从人工智能的应用看自动驾驶技术的发展

姓名：郑凯文 学号：2018011314

摘要：2018 年 3 月份发生的“Uber”无人车误撞道路行人致死案是全球首例无人驾驶汽车致死事故。人工智能技术在自动驾驶中发挥关键作用，但二者的结合还尚未成熟。人工智能自从 1956 年的达特茅斯会议后持续发展着，有高潮也有低谷。近来神经网络技术中深度学习方法的突破，结合硬件、互联网和大数据的发展产出了大量成果，将人们对 AI 的预期推向新的高峰。人工智能的突飞猛进为高精度的视觉感知识别、即时的智能决策提供了可能，助推自动驾驶技术的发展。而另一方面，理论上的不可解释性、潜在的安全漏洞、脆弱的可靠性以及法律的空白无疑是自动驾驶技术发展中的阻碍因素。针对这些问题，应对技术发展初始阶段不完美的自然规律具有理性认识，建立稳定的更新体系与防御体系，坚持有限制路测和重视驾驶权的及时交接，从权责划分等层面完善法律规范，促进自动驾驶技术的良性发展。

关键词：人工智能；神经网络；自动驾驶；道德法律

1 人工智能中的神经网络与深度学习技术

1.1 历史与成果

1956 年，一批远见卓识的科学家汇聚 DartMouth 学院，探讨用机器模拟智能的可能方案，并将人工智能（Artificial Intelligence，即 AI）作为新的术语而提出[3]。这件事标志着人工智能作为一门学科正式出现，机器学习（Machine Learning，ML）也随之成为其中的重要方向。在对于非结构化数据，如图像、语音的处理上，神经网络技术无疑是其中最具开创性的。

神经网络这一想法的提出来源于对大脑神经元网络的模拟。1943 年，神经网络的数学模型——MP 模型被提出，从此人工神经网络技术开始有了实质性的进展。一开始的单层神经网络对非线性可分问题无能为力，并出现了计算量过大的障碍。随后的多层神经网络与反向传播算法对这两个问题进行了一定的处理。而上世纪七八十年代，神经网络技术却又迎来了冬天，原因是因反向传播算法造成的梯度消失问题使系统停滞于局部最优解；过多的参数导致了过拟合问题，计算量仍未得到根本的优化[3]。在这个阶段，计算机科学家甚至要为不同的应用场景，如人脸识别、语音识别发明出专用算法[2]。

但之后脑神经科学研究的若干突破又一次鼓舞了研究者们。2000 年，Sharma 交换了幼年鼬鼠视觉和听觉神经的接合方式，

鼬鼠长大后却有正常的视觉和听觉，这说明大脑的不同神经元符合同一学习模式，具有通用性、普适性、可塑性。陆续的研究表面，大脑是一台“万用学习机”，在学习机制不变的前提下可因输入的不同而习得不同的能力[2]。

在神经网络的冬天里，Hinton 等研究者仍持续发力，终于突破了壁垒，提出了限制玻尔兹曼机下对神经网络的无监督训练策略，利用从初始数据中提取的重要特征对神经网络隐层进行有效初始化并对多个隐层进行叠加。这种方式也被称为深度学习（Deep Learning，DL）。此外，“丢弃”算法的使用，较好地解决了过拟合问题，增强了系统的鲁棒性[3]。

对特征的提取和叠加的过程，深度学习与大脑对视觉等信息的处理产生了惊人的相似性。下图表示了对人脸特征的提取过程，从边缘到局部再到整体，分别由底层、中层、顶层的神经网络来完成[2]。又如 AlphaGo 做出决策之前，利用已有的经验网络对棋局形势进行特征提取与分析，将落子在各处的概率进行合理初始化，从而跳出了暴力搜索导致计算量大，计算深度不足的限制。

深度学习神经网络经学习得到的不同层次的特征 (作图: Andrew Ng)

当前深度学习相比以往发展更加迅猛。摩尔定律下硬件性能的指数增长，以及 GPU 等新型加速器的出现提高了计算速度；分布式储存、数据仓库技术的发明增强了数据的储存与交互能力；互联网、物联网的飞速发展带来了海量的训练数据，神经网络构建愈加精确。目前，在许多领域，人工智能已全面超越人类。图像识别方面，在 2015 年的图像识别竞赛上，微软亚洲研究院的团队利用一个深 152 层的神经网络，对五个类别的识别率达到 96.43%，超越了人类的 95%；游戏博弈方面，国际象棋、围棋等复杂度居于前列的棋类阵地相继被人工智能攻破。[1][2]

1.2 缺陷

一方面，从单层神经网络到深度学习技术的不断完善，神经网络技术在许多领域有了不凡的表现。但在这一枝干长成参天大树蓬勃向上的同时，应注意到其根基仍是不稳固的：有一个根本的缺陷并未消除，即尚未建立一个有能力解释现有成果的理论体系，对机器学习到的各种参数，如权重分配缺乏逻辑上的解释。机器是真正理解了这些特征，还是只是将数据的输入反映到了亿万冷冰冰的参数之中？这一问题无法解决，此技术的社会认可度将无法得到本质的改善。[3]

另一方面，神经网络内部的各种映射关系是通过大量特定样本的输入输出训练而得到的，这样修正出来的模型不容易泛化到一般的数据集上。在实际应用中若出现陌生场景中的新数据，模型做出处理的准确性是无法保证的。机器利用现有知识适应新的条件与环境的能力，即迁移学习

的能力，还需在理论和应用层面进行更加深入的研究。[3]

2 人工智能在自动驾驶领域的应用

2.1 自动驾驶关键技术

一个自动驾驶系统的完整运行过程可大致划分几个阶段[1]：

准备阶段：利用传感器等外部感知组件采集环境信息并处理。

起始阶段：对信息进行综合分析，决定合理的行驶策略与控制策略。

运行阶段：利用搜索算法规划可行路径，进行自主导航。

结束阶段：利用行为控制技术控制车辆完成预期任务。

而实际上，在无人车行进时感知与决策实时进行而不间断，与环境互相作用形成了一个反馈与交互体系。感知与决策的及时性与准确性是保障自动驾驶安全性与稳定性的决定因素。

行驶在路上的车辆所处的是一个复杂而瞬息万变的环境，且具有小错误高代价的特点。传统的识别与决策算法在自动驾驶的应用中准确率低、反应速度缓慢，对车内乘客的生命安全造成巨大威胁；传统的算法在大样本的训练下学习速度滞缓，信息量逐渐超出存储和计算设备的极限。这种情况下，深度学习技术为自动驾驶的继续发展提供了途径，为无人车的现实应用提供了可能。[1]

2.2 视觉感知

在环境感知领域，视觉感知是 AI 的典型应用场景。从图像识别的准确率来看，深度学习技术在高精度方面有着较大优势，其中的卷积神经网络（CNN）已被证明在视觉感知领域具有很好的效果[6]。

传统的视觉识别算法需要专家人工设计特征提取框架，因而算法的鲁棒性无法保证，且耗时耗力。深度学习通过构建高达十层甚至百层的卷积层、池化层，经大量训练与自我反馈得到模型后，可进行迅速而较为准确的识别。[6]

硬件层面，芯片巨头 NVIDIA 在 2017 年推出了针对自动驾驶中深度学习的车载超级电脑 XAVIER，进一步强化了无人车的感知能力，如对道路、交通标志、车辆行人等物体的分类；对自身以及周边物体运动状态的位置跟踪和相对速度测定等。[6]

2.3 智能决策

智能决策需要根据路网信息、周遭环境及驾驶信息，并综合考虑乘坐体验实时规划出遵守规则、安全快速的驾驶策略，可分为全局路径规划和局部路径规划两部分。

通过感知与处理，自动驾驶系统实时地得到大量数据。对这些数据的即时分析与处理，当前最有效的解决方案是利用深度学习，让系统持续优化驾驶策略。车辆运行过程中可能遇到各种情形以及突发情况，这些大数据可在云平台上进行存储，

并作为样本训练出自动驾驶系统的“驾驶脑”，提高其驾驶技术及安全性[6]。

3 从人工智能的视角看自动驾驶的存在问题及解决措施

3.1 问题与隐患

人工智能到目前为止成果斐然，但本身的缺陷仍十分棘手。特别是运用到自动驾驶领域后，一个便民的技术演变为事关生命安全的核心技术，其中的任何可能的闪失都是不容忽视的。当前存在的问题与隐患大致可分为以下几点：

1) 技术可靠性与社会认可度[7]。从试验结果来看，其识别准确率固然很高，但也当然无法达到 100%。在理论体系尚未完善的现状下，系统的鲁棒性无法得到根本的保障，技术的可靠性无法让人信服；即使事故率降低，造成的生命财产损失同样难以令公众接受。
2) 可能遇到的道德困境[5]。自动驾驶系统作为一个决策系统，需要自主对行人避让、超车变道等做出判断与选择。这时若遇到一些进退两难的道德困境，如著名的“电车难题”，人类都很难抉择，人工智能做出怎样的反应才可称之为合理？
3) 系统的安全性与稳定性。深度学习系统大都建立在深度学习框架上，这些框架内部隐藏了很深的复杂度，其中的漏洞与安全盲点无法预知；不排除恶意攻击者利用漏洞或构建恶意的输入场景，如对基于 TensorFlow 的语音识别进行拒绝服务攻击，利用恶意图片令基于 Caffe 的图像识别出现内存越界，进一步可能引发整个系统的崩溃[8]。就系统本身而言，崩溃、卡顿这些很难避免的问题均会造成巨大的安全威胁[5]。
4) 法律的不健全。一是法律对车辆的规定不再适用于无人车，如《道路交通安全法》中离不开“机动车驾驶人”的参与，而无人车中并没有对应的概念[9]；二是法律对自动驾驶事故尚无明确的责任划分，这很显然要分不同的情况，并综合考虑技术提供者、车辆生产厂家、车辆操控者等多方的作用。

3.2 问题的解决途径

对于自动驾驶中可能存在的种种隐患，从程序编写者、无人车售卖者、政府管理者以及立法者均应具有超前意识。虽然当前自动驾驶汽车尚未完全渗透入人们的生活，但提前的预防措施能为无人车的大范围使用提前打好稳固的根基。有以下几方面的措施：

1) 技术层面。自动驾驶技术的安全应是多层次的。自身层面，技术提供者应具备稳定的系统更新体制，保持漏洞的实时发现与修复；对于外部入侵者，可建立严格的访问控制，将关键的控制部分隔离到一个安全的域中，还可利用加密认证、入侵监测/预防系统等技术来抵御可能的攻击[7]。
2) 使用层面。鉴于自动驾驶在路测时不完美的表现和对民众安全的威胁，在技术的发展阶段应采用有限制的路测。当技术趋于稳定和完美时，仍应特别突出无人车操纵者的作用，在突发情况下快速实现驾驶权的交接。
3) 社会层面。继续构建神经网络的理论体系，寻求对深度学习可靠性的解释；进行充分的试验与数据收集，从概率的角度证明无人车的安全性，逐渐改变社会公众的认知与接受度。

4) 法律层面。对准入标准和安全标准进行法律上的规定与规范，可借鉴国外已有法律法规，如美国《自动驾驶法案》中对安全标准更新频率的要求，对一些专业委员会建立的规划，英国《汽车技术与航空法案》对购买保险的强制性要求[9]。此外，对自动驾驶的权责划分明确界定，考虑完全自动驾驶和辅助驾驶等不同模式、人为过失与技术缺陷甚至碰瓷、自杀等特殊情形下合理的处理模式。

4 自动驾驶前景展望

可以看到的是，自动驾驶技术的发展已是大势所趋。国内《中国制造 2025》《新一代人工智能发展规划》等统领性纲要均提出了对无人车发展的要求[9]；企业方面，谷歌、百度等大型公司争相加入自动驾驶的时代浪潮，资本的大量涌入助推技术的推陈出新。

在 Uber 等一系列事件发生后，不少人对无人车的可行性提出了强烈的质疑，认为以生命安全为代价的技术没有发展的意义。不可否认无人车事故的出现对人们造成了冲击，但这并不代表自动驾驶技术的发展趋势就此被否定，毕竟自动驾驶技术的目的是为了降低事故发生率而非避免事故的发生。因此，承认这些问题的存在，在法律等方面做出合适的责任认定，避免其他方面的滞后限制技术的创新发展，这才是我们对自动驾驶应采取的态度。

参 考 文 献

[1] 王远桂,何欢.人工智能 2.0 给自动驾驶发展带来的影响[J].现代电信科技,2017,47(4):20-24.
[2] 顾险峰.人工智能的历史回顾和发展现状[J].自然杂志,2016,38(3):157-166.DOI:10.3969/j.issn.0253-9608.2016.03.001.
[3] 俞祝良.人工智能技术发展概述[J].南京信息工程大学学报,2017,9(3):297-304.DOI:10.13878/j.cnki.jnuist.2017.03.007.
[4] 田国强.人工智能技术在无人驾驶汽车领域的应用研究[J].江苏科技信息,2017,(14):56-57.
[5] 郭旭.人工智能视角下的无人驾驶技术分析与展望[J].电子世界,2017,(20):64-65.
[6] 邢星飞.深度学习人工智能在无人驾驶上的应用[J].科教导刊-电子版（下旬）,2018,(2):258.
[7] 贾瑞清,孙稚媛,张尚生.关于无人驾驶汽车存在问题的拟解决方案[J].测控技术,2018,37(8):1-4.DOI:10.19708/j.ckjs.2018.08.001.
[8] 贾如春.基于深度学习人工智能安全盲点攻击及威胁[J].电脑迷,2017,(29):175.
[9] 吴士东.人工智能自动驾驶法律规制——以“Uber 无人车致人死亡案”为视角[J].四川职业技术学院学报,2018,28(4):35-40.