效、更灵活和更智能的物流运作方式[1]。

工业制造业中负责物料传输的无人车辆在工业互联网中具有重要的作用。它们作为连接制造业传输的关键纽带，具体应用于制造业物料的及时配送、货物的高效运输以及仓储的智能管理[2]。此外，大型港口物料传输车辆承担着运输装载工业物料的关键任务，是工业制造业物流不可或缺的部分。这些车辆能够将原物料及时送达工业互联网制造生产线，保障了制造过程的顺利进行和物料的及时交付。同时，通过工业互联网实现对车辆的实时监控和调度优化，提高了运输效率[3]。高效的物流运作为工业制造提供了可靠的供应链支持，满足了工业互联网制造领域日益增长的供应链需求，也推动了工业互联网的数字化、智能化和高效化发展。

确保物流传输车辆的通信安全是维护工业互联网整体安全的基石，物流运输车辆通过车载网络互联，其安全性是保障整个工业系统物流安全高效运行的重要一环。基于车载网络架构的安全机制如图1所示。在设计和制造阶段，需将通信安全、启动安全、密码模块的安全要求纳入数字化设备的制造过程中[4]，确保设备不会遭受恶意攻击。工业互联网中负责物流运作的车载网络中部署的通信协议用于交换设备间的重要信息[5]，其安全性得到保障是工业互联网物流数据安全传输的前提[6]。

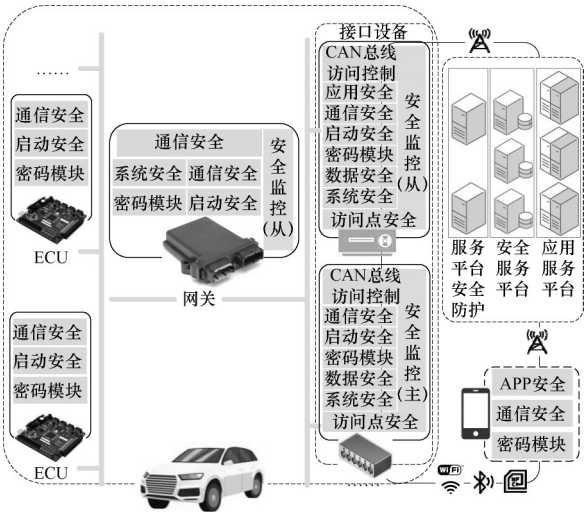

图1 基于车载网络架构的安全机制

随着工业互联网的快速发展，逐步开放的工业环境无疑增加了攻击者入侵物流车载网络的风险。身份认证是车载网络安全的第一道防线，利用密码模块实现数字化设备设计，确保电子控制单元（ECU, electronic control unit）间的通信安全，是数据访问的基础，也是最直接、最有效的安全防护手段。因此研究安全高效的身份认证和密钥协商协议可以确保车载网络ECU间节点授权访问和采集数据的安全传输，对车载网络发展有十分重要的意义[7]。

现有车载网络安全协议方案大多使用公钥基础设施（PKI, public key infrastructure）的体系框架实现身份验证、签名、完整性和不可否认性[8]。Groza等[9]针对车载网络提出了身份认证方案Libra-CAN，但是由于方案中不包含时间信息，因此无法抵抗重放攻击。在后续工作中，Groza等[10]针对此缺陷提出了一种有效的车载认证方案，但是Palaniswamy等[11]证明了该方案无法抵抗伪装攻击。Woo等[12]针对车载控制器局域网（CAN, controller area network）总线设计了一个认证密钥协商协议，但没有考虑到ECU资源受限节点的认证场景，此外，该方案在密钥协商阶段容易受到重放攻击[11]。Murvay等[13]提出了针对ECU安全通信的两种身份验证协议来解决已识别的弱点，基于ECU资源受限节点的协议使用对称密钥加密，基于ECU资源不受限节点的协议使用公钥加密。然而，所提协议缺乏有效的安全验证方法。尽管基于PKI的方案可以满足较高安全需求，并可提供高安全级别，但由于证书颁发和管理的复杂性，此类方案存在高通信开销的缺陷[14]。此外，证书吊销也可能会导致分组丢失率较高。

其他研究侧重于基于身份的密码体制，允许在不依赖于第三方的情况下实现公钥机制。Cheng等[15]提出了一种基于身份的ECU安全通信方案，该方案有效防止了攻击者发起伪装攻击。但是，由于缺乏ECU密钥协商，该方案易受到重放攻击。Groza等[16]在车载网络中使用基于身份的通信协议，实现并评估了短签名、基于身份的签名和基于身份的密钥交换。Tsai等[17]的方案无法抵抗伪装攻击。为了解决此缺陷并提高安全性，He等[18]通过使用基于身份的认证方法，设计了一种新的认证和密钥协商协议。Li等[19]提出了一种安全高效的基于身份的双向认证密钥协商协议，该协议不涉及复

杂的双线性配对计算，具有较低的计算成本。Carvajal-Roca等[20]设计了基于半集中式的车载认证协议，该协议考虑了ECU维护、密钥更新和管理。基于身份的密码体制减轻了对证书的需要和依赖，不需要额外的实体标识和公钥间映射管理，使用身份信息进行密码运算，解决了公钥真实性的问题，简化了密钥系统的管理和使用的复杂性。但是，基于身份的密码体制用密钥生成中心（KGC, key generation center）来生成实体的私钥，存在密钥托管的问题。

无证书的公钥密码体制消除了PKI中使用的证书，并解决了身份密码体制中密钥托管的问题。无证书的公钥密码学中用户私钥由KGC和用户联合产生，KGC不知道用户的完整私钥。Liu等[21]使用椭圆曲线提出了一种两层身份验证协议以解决设备和服务器之间无证书的身份验证。Cheng等[22]发现Kumar等[23]提出的轻量级方案无法满足前向安全性，并提出了基于匿名身份的认证和密钥协商协议。Sowjanya等[24]和Wang等[25]利用椭圆曲线密码体制（ECC, elliptic curve cryptosystem）提出了一种增强的端到端认证方案，以避免利用双线性配对导致高开销的缺陷。Xu等[26]基于ECC提出了匿名认证协议，并使用BAN（Burrows-Abadi-Needham）逻辑进行安全证明。Dwivedi等[27]通过哈希函数和ECC为车内和车间场景设计了认证协议，并且可以在两轮中生成有效的会话密钥。此外，一些研究针对车载网络采用无证书批量认证机制。Horng等[28]提出批量认证机制以减轻中心服务器的负担。Cui等[29]提出批量签名方案，并在随机预言模型中证明了对自适应选择消息攻击的存在不可伪造性。He等[30]提出了支持条件隐私保护的车载网络认证方案，该方案降低了隐私泄露的风险，实现了批量验证的功能。Karati等[31]提出了一种无证书认证方案，该方案使用双线性配对来解决身份认证问题，没有考虑计算成本的开销。Zhang等[32]对Karati等[32]方案进行了分析发现其无法抵抗伪装攻击，并为解决此缺陷提出了有效的轻量级认证方案。Yang等[33]证明了Zhang等[32]方案存在安全漏洞，但没有提出解决方案。Rezaeibagha等[34]也分析了Karati等[31]方案，证明了Karati等[31]方案不能抵抗伪装攻击，并提出了基于双线性配对的改进认证方案。Xiong等[35]声称其提出的无证书认证方案具有强大的安全机制和轻量级的计算成本，然而，Palaniswamy等[3]证明了其方案易受已知密钥泄露攻击，在泄露了前一轮会话密钥后，攻击者可以利用已知信息构建会话密钥。无证书密码体制不需要证书的管理，所需负载更小，因此更适用于低宽带需求和低能量消耗的车载网络应用环境。

综上所述，车载网络中无证书的公钥密码体制具有较大的优势。然而，现有基于无证书的公钥密码体制的大多方案使用双线性配对，存在资源开销大量消耗的缺陷。因此，车载网络中缺乏一种安全高效的轻量级无证书认证和密钥协商方案，并且没有考虑ECU资源受限节点快速认证的需求。此外，现有车载网络身份验证和密钥协商方案缺乏直观的形式化安全建模，攻击方式较少，且缺乏有效的形式化安全评估和验证方法。

本文的主要贡献如下。

1) 针对现有车载网络无证书认证和密钥协商大多使用双线性配对的高资源开销缺陷，本文提出了一种高效的轻量级无证书匿名身份认证和密钥协商方案。该方案利用哈希函数和异或运算轻量级方法实现高效无证书匿名性，通过椭圆曲线安全构建认证密钥对，实现会话密钥生成和更新。

2) 针对现有车载网络认证方案缺乏考虑ECU资源受限节点的认证问题，本文实施匿名识别和无证书批量验证机制，以满足车载网络中大量ECU快速认证的需求。

3) 本文采用有色Petri网（CPN, colored Petri net）安全协议形式化分析工具对本文方案进行形式化建模，并进行模型的一致性检验。

4) 本文提出了加入Dolev-Yao攻击模型的协议CPN形式化安全验证方法，设计了方案攻击者CPN模型并进行重放、伪装、已知密钥、已知特定会话临时信息攻击等多种不同类型的攻击。CPN状态空间结果表明，本文方案能够抵抗所发起的这些攻击，在不失可用性的前提下，满足匿名性、不可追踪性、完美前向安全性等多重安全属性。性能评估实验表明，本文方案与现有工作相比有一定的效率优势。

1　预备知识

1.1　车载网络系统模型

车载网络系统模型如图2所示。本文方案包括3个实体，即注册中心（RC, registration center）、安全控制单元（SeCU, security control unit）和ECU。

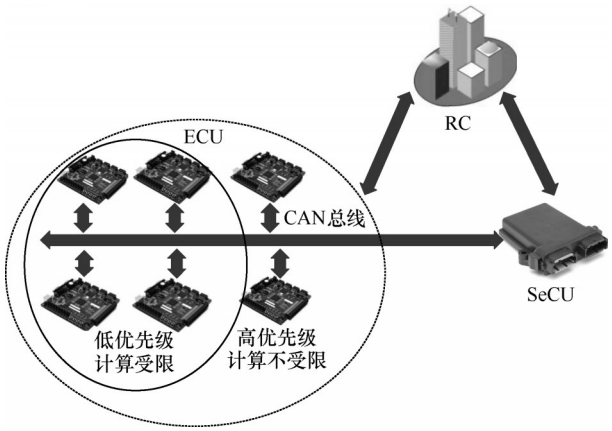

图2　车载网络系统模型

RC：车载网络中完全受信任的注册中心，拥有强大的计算能力，为SeCU和ECU生成部分私钥，并向任何合法用户提供系统参数。在现有框架中，可以使用多个RC服务器建立分布式注册中心，由多个实体共同管理和验证用户身份。此外，还可以通过去中心化区块链技术分发系统参数，实现身份认证的分布式管理，提高系统的鲁棒性和安全性。

SeCU：负责会话密钥的管理，并维护所有ECU的身份列表和计数器。

ECU：分为计算受限的ECU和计算不受限的ECU。计算受限的ECU具有低优先级，一般不使用较为复杂的密码运算。计算不受限的ECU具有高优先级，可用于执行烦琐的密码和计算。通常情况下，复杂的车辆功能对应着复杂的电子系统，如发动机控制、防抱死制动控制器等的ECU具有高优先级，而简单的功能如控制无线电等的ECU具有低优先级。

1.2　Dolev-Yao攻击者模型

Dolev-Yao攻击者模型是一种专门检验安全密码协议的模型。迄今为止，在安全协议研究中所引入的攻击者模型绝大部分采用Dolev-Yao模型[36]。Dolev-Yao模型将安全协议自身与安全协议内部采用的密码学机制进行区分，不研究协议具体密码学算法的安全性，而是将协议内在的安全属性作为研究目标。Dolev-Yao模型被概括为黑盒安全分析，有以下5个假设。

1) 攻击者具有强大的计算能力，能够窃听、阻止并截获、重放、篡改系统网络中所有信息。

2) 攻击者熟悉密码学操作，可以对截获到的信息进行存储、加密、解密、生成随机数、哈希运算、合成、分解，并作为合法实体参与协议交互流程。

3) 攻击者拥有自己的加解密密钥，可以与协议中的实体进行通信，并能够将窃听或接收到的消息存储到其知识库中。

4) 攻击者了解目标安全协议的完整知识，能够按定义的长度拆分出不同部分，并能在协议中随时插入新的消息。

5) 攻击者若得到了匹配的密钥，则可以将密文解密。

1.3　CPN Tools建模工具

目前，已有大量研究工作表明，只有形式化分析的方法才能使安全协议的验证更加高效和可信。BAN逻辑、串空间、状态机是早期被用于协议形式化分析的方法，这些方法注重于定理证明的形式化分析，没有针对协议语义进行形式化验证。近年来，ProVerif、Scyther、Tamarin Prover、CPN Tools等强大的形式化分析工具的出现可以针对协议进行形式化安全验证及语义分析。本文采用CPN Tools对方案进行形式化分析和验证。CPN Tools与目前主流的安全协议检测工具对比如表1所示。

表1　　安全协议检测工具对比

检测工具	攻击类型	攻击路径	直观模型	状态空间
BAN	√	×	×	×
Tamarin Prover	×	√	×	√
AVISPA	×	√	×	×
Scyther	×	√	×	×
ProVerif	√	×	×	×
CPN Tools	√	√	√	√

ProVerif方法基于逻辑编程，但计算的攻击路径受限，提取的攻击路径集远少于CPN Tools方法提取的攻击路径集[37]。Scyther和AVISPA都是协议模型验证工具，有多攻击路径的分析功能，但所用的算法较为单一，用同一种攻击者模型进行所有安全协议的状态空间分析，不能处理较新型的攻击手段[36]。Tamarin Prover能够穷尽搜索状态空间，但该方法和CPN Tools相比不够简单直观，同时，它也存在Scyther中因方法单一、无法加入新型攻击手段的缺陷[38]。CPN Tools能够完成安全协议语义和语法的证明，使协议建模者进行精确的协议分析和漏洞挖掘[1]，由于强大的状态空间分析能力和精准的建模错误定位提示，通常比其他协议安全检测工具更加高效。

2　方案设计

2.1　方案消息流模型

本文提出了一种无双线性配对的无证书匿名身份验证和密钥协商方案，针对计算不受限的ECU，方案主要由注册阶段、身份验证和密钥协商阶段组成；针对计算受限的ECU，认证主要由批量认证阶段组成，可以满足车辆电子部件中快速认证的需求。表2为本文方案中的符号及其含义。

表2　本文方案中的符号及其含义

符号	含义
公钥	X
私钥	x
部分公钥	R
部分私钥	d
系统主密钥	k
系统公钥	P_{pub}

2.2　系统初始化阶段

步骤1　SeCU随机选取一个大素数q，有限域上的椭圆曲线$y^2 \equiv x^3 + ax + b(\bmod q)$，其中，$a,b \in Z_q^*$，满足$4a^3 + 27b^2 \neq 0 \bmod q$。

步骤2　SeCU选取4个安全的哈希函数：H_1:$\{0,1\}^* \to Z_q^*$，H_2:$G \times G \times G \to Z_q^*$，$H_3$:$\{0,1\}^* \times G \times G \times \{0,1\}^* \to Z_q^*$，$H_4$:$G \times G \times G \times \{0,1\}^* \to Z_q^*$，其中，$G$是椭圆曲线的加性循环群。

步骤3　SeCU选取一个系统主密钥$k \in Z_q^*$，计算系统公钥$P_{\text{pub}} = kP$，其中，P是G的生成元。

步骤4　SeCU生成系统参数params = $\{q,P,G,P_{\text{pub}},H_1,H_2,H_3,H_4\}$。

2.3　注册阶段

图3为ECU和SeCU向RC进行注册的过程。在本文方案中，车载网络ECU以匿名身份来保存真实身份和信息。

步骤1　为了实现节点对实体身份信息的匿名保护，RC选择两个随机秘密值$u,v \in Z_q^*$，计算$\text{PID}_i = \{H_1(\text{ID}_i),h_{i_1},u\text{ID}_i \oplus vP_{\text{pub}}\}$。只有RC可以基于$h_{i_1}$来计算节点的实体身份信息$\text{ID}_i$。

步骤2　ECU节点选取一个随机秘密值$x_i \in Z_q^*$计算$X_i = x_iP$并保存x_i。ECU将身份信息PID_i和X_i合并成消息$\{\text{PID}_i,X_i\}$，并将其发送至RC请求生成部分密钥。

步骤3　RC选取一个随机数$r_i \in Z_q^*$，计算$R_i = r_iP$，$h_{i_1} = H_1(\text{ID}_i \| k)$，$h_{i_2} = H_2(h_{i_1},R_i,X_i)$，$D_i = r_i(1 + X_i) + kh_{i_2}$，并将$\{R_i,D_i,h_{i_1}\}$发送至ECU。

步骤4　ECU节点通过验证等式$D_iP = R_i(1 + X_i) + P_{\text{pub}}h_{i_2}$是否成立来判断$\{R_i,D_i\}$的合法性。如果等式不成立，则请求部分密钥失败；如果等式成立，ECU计算$d_i = D_i - x_iR_i = r_i + kh_{i_2}$作为其部分私钥。

步骤5　SeCU随机选取一个秘密值$x_s \in Z_q^*$，计算$X_s = x_sP$，保存x_s并将$\{\text{ID}_s,X_s\}$发送至RC请求生成部分密钥。

步骤6　RC选取一个随机数$r_s \in Z_q^*$，计算$R_s = r_sP$，$h_{s_1} = H_1(\text{ID}_s \| k)$，$h_{s_2} = H_2(h_{s_1},R_s,X_s)$，$D_s =$

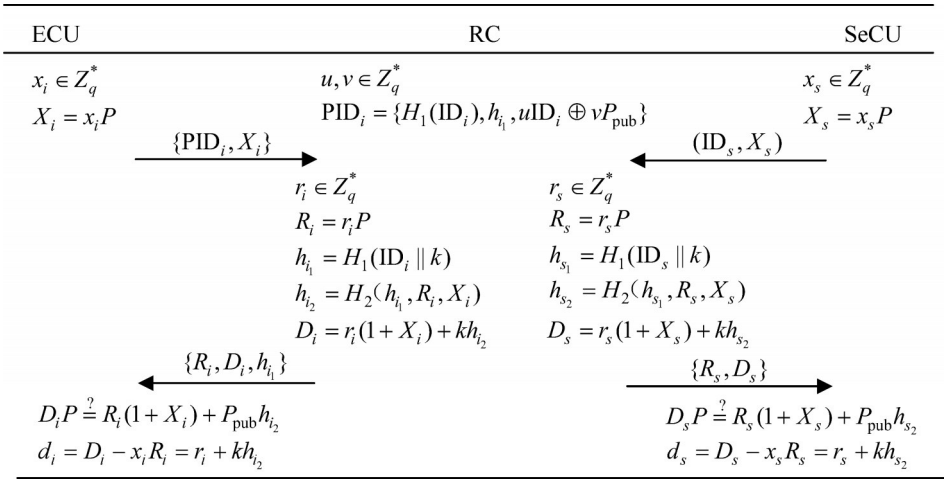

图3　ECU和SeCU向RC进行注册的过程

$r_s(1+X_s)+kh_{s_2}$，并将$\{R_s,D_s\}$发送至SeCU节点。

步骤 7 SeCU节点通过验证等式$D_sP=R_s(1+X_s)+P_{\text{pub}}h_{s_2}$是否成立来判断$\{R_s,D_s\}$的真实性。如果等式不成立，则请求部分密钥失败；如果等式成立，SeCU计算$d_s=D_s-x_sR_s=r_s+kh_{s_2}$作为其部分私钥。

2.4 认证和密钥协商阶段

ECU和SeCU按照认证和密钥协商阶段完成相互认证和一致的会话密钥协商。图4给出了认证和密钥协商阶段的具体步骤。

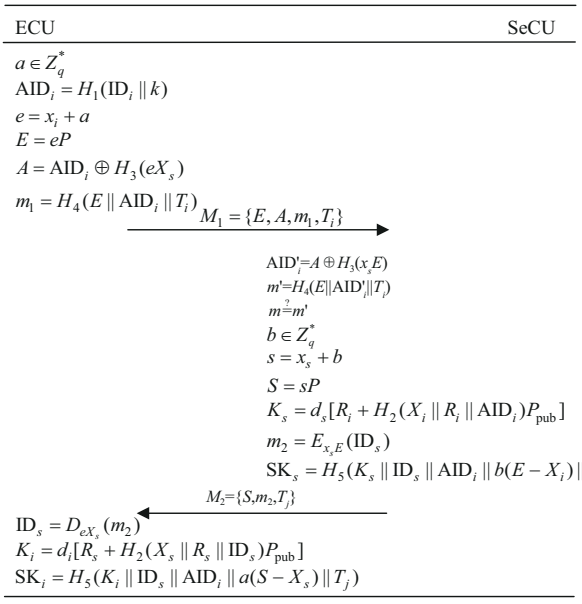

图4 认证和密钥协商阶段

步骤 1 ECU节点选取一个随机秘密值$a\in Z_q^*$，计算$\text{AID}_i=H_1(\text{ID}_i\|k)$，$e=x_i+a$，$E=eP$，$A=\text{AID}_i\oplus H_3(eX_s)$，$m_1=H_4(E\|\text{AID}_i\|T_i)$。ECU将请求消息$M_1=\{E,A,m_1,T_i\}$发送给SeCU。

步骤 2 SeCU收到消息M_1后，判断T_i是否有效。如果T_i有效，计算$\text{AID}'_i=A\oplus H_3(x_sE)$，$m'=H_4(E\|\text{AID}'_i\|T_i)$。SeCU通过验证$m$和$m'$是否相等来完成ECU的身份验证，如果$m=m'$，则身份认证成功；否则，身份认证失败。

步骤 3 ECU和SeCU通过身份验证后，接下来将进入密钥协商的阶段。SeCU选取一个随机秘密值$b\in Z_q^*$，随后开始计算$s=x_s+b$，$S=sP$，$K_s=d_s[R_i+H_2(X_i\|R_i\|\text{AID}_i)P_{\text{pub}}]$，$m_2=E_{x_sE}(\text{ID}_s)$，$\text{SK}_s=H_5(K_s\|\text{ID}_s\|\text{AID}_i\|b(E-X_i)\|T_j)$，并向ECU发送消息$M_2=\{S,m_2,T_j\}$。

步骤 4 ECU收到消息M_2后，判断T_j是否有效。如果T_j有效，计算$\text{ID}_s=D_{eX_s}(m_2)$以获得SeCU的真实身份。通过解密获得$\text{ID}_s$之后，ECU随后开始计算$K_i=d_i[R_s+H_2(X_s\|R_s\|\text{ID}_s)P_{\text{pub}}]$，$\text{SK}_i=H_5(K_i\|\text{ID}_s\|\text{AID}_i\|a(S-X_s)\|T_j)$。至此，ECU和SeCU成功完成了身份认证和密钥协商。

2.5 批量认证阶段

批量认证阶段由计算受限的ECU运行，其中，ECU对消息进行签名，SeCU对签名进行验证。批量认证阶段的具体步骤如图5所示。

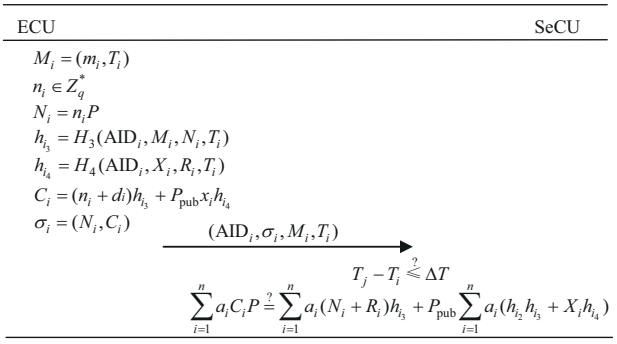

图5 批量认证阶段

步骤 1 ECU计算$M_i=(m_i,T_i)$，选取一个随机秘密值$n_i\in Z_q^*$，计算$N_i=n_iP$。

步骤 2 ECU计算$h_{i_3}=H_3(\text{AID}_i,M_i,N_i,T_i)$，$h_{i_4}=H_4(\text{AID}_i,X_i,R_i,T_i)$。

步骤 3 ECU计算$C_i=(n_i+d_i)h_{i_3}+P_{\text{pub}}x_ih_{i_4}$，生成数字签名$\sigma_i=(N_i,C_i)$。

步骤 4 ECU在网络中将广播消息$(\text{AID}_i,\sigma_i,M_i,T_i)$发送给SeCU。

步骤 5 当SeCU接收到来自ECU的广播消息$(\text{AID}_i,\sigma_i,M_i,T_i)$时，SeCU计算$T_j-T_i\leqslant\Delta T$是否成立，其中，$T_j$表示SeCU接收到广播消息的时间。

步骤 6 如果$T_j-T_i\leqslant\Delta T$成立，SeCU验证等式$\sum_{i=1}^{n}a_iC_iP=\sum_{i=1}^{n}a_i(N_i+R_i)h_{i_3}+P_{\text{pub}}\sum_{i=1}^{n}a_i(h_{i_2}h_{i_3}+X_ih_{i_4})$是否成立来判断消息$M_i$的签名$\sigma_i$的真实性。

步骤 7 如果步骤6中的验证等式成立，则与n个签名相对应的n个消息都是合法的；否则，与n个签名相对应的n个消息中存在非法签名。

3　形式化证明

3.1　CPN建模

为了清晰地描述本文方案流程中各个模块的功能，本文采用分层架构建立CPN模型。

协议顶层CPN模型如图6所示。ECU和SeCU通过接口C1~C4传递消息，攻击者（Adversary）通过网络层（Network）对双方通信发起攻击。

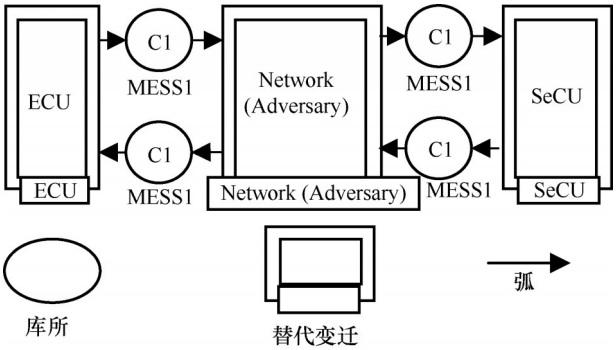

图6　协议顶层CPN模型

ECU替代变迁CPN模型如图7所示。Send Request子模块负责发送ECU认证消息，Receive Response子模块负责接收SeCU发来的消息并计算会话密钥，VeritySK子模块负责验证会话密钥的合法性。

SeCU替代变迁CPN模型如图8所示。Receive and Verify子模块负责判断时间戳T_i是否有效，接收ECU发来的认证消息，并进行身份验证；Calculate and Send子模块负责生成SeCU会话密钥，并与ECU进行密钥协商。

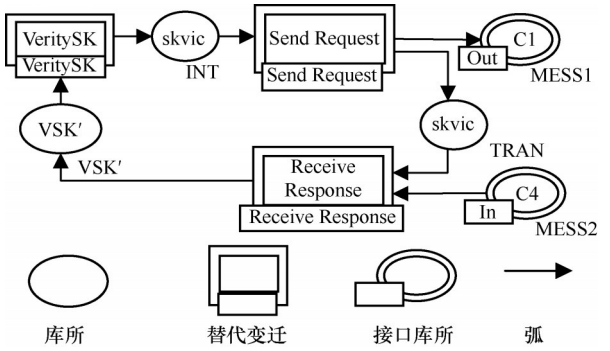

图7　ECU替代变迁CPN模型

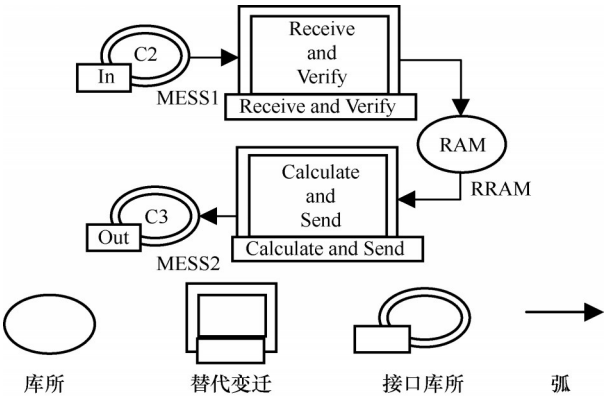

图8　SeCU替代变迁CPN模型

ECU的子模块Send Request替代变迁CPN模型如图9所示。变迁IDiK组成ID_i的匿名消息AID_i，变迁SE生成点乘运算E，变迁HeXs通过点乘和异或生成A，变迁Sm组合E、匿名AID_i和时间戳T_i并生成消息m_1，变迁MESS将E、A、m_1、T_i合并成消息M_1并将其发送给端口库所C1。

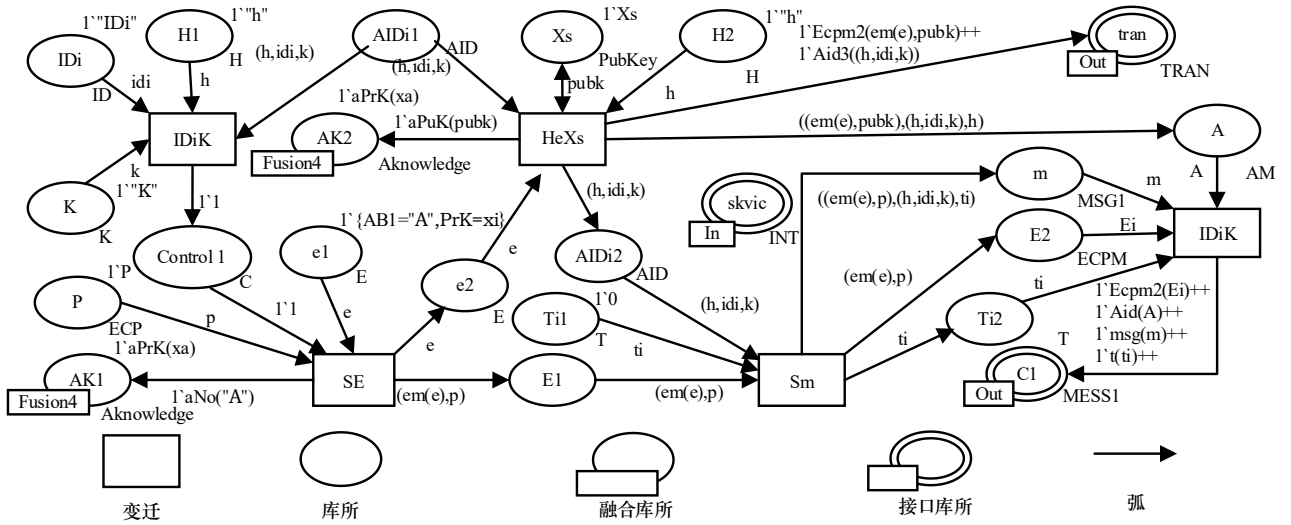

图9　ECU的子模块Send Request替代变迁CPN模型

SeCU 的子模块 Receive and Verify 替代变迁 CPN 模型如图 10 所示。变迁 Rec 对接收到的消息进行处理和分发；变迁 Verity1 通过变迁 SAID'得到消息 AID'_i；变迁 Sm'组合 E、匿名 AID'_i 和时间戳 T_i 并生成消息 m'_1；变迁 Verity 通过函数 checkMSG1 判断 m_1 和 m'_1 是否相等，如果相等，则通过 RAM 点火替代变迁 Calculate and Send 进入密钥协商阶段；如果不相等，则终止运行。

批量认证阶段子模块 Send Request 和 Receive and Verify 替代变迁 CPN 模型如图 11 和图 12 所示，分别表示了消息进行签名和验证的过程。

ECU 的子模块 VeritySK 替代变迁 CPN 模型如图 13 所示。变迁 VeritySK'和变迁 VeritySK 对相应的密钥消息进行处理和分发；变迁 compare 判断 ECU 的 K_i 和 SeCU 的 K_s 是否相等，如果相等，则进行下一步会话密钥的比较，如果不相等，则终止运行；变迁 cSK 通过 checkSK 函数判断 ECU 的会话密钥 SK_i 和 SeCU 的会话密钥 SK_s 是否相等，如果相等，则 ECU 和 SeCU 双方成功完成了会话密钥协商，如果不相等，会话密钥协商失败。

Network(Adversary)替代变迁 CPN 模型如图 14 所示。融合库所 Attack Knowledge 存储了从各个子模块中获得的攻击者知识，攻击者利用获得的攻击者知识发起各种攻击。实线矩形块表示攻击者利用攻击者知识库中的预共享信息发起伪装攻击和重放攻击，虚线矩形块代表攻击者利用新鲜随机数、公钥和部分私钥发起已知特定会话临时信息攻击和已知密钥攻击。

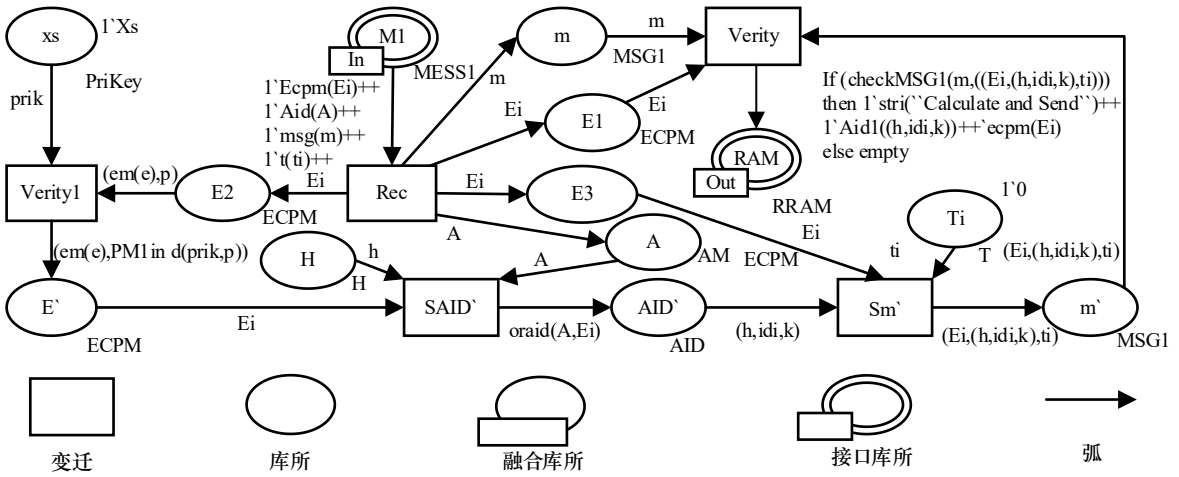

图 10 SeCU 的子模块 Receive and Verify 替代变迁 CPN 模型

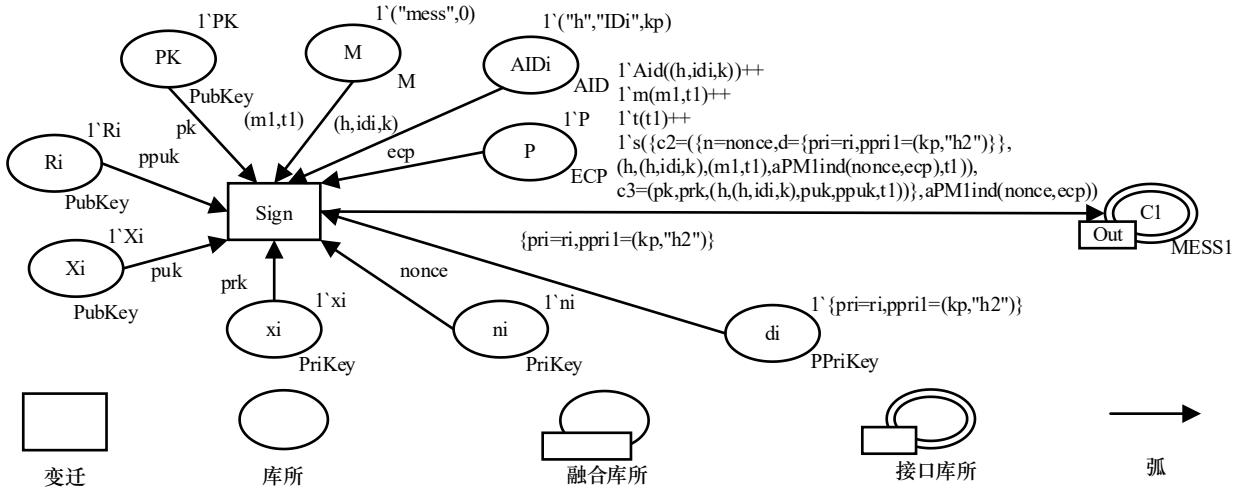

图 11 批量认证子模块 Send Request 替代变迁 CPN 模型

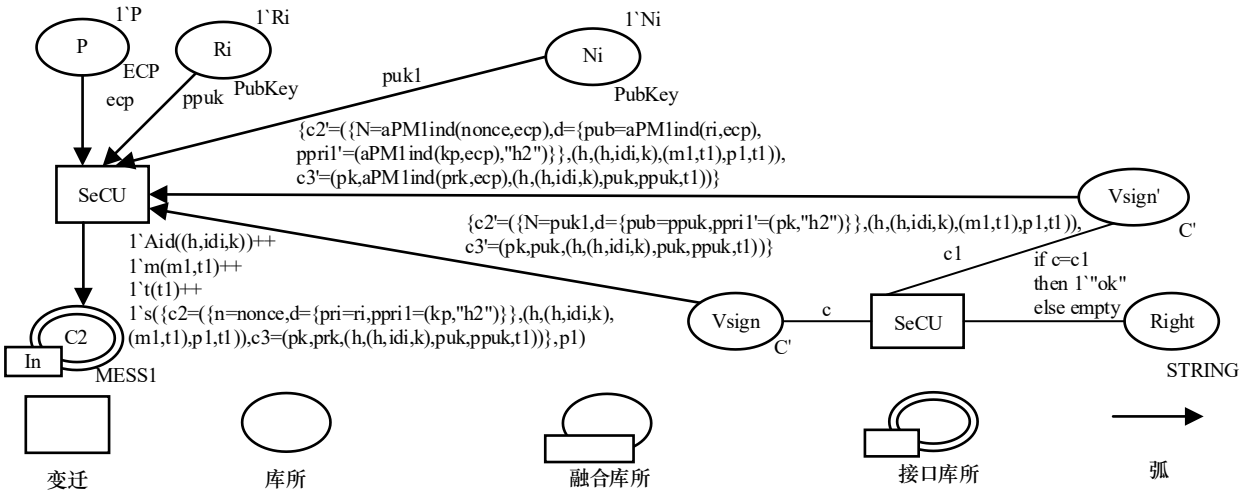

图 12　批量认证子模块 Receive and Verify 替代变迁 CPN 模型

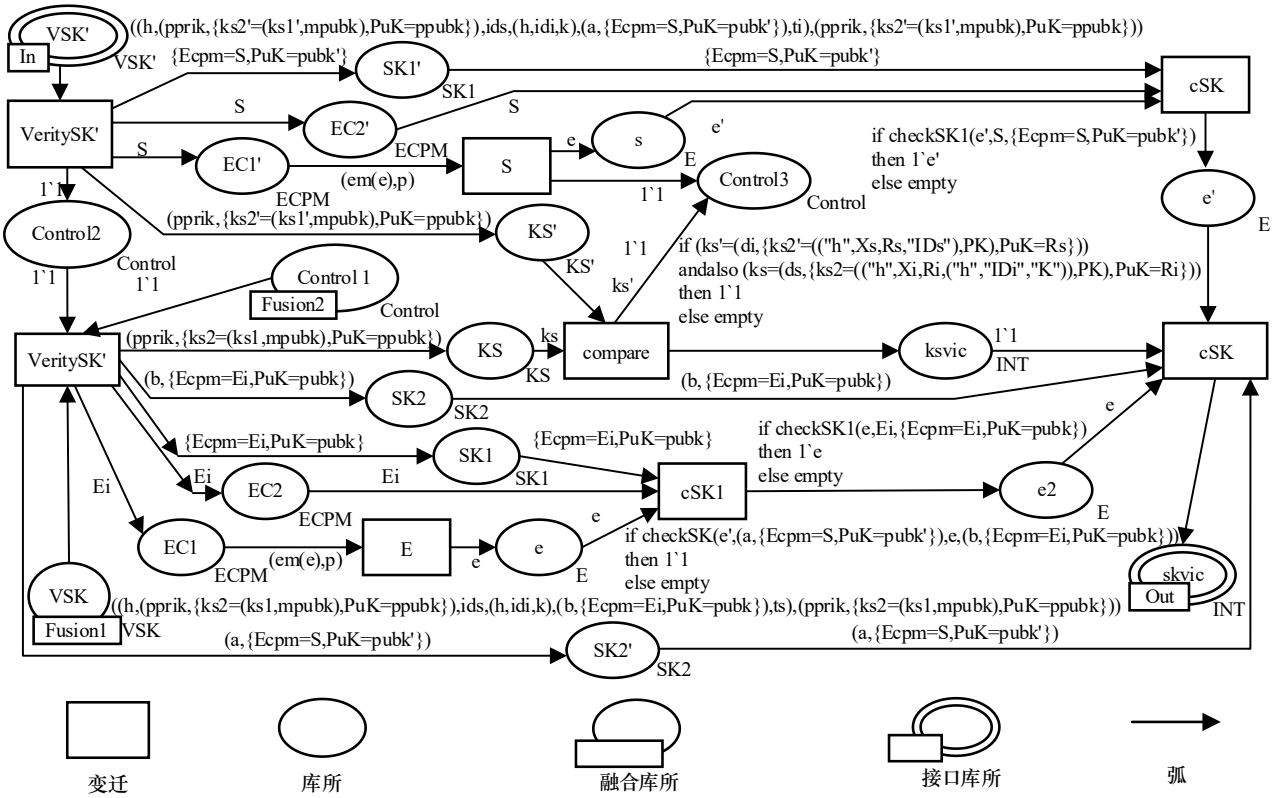

图 13　ECU 的子模块 VeritySK 替代变迁 CPN 模型

3.2　状态空间及模型检测结果

本节对基于本文方案建立的 CPN 模型进行调试，生成标准的状态空间报告。状态空间报告反映了所构建模型的准确性和活性等特征，有界性反映了库所可能达到的状态和状态持有的数量，活变迁反映了使可达状态永远发生所需的条件，死变迁是模型不能激活的部分，即状态不可发生或状态完成的终结。表 3 为本文方案原始 CPN 模型（无攻击者）的状态空间报告。

模型一致性检验结果表明，状态空间节点数和强连通节点数相同，状态空间有向弧数和强连通弧数相同，说明模型全部状态节点可达，不存在循环结构。原始 CPN 模型死节点数为 1，说明模型按照协议规范进行信息传输，存在一个数据传输完毕的状态。

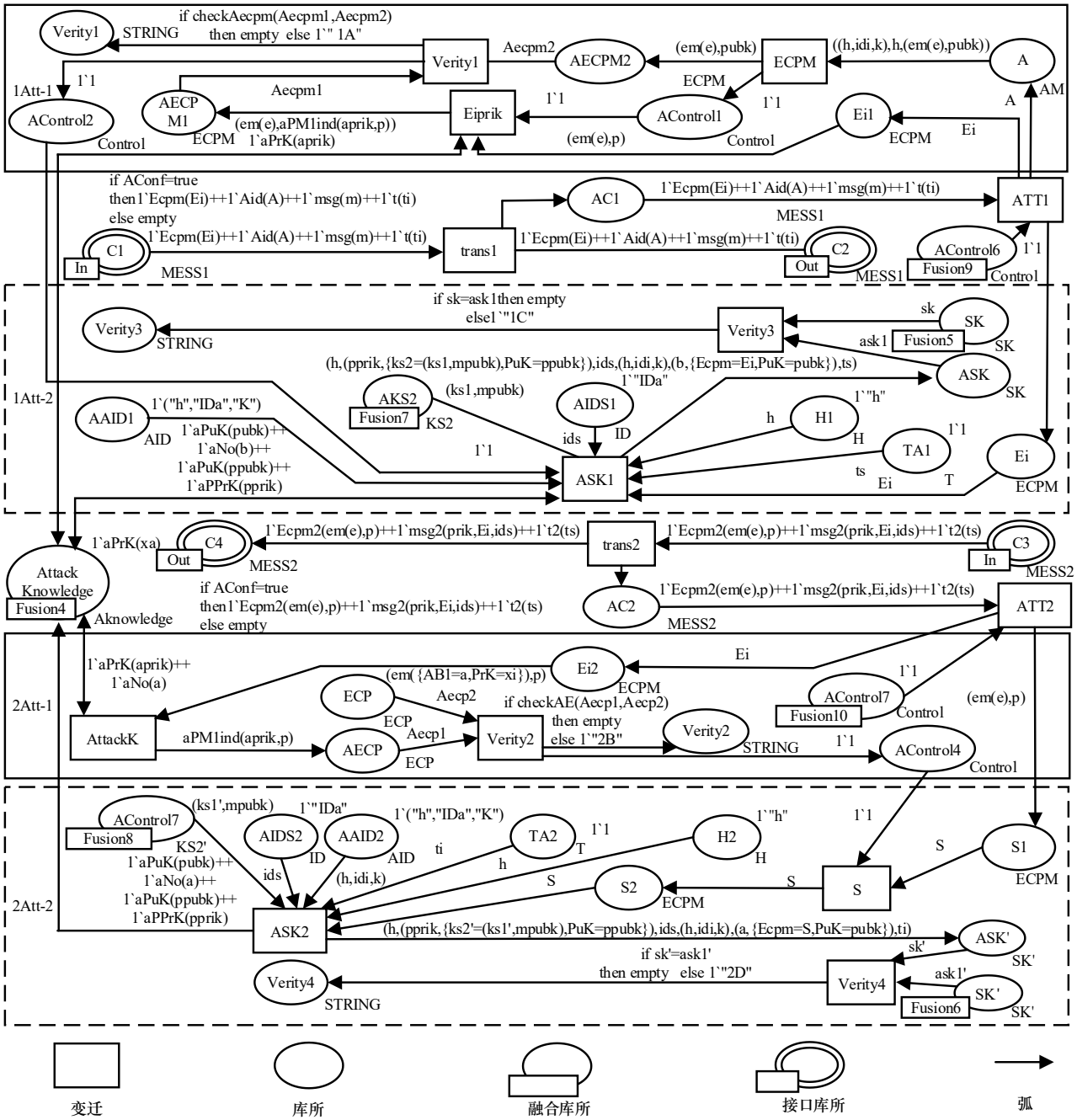

图 14　Network(Adversary)替代变迁 CPN 模型

表 3　本文方案原始 CPN 模型（无攻击者）的状态空间报告

状态空间信息	原始模型
状态空间节点/个	45
状态空间有向弧/条	44
强连通节点/个	45
强连通弧/条	44
死变迁、活变迁/个	0
死节点/个	1

表 4 为基于攻击者描述的安全评估模型状态空间及检测结果。攻击者模型的状态空间能够描述攻击者能力，是攻击者发起穷尽所有可能组合攻击的集合。1Att-1 为仅针对认证阶段发起重放攻击和伪装攻击，对应攻击者模型 trans1 信道中实线矩形块的攻击。1Att-2 为仅针对认证阶段发起已知特定会话临时信息攻击和已知密钥攻击，对应攻击者模型 trans1 信道中虚线矩形块的攻击。2Att-1 为仅

针对密钥协商阶段发起重放攻击和伪装攻击，对应攻击者模型trans2信道中实线矩形块的攻击。2Att-2为仅针对密钥协商阶段发起已知特定会话临时信息攻击和已知密钥攻击，对应攻击者模型trans2信道中虚线矩形块的攻击。All_Att为同时使用1Att-1、1Att-2、2Att-1、2Att-2后获得的状态空间报告。

表4　基于攻击者描述的安全评估模型状态空间及检测结果

类型	节点/个	弧/条	死节点/个	死节点查询
1Att-1	86	85	2	[82,86]
1Att-2	132	178	2	[82,132]
2Att-1	68	67	2	[65,68]
2Att-2	116	162	2	[65,116]
All_Att	3 143	11 121	4	[443,442,3 143,122]

3.3　安全验证结果

本节将基于攻击者的CPN模型进行死节点路径搜索，Network(Adversary)模型中定义4个Verity变迁，可以判断上述死节点路径是否为攻击路径。实线矩形块的变迁Verity1和Verity2验证了本文方案是否能抵抗伪装攻击和重放攻击，虚线矩形块的变迁Verity3和Verity4验证了本文方案是否能抵抗已知特定会话临时信息攻击和已知密钥攻击。

攻击者CPN模型的安全验证结果如表5所示。库所Verity1中的“1A”和Verity3中的“1C”表示ECU向SeCU发送认证请求消息后，攻击者从网络信道trans1发起攻击失败。库所Verity2中的“2B”和Verity4中的“2D”表示SeCU向ECU发送密钥协商请求消息后，攻击者从网络信道trans2发起攻击失败。

表5　攻击者CPN模型的安全验证结果

变迁	安全属性	验证值
Verity1（认证阶段）	抗重放攻击、伪装攻击	1A
Verity2（密钥协商阶段）	抗重放攻击、伪装攻击	1C
Verity3（认证阶段）	抗已知特定会话临时信息攻击、已知密钥攻击	2B
Verity4（密钥协商阶段）	抗已知特定会话临时信息攻击、已知密钥攻击	2D

1Att-1攻击下死节点路径的运行结果如图15所示。在82号死节点中，攻击者将trans1的AConf置为false，表明攻击者没有发起任何攻击。在86号死节点中，攻击者将trans1的AConf置为true，表明攻击者向认证阶段发起了重放和伪装攻击。库所Verity1中收到了消息“1A”，这说明认证阶段能有效抵抗上述攻击。

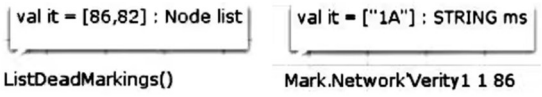

图15　1Att-1攻击下死节点路径的运行结果

1Att-2攻击下死节点路径的运行结果如图16所示。在82号死节点中，攻击者将trans1的AConf置为false，表明攻击者没有发起任何攻击。在132号死节点中，库所Verity3收到了消息“1C”，这说明认证阶段能有效抵抗已知特定会话临时信息攻击和已知密钥攻击。

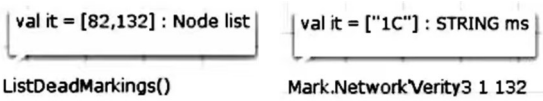

图16　1Att-2攻击下死节点路径的运行结果

2Att-1攻击下死节点路径的运行结果如图17所示。在65号死节点中，攻击者将trans2的AConf置为false，表明攻击者没有发起任何攻击。在68号死节点中，库所Verity2中收到了消息“2B”，说明密钥协商阶段能有效抵抗重放攻击和伪装攻击。

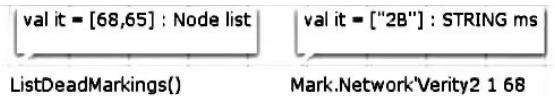

图17　2Att-1攻击下死节点路径的运行结果

2Att-2攻击下死节点路径的运行结果如图18所示。在65号死节点中，攻击者将trans1的AConf置为false，表明攻击者没有发起任何攻击。在116号死节点中，库所Verity4中收到了消息“2D”，说明密钥协商阶段能有效抵抗已知特定会话临时信息攻击和已知密钥攻击。

图18　2Att-2攻击下死节点路径的运行结果

图19为All_Att攻击下死节点路径的运行结果，包括库所Verity1、Verity2、Verity3、Verity4的

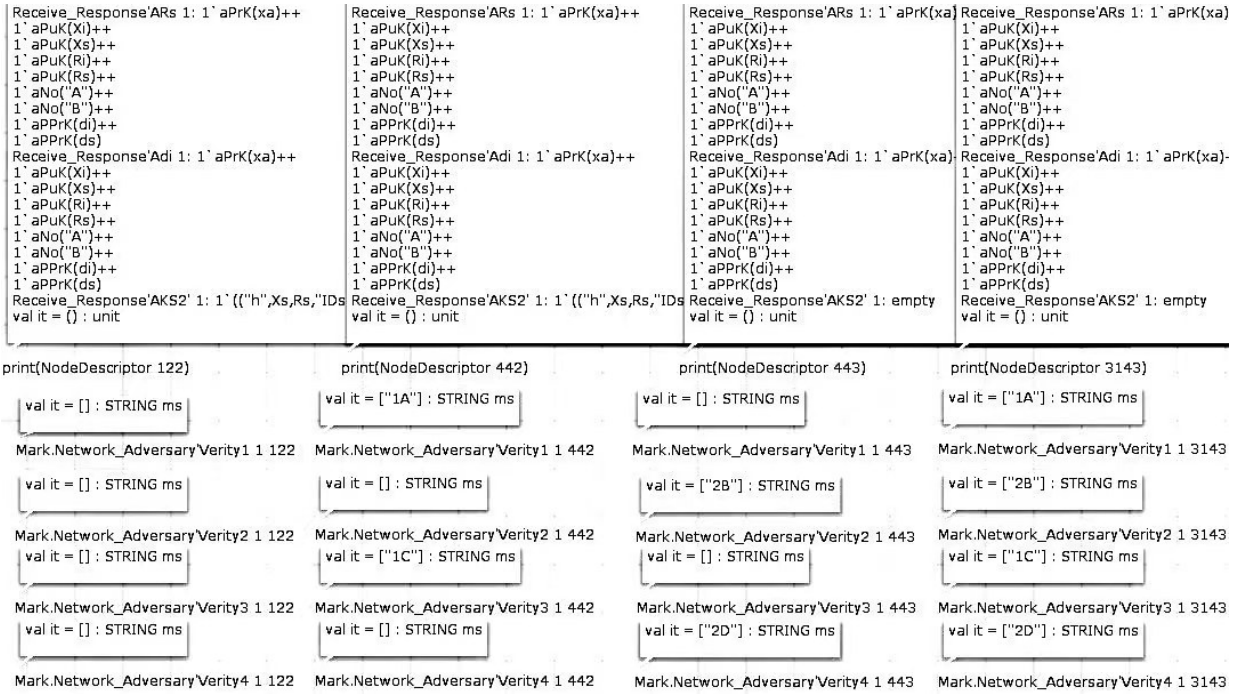

图19　All_Att攻击下死节点路径的运行结果

运行结果。然后通过NodeDescriptor函数查看死节点路径的攻击信息。

在122号死节点中，4个库所Verity没有收到信息，查看NodeDescriptor函数的库所AC1和AC2的内容可知，攻击者将trans1和trans2的AConf置为false，表明攻击者在122号死节点中没有发起任何攻击。

在442号死节点中，攻击者将trans1的AConf置为true，将trans2的AConf置为false，表明攻击者向认证阶段对应的网络信道trans1发起了攻击。而库所Verity1中收到了消息“1A”，Verity3中收到了消息“1C”，证明本文方案的认证阶段能有效抵抗恶意攻击。

在443号死节点中，攻击者将trans1的AConf置为false，将trans2的AConf置为true，表明攻击者向密钥协商阶段对应的网络信道trans2发起了攻击。而库所Verity2中收到了消息“2B”，Verity4中收到了消息“2D”，证明本文方案的密钥协商阶段能有效抵抗恶意攻击。

在3143号死节点中，攻击者将trans1的AConf置为true，将trans2的AConf也置为true，表明攻击者向本文方案各个阶段对应的网络信道trans1和trans2发起了攻击。库所Verity1中收到了消息“1A”，Verity2中收到了消息“2B”，Verity3中收到了消息“1C”，Verity4中收到了消息“2D”，证明本文方案的所有阶段均能有效抵抗恶意攻击。

4　安全性分析及性能评估

4.1　安全性分析

本节详细讨论了本文方案的抗攻击能力和安全功能。表6将本文方案与文献[3,19,27,30]方案在安全属性和功能特性2个方面进行了对比。安全属性是方案在面临恶意攻击时能够保持抗攻击的能力，定义SP_1表示抗重放攻击，SP_2表示抗伪装攻击，SP_3表示抗篡改攻击，SP_4表示抗中间人攻击，SP_5表示抗内部授权攻击，SP_6表示抗已知密钥攻击，SP_7表示抗已知特定会话临时信息攻击。功能特性是方案具备的安全功能，定义FP_1表示身份认证，FP_2表示密钥协商，FP_3表示设备匿名性，FP_4表示完美前后向安全，FP_5表示形式化证明。

表6　　安全属性和功能特性对比

方案	安全特性							功能特性				
	SP_1	SP_2	SP_3	SP_4	SP_5	SP_6	SP_7	FP_1	FP_2	FP_3	FP_4	FP_5
文献[3]	√	×	√	×	×	×	×	√	×	√	×	×
文献[19]	×	√	√	×	×	×	×	√	×	√	×	×
文献[27]	×	×	√	×	×	√	√	√	√	×	√	×
文献[30]	√	√	√	√	√	×	√	√	√	×	×	×
本文方案	√	√	√	√	√	√	√	√	√	√	√	√

1) 抗重放攻击。假设攻击者在网络信道窃取并不断地重放有效的消息，然而，由于攻击者发送的 m_1 此时已经过期，SeCU 计算 $\mathrm{AID}'_i = A \oplus H_3(x_s E)$，并通过时间戳 T_i 验证出 $m' = H_4(E \| \mathrm{AID}'_i \| T_i) \neq m$，从而可以判断出攻击者发送的消息是无效的。同理，在批量认证阶段，SeCU 通过验证 h_{i_3} 和 h_{i_4} 发现攻击者的重放消息。因此，本文方案可以有效抵抗重放攻击。

2) 抗伪装攻击。当攻击者希望获取车载网络服务时，需要冒充为合法车辆或合法SeCU窃取实体的信息。如果攻击者冒充为合法车辆，那么必须计算出正确的 $A = \mathrm{AID}_i \oplus H_3(eX_s)$。然而，攻击者无法获得秘密值 e，不能计算出正确的 A，SeCU通过 $\mathrm{AID}'_i = A \oplus H_3(x_s E)$ 得出 $m' \neq m$，从而判断出攻击者为恶意身份。同样，攻击者也不能冒充合法SeCU，ECU通过计算 $\mathrm{ID}_s = D_{eX_s}(m_2)$ 判断出攻击者为恶意身份窃取车辆信息。同理，在批量认证阶段，攻击者也不能计算出正确的 h_{i_3} 和 h_{i_4}，不能通过 C_i 的认证。因此，本文方案可以有效抵抗伪装攻击。

3) 抗篡改攻击。攻击者在网络信道试图篡改通信双方发送的消息。然而，由于认证向量包含哈希函数，SeCU 通过验证 $m' = H_4(E \| \mathrm{AID}'_i \| T_i) \neq m$ 避免攻击者篡改 E 和 AID'_i。会话密钥 SK_s 和 SK_i 也使用了哈希函数避免攻击者篡改 $b(E - X_i)$ 和 $a(S - X_s)$，攻击者只能截获和转发消息，而无法修改和获得额外信息。在批量认证阶段，也存在 h_{i_3} 和 h_{i_4} 抵抗攻击者恶意篡改。因此，本文方案可以有效抵抗篡改攻击。

4) 抗中间人攻击。攻击者通过在通信双方之间秘密拦截，达到窃取、篡改数据或冒充一方进行恶意活动的目的。本文利用CPN Tools建模工具，将Dolev-Yao攻击者通过模型进行了直观的展示，形式化模型建立了攻击者知识库，模拟了中间人攻击，验证结果证明了 $m' \neq m$，攻击者无法冒充任何一方合法实体协商出正确的会话密钥 SK_s 和 SK_i，不能在会话中插入伪造消息通过诚实实体的识别和验证。因此，本文方案可以有效抵抗中间人攻击。

5) 抗内部授权攻击。Dolev-Yao模型中攻击者具有强大的计算能力，能够熟悉密码学操作，并作为合法实体参与协议交互流程。本文方案加入Dolev-Yao模型，将攻击者能力存储在攻击者知识库中，运行后的状态空间检测表明攻击者无法获得 SK_s 和 SK_i 等密钥信息，证明了对内部授权攻击的抵抗力。因此，本文方案可以有效抵抗内部授权攻击。

6) 抗已知密钥攻击。攻击者已经获得了诚实实体的长期密钥，并试图与其他设备通信。但是由于每一次认证和密钥协商时，E 和 S 中都有随机数参与认证，攻击者无法计算出正确的 $e = x_i + a$ 和 $s = x_s + b$，从而无法被其他设备认证。因此，本文方案可以有效抵抗已知密钥攻击。

7) 抗已知特定会话临时信息攻击。攻击者可以访问由通信双方生成的随机数、部分私钥等临时信息。在认证阶段，攻击者无法获得全部私钥信息 e 和 s，不能成功生成正确的认证消息，无法计算出正确的 $A = \mathrm{AID}_i \oplus H_3(eX_s)$ 或 $\mathrm{AID}'_i = A \oplus H_3(x_s E)$。在密钥协商阶段，攻击者虽然可以计算出 K_s 和 K_i，但是攻击者无法获得 e 和 s，无法合成任何一方的会话密钥 SK_s 和 SK_i。因此，本文方案可以有效抵抗已知特定会话临时信息攻击。

8) 身份认证与密钥协商。ECU和SeCU通过生成随机数 a 和 b，利用椭圆曲线点乘运算对认证消息 m 进行验证并执行密钥协商。因此，本文方案可以实现ECU和SeCU的双向身份认证与密钥协商。

9) 设备匿名性。ECU的真实身份信息包含在假名 AID_i 中，任何通过公共通道传输的消息都不会直接包含主体的真实身份。攻击者很难在短时间内获得ECU的真实身份 ID_i，因此，本文方案可满足匿名性的需求。

10) 完美前后向安全。由于本文会话密钥协商过程中使用的部分私钥为 $d_i = D_i - x_i R_i = r_i + kh_{i_2}$ 和 $d_s = D_s - x_s R_s = r_s + kh_{s_2}$，有随机数 r_i 和 r_s 参与生成，且 a 和 b 也是临时随机数，通过椭圆曲线协商的会话密钥 SK_s 和 SK_i 也是随机变化的，攻击者无法从当前的会话密钥推测出前轮或后轮会话密钥。因此，本文方案可以满足会话密钥完美前后向安全。

11) 形式化证明。本文通过CPN Tools结合Dolev-Yao攻击者模型进行了方案的形式化证明和安全评估。形式化证明基于模型的逻辑检测，系统化地验证和证明了本文方案的正确性和安全性。

4.2　性能评估

本节对本文方案在认证与密钥协商阶段和批量

认证阶段2个不同场景下所需要的计算开销与通信开销进行了分析。在配置为Intel(R) Core(TM) i7-9750H、RAM为8.00 GB的Windows10环境下，于Visual6.0中使用密码学库PBC0.4.7对相应的密码操作时间进行了模拟，各项密码操作执行时间如表7所示。其中，T_h、T_a、T_m、T_{ep}、T_{bp}、T_{mp}、T_e、T_d分别表示进行一次哈希运算、椭圆曲线点加法运算、椭圆曲线点乘运算、指数运算、双线性配对、映射到其上的点、AES对称加密、AES对称解密所需要的时间。

表7 密码操作执行时间

密码学运算	执行时间/ms
T_h	0.000 1
T_a	0.005 1
T_m	1.205 1
T_{ep}	0.316 3
T_{bp}	3.482 6
T_{mp}	3.927 9
T_e	0.814 2
T_d	0.642 7

为了评估通信开销，本节将随机数、伪身份、时间戳、哈希函数、椭圆曲线点的位长大小分别设定为160 bit、160 bit、32 bit、256 bit和320 bit。为了评估本文方案在认证与密钥协商阶段的性能，将其与安全系数较高的文献[19-20,26-27]方案进行对比，得出了各方案下认证与密钥协商阶段各实体分别需要的计算开销、整体计算开销与通信开销，如表8所示。

由表8可知，文献[19,26-27]使用椭圆曲线提出了针对车载网络的认证方案，但本文方案计算开销更低；文献[20]使用复杂的双线性配对运算，计算开销较大。由上述结果可得，本文方案具有较低的计算开销。本文方案的通信开销包含M_1和M_2，M_1的位长为320+160+256+32=768 bit，M_2的位长为320+256+32=608 bit，总通信开销为1 376 bit。图20直观展示了各方案的认证与密钥协商阶段各实体分别需要的计算开销与总计算开销。

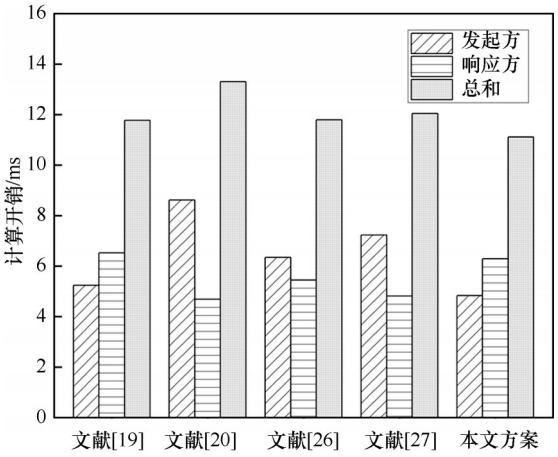

图20 认证与密钥协商阶段各实体分别需要的计算开销与总计算开销

为了评估本文方案的批量认证性能，将其与文献[3,28-30]方案进行对比，得出了各方案所需要的通信开销，以及相应的签名方、验证方及批量验证的计算开销，如表9所示。

文献[3,28-30]签名方、验证方及其总计算开销如图21所示，总计算开销分别为$8T_m$=9.641 ms、$4T_{bp}+2T_{ep}$=14.563 ms、$2T_m+2T_{bp}$=9.375 ms、$3T_{bp}+T_{ep}$=10.764 ms；本文方案签名和单个验证的总计算开销为$5T_m+5T_a+5T_h$=6.052 ms，通信开销为（160+320+256+32）=768 bit。图22比较了文献[3,28-30]与本文方案在批量验证中验证n个签名的计算成本。本文批量认证方案与文献[3,28-30]方案相比计算开销较小，且能保证较高的安全性。

表8 认证与密钥协商阶段各实体分别需要的计算开销、整体计算开销与通信开销

方案	发起方/ms	响应方/ms	总计算开销/ms	通信开销/bit
文献[19]	$3T_m+4T_h+2T_e$	$3T_m+5T_h+2T_e+2T_d$	$6T_m+9T_h+4T_e+2T_d$=11.774	1 984
文献[20]	$T_m+6T_h+T_{bp}+T_{mp}$	$7T_h+T_{bp}+T_m$	$2T_m+13T_h+2T_{bp}+T_{mp}$=13.305	3 328
文献[26]	$5T_m+2T_h+T_{ep}$	$4T_m+2T_{ep}+5T_h$	$3T_{ep}+9T_m+7T_h$=11.796	2 144
文献[27]	$6T_m+5T_h$	$4T_m+7T_h$	$10T_m+12T_h$=12.052	2 080
本文方案	$4T_m+5T_h+2T_a$	$4T_m+4T_h+2T_a+T_e+T_d$	$8T_m+9T_h+4T_a+T_e+T_d$=11.119	1 376

表9　批量认证阶段计算开销与通信开销

方案	签名方/ms	验证方/ms	批量验证/ms	通信开销/bit
文献[3]	$2T_m$	$6T_m$	$6nT_m$	928 n
文献[28]	$2T_m$	$2T_m + 2T_{ep}$	$(2n)T_m + (n+2)T_{ep}$	864 n
文献[29]	T_{bp}	$T_{bp} + 2T_m$	$(n)T_{bp} + (n+2)T_m$	1 056 n
文献[30]	$2T_{bp}$	$T_{bp} + T_{ep}$	$(n+2)T_{bp} + (n)T_{ep}$	832 n
本文方案	$3T_m + 2T_a + 2T_h$	$2T_m + 3T_a + 3T_h$	$(2n+2)T_m + 3nT_h + (2n+1)T_a$	768 n

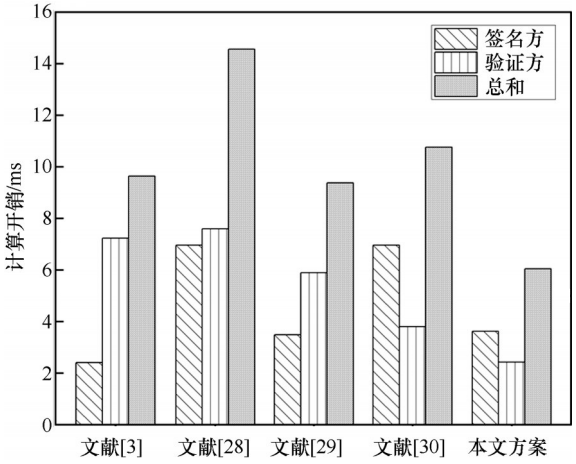

图21　批量验证阶段签名方、验证方及其总计算开销对比

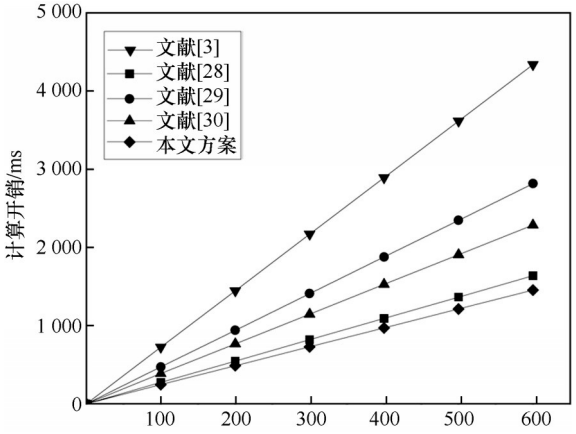

图22　批量验证阶段批量验证计算开销对比

5　结束语

本文提出了车载网络中基于无证书的匿名认证和密钥协商方案。针对计算受限的ECU，本文通过批量认证降低身份验证成本，以提供车载节点之间的高效密钥建立和快速认证。通过椭圆曲线和异或运算安全完成无证书认证并构建会话密钥，利用哈希函数实现匿名机制确保了车载网络安全的通信过程，实现了轻量级的方案，解决了现有车载网络无证书方案中双线性配对消耗大量资源的缺陷。本文提出了有色Petri网引入Dolev-Yao攻击者模型的形式化安全验证手段，构建了CPN模型并在认证和密钥协商阶段进行多种不同类型的攻击。状态空间验证结果表明，本文方案实现了匿名性、完美前后向安全性，能够抵抗重放、篡改、伪装、已知密钥、已知特定会话临时信息攻击。性能仿真实验表明，本文方案与现有工作相比计算开销较小。

参考文献：

[1] GONG X, FENG T. Lightweight anonymous authentication and key agreement protocol based on CoAP of Internet of things[J]. Sensors, 2022, 22(19): 7191.

[2] 彭维平, 韩宁, 宋成. 边缘计算环境下无证书车联网身份认证方案[J]. 北京邮电大学学报, 2022, 45(1): 46-51.
PENG W P, HAN N, SONG C. Certificateless identity authentication scheme for Internet of vehicles in edge computing environment[J]. Journal of Beijing University of Posts and Telecommunications, 2022, 45(1): 46-51.

[3] PALANISWAMY B, ANSARI K, REDDY A G, et al. Robust certificateless authentication protocol for the SAE J1939 commercial vehicles bus[J]. IEEE Transactions on Vehicular Technology, 2023, 72(4): 4493-4509.

[4] 张海波, 兰凯, 陈舟, 等. 车联网中基于环的匿名高效批量认证与组密钥协商协议[J]. 通信学报, 2023, 44(6): 103-116.
ZHANG H B, LAN K, CHEN Z, et al. Ring-based efficient batch authentication and group key agreement protocol with anonymity in Internet of vehicles[J]. Journal on Communications, 2023, 44(6): 103-116.

[5] DU J Z, TANG R, FENG T. Security analysis and improvement of vehicle Ethernet SOME/IP protocol[J]. Sensors, 2022, 22(18): 6792.

[6] 张海波, 黄宏武, 刘开健, 等. 车联网中可证安全的匿名可追溯快速组认证协议[J]. 通信学报, 2021, 42(6): 213-225.
ZHANG H B, HUANG H W, LIU K J, et al. Verifiably secure fast group authentication protocol with anonymous traceability for Internet of vehicles[J]. Journal on Communications, 2021, 42(6): 213-225.

[7] 肖敏, 毛发英, 黄永洪, 等. 基于属性签名的车载网匿名信任管理方案[J]. 网络与信息安全学报, 2023, 9(2): 33-45.
XIAO M, MAO F Y, HUANG Y H, et al. Anonymous trust management scheme of VANET based on attribute signature[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 33-45.

[8] 吴武飞, 李仁发, 曾刚, 等. 智能网联车网络安全研究综述[J]. 通信学报, 2020, 41(6): 161-174.
WU W F, LI R F, ZENG G, et al. Survey of the intelligent and connected vehicle cybersecurity[J]. Journal on Communications, 2020, 41(6): 161-174.

[9] GROZA B, MURVAY S, HERREWEGE A, et al. Libra-CAN: lightweight broadcast authentication for controller area networks[J]. ACM

Transactions on Embedded Computing Systems, 2017, 16(3): 90.
[10] GROZA B, MURVAY S. Efficient protocols for secure broadcast in controller area networks[J]. IEEE Transactions on Industrial Informatics, 2013, 9(4): 2034-2042.
[11] PALANISWAMY B, CAMTEPE S, FOO E, et al. An efficient authentication scheme for intra-vehicular controller area network[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3107-3122.
[12] WOO S, JO H J, LEE D H. A practical wireless attack on the connected car and security protocol for In-vehicle CAN[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 993-1006.
[13] MURVAY P S, GROZA B. Security shortcomings and countermeasures for the SAE J1939 commercial vehicle bus protocol[J]. IEEE Transactions on Vehicular Technology, 2018, 67(5): 4325-4339.
[14] 刘雪艳, 王力, 郇丽娟, 等. 车联网环境下无证书匿名认证方案[J]. 电子与信息学报, 2022, 44(1): 295-304.
LIU X Y, WANG L, HUAN L J, et al. Certificateless anonymous authentication scheme for Internet of vehicles[J]. Journal of Electronics & Information Technology, 2022, 44(1): 295-304.
[15] CHENG K, BAI Y B, ZHOU Y, et al. CANeleon: protecting CAN bus with frame ID chameleon[J]. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7116-7130.
[16] GROZA B, MURVAY P S. Identity-based key exchange on In-vehicle networks: CAN-FD & FlexRay[J]. Sensors, 2019, 19(22): 4919.
[17] TSAI J L, LO N W. A privacy-aware authentication scheme for distributed mobile cloud computing services[J]. IEEE Systems Journal, 2015, 9(3): 805-815.
[18] HE D B, KUMAR N, KHAN M K, et al. Efficient privacy-aware authentication scheme for mobile cloud computing services[J]. IEEE Systems Journal, 2018, 12(2): 1621-1631.
[19] LI Q R, HSU C F, RAYMOND CHOO K K, et al. A provably secure and lightweight identity-based two-party authenticated key agreement protocol for vehicular ad hoc networks[J]. Security and Communication Networks, 2019, 2019: 1-13.
[20] CARVAJAL-ROCA I E, WANG J, DU J, et al. A semi-centralized dynamic key management framework for in-vehicle networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(10): 10864-10879.
[21] LIU X G, JIN C H, LI F G. An improved two-layer authentication scheme for wireless body area networks[J]. Journal of Medical Systems, 2018, 42(8): 143.
[22] CHENG Q F, LI Y T, SHI W B, et al. A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network[J]. Mobile Networks and Applications, 2022, 27(1): 346-356.
[23] KUMAR M, CHAND S. A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network[J]. IEEE Systems Journal, 2021, 15(2): 2779-2786.
[24] SOWJANYA K, DASGUPTA M, RAY S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems[J]. International Journal of Information Security, 2020, 19(1): 129-146.
[25] WANG W M, HUANG H P, XIAO F, et al. Computation-transferable authenticated key agreement protocol for smart healthcare[J]. Journal of Systems Architecture, 2021, 118: 102215.
[26] XU C, HUANG X H, MA M D, et al. An anonymous handover authentication scheme based on LTE-A for vehicular networks[J]. Wireless Communications and Mobile Computing, 2018, 2018: 1-15.
[27] DWIVEDI S K, AMIN R, VOLLALA S, et al. B-HAS: blockchain-assisted efficient handover authentication and secure communication protocol in VANETs[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 3491-3504.
[28] HORNG S J, TZENG S F, PAN Y, et al. B-SPECS: batch verification for secure pseudonymous authentication in VANET[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1860-1875.
[29] CUI J, ZHANG J, ZHONG H, et al. SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 10283-10295.
[30] HE D B, ZEADALLY S, XU B W, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.
[31] KARATI A, ISLAM S H, KARUPPIAH M. Provably secure and lightweight certificateless signature scheme for IIoT environments[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3701-3711.
[32] ZHANG Y H, DENG R H, ZHENG D, et al. Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2019, 15(9): 5099-5108.
[33] YANG W J, WANG S P, HUANG X Y, et al. On the security of an efficient and robust certificateless signature scheme for IIoT environments[J]. IEEE Access, 2019, 7: 91074-91079.
[34] REZAEIBAGHA F, MU Y, HUANG X Y, et al. Fully secure lightweight certificateless signature scheme for IIoT[J]. IEEE Access, 2019, 7: 144433-144443.
[35] XIONG H, MEI Q, ZHAO Y N. Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments[J]. IEEE Systems Journal, 2020, 14(1): 310-320.
[36] 龚翔, 冯涛, 杜谨泽. 基于CPN的安全协议形式化建模及安全分析方法[J]. 通信学报, 2021, 42(9): 240-253.
GONG X, FENG T, DU J Z. Formal modeling and security analysis method of security protocol based on CPN[J]. Journal on Communications, 2021, 42(9): 240-253.
[37] YAN Z P, GU C L, HUANG H J. Analysis for threat models and improvement scheme of 5G AKA protocol based on petri-net[C]//Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT). Piscataway: IEEE Press, 2021: 11-17.
[38] GONG X, FENG T, ALBETTAR M. PEASE: a PUF-based efficient authentication and session establishment protocol for machine-to-machine communication in industrial IoT[J]. Electronics, 2022, 11(23): 3920.

[作者简介]

郑路（1997– ），女，河南郑州人，兰州理工大学博士生，主要研究方向为制造业信息化系统与网络安全、工业互联网、车联网等。

冯涛（1970– ），男，甘肃临洮人，博士，兰州理工大学研究员、博士生导师，主要研究方向为网络与信息安全、区块链、工业互联网安全、通信协议安全分析与设计、网络空间应用系统的设计与实现、网络空间系统隐私保护等。

苏春华（1981– ），男，广西钦州人，博士，日本会津大学高级副教授、博士生导师，主要研究方向为密码分析、密码协议、机器学习中的隐私保护技术和物联网安全与隐私等。