浙江大学因公出国（境）团组出访报告公示

<table>
<tr><td rowspan="3">基本信息</td><td>团组名称</td><td colspan="3">浙江大学阮伟等 2 人出访</td></tr>
<tr><td>出访期限</td><td>2019-06-17 至 2019-06-21</td><td>在外时间</td><td>总天数 5 天</td></tr>
<tr><td>出访国家
（地区）
（含过境）</td><td colspan="3">中国香港,香港</td></tr>
<tr><td>出访报告</td><td colspan="4">一、 访问情况：
应香港大学的邀请，浙江大学阮伟团队于 2019 年 6 月 17 日至 2019 年 6 月 21 日赴香港参加基于“机器人学习方法的大数据分析与工业应用”任务。
一、访问基本情况
6 月 17 日到达香港大学。
6 月 18 日参加香港大学统计及精算学院举办的“基于机器学习方法的大数据分析与工业应用会议”。在会议上，与徐锦峰教授进行了详细交流：为了研究在工业控制系统软硬件不完全可信的条件下，如何利用人工智能技术的自博弈模型（生成式对抗网络 GAN）自我生成学习样本，以解决工业控制系统攻防学习样本稀缺的问题，以刻画针对工业控制系统的攻防特征，对工业控制系统威胁进行实施侦测与阻击。在参观网络安全实验室的过程中，徐锦峰教授以“交通信号灯”和“电梯”为例进行了精彩的讲解，让大家一方面了解了在工业上虽然有的基础设施没有连接互联网但也不存在绝对的安全”
6 月 19 日到香港科技大学与计算机科学与工程学院的陈凯教授就大数据网络安全进行交流。陈凯教授于 2012 年加入香港科技大学计算机科学与工程学院，目前负责系统网络实验室，及微信-香港科技大学人工智能联合实验室。主要研究内容：数据中心网络；网络化系统设计与实现；云、大数据、人工智能系统的网络</td></tr>
</table>

支持；服务 RDMA 网络和支持 RDMA 的应用程序等。陈凯介绍了高速数据中心网络（Data Center Network, DCN）中拥塞控制问题的研究背景，指出随着链路带宽地不断增长，现有的拥塞控制方案已无法很好地满足数据中心网络应用低时延、高吞吐的传输要求。此外，数据中心网络中交换机由于成本问题，其缓存大小的增长无法与网络带宽增长相匹配，这将对基于标准 ECN 标记的拥塞控制方案在同时满足低时延、高吞吐需求方面带来巨大挑战。陈教授详细阐述了一种针对高速浅缓存数据中心网络设计的拥塞控制方案 BCC（Buffer-aware Congestion Control），该方案通过活跃缓存的数量来选择使用基于端口的标准 ECN 机制或基于共享缓存的 ECN 机制，以保证即使在多个端口均活跃被使用时拥塞控制依然可以在较高吞吐情况下减小丢包率。在陈凯教授带领下，参观了“系统网络实验室”以及香港科大-微信人工智能联合实验室。

6 月 20 日到香港中文大学系统安全实验室与张克环教授进行计算系统中的各种新型安全问题以及相应的防御技术进行探讨。香港中文大学系统安全实验室由张克环教授在 2012 年创立，目标是研究计算系统中的各种新型安全问题以及相应的防御技术。实验室的重点研究方向包括：物联网安全、人工智能安全、移动安全、Web 安全等。张克环教授去年发现 Android 内置的语音助手系统存在安全漏洞，遂设计出一套名为“VoicEmployer”的恶意软件，成功测试到黑客在未获授权的情况下，能轻易绕过现有 Android 系统的数据保护机制，操控受密码保护的手机，启动 Google 语音搜索并播放恶意语音指令，如任意拨号，还可以语音控制用户的手机发送恶意短讯、电邮，甚至查询手机的语音电邮(voice mail)、行事历、当前位置等数据。张克环博士介绍了在该领域中发现安全漏洞问题的解决方法，并提出建议，对信息安全专业的研究生如何进行科学研究提供了思路和帮助。

6 月 21 日从香港回杭州。

二、访问成果

在香港大学、香港科技大学、香港中文大学的访问重点交流了人工智能技术在工业控制系统信息安全方面的研究、Web 网站的防攻击、防篡改方面的研究，对建立工控系统控制层层主动防御模型、建立工控系统管理层主动防御模型具有很好的启迪作用，计划依托并在进行的上海工控靶场项目中进行测试验证，以丰富工控系统主动防御的理论研究、技术研究与装备研究。

三、工作建议

香港大学、香港科技大学、香港中文大学在物联网信息安全领域，特别是人工智能研究信息安全领域有着比较深厚的基础与领先研究成果，今后我们积极与其进行学术交流，请进来、 走出去，在联合研究、联合申报国家重大项目、联合培养学生方面有着较为广阔的合作前景。

备注：1. 团组（或本人）执行本次因公出访任务情况良好，主要任务、日程安排、团组成员等与任务申报时一致，如不一致，需详细说明；2．须于回国（境）后一个月内在本单位内部完成出访报告公示。