# 基于 CORBA 中间件的智能入侵检测系统①

## A CORBA-Based Middleware Smart Intrusion Detection System

范荣真 (浙江商业职业技术学院 信息技术系 浙江 杭州 310053)

**摘 要:** 针对目前入侵检测系统不能适应异构网络环境、缺乏协同响应的不足，提出了一种基于 CORBA 的分布式入侵检测系统模型,结合人工智能思想,实现了一种基于 CORBA 的入侵检测系统 CMDIDS(Corba MiddleWare Distrubite Intrusion Detection System)。详细讨论了系统的体系结构、特点和实现技术等，使所设计的系统能够对大型分布异构网络进行有效的入侵检测，对网络智能化入侵检测系统的设计有一定参考价值，对综合解决网络安全问题是一个有益的探索。

**关键词:** 网络安全 入侵检测 入侵协同响应 CORBA

随着网络技术的发展和网络应用的深入，网络安全问题日益严重,给网络和信息系统带来了严重威胁。究其原因，主要是网络攻击技术不断发展变化，并呈现出一些新的特点，而原有的安全解决方案不能迅速地适应这些新特点，导致网络的安全保障技术相对落后于网络攻击技术，从而出现防不胜防的尴尬局面。所以有必要引入新的技术和思想，来改进原有的安全解决方案。

## 1 分布式入侵检测

入侵是指试图破坏一个资源的完整性、机密性和可获得性的活动集合[1]。入侵检测技术可被分为误用入侵检测和异常入侵检测两种，前者通过检测固有的攻击模式发现入侵，后者通过检测系统或用户行为是否偏离正常模式发现入侵；按照数据来源可分为主机和网络入侵检测，主机入侵检测主要收集其运行主机的信息，例如 CPU、内存使用率，文件的访问控制等，网络入侵检测主要收集其所在局域网上传输的所有数据；按照入侵响应可分为主动响应和被动响应两种：如果检测出入侵后，能够自动重新配置防火墙、关闭适当的服务或反击入侵者，那么就被称为主动响应，若检测到入侵后仅给出警报或记录日志，那就是被动响应[2]。

入侵检测系统是基于以上几种模型相结合构建出的计算机软件，其作用就像一个防盗系统，能够实时地发现可能的入侵。目前的网络入侵检测系统和产品还很不成熟，基本上都是用来监控单一网段，功能较为简单。此外，随着网络应用的广泛和互连网络自身的分布异构性，网络入侵与攻击的方式已经变得越来越隐蔽，且趋于多样性、分布化和协同性[3]。因此，入侵检测系统也需要满足跨平台、可复用、易扩充、协同检测等新的应用需求。所以，研究利用分布计算技术，实现大型分布式入侵检测系统(DIDS)是有意义的。

CORBA 是由对象管理国际组织 OMG 制定的一套分布式对象交互的规范[4]。CORBA 与入侵检测相结合具有许多优点和特点：① CORBA 开发语言独立性和跨平台性，使得能够方便地集成多种多样的监测和安全程序；② 利用 CORBA 中间件所集成的下层软件与上层应用系统几乎无关，即当下层软件发生改变时，只要 CORBA 对外的接口定义不变，上层应用几乎不需修改；③ CORBA 具有好的扩展性，能方便地进行系统裁剪或组合，适应不同的具体需要和环境；④ CORBA 本身就有很好的安全机制。它提供标识与鉴别，授权与访问控制，对象间的安全通信、安全审计、安全管理等安全服务。

将 CORBA 的优点和 DNIDS 结合，不仅可以解决网络平台的复杂性和多样性，还能适应网络异构和动

① 收稿时间:2009-01-04

态变化的特性。因此，我们设计并实现了一个基于 CORBA 的入侵检测系统，称之为 CMDIS。

## 2　系统组成、结构与特点

CMDIDS 系统是一个集状态监测，入侵检测和入侵响应于一体、网络与主机检测相结合、适于大型网络结构的 DIDS。CMDIDS 系统主要由管理点、网络检测点、主机检测点和安全响应点 4 部分组成[5](见图 1)。在 CMDIDS 应用环境中，用户可将一个大型网络划分成多个域，每个域中可部署一个网络检测点，多个安全响应点和多个主机检测点。整个系统只需部署一个管理点。

网络/主机检测点的任务是采集原始数据，对原始数据按照用户要求进行过滤，并反馈给管理点，实现实时状态监测，或对原始数据进行误用入侵检测，将结果报告给管理点。它由数据采集引擎、数据过滤器、误用入侵检测分析器和域管理器 4 部分组成。

安全响应点是网络中除检测点以外涉及网络安全和网络管理的各种软件资源，例如防火墙组件、文件备份组件以及负载均衡组件等。

管理点的任务是管理和配置所有的网络检测点，负责它和检测点的信息交流，汇总和存储检测点上报的数据，并对这些数据归类分析，进行异样入侵检测和分布式误用入侵的检测。它包含了图形用户界面、数据库、异常入侵检测与误用入侵分析器和顶级管理器 4 个部分。

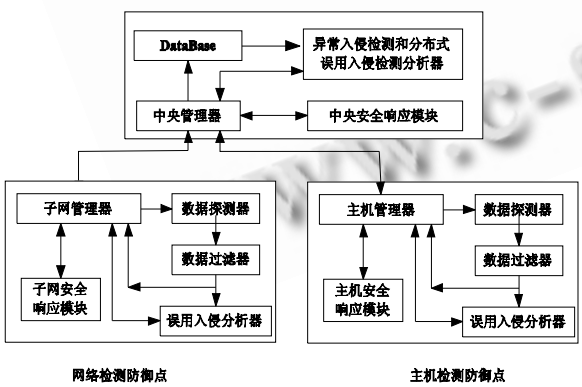


图 1　系统结构图

与其他现有的 DIDS 相比，CMDIDS 的一个特色在于实现了误用和异常的入侵检测的分离。前者放在检测点中，而后者放在管理点中。这是因为与计算机病毒相似，误用入侵攻击也具有明显的特征，这些特征也可被转化为规则，形成规则库，而且易于用编程语言实现。当前危害较大的 DDos 和蠕虫病毒攻击的共同特点都是在短时间内发送大量的数据包，拥塞网络或主机，从而造成设备瘫痪。如果将攻击数据照原样传送给管理点，不亚于将攻击的目标转移到管理结点。因此检测点在检测出误用入侵后只需和防火墙组件连动，切断有害连接，再将攻击的来源和特征报告给管理点。由管理点汇集这些信息进行进一步的分布式入侵检测分析，从而大大减少了检测点和管理点的数据通信，实现了局部与全局的监测的有机结合和对管理点的保护。

CMDIDS 的另一个特色是使用分布式计算和面向对象计算完美结合的 CORBA 技术，实现了检测和响应分离。用户可按照需要，选择检测点及不同安全组件之间的协作关系，建立了安全组件之间的相互通信和联动，提高了系统的可扩展性，实现整体安全防护。例如，当检测引擎检测到某种攻击后，会自动通知防火墙修改安全策略。从信息安全系统防御的角度出发，这种联动是必要的。联动包括了检测引擎与防火墙的联动，可封堵源自外部网络的攻击；检测引擎与网络管理系统的联动，可封堵被利用的网络设备和主机；检测引擎与操作系统的联动，可封堵有恶意的用户帐号；检测引擎和备份服务器联动，可以进行灾难恢复。

## 3　CMDIDS的设计和实现

CMDIDS 是一个基于 CORBA 的应用，那么系统设计的第一步就应该将系统中用到的 CORBA 对象提炼出来。CORBA 对象与我们平常所说的(本地)对象一样，也包含了对象属性和对象操作。但区别在于 CORBA 对象必须用 IDL 语言定义。IDL 定义了应用程序构件之间可互操作的接口。有了这个接口才使对象之间的远程调用成为可能。而 ORB 又保证了对象调用对用户的透明性。换句话说，CORBA 对象提供远程调用的接口，而本地对象则不可以。

### 3.1 CMDIS 对象模型

CMDIDS 在物理上由管理点、检测点和安全响应点 3 部分组成，因此管理点的顶级管理者需要和检测点的域管理者以及安全响应点的安全部件管理者通信。所以首先要将这 3 个管理者抽象为 CORBA 对象。然而在 CMDIS 中存在多个检测点和响应点，如果多个域管理者和安全部件管理者同时向顶级管理者返回数据，那么

就会使顶级管理者成为系统瓶颈，易造成单点故障。因此，我们在管理点设置一些和检测点与响应点相对应的通信对象，即检测点管理者和安全响应点管理者，由它们负责和检测点进行数据交换、解析检测点返回的数据、执行安全响应任务。这样顶级管理点的任务就简化为通过检测点管理者向相应的检测点和安全响应点发布命令，进行任务管理。从而将顶级管理点原有的任务管理和数据交互的功能分散在两类对象中。

顶级管理点要能够对检测点和响应点进行管理，它首先必须获得检测点和响应点的对象引用。在 CMDIDS 中是通过注册来实现的。检测点或响应点启动后主动向管理点报告，管理点接到检测点或响应点的注册请求后，为它生成一个检测点管理者或和响应点管理者，并记录它们的对应关系。

## 3.2 CMDIDS 系统的实现

### 3.2.1 误用入侵检测点

CMDIDS 利用专家系统进行误用入侵的检测。在系统实现时，先将有关入侵的特征转化为 IF－THEN 蕴含规则，其中 IF 部分是对入侵特征的描述，即判断攻击是否出现的必然条件，THEN 部分是系统的防范措施。推理机根据特征库中的规则，对待判别数据进行模式匹配，只有当规则左边的条件都满足时，规则右边的动作才会执行。知识库中的规则按照与上下文的关系可以分为两类。第一类规则具有上下文无关性，也就是说入侵分析无需知道其它数据包的信息，仅根据当前数据包中提供的信息就能分辨出是否有入侵出现。另一类则具有上下文相关性，当从一个数据包中无法判断出是否存在攻击时，需要综合与之相关的其它数据包的信息。也就是说对当前安全事件的分析要与过去所了解的相关历史信息联系起来，使结果更加准确可信。负责第一类规则匹配的推理机一直处于工作状态，每当捕获到一个数据包时，它都要使用上下文无关规则进行匹配分析，匹配成功就报警，否则就先将数据存储在特定的数据结构中，作为第二个推理机的输入；负责第二类规则匹配的推理机处于睡眠状态，间隔一段时间被唤醒一次。唤醒后，使用上下文相关规则对存储的数据进行匹配分析。匹配成功则报警，否则将数据传递到管理点进行下一步分析。攻击模式库作为系统的插件，能进行动态配置和更新，因此系统灵活，扩展性好。

这种方法的优点是对已知特征的攻击检测准确率和效率高、实时性好。缺点是防范入侵的有效性取决于专家系统知识库的完备性。为了能最大限度的保证系统的安全性，安全管理员需经常了解误用入侵的最新动态，提取新的入侵特征，并用规则表示之，最后加入知识库[6]。

### 3.2.2 异常入侵检测点

为了提高 CMDIDS 对未知攻击的适应，我们采用数据挖掘技术[7]，如图 2 所示。先将二进制表示的原始审计数据用 ASCII 码表示，原始数据可以是网络数据包、操作系统的系统调用过程或用户的操作行为。然后进行数据预处理工作，例如将原始数据归纳为 TCP 链接、Telnet 会话过程、用户执行命令集和用户使用系统时的等。将整理好的数据插入训练数据集后，作为某种数据挖掘算法的输入，就可从这个训练数据集中得到提取到的模式或特征。然后同样执行数据收集和预处理过程，得到评估数据集，用来评估新得到的模式或特征的准确率。若评估结果令人满意，则可将当前的模式或特征加入特征库，若不满意，则重新选取数据、挖掘算法，或重新设置算法中的参数。最后，就可用模式或特征库中已有的知识来处理的预言数据，得到预言结果。CMDIDS 系统使用分类算法和聚类算法可以发现未知的攻击形式，使用关联规则可以发现越权用户和假冒用户，同时还能在未知攻击的特征趋于稳定后，自动将攻击特征转化为规则，下发到检测点中，从而实现自动维护专家系统中的规则库。

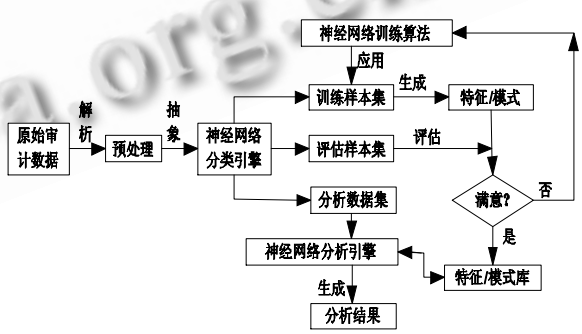


图 2　异常入侵分析器

### 3.2.3 安全响应点

CMDIDS 中央安全响应模块采用了主动响应和被动响应两种方式的混合形式[8]。具体协同如图 3 所示：

1) 防火墙组件。当检测点检测出入侵时，它在向管理点报告入侵事件的发生时间和攻击源的同时，也会通知本域中的防火墙组件。防火墙组件修改防火墙的策略，过滤掉攻击源的地址。然后，防火墙组件再将该消

息发送给管理点中的安全响应点管理者，由它再转发给其他的防火墙组件，相应调整各自的防火墙策略，保护网络中的其它结点不受攻击，起到预警的作用。

2) 负载均衡组件。CMDIDS 采用地址转换作为实现负载均衡的方法。具体采用 Linux 下的防火墙软件 iptables 作为地址转换器 NAT，同时根据性能监测引擎所监测到每台内部主机的性能数据作为挑选内部地址的依据。负载均衡组件每隔一段时间会轮询每个提供相同服务的服务器的负载情况，从中挑选出一个负载最轻的主机，同时会向防火墙组件发送消息，告知这个负载最轻的地址。当防火墙组件接到这个消息后，立即增加 NAT 地址转换策略。当有服务请求发送到防火墙时，就可以根据策略将请求目的地址转换为那个负载最轻的主机地址，这样就完成了负载均衡。

3) 灾难恢复组件。为了完成灾难恢复，需要将主机检测的文件监测引擎和文件备份协同起来。文件监测主要是通过对文件完整性的监测来完成的，其主要技术主要是根据文件内容提取一个数字摘要，通过对比两次的计算的数字摘要是否相同来发现文件是否被修改。进一步结合用户行为的检测，判断当前的修改是否非法。若是非法的，就选择一个文件备份组件对指定文件以流的形式还原。

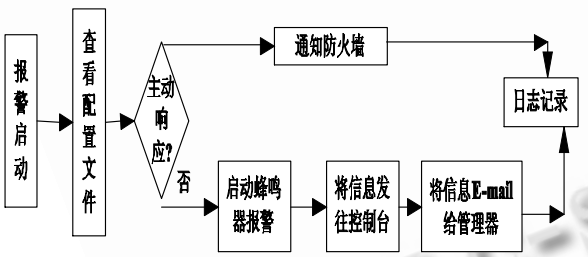


图 3　主动响应和被动响应工作流程

## 4　结语

CMDIDS 将 CORBA、人工智能、协同和 IDS 技术相结合，有效的解决了当前入侵检测系统面临的平台异构、无统一通信机制和安全策略等问题。

CMDIDS 已经被实现，通过在真实网络环境的初步应用表明，它基本能满足大型网络在性能、状态监控和入侵检测等方面的要求。当然，要使系统能够大范围推广应用，还有待完善和改进，例如，应完善对异常入侵的检测，增强系统的智能性，减少误报率；增加系统的容错能力与抗攻击能力；加强安全响应部件之间工作的协同性。

## 参考文献

1 Spafford E. Crisis and After Math. Communications of the ACM, 1989,32(6):678－786.
2 Stefan A. Intrusion Detection Systems: A Survey and Taxonomy 2004－6－9.
3 段海新,吴建平.分布式协同入侵检测—系统结构设计实现问题.小型微型计算机系统, 2001,22(6):646－560.
4 汪芸.CORBA 技术及其应用.南京:东南大学出版社, 1999.
5 吴晓南.基于智能的分布式网络入侵监测系统.西安:西北大学计算机科学系, 2003.
6 龚俭,董庆,陆晟.面向入侵检测的网络安全检测实现模型.小型微型计算机系统, 2001,22(2):145－148.
7 Adbelaziz M. Rule-based distributed intrusion detection. University of Namur, Belgium, 1997.
8 杨进,刘晓洁,李涛.人工免疫系统中变异算法研究.计算机工程, 2007,(17):45－46.