# 智能汽车:隐私与安全如何取舍

■本报记者 袁一雪

“近日,马斯克坦承特斯拉汽车内摄像头可以监视驾驶员一事,引发了车主对智能汽车内部安装摄像头与窃听器的不满。虽然这两种设备在智能汽车生产厂商眼中起到的是对驾乘人员的保护作用,但依然无法打消车主心中的疑虑。

智能汽车逐步发展,无人驾驶也在“路上”。未来,如何兼顾驾乘人员的安全与隐私,是个值得探讨和重视的问题。

日前,国外有用户在社交网站向特斯拉CEO埃隆·马斯克询问特斯拉的车内摄像头是否可以检测车主目光,马斯克回复“是的”。引发舆论关注的原因是,这是特斯拉方面首次承认通过车内摄像头来监视驾驶员。

在该用户提出疑问前,马斯克就曾在社交网站上发文称将收回一些车主的完全自动驾驶能力测试版(FSD beta)的试用权限。原因是这些车主在使用FSD beta功能时,没有对道路情况给予足够的关注。马斯克称,之所以是beta版本,就意味着还处在测试阶段,尽管目前没有出现任何事故,但不能放任不管。

显然,自动驾驶将赋予智能汽车更多权利,也意味着汽车内外需要加装更多传感器、摄像头和监听器等。但不论哪种设备,都对汽车内部相对隐秘空间内的驾乘人员隐私造成了威胁。

### 是监视还是保护

这不是特斯拉第一次曝出信息安全丑闻。去年,一位白帽黑客格林曝光特斯拉的车载计算机系统可能会导致个人隐私的泄露。接触过特斯拉的人都知道,特斯拉的车载计算机系统功能繁多,包含收音机、蓝牙电话、上网、玩游戏等。驾乘人员还可以通过Wi-Fi连接社交网站,甚至能存储联系人的电话号码。

但很多车主没有想到的是,暗藏在车载计算机系统屏幕背后的组件,正成为隐私数据泄露的源头。这位白帽黑客从某购物平台上购买到被换下来的自动辅助驾驶系统(AP)和媒体控制单元(MCU)。尽管这些组件已经有明显损坏迹象,但仍能从中获得之前车主的隐私,例如手机连接的电话本、通话记录、日历、家庭和工作地点的定位、导航去过的位置,以及允许访问网站的会话cookies。

之所以可以从MCU上获取个人信息,是因为特斯拉基于Linux内核搭载MCU。MCU使用的是镁光生产的嵌入式多媒体控制器(eMMC)存储颗粒,而特斯拉的车机系统并没有对这块eMMC硬盘进行任何的加密处理。

不仅是特斯拉,蔚来汽车“监控每位车主行程”也曾在网上闹得沸沸扬扬。此外,滴滴打车也为了确保驾乘人员安全,采取全程监听车内人员对话的措施。

尽管这些安装监听、监视设备的生产方打着“向善”的旗号,却往往没有明确告知消费者他们将会被收集哪些信息;亦无人知晓,这些信息是否真的会被妥善安全地保存。

而在信息技术飞速发展的现代,将安全性让渡给驾乘人员的隐私真的可行吗?前段时间,货拉拉公司货车女乘客跳车一事余温未了。社会上不乏对货拉拉公司为何不在车内安装监控系统的质疑之声。

安全与隐私应如何兼顾?在福州大学数学与计算机学院教授陈德旺眼中,安全与隐私是互相矛盾的名词。“想要获得更多安全性,就需要让传感器采集更多的数据。”

### 法规不应缺席

“目前,智能汽车要协助驾驶员对车辆进行控制时,主要采集驾驶车周边的车及所在道路场景的实时数据,例如前后左右车的位置、类型、速度,交通标志、道路线、障碍物等。而实现无人驾驶,只需要对车外进行监控即可。”中国科学院自动化研究所研究员王飞跃在接受《中国科学报》采访时解释道,“监控车内主要是为了对驾驶员采取主动安全措施,即发现驾驶员出现疲劳驾驶、视线漂移、不系安全带等危险行为时,进行主动提醒。目前,尚没有对监控范围和清晰度有明确的统一标准。”

诚然,伴随着人工智能的发展,关于人工智能伦理的讨论从未停歇,但讨论主题却一直集中在讨论可能性和对未来影响的理论工作,而对人工智能实际应用的研究则探讨较少。因此,学术界对人工智能伦理道德的关系进行探讨虽已持续了数年,却并没有弄清普遍的人工智能伦理到底是什么。

“人工智能在当代广泛应用,带来了各种益处,但人们也发现了诸多伦理问题。直接与技术相关的,包括算法歧视、侵犯隐私等技术的误用和滥用等,较为间接和远期的则有就业问题、平等、家庭和社会关系的危机等。”中国人民大学法学院副教授郭锐告诉《中国科学报》。

就这点而言,智能汽车对隐私构成的威胁似乎并没有上升到这一高度。“从安全隐私角度以及自动驾驶及车内主动安全的技术实现上,采集的数据都是可以实时处理、实时做出自动驾驶行为,不需要保留任何数据的。这和现有车的倒车影像的逻辑是一样的。”王飞跃坦言,“但是,不排除部分厂商为了不断提升自动驾驶及主动安全的技术能力,以及识别能力,而保留部分数据,进行算法的再学习。如果能征得用户授权同意,未尝不可。”

陈德旺也建议,车企最好将车内安装设备与收集哪些信息标注清楚,让车主保留选择的权利。“有些车主认为汽车安全比隐私更重要,就可以选择让智能后台对其信息进行收集。也有车主认为车内是隐私空间,那么可以选择减少收集内容,或者适当关闭一些功能。”

对此,郭锐认为,人工智能的决策则必须按照人类的伦理来评估和校正;人工智能对社会的影响很大,牵涉很多的人,因此应当更加强调归责性。“就车内检测技术如何与隐私保护平衡的问题,我认为可以从两个维度进行考量。第一,应该遵循知情同意原则,采取‘事前告知’‘事后删除’的模式;第二,立法应对何时收集、收集到何种程度、保存期限多久等问题做出规定,并要求商业主体定期审核。”

### 人工智能的尺度

“人工智能技术确实存在两面性,在带来驾驶安全性提升的同时,如果不加限制,确实也会带来侵犯隐私的隐患。但是解决方案提供商以及车厂,很容易通过法律和标准来约束产品和服务的隐私程度。例如,最关键的是要求不能留存数据、不能定位,这就解决了绝大部分的隐私问题。”王飞跃表示。

目前,人工智能和自动驾驶业内有分布式(联邦)数据共享、多方(联邦)数据智能计算等技术,也取得了初步的进展,能达到“数据可用不可见”的效果。王飞跃解释说,从技术上来讲,这种模式所形成的算法,与将数据聚集在一起计算训练的效果相同或者相近,从而能比较好地平衡数据隐私版权保护、数据要素开放共享服务两者之间的矛盾。正因如此,预计“数据可用不可见”是数据应用服务的未来趋势。

郭锐也表示,智能汽车收集的数据传统上被看作隐私问题。实际上,这个问题和传统隐私权语境有所不同。不同之处在于,它不是一个一方侵权、另一方被侵权的零和游戏,还展现了车主和汽车企业之间通过合同彼此信任、合作的一面。因此,个人信息保护在这个问题上可能比隐私权保护更加切合实际。

而且,相较于智能汽车驾乘人员隐私问题,网络隐私暴露更值得关注。“在技术上,科学研究者和业界也在探索是否可以达到利用数据的同时保护隐私的效果。在治理上,我们还应该支持市场的自治,企业之间的互相竞争某种程度上能够促进用户隐私的保护。比如在搜索引擎的竞争上,一些搜索引擎会以推出更加保护隐私的服务吸引消费者。”郭锐说,其实,人工智能发展过程中遭遇的最根本的伦理难题是创造秩序危机。创造秩序危机,简而言之,是人所创造的技术对人的反噬。反思人工智能伦理,是为了应对这个危机。伦理不是为了约束科学发展,而是为了防止我们在追求某一个具体目标的时候伤害人类的整体利益。

## 速递

### 俄首个可进行太空行走机器人进入研发阶段

**本报讯** 3月27日,俄罗斯国家航天集团旗下的中央机械制造研究所(TsNIIMash)和“能源”火箭航天集团公司,宣布开始研制俄罗斯第一个可进行太空行走的人形机器人“Teledroid”。不同于拥有类似人体身体结构和活动关节的“费多尔”,“Teledroid”的外形将取消双腿,仅保留躯干及以上部分。该机器人将安装在国际空间站的一个机械臂上以保证有广泛的移动范围。它可以通过舱内航天员实时操控,使用动作传感器捕捉,也具备独自工作的能力。 (原鸣)

### MIT开发收集信息软体机器人算法

**本报讯** 日前,麻省理工学院(MIT)的研究人员开发了一种新型的神经网络结构,既能优化传感器的位置,又能学习如何有效地完成任务,帮助工程师设计出能够收集更多周围环境有用信息的软体机器人。基于他们开发的算法,软体机器人体内的传感器得到了优化,因此能更好地在环境中感受自身、与环境互动。

相关论文《软体机器人任务与传感器布置的协同学习》将在2021年4月的软体机器人国际会议上进行展示。 (袁一雪)

### 柔性可穿戴器件供电系统评价指标出炉

**本报讯** 电池续航能力有限是当前制约可穿戴设备普及的重要因素,而柔性、绿色和可持续的能量供应仍存在技术瓶颈,评价指标体系也有待完善。针对这一问题,来自西南大学和西南交通大学的科研团队通过跨学科合作,对热电、运动及无线电波等能量源在可穿戴器件上的应用进行研究,首次提出了柔性可穿戴器件供电系统的评价指标,用于对柔性可穿戴系统的电源性能、能量转换机制、弯曲或拉伸条件下的功率折减等进行评估。

审稿专家认为,这项研究成果代表了未来柔性可穿戴器件供电系统的研究重点和发展趋势。研究提出的评价指标,有助于未来根据智能家居、人体健康监测、土木基础设施检测等不同应用场合需要对可穿戴设备的电源进行选型,从而推进可穿戴设备的设计标准化和产业化进程,进一步提高供电智能化水平。相关研究成果日前发表在国际学术期刊《能源与环境科学》上。 (原鸣)

# 搬开毫米波技术商用“绊脚石”

■本报记者 秦志伟 通讯员 唐瑭

毫米波频段正成为宽带卫星通信、5G移动通信发展的“黄金”频段,但如何解决毫米波无线通信传播距离受限问题成为一大难题。

科学家发现,大规模相控阵是解决这一难题的核心关键技术,但传统毫米波相控阵因该类芯片成本高且难以实现系统单片集成,又成为其大规模商业化的“绊脚石”。现在,东南大学研究团队攻关6年,踢开了这一“绊脚石”。

“我们探索出基于CMOS工艺和PCB工艺的大规模集成相控阵解决方案,具有超高集成度、超低成本等特点。”东南大学移动通信国家重点实验室主任、网络通信与安全紫金山实验室首席科学家尤肖虎告诉《中国科学报》。

近日,这项研究成果入选了2020年度“中国高等学校十大科技进展”。不久前,该成果还曾入选*Light: Science & Applications*与科学网评选出的“2020中国光学领域十大社会影响力事件”,并被评价为“一脚踢开了毫米波通信技术商用的‘绊脚石’”。那么,这一成果是如何踢开“绊脚石”的?为此,《中国科学报》记者走进尤肖虎团队一探究竟。

### 从CMOS工艺入手

尽管目前5G商用还处于起步阶段,但随着用户不断增加,网络将会愈加拥堵,带宽有限问题亟待解决。“毫米波的特点在于其带宽非常宽,但传播距离很近,容易受遮挡。”尤肖虎表示,如何解决这两个问题是毫米波技术能否规模化商用的关键难点之一。

为了解决传播距离问题,科学家使用天线阵列进行波束成形,通过构成的相控阵系统,将无线电能量集中起来以增加传播距离。

然而,传统的毫米波相控阵通常基于化合物半导体芯片加以实现,由于材料成本相对较高、工艺良率相对较低,极大地限制了其应用范围。“该系统的应用仅限于军事等特殊领域。”尤肖虎告诉《中国科学报》。

在诸多半导体工艺中,互补金属氧化物半导体(CMOS)工艺的材料成本最低、制造良率最高、产能最大,而且是诸多半导体工艺中唯一符合摩尔定律的工艺。为此,研究团队从CMOS工艺入手。

据尤肖虎介绍,超过95%的手机等电子产品都是基于CMOS工艺。该工艺是一项最容易实现低成本且大规模量产的工艺,和过去所使用的化合物半导体工艺之间在成本上有着量级上的差别。

### “将成本降低至原本的1/10”

但CMOS工艺本身也有缺点,“CMOS器件高频性能差,受高低温影响大。我们通过在器件版图、电路和系统架构上的创新,克服了CMOS器件的固有瓶颈,成功研制了用于5G毫米波和宽带卫星通信的CMOS毫米波相控阵芯片”。东南大学移动通信国家重点实验室教授赵涤燹告诉《中国科学报》。

2020年年初,该团队集成1024通道天线单元的毫米波大规模有源天线阵列,在世界上首次较为彻底地解决了阻碍CMOS毫米波通信的芯片问题,从芯片、模块到天线阵面全面实现自主可控。在此基础上,研究团队使用多层混压埋阻印制电路板(PCB)工艺,进一步实现了低成本、高性能4096通道集成相控阵。

赵涤燹表示,他们基于所研制的CMOS毫米波芯片实现了大规模“集成相控阵”,产品兼具低成本、低剖面、高集成和高性能的优势。

“在基于低成本CMOS工艺和PCB工艺相控阵集成度上,一般来说几百甚至上千都是比较少见的,而我们目前能够做到4096。”尤肖虎进一步解释道。据了解,4096通道集成相控阵是目前国际上基于低成本CMOS工艺和PCB工艺所实现的集成度最高、规模最大的相控阵天线系统。

CMOS毫米波大规模集成相控阵研制成功之后,“在相同工程量条件下,此项技术可以将成本降低至原本的1/10”。尤肖虎认为,随着此项技术的不断成熟,未来相控阵工程成本还将进一步降低,这也使得毫米波技术更容易推广应用。

研究人员在实验中。

“毫米波的特点在于其带宽非常宽,但传播距离很近,容易受遮挡。如何解决这两个问题是毫米波技术规模化商用的关键难点之一。研究人员基于所研制的CMOS毫米波芯片实现了大规模“集成相控阵”,产品兼具低成本、低剖面、高集成和高性能的优势。

### 逐步走向市场

据介绍,基于4096发射/4096接收超大规模集成相控阵,研究团队设计完成了毫米波相控阵卫通终端,使用中星16高轨卫星网络建立通信链路,并分别在车载、船载平台测试了相控阵卫通终端对同步轨道卫星信号的捕获及跟踪能力,并在此基础上测试了互联网访问功能。“卫星网络通信速度达到目前4G地面网络速度。”赵涤燹说。

当前使用的5G主要是低频段,即可用频谱资源已日趋匮乏的Sub-6GHz。“预计5G毫米波将在2022年北京冬奥会前后迎来大的发展。”尤肖虎说。

“未来,利用中低轨道卫星,这项技术还可以应用于手机等终端设备。”尤肖虎介绍,在地面时,手机可以接收地面信号,而当地面信号弱时,手机可以自动接收卫星信号,确保移动通信的稳定。“CMOS毫米波大规模集成相控阵成果对于支撑我国移动通信技术与产业发展意义重大。”

据悉,研究成果已在车载、船载和无人机宽带卫星移动通信和毫米波5G领域得到规模化应用。“已有30多个厂家正围绕着这项成果开发各自产品。可以说,这项技术已经走出实验室,逐步走向市场。”

随着移动通信向6G方向发展,尤肖虎团队也正考虑将该技术运用到6G中。

“目前来看,CMOS毫米波大规模集成相控阵技术在200GHz~300GHz频段上仍可以使用,那时会遇到更大的挑战。”尤肖虎表示,目前需要做好基础研究,当出现毫米波技术重大需求时,“有完全自主可控的技术可用是我们的目标和愿景”。

# 无人机送货不再『迷路』

当前,无人机送货正陆续投入使用,但与此同时也面临“找路”难题。比如,在局促的小区,相邻两栋楼不仅外形相似,而且相邻参照物也极为相似,要把快递准确送到某栋楼某单元门口,无人机导航很容易“迷路”。

杭州电子科技大学博士生王廷宇提出的“交叉定位”方案,有望解决这一难题。相关研究成果发表于IEEE《视频技术电路与系统》期刊。

众所周知,GPS是常用的全球定位系统,但在一些情况下GPS会出现定位不准,这时候就要近距离观察。无人机在送货时也要靠自己固有的“眼睛”来认路、飞行。这就意味着无人机会有两只“眼睛”,一只是GPS眼,一只是自有眼睛。

为此,王廷宇提出了一个简单有效的模型,在无人机利用卫星地图“认路”时,该模型可以主动利用卫星眼(GPS眼)和自有眼(摄像头)看到的信息,通过相互比对(主要依靠对周围物体的智慧识别),辅助目标的定位。

然而,卫星图和无人机图相互比对,做起来并不容易。卫星只能拍到大概的位置,用的是经纬度的坐标,是俯拍图。但无人机用的不是经纬度坐标,而且无人机为了到达比较隐蔽的目标,飞行轨迹可能异常复杂,这个时候拍出的图片可能是侧视图或者是其它角度的(航拍)图。这就意味着即便是同样的物体,卫星图和无人机图因为拍照角度不同、拍入的周围物体和环境不同,同样的物体乍看起来会给人“不一样”的感觉。

王廷宇设计的这个模型,并不需要两个视角图像的拍摄方向相同,即不需要特意使目标周边信息在两张图像中的位置相同,也能进行有效的比对。这样无人机在飞向微观目标物时,卫星导航与无人机拍照“认路”就可以互相配合,完成目标识别。

“这个模型的最大亮点就是,实现太空坐标、地球坐标、无人机自定义坐标之间的灵活转换,即交叉定位的内涵。”王廷宇表示,该模型也可以很方便地嵌入到已有的其它导航“认路”方法中,并提高现有方法的性能。

王廷宇的博士研究生导师、杭州电子科技大学智能信息处理实验室主任颜成钢告诉《中国科学报》:“他解决的是一个工程技术应用难题。他用交叉定位也就是匹配机制,从不同角度拍摄识别出同一物体。比如,我看你脸就可以看出是你,但我看你头顶也能看出是你,这个就很难了。而王廷宇设计的模型,可以做到这一点。” (沈春蕾 程振伟)

相关论文信息:
https://doi.org/10.1109/TCSVT.2021.3061265