# 人工智能技术的发展及其在通信安全领域的应用

Development of AI Technology and Its Application in Communication Security

颜 博(北京凤凰汇通科技有限公司,北京 100028)
Yan Bo(Beijing Phoenix Huitong Technology Co.,Ltd.,Beijing 100028,China)

**摘 要:**
随着大数据、机器学习等创新技术的发展,人工智能技术越来越成熟化,在社会生活的多个领域得到了广泛的应用,极大地推动了社会进步,同时也给安全领域带来了挑战。对人工智能技术的发展和政策背景进行概述,对标准化现状进行了介绍,在分析应用于通信领域的人工智能技术的基础上,探讨了人工智能在通信安全领域的应用。

**关键词:**
人工智能;通信;安全
**doi:**10.12045/j.issn.1007-3043.2019.04.019
**中图分类号:**TN915.08
**文献标识码:**A
**文章编号:**1007-3043(2019)04-0086-04

**Abstract:**
With the development of innovative technologies such as big data and machine learning, AI technology becomes more and more mature, and has been widely used in many fields of social life, which has greatly promoted social progress as well as brought the challenge to security fields. It summarizes the development of AI technology, introduces the standardization. Based on the analysis of AI technology used in communication field, it discusses the application of AI in communication security field.

**Keywords:**
AI;Communication;Security

**引用格式:**颜博. 人工智能技术的发展及其在通信安全领域的应用[J]. 邮电设计技术,2019(4):86-89.

## 0 引言

近年来,云计算、大数据、深度学习技术的发展推动人工智能产业的进步,尤其是2016、2017年AlphaGo横扫中日韩顶级围棋高手在人工智能产业界引起了极大反响。可以看到,人工智能正在推动工业进入第4次发展浪潮,并逐步开始在农业生产、工业制造、交通驾驶、医疗健康、文化传播、投资金融等各个领域进入商用化阶段,推动人类生产、生活的革命性变化。不论是政府、企业还是用户,都期待人工智能技术的标准化应用。

**收稿日期:**2019-02-15

## 1 人工智能技术发展及其标准化情况

### 1.1 人工智能概念

人工智能在不同的发展阶段被赋予了不同的内涵。在1956年的达特茅斯会议上,麦卡锡首次提出人工智能概念。百度百科中对人工智能的定义是计算机科学的一个分支,它企图了解智能的实质,并生产出一种新的能以人类智能相似的方式做出反应的智能机器。

### 1.2 人工智能政策

人工智能已经开始在智能制造、智慧医疗、智能

家居等各行各业的产品中得到了应用。我国发布的《新一代人工智能发展规划》中提出，要加强人工智能标准框架体系研究，到2020年初步建成人工智能技术标准体系，包括人工智能基础共性、互联互通、行业应用、网络安全、隐私保护等技术标准，以及无人驾驶、服务机器人等细分应用领域标准，鼓励参与或主导制定国际标准，以技术标准“走出去”带动产品和服务“走出去”。工信部正在编写的通信行业《“十三五”技术标准体系建设方案》中，已经提出建立人工智能标准体系，研制网络、平台、终端、安全、智能化水平等关键标准。

### 1.3 人工智能标准化

在通信网和人工智能融合这一大趋势下，各个标准化组织已纷纷开展行动。2017年10月，ISO/IEC JTC1正式成立新的人工智能分技术委员会，进行人工智能相关的标准研究工作。目前包括中国、加拿大、德国、法国、俄罗斯、英国、美国等18个全权成员国，以及澳大利亚、荷兰等5个观察成员国。2018年4月18—20日，人工智能分技术委员会第1次全会在北京成功召开，会议讨论确定了组织架构，下设基础工作组、计算方法与AI系统特征研究组、可信研究组、用例与应用研究组，重点在术语、参考框架、算法模型和计算方法、安全及可信、用例和应用分析等方面开展标准化研究。而在此之前ISO/IEC JTC1已经发布了100余项人工智能相关的标准，基本形成了较为完备的标准体系。

欧洲电信标准协会于2017年2月成立了ISG-ENI，期望通过人工智能提高运营商在网络部署和操作方面的体验，同时，根据用户需求和环境条件变化等，自适应地调整网络服务。2018年1月，ETSI又建立了ISG-ZSM，囊括了40多个单位或组织，最初将专注于网络切片管理等研究。随后，ETSI发布了《自动化下一代网络中的网络和服务操作的必要性和益处》白皮书，强调5G网络中服务管理、运营自动化的目标。

国际电信联盟-电信标准化部门在2017年11月成立了未来网络机器学习焦点组（FG-ML5G），具体包括3个工作组，分别关注服务和需求、数据格式和机器学习技术、机器学习感知网络架构。重点研究机器学习、人工智能在包含5G系统的未来网络中的应用。FG-ML5G第1次会议于2018年1月29日—2月3日在瑞士日内瓦举行，就组织架构、工作组设置、相关工作内容等达成了一致。会议决议成立用例与需求工作组、数据格式与安全工作组、网络架构组3个工作组来推动网络智能化的工作。会议就通信网络基础设施无法有效满足机器学习技术使用条件现状、焦点组聚焦研究内容范畴、数据在机器学习应用中的重要性以及标准化缺失阻碍机器学习技术应用等方面的判断和需求达成共识，同时决定焦点组将致力于解决工业界使用人工智能技术遇到的技术及数据障碍，进行相关标准制定，并针对不同案例应用输出技术报告以起到规范行业、引领发展的作用。

IEEE在2017年11月下旬，发布了3项人工智能领域标准。包括“机器化系统、智能系统和自动系统的伦理推动标准”“自动和半自动系统的故障安全设计标准”和“道德化的人工智能和自动系统的福祉衡量标准”。

2017年5月3GPP SA2#121会议上，基于Big Data/AI的FS-eNA立项通过，2018年6月中国移动牵头立项3GPP RAN大数据应用研究。前者主要关注用于网络数据分析的必要数据以及必要的输出数据，后者则面向无线大数据的采集与应用。

## 2 人工智能技术

目前主流的人工智能应用中，最主要的是机器学习和深度学习，它们专门研究计算机怎样模拟人类的学习行为获取新的知识或技能，从而不断改善自身的性能。

### 2.1 监督学习

在监督学习中，每个训练数据组都是由一个输入对象和一个期望的输出值组成的，目标是得出输入和输出数据的函数关系，并推断其他输入数据可能的输出值。函数的输出可以是一个连续的值或是预测一个分类标签。监督学习中常见的算法有K-邻近、决策树、朴素贝叶斯、逻辑回归、支持向量机等。

### 2.2 半监督学习

半监督学习是监督学习与无监督学习相结合的一种学习方法，输入数据包括有标签样本数据和无标签样本数据，根据这些数据集训练习，输出一个学习机，对数据集或者外界的无标签样本进行预测，以便大幅度降低标记成本。其中包括一些对常用监督式学习算法的延伸，如图论推理算法、拉普拉斯支持向量机等。半监督学习既减少了获取大量样本标签的代价，又能够带来比较高的准确性，因此越来越受到人们的重视。

### 2.3 无监督学习

无监督式学习输入无标签数据，学习模型推断出数据的内在结构。常见的应用场景包括关联规则的学习、聚类和降维等。常见算法包括Apriori算法、K均值聚类、主成分分析降维以及神经网络中的自组织映射聚类等。

### 2.4 强化学习

强化学习基于智能实体与环境之间的动态交互。当智能实体感知到环境信息后，依据自己采取动作可能带来的奖赏或惩罚确定策略，并进一步观察环境的反应，循环往复，直至收敛至某一稳态状态。常见的强化学习应用场景包括调度管理、信息检索、过程控制、动态系统以及机器人控制等。常见算法包括Q学习以及时序差分。

### 2.5 神经网络

神经网络也叫人工神经网络，是受生物神经网络启发而构建的算法模型，常用于解决非线性回归和分类问题。一个简单的神经网络的逻辑架构包括输入层、隐藏层和输出层。输入层负责接收信号，隐藏层负责对数据的分解和处理，输出层输出整合结果。

### 2.6 深度学习

早先的神经网络算法比较容易过度训练，准确率依赖于庞大的训练集，训练速度受限于计算机，分类效果并不优于其他方法。深度学习算法可通过多隐层的神经网络逐层预训练进行特征学习，具有自学习功能、联想存储功能和高速寻找优化解的能力，适用于模式识别、信号处理、优化组合、异常探测、文本到语音转录等数据量庞大、参数之间存在内在联系的场景。神经网络也从单纯的监督学习转向半监督学习和无监督学习领域，并且可以实现分类器、生成数据、降维等多种功能。

## 3 人工智能技术在通信安全领域的应用

### 3.1 基于人工智能的网络异常流量检测技术

随着因特网规模的不断扩大和迅速发展，网络用户在得到了极大的便利的同时也受到了一系列的攻击。近几年来大规模的流量攻击事件层出不穷，给各国经济都带来了巨大的损失，网络安全已经引起了人们的高度重视。当用户在请求网络服务时，会产生相应的网络流量，而流量的监测是网络管理的重要组成部分，网络流量数据为网络的运行和维护提供了极其重要的信息，这些数据反映出了网络的资源分布情况和容量划分情况，能够对网络服务质量进行分析，对网络发生的错误和攻击进行监测和隔离，从而为网络用户提供安全可靠的服务。

针对异常流量的检测主要分为基于特征的检测和基于异常的检测。目前，各网络采取最多的入侵检测技术是特征检测技术。它通过匹配已经建立的规则和模型来检测已知的攻击，然而在对未知的攻击检测时，很难将未知的攻击与正常行为区分开来，往往需要不断更新规则库。新攻击的海量流量数据的不断增加给网络安全带来了极大的挑战，因此，基于特征检测的技术已经不适用于当前网络对攻击行为进行实时检测。基于异常的入侵检测，不需要建立规则库，但是由于传统的入侵检测系统无法有效地对零日攻击进行检测，网络安全面临的挑战依然严峻。

以上网络安全问题，在工业界和学术界都引起了广泛的重视，各国政府机构出台了一系列政策，大力改善网络安全问题。入侵检测概念最早于1980年提出，并提出利用审计信息跟踪用户可疑行为的入侵检测方法。接下来的20年间，又陆续提出了各种入侵检测模型。近2年我国政府将“维护网络安全”写进政府工作报告，将这一计划上升到国家战略，根据360公司在2016年底的中国互联网政企安全报告显示：全球化的网络安全领域各项技术正在全面加速推进，在安全防御方面以开放数据挖掘为代表的威胁新动向是未来安全研究的新趋势。进入21世纪以来，随着人工智能和大数据分析的快速发展，国内外应用机器学习和深度学习方法对入侵检测的研究开辟了新的研究道路。

目前网络异常流量检测所面临的主要问题包括：

a）高速网络环境的性能改善问题。高速网络环境下，网络的吞吐量非常大，需要从大量的流量数据中检测出网络入侵的具体类别，同时提高检测速度和准确率，降低网络的误报率和漏报率，把入侵造成的损失控制在最小限度内。

b）入侵检测系统主动防御能力不足。大部分入侵检测系统是以检测漏洞为主，依靠漏洞库实现入侵检测，对于漏洞库中不存在的攻击，很难实现检测，一般只有在攻击发生后，才添加到库，这样无法做到提前防御未知攻击，只能依赖漏洞库的更新。

c）入侵检测系统体系结构问题。集中式的入侵检测无法适应分布式攻击的检测，需要采用中央代理以及大量分布在各地的本地代理组成分布式入侵检

测系统进行检测。

根据以上异常流量检测所面临的问题以及人工智能和大数据分析的优势，有必要研究基于人工智能和大数据的互联网异常流量检测技术。利用网络产生的大量流量数据进行分析，及时发现检测可疑的用户和攻击行为，维护网络安全，为用户提供安全可靠的服务。

### 3.2 智能运维

机器学习和数据挖掘处理，用于运维中的隐患预测和动态巡检。通过同步运维数据，集中优化平台数据，实现动态监控，从多个维度对现场操作和维护指标进行特征画像，使用人工智能技术实时预测重要警报，找到关键监测点并制定动态检查计划。通过关联工单系统，自动输出诊断计划，提高工单派单准确性，实现智能化的运维。利用数据挖掘技术，早发现问题，从被动处理问题到主动预防问题，提升运维效率。

### 3.3 故障溯源

随着创新型技术的迅速发展，电信网络设备日趋虚拟化、自动化和智能化。电信网络系统的规模和复杂度的不断增加，维护变得越来越繁杂，运维人员还必须面对各种高度集成的设备产生的大量实时信息。当异常情况发生时，现有系统无法为运维人员提供足够支持，导致许多问题无法及时发现，且不断传播和升级，进而影响所有业务。如果发生异常警报时需要花费大量时间查找问题的根源并分析得出解决方案，小问题也会被升级。基于人工智能技术，可实现通信网络中的告警全局监控和处理，实时采集告警数据，实现灵活的过滤和可追溯性，可适当地分析和处理当前警报中的关键信息。通过对告警信息进行过滤、匹配，确定并分类告警信息，同时关联告警信息，实现溯源，从而屏蔽低级别告警，实现网络故障的快速诊断，并协调相应的通信业务模型和网络拓扑，实现准确的故障定位。为了实现可追溯性，需要建立故障分析模型，实现智能识别。关联规则算法定义为从一个数据集中发现项之间的隐藏关系。在大量的告警数据中，需要识别出告警间关联关系根故障分析模型，通过多个不同的维度进行识别，如发生模式或规律，这些固有发生模式或规律就是根故障分析模型。

因此，基于人工智能的故障诊断和可追溯性，在分析大数据关联规则和人工智能技术的基础上，综合网络和业务数据，对所有报警和性能监控数据以及日志进行综合分析，从而发现故障特征和故障原因的规则。在实际的网络运行和维护中，根据发现的故障特征自动匹配诊断规则，从而智能化地发现故障点，并且给出处理建议。

### 参考文献：

[1] 黄兵明，郭慧峰，赵良，等. 人工智能在通信网络故障溯源的应用研究[J]. 邮电设计技术，2018(12)：35-40.
[2] 佚名. 机器学习的分类与主要算法对比[EB/OL].[2019-02-25]. http://blog.csdn.net.
[3] 尤肖虎，张川，谈晓思，等. 基于AI的5G技术——研究方向与范例[J]. 中国科学：信息科学，2018(12).
[4] 林龙成，陈波，郭向民. 传统网络安全防御面临的新威胁：APT攻击[J]. 信息安全与技术，2013(3).
[5] 王西点，王磊，龙泉，等. 人工智能及其在网络优化运维中的应用[J]. 电信工程技术与标准化，2018(7).
[6] 刘积芬. 网络入侵检测关键技术研究[D]. 上海：东华大学，2013.
[7] 于成丽，安青邦，周丽丽. 人工智能在网络安全领域的应用和发展新趋势[J]. 保密科学技术，2017(11)：10-14.
[8] 袁媛. 人工智能与网络安全[J]. 内江科技，2009，30(12)：103-103.
[9] 张新福. 人工智能开启网络安全的新模式[J]. 信息安全与通信保密，2017(11)：30-35.
[10] 李云龙. 基于人工智能的网络安全技术研究[J]. 信息与电脑(理论版)，2017(6)：146-148.
[11] 范亮，陈倩. 人工智能在网络安全领域的最新发展[J]. 中国信息安全，2017(4)：104-107.
[12] 郭华. 基于人工智能的网络安全技术[J]. 电子技术与软件工程，2017(23)：181-182.
[13] 马秀荣，王化宇. 简述人工智能技术在网络安全管理中的应用[J]. 呼伦贝尔学院学报，2005，13(2)：65-66.
[14] 胡东星. 基于人工智能的信息网络安全态势感知技术[J]. 信息通信，2012(6)：80-81.
[15] 刘飞. 人工智能技术在网络安全领域的应用研究[J]. 电子制作，2016(17)：32-33.
[16] 肖继海. 基于人工智能理论的网络安全管理关键技术的研究[J]. 电脑开发与应用，2014，242(10)：35-37.
[17] 杨博文. 基于人工智能和物联网应用的网络安全管理[J]. 电子技术与软件工程，2017(17)：213-213.
[18] 严立忠. 2018年人工智能和机器学习三大趋势[J]. 软件和集成电路，2018(1)：19-21.

作者简介：
颜博，博士，主要从事人工智能技术及相关领域应用的研究工作。