维普资讯 http://www.cqvip.com

一个基于 Multi-Agent 的计算机安全免疫系统模型

A Computer Security Immunology System Model Based on Multi-Agent

李 欢 梁意文 曹 霞 汤远闲

(武汉大学软件工程国家重点实验室 武汉 430072)

Abstract This paper presents a computer immunology system model, whose main components are defined according to the idea of Multi-Agent. Then the paper describes the structure and function of each agent. Also, the communication method between agents is described.

Keywords Computer immunology system, Multi-Agent, Computer security

一 引言

随着信息技术和 Internet 的迅速发展，计算机的安全问题越来越为人们所关注。Internet 无控制的开放性在带来许多便利的同时，也带来了计算机系统安全的脆弱性。

传统的安全技术，如：口令验证、反病毒软件、防火墙等，属于一种被动的防御措施，其主要特征是不停地补堵安全漏洞。与此同时，入侵者也在用各种有效的方法和手段测试并攻击这些保护屏障。因此，传统的安全技术只能防御一些已知的入侵方式。而在 Internet 这种动态环境中，这些安全技术的作用是有限的。

理想中的计算机安全系统所需要的是一种具备适应性、稳健性、自治性的技术。计算机系统自身应该能够从实际环境中"学习"如何保护自己，逐渐适应复杂、变化的环境，逐步得到更好的安全性。

从这一点上来看，自然免疫系统在人体中的作用与我们所要求的计算机安全系统在计算机中的作用非常相似。自然免疫系统保护生物，使之能够防御种类繁多的外来病原体，其本身具有记忆性、特异性和识别外来病原体的特征。借鉴自然免疫系统的思想、使我们有可能建立一个稳健的、适应性的计算机安全免疫系统。

本文将描述一个计算机安全免疫系统的模型，并在设计上引入"Multi-Agent"的概念和方法，用"Agent"定义来规范计算机免疫系统中各个部件的实现，利用"Agent"之间的通信，实现各部件之间的通信。

二 自然免疫系统概述

免疫学家认为："免疫就是识别"我(Self)"和"非我(Nonself)"，并消灭非我，是为了保证机体完整性的一种生理学反应"。"我(Self)"被认为是体内的细胞和分子，"非我(Nonself)"是任何一种异物，如细菌、病毒或寄生物。

免疫系统由细胞和分子组成，淋巴细胞是免疫系统中最主要的部分。抗原只有被淋巴细胞识别，才能开始免疫反应的第一步。即当免疫系统的识别器(淋巴细胞)与抗原结合时，就发生了识别行为。淋巴细胞与抗体的识别是特异性的，也就是说，每个识别器只识别一个结构上相关的有限抗原集合。当一个识别器与抗原结合时，就会引发一系列复杂的反应，最终常常导致抗原被消灭。免疫系统的最大特征在于它的处理过程(包括产生识别器、识别和消灭异物、并且记忆以前遇到的感染)是高度并行的。这也是免疫系统机制如此复杂的原因，但同时也是免疫系统对于单个部分失效和免疫系统自身被攻击具有很高的稳健性的原因。

自然免疫系统面对的问题与计算机安全面对的问题具有很大的相似性：一是都必须保护高度复杂的、动态改变的系统，使之免受大量的入侵；二是都必须保证系统的正常功能，并且必须保证防御机制不会严重损害系统。

免疫系统值得计算机借鉴之处包括多个方面，如：分布性、多样性、自治性、适应性、记忆性、动态覆盖性、异常检测等等。目前，以 Stephanie Forrest 为代表的研究人员对计算机免疫系统进行了比较深入的探讨并取得了许多研究成果(http://www.unm.edu/cs/forrest)，使计算机免疫学成为一个具体的研究方向。但是，这些研究往往只关注某个免疫系统部件的算法实现，而没有对整个免疫系统模型加以描述，因此无法从整体上把握免疫系统的特征，不能真正有效地模拟自然免疫系统。

三 Multi-Agent 概述

Agent 技术，特别是多 Agent 技术、为分布开放系统的分析、设计和实现提供了一种崭新的方法。一种较普遍的观点认为，Agent 是一个计算机系统，它的主要特征是自主性、反应性、适应性和社会性。自主性是指

维普资讯 http://www.cqvip.com

Agent 能在没有人或其他 Agent 直接干涉下持续运行，并能控制其行动和内部状态。反应性是指 Agent 能感知环境，并采取适当的行动以改变环境。适应性是指 Agent 能够对环境的变化作出反应，在适当的时候采取面向目标的行动，以及从其自身的经历、所处的环境和其他 Agent 的交互中学习。社会性即 Agent 能以平等的方式与其他 Agent 交互。

多 Agent 系统是一个松散耦合的 Agent 网络，这些 Agent 通过交互解决超出单个 Agent 能力或知识的问题。多 Agent 具有如下特征：(1)每个 Agent 拥有解决问题的不完全的信息或能力；(2)没有系统全局控制；(3)数据是分散的；(4)计算是异步的。

可以看出，Multi-Agent 中的 Agent 具备免疫系统中免疫细胞的基本特征。在计算机安全系统中引入 Multi-Agent 的概念，用 Agent 来模拟计算机免疫安全系统中的"免疫细胞"将更易达到自然免疫系统所要求的分布性、自治性、适应性等特点，可以相信，基于 Multi-Agent 的计算机免疫安全系统会具备更优的免疫模拟效果和更好的结构可伸缩性。

四　基于 Multi-Agent 的计算机免疫安全系统

4.1　基于 Multi-Agent 的免疫系统模型

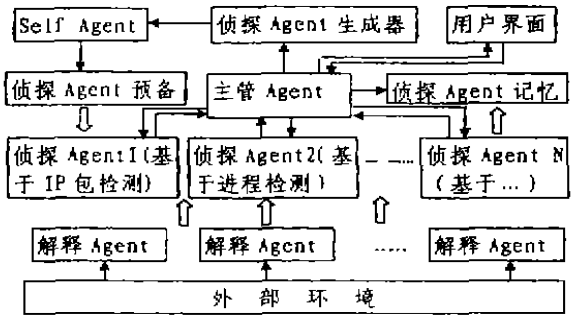

图 1　基于 Multi-Agent 的计算机免疫安全系统模型

4.2　各 Agent 部件的实现

4.2.1　侦探 Agent(Detector Agent)　在系统中存在着若干个侦探 Agent，负责侦察所有可能的入侵行为(图 2)。侦探 Agent 将翻译 Agent 送来的环境数据特征码放入消息池中，侦探器从消息池中取出特征码，并依据 nonself 池中的 nonself 数据对特征码进行匹配。如果匹配成功，则侦探 Agent 认为该消息来自一个入侵行为，消息发生器将向主管 Agent 发出警报。

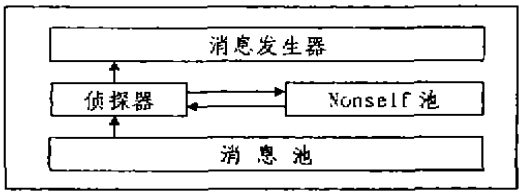

图 2　侦探 Agent 结构图

消息池中也可以存在来自其他侦探 Agent 和主管 Agent 的请求和命令，侦探 Agent 将会根据这些请求和命令做出相应的反应。

每个侦探 Agent 都有其生命周期。这是因为外界是一个动态的环境。对于不断变化的入侵行为，静态固定的侦探 Agent 集只能覆盖一部分入侵行为。只有不断对侦探 Agent"优胜劣汰"，才能获得比较满意的侦察效果。一个侦探 Agent 的生命周期如图 3。

侦探 Agent 可以独立地对系统进行检测，也可以相互进行交流和合作，共同解决问题。例如，当一个监视进程的 Agent 怀疑某一个用户进程有入侵嫌疑时，它可以要求负责 IP 包检测的 Agent 协助调查，负责 IP 包检测 Agent 对有关该可疑进程的 IP 包检测后，将检测结果反馈给负责进程检测 Agent，它将结合自己的数据和知识作出判断。

4.2.2　主管 Agent(Administrator Agent)　主管 Agent 对其他 Agent 的一切服务请求做出响应(图 4)。主管 Agent 接收来自其他 Agent 的请求消息，并将它们放入消息池中。消息处理器从消息池中取出消息进行处理。当有两个或两个以上的请求发生冲突时(如两个侦探 Agent 同时要求匹配一个入侵行为)，消息处理器将它们放入仲裁队列中，由仲裁器进行处理，处理的结果反馈给消息处理器做进一步处理。消息发生器将最终处理结果向外发出，建议相应的 Agent 应

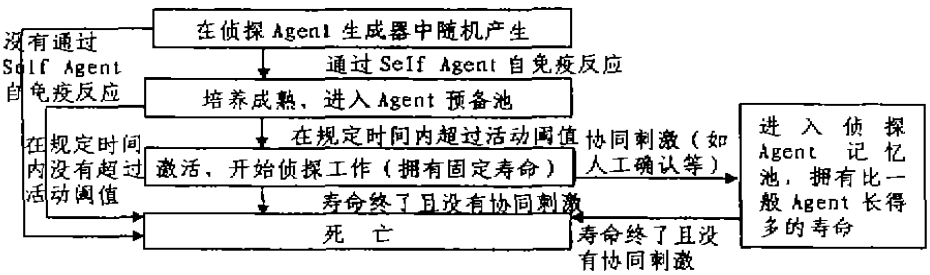

图 3　侦探 Agent 的生命周期

维普资讯 http://www.cqvip.com

如何采取行动。知识库为消息处理器提供消息处理依据，日志记录了消息处理器的运行轨迹，便于做故障判断，知识库也可以利用数据挖掘技术在日志中发掘有价值的规则，保持知识库中知识的动态更新。

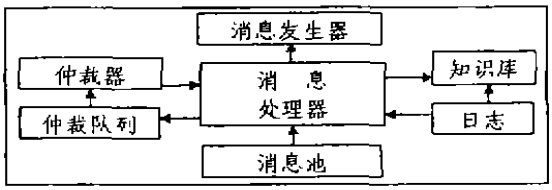

图 4 主管 Agent 结构

4.2.3 翻译 Agent(Interpreter Agnet) 其主要任务是对其所负责的环境(如网络环境、进程环境等)进行数据收集采样，并将其编译成侦探 Agent 可以理解的数据格式，然后发往侦探 Agent。一个翻译 Agent 的数据可以被多个侦探 Agent 所共享。翻译 Agent 的结构如图 5。

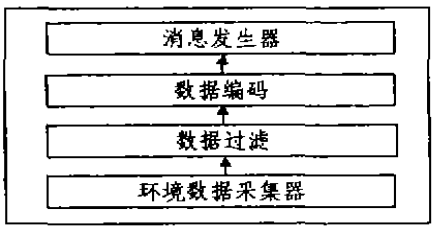

图 5 翻译 Agent 结构

4.2.4 Self Agent 负责收集一切正常行为(Self)的数据，并以此作为判断入侵行为(Nonself)的依据。由于 Self 的定义可以多种多样，因此 Self Agent 所包含的 Self 池是多种 Self 的集合。Self Agent 的主要功能是以新产生的侦探 Agent 做自免疫反应。保证通过自免疫反应的侦探 Agent 是一个只能识别 Nonself 的 Agent(图 6)。

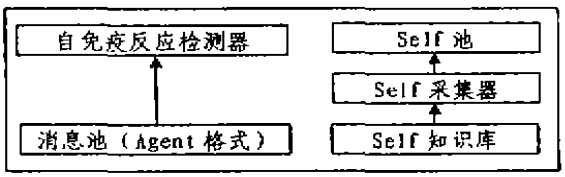

图 6 SelfAgent 结构

Self Agent 将侦探 Agent 生成器送来的新生成的侦探 Agent 放入 Agent 消息池中。自免疫反应检测器从消息池中取出侦探 Agent 进行处理：按照类型选定对应的 Self 集，将此 Self 集中的数据送入侦探 Agent，让它进行处理。如果 Self Agent 发现侦探 Agent 出现了报警信息(说明该侦探 Agent 对此 Self 集中某些数据匹配成功)，则发生了自免疫反应，它将会把某些正常行为误认为入侵行为。Self Agent 把通过自免疫反应的 Agent 送入 Agent 预备池，而把没有通过自免疫反应的 Agent 的寿命置为 0。

安全环境的正常行为也是处于动态变化之中的，Self 采集器根据 Self 知识库中的知识对安全环境进行数据采样分析，并将新的 Self 数据放入 Self 池中，同时删除一些旧的、过时的 Self 数据，维护 Self 与现实环境的动态一致性。

五 Agent 通信

在我们的模型中，各 Agent 之间的通讯是通过消息机制来完成的。消息发送方 Agent1 向消息接受方 Agent2 提出条件服务请求，Agent2 在接受到条件请求之后向 Agent1 作出条件允诺，允诺一旦条件满足它将主动地为 Agent 提供相应的服务，并通过消息机制将结果返回给 Agent1(图 7)。

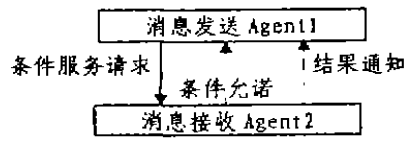

图 7 Multi-Agent 通信

结束语 本文引入了"Multi-Agent"的概念，对计算机免疫系统中各主要部件进行定义和规范，描述了一个"基于 Multi-Agent 的计算机免疫安全系统模型"。该模型能够更真实，更直接地模拟自然免疫系统的特征，提高了计算机免疫系统的开放性和可伸缩性，为适应各种安全策略的要求提供了基础，对计算机免疫系统的进一步研究也具有参考价值。

参 考 文 献

1 Forrest S, Hofmeyr S A. Computer Immunology. Communications of the ACM, March 1996
2 Forrest S, Hofmeyr S A. John Holland's Invisible Hand: An Artificial Immune System
3 Hofmeyr S A, Forrest S, Somayaji A. Lightweight Intrusion Detection for Networked Operation Systems
4 Warrender C, Forrest S, Pearlmutter B. Detecting Intrusions Using System Calls: Alternative Data Models
5 Forrest S, Longstaff T A. A Sense of Self for Unix Processes. In: Proc. of the 1996 IEEE Symposium on Research in Security and Privacy Los Alamitos, CA, IEEE Computer Society Press, 1996
6 Hofmeyr S A, Forrest S. Immunity by Design: An Articlal Immune System. In: Proc. of the 1999 Genetic and Evolutionary Computation Conference(GECCO). P1289～1296
7 张磊，卿斯汉. 一个基于 Agent 的防火墙系统的设计与实现. 软件学报，2000，11(5)：642～645
8 胡舜耕，张莉，钟义信. 多 Agent 系统的理论、技术及其应用. 计算机科学，1999，26(9)
9 毛新军，王怀民，陈火旺，刘凤岐. Multi-Agent 系统的主动合作计算模型. 计算机科学，1999，26(9)
10 杨鲲，崔永顺，刘大有. Agent 特性与分类. 计算机科学，1999，26(9)