5G车联网业务发展和安全通信关键技术

王梦晓[1] 刘学军[2] 方琰崴[3,4] 牛娇红[3,4]
1 东南大学成贤学院 南京 210088
2 南京航空航天大学 南京 211106
3 移动网络和移动多媒体技术国家重点实验室 深圳 518055
4 中兴通讯股份有限公司 南京 210012

摘 要 车联网是5G行业应用发展的重要组成，驱动5G ToB应用快速发展。安全通信系统是车联网部署中不可缺失的重要环节。文章提出5G运营和车联网结合的业务规划建议，介绍5G车联网通信系统的主要组成和接口协议，分析认证和授权、生成和配置密钥、切片和QoS业务质量资源保障、隐私数据保护和加密等关键技术，展望车联网安全通信的发展前景。

关键词 5G；车联网；发展建议；安全通信；关键技术

引言

5G网络典型的业务包括uRLLC(低时延高可靠)、eMBB(增强移动宽带)和mMTC(大连接低功耗)三大类。5G不但向传统意义上的消费者提供业务，而且还能向物网和企业提供多样化的工业应用。当前，新一轮科技革命和产业变革正在全球范围孕育兴起，以5G、大数据、云计算、人工智能为代表的新一代数字技术日新月异，传统行业数字化智能化转型是大势所趋。作为新基建的核心引擎，5G在支撑社会经济数字化、网络化、智能化转型方面潜力巨大。

一方面，3GPP R17版本的标准制定在2022年Q1冻结，并对R16版本进行了架构、特性和场景方面的改进，尤其对TSN(Time Sensitive Network，时间敏感网络)特性进行了增强，如提供终端之间的内生确定性通信能力，为车联网、工业制造、智能电网等行业应用奠定了坚实的理论基础。而作为5G行业应用的抓手，车联网已经成为业界讨论的热点话题，并在商用成熟度方面愈加完善，将为人们的出行以及工业自动化创造新的价值模式[1]。另一方面，据中国汽车工程学会统计，2019年，我国汽车累计产销量为2 572.1万辆，预计2025年V2X渗透率可达50%，仅新下线V2X车辆就有1 200万辆，我国实现5G连接的汽车将达到5 030万辆，联网汽车将在2025~2030年之间持续大幅增长。车联网为电信业开拓了宽广的市场，为5G的行业发展提供了极为广阔的前景[2]。

2021年3月12日发布的《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》中，明确提出将“加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”作为发展规划之一，这对网络空间安全提出了更高的发展要求。车联网的安全部署与交通安全息息相关，而来自于网络的攻击、网络拥塞，以及复杂多变的突发路况、雨雪雾等外界因素，都会对车联网的安全通信形成较大的影响，车联网的部署需要建设成熟稳定的安全通信系统[3]。

基金项目：航空基金(2019ZA052011)；国家重点研发计划项目(2020YFB1806700)

1 业务发展切入点和规划

1.1 电信运营商的价值定位

在车联网的业务发展中，电信运营商可以根据参与程度的不同，选择不同的价值定位，来切入5G车联网的业务发展。当作为连接提供商参与车联网建设时，运营商根据SLA(Service Level Agreement，服务等级)需求，收取网络连接费用，并提供道路网络覆盖、车载模块终端、道路设施模块终端，运营商需要重点解决网络覆盖、数据时延等问题[4]。

当作为平台使能提供商时，运营商还需要提供车联网平台支持。收入构成主要包括网络接入服务、车联网应用套件费用和逐年维护费用，以及个人移动业务。车联网应用套件资费包括云平台服务费，边缘计算的流量带宽占用、计算资源、存储费用，数据中台和行业套件服务费。由于车联网各方通常会有较长的业务合作周期，运营商可以简化资费模式，按季度或按年的模式制定收费标准。

如果运营商有深入拓展车联网业务的运营计划，还可以进而作为车联网业务集成商增值车联网业务提供商。作为业务集成商参与车联网时，运营商不仅需要提供车联网平台支持，还要提供端到端的业务集成服务，如车路协同应用、智能交通、智慧公交或部分业务，并能够收取定制集成费用、周期性维护管理费用，可与合作伙伴进行收入分成；而作为业务提供商时，运营商将直接面向消费者或者企业提供服务如共享出行，并能够收取定制场景应用服务费、固定的租赁费用以及按使用需求收取服务费用。

车联网的部署需要多方共同参与，不但运营商需要深度参与，建设GBA(Generic Bootstrapping Architecture，通用引导架构)安全通信系统，而且还要涉及到汽车主机、CA安全证书系统、车载终端和路侧设备、通信芯片、安全芯片、USIM等多方面，与交通运输管理部门协作，一定程度上还要面向个人以及企业消费者，因此建议在车联网运作初期，运营商作为平台使能提供商参与车联网业务，以网联化业务为主，选择封闭受限条件下智能驾驶。在条件成熟时，逐步开展远程驾驶、车辆编队、感知共享、自动驾驶、协同控制等增强型车联网业务。

1.2 初期部署场景

车联网的部署涉及到3大类，共17种典型的应用场景，电信运营商设计和部署5G车联网通信系统时，需要充分考虑和应对以下场景。1)V2V(Vehicle to Vehicle)包括5种场景：前向碰撞预警、盲区预警、路况预测和故障车辆提醒、紧急车辆避让、左转辅助；2)V2I(Vehicle to Roadway Infrastructure)包括9种场景：车内标牌、全路段禁停预警、前方行人提醒、前方学校提醒、向右及转弯预警、禁止鸣笛预警、前方加油站提醒、红绿灯消息推送/绿波通行、弱势交通参与者提醒；3)安全机制验证包括3种场景：伪造红绿灯防御、伪造紧急车辆防御、异常行为检测。

在业务开展初期，5G车联网通信要涵盖这些场景的需求，确保交通出行安全。

1.3 中长期规划

从长远发展来看，伴随着人工智能AI的引入，未来5G车联网安全通信将构建基于自动化、自防御、自适应、自调整的内生安全技术体系，对5G多接入技术进行协同[5]，把安全能力拆分到原子能力，建设安全大脑，基于SDS(Software Defined Security，软件定义安全)实现安全服务链编排，充分利用威胁情报，构建“防御、检测、响应、预测”的自适应安全体系。引入可信计算技术，实现5G车联网各构件的可信启动、可信度量，以及对各组成部分的远程可信管理，为网络基础设施提供主动防御能力。最终在云网融合的基础上，提供面向车联网提供的安全能力及服务。而随着代表着新突破与革新的5G-Advacned引入，5G能力锻强补弱，网络的高速率、大带宽和低时延的特性也将为车联网带来新的发展机遇，打造新的发展模式。

2 5G车联网通信系统的组网和接口

2.1 组网架构

如图1所示，5G车联网通信系统主要包括了V2X设备层、通信网络层、GBA能力层和业务应用层。

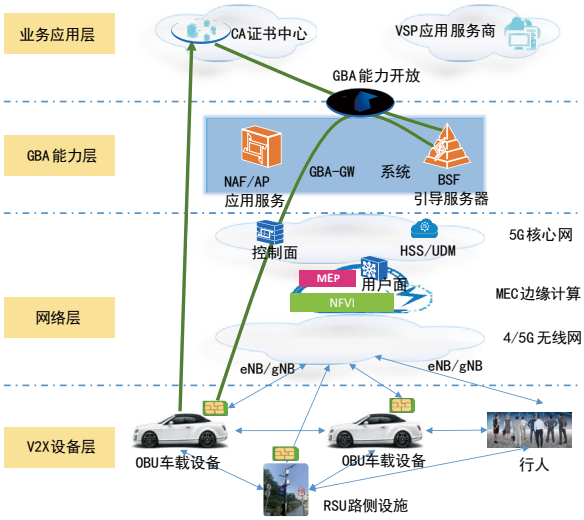

图1 5G车联网通信系统的组网架构

V2X设备层提供5G与V2X车联网技术融合点，以手机号作为设备标识，提供在线绑定，并以USIM为基础完成安全运算。OBU(On Board Unit，车载设备)安装在车辆上，负责V2X通信的实体。数据发送时，OBU使用CA签发给它的数字证书对其播发的信息进行数字签名和/或使用数据接收方证书对数据进行加密；数据接收时，OBU使用发送方的公钥对消息进行验证，同时可使用本地私钥对加密消息进行解密；RSU(Road Side Unit，路侧设备)安装在路侧交通控制设备和交通信息发布设备中，负责V2X通信的实体。数据发送时，RSU使用CA签发给它的数字证书对其播发的信息进行数字签名和/或使用数据接收方证书对数据进行加密；数据接收时，RSU使用发送方的公钥对消息进行验证和/或使用本地私钥对加密消息进行解密。

通信网络层提供4/5G信号覆盖及可靠数据传输服务，包括4/5G无线覆盖、MEC边缘计算平台、5G融合核心网。5G的网元包括UDM (Unified Data Management，统一用户数据管理)、PCF(Policy Control Function，策略控制功能)、AMF(Access and Mobility Management Function，接入和移动管理功能)和SMF(Session Management Function，会话管理功能)等在中心DC部署，而UPF(User Plane Function，用户面功能)在边缘DC部署[6]。MEC边缘计算平台下沉用户面算力，实现算力的灵活部署，提升车辆应对复杂路况的处理能力。

GBA-GW(Generic Bootstrapping Architecture Gateway，通用引导架构网关)提供开放的GBA安全能力，从5G网络获取认证向量认证V2X设备，生成“一事一密”专用会话密钥供上层使用。GBA-GW安全系统中包含BSF(Bootstrapping Server Function，引导服务器)和NAF/AP(Network Application Function，网络应用功能)，对于BSF部署在运营商网络，NAF/AP可以部署在运营商网络，或与应用服务器共同部署。GBA与V2X设备完成双向认证后，传输应用层会话密钥到应用服务器。V2X设备与应用服务器采用应用层会话密钥建立安全通道，并获取数字证书。

业务应用层包括CA(Certificate Authority，证书管理机构)中心和应用服务SP(V2X Service Provider，应用服务提供商)，向设备签发V2X数字证书。CA中心负责向车联网设备(OBU、RSU、VSP)签发各种通信证书，或签发证书撤销列表(Certificate Revocation List，CRL)，例如注册CA、应用CA、证书撤销机构(Certificate Revocation Authority，CRA)等。VSP(V2X Service Provider，服务提供商)负责道路交通的管理机构和在车联网系统里提供某种商业服务的服务机构。数据发送时，VSP使用CA签发给它的数字证书对其播发的信息进行数字签名和/或使用数据接收方证书对数据进行加密；数据接收时，VSP使用发送方的公钥对消息进行验证，同时可使用本地私钥对加密消息进行解密。VSP需要通过具有转发能力的路侧设备进行安全消息的发送和接收[7]。

2.2 接口协议

如表1所示，是车联网通信系统的主要接口以及通信协议。

表1 车联网通信涉及的主要接口

接口	协议	互通的网元	描述
Ua	HTTP	V2X设备—NAF/AP	用于用户业务访问认证方式的协商，用于用户业务访问交互操作信息的认证和转发
Ub	HTTP	V2X设备—BSF	UE与BSF之间的接口，实现UE与BSF之间引导流程的运行，生成UE和BSF的共享密钥，生成UE和NAF/AP的共享密钥
Zh	Diameter	BSF-HSS	BSF向HSS获取用户鉴权向量和签约信息
Zn	Diameter	BSF—NAF/AP	NAF/AP向BSF获取UE和NAF/AP的共享密钥
Ut	HTTP	NAF/AP—AS	用户业务访问交互操作信息的传递
开通接口	SOAP	GBA业务管理平台—HSS	业务开通
车辆信息查询接口	HTTP	GBA业务管理平台—NAF/AP	查询车辆信息

在车联网部署中，需要对这些接口进行充分联合调测，并根据网络的实际状况进行优化。需要对V2X网络层、消息层、安全层协议进行一致性测试，涵盖前向碰撞预警、交叉路口同行、闯红灯预警、道路危险状况提示、弱势交通参与者预警等典型应用场景，达到高稳定性和最优的部署性能[8]。

3 5G车联网安全通信关键技术

3.1 认证和授权

车联网的安全通信中，首先要考虑对V2X设备进行认证和授权，并与证书机构进行交互，确保设备能够顺利接入系统。

如图2所示，是车联网安全通信的认证流程。首先，V2X设备与GBA系统交互。如果V2X设备没有有效的GBA共享会话密钥，V2X设备接入GBA认证授权系统，发起认证授权请求；GBA认证成功后向V2X设备返回认证授权响应。BSF负责对V2X设备进行身份认证并向NAF/AP提供GBA密钥，NAF/AP负

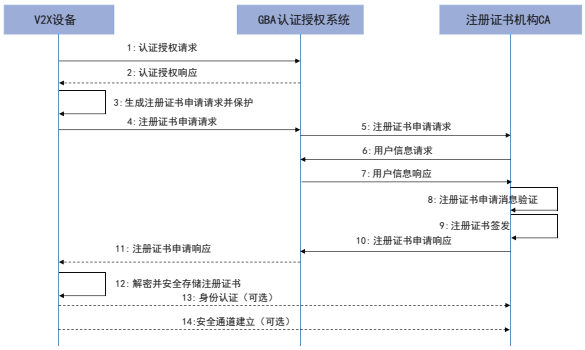

图2 5G车联网安全通信认证流程

责产生多个GBA共享会话密钥供ECA使用；V2X使用USIM生成的GBA共享会话密钥K1和K2对EC申请请求消息进行加密和完整性保护；V2X设备通过GBA认证授权系统向ECA发送经过保护的注册证书申请请求消息。

进入GBA与CA证书机构交互阶段后，GBA认证授权系统根据ECA服务器域名信息向ECA转发注册证书申请请求；ECA向GBA认证授权系统申请获取GBA共享会话密钥及用户信息；GBA认证授权系统生成GBA共享会话密钥K1、K2、K3、K4，并向ECA返回用户信息；ECA审核注册证书申请请求，通过后签发EC注册证书；ECA使用GBA共享会话密钥K1和K2对EC注册证书进行加密和完整性保护。

接下来，ECA通过GBA认证授权系统向V2X设备发送注册证书申请响应消息，应答成功。消息中包含签发并经保护的EC注册证书；GBA认证授权系统向V2X设备转发注册证书申请响应消息，应答成功；V2X设备请求USIM使用K1和K2对消息进行完整性保护校验和解密，并将EC注册证书安全存储；基于GBA共享会话密钥K3，ECA与V2X设备可选进行双向身份认证。

最终，基于GBA共享会话密钥K4，V2X设备与ECA之间可选建立安全通信通道，如TLS、应用层加密等，用于数据端到端的安全传输[9]。如果已经生成有效的GBA共享会话密钥，V2X设备也能够发起查询密钥和推送密钥的相关流程。

3.2 密钥生成和配置

V2X数字证书需要采用在线安全配置，提供“一事一密”的专用会话密钥，确保远程配置的安全性，才能顺利进行认证和授权。在这个过程中，用户OBU发起安全认证请求，与GBA系统间建立安全认证通道，GBA安全网关对设备真实身份进行认证。认证通过后，OBU通过GBA系统，向CA证书中心传递认证结果，验证密钥。随后，OBU从CA中心下载证书，不同的OBU之间利用合法证书实现安全通信[10]。

车联网的典型密钥生成，应遵循统一的生成规则：K(i) = KD Fnuction(Ks_int_NAF，字符串，B-TID，UE标识，应用服务标识)，其中i =1~5。

1)KD Function是密钥生成算法，采用国家密码管理局规定的商用密码算法实现，生成长度为128bit的会话密钥。

2)参数“Ks_int_NAF”是在USIM与NAF/AP间共享的GBA密钥，基于GBA_U方式产生。如表2所示，是NAF/AP生成的应用层会话密钥种类以及建议其所对应的参数“字符串”取值。

表2 密钥种类和对应的“字符串”参数取值

GBA应用层会话密钥	“字符串”参数取值	密钥功能
K1	V2X_Enc	证书请求/响应消息加密
K2	V2X_Int	证书请求/响应消息完整性保护
K3	V2X_Auth	V2X设备-CA服务器双向身份认证
K4	V2X_E2E_Sec	端到端安全通道建立
K5	V2X_ID_Sec	V2X设备用户身份隐私保护

3)参数“B-TID”是GBA引导事务标识，参数“UE标识”是V2X设备的标识IMPI，参数“应用服务标识”是CA服务器的FQDN域名，该域名全局唯一。

当前，业界普遍认为，基于QKD(Quantum Key Distribution，量子密钥分发)的安全服务成为保障数据安全的有效手段。QKD具有密钥协商、高熵值随机数等特性，可防止数据被破译、窃取。因此，在5G车联网通信系统架构中引入云化量子安全服务的中间件，可构建“云—网—端—用”全栈技术创新的量子可信云平台和一体化量子安全防护体系，为加密密钥提供生命周期管理，引入使用量子安全加密的TLS(Transport Layer Security，传输层安全)连接功能，在密钥生命周期管理中保护数据，进而形成量子虚机/容器/网盘/云桌面和量子信息加密传输等应用保障，提供量子安全云服务和信息的安全托管。

5G车联网终端安全配置方案结合了安全通信机制与V2X数字证书管理流程，用户只需要“一键触发”在线配置V2X设备，操作简单，能够有效实现V2X数字证书的在线安全配置。

3.3 切片和QoS保障

网络切片将5G网络进行逻辑划分，从逻辑上隔离资源和服务，把一个物理网络虚化出多个逻辑上的虚拟切片网络。不同等级的业务数据可以在不同逻辑层面的网络切片上传输，满足不同业务场景对网络的数据传输速率、安全性、可靠性等多方面的差异化需求。

如表3所示，车联网业务是综合性业务，不同场景对5G切片的需求也不同。

表3 车联网的5G切片部署方案

业务类型	业务场景	服务等级	5G切片类型部署
车对车V2V	碰撞告警，车队行驶等，安全距离制动等高精度协同业务	时延低于5毫秒，可靠性达到99.999%	部署V2X与uRLLC、mMTC切片组合[11]，结合MEC部署
车对基础设施V2I	信号灯预警，道路车速引导，道路流量优化等交通效率类业务		
车对行人V2P(Vehicle to Pedestrian)	路侧异常告警，行人告警等交通安全类业务		
车对网络V2N(Vehicle to Network)	高精度地图下载和导航，信号灯配时提醒等	带宽100M至1Gb/s	部署V2X与eMBB切片组合

运营商通常会结合切片ID和5QI(5G QoS Identifier，5G QoS标识符)对切片进行业务调度。此时，切片及切片内的业务会共享基站PRB资源。如果业务在抢占PRB(Physical Resource Block)资源过程中产生冲突，则根据5QI的优先级来调配资源[11]。

车联网业务涉及到交通安全和高度协同，比如交叉路碰撞预警、前后车事故预警、路侧异常预警以及车队编队行驶、远程遥控驾驶等，电信运营商需为

此类业务分配超高优先级切片并为其预设固定的PRB资源。预设的资源可以确保此类业务能够得到最高优先级资源并独享该资源，同时得到严格的安全隔离保障，从而确保低于5毫秒的时延和99.999%的高可靠性。而对于其他非紧急类业务如高精度地图下载、周边服务信息推送等，仍采用常规的切片共享PRB调度方式，所有切片共享资源[12]。

切片和PRB结合并统一管理的方式，既确保了车联网的业务要求，又提升了系统资源利用率[13]。运营商还可以引入动态保守调度、预调度增强、基于时延的调度等算法，完善调度编排[14]。

3.4 隐私数据保护和加密

在车联网场景中，V2X的用户、业务及网络多方数据会频繁交互，各个数据域较独立。OBU客户端在进行原始数据处理时，一方面会在本地进行训练和优化，另一方面也可能会对模型参数/梯度进行加密，随后通过GBA-GW上报到VSP服务器端。VSP对客户端的模型参数作分类、聚合，进行模型训练和不断迭代优化，并将训练好的模型下发给OBU。网络中可能会存在着漏洞和攻击的风险，因此需要重点加强隐私数据保护和加密[15]。

在5G车联网通信中，模型训练采集的数据涉及OBU车载设备、RSU路侧设备、5G无线、云核心网、VSP服务提供商等多种跨域设备，有必要引入如图3所示的基于联邦学习的5G车联网安全通信系统，以解决数据跨域互通时的数据隐私保护。

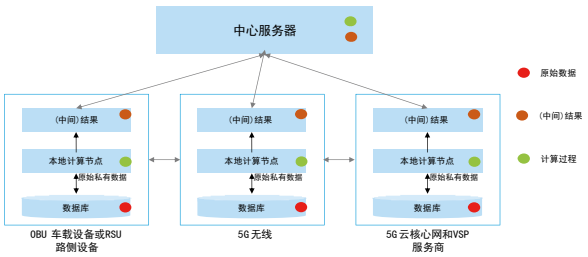

图3 基于联邦学习模型的5G车联网通信

联邦学习是一种机器学习模型[16]。电信运营商设中心服务器，在该服务器协调下，多个客户端互相合作，即使数据分散在客户端也能得到一个完整的机器学习模型。在传统的分布式机器学习模型中，客户端受服务端的指令，用户并不完全拥有数据控制权，而在联邦学习模型下，用户对设备和数据有绝对控制权，实现用户的隐私数据保护[17]。

如图4所示，基于联邦学习模型的5G车联网数据特征既可以是横向跨域的，如在OBU车载设备和RSU路侧设备、5G无线、5G核心网之间，也可以是纵向贯穿某个域的[18]。

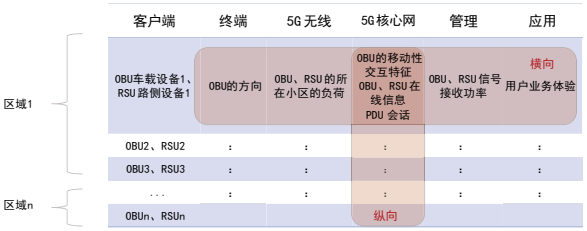

图4 基于联邦学习模型的5G车联网数据特征

可以考虑结合加密技术，常用的有安全多方计算、同态加密、差分隐私等。安全多方计算技术能够解决互不信任的参与方各自持有秘密数据，系统计算一个既定函数的问题，关键技术有秘密共享、不经意传输、混淆电路、隐私集合求交集等，以在纵向联合学习中采用隐私集合求交来对齐数据，实现梯度计算过程加密；同态加密是一种特殊的加密算法，允许对加密之后的密文直接进行计算，且计算结果解密后正好和明文的计算结果一致，用于保护计算过程，也可以用于梯度计算过程加密；差分隐私则基于建模结果在信息中添加“噪声”，这使攻击者无法从建模结果反推训练样本，解决单个查询的隐私保护问题。

电信运营商牵头部署联邦学习模型并结合这些加密技术，能够实现5G车联网相关的用户隐私数据的保护，以及对于原始数据、计算参数、计算过程的全方位加密。

3.5 基于机器学习的迭代优化

车联网涉及的环境复杂多变，已有的三大类17种场景不断发生变化，这17种场景的组合也会衍生出多种新

的场景。尽管在UDM放号签约及PCRF下发策略阶段都可以对车联网业务赋予高优先级定义，但与前向碰撞预警、紧急车辆避让等业务相比，路况预测、前方加油站提醒、高精度地图下载和导航这样的业务不需要设置同样的高优先级。因此在确保5G车联网安全通信QoS业务质量保障基础上，为了提升5G网络的引用效率，有必要引入机器学习能力，通常可以考虑部署K均值聚类算法(k-means clustering algorithm)，实现自我学习和优化。

这是一种典型的迭代求解的数据挖掘算法，处理者将数据分为K组，则随机选取K个对象作为初始的聚类中心，然后计算每个对象与各个种子聚类中心之间的距离，把每个对象分配给距离它最近的聚类中心。聚类中心以及分配给它们的对象就代表一个聚类。每分配一个样本，聚类的聚类中心会根据聚类中现有的对象被重新计算。这个过程将不断重复直到满足某个终止条件。终止条件可以是没有(或最小数目)对象被重新分配给不同的聚类，没有(或最小数目)聚类中心再发生变化，误差平方和局部最小[19]。

按照业务价值、对QoS业务保障的要求，假设把5G全网用户的实时采样数据分为4类，“高价值、需高QoS保障”如紧急车辆避让和前方行人提醒业务，“低价值、需高QoS保障”如路况预测和道路流量优化业务，“高价值、可低QoS保障”如红绿灯消息推送和绿波通行业务，“低价值、可低QoS保障”如道路周边加油站、旅游商圈信息推送业务，分别定义为4个组(Group1,Group2, Group3,Group4)，计算每个采样数据x和聚类中心a间的距离，并将其分到距离最小的聚类中心所对应的类别组Group里面，最终可以把用户分为4个类别组。

$$agr\min\{\lambda\sqrt{\sum_{i=1}^{n}\left|X_i-a_j\right|^{\lambda}} \tag{1}$$

为了简化处理，可取值λ=2，针对得到的每个类别组Group，重新计算该组的聚类中心作为新的均值点，进行新的迭代。

$$a_j=\frac{1}{|c_j|}\sum_{i\in c_j}X \tag{2}$$

在条件允许的情况下下，可以取值λ为3以及其余数值，并设置迭代次数、最小平方误差、簇中心点变化率等条件作为终止条件进行判断，不断进行收敛，最终识别出“高价值、需高QoS保障”的用户数据、行为特征和场景，并快速分配高优先级的QoS保障。对上述5G用户的类别组再次细分，即把K进一步扩大，则可以进一步细分，但这也对于5G车联网中心服务器、边缘计算中心的处理能力和带宽提出了更高的要求。

与车联网相关联的多数场景都可以归类为此种类别Group，当机器学习模型预测到5G网络可能会产生拥塞时，则由必要提前资源重分配并进行灵活调度。一方面考虑申请调度新的虚拟化资源确保车联网场景得到资源保障，设置合理的生命周期保证结束后释放资源；另外一方面可以将其他Group组别业务进行迁移，将“低价值、需高QoS保障”业务的用户迁移到5G低频段，将“高价值、可低QoS保障”“低价值、可低QoS保障”业务的用户迁移到4G网络上，实现用户无感知迁移。

经过验证，在采用了QoS增强以及迭代优化的机器学习改进算法后，5G车联网安全通信实现提高网速、超可靠、低时延通信的目的。在测试的环境条件下，当自动驾驶的汽车速度为60公里/小时，指令紧急制动时延为5.2毫秒，指令紧急制动距离大约8.5厘米。超可靠性达到六个九，即99.9999%，低时延最快可以实现5毫秒以内的端到端，基本满足我国城市一般环境下无人自动驾驶的高可靠通信要求，并同时满足密钥生成、配置和隐私数据保护的安全通信要求。

4 结束语

当前提供车辆出行的第三方管理平台种类比较多，车辆厂商也有较为固定的合作方。电信运营商需尽早开拓合作领域，与业务应用层的诸多合作伙伴进行多层次、多方面的探讨，发挥自身技术平台优势，激活

5G算力下沉到边缘DC的效能，筑牢云边一体化可信防护，为用户提供可靠的通信途径，利用全面的车联网解决方案，引领自动驾驶和车路协同的发展。

参考文献

[1] 汤立波.车联网产业发展分析[J].中兴通讯技术,2020,26(1):56-59

[2] 宋蒙,刘琪,许幸荣,等.C-V2X技术在智能网联行业中应用探讨[J].中兴通讯技术,2020,26(1):60-63

[3] Wai CHEN,李源,刘玮.车联网产业进展及关键技术分析[J].中兴通讯技术,2020,26(1):5-11

[4] 李立平,孙彪,方琰崴.5G运营的商业模式分析[J].信息通信技术,2019,13(S1):16-21

[5] 牛娇红,方琰崴,郑兴明,等.基于AI算法的5G多接入协同方案及关键技术[J].移动通信,2022,46(1):67-71,83

[6] 3GPP TS23.501 5G; System Architecture for the 5G System, (16.3.0) [S]. 2019

[7] 罗薇,汪梦珍,许玲.车联网高层协议关键技术[J].中兴通讯技术,2020,26(1):35-39

[8] 张海霞,刘文杰,薛彤,等.基于车辆行为分析的车联网超可靠低时延通信关键技术[J].中兴通讯技术,2020,26(1):12-18

[9] 付思雨,姜之源,张舜卿.基于C-V2X直连通信的车辆编队行驶性能优化[J].中兴通讯技术,2020,26(1):30-34

[10] 方琰崴,陈亚权.基于虚拟化的电信云网络安全解决方案[J].移动通信, 2018,42(12):1-7

[11] 方琰崴,陈亚权,李立平,等.5G网络切片解决方案和关键技术[J].邮电设计技术,2020(3):70-74

[12] 方琰崴,李立平,陈亚权.5G 2B专网解决方案和关键技术[J].移动通信,2020,44(8):1-6

[13] 方琰崴.5G网络切片的管理和运营支撑[J].信息通信技术,2020,14(6):63-67,73

[14] 张杰.C-V2X与智能车路协同技术的深度融合[J].中兴通讯技术,2020,26(1):19-24

[15] 中国信息通信研究院安全研究所. 2020年网络安全威胁信息研究报告(2021年)[R]. 2021

[16] 微众银行人工智能部. 联邦学习白皮书2.0 [R/OL]. 2020

[17] 3GPP TR 23.700-91, Study on enablers for network automation for the 5GS; Phase 2, (17.0.0) [S].2020

[18] 3GPP TS 23.288, Architecture enhancements for 5G System to support Network Data Analytics Services, (17.2.0) [S].2021

[19] Polykovskiy,D,Novikov,A. Bayesian Methods for Machine Learning[J].Coursera and National Research University Higher School of Economics.2018

作者简介

王梦晓

硕士，东南大学成贤学院讲师，主要研究方向为电信云与核心网的组网和关键技术、移动网络和移动多媒体技术等，发表论文十几篇，获三项发明专利。

刘学军

博士，南京航空航天大学计算机学院教授，中国计算机学会生物信息学专委会委员，江苏省人工智能学会模式识别专委会委员，江苏省生物信息学专委会委员，《数据采集与处理》编委，主要研究方向为机器学习及应用，已发表学术论文60余篇。

方琰崴

硕士，高级工程师，主要研究方向为NFV/SDN云核心网的架构演进、5G核心网的关键技术、云原生等。发表论文六十余篇，获授权发明专利十余项。

牛娇红

硕士，高级工程师，主要研究方向为5G、6G新技术预研，包括网络智能化、数字孪生、意图网络、电信云原生等，发表论文10余篇。

5G IoV Services Development and Key Technologies of Security Communication

Wang Mengxiao[1]
Liu Xuejun[2]
Fang Yanwei[3,4]
Niu Jiaohong[3,4]

1 Southeast University Chenxian College, Nanjing 210088, China
2 Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
3 State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China
4 ZTE Corporation, Nanjing 210012, China

Abstract Internet of Vehicles is an important component of 5G industry application development, which drives the rapid development of 5G ToB applications. The secure communication system is an indispensable part of the Internet of Vehicles deployment. This paper puts forward the service planning suggestions of the combination of 5G telecom operation and IoV, describes the main part and interface protocols of the 5G IoV communication system. It analyzes key technologies such as authentication and authorization, key generation and configuration, slicing and QoS service quality resource guarantee, and privacy data protection and encryption. It forecasts the prospect of IoV secure communication.

Keywords 5G; Internet of Vehicles; Development Suggestions; Secure Communication; Key Technologies