免疫原理在多Agent入侵检测系统中的应用

吴 知，许家玲

(电子科技大学应用数学学院 成都 610054)

【摘要】将免疫学原理应用于多Agent入侵检测系统，提出免疫智能体的概念。在设计建立免疫智能体的核心算法基础上，给出一种产生多样性、遗传性、健壮性的抗体解集的方案，并建立了基于免疫智能体的分布式入侵检测系统模型，该系统模型具有自适应性、健壮性、自治性等特点。

关 键 词 入侵检测系统; 免疫智能体; 分布式; 多Agent; 免疫学原理

中图分类号 TP393.08 文献标识码 A

Immune Principles Applications of Multi-Agent-Based IDS

WU Zhi，XU Jia-yi

(School of Applied Mathematics, UEST of China Chengdu 610054)

Abstract This paper presents a new method of putting Agent-based IDS and mmunological principles together, and presents a concept of immune agent. A solution set scheme of antibody with the variety transmissibility and haleness is presented after the core algorithm of immune agent. to be desinged .A immune agent-based distributing IDS model is set up. This intrusion detection system is designed to be adaptable, robustness, autonomy.

Key words intrusion detection system; Immune Agent; distributing; multi-agent; immune principles

入侵检测系统(Intrusion Detection System, IDS)，作为一种重要的安全部件，是网络信息安全防护体系的重要组成部分，是对传统计算机安全机制的重要补充。特别是近几年IDS作为一种主动防御技术，已成为研究的热点[1]。本文将免疫学原理与智能体概念相结合，提出免疫智能体的概念。设计一种新的基于免疫智能体的系统结构，为免疫学原理在IDS中的应用提供一种新的思路。

1 基于Agent的入侵检测

由于Agent的独立性和自治性为系统提供了良好的扩展性和发展潜力，因此，近年来对基于Agent的入侵检测技术的研究成为网络信息安全的重要研究课题。一个Agent可以简单到仅仅对一段时间内某条命令被调用的次数进行计算，也可以复杂到利用数学模型对特定应用环境中的入侵做出判断。如Purdue大学的研究人员为基于Agent的入侵检测系统建立了一个称为入侵检测自治代理(Autonomous Agent for Intrusion Detection)的基本原型[2]。当前，对基于Agent的IDS的体系结构，实现技术和算法的研究，已成为国内外智能入侵检测技术的研究热点。

收稿日期：2004 – 11 – 26
基金项目：四川省科技厅资助项目(04JY029-017-1)
作者简介：吴 知(1980 –)，男，硕士，主要从事网络信息安全与计算智能方面的研究.

2 免疫学原理

神经网络算法、遗传算法、免疫算法是基于生物系统的三大人工模拟算法，是近年来人工智能技术的重要研究方向[3]。University of New Mexico 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，发现他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[4]。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 ”，即是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[5,6]，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。

3 基于免疫智能体的入侵检测系统

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，免疫细胞具备分布式和独立性的特点[7]，将免疫原理应用于多Agent系统中，提出免疫智能体的概念，建立一种新的入侵检测模型。

3.1 免疫智能体IA

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，引入一种新的Agent概念，即免疫智能体(Immune Agent, IA)。

IA除了一般Agent的共性外还具有进化性、防御性、记忆性、耐受性的特点。

3.2 免疫多Agent入侵检测模型

系统的主要实体包括：监理器、IA专理器(简称专理器)、IA和用户接口。系统采用多Agent的分布式分层结构，系统的逻辑结构如图1所示。

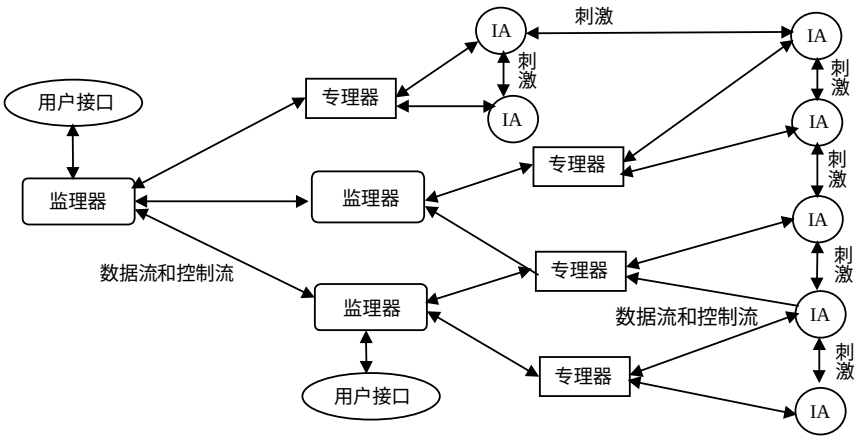

图1 基于多IA的系统逻辑结构图

1) 监理器：监理器负责监督和控制多个专理器，并具有一个黑板系统供专理器交流信息。监理器可以访问广域网络，从而进行高层控制协调，检测涉及多个主机的入侵。监理器之间也可以构成分层的结构。监理器负责同用户进行交互，从用户界面获取控制命令，向用户报告检测结果等。

2) 专理器：专理器负责对IA监督和控制，向IA发送控制命令，对IA发送来的数据进行精简。在对IA的工作状态进行监督的同时，还要决定各IA的生存适合度，以促进IA的进化。专理器还具有一个黑板系统，作为各IA发布请求信息的场所，IA将自己学习到的经验(又称疫苗)发布在专理器的黑板系统上，供其他IA学习。各专理器还可向一个或多个监理器发送信息，避免由于监理器故障造成的单点故障。

3) 免疫智能体IA：IA是系统中最重要、最核心的部分。如图2所示，IA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IA的核心部分。

IA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IA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。

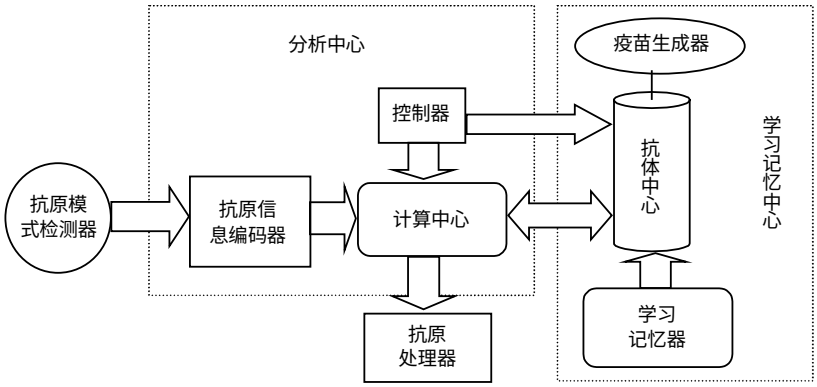

图2　免疫智能体IA的基本结构

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。

IA能将自己积累的经验(抗体)转化为疫苗在专理器上进行发布，或者以刺激的方式传递给其他IA以补充和修正领域知识和实现与其他IA的知识共享。IA的二次应答特性，可以使其对于其他IA发布的参考经验(疫苗)学习记忆，从而不断充实和更新本地知识库，以增强自身免疫防御机能。一个IA也可以向多个专理器发布信息，以便在更广的范围内快速的进行疫苗信息发布。

3.3　抗体产生选择算法

识别抗原并产生相应抗体的过程，也即系统进行入侵检测的过程。在抗原已成功编码后,计算中心如何选择最合适的抗体进行应对，是IA免疫性的关键。将免疫原理应用于抗体选择产生，使得抗体选择具有多样性、进化性等特点。抗体选择过程如下：1) 对抗体中心储存的领域知识内的已知抗原信息进行分类(即对入侵行为分类)；2) 从抗体中心的攻击类型库中随机选择大量的抗体(即系统存贮的经验信息)；3) 计算中心对记忆细胞中的抗体与抗原进行亲和力计算，并将计算得到的亲和力更高的抗体替换原亲和力较低的抗体；4) 为避免抗体群无限扩大，将一些亲和力很低的抗体抑制死亡(即将此抗体删除)。抗体群中高亲和力抗体受到促进，即抗体群中亲和力高的抗体数量会不断增加，但为了保持抗体的多样性，避免问题不成熟收敛；当高亲和力抗体浓度达到一定程度时又会受到抑制；5) 当抗体群的大小达到要求时则终止更新，选择最高亲和力的抗体处理抗原，并将相关信息储存到抗体中心。

抗体生成选择算法如下：

1) Begin初始化

Get_radom_Antibodys(A_1, …, A_n)；/*由抗体库中随机选取一个待选抗体群{A_1, …, A_n}*/

Create_Antibodys(U)；/*建立抗体解集U*/

2) 抗体的选择

i＝1;　K_first=0;

While　Number_U<　Require_number　do　　/*若抗体解集U未达到要求大小*/

Begin

K_second=K(A_i);　　/*选取抗体A_i, 计算亲和力K(A_i)*/

/*亲和力计算*/

i= i+1;

If K_second < Standar_K /*若A_i的亲和力小于预定的标准值*/

Then delete(A_i); /*抗体A_i被删除*/

3) 抗体的进化

Else

If K_second > K_first /*比较抗体A_i与抗体A_{i-1}的亲和力*/

Then K_first=K_second;

Add_new_Antibody(A_i,U); /*将亲和力较高的抗体A_i添加到抗体解集U中*/

Else Add_new_Antibody(A_{i-1},U); /*否则将抗体A_{i-1}添加到抗体解集U中*/；

4) 抗体的抑制

If Number_max_K(A_i) > Limit /*若亲和力最高的抗体的浓度大于预定值Limit */

Then Delet_some_Antibody(max_K(A_i)); /*删除一定数量的最高浓度亲和力抗体*/

End； /*产生抗体解集U*/

End.

4 结 束 语

建立了一个基于免疫原理的多Agent系统，该系统同时继承了多Agent系统和免疫系统的优点，具有以下特点：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，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] 戴英侠, 连一峰, 王 航. 系统安全与入侵检测[M]. 北京: 清华大学出版社, 2002

[2] 何炎祥, 陈莘萌. Agent与多Agent系统的设计与应用[M]. 武汉: 武汉大学出版社, 2001

[3] 孙 剑, 许家珆. 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

[4] 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

[5] Chittur A. Model generation for an intrusion detection system using genetic algorithms[D]. New York: Ossining High School, Ossining, 2001

[6] Muhammad M S, Brian J G. Information security on internet enterprise managed intrusion detection system (EMIDS) [J/OL]. IEEE 2001. 0-7 803-7 406-1/01

[7] Dozier G, Brown D, Hurley J, et al. Vulnerability analysis of AIS-based intrusion detection systems via genetic and particle swarm red teams[J/OL]. IEEE 0-7 803-8 515-2/04

编 辑 孙晓丹