5G 网络下车联网通信数据加密与隐私保护方法设计

赵 巍[1] 万宇菲[1] 阮聿杰[1] 焦子安[1] 毛诗雨[1]
ZHAO Wei WAN Yufei RUAN Yujie JIAO Zi'an MAO Shiyu

摘 要 目前车联网通信数据安全与隐私保护方案主要使用 TSN（time sensitive network）时间敏感网络进行终端通信验证，但是，在 5G 网络下，车辆网中离散数据过多，这种加密方式易受离散因素影响，导致加密开销过高。设计一种适用于 5G 车联网通信数据加密与隐私保护方法。针对离散通信数据问题，利用同态加密技术，在加密的过程中需要选取有效的加密随机数，根据明文的同态性质进行拆分处理，再利用密钥生成算法设置解密私钥，降低在不同加密节点的加密计算开销。在保证原始密文格式的基础上进行了加密运算，确保数据在传输过程中的安全性。设计一种适用于 5G 技术的通信数据隐私保护认证架构，可以确保通信双方的身份真实可靠，防止中间人攻击和数据泄露。在加密与保护认证架构的基础上。利用 V2V 车联网通信场景，生成车联网通信数据安全与隐私保护的优化方案。实验结果表明，设计方案的时间开销较低，同时具备强大的抗攻击能力，能够有效确保数据的安全性。

关键词 5G 技术；车联网；通信数据安全；隐私保护；安全加密

doi：10.3969/j.issn.1672-9528.2024.01.037

0 引言

车联网是一种全新的车载网络，具有自组织特性，能够实现车辆间的实时信息交流，并为车辆提供多样化的服务[1]。举例来说，车联网通过调整车辆之间的间距，有效地避免了碰撞的发生。此外，借助车联网，车辆可以与其他车辆进行通信导航，确保交通运输的可靠性[2]。然而，随着 5G 计算在车联网中不断产生大量的通信数据，通信安全性逐渐下降，隐私数据泄露的风险也变得日益严重，给经济造成了严重的损失[3-4]。因此，迫切需要设计一种适用于 5G 车联网通信数据与安全隐私保护的具体方案，来解决上述问题。

在这一方面的研究中，相关研究人员针对车联网通信数据特点设计了几种常规的车联网通信数据安全与隐私保护方案。文献 [5] 设计一种基于强化学习的车联网通信数据安全与隐私保护方案，其主要设置了资源优化模块，建立了强化学习决策进行安全评估，实现通信数据安全与隐私保护。文献 [6] 考虑数据高效分布关系的车联网通信数据安全与隐私保护方案，根据多角色的数据共享需求设置主从链路结构，进行保护单元优化，从而完成通信数据安全与隐私保护。

但大多数通信数据安全与隐私保护方案主要使用 TSN 时间敏感网络进行终端通信验证，在 5G 网络中，由于数据流量增大，易受突发网络攻击因素影响，导致验证开销过高，不符合车联网的运行安全要求，因此，设计一种针对 5G 车联网通信数据的安全与隐私保护方法。

1 车联网 5G 技术通信数据加密与身份认证方法设计

1.1 车联网通信数据安全同态加密方法设计

同态加密是一种有效的加密手段，其可以保留基础的代数结构，利用第三方完成明文密文计算[7]，因此，为了提高车联网通信数据安全与隐私保护方案的综合性能，本文设计了一种适用于车联网通信数据的同态加密协议，在保证原始密文格式的基础上进行了加密运算。同态加密可以大幅度降低车联网原始数据的泄露风险，增加数据的安全统一性。在设计车联网通信数据安全同态加密前，本文预先分析了数据的复合同态性质，给定有效的安全参数，进行公钥计算。此时针对每一个车辆数据明文产生的密文 c 公式为：

$$c=\kappa(m,r)=g\cdot r^{n}\bmod n^{2} \tag{1}$$

式中：$\kappa(m,r)$ 代表明文公钥，g 代表随机生成元，r^{n} 代表计算的密文素数，n 代表明文随机数。在上述的密文解密过程中[8-9]，可以使用指定的私钥将随机数进行同态处理，获取明文的相互作用属性，从而满足车联网通信数据的实际要求。

针对离散通信数据，在加密的过程中需要选取有效的加密随机数，根据明文的同态性质进行拆分处理，再利用密钥生成算法设置解密私钥。为了提高数据安全同态加密协议的加密效率[10]，降低在不同加密节点的加密计算开销。本文设

1. 南昌交通学院 江西南昌 330100
[基金项目] 江西省教育厅科学技术项目（编号：GJJ2203104）；江西省大学生创新训练项目（编号：S202313431006）

计的方案针对某一节点选取了一个初始的随机数，生成了数据安全同态加密协议，该协议的加密密文 c_a 公式为：

$$c_a = cm_i + H(ek_i \| r) \bmod q \quad (2)$$

式中：m_i 代表节点的明文，$H(ek_i \| r)$ 代表其他节点的加密分配密钥，q 代表最大素数，此时利用 sink 节点进行解密 [11]，获取任意节点的同态性质及加密随机数。

在 5G 车联网通信网络数据场景中，数据安全与隐私保护的难度相对较高，因此，为了提高车联网通信数据安全同态加密协议的加密效果，本文利用了高效保密余弦相似度计算了同态加密余弦值。针对给定的安全参数进行了数据保密处理，保证最终的数据同态加密协议满足隐私保护安全约束要求。在加密过程中，若存在车联网保密数据查询问题，可以预设 1-R 的数据排序编码，重新调整协议的执行过程，优化执行编码的排名，为后续的数据安全与隐私保护优化方案设置奠定基础。

1.2 5G 网络下通信数据隐私保护认证架构设计

5G 网络下通信数据隐私保护认证架构设计是为了在 5G 网络环境下，为车联网通信数据提供隐私保护。通过设计一种认证架构，可以确保通信双方的身份真实可靠，防止中间人攻击和数据泄露。因此，本文设计的方法，以 5G 技术为基础，通过有效的通信数据隐私保护认证架构来实现隐私保护。图 1 显示了该架构的示意图。

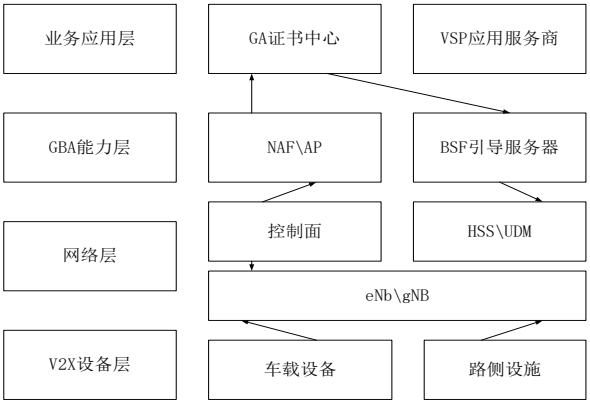

图 1 通信数据隐私保护认证架构

根据图 1，5G 车联网通信数据与隐私保护架构的主要组成部分包括业务应用层、能力层、网络层和设备层。各层扮演着不同的角色来实现数据的安全保护。以下是对各层的说明。

业务应用层：主要包括应用服务 SP，负责签发数据安全证书，并利用本地私钥完成数据的加密。在通信接口方面，业务应用层与其他层进行数据交互。

能力层：该层主要通过引导网关完成设备横纵认证，并利用专业会话密钥完成运营处理。通过建立会话通道和生成可靠的数字证书，能力层提供安全的认证和授权功能。

网络层：网络层以 5G 技术为支持，在满足可靠数据传输要求的基础上，完成无线覆盖。通过 UDM（用户数据库）完成 5G 网元的安全管理，灵活部署加密算力，提升数据安全与隐私保护方案的处理能力。

设备层：设备层作为车联网的通信技术融合点，将其作为基础表示进行安全保护绑定。设备层使用 USIM（通用 SIM 卡）进行安全运算。当数据发送时，OBU（车载单元）可以立即收发数字签证，验证消息的真伪，并使用私钥完成解密。此外，还可以使用 RSU（路侧单元）设备对通信数据进行加解密处理。车联网通信数据安全与隐私保护通信接口如表 1 所示。

表 1 车联网通信数据安全与隐私保护通信接口

接口	协议	互通网元	描述
Ua	HTTP	V2X 设备 NAF\AP	用户业务访问认证协商，转发认证交互信息
Ub	HTTP	V2S-BSF	生成 BSF 引导流程，共享 AP 密钥
Zh	Diameter	BSF-HSS	BSF 向 HSS 获取鉴权向量
Zn	Diameter	BSF-NAF\AP	NAF\AP 获取共享密钥
Ut	HTTP	NAF\AP-AS	传递交互操作信息
开通接口	SOAP	GBA-HSS	开通业务
车辆信息查询接口	HTTP	NAF-AP	查询车辆信息

由表 1 可知，在车联网通信数据安全与隐私保护方案部署的过程中，需要上述的隐私保护通信接口作支持。

1.3 生成车联网通信数据安全与隐私保护方案

通过设计的车联网通信数据安全加密与隐私保护架构，结合上述两种方法，综合考虑车联网通信数据的安全和隐私保护需求，生成一个综合的优化方案。该方案应该能够兼顾数据的安全性和隐私性，提供高效、可靠的通信服务。在常规的 V2V 车联网通信场景下，提出了对数据安全与隐私保护的优化方案。该方案根据车辆信息的交互关系，建立了具体的模型，如图 2 所示。

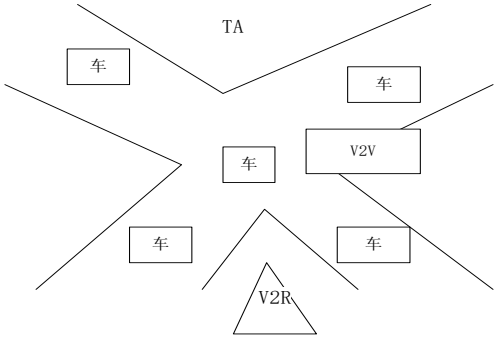

图 2 通信数据安全与隐私保护优化方案模型

从图 2 中可以得知，车联网的运维创建者（以下简称 TA）担负着重要的责任和任务。TA 可以对车联网进行同态加密处理，优化各项参数，并获取准确的密钥。此外，TA 还

能够通过设计的隐私保护框架，辨别恶意消息的发送者真实身份。具体过程如下。

通过有限信道，TA 可以完成 5G-RSU 通信，确保车联网通信数据的安全性。除了 TA 之外，车联网中还有各个车辆代表着移动节点。为了满足时间信息的无线传输需求，这些移动节点可以利用 V2V 进行通信。在通信过程中，RSU 作为路侧固定设备起到关键的作用，确保满足对恶意节点的通信追踪要求。它可以计算每个采样数据的距离，并将用户划分成不同类别组，计算式 E 为：

$$E = c_a agr \min\left\{\sum\left|x_i - a_j\right|\right\} \tag{3}$$

式中：agr 代表加密均值迭代参数，x_i 代表采样数据的距离，a_j 代表业务组别，计算加密均值迭代式 A_D 为：

$$A_D = \frac{E}{|C_D|}\sum X \tag{4}$$

式中：C_D 代表加密处理迭代次数，X 代表初级分配保障，根据上述参数，可以生成的加密动态敏感隐私保护参数 α 为：

$$\alpha = \frac{A_D}{n}\sum_{n=1}\left(Y_j \cdot \iota_n\right) \tag{5}$$

式中：Y_j 代表加密描述特征，ι_n 代表时间序列步长。

通过采用上述加密与隐私保护方案，可以最大限度地确保车联网通信数据的安全性，并降低车联网运行的风险。通过认证性、机密性、匿名性、不可链接性和消息完整性等核心特点的结合，有效保护了车联网通信数据的安全和隐私，为车联网领域提供了可靠的数据保护解决方案。

2 实验与分析

为了验证设计的基于 5G 技术的车联网通信数据安全与隐私保护方案的保护效果，本文配置了基础实验平台，将其与文献 [5]、文献 [6] 两种车联网通信数据安全与隐私保护方案对比，进行了实验如下。

2.1 实验准备

根据车联网通信数据安全与隐私保护方案验证实验要求，本文选取 Sinulator 作为仿真实验平台，随机设置了不同的数据传感器。为了降低数据暴露风险，本文将设置的传感器节点随机放置在 300 m×300 m 的空间的车辆中，将通信半径设置为 30 m，此时，可以发送不同大小的通信数据包。实验仿真模型如图 3 所示。为了提高实验的真实性，本文将 T-Drive\Roma Taxi 真实数据集作为实验数据集，其包含了不同时间段的车联网数据，且通过 GPS 生成行车轨迹。实验的采样间隔为 5 s，设置了有效的时间戳。在实验开始前，需要对原始实验数据集进行预处理，抽取不同的车联网参数组合成全新的实验数据集。此时可以配置基础实验环境：CPU 3.6 GHz，RAM 16 GB，选择 Microsoft Windows 10 作为操作系统。除此之外，本实验选择 PyCharm 开发实验程序，记录不同方案的实际开销，作为重要的实验指标，现在车辆的攻击面非常广，下面攻击面分析的图片中，每个红点都是一个安全攻击面，如图 4 所示。

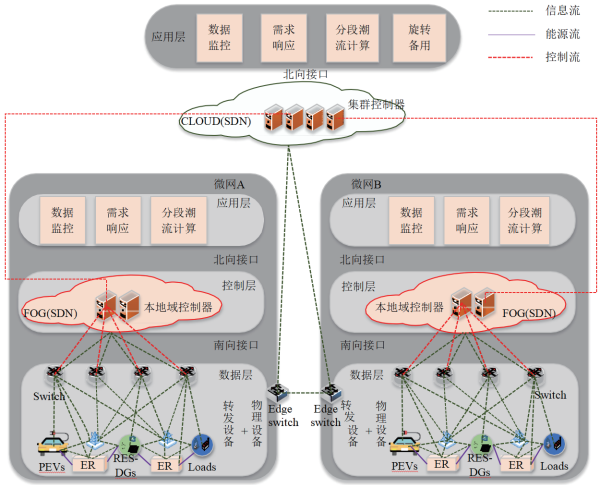

图 3 实验仿真车联网模型

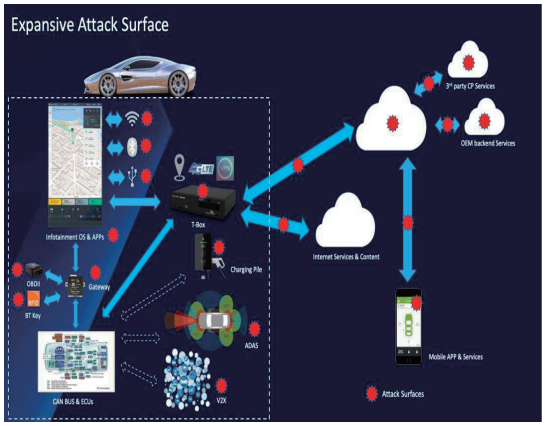

图 4 实验攻击反馈示意图

由图 4 可知，上述的实验攻击反馈过程通过传感器实时获取内部信息，发布攻击指令，再由相关的程序进行集成处理，上传攻击资源，有序地执行攻击任务，根据上述设置的实验平台，即可验证后续的通信数据安全与隐私保护实验结果。

2.2 实验结果与讨论

2.2.1 时间开销分析

结合上述的实验准备，可以进行车联网通信数据安全与隐私保护实验，即分别使用本文设计的基于 5G 技术的车联网通信数据安全与隐私保护方案，文献 [5] 基于强化学习的车联网通信数据安全与隐私保护方案以及文献 [6] 考虑数据高效分布关系的车联网通信数据安全与隐私保护方案进行通信，记录三种安全隐私保护方案在不同消息数量下的时间开销，实验结果如表 2 所示。由表 2 可知，随着消息数量增加，三种方法的验证开销也逐渐增加，但本文设计方法在批量验证和普通验证中的总体开销较小，且始终在 4.81 ms 和 6.11 ms 以下。而文献 [5] 以及文献 [6] 两种方案的开销明显较高，批量验证的时间开销最高可达 9.98 ms、10.65 ms，普通验证的

时间开销分别达到 10.98 ms、10.93 ms。上述实验结果证明，本文设计的基于 5G 技术的车联网通信数据安全与隐私保护方案的性能良好，具有一定的应用价值。

表 2 不同方法的时间开销

消息数量 / 百个	本文设计方法的验证开销 /ms		文献 [5] 方法的验证开销 /ms		文献 [6] 方法的验证开销 /ms	
	批量验证	普通验证	批量验证	普通验证	批量验证	普通验证
2	3.51	4.02	8.05	9.11	8.18	9.15
4	3.63	4.13	8.14	9.15	8.23	9.22
6	3.79	4.22	8.22	9.18	8.31	9.33
8	3.88	4.36	8.38	9.22	8.44	9.46
10	3.92	4.48	8.46	9.35	8.55	9.55
12	4.02	4.69	8.59	9.46	8.69	9.64
14	4.18	5.01	8.67	9.52	8.76	9.72
16	4.26	5.28	8.73	9.63	8.84	9.88
18	4.39	5.47	8.89	9.74	8.98	9.91
20	4.42	5.64	8.94	9.83	9.25	10.16
22	4.56	5.87	9.14	9.95	9.41	10.28
24	4.65	5.92	9.28	10.23	9.65	10.54
26	4.78	6.01	9.54	10.48	9.82	10.75
28	4.81	6.11	9.98	10.98	10.65	10.93

2.2.2 数据保护效果分析

为了进一步测试设计方法的数据安全与隐私保护能力，随机选取 T-Drive\Roma Taxi 数据集中的 100 个数据，在 DDoS 攻击下，测试三种方法的数据保护能力，为避免实验结果的偶然性，进行 5 次实验，结果如图 5 所示。

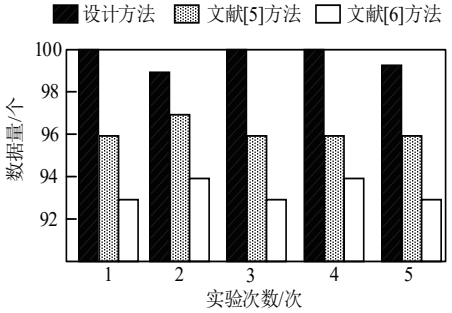

图 5 数据保护效果测试

由图 5 可知，设计方法在 DDoS 攻击下的数据量始终在 99 个以上，具有良好的数据保护能力。而文献 [5] 以及文献 [6] 方法在 DDoS 攻击下的数据量分别在 96 个、94 个左右，虽然也具有一定的抗攻击能力，但相比于设计方法而言，数据保护效果还需进一步提升。

3 结语

目前，5G 车联网内部数据的快速增长带来了不明来源的问题，这容易导致数据安全问题，严重威胁人身安全和经济损失。为解决这一问题，本文在 5G 技术下，设计了一种全新的车联网通信数据安全与隐私保护方案。实验结果表明，该方案在保障通信数据安全和隐私保护方面表现良好，且开销较低，具备有效性。因此，该方案具有一定的应用价值，为提高车联网的运行可靠性做出了贡献。

参考文献：

[1] 孙彦景 , 余政达 , 陈瑞瑞 , 等 . 车联网中基于深度强化学习的高可靠资源分配算法 [J]. 重庆邮电大学学报 (自然科学版), 2023, 35(4):706-714.

[2] 田柳 , 林黄智 , 龚光军 , 等 . 基于热度统计的车联网内容传输带宽动态分配方法 [J]. 长春工程学院学报 (自然科学版), 2023, 24(1):124-128.

[3] 郭晓晗 , 彭理群 , 马定辉 . 基于车联网 BSM 数据与路侧视频融合的港口集装箱卡车碰撞危险辨识方法 [J]. 交通信息与安全 , 2023,41(1):1-12.

[4] 李松 , 王新荣 , 王博文 , 等 . 基于随机网络演算的车联网边缘计算多跳任务卸载性能分析 [J]. 电子与信息学报 , 2023, 45(7): 2459-2466.

[5] 章航嘉 , 谢志军 . 基于强化学习的车联网隐私保护和资源优化策略 [J]. 传感技术学报 , 2022,35(8):1073-1079.

[6] 莫梓嘉 , 高志鹏 , 杨杨 , 等 . 面向车联网数据隐私保护的高效分布式模型共享策略 [J]. 通信学报 ,2022,43(4):83-94.

[7] 韦睿 , 祝长鸿 , 王怡 , 等 . 基于软件定义网络和移动边缘计算的车联网高效任务卸载方案 [J]. 计算机应用研究 , 2023, 40(6):1817-1824.

[8] 闫春 , 荆建业 , 孙晓红 , 等 . 基于改进 XGBoost 算法的 UBI 车险费率等级判定模型研究 [J]. 计算机应用与软件 , 2022, 39(10):254-258+349.

[9] 尹立强 , 张鹤杨 , 霍俊臣 , 等 . 编队行驶系统中基于 Kalman 滤波的相对定位算法研究 [J]. 河南科技学院学报 (自然科学版), 2022,50(4):71-78.

[10] 郑国峰 , 林鑫 , 张承伟 , 等 . 车联网数据的 PCA-LVQ 行驶工况识别方法与测试 [J]. 重庆理工大学学报 (自然科学), 2022, 36(6):96-104.

[11] 顾金媛 , 章国安 , 张鸿来 . 软件定义车联网中缓存辅助的 NOMA 功率分配方案研究 [J]. 计算机应用研究 , 2022, 39(8): 2459-2464+2468.

【作者简介】

赵巍（1977—），男，满族，江苏无锡人，硕士，副教授，研究方向：电子通信。

万宇菲（2003—），女，江西南昌人，本科，研究方向：电子通信。

阮聿杰（2002—），男，福建福州人，本科，研究方向：电子通信。

焦子安（2004—），男，江西南昌人，本科，研究方向：电子通信。

毛诗雨（2004—），女，浙江宁波人，本科，研究方向：电子通信。

（收稿日期：2023-09-12）