科技文摘报
2017年7月20日 编辑/于 翔

真正的无人驾驶 2075年才会出现

自动驾驶系统已经逐渐装配在现代的汽车上，但是它们大多只能在特定的条件下做辅助驾驶。即使汽车生产厂商和消费者都望眼欲穿地期待着全自动驾驶的汽车，想要真正实现这个目标，还有很多不同的自动化阶段需要经历。

国际汽车工程师协会定义了关于自动驾驶的五个阶段。前三个阶段的技术，全部需要依靠人类来处理行驶过程中的紧急情况，其中第三阶段的系统允许驾驶员在特定场景中切换到自动驾驶状态，比如在高速公路上堵车时。第四个阶段的系统可处理所有与驾驶相关的任务，但是使用场景严格限定在封闭停车场或高速专用车道上。顶级的第五阶段就是完全自动化的汽车了。

无论公众怎么看，人类驾驶员还是非常善于避免严重车祸的发生。2011年美国交通安全统计数据显示，大概驾驶330万小时会发生一起致命碰撞；驾驶64000小时会发生一起致伤碰撞。这些数字为自动驾驶系统设立了重要的安全目标。想要自动驾驶的可靠性达到这个标准，还有很长的路要走。

想想你的笔记本电脑多久死一次机，如果这样的软件用于汽车驾驶，软件延迟十分之一秒响应都有可能引发交通事故。所以，自动驾驶涉及的软件，必须使用截然不同的标准来设计开发。要达到这些标准极其困难，需要在软件工程和信号处理上都取得根本性的突破才行。

自动驾驶的汽车，行驶时前后都有很多车辆，还有可能出现突然闯入眼帘的障碍物，面临突发问题，汽车的自动驾驶系统都需要在几微秒之内做出决策。因此，和飞机上使用的自动驾驶系统和代码相比，这个系统复杂了几个数量级。

我想说，到2075年完全自动化的驾驶系统都很难实现。

我们可以畅想，在未来十年间极有可能出现自动泊车系统。它允许驾驶员在车场入口处下车，让车自动进入装备完善、不允许行人和非自动化汽车进入的场地。在城市中的人行区、商业区、大学校园和其他不允许高速车辆通过的地方，低速的无人驾驶客车也很适用。这些环境中，性能有限的传感器也能有效探测行人和骑自行车的人。这些场景一定能实现，甚至很快就能实现。

《北京日报》2017.7.12
文/史蒂文·施多福

万物互联时代到来 网络安全出现新动向

GPS被“劫持”了怎么办?

有专家表达了担忧：网络安全领域的人工智能也可能变成一把“双刃剑”，如果黑客使用了人工智能的恶意软件，就能更轻松地弄清楚它周边的环境，并模仿系统中用户的行为，从而造成更大的危害。

“你的GPS被‘劫持’了!”

这并非科幻电影中的场景。现实中，在我们越来越多打开手机的GPS定位来预定外卖、打车或解锁共享单车时，由于GPS发射的信号未经加密，“黑客”可以利用SDR（软件定义的无线电）设备伪造卫星信号，发射到指定的区域内，进而影响这一范围内的目标设备。这时，你的手机可能会被“定位”在一个你从未去过的地方，时间设置也可能“穿越”到过去或未来。而这暴露出的不过是网络安全威胁的“冰山一角”。

未来的物联网城市什么样？科学家们是这样描绘的：一切都变得越来越智能，路上行驶着自动驾驶的汽车，空中有无人机送货，股票外汇交易、城市服务与管理、紧急救援、食品安全保障都需要通过装载GPS的设备来实现。如果这些设备的GPS被“黑”，造成的影响和损失可不是那么简单。

市场机构预计，到2020年，全球将有500亿台物联网设备。届时随着5G通信技术和物联网的大规模应用，万物互联将成为现实，物理世界和虚拟世界被打通，对虚拟世界的攻击可作用到物理世界，基础设施也将会面临更加严峻的安全威胁。

中国移动通信集团信息安全与运行中心总经理张滨认为，物联网时代将有两个“无处不在”：一是物联网的应用无处不在，智能家居、智慧交通、智慧城市将从各个方面影响人们的生活；二是它所带来的风险也将无处不在。

目前，个人隐私、家庭安防等领域都是物联网安全的“重灾区”。亚信安全首席技术官张伟钦介绍，今年年初，奥地利一家酒店的电子门禁系统就曾多次遭到黑客的攻击，使得客人无法进入或走出房间。酒店只得向黑客支付了价值1500欧元的比特币，然而，黑客在获得赎金以后，还在系统留下了“后门”，这意味着他们随时都可以卷土重来。

随着人工智能的发展，网络安全厂商正在积极探索机器学习在安全数据挖掘、网络安全、威胁检测等方面的应用，通过人工智能来强化网络安全防护。

亚信安全CEO张凡指出，应对有组织的网络攻击，除了要打破各自为战的局面，还需要转变防护观念，由被动防御向主动保护发展，建立一体化的防御体系。《人民日报》2017.7.14 文/谷业凯

超级高铁首次测试

速度仅为110公里/小时

有着“科技狂人”之称的马斯克提出超级高铁的概念后，业界有不少人提出质疑，毕竟这一概念提出了很久，并且目前看不到商用的可能性，而且实验进展缓慢。但是超级高铁公司Hyperloop One7月14日宣布，就在5月份，这家公司在北拉斯维加斯的开发测试跑道上完成了首次全系统测试。Hyperloop One运用磁悬浮技术，在实验跑道上时速达到70英里（约为113千米/小时），而且是在真空环境下进行。

据了解，这次的全系统测试时间也很短，测试车在真空管道中只跑了5.3秒。Hyperloop One创始人兼执行总裁谢尔文·皮实瓦尔认为虽然时间都很短，但是都是一个新的交通方式出现的里程碑。

不过，此次仅有70英里/小时的速度与原先设想至少750英里/小时的速度相比还不到1/10，而且还不及目前已经商用的中国最新高铁“复兴号”的1/3。不过，皮什瓦尔称：“这是100年来首次出现新交通模式。Hyperloop不仅仅只是停留在纸面，而是开始成为现实”。

目前，Hyperloop One下一阶段的目标已经提出，要将超级高铁时速将提升至250英里/小时(约合402千米/小时)，并且首次安装乘客舱，测试距离也将更长。皮什瓦尔相信他们测试的“超级高铁”将成为在陆地上移动最快的交通工具。

环球网 2017.7.14 文/陈健

将数据存进活细胞

英国《自然》杂志发表了一项生物技术重要成果：科学家利用CRISPR（基因编辑技术）手段，成功将图片和视频短片编码进了细菌的DNA中，通过测序DNA再重新提取出来后仍相当准确。其证明了活细胞作为一种可靠媒介，存储一定数量的数据完全有可能。

CRISPR被称为“生物科学领域的游戏规则改变者”。最近的一些研究成果已经显示，CRISPR技术具有一种能力：可以使用两种蛋白质将遗传密码插入目标细胞的DNA中，从而将信息传输至活细胞。

为了证明这一点，美国哈佛医学院研究人员塞斯·施普曼及其同事使用CRISPR手段，将多张图片和一段GIF（一种简单的动画），成功编码进了大肠杆菌中。

此次所采用的图片和短片，都来自埃德沃德·迈布里奇的《人类和动物的运动》。其中，这段GIF格式的视频是名为Annie G的马奔跑的5帧影像，大小为36×26像素。研究团队使用DNA的基本组成核苷酸生成代码，一个代码关联一张图片的单个像素。至于GIF视频，他们则将序列逐帧传至活细菌，并按传输顺序将它们插入细菌基因组中。

被插入大肠杆菌的基因组中之后，这些数据还可以再通过测序DNA重新提取出来，通过读取像素核苷酸代码，可以将图片重构出来，准确度达90%左右。

《科技日报》2017.7.13 文/张梦然

你乐意搭载无人驾驶的“飞的”吗?

迪拜道路交通局宣布，空中出租车服务将在10月至12月间在某个时间进行试飞，并由德国航空公司Volocopter提供飞机。最近YouGov的一项新的研究表明，美国消费者可能不是很乐意使用空中无人驾驶的士服务。有一半的成年人表示他们觉得无人驾驶的士不安全，只有5%的人认为该技术可靠。尽管如此，分析师认为，无人驾驶空中的士将会在5年之内兴起。 威锋网 2017.7.11

把物质从地球传送到太空 中国科学家创纪录

英国《卫报》网站刊登题为《“传送我吧，斯科蒂!”科学家把光子远传至300英里外的太空》的文章称，虽然《星际迷航》中的科技依然很遥远，但科学家成功测试从地球到太空的远距离量子纠缠，为实现黑客无法入侵的量子互联网带来了希望。

文章称，就像科幻小说里描述的那样，中国科学家们把一个物质从地球传送到300英里（约合493公里）以外的卫星上，这创造了量子隐形传态的新纪录。

量子隐形传态是一种神秘的现象。处于纠缠态的两个量子，其中一个量子状态发生改变，另一个的状态也会瞬时发生相应改变，即实现远距离隐形传态。科学家们说，这是向创建黑客无法入侵的量子互联网迈出的重要一步。

由中国科学技术大学教授陆朝阳带领的团队在论文中说：“空间尺度上的隐形传态是可以实现的，这有望在未来的分布式量子互联网中发挥关键作用。”

这项工作可能让人联想到斯科蒂在《星际迷航》里传送“企业”号星舰上的人员，但短时间内科学家还不可能实现瞬时把人类传送到一个遥远的地方。隐形传态效应还仅限于量子级别的物体，如基本粒子。

在这次实验中，科学家从位于西藏阿里的地面站，向距离地球300英里的中国“墨子号”卫星发射光子。这项研究旨在证明量子纠缠这种神奇现象。

量子隐形传态可以用于建设新型通讯网络，在这种网络内，信息将以纠缠光子的量子态为编码，而不是0和1。其巨大的安全优势是，黑客如果不能干扰光子并揭示它们的存在，就无法测定光子的形态。

英国牛津大学实验物理学教授伊恩·沃姆斯利说，最新的研究成果向着这一目标迈出了了不起的一步。他说：“这证明了该领域已经不再局限于科学家们坐在实验室里思考这些奇怪的现象。量子现象的确是有用的，它可以带来一些重要的新技术。”

参考消息网 2017.7.14

地址:北京市复兴路15号 邮编100038 电话010-58884136/37/38 传真010-58884135 每周四出版 广告许可证:京海0163 全年订价:99.84元 零售价:2.00元