中南财经政法大学
青年学术文库

基于免疫原理的自适应入侵检测建模研究

孙夫雄 著

长江出版传媒 | 湖北人民出版社

前　言

当前世界各国信息化快速发展，信息技术的应用促进了全球资源的优化配置和发展模式的创新，互联网对政治、经济、社会和文化的影响更加深刻，信息化渗透到国民生活的各个领域，围绕信息获取、利用和控制的国际竞争日趋激烈，保障信息安全成为各国重要议题。中国是网络大国，也是面临网络安全威胁最严重的国家之一，网络安全已经成为关系国家安全和发展、关系广大人民群众切身利益的重大问题。

随着网络技术的不断发展和网络应用范围的不断扩大，对网络的各类攻击与破坏也与日俱增，同时攻击的手段日新月异，攻击的方式层出不穷，因此入侵检测系统面临着严峻的挑战。如何改善入侵检测系统的性能如有效性、健壮性和适应性等，是当前急需解决的问题。而自然免疫系统拥有多层次、多样性、独特性、动态防护性、自适应性、联想记忆等众多优点，由于其在抵抗病毒和细菌等病原体的入侵方面担当着与入侵检测系统类似的任务，因此自然免疫系统为解决入侵检测问题提供了一个自然的模板。本书基于免疫原理研究入侵检测技术，即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。

本书可供信息安全专业的师生了解计算机网络入侵检测领域的一般方法，并了解基于生物免疫系统的原理研发相应的入侵检测系统的总体框架及流程。

全书分为七章。第一章为绪论部分，介绍了本书的研究背景、意义及

目的；综述了入侵检测模型的研究现状与进展。第二章介绍了免疫学的理论基础知识，分析了计算机安全和自然免疫系统之间的共同之处，以及两者间的差异。第三章从自然免疫系统的抽象模型研究入手，重点分析了当前入侵检测系统的免疫模型研究中存在的不足，给出了免疫模型的设计原则、建模思路和目标，并提出了一种新的基于免疫原理的自适应入侵检测模型 IAIDM（Immune-based Adaptive Intrusion Detection Model），概述了 IAIDM 的结构和工作原理。第四章类比自然免疫系统中先天 B 细胞的原理，提出了以最小候选检测器集合的概念来定义覆盖整个入侵检测的问题域所需检测器的最低数量，并对其空间覆盖特性、生成算法和初始化方式进行了深入的研究。第五章基于自然免疫系统中抗原显现的机制，深入研究与分析入侵检测系统中检测时间与检测空间之间存在的矛盾。第六章从入侵检测的有效性以及系统的适应性和柔性检测几个方面对基于免疫原理的自适应入侵检测模型的性能进行了测试和评价，并进行了扩展和优化。给出了最终系统实验及其结果分析。第七章进行总结和展望。

笔者长期从事信息安全的研究工作，对免疫系统在信息安全领域的运用进行了较深入的研究，取得了较多的研究成果，参与了多项纵横向课题的研究工作，主持并参与了省部级相关项目多项，在国内权威学术期刊及国际会议上发表学术论文数十篇，其中 EI 收录 11 篇。

书中有关内容直接引用、参考了国内外许多文献资料，在此向所有被引用文献的作者表示感谢。在书稿的完成过程中，自始至终得到了武汉大学黄天戍教授、孙涛教授等学者的指导和帮助。

本书得到中南财经政法大学中央高校基本科研业务费专项资金资助（2722020JCT034）。

笔者希望尽力将本书写好，但由于水平有限，时间有限，书中难免出现疏漏，留下一些遗憾，希望读者提出宝贵意见，以便再版时修改和完善，甚为感谢。

目　录

1 绪论

1.1 研究概述

随着医学、生理学研究的长足进步，人们已发现自然免疫系统不仅仅是单纯排除外来入侵物，而且具有在多变的环境中保存和延续自己的重要功能。也就是说，各种淋巴细胞不是简单地在体液中散乱浮游，而是通过彼此通信，在有效性、适应性、可扩展性以及健壮性等方面具有先天的优势，基于自然免疫原理的人工免疫系统（AIS，Artificial Immume System）已经发展成为应用仿生学的一个重要分支，AIS 凭其强大的信息处理能力，在自动控制、计算机安全、机器人、故障检测与恢复以及优化问题等方面取得广泛的应用。

本书在深入研究生物免疫机制的基础上，结合入侵检测系统自身的特点，研究基于免疫原理的自适应入侵检测模型。具体目标是针对现有计算机免疫安全系统在可靠性、知识性方面的缺陷问题，研究自然免疫系统中 B 细胞进化、抗原显现、B 细胞的克隆选择与高频突变、抗体间抑制与激励等重要的免疫机制，研究检测器在不同检测阶段中的演变形式及其行为属性，设计检测器的活化函数和相互间激励或抑制的算法，实现检测器动态更新和联想记忆的功能。

1.2 研究背景及意义

近年来互联网的迅速发展，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已经越来越大，计算机网络已经成为信息化社会发展的重要保证。互联网在中国的发展更是迅猛，中国互联网络信息中心（CNNIC）于2018年1月31日发布了第41次《中国互联网络发展状况统计报告》，报告显示截至2017年12月，我国网民规模达7.72亿，手机网民规模达7.53亿，普及率达到55.8%，超过全球平均水平（51.7%）4.1个百分点，超过亚洲平均水平（46.7%）9.1个百分点。中国上市互联网企业超百家，市值接近9万亿元，互联网正在以超出人们想象的深度和广度迅速发展，已经发展成为中国影响最广、增长最快、市场潜力最大的产业之一，给人们的日常生活提供了极大的便利。

世界各国信息化快速发展，信息技术的应用促进了全球资源的优化配置和发展模式的创新，互联网对政治、经济、社会和文化的影响更加深刻，信息化渗透到国民生活的各个领域。一方面各国围绕信息获取、利用和控制的国际竞争日趋激烈，另一方面网络系统自身安全脆弱性的客观存在，操作系统、应用软件、硬件设备不可避免地会存在一些安全漏洞，网络协议本身的设计也存在一些安全隐患，这些都为黑客入侵系统提供了可乘之机，即便是安全防范严密的军事网络系统也曾多次遭受攻击。所以，网络安全已成为制约信息化发展的一个关键问题，亟待解决。因此，如何保障信息安全成为各国重要议题。

在我国，网络空间安全问题尤为严重。据统计有近1.28亿互联网用户遭遇过身份盗用、交易诈骗、网络钓鱼等，初步估计损失超过150亿元人民币。国家互联网安全响应中心数据显示，2014年国内有1100余万台主机被4.2万台境外服务器控制，国家信息安全漏洞共享平台（CNVD）收录到的漏洞达9163个，被植入后门的网站达4万余个，约有3万个网站被恶意篡改，超过620余万台主机感染了木马或僵尸程序，导致我国成为分布式拒绝

服务（DDOS）攻击的全球最大受害国（约占 64.6%）和全球最大来源国（约占 46.6%）。2014 年国内网民有超过 31.8%的用户接触过钓鱼网站或木马程序，造成的经济损失同比 2013 年增长了 400%。2015 年发生的“12306 网站撞库事件”“网易邮箱用户信息泄露”等事件表明，网络安全关乎每个人的生活。

面临日益严重的网络空间安全问题和日益激烈的国际竞争，习主席强调“没有网络安全就没有国家安全，没有信息化就没有现代化”。日新月异的渗透手段和攻击技术对我国的安全防御能力提出了新的挑战。保障网络空间信息安全，已成为我国的国家安全发展战略。我国国家互联网信息办公室发布《国家网络空间安全战略》，指出网络空间安全事关人类共同利益，事关世界和平与发展，事关各国国家安全。维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障。

网络空间安全的研究具有巨大的市场价值。2016 年全球信息安全市场规模同比增长 7.9%，预计 2020 年市场规模将达到 1130 亿美元，以美国为主导的北美市场仍然占据全球最大的市场份额。预计 2016—2020 年中国信息安全产品市场规模将保持 18%以上的增长率，2020 年市场规模预计达到 761.95 亿元。在政策方面，2014 年成立中共中央网络安全和信息化领导小组，2016 年，网络安全被正式列入“十三五”规划重点建设方向；2017 年 6 月 1 日起，我国网络安全法正式实施。目前我国在网络安全方面的投入占整个 IT 行业的比重仍低于美国等发达国家，在网络安全法的推动下，产业投入有望持续增加。

入侵检测技术是继“防火墙”“数据加密”等传统安全保护措施后的新一代安全保障技术。作为一种积极主动的安全防护技术，它有效地补充和完善了其他安全技术和手段，提高了信息安全基础结构的完整性。一个有效的入侵检测系统（Intrusion Detective System，IDS）不仅要求能够正确地识别系统中的入侵行为，而且还要考虑到检测系统本身的安全以及如何适应网络环境发展的需要。随着各种攻击手段的不断提高，网络流量持续增大，迫切要求新型的具有自学习和自适应能力的智能入侵检测系统的出现，

所以入侵检测技术的研究涉及计算机、数据库、通信、网络、密码学和人工智能等综合知识，具有重要的理论研究意义。

动态的、自适应的以及智能的入侵检测系统是当前入侵检测技术的研究方向，生物的自然免疫系统在抵抗病毒和细菌等病原体的入侵方面担当着与入侵检测系统类似的任务，其分布性、扩展性、健壮性及适应性等特性为设计高性能的入侵检测系统提供了新的思路。本书旨在针对当前入侵检测系统存在的不足，深入地研究与借鉴生物免疫的原理，提出网络入侵检测新的免疫模型以解决当前入侵检测模型自适应能力不强、可扩展性较差及检测效率较低等问题。

1.3 国内外研究现状

1.3.1 入侵检测概述

网络安全模型由主体、对象和访问控制规则组成。它定义了主体如何按照访问控制规则访问对象，访问控制规则决定于网络的安全策略，网络安全策略规定了如何处理信息，是对网络系统的用户和软件行为许可的定义或描述，通常由系统管理员规定。安全模型是定义和实现安全策略的方法的抽象。概括地说，计算机网络安全的目标有以下五个方面。

（1）机密性（Confidentiality）。只有授权用户才能访问机密或限制性的数据。

（2）完整性（Integrity）。保证数据不由于恶意或偶然原因而被破坏。

（3）可用性（Availability）。保证合法用户能够有效地访问相关信息和系统资源。

（4）可说明性（Accountability）。在发现网络系统受损的情况下，网络安全系统能够保留足够的信息来确定受损原因。

（5）正确性（Correctness）。安全系统由于错误判断导致的误报警次数应该低于允许的阈值。

传统的网络安全方法主要是利用操作系统的识别和认证（IA，Identification and Authentication）、访问控制机制、防火墙和加密系统等，它们分别提供系统和网络级的安全保护。

访问控制机制由于以下两方面的原因，带来了潜在的安全问题。①配置问题：访问控制规则没有被正确地定义，为黑客攻击提供了可能。②程序错误：程序实现中的错误也使黑客可能利用访问控制机制攻击系统。

防火墙被用来在一个不可信网络（如因特网）与一个可信网络（如机构专用网）之间提供一个安全的边界。防火墙通常包含一个数据包过滤器、一组代理服务器、安全 IP 通道或虚拟专用网 VPN 等。防火墙是最广泛应用的网络级访问控制产品，为了能使防火墙生效，进入可信网络的所有网络传输都必须经过防火墙。但是，由于防火墙可能的配置错误以及防火墙实现中存在的缺陷等原因，防火墙也成为黑客攻击网络的通道。网络流量以指数方式增长的趋势和网络安全问题日渐严重的现实，传统的网络安全方法存在的局限性以及相关的网络技术的迅速发展，牵引和推动了一个新的网络安全技术即入侵检测技术的应运而生。

1986 年，多萝西·丹宁（Dorothy Denning）首次提出了一种通用入侵检测模型，如图 1-1 所示。模型的三个主要部件是事件生成器（Event Generator）、活动记录器（Activity Profile）和规则集（Rule Set），目前，该模型仍然得到广泛的应用。

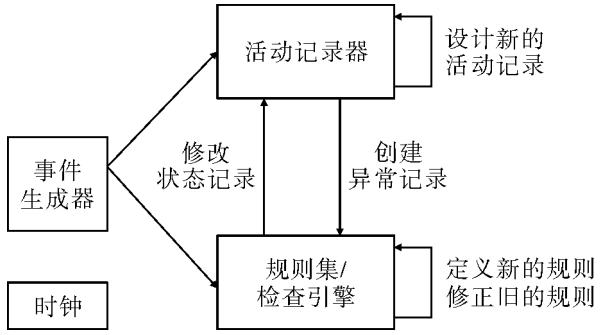

图 1-1　通用入侵检测模型

丹宁的通用入侵检测模型标志着入侵检测技术成为一个独立的研究领域。IDS 通过收集、分析有关网络安全的信息，寻找网络系统的违规模式和

未授权的访问尝试。当发现违规模式和未授权访问时，IDS 根据系统安全策略做出快速的反应。IDS 根据其采用的技术，可划分为异常入侵检测和误用入侵检测两大类型。

1.3.1.1 异常入侵检测

异常入侵检测是指能够根据用户的行为和对网络系统资源使用的异常所进行的检测。异常入侵检测试图用定量方式描述可接受的行为特征，以区分非正常的、潜在的入侵行为。它首先建立所保护的系统的正常特征轮廓，然后监测从审计数据报告上来的实际活动，通过它们与正常轮廓间的偏离程度来判别出异常行为活动。

异常入侵检测与系统相对无关，不需要系统及其安全性缺陷专门知识，通用性较强，能够检测出一些未知的攻击方法。但由于不可能对整个系统内的所有用户行为进行全面的描述，而且每个用户的行为是经常改变的，所以它的主要缺陷在于误检率很高，而且配置和管理起来比较复杂，尤其在用户数目众多，或工作方式经常改变的环境中。另外，由于行为模式的统计数据不断更新，入侵者如果知道某系统处在检测系统的监视之下，他们可以通过恶意训练的方式，促使检测系统缓慢地更改统计数据，以至于最初认为是异常的行为，经一段时间训练后也被认为是正常的，这是目前异常入侵检测所面临的一大困难。

1.3.1.2 误用入侵检测

误用入侵检测是指利用已知的攻击模式来检测入侵。误用入侵检测又称为基于签名的入侵检测和基于知识的入侵检测。

与异常入侵检测相反，误用入侵检测主要是通过按预先定义好的入侵模式对用户活动行为进行模式匹配来检测入侵行为，它能直接检测不利的或不可接受的行为。误用入侵检测准确度和效率都很高，但其缺陷是无法检测到新的攻击行为。另外，误用入侵检测系统对目标系统的依赖性太强，因而系统移植性不好，维护工作量大。

从入侵检测体系结构的角度，通常将 IDS 划分为基于主机的 IDS、基于网络的 IDS 和混合分布式的 IDS。

（1）基于主机的 IDS。早期的 IDS 大多属于这种类型，用于审计用户的

活动以检测入侵，比如用户的登录、命令操作、应用程序使用资源情况等，运行在被检测的主机或单独主机上，丹宁通用入侵检测模型就是建立在这类主机之上的。

（2）基于网络的 IDS。通常置于比较重要的网段内，通过线路窃听的手段对截获的网络分组进行处理，从中提取有用的特征模式，再通过与已知入侵特征相匹配或与正常网络行为原型相比较来识别入侵事件。基于网络的 IDS 根据网络流量、协议分析、简单网络管理协议信息等数据来检测入侵。

（3）混合分布式的 IDS。随着网络系统结构的复杂化和大型化，网络入侵手法趋向于多样化，入侵行为不再是单一的行为，而是表现出相互协作入侵的态势，单是基于主机的入侵检测系统或是基于网络的入侵检测系统都会造成主动防御体系不全面。不同类型的 IDS 之间需要优势共享、缺陷互补与协同检测，以便能够组合各种入侵检测的信息，更精确地识别和定位入侵行为，这也就形成了混合分布式入侵检测系统。

1.3.2 入侵检测模型研究现状

从丹宁提出通用入侵检测模型至今，入侵检测技术已经经历了 30 多年的发展历程。随着网络技术与科学技术的迅速发展，各种分析方法（如专家系统、统计分析、数据挖掘、人工智能及机器学习等）被广泛运用于入侵检测的建模研究，其中具有代表性的入侵检测模型有以下几种。

1.3.2.1 基于专家系统的模型

专家系统（Expert System）是最早的误用入侵检测方案之一，基于由专家经验事先定义规则的推理系统，它将策略声明和已知的攻击编码成一个规则集，其中规则具有 if-then 格式，当规则左边的条件得到满足时就执行右边的动作。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。专家系统的优点在于把系统的控制推理过程从问题解决的描述中分离出来，用户不需要理解或干预专家系统内部的推理过程，而只需把专家系统看作是一个自治的黑盒子（Black Box）。专家系统应用于入侵检测时，不能检测出未知入侵。

1.3.2.2 基于统计分析的模型

基于统计分析模型是最早的异常入侵检测系统，首先收集大量的训练数据，对训练数据中各个属性的取值范围划分统计度区间，确定统计度量值 Q，由 Q 值计算统计测度 S。对数据中的每个元素按时间间隔计算特征属性 S_i，进而计算出各时间段的用户轮廓 T_i^2，形成正常行为轮廓库。在检测时，对于采集到的每一网络事件，把其属性值与已有的统计区间相比较，计算各元素对应的 Q 值，由 Q 值计算 S，再计算 T^2，把 T^2 与轮廓库中的 T^2 相比较，以确定该事件的性质。其问题在于其不能反映事件在时间顺序上的前后相关性，然而许多预示着入侵行为的系统异常都依赖于事件的发生顺序。

1.3.2.3 基于规则的模型

属于异常入侵检测模型。模型动态建立和维护一个规则库，如树形规则库以及基于时间的规则推理库等，利用规则对事件进行层层判别，与统计异常入侵检测类似。其区别在于：基于规则的入侵检测模型使用一系列的规则（rules）而不是统计出的系统度量（metrics）来表示系统的使用模式。

1.3.2.4 基于数据挖掘的模型

数据挖掘指从大量实体数据中抽取出模型的处理，这些模型经常在数据中发现对其他检测方式来说不是很明显的事实。计算机网络导致大量审计记录和网络连接记录，单独依靠手工方法去发现记录中的异常现象是不现实的，也不容易找出记录间的相互关系。利用数据挖掘技术，建立具有“if…then…”形式的分类规则模型，来检测异常行为和已知的入侵。其缺点在于局限于已知的入侵类型上，不能适应网络升级和未知入侵的有效检测需要。

1.3.2.5 基于代理的检测模型

基于代理的检测模型是在一个主机上执行某种安全监控功能的软件实体，由于代理的检测通常以自治的方式在目标主机上运行，因此本身只受操作系统的控制，不会受到其他进程的影响，这为系统提供了良好的扩展性和发展潜力。基于代理的入侵检测系统的灵活性保证它可以为保障系统

的安全提供混合式的架构，综合运用误用入侵检测和异常入侵检测，从而弥补两者各自的缺陷。

1.3.2.6 基于神经网络的模型

基于神经网络的模型通过自主学习算法来发现数据中隐藏的结构，包含两个阶段。第一阶段是构造入侵分析模型的检测器，通过对代表用户行为的历史数据集进行训练，完成网络的构建和组装；第二阶段则是入侵分析模型的实际运作阶段，网络接收输入的事件数据，与参考的历史行为相比较，判断出两者的偏离度。其优点是具备非参量化统计分析，即不使用固定的系统属性集来定义用户行为，属性的选择是不相关的，对所选择的系统度量不做预期统计分布的提前假定；其缺陷在于很难提取相关的入侵特征知识，无法满足安全管理需要。另外，模型训练时在很多情况下不能从训练数据中学习到特定的知识，系统趋向于形成某种不稳定的网络结构。

1.3.2.7 基于免疫原理的入侵检测模型

受入侵检测系统和生物免疫系统之间存在的可类比性的启发，借鉴生物免疫机制如“自我/非自我”（self/nonself）识别机制、抗体的耐受过程等进行入侵检测建模。1994 年新墨西哥大学的福莱斯特等率先提出了将生物免疫机制引入计算机系统的安全保护框架中，使用否定选择算法来检测受保护的数据和程序文件的变化，为研究入侵检测系统开辟了崭新的领域，国内外许多学者在这一领域进行了大量卓越的工作。1999 年霍夫迈尔等人将免疫的原理和思想推广到网络入侵中去，并进行了深入的理论分析和研究。其优点是系统能检测到未知的入侵行为，具备误用入侵检测和异常入侵检测的能力。其缺点是在很有限的程度上利用了免疫系统的免疫机制、体系结构及从中抽象提取的算法，通常只能保护静态的数据文件和软件，有待于提高到动态环境。

还有许多研究人员对入侵检测模型进行了大量的研究工作，提出并实现了其他一些入侵检测模型和原型系统，不同的建模方法会在不同的方面有所侧重，例如遗传算法模型、机器学习和模式识别模型、互信息和熵模型等，这里不再列举。

评价入侵检测模型的优劣一般从四个方面来考虑，即检测性能、适应

性、可扩展性以及健壮性。检测性能是指 IDS 具有高的检测率和低的误检率即有效性；适应性是指系统能够适应变化的入侵，又能够容忍自身的变化；可扩展性指系统易于融入新的检测模块或易于适应网络环境的变化；健壮性是指系统的部分检测组件发生故障或不起作用时，系统总体检测性能虽然会受到一定程度的影响，但不会导致系统整个崩溃或完全失去检测能力。总的来说，当前的入侵检测模型存在以下几个方面的问题。

（1）检测性能方面。自 1987 首次向研究界引入基于异常的入侵检测以来，该领域的发展迅速，检测攻击的各种方法和技术大量涌现，但由于入侵者总是想方设法掩盖其攻击的痕迹，并不断地采用各种方法逃避入侵检测系统的检测，如阻止审计记录的产生、篡改日志记录或伪装数据包、持续而缓慢的攻击等，使得入侵检测系统无法得到可靠的数据源。虽然学术界提出了各种异常入侵检测技术，在实验研究报告中取得了在低误报率为 1%、高检测率为 98%的成果，但在实际运行环境中性能远未达到人们的理想水平，这也是为什么基于异常的入侵检测方法仍不被工业界所采用的原因。而检测新型入侵的能力只能采用异常入侵检测的方法，异常入侵检测的计算代价非常大，检测效率低且引起过多的虚警。因此，提高入侵检测系统对新型攻击的检测率并降低虚警率是当前入侵检测系统面临的最重要的问题。

（2）适应性方面。基于误用入侵检测技术的 IDS 无法检测将来出现的新型的攻击，并且由于其学习方法的局限性，更新速度慢，因而往往难以适应目前层出不穷的新的攻击方式。基于异常入侵检测技术的 IDS 虽具备检测新型攻击的能力，但其保护的系统是动态变化的如增加新的用户、新的服务，即建立起的正常行为轮廓不是一成不变的，因此动态变化的网络环境以及层出不穷的攻击方式都对传统的静态的入侵检测系统构成严重的挑战。

（3）可扩展性方面。当前的入侵检测系统往往对检测环境进行预先假设，以至不能根据其应用环境进行灵活的配置。如基于神经网络等方法的检测模型，要么依赖于特定类型的操作系统，要么依赖于特定的网络结构。

（4）健壮性方面。当前的入侵检测系统通常对检测过程的集中控制程度较高或不同检测组件之间的依赖程度较大，导致其某个检测组件突然失