学校编码：10384
学号：200428008

分类号____密级____
UDC_____

硕 士 学 位 论 文

基于免疫原理的 NIDS 研究

Research on NIDS Based on Immunological Principle

邓文亮

指导教师姓名： 倪子伟 副教授
专 业 名 称： 计算机系统结构
论文提交日期： 2007 年 5 月
论文答辩时间： 2007 年 月
学位授予日期： 2007 年 月

答辩委员会主席：_____
评 阅 人：_____

2007 年 5 月

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年　月　日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1.保密（　），在年解密后适用本授权书。

2.不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

摘　要

生物免疫系统是一个自适应、自学习、自组织、并行处理和分布协调的复杂系统。人工免疫系统的研究旨在抽取生物免疫系统中独特的信息处理机制,研究和设计相应的模型和算法，进而解决各种复杂问题。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。

生物免疫系统的基本功能是识别自我和非我，并将非我分类清除，具有免疫识别、免疫记忆、免疫调节、免疫宽容和免疫监视等功能特征。通过深入研究生物免疫系统所蕴含的各种信息处理机制，构建和设计有效的入侵检测模型和算法，对于建立基于生物免疫系统的入侵检测新理论、新方法，改变当前网络安全状况具有至关重要的意义。

本论文深入探索和研究生物免疫系统所蕴含的学习与检测机制，利用人工免疫技术，面向入侵检测系统设计出高效的模型和算法。本论文主要研究工作有:

首先,在讨论了检测器的生成和更新的基础上，改进了现有的人工免疫算法，在协同刺激、记忆检测器变异、冗余消除、检测器进化等方面做了修改，使人工免疫模型更具合理性。

其次，提出了改进的克隆选择算法用于检测器的进化，引入了遗传机制和再选择机制，生成具有更高检测效率的记忆检测器，并通过实验，证明了算法的优越性。

再次，提出了改进的动态克隆选择算法用于入侵检测，引入了变异机制和冗余消除机制，并通过实验，证明了算法的有效性。

最后，提出了一个基于免疫原理的分布式入侵检测模型，将上述两种算法运用到模型中，使整个系统具有更高的检测效率。

关键词：生物免疫；入侵检测；分布式

Abstract

Biological immune system is a complex system of self adaptive, self-learning, self-organization, parallel processing and distributed coordination. The research purpose of Artificial Immune System is to extract special information processing mechanisms contained in biological immune system, and then to study and design the corresponding models and algorithms that could be used to solve many kinds of complex problems. In recent years, immune-based intrusion detection has become a key research area in intrusion detection system, exploring natural immunological theories, mechanisms and principles for detecting and reacting to intrusions.

The basic function of biological immune system is to recognize self and non-self, and then to classify and eliminate non-self. Biological immune system has the characteristics of immune recognition, immune memory, immune regulation, immune tolerance, immune surveillance etc. By deeply researching into various information processing mechanisms contained in biological immune system, many effective models of intrusion detection and algorithms can be established and designed, and it is of great significance to the establishment of new theory and new method of intrusion detection based on biological immune system, also to the change of the current situation of network security.

The purpose of this paper is to explore and research into the learning and detecting mechanisms contained in biological immune system, and then to use the technology of artificial immune, to design efficient models and algorithms for intrusion detection system. The main research work of this paper can be summarized as follows:

Firstly, on the basis of discussing the creation and updating of the detector the paper makes some improvement on existing artificial immune algorithms. The modification includes co-simulation, mutation of detector, redundancy avoided and evolution of detector, making the artificial immune model reasonable.

Secondly, the paper introduces inheritance mechanism and reselection mechanism into clonal selection algorithm, comes up with an improved clonal selection algorithm used for evolving detector, creates memory detector with higher efficiency of detection, and then the experimentation proves the advantage of the algorithm.

Afterwards, the paper introduces mutation mechanism and redundancy avoided mechanism into dynamic clonal selection algorithm, comes up with an improved dynamic clonal selection algorithm used for detecting intrusion, and then the experimentation proves the efficiency of the algorithm.

Finally, the two algorithms discussed above the paper come up with a distributed network intrusion detection system with higher efficiency of detection.

Key words: Biological immune; Intrusion detection; Distributed

目 录

CONTENT

第一章　　绪 论

当今社会信息化程度越来越高，信息的重要性带来了互联网的高速发展。网络技术发展的同时伴随了大量的安全隐患，信息安全受到了很大的冲击，引起了人们的重视，在网络中引入安全防范机制成为人们的共识。入侵检测系统（IDS: Intrusion Detection System）是近年出现的新型网络安全技术，是一套软件和硬件的结合体,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。入侵检测是一个全新的、迅速发展的领域，并且已成为网络安全中极为重要的一个课题。入侵检测方法及其产品也在不断的研究和开发之中，并且已经在网络攻防实例中初步展现出其重要价值。因此对入侵检测理论和技术的研究具有很强的现实性和紧迫性。

1.1　入侵检测的产生背景

互联网的高速发展，极大地加快了社会信息化的步伐。随着计算机技术和通信技术在金融、政府、医疗、制造业、商业、教育各界的广泛应用，网络安全问题已经越来越受人们重视。借助于计算机网络环境，实现了跨地区的电子银行、电子商务、电子政务、金融网络、制造资源管理和网络虚拟社区等多种应用。但是，网络的开放性也为信息的窃取、盗用、非法修改以及各种扰乱破坏提供了可乘之机，使得信息在存储、处理和传输等各个环节，都有可能遭到入侵者的攻击或病毒的危害，造成系统的瘫痪或重要数据的丢失。为了保护网络和系统的安全，人们针对信息的存储、处理和传输的各个环节使用了各种安全技术。但是人们发现单独的使用一种安全技术是不可靠的，只有将各种安全技术综合地使用在一个整体的安全方案中，才可以尽可能地保护信息和系统的安全。传统上，人们针对内部网络一般采用防火墙作为安全的第一道防线，但是随着攻击技术的日趋成熟，攻击工具与方法的日趋复杂多样，单纯的防火墙策略已无法满足对安全高度敏感部门的需要，对网络的保护必须采用深层次、多样化的手段。与此同时，如今的网络环境也变得越来越复杂，各种各样的设备升级、系统补丁使网络管理员的工作不断加重，不经意的疏忽便有可能造成安全的重大隐患。

入侵检测系统正是在这种背景下，经过了近二十年的发展成为安全领域内的重要技术和研究方向。与传统的被动式防御的防火墙相比，入侵检测作为一种积极主动的安全

防护技术，提供了对内部攻击、外部攻击和误操作的实时保护。它能很好地弥补防火墙的不足，在不牺牲网络性能的前提下对网络进行检测，可以看作防火墙之后的第二道安全闸门。它是对系统中未授权访问或异常现象、活动与时间进行审计、追踪、识别和检验的全过程。它可以识别出系统是否被入侵，从而做出及时的反应，切断网络连接、记录时间和报警，提醒系统管理员采取相应的措施，进一步可以提供法律上的依据，避免系统受到进一步的侵害。

1.2　入侵检测的概念

1980 年 James Anderson 首先提出了入侵检测的概念，他将入侵尝试（Intrusion Attempt）或威胁（Threat）定义为潜在的有预谋的未经授权的访问信息操作信息致使系统不可靠或无法使用的企图，他提出审计追踪可应用于监视入侵威胁。

入侵（Intrusion）指的就是试图破坏计算机保密性、完整性、可用性或可控性的一系列活动。入侵活动包括非授权用户试图存取数据，处理数据，或者妨碍计算机的正常运行。入侵检测就是对计算机网络和计算机系统的关键结点的信息进行收集分析，检测其中是否有违反安全策略的事件发生或攻击迹象，并通知系统安全管理员（Site Security Officer）。

在国标 GB/T18336 指出，入侵检测是指“通过对行为、安全日志或审计数据或其它网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图”。入侵检测是检测和响应计算机误用的学科，其作用包括威慑、检测、响应、损失情况评估、攻击预测和起诉支持。

1.3　入侵检测的分类

可以从检测技术、检测对象等标准对入侵检测进行分类。

1.3.1　基于检测技术分类

根据所采用的检测技术不同，入侵检测一般分为异常检测（Anomaly Detection）和误用检测（Misuse Detection）。

异常入侵检测是根据将观察到的异常行为与系统历史正常行为进行比较来发现入侵，亦即检测与可接受行为之间的偏差。如果可以定义每项可接受的行为，那么每项不

可接受的行为就应该是入侵。首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型漏报率低，误报率高。因为不需要对每种入侵行为进行定义，所以能有效检测未知的入侵。

误用检测模型（Misuse Detection）：误用入侵检测是根据定义好了的攻击行为的特征集合或规则集合进行特征匹配或规则匹配,当有匹配发生时指示发现入侵，亦即检测与已知的不可接受行为之间的匹配程度。如果可以定义所有的不可接受行为，那么每种能够与之匹配的行为都会引起报警。收集非正常操作的行为特征，建立相关的特征库，当检测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。这种检测模型误报率低、漏报率高。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且特征库必须不断更新。

1.3.2 基于检测对象分类

从检测对象上划分，入侵检测一般分为基于主机的入侵检测、基于网络的入侵检测和混合的入侵检测：

基于主机（Host-Based）：系统分析的数据是计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录。主机型入侵检测系统保护的一般是所在的主机系统。

基于网络（Network-Based）：系统分析的数据是网络上的数据包。网络型入侵检测系统担负着保护整个网段的任务，基于网络的入侵检测系统由遍及网络的传感器（sensor）组成，传感器是一台将以太网卡置于混杂模式的计算机，用于嗅探网络上的数据包。

混合型：基于网络和基于主机的入侵检测系统都有不足之处，会造成防御体系的不全面。综合了基于网络和基于主机的混合型入侵检测系统既可以发现网络中的攻击信息，也可以从系统日志中发现异常情况。

1.3.3 基于实时性的分类

根据系统的实时性分类，入侵检测系统一般分为定时入侵检测系统和实时入侵检测系统和两者混合型的入侵检测系统。

定时入侵检测系统：定时系统首先收集网络和审计数据并存储到数据库中，然后根据预先设定的时间对数据进行批量处理，集中进行检测，产生入侵报警。这种检测方式

的缺点在于缺乏必要防范，无法及时对入侵做出有效的响应，实时性差；优点在于减少对系统紧缺资源的占用，提高用户日常任务使用效率。

实时入侵检测系统：系统对网络和审计数据边收集、边检测，实时响应异常事件，产生入侵报警。这种检测方法的优点在于能够在受保护对象被攻击之前做出有效的响应，实时性好，所以该方法是大多数IDS的首选方法；缺点在对计算机系统性能要求高，但是这几年随着计算机硬件速度的大幅度提高，这种检测方法已经得到广泛应用。

混合型：在网络流量负荷太重，实时系统不能及时数据进行详细分析，影响系统检测效果时，我们考虑用把实时分析和定时的批处理结合起来，先用实时分析对数据进行初步处理，尽快发现潜在入侵企图，计算明显的攻击特征，监视可疑网络行为，然后批处理进行详尽分析，分析的结果还可以用来训练和学习误用检测系统。

1.4　入侵检测系统组成

入侵检测一般有三个步骤：数据提取、数据分析和响应处理，所以入侵检测系统至少包括三个主要模块：数据采集模块、数据分析模块和响应处理模块，此外，还可能结合规则知识库、入侵与日志数据库、监控中心等功能模块，提供更为完善的安全检测及数据分析功能。入侵检测系统结构如图1.1。

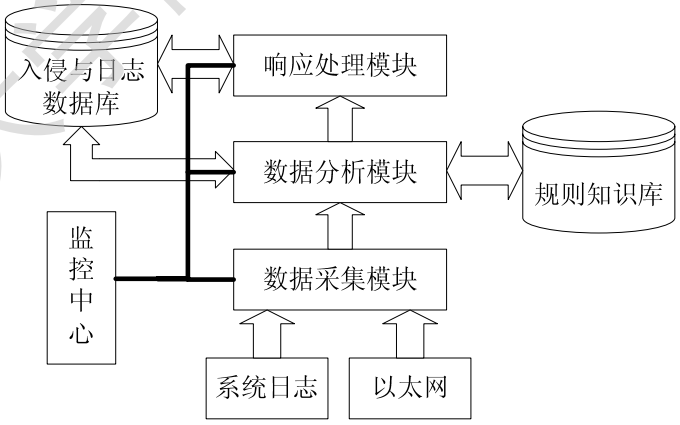

图1.1 入侵检测系统结构

数据采集模块：主要负责收集网络和系统用户的状态和行为，并完成数据的过滤及其他预处理工作，为数据分析模块提供原始的安全审计“事件”数据。数据采集模块是整个IDS的基础，所以设计时要注重对重要数据的识别，提高数据采集和预处理的效率。

功能和效率直接影响IDS的性能。

数据分析模块：对收集的数据进行同步、整理成格式化的事件记录，提取其中蕴含的系统活动特征或网络行为模式，然后对事件记录进行组织和分类，结合先验知识，利用模式匹配、统计分析和完整性分析等技术，将记录分类为正常和异常，并将分析结果传达给响应处理模块，同时更新规则知识库和入侵数据库。

响应处理模块：响应部件对确认的入侵行为按照预先设定的规则采取响应措施。检测系统一般采取两种响应措施。一是采取消极的相应措施，如给管理员发送报警信息、设置SNMP陷阱等。二是采取保护性措施，如切断入侵者的TCP 连接、修改路由器的访问控制策略、入侵取证等。

监控中心：是系统中对其它各个部件进行控制协调工作的部分，通过主控部件可以直接对其它各个部件进行相应的操作。

1.5　论文的主要内容

本文分成五章，其主要内容如下：

第一章是绪论，首先介绍了入侵检测的背景、概念、分类和系统组成；然后，从入侵检测系统的现状出发，论述本文的研究背景和意义。

第二章简述了生物免疫系统的基础知识，主要介绍了免疫耐受、免疫学习和记忆、克隆选择和扩增等免疫系统的工作机制，在此基础上讨论了人工免疫系统（AIS），包括AIS的概念、通用框架和主要算法。最后阐述生物免疫系统和入侵检测系统的相似性以及免疫原理对入侵检测技术的启示，为免疫系统应用于入侵检测系统提供了依据。

第三章从集合论的角度对基于免疫的入侵检测模型进行了数学描述，分析了否定选择和克隆选择免疫模型在入侵检测系统中的具体实现。包括入侵检测的编码方式、匹配规则、亲和力计算，通过对检测器的生成、更新和进化的分析，改进了否定选择算法、克隆选择算法和动态克隆选择算法，并运用到具体的入侵检测实验中。

第四章提出了一个分布式检测系统模型，从自适应性、分布式特性、可扩展性和健壮性等方面分析了系统的可行性。

第五章总结本文的主要工作和贡献，并给出了一些有待进一步研究的问题。

第二章　　生物免疫及人工免疫原理

进入 20 世纪以来，人们对免疫学的研究产生了浓厚的兴趣，随着试验技术的进步，人们发现一直以来被认为由感染直接引起过敏反应其实就是生物免疫现象。20 世纪中叶以后，借助第三次科技革命的成果，自然科学得到了飞跃式的发展。随着理论知识和试验技术的不断发展，人们在免疫学方面的研究取得了巨大的进步，逐步形成了现代免疫学。

2.1　生物免疫系统概述

免疫学（Immunology）是研究机体免疫系统组织结构和生理功能的科学[2]。免疫是指机体对“自我（Self)”和“非我（Nonself)”的识别并排除“非我”，即机体识别和排除抗体性异物籍以维持机体的生理平衡和稳定的功能[2]。

免疫系统最重要的生理功能是对“自我”和“非我”抗原分子的识别及应答，对“自我”抗原形成天然免疫耐受，对“非我”抗原产生排斥作用的一种生理功能，这种识别及应答作用是由免疫细胞完成的。抗原（Antigen，Ag）是指能诱导免疫系统发生免疫应答，并能与其产生的抗体或效应细胞在体内或体外发生特异性反应的物质。机体内的免疫系统一般执行以下功能：

1、免疫防御（Immunological Defence)：机体免疫系统对“自我”抗原形成天然免疫耐受，抵抗“非我”抗原入侵，清除侵入的病原体及其他异物，以保护机体不受外来异物的侵害。

2、免疫自稳（Immunological Homeostasis)：不断清除衰老死亡的细胞，保持体内的净化更新，以保持机体的生理平衡。

3、免疫监视（Immunological Surveillance)：及时识别和清除染色体畸变或基因突变的细胞，防止癌瘤的发生。

2.2　免疫系统组成

免疫系统（Immune System）是执行免疫功能的物质基础，免疫系统一本由免疫器官、免疫细胞和免疫分子组成。