人工智能时代计算机网络安全课程教学改革路径研究

肖琛　牟云飞　马媛媛
泰山科技学院

摘　要：当下，人工智能技术在金融、医疗、交通等诸多领域广泛渗透。于计算机网络安全层面，既带来精准高效的智能防护手段，如智能算法实时监测网络流量，及时察觉异常；也面临恶意攻击者借助人工智能开发隐蔽性强、破坏力大的新型攻击工具的严峻挑战。本文紧扣人工智能时代特性，深入剖析计算机网络安全课程教学改革的紧迫性与必要性，探讨现存教学内容滞后、方法单一等问题，从教学内容更新、方法创新、强化实践及师资队伍建设等维度，提出切实可行的改革路径，致力于培育契合人工智能时代需求的高素质专业人才。

关键词：人工智能；计算机；网络安全
【DOI】10.12252/j.issn.2096-6288.2025.04.162

引言

人工智能（AI）技术的迅猛发展，如机器学习、深度学习、自然语言处理等，正深刻地改变着社会的各个层面。在计算机网络安全领域，人工智能技术既为防范网络攻击提供了新的手段，如通过智能算法实时监测和分析网络流量，及时发现异常行为；同时，也带来了前所未有的挑战，恶意攻击者利用人工智能技术开发更具隐蔽性和破坏性的攻击工具。在这样的背景下，传统的计算机网络安全课程教学已经不能满足时代对专业人才的需求，亟待进行教学改革，培养具备扎实理论基础、熟练实践技能和创新思维的计算机网络安全专业人才，为人工智能时代有效地应对各种网络安全威胁做出贡献。

一、人工智能时代计算机网络安全课程教学改革的必要性

（一）适应行业发展需求

在人工智能广泛应用的今天，网络安全行业对人才的要求有了很大变化。企业不仅要求网络安全专业人员掌握传统的网络安全知识，如防火墙配置，入侵监测系统使用等，更要求其具备运用人工智能技术解决网络安全问题的能力。例如可以应用机器学习算法构建网络安全态势感知模型，预测潜在的网络攻击风险；应用深度学习技术对网络流量进行分类和识别，及时发现新型网络攻击。因此，计算机网络安全课程教学要紧跟行业发展趋势，进行相应的改革，使学生所学的知识和技能与行业实际需要接轨，提高学生的就业竞争力。

（二）提升学生综合素养

人工智能时代网络安全问题更复杂，更多样化，需要专业人员具备跨学科的知识与综合素养。计算机网络安全课程教学改革能够增加学生的知识面，培养学生的创新精神和解决实际问题的能力。将人工智能相关知识引入课程教学中，让学生了解人工智能技术在网络安全领域的应用原理和方法，学会用人工智能工具进行网络安全分析和防护。同时，学生在学习中还需要掌握数学、统计学、计算机科学等多学科知识，有利于提高学生的综合素质，使其成为知识面广、适应能力强的复合型人才。

（三）应对网络安全新挑战

借助人工智能技术，网络攻击手段智能化，自动化，隐蔽化。传统的基于规则匹配的网络安全防护技术，在面对这些新型攻击时往往显得力不从心。例如由人工智能驱动的恶意软件可以在短时间内自动学习和适应网络环境，躲避传统杀毒软件的检测；自动化的网络攻击工具可以在短时间内对海量的目标发起攻击，给网络安全防护带来巨大压力。为了很好地应对这些新的挑战，计算机网络安全课程教学需要进行改革，培养学生具备识别、分析、防范人工智能时代网络安全威胁的能力，使其能够在未来的工作中保障网络系统的安全稳定运行。

二、当前计算机网络安全课程教学存在的问题

（一）教学内容滞后

当前，许多高校计算机网络安全课程教学内容仍以网络安全基础理论、网络协议安全、密码学等传统网络安全知识为主。这些虽然是计算机网络安全的重要基础，但这些内容在人工智能时代教学内容明显滞后。人工智能技术在网络安全领域的应用，诸如人工智能驱动的网络安全防护技术，网络安全漏洞检测中的人工智能方法等，涉及较少。这使得学生所学知识与当前网络安全行业的实际需求脱节，毕业后很难快速适应工作岗位的要求。

（二）教学方法单一

在教学方法上，大多数教师仍然采用传统的讲授式的教学方法，重视理论知识的教学，忽视了学生实践能力、

创新思维的培养。在课堂上教师通过讲解教材内容，演示相关案例，学生被动接受，很少有主动参与、思考的机会。这种单一的教学方法导致课堂气氛沉闷，学生学习积极性不高，难以达到良好的教学效果。此外，实践教学环节，往往停留在网络设备配置、安全工具使用等简单的实验操作上，没有丰富的、富有创造性的实践项目，难以使学生提升解决实际网络安全问题的能力。

（三）实践教学不足

实践教学是计算机网络安全课程教学的重要内容，对培养学生的实践能力和创新精神具有重要作用。但目前实践教学比较缺乏。一是实践教学设施不全，很多高校的网络安全实验室设备陈旧、数量不足，不能满足学生的实践需要。另一方面，实践教学与真实的网络安全环境脱节，学生在实验室中的实验往往是在一种理想化的条件下进行的，与现实的网络安全情景相去甚远。这就使得学生在遇到实际的网络安全问题时，缺乏经验，更缺乏解决问题的能力。

（四）师资队伍建设有待加强

人工智能时代的计算机网络安全课程教学对教师的专业素养提出了更高的要求。教师不仅要有较好的计算机网络安全的专业知识，而且还要能够熟练地掌握人工智能相关技术并能将其融入课程教学中。但当前很多高校的计算机网络安全课程教师人工智能知识储备不足，教学能力有限。部分教师在有网络安全教学经验的情况下，对人工智能技术相对缺乏了解和应用，无法胜任人工智能时代的教学任务。此外，高校对师资队伍建设投入不足，缺乏对教师进行人工智能技术培训和进修的机会，也在一定程度上制约了课程教学改革的推进。

三、人工智能时代计算机网络安全课程教学改革路径

（一）更新教学内容

1. 融入人工智能技术相关知识

在计算机网络安全课程教学内容中要增加人工智能技术在网络安全领域的应用知识。比如专门开设章节介绍机器学习，深度学习在网络入侵检测，恶意软件检测，网络安全态势感知等方面的应用原理和方法。通过理论讲解和实际案例分析，让学生了解如何利用人工智能算法对网络数据进行处理和分析，实现对网络安全威胁的实时监测预警。

2. 引入网络安全新热点

关注网络安全领域的最新动态和热点问题，及时将其作为教学内容。比如，物联网，云计算，大数据等新技术的发展，都引发了与之相关的网络安全问题。在教学中，引入物联网设备安全，云计算安全，大数据安全等方面的知识，让学生了解这些新兴技术环境下的网络安全挑战以及应对策略。同时，也可以引入人工智能时代的网络安全伦理问题，引导学生在利用人工智能技术保障网络安全的同时，避免出现伦理道德问题。

3. 优化传统教学内容

在保留传统计算机网络安全核心知识的基础上进行优化与更新。比如密码学教学中除了传统的加密算法外，还应介绍量子密码学等新密码技术，使学生了解密码学发展最新趋势。在网络协议安全教学中，结合人工智能时代网络应用的特点，分析网络协议在面对新型攻击时存在的安全漏洞和防范措施。从而优化传统教学内容，使之与人工智能时代网络安全需求相适应。

（二）创新教学方法

1. 采用项目驱动式教学

所谓项目驱动式教学，是以项目为导向，学生在完成项目过程中进行的主动学习和应用知识的教学方式。在计算机网络安全课程教学中可以设计一系列与人工智能时代网络安全实际问题相关的项目，例如基于机器学习的网络入侵检测系统设计，利用人工智能技术构建网络安全态势感知平台等。把学生分成若干小组，每小组负责一个项目。在项目实施过程中，学生需要自己查阅资料，分析问题，设计解决方案，进行实践操作。而教师则作为指导者，为学生提供必要的技术支持和指导。通过项目驱动式教学，激发学生的学习兴趣和主动性，培养学生的团队协作能力和解决实际问题的能力。

2. 开展案例教学

案例教学是指通过分析真实案例，传授知识，培养学生思维能力的教学方法。收集和整理人工智能时代网络安全领域中的真实案例，例如著名的网络攻击事件，成功的网络安全防护案例等，并在课堂上进行深入分析。指导学生从案例中发现问题、分析问题，并利用所学的知识提出解决方案。通过案例教学，可以让学生更好地理解网络安全知识在实际中的应用，提高学生分析问题、解决问题的能力。同时，案例教学还能够开阔学生视野，了解网络安全行业的最新动态和发展趋势。

3. 运用翻转课堂教学模式

翻转课堂教学模式是一种将传统课堂教学中的知识传授和知识内化过程进行颠倒的教学方法。在计算机网络安全课程教学中，教师可以将教学内容制作成微视频、在线课件等教学资源，发布在网络教学平台上，让学生在课前自主学习。课堂上，教师则主要组织学生进行讨论、答疑、实践操作等活动，帮助学生解决在自主学习过程中遇到的问题，实现知识的内化。翻转课堂教学模式能

够充分发挥学生的主体作用，提高学生的自主学习能力和学习效果。

（三）强化实践教学

1. 完善实践教学设施

加大对网络安全实验室建设的投入，更新和完善实验室设备。配备先进的网络安全实验平台，如网络攻防演练平台、网络安全监测平台等，为学生提供更加真实、丰富的实践环境。同时，利用虚拟化技术，构建虚拟网络安全实验室，使学生能够在虚拟环境中进行各种网络安全实验，提高实验教学的效率和灵活性。此外，还可以与企业合作，建立校外实践教学基地，让学生有机会参与到实际的网络安全项目中，积累实践经验。

2. 设计综合性实践项目

在实践教学环节，设计一系列综合性实践项目，将人工智能技术与计算机网络安全知识有机结合起来。例如让学生设计并实现一个基于人工智能技术的网络安全防护系统，它必须具有网络入侵检测、恶意软件识别、安全漏洞扫描等功能。学生通过完成这样的综合性实践项目，能够将所学的理论知识应用到实际中，提高自己的实践能力和创新能力。同时，综合性实践项目还可以培养学生系统设计和工程实践的能力，使学生更好地适应未来工作岗位的要求。

3. 开展网络安全竞赛活动

积极组织学生参加全国大学生信息安全竞赛、网络安全技术大赛等各类网络安全竞赛活动。网络安全竞赛是以竞赛的形式来检验和提高学生网络安全知识和技能的有效方法。通过竞赛能够接触到来自不同高校的优秀选手，了解行业内最新的技术和发展趋势，扩大自己的视野。同时，竞赛活动还能激发学生的学习兴趣和竞争意识，培养学生的团队协作精神和创新能力。学校可以成立专门的竞赛指导小组，对参赛学生进行培训和指导，提高学生的竞赛成绩和实践能力。

（四）加强师资队伍建设

1. 提升教师人工智能技术水平

高校应当加强对计算机网络安全课程教师的培训与进修，提供更多地学习人工智能技术的机会。可组织教师参加人工智能相关的学术研讨会，培训班，企业实践等活动，让教师了解人工智能技术的最新发展动态和应用案例，融入课程教学中。同时鼓励教师进行人工智能技术在网络安全领域的应用研究，通过科研项目提升自己的专业素养和教学能力。

2. 引进具有跨学科背景的教师

高校可引进具有计算机科学、人工智能、数学等跨学科背景的教师来满足人工智能时代计算机网络安全课程教学需求。这些教师可以丰富课程教学内容，给课程教学带来新的思路、方法。同时，还可以推动学科之间的交叉融合，促进学科建设与发展。另外，高校还可以聘请企业中的网络安全专家、人工智能技术人才作为兼职教师，教授在实际工作中的经验与技能，使教学内容更贴近行业实际。

3. 建立教师团队合作机制

鼓励计算机网络安全课程教师团队合作开展课程建设、教学改革和科研项目研究。通过团队合作，教师可以互相学习，交流经验，充分发挥各自的专业优势，提高教学质量和科研水平。再如具有网络安全专业背景的教师可以与具有人工智能专业背景的教师合作，共同设计和开发人工智能时代的计算机网络安全课程教学内容和实践项目。同时教师团队还可以和企业进行产学研合作，为企业解决实际的网络安全问题，提高教师的实践能力和社会服务能力。

结语

人工智能时代的到来，给计算机网络安全课程教学带来了新的机遇和挑战。通过更新教学内容，创新教学方法，强化实践教学，加强师资队伍建设等一系列改革路径的实施，使计算机网络安全课程教学更好地适应人工智能时代的发展需要，培养出具备扎实理论基础、熟练实践技能、创新思维的高素质计算机网络安全专业人才。这些人才将会在今后的工作中，为保证网络系统的安全稳定运行，推动网络安全行业的发展做出重大贡献。与此同时，计算机网络安全课程教学改革是一个持续的过程，需要高校、教师以及企业的共同努力，不断探索与创新，以适应不断变化的网络安全环境和行业需求。

参考文献

[1] 班海琴．网络安全与执法专业计算机网络实验课程教学改革研究 [J]．电脑知识与技术，2024,20(22):133-136.

[2] 曹小颖．大数据时代计算机网络安全课程教学改革路径研究 [J]．网络安全技术与应用，2023,(12):99-101.

[3] 刘振华．探讨大数据视域下的网络安全课程教学改革创新 [J]．江西电力职业技术学院学报，2022,35(03):52-54.

[4] 匡憨．高校计算机网络安全课程教学改革探讨 [J]．电脑知识与技术，2021,17(27):179-180.

[5] 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.

作者简介：肖琛，女，（1982 年 8 月），汉，学历：硕士研究生，职称：高级工程师，研究方向：计算机网络，泰山科技学院。