基于免疫 Agent 的网络入侵检测系统*)

李永忠　徐　静　罗军生　孙　彦
(江苏科技大学电子信息学院　镇江 212003)

摘　要　结合计算机免疫学原理和多 Agent 技术构建了一个网络化、分布式、智能化的入侵检测系统，该系统融合了两者的优势，同时继承了多 Agent 系统和免疫系统的优点。其特点是能同时进行多层次的监测和不同级别的响应。系统是完全分布式结构，监视 Agent 生成后在网络上漫游，各个 Agent 分布在网络的各个结点上，单个结点受到攻击不会影响其他结点的检测能力，避免了单点失效问题。将疫苗概念引入系统，使得各个 Agent 可以实现互相学习，增强了整个网络的耐受性、"记忆"机制及新抗体生成机制的能力，提高了系统的适应性，不仅能检测到已知的攻击，而且还能检测到未知的攻击。

关键词　入侵检测系统，免疫学原理，免疫 Agent，多 Agent

Intrusion Detection System Based on Immune Agent

LI Yong-zhong　XU Jing　LUO Jun-sheng　SUN Yan
(School of Electrics and Information, Jiangsu University of Science and Technology, Zhenjiang 212003, China)

Abstract　A new intrusion detection system (IDS) based on immune agent was presented. It combines multi-agent technology with immune principles, a concept of immune agent was also presented. Compared with the traditional system, this system is flexible, distributed, intelligent and so on. In this system, scout agents, which are based on immunity, roam around the nodes, and monitor the situation in the network at different levels, including the user level, system level, process level and packet level. These scout agents can learn and adapt to the environment dynamically. This system model possesses characteristics such as distribution, robustness, intelligent nature and adaptability etc, the adaptability and other characteristics network security system are increased. This system not only detects the given intrusions, but also the unknown intrusions.

Keywords　Intrusion detection system (IDS), Immune principles, Immune agent, Multi-agent

1　引言

入侵检测技术是一种利用入侵留下的痕迹来有效地发现来自外部或内部的非法入侵的技术。入侵检测为系统提供了实时保护，被认为是防火墙之后的第二道安全闸门。传统的入侵检测系统处理方式比较单一，维护过于复杂。虽经过不断发展，但是有些不足之处，其本身很难克服。主要缺陷：①扩展性差；②漏报警和误报警率较高；③ IDS 自身易受到攻击；④手工操作居多，维护较复杂[1-3]。另外，现有的网络入侵检测系统一般采用模式匹配或统计分析等技术，其致命缺点是智能水平较低，表现为自学习水平弱，不能识别未知入侵模式。

随着网络技术的发展，新的网络入侵方法层出不穷，因此不能简单地以传统的分析已有入侵的手段来解决网络入侵检测的问题，而是要让入侵检测系统具有自我学习和智能判断能力。入侵检测技术将朝着分布式入侵检测、智能化入侵检测、全面的安全防御方案等方向发展。

代理(Agent)技术起源于人工智能，是软件应用里的一个新领域。Agent 具有自治性、反应性、社会性和移动性等特性[1,4,5]，它们之间可以互相通信，互相协作来共同完成任务。应用 Agent 技术的 IDS 具有以下良好特性：网络负载小，网络延时短；自治、异步地运行；能动态适应网络变化，可扩展性好，能在异构环境下运行[4-7]。

在抵御外界物质入侵方面，生物免疫系统给了人们极好的启示。神经网络算法、遗传算法、免疫算法是基于生物系统的 3 大人工模拟算法，是近年来人工智能技术的重要研究方向[8,9]。New Mexico 大学的研究人员在对生物免疫系统和计算机系统的保护机制进行研究的基础上，发现它们之间的某种相似性，提出了基于人工免疫原理的入侵检测技术[9-14]。免疫系统最重要的功能是免疫识别，识别的本质是区分"自我/非自我"，即识别哪些组织是属于正常机体的(即自我)，不属于正常的就认为是异常(即非自我)，这与入侵检测中的异常检测的概念极其相似。免疫系统中抗体的产生又具有多样性以及记忆性的特点，将抗体产生的这种观念引入到计算机系统中为实现系统的耐受性和学习能力提供了可能。

如果把免疫机理与 Agent 技术融合在一起，就可以构造出一个具有免疫特征的 Agent 单元即免疫 Agent。Agent 是一种智能化的自治实体，具有分布性和独立性的特点。人工免疫系统也具有自学习和记忆能力，免疫细胞也具备分布式和独立性的特点[9-12]，将免疫原理应用于基于 Agent 的入侵检测系统中，可以提高入侵检测系统的自我学习能力和智能判断能力。目前国际国内对计算机免疫和 Multi-agent 技术

*)基金项目：江苏省教育厅/江苏科技大学基金(2005DX006J)。李永忠　教授，硕士生导师，主要研究方向为计算机网络与信息安全、计算机网络通信等；徐　静、罗军生、孙　彦　硕士研究生。

相结合的学术研究才刚刚起步，还不成熟。本文结合计算机免疫学(Computer Immunology)原理和多 Agent 技术构建了一个网络化、分布式、智能化的入侵检测系统——基于免疫 Agent 的分布式网络入侵检测系统。

2 Agent 技术与网络入侵检测模型

Agent 技术起源于人工智能，是软件应用里的一个新领域。Agent 可以被定义为在特定环境下自治和连续运行的软件实体，它以灵活和智能的方式运作，可以对环境的变化作出反应，并能从经验中学习[1-7]。Agent 能够在特定的环境下，无需人的干预或监督完成任务，又能和其它 Agent 协作共同完成任务而且还能接受控制，通过感应环境的变化来影响环境。Agent 具有以下基本特征：自治性、主动性、推理性、反应性、协作性、社会性、智能性。单个的 Agent 对问题的解决能力有限，这就导致了 Multi-agent 系统(MAS)的出现。MAS 在使单个 Agent 保持独立完成某一问题的求解能力的同时，还使多个 Agent 相互协助以完成更复杂的问题求解。由于 Agent 的特性，基于 Agent 的系统应是一个集灵活性、智能性、可扩展性、鲁棒性、组织性等诸多优点于一身的高级系统。Agent 技术的这些优异的特性特别适合于构造分布式入侵检测系统。应用 Agent 技术的 IDS 具有以下良好特性：网络负载小，网络延时短；自治、异步地运行；能动态适应网络变化，可扩展性好；能在异构环境下运行。

目前，国外基于 Agent 的 IDS 研究已经取得一定的成果[1-3]，由 Purdue 大学提出并实现的入侵检测自治代理(Autonomous Agents For Intrusion Detection，AAFID)是一个层次结构的基于 Agent 的 IDS。AAFID 的最下层由 Agent 组成，执行特定的检测任务，并向转发器汇报检测结果；转发器监控 Agent 的运行，对 Agent 汇报的数据进行分析，并将结果汇报给监视器；监视器监控转发器的运行，对转发器汇报的数据进行综合。由 SRI 提出的 EMERALD 是另一个基于 Agent 的 IDS，主要面向大型的、松散的企业网络，EMERALD 充分体现了“分而治之”的思想。日本安全机构 IPA 提出的 IDA(Intrusion Detection Agent System)的最大特点是利用 Mobile Agent 实现了入侵追踪。IDA 是一种层次结构的多主机 IDS，它由一个管理器、多个传感器、布告板和信息板(用于 Agent 之间的通信)、追踪 Agent 和信息收集 Agent 等组成。IDA 自定义一种可疑入侵者踪迹(Marks Left by Suspected Intruder，MLSI)来检测入侵。美国 Columbia 大学提出的 JAM(Java Agent for Meta-learning)系统利用移动代理(MA)技术，将分布式数据挖掘和后向学习(Meta-learning)技术应用到入侵检测中。美国 Iowa 州立大学发展的 MAIDS 系统(Mobile Agents Intrusion Detection)是基于 MA 的分布式入侵检测系统。MAIDS 先采用软件故障树分析(Soft Fault Tree Analysis，SFTA)对一个入侵建模，再使用有色 Petri 网(Colored Petri Net，CPN)将 SFT 模型转化成入侵检测建模，接着用 MA 技术来实现一个 CPN，包括一个从静态 Agent 到移动 Agent 的转化过程。MAIDS 可以对一个入侵的检测建立精确的模型，对分布式入侵的检测有独到的能力，如在 MAIDS 的实验中成功检测了涉及多个主机的 FTP 反弹攻击。缺点是只能检测到已知模式的入侵，且建模的过程非常繁杂。

与传统的 IDS 体系结构相比，基于 Agent/Mobile Agent 的 IDS 具有下列优点：

(1)独立性：IDS 组件之间有一定的配置独立性，即一个组件的配置变化对其它组件产生的影响较小；IDS 组件的开发也体现出一定的独立性，当要对一种新的数据源进行检测时，可以独立开发针对此数据源的组件，完成后将其加入原系统。

(2) 可扩展性好：能以较小的代价增添 IDS 组件以适应应用环境的新变化。

(3) 协作性：IDS 组件之间可以相互协作，完成一些复杂的检测任务。

(4) 数据来源不受限制，便于监控多种数据源，适于构建大型的 IDS。

3 免疫学原理

New Mexico 大学的研究人员在对生物免疫系统和计算机系统的保护机制进行研究的基础上，发现它们之间的某种相似性，提出了基于人工免疫原理的入侵检测技术[9-12]。免疫系统最重要的功能是免疫识别，识别的本质是区分“自我/非自我”，即识别哪些组织是属于正常机体的(即自我)，不属于正常的就认为是异常(即非自我)，这与入侵检测中的异常检测的概念极其相似。免疫系统中抗体的产生又具有多样性以及记忆性的特点，将抗体产生的这种观念引入到计算机系统中为实现系统的耐受性和学习能力提供了可能，将生物免疫的原理运用到入侵检测中能降低误检率[10-16]。

免疫系统与 MAS 的共性：它们都由许多自治的实体构成，免疫细胞及 Agent 都具有自治性。

(1) 都具有学习能力。如免疫系统的免疫调节和记忆，MAS 的学习算法。

(2) 都有自适应性。能够根据环境的变化来调节自己的能力。

(3) 系统中的实体都具协作性和社会性。

MAS 和免疫系统有着诸多共性，可以用免疫的一些机制来改进 MAS 的一些学习和决策过程，使 MAS 具有两者的优势。

4 基于免疫 Agent 的分布式网络入侵检测模型

免疫系统从整体上看是分布式多智能体的协调自治系统，免疫细胞又具有防御、监视、维持自稳定的特点。免疫学原理和 Multi-Agent 技术虽然是两种不同的技术，但两者都是分布式系统，有多个自主实体，能进行自我学习，感知外界环境的变化并能做出相应的反应。因此，本文将免疫学原理和 Multi-Agent 技术结合构建了一个分布式、智能化的免疫 Agent 入侵检测系统。

4.1 免疫 Agent

把免疫机理与 Agent 技术融合在一起，就可以构造出一个具有免疫特征的 Agent 单元即免疫 Agent(Immune Agent)。免疫 Agent 一般都是动态 Agent，相当于生物系统中的免疫细胞。这种免疫 Agent 有不同的类型，执行不同种类的检测任务，相当于生物系统中针对不同种类抗原的不同抗体。所有这些免疫 Agent 分布于网络的各个节点上，实时地监控网络安全情况。免疫 Agent 除了一般 Agent 的共性外还具有进化性、防御性、记忆性、耐受性等特点。

免疫 Agent 是分布式网络入侵检测模型系统中最重要、最核心的部分[16-20]。其结构如图 1 所示，免疫 Agent 由抗原模式检测器、分析中心、学习记忆中心和抗原处理器 4 个主要

部分组成。其中，分析中心和学习记忆中心是免疫 Agent 的核心部分。免疫 Agent 的抗原模式检测器，用以感知异常情况(即抗原)的存在并识别其变化趋势。作为 IA 核心部件的分析中心主要由抗原信息编码器、计算中心和控制器构成。抗原信息编码器对抗原数据进行过滤精简，处理后的编码为计算中心需要的编码格式。控制器负责控制协调计算中心和抗体中心的工作。计算中心完成免疫 Agent 工作过程中的重要的计算功能，主要是负责抗体选择以及亲和力的计算。计算中心还具有一些负责暂时储存抗体的记忆单元，称为记忆细胞。IA 的学习记忆中心主要由抗体中心、学习记忆器、疫苗生成器构成。抗体中心储存管理各种抗体集和包含产生多种新抗体的抗体生成器；学习记忆器对疫苗进行学习记忆，并将学习到的抗体存储到抗体中心；疫苗生成器负责将新产生的抗体转化为疫苗形式。抗原处理单元则负责对抗原的最后处理。

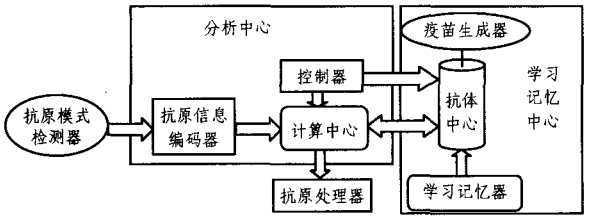

图 1　免疫 Agent 的基本结构

4.2　免疫 Multi-Agent 入侵检测模型

免疫 multi-Agent 入侵检测系统采用类似 MAIDS 的层次结构，如图 2 所示。检测模型中的监视层 Agent、通信层 Agent、决策层 Agent 和行动/防御层 Agent 采用免疫 Agent 结构，分别完成入侵检测、决策、防御和控制等任务。图中监视层的免疫 Agent 分为成熟细胞检测 Agent 和记忆细胞检测 Agent，负责在用户、系统、进程和网络等 4 个层次对系统进行动态免疫监视，若发现异常行为，则通过层 Agent 向决策 Agent 报警；决策 Agent 负责处理报警信息和接收疫苗，防御/行动 Agent 依据决策 Agent 的决策信息采取相应的防御行动措施，例如在网络层采取断掉网络连接，改变防火墙规则，在进程层杀死可疑进程等；控制 Agent 负责刺激应答，更新自体集，管理和控制 Agents 以及提供用户界面等任务。

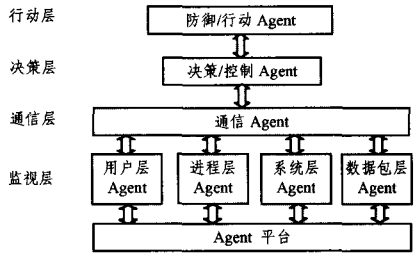

图 2　免疫 Agent 的网络入侵检测框架

4.3　工作原理

(1)免疫 Agent 工作原理：免疫 Agent 作为入侵检测的基本组件分布于网络各节点，模拟免疫细胞执行入侵检测任务，其实现机制如图 3 所示。免疫 Agent 是建立在体细胞理论和免疫网络理论的基础之上的。算法过程如下：①系统从候选抗体库中随机抽取一组基因，通过交叉、变异产生新生免疫代理，为了防止因自免疫而产生虚警，即将正常的网络行为误报为异常，因此需要将其与特征提取过程所产生的自身行为或网络特征进行比较，所有匹配自身特征模式的免疫代理必须丢弃，这就是模拟生物免疫的负选择过程。经过负选择过程后的成熟免疫代理被分发到各检测主机上，根据各自规则自主识别异常数据完成实时的检测任务。②一个新的免疫 Agent 如果匹配到某种网络异常，便发生应答，及时切断这些异常数据包的网络连接，并保存异常特征(基因)到候选规则库以供其它检测子共享。它自身也成为一个记忆免疫 Agent，通过与同类型免疫 Agent 比较亲和度来竞争扩增机率，亲和度越大，则复制机率越大，进而又会增加其亲和度，形成正向激励。记忆免疫代 Agent 过扩增复制自身到其它节点使其具有快速检测能力。③为了降低网络负荷，免疫 Agent 必须根据检测异常数据的能力(抗原结合亲和度)及有效时间(生命周期)决定何时注销。通过模拟生物界优胜劣汰机制可以实现候选基因库的进化，提高系统性能，由于只需保存有限基因从而降低了系统负荷。通过设置合适的基因库容量和生存期可以保证那些低亲和度和未达到激活阈值的免疫 Agent 也有足够的进化时间。

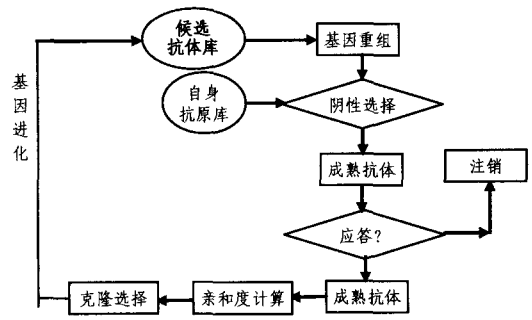

图 3　免疫 Agent 工作流程

(2) 监视层 Agent：监视层 Agent 在网络节点之间巡逻，并与特定意图的设备通信。监视 Agent 同时监视不同层次上的多个参数。例如，在用户层寻找异常用户行为模式；在系统层统计系统资源的使用情况，如 CPU、存储器和 I/ O；在进程层检查无效或者非授权的进程和优先级违例；在数据包层监视数据包的数目、大小以及连接的类型、源地址与目的地址等。入侵检测系统中存在多个不同的监视 Agent，其中一些免疫 Agent 利用负选择算法监视系统的异常变化；而其他 Agent 则监测已知入侵的出现。监视层 Agent 的算法如图 4 所示[18-20]。

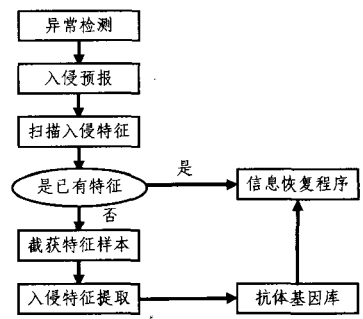

图 4　监视 Agent 的检测算法流程图

由于监视层 Agent 相当于机体中的免疫细胞，而免疫细胞具有免疫耐受机制，免疫耐受是机体对抗原刺激表现为“免疫不应答”的现象，因此 IDS 中的监视 Agent 也要具有这种机制，使它能识别“自我”，即正常的网络行为，而不至于对正常的行为产生破坏。免疫 Agent 的生成过程如下：首先，建立

一个原始抗体基因库，将各种对网络安全有威胁的因素放入基因库中，如 IP 地址、服务端口、协议类型等。然后，从基因库中随机产生一些抗体，对这些未成熟的抗体作免疫耐受训练和筛选，将与网络行为相吻合的成熟抗体筛选出来，这些成熟的抗体就是免疫 Agent，可以发布到网上实施监测工作。

(3) 通信层 Agent：通信层 Agent 充当其他 Agent 通信联络的消息邮递员。它们相当于自然免疫系统中 T 细胞分泌的淋巴激活素，用于激活 B 细胞的抗体。多 Agent 之间通信、协调和协作的实现可仿照计算机通信的方法建立多 Agent 通信协调层次模型。本系统多 Agent 的通信和协调分为 3 个层次，如图 5 所示。

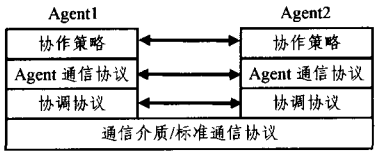

图 5　Agent 通信结构示意图

(4) 决策/控制 Agent：决策 Agent 进行决策，确定需要激活的其他 Agent 或者根据系统安全策略执行特定的任务。控制 Agent 负责刺激应答、更新自体集、管理和控制 Agents 提供用户界面等任务。

(5) 防御/行动 Agent：根据入侵的特性与强度激活一个适当的反应 Agent 集合，包括助手 Agent 、杀手 Agent 和抑制 Agent 。助手 Agent 用户报告环境状态或者显示决策报表。如在目标网络行为出现偏离或者违例时，助手 Agent 可以通过 e-mail ，pager 等方式向安全主管发出警告，报告入侵事件。同时，助手 Agent 实现一个 CUI 的报警接口，用于显示入侵活动的强度。杀手 Agent 是在出现真实入侵与恶意活动时采取猛烈的反应措施。例如，在系统层杀手 Agent 可以关闭一台主机或者断开某个节点；在进程层 kill 一个进程；在用户层杀手 Agent 可以停止用户会话，关闭用户帐号；在网络层，如果数据包包括一个可疑会话，杀手 Agent 可以丢弃一个数据包流。在面临真实危险时，杀手 Agent 可以经过通信 Agent 由多个 Agent 共同激活。抑制 Agent 干扰其他决策 Agent 采取更进一步的行动。抑制 Agent 能够在入侵检测/反应过程的后期，防止系统对假阳性错误采取其他行动。

正常工作时，监视 Agent 都在网络中漫游，监视网络状态。如果网络某个部分出现异常情况，并被监视 Agent 发现，它试图理解所发生的事件，并作出相应的决策。在有些场合下，Agent 作出决策时要咨询周围的其他 Agent，这相当于免疫反应中协同刺激的第二信号。作出决策之后，由通信 Agent 通知行动/决策 Agent，采取特定的行动。

结束语　本文结合计算机免疫学原理和多 Agent 技术构建了一个网络化、分布式、智能化的入侵检测系统，该系统融合了两者的优势，同时继承了多 Agent 系统和免疫系统的优点，具有以下特点：它能同时进行多层次的监测和不同级别的响应。系统是完全分布式的，监视 Agent 生成后在网络上漫游，各个 Agent 分布在网络的各个结点上，单个结点受到攻击不会影响其他结点的检测能力，因此一个节点被攻破不会导致整个系统丧失检测功能，从而提高了系统的健壮性，避免了单点失效问题；将疫苗概念引入系统，使得各个 Agent 可以实现互相学习，增强了整个网络的耐受性、“记忆”机制及新抗体生成机制的能力，提高了系统的适应性，不仅能检测到已知的攻击，而且还能检测到未知的攻击。

参 考 文 献

[1] 李永忠，罗军生，孙彦. 基于移动 Agent 的智能化入侵检测系统结构研究[J]. 计算机研究与发展，2006，43：296-301

[2] 李永忠，孙彦，徐静，等. 一种新的免疫克隆选择算法[J]. 江南大学学报：自然科学，2007，6：4-8

[3] 李永忠，孙彦，罗军生. WINEPI 挖掘算法在入侵检测中的应用[J]. 计算机工程，2006，32(23)：159-161

[4] (英)Wooldridge M. An Introduction to Multi Agent System[M]. 石纯一，等译. 北京：电子工业出版社，2003

[5] (加)Liu Jiming. Autonomous Agents and Multi-agent Systems [M]. 靳小龙，等译. 北京：清华大学出版社，2003

[6] 张仕山，庄镇泉，狄晓龙. 一种基于移动智能体的网络安全模型系统[J]. 计算机与应用，2003，17(14)：153-156

[7] Fenet S , Hassas S . A distributed intrusion detection and response system based on mobile autonomous agents using social insects communication paradigm[C]// Proc. Fifth International Conference on Autonomous Agents (Agents 2001). Montreal, Canada, May 2001

[8] 孙剑，许家珀. 神经网络算法在智能体 IDS 系统中的应用[J]. 电子科技大学学报，2004，33(3)：289-292

[9] 莫宏伟. 人工免疫系统原理与应用[M]. 哈尔滨：哈尔滨工业大学出版社，2003

[10] 李涛. Computer Immunology [M]. 北京：电子工业出版社，2004

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

[12] Dasgupta D . Immunity Based Intrusion Detection Systems : A General Framework[C]// The Proceedings of the 22nd National Information Systems Security Conference (NISSC). October 1999

[13] Anchor K P, Williams P D, et al. The computer defense immune system: current and future research in intrusion detection[C]// Proceedings of the 2002 Congresson Evolutionary Computation. vol. 2, May 2002: 1027-1032

[14] Bentley K J. Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Dynamic Clonal Selection [C] // The Proceeding of the Congress on Evolutionary Computation. Honolulu, USA, 2002: 1015-1020

[15] Lau H Y K, Wong V W K. Immunologic Responses Manipulation of AIS Agents[C]// Proceedings of the third International Conference on Artificial Immune Systems (ICARIS 2004). Lecture Notes in Computer Science. Catania, Sicily, Italy, Sep. 2004: 65-79

[16] 焦李成，杜海峰. 人工免疫系统进展与展望[J]. 电子学报，2003，31(10)：1540-1548

[17] 肖毅，胡伟雄，肖明，等. 基于免疫的入侵检测系统研究[J]. 计算机工程，2006，32(20)：2797-2799

[18] 朱浩，周莲英，陈东彬. 基于免疫 Agent 的入侵检测系统模型的研究[J]. 计算机应用与软件，2005，22(3)：34-36

[19] 邓贵仕，刘金峰. 基于免疫原理的网络入侵检测系统的研究[J]. 计算机应用研究，2004，(9)：139-141

[20] 吴知，许家珀. 免疫原理在多 Agent 入侵检测系统中的应用[J]. 电子科技大学学报，2005，34(3)：381-384