 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5738

Research on the Teaching Mode of Computer Network Security for Postgraduates under the Background of Emerging Engineering Education

Yihua Zhou Weimin Si Wei Ma Yuguang Yang

Beijing University of Technology, Institute of Information Security, College of Computer Science, Department of Informatics, Beijing, 100124, China

Abstract

In view of the problems existing in the teaching of computer network security for graduate students, such as different specialties, different research directions, different research bases, different research types and insufficient school hours, this paper analyzes the characteristics of the course and the challenges it faces, aiming at the four-dimensional development of ideology and politics, quality, innovation and practice, this paper puts forward some new teaching models, such as practical hot-spot guidance, transfer learning, hot-spot guidance and mixed teaching, the practice teaching shows that the teaching mode adopted in this paper improves students'study interest, scientific research innovation and ability to solve complex engineering problems, and optimizes the teaching effect.

Keywords

network security; transfer learning; hotspot guidance; hybrid teaching

新工科背景下研究生计算机网络安全教学模式研究

周艺华 侍伟敏 马伟 杨宇光

北京工业大学信息学部计算机学院信息安全研究所，中国·北京 100124

摘 要

针对研究生计算机网络安全教学中存在的专业不同、研究方向不同、研究基础不同、研究类型不同以及学时不足等问题，论文分析了课程的特点和面临的挑战，以思政、素质、创新、实践四元发展为目标，提出了基于实事热点引导、迁移学习、热点引领、混合式教学等新型教学模式，实践教学表明论文采用的教学模式提高了学生的学习兴趣，提升了学生的科研创新及解决复杂工程问题的能力，优化了教学效果。

关键词

网络安全；迁移学习；热点引导；混合式教学

1 计算机网络安全课程教学的现状分析

随着信息和网络通信技术的高速发展，特别是人工智能、5G 网络、社交网络、云计算、大数据等热点领域的研究和发展，各种数据驱动的项目应运而生，信息已成为重要的战略资源。但是，危害网络与信息安全的事件不断出现，斯诺登事件、伊朗震网病毒事件以及勒索病毒的出现，更是将网络空间的地位提升到各个国家的战略层面，习近平总书记提出“没有网络安全，就没有国家安全”，网络安全事关国家安全、事关社会稳定，因此必须采取有效措施，保障中国的网络空间安全。网络空间安全的竞争关键在于网络安全人才的竞争，由于中国网络安全研究起步较晚、网络安全意识较为淡薄、国际上网络安全技术封锁、网络安全法律法规不健全等原因，网络攻击及泄密事件时有发生，如何培养网络空间安全高端人才的形式非常严峻。《计算机网络安全》课程作为计算机专业学术及专业学位研究生的核心课程，担负着培养网络空间安全高端人才的重任，课程教学质量的好坏直接影响到学生后期的选题及培养。由于受到研究生研究基础的差别、研

【基金项目】北京工业大学研究生精品课程建设项目（项目编号：CR201906）；北京工业大学密码学混合式课程建设项目（项目编号：KC2018MT008）；2020 年北京工业大学信息学部计算机学院院级教育教学项目（项目编号：2020JSJJX007）。

 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5738

究方向的差别、学硕与专硕培养目标的差别等影响，很难选取或编写一部针对所有研究生都适用的教材，在没有国家指导教材为依据的前提下，非常有必要对研究生《计算机网络安全》的教学模式进行探索和改革。

中国和国际上很多教学和研究机构对《计算机网络安全》教学模式进行了探索和研究 [1-6,8]。谈潘攀针对高校计算机网络安全多以理论为主、内容较为抽象、课时缩减等问题，提出了以点带面、翻转课堂、自主学习等教学改革思路 [1]；胡晶晶等针对大数据时代的网络安全问题，从安全意识教育、多媒体手段、加强监管等方面强化计算机网络安全教育和教学 [2]；王宓针对高职院校计算机网络安全课程教学的特点，提出了项目驱动、师生互动的教学方法 [3]；肖耿毅、顾军等分别从工程教育、OBE 的视角，提出了科学创设实践项目、创新教学实践路径的工程教学模式探索 [4-5]；段立娟等针对本科生的特点，提出了采用启发式教学、理论联系实际等方法，提高学生的动手能力 [6]；刘昉等针对学生重理论轻实践，重结果轻过程的特点，提出了任务驱动的教学方法 [7]。

目前的研究成果主要针对本科生或高职学生的特点，对计算机网络安全的教学模式进行探索，鲜有针对研究生课程教学改革的相关文献，因而研究和改进新工科背景下研究生网络安全课程的教学模式，对提高研究生培养质量、提升中国网络空间安全高端人才的质量、推动中国网络空间安全事业的健康发展具有重要的理论和实际意义。

2 研究生网络安全课程的特点与挑战

研究生网络安全课程教学同本科生网络安全课程教学有很大差别。本科生课程教学侧重于对基础知识的讲解和基本实践能力的培养，由于本科生是从零开始接触网络安全相关知识，对网络安全存在新鲜感和较为浓厚的兴趣，因而只需循序渐进地把基础知识教好， 一般不会出现问题。研究生网络安全教学则有很大不同，计算机学院的研究生来自不同层次的学校、不同的学科专业，具有不同的研究基础、不同的研究方向、不同的培养目标， 稍有不慎，就会引起部分研究生不满情绪，甚至会造成冲突。研究生计算机网络安全教学主要存在如下突出问题：

（1）研究生教学普遍存在侧重视知识传授，忽视价值引领的问题。

（2）研究生研究方向的多样性与教学内容一致性之间存在矛盾。

（3）研究生研究基础的差别与单一课程教学目标的之间存在矛盾。

（4）学术学位重理论与专业学位重工程之间存在矛盾。

（5）教学内容的丰富性与学时不足之间存在矛盾。

3 新工科背景下研究生计算机网络安全教学模式研究

针对研究生网络安全课程的特点，探索一套新工科背景下研究生计算机网络安全教学模式：以思政、素质、创新、实践四元发展为目标，以价值引领、热点研究、迁移学习、混合式教学为手段，全面提升研究生的科研及解决复杂工程问题的能力，培养符合社会需要的高端网络空间安全人才。

3.1 以实事热点引导，探索知识传授与价值引领的有机统一机制

在新工科背景下推进课程思政，重在课堂育人，将思政元素融入课程教学，构建网络安全人才文化价值体系。传统的计算机网络安全教学侧重知识传授，学生往往感觉枯燥无味，缺乏学习动力，选取接地气、实实在在的时事热点和经典案例教育引导学生。例如，引入对华为断供事件的深入分析，使学生深刻明白断供的原因是华为掌握了领先的5G技术、领先的网络技术、领先的手机设计技术等几乎全产业链核心技术，从而激发学生的爱国热情、民族自信心和使命感，激发学生的研究兴趣和责任担当，鼓励学生发愤图强，努力开发和掌握核心技术，从而让思政教育真正做到润物细无声，培养具有“工匠精神”的新工科网络安全人才。

3.2 以迁移学习为手段，探索适合不同研究方向的新型教学方法

研究生的研究方向涉及密码学、入侵检测、防火墙、物联网、态势感知等，呈现出多样性的特点，如果按固定不变的教学方法，不可避免地会出现顾此失彼的情况，因而在教学实践过程中，探索出以学科交叉、迁移学习为手段，适合多研究方向的新型教学方法。深度伪造（DeepFake）技术是当今人工智能安全的研究热点，通过在熊猫的特征中加入长臂猿的特征，可以使模式识别算法出现错误，将视觉上是熊猫的图像识别为长臂猿，利用同样的技术还可以实现各种换脸技术、声音伪造技术以及控制说话人口型的技术等。该技术主要用于图像、视频及声音的伪造，通过类比及迁移技术

 DOI: https://doi.org/10.26549/jxffcxysj.v3i14.5738

加以引导，就可以将此技术引入的网络攻击的范畴。例如，已知的攻击模型容易被检测，攻击者在攻击模型中加入其他的正常应用的部分特征，就可以使模型检测失效，从而起到逃避检测的目的，因而一种技术通过迁移手段就可以适合不同研究方向的研究生学习。同样的技术还有联邦机器学习算法，机器学习同样是模式识别算法，但通过加入同态加密等模型保护算法，将模式识别迁移到安全的模式识别算法。通过迁移学习技术，激发了学生的学习兴趣，提高了学生的跨学科学习能力和创新能力。

3.3 以研究热点引领，探索不同基础、不同培养目标研究生之间的互助合作机制

拟态防御技术是一种内生性安全的防御技术，能模拟生物根据周围环境变化，主动改变自身颜色、形态及行为能力，根据场景的变化动态调整自身结构和外在表现，构建动态防御体系，是当今网络安全的研究热点。动态异构冗余构造（dynamic heterogeneous redundancy，DHR）是一种超高可靠性架构的典型拟态防御技术，在非相似冗余架构的基础上，增加了策略分发、动态调度、多模表决等环节以及基于池化资源的可重构、可重组、可重建、可重定义、虚拟化等多维动态课重构要素构成的异构服务集合。因此，利用 DHR 可以将不同目标、不同基础的研究生组合起来，由学术学位侧重理论的研究生研究动态调度算法、多模表决算法，由专业学位的侧重实践研究生实现不同的构建模块。例如，基于 Windows、Linux、Mac 的构建模块，通过拟态防御这一热点技术，提高了学生的学习兴趣，有效地实现了不同类型研究生的互助合作机制。

3.4 以线上 / 线下混合式教学模式，探索教学内容与学时不足的冲突解决机制

计算机网络安全研究生课程涉及密码学基础、底层协议的安全性、高层协议的安全性、无线网络安全、分布式入侵检测、网络攻击与防护、主动防御技术以及创新性网络安全技术等，根据研究生的特点，教学内容非常丰富；即要覆盖到面，又要照顾到点。一般的 32 课时教学安排，是不可能有效完成相应的教学内容的，为此我们探索了线上 / 线下混合式教学方式，与通常的线上为主，线下为辅的方式不同，采用了线下为主、线上为辅的混合式教学模式，线下主要是讲授、交流前沿研究内容，线上提供微课、基础课视频、答疑视频及综合课题供学生学习和讨论。主要原因是学生线上学习的主动性一般不高，容易受到各种因素干扰，不能集中精力。而通过线下组织热点的教学内容，可以极大程度地吸引学生的注意力和兴趣，会激发学生通过线上视频资料去补足自己的学习短板。通过线上 / 线下混合式教学模式，极大地弥补了教学内容与学识不足的矛盾。

4 结语

论文针对研究生计算机网络安全课程教学的特点，对新工科背景下研究生计算机网络安全教学模式进行了研究，提出了实事热点引导、迁移学习、热点引领、混合式教学等新型教学模式，有效地解决了研究生专业不同、研究方向不同、研究基础不同、研究类型不同以及学时不足的问题，激发了学生的学习兴趣，使学生选课人数达到了班级上限，甚至有学生为选不上该课程感觉可惜，同时激发了学生的自学习能力，优化了学习效果。

参考文献

[1] 谈潘攀 . 本科计算机专业《计算机网络安全技术》课程教学改革探讨 [J]. 电脑知识与技术 ,2019(33):138-139.

[2] 胡晶晶 , 刘勇 , 王忠义 . 大数据时代计算机网络信息安全及防护教学研究 [J]. 农村经济与科技 ,2020(16):277-278.

[3] 王宓 . 高校计算机网络安全课程教学改革探讨 [J]. 计算机产品与流通 ,2020(10):110.

[4] 肖耿毅 . 工程教育视角下高校计算机网络安全教学的改革创新路径探析 [J]. 教育观察 ,2020(22):93-95.

[5] 顾俊 , 姜秀柱 , 李锡渝 . 基于 OBE 的信息安全专业“计算机网络”教学研究 [J]. 科技文汇 ,2020(08):88-90.

[6] 段立娟 , 周艺华 . 网络安全课程教学研究与探讨 [J]. 计算机教育 ,2008(10):74-75.

[7] 周艺华 , 蔡永泉 . 数字鉴别与认证课程教学的几点看法 [J]. 计算机教育 ,2010(24):120-123.

[8] 刘昉 . 任务驱动教学法在高职计算机网络安全教学的应用评价 [J]. 求知导刊 ,2014(11):15-16.