摘要

随着计算机技术和网络技术的迅猛发展，计算机系统已经从独立的主机发展到复杂的、互联的开放式系统，这种情况导致计算机及网络的入侵问题越来越突出，为保护系统资源，需要建立不同于防火墙和防病毒软件的主动防御机制检测入侵。入侵检测系统就是监控网络或计算机系统的动态行为特征并据此判断是否有入侵的主动防御措施。入侵检测技术作为确保计算机网络信息安全的一个重要手段正成为信息安全领域的研究热点之一。入侵检测系统的运行机理与人体免疫系统有着天然的相似之处，人体免疫系统成功保护肌体免受各种侵害的机理为研究入侵检测提供了重要的方法。

基于免疫学的入侵检测是近几年来入侵检测领域研究的热点，它的突出特点是利用生物免疫系统的原理、规则与机制来实现对入侵行为的检测和反应[1,2,3]。目前多数商业化的入侵检测产品采用简单模式匹配技术，它只适用于较简单的攻击方式且误报率高，只能检测出已知攻击模式。而基于免疫原理的入侵检测系统能够利用不完备信息检测出未知攻击模式，具有很强的现实意义。

在入侵检测系统中，初始检测器的生成是非常关键的一步，它关系到整个系统的检测速度和效率。本文在深入学习免疫学原理与人工免疫系统工作机理的基础上，分析了现有的几种检测器生成算法，主要对否定选择过程中检测器生成方法进行了深入的研究。在分析已有的算法基础上提出了一种新的基于海明距离的检测器生成算法，通过使用模板来消除冗余的检测器，从而提高系统的检测效率。最后本文通过实验分析了算法的性能，实验表明，新算法能够尽可能多的覆盖“非我”空间，在性能上优于传统的否定选择算法，为进一步研究入侵检测系统提供了一种新的算法依据，为计算机安全领域引入了新的思路。研究入侵检测算法具有广泛的应用前景。

关键字：入侵检测 人工免疫系统 否定选择 检测器生成算法

Abstract

With the development of computer and technologies, computer system has been developed to a complicated and interconnected opening system, which results in more serious problems of intrusion detection. Intrusion detection system (IDS) is a system that continuously monitors some dynamic behavioral characteristics of network or computer system to determine if an intrusion has occurred. The intrusion detection technique is an important method to insure the computer network security. It is becoming one of hot research topics in information security field. The operating mechanism of intrusion detection systems is naturally similar to the human immune system. The theory that the immune system can protect body from invasion provides an important approach to investigating the intrusion detection technique.

In recent years, immune-based intrusion detection technology has become a key research field in intrusion detection system. Its prominent character is that it can explore natural immune logical theories, mechanisms and principles for detecting and reacting to intrusions.

At present, the majority of commercialized intrusion detection products just adopt the simple template match technique, which can be only adapted for some simpler attack modes with a high misrepresentation rate and just can detect known attack modes. Whereas immune-based intrusion detection system can detect unknown attack modes according to immature information, which has great actual significance.

The generation of detector is an important stage in the intrusion detection system. On the basis of studying the immune theory and the working mechanism of artificial immune system completely the

paper analyses some detector generating algorithms and the paper mainly researched on the detection generation algorithms applying in the process of negative selection . By the analyses on the existing detector generating algorithms, a new algorithm of detector generation based on Hamming distance is introduced. The efficiency of detecting is improved by using model and eliminating the reluctant detectors. At last, some experiments of new algorithm are given . The results show that the new algorithm can cover the non-self space as much as possible and has better affect than traditional negative selection algorithm. The work can provide a new method to study intrusion detection system. The proposed detector generating algorithms has great potential.

Key words: Intrusion detection, Artificial immune system, Negative selection, Detector generating algorithm

华南师范大学学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确的方式标明。本人完全意识到本声明的法律结果由本人承担。

论文作者签名：

日 期：2007年 6月 3 日

学位论文使用授权声明

本人完全了解华南师范大学有关收集、保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属华南师范大学。学校有权保留并向国家主管部门或其指定机构送交论文的电子版和纸质版，允许学位论文被检索、查阅和借阅。学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印、数字化或其他复制手段保存、汇编学位论文。（保密的论文在解密后遵守此规定）

保密论文注释：本学位论文属于保密范围，在___年后解密适用本授权书。非保密论文注释:本学位论文不属于保密范围,适用本授权书。

论文作者签名：　　导师签名：

日 期：2007年 6月 3日　　日 期：2007年 6月 3日

第一章 绪论

随着科学技术的飞速发展，人们已经进入了信息化时代，计算机技术和网络技术已经深入到社会的各个领域。大型信息系统将众多的计算机和智能化设备联接起来，共享丰富的数据库信息和计算机资源，完成异地的数据交换与通信。Internet 给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度越来越大。尤其是近年来网络上各种新业务的兴起，如网络银行、电子钱包和电子商务的快速发展，使得网络的重要性及其对社会的影响也越来越大，网络与人们的日常生活密不可分。然而，人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。人们在提供网络服务、参与网络活动的同时，往往只看到其便利、有益的一面，而降低了警惕性，忽视了潜在于网络中的安全问题。互联网具有天然的开放性和协议的简便性，它在展示其无所不能的强大威力的同时，也不可避免的伴随了大量的安全隐患。网络结构组织各方面的缺陷、系统与应该软件的漏洞，以及网络管理员的水平低下和疏忽大意，都可能使网络攻击者有机可乘，恶意的入侵者干扰正常业务、销毁或篡改重要数据，甚至使更多的服务器失去控制，造成一系列严重后果。因此，信息安全和网络安全的问题已经引起了各国、各部门、各行各业以及每一个计算机用户的充分重视。如何设计安全措施来防范未经授权的数据访问和非法的资源利用，是当前网络安全领域一个十分重要而迫切的问题。

目前，要想完全避免安全事件的发生是不现实的，安全管理人员所能做到的是尽量发觉和察觉入侵及入侵企图，以便及时采取有效措施来堵塞漏洞和修复系统。目前解决网络安全采取的主要技术手段有防火墙、安全路由器、身份认证系统等，这些防御手段对防止系统被非法入侵有一定的效果。防火墙是一种应用层网关，按照设定的规则对进入的网络的 IP 分组进行过滤，同时也能针对各种网络应用提供相应的安全服务。利用防火墙技术、经过仔细的配置，通常能在内外网之间实施安全的网络保护机制，降低风险。但仅仅用防火墙保障网络安全是远远不够的，防火墙技术属于一种表态、被动的防御措施，只能防御已知的计算机病毒，无法抵御未知

的网络入侵方式，所以不能从根本上解决安全问题。因此，对于一个安全的网络系统来说应该既要有防火强等防御手段，还要有能够对网络安全进行实时监控、识别攻击并进行反攻击的网络入侵检测系统。入侵检测系统（IDS）是近年出来的新型网络安全技术，是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术；是一种用于检测计算机网络中违反安全策略行为的技术；它的目的是检测出系统中未经授权的使用、滥用计算机资源的行为，保护资源的完整性和可用性，它是一个自动的过程。IDS 的应用，是使在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击，在入侵攻击中，能减少攻击所造成的损失，在被入侵后，收集入侵的相关信息，作为防范系统的知识，添加入知识库内，以增强系统的防范能力。IDS 能弥补防火墙的不足，为受保护网络提供有效的入侵检测及采取相应的防护手段。

1.1 IDS 的发展过程

IDS 是随着网络技术的发展而发展起来的一种保护网络安全技术，它从提出到现在主要经过了以下几个过程：

1.1.1 精简审计问题的提出

1980 年 4 月，James P. Anderson 为美国空军做了一份题为《Computer Security Threat Monitoring and Surveillance》（计算机安全威胁监控与监视）的技术报告，第一次详细阐述了入侵检测的概念[4]。报告中明确指出精简审计的目标在于从安全审计踪迹数据中消除冗余和无关的记录。Anderson 建议改变计算机审计机制以便为研究跟踪问题的计算机安全人员提供信息，他提出了一种对计算机系统风险和威胁的分类方法，并将威胁分为外部入侵、内部和外部不法行为三种，还提出了利用审计跟踪数据监视入侵活动的思想。因此这个报告被公认为是入侵检测技术研究的开创性文献。

Anderson 的报告清楚地阐述了安全审计机制的下列目标：

(1) 应为安全人员提供足够多的信息，使他们能够定位问题的所在；但

另外一方面，提供的信息要不足以使他们自己能进行攻击。

(2) 应优化审计跟踪的内容，以检测发现的问题，而且必须能从不同的系统资源收集信息。

(3) 对一个给定的资源，审计分析机制应当能分辨出那些看似正常的活动，以发现内部的计算机系统的不正当使用。

(4) 设计审计机制时，应将系统攻击者的策略考虑在内。

1.1.2 入侵检测专家系统（IDES）

从 1984 年到 1986 年，乔治敦大学的 Dorothy Denning 和 SRI/CSL（SRI 公司计算机科学实验室）的 Peter Neumann 研究出了一个实时入侵检测系统模型，取名为 IDES（入侵检测专家系统）[6]。该模型由六个部分组成：主体、对象、审计记录、轮廓特征、异常记录、活动规则。它独立于特定的系统平台、应用环境、系统弱点以及入侵类型，为构建入侵检测系统提供了一个通用的框架。这项研究由美国海军空间和海军战争系统司令部资助，它提出了反常活动和计算机不正当使用之间的相关性，是 IDS 早期研究中最重要的成就之一。IDES 模型基于这样的假设：有可能建立一个框架来描述发生在主体（通常是用户）和客体（通常是文件、程序或设备）之间的正常交互作用。这个框架由一个使用规则库（规则库描述了书籍的违例行为）的专家系统支持。这能防止使用者逐渐训练（误导）系统把非法的行为当成正常的来接受，也就是说让系统“见怪不怪”。Denning 于 1987 年发表的关于这个问题的论文，被认为是另一篇研究 IDS 技术的奠基性论文。1988 年，SRI/CSL 的 Teresa Lunt 等人改进了 Denning 的入侵检测模型，并开发出了一个 IDES。该系统包括一个异常检测器和一个专家系统，分别用于统计异常模型的建立和基于规则的特征分析检测，系统的框架如图 1.1 所示：

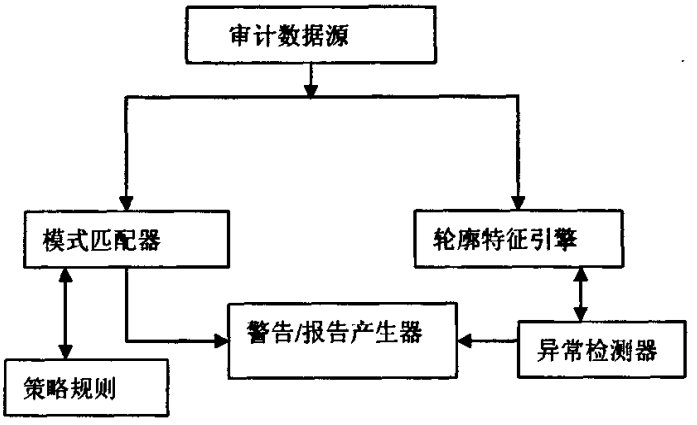


图 1.1IDES 的框架

Fig1.1 The Framework Architecture of IDES

Anderson 的报告以及 IDES 的研究导致了随后几年的一系列 IDS 系统原型的研究，如 Audit Analysis、discovery、Haysatck、MIDAS、NADIR、NSM、Wisdom 和 Sense 等。

1990 年是入侵检测系统研究发展史上的一个分水岭。这一年，加州大学戴维斯分校的 L、T. Heberlein[6]等人开发了 NSM (Network Security Monitor)。该系统第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异种主机。从此之后，入侵检测系统发展史翻开了新的一页，两大阵营正式形成：基于网络的 IDS 和基于主机的 IDS。混合型的入侵检测系统可以弥补一些基于网络与基于主机的片面性缺陷。此外，文件的完整性检查工具也可以看作是一类入侵检测产品，现在很多基于主机的 IDS 都集成了这个功能。

1994 年，Mark Crosbie 和 Gene Spafford[7]建议使用自治代理（autonomous agents）以便提高 IDS 的可伸缩性、可维护性、效率和容错性。1996 年提出的基于图的入侵检测系统（Graph-based Intrusion Detection System, Grids）[8,9]的主要目标也是解决绝大多数入侵检测系统伸缩性的问题。该系统使得对大规模自动或协同攻击的检测更为便利，这些攻击有时甚至可能跨过多个管理领域。这些年来，入侵检测的主要包括：1997 年 Forrest 等将免疫原理运用到入侵检测领域[10,11]。1998 年 Ross Anderson 和 Abida Khatrtak[12]将信息检索技术引进到入侵检测中。2000

年 Terran D. Lane 利用机器学习技术检测入侵[13]。

1.1.3 商业产品的出现

在过去的十几年中，人们研制出大量的入侵检测系统，但是其中许多只是纯粹的研究原型，目前并没有与之相对应的商业产品。本节将介绍那些已经成为市场上的商业产品的入侵检测系统，并对它们的特性进行简要的分析。下表中是一些比较常见的商业入侵检测系统[14]。

表 1.1 入侵检测系统商业产品表

产品	开发商
Real Secure	Internet Security Systems (ISS)
Intruder Alert	Axent Technologies, Inc.
Net Ranger	Cisco Systems, Inc
Stake Out I.D	Harris Communications, Inc
Kane Security Monitor	Security Dynamics (formerly Intrusion Detecton,Inc)
Session Wall-3	AbirNet
Entrax	Centrex Corporation
CMDS	Science Application International Corporation (SAIC)
SecrueNet PRO	MimeStar, Inc.
CyberCop	Network Associates, Inc.
INTOUCH INSA	Touch Technologies, Inc.
T-Sight	EnGarde Systems, Inc.
NIDES	SRI International
ID-Trak	Internet Tool, Inc.
SecureCom Suite	ODS Networks
PolyCenter	Compaq (formerly Digital Equipment Corp)
Network Flight recorder	Network Flight Recorder Inc.

Table1.1 Commercialized Intrusion Detection Products

1.1.4 非商用入侵检测系统

非商用入侵检测系统是以科学研究为主要目的，大多公开源代码。最著名的是 Snort，其他还有 SRI 公司的 NIDES 和 EMERALD，Purde 大学 CERIAS 小组的 ESP 等。

1.2 入侵检测研究现状

入侵检测是对面向计算资源和网络资源的恶意行为的识别和响应。入侵是指任何试图破坏资源完整性、机密性和可用性的行为，且还包括用户对系统资源的误用。作为重要的网络安全工具，它可以对系统或网络资源进行实时检测，及时发现进入系统或网络的入侵者，也可以预防合法用户对资源的误操作。IDS 通过对系统或网络日志的分析，获得系统或网络目前的安全状况，发现可疑或非法的行为。入侵检测被认为是防火墙之后的第二道安全门，在不影响系统或网络性能的情况下对对其进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

虽然入侵检测已有二十几年的发展历史，但仍是一种比较新的技术，尤其是在国内，它的兴起并没有多长的时间。因此，当前的入侵检测技术研究无论在理论方面还是技术方面都还有很多有待完善的地方。特别是在技术实现方面，随着网络技术的迅速发展，网络传输速度日益快捷，数据量空前膨胀，已有入侵检测技术越来越难以满足本地主机和网络系统的安全要求。

在入侵检测发展过程中，研究人员不断地探索新的开发思路和方法。尽管研究人员已经积极研究入侵检测二三十年，但其现状是入侵检测主流仍停留在研究和实验样品阶段，部分产品也是在近期才获得较广泛的应用。

IDS 的体系结构就是其各个组件在计算机网络上的分布，以及他们之间的关系。按照各个组件运行的分布方式不同，IDS 可以分为：集中式和分布式。几乎所有的 IDS 都是集中式的，而基于入侵检测自治代理[15,16,17]（Autonomous Agents for Intrusion Detection, AAFID）结构的 IDS 是分布式的。根据数据来源的不同，IDS 常被分为基于主机（Host-based）和基于网络（Network-based）的 IDS[18, 19]。前者在每个要保护的主机上运行一个或多个监控程序，以计算机主机作为目标环境，而后者收集网络传输的数据包，保护的目标是整个网络的运行。网络异常检测和入侵报警器（Network Anomaly Detection and Intrusion Reporter, NADIR）[20]是对网络各主机以及网络传输进行监视的 IDS，NSM 是只对网络传输监视的

IDS。

目前，大多数入侵检测系统主要采用行为统计[21]、专家系统[22]、神经网络[23,24]、模式匹配[25]、状态转换分析等技术[26]，分析事件的审计记录、识别特定的模式、生成报告和最终分析结果。但是随着网络入侵技术的不断发展，入侵行为表现出不确定性、复杂性和多样性等特点。使得在提取行为特征时，很难提供确定的统计模式，即便是专家知识也带有随机性、不确定性等因素。为保证检测的效率和正确性，尽管许多研究机构和大学、如著名的 Stanford Research Institute International、Purdue University 和 IBM 等一直从事这方面的技术研究工作，但仍没有获得突破性进展。因此运用新技术、新学科等加强入侵检测技术的研究十分必要。

1.3 现有入侵检测方法所存在的不足

入侵检测系统作为网络安全的关键性防范系统已经起得了一定发展，但仍然存在很多问题，还有待于进一步完善，以便为以后的网络发展提供有效的安全手段。从性能上讲，入侵检测系统面临的一个矛盾就是系统性能与功能的折衷，即对数据进行全面复杂的检验构成了对系统实时性要求很大的挑战。从技术上讲，现有的入侵检测系统主要是在检测方法上存在明显的不足，主要体现在：

（1）可扩展性方面

一个好的IDS应该能够根据其应用环境进行了灵活配置，检测方法不应该对检测系统的环境做出假设，否则将会影响检测系统的可扩展性。但像基于神经网络等方法的检测系统要么依赖于特定的类型操作系统[27]，要么依赖于特定的网络结构[28]。

（2）检测效率方面

实际的IDS通常很难检测出具有欺骗性的入侵。异常检测的计算代价非常大，因为系统维护的活动记录要随着每个事件更新。误用检测一般都采取专家系统shell来编码和匹配攻击特征，这些shell需要解释规则集，因而运行时刻费用很高，而且规则集合只允许间接定义序列事件的相互关系。现有IDS的性能不能够适应高速网络发展，特别是100M，Gigabit网的

应用。一种可行的解决方法是高速网络下IDS产品的负载均衡技术（Load balancing）[29]。

(3) 可维护性方面

维护一个IDS需要的技能远远超过专门的安全知识。更新规则集合需要了解专家系统规则语言，并理解系统如何处理这些规则，如此才能够避免系统中已有规则和新增规则之间不必要的关联，为统计检测模块增加新的统计变量时也存在同样的问题。

（4）可移植性方面

迄今为止的IDS都是为某个单一的环境构建的，很难直接应用于其他环境，即使它们具有类似的安全策略和安全目标。例如，将一个单层自主存取控制系统的检测部件移植到一个具有相同安全目标的多层安全系统就非常困难。这是因为IDS的大部分都是目标系统特有的，是为目标系统进行过定制的。这些系统的重用和重新定位都非常困难，除非系统一开始就设计成一种通用模式，但通用模式下的系统效率较低，且功能受限。

因此，IDS技术要想很好的为系统提供服务将面临着三大挑战：如何提高IDS的检测速度，以适应网络通信的要求；如何减少IDS的漏报和误报，提高其安全性和准确性以及如何提高IDS的互动性能，从而提高整个系统的安全性能。

基于人工免疫系统的入侵检测方法具有分布式、自适应、自治及健壮性等特点，而且检测效率高，可维护性好，有着广阔的发展前景。

1.4 论文的研究内容和组织结构

现代科学和技术的发展，正改变着传统的学科划分和科学的研究。“数、理、化、天、地、生”这些曾经以纵向发展为主的基础学科，与日新月异的新技术相结合，推出了横跨多学科门类的新兴领域，这已成为发展的一个重要特征。如人我免疫学科的兴起，为许多领域的研究提供了新的途径。本文将人工免疫学的新技术引入到入侵检测中，从新的角度来研究和探讨入侵检测技术。这一研究以生物免疫系统的阴性选择原则和不完全匹配等特性为依据，并使该入侵检测技术有免疫系统区分“自己”和“非

己”的本质特征。

1.4.1 研究内容

① 总结了入侵检测技术研究的前期成果，简单地概括了入侵检测技术的发展过程。

② 详细阐述了入侵检测技术的研究现状和未来的发展趋势，提出了现有入侵检测技术存在的不足之处，为将人工免疫技术引入到入侵检测中来做下铺垫。

③分析了自然免疫学基础和人工免疫系统的原理、框架、研究领域以及未来的发展方向和在IDS中的应用。

④ 分别分析和研究了几种不同的检测器生成算法，重点对否定选择算法进行了深入的分析，并在此基础上提出了一种新的检测器生成算法，并对其关键技术进行深入的研究。

⑤ 对新的算法进行实验，同时比较了在不同参数下两种算法的性能，分析了新算法的优缺点，并提出进一步所要做的工作。

1.4.2 论文的组织结构

本论文共分为六章，具体内容为：

第一章：论述论文的研究背景、入侵检测技术的发展过程、相关技术的研究现状、现有入侵检测技术存在的不足以及论文的研究内容和组织结构。

第二章：对入侵检测技术的基本概况，包括入侵检测系统的各种分类以及入侵检测技术的发展方向进行了综合论述。

第三章：人工免疫系统及免疫学基础概述。作为全文的理论基础，首先叙述自然免疫学基础知识，包括免疫细胞、免疫识别、受体多样性和免疫耐受等内容，是论文研究工作需要借鉴的免疫学原理知识。在此基础上探讨人工免疫系统（AIS），分析AIS与IDS的共性。

第四章：讨论入侵检测技术的几种基于否定选择的检测器生成算法，并

对它们进行深入的分析比较，然后在此基础上提出一种新的检测器生成算法

第五章：对新的算法进行了的实验，并与原有的算法进行性能上的比较，通过实验结果分析算法的可行性和算法有待改进的地方。

第六章：总结本文的工作和主要贡献，并给出一些有待进一步研究的问题。

第二章 入侵检测系统概况

2.1 入侵检测系统的CIDF模型

尽管各种入侵检测系统的功能和特性各不相同，但它们的核心结构非常相似，因为它们都是在通用入侵检测结构框架（Common Intrusion Detection Framework, CIDF）[30]的基础上发展而来的。CIDF最初是由美国国防部高级研究计划局（Defense Advanced Research Project Agency, DARPA）资助的入侵检测和响应（Intrusion Detection and Response, IDR）项目研究工作组设计开发的，它的设计目标是为不同类型的IDR子系统之间以及IDR不同构件之间实现信息共享和协同工作设计一组规范。CIDF的规格文档由四部分组成，分别为：

体系结构（The Common Intrusion Detection Framework Architecture）

规范语言（A Common Intrusion Specification Language）

内部通讯（Communication in the Common Intrusion Detection Framework）

程序接口（Common Intrusion Detection Framework APIs）

CIDF的体系结构文档阐述了一个标准的IDS的通用模型；规范语言定义了一个用来描述各种检测信息的标准语言；内部通讯定义了IDS组件之间进行通信的标准协议；程序接口提供了一整套标准的应用程序接口（API函数）。CIDF将IDS需要分析的数据统称为事件（event），它可以是基于网络的IDS从网络中提取的数据包，也可以是基于主机的IDS从系统日志等其它途径得到的数据信息。

CIDF组件之间的交互数据使用通用入侵检测对象（generalized intrusion detection objects，gido）格式，一个gido可以表示在一些特定时刻发生的一些特定事件，也可以表示从一系列事件中得出的一些结论，还可以表示执行某个行动的指令。CIDF将一个入侵检测系统分为以下组件：

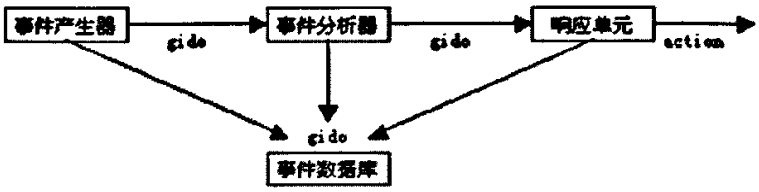


图 2.1 CIDF 组件

Fig 2.1 Common Intrusion Detection Framework

事件产生器（Event generators）：从入侵检测系统外的整个计算环境中获得事件，并以 CIDF gidos 格式向系统的其他部分提供此事件。事件产生器是所有 IDS 所需要的，同时也是可以重用的。

事件分析器（Event analyzers）：从其他组件接收 gidos，分析得到的数据，并产生新的 gidos。如分析器可以是一个轮廓特征引擎。

响应单元（Response units ）：是对分析结果做出反应的功能单元，它可以终止进程、重置连接、改变文件属性等，也可以只是简单的报警。

事件数据库（Event databases）：是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

在 CIDF 模型中，事件产生器、分析器和响应单元是以程序的形式出现，而最后一个则往往是文件或数据流的形式。

2.2 入侵检测系统中的分类

入侵检测系统根据不同的分类标准可以分为不同形式的入侵检测系统，下面主要从数据源、总体结构和入侵检测技术三个方面来讨论入侵检测系统中的分类情况。

2.2.1 根据检测数据源的分类

入侵检测系统根据其输入数据的来源看，可以分为两类：基于主机的入侵检测系统（Network-based Intrusion Detection NIDS）和基于网络的入侵检测系统（Host-based Intrusion Detection HIDS）。

（1）基于主机的入侵检测系统（HIDS）

基于主机的入侵检测系统检测目标主要是本地主机系统和网络系统中

的本地用户[31,32,33]。它往往以系统日志、应用程序日志、主机的审计记录等作为数据源，当然也可以通过其他手段（如监督系统调用）从所在的主机收集信息进行分析。在实际应用中，基于主机的 IDS 一般监视 Window NT 上的事件、安全日志以及 UNIX 环境中的 syslog 文件。一旦发现这些文件发生变化，IDS 将比较新的日志记录与攻击特征以察看它们是否匹配。如果匹配，IDS 就向管理员发出入侵报警，并采取相应的防护措施。

基于主机的入侵检测系统的优点是对分析“可能攻击行为”非常有用，误报率低，适用于被加密的和交换的环境，并且不需要额外的硬件。缺点是安装了入侵检测系统后会降低应用系统的效率，同时会带来一些额外的安全问题。安装了主机入侵检测系统后，将本来不允许安全管理员有权力访问的服务器变成他可以访问了，另外，它依赖于系统的日志功能，若系统没有配置日志功能，则必须重新配置，这将会给运行中的系统带来不可预见的性能影响。另外，主机入侵检测系统只能检测到自身的主机，不能监视网络上的情况。如果要将所有主机都用入侵检测系统保护代价非常大，因此，企业一般是选部分主机进行保护，这样入侵者可以利用那些没有保护的主机进行攻击。

（2）基于网络的入侵检测系统（NIDS）

NIDS 使用原始的网络分组数据包作为入侵分析的数据源[34, 35]。通过监听某个网段的流量，一个 NIDS 可以监控并分析该网段发生的事件，从而保护该网段的所有主机。一旦检测到攻击，NIDS 的响应模块按照配置对攻击做出响应。通常这些反应包括发送电子邮件、寻呼、记录日志、断开网络连接等。

NIDS 的优点是可以检测来自网络的攻击，检测到超过授权的非法访问[36]。一个 NIDS 不需要改变服务器等主机的配置；它不会在业务系统的主机中安装额外的软件，所以不会影响业务系统的性能。由于 NIDS 不像路由器、防火墙等关键设备方式工作，它不会成为系统中的关键路径；NIDS 发生故障时不会影响正常业务的运行；部署一个 NIDS 的风险也比 HIDS 要小得多。

NIDS 的缺点是只检查它直接连接网段的通信，不能检测在不同网段的

网络数据包。在作用交换以太网的环境中就会出现监视范围的局限，在高速或大型的网络上，NIDS 可能处理不了所有的数据包，因而可能检测不到某些攻击；同时 NIDS 不能分析加密信息；另外，多数 NIDS 只能检测了攻击者使用的攻击方法，不能确定攻击是否成功，所以当检测到一次攻击之后，安全管理员必须再作调查才能确定主机是否已被成功入侵。

2.2.2 根据入侵检测方法的分类

入侵检测系统根据入侵检测方法的不同可以分为两类：误用检测（Misuse Detection）[37]和异常检测(Anomaly Detection)[38]。

（1）误用检测

误用入侵检测原理是：入侵总能表示成模式或特征的形式。系统预先对已知薄弱环节的入侵方式进行定义，通过监视特定目标上的特定活动并与预先设置的模式匹配来检测入侵[39]。如在入侵检测专家系统（Intrusion Detection Expert System, IDES）[20, 40]中，已知的入侵模型由专家编码成专家系统规则，利用专家系统匹配已知的入侵形式。这种方法由于依据具体特征库进行判断，所以检测准确度很高，并且因为检测结果有明确的参照，也为系统管理员做出响应措施提供了方便。但是它的主要缺点在于与具体系统依赖性太强，不但系统移植性不好，维护工作量大，而且将具体入侵手段抽象成知识也很困难。并且检测范围受书籍知识的局限，尤其是难以检测内部人员的入侵行为，如合法用户的泄漏，因为这些入侵行为并没有利用系统的脆弱性。典型的采用误用检测技术的 IDS 如图所示。

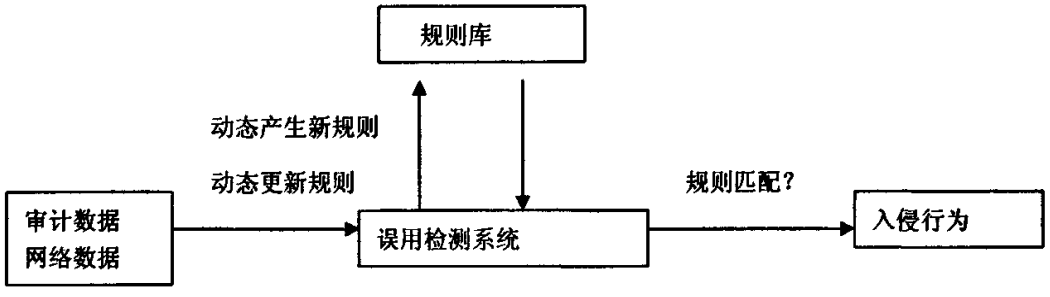


图 2.2 采用误用检测技术的 IDS

Fig 2.2 The Framework of Misuse Detection

由于误用入侵检测方法存在上述问题，因此大多数入侵检测系统都采用异常入侵检测方法。

（2）异常检测

异常入侵检测假设入侵活动是异常活动的子集，利用系统或用户的正常行为模式检测入侵[41]。该方法首先建立正常行为模式，当系统运行时，异常检测程序比较实时行为模式与正常行为模式，一旦发生显著偏离即认为是入侵[42]。如基于神经网络的入侵检测系统[43, 44]，它首先利用用户正常行为样本的特征，构造用户正常行为的特征轮廓（profile），然后用神经网络扫描从审计记录得到的检测样本。并与用户特征轮廓进行比较，以两者的偏差作为证据检测入侵。这种方法与系统相对无关，通用性较强。它可以检测出以前未出现过的攻击方法，不像误用检测受已知脆弱性的限制。但因为不可能对整个系统内的所有用户行为进行全面的描述，况且每个用户的行为是经常改变的，所以该方法的难点是如何建立正常行为特征以及如何设计检测算法。异常检测的主要缺陷就是误报率高，其次由于用户特征轮廓要不断改变，入侵者如果知道某系统在检测器的监视之下，他们会慢慢地训练检测系统，以至于最初认为是异常的行为，经一段时间训练后也认为是正常的了。典型的采用异常检测技术的 IDS 如图所示：

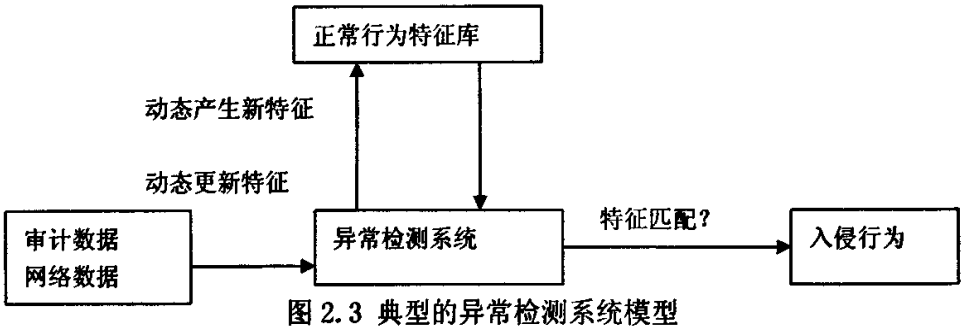


图 2.3 典型的异常检测系统模型

Fig 2.3 The Framework of Anomaly Detection

主要的误用检测系统类型有专家系统、按键监视系统、模型推理系统、误用预测系统、状态转换分析系统和模式匹配系统。

（3）误用检测和异常检测的比较

误用检测和异常检测都可以用来检测入侵行为，但是它们还是有比较明显的区别的，具体的区别比较如表 2.1 所示：

表 2.1：误用检测与异常检测的对比

	误用检测	异常检测
入侵行为的检测	只能发现已知行为	可以发现未知行为
对具体行为的依赖	依赖	不依赖
对具体系统的依赖	依赖	不依赖
误报率	低	高

Table 2.1: The Comparison of Misuse Detection and Anomaly Detection

2.2.3 根据系统体系结构的分类

入侵检测系统的体系结构就是其各个组件在网络上的分布，以及它们之间的关系。根据体系结构，入侵检测系统主要可以分为两种：集中式入侵检测系统和分布式入侵检测系统。

（1）集中式入侵检测系统

集中式入侵检测系统可能有多个分布于不同主机上的审计程序，但只有一个中央入侵检测服务器。审计数据由分散的主机审计程序收集后传送到中央入侵检测服务器，由服务器对这些数据进行分析。图 2.4 为集中式 IDS 的体系结构示意图。

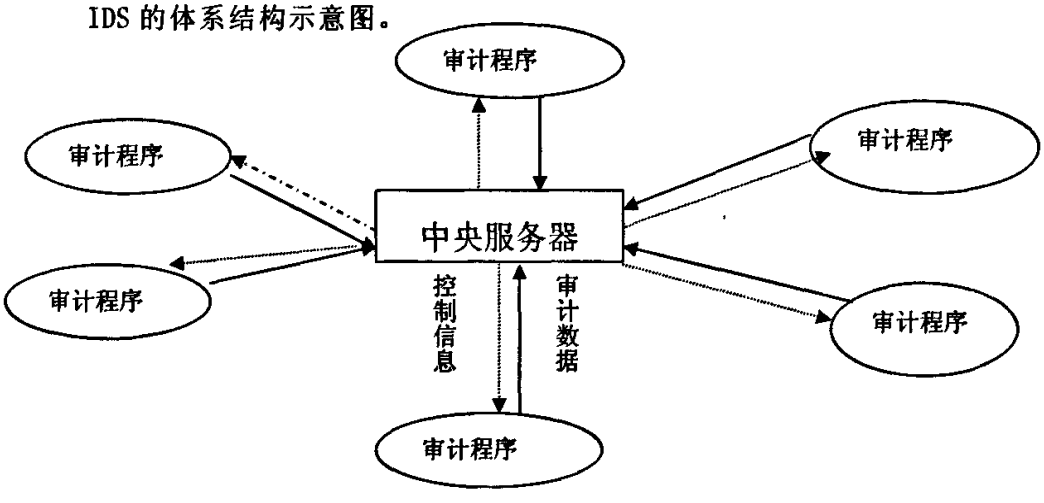


图 2.4：集中式 IDS 体系结构

Fig 2.4: The Architecture of Concentrated IDS

集中式 IDS 的优点是设计简单，适用于小型网络中的入侵检测。但是随着网络规模的扩大，主机审计程序和服务器之间传送的数据量就会大大增加，导致网络性能大大降低，并且一旦中央服务器受到攻击，那么整个受保护系统就会处于不安全状态，因此，这种类型的入侵检测系统的可扩展性、健壮性和可配置性都存在严重的缺陷。

（2）分布式入侵检测系统

分布式IDS的各个组件分布在网络中不同的计算机、设备上。分布式入侵检测系统一般由监视器(Monitor) 、中心分析器(Central Analyzer) 、控制台(Console) 和全局配置库(Global Config Base) 组成(如图1 所示)[45] 。Monitor 是一个本地的入侵检测系统,负责监视各自管辖的网段。对于一些简单的入侵行为,如果Monitor 能够独立判断出来,则按照预先的配置给出相应的反应。而对于一些分布在各个网段上的入侵行为,Monitor 可能只是觉得可疑,并不能完全鉴别,此时就需要把检测到的可疑事件提交给中心分析器,由Central Analyzer 从各个网段收集信息来最终决定是否有入侵行为。为了解决单点失效的问题,Central Analyzer 有多个,但每一个时刻最多只有一个Central Analyzer 处于活动状态。Console 主要是用来查询Monitor 、Central Analyzer 的检测结果,修改它们的检测策略,给管理员一个可视化的图形接口。全局配置库主要用来存放检测策略和结果。Console 、Central Analyzer 和Monitor 之间的通信均被加密。

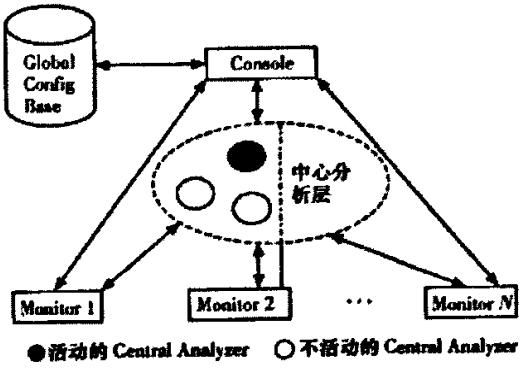


图 2.5：分布式 IDS 的结构模型

Fig 2.5:The Structure Model of DIDS

2.3 入侵检测系统的目标

入侵检测系统的特点是实时性、分布式、智能化和健壮性。设计入侵检测系统是为了更好地维护系统的安全，其根本目标是使系统能快速适应环境的改变和不断变化的、复杂的攻击方式，作为一个良好的入侵检测系统，在设计时应该达到以下目标：

（1）实时性：系统对每一种威胁行为严格定义，从而能够及时发现入侵行为并做出相应的反应。

（2）智能性：根据网络上的情况变化，在判断和识别入侵的过程中不仅能运用数据库的模式识别，而且能结合统计方法识别，自动采取有效的措施，并能把新出现的攻击方式添加到入侵行为的模式库中。

（3）健壮性：相互监视和控制程序的运行，确保系统的健壮性。

（4）可交互性：入侵检测系统与管理员有良好的交互性，方便管理员对系统的管理。

（5）可扩展性：由于网络的构成形式和操作系统的多种多样，入侵检测系统应该能够适应系统的需求、易于扩展。

2.4 入侵检测系统的发展趋势

入侵检测系统大致可以沿着下述几个方向发展：

（1）随着网络系统的复杂化和大型化以及海量存储和高带宽的传输技术，使得集中式的入侵检测越来越不能满足系统需求， 因而入侵检测系统在体系结构上，将会由集中式结构向分层式和分布式结构为主。

（2）目前，“黑客”攻击技术层出不穷，相应的检测技术已明显落后于攻击技术的更新， 故高效率的检测算法将成为IDS的研究热点。 另外，入侵模式确认、入侵描述语言、入侵实时检测也将是入侵检测系统的重要的研究方向。 IDS 将会更多地引入人工智能技术，使其产品具有自学习和自适应的智能化功能。

（3）IDS自身的安全性和易用性。现在IDS面临自身安全性的挑战， 一旦系统中的入侵检测部分被入侵者控制，整个系统的安全防线将面临崩溃的危险。 如何防止入侵者对IDS功能的破坏的研究将在是未来的一

个发展方向，同时，对IDS易用性的研究也将日益增强。

（4）高速网络中的入侵检测以及入侵检测系统与其它系统的协同工作的研究将持续下去。 要解决当前的实际网络安全需求，入侵检测系统将与防火墙系统、应急响应系统等逐渐融合， 构成一个全方位的安全保障系统。

第三章 免疫原理与人工免疫系统

3.1 免疫系统的相关原理

3.1.1 生物免疫系统简介

自然免疫系统[46-49]是一个复杂的自适应系统，可保护人体不受外部病原体的侵害，并把体内所有的细胞或分子分成或者属于自己的种类（自体细胞），或者属于外来源的非自体分子种类。免疫系统不依靠任何中心控制，具有分布式任务处理能力，具有在局部采取行动的智能，也通过起交流作用的化学信息构成网络，进而形成全局观念。生物免疫系统多种多样，具有独特性。同样是人，一个人和另外一个人的免疫系统除了本质构成一样外，具体的状态、功能则千差万别。免疫系统是生物，特别是脊椎动物和人类所具有且必备的防御机制。人工免疫系统最为复杂，它由免疫效应分子及有关的基因及具有免疫功能的细胞、组织、器官等组成，可以保护机体，抗御病原体、有害异物等病因素的侵害。免疫系统的主要功能是：免疫防御，免疫稳定，免疫监督。免疫系统基本元素包括巨噬细胞、淋巴细胞及其抗体，抗体识别特定抗原并清除抗原。生物系统具有大量发达的抗体系统，能够适应不断变化的环境。

免疫系统分为两个主要部分：固有免疫系统和自适应免疫系统。因有免疫系统是抵抗抗原感染的第一道防线，抗原多数在这里被阻止。如果固有免疫系统被攻破，则自适应免疫系统针对特定感染病原体开始发挥作用。自适应免疫系统能够记录入侵的抗原特征，预防下一次袭击。适应性免疫调节有两个分支：体液免疫，由 B 细胞及其产物介导；细胞免疫，由 T 细胞介导。两个分支都对防御遵循类似的步骤顺序---扩增、感应、分化、分泌、袭击、抑制、记忆；但是，它们以不同方式完成任务。

免疫系统有两种应答方法：初次应答和二次应答。初次应答发生在免疫系统遭遇到第一次未见到过的抗原并对其反应的时候。免疫系统能够学习抗原，该机制产生免疫记忆，这样为身体再次遇到同样的抗原时产生二次反应。当抗体结合一个抗原时，B 细胞受刺激产生自体克隆，成长的克

隆体现一种变异机制使免疫系统具有适应性。

生物进化和免疫系统进化之间在时间范围和目的上有显著区别：在生物进化系统中，进化需要长时间进行才能改善一个物种种群的性能；在免疫系统中，寻找合适的抗体种群成员的目标所用时间可以短到几天。免疫系统的进化可分为两个不同模式：缓慢进化模式，体现在 DNA 分子的进化（全局优化）；快速进化模式，体现在免疫系统在与外部抗原斗争时的自适应性（局部优化）。

3.1.2 免疫识别

在免疫系统中，如果淋巴细胞表面的抗原识别受体绑定病原体的抗原决定基，就会产生检测事件。受体和抗原决定基的结构和极性互补，绑定就愈可能发生。免疫识别的过程如图 3.1 所示，受体和抗原决定基之间的绑定能力称作亲和力（Affinity）。一般来说，受体是专用的，因为它们只能绑定一部分类似的抗原决定基结构或模式。这种专用性可以推广到淋巴细胞本身：不同的淋巴细胞上的受体可以互不相同，而在同一个淋巴细胞上的所有受体都是相同的，淋巴细胞只能够对具有类似抗原决定基的结构集合起作用，这种特性称作特异性。

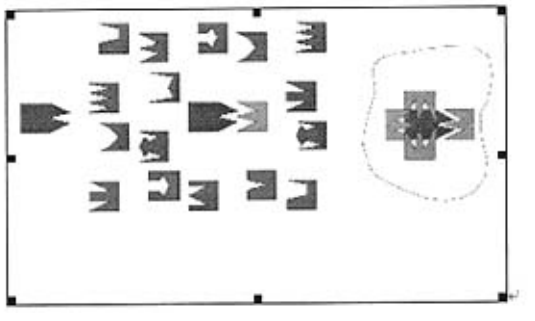


图 3.1: 免疫识别过程

Fig 3.1: The Process of Immune Recognition

淋巴细胞的行为由亲和力描述，当绑定的受体超过某个阀值时，淋巴细胞被激活此时定义为发生了一个检测事件，这个阀值被称作亲和力阀

值。因此，淋巴细胞只有当其受体与病原体的特殊抗原决定基具有高亲和力时才被激活，而且要求淋巴细胞周围有足够多的病原体。这种激活方式允许淋巴细胞用作通用的检测器：一个淋巴细胞能够检测众多具有类似结构的抗原决定基，将抗原决定基空间看作模式集合，单个淋巴细胞能够检测这些模式中的某个子集，称作相似性子集。这也要求特殊的淋巴细胞，如免疫记忆细胞，应该具有比其他淋巴细胞更低的激活阈值，只需要绑定较少的受体就能激活。

基于免疫学的 IDS 采用检测器机制，其检测器也是采用近似的检测规则，负责检测网络中出现的异常模式。

3.1.3 免疫应答

免疫应答(immune response)指机体受抗原性异物刺激后，体内免疫细胞发生一系列反应以排除抗原性异物的生理过程。初次免疫应答（primary response）的过程是由多种免疫细胞和细胞因子相互作用共同完成的复杂过程，可人为地分为三个阶段：

- 感应阶段：抗原呈递细胞捕获、加工、呈递抗原和抗原特异性淋巴细胞（B 细胞和 T 细胞）识别抗原后启动活化的阶段。
- 反应阶段：抗原特异性淋巴细胞（T、B 细胞）接受抗原刺激后，在细胞因子参与下活化、增生、分化为效应 T 细胞和浆细胞（由 B 细胞产生）的阶段，又称增生分化阶段。在此阶段，有部分淋巴细胞中途停止分化，成为静止状态的免疫淋巴细胞。这些细胞为长命淋巴细胞，在间隔相当长的时间后，当它们与相同抗原再次相遇时，可迅速增生分化为效应 T 细胞和/或浆细胞，这种淋巴细胞称为记忆细胞。
- 效应阶段：浆细胞分泌抗体，抗体可与抗原特异性结合，从而杀灭抗原，产生体液免疫效应；效应 T 细胞发挥特异性细胞杀伤作用，产生细胞免疫效应的过程。

免疫反应过程如图 3.2 所示[50]：

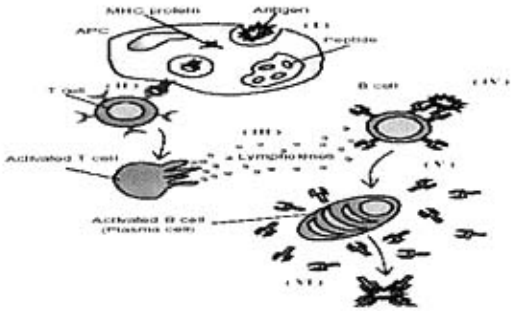


图 3.2 免疫反应过程示意图

Fig 3.2 The Process of Immune Response

3.1.4 否定选择原理

为了识别自己和非己，生物免疫系统一般存在专门检测抗原的 T 细胞。生物体中的 T 细胞分两类，一类是约占总数 65%的辅助性 T 细胞 Th(它们负责促进 B 细胞分泌抗体，增强 T 细胞和巨噬细胞的免疫功能)；另一类是毒性 T 细胞 Tc，在细胞因子作用下活化，形成效应细胞，并能杀伤靶细胞。在胸腺中 T 细胞的产生过程与 MHC(major histocompatibility complex)，主组织相容性复合物)关系密切。MHC 由基因决定，并在有机体生命期间不变化，MHC 是遗传多样性的代表。MHC 的遗传多样性如此重要，以致有人认为有性繁殖持续的主要原因是把最大多样的 MHC 类型遗传给后代。人类的 MHC 通常称为人类白细胞抗原(HLA，humanleukocyte antigen)。MHC 的主要功能是以其产物提呈抗原肽进而激活 T 细胞，由此形成 T 细胞对抗原和 MHC 分子的双重识别，因而 MHC 在启动特异性免疫应答中起重要作用。

由图3.3可知，胸腺中的T 细胞随机生成，它不能直接释放到体内，因为部分T细胞可能会与身体内的正常细胞结合从而导致免疫系统误伤正常组织和器官。为清除这些T 细胞，胸腺还要使用MHC 中的蛋白质过滤这些新产生的T 细胞，如果MHC 中的蛋白质与某些T 细胞能够结合，则将这种 T 细胞清除，否则就通过了MHC 的检测，可以释放到体液中循环。由于T 细胞不可能与代表自身的MHC结合，反之如果能够与T 细胞结合的细胞或物

质必然是代表非我的抗原。因此T 细胞的产生过程可以看成一个在MHC 监督下的有监督的学习过程，即通过大量体现自身信息的MHC 来训练T 细胞集合的过程。因此免疫系统能够根据自身包含的信息来区分自身和抗原，这一原理对于入侵检测系统极大的启发。

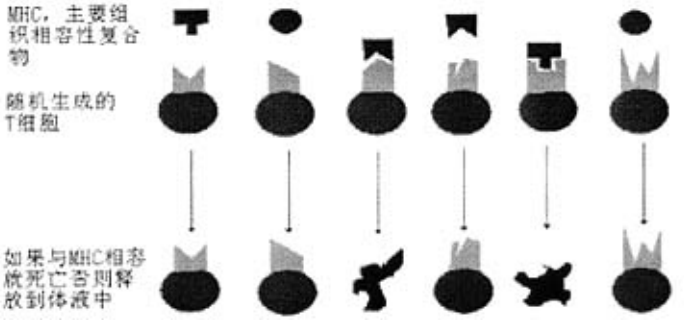


图 3.3 否定选择过程示意图

Fig 3.3 Illusion of negative selection mechanism

3.2 生物免疫系统的特性及与计算机免疫的关系

生物免疫系统在完成其防御功能时表现出许多优良的特性，正是由于这些特性的启示使得人们构造出多种人工免疫系统。下面介绍几种比较突出的特性。

3.2.1 识别多样性

免疫系统的多样性识别能力表现在[51,52]：对于任何一种抗原，至少存在一种抗体可以识别它。免疫系统的识别多样性首先源于抗体是抗体基因库中的基因组合重排而产生的，这就形成了汇合多样性；其次，识别抗原是一个不完全匹配，只要有部分匹配且二者的亲和力超过某一阈值，则相应免疫细胞就被激活，识别过程就完成了；再次，在免疫应答过程中，存在着“细胞超变异”的现象，即被激活的免疫细胞，不仅进行大量的克隆并且也会发生部分变化，从而产生可以更好地识别和消灭相应抗原的抗体，以及对付变种的抗原的抗体，自适应地增强免疫细胞的识别多样性。

因此，人的一生中，免疫系统以有限的抗体（10^7）可以应付环境中可能出现的几乎无限的抗原（10^{16}）。

3.2.2 联想记忆及再次应答

免疫系统对于它所遇到过的抗原有记忆[52,53]。如上所述，在免疫应答的反应阶段，被某一抗原激活的免疫细胞会增殖分化，最后成为可以杀灭抗原的成熟细胞，但有一部分这样的免疫细胞在中途停止分化，处于静止状态，成为对该抗原有记忆的长命细胞。当记忆细胞再次与同一种抗原相遇时，就会直接进入反应阶段，快速、准确、高效地杀灭抗原，即发生所谓的“再次应答（secondary response）”。

另外，免疫记忆是联想记忆。这是因为免疫的识别不要求抗原和抗体完全地匹配，所以对某一抗原的记忆细胞，也可能对与该抗原相似的另一抗原做出反应。

3.2.3 疫苗接种

医学工作者利用免疫记忆，用人工接种的方法给机体输入抗原性物质，使机体免疫系统因抗原刺激而发生类似于隐性感染时所发生的免疫应答过程，使机体获得特异性免疫力的过程[54]。人工免疫功能的实现是人们对疫苗（先验知识）的认识和免疫系统的记忆功能的共同作用的结果[55,56]。

3.2.4 免疫系统与计算机免疫系统的关系

从一个高度抽象的角度来看，在逻辑上免疫系统和计算机免疫系统有如下的映射关系[57]：

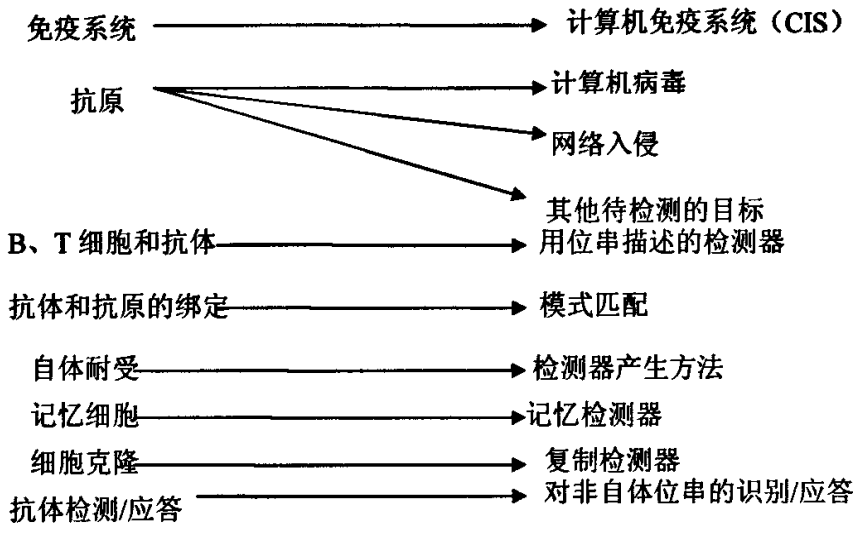


图 3.4 免疫系统与计算机免疫系统的对应关系

Fig3.4 The comparisons of immune system and computer immune system

从图 3.4 我们可以看出，计算机免疫与生物免疫有本质上的相似性。当前抗病毒技术主要采用特征扫描和启发式扫描技术，这些技术只适用于已知病毒。我们现在迫切地希望拥有一套能够快速、自动、演绎的查杀各种已知和未知病毒的技术，这对于抑制病毒的快速繁衍和传播将会起到重要作用，而生物免疫系统的特征恰恰符合这一要求。它们可以学习并记忆新的知识，同时免疫系统的学习过程还借鉴了遗传系统的进化机理，在选择性进化的过程中自主地识别新型病毒特征。计算机的安全问题与生物免疫系统所遇到的问题也具有极大的相似性，两者都要在不断变化的环境中维持系统的稳定性。人体免疫系统具有生物免疫系统的功能是保护生物体自身免受外来病菌的侵扰。当外部抗原侵入机体时，免疫系统能够识别“自体”和“非自体”[58]，人体免疫系统具有天生发现并消灭外来病原体的能力，生物免疫系统所具有的这些特性正是计算机科学工作者所梦寐以求的。这使得利用生物的免疫原理构建功能强大反应迅速的计算机免疫系统成为可能。

综上所述，免疫系统是一个并行的、分布式的、自组织自适应的鲁棒性系统。它具有许多其他研究和应用领域所追求的优良特性。深入研究免

疫系统各种特性及其机理，并构造出相应的人工免疫系统模型用于不同问题，确实是一个值得引起关注的研究方向。

3.3 人工免疫系统（AIS）

3.3.1 人工免疫系统的含义

AIS 是生物计算机的一个新领域，近几年来引起研究人员和业界的浓厚兴趣。AIS 已经被成功地应用于多个领域。越来越多的研究工作表明，AIS 是一个有效的计算模式。AIS 是一个相对较新的领域，正处于快速发展的阶段，因此有必要从外延和内涵上对 AIS 的含义进行探讨。

Starlab 给出的 AIS 定义为：AIS 是进行数据处理、分类、推理和表达的方法学，它遵循一个有争议的生物学范例------生物体的免疫系统[59]。

美国学者 Dasgupta 早在 1998 年就对 AIS 有了比较深刻的定义：AIS 包含若干智能的方法，根据自然免疫系统的原理，应用于解决实际问题[60,61]。

英国的 Jon Timmis 博士在 2000 年对 AIS 定义是相当简洁的：AIS 是一个基于自然免疫系统的计算系统[62,63]。

现于英国 UKC 作博士后研究的巴西学者 de Castro 在 2001 年专门诠释了 AIS 的含义：AIS 是一种计算系统，受理论免疫学的启发，借鉴观测到的免疫系统功能、原理和模式，应用于解决复杂问题[59,64,65]。

总的看来，AIS 具有以下基本内涵：

属于计算系统；

以生物体免疫系统为借鉴；

面向于解决复杂问题。

在前人的基础上，我们对 AIS 做出如下定义：

AIS 是一个计算系统，借鉴自然免疫系统的原理、方法和模型，解决复杂的计算问题。

3.3.2 AIS 的一般框架

AIS 是一个计算系统，而计算系统最重要的是数据表示与计算过程，所

以 AIS 一般性框架需要解决以下问题：

① 描述 AIS 的组成部件；

② 描述 AIS 部件之间的相互关系；

③ 对 AIS 进行更高层次的抽象描述；

④ 研究通用的方法过程，以便应用于不同的领域。

AIS 框架描述了 AIS 解决实际问题的一般过程，如图 3.5 所示：

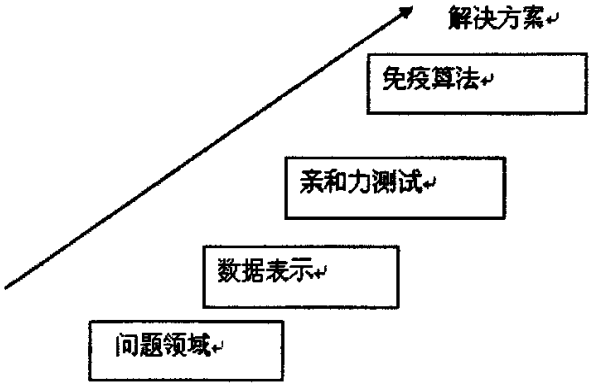


图 3.5 人工免疫系统的一般框架

Fig3.5 The framework of AIS

3.3.3 人工免疫系统与入侵检测系统的关系

人工免疫系统与入侵检测有功能上的相似之处。入侵检测系统负责保护计算机网络系统不受来自内部和外部的入侵行为的侵害。而人工免疫系统能够保护人体不受细菌、病毒、寄生虫、毒素等外来病菌的侵害，免疫系统的分布性、多样性、自成体系、完备性和精简性使它精确有效地保护着人体[66,67]。因此它在人体中的角色类似于计算机或网络系统中的入侵检测系统，根据功能的相似性，表 3.1 列出了人工免疫系统与入侵检测系统的对应关系。这使得人们希望借助于人工免疫系统的原理更好地实现入侵检测的功能，在合法的“自体”行为中判别出非法的“非自体”行为。

表 3.1 人工免疫系统与入侵检测系统的对应关系

缩氨酸/抗原决定基	被检测的行为模式串
抗体	检测模式串
单克隆淋巴细胞（T-细胞、B-细胞）	检测器
抗原	非己模式串
绑定	检测模式串和非己模式串的匹配
耐受性（阴性选择）	阴性选择
淋巴细胞克隆	检测器复制
抗原检测	入侵检测系统的检测
抗原清除	检测器响应

Table 3.1 The comparisons of AIS and IDS

比较 IDS 和 AIS，我们可以总结出以下共同点：

①分布式检测

AIS 的检测器与记忆系统都是高度分布式的，没有中心控制节点，也不是层次式结构。这样就避免了由于主控节点被入侵而导致整个系统崩溃。

DIS 的结构相应地也有三种:集中式、层次式和分布式。从系统鲁棒性角度来看，分布式的结构具有最好的可靠性。

②个体检测器的独立性

AIS 中检测器可用不同的方式实现，其数据源、检测方法与实现结构可以互不相同。 类似地，大型网络中各个主机的 IDS 系统也应该是相互独立的，即使某台主机被入侵也不会导致整个网络瘫痪。

③对新模式的检测能力

生物体免疫系统能够检测新类型抗原和病毒，这样才能够保护生物体在未知环境中生存下去，AIS 继承了自然免疫系统的这一特性。新的入侵手段不断出现，这也要求 IDS 必须尽可能检测出未知的入侵模式。

④非完备的检测

并不是所有的抗原都能够立即被生物体的免疫系统检测出并消灭，免疫系统借助免疫学习来解决这个问题，二次免疫应答能够逐渐学习并趋向完备。AIS 采用的是非精确匹配，一般都具备学习能力。同样地，一个 IDS 也不可能检测出所有的入侵模式。一个好的 IDS 应该具有学习

能力，不断地根据应用环境进行动态调整。

3.3.4 AIS 的应用概述

AIS 主要的研究目的就是面向于解决实际问题，实践的需求促成了 AIS 的迅速发展，研究人员不断地尝试将 AIS 应用于解决各种问题，并且取得了很多的成果。

① 异常诊断

防止计算机受到病毒和未授权人员入侵是一个很有研究价值的异常诊断领域。Forrest 于 1994 年把计算机保护系统问题与免疫系统学习区分自体—非自体相比较[65]，基于人工免疫系统的胸腺阴性选择原理，描述了一种变化诊断策略。

② 机器学习

Hoffmann 将免疫系统、免疫网络和免疫应答与神经网络进行了比较研究[68]，而 Famer 和 Bersini 以及 Varela 将上述内容与学习分类器进行了比较研究[69]。这些研究人员的工作表明，AIS 可以作为一种机器学习方法。

③ 任务规划

Hart 等人将 AIS 应用于规划动态的 job-shop 问题，其中 job 连续到达，并且环境处于不断的变化中，他们采用遗传算法进化 AIS，解决了可预测和不可预测条件下的规划问题。

④ 网络安全

计算机系统是动态的，持续改变行为模式，传统计算机安全机制大部分都是静态的，所以很难与动态环境协调一致。Forrest 于 1997 年，Hofmeyr、Forrest 于 1999 年和 2000 年对人工免疫系问题进行了研究，并将抽象出来的原理应用到计算机网络安全，提出 ARTIS 系统，用 LISYS 系统实现[70]。

⑤ 计算机病毒检测和消除

在 Kephart 发展的系统中，产生一组没有遇到过计算机病毒的抗体促进对未来感染病毒时更快、更强烈的反应，并考虑了最大程度降低自

体免疫应答的风险，其中计算机免疫系统会错误识别合法软件为非法。Okamoto 和 Ishida 提出了一种通过自治和异类 agents 诊断和消除计算机病毒的分布式方法[71]。该系统通过匹配当前主机文件的自体信息（像文件头的前几个字节，文件大小和路径）来诊断病毒。系统通过重写感染文件上的自体信息来消除病毒，通过计算机网络从其他未受感染主机拷贝同一个文件来恢复感染文件。

第四章 一种新的基于海明距离的检测器生成算法

4.1 基于人工免疫的入侵检测问题描述

定义 4.1 模型环境定义一个总体集 U，U 表示一个有限模式的有限集，U包括两个子集 S和 N，S表示“自己”(self)，N表示“非已”(nonsefl)，即 $S\cup N=U, S\cap N=\phi$，“自己”模式代表了合法的事件，而“非已”模式代表了非法事件。

定义 4.2 针对于入侵检测系统的问题是这样描述的，已知一个有限的资源，分类一个模式 $s\in U$是正常的，即对应于“自己”集，否则是异常的，对应于“非已”集。一个检测系统 D由两个组件组成，$D=(f, M)$，f是分类函数，M是从 U中选取的表示“自己”的模式集，$M\in U$，分类函数 f对照 M与一个模式 $s\in U$以一个分类“正常”与“异常”，即

$$f(M,s)=\begin{cases}\text{正常} & \text{如果 } s\in M\\ \text{异常} & \text{否 则}\end{cases}$$

定义 4.3 当一个“自己”模式被检测系统 D分类为异常时就是假阳性，也就是常说的误报。

定义 4.4 如果一个“非已”模式被分类成正常，这就是常说的漏报。

4.2 人工免疫系统中的近似匹配算法

匹配方法可以分为完全匹配和部分匹配。如果两个等长字符串的每个对应位上的符号都相同，那么这样的匹配称为完全匹配。，但是，在人工免疫系统中，受体和抗原的结合，大多数表现的是不完全匹配，完全匹配只是其中的一个特例，因此，在入侵检测系统中一般都是运用部分匹配规则。有许多的部分匹配规则，如 Hamming 规则、连续 r 位的匹配规则、rcb 法等等[14]。

4.2.1 海明距离公式

对于二进制编码的系列 X 和 Y（X，Y$\in\{0, 1\}^N$），它们之间的海明距

离可用下列公式计算：

$$f_H(X,Y)=\frac{1}{N}\sum_{i=1}^{N}X_i\oplus Y_i,\ f_H\in(0,1)$$

其中，f_H(X，Y)表示 X，Y 之间的海明距离，N 表示 X 与 Y 的二进制位数，⊕表示异或操作。

两个字符串之间的距离越小，表示这两个字符串越相似。

4.2.2 连续 r 位的匹配规则

在人工免疫系统中应用最多的是 r 连续位匹配规则(r-contiguous-bit,rcb)，其规则指，两个字符串至少有连续 r 个对应位上的符号相同，即有任意两个串 X 和 Y，如果 X 和 Y 至少有连续 r 位上的符号相同，则称 X 和 Y 相匹配，表示为 comp(X，Y)=1，否则是 comp(X，Y)=0。它采用绑定子串的长度 r 代表抗原与抗体的亲和力。例如设两字符串 X，Y：

X：A B C E D A C E A

Y：B D E D A C B C B

则当 r≤4 时，X，Y 匹配成功。

4.2.3 r-chunk(rch)

在 rcb 匹配规则中，X，Y∈U 且长度相等，rcb 匹配规则要求 X 与 Y 从任意位置开始的连续 r 位置相同即可。如果对 r 连续位子串的起始位置进行限定，要求 X 与 Y 从相同位置开始的连续 r 位相同，就得到另外的一种匹配规则，rch 规则。考虑如下的例子：

X：A B C E D A C E A

Y：B D E D A C B C B

则当 r=4 时，对于 rcb 规则，X 和 Y 匹配成功。而对于 rch 规则而言，X 和 Y 就不匹配了。

4.2.4 Landscape-Affinity 匹配

在人体免疫中的“识别”抗原是通过物理的、化学的对它绑定，即只

能正确反转蛋白质结构以及以高亲和力与抗体或 MHC 附着的化学互补式绑定。在人工免疫系统中除了通过以上介绍的 Hamming 规则、rcb 规则对二进制位或字节进行比较外，还有一些扩展的变种匹配方法，这些方法都是在相当高的抽象概念上捕获化学与物理匹配过程，这里介绍三种亲和力测量手段：差别亲和力（difference affinity），坡度亲和力（slope affinity）和物理亲和力（physical affinity），再利用这些值与一个阀值比较，如果亲和力超过阀值，则表明匹配成功。

在这些方法中，比较串表示成字节，并且将其转换为一个正整数，比较过程可以通过“滑动窗口”方式实现。

对于 X，$Y \in \{0 \cdots 255\}^l$，则

①在差别亲和力比较规则中，计算字节串中有差别的值为：

$$f_{difference} \sum_{i=1}^{l} |(X_i - Y_i)|$$

在坡度亲和力比较规则中，考查两字节序列中相邻字节的变化的差异：

$$f_{slope} = \sum_{i=1}^{l} |(X_{i+1} - X_i) - (Y_{i+1} - Y_i)|$$

在物理亲和力比较规则中，有：

$$f_{physicial} = \sum_{i=1}^{l} (X_i - Y_i) + 3|u|$$

其中　u=min$((\forall i,(X_i - Y_i))$

4.3 基于否定选择的检测器生成算法

在人工免疫入侵检测算法中，非常关键的一个问题就是如何生成有效的检测器集合。否定选择算法模拟了T 细胞在胸腺中的成熟过程。

以下将对几种不同的基于否定选择检测器生成算法进行讨论和分析。先进行如下定义：

P_M：匹配概率。生成的位串与检测器匹配的概率。

P_f：检测失败概率。nonself 位串其未被检测器集中的任何检测器匹配的概率。

N_t：集合X 的规模N。N_s表示self 中位串的个数，N_r 表示检测器集的规模。

r：匹配长度。

m：位串的字母大小。

l：位串长度。

检测器生成算法的目的在于快速有效地产生检测器集R，尽可能多的匹配nonself 位串，不匹配self 位串。

4.3.1 否定选择算法

否定选择算法（Negative Selection Algorithm）的目的是找出一个检测器集合 R，它在不与自体集合中任何元素匹配的前提下，能尽可能多的匹配非自体集合中的元素。否定选择的核心思想是定义一个自我集作为训练集来产生不与自我集模式匹配的检测元集，使用这些检测元来进行入侵检测。基算法过程如下所述：

1. 定义自体为一长度为L 的字符串的集合S；
2. 随机产生一个长度为L 的字符串a；
3. 将字符串a 依次与集合S 中的字符串匹配；
4. 根据匹配规则，如果a 遇到与之匹配的字符串，则结束匹配，转到步2；
5. 如果a 不与S 中任何字符串匹配，则a 成熟，将a 加入到检测器集中。图4.1表示了这个过程。

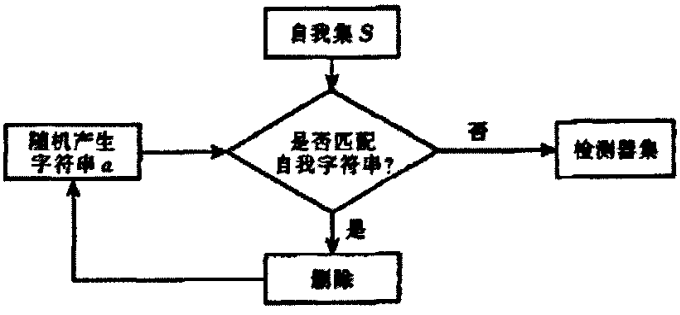


图 4.1 否定选择算法过程

Fig 4.1 The Process of Negative Selection Algorithm

算法的伪代码如图 4.2 所示：

```
Procedure                                    /*Forrest 否定选择算法*/
 Begin
    Get Random_Detector (B1, B2, B3... Bm);  /*产生大量候选检测器*/
      for m do
        begin
          while not Self_data end do         /*和自体库的否定选择*/
            begin
                compute Appetency ;          /*亲和力计算*/;
                if Appetency >= Standard_appetency
                   begin
                      delete;                /*删除当前初始检测器*/
                      break out;
                   end;
            end;
          if not delete                      /*如果没被删除*/
            send to Eligible_ Detector;      /*放入合格检测器集合*/
        next Random_Detector;                /*下一候选检测器*/
      end
 end;
```

图4.2 否定选择算法过程

Fig 4.2 The pseudocode of Negative Selection Algorithm

否定选择算法是生成检测器的一种基本算法，针对于否定选择算法已经提出了很多种基于否定选择算法的改进算法[72,73]，其目的都是为了提高检测的效率，降低漏报和误报的概率。

4.3.2 否定选择变异算法

阴性选择变异算法如下：

1. 生成自身数据集和测试数据集；

2. 对于特定的数据集，确定匹配阀值 r ；

3. 选择期望的 P_f（检测非自身失效的概率）值，并计算 P_m（检测非自身的概率，$Pm=1/Ns$）。

4. 按照公式 $N_R=\frac{-\ln P_f}{P_m}$ 确定 N_R 的值；

5. 设置变异概率 $mut\ Prob$ 和变异限 $mutLim$ 的值；

6. 当 Ns 的大小逐渐增加时，执行（1）—（3）一定的次数；

（1） 通过生成随机串实验确定 N_{R0} （ 候选检测者的群体，

$N_{R0}=\frac{-\ln P_f}{P_m\times(1-P_m)^{N_s}}$），直到$N_R$个有效的检测者被确定。

（2）当自身串与一个候选检测者之间匹配，或者在检测者集中存在重复时，实施均匀变异，直到候选检测器成为一个合格检测器，然后将该检测器添加到有用的检测器集合。

（3）变异实行的次数由$mutLim$（固定值）限制。

该算法的时间复杂度为：

$$o(2^l gN_s)+o(N_R g2^r)+o(N_R)$$

空间复杂度为：

$$o(l\cdot(N_s+N_R))$$

候选检测器集N_{R0}的规模与self 集成指数关系。

文献[12]中进行了算法字母大小、位串长度、匹配长度、检测器数量选择讨论。

4.3.3 r 可变否定选择算法

在否定选择算法下，无论采用何种匹配规则，都有“黑洞”存在。所谓“黑洞”就是：一非我模式$a\in N$是一个黑洞，如果存在检测器 s，使得 Match(a, s)，则$\exists t\in S$,使得 Match(t, s)。也就是说，黑洞中的非我模式串是无法产生相应的检测器来检测出来的。

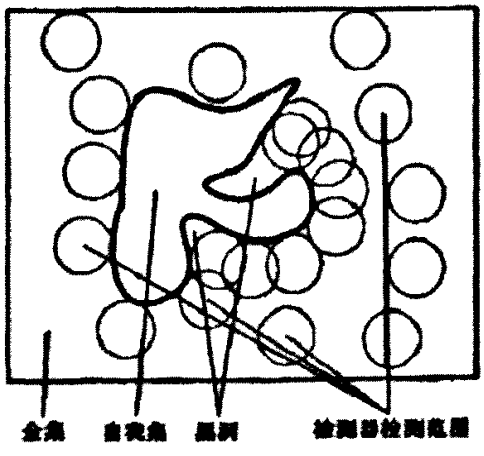


图 4.3 黑洞的直观图

Fig 4.3 The Chart of Black “blank”

为了减少黑洞的数量，文献[74]提出了一种 r 可变的检测器产生算法，通过调整匹配阈值这一比较简单的方法来大幅度降低黑洞的数量，其算法描述如下所示：

1）定义自体为一长度为 L 的字符串的集合 S；

2）随机产生一个长度为 L 的字符串 a，初始匹配阈值为 r_1；

3）将字符串 a 依次与集合 S 中字符串匹配；

4）根据匹配规则，如果 a 不与 S 中任何字符串匹配，则 a 成熟，将 a 与匹配阈值加入到检测器集中，转到步骤 2；

5）当 a 遇到与之匹配的字符串，则将匹配阈值调整为 r’，如果 r’ $>r_c$，转到步骤 2；否则转到步骤 3；

在算法中，设匹配阈值 r 的变化为 r_1，r_2，…r_3，共 C 个，且 $r_1<r_2<r_3\cdots<r_c$，r_c 为最大匹配阈值。

4.3.4 多级否定选择算法(M-NSA)

否定选择算法容易产生漏洞，并且假定自己集随机分布在整个空间，这不太符合现实。而MNS(多级否定选择)[75] 算法则假定：自体集不是随意分布而是聚集在某个子空间且自体集仅仅占用了整个空间的一小部分。多级否定选择算法的主要思想是综合克隆选择和否定选择生成不同尺度的检测器，克隆选择使用局部最佳技术产生更精确识别力的检测器。采用多级否定选择算法来生成成熟检测器，具体算法描述如下：

```
Begin
{
  产生一个大尺度的检测器，使得识别器的识别空间总数覆盖整个空间；
  if (识别距离> 阈值)
    {
      进行克隆选择，生成识别距离更小的检测器；
      经历否定选择；
    }
```

}

End

此算法中的阈值可保证所需的精度,所获得的检测器具有不同的尺度,即不同的检测能力。为了简化描述,以二元空间为例,假定检测器的坐标是(x, y),识别距离是dis,那么它的识别空间是一个正方形(x - dis, y - dis),(x- dis, y + dis),(x + dis, y - dis),(x + dis, y + dis),若此检测器经否定选择不匹配自己模式,则克隆4 种级别(x -dis, y - dis),(x - dis, y + dis),(x + dis, y - dis),(x + dis ,y + dis) 的检测器,其中dis 变为dis/ 2 ,即这4个检测器的识别距离变为dis/ 2 且能覆盖父检测器的识别空间,然后4 种检测器再经历否定选择,不匹配再分别对这4个检测器进行克隆,此过程不断继续下去,直到检测器识别距离达到设定的阈值为止。

4.3.5 几种算法的比较分析

以上介绍了几种针对否定选择算法的改进算法,由于否定选择算法容易产生黑洞,因此,以上算法的基本出发点都是针对减少黑洞数目,对于系统其它方面的性能考虑较少,甚至要牺牲其它的代价来达到减少黑洞的目的。例如,否定选择变异算法和r 可变否定选择算法在一定程度上可以减少黑洞的数目,但是,它们都是以牺牲时间为代价的。在前者中,如果候选检测器与自体检测器匹配时将产生变异,而变异的过程将花费更多的时间,同时,候选检测器的规模与 Self 集成指数的关系,随着信息的不断增加,Self 集也将会不断的更新并且规模也越来越大,因此,就需要更多的候选检测器来满足入侵检测的要求,这又会增加了检测过程中的时间消耗。在后者中,匹配阈值 r 是关键,r 较小时,迭代次数过大;r 过大时迭代次数小,但要达到一定的检测率需要的检测器数目更多,因此,产生一个合适的匹配阈值需要进行多次分析和实验,这必然增加整个过程的时间消耗。M-NSA 是建立在一个假设的基础上,即假设自体集不是随意分布而是聚集在某个子空间且自体集仅仅占用了整个空间的一小部分,但是实际应用中自体集往往是分布在整个空间的,因此,从理论上讲此算法能

够提高检测率，但实际却并非如此。

4.3.6 一种新的基于海明距离的否定选择算法(h-NSA)

以上几种算法所采用的匹配规则都是连续 r 位相同规则，通过对以上几种算法的分析可知，一个好的检测器生成算法不仅要尽可能多的减少黑洞的数目，而且要考虑到算法的时间消耗以及检测器的数目，本文从这几个方面出发，提出了一种基于海明距离的检测器生成算法。

4.3.6.1 典型的基于 Hamming 的部分匹配规则的否定选择算法（t-NSA）

典型的基于海明距离的部分匹配规则的检测器产生算法如下所示：

（1） l：表示自体字符串的长度；

（2） r：海明距离参数。如果两个字符串之间的海明距离小于 $l-r$，则这两个字符串相匹配，换句话说如果两个字符串相对应的位置上连续相同的位数大于或等于 r，则它们是匹配的，反之就不匹配；

（3） S：表示自体集；

（4） R：表示检测器集，初始化为空集；

（5） 随机产生一个侯选检测器 d；

（6） 对任何字符串 $s \in S$，如果 d 与 s 匹配，则转到（5）；

（7） 将 d 加入到检测器集合 S 中，即：$R \leftarrow R \cup \{d\}$；

（8） 结束。如果 R 达到了预先设定的值或其它结束条件已满足，则退出，否则转到（5）。

此算法要求产生一定数目的侯选检测器，并且侯选检测器的数目要比期望的检测器要多很多。设 N_S 表示自体集的规模；N_{R0} 表示侯选检测器的数目；N_R 表示检测器集合的规模。则算法的时间复杂度与 N_{R0} 和 N_S 成正比，空间复杂度由 N_S 决定：

时间复杂度为：

$$O(N_{R0} \cdot N_s) = O(\frac{-\ln(P_f)}{P_m(1-P_m)^{N_S}} N_S), \qquad \text{（公式 4.1）}$$

空间复杂度为：$O(N_S \cdot l)$ （公式 4.2）

检测失败的概率为：

$$P_f = (1-P_m)^{N_R} \qquad \text{（公式 4.3）}$$

其中 P_m 表示两个字符串匹配的概率，这里采用的是海明距离：

$$P_m = \sum_{i=r}^{l} C_l^i \cdot (\frac{1}{2})^i \cdot (\frac{1}{2})^{l-i} = \frac{1}{2^l}(\sum_{i=r}^{l} C_l^i) \qquad \text{（公式 4.4）}$$

一般来讲，P_m 是很小的，表 4.1 列出了一些 P_m 的可能值：

表 4.1：不同的 l 和 r 下 P_m 的值

l	r	P_m	l	r	P_m
8	6	0.1445	32	20	0.1077
8	7	0.0351	32	24	0.0035
16	11	0.1051	32	28	9.6506e-6
16	12	0.0384	32	30	1.2317e-007
16	13	0.0106	64	40	0.0300
16	14	0.0021	64	48	3.8665e-005
16	15	0.0003	64	56	2.7813e-010

Table 4.1: Some Values of P_m with different l and r

本文也在否定选择算法的基础上，应用基于海明距离的部分匹配规则，提出了一种新的检测器生成算法，我们把上面提到的典型的否定选择算法称为 t-NSA，文中新的算法称为 h-NSA。

4.3.6.2 h-NSA 的一些定义

定义 4.5 模板：在一个长度为 l 的字符串中，如果有 l-i 个位置是未确定的（在这里我们可以用*代替），则我们就称这是一个长度为 l，阶数为 i 的模板。例如字符串“11*1*11”，则它是一个有两个未确定位置的阶为 5 的模板。

本文中的检测器是由{0，1，*}组成的一序列字符串，其中*可以匹配字符“0”和“1”。因此，如果一个模板不能与自体集中的任何个体相匹配，则这个模板就可以称为是一个检测器，通常一个模板都被看着是一个侯选检测器。例如：有这样一个自体集是{0010，1001}，并且 L=4，r=3，则模板“111*”就是一个有效的检测器，因为不管*是“0”还是“1”它都不能与自体中的任何个体相匹配。很明显，这个检测器的定义会扩大检

测器集合的覆盖范围，通过给定一个检测概率能有效的减少检测器的数目。

定义 4.6 自体位串侯选检测器模板：给定一个字体字符串 $s=x_1x_2x_3\cdots x_l$，阶数为 c（$c=l-r+1$）的侯选检测器模板 T_s可以这样来产生：随机从 s 中选择 c 位并且确定这 c 位上的字符，其它的 r-1 位是未确定的。例如：下面这些模板都可以看作是一个 T_s：

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_c * *\ldots *$$

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_{c-1} * \overline{x}_{c+1} *\ldots *$$

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_{c-2} **\overline{x}_{c+1} *\ldots *$$

$$\cdots\cdots$$

$$\text{or} \quad * *\ldots * \overline{x}_r\ldots\overline{x}_{l-1}\overline{x}_l$$

模板 T_s有 r-1个未确定的位和 c个确定的位，c个确定位中的每一位都可能是 x_1，x_2，$x_3\ldots x_l$的任何一位，因此，像T_s这样的模板数目应该有 C_l^{r-1}个。

定义 4.7 定义 $c+k$ 阶模板 $T_{t,s}$：给定一个自体字符串 $s=y_1y_2y_3\cdots y_l$和一个 c 阶侯选检测器模板 t，则 $T_{t,s}$可以由下列方法产生：如果 $k\leqslant l-c$，则随机选择 $l-c$ 中的 k 位，每一位上的数都属于自体字符串 s，其它的 $l-c-k$ 位仍然是未确定的。相反，如果 $k>l-c$，像这样的侯选检测器模板是不存在的。例如：

如果 $t=\overline{x}_1\overline{x}_2\ldots\overline{x}_c * *\ldots *$ 则 $c+k$ 阶模板 $T_{t,s}$可以是下列中的一个：

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_c\overline{y}_{c+1}\ldots\overline{y}_{c+k} *\ldots *$$

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_c\overline{y}_{c+1}\ldots\overline{y}_{c+k-1} * \overline{y}_{c+k} *\ldots *$$

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_c\overline{y}_{c+1}\ldots\overline{y}_{c+k-1} **\overline{y}_{c+k+1} *\ldots *$$

$$\cdots\cdots\cdots$$

$$\overline{x}_1\overline{x}_2\ldots\overline{x}_c * *\ldots * \overline{y}_{l-k+1}\ldots\overline{y}_{l-1}\overline{x}_l$$

很明显，模板 $T_{t,s}$有 $l-c-k$ 个未确定的位和 $c+k$ 个确定位，因此像这样的模板共有 C_{l-c}^{k}个。

4.3.6.3 h-NSA 算法描述

假设有效检测器集合为 R，则 h-NSA 的执行过程为：

（1） 初始化有效检测器集合 $R=\varnothing$

（2） 随机选择一个自体自符串 s_r（$1\leqslant r\leqslant Ns$），然后随机产生一个 $c(c=l-r+1)$阶侯选检测器模板 d，则 d有 $r-1$ 个未确定位，并且 $m=r-1$。

（3） 设置一个变量 i=0。

（4） i=i+1.

a) 如果 i=r 则转向（4）

b) 如果 i>Ns,则将模板 d加入到有效检测器 R中，即 $R\leftarrow R\cup\{d\}$。

如果 R中检测器的数目已经达到了预先设置的阈值或者其它的结束条件满足了，则算法结束，否则转向步骤（3）。

c) 如果 i$\leqslant Ns$

i．计算模板 d和自体字符串 s_i中相应位置上连续相同的位数，记为 k。

ii．如果 $k\geqslant r$，则删除 d，然后转向步骤（2）

iii．如果 $k=r-1$，则模板 d中未确定的位都用 s_i中相应位的相反数来替换，然后设置 $m=0$，再转向步骤（4）

iv．如果 $k<r-1$ 并且 $k+m\leqslant r-1$，则模板 d和未确定的位数 m 仍然保持不变，程序转向步骤（4）。

v．如果 $k<r-1$ 并且 $k+m>r-1$，则从侯选检测器模板 d和 s_i中随机产生一个阶为 $l-(r-1-k)$的侯选检测器模板 t，并设置 $d=t, m=r-1-k$，再转到步骤（4）。

上述算法中产生的检测器字符串都是由 0、1 和*组成的，并且*号可以 0 和 1。假设一个有 b 位未确定位的检测器 d，则任何字符串能和这个检测器匹配的概率是：

$$P_{m,b}=\begin{cases}1, b>r\\ \sum_{i=r-b}^{l-b} C_{l-b}^{i}\left(\frac{1}{2}\right)^{i}\left(\frac{1}{2}\right)^{l-i}, b\leq r\end{cases}\qquad\text{（公式 4.5）}$$

下表中给出了一些 $P_{m,b}$ 的值：

表 4.2 不同的 r 和 b 对应的 $P_{m,b}$ 的值

l	r	b	$P_{m,b}$	l	r	b	$P_{m,b}$
16	14	0	0.0021	32	28	0	9.6506e-006
16	14	2	0.0065	32	28	2	2.9738e-005
16	14	4	0.0193	32	28	4	8.9996e-005
16	14	6	0.0547	32	28	6	0.0003
16	14	8	0.1445	32	28	8	0.0008
16	14	10	0.3438	32	28	10	0.0022
16	14	12	0.6875	32	28	12	0.0059

Table 4.2 Some values of $P_{m,b}$ with different r and b

给定一个检测器集合 $R=\{d_1,d_2...d_{N_R}\}$ 和未确定的位数集合 $\{b_1,b_2,...,b_k\}$，则不能被这 N_R 个检测器检测的概率为：

$$P_f = \prod_{i=1}^{N_R} (1 - P_{m,b_i}) \qquad \text{（公式 4.6）}$$

第五章 h-NSA 算法实验与结果分析

为了方便起见，我们把传统的否定选择算法称为 t-NSA，新的算法称为 h-NSA。下面的实验都是为了检测算法的性能，每个实验单独运行十分钟。

5.1 实验描述

在实验中，用来测试的数据集称为 N_T，测试数据集是一个个随机产生的并且是各不相同的异常字符串，也就是说如果某个字符串能够和测试数据集中的任何一个字符串匹配，它就不能加入到测试数据集中。假如字符串的长度为 l，那么测试集中的字符串可以由下面的步骤来产生：

（1）随机产生一个 0 到 2^l-1 之间的整数，然后将它转换成二进制字符串。

（2）如果这个字符串能够和自体集和测试数据集中的任何个体匹配，则转到（1）重新生成一个新的字符串，否则就将它加入到测试数据集中。

在实验中，我们用 G_M 来表示所有的侯选检测器和自体自符串匹配的次数，$C_G=\frac{G_M}{N_R N_S}$ 表示产生一个成熟检测器的平均花费时间；D_R 检测概率，所以有 $D_R=1-P_f$

在这两种算法中，基本的操作就是侯选检测器与自体字符串的匹配，因此，产生一个检测器的平均匹配次数能在一定程度上反应它们的时间开销。检测概率是判断一个算法好坏的重要参数，检测失败的概率为 P_f，检测概率为 $D_R=1-P_f$。本章从这两个方面进行对 t-NSA 和 h-NSA 进行了实验，最后对两种算法中产生相同的成熟检测器 N_R 所需要的时间进行了分析。

5.2 h-NSA 与 t-NSA 中 G_M 的比较

本实验主要是为了估计产生一个检测器所需要的平均匹配次数，在 t-NSA 和 h-NSA 中，所有的侯选检测器都是随机产生的，并且有一些由于

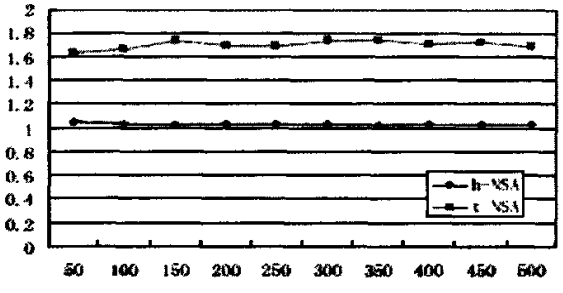
能够与字体集合中的个体相匹配而被删除。在实验中，假设自体集的大小 N_S是固定不定的，而检测器集的数目 N_R是可变的，并设 l=16，r=14，N_S=300，N_F=10000，则两种算法中，G_M的变化情况如表 5.1 所示

表 5.1：N_S 不变、N_R可变的 h-NSA 和 t-NSA 中 G_M的比较

N_R		Max G_M	Min G_M	AVG G_M	STDDEV
50	h-NSA	16120	15167	15675.7	365.22
	t-NSA	28545	22280	24527.7	1792.28
100	h-NSA	31513	30152	30879.1	523.31
	t-NSA	54513	46722	49757.6	2552.35
150	h-NSA	47259	45413	46127.4	646.26
	t-NSA	85156	72262	77705.6	3711.31
200	h-NSA	62433	60703	61734.7	545.77
	t-NSA	109638	94355	101503.9	4410.65
250	h-NSA	79305	76100	77314.0	1008.22
	t-NSA	139078	121987	126130.4	5260.17
300	h-NSA	94836	91775	92897.3	1205.18
	t-NSA	163775	148562	155445.2	5053.12
350	h-NSA	108330	106551	107743.4	600.72
	t-NSA	187053	175327	182479.2	3808.99
400	h-NSA	125041	122900	123915.1	656.90
	t-NSA	215162	197034	204130.6	5960.36
450	h-NSA	141056	138041	139746.7	1108.97
	t-NSA	242589	222226	232088.5	6304.61
500	h-NSA	156130	153357	154610.9	953.22
	t-NSA	260032	246993	252299.7	4340.26

Table 5.1: Comparisons on G_M between h-NSA and t-NSA when fixing N_S and varying N_R

产生一个成熟检测器的平均时间消耗 C_G的变化情况如图 5.1(a)所示。

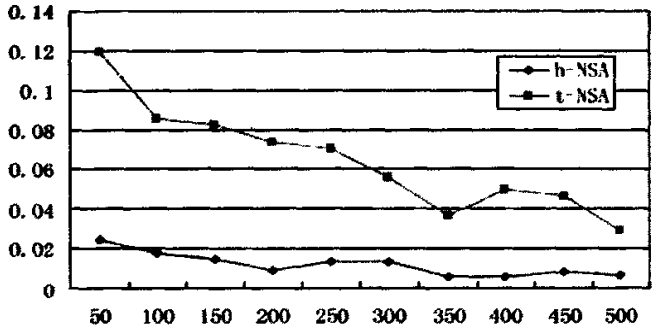


(a)

图 5.1(a)：t-NSA 与 h-NSA 的 C_G比较

Fig5.1(a)：Comparisons on C_G between h-NSA and t-NSA when fixing N_S and varying N_R

两种算法中的 C_G标准偏差如图 5.1(b)所示



(b)

图 5.1(b) t-NSA 与 h-NSA 中 C_G的标准偏差比较

Fig5.1(b)：Standard deviation of C_G between h-NSA and t-NSA when fixing N_S and varying N_R

从图 5.1 可以看出，在 N_S不变情况下，随着 N_R的变化，两种算法中的 C_G都没有明显的变化，但是，从表 5.1 可以看出，随着 N_R的不断变大，要产生相同数量的成熟检测器，h-NSA 要比 t-NSA 更容易，因为在 h-NSA 中产生一个成熟检测器所需要的平均匹配次数比 t-NSA 中要少的多。

现在假设 N_S可变，N_R不变，并且设定 l=16，r=14，N_R=100，N_T=10000，实验的结果如表 5.2 和图 5.2 所示：

表 5.2：N_S可变、N_R不变的 h-NSA 和 t-NSA 中 G_M的比较

N_S		Max G_M	Min G_M	AVG G_M	STDDEV
50	h-NSA	5000	5000	5000.0	0
	t-NSA	5686	5252	5426.8	151.14
100	h-NSA	10000	10000	10000.0	0
	t-NSA	12434	11360	11716.2	344.96
200	h-NSA	20383	20000	20107.3	148.86
	t-NSA	30275	26272	28499.5	1365.31
300	h-NSA	32055	30527	31052.8	448.16
	t-NSA	56718	44809	49433.9	3574.93
400	h-NSA	44248	40796	42513.5	979.37
	t-NSA	95220	73279	81900.0	6532.52
500	h-NSA	58264	53215	55599.7	1324.18
	t-NSA	145005	120985	129361.7	7175.92
600	h-NSA	71615	65516	68209.4	1916.98
	t-NSA	212944	168734	187648.0	13928.35
700	h-NSA	88921	78691	82592.2	3309.34
	t-NSA	332533	225637	275329.4	33571.90
900	h-NSA	119346	111265	115244.9	3135.51
	t-NSA	688482	471133	562326.6	75176.57
1100	h-NSA	165563	135428	151418.2	9687.97
	t-NSA	1199136	969823	1124476.0	69780.24

Table 5.2: Comparisons on G_M between h-NSA and t-NSA when fixing N_R and varying N_S

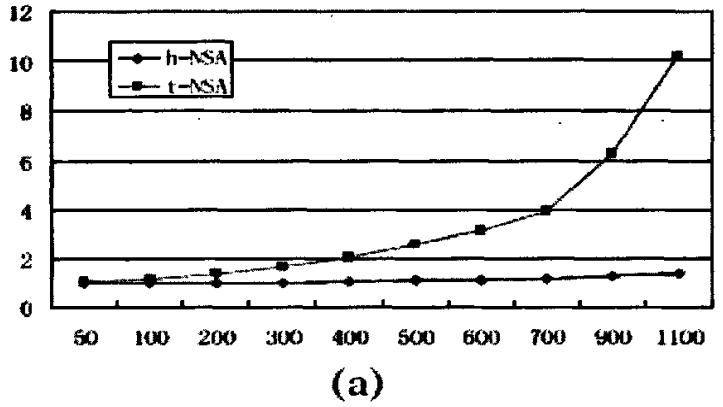


图 5.2(a)：N_R不变、N_S可变时 C_G的比较

Fig5.2(a)：Comparisons on C_G between h-NSA and t-NSA when fixing N_R and varying N_S

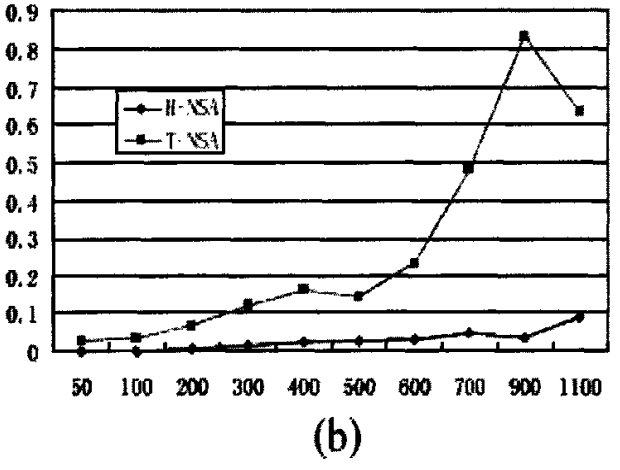


图 5.2(b)：N_R不变、N_S可变时 C_G的标准偏差比较

Fig5.2(b)：Standard deviation of C_G between h-NSA and t-NSA when fixing N_R and varying N_S

从表 5.2 可以看出，当 N_R不变时，两种算法中的 C_G都随着 N_S的增加而增大，但是 h-NSA 中产生一个成熟检测器的平均匹配次数要比 t-NSA 中少的多，N_S越大，这种差别就更明显，从图 5.2 中可以看出，随着的增加，t-NSA 中产生一个成熟检测器的平均时间消耗也逐渐增加，而 h-NSA 中却没有多大的改变，并且 h-NSA 中 C_G的变化率要比 t-NSA 中小的多。

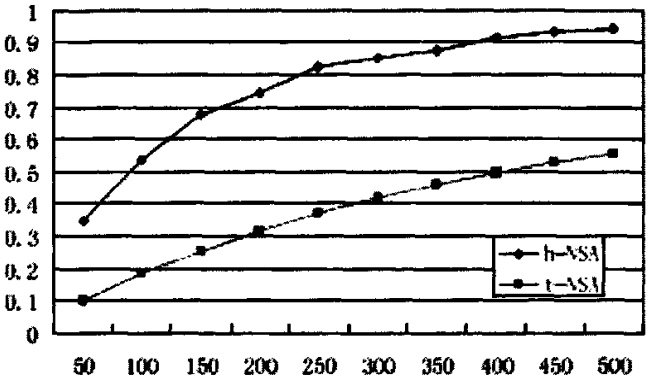
5.3 t-NSA 和 N-NSA 中 D_R 的比较

检测概率是判断一个算法好坏的重要参数，检测失败的概率为 P_f，因此，检测概率为 D_R=1-P_f，在这个实验中同样有两种情况，一种是保持 N_S 不变、N_R 可变，一种是保持 N_R 不变，N_S 可变，在第一种情况下 h-NSA 和 t-NSA 中检测概率 D_R 的情况如表 5.3 和图 5.3 所示：

表 5.3：h-NSA 和 t-NSA 中 D_R 的比较

N_R		Max D_R	Min D_R	AVG D_R	STDDEV
50	h-NSA	0.3884	0.3082	0.34549	0.027677
	t-NSA	0.1027	0.0918	0.09719	0.004307
100	h-NSA	0.5645	0.4893	0.53586	0.028648
	t-NSA	0.1886	0.1777	0.18409	0.003038
150	h-NSA	0.7112	0.6512	0.67375	0.017377
	t-NSA	0.2621	0.2468	0.25434	0.005868
200	h-NSA	0.7621	0.7025	0.74181	0.017484
	t-NSA	0.3206	0.3072	0.31461	0.003802
250	h-NSA	0.8348	0.8074	0.82325	0.008856
	t-NSA	0.3754	0.358	0.36893	0.004837
300	h-NSA	0.8799	0.8442	0.85341	0.010391
	t-NSA	0.4198	0.4076	0.41702	0.003696
350	h-NSA	0.8932	0.8579	0.87326	0.011136
	t-NSA	0.4625	0.4522	0.45768	0.003748
400	h-NSA	0.922	0.9008	0.91421	0.007709
	t-NSA	0.503	0.4819	0.49338	0.007111
450	h-NSA	0.9422	0.9166	0.9306	0.008074
	t-NSA	0.5326	0.5231	0.52762	0.003233
500	h-NSA	0.9532	0.9285	0.94278	0.007652
	t-NSA	0.5642	0.5487	0.55522	0.00499

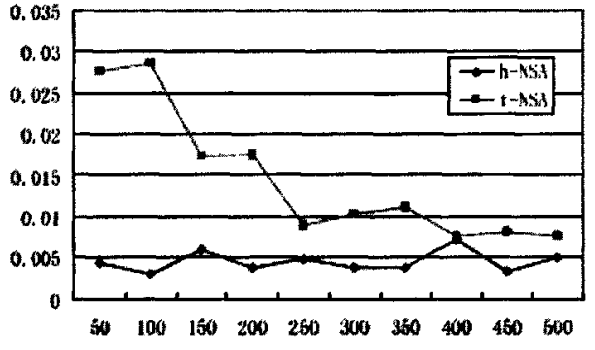
Table5.3: Comparisons on D_R between h-NSA and t-NSA when fixing N_S and varying N_R



(a)

图 5.3(a)：h-NSA 和 t-NSA 中 D_R的变化图

Fig5.3(a)：Comparisons on $D_R$between h-NSA and t-NSA when fixing N_S and varying N_R



(b)

图 5.3(b)：两种算法中 D_R的标准偏差

Fig5.3(b)：Standard deviation of $D_R$between h-NSA and t-NSA when fixing N_S and varying N_R

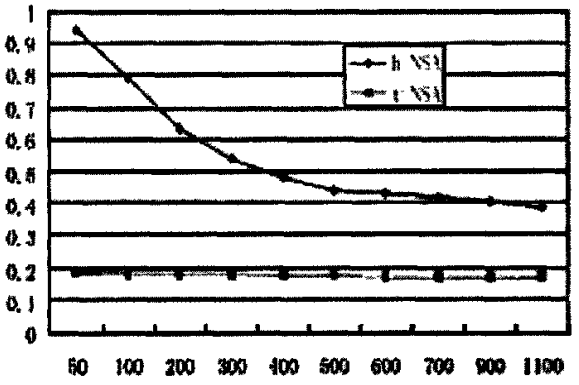
从表 5.3 和图 5.3 可知，检测概率 D_R随着 N_R的增加而增加，但是在相同的成熟检测器的情况下，h-NSA 的检测效率要明显高于 t-NSA，标准偏差也比 t-NSA 要低，因此，h-NSA 比 t-NSA 要更稳定。

在 N_R不变，N_S可变的情况下，设定 l=16，r=14，N_R=100，N_T=10000，实验结果如表 5.4 和图 5.4 所示：

表 5.4：Ns 可变、N_R不变的 h-NSA 和 t-NSA 中 D_R的比较

N_S		Max D_R	Min D_R	AVG D_R	STDDEV
50	h-NSA	0.9543	0.9303	0.94203	0.008844
	t-NSA	0.1876	0.1814	0.1849	0.002486
100	h-NSA	0.8474	0.7381	0.79412	0.028445
	t-NSA	0.1894	0.1751	0.18214	0.004446
200	h-NSA	0.6863	0.5956	0.63463	0.032304
	t-NSA	0.1911	0.1751	0.18222	0.005227
300	h-NSA	0.5652	0.5154	0.53954	0.019914
	t-NSA	0.1882	0.1763	0.18168	0.003982
400	h-NSA	0.5125	0.4433	0.48044	0.025536
	t-NSA	0.1868	0.1709	0.17724	0.005197
500	h-NSA	0.4869	0.3991	0.44081	0.027283
	t-NSA	0.1789	0.1674	0.17409	0.003515
600	h-NSA	0.4684	0.3966	0.43301	0.025968
	t-NSA	0.1803	0.164	0.17158	0.005298
700	h-NSA	0.4454	0.3975	0.41809	0.015273
	t-NSA	0.1782	0.1645	0.17116	0.00441
900	h-NSA	0.4425	0.3809	0.40513	0.020728
	t-NSA	0.1772	0.1663	0.17173	0.003877
1100	h-NSA	0.4121	0.3635	0.38717	0.016699
	t-NSA	0.1771	0.1567	0.16774	0.00544

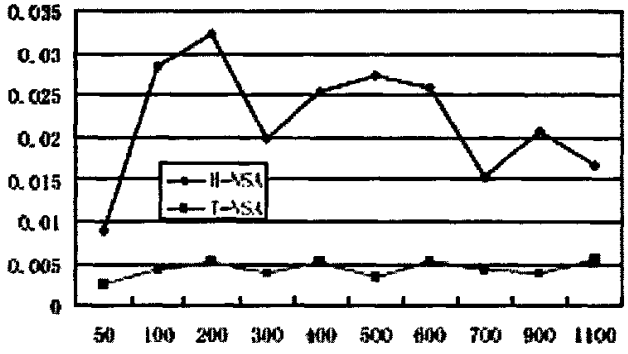
Table 5.4: Comparisons on $D_R$between h-NSA and t-NSA when fixing N_R and varying N_S



(a)

图 5.4(a)：N_R不变、N_S可变时 D_R的比较

Fig5.4(a): Comparisons on D_R between h-NSA and t-NSA when fixing N_R and varying N_S



(b)

图 5.4(b)：N_R不变、N_S可变时 D_R的标准偏差

Fig5.4(b)：Standard deviation of D_R between h-NSA and t-NSA when fixing N_R and varying N_S

从表 5.4 和图 5.4 可以看出，当 N_R不变时，检测率 D_R随着 N_S的增加而逐渐减小，但是 h-NSA 的检测率总是高于 t-NSA 的。同时，从图 5.4(b)中可以看出，h-NSA中的 D_R偏差要比 t-NSA中的大一些，但它总是小于0.055的，因此在检测率更高的情况下这个偏差是可以接受的。

5.4 实验结果分析与比较

5.4.1 N_R的分析比较

在 t-NSA 中，N_R的值是由公式 $N_R = -\frac{\ln P_f}{P_m}$ 来计算，在 h-NSA 中，N_R是由下面的步骤来产生的：

（1） N_R=0，CP_f =1；

（2） 根据 h-NSA 产生一个检测器；

（2．1）应用公式计算 $P_{m,b}$

（2．2）$CP_f = CP_f * (1-P_{m,b})$；

（2．3）$N_R = N_R + 1$；

（3） 如果 $CP_f > P_f$ 转到（2）；

（4） 结束。

表 5.5 给出了在 P_f=0.1 时两种算法的 N_R的对比情况：

表 5.5：h-NSA 与 t-NSA 中 P_f=0.1 时 N_R的对比

				h-NSA		t-NSA	
l	r	N_S	N_T	N_R	P_f (actual)	N_R	P_f (actual)
16	12	40	10000	41	0.07807	60	0.09135
16	12	60	1000	44	0.0883	60	0.0817
16	14	400	10000	412	0.11729	1102	0.23623
16	14	600	10000	550	0.10292	1102	0.25111
16	14	800	10000	634	0.07293	1102	0.28565
18	16	600	10000	345	0.13309	3510	0.51912
18	16	800	10000	402	0.12499	3510	0.57223
20	18	800	10000	267	0.13108	11443	0.71051
20	18	1000	10000	286	0.13679	11443	0.75233

Table5.5 Comparisons on N_R between h-NSA and t-NSA with P_f=0.1

从 5.5 表中可以看出，在 P_f相同的情况下，h-NSA 比 t-NSA 需要更少的成熟检测器 N_R，并且 P_f 的值也更接近期望的 P_f值。事实上，随着 Ns 和 P_a的增加，P_f还是会比 0.1 要大很多的。从生成一个成熟检测器来看，h-NSA 的时间开销要比 t-NSA 要少的多。

5.4.2 算法复杂度分析

算法的时间复杂度是衡量一个算法好坏的重要标准之一，现在我们来分析比较一下两种算法的时间复杂度，在两种算法中最基本的操作都是自体字符串与侯选检测器之间的匹配操作，因此，匹配的次数 G_M能够在一定程度上反映时间的开销，从前面实验结果可以看出，在相同的参数下，h-NSA 的 G_M要比 t-NSA 中的小的多，所以多实验的结果也可以看出 h-NSA 的时间开销要比 t-NSA 少，但是从数量级上来看，两种算法的时间复杂度都可以用下面的公式来表示：

$$O(N_{R0}\cdot N_S)=O(\frac{N_R}{P_S}\cdot N_S) \qquad \text{（公式 5.1）}$$

P_S表示一个随机产生的初始检测器能够存活的概率。

从公式（4.4）和（4.5）可以看出 $P_{a,b}\geq P_a$，当且仅当 b=0 时才取等号，同样根据公式(4.3)和（4.6）也可以得出 $P_{a,b}\geq P_a$，因为在相同的 P_f下，h-NSA 需要的检测器数量 N_R比 t-NSA 要少。对于 h-NSA 来说，在初始的侯

选检测器中有 $r-1$ 个未确定位，这些未确定的位数随着匹配其它自体字符串而逐渐减少，当未确定的位数等于 0 时，h-NSA 中相应的侯选检测器与 t-NSA 具有相同的存活率，存活率可以用公式

$$P_S = (1 - P_m)^{N_S^L} \qquad \text{（公式 5.2）}$$

其中 N_S^L 表示当自体字符串左边未确定位数为 0 时的匹配数目，很显然，$N'_S < N_S$，所以在 h-NSA 中的检测器存活率 P_s 要高于 t-NAS。在 h-NSA 中，在初始的侯选检测器中有 $r-1$ 个未确定位，也就是说如果在 t-NAS 中应该有 2^{r-1} 个初始侯选检测器，并且在 h-NSA 中一个初始检测器的存活概率 P_s 是 t-NAS 中的 2^{r-1} 倍。因此，根据公式 5.1 可以看出，h-NSA 的时间复杂度要低于 t-NSA，两种算法的空间复杂度基本相同。

第六章 结论与展望

入侵检测是计算机安全的重要组成部分，是传统安全工具的补充。免疫系统与入侵检测系统具有本质的相似性，将自然免疫系统的原理、机制与规则应用于入侵检测系统研究，构建基于免疫原理的入侵检测系统，是近几年入侵检测领域研究的热点，具有广阔的发展前景。

6.1 本文的主要工作

① 分析了入侵检测技术的发展历程、分类以及现有入侵检测系统的不足之处，总结了入侵检测技术的现状与发展趋势，深入研究生物体的免疫机制和免疫特性，并在此基础上对免疫算法进行了简单的分析。

② 详细介绍人工免疫系统的基础知识以及人工免疫系统与入侵检测系统的关系，指出了人工免疫系统在入侵检测系统中的重要作用，分析了基于人工免疫系统的入侵检测技术现状与应用。

③ 研究了几种检测器生成算法，并对各种算法进行了分析。主要对否定选择算法进行了深入的分析，并在此基础了提出了一种基于海明距离的检测器生成算法，通过引入模板的概念来达到消除冗余检测器，从而提高了检测效率

④ 对两种算法进行了仿真实验，并从各个方面比较了两种算法的性能，其中包括时间复杂度、空间复杂度、检测效率以及检测标准误差等等。实验结果表明，新的检测器生成算法具有更好的性能，能够有效的提高检测效率，减小漏报率与误报率。

6.2 进一步的工作

由于时间仓促加之本人水平有限，本研究只在这一领域做了初步的工作，为进一步提高入侵检测效率、降低误报率与减少人工干预，无论在新免疫机制的引用以及免疫计算算法的效率上都有待改进，要使它应用于产品开发中还需要继续研究与探索。我们认为以后还要在以下几个方面做更

深一步的研究：

① 掌握更多的自然免疫学知识，进一步研究人体免疫机制，寻找能解决网络安全、入侵检测的新免疫机制。

② h-NSA 算法还只是停留在仿真实验阶段，要想真正应用到实际应用当中，还需要做进一步的工作

③ 研究出更好的检测入侵的算法，以解决检测器生成算法中存在的不足，如计算代价太高，算法分析方法有局限性等。

④ 将人工免疫技术与神经网络、遗传算法、数据挖掘等技术结合起来，综合各种算法的优点，取长补短，以取得更好的检测结果；或者利用一种方法加强另一种方法，开发更为有效的智能检测算法

参考文献

[1] Franciszek Seredynski, Pascal Bouvry. Some Issues in Solving the Anomaly Detection Problem using Immunological Approach. Proceedings of the 19th IEEE International Parallel and Distributed Processing symposium(IPDPS' 05), 2005IEEE

[2]YU HUA, CHAN-LE WU. Intrusion detection based on artificial immune system with self-similar traffic[J]. Proceedings of the Second International Conference on Machine Learning and Cybernetics, Xi' an, 2003, 11, pp:2-5

[3] Jungwon Kim, Peter, J, Bentley. Immune system approaches to intrusion detection-a review. Natural Computing, Springer, 2007

[4] Anderson J P. Computer security thread monitoring and surveillance[R]. Fort Ishington, PA: Jame A Anderson Co, 1980.

[5] Denning D E. An intrusion-detection mode[J]. IEEE Transaction on Software Engineering, 1987, 13(2):222-232

[6] Heberlein L T. A network security monitor[A]. In Proceedings of the IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA:IEEE, 1990:296-304

[7] Crosbie M, Spafford G.. Defending a computer system using autonomous agents[R]. Purdue University: COAST Laboratory, Department of Computer Sciences, 1994.

[8] Chen S S, cheung S, Dilger M, et al. GrIDS-A graph based intrusion detection system for large networks[R]. Baltimore, MD: The 19th National Information Systems Security Conference, 1996.

[9] Cheung S, Craford R, Dilger M, et, al. The design of GrIDS: a graph-based intrusion detection system[R]. University of

California: Department of Computer Science, 1999.

[10] Forrest S, Hofmeyr S, Somayaji A. Computer immunology [J]. Communications of the ACM, 1997, 40(10): 88-96

[11] Forrest S, Hofmeyr S, Somayaji A, et al. A Sense of Self for Unix Processes[A]. In Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy[C]. 1996:120-128

[12] Andersion R, Khattak A. The use of information retrieval techniques for intrusion detection[R]. Louvain-la-Neuve, Belgium: Proceeding of RAID' 98, 1998

[13] Terran D L. Machine Learning Techniques for the Computer Security Domain of Anomaly Detection[D]. Purdue University, 2000.

[14] 葛丽娜. 基于人工免疫的入侵检测模型与方法研究[M]. 广西大学硕士毕业论文. 2004.5 PP: 2-4

[15] Dong Y L, Qian J, Shi M L. A cooperative intrusion detection system based on autonomous agents [A]. In Proceedings of IEEE Conference on Electrical and Computer Engineering (IEEE CCECE 2003)[C]. 2003, 2: 861-863

[16] Adma J. Rocke, Ronald F. Demara. Confidant:Collaborative Object Notification Framework for Insider Defense using Autonomous Network Transactions. Autonomous Agents and Multi-Agent System[J]. Vol12(1), 2006, 1, pp:93-114

[17] Spafford E, Zamboni D. AAFID: Autonomous Agents for Intrusion Detection [A]. Web proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID' 98)[C]. 1998

[18] Giacinto G, Roli F. Intrusion detection in computer networks by multiple classifier systems[A]. In Proceedings

of the 16th International conference on Pattern Recognition[C]. 2002,2:390-393.

[19]Xiao Yun, Han Chongzhao, Zheng Qinghua, Zhang Junjie. Network Intrusion Detection Method based on RS-MSVM. Journal of electronics(China). Vol 23(6), 2006, 11, pp:902-905

[20] Jackson K A, Dubois D H, Stallings C A. NADIR-A Prototype Network Intrusion Detection System[R]. LA-UR-90-3726, Los Alamos National Laboratory, 1990.

[21] Ye N, Emran S M, Li X Y, et al. Statistical process control for computer intrusion detection[A]. In Proceedings of DARPA Information Survivability Conference & Exposition II (DISCEX' 01)[C]. 2001,1:3-14

[22] Garcia R C, Cannady J, Boundary expansion of expert systems: incorporating evolutionary computation with intrusion detection solutions [A]. In Proceedings of IEEE SoutheastCon[C]. 2001:96-99

[23] Zhen L, Florez G, Bridges S M. A comparison of input representations in neural networks: a case study in intrusion detection[A]. In Proceedings of the 2002 International Joint Conference on Neural Networks (IJCNN' 02)[C]. 2002, 2:1708-1713

[24] Qinzhen Wu, Luxi Yang, Qingfu Zhao, Zhenya He. A novel intrusion detection mode based on understandable neural networktrees. JournalofElectronics. Vol23(4), 2006, 7, pp:574-579

[25] Kuri J, Navarro G, Me L, et al. A Pattern Matching Based Filter for Audit Reduction and Fast Detection of Potential Intrusions [A]. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection

(RAID' 2000)[C]. 2000:17-27

[26] Payer U. State-driven stack-based network intrusion detection system [A]. In Proceedings of the 7th International Conference on Telecommunications (ConTEL2003)[C]. 2003, 2:613-618

[27] Kumar S. Classification and Detection of Computer Intrusions. Phd Thesis, Purdue University, August 95.

[28] Ryan J, Lin M and Miikkulainen R. Intrusion Detection with Neural Networks. In Jordan, M, 1998

[29] Me, Michel. Intrusion Detection: A Bibliography. 2001

[30] Clifford Kahn, Phillip A. Porras, Stuart Staniford - Chen, Brian Tung. The Common Intrusion Detection Framework Architecture [EB/ OL] .http:/ / www. gidos. Org. July 15, 1998

[31] Lindqvist U, Porras P A. eXpert-BSM: a host-based intrusion detection solution for Sun Solaris [A]. In Proceedings of the 17th Annual computer Security Applications conference (ACSAC 2001)[C]. 2001:240-251

[32] Draelos T, Duggan D, Collins M, et al. Adaptive critic designs for host-based intrusion detection [A]. In Proceedings of the 2002 International Joint Conference on Neural Networks (IJCNN' 02) [C]. 2002, 2:1720-1725

[33] Lichodzijewski P, Nur Zincir-Heywood A, Heywood M I. Host-based intrusion detection using self-organizing maps [A]. In Proceedings of the 2002 International Joint conference on Neural Networks (IJCNN' 02) [C], 2002, 2:1714-1719

[34] Li M, Jia W J, Zhao W. Decision analysis of network-based intrusion detection systems for denial-of-service attacks

[A]. In Proceedings of International conferences on Info-tech and Info-net (ICII' 01)[C]. Beijing: 2001,5:1-6

[35] Wang L N, Yu G, Wang G R, et al. Method of evolutionary neural network-based intrusion detection [A]. In Proceedings of International conferences on Info-tech and Info-net (ICII' 01)][C]. Beijing: 2001, 5:13-18

[36] Koutsoutos, Stefanos, christou, Ioannis, Efremidis. An Intrusion Detection System for Network-Initialted Attacks Using a Hybrid Neural Network. International Federation for Information Processing (IFIP) 2006, pp: 228-235

[37] Erbacher R F, Walker K L, Frincke D A. Intrusion and misuse detection in large-scale systems[J]. IEEE Computer Graphics and Applications, 2002, 22(1): 38-47

[38] Carrascal A, Couchet, J, Ferreira, E, Manrique D. Anomaly Detection using prior knowledge:application to TCP/IP traffic. In IFIP International Federation for Information Processing, Voluine 217, Artificial Intelligence in Theory and Practice, ed. M. Brainer, (Boston: Springer), 2006, pp: 139-148.

[39] Kumar S, Spafford E. H. A Software Architecture to Support Misuse Intrusion Detection. Technical Report CSD-TR-95-009, Purdue University, Department of Computer Science March 1995.

[40] Lunt T. IDES: An intelligent System for detecting Intruders [A]. In Proceedings of the symposium: computer Security, Threat and Countermeasures[C]. Roma, Italy: 1990

[41] Tan K M C, Maxion R A. Determining the operational limits of an anomaly-based intrusion detector [J]. IEEE Journal on Selected Areas in Communications, 2003 21(1): 96-110

[42] Estevez-Tapiador J M, Garcia-Teodoro P, Diaz-Verdejo J E. Stochastic protocol modeling for anomaly based network intrusion detection [A]. In Proceedings of the first IEEE International Workshop on Information Assurance (IWIAS 2003)[C]. 2003:3-12.

[43] Daejoon J, Taeho H. Ingoo H. The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors [J]. Expert Systems with Applications, 3003, 25(1): 69-75

[44] Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines [A]. In Proceedings of the 2002 International Joint conference on Neural Networks (IJCNN' 02)[C]. 2002, 2:1702-1707

[45] Peng Ning, Douglas S Reeves, Yun Cui. Correlating Alerts Using Prerequisites of Intrusions [A]. ICPADS 2002 [C] .2002.

[46] 莫宏伟. 人工免疫系统原理与应用[M].哈尔滨工业出版社. 2002.11, PP: 4-5

[47] 李红燕.基于免疫原理的网络入侵检测技术的研究(D) .西安电子科大，2003，1

[48] 朱锡华.生命的卫士-免疫系统.北京：科学技术文献出版社,1999

[49] L. N. de Castro, Fernando José Von Zuben. Artificial Immune Systems: Part I - Basic Theory and Applications. Technical Report TR - DCA 01/99, FEEC/UNICAMP, Brazil, December 1999, 95p.

[50] T.B.Kepler, A.S.Perelson, Somatic Hyper-mutation in B Cells: An Optimal Control Treatment. [J]. Theror. Biol., 1993, 164:37-64.

[51] Calada, F.and Seiden, P.E. Affinity Maturation and

Hyper-mutation in a Simulation of the Humeral Immune Response", Eur. J. Immunol, 1996, 26:1350-1358

[52] Smith, Derek, Stephanie Forrest, and Alan Perelson. Immunological Memory is Associative. D. Dasgupta, Artificial Immune Systems and their Applications, Springer-Verlag, Berlin Germany, 1998, 105-115.

[53] F. Abbattista, G. Di Danto, G. Di Gioia & M. Fanelli. An Associative Memory Based on the Immune Network. Proceedings of IEEE International Workshop on Neural Networks. Ishington: USA, IEEE. 1996.

[54] 葛红. 免疫算法及核聚类人工免疫网络应用研究. 华南理工大学博士论文, 2003, 5

[55] D. J. Smith, S. Forrest and D. H. Ackley, and A. S. Perelson. Variable Efficacy of Repeated Annual Influenza Vaccination. Proceedings of the National Academy of Sciences, 1999, 96:14001-14006.

[56] D. J. Smith, S. Forrest and D. H. Ackley, and A. S. Perelson. Using Lazy Evaluation to Simulate Realistic-size Repertoires in Models of the Immune System. Bulletin of Mathematical Biology, 1998, 60: 647-658.

[57] 李涛. 计算机免疫学[M]. 电子工业出版社, 2004. 48-49

[58] S. Forrest, A. S. Perlson, L. Allen, andR. Cherukuri. Self-Nonself Discrimination in a computer. Proc. The 1994 IEEE Symposium on Research in Security and Privacy, Los Alamitos, CA (1994) 202-212

[59] De Castro, L, N. & Von Zuben, F. J. Artificial Immune Systems: Part II-Asurvey of Applications. Technical Report - RT DCA 02/00, 2000, pp: 65

[60] D. Dasgupta and F. A. Gonzalez. Evolving complex Fuzzy Classifier Rules Using a Linear Genetic Representation. In the Proceedings of the International conference Genetic and

Evolutionary Computation (GECCO), San Francisco, California July 7-11, 2001

[61] Dipankar Dasgupta, Immunity-Based Intrusion Detection Systems: A General Framework. In the proceedings of the 22th National Information systems Security conference (NISSC) [C], October 1999, PP: 18-21

[62] Jon Timmis. Artificial immune systems: A novel data analysis technique inspired by the immune network theory. PhD thesis, Department of Computer Science, University of Wales, Aberystwyth, Ceredigion, Wales, August 2000

[63] Guiliang Yin. A Distributed Generation Islanding Detection Method Based on Artificial Immune system.2005IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific[C].pp:1-4

[64] De Castro, L, N & Von Zuben, F, J. The clone Selection Algorithm with Engineering Applications. In Proceedings of GECCO' 00, Workshop on Artificial Immune Systems and Their Applications, 2000, pp: 36-37

[65] De Castro, L, N & Von Zuben, F, J. An Evolutionary Immune Network for Data Clustering In Proceedings of the IEEE SBRN' 00 (Brazilian Symposium on Artificial Neural Networks), 2000,pp: 84-89

[66] Jianyong Tuo,Shouju Ren,Wenhuang Liu,Xiu Li, Bing Li,Lin Lei. Artificial Immune System for Fraud Detection.2004IEEE International Conference on Systems, Man and Cybernetics.pp:1407-1411

[67]Felipe Campelo,Frederico G,Guimaraes, Hajime Igarashi. Overview of Artificial Immune systems for Multi-objective Optimization. S. Obayashi et al. (Eds.): EMO 2007, LNCS 4403,

pp. 937 - 951, 2007.

[68] [71] Hoffmann G W. A Neural Network Model Based on the Analogy with the immune System [J]. Theoretical Biology, 1986(122), pp: 33-67

[69] Famer, J D, Packard, N, H & Perelson, A, S. the Immune System, Adaptation, and Machine Learning, Physical 22D, 1986, pp: 187-204

[70] Bersini H, Varela F J. Hints for Adaptive Problem Solving Gleaned form Immune Networks. In Proceedings the First Workshop on Parallel Problem Solving from Nature 1990, pp: 343-354

[71] Hofmeyr S A. Forrest S. Architecture for an Artificial Immune System. Submitted to Evolutionary computation, 2000

[72] Okamoto T. Ishida y. Multi-agent Approach against computer Virus: An Immunity-Based System. In Proceedings of the AROB' 99, 1999, pp: 69-72

[73]X. Z. Gao, S. J. Ovaska, X. Wang, M. Y. Chow. A neural networks-based negative selection algorithm in fault diagnosis. Neural & Application [J]. 2007, 1, pp: 521-529

[74] 张衡，吴发，张毓，曾庆凯. 一种 r 可变阴性选择算法及其仿真分析. 计算机学院，2005，28(10)，pp：1614-1619

[75] 冯艳华，钟诚，李智. 一种基于多级否定选择的入侵检测器生成算法. 计算机技术与发展, 2006，16(4)，pp：234-236

致　谢

三年来的求学生涯，我要感谢导师葛红副教授对我的教诲、关心和帮助。本文在葛老师的关怀和悉心指导下才能得以顺利完成。葛老师渊博的理论知识和深厚的专业素养不但给我指明了研究方向，而且还在许多技术细节上给予我具体的指导。葛老师倡导的自由研究风气以及她开朗豁达的性格、平易近人的作风，给我留下了极深刻的印象。她不仅在学业上对我耐心引导启发、严格要求，而且在生活上也给予了我极大的关心和鼓励，同时更注重对自身素质和能力的培养。她经常与我们交流思想，教导我们如何做人，如何找准自己的人生方向。从她那里，我不仅学到了许多知识，也学到了许多做人的道理，这将使我终生受益。在此，向葛老师表示崇高的敬意和诚挚的谢意！

广东航海专科学院的钟碧良教授在学业上给予了我无私的帮助和鼓励，在此表示诚挚的谢意。

感谢计算机学院的鲍苏苏院长、林伟雄书记等领导和王敬、谢金丽等老师三年的关心和帮助。

感谢徐春鸽同学给予了我许多有益的借鉴和宝贵的意见。

感谢彭丰平、倪宇斌、张树伟、裴颂伟、何旭暑、蒋鹏、李海涛、张永华等兄弟在学习和生活上给予的关心和帮助，同他们愉快的相处将成为我美好的回忆！

在此，我还要深深感谢我的父母和家人以及我的女朋友和她的家人，正是由于他们对我毫无保留的关心和支持，才使我得以顺利的完成研究生学业！

最后，感谢审稿的各位评委和专家在百忙之中抽空审阅我的论文。

祝所有关心和帮助过我的老师、同学和朋友们身体健康、工作顺利、家庭幸福！

攻读硕士学位期间撰写及发表论文情况

1. 章登科，葛红. 基于人工免疫系统的计算机安全研究. 网络安全技术与应用，2007 年 1 月第1 期.

2. 章登科，葛红，徐春鸽. 基于人工免疫系统的异常检测中检测器生成方法研究. 计算机应用研究，2007 年 9 月第 1 版

3. 葛红，章登科，徐春鸽. 核聚类人工免疫的评价函数研究. 哈尔滨工业大学学报， 2006 Vol. 27 No. z1

4. 徐春鸽，章登科，葛红. 人工免疫系统在数据挖掘中的应用. 计算机技术与发展，2007 Vol, 17 No. 4