规模分布式网络入侵检测方法研究

闫映松　王志坚　周晓峰
（河海大学计算机及信息工程学院　南京210098）

A Survey to Scalable Distributed Intrusion Detection Methods

YAN Ying-Song　WANG Zhi-Jian　ZHOU Xiao-Feng
(Institute of Computer & Information Engineering, Hehai Universty, Nanjing 210093)

Abstract　With the rapid development of Internet, network security becomes more serious problem. Traditional technology can not meet the demand of scalable distributed network security, and distributed intrusion detection architecture can solve the problems. However, present intrusion detection systems still have many problems such as accuracy, reliability and adaptability. This paper discusses the present situation of intrusion detection and analyzes the problems that distributed intrusion detection exists and propose some technology and researches in point.

Keywords　Distributed intrusion detection, Component technology, Agent technology, Date mining

1　引言

随着网络经济的到来，Internet 在为发展带来巨大机会与可能性的同时，也带来了恶意入侵的风险。单纯的防火墙已经不能满足系统安全的需求，因为它无法控制内部网络用户和透过防火墙的入侵者的行为，无法处理合法用户的越权存取行为问题。因而需要建立多方位、多样化的手段来保证网络的安全。入侵检测系统是一类专门面向网络入侵检测的网络安全监测系统，而且正在成为网络安全解决方案中的重要组成部分，发挥着越来越重要的作用。

入侵检测经过十多年的发展，已由传统的使用分析 TCP 包和审计日志等单一方法发展到集中式的入侵检测乃至最近兴起的分布式入侵检测。随着规模网络的兴起和广泛应用，如何建立一种高度分布、扩展性强的高效入侵检测方法是目前该领域研究的热点之一，本文就这一问题进行了初步的探讨，并提出了相应的对策。

2　入侵检测系统综述

2.1　入侵检测系统

网络入侵是指任何试图破坏信息系统的完整性、机密性和可用性的网络活动的集合。入侵按分类法可分为6类：闯入攻击、假冒攻击、泄露、拒绝服务、攻击安全控制系统和恶意行为。入侵防御技术例如用户认证（密码或指纹等），避免程序错误以及信息保护（如加密）常被用来作为入侵防御的第一道防线。

入侵检测常作为计算机安全监测系统的第二道防线。入侵检测中心元素包括：目标系统中被保护的资源（如用户帐号，文件系统，系统内核等）、描述这些资源正常或合法行为的模型，将系统活动与模型相比较识别出异常或侵犯性的活动的技术。

入侵检测系统是完成入侵检测的软件和硬件的集合。图1描述了一个带有普遍性的 IDS 的结构。

它至少由以下部分组成：

（1）审计记录收集部件：入侵检测系统的数据可能来源于系统的不同部分：键盘输入、系统日志、应用日志等。然而，典型的数据来源于网络活动、基于主机的安全日志或者二者兼有。

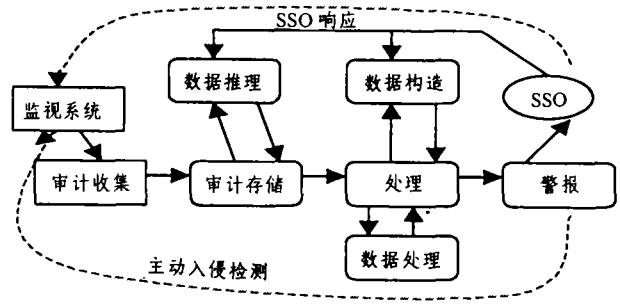

图1　IDS 的组成

（2）审计记录存储部件：一般来说，审计记录流量非常大，采用怎样的策略来进行存储以减少冗余是 IDS 运行效率的关键。

（3）处理（检测）部件：该块是 IDS 的中心部件。多种语法被用来寻找可疑活动的证据，有三种方法：基于异常的入侵检测、基于规则的入侵检测及基于签名的入侵检测。

（4）数据构造部件：构造数据以转化成 IDS 能够识别和操作的格式。

（5）数据推理部件：存储已知的入侵模式和/或正常行为的轮廓（profile）。

（6）活动/处理部件：存储中间结果。

（7）警报：对入侵事件向 SSO 发出警报。

2.2　入侵检测模型与技术

网络安全的研究人员提出并实施了各种各样的模型，这些模型都是基于 Denning[2] 所提出的假设，即假设所有的正常行为和异常行为都可以通过适当选择一套模型化的系统特征来精确地表示。相应地，入侵检测分为基于异常的入侵检测和基于误用的入侵检测。

2.2.1　*异常入侵检测*　基本思想是假定所有入侵行为均是与正常行为不同的，实施这样一个检测首先要对目标系统建立一个正常行为的描述模式。这种模式可通过两种方法建立：**阈值检测和基于轮廓**（profile）。**阈值检测**是在一个时间

区间内对专门的事件出现次数进行计数，如果计数超出了被认为合理的数值，就假定发生了入侵。这种方法简单，容易实现，对于简单的入侵检测是有效的，但对于复杂的攻击就难以实施有效检测。基于轮廓的方法是从审计记录中抽取一些相关量(measure)进行统计，为每个用户建立一个用户扼要描述文件(profile)。轮廓是用户正常行为的统计概要，当用户行为与他以前所建立的轮廓相差较大时，可认为有入侵行为发生。

异常检测能对整个系统中各种异常行为进行检测，能检测出未知的攻击；缺点是计算复杂，存在漏检和误检。

2.2.2 *误用入侵检测* 通过预先精确定义的入侵模式对观察到的用户行为和资源使用情况进行监测。首先对入侵行为进行特征化描述，建立某种入侵行为的特征行为模式，然后将当前用户行为与模式相匹配，如果与某个模式一致就表示发生了这种入侵。误用检测使用的方法主要有专家系统、状态转换分析、基于模型的方法和模式匹配方法。随着对计算机系统弱点、漏洞和入侵行为分析研究的深入，误用检测在入侵检测系统中担负起越来越重要的角色。其主要优点在于检测过程简单、直接、检测效率高，但由于已知攻击种类繁多、技术复杂，造成多种攻击类别检测效率低下，且无法检测到未知的攻击。

将两种检测方法结合起来可得到系统正常行为及异常行为的模式，称之为 signature inspired。它发挥了两种检测方法的优点，但却增加了系统的开销并降低了运行效率。目前入侵检测中出现了一些诸如人工智能、免疫检测和自主代理等新技术，这些技术在很大程度上提高了检测的效率和质量。

2.3 入侵检测系统分类

根据入侵检测的数据来源，入侵检测可分为基于主机的 IDS 和基于网络的 IDS。基于主机的 IDS 从所在的主机收集审计信息(如：系统日志、应用程序日志等)，它保护的范围仅限于它所在的主机，但它能对该主机进行全面的监控。由于不同 OS 的审计记录格式不同，这种 IDS 的移植性很差。基于网络的 IDS 所需的数据来源于网络和 OS 中传输的数据包，它允许系统检测多台主机中传送的信息。在实际应用中，两种方式经常一起使用，共同完成检测任务。

2.4 入侵检测系统体系结构

2.4.1 *集中式的 IDS 体系结构* 集中式的 IDS 集中地收集和分析来自于多台主机的源审计记录，所有事件信息均要传送到中央处理机上，分析并做出响应。典型的 IDS 如由国家计算机安全中心(NCSC)与 SRI 组织共同研发的 MIDAS[1]，它应用 P-BEST 进行入侵检测，专家系统集中分析并做出响应，COAST 中心研制的将 Petri-nets 应用于入侵检测的 IDIOT 系统[2]，以及应用嵌入过滤机制分层进行入侵检测的 BRO 系统[3]。近年来，随着规模分布式网络(scalable distributed network)的兴起和广泛应用，集中式的入侵检测体系结构面临诸多挑战：

(1)事件产生和存储：审计数据的产生和存储一般是一种集中式的活动，而且通常聚集了大量冗余信息在各抽象层。集中式的审计机制大大加重了 CPU 和 I/O 的负担，并且不能很好地适应大量用户的增容。另外，这种集中式的审计机制也不能容括各种空间上分布的组件(如路由器、过滤器、DNS、防火墙等)及公共服务。

(2)状态-空间管理和规则复杂度：在基于签名的分析方法中，规模复杂度和性能有着直接的关系。一个复杂的规则结构能够用详尽的先后条件精确表示出入侵事件的定义。然而，它加重了维护分析过程中产生的大量状态信息的工作量，因而也限制了处理事件的规模。反之，简单的规则可以减轻分析和维护的负担，能够适应处理事件的规模和效率。但它又不能精确表示误用(misuse)和异常(anomaly)。由此可见，复杂且表达能力强的规则模型与要求最小的状态空间管理和分析的简单规则需要折衷。

(3)知识库(knowledge respository)：专家系统把知识库(由与目标系统相关的推理规则和状态信息组成的库)与分析引擎和响应逻辑相分离，以增加整个检测系统的模块性。在一个集中存储在本地的库中维护这些知识(如根据实际需要增加，修改知识库)是有一定益处的。然而，在高度分布和大流量的规模系统中，集中存储的单个库连同简单的分析引擎势必成为检测系统运作的瓶颈。而且，单个点的失败可能导致整个库的不可用。

(4)推理体系结构：基于签名的专家系统的核心，是有一套接收输入(活动日志)和基于某种推理规则集定位搜索新信息的运算法则。这种推理引擎模型本质上是集中式的。在一个大型网络系统中，各种事件和数据流异步地在网络中传输，这不论是在并行度上还是在流量上都是集中式的分析技术所不能处理的。并且集中式分析要求集中地收集事件信息，这大大加重了该推理引擎所在的部件的负担。因而，在中央式的专家系统方法和完全分布的推理引擎分析方案间找到一种优化的范例是构建规模推理体系结构面临的主要挑战。

集中式体系结构存在单点失效、可扩展性有限、IDS 重新配置或增加功能困难等问题。另外，中心服务器对攻击数据的关联和分析能力低下，导致过多的人工干预；系统自适应能力差，不能根据环境变化而进行自动配置。因而，集中式的体系结构，如果部署在高度分布的网络环境中，就很难有效地发挥它的作用。

2.4.2 *分布式 IDS 体系结构* 这种体系结构的网络检测任务由分布于网络各处的检测单元协作完成。这些检测单元还能够进行更高层次结构上的扩展，以适应网络范围的扩大。一个分布式 IDS 体系结构解决方案[4]如图2。它由三部分组成：主机代理模块、局域网监视器代理模块以及中央管理者模块。

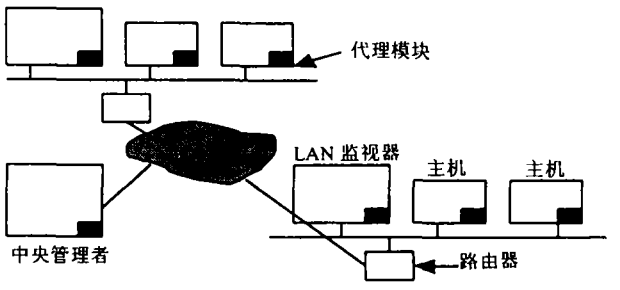

图2 分布式入侵检测体系结构

(1)主机代理模块：在受监视系统中作为后台进程运行的审计收集模块。其目的是收集主机上与安全相关的事件信息，并将数据传输给中央管理者。

(2)局域网监视器代理模块：与主机代理模块类似，它除了分析局域网通讯量，还将结果报告给中央管理者。

(3)中央管理者模块：接收包括来自局域网监视器和主机代理的报告，关联这些报告来检测入侵。该模块由入侵检测的专家系统、控制整个系统信息流的通讯管理块、SSO 友好接

口组成。

在这个体系结构中，代理截获审计收集系统生成的审计记录，应用过滤器去掉与安全无关的记录，然后将这些记录转化成一种标准格式以实现互操作。然后，代理中的分析模块分析记录，并与该用户的历史轮廓相比较，当检测出异常时，向中央管理者报警。局域网监视器代理审计主机与主机之间的连接以及使用的服务和通讯量的大小，以查找出显著的事件，如网络负载的突然改变、安全相关服务的使用等。

分布式体系结构可以从单独的入侵检测扩展成能够关联许多站点和网络行为的检测系统。它相对于其他检测方法，有以下优点：

(1)扩展能力强：通过扩展检测单元来实现网络安全范围的扩张。

(2)容错能力强：分布式的独立结构解决了单点失效问题。

(3)兼容性：即可包含基于主机的ID，又可含有基于网络的ID，超越了传统ID模型的界限。

(4)适应性强：当网络和主机状态改变时，如升级或重构，分布式IDS可以容易地作相应修改。

3 规模分布式IDS存在的问题及其对策

在规模分布式网络中，由于网络接口和控制物理及逻辑上的多样性、规模性及分散性，决定了必须以分布式的分析体系结构来适配。但是，这种体系结构还存在很多尚未解决的问题。Porras指出了在设计分布式入侵检测系统时要考虑的几个主要问题[5]：

(1)分布式入侵检测系统可能需要采用不同的审计收集系统，而不同的审计收集系统采用不同的记录格式。因而需要处理不同的格式以实现不同IDS间互操作。

(2)网络上的一个或多个结点将作为对来自网络中各系统数据的收集和分析点，因此原始的审计数据或者总结数据必须通过网络进行传输，因而存在一贯保证这些数据完整性和机密性的需求。需要完整性是为了防止入侵者通过修改传输的审计信息来掩盖其行为，需要机密性是因为传输的审计信息可能是有价值的。

(3)集中的或分散的体系结构都可以使用。对于集中式的体系结构，存在对所有审计数据进行收集和分析的中央点。这方便了关联输入报告的工作，但造成了潜在的瓶颈和单点故障。对于分散的体系结构，存在多个分析中心，但是它们必须能够协调各自的行为并交换信息。

3.1 IDS标准

在分布式入侵检测体系结构中，为了满足多种异构网共存及各级域不同的安全需要的要求，需要配置多种功能和结构各异的IDS来适应。为了实现这些IDS之间的交互性和互操作以协同完成整个系统的入侵检测任务，不同IDS需采用标准的框架。目前，两个组织在做IDS的标准化工作，一个是美国国防部高级计划研究局的CIDF工作组和Internet工程任务组的IDWG，本文主要介绍CIDF的有关标准。

CIDF[6]把IDS从逻辑上分为面向任务的组件，并开发出一套规范。这套规范允许不同IDR(intrusion detection and response)组件互操作和信息共享，并允许不同的IDR子系统根据需要重用。CIDF还制定了一个IDS的通用模型(Common Intrusion Detection Framework，简称CIDF)，将IDS分为四个基本组件：事件产生器、分析引擎、事件响应单元、事件库，如图3所示。

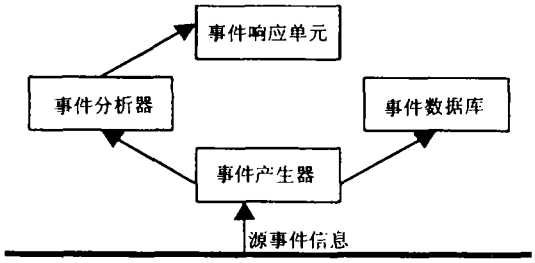

图3 CIDF组件

(1)事件产生器：收集整个计算机系统的事件信息源，并转化成标准格式以实现互操作。事件特指在数据源发生，被监视器检测到，可能导致警报传输的行为。事件可以来源于网络元素，应用，主机审计记录或其他任何感兴趣的部件。

(2)事件分析引擎：获取组件传送来的事件信息并分析。各种分析方法均可采用，例如统计分析方法、类型识别方法等。

(3)事件数据库：对存放事件产生器采集的事件信息及分析引擎产生的中间结果和最终结果的地方的统称。

(4)事件响应单元：根据分析引擎产生的入侵判断执行预定的对抗措施。

3.2 组件技术

入侵检测系统当环境参数变化时，其配置应能方便地重构；另外，随着系统的升级和优化，IDS也应做出相应的调整，例如增加功能、增删模块等。然而，现有的IDS普遍不能很好地解决这些问题，为此，我们将组件技术的思想引入到IDS，来解决IDS普遍难以升级和重构的问题。

3.2.1 组件的基本概念 Bertrand Mayer对组件作了如下定义[7]：组件是一个软件系统的一个部分，它能够和其他部分组装在一起以组成更大部分或一个系统。我们可以从三个不同角度看组件：

(1)包的角度：这是从组件的组织角度出发，强调组件是一组可复用的元素的集合。在UML1.0中就是从这个角度定义的：组件是一个提供模块元素物理包装的可复用部分。这种包结构是基于组件的分布式部署应用所必需的特性。

(2)服务的角度：组件是服务的提供者。它通过接口向其它组件或客户提供服务。

(3)整体的角度：这个角度定义组件是一个实施封装的边界。它强调组件是一个独立的可替代的行为单元。

从上面可以看出，组件遵循一定的标准：可以被其它客户或软件元素使用；包括所有依赖元(硬件和软件平台，其他组件)的规范；包括提供的功能的一个详细说明书；在说明书的基础上就可用，而不需了解其内部细节；可和其他组件组合；可快速平滑地集成到系统中。

3.2.2 组件的优点 利用组件技术的目的主要在于它可方便地将可重用的块插入到各种系统中，而不需了解其细节。另外，组件技术对于系统的更新、扩展和优化也是很方便的，因为它的整体性和独立性使其可轻易地被其他组件所替代。

3.2.3 组件和IDS 以CORBA、COM/DCOM和JavaBeans为代表的分布式组件具有位置透明性，即不同功能的组件可分布在不同的位置，组件之间可以跨平台、跨网络相互调用与合作，可以完成复杂的问题。它是支持分布式计算的重要技术。

根据通用入侵检测框架 CIDF 标准，可以将 IDS 的不同部件组装在一起，实现分布式体系结构和协作收集和分析事件信息，并均衡负载，从而不断扩展系统。SRI 组织研制的 EMERALD[8]是基于这一思想的初步雏形。它采用一种组块的方法，这种方法使用独立的分布式监视器组件（由资源对象、基于轮廓的异常检测单元、误用检测单元和响应单元组装而成）来构成一种分层（服务级、域级、企业级）的分析结构，从而可以检测到对主机以及跨域攻击活动。

3.3 代理技术

代理是在一定环境下连续、自主运行的软件实体。移动代理技术是一种功能和控制灵活分布的技术，它提供了一种灵活的基于 Internet 的分布式计算范例，具有移动性、自主性、安全性、协同性、智能等特性。它将远程交互改为局部交互方式，工作原理如图4。

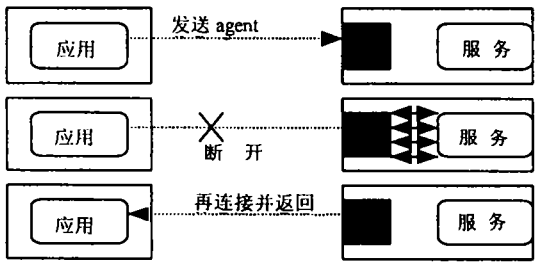

图4 移动代理的工作原理

当服务请求处理数据时，应用主机与服务主机建立连接，并发送 agent 到该服务的 MA 平台，然后断开连接。MA 携带智能的处理程序在本地进行数据处理。当处理完毕后，应用建立连接并回收 MA。在多个应用的环境中，代理可以从一个应用移动到另一个应用上，因而避免了大量数据在网络中传输。另外，移动代理隐藏了网络结构多样性和复杂性，屏蔽了数据源和通讯协议的差异，因此是异构环境下分布处理的一种很有前景的解决方法。移动代理具有如下优点：(1)坚强性：不需要持续的网络连接，不会因为代理的崩溃导致整个系统的瘫痪；(2)效率：避免了多个请求的多次远程交互，从而提高了执行效率；(3)灵活性：请求再响应的方式。当系统增加应用时，不需要额外的配置，只需要增加相应应用的代理即可。

在 IDS 中，一个代理可以执行一项专门的安全管理、入侵检测或响应功能。由于代理是独立运行的实体，因此可以在不改变其他部件且不需要重新启动 IDS 时加入、删除和重新配置代理。也可以根据需要灵活组合多个代理以协同完成复杂的入侵检测任务。基于代理的入侵检测系统最大的优点在于它减少了网络流量，减轻了网络的传输负载。但它也带来了代理本身的安全性问题。代理安全特指代理的属性（包括代码、数据等）不被偷窥和修改。解决的途径有加密算法、通过变换增加代理本身的理解难度等。在文[9]中提出了一种基于公钥的解决方案。

3.4 数据挖掘技术

规模分布网络中存在多个刺入点，这些脆弱点遍布在网络层和主机层上，如网络层上传输的恶意 IP 包、主机层的系统漏洞等，而且不同刺入点的活动被记录进不同的审计收集系统中，这些不同格式和不同定义的数据源给 IDS 利用审计记录有效地实施入侵检测增加了困难。IDS 也经常需要扩展，增加额外的模块来对某些网络部件（如主机、子网等）实施专门的保护。另外，新的系统安全漏洞和攻击方法不断地被发现，因而也需要经常和及时地更新 IDS。现今的 IDS 由于各方面因素影响，其扩展性和适应性很有限，而且它们的更新也是一项缓慢且代价高昂的工作。在规模网络中，审计记录的数量及系统特征的数目都是相当巨大的，需要高效、智能的数据分析工具来发现系统的异常活动。数据挖掘技术是解决这些问题的重要技术。U. Fayyad 对数据挖掘作如下定义：数据挖掘是从海量数据中获取有效的、新颖的、潜在有用的、最终可理解的模式的非平凡过程。

数据挖掘技术的迅速发展，已经发展了一套从统计学、类型识别、机器学习以及数据库抽取出来的语法规则。几种语法对审计数据的挖掘特别有用：分类、关联分析及序列分析。目前已有一些机构在做这方面的研究，文[10]中提出了一种利用元学习（meta-learning）方法对审计数据进行挖掘以搜索出隐藏的或未被发现的入侵模式，并建立新的入侵模式，将新模式加入到已有的 IDS 中，从而提高了 IDS 的适应性。文[11]提出了一种在基于代理的入侵检测系统中应用数据挖掘的方法。它将代理分为两类代理：从大量审计数据中抽取出精确的入侵模式的学习代理以及实施入侵检测的检测代理。

3.5 其他相关技术与研究

在分布入侵检测系统中，不同种类的数据和信息必须经过统一处理以生成入侵知识，这个过程称为数据聚合（data fusion）。它是一种从不同数据源的数据中推出异常事件、活动和位置的新技术。文[12]中介绍了多传感器数据聚合的方法和过程。IDS 的免疫性和抗毁性也是 IDS 的研究热点，文[13]提出了一种 IDS 抗毁性结构框架并进行了初步探讨。美国的 DARPA 组织及 IBM 对 IDS 的免疫性进行了相关的研究。

结束语 本文在分析了传统的入侵检测系统及集中式的入侵检测系统存在的缺陷后，对规模分布式入侵检测的问题和现状进行了分析，并探讨了解决这些问题的一些相关技术和研究。组件技术的思想能够解决目前入侵检测系统的扩展问题。代理技术可以较好地解决分布入侵检测系统存在的网络流量负载过高的问题。数据聚合和数据挖掘技术可以解决数据源的异构性、多元性等问题，并从审计记录中抽取出新的入侵模式，解决入侵检测的适应性问题。分布式入侵检测是网络入侵检测的发展方向，但还不成熟，许多研究和技术还处于理论研究和实验阶段，还需要进一步的研究解决。

参 考 文 献

1 Sebring M M. Expert System in Intrusion Detection : A Case Study. In:Proc. of th 11th National Computer Security conf. 1988. 74～81

2 crosbie M, Dole B. IDIOT---users Guide:[The COAST Project Technical Report]. 1996

3 Paxon V. Bro: A System for Detection network intruders in real time. In:proc. of the 7th USENIX Security Symposium, 1998

4 Snapp S R. The DIDS (distributed intrusion detection system) Prototype. In:Proc. of the Summer USENIX conf. 1992. 227～233

5 Porras P. STAT. A state Transition Analysis Tool for Intrusion Detection. Mater's thesis, university of California at Santa Barbara ,1992

6 Kahn C, Porras P. A Common Intrusion Detection Framework. Available URL: http: // seclab. cs. ucdavis. edu/cidf/papers/jcs-draft/cidf-paper. ps, 1999

7 Brown A. Building System from Pieces with Component-Based

Software Engineering
8 Porrsa P A, Neumann P G. EMERALD: Event Monitoring Enabling Response to Anomalous Live Disturbances. In: Proc. of the 20th National Information System Security Conf. 1997. 353～365
9 Ausgefuhrt am. A distributed security management system based on mobile agents. Available URL: http://citeseer.nj.nec.com/462131.htm ,2001
10 Lee W. A data mining framework for building intrusion detection model. In: Proc. of the IEEE symposium on security and privacy. 1999
11 Stolfo S J, Lee W. Data mining approaches for intrusion detection. Availableat: URL: http://www.cs.columbid/wenke/papers/usenix/usenix.htm. 2000
12 Tim BASS. Intrusion detection system and multisensor data fusion. Communications of the ACM, 2000, 4: 99～105
13 韩宏，卢显良. 一种分布式入侵检测系统框架. 计算机科学，2001，28
14 Asaka M, Okazawa S, Taguchi A. A method of Tracing Intruders by use of Mobile Agents. Available URL: http://citeseer.nj.nec.com/asaka99method.html, 2000
15 Gruber B. A glimpse into the future of intrusion detection. The USENIX association magazine, 1999. 7

（上接第21页）

个的计算机提供的服务由网格的这些服务供给，就是说，具有关于位置、命名、安全性等方面的透明性。换言之，这种观点将网格软件的角色定义成一个虚拟机。这种看法与 Ian Foster 等提出的广泛的部署和互操作性的初衷不一致。

适合的模式应该是 Internet 协议系列，这些协议系列大量地提供解决在网格环境中出现的惟一性事件的互不相交的服务。网格环境中遇到的巨大的物理和管理方面的异质性意味着，传统的透明性是不可能获得的，因而这样的虚拟机也不可能实现；另一方面，在标准协议之上的一致看来是可行的。在我们的专题综述中，系统地介绍了由 Globus 提出的理论框架和体系结构。Ian Foster 等如此系统地公开他们的网格技术内涵，而不只是亮出基本观点是经过深思熟虑的。网格的要害是将一个资源必须讲的简洁和最低限度的协议集定义为“在网格中”。除此以外，仅仅试图提供一个框架，在此框架中可以规定许多行为。

当今的网格的研究中，有此观点/看法的人不在少数。这种观点实在是一个认识误区。问题在于这种看法确实仅仅是观念性的，缺乏体系结构和可行性方面的支持，对网络环境下操作系统的透明性和复杂性认识不足，不具备切实可用的基础。

观点4 网格要求新的程序设计模式

网格环境中的程序设计引入在串行或并行计算机中不曾遇到挑战。比如，多管理域，新的失败方式以及在性能方面的大的变化。然而，Ian Foter 等认为，这些问题并非主要的或中心的问题，网格的基本的程序设计问题并没有根本的不同。如同在其它背景下，抽象和封装能降低复杂性并改善可靠性一样。而且，也正如在其它背景下那样，允许构建各种高级抽象是所希望的，而不是实施一种特别的解决方法。

因此，例如，认为通用分布式共享存储模式能简化网格应用的开发者，将通过网格协议的形式实现此种模式，扩展或替换这些协议仅当他们证明这些协议不适合此种模式。类似地，认为所有的网格资源应以对象的形式呈现给用户的开发者，只需简单地通过网格协议实现面向对象的“API”。所以，网格不需要新的程序设计模式。

观点5 网格使得高性能计算机失去意义

在 VO 中，如果能以有意义的方式利用，成千上万（或更多）的处理器表示一种有重要意义的计算能力资源，这是一种松耦合的计算能力集成。然而，这并不意味着传统的高性能计算机是过时的，许多问题要求计算机与低等待时间和高通信带宽的紧耦合。通过使得访问更加容易，网格计算能够很好地增加，而不是减少对这种系统的要求。

结束语 本文，我们首先对当今一些主要的分布计算技术的基本功能及特点进行了概括性的介绍，分析了它们与网格技术的联系与区别，指出了网格技术的运用能够对这些技术带来质的提高。这些内容对“网格：面向虚拟组织的资源共享技术”一文中的第四个问题（即：“网格与当前的其它主要技术趋势有何区别？”）做了尽可能详尽的分析与讨论。其次，我们讨论了网格的进一步发展的相关问题，即网格间互联协议的需求问题，也对网格的一些不同观点进行了讨论，并给出 Ian Foster 等对这些观点的看法。

由于网格是一门新的学科，关于它的研究与发展还有很多事情要做，在这方面花大力气投入是值得的。回首看，在计算机科学与技术领域，特别是关键理论与关键技术，我们与先进国家的水平可能不在一个档次上。对网格这样新兴的并且是当今最具代表性的主流技术之一，即早参与研究和发展最起码不会加大与人家的差距，并有平等对话交流的机会。从研究成果转化为生产力来看，由于网格是一种典型的面向应用的技术，最终可广为应用的是一系列可共享全球各种不同类型的资源，并实现高度灵活可控可调，且使用简便的基础结构软件系列，或者曰超级中间件。这样的工作称之为一种贡献，也许不算过分。

参 考 文 献

1 Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations, Intl. J. Supercomputer Applications, 2001, 15(3)
2 高全泉. 企业级分布计算的基本需求及中间件技术. 计算机科学，2001，28(8)
3 Aiken R, Carey M, Carpenter B, Foster I, et al. Network Policy and Services: A Report of a Workshop on Middlewar. IETF, RFC2768, 2000. http://www.ietf.org/rfc/rfc2768.txt.
4 高全泉. 基于企业准则的 CORBA 与 DCOM 之特别比较. 计算机科学，2001，28(8)
5 Enterprise Javabeans Specification, Version 2.0 (EJB 2.0 specification). http://java.sun.com/products/ejb.
6 Java2 Platform, Enterprise Edition Specification Version 1.3. http://java.sun.com/j2ee/docs.html
7 Christiansen B O, Cppello P, et al, Javelin: Internet-Based Parallel Computing Using Java. http://www.cs.ucsb.edu/research/javelin.
8 Vahdat A, Belani E, et al. WebOS: Operating System Services For Wide Area Applications. In: 7th Symposium on High Performance Distributed Computing, July, 1998
9 Clarke I, Sanderg O, et al. Freenet: A Distributed Anonymous Information Storageand Retrieval System. In: ICSI Workshop on Design Issues in Anonymity and Unobservability, 1999
10 Grimshaw A, Wulf W. Legion--A View from 50,000 Feet. In: Proc. 5th IEEE Symposium on High Performance Distributed Computing, 1996, IEEE Press, 1996. 89～99
11 http://www.sun.com/jini/whitepapers/architecture.html
12 高全泉. 网格：面向虚拟组织的资源共享技术. 计算机科学，2003，30(1)
13 高全泉. 网格体系结构详解. 计算机科学，2003，30(1)