ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.13, No14, May 2017
E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

基于网格技术的分布式入侵检测系统

刘航宇[1],赵斐[2]

(1.中国石油天然气股份有限公司销售分公司,北京 100007;2.北京华虹集成电路设计有限责任公司,北京 100015)

摘要: 针对目前入侵检测系统中存在的误报率、检测率和高带宽通信量下的处理能力等问题,结合网格技术的应用背景,提出基于的网格的分布式入侵检测系统的应用模型。该文对其产生的原因、该系统的特点,该系统的应用平台、工作流程进行了详细的阐述。目的是在网格虚拟环境下实现高性能协同工作和资源共享的入侵检测系统,以解决常用入侵检测系统存在的一些问题,实现网络资源的全面共享,提高工作效率。

关键词: 网格技术;入侵检测系统;资源共享

中图分类号:TP309 文献标识码:A 文章编号:1009-3044(2017)14-0044-03

The Application and Research of DIDS Based on Grid

LIU Hang-yu[1], ZHAO Fei[2]

(1. Petrochina Marketing Company, Beijing 100007, China ; 2. Beijing Huahong IC Design Co., Ltd., Beijing 100015, China)

Abstract: To resolve the problems such as wrong report rate, measuring rate and handling capacity under the high bandwidth communication amount existing in the IDS at present, application background on it combine the grid, it propose on the basis of application model to DIDS based on grid. This paper set forth the procreant reason、the characteristic、the application of platform and work flow of the system on grid. The purpose is to realize the IDS based on grid with high-performanced resource-sharing and works in coordination under the fictitious environment, solve generally existing problem of the IDS, realize the overall sharing of the resources of the network, improve working efficiency.

Key words: Grid;IDS;resource share

DOI:10.14004/j.cnki.ckt.2017.1525

1 基于网格技术的入侵检测系统产生的原因

随着科学技术的发展,计算机已经走进了人们的生活,小到银行、超市,大到科技、国防。然而在这自动化、快节奏生活的背后也存在潜藏的问题。现如今,计算机入侵行为越来越猖獗。不管是对个人电脑还是对服务器,入侵次数越来越多,攻击手段也在不断升级,网络与信息安全也随之成为了社会关注的焦点。常用的入侵检测系统原理如下:在系统受到攻击时自动进行检测,同时发出警报通知系统管理员;在攻击已经发生的情况下与其他安全系统联动来消除入侵带来的隐患。但由于现有入侵检测系统分析方法的不足以及自身原始数据来源的缺陷,所面临的主要问题如下:

1) 现有入侵检测系统的检测手段主要依靠模式匹配方式,对模式库的组织模式、及时性、完整性有很高的要求,并且无法对未知攻击做出反馈;

2) 现有入侵检测系统的检测能力主要依赖单一节点的计算能力。随着网络带宽的迅速增长及网络规模的不断扩大,现有入侵检测系统的处理响应时间成为主要瓶颈,无法匹配对应的网络数据量从而造成漏报;

3) 网络入侵方式越来越多,攻击复杂性日趋加剧,也加重了现有入侵检测系统的误报、漏报现象。

随着互联网技术的迅速发展,网格技术也有了突飞猛进的进步。网格技术主要原理如下:将分散在不同地点的计算机通过互联网相联,使得所有资源能够整合为一个虚拟的计算能力。每一台计算机都是虚拟计算网络中的一个“节点”,不同地点的各个“节点”组成一张完整的“网格”。网格技术利用其松耦合的技术特点解决了现有系统中的技术异构、接口异构等问题[3],将网格内所有节点的处理能力结合在一起,提高了网格内不同节点间的自适应性、可扩展性以及智能性和交互性,为各种大数据应用提供了强大的处理能力。

随着网络入侵技术的发展,入侵检测技术也日趋分布化和动态化。为了应对日益分布化、协同化的网络攻击,更好的提升现有入侵检测系统在大数据量及大规模网络环境下的各项性能(例如智能性、实时性、交互性、主动性、自适应性、可扩展性等),本文提出一种基于网格技术的分布式入侵检测系统。

基于网格技术的分布式入侵检测系统工作原理如下:将本地计算机的检测任务分配给网格内其他节点,这些节点由分布式系统统一调度,协同监控网格内某些特定行为及动作。基于网格技术,能有效降低系统对网络共享数据量的需求,显著提

收稿日期:2017-04-13

作者简介:刘航宇(1983—),男,北京人,工程师,学士,主要研究方向为信息化;赵斐(1982—),男,北京人,工程师,硕士,主要研究方向为入侵检测。

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

高了系统的各项性能。

2 Globus网格体系结构

美国Argonne国家实验室联合多家研究机构研发了Globus[2],后续又与南加州大学信息科学学院(ISI)合作开发了基于此架构的Toolkit。随着多家计算机软硬件厂商(如IBM、Microsoft、Compaq、SGI、Sun、Fujitsu、Hitachi、NEC等)宣布支持Globus Toolkit,该网格体系已逐渐被认可,成为网格计算技术中的典型代表和实际规范。Globus Toolkit采用开放式架构和标准,为基于此技术构建的网格应用提供相应的安全、资源发现、资源管理、数据访问等服务。Globus的体系结构为五层沙漏结构,如图1所示。

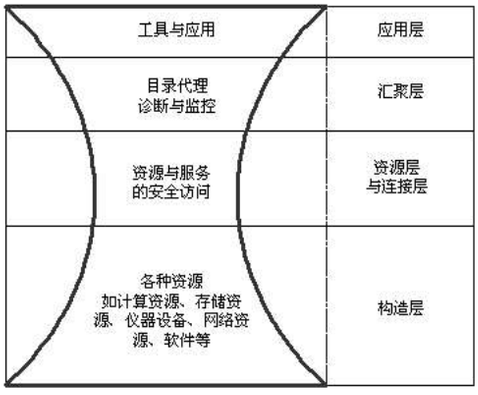

图1　五层沙漏结构

将Globus网格体系结构以协议为中心进行抽象,得到一个层次结构模型,即为五层沙漏结构。该体系结构通过协议建立一种协商共享机制。通过该协商共享机制,网格体系不但能够快速的进行节点间资源及数据共享,还能够方便快捷的实现节点间管理及新节点共享开发等任务。通过标准化的开放结构,　Globus网格体系能够提供更好的扩展性、互操作性、一致性以及代码共享服务。

因为各部分协议数量的分布不均匀,决定了五层沙漏结构的一个重要特点——沙漏形状。在Globus网格体系中,核心部分作为中间件层需要同时解决上层各种协议(沙漏的顶层)对核心部分的映射及核心部分对下层各种协议(沙漏的底层)的映射两个问题。为了解决各层间协议的映射问题,网格体系各层都需要支持核心部分协议;但是考虑到核心部分移植、升级的便捷性,核心部分协议的数量又必须足够精简。上诉原因使得核心协议成为了协议层次结构的瓶颈。

网格系统可以分为三个基本层次:资源层、中间件层和应用层。

网格资源层对应图中的构造层。构造层是构成网格系统的硬件基础,包括网格体系中的各种软硬件资源,例如计算机节点、网络设备、数据、各种应用软件等。网格资源层仅限于在物理层面实现网格体系内各节点间简单的互联互通,无法从本质上解决整个网格体系内各节点间逻辑层面的资源共享问题。为了能有效的整合各节点的计算资源,解决网格系统逻辑层面的资源共享问题,在网格资源层的基础上设计出网格中间件层。

网格中间件层对应图中的汇聚层、资源层及连接层。网格中间件层也称为网格操作系统(Grid Operating System),包括网格资源共享所需的各种工具及协议。网络中间件层通过整合网格资源层中各节点间分布、异构的计算资源向网格应用层提供了透明、统一的用户编程接口和环境,很好的解决了各层间协议的映射问题,为网格应用的开发工作提供了必要的支持。

网格应用层对应图中的应用层。应用层面向最终用户,所以能否在应用层方便快捷的解决用户面临的各种大型计算问题是衡量网格系统优劣的直观体现。最终用户在网格中间件层的支持下,使用其提供的工具或环境开发各种网格应用,实现具体需求。

3 基于网格技术的分布式入侵检测系统的特点

在Globus网格架构中所有计算机节点、网络数据、分布式软件、分布式系统等软硬件资源都是可共享的。网格技术通过基础的跨管理域、多样化、资源动态共享等功能特性,将所有共享资源整合成一个分布式的动态异构计算平台。基于网格技术的系统工作原理如下:根据需求自定义共享资源所需的各个接口,通过自定义接口动态调用网格中的所有资源,协同响应服务请求,完成大规模计算要求。因此基于网格技术的入侵检测系统具有如下的特点[1]:

分布性与共享性:分布性是网格技术最主要的特点。因为网格节点的特性决定了网格资源具有规模大,类型复杂,跨越地理范围广等特点,所以基于网格技术的入侵检测系统一定采用的是分布式计算。基于上述观点可以看出,网格技术的分布性还需要解决不同节点间的资源调度、任务协调分配、数据安全传输、操作人员与非本地系统互操作等诸多问题。网格资源虽然是分布的,同时也是共享的。共享性的定义非常宽泛,不仅指节点间简单的资源共享及任务协作,还指中间结果、数据库、专业模型库以及人才资源等方面的共享。解决分布式资源的共享问题是网格技术的最终目标,也是是网格技术的核心内容。

自相似性:自相似性大量存在于自然和社会现象中,是网格技术的一个重要特征。一般复杂系统通常都具有这种特征。

动态性与:动态性需要网格技术在规模、能力、兼容性等方面拥有极高的扩展性,能同时满足动态增加和动态减少两个方面的需求。同时网格资源是异构和多样的。网格系统必须能够解决不同体系结构的计算机系统和不同类别、不同结构的资源之间的通信和互操作问题。

4 基于网格技术的分布式入侵检测系统框架

遵照Globus网格系统的五层结构,同时考虑到入侵检测系统应用需求,基于网格技术的分布式入侵检测系统框架结构如图2所示。

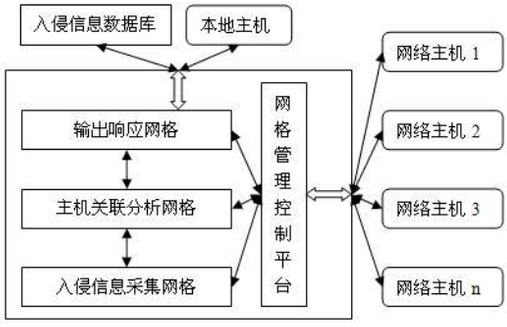

图2　基于网格技术的分布式入侵检测系统框架

基于网格技术的分布式入侵检测系统由以下四个部分组成:

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

入侵信息采集网格：入侵检测的第一步是数据采集，包括对网络、系统、数据以及应用活动状态及行为的实时跟踪和记录。在传统的入侵检测系统中，数据采集模块仅仅只监听所在网络的某些网段或某几台主机的网络数据，经过数据采集及预处理后得到网络、系统、数据以及应用活动的状态及行为的相关信息。在基于网格技术的入侵检测系统下，可用的带宽空间是无限的，所以能尽可能减少因为带宽问题而造成的数据丢失问题。入侵信息采集网格能够动态的协调整个网格内的资源，在网格系统中的若干不同关键点（不同网段和不同主机）收集信息。这种技术不但尽可能的扩大了检测范围，更重要的作用是从一个节点采集到的信息有可能看不出疑点，但是从几个不同节点采集到的信息的不一致性却是可疑行为或入侵的最好标识。

主机关联分析网格：该网格采用混合型入侵检测机制。基于网络的入侵检测系统侧重于精确地监视网络内的各种分布式活动，特别是原有系统检测的盲区；而基于主机的入侵检测系统局限于监视本节点系统内的各种活动。基于网格技术的分布式入侵检测系统既可以共享各个主机的特征数据库来解决误用检测中因为攻击数据库的不足而造成的漏报较多的问题，又可以利用网格强大的数据处理能力来解决异常检测中数据误报和高带宽通信量下数据处理能力不足的问题。

输出响应网格：输出响应网格是入侵检测系统的关键，是入侵检测系统的最终实现方式。现有的入侵检测系统很多还只是具有报警功能（被动响应），这远远未达到响应系统的要求。主动对抗响应是必不可少的。该网格同时采用主动响应和被动响应，对确定为攻击的活动采用主动响应模式，阻止正在进行的攻击，使得攻击者无法继续访问节点；对不能确定的活动采用被动响应模式。自动通知就是一种比较简单的被动响应模式，当检测到不确定活动发生时，被动响应模式直接向管理人员发出警报通知。这种响应比较简单，一般用于提高入侵检测系统效率及增加管理人员反应时间，无法阻止入侵行为。确定为入侵攻击的活动会写入入侵信息数据库，为以后的检测提供数据支持。

网格管理控制平台：该模块是入侵检测系统的集中控制管理单元，通过网格技术对系统内节点实行统一协调控制，使得后续加入的节点与网格内现有节点间实现了无缝互联互通和互操作，使得整个入侵检测系统能够发挥出最大功用[6]。

5 结束语

网格技术通过整合不同地点及网络内的计算资源，实现了一种可共享的经济、标准、可靠的计算能力。本文将网格技术与入侵检测系统相结合，对网络内发生的入侵行为采用分布式方法进行检测。与现有入侵检测系统相比，该方法对于检测DDOS攻击[5]等分布式攻击更加有效。传统的入侵检测系统主要基于单一的主机或网络，不同的主机或网络之间无法协同工作。本文基于网格技术增加了不同主机或网络之间独立入侵检测系统的协同工作能力，体现了入侵检测技术发展的趋势。

参考文献：

[1] Foster I,Kesselman C,Nick JM,etal.Grid Services for Distributed System Integration[J].Computer,2002,35(6).

[2] Ian Foster,Carl Kesselman.The Grid:Blueprint for a New Computing Infrastructure[M]. 北京:机械工业出版社,2005.

[3] 徐志伟,冯百明,李伟.网格计算技术[M].北京:电子工业出版社,2004.

[4] 戴英侠,连一峰,王航。系统安全与入侵检测[M]。北京：清华大学出版社,2002.

[5] Peng Ning,Jajodia S,Wang X S.Design and implementation of a decentralized prototype system for detecting distributed attacks[J].computer communications,2002(25).

[6] C Krugel,T Toth.Distributed pattern detection for intrusion detection[C].The Network and Distributed System Security Symposium Conf,SanDiego,CA,USA,2002.

[7] Comer D E.用TCP/IP进行网际互联(第1卷)[M].北京:电子工业出版社,2001.

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net