
哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

# 基于公钥基础设施与信任管理的车联网数据认证系统

**答辩人**：夏天怡　　**指导老师**：于萍

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

# 目录

CONTENTS


PART 1 研究背景与意义

PART 2 国内外研究现状

PART 3 研究内容及关键问题

PART 4 研究方法及技术路线

PART 5 进度安排

# 1 研究背景及意义

车联网（IoV）中，车辆和路边基础设施（RSU）之间需要频繁的通信，如位置更新、行驶状态、交通信息等。这些数据在传输过程中可能面临恶意节点攻击、数据篡改、重放攻击等安全问题。因此，保障数据的安全性和可信性，同时快速识别并隔离恶意节点，是一个重要的研究课题。

- 数据安全性问题

车联网中的数据在传输过程中容易受到中间人攻击、窃听等威胁，如何确保数据传输的安全性至关重要。

- 数据可信性问题

在车联网中，车辆之间的数据交换量非常大，但存在恶意节点发送虚假数据的问题，如何保证数据的真实性和完整性是关键。

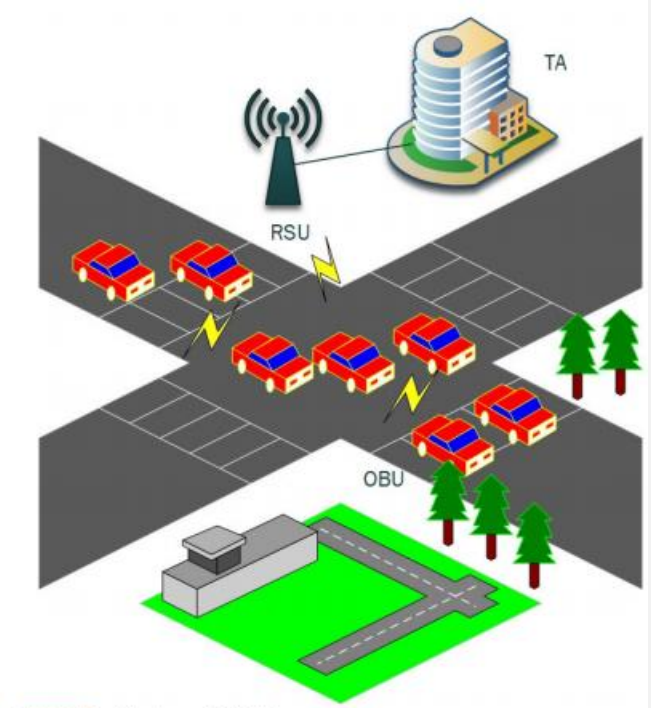


FIGURE 1. Structure of VANET.

# 2.1 研究现状——隐私保护

车联网隐私保护主要分为三种类型：

01 **身份隐私保护：**

Maxim Raya et al. 提出了一种基于PKI密钥管理方案，以保障车载自组网的安全。H. Sikarwar提出了一种轻量级的认证和批量验证方案，旨在提升车联网（IoV）环境中的安全性和效率。

02 **位置隐私保护：**

Amit et al. 讨论了一种基于混合区域模型和其他方法保护位置隐私的有效和可扩展的位置隐私架构。

03 **轨迹隐私保护：**

M. Cao et al. 提出了一种个性化轨迹隐私保护机制。采用基于Hilbert曲线的最小距离搜索算法,并提出了一种新的用于位置扰动的Permute和Flip机制，同时改善了隐私和服务质量之间的平衡。


- Maxim Raya and Jean-Pierre Hubaux. 2007. Securing vehicular ad hoc networks. J. Comput. Secur. 15, 1 , 39–68.
- H.Sikarwar and D. Das, "Towards Lightweight Authentication and Batch Verification Scheme in IoV," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3244-3256.

# 2.2 研究现状——信任管理

车联网信任管理机制主要分为三种类型：

01 **基于实体的信任管理：**

基于实体的信任管理方案旨在评估参与车联网内数据转发和交换的**节点的可信度**，根据信任级别的评估，将信任值较低的节点排除出网络。

02 **基于数据的信任管理：**

在基于数据的信任管理方案中，信任评估**与消息内容相关**，通过评估数据的真实性建立信任管理。数据的信任评估通常综合考虑时间、内容接近度、位置和事件类型等信任因素。

03 **混合方式：**

混合信任管理方案综合考虑了实体和数据对可信度的影响。

# 2.3 研究现状与分析

## 国内外现状分析

- **信任值计算的单一性**
  - 很多系统只基于通信行为或历史进行信任值调整，没有考虑**多维度因素**，如车辆环境、异常模式检测等。
- **实时性不足**
  - 在面对大规模车联网环境时，难以实现**高效低延迟**的**信任值传播**和**恶意节点检测**。
- **动态适应性不强**
  - 大部分信任管理机制在面对复杂场景（如车辆高速移动、短暂失联等）时，无法快速适应网络变化。

# 3.1 研究内容

本项目旨在通过PKI确保车辆身份认证，并通过信任管理机制动态评估车辆数据的可信度，从而构建一个安全可靠的车联网数据认证体系。

系统主要分为两个部分：

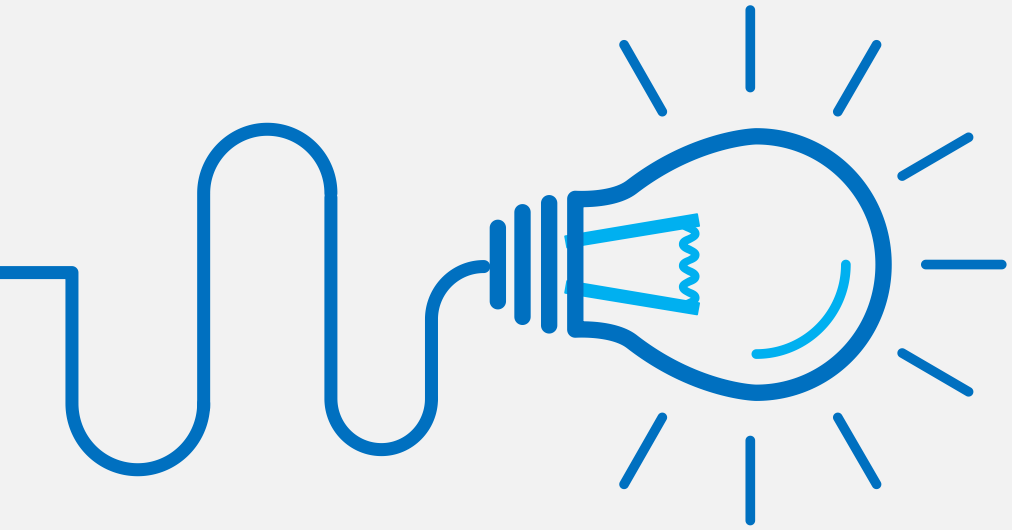
## 01、PKI身份认证层

基于椭圆曲线密码学的公钥加密和数字签名算法，为每辆车分配唯一的公钥和私钥，实现双向加密通信和身份验证。

## 02、信任管理层

基于车辆的历史行为和通信记录，动态调整车辆的信任值。低信任值的节点会被自动隔离，减少恶意数据传播的风险。

# 3.2 创新点设计



## 1 多维度信任评分机制

引入基于**车辆环境、数据来源、历史行为、网络状况**的多维度信任值计算框架，通过多种特征的综合分析提高信任评分的准确性和可靠性。

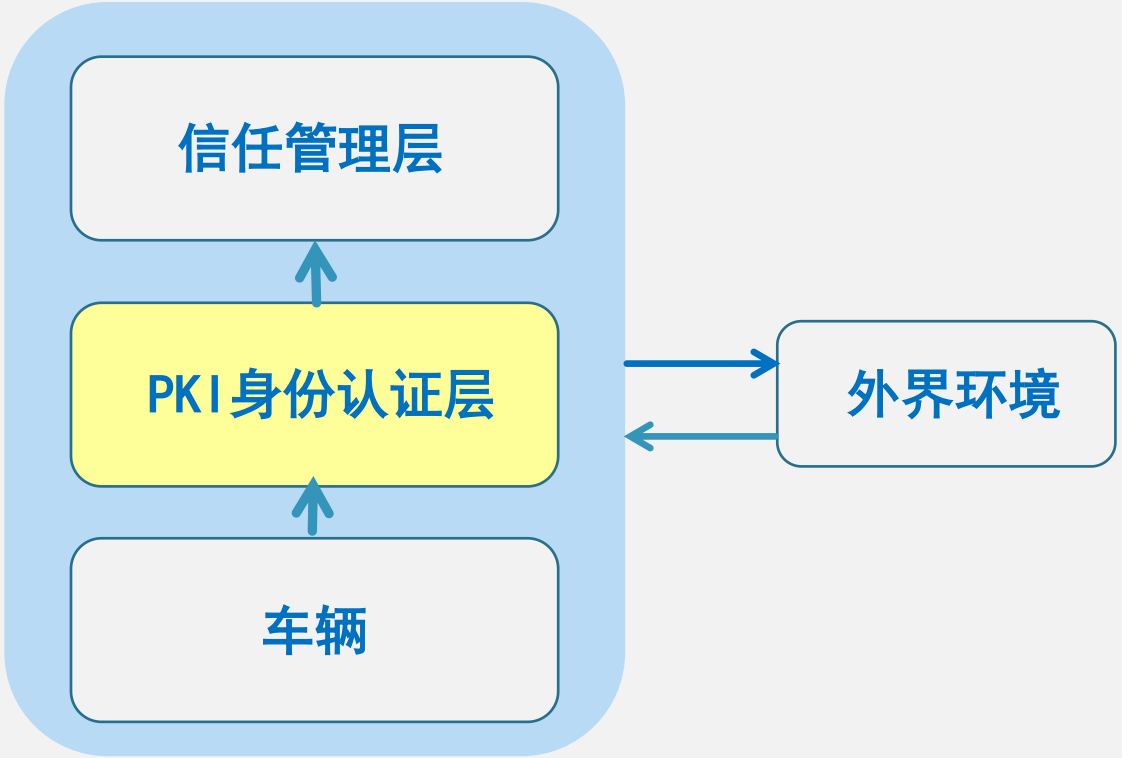
## 2 自适应信任传播机制

针对车联网动态环境的变化，设计一种**自适应信任值传播算法**，通过邻近节点的实时反馈调整车辆信任值传播速率，提升系统的实时性。

## 3 基于机器学习的异常行为检测

利用**机器学习算法（如随机森林、决策树）检测车辆异常行为**，如数据重放攻击、伪造数据等。结合信任管理机制，通过模型学习和行为预测，快速发现恶意节点并隔离。

# 4.1 研究方法




## 系统开发

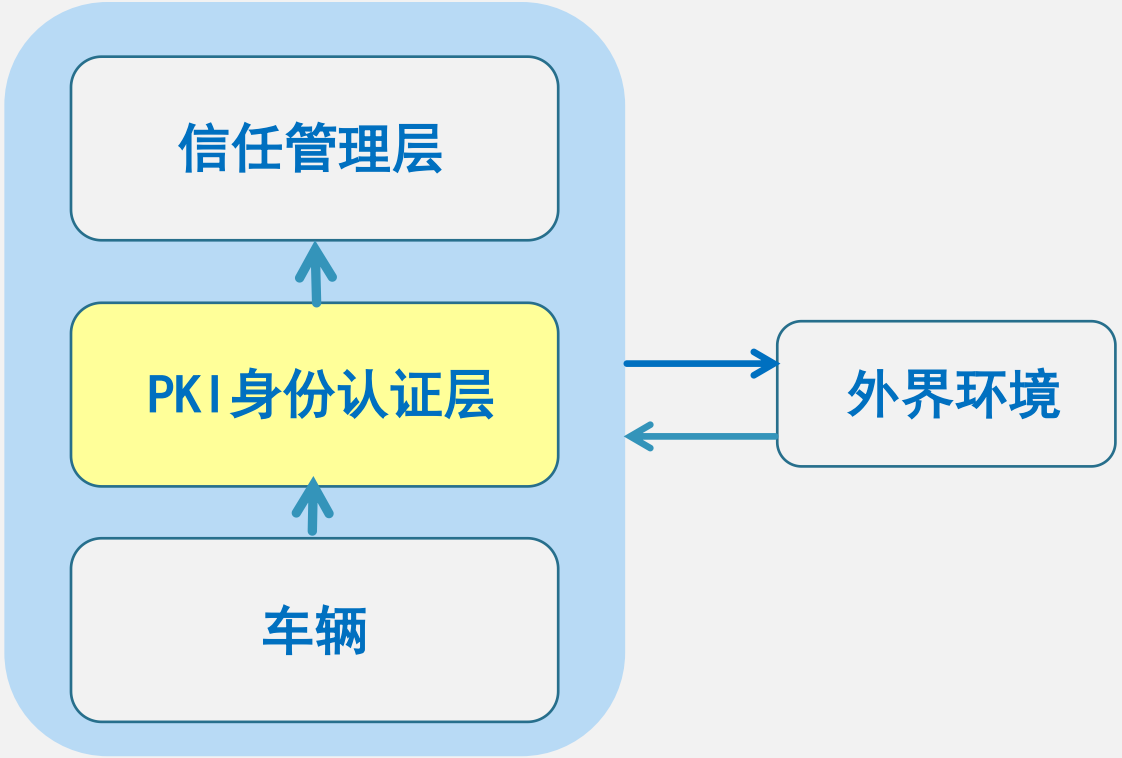
### PKI身份认证层：

1.基于椭圆曲线密码学的身份认证

椭圆曲线密码学（ECC，Elliptic Curve Cryptography）是一种高效的公钥加密算法，其关键特点是能够在**更小的密钥长度**下提供与传统公钥加密（如 RSA）相同的安全性。

同时，ECC在数字签名中通过其特有的**椭圆曲线数字签名算法**（Elliptic Curve Digital Signature Algorithm，ECDSA）来实现消息的签名和验证。

# 4.1 研究方法



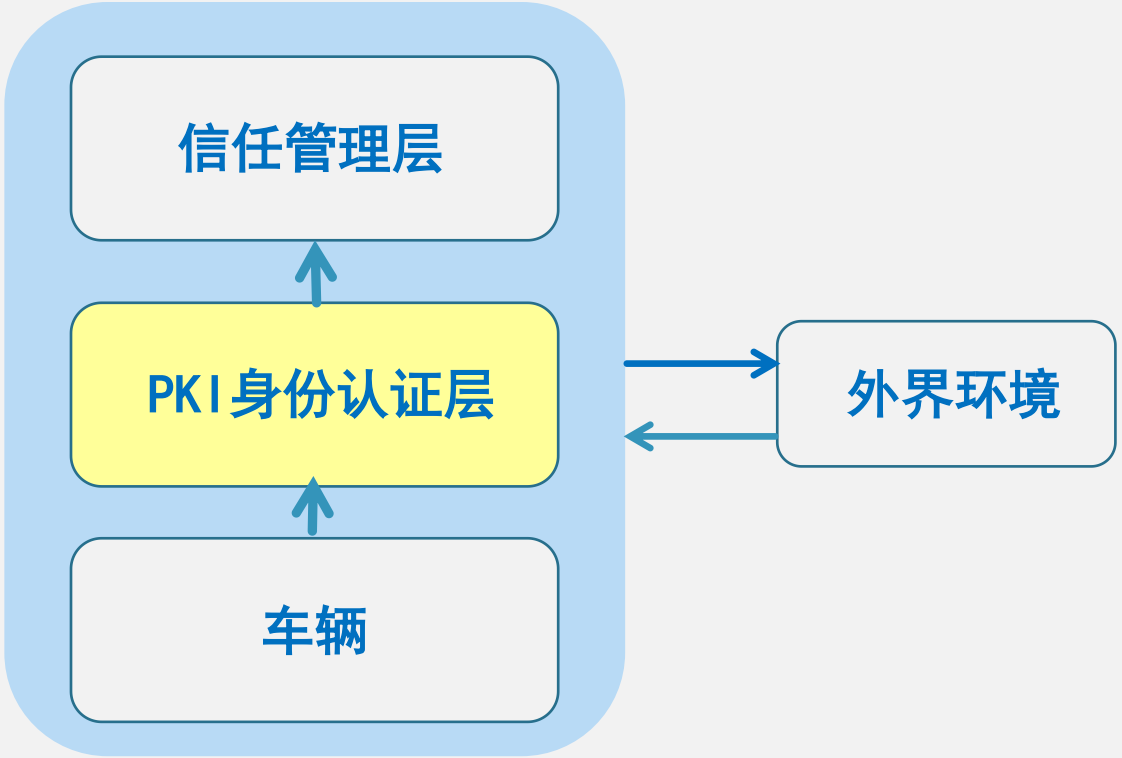

## 系统开发

### PKI身份认证层：

2. 基于OpenSSL的公私钥颁发

- **公钥和私钥对的生成**：**OpenSSL** 可以生成多种公私钥对，包括 RSA、**ECC**、DSA 等。公私钥对用于加密、解密、签名和验证等操作。

# 4.1 研究方法



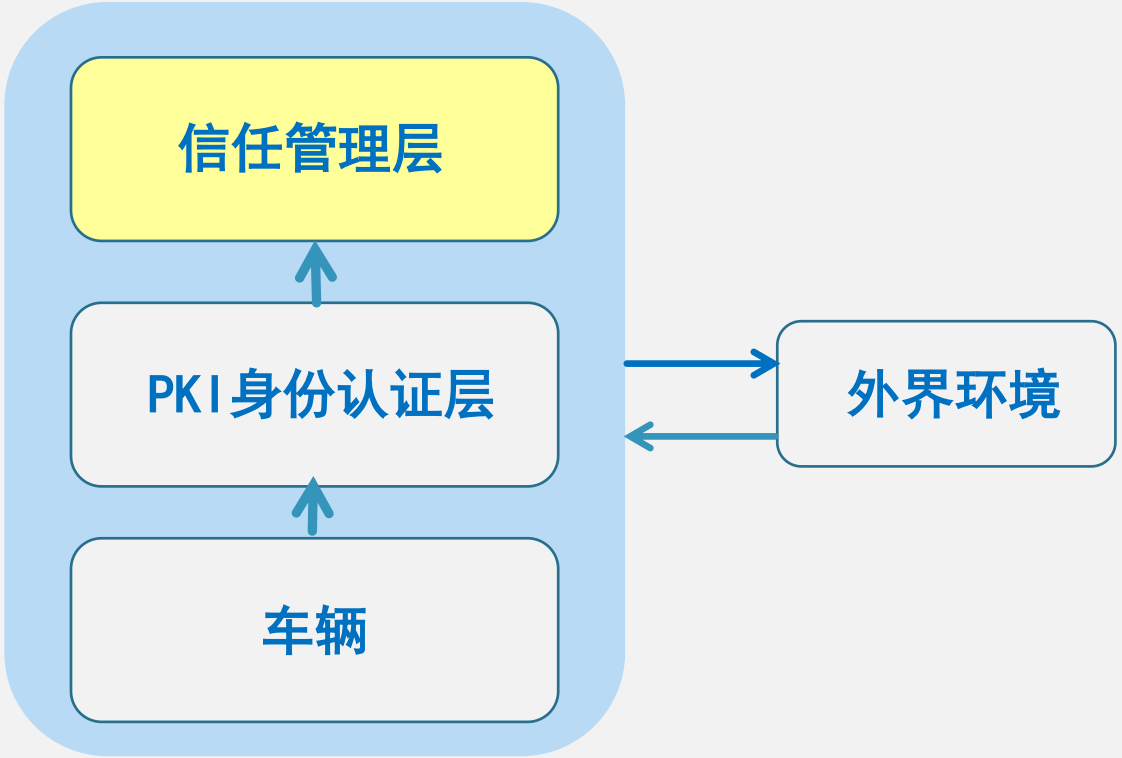

## 系统开发

### PKI身份认证层：

2. 基于OpenSSL的公私钥颁发

- **数字证书的颁发**：OpenSSL 可以作为证书颁发机构（CA），为用户、设备或服务器颁发数字证书。证书中包含了公钥和相关的身份信息，用于验证持有者的身份。
  - 证书通过私钥进行签名，并由CA验证其真实性。
  - 公钥用于解密签名并验证数据，保证通信双方的身份和通信数据的安全性。

# 4.1 研究方法




## 系统开发

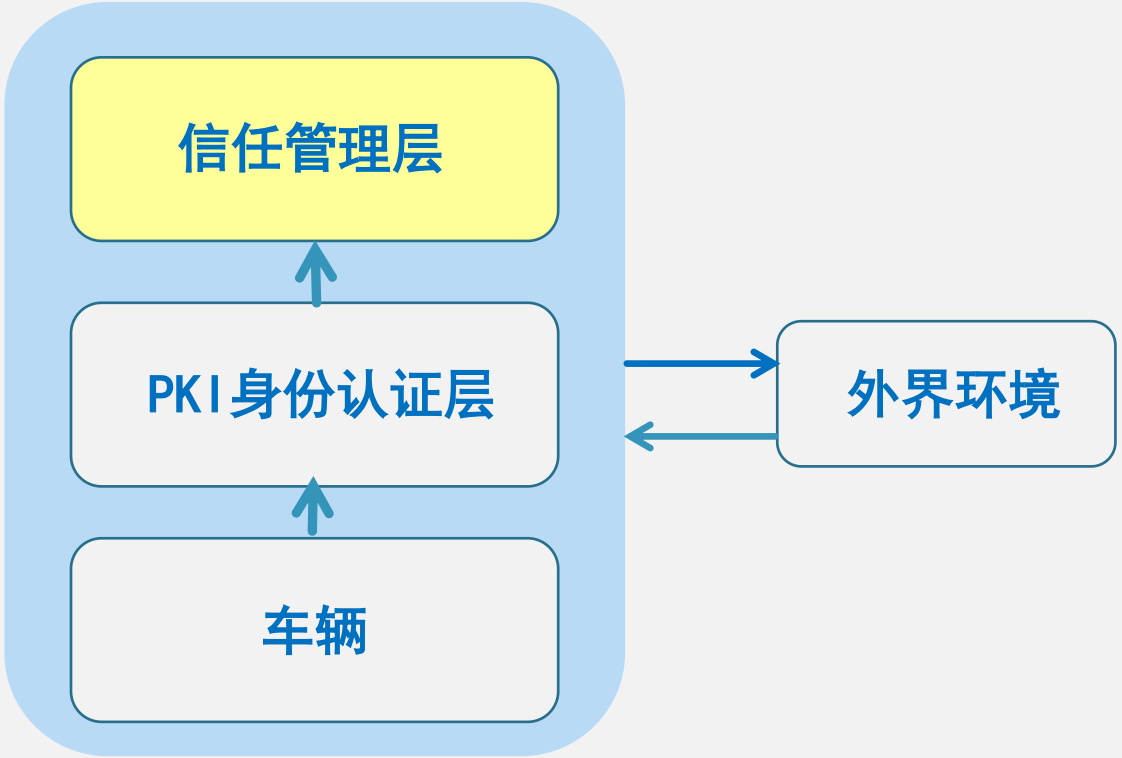
### 信任管理层：

1. 信任评分机制

信任评分基于以下维度进行动态调整：

- **数据准确性**：接收到的数据是否与其他车辆或RSU的数据相一致。
- **通信频率**：车辆的通信行为是否正常（例如，频繁发送无效信息则会降低信任值）。
- **行为历史**：车辆在之前的通信中是否出现过异常行为或攻击迹象。
- **网络状况**：考虑到网络状况的变化，特别是车辆在某些区域短暂失联时，给予更灵活的信任调整机制，避免误判。

# 4.1 研究方法




## 系统开发

### 信任管理层：

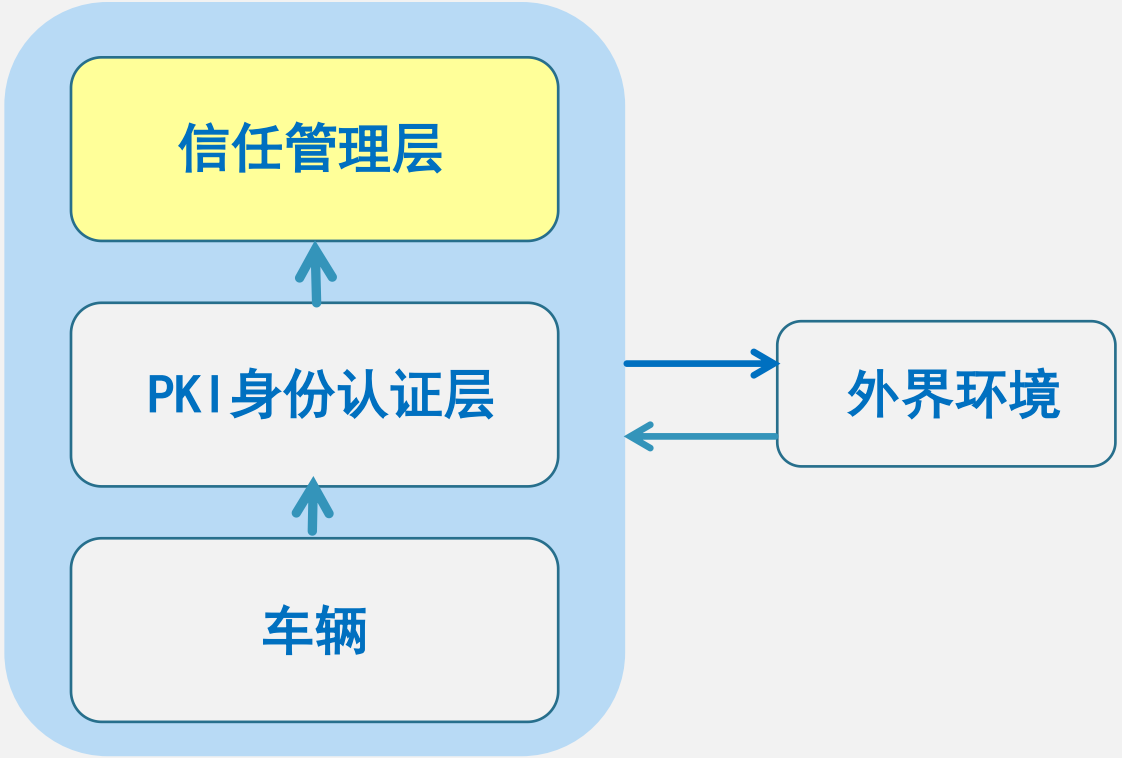
1. 信任评分机制

每个维度都可以通过权重进行加权计算：

$$Trust_i = \alpha_1 \times \text{数据准确性} + \alpha_2 \times \text{通信频率} + \alpha_3 \times \text{行为历史} + \alpha_4 \times \text{网络状况}$$

其中，$\alpha_1$，$\alpha_2$，$\alpha_3$，$\alpha_4$是根据具体场景动态调整的权重系数。

# 4.1 研究方法




## 系统开发

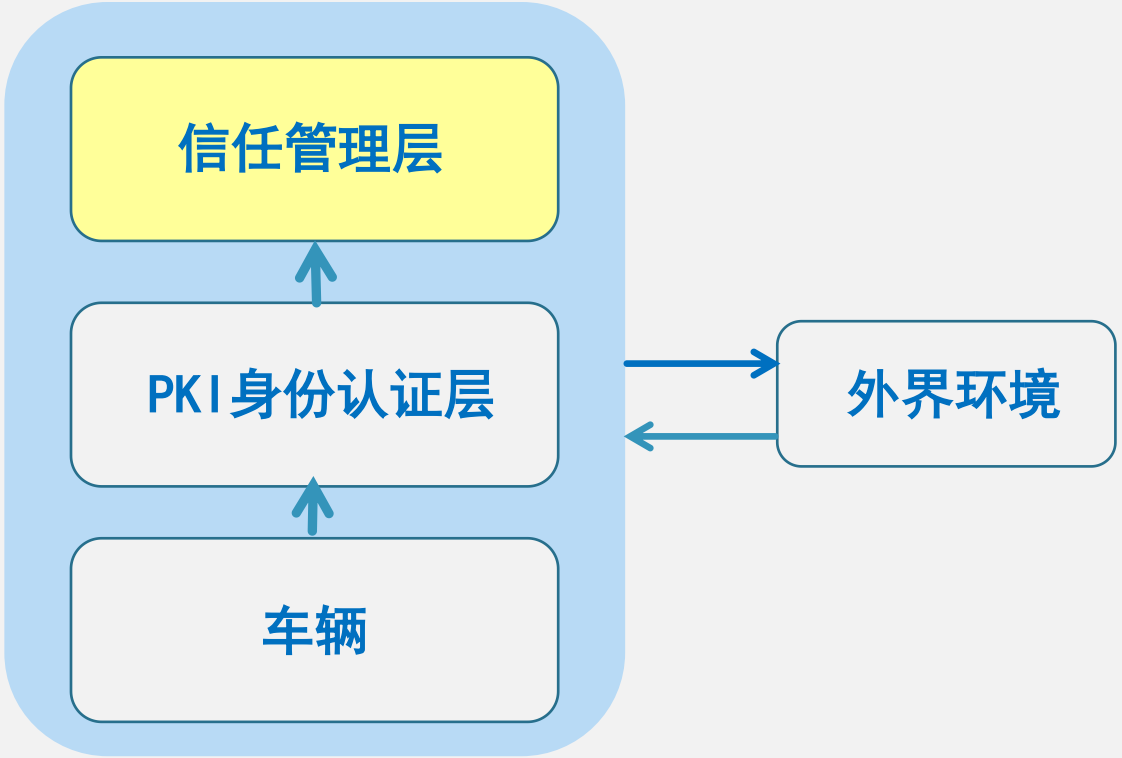
### 信任管理层：

2. 自适应信任传播机制

- 基于**邻近车辆反馈**：当车辆通过广播信任值时，邻近节点可以快速给出反馈，判断该车辆的行为是否异常，迅速传播信任值变化。
- **动态传播速率**：根据网络负载和车辆密度，调整信任值传播的速率，确保在高车流量或恶劣网络环境中仍能有效进行信任评估。

创新点：提出一种**基于区域自适应性的信任值传播机制**，利用邻近车辆的反馈来加速恶意节点检测，并减少信任值传播的冗余数据传输。

# 4.1 研究方法




## 系统开发

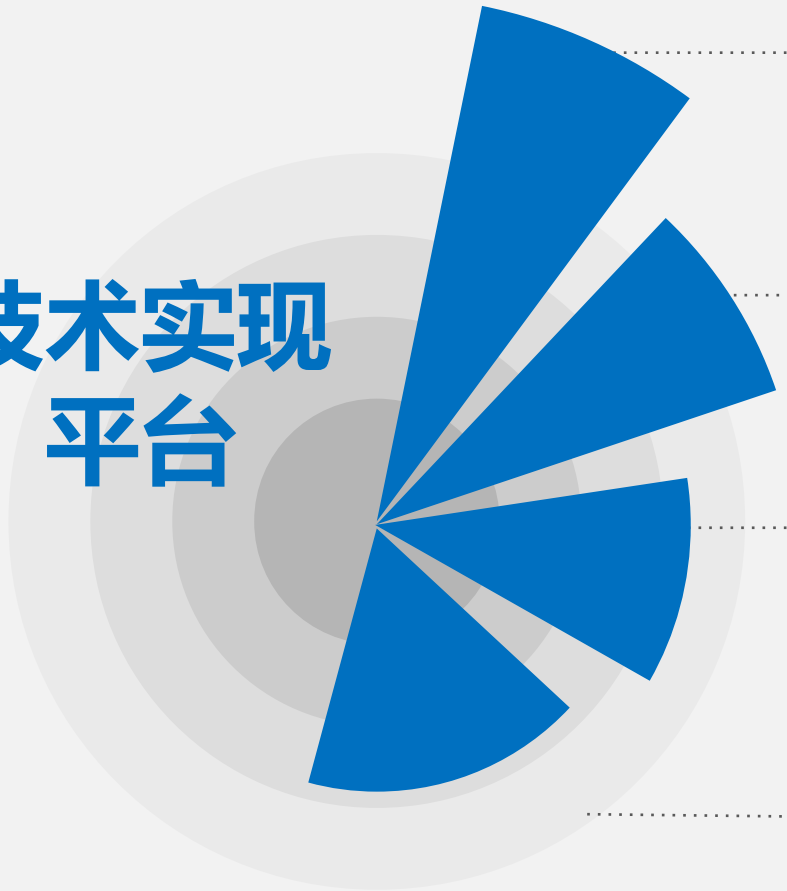
### 信任管理层：

3. 恶意节点检测与隔离

- **恶意节点模拟**：在仿真中设置恶意节点，模拟数据篡改、伪造身份、重放攻击等行为。
- **基于机器学习**的异常检测：引入机器学习算法，通过车辆的通信行为模式和数据特征来识别恶意行为。可以采用常见的机器学习算法（如决策树、随机森林）进行车辆行为分类，识别恶意车辆。

创新点：利用机器学习模型进行**行为模式学习**，通过车辆的历史数据建立模型，检测异常数据流和异常行为，**提前预警**恶意节点的可能性。

# 4.2 技术路线




## 1. PKI身份认证实现

OpenSSL：使用OpenSSL为每辆车生成公钥和私钥，设计车辆之间的轻量级数据加密协议，并实现双向认证机制。

## 2. 信任管理机制与信任传播

TrustChain：参考其去中心化的信任管理架构，设计车辆之间的信任值传播和反馈机制。

## 3. 数据通信仿真平台

Veins+SUMO：模拟车辆与RSU的通信，测试不同信任评分下的车辆行为对数据通信的影响。

## 4. 机器学习模型的实现

Scikit-learn：用于训练和测试车辆通信行为的分类模型，检测恶意行为。

# 5. 进度安排

- 2024年10月，项目准备与需求分析
- 2024年11月，系统开发与模块实现，实现PKI身份管理层
- 2024年12月，系统开发与模块实现，实现信任管理机制
- 2025年01月，仿真与系统优化，如添加恶意节点等
- 2025年02月，系统测试与完善
- 2025年03月-结题，文档撰写与答辩准备


哈爾濱工業大學

HARBIN INSTITUTE OF TECHNOLOGY

# 请各位老师批评指正