仿生算法优化的神经网络在入侵检测中的应用综述

魏鹏1, [[1]](#footnote-1)†，姓名2，姓名1,\*

信息工程大学信息技术研究所， 河南，郑州，450001

联系人（魏鹏）：17638108216

摘要：至少5～6个整句，内容包括目的、方法、结果、结论（四要素缺一不可）等。摘要应以第三人称撰写，避免使用“本文”、“作者”等词汇。应写成报道性文摘，并具有独立性和自明性，即不阅读全文，就能获得全文的主要信息（特别注意所述内容均应包含在正文中，且数据一致）。不要重复题目，给出文中的主要信息、关键步骤或数据，以便于检索；篇幅：报道性的以300字左右，指示性的以100字左右，报道—指示性的以200字左右为宜；英文摘要一般与中文摘要内容相对应；缩写词首次出现时请给出全称，如：基质辅助激光解吸/电离飞行时间质谱（MALDI-TOFMS）。（字体：宋体，五号）

关键词：仿真算法；神经网络；入侵检测

**Title (Word Style “Times New Roman”)**

**The title should accurately, clearly, and concisely reflect the emphasis and content of the paper. The title must be brief and grammatically correct.** **The initial (first letter) of substantive words should be capitalized**

Author Name1,†, Author Name2, Author Name1,\*

(Word Style “Times New Roman”). All letters of family name and initial of first name should be capitalized (e.g., YANG Zhen-ning).

(1. *Address, Address, City Post Code, Country*;

2. *Address, Address, City Post Code, Country*)

**Abstract**: (Word Style “Times New Roman”). The abstract should briefly state the problem or purpose of the research, indicate the theoretical or experimental plan used, summarize the principal findings or the significant results, and point out major conclusions. All letters must be accompanied by an abstract containing about 250 words and at least 6 single sentences. Acronyms should be provided their full names, e.g., matrix-assisted laser desorption/ionization time-of-flight mass spectrometry (MALDI-TOFMS).

**Key words**: List 3-8 key words (Word Style “Times New Roman”, Acronyms should be provided their full names, e.g., gas chromatography-mass spectrometry (GC/MS))

# **0** 引言

从古至今，自然界就是人类产生各种技术和工程原理甚至重大发明的源泉，一直以来很多重要仿生学技术就推动着人类文明的发展。本文中提到了很多应用于入侵检测技术的仿生学算法，它们都可以通过优化神经网络来提高入侵检测技术的效率。其中的神经网络指的是人工神经网络，是一种模仿动物神经网络特征进行信息处理的数学模型，它在本文中用于对非法入侵数据的识别检测。常用的仿生算法有蚁群算法、人工鱼群算法、遗传算法等，它们在提升入侵检测系统性能方面发挥着很重要的作用。

# **1** 研究背景

## **1.1** 入侵检测技术、神经网络和仿生学

**1.1.1**入侵检测技术 入侵检测技术是指通过安全日志、行为、审计数据或从网络中收集到信息进行相关操作，从而检测到外界对系统的入侵或企图入侵行为的技术。入侵检测技术的目的是为了保护计算机而设计的可以及时发现报告系统中异常现象的技术，它可以用于检测计算机网络中非法入侵的行为。入侵检测系统采用的技术可以分为特征检测和异常检测。其中特征检测是假设入侵者活动可以用一种模式来表示，通过检测主体的活动是否符合这些模式来判断是否有入侵行为，异常检测则是通过将当前主体的活动情况与建立好的一个主体正常活动的“活动简档”相比较，若违反“活动简档”的统计规律则判断当前活动可能是一种入侵行为。

**1.1.2**神经网络 本文中应用于入侵检测技术的神经网络一般指的是人工神经网络，它是人工智能领域兴起的热点。从信息处理角度出发，人工神经网络是对人脑神经元的抽象，它是由大量的节点相互联结而成，其中每个节点代表一种输出函数，且每个节点可能有对应的偏置值，每两个节点之间的连接都有一个连接信号加权值，根据节点不同的联结方式就组成了不同的神经网络。神经网络有自学习、联想存储、高速寻找优化解等三个重要的功能。经过长期的研究和发展，它的应用领域已经十分广泛，在模式识别、自动控制、信号处理等反面都取得了非常大的成功。

**1.1.3** 仿生学 仿生学是一种利用生物结构和功能原理模仿自然界生物的一门学科，可以用来研制新技术和新设备等。仿生学能得到广泛应用，是因为有一些生物的功能比任何人工结构都要优越合理，本文中的仿生学优化算法就是利用自然界生物功能解决或优化工程上的一些技术问题，它们都能够取得比原算法更好的效果，能很好地体现它们的优化作用。很多生物有着很长的历史，甚至比人类存在时间还长。它们通过长期与大自然作斗争而不断进化，逐渐获得了适应大自然的能力和许多卓有成效的本领，并形成了极其精确和完善的机制，如体内的能量转换、信息的接受和传递、对外界的识别、导航等，显示出许多机器所不可比拟的优越之处。生物的小巧、灵敏、快速、高效、可靠和抗干扰性等特点也令人惊叹。

## **1.2** 入侵检测、神经网络和仿生学的发展历史

**1.2.1**入侵检测的发展历史 1980年，美国空军首次做了一份题为计算机安全威胁监控与监视的报告，详细阐述了入侵检测的概念。1984年-1986年，乔治敦大学首次研究出了一种实施入侵检测系统模型。1988年，SRI/CSL改进了乔治敦大学的入侵检测系统模型，并研发出了实际的IDES。1990年，加州大学戴维斯分校首次将网络数据作为审计检测数据的来源。1988年，美国重要部门、军队、实验室等开展对分布式入侵检测系统的研究，将基于主机和基于网络的检测方法集成在一起。20世纪90年代至今，入侵检测技术被争相研究，智能化和分布式入侵检测这两个方向取得了很大的进展。

**1.2.2**神经网络的发展过程 1943年，心理学家W·Mcculloch和逻辑学家W·Pitts首次提出沿用至今的神经元数学模型，他们两人是人工神经网络的先驱。1948年，冯·诺依曼提出以简单神经元构建再生自动机网络结构。19世纪50年代末，F·Rosenblatt设计了感知机结构，一种多层的神经网络。19世纪60年代初，Widrow提出一种自适应线性元件网络，一种连续取值的线性加权求和阈值网络，它就是人工神经网络的模型。19世纪80年代中期以来，神经网络引起了研究者的研究热潮。

**1.2.3**仿生学的发展历史 1940年，首次出现调节理论，将生物和机器的一般意义做对比。1944年，一些科学家也明确了机器和生物体内的通信、控制和统计力学的问题都是一致的。1947年，控制论学科由维纳等人提出，他将其定义为“关于在动物和机器中控制和通讯”，这个定义把机器和生物的认识联系在了一起。现实中有许多生物学应用于工程技术的实例，蝙蝠与雷达，电鱼与伏特电池，蛋壳与薄壳建筑等。1994年，中科院曾邦哲提出了系统生物工程与系统遗传学的概念与原理，是首次将仿生学与遗传学整合的系统生物工程的理念。1994年至今，仿生学已经广泛用于力学、分子学、能量学、信息与控制学等学科中，并发挥着非常重要的作用。

## **1.3** 基于仿生算法优化神经网络的入侵检测技术

遗传算法，是一类借鉴生物界的进化规律演化而来的随机化搜索方法，由美国的J.Holland教授1975年首先提出。黄勤等人在文献[1]中提出了一种改进的遗传算法来优化神经网络，解决了单独使用遗传算法不能在短时间内寻找到优化解的问题。蚁群算法是一种用来寻找优化路径的概率型算法。它由Marco Dorigo于1992年在他的博士论文中提出，其灵感来源于蚂蚁在寻找食物过程中发现路径的行为。吴春琼在文献[2]中提出了一种改进蚁群算法来优化神经网络，克服传统神经网络权值确定难度大、收敛速度慢等问题。变异粒子群算法，也称粒子群优化算法或鸟群觅食算法，J. Kennedy和R. C. Eberhart等在1995年开发的一种新的进化算法。宋玲等人在文献[3]中通过使用变异粒子群算法来优化BP神经网络，使神经网络具有更好的精度和收敛速度。人工鱼群算法是李晓磊等人于2002年在动物群体智能行为研究的基础上提出的一种新型方盛优化算法，该算法根据水域中鱼生存数目最多的地方就是本水域中富含营养物质最多的地方这一特点来模拟鱼群的觅食行为而实现寻优。朱小华在文献[4]中通过人工鱼群算法来优化神经网络，提高了入侵检测的效率和准确率。人工蜂群算法是一个由蜂群行为启发的算法，在2005年由Karaboga小组为优化代数问题而提出。沈夏炯等人在文献[5]中利用人工蜂群算法来优化神经网络，避免神经网络陷入局部最优和收敛速度慢的问题。猴群算法是于2008年由Zhao和Tang提出的一种新的用于求解大规模、多峰优化问题的智能优化算法。黄晓等人在文献[6]中利用猴群算法来优化BP神经网络，可以有效避免神经网络陷入局部最优值。蝙蝠算法是Yang 教授于2010年基于群体智能提出的启发式搜索算法,是一种搜索全局最优解的有效方法。 刘羿在文献[7]中利用蝙蝠算法来优化神经网络，提高了入侵检测的正确率。

# **2** 入侵检测中优化神经网络的仿生算法

## **2.1** 基于遗传算法优化的检测方法

遗传算法模仿了达尔文生物进化论和遗传学机理的生物进化过程，通过模拟自然进化的过程达到搜索最优解的目的。但由于仅仅使用遗传算法不能在短时间内寻找到接近最优解的问题，于是采用改进的遗传算法来提升入侵检测的效率。可以先用遗传算法优化BP神经网络权值或阈值的主要思想是：首先，用遗传算法对初始权值或阈值的分布进行优化,在解空间中找出一个较好的搜索空间；然后，再用BP算法在这个较小的解空间中搜索出最优解。用改进的遗传算法优化神经网络权值(阈值)能够更好地防止搜索陷入局部极小值算法来优化神经网络权值。

## **2.2** 基于蚁群算法优化的检测方法

蚁群算法模拟蚂蚁整体觅食过程中所表现出的智能行为。蚁群可以在不同环境中寻找到到达食物的最短路径。它们在搜索食物的途中可以释放一种类似与信息素的物质，其他经过相同路径的蚂蚁对这种信息素会有感知，随着信息素浓度会越来越高，蚂蚁会沿着信息素浓度高的路径行走，于是便逐渐找到一条通往食物的最短路径。蚁群算法是一种寻找优化路径的几率型技术，与具体问题关系并不大，于是相关研究者便提出一种改进的蚁群算法。这种改进的蚁群算法以蚁群算法和量子遗传算法为基础，借鉴了这两种算法的优点，并且摒弃了不足。首先通过量子遗传算法获取信息素分布，每组代表蚂蚁实时位置信息的量子比特分别由一只蚂蚁携带。第一步，以信息素强度以及可见度构造选择概率为主要依据，制定蚂蚁前进目标；第二步，对于蚂蚁所携带的量子比特，要利用量子门进行更新; 蚂蚁位置变异的实现则需要利用量子非门；第三步，以变动后的位置为主要依据，更新蚁群信息素的强度以及可见度。

## **2.3** 基于粒子群优化的检测方法

粒子群算法模拟的是鸟群的捕食行为，描述的是一群鸟在搜索一块食物，它们都不知道鸟具体在哪个位置，只知道它们离食物的距离，为了能够找到这块食物，可以通过搜寻目前离食物最近的鸟类的邻近范围来寻找这块食物。但是基本粒子群算法容易陷入局部最优并出现过早收敛问题，故相关研究者提出一种变异粒子群算法来解决容易陷入局部最优的问题，并提高了求解高维函数时的搜索精确度。

## **2.4** 基于人工鱼群算法优化的检测方法

人工鱼群算法模拟的是鱼类的觅食、聚群等行为，在某一片水域中，鱼类通过自行或者尾随其他鱼类找到营养物质最多的地方，也就找到了鱼生存数目最多的地方。人工鱼群算法中鱼类有四种行为，觅食行为，随机游动的鱼向食物逐渐增多的地方游去；聚群行为，游动过程中的鱼为了生存或躲避危害会自然聚集成群；追尾行为，当鱼群中一条或多条鱼发现发现食物时，临近的鱼群会尾随其后赶往食物点；随机行为，单独的鱼为了可以更大范围寻找食物或者伙伴，一般都是随机游动的。

## **2.5** 基于人工蜂群算法优化的检测方法

人工蜂群算法模仿了蜜蜂的觅食行为。蜜蜂是一种群居动物，单个蜜蜂行为非常简单，但群体表现出来的智慧令人惊叹，它们能够在任何环境下，以较高效率从食物源采集花蜜。蜂群产生的群体智慧模型有基本的三个组成要素：食物源、被雇佣的蜜蜂和未被雇佣的蜜蜂，和两个基本的行为：为食物源招募蜜蜂和放弃食物源。人工蜂群算法优化神经网络过程中，对权值和阈值进行了优化。当神经网络的自学习训练的准确性还不够时，可以把神经网络的误差函数作为人工蜂群算法的适应度，蜂群算法中蜜源的位置可以用权值和阈值来代替，每一个蜜源适应度都可以通过误差函数计算得到。蜂群算法通过采蜜过程可以得到最好的适应度和蜜源，然后比较每个蜜源的当前适应度和历史值便可以得到最好的一组蜜源，通过多次迭代后把最优的蜜源作为BP神经网络的权值和阈值。

## **2.6** 基于猴群算法优化的检测方法

猴群算法是一种模拟了猴群爬山过程的算法，是一种多群体智能算法，适合于解决多峰优化问题，它有三种动作，爬，迭代寻找局部最优解；望，对局部最优解的领域进行搜索，寻找更优解；跳，从当前解跳到更优解的过程。猴群算法不受优化问题的维数影响，和优化问题的可行域大小也无关，并且运行速度快，精确度也比较高。猴群算法可以用于优化BP神经网络，BP算法是一种局部寻优算法，可以通过使用猴群算法控制BP算法离开局部最优值。可以通过把代价函数描述为猴群算法的望和跳的目标函数，我们就可以实现优化神经网络，其中BP神经网络中的参数可以代表每个猴子i，在多维空间随机搜索寻找最优解。因为神经网络中代价函数有最小值，我们可以把神经网络局部最优值转换为求取函数最优值的问题。如果猴子跳跃成功，就顺利跳出局部最优值，从而神经网络的参数进入新的搜索空间，便实现了逼近全局最优解的目的。

## **2.7** 基于蝙蝠算法优化的检测方法

蝙蝠算法模拟自然界中蝙蝠利用声呐来觅食和规避障碍物的一种随机搜索方法，它将种群数量为m的蝙蝠个体，映射到多维问题空间的m个可行解，蝙蝠个体的移动和搜寻猎物的行为可以用，利用适应度函数值来确定蝙蝠所处位置的优劣。将蝙蝠算法用于优化神经网络时，神经网络的权值和阈值可以用来代表蝙蝠所处的位置，每一个蝙蝠都代表着一个网络，网络训练过程中，蝙蝠前后位置的变化则代表着权值和阈值的更新，每一次训练就代表对神经网络权值和阈值的更新，最终能找到最优的权值和阈值。

# **3** 入侵检测技术的发展趋势及应用前景

## **3.1** 入侵检测技术的发展趋势

**3.1.1** 高效智能入侵检测 当前入侵检测技术在算法、模型和方法方面有一定的发展，也有着自动化学习、自适应等特征，但是实际运用到应用当中就会出现各种问题，随着网络环境变得异常复杂、数据的泛滥、和入侵手段的提升，给入侵检测带来了很大困难。入侵检测技术的检测率的高低不同与环境条件有很大关系，可以通过调节阈值来使不同攻击在不同环境的检测率达到最好的效果。如何提升大数据环境下的处理能力和不同环境下阈值的自我调节都是未来的研究重点。

**3.1.2** 无线网络入侵检测 随着移动互联网技术的发展，无线网络的安全已经引起了人们的广泛关注，但是相比于有线网络安全并不是很成熟，还有很大的发展空间。在大规模复杂的环境下，如何提高无线网络入侵检测的效率以及满足大量无线网接入用户，是无线网络未来入侵检测的研究目标。

**3.1.3** 多学科融合 入侵检测技术是一门基于人工智能、计算机科学等的交叉学科，它可以通过、计算机免疫学和法学相融合形成一门新的技术，计算机取证技术引起了人们争相研究。多学科的融合扩大了入侵检测技术的引用范围，并有效提高了相关应用的效率。

**3.1.4** 面向Ipv6的入侵检测技术 随着互联网用户的增多，网络地址被大量占用，当前的IPv4资源有限，采用32位地址长度，制约着互联网的发展。IPv6采用128位地址长度，它的出现解决了资源数量不足的问题，并解决了多种接入设备接入互联网的障碍。目前的入侵检测技术是针对IPv4协议的，其在IPv6协议失去了作用。虽然IPv6解决了IPv4的部分安全性方面的问题，例如在网络层实施一些安全措施，为上层提供可靠的服务，但也还是存在部分安全问题。所以IPv6协议下的入侵检测成为了人们新的研究热点，IPv6只是针对IP协议发生了一些改变，其它层协议并没有发生改变，对于其他层照样会存在和IPv4相同层的安全问题。另外IPv6协议本身也存在一些安全隐患，会引起新的网络安全问题的发生，这个时候对于IPv6下入侵检测技术的研究非常有必要。

## **3.2** 入侵检测技术的应用前景

**3.2.1** 云计算下的入侵检测 随着分布式计算技术和互联网应用的发展，云计算已经成为了一种成熟的技术。云计算是一种按照使用量付费的模式，它通过提过网络、服务区、存储等资源，满足互联网用户的各方面需求，这些资源都可以被快速提供而且与服务供应商的交互很少。随着云计算的普及，也面临越来越多的安全问题，如何加强对云服务的安全保护，防止黑客恶意窃取用户数据等网络资源已经成为了一个重要的研究问题。但是云计算是一个异构虚拟的环境，不可能直接将入侵检测技术应用于云计算，必须要开展面向云计算环境的入侵检测技术研究工作，保证云计算服务的安全防护能力。

**3.2.2** SDN下的入侵检测 随着服务器和互联网用户人数规模的激增，传统的TCP/IP网络架构已经逐渐无法满足当前的环境，研究者们开始越来越多地提到新型网络体系结构概念。SDN便是新型网络体系结构的一种，其核心技术将控制层面和应用层面相分离，实现了网络虚拟化并带来了可编程的特性。新的网络体系结构的兴起，引发了来自各方面的安全问题，重要性不亚于原有体系结构，其安全问题主要在控制层面、数据层面和应用层面上。随着网络体系架构和协议的改变，当前入侵检测系统也不再适用于新的网络体系架构，如何研究SDN环境下入侵检测技术成为了一个越来越重要的问题。

**3.2.3** 物联网下的入侵检测 随着物联网的应用研究受到广泛关注，物联网的安全问题也日益凸显。物联网涉及民生、工业和军事等各个领域，其网络安全非常重要。若黑客入侵、恶意病毒的破坏造成的损失将比传统网络类似情况范围更大、影响更广。传统的安全机制相对比较被动，不论如何升级和更新都会被入侵者找到漏洞，然后进行攻击行为，而入侵检测却可以主动为网络进行安全检测并进行相应的措施，在很大程度上弥补了安全防御的不足。

**3.2.4** 拟态防御与入侵检测技术相融合 随着网络安全环境越来越复杂和网络入侵行为越来越普遍，新的网络安全技术应运而生，拟态防御技术就是为了应对当前网络安全易守难攻的现状，由邬江兴提出的一种主动防御技术。拟态防御技术思想类似于自然界生物的拟态防御功能，在网络空间防御领域，在目标对象给定服务功能和性能不变前提下，其内部架构、冗余资源、运行机制、等环境因素，以及可能附着其上的未知漏洞后门或木马病毒等都可以做策略性的变化，从而达到扰乱攻击者的目的，使其的攻击难度大大增加。新的网络技术和传统网络安全技术相结合产生的作用非常巨大，比如，通过拟态防御技术和入侵检测这种传统安全技术相结合，利用拟态防御技术构筑第一道外部防线，将大部分的入侵行为拒之门外，而入侵检测技术可以构筑第二道防线，也就是内部防线，将那些漏网的攻击行为一网打尽。

# **4** 结论

随着各种新型网络病毒的研发以及黑客入侵手段的多样化，对网络的安全造成了极大地威胁，为了应对各种威胁，必须不断创新入侵检测的手段，或者与新技术相融合，提高入侵检测的效率。本文中入侵检测技术与仿生学相结合，仿生学算法利用自然界生物功能解决或优化了应用于入侵检测技术的神经网络，它们能很好地提高入侵检测的效率。当前的入侵检测技术并不完善，还有很大的发展空间。通过将入侵检测技术与其他学科相融合或引入新的技术，入侵检测技术才可能有效应用于未来的许多环境，例如物联网、云计算或新型网络体系结构中。如何创新入侵检测技术并使其应用于云计算等新的环境中成为了当前的研究重点。

参考文献**：**（五号，黑体，左起顶格）

参考文献择主要的列出，按先后引用顺序编号。参考文献必须是公开发表的、文中直接引用的，著录项目要齐全，**在每篇参考文献的结尾列出该文献的出处(出自那个数据库？来源与哪个网站？……)**。参考文献录入请严格按照下面的格式：

1. **小五，宋体，英文和数字用“Times New Roman”，中国人和外国人的姓名一律采用姓前名后著录法，英文名缩写为首字母，缩写名后不加点“．”，**作者是三位的必须全部列出，四位作者以上的列出前三位作者，然后用“等”（英文文献“et al”），**英文题名实词的首字母大写，**起止页码用“～”，结束处用英文句号“.”。
2. 著者. 篇（题）名[J]. 刊名，出版年，卷号（期号）：起止页码. **期刊－连续出版物（J）**
3. **主要著作责任者. 书名[M]. 版次[第一版可略]. 出版地：出版者，出版年： 起止页码.** **专著（图书）（M）**
4. **作者. 篇（题）**名**[D].学位授予单位. 保存地点：保存单位，年. 学位论文（D）**
5. **作者（报告人）.题名.见（In）：编者（ed，eds）.会议录或会议名，会址：开会年. 出版者，出版时间：页码.** **会议文献**
6. **专利申请者（所属单位）.专利题名[P].专利国别：专利号，出版日期. 专利文献**
7. **起草责任者．标准代号 标准顺序号—发布年 标准名称．出版地：出版者，出版年.（也可略去起草责任者、出版地、出版者和出版年）标准文献**

**例如：**

[1] 张晓帆, 何明一. 基于FDK法的三维 CT快速计算方法. 计算机工程与应用, 2004.(维普数据库)

[22] NVIDIA’s Next Generation CUDA Compute Architecture Fermi, NVIDIA Corperation.(NVIDIA官方网站)

1. 基金项目：项目名称（编号）

   †作者简介：姓名：魏鹏（出生年：1994），性别：男（民族：汉）籍贯：湖北武昌，职称或学历：研究生，研究方向或专业：信息与通信工程。E-mail: willerise@163.com

   \*通讯作者：姓名：魏鹏（出生年：1994），性别：男（民族：汉），籍贯：湖北武昌，职称或学历：研究生，研究方向或专业：信息与通信工程。E-mail: willerise@163.com [↑](#footnote-ref-1)