基于管理代理的分布式入侵检测系统设计

康松林，樊晓平，费洪晓，胡赐元，孙永新

(中南大学 信息科学与工程学院，湖南 长沙，410083)

摘 要：将网络管理系统与入侵检测系统相结合，建立基于管理代理的分布式入侵检测系统框架结构。研究管理代理的自治性、协同性以及管理代理间消息通信机制，建立管理代理的功能结构，设计基于遗传算法的调度Agent算法。从网络的各个层次分析管理信息库中与入侵检测有关的管理对象，建立检测规则库。完成分布式多层次结构化的具有自安全性的入侵检测系统的开发，达到管理代理对网络和主机监听目的。研究结果表明：根据攻击的本质特征，使用从管理信息库的统计数据中获取检测规则的方法，能有效实现对隐蔽和复杂攻击的检测。

关键词：入侵检测系统；网络管理；管理代理；遗传算法

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1672-7207(2007)06−1174−05

Design and implementation of distributed intrusion detection system based on management agent

KANG Song-lin, FAN Xiao-ping, FEI Hong-xiao, HU Ci-yuan, SUN Yong-xin

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: Combined network management system with intrusion detection system(IDS), the architecture of distributed intrusion detection system based on management agent was established. Good properties such as autonomy, cooperativity, communication mechanism among management agent were studied. Function structure of management agent was established and scheduling agent algorithm was also designed based on genetic algorithm. Management objects related to intrusion detection in management information base(MIB) were analyzed to form rules from different network levels. A distributed intrusion detection system with hierarchical structure and self-security was designed to monitor the running context of the system, and the rules were mined in intrusion detection from MIB according to the essence of network attack. The result shows that this method is efficient enough to meet the need of active detect complex intrusion.

Key words: intrusion detection system; network management; management agent; genetic algorithm

自 1980 年 Aderson 提出入侵检测的概念以来，经过 20 多年的发展，在系统模型和检测技术方面都取得了长足的发展。SRI/CSL 开发的 NIDES (Next-generation Intrusion-Detection Expert System)集中反映了入侵检测研究的最新成果[1]。NIDES 是采用统计和规则分析从监测主机收集信息的实时入侵检测系统，较好地实现了已知入侵的检测。但它存在很多不足，如：信息源过分依赖主机收集，一旦主机受到攻击，系统同时失效；采用规则分析方法很难检测到不断出现的一些新的互相协作的未知入侵；构件的封装使得它不能实现各组成单元之间动态地调节检测规则。一个分布式入侵检测系统面对当前高度分布异构复杂的

收稿日期：2007−02−08；**修回日期**：2007−04−25

基金项目：国家自然科学基金资助项目(60173041)；湖南省自然科学基金资助项目(05JJ30119)

作者简介：康松林(1968−)，男，湖南新化人，博士研究生，副教授，从事网络管理与网络安全研究

通信作者：康松林，男，博士研究生；电话：0731-2656132(H)，13548652875；E-mail: sunkang@mail.csu.edu.cn

网络环境和海量入侵信息，面临着严峻挑战[2−3]。在此，本文作者将入侵检测与智能代理、网络管理等技术相结合，设计了一个分布式多层次结构化的具有自安全性的入侵检测系统。该系统根据攻击的本质特征，使用从网络管理系统的统计数据中获取检测规则的方法，以便有效实现对隐蔽和复杂攻击的检测。

1　分布式多层次结构化的入侵检测系统框架结构设计

1.1　入侵检测系统框架结构

为了适应大规模、多管理域网络的入侵检测需求，设计并实现了一个基于网络管理的入侵检测系统，总的体系结构如图1所示。整个系统由中心检测器(Center detection)和检测代理(Agent detection)组成，中心检测器和管理代理以及管理代理之间通过SNMPv3协议实现安全有效的通信。中心检测器具有完整的入侵检测功能，它由收集器和分析器组成，能收集全局的监控信息并发现全局的入侵行为。管理代理由3种类型的实体组成：收集器(Collection)，分析器(Analyzer)和管理信息库(Management information base, MIB)组件。低层是2类探测器，即传感器和监控模块[4]，其中传感器通过协议分析负责收集通信子网和传输层的信息；监控模块通过内存映射收集应用层程序运行状态信息。它们都是受控于管理代理中的分析器的自治代理(Autonomous agents)[5]。自治代理的主要功能为：对入侵信息进行检测；对所在主机的网络报文进行预处理，保证报文的正确性；过滤检查审计内容，报告重要事件；对入侵予以初步响应：消灭已知攻击，抑制异常攻击(在系统被侵害之前发出警告)；向中心服务器报告等。

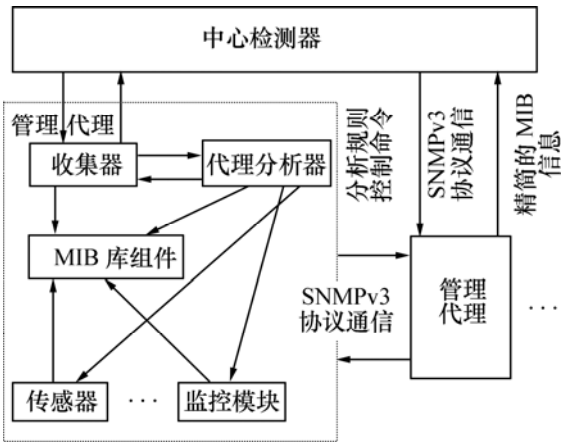

图1　分布式入侵检测系统结构

Fig.1　Structure of distributed intrusion detection system

在入侵检测系统结构中每个主机和通信结点机上都安装管理代理，管理代理中MIB库组件将传感器和监控模块传过来的MIB信息抽象成标准的MIB信息，收集器用来收集这些标准化的MIB信息并传给分析器，分析器通过分析这些结构化数据来检测简单和局部的入侵行为，并向各管理代理发送入侵指令使其完成入侵响应。管理代理还可以向邻近的管理代理发送请求信息以获取相关MIB信息，实现协同检测[6]。若分析器发现具有全局性的或超出代理分析器能力的可疑网络行为，则向收集器发送相应指令，此时，收集器把与这些行为相关的MIB信息传给上一层检测中心。在上一层，检测中心的分析器对于每个管理域都有详细的分析系统，由低层收集器收集的MIB信息在这里得到进一步分析，并将检测结果报告给管理者和各个低层管理代理，作出全局的入侵响应。中心检测器还可以将MIB信息移交给追踪更大管理域的更高层次的分析器，以实现更大范围的入侵检测[7]。

1.2　层次结构与管理代理机制

系统采用层次结构能很好地适应于网络环境下的入侵检测，层层精简入侵信息，一方面实现了入侵信息的有效传输，另一方面降低了通信系统和高层分析器的负担。管理代理的引入使得入侵检测能够很好地实现层次化的分布式检测。管理代理具有很好的专用性、独立性、可移植性、自适应性，管理代理的这些特点使得它很好地满足了入侵检测需求：它的专用性使得可以开发针对单一的信息收集和处理的智能体；独立性使得其可以分布在被监视系统环境的任意位置，实现有针对性的入侵检测，满足不同的需求；可移植性使得开发的代理能够得到有效地重用；自适应性使得其能够不断自我更新，以适应不断变化的检测环境。

1.3　管理代理间消息通信机制

管理代理间利用消息来实现通信。消息对象包括2个属性：一个代表消息的类型，用字符串表示，另一个代表消息的内容，内容可以为任何类型。消息分为基本消息和复杂消息。基本消息的内容由几个简单域组成。复杂消息的内容为自定义类实例。基于安全考虑，管理代理间并不直接进行消息通信，而是通过代理接口 proxy 来沟通[8]。proxy 是作为管理代理的一个外壳，防止其他管理代理直接访问其公有方法，确

保管理代理的安全。当一个管理代理想要与另一个管理代理通信时，只需在本地主机的管理代理环境中产生对另一个管理代理的代理接口，并与此代理接口通信。

管理代理间将利用代理接口提供的sendMessage方法，采用同步传送、异步传送、单点传送和多点传送4种方式进行消息传送。由于消息有轻重缓急之分，所以，利用setPriority方法为不同消息类型赋予不同的优先级。同时，为了防止消息丢失，每个管理代理都有一个由系统创建和管理的消息队列，所有接收到的消息都存储于消息队列中并根据消息的优先级进行处理。管理代理使用自身的handleMessage方法来处理收到的消息，它根据消息的不同类型采取不同的处理方式。此方法有2类返回值：一类是布尔变量，反映接收方是否正确地处理了消息；另一类返回值是返回一个对象，这个对象用于传递消息处理后的结果。

2 关键技术的研究和实现

2.1 基于MIB库的入侵检测策略分析

入侵检测系统(IDS)按所监测的对象分为以下几种[9]。

a. 基于主机的IDS：通过监视与分析主机的审计记录检测入侵。

b. 基于网络的IDS：通过在共享网段上侦听采集数据，分析可疑现象检测入侵。

c. 基于网关的IDS：从网关中提取相关信息，提供对整个信息基础设施的保护。

由此收集MIB中不同组的管理对象的值[10−11]，经过分析，对网络进行入侵检测。

2.1.1 非法IP地址检测

周期性地Ping本网段的所有IP地址，将所有Ping通的设备IP地址和数据库中已注册的合法IP地址进行比较，若发现某IP地址在数据库中未注册，则认为该设备非法(这里非法指的是有可能在没有身份认证的情况下对本网络进行访问，有潜在攻击的威胁)，此时向网络管理员报警。

2.1.2 非法路由检测

定时轮询IP地址组中ipRouteTable表，检查表中每一条记录的目的IP地址(ipRouteDest)和下一个路段的IP地址(ipRouteNextHop)，若2个对象的值和数据库中合法的路由信息(路由器IP和网关IP)不匹配，则说明网络的信息正向一个未经授权的IP地址传输，可认为该路由为非法路由。

2.1.3 源IP地址欺骗检测

网络管理站的数据库中存储着管理域范围内主机的MAC地址，安全检测模块定时轮询关键节点的MIB中表ipNetToMediaTable，得到的结果通过与数据库中的MAC地址比较，检查该设备是否进行了IP地址欺骗。

2.1.4 非法TCP连接检测

安全检测模块查询或定时轮询关键设备的MIB中的tcpConnTable表，检查表中tcpConnState状态为established或timeWait的表项，将这些表项的远端IP地址(tcpConnRemAddress)和管理站数据库中的授权IP地址进行比较，若有未经授权的IP地址，则此连接为非法TCP连接。

2.1.5 非法TCP/UDP端口使用检测

安全检测模块定时轮询关键设备的MIB的Tcp组的tcpConnTable表，检查表中每一条记录的tcpConnLocalPort的值,将其与数据库中网络允许使用的端口号(服务)进行匹配,若没有找到匹配的值，则说明网络不提供这种服务，该TCP端口为非法端口。非法UDP端口的检测是通过访问MIB的Udp组的udpTable表实现的，其原理和方法与检测TCP端口的相同。

2.2 MIB信息读取及数据库的设计

利用WinSNMP API来实现MIB信息的读取[11−12]。对于每次MIB信息读取，其实现的步骤为：

a. 用SnmpStartup函数打开WinSNMP应用程序；

b. 用SnmpOpen函数打开1个或多个WinSNMP会话；

c. 用SnmpRegister函数注册接收自陷或通知；

d. 用SnmpCreateVbl, SnmpDuplicateVbl, SnmpSetVb函数产生1个或多个变量绑定列表结合到1个PDU中；

e. 用SnmpSendMsg函数提交1个或多个SNMP操作请求；

f. 用SnmpRecvMsg函数检取SNMP操作请求的应答；

g. 使用应用程序特定逻辑处理请求应答；

h. 用SnmpClose函数关闭每一个WinSNMP会话；

i. 用SnmpCleanup函数关闭WinSNMP应用程序。

表 1 所示为存储 MIB 信息数据库的功能和结构。

表 1　数据库中表的作用及内容

Table 1　Function and content of table in database

	检测功能	关键字段内容
合法主机表	非法主机接入检测	允许接入网络的主机名
合法路由表	非法路由检测	合法的路由信息
IP/MAC 对照表	源 IP 地址欺骗检测	IP 地址及对应的 MAC 地址
合法 TCP/UDP 连接表	非法 TCP/UDP 连接检测	允许建立连接的远程 IP 地址
TCP/UDP 开放表	非法 TCP/UDP 端口占用检测	开放的端口及端口类型

从表 1 可以看出，在这个系统中，数据库相对简单，它的作用就是保存那些预先设定好、用于检测时从 MIB 库中获取的管理对象值。在设定数据库时，该数据库中的内容可以在结构设计时就设定好，也可以在系统应用时根据需要进行添加。但是，不管是什么时候设定好的数据，都必须合理，否则，会影响该入侵检测系统的作用。

2.3　基于遗传算法的调度Agent的实现

管理代理功能结构由多种 Agent 共同完成，如图 2 所示。

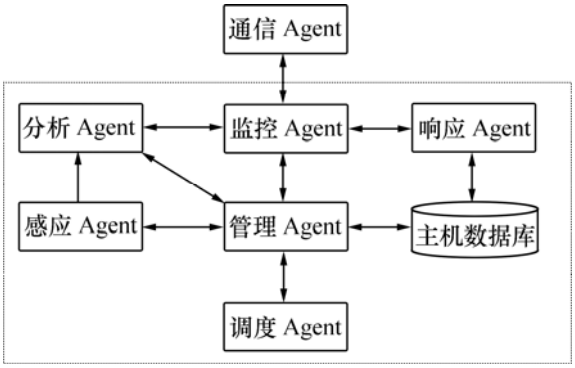

图 2　管理代理功能结构图

Fig.2　Function structure of management agent

监控 Agent 是控制中心，它管理和控制运行环境内的其他 Agent。同时，它也是对外的接口，接受 Server 的管理和指挥。管理 Agent 最主要的任务是维持一个注册表，表中记录了当前主机中 Agent 的基本信息[13]。响应 Agent 是系统针对检测到的入侵进行回应。调度 Agent 的主要作用是合理使用和分配移动 Agent，合理地给他们分派任务。它利用遗传算法实现 Agent 的调度[14−15]，其调度过程如下：当移动 Agent 向调度 Agent 发出请求时，调度 Agent 首先检测本机负载，本机负载度若大于阀值 α，则允许迁移。通过与其他网络上的机器通信，取得其负载度。采用二进制编码串来实现问题的编码，串的长度为网段中其他主机个数，即串的每一位对应网段中的 1 台主机。当串中某位值为 1 时，表示向此位置所对应的主机发送迁移请求；若该位值为 0，则不发送此请求。利用随机法产生多个串(具体数量由实现操作决定)，生成一个遗传操作的初始群体 Q。通过适应度函数计算初始群体中每个串的适应度，从而得到各串进入下一代的概率。对于概率最高的几个串采用最佳个体保存方法，直接进入下一代的群体。对其他个体串进行交叉变异操作，获取新的串。交叉操作是指把 2 个个体的部分结构加以替换重组而生成新的个体。而变异操作是指对群体中个体的某些基因或基因组进行一些变动。新串和保留的串组成新的群体后，重新计算群体中各串的适应度，直到得到一个最优串，此即为问题的解。将该结果发送给移动 Agent，让其知道要迁移的目标。

3　结　论

a. 系统底层采用协议分析和内存映射全面收集被监控系统的信息，检测信息高度结构化、标准化，能有效提高检测的效率和精确度。

b. 管理代理引入 MIB 库组件，使其具有很好的移植性、可扩展性。

c. 系统中实体采用 SNMPV3 协议进行通信，有效实现了自身的安全性。

d. 系统采用检测中心和管理代理结构，能有效进行分布式检测和全局性检测。

e. 系统中的每个收集器和分析器实体都能对数据进行处理，只是处理数据的能力不同。因此，在计算机设备上的开销不会很大，这符合IDS的一个基本设计原则。此外，收集器能在几乎没有监控的环境下工作，分析器能对历史数据进行进一步检测。

f. 系统由许多分布在整个网络中分散的管理代

理组成，所以，IDS不存在单点失效现象，可靠性高。

参考文献：

[1] Philip H. Integrated security and network management remain elusive[J]. Network Security, 2004, 10(6): 15−16.

[2] Frey J, Tannenbaum T, Livny M, et al. Condor-G: A computation management agent for multi-institutional grids[C]//The Tenth International Symposium on High Performance Distributed Computing. San Francisco: IEEE Press, 2001: 55−63.

[3] 王 军, 熊 伟, 肖德宝. 基于SNMP的入侵检测系统的设计与实现[J]. 计算机工程与应用, 2003, 39(17): 177−180.
WANG Jun, XIONG Wei, XIAO De-bao. Design and implementation of a SNMP-based intrusion detection system[J]. Computer Engineering and Applications, 2003, 39(17): 177−180.

[4] 康松林, 费洪晓, 施荣华. 网络应用软件监控系统监控模块的设计与实现[J]. 中南大学学报: 自然科学版, 2004, 35(6): 993−997.
KANG Song-lin, FEI Hong-xiao, SHI Rong-hua. Design and implementation of monitor module in net monitor system for application Software[J]. Journal of Central South University: Science and Technology, 2004, 35(6): 993−997.

[5] 康松林, 费洪晓, 施荣华. 网络应用软件监控系统监控信息传输的设计与实现[J]. 中南大学学报: 自然科学版, 2006, 37(2): 341−346.
KANG Song-lin, FEI Hong-xiao, SHI Rong-hua. Design and implementation of monitor message's transmission in net monitor system for application software[J]. Journal of Central South University: Science and Technology, 2006, 37(2): 341−346.

[6] 林立新, 蒋新华, 陈特放. 网络监控原理及实现[J]. 计算机工程, 2004, 30(7): 92−94.
LIN Li-xin, JIANG Xin-hua, CHEN Te-fang. Principle and realization of network monitoring[J]. Computer Engineering, 2004, 30(17): 92−94.

[7] 胡志刚, 阎朝坤. 基于网格的现代协同设计方法[J]. 中南大学学报: 自然科学版, 2004, 35(6): 988−992.
HU Zhi-gang, YAN Chao-kun. Research on modern collaborative design based on grid[J]. Journal of Central South University: Science and Technology, 2004, 35(6): 988−992.

[8] 陈旭东, 周华春. 基于注册服务的网络管理研究[J]. 计算机工程与应用, 2003, 39(9): 144−145.
CHEN Xu-dong, ZHOU Hua-chun. Network management study based on register service[J]. Computer Engineering and Applications, 2003, 39(9): 144−145.

[9] 唐亚哲, 陈传峰, 李增智. 基于结构反射的可扩充网管系统的设计与实现[J]. 小型微型计算机系统, 2003, 24(5): 859−862.
TANG Ya-zhe, CHEN Chuan-feng, LI Zeng-zhi. Design and implementation of an extensible network management system based on structural reflection[J]. Mini-Micro Systems, 2003, 24(5): 859−862.

[10] 刘 兰, 李之棠, 林 军. 安全网络管理MIB标准化研究[J]. 计算机工程与应用, 2004, 40(15): 151−153.
LIU Lan, LI Zhi-tang, LIN Jun. Research of standard secure network management MIB[J]. Computer Engineering and Applications, 2004, 40(15): 151−153.

[11] 俞承志, 王淑静, 宋瀚涛. 基于MIB-2网络安全入侵检测策略[J]. 北京理工大学学报, 2004, 24(8): 696−700.
YU Cheng-zhi, WANG Shu-jing, SONG Han-tao. Network intrusion detection strategies based on MIB-2[J]. Transactions of Beijing Institute of Technology, 2004, 24(8): 696−700.

[12] 杨海兰, 程 龙, 吴功宜. 基于SNMP进行数据挖掘的入侵检测系统研究[J]. 计算机工程, 2004, 30(2): 20−22.
YANG Hai-lan, CHENG Long, WU Gong-yi. Intrusion detection system based on SNMP data mining[J]. Computer Engineering, 2004, 30(2): 20−22.

[13] Comer D E, Stevens D L. 用 TCP/IP 进行网际互联. 2 卷: 设计、实现与内核[M]. 赵 刚, 林 瑶, 蒋 慧, 等译. 北京: 电子工业出版社, 2001.
Comer D E, Stevens D L. Internetworking with TCP/IP. Vol Ⅱ: Design, Implementation and Internals[M]. ZHANG Gang, LIN Yao, JIANG Hui, et al transl. Beijing: Electronics Industry Press, 2001.

[14] 费晓琪, 孟庆丰. Microsoft.Net 平台上用远程对象模型实现远程监测映像节点[J]. 计算机工程与应用, 2003, 39(7): 141−143.
FEI Xiao-qi, MENG Qing-feng. Implementation of remote monitoring node based on remote object model on the platform of Microsoft.Net[J]. Computer Engineering and Applications, 2003, 39(7): 141−143.

[15] 丁 柯, 金蓓弘. 通用网络编程接口包的设计和实现[J]. 小型微型计算机系统, 2003, 24(1): 5−9.
DING Ke, JIN Bei-hong. Design and implementation of wrapper for general network programming[J]. Mini-Micro Systems, 2003, 24(1): 5−9.