Advances in Social Sciences 社会科学前沿, 2022, 11(9), 3926-3932
Published Online September 2022 in Hans. http://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2022.119538

Hans汉斯

结合人工智能技术的网络空间安全专业课程建设探索

苑春苗[1]，孙　娜[1]，杨清永[2]

[1]天津工业大学软件学院，天津
[2]天津中德应用技术大学软件与通信学院，天津

收稿日期：2022年8月9日；录用日期：2022年9月10日；发布日期：2022年9月16日

摘　要

本文结合人工智能在网络空间安全的应用情况，探索结合人工智能的网络空间安全专业课程建设，进行多样性、智能化和多模式的网络空间安全课程教学内容建设和教学模式建设。

关键词

人工智能，网络安全空间，课程建设

Exploration on the Course Construction of Cyberspace Security Combined with Artificial Intelligence Technology

Chunmiao Yuan[1], Na Sun[1], Qingyong Yang[2]

[1]School of Software, Tiangong University, Tianjin
[2]School of Software and Communication, Tianjin Sino-German University of Applied Sciences, Tianjin

Received: Aug. 9th, 2022; accepted: Sep. 10th, 2022; published: Sep. 16th, 2022

Abstract

Based on the application of artificial intelligence in Cyberspace Security, this paper explores the construction of cyberspace security professional courses combined with artificial intelligence, and carries out the construction of diversified, intelligent and multi-mode teaching contents and teaching models of Cyberspace Security courses.

文章引用: 苑春苗, 孙娜, 杨清永. 结合人工智能技术的网络空间安全专业课程建设探索[J]. 社会科学前沿, 2022, 11(9): 3926-3932. DOI: 10.12677/ass.2022.119538

Keywords

Artificial Intelligence, Cyberspace Security, Curriculum Construction

Copyright © 2022 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

近年来，世界上很多国家都将网络空间安全作为国家战略计划，我国也自 2015 年起出台了一系列指导意见、法律法规来明确网络空间安全的战略意义。2016 年 6 月，中央网信办、教育部等联合发文《关于加强网络安全学科建设和人才培养的意见》，要求加快网络安全学科专业和院系建设，完善本专科、研究生教育和在职培训网络安全人才培养体系[1]。2017 年 6 月，《网络安全法》正式实施[2]。目前，绝大多数的大型政府机构、大型央企都已经组建了或正在组建自己的网络安全专业团队。但很多县、市一级的地方政府部门，大量的中小企业，都还普遍缺乏足够的网络安全建设能力，缺少相应的网络安全人才，甚至根本没有设置网络安全的相关岗位。因此，在《网络安全法》、国家网络安全等级保护制度的强力推动下，国内广大政企机构将会迅速形成对网络安全人才的紧迫需求，网络空间安全专业建设迎来良好契机。

网络空间专业涉及的核心知识领域包括计算机科学基础知识领域、网络空间安全基础知识领域、密码学知识领域、网络安全知识领域、系统安全知识领域和应用安全知识领域六个部分。目前专业课程偏重单纯的网络相关和网络空间专业相关知识，知识体系着重介绍网络基础原理和知识、网络安全原理和知识，知识体系单一，学科交叉程度低。随着近年来人工智能的快速发展，理论和技术自诞生以来日益成熟，应用领域也不断扩大，除了包括机器学习、深度学习、模式识别、语言识别、图像识别、自然语言处理等，在网络空间安全领域也有着很多应用，并且取得了显著成果，解决了以往的网络空间安全领域的技术难题，提升了算法效率。

因此本文拟结合人工智能技术在网络空间安全专业方向的最新研究进展和实际应用情况，对网络空间安全相关课程进行建设，进行多样性、智能化和多模式的网络空间安全课程内容和教学模式建设。通过重塑课程内容，增强网络空间安全专业和人工智能的结合度，增强学科交叉度，在教学过程中传授最新的网络知识和科研成果，从而开阔学生眼界、提升教学质量，将学术研究、科技发展的前沿成果引入课堂；通过探索创新的教学模式和方法，注重引导学生进行探究式与个性化学习，加大学习投入、科学“增负”，培养学生深度分析、大胆质疑、勇于创新的精神和能力。通过课程改革创新，进一步提升课程的高阶性、创新性和挑战度，培养专业创新性、复合型、应用型人才。

2. 建设思路和计划

人工智能是一门新的计算机科学技术分支，开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统，是认知、决策、反馈的过程[3]。人工智能由于其具有自学习能力、理解和推理能力、协同合作的能力，因此可以对不确定性数据进行快速处理，及时响应并能进行整体和综合分析，并可以根据以往信息对未知现象进行推理分析[4]。人工智能研究的主要内容包括知识表示、自动推理和搜索方法、机器学习和知识获取、知识处理系统、自然语言理解、计算机视觉、智能机器人、自动程序设计等方面，这些技术可以对网络空间防御进行辅助决策、快速响应以及海量数据处理等。

网络空间安全课程体系由主干学科、核心知识领域、专业核心课程及主要实践性教学环节组成。网络空间安全专业属于计算机类专业，其主干学科是计算学科学与技术、网络空间安全。专业核心课程包括高级语言程序设计、计算机网络、网络空间安全专业概论、网络攻击与防护、网络安全应用基础、入侵检测与防御、无线网络技术等。结合人工智能技术在计算机网络、网络安全、无线网络等领域的多种不同的应用及显著成果，我们拟根据人工智能技术在网络空间安全知识体系的应用情况，按如下思路进行建设：

1) 教学内容建设：结合人工智能在网络空间安全的应用，并考虑课程持续性及课程顺序选取代表性课程进行教学内容建设，在教学中增加人工智能在该领域的应用内容，从而可以使学生了解最新科技动态，开拓学生思路。

2) 教学方式探索：在进行教学内容建设同时，探索新的教学方式。探索开展翻转教学，分组教学等方式，改变传统以教师为主导的教学模式为学生主导的教学模式，增加学生学习主动性。

为保证建设效果，建设至少经过两个周期建设完善，建设计划如下：

第 1 周期：基础建设周期。根据课程性质和开设时间选取 4 门本科课程，包括计算机网络(学科基础课，第三学期)、入侵检测与防御(专业课，第四学期)、网络攻击与防护(专业课，第五学期)、无线网络技术(专业课，第七学期)进行教学内容建设，增加该课程与人工智能结合内容，设计与实施主动式教学模式，评价翻转教学效果、积累教学经验。修订教学大纲，设计示范性教学案例。对新增教学内容、学时和学习效果进行跟踪评价，优化教学方案。

第 2 周期：推广建设周期。在前期课程建设取得一定建设成果以后，总结课程建设中出现的问题，推广课程建设中总结出的经验，对其他专业课程进行建设，之后覆盖更多其他的网络空间安全专业课程。对建设的教学内容和教学模式进行持续改进并跟踪评价，对学生自主学习数据和达到的学习效果进行评价。

3. 课程内容建设

3.1. 计算机网络课程教学内容建设

计算机网络课程是网络空间安全专业重要的专业核心课程，直接关系着人才的培养。课程讲述计算机网络的核心概念、计算机网络体系结构和工作原理、各层协议的特点、原理及应用，以及常见计算机网络的技术特点。

在计算机网络中，存在着大量的网络流量数据，可以使用人工智能技术对网络流量数据进行分析、处理、搜索和分析，使计算机网络系统能够提供更加智能化、人性化的服务[5]。因此，对计算机网络课程教学内容进行如下建设：

1) 讲解 IP 协议时增加网络流量智能监测知识

网络流量监视软件可以通过对流经网卡的数据进行采集分析。在网络流量监测系统中使用人工智能的推理能力来对收集来的网络流量数据信息展开全面分析，智能分析出其中的异常流量并及时应对，可以有效的识别网络攻击、恶意网络流量。

2) 讲解应用层协议时增加智能网络综合管理知识

传统的网络管理由人工实现，费时费力，而借助人工智能的专家系统，实现网络的综合管理，对网络的负载均衡进行人工智能分析，解决网络管理中的技术问题。

3) 讲解电子邮件协议时增加智能反垃圾系统知识

智能反垃圾邮件软件系统使用人工智能技术通过扫描邮箱来维护用户邮箱的安全，搜索垃圾邮件和识别病毒邮件。利用人工智能技术对不可预见问题的处理能力和学习推理功能的处理技术，全面、高效地监控邮件内容，对邮件信息进行分类。

3.2. 网络攻击与防护课程教学内容建设

网络攻击与防护课程主要讲解网络安全概述、远程攻击的一般步骤、网络监听与防御技术、欺骗攻击与防御技术、Dos 攻击与防御技术、基于系统的攻击与防御、基于 Web 的攻击与防御、恶意代码攻击与防御等八个教学模块。

目前网络中由于漏洞存在，如何保护用户的安全成为越来越重要的问题。在网络安全中使用人工智能技术，可以更大程度地保护用户的隐私，提高用户安全感，增强用户信任感[6]。因此，对网络攻击与防护课程教学内容进行如下建设：

1) 在讲解防火墙部分知识时，增加智能防火墙技术

网络中设置防火墙可以有效的保护文件信息，以防文件信息被恶意窃取[7]。使用智能防火墙技术，可以解决传统的防火墙技术存在的缺点，如程序内容固定，可以改变传统的以手工方式逐个筛选信息，利用神经网络从海量的信息中找到丰富的特征值，降低网络危害，拦截不良信息，保护网络系统。

2) 增加介绍使用人工智能技术进行欺诈识别、僵尸网络监测、安全的用户身份验证、安全事件预测等网络安全领域知识。

3.3. 入侵检测与防御课程教学内容建设

入侵检测与防御课程介绍入侵检测的基本概念、分类；入侵检测系统的基本模型、工作模式、部署方式，其中重点讲解了入侵检测信息收集、信息分析、告警与响应三个过程；介绍入侵防御基本概念、分类与入侵检测的区别；入侵防御系统的功能、原理与部署、关键技术等。在讲解入侵检测部分知识时，增加智能入侵检测系统原理及应用讲解，具体内容如下：

智能入侵检测系统是一个能够检测、访问和检索档案信息的网页。有些网页只是信息过滤，但有些网页包含病毒或其他程序，以便于恶意窃取存档后的信息。应用人工智能可以访问页面中隐藏的程序进行检查，对一些入侵类型的程序可以及时发出安全警告，甚至执行及时封锁程序。

3.4. 无线网络课程教学内容建设

无线网络技术课程讲解无线网络的物理层、数据链路层概念；无线局域网、无线个域网原理及应用；无线传感器网络、移动 ADhoc 网络技术特点；以及无线网络安全等知识。近年来，无线网络技术新技术不断涌现，关键技术不断提升，应用在社会各行业，越来越多的研究将人工智能应用在无线网络技术上，通过与无线架构、无线数据、无线算法和无线应用结合，构建新型无线网络架构和空中接口，实现无线网络技术的突破[8]；通过人工智能技术优化聚类等方法实现无线网络的智能客户体验、负载均衡等[9] [10]。因此拟在无线网络课程的移动通信部分教学过程中增加以下和人工智能技术相关内容：

1) 增加新型无线网络架构知识

充分利用网络节点之间的通信能力、计算和感知能力，结合分布式学习、群智感知技术以及云技术，够构建新的网络生态，可以支持多种不同的人工智能活动，最终实现具有普适性的智慧感知、通信和计算能力的网络。

2) 增加新型空中接口知识

通过人工智能技术的学习能力增强数据平面和控制信令的连通性、效率和可靠性，定制技术模块，利用机器学习技术充分挖掘无线环境、资源、干扰以及业务的多维特性，优化能效，从无线使用信息中挖掘并重构未知的物理信道，设计最优的传输方式，提高频谱利用率，根据节点的传输反馈，动态调整波束方向，提高资源使用效率。

3) 增加智能业务体验保障知识

结合人工智能技术通过 QoE 预测与优化、空口状态预测等方式采集预测数据，如信噪比、信道质量信息、小区负载等信息，利用机器学习技术分析历史无线信号数据，指导网络策略进行 QoE 保障，优化和无线网络资源分配，优化业务的编码速率、压缩比、TCP 窗口，最终实现无线网络、传输和业务协同优化。

4) 增加智能负载均衡知识

通过引入小区场景聚类、强化学习、小区级/用户级预测、无线网络指纹地图等基础人工智能能力，动态学习网络切换、重选和负载均衡算法参数，优化负载均衡算法参数，预测小区负载、流量、用户业务流量、用户覆盖等信息，实现多频段的负载均衡，从而提升用户体验，提升无线频谱使用效率。

4. 教学模式建设

传统教学模式以教师为主导，不易激发学生学习动力，因此本次课程建设主要采取启发式教学，针对教学目的、内容及学生的知识水平，运用各种教学手段，采用启发式教学方式传授知识、激发学习兴趣，促使学生主动探索、发现问题、解决问题。根据以往的教学经验，本次课程建设采用翻转课堂教学模式和分组讨论教学模式。

4.1. 翻转课堂教学模式

翻转课堂教学[11]形式对课堂内外的时间分配作了重新调整，强调学生课前学习和师生课堂交流，极大地契合了“教师为主导，学生为主体”的教学理念。翻转课堂教学设计包含教学内容与难点、考察能力、教学策略、课前预习要求、翻转教学挑战度、学生参与设计和常见问题解决方案等部分。实施后，对教学效果评价并改进教学设计。

网络空间安全专业教师已经对翻转课堂教学进行了几年尝试，例如，无线网络技术课程近几年来都开展了翻转课堂教学，采用教师提前布置任务，要求学生提前自学无线网络相关技术，学生自主命题开展专业知识汇报。下表 1 为 2021 年学生翻转汇报主题汇总。

Table 1. Topics reported by students in flipped classroom of wireless network technology course in 2021
表 1. 2021 年无线网络技术课程翻转课学生汇报主题

分组	题目(自主命题)
1 组	基于 O-RAN 架构的无线网络(5G)嵌入式人工智能探索
2 组	无线与我们的生活
3 组	LPWAN 技术 Sigfox
4 组	Zigbee
5 组	家用 WiFi 组网思路
6 组	5G 的发展历程及 2020 年 5G 相关事件
7 组	基于 WiFi 信号的人体行为感知技术
8 组	红外技术
9 组	北斗系统
10 组	自强与创新——北斗系统的发展历程
11 组	神奇的北斗系统

2021 年汇报采用线上录制视频形式进行，从汇报结果可以看出，学生自学意愿强，选择学习汇报的内容丰富，汇报准备充分，一些分组同学对汇报视频进行了精心剪辑，并配有动画、音乐等，汇报视频制作效果良好，总体汇报效果较好，但也存在部分小组汇报时对原理汇报不深入、原理讲解不够清晰等问题。因此，在结合人工智能进行课程建设时，结合以往翻转课堂经验，对一些新颖的相关知识点，可以尝试开展翻转课堂形式教学，提前发布课前预习题目、课程讨论题目，充分激发学生的主观能动性，提高课堂效率，同时也要改进以往存在的问题。

4.2. 分组讨论教学模式

分组讨论教学[12]是目前常见的一种教学形式，通过布置分组任务，教师引导学生积极思考，通过讨论达到对教学内容的真正理解，培养学生探索问题的兴趣和思考能力；启发学生思考，帮助其领悟。目前网络空间安全专业多门课程已经采取过分组教学模式，部分应用见表 2。

Table 2. Implementation of group teaching of some cyberspace security courses
表 2. 部分网络空间安全课程分组教学实施情况

课程名	教学实施部分	分组人数	是否互评
计算机网络	翻转课	6	是
计算机网络	实验	6	否
计算机网络	综合实验	2	否
无线网络技术	翻转课	6	是
无线网络技术	实验	6	否
网络协议分析与设计实习	整个实习过程	2	否

在实施分组教学时，我们发现大部分学生可以充分利用分组优势，在教师指导下，对任务可以自行讨论，完成效果较好，但是也存在组内个别同学不积极问题。可以看出，分组教学更容易发挥学生特点和优点，有利于人才的培养；便于学生的交流合作，有利于增强学生的竞争与合作意识，强化学习动机。因此，在课程建设时，我们准备继续探索分组教学方式，除在翻转课、实验实习环节开展分组教学外，在常规课堂教学时也尝试选取一些容易引起讨论话题的内容开展分组讨论教学，激发学生主动学习兴趣，培养学生的分组合作能力、表达能力、组织能力、管理能力、以及问题解决能力，同时也通过加强组内自评和组间评价解决目前分组教学存在个别学生不积极问题。

5. 总结

现有网络安全技术一般采用静态防御方式，检测到攻击后响应，在功能上存在着很多弊端。人工智能技术目前已经广泛应用于社会各行各业，成功的解决了多种复杂的科学问题。采用神经网络、机器学习、自然语言处理等技术的人工智能技术可以对网络空间防御进行辅助决策、快速响应以及海量数据处理等，近年来在网络空间防御中涌现出大量的研究和成果。因此，本文结合人工智能技术在网络空间安全领域的应用，进行网络空间安全专业领域课程建设探索，从而更好的进行网络空间安全学科建设，开阔学生视野，增加学科交叉度，培养具备最新知识体系的网络空间安全专业人才。

基金项目

本文受 2021 年第二批产学合作协同育人项目(项目编号：202102535006)资助。

参考文献

[1] 姜建国. 网络安全保密学科建设与人才培养的实践和思考[J]. 保密科学技术, 2017(9): 16-20.

[2] 石倩. 我国《网络安全法》正式实施网络空间法制化进程实质性推进[J]. 网信军民融合, 2017(1): 48-53.

[3] 吴东杰, 王海伟. 人工智能背景下工匠文化融入教育教学研究[J]. 新一代: 理论版, 2021(8): 39-40.

[4] 李艳萍. 大数据时代下计算机网络技术中的人工智能应用——评《人工智能从入门到进阶实战》[J]. 中国科技论文, 2020(12): 1463.

[5] 谢晓广. 浅析大数据时代背景下人工智能在计算机网络技术中的应用[J]. 科学技术创新, 2019(5): 96-97.

[6] 苏玉燕. 基于人工智能技术的网络安全防御系统设计分析[J]. 信息记录材料, 2021, 22(9): 151-152.

[7] 孙晓东, 秦焕亮, 梁志军, 等. 智能工业防火墙新技术[J]. 自动化博览, 2018(5): 80-83.

[8] 田文强, 沈嘉, 肖寒, 等. 智启无线: 下一代智能无线通信系统的需求与构建[J]. 无线电通信技术, 2022, 48(4): 623-629.

[9] 谭翠平. 基于人工智能的 5G 无线网络优化[J]. 通讯世界, 2021, 28(7): 175-176.

[10] 李丽智, 刘志堃, 林亮. 基于人工智能的 5G 无线网络智能规划和优化[J]. 电子技术与软件工程, 2021(2): 26-27.

[11] 张萍, Ding Lin, 张文硕. 翻转课堂的理念、演变与有效性研究[J]. 教育学报, 2017, 13(1): 46-55.

[12] 于莎莉, 陈刚, 韦海燕, 等. 基于混合式翻转课堂教学模式在“环境卫生学”分组教学实践中的研究[J]. 教育现代化, 2020, 7(25): 89-92.