文章编号：1001 – 2486(2002)04 – 0042 – 06

基于免疫学的多代理入侵检测系统*

吴作顺，窦文华，刘志峰

（国防科技大学计算机学院，湖南 长沙　410073）

摘　要：在探讨免疫学基本原理的基础上，提出了基于免疫学的多代理系统，用于联网计算机的入侵检测与反应。在这个框架中，基于免疫学的安全代理在联网节点之间漫游，监视网络状态。这些代理相互识别对方的活动行为，以等级方式进行合作，并根据底层安全规则采取相应的行动。移动代理具有学习能力，能动态适应周围环境，检测出已知与未知的入侵。多代理检测系统同时在不同层次监视联网计算机的活动情况，包括用户级、系统级、进程级和数据包级。基于免疫学的多代理入侵检测系统是灵活的、可扩展的和可适应的，能够根据管理员的需要与参数配置实时监视网络。

关键词：计算机免疫学；入侵检测系统；移动代理；多代理系统

中图分类号：TP393.08　　文献标识码：A

Immunity-Based Multi-agent Intrusion Detection System

WU Zuo-shun，DOU Wen-hua，LIU Zhi-feng

（College of Computer，National Univ. of Defense Technology，Changsha 410073，China）

Abstract：Based on investigating immunological principles，the paper presents a multi-agent system for intrusion detection and response in networked computers. The immunity-based agents roam around the nodes，and monitor the situation in the network. These agents can mutually recognize each other's activities，coordinate in a hierarchical fashion，and take appropriate actions according to the underlying security policies. Mobile agents can learn and adapt to the environment dynamically and can detect both known and unknown intrusions. The multi-agent detection system can simultaneously monitor networked computer's activities at different levels，including the user level，system level，process level and packet level. The immunity – based multi – agent intrusion detection system is designed to be flexible，extendible，and adaptable that it can perform real – time monitoring in accordance with the needs and preferences of administrators.

Key words：computer immunology；intrusion detection system；mobile agent；multi-agent system

生物体的免疫系统负责抵御外部病原的入侵。自然免疫系统是一个分布式的自适应系统，它采用多层防护机制，对致病微生物产生快速、准确的防护反应。免疫系统使用免疫记忆（memory）来记住已经出现过的抗原特征，并利用组合学构建抗体，以实现有效检测。免疫系统的系统行为是多个局部系统交互作用的结果。免疫反应可以是局部的，也可以是系统范围的，取决于抗原入侵的路径和特性。

免疫系统主要包括两种免疫细胞，即 B 细胞和 T 细胞。免疫细胞在生物体内不同淋巴器官间循环，免疫系统精确控制不同位置上的免疫细胞数目。生物体内淋巴细胞群在不同位置间的迁移称作导归作用（homing）。免疫记忆细胞倾向于回归致它们首次遭遇抗原的组织类型，因为这种位置重新出现类似抗原的机会较大。免疫反应采取的机制能够自我调整。免疫系统没有一个中心器官来控制整个系统的功能。B 细胞的克隆扩展和增殖都需要协同刺激机制，以防止发生自免疫反应。协同刺激第二信号能够确保免疫耐受，辨别危险的与无害的入侵者，减少检测系统虚警数目，并在发生真实入侵的情况下采取决定性的反应措施。免疫系统的这些有用特性促进了研究人员将其应用于解决实际问题，包括计算机反病毒、故障恢复和异常检测等，形成了计算机免疫学这个新的研究领域。

* 收稿日期：2002 – 03 – 19
作者简介：吴作顺（1974 – ），男，博士生。

1 计算机免疫系统

计算机的安全问题与自然系统的免疫功能类似。计算机面临的威胁与危险，如对保密性、完整性和可用性的侵犯，都可能由内部和外部的部件故障或者入侵行为引起。

将免疫学原理应用于计算机安全最早出现于 1994 年，Stephanie Forrest 和她的研究小组一直致力于为计算机构建一个人工免疫系统，这个系统能够比现有操作系统提供更好的一致性保护，并在此基础上提供一个通用的防护系统[1]。计算机系统的安全包括检测计算机资源的非法使用、数据文件的一致性维护以及防止计算机病毒扩散等。

保护计算机免遭有害病毒的破坏，可以看作是区分 Self（如合法用户）和其他危险 Nonself（非法用户、计算机病毒等）问题的一个示例。这种方法称作负选择（negative selection）算法，是对传统密码学和确定性计算机安全措施的补充。负选择算法最初的应用是作为文件鉴定方法，用于计算机病毒检测[2]。

1.1 欺诈检测

免疫型欺诈检测 CIFD（Computational Immunology Fraud Detection）的目标是检测零售部门金融交易与电子商务中潜在的欺诈活动。系统采用免疫学的原理，发现和跟踪欺诈行为。

基于免疫学的欺诈检测方法在可靠性和性能上都是可行的。在异常检测实验中，免疫学检测方法能够取得小的假阳性错误率与假阴性错误率，这说明该方法是可靠的。另外，高实时性能以及较小的管理负担都是免疫学异常检测系统的固有特性。

免疫型欺诈检测系统包括两类系统，主机型检测系统和网络型检测系统。这两类系统相互协作，类似于一个复合的免疫系统。系统包括一系列的 CIFD 检测器，部署在一个可扩展的、通用的 CI 框架里。CI 框架为终端用户和检测器之间的通信提供机制和工具，并负责配置检测器，报告和记录事件，与其他安全系统协调工作。

CIFD 系统利用 2 个现实世界的数据源，作为异常/正常数据集合。第一个数据集是 DARPA 公开的入侵检测领域的训练集与测试集；第二个数据集是公开的金融活动记录集合。在这些数据集的基础上，CIFD 系统首先作用于正常活动模式，对检测系统进行训练。当检测系统学习完所有正常模式后，再使用包括正常/异常活动的数据集进行测试，从而检测出所有内部和外部的异常部件。

1.2 UNIX 进程监测

将负选择算法应用于 UNIX 进程监测，可以检测出对计算机系统的有害入侵[1]。采用这种方法是为了鉴别 UNIX 进程的 Self 特性，因此将 Self 定义为动态计算机环境下进程的合法活动。Self 的这种定义对恶意攻击非常敏感。

一般情况下，UNIX 环境中 root 进程的系统调用可能造成的危害远比用户进程大。而且 root 进程的行为受限，相对比较稳定。定义 Self 为进程系统调用的短距离相关性。Self 的这种定义在多个标准 UNIX 程序正常状态下是稳定的，而且能够用于检测若干常见的入侵。选择 sendmail 作为例子进行测试，对异常的 sendmail 行为进行 3 类追踪，即成功的 sendmail 攻击、失败的 sendmail 入侵尝试以及系统错误。

实验结果表明，系统调用短序列提供了稳定的特征，能够用于检测 sendmail 常见的异常模式。由于这种方法采用的量度标准简单，易于计算，并且存储空间要求不大，因此可以将其作为在线系统。在线方式下，UNIX 内核检查 root 进程的每个系统调用。所有站点都会根据本地硬件/软件配置和使用模式产生本地的正常模式数据库，站点之间互不相同。因此，对一个站点的成功入侵并不意味着能成功入侵所有的站点，即使它们都运行协同的软件，这样就提高了入侵被发现的概率。

2 入侵检测与移动代理

入侵检测系统是一个专家系统，能够观测用户的活动模式，并在出现异常时通知系统管理员。入

侵检测是计算机安全的重要组成部分，它提供了在物理安全、识别鉴定和访问控制之外对计算机资源的附加保护层。入侵检测最早由 James Anderson 在 1980 年提出[3]，但直到 Dorothy Denning 发表其经典入侵检测模型[4]后才开始真正发展起来。

早期的 IDS 一般采用整体结构，所有数据都在单个节点收集，并由中心节点分析，中心节点通常就是数据收集节点或者接近它。由于在单一节点上监测用户活动模式并不能够检测多台计算机同时发起的入侵，IDS 领域出现了基于网络的 IDS。基于网络的 IDS 监视网络数据流，监测计算机间通信底层网络数据包中的异常或误用。网络型 IDS 的出现标志着入侵检测由以主机为中心转化为以网络为中心。

第一代 IDS 结构一般包含两个部件，即数据收集过程和分析过程。数据收集过程通过主机的审计记录与内部接口或者目标网络的数据包收集信息；这些信息由中央分析过程进行分析。中央分析过程可以采取一种或者多种检测技术。这种结构在被监视主机较少时是有效的，因为中心分析方法限制了其应用于大规模环境。解决扩展性问题的一种方法是在数据收集过程采用即时的预处理与统一合并，然后再交分析过程处理。

最近出现的商用 IDS 一般采用层次结构。信息收集在叶节点处完成，叶节点可能是主机型或者网络型收集节点。叶节点收集的信息向内部节点传送，由内部节点进行合计。信息聚集、抽象与数据约简在内部节点一直进行下去，直到达到根结点。根结点通常是命令和控制系统，它负责评估入侵情形，采取相应的反应措施。更常见的情形是根结点向操作员控制台报告，由管理员评定入侵情况，并发出反应命令。

部分 IDS 采用了网状结构，信息可以在任意两个节点之间流动。网状结构 IDS 将信息收集、聚合、命令与控制功能集成为单一部件，这些部件部署在每个被监测的系统上。当某个位置检测出重要事件时，该位置上的安全部件就会向连接发起方的位置报告。当连接发起方是通信链路的中间节点时，该位置的安全部件必须递归地向通信链路的前一站报告，直到达到连接最初的发起方为止。由于通信链路和网络结构的随意性，这种通信方式必然是低效率的。

软件代理经过个人或者组织的授权，为了一定的目的自治地工作，并可以与其他代理相互作用。一个软件代理包括执行计算所需要的代码和状态信息，并且要求有一个代理运行支撑平台。软件代理可以是静态的，也可以是动态的。静态代理固定在一个平台上；而动态代理则能够在某个位置上停止运行，然后移动到其他平台上，接着执行后续代码。将软件代理应用于入侵检测不是一个全新领域[5]，但很多工作都只使用静态代理，而不是移动代理技术。

要将移动代理应用于入侵检测系统，参与检测的节点，如主机和网络设备，必须安装有代理平台。采用移动代理技术后，数据收集节点、内部聚合节点和控制命令节点就不必停留在一个固定物理位置上。例如，一个移动代理在网络中处于适合位置时就可以发挥数据聚合的功能。移动代理之间也有分工，不同的代理检测不同的入侵，处理各自的数据。

3 基于免疫学的多代理 IDS 框架

通过对计算机行为特性的长期观察，可以对其正常行为模式进行建模。异常检测问题可以看作是监视目标系统特征属性的非许可偏离，因为入侵者的活动总是在某些方面与正常用户不同。基于免疫学的入侵检测方法仿效自然免疫系统的某些机制，可以成功地检测特定类型的入侵。

多代理异常检测和反应系统应用免疫系统的计算特性，并将它们集成于单一框架下。检测系统监视多个层次上的参数，确定这些参数在入侵活动中的相互关系。基于免疫学的系统具有其他自治代理系统所共有的 3 个特性：移动性、适应性和协作性。移动性使得代理能够在网络中自由移动，并监视网络状态[6]。这些代理能够相互识别对方的活动，并产生特定的反应。移动代理具有学习能力，能动态适应周围环境。在其他代理的协作下，它们能够作一些复杂的决策。系统的免疫代理能够与其他代理相互作用，每种类型代理的空间类似于自然免疫系统中的免疫细胞。

（1）监视代理

监视代理在网络节点之间巡逻，并与特定意图的设备通信。监视代理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。检测系统中存在多个不同的监视代理集合，其中一些代理工作在 Nonself 空间，利用负选择算法监视系统的异常变化；而其他的代理则监测已知入侵的出现。

（2）通信代理

通信代理充当其他代理通信联络的消息邮递员，或者是具有指定能力的谈判代表。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 细胞和抗体。

（3）决策/行动代理

这种代理进行决策，确定需要激活的其他代理；或者是根据系统安全策略执行特定的任务。行动代理根据入侵的特性与强度激活一个适当的反应代理集合，包括助手（helper）代理、杀手（killer）代理和干扰抑制（suppressor）代理。

助手代理由行动代理通过通信代理激活。一旦激活后，助手代理向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，助手代理可以通过 e－mail、pager 等方式向安全主管发出警告，报告入侵事件。同时，助手代理实现一个 GUI 的报警接口，用于显示入侵活动的强度。

杀手代理在出现真实入侵与恶意活动时采取猛烈的反应措施。例如，在系统层杀手代理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；在用户层杀手代理可以停止用户会话，关闭用户帐号；在网络数据包层，如果它包括一个可疑会话，杀手代理可以丢弃一个数据包流。在面临真实危险时，杀手代理可以经过通信代理由多个代理共同激活。

干扰杀手代理由行动代理通过通信代理激活，它们会干扰其他决策代理采取更进一步的行动。干扰抑制代理能够在入侵检测/反应过程的后期，防止系统对假阳性错误采取其他行动。

多代理入侵检测系统能够评估当前状态，并且采取一系列的反应措施，作为决策的一部分。在这个框架下，不同代理的活动以等级方式进行协调。如图 1 所示。

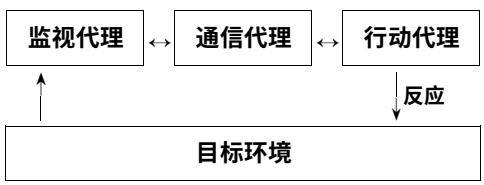

图 1 多代理入侵检测系统框架

Fig.1 Framework of multi-agent IDS

图 1 中每种代理的功能互不相同，它们以协作的方式工作。分布式多代理检测系统的不同部分根据网络环境的状态可能处于下面的工作模式：

（1）感知（Sensing）模式。检测系统监视网络环境的信息源，并且在不同层次上识别异常事件。

（2）识别（recognition）模式。当通信代理和行动代理在特定节点被激活后，检测系统在当地处于识别模式，根据预定义的安全策略作出适当的决策。

（3）反应（response）模式。检测系统在感染节点采取适当行动，激活特殊类型的代理，如杀手代理等。

大部分时间内监视代理都在网络中漫游，监视网络状态。如果网络某个部分出现异常情况，并被监视代理发现，协作型代理就进入识别模式，试图理解所发生的事件，并作出相应的决策。在有些场合下，代理作出决策时要咨询周围的其他代理，这相当于免疫反应中协同刺激的第二信号。作出决策之后，代理进入反

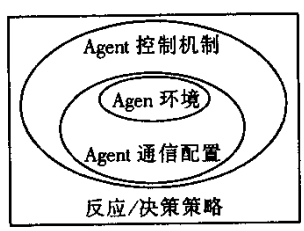

图 2 检测系统不同的功能模块

Fig.2 Components of detection system

应模式，采取特定的行动。入侵检测系统的功能模块如图2所示，图中内部模块与外部模块比较起来更加具有分布性。

支持多代理入侵检测系统的软件在面向对象平台上提供了必要的代理互作用部件与应用程序环境。不考虑代理内部结构的设计细节，软件平台包括3个主要模块，即代理通信配置、代理控制机制和反应/决策策略。不同种类代理的设计需要特定网络环境的知识；而且部分代理可能具有有限生命周期，只能够在特殊的时间段工作。多代理检测系统能够在大型网络环境下运行，并根据其决策目标和安全策略对入侵事件采取实时反应。

4 框架实现设计

4.1 多层参数监测

联网计算活动从下向上包括了网络数据包层、进程层、系统/资源层和用户层等4个层次，这些层次都是多代理IDS必须监测的。

为检测用户层的活动，下列参数需要保存在审计记录中，并通过统计分析用于构造正常用户行为模式的轮廓文件（profile）：

· 用户类型和用户特权
· 登录/退出时间和位置
· 用户击键模式
· 系统资源和目录访问
·用户使用的软件、程序类型

系统层参数给出了资源的使用情况，包括：累积的和用户平均的CPU使用情况；物理内存和虚拟存储器的使用情况；当前可用的交换空间；空闲存储器总量；I/O和磁盘使用情况。

入侵检测在进程层需要监视的参数有：

· 进程总数和类型
· 进程之间的关联
· 进程的运行时间
· 进程的当前状态（包括运行、阻塞和等待）以及失控进程
· 不同状态进程占用的时间，如用户态进程、系统级进程和空闲时间

检测系统通过监视下列参数，收集数据包层的信息，包括：连接数目和状态；平均收发数据包数目；连接的持续时间；连接类型（本地的/外部的）；使用的协议与端口。

入侵活动通常由外部连接进入目标网络，因此系统必须监视流入与流出目标网络的所有数据包，而且还必须使用上述参数来监视外部连接的数量与合法性。

检测系统收集目标网络在正常状态下所有监测参数的历史数据，得到正确的正常行为模式统计度量。在检测阶段，移动代理比较监测变量当前取值与正常轮廓文件的值，判断参数取值的偏离程度。代理之间的通信以及代理与检测系统其他部件的交互都通过通信代理进行。

4.2 决策支持部件

决策/行动代理在采取行动之前，需要根据不同的规则进行决策。代理所使用的规则集合既可以由领域专家手工添加，也可以根据历史数据进行合成。规则集的目标是监测参数偏离值的相互关系，从而确定入侵类型，并采取相应行动。决策规则集通常根据不同层检测参数的重要程度构造。在测试过程中，监测参数往往需要调整以作出更好的决策，影响系统性能的参数要添加到监测参数集合中。多代理入侵检测系统采用机器学习和数据挖掘[7]技术，学习被监测系统的正常行为，并自动适应网络环境的合法变化。根据决策规则集，代理可能采取下面一个或者多个行动：

· 终止网络连接
· 通过email等方式向安全主管报告

· 封闭指定 IP 或者发送方
· 拒绝外部连接请求
· 断开用户会话
· 改变用户访问权限
· 更改进程优先级

多数情况下，系统管理员只采纳决策/行动代理的建议，而不是由它们采取行动。行动代理与网络管理系统相互作用，获得网络拓扑结构，对网络的异常改变进行响应。

5 总结

入侵检测是计算机安全的重要组成部分，它在物理防护、识别认证和访问控制之外提供了另外的保护层。迄今为止，出现了多种入侵检测模型和产品。但没有一个入侵检测产品能够检测所有类型的入侵，每个检测模型都有自己的优势和弱点。入侵检测领域出现了多种新技术，计算机免疫学就是其中一个。

基于免疫学的计算机安全模型仿效自然免疫系统的某些功能部件，已成功应用于病毒检测、欺骗防护和入侵检测等领域。本文介绍的基于免疫学多代理入侵检测系统在单一框架下集成免疫系统的多个有用特性，是一个智能的、鲁棒的入侵检测系统。

多代理入侵检测系统同时进行多层次的监测，检测已知与未知的入侵，并进行等级方式的反应，减少检测的假阳性与假阴性错误。系统是完全分布式的，代理生成后在网络上漫游，因此一个节点被攻破不会导致整个系统丧失检测功能。

参考文献：

[1] Forrest S，Hofmeyr S A，Somayaji A，et al. A sense of self for unix processes [A]. In Proceedings of IEEE Symposium on Research in Security and Privacy，Oakland，CA，1996.

[2] Forrest S，Perelson A S，Allen L，et al. Self – Nonself iscrimination in a Computer [C]. In Proceedings of IEEE Symposium on Research in Security and Privacy，pages 202 – 212，Oakland，May 16 – 18 1994.

[3] James P Anderson. Computer Security Threat Monitoring and Surveillance [R]. Technical Report，James P. Anderson Co.，Fort Washington，PA，April 1980.

[4] Dorothy E Denning. An Intrusion Detection Model [J]. IEEE Transactions on Software Engineering，SE – 13 (2)：222 – 232，February 1987.

[5] Jansen W，Mell P，Karygiannis T，et al. Mobile agents in intrusion detection and response [C]. In Proceedings of the 12th Annual Canadian Information Technology Security Symposium，Ottawa，Canada，June 2000.

[6] Dipankar Dasgupta. Immunity – Based In trusion Detection Systems：A General Framework [C]. In the proceedings of the 22nd National Information Systems Security Conference (NISSC)，October 18 – 21，1999.

[7] Wenke Lee，Salvatore J Stolfo. Data Mining Approach for Intrusion Detection [C]. In Proceedings of the 7th USENIX Security Symposium，1998.