文章编号:1671-4598(2020)07-0029-05 DOI:10.16526/j.cnki.11—4762/tp.2020.07.007 中图分类号:TP393.08 文献标识码:A

基于 Agent 人工智能技术的分布式入侵检测系统设计

李 刚,孙耀文,于德新,付 海,赵邵蕾
(潜艇学院 教研保障中心,山东 青岛 266199)

摘要:针对当前动态加速技术(intel dynamic acceleration,IDA)系统中由于数据集中处理缺陷,影响系统入侵检测精准性的问题,提出了基于 Agent 人工智能技术的分布式入侵检测系统设计;在系统总体结构支持下,分析控制中心、网络主机、分区控制中心和 Agent 库;根据响应库中的响应规则采取对应的响应策略,利用通信模块及时判断入侵行为是否异常,使用 S5720S—28P—SI—AC 24 口全千兆三层网管企业级网络核心交换机,进行数据交换;选择 AD2032 型号的报警响应器,能够监视外来入侵行为;通过 V1.2 绿色电脑信息检测器,对系统内存和驱动磁盘进行全方位评估;分析主体通信的实现方式、通信消息格式和通信协议,设计以 Agent 为基础的数据移动过程;借助 Libpcap 库函数,设计入侵检测流程;设置攻击环境与参数,由系统调试结果可知,该系统最高检测精准度可达到 99%,为保证网络安全使用提供设备支持。

关键词:Agent 人工智能;分布式;入侵检测

Design of Distributed Intrusion Detection System Based on Agent Artificial Intelligence Technology

Li Gang, Sun Yaowen, Yu Dexin, Fu Hai, Zhao Shaolei
(Teaching and Research Guarantee Center, Submarine Academy, Qingdao 266199, China)

Abstract: For the current dynamic acceleration technology (Intel Dynamic Acceleration, IDA) system, due to defects in centralized data processing, the accuracy of system intrusion detection is affected. The design of distributed intrusion detection system based on Agent artificial intelligence technology is proposed. With the support of the overall structure of the system, the analysis control center, network host, partition control center and Agent library are analyzed. According to the response rules in the response library, the corresponding response strategy is adopted, and the communication module is used to timely determine whether the intrusion behavior is abnormal. The S5720S—28P—SI—AC 24—port full Gigabit Layer 3 network management enterprise—level network core switch is used for data exchange. Select AD2032 type alarm responder to be able to monitor the behavior of foreign intrusion. Through V1.2 green computer information detector, comprehensive evaluation of system memory and drive disk. Analyze the implementation method, communication message format and communication protocol of the subject, and design the data movement process based on Agent. With the help of Libpcap library function, design the intrusion detection process. Set the attack environment and parameters. According to the system debugging results, the highest detection accuracy of the system can reach 99%, and equipment support is provided to ensure the safe use of the network.

Keywords: Agent artificial intelligence; distributed; intrusion detection

0 引言

智能主体技术问世和发展为人工智能与网络技术融合的共生品,智能主体技术为一种新型的软件设计形式,拥有自主性、交互性以及移动性等特性,目前在人工智能、网络管理、网络安全和软件工程等领域得到了广泛的应用[1]。智能主体技术为包含除入侵检测之外,还有以网络为基础的分布式计算等领域提出了一个崭新的设计方案。所以,研究以智能主体技术为基础的分布式入侵检测的理论价值与实际应用具有重要作用[2]。

因为智能主体技术在入侵检测过程中具备使网络负载减弱,能够依靠异步方式自主运行,拥有天然的异构性以及应变能力很强等优势,众多机构与研究实验室都将其应用在入侵检测过程中。以往设计开发的 IDA 系统,IDA 凭借移动 Agent 对入侵者信息进行追踪以及采集收取[3]。借助 Agent 的移动性,IDA 灵活性很强,但集中处理数据会增加管理者的负担,与此同时,检测与响应入侵的实时性亦会受到影响,而且 Agent 在许多主机间移动,这造成安全管理产生了一些难题,对于智能主体在网络入侵检测时低效、安全性弱等难题,凭借研究许多 Agent 技术在以主机为基础的入侵检测系统、以网络为基石的入侵检测系统的应用,设计出以 Agent 人工智能技术为基础的分布式入侵检测系统。

1 系统总结架构设计

系统的物理拓扑网络中,防火墙、路由器、交换机、

收稿日期:2020-03-26; **修回日期**:2020-04-21。

作者简介:李 刚(1982-),男,山东青岛人,硕士,工程师,主要从事网络系统架构、人工智能方向的研究。

主机与服务器等构件与网络主机、分区控制中心、Agent 库以及控制中心共同构成了系统总体架构如图 1 所示。

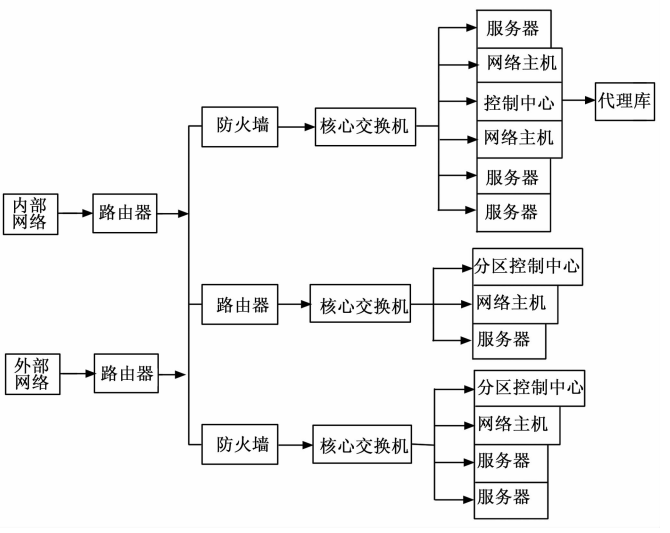

图 1 系统总体架构

各个模块描述如下：

针对控制中心协助问题，使用专业性较强的服务器控制中心，系统管理员能够凭借它完成全部规则集的更新任务[4]。

分区控制中心管制某区段网络、子网络的网络主机处理是它负责的任务，收到控制中心任务后，命令管辖的主机执行网络主机的上报信息接收任务，并且将诊断信息监测中的非正常情况，以入侵特征模式输入数据库之中，再将分析结果向控制中心进行上报[5-7]。

网络主机是可以为移动供给运行环境的移动代理平台，倘若网络主机优先处置疑似情况，然而自己却不能判断，那么就把有关数据向分区控制中心反馈，再进行更深层次的分析处理，来发现众多台主机入侵网络行为的有无[8]。

Agent 库在入侵检测系统过程中具有重要地位，尤其在执行操作中，控制中心直接管控管理部分，使其可产生的新配置能够依据实际需求执行相应工作，能够将原有的执行重新配置，删除不再需要的也可以实现[9]。

2 硬件结构

Agent 之间的通信借助消息传递的方式运行，系统中借助传递消息达成相互通信的目的。系统硬件结构如图 2 所示。

在图 2 中，中心 Agent 控制中心服务器，管控作用目的是管理、协调、控制、受检主机上的移动代理，接收移动代理的情况报告、获取报警信息，同时将下级不能判别的事情处理，响应入侵事件[10]。与此同时，控制中心还可显示人机交互界面，报告运行状态给管理人员、拉响警报，接收上级指令，改变运行状态，供给全部系统的 Agent 库，派遣、收回各节点的 Agent[11]。中心管理分析、处理，特征库作为后盾的条件下作用是将下层传送的数据执行综合

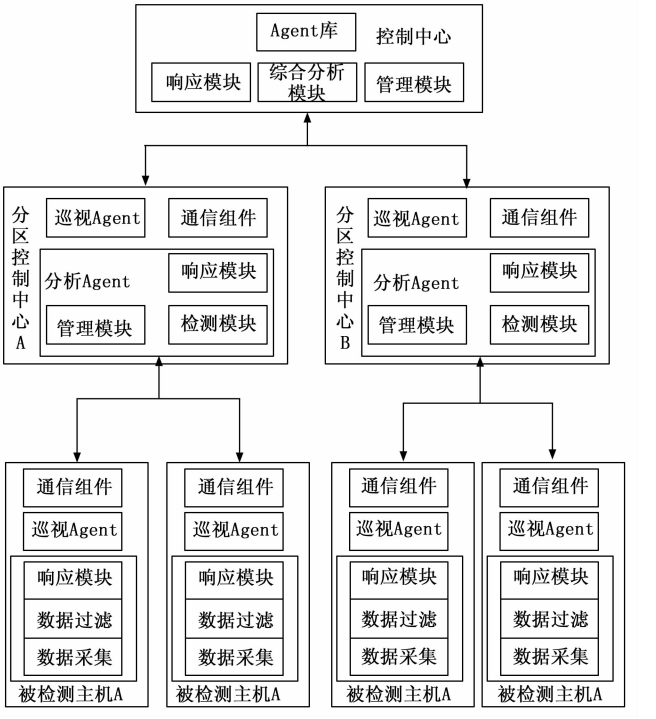

图 2 系统硬件结构

分析操作，响应库作为后盾的前提下对入侵行为反应，下层的移动 Agent 也由其管控。主机 Agent 运行监控中的主机上，通过采集系统、网络相关数据，可对其进行初步分析和过滤[12]。去除海量冗余数据，减少系统工作量。不同系统间层次是通信模块中扮演保护层的角色，借助各个层次实现数据高效传输与协调。

2.1 主机 Agent

主机 Agent 有探测器、存储、取出取控制库、规则库、响应库与通信模块，其结构如图 3 所示。

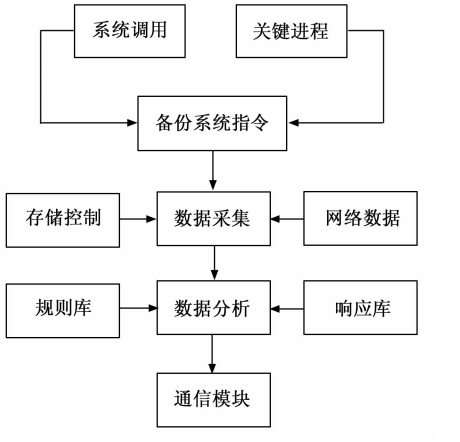

图 3 主机 Agent 结构

主机 Agent 结构主要工作机理如下所示：通过探测器进行数据采集时，应采取控制管控原则，在该原则获取主机数据[13]。将数据执行初步分析，把分析处理后的数据依照选取原则进行一一匹配，一旦匹配成功，则说明该行为

是入侵行为，具有一定危险性。依据响应规则采取对应策略，比如网络终端、预警等，将最终获取的数据传输给上级主机 Agent 之中[6]。如果不能判别此行为的正常与否，那么借助通信模块把数据传输给 Agent 作深层处理，每主机上可供多个主机 Agent 同时运行。

2.2　核心交换机

使用 S5720S－28P－SI－AC 24 口全千兆三层网管企业级网络核心交换机，各个接口示意图如图 4 所示。

图 4　核心交换机接口示意图

接入层指的是网络中用户直接连接或访问的网络层次，该层次及核心层次之间的部分为汇聚层。接入层主要功能就是将用户连接到终端网络之中，使用该交换机接口具有成本低、密度性高的优势[14]。

汇聚层作为交换机进行数据汇聚的中心层次，其作用是将接入层的数据进行高效处理，并将结果传输到上行链路中。

核心层是网络主干部分，该部分主要作用是对通信数据的高效转发，并将数据传输给骨干结构，既能提高核心交换机数据的吞吐量，又能保证系统可靠运行。

2.3　报警响应器

当系统出现报警调用图像时，选择 AD2032 型号的报警响应器，能够监视外来入侵行为。每台报警响应器都具有独立的 32 个继电器，每 16 个为一组，共两组，每组摄像机地址都是可以单独设置的。其报警器型号及设置如表 1 所示。

表 1　报警器型号及设置

报警器	A	B	C	D	E
1－15	0	0	0	0	0
16－30	0	0	0	0	1
31－45	0	0	0	1	0
46－60	0	0	0	1	1
0＝OFF;1＝ON					

2.4　信息检测器

使用 V1.2 绿色电脑信息检测器是一款轻量级电脑配置，如图 5 所示。

图 5　电脑信息检测器

电脑信息检测器能够详细显示电脑主机每个方面的信息，不仅具有协助超频，还能监测压力，并对系统内存和驱动磁盘进行全方位评估。

3　软件部分设计

因为分析 Agent 的操作对象与具体的主机分开，完全分离于所有操作系统，因此，分析的数据主要来源于各个主机 Agent，其重要功能是对主机 Agen 传输来的数据进行深入分析。

3.1　基于 Agent 移动分析

系统中智能主体之间通信机制如下所示。

1）主体通信的实现方式：

在 Agent 系统中智能主体间的通信是借助 Message 对象完成的，Agent 供应了如下消息处理方法，Send Message 和 send Oneway－Message 功能是发送消息，handle Message 的功能是对收到的消息进行处理，各个 Agent 均有一个消息队列用于存储收到的消息。

2）通信消息格式和通信协议：

Agent 系统中，应用 IDWG（互联网工程任务组的入侵检测工作组）设计制作的入侵检测消息交换格式（IDMEF）与入侵检测交换协议（IDXP）规范完成有关智能主体的通信机制。

①IDMEF 数据模型格式：

IDWG 应用以针对对象的方式对入侵检测的数据模型进行定义与设计，作用是对于不同检测组件间交互的各种各样的警报消息、控制命令以及配置信息等通信数据进行有关描述；应用以 XML 为基础的 ID－MEF 消息格式对此数据模型执行了形式化描述以及实现。

②IDXP 入侵检测交换协议：

Agent 系统中智能主体间的通信应用 IDXP，IDXP 协议为一个目的是对实体之间交互数据的应用层协议进行入侵检测，可以达到 IDMEF 消息、非结构文本和二进制数据在检测实体组件之间的交互的目的，与此同时面向对某些

安全特征进行连接，如协议之上的双方认证、完整性以及保密性等。

以 Agent 为基础的移动的移动过程图如图 6 所示。

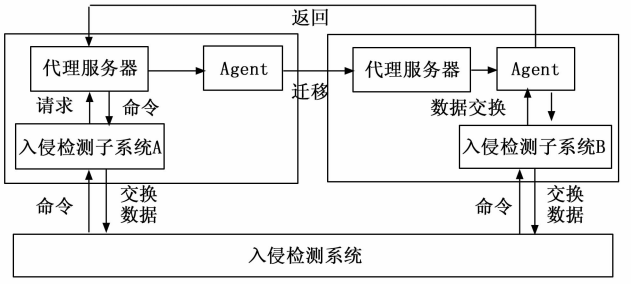

图 6 以 Agent 为基础的移动过程图

图 6 显示，入侵检测子系统 A 在检测出异常信息后，受到自身机体限制影响，导致其不能做出正确判断，为此，机器上的代理服务器将发出服务信号，直接委派多个代理模块进行信号处理。处理的结果将传输到入侵检测子系统 B 上，派出的代理与系统 B 直接进行相关执行操作，使异常信息得到快速处理，最终被派出的代理把处理后的结果信息运回主机 A，入侵检测子系统 A 紧接着供应对应的处理方法。

3.2 入侵检测流程设计

入侵检测系统开启之后，执行完初始化工作，解释口令，读取进系统的规则数据库，形成检测入侵的二维规则链表，之后执行循环抓包、规则匹配操作。入侵检测流程如图 7 所示。

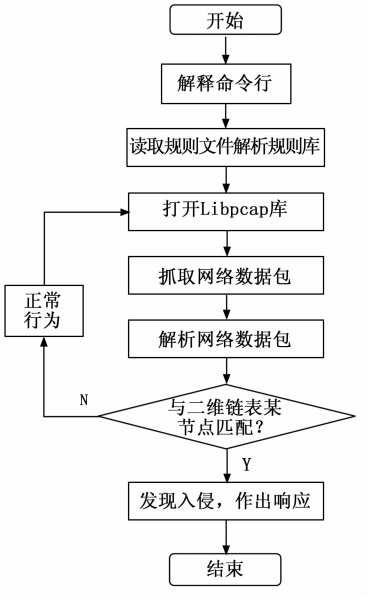

图 7 入侵检测流程

程序借助 Libpcap 库函数在网络中随机选取一个数据包，对数据包进行调用用于解析函数，依据数据包的类型以及位于的网络层次，协议解析数据包，包含数据链路层、网络层以及传输层。数据包解析成功之后，检测引擎会被自动触动，把解析完的数据包的数据以及依据规则数据库形成的二维规则链表执行依次对比操作。倘若匹配的规则条目被找到，该入侵行为成立被认为成立，依据规定的响应方式执行响应，在完成单个数据包的处理后，随机选取下一个数据包；倘若未发现匹配的规则条目，认定为正常行为，直接返回，处理下一个数据包。

4 系统调试

借助网络仿真软件 NS2 将系统性能执行仿真测试，按照不同的攻击次数，分开对系统的检测准确率以及系统 CPU 应用率进行考虑。在模拟入侵攻击方式时，应用 flooding 攻击，这是拒绝服务（DoS）的攻击方式之一，换而言之，即是发送非正常的数据包给目标节点。通常情况下根据 IDS 数据包的尺寸以及传送率的改变正常和非正常的数据包加以区分。以此调试基于 Agent 人工智能技术分布式入侵检测系统，验证其设计是否合理。

4.1 攻击环境与参数设置

目的是对文中所设计系统进行验证，在电子科技大学信息中心开发室执行了模拟的以网络为基础的入侵检测试验。因为条件的限制，试验环境只是在电子科技大学校园网内选定了 2 处位置安装 Aglet 平台来进行试验，如图 8 所示。

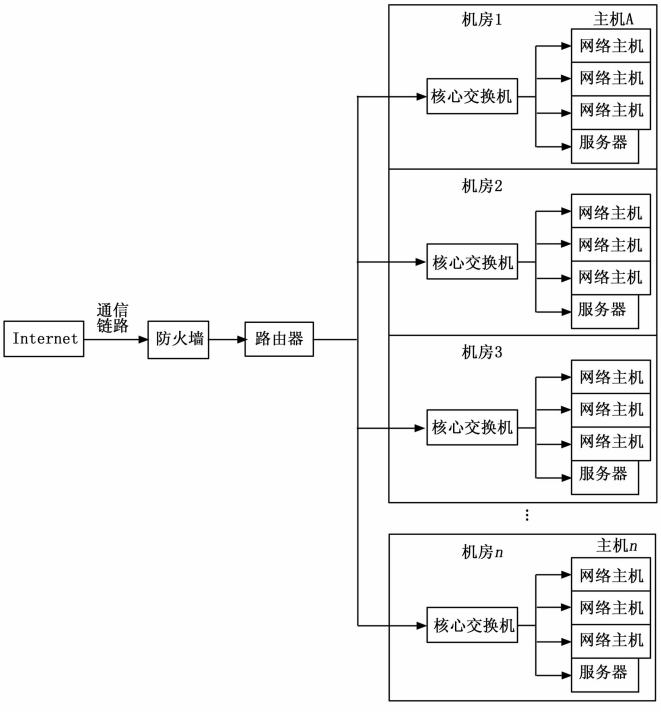

图 8 调试环境

机房 1 是实训楼的管控中心，1 台监控服务器与数台主机陈列于内；机房 2，机房 3 陈列在各楼层，各机房陈列 1 台服务器以及多台主机，服务器与主机借助交换机互联，每机房间路由器相互连接，校园网内部的 TCP/IP 网段的网络背景。该试验选定陈列于五楼的机房 2 与机房 3 和陈列在

六楼的机房 1 为布局环境，在机房 1 的主服务器上中心 Agent 与主控台的运行，在机房 2 与机房 3 的服务器 A 和服务器 B 上实现 Agent 运行、分析，选择三机房中的主机 A、主机 B，主机 C、主机 D 均为攻击主机，主机 E 是攻击发起机，主机 C 与主机 D 协助系统扩展性实验。

参数设置如表 2 所示。

表 2　参数设置

设备	参数
操作系统	Win8
IP	202.112.14.125
CPU 内存	512M
以太网卡	100Mbps

当攻击发起方向主机发送数据时，攻击发起机发送的数据包如表 3 所示。

表 3　攻击发起机发送的数据包

服务器和客户端连接：Socket[addr=/192.168.1.3]建立连接	
攻击发起机 1	1 个数据包
攻击发起机 2	2 个数据包
攻击发起机 3	3 个数据包
攻击发起机 4	4 个数据包
攻击发起机 5	5 个数据包
攻击发起机 6	6 个数据包
攻击发起机 7	7 个数据包
攻击发起机 8	8 个数据包
攻击发起机 9	9 个数据包
攻击发起机 10	10 个数据包
服务器关闭连接完成	

4.2　调试结果与分析

依据上述内容，对样本测试数据进行伪装入侵检测，数据采样序列在幅频表现如图 9 所示。

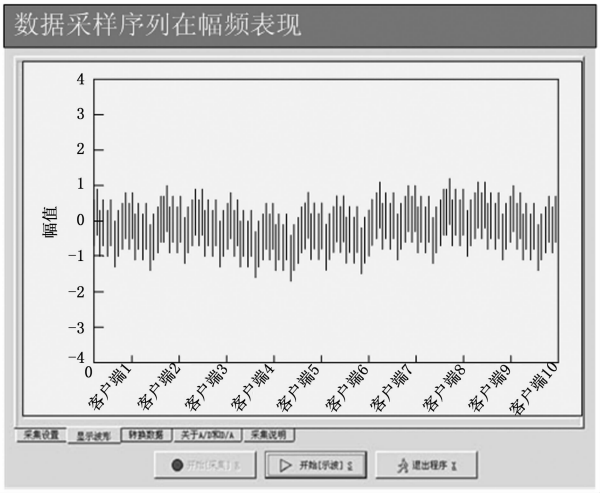

图 9　数据采样序列在幅频表现

由图 9 可知：数据采样序列在幅频率波动频率是具有规律性的，在 10 个客户端下，数据采样序列通常是在[－1，1] 范围内波动的，以此对入侵行为检测。

将 10 个客户端的 10 种发送的 TCP 数据包数目分为两类，一种是前 5 个客户端设为 S1，另一种是后 5 个客户端设为 S2。采用 IDA 系统和基于 Agent 系统对分布式入侵行为进行检测，检测结果如图 10 所示。

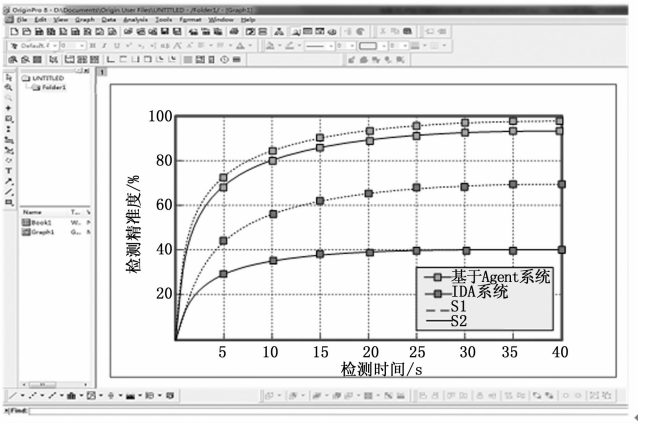

图 10　两种系统检测精准度对比分析

由图 10 可知：两种系统随着检测增加，检测精准度也随之改变。对于 IDA 系统，前 5 个客户端遭受入侵行为时，自身的检测功能能够及时检查异常情况，在检测时间为 40 s 时，检测精准度为 70%。而在后 5 个客户端遭受入侵行为时，自身的检测功能尚未完善，在检测时间为 25 s 时，检测精准度就不再升高，直到 40 s 时检测精准度一直保持 40%。

对于基于 Agent 系统前 5 个客户端遭受入侵行为时，检测精准度始终较高，最高可达到 99%。而在后 5 个客户端遭受入侵行为时，检测精准度最高可达到 95%。因此，采用该系统检测精准度较高。

综上所述：根据系统调试结果可证明基于 Agent 人工智能技术分布式入侵检测系统设计是具有合理的。

5　结束语

因为实际条件受限制，该文仅仅描述了网络环境下入侵检测系统，该系统本质较为复杂。分布式入侵检测系统诸多问题尚有待处理，移动代理运用载入侵检测中研究将持续进行，而检测算法的研究也并未休止。

在日后的工作实践以及研究中，如下工作需要进行：持续探讨研究移动代理的协作性以及智能性。把移动代理技术在入侵检测系统，能提升系统的动态迁移性和灵活性，但移动代理的协调工作以及智能性尚有待改善。该系统对移动代理之间的信息交互进行了初步的验证，尚且还未囊括多代理协调工作，代理的智能性无深层研究，事先规划移动路线，移动中不随实际需要变化。目的使系统对分布式环境大数据量的协调分析的适应性更强，完成移动代理的复杂的高级智能性、多代理的合作。

（下转第 38 页）