博士文库

云南民族大学
学术文库

基于支持向量机的入侵检测算法研究

谷 雨 著

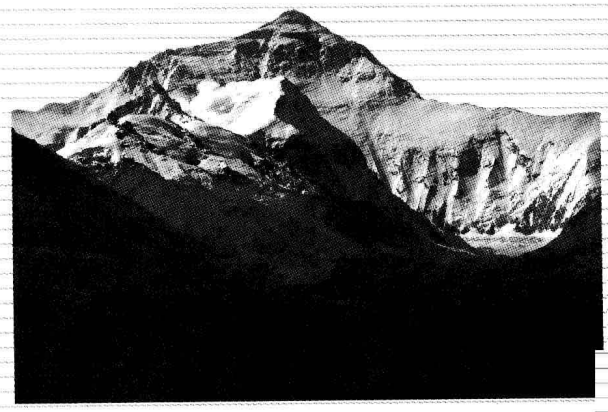
西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

博士文库

云南民族大学

基于支持向量机的入侵检测算法研究

谷 雨 著



西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

内容简介

本书系统地介绍了入侵检测系统的基本概念与检测技术，对入侵检测的核心技术——检测算法进行了深入、系统地研究。主要利用支持向量机在解决小样本、非线性及高维问题时所具有的良好性能，来对入侵行为进行高速检测。在此基础上，充分考虑入侵检测环境中的单点失效问题、多个检测器的协作问题，将集成学习、人工免疫等新兴技术引入到入侵检测环境中，从而提高检测精度和入侵检测系统的鲁棒性。

本书针对有计算机、信息科学、通信技术基础的中、高级读者，适合从事网络信息安全、人工智能、数据挖掘的研究人员，以及高校计算机、信息科学、通信等专业高年级本科生和研究生参考使用。

图书在版编目(CIP)数据

基于支持向量机的入侵检测算法研究/谷雨著. —西安：西安交通大学出版社，2011.8
ISBN 978-7-5605-3973-7

Ⅰ.①基… Ⅱ.①谷… Ⅲ.①计算机网络-安全技术 Ⅳ.①TP398.08

中国版本图书馆 CIP 数据核字(2011)第 143437 号

书　　名	基于支持向量机的入侵检测算法研究
著　　者	谷　雨
责任编辑	王　欣
出版发行	西安交通大学出版社 (西安市兴庆南路 10 号　邮政编码 710049)
网　　址	http://www.xjtupress.com
电　　话	(029)82668357　82667874(发行中心) (029)82668315　82669096(总编办)
传　　真	(029)82668280
印　　刷	西安明瑞印务有限公司
开　　本	787mm×1092mm　1/16　**印张**　10.75　**字数**　230 千字
版次印次	2011 年 8 月第 1 版　2011 年 8 月第 1 次印刷
书　　号	ISBN 978-7-5605-3973-7/TP·553
定　　价	25.00 元

读者购书、书店添货、如发现印装质量问题，请与本社发行中心联系、调换。
订购热线：(029)82665248　(029)82665249
投稿热线：(029)82664954
读者信箱：jdlgy@yahoo.cn

前　言

随着网络技术和网络规模的不断发展，信息安全已经成为全球性的重要问题之一。信息的安全性主要取决于3个方面：检测计算机设备的非授权使用情况、维护数据文件的完整性和防止计算机病毒扩散。而安全的核心问题是对于非法入侵的检测，即通过监视网络系统的运行状态，进而发现各种攻击企图、攻击行为或者攻击结果。

目前，针对网络系统的攻击越来越普遍，攻击手法日趋复杂，传统的入侵检测系统已经很难适应这种变化。现有的检测技术通常存在误报率高、自学习性和鲁棒性差等方面的不足，所以，如何能快速、准确、有效地识别已有的攻击和日益增多的新的攻击就成为入侵检测系统亟待解决的关键问题。

本书的内容主要集中于对入侵检测的核心技术——检测算法的研究，主要利用支持向量机在解决小样本、非线性及高维问题时所具有的良好性能，来对入侵行为进行高速检测。

支持向量机的相关研究是近年机器学习与人工智能、数据挖掘等研究方向的重要研究内容。它是由Vapnik等人在统计学习理论与结构风险极小化原理的基础上提出的一种学习算法。支持向量机根据有限的样本信息在模型的复杂性和学习能力之间寻求最佳折中，在很大程度上克服了传统机器学习（神经网络、决策树等）的维数灾难和局部极小等问题，从而获得了较好的泛化能力。近年来，在文本分类、目标识别、基因分析等生物信息领域的实际应用中，支持向量机都取得了极大成功。在入侵检测领域，支持向量机也表现出优异的成绩，关于支持向量机的研究方兴未艾。本书详细地介绍了统计学习理论、支持向量机、核函数的有关基础理论和算法，并对支持向量机的研究进展进行了讨论。

面对一个实际的问题，我们应如何应用支持向量机来解决呢？从通用的层面看，首先应把问题转化为能用支持向量机求解的数学模型。这一过程称为模型选择。对于任何一个学习问题，模型选择都是一个不可回避且非常困难的问题，它通常是指学习机的构建或拓扑结构的设定。支持向量机模型选择的问题主要有：①支持向量机类型的选择；②支持向量机中核函数和其他参数的选择。核函数技术是支持向量机强大非线性处理能力的关键因素，因此，支持向量机的核函数及参数选择是模型选择的研究重点。本书采用误差分解理论研究支持向量机的性能，讨论了支持向量机在不同核函数（高斯核、多项式核和点积核）下的误差分解特性，并

在入侵检测基准数据集上用可视化方法研究了支持向量机参数对学习性能的影响。我们的研究充分说明了支持向量机应用于入侵检测环境时存在的模型选择困难等问题。

另一方面，由于某些入侵活动靠单一检测器不能检测出来(如分布式攻击)，而且不同的检测器之间没有协作，结果造成缺少某种入侵模式而导致入侵检测系统不能发现新的入侵活动。因此，本书将集成学习引入到入侵检测环境中，通过多个支持向量机分别对入侵行为进行建模，然后把它们的结果综合起来，以达到协作检测的目的，从而提高了检测精度和检测系统的鲁棒性。

本书的主要工作包括：针对标准支持向量机算法对入侵行为的漏警率高的重大缺陷，提出一种新的、基于不同特征提取的入侵检测集成分类系统；针对入侵检测环境中新攻击行为层出不穷的现实，提出采用存活因子控制样本的存活周期数，对入侵检测问题实现增量式学习；针对入侵检测环境中漏警与误警损失的矛盾性问题，提出解决这一矛盾的多目标优化 Pareto 解方法；针对入侵检测数据的噪声冗余问题，提出一种新的基于支持向量机嵌入式特征选择方法，把特征选择问题嵌入到支持向量机学习过程中；针对支持向量机的核参数选择难题，提出基于负相关学习的支持向量机集成方法，无需精确选择核函数及其参数；针对入侵检测系统存在的单点失效问题，提出一种新的、基于免疫多样性的多检测器联合检测算法。

本书的编写过程得到了西安交通大学博士生导师徐宗本教授的支持与帮助。曹怀信教授、张建华教授、高飞教授对本书提出了有益的修改意见和建议，作者在此表示衷心的感谢。

本书的出版得到了云南民族大学学术著作出版基金、国家自然科学基金(60963026)、云南省高校无线传感器网络技术重点实验室基金的支持，在此表示感谢。

谨请读者不吝赐教，对本书的不足与错误之处批评指正。

作　者

2011 年 5 月

目　录

第 1 章　入侵检测基础

1.1　研究背景

随着计算机和网络技术的发展，计算机网络已成为社会生活不可或缺的一部分。电子商务、电子政务、虚拟社区等建立在 Internet 网络上的电子在线服务呈快速增长的趋势，人类社会对数字信息的依赖达到前所未有的程度，计算机网络成为现代社会经济运行的基础平台。

然而，人们在得益于信息社会提供的服务的同时，也不得不面对信息安全问题的严峻考验。2011 年 1 月 19 日，中国互联网络信息中心（CNNIC）在北京发布了《第 27 次中国互联网络发展状况统计报告》[1]。《报告》显示，截至 2010 年 12 月底，我国网民规模达到 4.57 亿，较 2009 年底增加 7330 万人。最引人注目的是，网络购物用户年增长 48.6%，是用户增长最快的应用，这预示着更多的经济活动步入互联网时代。而另一方面，2010 年，遇到过病毒或木马攻击的网民比例为45.8%；有过账号或密码被盗经历的网民占 21.8%。《报告》指出“网络安全形势严峻”。图 1-1 所示的计算机网络应急技术处理协调中心（CERT/CC）对 20 余年来安全事件的邮件信息处理的统计结果也清晰地说明了这一点。[2]

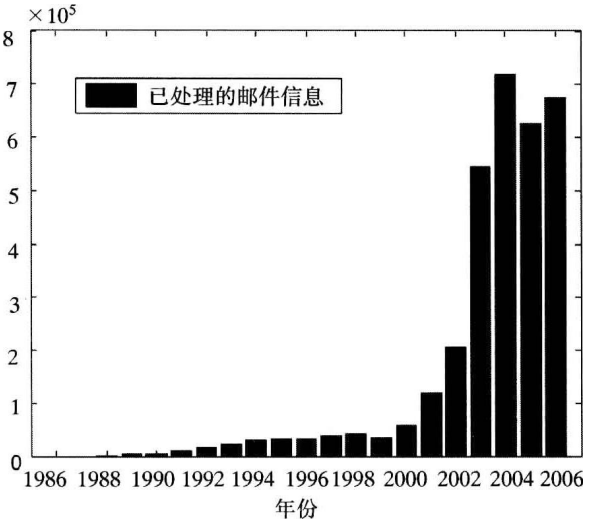


图 1-1　CERT/CC 安全事件处理报告统计①

在中国互联网络面临大发展的今天，业界人士已经形成了普遍的共识——中

①CERT/CC 安全事件处理报告统计数据仅提供到 2006 年

国互联网在基础设施的构建上已逐步走向成熟，加强信息安全是目前运营和维护网络生态环境的关键所在。因此，大力发展信息安全技术，使日益增加的计算机及网络犯罪受到应有的制裁，进一步保护国家的安全不受侵犯，保障国家的经济秩序不被破坏，保护网络用户的合法权益不受侵害，具有非常重要的现实意义。

1.2 计算机安全及关键技术

1.2.1 计算机安全概念

计算机安全是指为数据处理系统建立和采取的安全保护，它保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。[3]

安全的计算机系统应该具有以下几个特征：

①机密性(confidentiality)：使信息不泄露给非授权的个人、实体或进程，不为其所用；

②完整性(integrity)：防止系统内软件(程序)与数据被非法删改和破坏；

③可确认性(accountability)：对信息的访问、传播以及具体内容具有确认性和控制能力。同时还要求系统对信息的访问进行审计，当出现泄密现象时，计算机的安全系统必须能够借助所保存的足够多的信息来追踪和识别入侵攻击者。

④可用性(availability)：计算机资源和系统中的数据信息在系统合法用户需要使用时，须是可用的。

1.2.2 常见的安全威胁

随着电子商务等网上经济活动的蓬勃兴起，来自网络的各种各样的安全威胁也越来越多，这些威胁主要有以下几种。

1. 伪装用户身份

用户的个人信息被黑客获取，其伪装成身份合法的用户(或者黑客通过某种技术手段突破系统的身份验证机制)获取对系统的访问权，使合法用户受到损失，进而破坏系统的安全。

2. 篡改数据

黑客或者病毒对数据进行恶意篡改，破坏数据的完整性。在电子商务活动中，这种威胁将给用户带来巨大的损失。

3. 否认

接收数据的人或者是发送数据的人为了某种目的否认他们所做过的操作。在电子商务活动中必须采用不得否认技术作为解决争端的证据。不得否认服务一般

有两种形式：带有来源证据的不得否认，它可以用来对付发送者对数据或者内容已经发送的虚假否认；另一种形式是带有投递证据的不得否认，它可以用来对付收件人对已经接收到的数据或者内容进行的虚假否认。

4. 泄露内部信息

在使用互联网时，用户应要求将自己的身份证号、信用卡号等敏感信息存放在提供服务的 Web 站点上，这些信息应该以保密的方式存放在安全的位置，除了司法调查，不能泄露给任何人。但是，当这些信息在两台计算机之间传输时，有可能被窃听者捕获，从而被他人非法使用。

5. 拒绝服务

实施拒绝服务(DoS)时，合法用户将无法享受到应有的服务。例如，使用户暂时无法得到或者暂时无法使用系统，或者强制重新启动用户的计算机等。拒绝服务的威胁是用户和服务提供者很容易受到的威胁之一，特别是分布式拒绝服务(DDoS)攻击的出现，更使这种威胁不容易防范。

6. 提高优先权

攻击者通过特洛伊木马等手段，使不具备系统访问权限的用户得到对系统访问的优先访问权，因此具有足够的能力来削弱或者破坏整个系统。这种威胁的危险性在于：攻击者可以在系统管理员不知道的情况下使用他的优先权来控制整个系统，并发动其他种类的攻击，这使攻击者能够对系统造成极严重的破坏。

1.2.3 网络安全关键技术

为了保护网络信息不受损害，目前已经发展出众多网络安全关键技术[4]。这些技术主要有访问控制技术、数据加密技术、认证技术、漏洞扫描技术、防火墙技术、入侵检测技术等。

1. 访问控制技术

计算机访问控制技术产生于 20 世纪 60 年代，主要分为自主访问控制(Discretionary Access Control，DAC)和强制访问控制(Mandatory Access Control，MAC)。访问控制系统由主体、个体和安全访问策略组成。访问控制根据事先确定好的规则(安全访问策略)来决定主体对客体的访问是否合法，主要规定了哪些主体可以访问，以及访问的权限和类型。

自主访问控制最初出现于 20 世纪 70 年代的分时系统中，是目前最常用的访问控制技术。其核心思想是，允许某个主体控制其他主体对该主体所拥有的信息资源享有何种权限，以及可以执行的访问类型，具有灵活性和易用性等优点，缺点是资源管理分散、用户不易管理、信息容易泄露、无法抵御特洛伊木马等。

强制访问控制技术(MAC)出现于 Multics 系统中,是 TESEC 中 B 级安全系统主要评价指标之一。MAC 的基本思想是每个主体和客体都有既定的安全属性,客体对主体的访问由两者之间的安全属性关系决定。它的特点是信息的单向流动性,即信息只向高安全属性的方向流动,从而防止信息扩散,抵制特洛伊木马攻击。缺点是 MAC 针对具体应用开发,这使得其应用领域狭窄,通用性和灵活性差,对高安全级别信息的完整性控制不够完善。

2. 数据加密技术

加密(cryptography)技术是指明文经过密钥和加密函数转换成非法接入者无法理解的密文的过程。采用加密技术,信息以密文方式存储,使得即使因各种原因造成数据泄露,未授权者由于不能解读密文,从而保障计算机数据的安全。通常系统保密性不依赖于加密体制或算法的保密性,而只依赖于密钥。

根据密钥特点,加密算法可以分为两类:私钥密码体制和公钥密码体制。私钥密码体制(或称对称密码体制)的特点是加密密钥和解密密钥相同,代表算法是 DES;公钥密码体制(或称非对称密码体制)的特点是加密密钥和解密密钥不同,且很难从一个推导出另一个,代表算法是 RSA。对称密码体制的优点是计算速度快,缺点是密钥分配和管理复杂;而非对称密码体制的优点是密钥分配和管理简单,可以实现数字签名和密钥交换,缺点是算法复杂,运算效率低。

在实际应用中常采用私钥密码和公钥密码算法混合的方法,即私钥密码用来加密大量的明文,而公钥密码加密核心机密数据如私钥密码。

3. 认证技术

认证(authentication)技术是为防止入侵者对信息系统进行主动攻击,用交换信息的方式来识别实体身份的过程。一个安全的认证体制需要满足如下要求:

① 允许的接收者能检验和证实消息的合法性、真实性和完整性;

② 消息的发送者对所发送的消息不能抵赖,有时要求消息的接收者不能否认所收到的消息;

③ 除了合法的消息发送者外,其他人不能伪造发送消息。

认证可以分为身份认证和消息认证。身份认证的目的是验证信息收发是否持有合法的身份认证符(口令、密钥和实物证件等),可分为通行字方式和特征方式。消息认证是指通过对消息或消息相关信息进行加密或数字签名进行的认证,包括消息内容认证(消息完整性认证)、消息的源和宿认证(身份认证)及消息的序号和操作时间认证等。

在公钥密码体制基础上发展起来的公钥基础设施 PKI(Public Key Infrastructure)为互联网及相关网络应用提供了全面的安全服务,如安全认证、密钥管理、数据完整性检验和不可否认性保证等。

4. 漏洞扫描技术

漏洞扫描(vulnerability scanning)也称安全性评估或脆弱性分析,主要通过对整个网络范围扫描发现网络中存在的漏洞,及时给出修补方案,防止黑客利用该漏洞进行入侵活动。

漏洞扫描技术一般分为两类:主机漏洞和网络漏洞。主机漏洞主要是系统自身的安全配置缺陷,以及同安全规则相抵触的对象;而网络漏洞是通过执行一些入侵程序或脚本代码模拟对系统进行攻击的行为并记录系统反应从而发现其中的安全缺陷。主机漏洞检测技术一般有端口扫描技术和漏洞库匹配检测法;网络漏洞检测技术有插件技术。端口扫描技术是一项自动探测本地和远程系统端口开放情况的策略及方法,它使系统用户了解系统向外界提供了哪些服务;漏洞库匹配检测方法是在端口扫描后得知目标主机开启的端口以及端口上的网络服务,然后将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配,查看是否有满足匹配条件的漏洞存在;插件技术是通过黑客的攻击手法,对目标主机系统进行攻击性的安全漏洞扫描,若攻击成功,则系统存在漏洞。

5. 防火墙技术

防火墙(firewall)通过控制和检测网络之间的信息交换和访问行为来实现对网络安全的有效管理,遵循允许或禁止访问的网络通信安全机制。根据防范的方式和侧重点的不同,防火墙大致可分为三大类。

(1)数据包过滤

该技术在网络层对数据包进行选择,选择的依据是系统内设置的过滤逻辑,即访问控制表。通过检查数据流中每个 IP 数据包的源地址、目的地址、所用的端口号、协议状态,以及它们的组合来确定是否允许该数据包通过。这种防火墙通常安装在路由器上。

(2)应用级网关

应用级网关在网络的应用层上建立协议过滤和转发功能。针对特定的网络应用服务协议,它使用指定的数据过滤逻辑并在过滤的同时对数据包进行必要的分析、登记和统计,形成报告。应用级网关通常安装在专用的工作站系统上。

(3)代理(proxy)服务器

代理服务器也称链路级网关(或 TCP 通道)。它将所有跨越防火墙的网络通信链路分为两段,防火墙内外、计算机系统间的应用层的"链接"由两个终止于代理服务器上的"连接"来实现。外部计算机的网络链路只能到达代理服务器,从而起到了隔离防火墙内外计算机系统的作用。此外,代理服务器也对过往的数据包进行分析、注册登记,形成报告,一些代理服务器发现攻击迹象时会向网络管理员发出警报,并保留攻击痕迹。

防火墙作为网络安全的一种重要的防护手段得到了广泛的应用。然而，它仍然有一定的局限性：

①入侵者可以寻找防火墙背后可能敞开的后门而绕过防火墙；

②防火墙完全不能阻止内部攻击；

③由于性能的限制，防火墙通常不能提供实时的入侵检测能力；

④防火墙对于计算机病毒的防范能力不足；

⑤无法做到安全与速度的同步提高；

⑥防火墙无法有效解决自身的安全问题；

⑦防火墙是一种静态安全技术，需要人工来实施和维护，不能主动跟踪入侵者。

因此，仅在 Internet 入口设置防火墙系统不能实现系统足够安全的目标，必须采取其他安全保护措施来配合防火墙系统以共同实现信息网络的安全。

6. 入侵检测技术

入侵检测(Intrusion Detection，简称 ID)是用于检测任何损害或企图损害系统的保密性、完整性或可用性行为的一种网络安全技术。它以对网络系统的实时监测和快速响应的特性，逐渐发展成为保障网络系统安全的关键部件。它通过监视受保护系统的状态和活动，采用误用检测或异常检测的方式，发现非授权的或恶意的系统及网络行为，为防范入侵行为提供有效的手段[3,5]。

一个入侵检测系统(Intrusion Detection System，IDS)的作用如图 1-2 所示。在网络安全体系中，入侵检测系统是唯一一个通过数据和行为模式判断其是否有效的系统[6]。防火墙可以阻断某些攻击，但不能阻断“伪装”攻击，对内部攻击更是无能为力；访问控制系统可以防止越权的操作，但不能保证获取高权限的人做破坏工作，也无法阻止较低权限的人非法获取高级权限；而漏洞扫描系统可以发现系统和网络存在的漏洞，但无法对系统进行实时扫描。

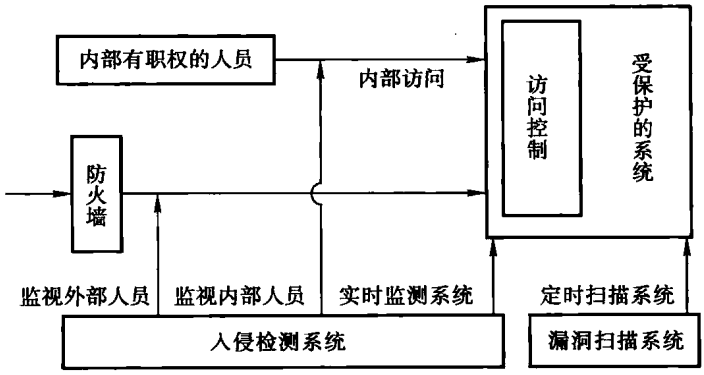


图 1-2　入侵检测的作用

入侵检测作为一种新型的信息系统安全机制，通过监控系统的使用情况来检测系统的用户越权使用以及系统外部的入侵者利用系统的安全缺陷对系统进行入侵的企图。如果系统遭到攻击，IDS 可以尽可能地检测到，甚至是实时地检测到，然后采取恰当的补救措施，以减少攻击所生成的影响和防止攻击的再度发生。IDS 所起到的作用是安全触发器的作用，通过实时地检测入侵事件，就可以及时阻止事件的发生和事态的扩大。

1.3 入侵检测技术研究概述

1.3.1 入侵检测发展历程

自 20 世纪 80 年代以来，入侵检测经过二十多年的不断发展，从最初一种有价值的研究想法和单纯的理论模型，迅速发展出种类繁多的各种实际原型系统，并且在十年内涌现出许多商用入侵检测系统产品，成为计算机安全防护领域不可缺少的重要的安全防护技术[7,8]。

入侵检测的整个发展过程中有几个重要的里程碑。

1980 年，Anderson 第一次详细阐述了入侵检测的概念[9]，给出了对计算机系统风险和威胁的分类方法，并建议利用审计跟踪数据来监视入侵活动，成为入侵检测系统设计和开发的基础。1983 年出版的《可信计算机评估准则》(即黄皮书)，为计算机安全控制提供了一系列有效的评估准则。

1984—1986 年，乔治敦大学的 Denning 和 Neumann 研究出了一个实时入侵检测系统模型，IDES[10]。IDES 系统具有如下特点：根据用户的历史行为档案来判断审计记录中的用户行为是否正常；根据设定的周期持续地更新用户行为档案；当异常发生时发出警报。这个模型提供了访问控制所不能发现的入侵检测和安全事件的告警功能。IDES 中的专家系统通过基于规则和统计的模型来识别入侵。

1987 年，Denning 发表了经典论文《An Intrusion Detection Model》[11]，文中提出入侵检测的基本模型，并提出了几种用于入侵检测的统计分析模型。Denning 的论文正式启动了入侵检测领域内的研究工作。

1988 年加利福尼亚大学的 Smaha 设计了 Haystack 系统来辅助空军安全部门进行空军基地主架构的误用检测[12]。Haystack 同时采用了两种不同的统计分析检测技术(基于模式分析和基于统计分析)来发现异常的用户活动。早期的原型系统采用批处理的离线处理方式。

Sebring 等开发了 MIDAS (Multics Intrusion Detection and Alerting System)[13]。MIDAS 基于启发式入侵检测的思想，作者以人类安全专家对审计记录进行分析来发现入侵行为得到样本，进行用户轮廓统计。

1989 年美国安全系统研究所的 Lunt 等人重新定义了 Denning 提出的入侵检测术语并设计和构造了 IDES 原型系统[14]。该系统可以检测出在行为上逐步变化的入侵企图，并使误警率最小化。

1990 年 UC Davis 大学的 Heberlein 等人提出了网络入侵检测器 NID (Network Intrusion Detector)[15]，标志着入侵检测第一次将网络数据包作为实际输入的数据源。NID 通过主动监测局域网内的网络流量检测可疑行为取代了对于主机系统的审计追踪，它通过截获网络数据包来监控异构网络环境下的入侵活动，把入侵检测系统扩展到异构网络环境中。

1991 年 Jackson 等人设计了网络入侵检测和入侵告警系统 NADIR(Network Anomaly Detection and Intrusion Reporter)[16]，通过从多个主机收集审计数据并进行汇总来抵抗对一系列主机的联合攻击。该系统基于下述三个假设：第一，对计算机系统和用户行为的统计分析可以用来刻画正常的系统行为和用户行为，因此在统计分析下可以识别异常行为；第二，专家系统技术可以用于用户安全审计和入侵检测中；第三，通过监控有限的网络活动可以检测到入侵的发生。NADIR 把原来由安全人员手工评价审计日志改为由实时专家系统自动完成，大大提高了入侵检测效率。

同年，分布式入侵检测系统 DIDS(Distributed Intrusion Detection System)被提出[17]。DIDS 首次将主机入侵检测和网络入侵检测技术进行了集成，它通过目标环境的扩展来监测来自网络的多主机攻击。其组成部件包括一个 DIDS 检测器和在每个监控网段上配置的单独的网络监控器。这些分布式组件收集信息并发送到中央机进行分析，从而具有了汇总能力。

1992 年，Ilgum 等人提出了状态转移分析的入侵检测技术[18]，并实现了原型系统 USTAT(State Transition Analysis Tool for UNIX)。该系统将攻击表示成一系列被监控的系统状态转移。攻击模式的状态对应于系统状态，并具有迁移到另外状态的触发条件，允许把事件类型植入到模型中。

1994 年 Anderson 对 IDES 进行了改进，提出了 NIDES(Next-generation Intrusion Detection Expert system)[19]。NIDES 系统是一个高度模块化的、界面良好的入侵检测系统，它建立在一个客户-服务器结构之上。它通过在自己的工作主机上对目标主机上的用户活动进行实时监测，从中检测出异常和可疑行为。NIDES 采用两种不同的入侵检测机制：一种是基于规则的检测分析子系统，另一种是基于统计方法的检测子系统。

1995 年 Crosbie 和 Spafford 提出了自治代理的概念[20,21]。其基本思想是利用分布的独立模块完成对入侵检测的数据采集和数据分析，通过所有模块的相互协作，实现对整个系统的整体监控。这种方法在系统开销、可伸缩性、故障承受能力和机动性方面，都表现出了明显的优势。

1996 年 Cheung 指出了当前入侵检测系统在可伸缩性方面的局限性，设计了 GrIDS。该系统便于监测大规模的自动或联合攻击，甚至可以跨越多个管理域。GrIDS 把被保护的组织和网络进行层次性分解，把关于网络通信和异常事件的报告组织成图，逐级汇总并向上传递。GrIDS 各组件之间通信采用消息收发模型，并将网络组织成树状层次结构，由分布在不同主机上的模块控制器在软件控制器的协调下以分布式的方式运行。GrIDS 提出的一些概念和设计思路对入侵检测技术的发展起到了重要的启发作用。

1998 年 Balasubramaniyan 等人提出了基于自治代理技术的入侵检测体系结构 AAFID(Autonomous Agents For Intrusion Detection)[22]。该结构是一个由代理(Agents)、过滤器(Filters)、收发器(Transceivers)、监控器(Monitors)和用户界面(User interfaces)组成的分层体系。其基本思想是由被称为自治代理的实体负责分布式数据的收集和分析任务，集中分析任务则由基于所有主机和网段的更高级的被称为收发器和监视器的实体来完成。该结构可以有效克服以往体系结构中单点处理所带来的通讯开销和计算开销。

2004 年悉尼科技大学的 Li 等提出了基于移动代理技术的分布入侵检测体系结构 MA - IDS[23]，MA - IDS 利用移动代理 MA(Mobile Agents)技术对来自每个监视主机的信息进行协同处理，然后完成入侵行为的全局信息抽取任务，并设计了原型系统。该系统的主要优点是：

①即使一些代理失效系统仍可正常运行；

②通过数据收集和协同检测来发现分布式入侵攻击。

2007 年 Bolzoni 等人提出了用于网络入侵检测系统报警确认的体系结构 ATLANTIDEs[24]，目的是降低误警率。该系统采用了基于异常的自动分析技术来分析系统的输出，为相关服务提供了可用的上下文信息。通过把进入网络的流量与输出的异常信息相结合来降低误警率。实验结果表明误警率可以降低 50% ～ 100%。同年德国柏林工业大学的 Luther 等人提出了用于入侵检测的协同人工免疫系统 AIS(Artificial Immune System)架构[25]，使用生物免疫系统规则和 P2P 通讯技术来设计分布式异常入侵检测系统。应用人工免疫 AIS 代理可以获得较低的误警率，而使用 P2P 技术可以有效避免单点失效问题并提高系统的健壮性。

1.3.2 通用入侵检测模型

入侵检测系统专用于对付网络攻击，扩展系统管理员的安全管理能力，维护计算机系统的完整性、机密性和可用性。它从计算机网络中的若干个关键点收集信息并分析，在不影响性能的情况下检测网络，从而提供对内部攻击、外部攻击和误操作的实时保护。