基于移动 Agent 的分布式入侵检测系统的体系研究*)

Research on Distributed Intrusion Detection System based on Mobile Agent

肖建华　张建忠　吴功宜

(南开大学计算机与系统科学系　天津 300071)

Abstract　This paper is an initial exploration into the filed of using Mobile Agents (MAs)for IDSs (Intrusion Detection System). In this paper , a new distributed intrusion detection system architecture based on mobile agents—— MAIDS is proposed, which combines the technique of host-based IDS and network-based IDS. MAIDS exploits the advantages of mobile agent to improve the system performance, and make the system have certain flexibility and intelligence.

Keywords　Intrusion detection, IDS, Mobile agent, MAIDS

1　引言

随着网络的发展,网络的安全问题日益突出。单纯的被动防御安全体系——防火墙已不能胜任当前的需要,因此在安全领域中综合使用多种技术成为一种趋势。入侵检测技术的研究是网络安全研究的一个重要方面,它能够为网络提供一种主动的安全防御措施,与防火墙、系统漏洞检测等技术结合在一起,构成完整的安全防御体系(如图 1 所示)。

入侵检测技术(IDS)是目前安全领域的一个研究热点,研究方向包括基于主机与基于网络的 IDS、集中式与分布式的 IDS,异常检测和误用检测等等。但传统的入侵检测系统大多存在一定的缺陷(例如不灵活、扩展性差、效率低等)。因此,探索新的实现方法,将多种技术融合使用成为一种趋势。

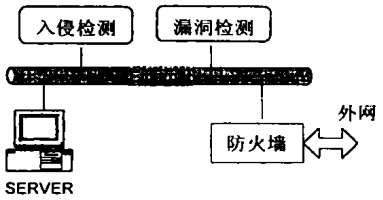

图 1　完整的安全防御体系结构图

本文在入侵检测系统中引入智能领域中的移动 agent 技术,并对其在系统中的应用做了初步研究,提出了基于移动 agent 的分布式入侵检测系统体系 MAIDS。它将数据的收集和分析任务分配到各个 MA 中,以解决常规 IDS 中存在的一些问题。

2　网络入侵技术及移动 agent 技术简介

2.1　网络入侵技术

入侵检测(Intrusion Detection)就是通过对运行系统的状态和活动进行监控,分析出非授权的网络访问或恶意的网络行为,从而迅速发现入侵企图,为入侵防范提供有效的手段。而 IDS(入侵检测系统)就是实现入侵检测功能的软硬件系统。

入侵检测系统可以从不同的角度进行分类[1]。根据系统检测的信息源,可以分为基于网络的入侵检测系统和基于主机的入侵检测系统;根据入侵检测系统采用的策略,可以分为误用检测(又称为基于知识的检测)和异常检测(又称为基于行为的检测);根据系统的控制方式,可以分为分布式入侵检测和集中式入侵检测。

为了促进入侵检测系统的研究,标准组织制定了一些标准(如公共入侵检测框架 CIDF 和正在制定的入侵检测消息交换协议 IDMEP 等);实际产品也有很多(如 ISS 的 RealSecure, NAI 的 Cybercop, SVC 的 NetProwler IDS, CA 的 SessionWall-3 等)。

目前 IDS 研究的热点和趋势包括引入智能技术和数据挖掘技术、采用分布式结构、基于主机与基于网络的 IDS 的结合、异常检测和误用检测技术的结合等等。其主要目的就是力求在对已知攻击类型实现准确检测的同时,增强对未知攻击的识别能力,保证系统的性能及其自身的可靠性。

2.2　移动 agent 技术

agent 的研究起源于人工智能领域,它是指模拟人类行为和关系,具有一定智能并能够自主运行和提供相应服务的程序。一般而言,agent 具有反应性、自治性、面向目标性和针对环境性等特点。移动 agent 是众多 agent 中的一种,除了具有一般 agent 的特性外,还具有移动性,可在一定控制机制之下,携带自身状态、信息和代码等在网络中转移到另一个环境中去,并在该环境中恢复执行。同时,如果需要,它还可以返回源点(自身返回或由控制系统调回)。移动 agent 的提出使得 agent 技术具有了动态性和分布计算的特点,进一步扩展了 agent 处理事务的功能或应用范围。

在移动 agent 研究领域也有一些标准,其中 OMG 制定的 MASIF(Mobile Agent System Interoperability Facility)[3] 标准定义了移动 agent 的管理、迁移、系统类型和定位等有关内容。

目前移动 agent 的系统主要有 IBM 的 Aglet, General Magic 的 Odyssey, 三菱的 Concordia 和 ObjectSpace 的 Voyager 等。其中 IBM 的 Aglet 系统是一个较为成熟的移动 agent 系统,可以作为本 MADIS 系统的开发和实验平台。

移动 agent 的特性和优势,使得它进入了电子商务、信息

*)天津市自然科学基金重点资助项目(编号:013800211)。肖建华　硕士,主要研究方向为计算机网络和信息安全,Internet/Intranet 工程。张建忠　副教授,硕导,研究方向为网络管理、网络安全及电子商务。吴功宜　教授,博导。

搜索、个人助理等广泛的应用领域。网络管理与网络入侵检测也开始引入移动 agent 技术，并取得了一定研究成果。

3 MAIDS 分布式入侵检测体系结构

3.1 MAIDS 体系结构的提出及目标

目前，入侵检测系统仍存在很多问题。不论集中式的入侵检测系统还是分布式入侵检测系统，或多或少都存在效率低、误报率高、维护困难、灵活性差、易受攻击和欺骗、响应能力有限等缺陷。面对这些缺陷，人们开始探索新的技术。而起源于人工智能的 agent 技术的发展，尤其是移动 agent 技术的出现，为网络领域的研究提供了新的思路。虽然移动 agent 的出现不是为了入侵检测，但是其思想在入侵检测系统的研究中是可以、也是值得借鉴的。在这方面，相继出现了一些研究成果（例如 IDA，ATIRP，JAM 等），这些研究分别探讨了移动 agent 技术在入侵检测中某个方面的应用，取得了一些令人满意的结果。

在这个背景下，我们研究了移动 agent 技术的特点，借鉴上述研究系统的一些成果，提出了基于 agent 移动的分布式入侵检测系统体系 MAIDS，欲达到以下目标：

（1）基于主机和基于网络的检测方式结合，能同时监视整个网络和网络中的主机。

（2）分布式体系结构，减轻网络负载，避免单点失效隐患，并增强灵活性和可靠性。

（3）移动 agent 之间可以协作，具有一定智能性和适应能力。

3.2 MAIDS 体系结构

MAIDS 整个体系结构主要由控制台界面、监视器、规则/事件库、响应库、移动 agent 库、移动 agent（MA）和 agent 运行环境七个部分组成（如图 2 所示）。下面对各个部分的功能进行阐述。

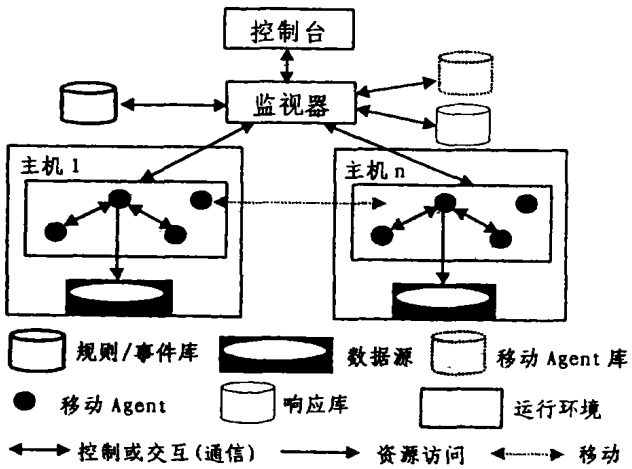

图 2 MAIDS 体系结构图

控制台界面 用户界面，便于用户的管理和维护。它主要是提供管理入侵检测系统的接口，管理人员可通过它对整个系统进行设置。

监视器 充当移动 agent 发布器，并负责控制和回收它们，同时还可以处理涉及多个主机的检测。监视器之间在必要的时候可以进行协作，以增强对大规模网络的管理能力。

规则/事件库 存放各种入侵规则/事件的特征描述，用某种固定格式进行编写。

响应知识库 存放根据规则/事件库中定义的各种入侵模式而制定的相应响应措施，其描述方法与规则/事件库类似。将相应知识库与规则/事件库分离的主要目的是使系统结构更加清晰，以方便响应方式的扩展。

移动 agent 库 存放各种移动 agent。系统开始运行时，监视器会根据网络情况和配置的需要，从移动 agent 库中选择合适的 agent，并将其实例化，然后发布出去。系统中的移动 agent 可以有很多种，可按照各自针对的特定目标而设计。根据入侵检测系统功能的需要，MAIDS 将移动 agent 分为主机移动 agent、网络移动 agent、响应移动 agent、协作移动 agent 等几种类型。其中每种又可根据具体任务分成若干不同的子类。移动 agent 库的实现为系统规模和功能的扩展提供了方便的途径，必要时只需创建新的移动 agent，并将其添加到库中即可。

移动 agent 是 MAIDS 系统中最重要的实体，入侵检测的任务主要就是由它们来完成的。系统中不同类型的 agent 的任务不同，例如主机 agent 被发布到各个主机后，可以根据自身的任务，监视主机的某个部分，必要时做出响应；网络 agent 则可以根据自身的检测任务，侦听网络中相关数据包，并进行分析处理，条件允许时可做出实时响应。移动 agent 除了能完成自身的任务外，在某些情况下，它们之间还可进行一定的协作，对新环境进行自学习，增强自己的知识库，从而加强对攻击的检测能力。

运行环境 作为移动 agent 运行的支撑环境，安装在网络中各个受监视主机中，为各种移动 agent 的执行提供了必要的条件。该环境一般可以跨越平台，以使移动 agent 能在异构网络中运行，访问不同系统里的资源。

3.3 MAIDS 的运行机理

系统开始工作时，监视器从移动 agent 库中调出所需的移动 agent，创建 agent 实例。根据任务的不同，系统从规则/事件库和响应库中选择对应的知识信息分配给各个移动 agent，之后将它们发布到指定的地点（网络中的主机和其他设备）。移动 agent 到达目的地后，就可在运行环境中运行，执行自己的检测任务。

每个主机可接受多个移动 agent，并为它们提供相应资源。这些移动 agent 之间并发地执行各自的任务（出于冗余考虑，允许各主机间出现一些功能重叠的移动 agent）。在某些主机出现故障时，该主机中的网络移动 agent 可根据一定算法随机选择移动到其他主机中继续运行，或是向监视器报告，由监视器将其收回并重新分配到一个新的位置。此外，移动 agent 还可通过与其他 agent 进行协作来补充自己的信息库，增强自己的能力。

监视器除了在系统初始化时执行移动 agent 的发布操作外，在需要的情况下，可调回已完成任务或因某种故障而不能继续执行任务的移动 agent。同时，监视器还可根据需要发布新的移动 agent（例如根据某些移动 agent 的请求，发送响应移动 agent 来处理单个 agent 无法解决的问题），接收多个 agent 发来的消息（特别是不同主机反馈回来的信息），并根据这些消息实现对涉及到多个主机的攻击的检测。此外，一个监视器还可跟其他监视器协作，处理大规模网络内的可疑入侵行为。

结束语 MAIDS 体系结构利用了移动 agent 技术的优势，以 IBM 的 Aglet 系统作为移动 agent 的开发平台，主要优势表现为：（1）具有分布式性质，提高了检测效率，避免了单点

（下转第 35 页）

动态接入费率算法由 Mackie Mason 于 1993 年提出，至今也没有一个可以称得上成功实际应用。动态接入费率算法所带来的问题是它使用户过多地考虑为达到一定程度的服务质量所需要承担的费用，而精确的费用往往是用户不可能知道的。用户要么付出了过多的价钱，要么因为估计错误少付了费用，而没有得到所需要的服务质量。另一方面，过度复杂的费率调整使得用户忽视了所使用的具体业务，这将使网络运营商在确定不同业务的费用方面的灵活性大大降低，同时也使得计费软件的设计十分复杂。这无疑不符合简单的原则。同时，它要求用户对网络运营状况以及对其他用户比较了解，这又不符合相对分离和异步资源管理的原则。这些都直接导致了动态接入费率算法最终的失败。

5 E2E QoS

随着 VoIP、VOD、视频会议以及众多多媒体业务的出现，E2E QoS 控制问题，即网络数据如何从源端传递到目的端，如何保证时延、抖动以及丢失率等指标，日益受到业界的瞩目。一个典型的 E2E QoS 问题如图 1 所示。

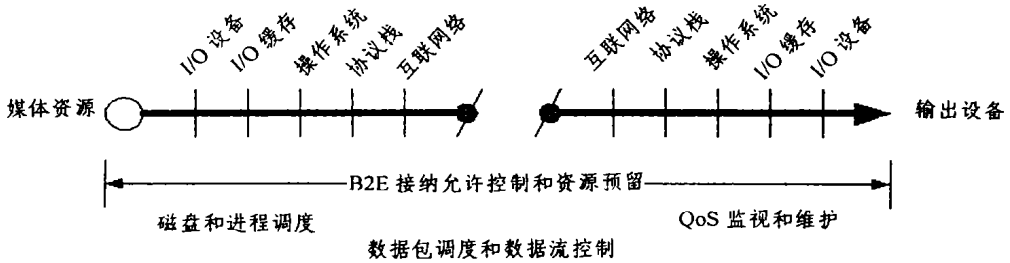

图 1 典型的 E2E QoS 问题

从图 1 可以看出，当数据包从源端传递到目的端时，QoS 依赖于若干因素，包括 I/O 设备、缓存管理、操作系统的支持、协议栈以及网络。这其中，存在着许多问题有待于进一步的研究：如接纳允许算法、资源预留机制、服务区分机制、QoS 监视和维护策略，甚至还要包括磁盘和进程调度算法的改进。所有这些问题都包含在 E2E QoS 问题之中。

根据作用对象的不同，E2E QoS 问题可以分为以下四类：

- 网络主机 QoS 问题：包括网络主机（服务器或客户机）I/O 设备的管理、操作系统中的进程调度算法的设计、协议栈软件的设计、接纳允许算法的设计等；
- 路由器 QoS 问题：包括输入/输出队列管理、区分服务（Diff-Serv）、数据包调度算法等；
- 网络 QoS 协议及体系结构：包括资源预留（RSVP）、多协议标签交换（MPLS）、QoS 策略以及 QoS 体系结构（QoS-A）等；
- QoS 策略：包括策略决策点 PDP（Policy Decision Point）以及策略执行点 PEP（Policy Enforcement Point）等的研究。

小结 本文讨论了有关端到端 QoS 控制方法的有关问题，包括：QoS 的概念、QoS 原则、研究 QoS 问题的必要性以及 E2E QoS 等问题。应该指出的是，本文所讨论的问题只是从综述的角度出发的，因而有些方面还非常肤浅，恳请广大同仁斧正。

参 考 文 献

1 Ferguson P, Huston G. Quality of Service. John Wiley & Sons, 1998
2 Braden R, Clark D, Shenker S. Integrated Services in the Internet Architecture: an Overview. Internet RFC 1633, Jun. 1994
3 Jain R. Myths about Congestion Management in High Speed Networks. Internetworking: Research and Experience, 1992, 3: 101～113
4 Shenker S, Partridge C, Guerin R. Specification of Guaranteed Quality of Service. RFC 2212, Sept. 1997
5 Braden R, et al. Resource ReSerVation Protocol RSVP Version 1 Functional Specification. RFC 2205, Sept. 1997 txt), May 1998

（上接第 40 页）

失效隐患，而且便于扩展；(2)结合使用了基于主机和基于网络的检测模式，能同时对整个网络和网络中的主机进行检测；(3)系统中的运行实体移动 agent 具有一定智能，可实现交互，而且添加方便，从而提高了整个系统的灵活性和智能性。

但是，目前移动 agent 的技术发展还不很成熟，还有许多技术难点有待解决，因而本体系只是对移动 agent 在入侵检测领域中应用的初步探索和简单实现，还存在一些不足，例如目前系统中主要采用的只是误用检测策略，功能还不是很强等。利用移动 agent 的智能性和协作性，在系统中结合异常检测和误用检测技术，增加响应方式（例如可实现攻击诱骗技术），以及增强自身的抗攻击性等是未来的研究方向。

总之，移动 agent 技术的发展，为入侵检测系统的研究提供了一个新兴方向。由于移动 agent 所具有的优点，使得它在入侵检测领域有着很好的应用前景，本系统就是一个有益的尝试。

参 考 文 献

1 Bace R, Mell P. Intrusion Detection Systems. NIST Special Publication on Intrusion Detection Systems. 1999
2 Huhns M N. Mobile Agents. IEEE Internet Computing, May. June 1997
3 http://www.focus.gmd.de/usr/covaci. The First Reference Implementation of the OMG MASIF -Mobile A gent System. Interoperability Facility, 1998