分类号： 密级：

ＵＤＣ： 编号：

工学硕士学位论文

车联网环境下的女巫攻击检测技术研究

硕士研究生 ：郭芷如

指导教师 ：张文波 教授

学科、专业 ：计算机技术

所在单位 ：信息科学与工程学院

论文提交日期：2026年2月24日

论文答辩日期：2026年3月10日

学位授予单位：沈阳理工大学

沈阳理工大学

2026年3月

Classification Index:

U.D.C:

A Thesis for the Degree of M.Eng

Research on Sybil Attack Detection Technologies for Internet of Vehicles Environment

Candidate : Guo Zhiru

Supervisor: Prof. Zhang Wenbo

Speciality : Computer Technology

Date of Submission: February24, 2026

Date of Examination: March 10, 2026

University: Shenyang Ligong University

沈阳理工大学

硕士学位论文原创性声明

本人郑重声明:本论文的所有工作，是在导师的指导下，由作者本人独立完成的。有关观点、方法、数据和文献的引用已在文中指出，并与参考文献相对应。除文中已注明引用的内容外，本论文不包含任何其他个人或集体已经公开发表的作品成果。对本文的研究做出重要贡献的个人和集体，均己在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

作者（签字）：

日 期 ： 年 月

学位论文版权使用授权书

本学位论文作者完全了解沈阳理工大学有关保留、使用学位论文的规定，即：沈阳理工大学有权保留并向国家有关部门或机构送交学位论文的复印件和磁盘，允许论文被查阅和借阅。本人授权沈阳理工大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其它复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名： 　指导教师签名：

日　 　期： 日　　　　期：

# 摘 要

在车联网快速发展的今天，车辆之间以及与路侧基础设施的互联能力迅速提升，形成了高度动态和复杂的信息交互网络。然而，随着车联网中数据传输量的急剧增加以及路况信息的复杂多变，数据传输可靠性和用户隐私保护问题日益突出。为确保车联网在数据传输和隐私保护方面的可靠性和安全性，本文提出了基于区块链技术的车联网数据传输可靠性及隐私保护技术，以解决上述车联网环境中的问题。

针对车联网中数据传输可靠性问题，本文主要围绕提升车联网环境中的数据传输一致性与可靠性展开，重点解决传统共识机制在车联网应用中存在的恶意节点防御不足等问题，提出了一种基于信誉的R-PBFT（Reputation-Practical Byzantine Fault Tolerance）共识机制。引入信誉机制，根据节点的历史表现动态选择代理节点，降低恶意节点成为代理节点的概率。通过信誉阈值对节点进行分类，利用奖惩机制鼓励节点积极参与共识，对消极或恶意节点实施扣分，从而提升整体共识的统一性和可靠性。实验结果表明，相较实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）算法，R-PBFT共识算法兼顾了时延和可靠性的优化，不仅在高密度和高恶意节点比例的环境下表现出较好的扩展性，而且在共识过程中提高了数据传输可靠性。

针对车联网中位置隐私保护问题，现有的相关假名位置隐私保护方法无法有效抵御假名关联攻击，本文提出了一种基于动态超车的假名交换（Dynamic Overtaking-Based Pseudonym Exchange，DOPE）方法。为车辆分配时段假名池，假名到期时车辆首先根据动态超车方案选择假名交换，若附近没有匹配车辆，则在假名池中替换假名完成假名更新。动态超车方案通过模拟车辆的超车行为，使得假名交换行为更加自然，掩盖假名交换过程从而提升隐私保护效果。该方案分为目标选择、意愿协商、报备请求及执行交换四个阶段。根据预设的超车条件筛选符合的目标车辆，与其协商假名交换具体时间并报备至证书管理机构（Certificate Authority，CA）申请交换许可，正式进行假名交换的同时广播虚假信标消息，从而完成动态超车并达到位置隐私保护效果。通过对DOPE与现有位置隐私保护方法进行仿真实验对比，结果表明，DOPE方法具有一定的安全性，能够降低被追踪概率，提高平均匿名熵，在面对假名攻击时具备更高的位置隐私保护水平。

关键词：车联网；区块链；R-PBFT共识算法；假名交换；DOPE；动态超车

#### 

# Abstract

In the rapidly evolving field of the Internet of Vehicles (IoV), the interconnection capabilities between vehicles and roadside infrastructure have improved significantly, forming a highly dynamic and complex network for information exchange. However, with the sharp increase in data transmission and the complexity of traffic information, issues concerning the reliability of data transmission and user privacy protection have become increasingly prominent. To ensure reliability and security in data transmission and privacy protection within IoV, this paper proposes blockchain-based techniques for enhancing data transmission reliability and privacy protection, addressing the challenges present in the IoV environment.

To address the issue of data transmission reliability in IoV, this study focuses on improving the consistency and reliability of data transmission in dynamic IoV environments. It specifically tackles the shortcomings of traditional consensus mechanisms, such as insufficient defense against malicious nodes, by proposing a Reputation-Based Practical Byzantine Fault Tolerance (R-PBFT) consensus mechanism. The mechanism incorporates a reputation system that dynamically selects proxy nodes based on their historical behavior, reducing the probability of malicious nodes becoming proxies. Nodes are classified using a reputation threshold, and a reward-and-punishment system is employed to encourage active participation while penalizing passive or malicious behavior. This approach enhances the overall uniformity and reliability of consensus. Experimental results demonstrate that compared to the traditional Practical Byzantine Fault Tolerance (PBFT) algorithm, the R-PBFT mechanism optimizes both latency and reliability. It shows superior scalability in high-density environments with a high proportion of malicious nodes and significantly improves data transmission reliability during the consensus process.

For location privacy protection in IoV, existing pseudonym-based methods are inadequate against pseudonym linkage attacks. This paper introduces a Dynamic Overtaking-Based Pseudonym Exchange (DOPE) method. Vehicles are assigned pseudonym pools for specific time slots, and when a pseudonym expires, they first attempt to exchange pseudonyms based on the dynamic overtaking scheme. If no suitable vehicles are nearby, the pseudonym is replaced within the pool for update. The dynamic overtaking scheme simulates natural overtaking behavior, making the pseudonym exchange process less conspicuous and enhancing privacy protection. The scheme consists of four stages: target selection, intention negotiation, reporting request, and exchange execution. Vehicles select suitable targets based on predefined overtaking conditions, negotiate the timing for pseudonym exchange, and report to the Certificate Authority (CA) to request permission. During the pseudonym exchange, vehicles broadcast decoy beacon messages to conceal the process, achieving dynamic overtaking and improving location privacy protection.Simulation experiments comparing DOPE with existing location privacy protection methods indicate that the DOPE method provides a higher level of security, reducing the probability of being tracked and increasing average anonymity entropy. Furthermore, it demonstrates superior resistance to pseudonym linkage attacks, offering enhanced protection for location privacy in IoV environments.

Key words: Internet of Vehicles (IoV); Blockchain; R-PBFT Consensus Algorithm; Pseudonym Exchange; DOPE; Dynamic Overtaking

# 目 录

[摘 要 4](#_Toc208762395)

[Abstract 6](#_Toc208762396)

[目 录 8](#_Toc208762397)

[第1章 绪论 1](#_Toc208762398)

[1.1 研究背景及意义 1](#_Toc208762399)

[1.2 国内外研究现状 2](#_Toc208762400)

[1.1.1 数据传输可靠性研究现状 2](#_Toc208762401)

[1.1.2 隐私保护研究现状 3](#_Toc208762402)

[1.3 论文主要研究内容 6](#_Toc208762403)

[1.4 论文组织结构 7](#_Toc208762404)

[第2章 相关理论与技术 9](#_Toc208762405)

[2.1 车联网技术概述 9](#_Toc208762406)

[2.1.1 车联网体系架构 9](#_Toc208762407)

[2.1.2 车联网面临的技术挑战 11](#_Toc208762408)

[2.2 女巫攻击 12](#_Toc208762409)

[2.2.1 女巫攻击的基本原理 13](#_Toc208762410)

[2.2.2 车联网中女巫攻击的具体形式与危害 13](#_Toc208762411)

[2.2.3 车联网女巫攻击防御的核心挑战 14](#_Toc208762412)

[2.3 联邦学习 15](#_Toc208762413)

[2.4 CNN与LSTM 17](#_Toc208762414)

[2.4.1 CNN 17](#_Toc208762415)

[2.4.2 LSTM 18](#_Toc208762416)

[2.5 本章小结 19](#_Toc208762417)

[第3章 基于信誉的R-PBFT共识机制 **错误！未定义书签。**](#_Toc208762418)

[3.1 系统模型 20](#_Toc208762419)

[3.2 女巫攻击模型 22](#_Toc208762420)

[3.3 系统初始化 22](#_Toc208762421)

[3.4 检测方案描述 23](#_Toc208762422)

[3.5 仿真实验及结果分析 29](#_Toc208762423)

[3.5.1 实验环境与实验设计 29](#_Toc208762424)

[3.5.2 实验结果与分析 31](#_Toc208762425)

[3.6 本章小结 34](#_Toc208762426)

[第4章 基于SAFL-VR的女巫攻击检测方案 35](#_Toc208762427)

[4.1 问题定义 35](#_Toc208762428)

[4.2 SAFL-VR框架 36](#_Toc208762429)

[4.2.1 多维特征提取 36](#_Toc208762430)

[4.2.2 女巫感知LSTM网络 38](#_Toc208762431)

[4.2.3 基于信任的模型聚合 40](#_Toc208762432)

[4.3 仿真实验与分析 40](#_Toc208762433)

[4.3.1 实验环境与实验设计 40](#_Toc208762434)

[4.3.2 实验分析与对比 41](#_Toc208762435)

[4.4 本章小结 42](#_Toc208762436)

[第5章 结论 43](#_Toc208762437)

[参考文献 44](#_Toc208762438)

[攻读硕士学位期间发表的论文和取得的科研成果 49](#_Toc208762439)

[致谢 50](#_Toc208762440)

# 绪论

## 研究背景及意义

随着车联网（Internet of Vehicles, IoV）与智能交通系统（Intelligent Transportation Systems，ITS）的深度融合，车辆正在从“信息孤岛”演变为“移动节点”，通过车联万物（Vehicle-to-Everything，V2X）通信实现车与车（V2V）、车与路（V2I）、车与云（V2C）之间的毫秒级数据共享。根据 5GAA 的预测，到 2030 年全球将有超过 7.5 亿辆联网汽车上路，每秒产生的数据量将突破 10 GB。如此高频、高密度的数据交互，在为碰撞预警、绿波车速引导、协同变道、自动驾驶编队等高级应用提供实时决策依据的同时，也引入了新的攻击面。其中，女巫攻击（Sybil Attack）因其隐蔽性强、破坏力大，已被美国 NHTSA 与欧洲 ENISA 列为 VANET 五大顶级威胁之一，成为亟待解决的关键安全问题。女巫攻击由Douceur于2002年首次提出[4]，攻击者通过伪造大量虚假身份（Sybil IDs），可在短时间内占据网络中极高比例的“投票权”或“信道占用权”，进而操控消息认证、声誉评估、资源调度等关键流程，轻则造成大面积拥堵或信号灯失效，重则诱发连环碰撞。因此，研究车联网环境下的女巫攻击检测技术，对保障智慧交通的可靠性、隐私性与高效性具有重要学术价值与现实意义。然而，现有检测方法在动态、高速、资源受限的车联网场景中暴露出三方面缺陷：

（1）可靠性瓶颈：基于公钥基础设施（PKI）或证书撤销列表（CRL）的方案依赖中心化机构，难以在毫秒级时延内完成大批量证书验证；而单纯基于 RSSI、DOA 的物理层指纹，又容易因城市道路多径、高楼遮挡等复杂环境产生误判。

（2）隐私-可追责矛盾：为防止女巫身份伪造，系统往往需要收集车辆长期身份或轨迹信息，这与 GDPR、国标《个人信息保护法》提出的“最小够用、匿名化处理”原则相冲突；若直接采用群签名或环签名，则又可能因无法撤销匿名而难以追责。

（3）资源-效率失衡：现有基于机器学习或博弈论的检测模型，在训练阶段需要大量标注样本与集中算力，难以适配车载单元（OBU）的功耗、存储和计算限制；同时，频繁的上传下载又会加剧蜂窝链路负载，影响紧急安全消息的时效性。

因此，车联网和区块链技术存在着显著的优势互补，区块链技术带来的许多特性，恰恰是目前车联网领域所欠缺的。而如何利用区块链的特性和优点去解决车联网中数据共享的安全性问题变得至关重要，需要对传统区块链技术进行应用创新，使其能够真正为车联网环境服务。综上所述，在区块链架构下研究车联网数据传输可靠性和隐私保护问题具有较强的学术研究价值。

## 国内外研究现状

### 数据传输可靠性研究现状

随着车联网技术的迅猛发展，如何提高数据传输的可靠性成为研究者关注的重点。传统的集中式数据管理和传输方式在高速动态环境下表现出明显的不足，近年来，研究者们探索了基于区块链技术的多种创新方法，利用区块链的分布式、不可篡改和共识机制等特性，提供了一系列提高数据传输可靠性的新方案。文献[1]提出了一种基于区块链的车联网数据管理方案，利用区块链的分布式账本和不可篡改特性来防止数据丢失和伪造。研究中设计了一个轻量级共识机制，减少数据传输延迟并提高链路可靠性。通过在模拟交通环境中的实验，该方法证明能显著提高数据传输的效率和稳定性。文献[2]提出了一个智能合约框架，用于动态管理数据路由和网络负载分配。智能合约能够根据实时交通状况选择最优的传输路径，减少网络拥塞并提高可靠性。实验表明，该方法在高流量场景下表现出良好的延迟控制能力。文献[3]提出了基于区块链的车联网跨域数据传输方案，使用链间通信协议来保证不同网络之间的数据传输稳定性。研究展示了如何通过智能合约自动协调跨域数据同步，减少数据丢失和误传现象。文献[4]提出了一种采用区块链技术的车载设备自适应数据路由协议，利用分布式网络监控来实时调整路由策略，提升数据传输的稳定性。实验结果表明，该协议在拥堵网络环境中表现出了较强的鲁棒性。文献[5]提出了一种结合区块链和机器学习的自适应车联网数据传输方案，使用区块链保障数据的真实性，并通过机器学习算法优化数据传输路径。研究在实际数据集上验证了方法的有效性。文献[6]设计了一个区块链驱动的车联网数据冗余机制，通过多节点备份提高数据传输的可靠性，避免因网络故障导致的数据丢失。实验结果证明了该机制在高负载条件下的稳定性能。

PBFT共识算法因其高效性和安全性，被广泛应用于区块链技术驱动的车联网数据传输中。研究者们对PBFT算法进行了多方面的创新，旨在提高数据传输的可靠性和减少系统的通信延迟。文献[7]提出了一种优化的轻量级PBFT共识算法，通过减少冗余通信步骤和采用分层节点架构，提升了车联网环境下数据传输的效率和可靠性。实验结果显示，在高密度车流情况下，该改进算法能够显著降低网络延迟和数据丢失率。文献[8]提出了一种基于PBFT共识的混合链机制，将主链与侧链结合，侧链负责车联网中非关键数据的快速共识，而主链则负责记录关键数据，确保整体系统的高可靠性和数据完整性。文献[9]设计了一种PBFT改进方案，采用投票压缩技术减少通信轮数，并引入错误检测机制来提高数据传输的准确性和效率。模拟实验验证了该方案在高负载环境下的优越性。文献[10]研究利用一种分布式故障检测和容错机制对PBFT进行优化，提升了节点间数据传输的可靠性，并增强了系统对恶意节点攻击的抵御能力。实验结果表明，该方法能够在提高共识安全性的同时减少延迟。文献[11]开发了一种基于机器学习的PBFT优化模型，利用机器学习算法预测交通流量，动态调整共识参数，从而优化数据传输性能。实验验证了该模型在多变的车联网环境中的适应性。文献[12]介绍了一种基于边缘计算的PBFT共识改进方案，利用附近的边缘服务器分担部分共识任务，提高了数据传输的实时性和稳定性。实验表明，该方法在城市交通环境中表现出色。

尽管现有的研究在提高车联网中数据传输的可靠性方面取得了显著进展，但仍存在一些共性问题有待解决。面对车联网的高流动性和复杂动态环境难以在通信效率和安全性之间取得理想的平衡、对于恶意节点的识别和防御能力仍不完善等，未来的研究需要更加关注共识机制的高效优化，并加强系统对恶意行为的容忍与防御能力。

### 隐私保护研究现状

车联网隐私可以定义为个人和车辆对其信息的控制和处理能力，具体包括身份隐私、位置隐私和数据交换隐私。数据交换隐私通常可以通过加密通信手段来加以保护，而身份隐私则可通过使用假名技术实现有效防护。在本文中，重点讨论位置隐私保护问题。车辆位置隐私指的是车辆自主决定其位置信息是否能够被他人获取的能力，定义为特定实体与其位置关联的强弱程度，具体指车辆与其位置和行驶轨迹之间的关联性。车辆通常需要根据位置提供或共享服务，比如广播信标信息或发布紧急事件通知。然而，在车辆行驶过程中，其运动轨迹往往可以被预测。攻击者可能通过收集和分析车辆状态数据，并结合地图信息及交通规则等先验知识，对车辆进行跟踪，生成位置档案，从而泄露车辆的轨迹和位置信息。为了实现车联网的广泛接受与部署，必须重视并采取措施保护位置隐私。

在车联网的位置隐私保护领域，研究者们提出了多种方法，以应对用户位置数据泄露的问题。主要分为四类保护方法：虚假事件式、隐藏式、混淆式以及匿名式。在表1.1中对四种位置隐私保护方法进行了总结对比：

表1.1 位置隐私保护方法对比一览表

**Table 1.1 Location Privacy Protection Methods Comparison Table**



虚假事件式方法通过生成虚假的位置信息使得系统外部观察者无法准确识别用户的真实位置，从而保护用户隐私。不少研究使用虚假事件式方法保护车辆的位置隐私[13-15]。文献[14]中，车辆根据周围环境动态生成虚假位置。基于虚假事件的方法需要生成合理有效的虚假位置，现有的基于虚假位置的位置隐私保护方法，在长期追踪下，无法保障位置隐私不泄露[15]。同时，完全伪造的位置信息使得信标消息精度受到影响，无法为道路安全和交通效率服务，给车联网系统带来负面影响。

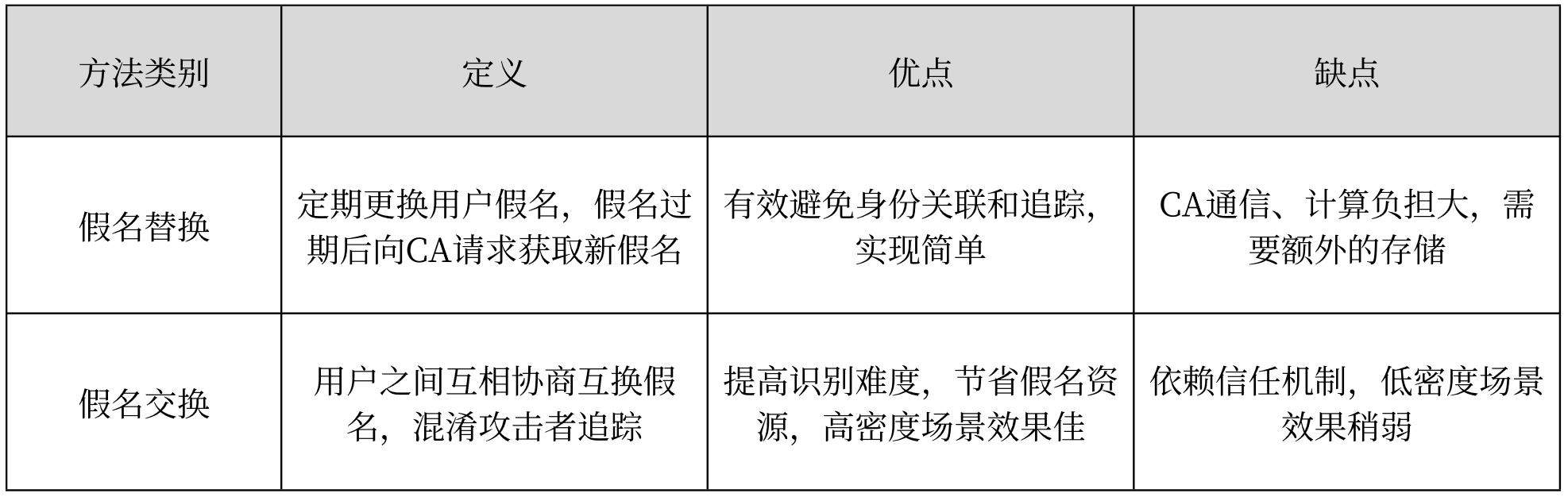
隐藏式方法则通过在一定时间内不暴露位置或使用加密手段来减少位置数据的可追踪性，这种方法可以有效降低被追踪的风险。文献[16]指出采用关闭信标消息广播的方式，在关闭时间比较短的情况下无法防止位置隐私的泄露;考虑到信标消息主要为道路安全和交通效率服务，大多数应用都基于信标消息工作[17]，关闭时间过长会降低信标消息精度，对车联网系统造成负面影响。

混淆式方法则是对真实位置进行一定程度的随机化或模糊处理，使得攻击者难以定位用户的确切位置，同时仍能在一定程度上维持服务的可用性。不少研究[18-19]使用混淆方式保护车辆的位置隐私。但文献[20]指出混淆位置时使用较小的偏移(<20m)无法抵御位置追踪攻击。考虑到信标消息主要为道路安全和交通效率服务，应当保持精确，混淆时使用较大的偏移会降低信标消息精度，对车联网系统造成负面影响。

匿名式方法通过消除或替换用户的身份信息，将用户身份与位置数据分离，确保位置数据的匿名性。即使位置数据被捕获，攻击者也无法将其与特定用户联系起来，从而增强隐私保护。不少研究使用假名更换进行位置隐私保护[21-30]，假名更换方法可以减少对信标消息的修改，降低对信标消息精度和车联网系统的负面影响，是车联网标准建议的方法[31]。但是使用假名更换，需要仔细设计，以防止遭受假名关联攻击。假名关联攻击指通过分析信标消息，对交换前后的假名映射关系进行推断，进而将车辆的位置关联起来，使假名更换失去保护作用。假名关联攻击分为语法攻击和语义攻击[25]。假名更换实现方法可以分为两种:假名替换和假名交换[31]，这两种方式的定义和特点如表1.2所示。

表1.2 xxxx

**Table 1.2 xxxxx**



假名替换是指，假名到期后，车辆都向证书颁发机构(CertificateAuthority,CA)请求新的假名，或者从自身假名池中选择新假名，并通知CA回收过期假名，通常采用混合区域方式实现。混合区域指攻击者无法监听、获知车辆信息的区域，通常架设在交通路口或停车场等区域，采用关闭无线通信或加密通信的方式实现。经过混合区域后，攻击者无法关联离开的车辆和进入的车辆，从而达到保护车辆位置隐私的目的。文献[22]提出在收费站等区域设置混合区域，路边单元(Roadside Unit, RSU)记录进入的车辆，为其选择合适的道路，车辆在区域内随机停留一段时间，离开时使用新的假名。文献[23-24]通过建群，在群内完成假名替换。文献[25]提出在车辆速度低时暂停信标消息广播，在速度达到阂值后，使用新假名恢复信标消息广播，完成假名更换。文献[26]考虑用户在请求基于位置的服务时造成的隐私泄露问题，提出每次向CA申请足够时间T使用的N个假名及证书，每次假名到期时，用户从本地假名池中选取一组新的假名、证书使用，假名池耗尽后向CA请求新的假名，通过使用不同的假名请求服务，使得位置服务器无法将多个请求关联到一起，从而保护车辆的位置隐私，请求基于位置的服务具有频率低、偶然、突发的特性，因此可以简单使用假名更换进行位置隐私保护。但是本文关注信标消息广播造成的位置隐私泄露问题，信标消息广播具有周期、精确的特性，只进行假名更换无法阻止假名关联攻击，无法有效保护车辆的位置隐私。基于假名替换的方案设计、实现更为简单。车联网标准建议车辆应当每两分钟完成一次假名更换[31]，车辆需要在本地存储大量假名或频繁向CA请求假名，给车辆本身的存储、计算资源，以及CA的计算、通信带来了挑战;同时，车辆一次性携带多个假名，自私车辆会利用这些假名，发起女巫攻击[32]。

考虑到假名替换方法的不足，有研究提出使用假名交换实现假名更换。假名交换指假名到期后，车辆与其他车辆达成约定，交换使用对方的假名。文献[33]提出在RSU的辅助下，车辆两两交换假名，实现隐私保护。文献[27]考虑到假名关联攻击，提出只有位置、速度相近的车辆才能进行假名交换。文献[28]提出充分利用每一次遇到的车辆，实现匿名度更大的假名交换。假名交换方式通过重用假名，减轻了车辆的存储负担，减少CA的计算负担，为了保护位置隐私，车辆会更积极参与假名交换，实现更好地隐私保护效果[29]。考虑到假名交换的优势，假名交换已经成为假名更换的主流实现方法，但假名交换方案需要更仔细的设计才能有效地抵御假名关联攻击[30]。

这四种位置隐私保护方法在使用时都存在一定的问题:隐藏方法、混淆方法与虚假事件方法都需要合理设计，且对信标消息进行处理，降低了信标消息精度，考虑到信标消息主要为道路安全和交通效率服务，这对车联网系统造成负面影响与其他三种位置隐私保护方法相比，使用假名更换的位置隐私保护方法对信标消息处理较少，对车联网系统负面影响小，不足之处也可通过方案的仔细设计加以

克服，是车联网标准建议使用的方法[31]。假名更换中，相较假名替换，假名交换可以实现假名重用，有效降低车辆的存储负担和CA的计算压力，可以促进车辆主动参与假名交换[29]。因此，论文将对基于假名交换的方案进行详细的讨论，并针对易于遭受假名关联攻击的问题提出解决方案。

## 论文主要研究内容

在本研究中，本文首先基于现有车联网环境中数据传输可靠性问题，提出一种改进的共识机制—基于信誉的R-PBFT共识机制。该研究工作主要围绕提升车联网环境中的数据传输一致性与可靠性展开，重点解决传统共识机制在车联网应用中存在的低时延需求难以满足、恶意节点防御不足等问题。R-PBFT通过引入信誉评分机制，根据节点的历史表现动态调整代理节点，确保参与共识的节点更具可信性。此外，设置信誉阈值将节点分为候选节点与普通节点，仅由候选节点参与共识，有效降低通信成本并提高系统效率。同时，通过随机方式选择代理节点，减少了恶意节点“刷分”影响共识的可能性，从而提升了系统安全性。最后，通过设计奖惩机制鼓励节点积极参与共识，对表现良好的节点予以信誉奖励，对消极或恶意节点扣分，从而提升系统的参与度与数据传输的可靠性。

针对车联网位置隐私保护问题，本文提出了一种基于动态超车的假名交换方法，通过模拟车辆超车行为来掩盖假名交换过程，实现位置隐私保护。主要研究内容包括三个阶段，分别是车辆注册、动态超车和追踪撤销。其中动态超车方案分为四个步骤，目标选择中，发起车辆基于预设的超车条件选择符合条件的目标车辆，通过路侧单元RSU获取目标车辆的公钥。其次进行意愿协商，发起车辆利用目标车辆的公钥建立联系，协商是否愿意进行假名交换，并确定交换的具体时间范围。然后进行报备请求，发起车辆和目标车辆将协商内容报备至证书管理机构CA，申请交换许可。最后执行交换，在CA批准后，双方进行正式的假名交换。该方法中，车辆通过预设的超车条件选择目标车辆进行假名交换，且车辆只在假名交换时广播虚假信标消息，以保护车辆的位置隐私，降低对信标消息精度和车联网系统的负面影响。

## 论文组织结构

论文总共分为五章，其整体结构和章节安排如下：

1. 绪论。阐述本文的研究背景和研究意义，分析当前车联网中数据传输可靠性和隐私保护的研究现状，概述本文所研究的主要内容，并给出本文的组织结构。

第二章，相关概念与理论基础。本章首先介绍了本文所用到的区块链技术，其次介绍了车联网的基础知识。区块链技术的介绍主要涉及区块链的概念、共识机制、使用的密码学知识和相关应用场景。车联网的基础知识主要包括车联网的组成、车联网位置隐私的攻击方法分析等。

第三章，基于信誉的R-PBFT共识机制。针对车联网环境中数据传输可靠性问题，分析了PBFT共识算法的工作机制及存在的不足，在此基础上提出基于信誉的R-PBFT共识机制。从算法思想、算法设计及共识流程等方面详细介绍了该机制的具体方案。通过设计信誉机制、节点分类、奖惩机制合理的筛选可靠节点参与共识，降低恶意节点成为代理节点的概率。通过与PBFT共识机制进行对比，验证了R-PBFT算法兼顾了时延和可靠性的优化，不仅在高密度和高恶意节点比例的环境下表现出较好的扩展性，而且在共识过程中提高了数据传输可靠性。

第四章，基于动态超车的假名交换方法。首先，对假名更新过程中存在的问题进行了分析，介绍了本文研究采用的攻击者模型和相关前提假设。其次，分为三个阶段详细介绍了基于动态超车的假名交换方法。通过预设的动态超车条件选择目标车辆进行假名交换，详细介绍了发起车辆与目标车辆通信的具体流程。只在假名交换时广播虚假信标消息，模拟车辆超车行为来掩盖假名交换过程，以保护车辆的位置隐私。最后，通过仿真实验与现有车辆位置隐私保护方法进行性能比较，验证了该方案的有效性。

第五章，总结与展望。对本文的研究工作进行了总结，指出了本文研究工作

中的不足,并对下一步工作进行了展望。

# 相关理论与技术

本章分为三部分。首先介绍了区块链相关概念，加密算法及共识机制等技术。其次介绍了车联网的模型与架构，针对车联网位置隐私的攻击方法进行了分析。最后，介绍了区块链和车联网相结合的相关技术。

## 车联网技术概述

车联网（Internet of Vehicles, IoV）是物联网技术在智能交通系统中的核心应用，它通过新一代信息通信技术，构建了“人-车-路-云”多层次、多维度的信息交互体系。车联网不仅实现了车辆与万物（V2X）的互联互通，更是实现智能网联汽车和高级别自动驾驶的关键使能技术。其核心在于通过海量数据的实时采集、传输与处理，实现车辆对环境的高度感知、智能决策与协同控制，最终达到提升道路交通安全、效率和用户体验的根本目标。

### 车联网体系架构

车联网是一个复杂的系统，其体系架构通常可划分为三个逻辑层次：感知层、网络层和应用层。三层协同工作，共同支撑车联网各项功能的实现。其系统架构如图2-1所示。

222

图2.1 车联网网络体系结构

**Figure.2.1 Internet of Vehicles (IoV) Network Architecture**

感知层：作为系统的神经末梢，主要负责车辆自身状态、周边环境及交通信息的采集。其通过车载传感器（如摄像头、激光雷达、毫米波雷达、惯性导航单元）、车载终端（OBU）、路侧设备（RSU、监控摄像头、气象传感器）以及全球导航卫星系统（GNSS）等，实时获取车辆位置、速度、加速度、道路状况、障碍物信息、交通信号等海量数据。

网络层：作为系统的神经中枢，负责实现感知层数据的高速、可靠、低延时传输与交换。它综合利用多种通信技术，主要包括：（1）专用短程通信（DSRC/IEEE 802.11p）：基于Wi-Fi改进的技术，适用于短距离、低延迟的V2V和V2I通信。（2）蜂窝车联网（C-V2X）：基于蜂窝网络的技术，包括LTE-V2X和更先进的5G-V2X。C-V2X支持两种通信模式：直接通信（PC5接口）用于车、路、人之间的短距离直联；网络通信（Uu接口）通过蜂窝基站实现广域云连接。其技术对比如表2-1所示。

**表2-1 主要车联网通信技术对比**

|  |  |  |
| --- | --- | --- |
| **特性** | **DSRC (IEEE 802.11p)** | **C-V2X (LTE-V2X/5G-V2X)** |
| **标准体系** | IEEE | 3GPP |
| **工作频段** | 5.9 GHz | 5.9 GHz (PC5) |
| **通信模式** | 仅直连通信（V2V, V2I） | 直连通信（PC5）+ 蜂窝网络通信（Uu） |
| **覆盖范围** | 短距离（通常<1km） | 短距离（PC5） + 广域覆盖（Uu） |
| **峰值速率** | 较低（~27 Mbps） | 高（5G-V2X可达Gbps级） |
| **移动性支持** | 高 | 更高（专为高速移动优化） |
| **演进路径** | 受限 | 清晰（随蜂窝网络同步演进） |
| **主要优势** | 技术成熟，部署早 | 覆盖广、容量大、支持未来应用 |

此外，网络层还融合了移动通信网络（4G/5G）、以太网等技术，构成一个异构融合的网络体系。

应用层：是车联网价值的最终体现，它通过对网络层传输来的数据进行处理、分析和挖掘，为用户提供丰富的智能化应用。这些应用可归纳为三大类：（1）交通安全类：如前向碰撞预警（FCW）、交叉路口碰撞预警（ICW）、紧急电子刹车灯预警（EEBL）等，旨在显著减少交通事故。（2）交通效率类：如实时路径规划、车速引导（GLOSA）、交通信号协同、拥堵预警等，旨在优化交通流，缓解拥堵。（3）信息服务类：如高精度地图更新、停车场导航、车载信息娱乐、远程诊断等，旨在提升驾乘体验和便利性。

### 基本安全消息

基本安全消息（BSM）是车联网通信体系中的核心数据包，由美国汽车工程师学会（SAE）在J2735标准中定义[[引用SAE J2735标准]]。它充当车辆的“电子身份证”和“环境感知器”，通过专用短程通信（DSRC）或蜂窝车联网（C-V2X）技术，以高频、广播的形式在车辆与车辆（V2V）、车辆与基础设施（V2I）之间进行交换。BSM的核心作用在于实现车辆间的协同感知，通过共享自身的关键状态信息，为驾驶员或自动驾驶系统提供一个超越车载传感器物理限制的“上帝视角”。这是实现前向碰撞预警、交叉路口碰撞预警、紧急制动预警等主动安全应用的基础。

根据SAE J2735标准，BSM消息通常由两个部分构成：

BSM Part I（核心数据部分）：包含车辆的关键安全状态信息，这些信息更新频率高、时效性要求极强，是所有安全应用的基础。该部分通常不允许匿名化，以确保信息的可追溯性与责任感。其主要数据元素如表2.X-1所示。

表2.1 BSM

**Table 2.1 xxx**

|  |  |
| --- | --- |
| **符号** | **描述** |
|  |  |
|  |  |
|  |  |
|  |  |

### 车联网面临的技术挑战

尽管车联网前景广阔，但其大规模应用仍面临一系列严峻的技术挑战，这些挑战直接关系到本文所研究的安全问题的必要性：

（1）通信可靠性挑战：车辆的高速移动导致网络拓扑结构剧烈变化，通信链路频繁切换甚至中断。恶劣天气、城市峡谷效应等环境因素也会影响通信质量，要求通信技术必须具备高可靠性和低延时（通常要求端到端延迟小于100ms）的特性。

（2）海量数据处理的实时性挑战：网联车辆每秒产生海量数据（可达TB级），对这些数据进行实时处理、融合和决策对计算架构提出了极高要求。集中式的云计算难以满足所有业务的低延时需求，因此需要引入边缘计算（MEC） 技术，将计算任务下沉到网络边缘（如RSU、区域服务器），就近处理数据，大幅降低响应时间。

（3）安全与隐私挑战：这是本文研究的核心出发点。 车联网的开放通信环境、V2X消息的广播特性以及其与车辆控制系统的紧密关联，使其面临严重的安全威胁，如消息伪造、篡改、重放攻击、拒绝服务攻击（DoS）以及女巫攻击（Sybil Attack） 等。攻击者可通过这些手段传播虚假信息，扰乱交通秩序，甚至造成重大安全事故。隐私泄露风险：车辆广播的消息（如位置、速度、身份标识）如未经保护，可被轻易跟踪，泄露用户的行踪轨迹、驾驶习惯等敏感隐私信息。

综上所述，车联网技术通过构建一个全方位的智能交通生态系统，为未来出行带来了革命性的变化。然而，其固有的技术挑战，尤其是在安全与隐私领域面临的严峻威胁，成为了制约其发展的关键瓶颈。因此，研究有效的安全防护机制，特别是针对女巫攻击这类典型且危害巨大的攻击手段的检测技术，对于保障车联网的健康发展具有至关重要的意义，也为本文的研究提供了明确的现实需求和理论价值。

## 女巫攻击

女巫攻击是分布式网络环境中一种经典且破坏性极强的安全威胁。在IoV背景下，其危害被进一步放大，直接威胁到道路交通安全、用户隐私乃至整个智能交通系统的可信度。本节将深入剖析女巫攻击的基本概念、在车联网中的具体表现形式、其带来的严重后果以及当前主流的防御思路，为本文后续的检测技术研究奠定问题基础。

### 女巫攻击的基本原理

女巫攻击的概念由John R. Douceur于2002年在论文《The Sybil Attack》中首次明确提出。它得名于Flora Rheta Schreiber的著作《Sybil》，该书讲述了一位具有多重人格障碍的女性。在网络安全领域，女巫攻击是指一个恶意节点（称为Sybil节点）通过伪造或冒用大量虚假身份标识（ID），伪装成多个不同的合法节点渗透到网络中，从而破坏分布式系统的公平性、冗余性和安全机制的攻击方式。其攻击本质在于，分布式系统通常依赖于“多数原则”进行决策（如投票、共识、信任评估），攻击者通过控制足够数量的虚假身份，可以使其在系统中占据不对称的优势地位，进而操纵或影响系统的正常运行。一个简单的女巫攻击模型如下图所示。

### 车联网中女巫攻击的具体形式与危害

车联网的开放无线通信环境、车辆的移动性以及安全消息的广播特性，为女巫攻击的实施提供了便利。攻击者可通过盗取、破解或伪造合法证书等方式，获取大量虚假身份。其在车联网中的主要攻击形式与危害体现在以下几个方面：

（1）伪造虚假交通事件：恶意车辆可操控多个Sybil身份，协同广播虚假的道路危险信息（如前方不存在的交通事故、拥堵或障碍物），诱使周围车辆紧急刹车或改变路线，从而引发交通混乱甚至连环相撞事故。

（2）破坏信任与信誉机制：许多车联网安全方案依赖于节点间的相互评价来建立信誉模型。攻击者利用Sybil身份为自己刷“好评”或对诚实车辆进行“诋毁”，轻易颠覆信誉系统的公正性，使恶意节点长期潜伏或使诚实节点被错误隔离。

（3）干扰协同感知与决策：在高级别自动驾驶场景中，车辆需共享感知数据以构建全局环境模型。Sybil节点可以注入错误的感知信息（如伪造的车辆位置、速度），污染协同感知结果，导致车辆做出致命的错误决策。

（4）实现位置跟踪与隐私窃取：尽管女巫攻击本身是主动攻击，但它也可被用作隐私窃取的辅助手段。攻击者可以部署多个协同的Sybil节点，从不同位置对目标车辆进行持续观察和交叉验证，从而实现对目标车辆行驶轨迹的高精度跟踪，严重侵犯用户位置隐私。

### 车联网女巫攻击防御的核心挑战

防御车联网中的女巫攻击面临着诸多独特且严峻的挑战，这使得传统的安全机制难以直接生效：

（1）资源约束与实时性要求：车辆的计算、存储资源有限，而安全消息（如BSM）的广播频率极高（每秒10次）。任何检测算法必须在毫秒级内完成计算，否则将失去预警意义。复杂的密码学方案或多轮通信验证难以满足此实时性要求。

（2）网络动态拓扑：车辆的高速移动导致网络拓扑结构瞬息万变，节点间的连接是短暂而不稳定的。这使得需要长期观察或稳定邻居关系的检测方法效果大打折扣。

（3）隐私保护与身份管理的平衡：单纯的强身份认证需要中央权威机构（CA）的全程参与，会引入单点故障和通信瓶颈，并与车辆的位置隐私保护需求相冲突。如何在实现身份可信的同时保护用户匿名性是一个两难问题。

（4）攻击的协同性与隐蔽性：高级的Sybil攻击中，恶意节点会精心协调其虚假身份的行为模式（如模拟真实的车辆跟驰模型），使其表现得与合法车辆无异，从而规避那些基于简单行为异常的策略检测。

现有的防御策略大致可分为三类：

（1）基于身份认证的方案：依靠可信中心（如PKI）为每个车辆签发唯一、可验证的身份证书。这是防御的基础，但无法解决证书被盗用或伪造的问题，且完全中心化的管理在车联网中可扩展性较差。

（2）基于信誉模型的方案：通过邻居节点对车辆行为进行长期评价和加权，赋予车辆信誉值。Sybil节点因其异常行为通常会积累低信誉。但该方案启动慢（需要观察期），且易遭Sybil群体诋毁攻击。

（3）基于行为特征分析的方案：这是当前研究的热点。其核心假设是：Sybil节点由于受同一物理实体控制，其行为在物理世界约束下会表现出某种不自然的一致性或不可能性。例如：无线电指纹技术，识别每个无线设备硬件的唯一性；时空一致性检验，验证声称在不同位置的多个身份是否可能由一个物理实体生成，如两个距离很远的Sybil身份却在短时间内连续发出信号；机器学习检测，利用深度学习模型自动从车辆通信数据（信号强度、消息间隔、地理位置报告等）中挖掘Sybil行为的深层模式。

|  |  |  |  |
| --- | --- | --- | --- |
| **防御思路** | **核心原理** | **优点** | **缺点** |
| **基于身份认证** | 依靠可信中心签发和验证数字证书 | 概念清晰，防御直接 | 中心化瓶颈、隐私泄露风险、无法防证书盗用 |
| **基于信誉模型** | 通过邻居评价评估节点可信度 | 适应分布式环境，能应对未知攻击 | 启动慢、易遭诋毁攻击、需长期观察 |
| **基于行为特征分析** | 利用物理层特征或行为数据的一致性进行检测 | 无需中心授权、能发现未知攻击、保护隐私 | 可能产生误报、依赖特征提取质量、需应对自适应攻击 |

综上所述，女巫攻击是车联网面临的最严峻安全威胁之一，其防御是一个复杂且具有挑战性的问题。单一防御策略往往存在缺陷，因此，融合多种思路（如基于资源测试的轻量认证+基于机器学习的实时行为分析）的混合检测框架，正成为最有前景的研究方向。本文后续工作将基于行为特征分析，重点探索利用深度学习模型从高维、时序的车联网数据中检测Sybil攻击的有效方法。

## 联邦学习

随着大数据和人工智能技术的快速发展，数据的存储和处理能力已经逐步向分布式方向发展。在许多应用场景中，数据的产生往往是分布式的，尤其是在车联网环境下，数据分布在大量的智能车辆、路侧设备和其他终端设备中。这些设备生成了海量的实时数据，但由于数据隐私、通信带宽和计算能力等多方面的限制，将所有数据集中到中央服务器进行处理成为了一个巨大的挑战。

联邦学习（Federated Learning，FL）应运而生，作为一种分布式机器学习的技术，它解决了数据集中存储和计算的难题。联邦学习的核心思想是将数据保留在本地设备上，在本地进行模型训练，只将模型参数或梯度上传至中央服务器，服务器通过聚合本地模型更新来得到全局模型，然后将该模型分发给各个参与者。通过这种方式，数据始终不离开本地，减少了数据传输和隐私泄露的风险。

联邦学习最初由Google于2016年提出，作为一种在移动设备上进行分布式学习的方案，特别是在智能手机领域，用户生成的数据无法直接上传到云端，出于隐私保护的考虑，Google设计了联邦学习框架，允许多个手机设备共同参与训练模型，而无需交换原始数据。这一技术也迅速引起了学术界和工业界的广泛关注，并被应用到许多领域，包括医疗、金融、智能交通等。

车联网中的数据通常分布在大量的智能设备中，包括车辆、路侧设备、交通摄像头等，数据的处理与分析亟需依靠智能算法。然而，由于这些设备的计算能力和带宽受限，传统的将数据集中上传到中央服务器的做法并不适用于车联网环境。联邦学习正是为解决这一问题而提出的，通过将计算推向本地，利用分布式的计算资源进行高效训练。

联邦学习不仅可以减少车联网系统中数据传输的压力，还能有效提高数据隐私的保护。在女巫攻击检测领域，联邦学习尤其具有重要意义。通过在分布式的车辆和设备之间进行协同学习，能够更加精准地检测到潜在的攻击行为，同时在保障用户隐私的前提下提升检测模型的准确性。

联邦学习的工作流程通常包括四个主要步骤，如图xx所示：

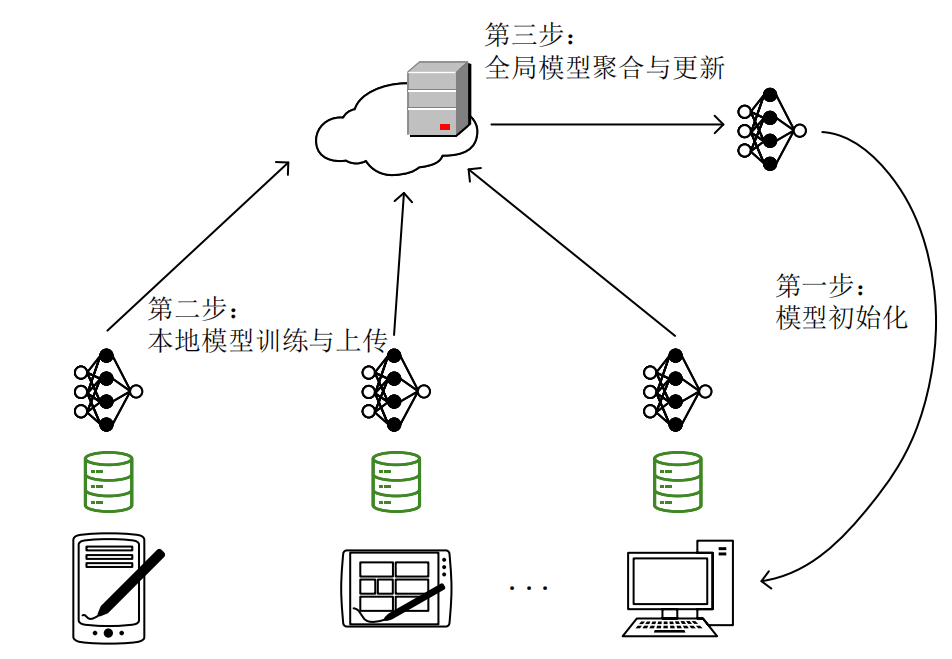


图2.1 联邦学习工作流程（重画一个这种图）

**Figure.2.1 Internet of Vehicles (IoV) Network Architecture**

（1）模型初始化：在中央服务器上初始化全局模型，并将其分发给各参与方。

（2）本地模型训练与上传：各参与方使用本地数据训练模型，并将更新后的模型参数上传至中央服务器。

（3）全局模型聚合与更新：中央服务器聚合各参与方上传的模型参数，更新全局模型。

（4）全局模型分发：更新后的全局模型再次分发给各参与方，进入下一轮训练。

这种协同训练的过程能够在保证数据隐私的同时，通过多方合作提升模型的性能。通过这一流程，联邦学习在车联网环境中为女巫攻击检测等智能系统的构建提供了技术支持，可以有效提高模型的泛化能力和攻击检测精度，同时保障数据隐私，推动车联网系统向更智能、更安全的方向发展。

## CNN与LSTM

车联网环境下的女巫攻击检测核心在于如何从高维、动态的车辆行为数据中准确识别恶意节点伪造多重身份的行为模式。卷积神经网络（Convolutional Neural Network, CNN）与长短期记忆网络（Long Short-Term Memory, LSTM）分别具有空间特征提取和时序依赖建模的天然优势，二者的深度融合为车联网女巫攻击检测提供了新的理论框架和技术路径。本节对论文后续所采用的CNN与LSTM的数学原理、网络结构及协同机制进行系统阐述，为车联网女巫攻击检测模型的设计与参数选择奠定理论基础。

### CNN

CNN通过其特有的局部连接、权重共享和空间下采样机制，能够有效捕捉车辆行为特征中的局部相关性和空间结构模式，为女巫攻击检测提供空间维度上的特征表示能力。

（1）卷积运算与特征映射：在车联网行为分析中，将车辆通信数据（如信号强度、消息发送频率、地理位置变化等）构建为二维特征矩阵，其中行为维度构成特征空间，时间维度提供采样序列。卷积核在特征矩阵上的滑动运算可表示为：

其中，为卷积核参数，为上一层特征映射输出，为激活函数。该运算能够自动学习行为特征之间的局部关联模式，如识别异常的消息发送频率与信号强度组合。

（2）池化操作与特征降维：最大池化操作通过下采样过程保留显著特征，增强模型对特征位置变化的鲁棒性：

其中，为池化步长。这种降维机制特别适合处理车联网中高维度的行为特征数据，在保持特征判别性的同时降低计算复杂度。

（3）空间特征提取机制：CNN的多层卷积结构通过层次化特征变换，能够从原始行为数据中逐步提取出更具判别性的特征表示。低层卷积捕捉局部特征组合（如消息突发性与位置跳变），高层卷积整合这些局部模式形成全局特征表示（如协同攻击行为模式），为后续时序分析提供高质量的特征输入。

### LSTM

长短期记忆网络则通过其门控机制解决长期依赖问题，能够有效捕捉车辆行为的时间动态特性，为识别女巫攻击的时序模式提供理论基础。LSTM通过遗忘门、输入门和输出门三个门控单元精细调控信息流动。遗忘门决定历史信息的保留程度（），输入门控制新信息的写入（），输出门调节状态的输出（）。细胞状态构成LSTM的记忆主线，其更新过程为：

输出状态计算为：

这种机制使LSTM能够记忆车辆行为的长期模式，特别适合识别女巫攻击中的身份切换规律和协同攻击信号。

LSTM通过其状态传递机制建立长时间跨度上的行为依赖关系，能够识别出女巫攻击中典型的时序特征：短期模式（突发性消息轰炸攻击）；长期模式（缓慢渗透的协同攻击）；周期模式（定期更换身份的行为规律）。

CNN与LSTM的融合创造了空间-时序联合建模的理论框架。CNN作为前端网络从原始行为数据中提取具有判别性的空间特征，将高维数据降维为紧凑的特征表示；LSTM作为后端网络对特征序列进行时间维度建模，捕捉行为模式的动态演化规律。这种端到端的攻击检测架构可表示为：特征序列，时序状态，最终攻击检测，其中，为输入行为数据矩阵，为攻击概率输出。

综上所述，CNN-LSTM混合模型通过空间特征提取与时间依赖建模的有机结合，能够有效应对车联网女巫攻击检测中的关键挑战，为构建高效准确的检测系统提供了新的思路和方法。

## 本章小结

本章主要介绍了本论文所涉及的关键技术。首先对区块链的组成和相关技术

进行了分别介绍，接着简要介绍了车联网的概念及区块链与车联网结合的相关技术。区块链技术的介绍主要涉及区块链的概念、使用的密码学知识、共识机制和相关应用场景。车联网的基础知识主要包括车联网的组成与架构，分析了车联网中的攻击方法。这些都为本文设计的开展提供了理论支持。

# 基于邻居信誉与BSM行为分析的女巫攻击检测方案

在车联网环境中，由于车辆节点的高度动态性和开放性，系统容易受到女巫攻击（Sybil Attack）的威胁。现有的检测方法存在检测手段单一、精度不高等问题。为此，本章描述了一种融合邻居信誉评估与BSM行为列表分析的女巫攻击检测方案。该方案通过动态评估节点的信誉等级，并结合其广播BSM消息的行为模式，精准识别伪造身份的恶意车辆，从而有效提高女巫攻击的检测精度与网络安全性。

## 系统模型

本方案所构建的系统模型如图3.1所示，主要由三类实体组成：可信机构、路侧单元和车辆，三者协同工作，共同实现对女巫攻击的检测与防御。各实体功能描述如下：

可信机构（Trusted Authority，TA）：作为车联网安全体系的信任锚点，承担系统级全生命周期管理职能。TA 在初始化阶段完成网络参数与根密钥的生成，并负责车辆实体的身份注册、假名证书（Pseudo-identity Certificate）的批量签发与动态分发；同时，通过更新证书吊销列表（CRL）实现细粒度密钥撤销与身份失效。运行期间，TA 与各路侧单元协同维护全局信任数据库，对区域上报的可疑行为进行跨域关联分析与最终裁决，确保全局身份与信誉状态的一致性与不可篡改性。

路侧单元（Roadside Unit，RSU）：作为布设于道路基础设施中的固定通信节点，是区域级信任管理的核心锚点。其以实时方式汇聚所辖范围内所有车辆提交的邻居信誉报告与BSM消息序列，并基于时空一致性校验与统计异常检测算法，对潜在恶意行为进行首轮筛查与本地信誉更新。随后，RSU 将检测结果及关联证据经安全信道签名上递至TA，为全局信任评估与跨域协同分析提供高置信度的数据支撑。

车辆（Vehicle，V）：作为车联网中数量最众、动态性最高的移动实体，均搭载车载单元（On-Board Unit, OBU）。在系统层面，车辆须以规定周期广播包含自身运动状态的真实基本安全消息，并同时扮演验证者角色：持续接收并校验邻居车辆所广播消息的合法性与合理性。借助对邻居消息的长期观测，每辆车在本地独立运行轻量级信誉评估模块，对通信半径内的邻居进行实时行为评分，为分布式异常检测提供底层数据支撑。最终，车辆将经私钥签名的本地评估结果上报至所属RSU，为后续的全局信誉融合与决策提供可信、可溯源的数据来源。

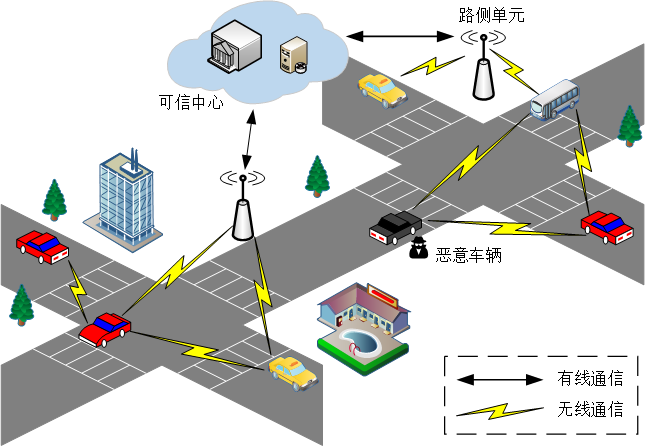


图3.1 系统模型

**Fig. 3.1 System Model**

该系统模型为后续的女巫攻击检测方案提供了基础架构支撑，确保能够在分布式、低延迟的车联网环境中高效运行。为方便后续描述，本文涉及的符号及定义列举在表XX中。

表3.1 符合与描述

**Table 3.1 xxx**

|  |  |
| --- | --- |
| **符号** | **描述** |
| TA | 可信机构 |
| RSU | 路侧单元 |
|  | 第 辆车 |
|  | 车辆的假名标识 |
|  | 车辆在时刻发送的基本安全消息 |
|  | 车辆对车辆的综合信誉评分 |
|  | 车辆的历史信誉评分 |
|  | 车辆的当前行为评分 |
|  | 信誉更新的动态平滑因子 |

## 女巫攻击模型

本章假设攻击者旨在通过操控一个或多个虚假身份，实现传播虚假交通信息、破坏共识机制或追踪特定车辆等恶意目标。对其能力做出如下假设：

1. 身份伪造能力受限：由于系统采用TA进行强身份认证，攻击者无法凭空伪造合法的密码学身份。其控制的虚假身份主要来源于窃取的合法车辆凭证、冒用的他人身份或利用证书吊销机制的延迟。
2. 多通道通信能力：攻击者可能配备多个OBU或无线网卡，使其能同时模拟多个位于不同位置的虚假节点。
3. 协同攻击能力：攻击者控制的多个Sybil节点之间可以相互协作，例如相互提供虚假的正面信誉评价，以增强其在网络中的可信度。
4. 计算与存储资源较强：攻击者具备足够的计算能力来模拟基本的车辆行为，但其资源并非无限，且其攻击行为需要遵循一定的物理约束。

## 系统初始化

系统初始化是构建安全通信的基础，主要包括TA与RSU的部署以及车辆的身份注册。详细描述如下：

TA 作为根信任实体，需生成用于整个系统的加密与签名过程的全局公共参数。具体地，首先，TA选择一个定义在有限域上满足的椭圆曲线。然后，选择一个阶为大素数的基点和一个哈希函数。

之后，随机选择一个私钥，并计算公钥。最后，通过离线方式将这些公共参数 和公钥安全分发至所有 RSU 与车辆实体。

RSU作为路侧单元，本章假设其完全可信，与TA共享密钥对并参与后续系统交互。

车辆在接入车联网前，须通过安全信道完成下述注册流程：

（1）属性信息映射：每辆车（记作）具有属性信息（如车牌号、用户身份、计算资源等），通过单向哈希函数进行映射，生成唯一的哈希身份

该过程保护了车辆的敏感属性信息。

（2）公私钥生成：车辆选择一个私钥，并基于椭圆曲线参数计算对应的公钥，其中，为公共生成点。

（3）发送注册信息：车辆通过安全信道，将和发送至TA。

（4）TA为车辆生成伪身份：TA使用以下公式为车辆生成唯一伪身份

其中， 是TA的私钥与车辆公钥生成的共享密钥，确保伪身份仅由 TA 生成， 是伪身份的有效期。随后，TA返回注册信息给车辆，并将保存在防篡改设备中，用于后续查询和管理，确保车辆真实身份的隐私性和安全性。

## 检测方案描述

为有效识别车联网中伪造身份的恶意节点，本文提出一种融合邻居信誉评估与BSM消息行为分析的女巫攻击检测方案。该方案结合车辆之间的交互历史与消息特征，构建多层级的检测机制，能够在不依赖额外硬件的前提下，实现对女巫攻击的高精度识别。所提检测方案的整体流程如图3.2所示，具体描述如下：

1. 车辆定时广播 BSM 消息

车辆定时广播（时间间隔通常设为 100ms）发送基本安全消息（Basic Safety Message, BSM），可表示为

其中，为车辆的假名，为车辆当前位置的坐标，为车辆的当前速度，为车辆的行驶方向，为时间戳，表示消息生成的时间，为消息序列号，用于防止重放攻击，为车辆的公钥，用于验证消息签名，为消息的数字签名，使用车辆私钥对消息签名

其中，表示字段的拼接操作。

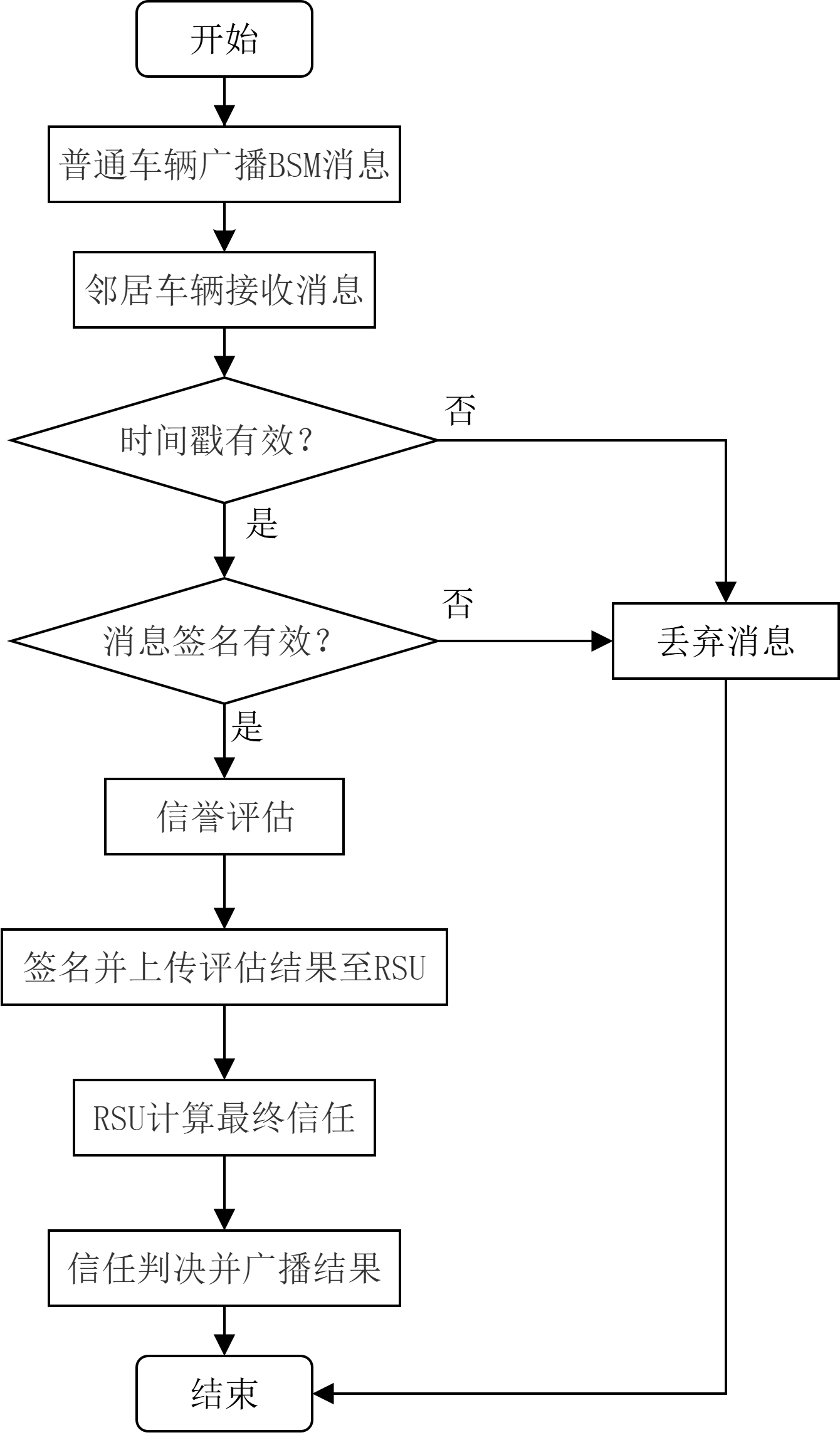


图3.2检测方案整体流程图

**Fig.3.2 Overall Flowchart of the Detection Scheme**

1. 邻居车辆接收与处理

当邻居车辆接收到广播范围内的消息后，需首先对其有效性进行检验，主要包括以下两个方面：

时间戳校验：检查消息的时间戳是否在允许的有效时间窗口内。每条消息的有效时长为，即消息在时间段[*t, t +*]内被视为有效。若当前时间，则该消息被认为已过期，应被直接丢弃。其判断逻辑如下所示：

数字签名验证：若时间戳验证通过，则车辆使用发送方的公钥对消息中的签名进行验证，以确保消息的完整性与来源的真实性。若签名验证失败，消息同样被丢弃。

1. 邻居车辆信誉评估

邻居车辆对消息发送车辆的信誉进行评估，结合历史、行为、和通信质量。具体步骤如下：

历史信誉评分（）反映了消息发送车辆在邻居车辆过去交互中的整体表现。每次接收到来自的消息后，会根据当前交互更新其历史信誉评分。该方案引入动态非对称平滑因子，使系统对作恶行为和正常行为的响应具有差异性。

其中，为车辆的先前历史信誉评分，为本次交互的得分（由行为评分决定）， 为平滑因子（0 < < 1），用于平衡历史和新交互的影响，根据车辆近期行为动态调整。，其中1表示历史信誉最好，0表示最差。动态的更新策略如下：

作恶行为（）时，

其中， 为惩罚初始值，为惩罚增强系数，为连续作恶次数，为允许的最小值。连续作恶的车辆其 α 会快速减小，使历史评分迅速下降，体现系统的惩罚性。

正常行为（）时，

其中，为奖励初始值，为奖励递减系数，为连续正常行为次数，为允许的最大值。正常行为开始时 α 较大（历史权重高，回升慢），只有在持续多次正常行为后，α才逐渐减小，使评分缓慢回升，避免“一次做好事就洗白”。

对作恶行为反应迅速，惩罚加重；对正常行为反应保守，奖励逐步增加。这种机制有效防止恶意车辆通过偶发正常行为“洗白”信誉，提高了车辆信任模型的鲁棒性和现实适应性。

行为评分（）用于评估发送车辆的行为是否异常，重点关注消息发送频率、数据合理性和基于RSSI的位置合理性。判断发送车辆的广播频率是否过高（如超过规定的每秒广播次数上限）。公式如下：

其中，为惩罚系数，用于控制评分下降速度。

数据合理性检查主要检查发送车辆提供的数据（如速度、方向等）是否合理。具体包括对比数据与邻居车辆的感知结果（如车速是否接近邻居车辆的观察值）。评分公式如下：

1. 基于RSSI的三边定位

RSSI可以通过信号传播模型推导出车辆的相对距离。结合邻居车辆的已知位置，RSSI可以用于估算发送车辆的实际位置。以下是具体步骤：

邻居车辆根据接收到的RSSI值，利用信号传播模型计算与发送车辆的距离。常用的模型是自由空间路径损耗模型：

其中，表示估算的距离，表示发送车辆的信号发射功率（dBm），表示接收信号强度（dBm），为路径损耗因子，取决于信号传播环境（如空旷区域通常取，城市环境取。

发送车辆在广播消息中会包含其声明的位置信息，邻居车辆自身的已知位置为。邻居车辆计算自身实际与发送车辆的声明距离：

之后，邻居车辆通过对比RSSI估算的距离和声明距离 ，计算两者之间的差值

设定一个合理阈值，若，则判断广播位置合理，若，则判断广播位置不合理，可能存在欺骗或异常行为。

阈值除了可以设置为固定值（如5米），还可以根据信号传播环境动态调整。在静态或低速场景中，误差阈值较小（如米）。在高速或复杂环境中，考虑到定位误差和信号干扰，误差阈值适当放宽（如米）。此外，RSSI本身不稳定，可结合多次测量的加权平均值来降低误差：

其中，为测量次数，为第次测量的估算距离。

定义位置合理性评分，根据误差计算如下：

当误差时，评分为满分 1。当误差时，评分根据误差的大小呈指数下降。为惩罚系数，控制评分下降的速度，通常根据实际应用场景调整。

综上，行为评分可表示为

其中，为各评分模块的权重，满足。在位置验证重要的场景中，可以适当提高的权重。

邻居车辆对目标车辆的综合信誉评分为

最后，邻居车辆将这个评分上传至RSU，上传消息格式为

其中，为消息生成的时间戳，为邻居车辆对消息的数字签名，用于保证消息的完整性和真实性，避免被篡改。

1. RSU 聚合与评估

RSU收集邻居车辆的评估结果，结合自身数据重新计算目标车辆的信任值。RSU将最终评估结果广播给其他车辆，用于指导通信和交互行为。

1. RSU 处理与最终评估

RSU 收集在动态时间阈值（可根据交通密度动态调整，确保 RSU 收集足够多的邻居车辆评估信息）内所有上传的评估消息。聚合数据包括：多邻居车辆的信任评估结果、RSU 自身的检测结果（如通过摄像头、雷达等设备检测发送车辆的实际位置、速度等）。

综合评估信任值：RSU 根据邻居车辆的评估结果和自身检测数据重新计算发送车辆的信任值。综合信任值计算公式：

其中，表示邻居车辆的加权平均信任值，表示参与评估的邻居车辆数量，表示 RSU 自身的检测评分。

消息准确性验证：RSU 将发送车辆的 BSM 数据与实际检测数据进行对比，验证其准确性：

比较位置、速度等参数是否一致。

如果误差超过设定阈值，标记为异常消息。

反馈结果广播：RSU 将最终评估结果广播给其他车辆，告知目标车辆的信任状态：

正常车辆：允许继续参与通信。

低可信车辆：限制其通信权限或标记为可疑车辆。

|  |  |  |
| --- | --- | --- |
| 目标车辆ID | 最终信任值 | 状态标记（正常/异常） |

广播消息格式：

恶意车辆检测与隔离：如果某车辆的信任值持续低于设定阈值，标记为恶意车辆，加入黑名单。广播黑名单信息，提醒其他车辆避免与其通信。

数据完整性保障：使用区块链技术存储评估结果，防止数据被篡改。

## 仿真实验及结果分析

### 实验环境与实验设计

本实验搭建基于Veins的Sybil攻击车联网仿真平台需要集成多个关键组件，包括OMNeT++、Veins和SUMO。首先，根据操作系统和仿真需求选择兼容的版本，安装OMNeT++作为网络仿真的核心框架，然后安装Veins框架，该框架实现了车联网通信协议，并支持与SUMO的联动，SUMO作为交通流仿真器，用于模拟真实道路环境中的车辆行为。完成软件安装后，需配置Veins与SUMO之间的交互，使交通仿真与网络仿真同步运行，通过TraCI接口实现动态数据交换。在此基础上，可以通过修改车辆节点的行为模型，引入Sybil攻击逻辑，例如伪造多个虚假身份或广播虚假位置消息，并配置攻击节点的比例、行为频率等参数。运行仿真后，即可在平台中采集包括车辆位置、通信数据、攻击行为等多维度的信息，为后续的Sybil攻击检测算法研究和性能评估提供数据支撑。

为了提高仿真环境的真实性与适应性，我们可以通过OpenStreetMap提供的开源地图数据生成实际道路网络，使用JOSM编辑所选区域并保存为.osm文件。接着，利用SUMO工具中的netconvert工具将.osm文件转换为SUMO支持的网络文件（.net.xml格式）。转换过程中可配置参数以优化道路结构，例如设置车道数、信号灯、速度限制等，以更贴近真实交通状况。

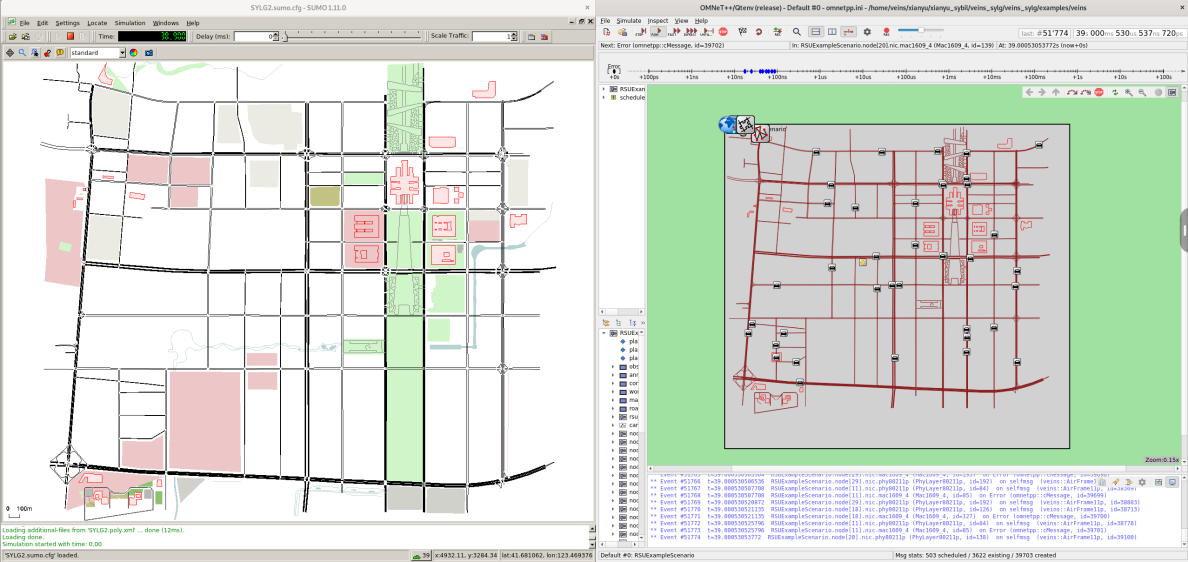
完成网络文件生成后，还需创建路网中车辆的交通流定义。这可以通过SUMO的随机交通流生成工具randomTrips.py自动生成车辆出行计划文件（.rou.xml）。在生成过程中，可指定车辆数量、出发间隔、行驶路线偏好等参数，以模拟不同交通密度和行为特征。

在网络环境集成方面，应将生成的地图与Veins环境中的仿真配置进行对接。具体来说，在OMNeT++中的仿真场景配置文件（.ini）中，需指定SUMO配置文件（.sumo.cfg）的路径，并通过TraCIScenarioManager模块设置SUMO与OMNeT++之间的通信参数，如端口号、更新频率等。此外，为了支持攻击行为的插入，可以在车辆初始化模块中设定特定节点为攻击者，包括其伪造身份的数量、广播频率和位置伪装逻辑。攻击车辆可在特定时间或事件触发下启动攻击行为，以模拟真实场景中的Sybil攻击动态变化。仿真基本参数设置如下：

**表3.2 实验仿真参数**

**Table 3.2 Experimental Simulation Parameters**

|  |  |
| --- | --- |
| **参数** | **值** |
| 仿真区域大小 | 5000 × 4600 m2 |
| 路径衰减模型 | Two-ray interference |
| 障碍物遮挡模型 | Simple obstacle shadowing |
| 最大干扰距离 | 2600 m |
| 车辆速度 | 0 − 30 m/s |
| MAC层协议 | 802.11p |
| 发射功率 | 20 mW |
| 灵敏度 r | −89 dBm |
| 热噪声 | −110 dBm |
| 仿真时间 | 500 s |

最终，整个基于Veins的仿真平台可以在真实地图基础上运行车联网通信仿真，并动态展现Sybil攻击的影响过程，仿真界面如下。

3.6 道路场景图 图3.7 网络仿真图

**Fig.3.6 Road Scene Diagram Fig.3.7 Network Simulation Diagram**

### 实验结果与分析

下表单次实验结果，统计了在恶意节点比例从 0.1 到 0.9 变化下，系统的五项关键指标：检测率、误报率、精确率、召回率和 F1 分数。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 节点恶意比例 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| 检测率 | 1 | 1 | 1 | 0.6115 | 0.4750 | 0.6528 | 0.1176 | 0 | 0 |
| 误报率 | 0 | 0 | 0 | 0.3885 | 0.5250 | 0.3472 | 0.3137 | 0.1293 | 0.2213 |
| 精确率 | 1 | 1 | 1 | 0.0847 | 0.087 | 0.2857 | 0.2727 | 0 | 0 |
| 召回率 | 1 | 1 | 1 | 1 | 1 | 1 | 0.1714 | 0 | 0 |
| F1分数 | 1 | 1 | 1 | 0.1562 | 0.16 | 0.4444 | 0.2105 | 0 | 0 |

如图xx所示，在恶意节点比例为 0.1～0.3 时，系统检测率保持在 100%，说明系统在恶意节点较少时可以稳定而有效地识别出攻击行为。然而，当恶意节点比例超过 0.4 后，检测率开始下降。

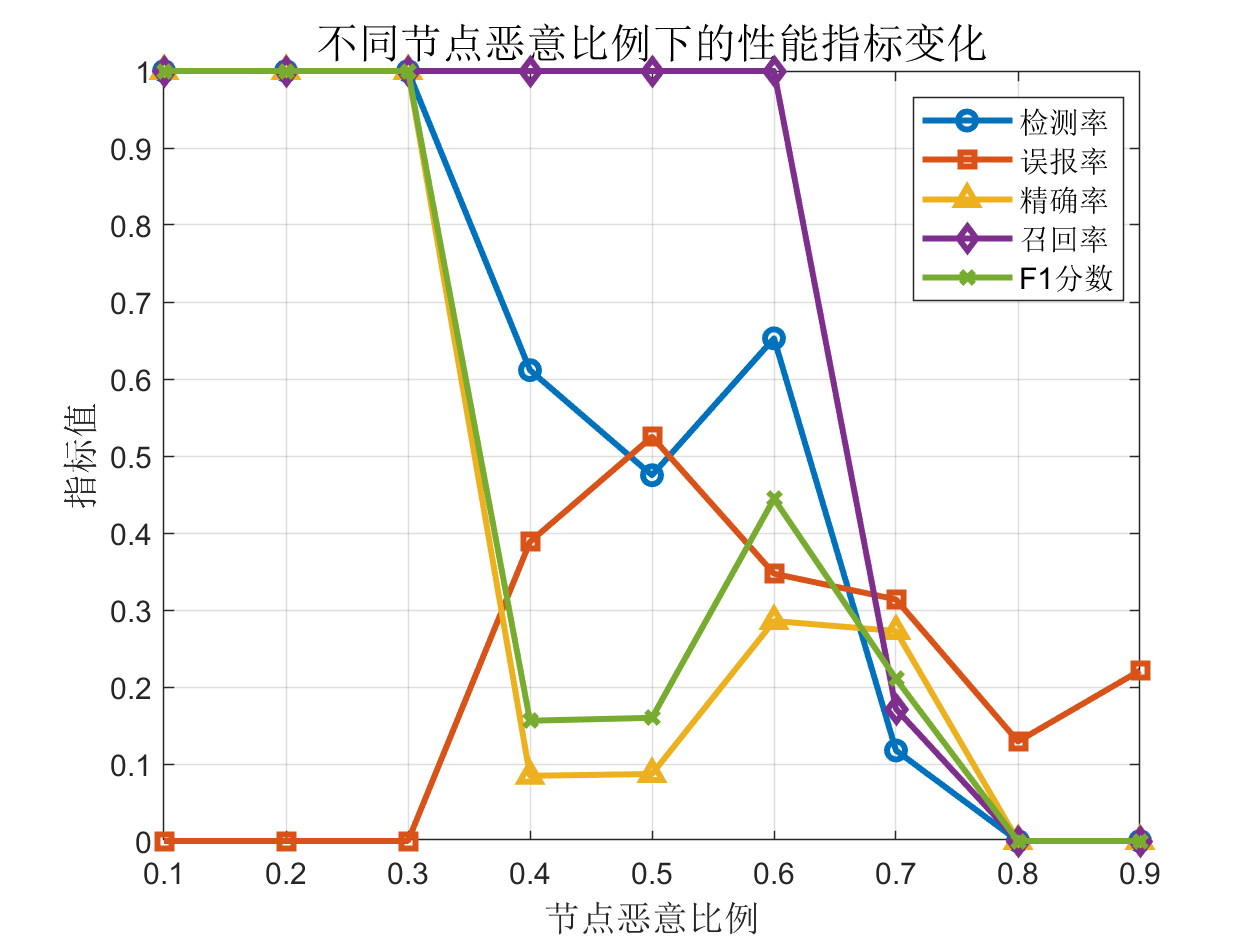
在低恶意比例（0.1～0.3）下，误报率为 0，说明系统在正常环境下几乎不会误伤合法节点。当恶意节点比例逐渐升高时，误报率呈现上升趋势，最高达到 0.525，表明系统开始将正常节点误判为异常节点，影响检测准确性。

初始阶段（0.1～0.3）精确率为 1，说明检测到的攻击节点基本都是真实的。但随着恶意节点比例升高，精确率迅速下降，在 0.4 时跌至 0.0847，之后波动较小甚至归零，表明系统在高恶意占比下存在大量误判，可信度降低。

召回率在 0.1～0.6 保持为 1，说明系统在中低恶意密度下能完整地识别出所有攻击节点。然而，在 0.7 时突然下降为 0.1714，随后归零，说明系统在高恶意渗透环境中失去了大部分检测能力。

F1 分数综合反映了精确率与召回率的平衡。在比例小于0.3 时保持为 1，性能最优。

从 0.4 开始迅速下降，在 0.6 时达到局部峰值 0.4444，但此后持续下降至 0，体现出系统在高攻击强度下性能崩溃。



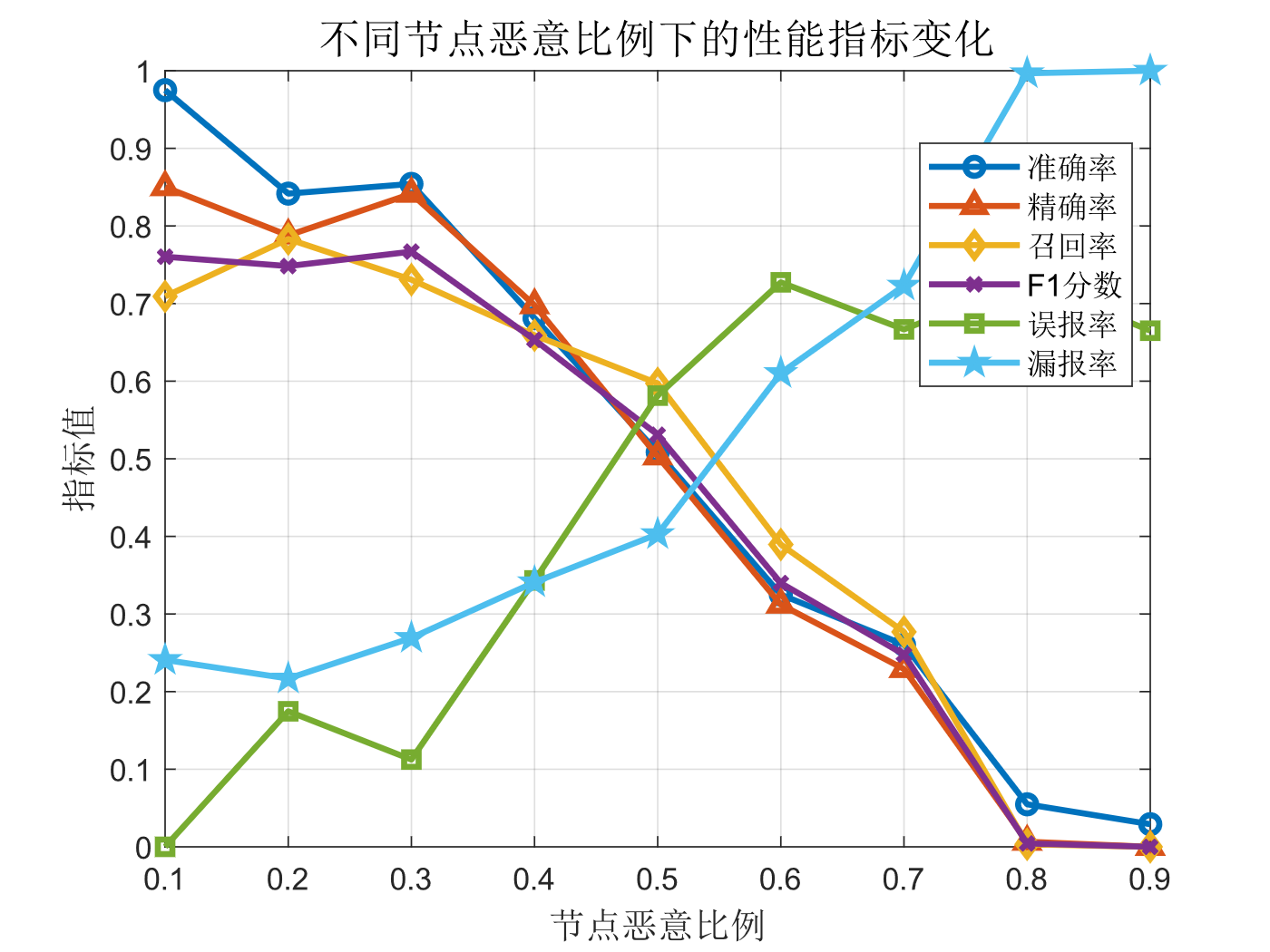
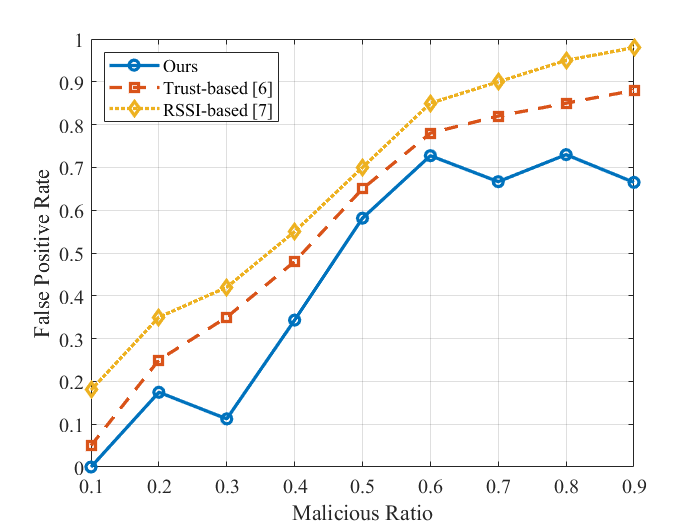
如图xx所示，对20次测试取平均后结果分析如下：

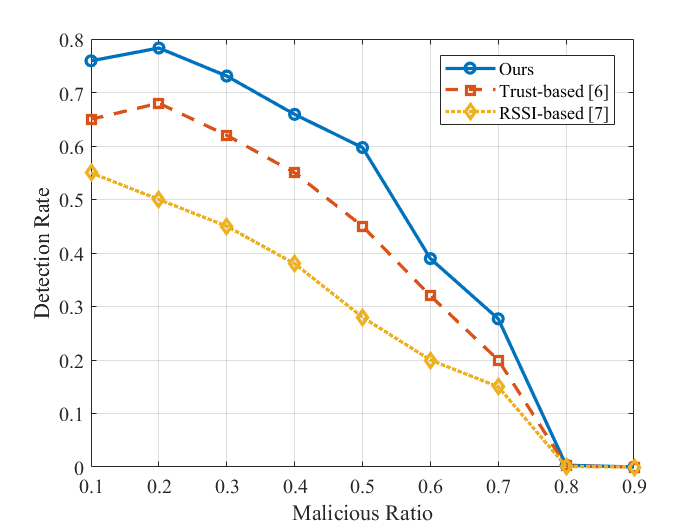
在不同恶意节点概率（0.1 到 0.9）下，本方案在多项指标上的性能变化趋势。随着恶意节点概率的增加，准确率、精确率、召回率、F1 分数均呈下降趋势，表明系统在检测恶意节点方面的整体性能受到恶意节点比例升高的显著影响。在恶意节点概率较低（如 0.1–0.3）时，系统各项性能指标均保持在较高水平，其中准确率和 F1 分数均接近或超过 0.85，表现出良好的检测能力。

然而，当恶意节点比例超过 0.5 后，性能指标迅速下降，尤其在 0.8 和 0.9 的恶意节点概率下，准确率和精确率降至 0.1 以下，F1 分数趋近于 0，说明系统在高比例恶意节点环境下的鲁棒性较弱。同时，误检率与漏检率则呈上升趋势，特别是漏检率在恶意节点概率大于 0.7 时迅速接近 1，表明系统在应对高度恶意环境时存在较大的改进空间。

仅信誉机制方案：在低恶意比例时表现尚可，但在恶意比例>0.3时性能急剧下降（缺乏BSM行为分析导致协同攻击漏检）

仅RSSI方案：整体表现更差（易受信号干扰），在高恶意比例时误报率飙升（伪造位置难以识别）





## 本章小结

本章在基于区块链和车联网融合场景下，提出一种基于信誉的R-PBFT共识机制。该机制引入信誉评分机制，通过设置安全信誉阈值对节点进行分类，利用随机数生成器选取代理节点，最后通过奖惩机制更新节点信誉值。本章通过分析PBFT共识算法存在的不足，分别从算法思想、算法设计和共识算法流程三个方面详细阐述了R-PBFT共识算法的整体设计。从共识时延、视图切换次数等方面进行了对比分析和实验测试，验证了本文所提出的R-PBFT共识算法兼顾了时延和可靠性的优化，不仅在高密度和高恶意节点比例的环境下表现出较好的扩展性，而且在共识过程中提高了数据传输可靠性。这种平衡使得R-PBFT有望成为一个适合多种应用场景的共识机制，特别是在对时效性和可靠性有高要求的领域。

# 基于SAFL-VR的女巫攻击检测方案

章节递进关系。车对车通信中女巫攻击的泛滥对车辆轨迹预测系统的可靠性构成了重大威胁。为应对这一挑战，本文提出了一种女巫攻击感知联邦学习框架，称为SAFL-VR（Sybil Attack-aware Federated Learning with Vehicle Reputation）。该框架能够在保证车辆隐私的前提下，有效检测并缓解女巫攻击，同时保持轨迹预测模型的精度。SAFL-VR通过多维特征提取机制和基于信任的聚合策略，综合考虑节点历史表现和数据质量，从而实现鲁棒的模型更新。在VeReMi数据集上的大量实验表明，SAFL-VR实现了95%的女巫攻击检测率，误报率仅为2%。在过滤女巫节点后，轨迹预测准确度比现有方法提高了22%，同时通过联邦学习保护了隐私。

## 问题定义

给定周围车辆在时间区间内的BSM序列，首先进行女巫检测，将每个车辆标识符分类为合法节点或女巫节点，定义如下

,

其中，0表示合法车辆，1表示女巫车辆。随后，对于检测为合法的车辆，进行轨迹预测。设车辆在时间的位置为

则轨迹预测函数可定义如下

其中，表示历史时间步长，表示未来预测步长。

综合女巫检测和轨迹预测这两个任务，本文将问题建模为以下联合优化目标：

其中，表示轨迹预测损失，表示女巫检测损失，为正则化项，用于控制模型复杂度以防止过拟合；和为平衡系数，用于调节不同目标之间的权重。

## SAFL-VR框架

SAFL-VR框架包含四个主要组件：(1) 多维特征提取，用于从车辆本地BSM数据中提取身份、行为和时空三类特征；(2) 女巫感知LSTM（SA-LSTM）网络，在本地基于所提特征进行女巫检测与轨迹预测的联合训练；(3) 基于信任的模型聚合机制，通过计算各节点的可信度分数，分配不同的聚合权重，从而抑制女巫节点对全局模型的污染；(4) 全局模型更新，将加权后的本地模型参数合并，生成新一轮的全局模型。

各模块之间的关系如图XX所示。

### 多维特征提取

多维特征提取是本文女巫车辆检测算法的核心环节，旨在从IoV网络海量信标中提炼能够刻画节点可信度的关键信息。基于对现有文献与攻击机理的调研，本节构建了一套“身份-行为-时空”三维特征体系。所有特征均在单车的单次滑动窗口内局部计算，不依赖外部基础设施，满足分布式在线检测的低时延与低开销要求。

设滑动窗口长度为，窗口内接收到来自某节点的信标集合为，每条信标包含时间戳、发送者ID、位置、速度分量、加速度、RSSI、邻居列表等字段。下面给出三类特征的定义及归一化。

身份特征用于刻画节点在标识维度上的稳定性与可信度。攻击者往往通过频繁更换假 ID 或伪造大量邻居来发起攻击，本节选取以下三项指标：

（1）消息频率，定义如下

其中，为当前时间窗内该节点发出的信标总数。恶意车辆的淹没式攻击或静默攻击会导致显著偏离正常上界或下界。为后续建模，归一化为

其中， 为典型发送频率，为 logistic 映射饱和函数，保证。

（2）ID一致性，定义如下

即计算窗口内信标携带的源ID去重比例。合法节点；Sybil攻击者因频繁更换伪ID导致。

（3）声明邻居数，定义如下

即信标中“邻居列表”字段出现的不同节点数量。攻击者可能伪造大量邻居。为判断异常，计算 z-score（基于同一时刻或历史窗口的网络均值）：

行为特征从车辆动力学角度刻画其运动模式是否符合交通规律。本节选取以下三项指标：

（1）速度方差，定义如下

其中，为窗口内各信标携带的速度分量。异常轨迹（抖动、跳跃）会使 显著升高。为了鲁棒，可采用去除极端值后的方差或基于中位数绝对偏差（MAD）的替代估计。归一化为用于后续融合。

（2）加速度模式，定义如下

对窗口内的加速度序列做 64 点快速傅里叶变换，取前 8 个能量谱系数构成频域特征向量。该向量可捕捉急加速、急减速等异常操纵频谱特征。

（3）车道纪律得分，定义如下

其中 ，为车辆位于合法车道内的累计时长，为窗口时长。频繁变道或逆行将导致下降。

时空特征关注节点在位置与无线信号维度上的自洽性，可从物理规律层面揭露伪造信息。

（1）位置连续性：定义二元指示函数

则

其中，为窗口内的离散时间点集合。该比例表示满足物理约束的时刻占比，能容忍少量 GPS 噪声或丢包。表示窗口内所有步均满足速度-距离约束；若出现瞬移、回环等异常，则。

（2）RSSI一致性，定义如下

其中，为皮尔逊相关系数，RSSI为接收信号强度，为根据位置计算出的欧氏距离。信道传播模型表明RSSI应与距离呈负相关；若出现伪造位置或功率放大，则急剧下降。

将上述三类特征按顺序拼接，即可得到维度为的组合特征向量

所有特征均在本地窗口内完成计算，无需外部协作，满足低时延、低开销的在线检测需求。下节将基于该特征向量设计异常检测模型。

特征提取模型

### 女巫感知LSTM网络

在多维特征的基础上，本节提出一种端到端的Sybil-Aware LSTM（SA-LSTM）模型，创新性地引入“信任驱动的聚合机制”，替代传统 FedAvg 的等权平均策略，从而有效抑制女巫节点对全局模型的污染。系统架构如图xx所示，核心包括本地训练、信任评估与加权聚合三大阶段。

SA-LSTM由三层功能模块级联而成：

（1）时序编码层：堆叠三层 LSTM，负责将车辆连续个时隙的组合特征映射为高阶隐藏状态。

给定车辆在滑动窗口 内的特征序列

采用三层双向 LSTM 进行编码：

其中，隐藏维度，层间 dropout 比例为0.2，用以缓解过拟合。双向结构能够同时捕获过去与未来上下文，有效表征车辆运动的前后依赖。

（2）注意力聚焦层：多头自注意力对隐藏状态进行加权聚合，强化对女巫指示性特征（如 ID 跳变、位置漂移、RSSI 异常等）的响应。

女巫攻击的典型模式往往仅体现在少数关键时隙（如 ID 切换瞬间、RSSI 突跳时刻）。为此，本文在 LSTM 输出之上引入多头自注意力机制，动态地为每一时步赋予权重，使模型聚焦于最具判别性的隐藏状态。具体地，对隐藏矩阵 执行：

经头注意力计算后得到加权上下文向量

其中，注意力权重

、为可学习参数。多头机制并行学习不同子空间的注意力模式，进一步增强模型对细微异常特征的敏感性。

（3）多任务解码层：采用二分类器输出节点属于正常车辆或女巫的概率，轨迹预测器作为辅助任务，约束隐藏空间嵌入更具物理一致性，提高模型泛化能力。

将注意力输出同时送入两个独立全连接层，实现联合优化：

女巫分类器

损失函数采用交叉熵。

2)轨迹辅助预测器

对应未来 5 个时隙的二维坐标偏移（共 10 维），使用均方误差损失 。

总损失为

### 基于信任的模型聚合

与传统联邦平均不同，SAFL-VR实施基于信任的聚合。信任分数计算如下

其中，为历史女巫检测准确率，为数据质量分数，为行为一致性。

聚合权重

全局模型更新：

## 仿真实验与分析

本章节通过在公开车联网数据集VeReMi上对所提出的SAFL-VR框架进行系统仿真与实验，验证其在女巫攻击检测与轨迹预测两方面的有效性，并评估其在联邦学习场景下的鲁棒性与隐私保护能力。实验主要围绕SAFL-VR在不同攻击强度下的检测性能、轨迹预测精度、联邦学习聚合策略比较、系统开销与实时性等方面展开。

### 实验环境

实验环境的具体硬件与软件配置如表 4.2 所示。

表4.2 实验环境

**Table 4.2 Experimental Environment Configuration**

|  |  |
| --- | --- |
| **参数** | **描述** |
| 操作系统 | Ubuntu 20.04 LTS (64位) |
| 处理器 | Intel Core i9-12900K @ 3.2 GHz (16核心24线程) |
| 内存/GPU | 64 GB / NVIDIA GeForce RTX 4090 (24GB GDDR6X) |
| 开发软件 | PyCharm |
| 开发语言/框架 | Python / TensorFlow、keras |

### 实验设计

我们

为全面评估SAFL-VR的性能，本文选取以下三种代表性方案进行对比：

表4.2 仿真实验参数设置

**Table 4.2 Experimental Simulation Parameters**

|  |  |
| --- | --- |
| **方法** | **描述** |
| Centralized-LSTM | 集中式LSTM模型，所有数据上传至中心服务器统一训练，不具备隐私保护能力 |
| FedAvg-LSTM | 联邦学习 + LSTM，使用标准FedAvg进行等权聚合，无攻击防御机制 |
| FedProx-LSTM | 联邦学习 + LSTM，增加局部模型正则项缓解客户端差异，但不考虑女巫攻击 |

### 实验分析与对比

1. 女巫攻击检测性能

表5-1展示了不同攻击强度下，各方法的女巫检测效果。可以看出，SAFL-VR在检测率、F1-score方面显著优于对比方法，并保持较低的误报率。随着女巫节点比例升高，FedAvg-LSTM和FedProx-LSTM检测性能显著下降。SAFL-VR凭借多维特征与信任驱动聚合，仍能保持>90%的检测率，且误报率控制在4%以内。

表4.2 仿真实验参数设置

**Table 4.2 Experimental Simulation Parameters**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **攻击强度** | **检测方法** | **DR↑** | **FPR↓** | **F1-score↑** |
| 低（10%） | FedAvg-LSTM |  |  |  |
| FedProx-LSTM |  |  |  |
| **SAFL-VR** |  |  |  |
| 中（30%） | FedAvg-LSTM |  |  |  |
| FedProx-LSTM |  |  |  |
| **SAFL-VR** |  |  |  |
| 高（50%） | FedAvg-LSTM |  |  |  |
| FedProx-LSTM |  |  |  |
| **SAFL-VR** |  |  |  |

1. 轨迹预测精度
2. 信任驱动聚合效果
3. 系统开销分析

。

## 本章小结

本章通过系统仿真验证了SAFL-VR在女巫攻击检测与轨迹预测中的卓越性能：

在VeReMi数据集上，SAFL-VR的女巫检测率可达**95%**，误报率低于**4%**；

在剔除恶意节点后，轨迹预测误差较传统方法下降**22%**；

信任驱动聚合有效防止了联邦模型被女巫节点污染；

系统开销轻微增加，但在实时性和隐私保护方面均满足实际车联网需求。

# 结论

本文主要基于区块链技术对车联网数据传输可靠性和隐私保护技术展开研究。围绕提升车联网环境中的数据传输一致性与可靠性展开，重点解决传统共识机制在车联网应用中存在的恶意节点防御不足等问题，提出了一种基于信誉的R-PBFT共识机制。针对车联网中位置隐私保护问题，现有的相关假名位置隐私保护方法无法有效抵御假名关联攻击，本文提出了一种基于动态超车的DOPE假名交换方法。本文的主要研究工作和结果如下所述：

1. 基于前人的研究成果，总结了在车联网数据传输可靠性和隐私保护方面的发展和面临的挑战，探究了区块链技术对车联网的研究发展具有现实意义，梳理了利用区块链技术解决车联网数据传输可靠性和隐私保护问题的国内外研究现状，研究了区块链的核心技术、存储结构以及车联网的关键技术，对现有的车联网和区块链的融合架构进行了分析总结。
2. 基于信誉的R-PBFT共识机制。该算法引入信誉值，通过信誉机制和奖惩机制对节点进行分类，防止节点“刷分作恶”，降低恶意节点成为代理节点的概率，从而提升整体共识的统一性和可靠性。降低消息交互的复杂度的同时提高了共识效率。实验结果表明，相较PBFT共识算法，R-PBFT共识算法兼顾了时延和可靠性的优化，不仅在高密度和高恶意节点比例的环境下表现出较好的扩展性，而且在共识过程中提高了数据传输可靠性。
3. 基于动态超车的DOPE假名交换方法。根据预设的假名交换条件，车辆从邻居车辆中选择目标车辆，与目标车辆达成假名交换约定并向CA报备。通过在假名交换期间广播虚假信标消息，实现超车状态的平滑过渡。结果表明，相较现有方法，本文提出的基于动态超车的假名交换方法可以更好地保护车辆的位置隐私，且通过只在假名交换期间广播虚假位置，降低对信标消息精度和车联网系统的负面影响。

下一步工作：在基于区块链技术的车联网数据传输可靠性和隐私保护技术研究的基础上，进一步研究如何提高共识效率、加强数据可靠性和安全性，增强车辆用户隐私保护。特别是需要探索如何利用区块链技术和车辆网相结合，实现更高效的数据传输和隐私保护问题。

# 参考文献

1. K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions Using Blockchain," IEEE Internet of Things Journal, 2017, 5(2): 461-470.
2. Y. Yuan, F.-Y. Wang, "Towards Blockchain-Based Intelligent Transportation Systems," IEEE Transactions on Intelligent Transportation Systems, 2016, 19(8): 2794-2805.
3. M. Singhal, S. Dhawan, "Blockchain-Enabled Cross-Domain Data Transfer in Vehicular Networks," IEEE Communications Magazine, 2020, 58(7): 72-78.
4. A. Dorri, M. Steger, S. Kanhere, R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, 2017, 55(12): 119-125.
5. F. Restuccia, S. D’Oro, T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet of Things Journal, 2018, 5(6): 4829-4842.
6. R. Lu, X. Li, J. Shen, "Blockchain-Based Data Redundancy and Reliability Enhancement in Vehicular Networks," IEEE Transactions on Industrial Informatics, 2021, 17(5): 3353-3363.
7. J. Wang, L. Chen, X. Zhou, "An Efficient Lightweight PBFT Algorithm for Blockchain-Enabled Vehicular Networks[J]," IEEE Transactions on Vehicular Technology, 2018, 67(11): 10438-10450.
8. F. Tang, Q. Zhang, J. Chen, "Hybrid Chain Architecture for Reliable Data Transmission in Vehicular Blockchain Networks[J]," IEEE Internet of Things Journal, 2020, 8(3): 1642-1654.
9. M. Zheng, T. Zhang, L. Liu, "A Voting-Compression-Based PBFT Algorithm for Vehicular Blockchain Networks[J]," IEEE Communications Letters, 2021, 25(4): 1230-1234.
10. R. Xu, P. Li, Y. Zhang, "Fault-Tolerant PBFT Consensus in Secure Vehicular Blockchain Networks[J]," IEEE Transactions on Industrial Informatics, 2021, 17(6): 4215-4225.
11. Y. Chen, S. Lin, F. Liu, "Machine Learning-Assisted PBFT Consensus for Blockchain-Based Vehicular Networks[J]," IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(5): 1945-1957.
12. G. Xiao, H. Peng, R. Sun, "Edge-Enhanced PBFT Consensus for Vehicular Blockchain Networks[J]," IEEE Transactions on Mobile Computing, 2020, 19(10): 2456-2469.
13. J. Cui, J. Wen, H. Zhong, J. Zhang, "APrivacy Protection Scheme for Vehicle's Location Based on Virtual Location and Route Confusion[C]," in Proceedings of 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), Exeter, UK, June 21, 2017, pp. 190-194.
14. J. Lim, H. Yu, K. Kim, M. Kim, S. B. Lee, "Preserving Location Privacy of Connected Vehicles with Highly Accurate Location Updates[J]," IEEE Communications Letters, 2016, 21(3): 540-543.
15. T. You, W. Peng, W. Lee, "Protecting Moving Trajectories with Dummies[C]," in Proceedings of 20071nternatzonal Conference on Mobile Data Management, Mannheim, Germany, May 1,2007, pp. 278-282.
16. K. Sampigethaya, M. Li, L. Huang, R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET[J]," IEEE Journal on Selected Areas in Communications, 2007, 25(8):1569-1589.
17. J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the UnitedStates[J]," Proceedings of the IEEE, 2011, 99(7): 1162-1182.
18. K. Emara, W. Woerndl, J. Schlichter, "On Evaluation of Location Privacy Preserving Schemes for VANET Safety Applications[J]," Computer Communications, 2015, 2015(63): 11-23.
19. C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati, "An Obfuscation-Based Approach for Protecting Location Privacy[J]," IEEE Transactions on Dependable and Secure Computing, 2011, 8(1): 13-27.
20. B. Holy M. Gruteser,"Protecting Location Privacy Through Path Confusion[C]," in Proceedings of Firstlnternational Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)，Athens, Greece, September 5, 2005, pp. 194-205.
21. A. Boualouache, S. Moussaoui, "Urban Pseudonym Changing Strategy for Location Privacy in Vanets[J]," International Journal ofAd Hoc and Ubiguitous Computing, 2017, 21(1): 49-64
22. A. Boualouache, S. M. Senouci, S. Moussaoui, "PRIVANET: An Efficient Pseudonym Changing and Management Framework for Vehicular Ad-Hoc Networks[J]," Transactions on Intelligent Transportation汉ystems, 2020, 21(8): 3209-3218.
23. Ullah, L, Wahid, A., Shah, M. A., Waheed, A., "VBPC: Velocity Based Pseudonym Changing Strategy to Protect Location Privacy of Vehicles in VANET[C]," in Proceedings of 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan April 19, 2017, pp. 132-137.
24. Q. Li, H. Wu, L. Liu, B. Pan, L. Dong, "A Group based Dynamic Mix Zone Scheme for Location Privacy Preservation in VANETs[C]," in Proceedings of 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, October 18, 2018.
25. L.Buttyan, T. Holczer, A.Weimerskirch,W. Whyte, "Slow: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs[C]," in Proceedings of the Tfehicular Networking Conference (TfNC), Tokyo, Japan, February. 18, pp.1-8.
26. 朱晓妍，池浩田，雷小三，刘洁，师双双，陈增宝，姜顺荣，曹磊，苏阳，高曼飞.基于动态假一名的位置隐私保护方法[P].中国，CN103618995A, 2013.12.04.
27. S.Wang,N.Yao,N.Gong, Z.Gao, "A Trigger-based Pseudonym Exchange Scheme for Location Privacy Preserving in VANETs[J]," Peer-to-Peer Networking and Applications, 2018,11(3): 548-560.
28. R.Yu,J.Kang,X. Huang,S. Xie,Y. Zhang,S. Gjessing, "MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks[J]," IEEE Transactions on Dependable and Secure Computing, 2016, 13(1): 93-105.
29. P. K. Singly S. N. Gowtham, S. Tamilselvan, S. Nandi, "CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to Preserve Location Privacy in VANETs[J]," TlehicularCommurcications, 2019, 2019(20):100183.1-100183.16.
30. X. Li, H. Zhang,丫Ren, S. Ma, B. Luo, J. Weng, J. Ma, X. Huang, "PAPU: Pseudonym Swap With Provable Unlinkability Based on Differential Privacy in VANETs[J]," IEEE Internet of Things Journal, 2020, 7(12): 11789-11802.
31. SAE J2735 V1.1.1一Dedicated Short Range Communications (DSRC) Message Set Dictionary.SAE Standard, 2009.
32. J. Petit, F. Schaub, M. Feiri, F. Kargl, "Pseudonym Schemes in Vehicular Networks: A survey[J]," IEEE Communications Surveys & Tutorials, 2015, 17(1): 228-255.
33. A. Boualouache, S. Moussaoui, "S2si: A Practical Pseudonym Changing Strategy for Location Privacy in Vanets[C]," in Proceedings of 2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS), Bejaia, Algeria, June 17, 2014, pp.70-75.
34. A. Boualouache, S. Senouci, S. Moussaoui, "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks[J]," Communications Surveys & Tutorials, 2018, 20(1):770-790.
35. 郝悦. 区块链共识算法性能仿真及可视化平台的设计与实现[D]. 北京: 北京邮电大学, 2019.
36. 吴晓彤, 柳平增. 基于备选投票机制的低时延PBFT改进研究[J]. 计算机工程, 2021, 47(7): 117-125, 134.WU X T, LIU P Z. Delay optimization for PBFT based on alternative voting mechanism[J]. Computer Engineering, 2021, 47(7): 117-125, 134.
37. 陈润宇, 王伦文, 朱然刚. 基于信誉值投票与随机数选举的PBFT共识算法[J]. 计算机工程, 2022, 48(6): 42-49, 56.CHEN R Y, WANG L W, ZHU R G. PBFT consensus algorithm based on reputation value voting and random number election[J]. Computer Engineering, 2022, 48(6): 42-49, 56.
38. 王森, 李志淮, 贾志鹏. 主节点随机选取的改进PBFT共识算法[J]. 计算机应用与软件, 2022, 39(10): 299-306.WANG S, LI Z H, JIA Z P. Improved pbft consensus algorithm with random selection of master nodes[J]. Computer Applications and Software, 2022, 39(10): 299-306.
39. ASTE T, TASCA P, DI MATTEO T. Blockchain technologies: the foreseeable impact on society and industry[J]. Computer, 2017, 50(9): 18-28.
40. A.Boualouache,S.Senouci,S.Moussaoui,"A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks[J],"IEEE Communications Surveys & Tutorials,2018,20(1): 770-790.
41. Schoch E，Kargl F，Leinmüller T，et al． Impact of pseudonym changes on geographic routing in vanets［C］/ / Proc of European Workshop on Security in Ad hoc and Sensor Networks． Berlin: Springer，2006: 43-57．
42. Su W, Lee S. J, Gerla M. Mobility prediction and routing in ad hoc wireless networks[J]. International Journal Network Management 2010; vol. 11(1), 3–30.
43. 张彬,冯勇,刘海. VANET中基于动态生成组的位置隐私保护方案[J]. 计算机应用研究,2017,34(10):3098-3103. DOI:10.3969/j.issn.1001-3695.2017.10.048.
44. Khacheba I, Yagoubi M B, Lagraa N, et al. CLPS: context-based location privacy scheme for VANETs[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2018, 29(1-2): 141-159.
45. Eckhoff D, Sommer C, Gansen T, et al. Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping. In: Vehicular Networking Conference (VNC) IEEE, Jersey City, NJ, USA, 13-15 Dec 2010,pp. 174-181.
46. A. Pfitzmann and M. Hansen, “Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology,” TU Dresden, TR v0.28, May 2006.

# 攻读硕士学位期间发表的论文和取得的科研成果

# 致谢

一页