人工智能若干前沿技术及其在信息对抗中的应用展望*

徐从富[1],陈 峰[2],范 晶[1]

(1. 浙江大学计算机学院,浙江杭州 310027;2. 浙江省公安厅科技处,浙江杭州 310009)

摘 要:讨论了机器学习、数据挖掘、统计学习理论与支持向量机的研究现状,简要介绍了近年来涌现的一些比较前沿的新方法,如概率图模型、马尔可夫逻辑网络等。在此基础上,结合信息对抗的需求和特点,初步探讨了这些AI技术和方法在信息对抗中的可能应用。

关键词:人工智能;机器学习;数据挖掘;信息对抗

Advanced Artificial Intelligence Techniques and Their Applications in Information Countermeasure

XU Cong-fu[1], CHEN Feng[2], FAN Jing[1]

(1. College of Computer Science, Zhejiang University, Hangzhou, Zhejiang 310027, China;
2. Department of Science & Technology, Zhejiang Provincial Bureau of Public Security, Hangzhou, Zhejiang 310009, China)

Abstract: In this paper, we discuss research advances in machine learning, data mining, statistical learning theory and support vector machine, and briefly introduce some novel artificial intelligence (AI) techniques that have just been presented in recent years, such as probabilistic graphical models, Markov logic networks etc. In the meantime, according to the requirements and characteristics of information countermeasure, we discuss some possible applications of the above novel AI techniques in information countermeasure.

Keywords: artificial intelligence; machine learning; data mining; information countermeasure

1 引言

人工智能(Artificial Intelligence, AI)[1] 50多年的发展可粗略地分为如下4个主要阶段:1)以符号逻辑推理方法为主的阶段,即AI初创的10余年间(1956-1969)。目前,AI界比较公认的观点是,符号逻辑推理方法更适用于高层的知识推理,而对于海量信息的处理能力则相对较弱。2)以知识工程及专家系统为主的阶段,主要是20世纪70-80年代,包括90年代初。专家系统及其开发工具已在医疗、军事等各领域中得到了广泛应用。3)以人工神经网络为主的阶段,主要是20世纪80年代中后期至90年代。其代表性成果为BP网及其应用,主要不足是其推广性没有理论保证,容易出现过学习、欠学习等问题。4)以统计机器学习方法为主的阶段,从20世纪90年代开始都属于该阶段。代表性成果是统计学习理论和支持向量机,以及一系列新的机器学习方法,

收稿日期:2007-07-24
* 基金项目:国家自然科学基金(No. 60402010);浙江省自然科学基金(No.Y105250)

其优势是建立在坚实的概率统计等数学基础之上。

在上述4个大阶段的同时，还涌现出其它研究方向[1]。例如：1)智能Agent及多Agent系统。自20世纪90年代中期开始，代表性成果有足球机器人、Web Spider等，Agent的观点是将AI领域目前分离的子领域重新组织为一个有机整体，目前其研究重点主要有增强学习(Reinforcement Learning)和大空间中的搜索(Search in Large Space)等。2)遗传算法与进化计算。起步于20世纪70年代，现在又重新成为AI界的研究热点之一，其应用效果虽较好，但理论基础仍不够坚实。3)软计算(Soft Computing)与粒度计算(Granular Computing)。主要代表有模糊集(Fuzzy Sets)、粗糙集(Rough Sets)等，其优点是可表达、处理模糊、含糊等知识，主要不足是理论基础仍有待继续完善。4)数据挖掘。20世纪80年代末开始兴起，目前受到国内外学术界和产业界的广泛关注，其应用性极强，较易受数据和需求的限制。

本文着眼于以统计机器学习方法为主的AI发展阶段，重点讨论机器学习、数据挖掘、统计学习理论与支持向量机的研究现状，同时简要介绍了近年来刚刚涌现的一些比较前沿的新方法，如概率图模型、马尔可夫逻辑网络等。在此基础上，结合信息对抗的需求和特点，初步探讨了这些AI技术和方法在信息对抗中的可能应用。

2　研究现状

2.1　机器学习

机器学习(Machine Learning, ML)[2-4]不仅是人工智能的核心内容，而且已成为整个计算机领域中最活跃、应用潜力最明显的研究方向，已成为智能系统的核心共性支撑技术之一。2001年9月出版的《Science》指出："机器学习对科学研究的整个过程正起到越来越大的支持作用，该领域在今后的若干年内将取得稳定而快速的发展。"

文献[5-6]指出今后10年间机器学习领域存在的5个挑战性问题：1)泛化能力。目前，泛化能力最强的两种技术是支持向量机(SVM)和集成学习，其中，SVM的产生途径是从理论(特别是统计学)到实践，而集成学习的产生途径则是从实践到理论。2)速度。目前，机器学习领域最关心的一个问题是"训练速度"与"测试速度"之间的关系，以及如何使这两者之间不发生矛盾。3)可理解性。绝大多数领域的学习或推理过程都希望有"可理解性"，而目前功能强大的机器学习方法基本上都是"黑盒子"。4)数据利用能力。当前，绝大多数领域都将面临着大量未标记的数据，含有大量噪声、属性缺失、不一致的"坏/脏"数据，以及"不平衡"数据等。如何充分利用这些没有标记的数据、"坏/脏"数据和不平衡数据是一个挑战性问题。5)代价敏感。不同领域所能容忍的错误代价并不一样，即使同一领域中不同的判断所对应的代价也不同。而传统的机器学习技术基本上只考虑同一代价，如何处理代价敏感性？这就带来了一个很大的挑战。近年来，不少学者将信号处理、医学诊断中的ROC(Receiver Operating Characteristics)分析方法引入机器学习领域，有望在这方面取得新的突破[7]。

2.2　数据挖掘

数据挖掘[8]兴起于20世纪80年代末，发展的势头十分迅猛。其研究内容主要包括：频繁模式和关联规则挖掘、聚类分析、分类和预测(如决策树等)、结构化数据挖掘(如序列挖掘、图挖掘等)、数据流/传感器网络和RFID数据库的挖掘、隐私保护数据挖掘、Web挖掘、多媒体数据挖掘、社会网络挖掘、生物信息学和系统生物学(System Biology)中的数据挖掘、文本挖掘等。因篇幅所限，下面简要介绍Web挖掘中的研究热点。

Web挖掘主要包括：Web的内容挖掘(即文本挖掘)、Web的结构挖掘(即图挖掘)、Web的用户日志挖掘。其中，文本挖掘是一个多学科交叉领域，涉及机器学习、统计学习、信息检索、自然语言处理等。当前，Web智能(Web Intelligence, WI)已成为AI与Internet密切结合的新秀之一。由于Internet上的资源取之不尽、用之不竭，将AI应用于Internet具有潜在的巨大商业价值，因此2006年美国人工智能大会(AAAI-2006)专门将WI设为新的研究专题。需特别指出的是，Web信息存在着良莠不齐的特殊性，"良"体现在Web信息的极其丰富，可对其进行深层次挖掘和利用，如研制网上商品的个性化推荐系统等；"莠"体现在网上充斥着各种虚假、有害信息，这就需要对这些信息进行甄别和过滤，如垃圾邮件过滤(Spam Filtering)已成为继搜索引擎之后的第二大研究领域。

3　最新动态

3.1　统计学习理论与支持向量机

统计学习理论(Statistical Learning Theory, SLT)[9]是一种专门研究有限样本(也称小样本)情况下机器学习规律的理论。而支持向量机建立在统计学习理论的VC维(VC dimension)理论和结构风险最小化(Structural Risk Minimization, SRM)原理基础上，根据有限样本信息在模型的复杂性和学习能力之间寻求最佳折衷，以期获得最好的推广能力(Generalization Ability)。支持向量机的主要

优点有:1)专门针对有限样本情况,其目标是得到现有信息下的最优解,而不仅仅是样本趋于无穷大时的最优值;2)算法最终将转化为一个二次型寻优(即二次线性规划)问题,解决了在神经网络方法中无法避免的局部极值问题;3)保证学习器(或分类器)有较好的推广能力,同时,它巧妙地解决了维数问题,且算法复杂度与样本维数无关。

目前,SVM算法在模式识别、回归估计、概率密度函数估计等方面都有非常成功的应用。例如,在模式识别方面,对于手写数字识别、语言识别、人脸图像识别、文本分类等问题,SVM算法在精度上已经超过传统的学习算法或与之不相上下。由于统计学习理论和支持向量机尚处于发展阶段,很多方面还不够完善,比如:在SVM方法中如何根据具体问题选择适当的内积函数至今还没有理论依据,等等。

3.2 概率图模型

2000年由美国加州大学柏克利分校(UC Berkeley)的Michael I. Jordan教授构建了概率图模型(PGM)的理论框架,该理论的代表为《An Introduction to Probabilistic Graphical Models》[10]。PGM的优点是具有坚实的数学基础,将不确定性知识推理映射为概率数据库(Probability Database)的查询过程,它涵盖有向图(贝叶斯网络、隐马尔可夫模型)和无向图(Markov随机场)等。PGM是概率论(Probability Theory)与图论(Graph Theory)的一次联姻,目前,它已成为AI之新宠,受到了广泛关注。

3.3 马尔可夫逻辑网络

近年来,美国华盛顿大学的Pedro Domingos教授提出了马尔可夫逻辑网络(Markov Logic Network,MLN),这是规则/逻辑(Rules/Logics)方法与统计学(Statistics)方法的一次联姻。在2006年的美国人工智能大会(AAAI-2006)上,Domingos教授作了题为《Unifying Logical and Statistical AI》[11]的特邀报告。马尔可夫逻辑网络的基本思想是,底层的学习利用统计机器学习方法,高层的推理用一阶谓词逻辑(产生式规则),其主要贡献是填补了传统的符号推理与当前非常热门的统计机器学习的"鸿沟",它是符号逻辑与统计逻辑的综合集成。当前,马尔可夫逻辑网络似乎已成为AI界的一匹黑马。

当前,其它新的机器学习方法不断涌现,例如,集成学习(Ensemble Learning)、增强学习(Reinforcement Learning)、流形学习(Manifold Learning)、多示例学习(Multi-instance Learning)、半监督学习(Semi-supervised Learning)、Ranking学习(Ranking for Learning)等等[12]。

4 应用展望

随着信息技术的飞速发展,信息对抗已成为现代战争的重要手段之一。信息对抗主要研究进攻与防御信息战技术系统及其决策支持系统,以及信息安全防护系统等。从电子战的角度来说,它包括通信对抗、雷达对抗、光电对抗、制导对抗、引信对抗、网络对抗等主要研究方向;从技术层面来说,它包括电子侦察与反侦察、电子干扰与反干扰、入侵检测、攻击源追踪等。为简便起见,下面以通信对抗中的通信侦察情报处理为例,初步探讨机器学习、数据挖掘等AI中的前沿技术在信息对抗中的可能应用。

4.1 机器学习在信息对抗中的应用展望

在实际的通信侦察过程中,借助于通信侦察设备可获得海量的通信侦察情报。但是,如何从这些数据海洋中准确快速地找出所要的电台及其网络?这是通信侦察中的难点问题之一。从机器学习的角度来看,这是一个非常典型的"无标记"数据的学习问题,而且由于存在电磁干扰、电子欺骗等手段,所以,又是一种"坏/脏数据"的学习问题。此外,敌军真实的电台及其网络所发出的数据占整个数据集的很少部分,因此,这又是一个"不平衡"数据的学习问题。对于"无标记"数据的学习问题,通常可采用如下的处理办法:对侦察到的部分样本信息进行人工标记,在此基础上,利用机器学习方法(如统计学习理论和SVM等)构造分类器,然后,对剩下的数据进行分类或预测。对于含有大量噪声、属性缺失、不一致的"坏/脏数据"的学习问题,可通过滤波、去噪、修补、矫正、嫁接等手段进行预处理,在获得比较"干净"的数据集的基础上,利用合适的机器学习方法进行分类和预测。而对于通信侦察中的"普通民用电台"样本要远多于期望侦察到的"敌方军用电台"样本的"不平衡"数据,由于该数据集呈现出一种稀疏分布的规律,这时可以采用流形学习方法进行聚类分析。

如前所述,通信对抗中同样存在代价敏感问题,即"将敌方军用电台误认为普通民用电台的代价"与"将普通民用电台误认为敌方军用电台的代价"是不同的。这时,可以采用ROC方法对分类和预测结果进行更合理的分析。具体地说,ROC方法有4个评价指标,分别是原本正确的被判定为正确的比率、原本正确的被误判为错误的比率、原本错误的被误判为正确的比率,以及原本错误的被判定为错误的比率。这样,就比原来简单地以正确率和错误率来判定更为科学合理。

4.2 数据挖掘在信息对抗中的应用展望

从数据挖掘的角度来看，对海量通信侦察信息进行分析处理则是一个典型的数据挖掘应用问题，而且更重要的是一个“孤立点”检测问题，因为真正需要挖掘出的“敌方军用电台”及其网络就是极为个别的、偶尔才出现的“孤立点”。如何判断这些“孤立点”究竟属于有价值的情报，还是一些噪声干扰或“毛刺”，这是数据挖掘中所要解决的重要技术问题之一，有很多方法可供尝试。至于通信侦察数据中的关联规则发现、时序数据挖掘等更是数据挖掘的强项，故不再赘述。

4.3 其它方法在信息对抗中的应用展望

在通信侦察情报分析中，在识别出“敌军电台”的基础上，一般需要进一步给出这些敌军电台所组成的通信网络。这时可以利用概率图模型（如贝叶斯网络等）来绘制出各电台之间的通联关系，并绘制出一张电台通联图，即为所求的通信网络。另外，因马尔可夫逻辑网络充分结合了传统的规则逻辑推理方法和当今热门的统计机器学习方法的优点，故在进行通信侦察情报分析处理过程中，对于海量的底层数据，可利用上述统计机器学习方法进行分类和预测，同时，可充分利用通信对抗专家在长期的实战中总结出的宝贵经验，并形成高层的推理规则（可形式化地表示成一阶谓词逻辑或产生式规则），以达到优势互补的目的，从而取得更好的效果。同样地，集成学习、增强学习、多示例学习、半监督学习、Ranking学习等方法都可以在通信对抗中找到用武之地。因篇幅所限，不再展开论述。

5 结束语

当前，虽然基于知识的智能系统已不再是AI领域的前沿，但在实际应用中仍大有用武之地，特别是与基于统计的机器学习方法相结合，将发挥很大的作用。而基于统计的机器学习方法虽如日中天，但困难依然存在，如SVM中的核选择问题至今悬而未决。至于数据挖掘及其应用，虽然挖掘方法已经很多，但往往出现比较尴尬的局面，即有技术能力的单位无法获得真实的数据和需求，而有真实数据和需求的单位，却缺乏人才和技术来进行数据挖掘。此外，需要特别关注的是国内外关于脑科学、神经信息学、脑机工程（Brain Machine Engineering，BME）等新兴交叉学科的最新成果，一旦这些新兴学科取得突破性进展，将对AI及其应用产生极大的推动作用，其前景十分诱人。

人工智能自诞生之日起就一直与军事应用领域密不可分，已在航空航天、情报分析、战场态势分析、军用智能机器人、智能化武器等方面得到了广泛、深入的应用，并取得了很好的成效。同样地，人工智能技术已在信息对抗领域得到了很好的应用，并将继续有力地促进智能信息对抗的发展。

参考文献：

[1] Russell S, Norvig P. 人工智能：一种现代方法[M].姜哲，金奕江，张敏，等译.第2版.北京：人民邮电出版社，2004.

[2] Mitchell T M. 机器学习[M]. 曾华军，张银奎，译.北京：机械工业出版社，2005.

[3] Mitchell T M. The Discipline of Machine Learning[R]. Technique Report, CMU-ML-06-108, July 2006.

[4] Mitchell T M. Does Machine Learning Really Work?[J] AI Magazine, Fall 1997, 18(3): 11-20.

[5] 周志华. 机器学习及其挑战 [EB/OL]. 2003-12-27.http://dragonstar.ict.ac.cn/workshop/ws023.ppt.

[6] 周志华. 机器学习的研究 [C/OL]// 国家自然科学基金委员会信息科学部AI战略研讨会，2005-06.http://www.intsci.ac.cn/research/zhouzh05.pdf.

[7] 徐从富，李石坚，王金龙. 机器学习研究与应用新进展[EB/OL]. 2006-10-17.http://www.cs.zju.edu.cn/people/xucf/Teaching.html.

[8] Han Jiawei, Kamber M. 数据挖掘概念与技术[M]. 范明，孟小峰，译.北京：机械工业出版社，2001.

[9] Vapnik V N. 统计学习理论的本质[M]. 张学工，译. 北京：清华大学出版社，2000.

[10] Jordan M I. An Introduction to Probabilistic Graphical Models [EB/OL]. http://www.cs.berkeley.edu/ ~jordan/publications.html.

[11] Domingos P, Kok Stanley, Poon H, et al. Unifying Logical and Statistical AI [C]// AAAI.Proceedings of 21st National Conference on Artificial Intelligence (AAAI-2006), Boston, MA, July 16-20, 2006: 2-7.

[12] 王珏，周志华，周傲英. 机器学习及其应用[M]. 北京：清华大学出版社，2006.

作者简介：

徐从富(1969-)，男，博士，副教授，硕士生导师，主要研究方向有人工智能、数据挖掘、信息融合等。

陈　峰(1970-)，男，高级工程师，主要研究方向为计算机应用等。

范　晶(1980-)，女，工程硕士，主要研究方向为人工智能、数据挖掘等。