文章编号: 1001-0920(2008)08-0944-05

“软件人”群在入侵检测系统中的协调控制

马占飞[1,2], 郑雪峰[1], 曾广平[1], 涂序彦[1]
(1. 北京科技大学 信息工程学院, 北京 100083; 2. 内蒙古科技大学 包头师范学院, 内蒙古 包头 014030)

摘　要: 在深入研究大系统控制理论、人工智能和“软件人”智能检测技术的基础上,采用先进的分布式体系结构,提出一种基于“软件人”群(MSM)的智能入侵检测协商模型. 模型采取无控制中心的“软件人”群体结构,避免了单个中心分析器带来的单点失效问题. 每个数据采集部件、检测部件和分析部件都是独立的单元,不仅实现了数据采集的分布化,而且将入侵检测和实时响应分布化,提高了系统的健壮性,真正实现了分布式检测的思想.

关键词: 软件人; 入侵检测; 协调控制; 代理; 迁移; 信息推拉技术
中图分类号: TP393.08　　**文献标识码**: A

Multi-SoftMan coordination control in intrusion detection system

MA Zhan-fei[1,2], *ZHENG Xue-feng*[1], *ZENG Guang-ping*[1], *TU Xu-yan*[1]
(1. School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China; 2. Baotou Teachers College, Inner Mongolia University of Science and Technology, Baotou 014030, China. Correspondent: MA Zhan-fei, E-mail: mazhanfei@163.com)

Abstract: Through the study on large system cybernetics, artificial intelligence and SoftMan intelligent detection technology, a negotiation model of intelligent intrusion detection based on multi-SoftMan, which adoptes distributed architecture, is presented and researched deeply for network security systems. In order to reduce the relativity of each detection components as far as possible and avoid the simple point failure caused by the single central analyzer, the model adoptes the non-control center multi-SoftMan architecture. All the components in model, such as data collection units, intrusion detection and analysis units, are independent, which realizes the distributing data collection and the real-time detection and response. Finally the robustness of the system is enhanced, the distributing detection is realized.

Key words: SoftMan; Intrusion detection; Coordination control; Agent; Migration; Information push-pull technology

1 引　　言

随着对入侵检测系统(IDS)研究的深入,IDS 逐渐呈现出智能性和分布性的特点. 在最近 10 年中,入侵检测系统正走向这样一种结构:它们由一组分布式的监测器构成,在这个结构中每个监测器都负责本地的检测并为全局检测提供信息,如:DIDS[1], GrIDS[2], EMERALD[3]和 AAFID[4]等. 可以发现,它们都采取一种分布式数据采集和层次化的数据分析方式来对网域进行监控. 采用这种方式构造分布式入侵检测系统,结构简单、系统逻辑结构严谨. 但也有明显的不足,主要表现在两个方面:1) 集中分析构件承受的负载较高,可能会成为系统的瓶颈和单一失效点;2) 层次化的分析降低了系统的实时性.

针对上述问题,本文引入了“软件人”(SM)技术[5],并对传统的层次化结构的分布式入侵检测系统进行改进,旨在尽量避免巨大的网络数据传输开销、降低系统资源占用率、增强系统的健壮性、有效提高入侵检测效率,以及对入侵者的意图进行跟踪与预测等. 通常,“软件人”能够在网上自由迁移,采用“信息推拉技术”自动地处理某些指定的任务,充当一些特定角色(如网络通信“软件人”,数据采集“软件人”,入侵检测“软件人”,入侵分析“软件人”和入侵响应“软件人”等). 而“软件人”群(MSM)是指由多个“软件人”组成的系统,它是为了解决单个“软件人”不能解决的复杂问题,由多个“软件人”协调合作形成的自律分散系统[6]. 为了使“软件人”群之间

收稿日期: 2007-05-30; **修回日期**: 2007-07-24.
基金项目: 国家自然科学基金项目(60375038, 60503024); 北京市自然科学基金项目(4072018).
作者简介: 马占飞(1973—),男,内蒙古包头人,副教授,博士生,从事计算机网络技术与信息安全、人工智能的研究; 郑雪峰(1951—),男,福州人,教授,博士生导师,从事计算机网络技术与信息安全等研究.

能够合理高效地进行工作,各“软件人”之间采用协作、协调和协商机制.

2 “软件人”概述

2.1 “软件人”的定义

“软件人”是在 Agent(代理)、智能机器人、人工生命等技术基础上提出的一个新概念,是移动 Agent 的发展,它是具有拟人智能的、生存并活动于计算机网络世界中的一类软件人工生命,是一种“虚拟机器人”,具有拟人属性、拟人功能、拟人行为和拟人结构[7].

2.2 “软件人”的状态属性描述

“软件人”的状态属性包括:拟人属性、拟人功能、拟人行为和拟人结构,具体内容如下:

拟人属性 $A = \{A_{auto}, A_{acti}, A_{sens}, A_{reac}, A_{mobi}, A_{soci}\}$,即自主性、主动性、敏感性、反应性、机动性和社会性;

拟人功能 $F = \{F_L, F_O, F_W\}$,即学习功能、组织功能、工作功能;

拟人行为 $B = \{B_{adap}, B_{evol}, B_{gene}, B_{acti}\}$,即拟人适应、拟人进化、拟人繁殖和拟人活动.

拟人结构 $S = \{S_b, S_{so}, F_{eo}\}$,即软件人脑(思维、信息处理)、软件人感觉器官(感知和获取信息)、软件人效应器官(行为和信息利用).

“软件人”模型可用下列五元组表示:

$$SM = \{A, F, B, S, E\},$$

其中:A, F, B, S, E 均为集合(E 为环境因素集合),它们的元素是相应对象的集合. 如 F 中的 F_W 是 SM 的工作功能集合,$F_W = \{W_i \mid i = 1, 2, \cdots, N\}$,$N$ 即为 SM 定义和实现的工作功能数. 作为一个“活体”,“软件人”表现出来的是“行为”.“行为”的启动、延续和停止就是“软件人”在网络时空中的活动轨迹. 其状态 $V_i = \{[状态集合], 初态, [激发条件]\}$ 是刻画“软件人”活动的三要素,因此,“软件人”系统的活动状态模型可用如下六元组表示:

$$SM|_{act} = \{SM, V_i\} = \{A, F, B, S, E, V_i\}.$$

也就是说,“软件人”是具有生命特征的智体. 它具有拟人的智能特性,同时还应具有人类的某些特征,如知识、信念、意图、目的、承诺等心智状态以及遗传性、变异性、繁衍性和学习性等生理特征.“软件人”位于特定的环境中,具有高度的灵活性和自治性,它可以在目标的驱动下采取社交、学习等行为,对环境的变化做出主动反应并完成特定的任务.“软件人”可以用作网上“安全警察”、网上“垃圾清洁工”和网上“信息服务员”等.

2.3 “软件人”的科学基础

“软件人”的科学基础包括:分布式人工智能(DAI)、智能机器人(IR)、智能网络(IN)、人工生命(AL)和软件工程学(SE)等[8].

3 “软件人”体系结构

“软件人”是一个智能体,它具有分析问题与解决问题的能力. 因此,设计“软件人”最重要的内容就是设计其信息处理系统及执行系统.“软件人”具有自学习和自进化的能力,当其处于陌生环境或对待陌生事件时,能用以前积累的经验去解决,如果解决不了或效果很差时,则通过学习或联想记忆法去尝试其他方法,将最成功的方法记录并保存下来,而且可以遗传给子“软件人”.“软件人”体系结构如图 1 所示.

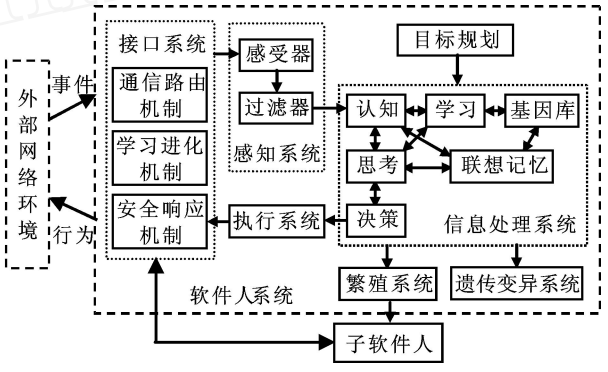

图 1 “软件人”体系结构

“软件人”的最外层接口系统由通信路由机制、安全响应机制、学习进化机制组成. 其中:通信路由部分是“软件人”与外界通信的中介,采用“软件人”通信的协议,保证使用相同通信语言的“软件人”和服务设施之间的正确通信,以及和其他“软件人”之间的协调、协商与协作,同时实现“软件人”的移动控制,并按照一定的路由策略决定“软件人”的移动路径,可以是静态路由也可以是动态路由;安全响应部分执行“软件人”的安全策略,阻止外界环境对“软件人”的非法访问,并对异常行为作出响应;学习进化部分是“软件人”区别于 Agent(包括移动 Agent,多 Agent)的关键所在,“软件人”通过以往积累(经验)的知识学习和修正自己的行为来适应环境,还可根据其当前的知识和经验,对未来进行预测.

感知系统包括感受器和过滤器,使“软件人”能够按照当前任务需求,滤除对当前行为需求没有用的、多余的感知信息. 当前任务需求有来自环境变化而产生的任务、指定的任务或其他“软件人”发来的消息任务等.

信息处理系统的任务是将感知到的信息进行处理,它是“软件人”的“大脑”,主要负责认知、学习、思维、联想记忆及决策等职能. 首先对感知到的

数据进行抽象加工,建立认知模型,采用联想记忆法来思考问题,从基因库中搜索模型方法,以决定采取何种策略.如果对感知到的数据无法建立认知模型,仍可通过联想记忆学习来建立,并将其存储到基因库中.基因库中存放"软件人"的基因(如源代码片段或规则)、方法、函数、认知模型等.信息处理过程在目标规划牵引下进行.

执行系统可以自主运行,感知外部环境的请求信息,并依据信息处理系统处理的结果产生动作,对环境产生一定的影响.

"软件人"可进行自复制,产生子"软件人",构成繁殖系统.子"软件人"承了"软件人"的所有特征,同时在其生命周期中通过在变化的环境中学习,以提高自己的适应能力和处理问题能力.

"软件人"自身具有遗传变异系统.基因库中拥有大量的基因,具有遗传效应,并储存遗传信息,可以准确地复制,遗传信息也能够发生突变."软件人"通过对基因复制和交叉使其形状的遗传得到选择和控制,同时通过基因重组和基因变异产生丰富的变异现象.

"软件人"具有拟人智能、拟人行为和功能,而且具有环境识别和自主决策能力及自由意志,同时还具有一定的数字生命特征,如自主性、学习进化能力、遗传性、变异性和情感等[9].

4 Multi-SoftMan 入侵检测体系结构

"软件人"集智能体与机器人的优势于一身,能在特定的环境下无须人工干预和监督从事各种管理、服务、监督等工作.由于其具有生命特征,可以根据需要进行自繁殖、自学习、自进化,也可以随环境的变化而改进其功能,具有很强的自适应性、智能性和协作性."软件人"既能独立地完成自己的工作,又能与其他"软件人"协作共同完成某项任务,而且"软件人"还能够接受控制,并能感知环境的变化而影响环境.因此,将"软件人"群引入大规模分布式入侵检测与防御系统中,为解决现有入侵检测系统提供了一个全新的思路.鉴于此,本文提出了基于"软件人"群的入侵检测系统(MSMIDS)模型,该模型综合了层次模型和协作模型的优点,具有较强的智能性.MSMIDS 采取无控制中心的分布式"软件人"群体结构,充分利用"软件人"本身的独立性与自主性,尽量降低各检测部件间的相关性.各个数据采集部件、检测和分析部件都是独立的单元.不仅实现了数据收集的分布化,而且将入侵检测和实时响应分布化,真正实现了分布式检测与防御的思想[10-12].

4.1 MSMIDS 集成模型

MSMIDS 模型以自治"软件人"为组织单元,主要有 4 类自治"软件人":网络通信"软件人"(NCSM)、数据采集"软件人"(DCSM)、入侵检测"软件人"(IDSM)和入侵分析"软件人"(IASM).如图 2 所示.

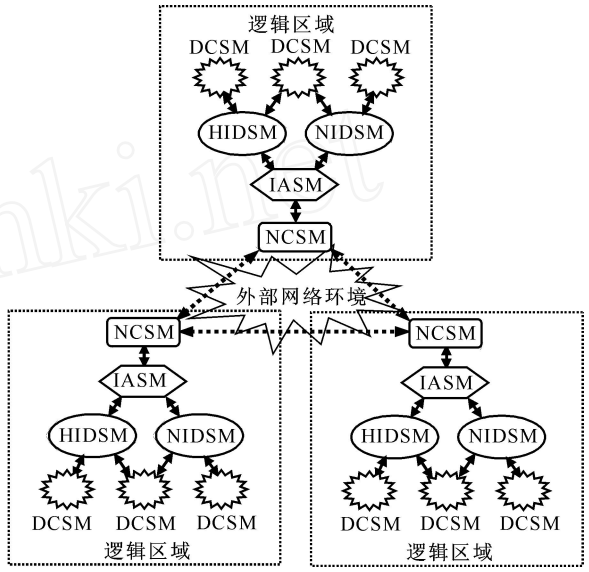

图 2 Multi-SoftMan 入侵检测系统逻辑模型

4.1.1 网络通信"软件人"(NCSM)

NCSM 主要帮助自治"软件人"在各个平台之间自主移动,执行、访问相关服务以及与其他"软件人"进行本地或异地交互,执行安全策略,并完成和其他"软件人"之间的协调、协商与协作.

4.1.2 数据采集"软件人"(DCSM)

DCSM 是专门用于采集数据的"软件人".它可以位于网络中任何一台需要检测的主机上,同一台主机上也可以同时部署多个相同或不同类型的 DCSM.DCSM 采集的数据包括主机的审计记录、应用程序日志、应用程序调用序列和网络流量等,因此容易实现数据源的异构.当 DCSM 与 IDSM 不在同一机器上时,会带来检测数据的网络传输问题.为了减小网络流量,减轻 IDSM 负担,DCSM 要对原始数据进行必要的预处理,包括数据的过滤、格式化、提取及分析.完成预处理后,DCSM 将数据传送给等待其服务的一个或多个 IDSM.

4.1.3 入侵检测"软件人"(IDSM)

IDSM 是专门用于检测的"软件人",是本模型的基本检测单元.每个 IDSM 独立承担一定的检测任务,负责检测系统或网络某一方面的安全问题.根据检测任务与环境的不同,IDSM 采用不同的检测技术和方法,对用户的异常或可疑行为进行检测.在模型中,不同类型的 IDSM 可以有相同的数据源,以

实现检测方法的互补,从而提高检测率. DCSM, IDSM 与 IASM 可以位于同一个主机上,也可以位于不同的主机上,IDSM 需要把检测到的事件向 IASM 汇报.

根据 IDSM 所处理的数据源的不同,可将 IDSM 分为两大类:基于主机的 IDSM(HIDSM) 和基于网络的 IDSM(NIDSM).

4.1.4　入侵分析“软件人”(IASM)

IASM 是用于分析和响应的“软件人”. 每个检测区域内包含一个唯一的 IASM. IASM 与 IDSM 之间是一种层次型的从属关系,IDSM 负责检测安全事件,并向所属的 IASM 汇报,IASM 对 IDSM 上报的信息进行聚合分析. 各个检测区域中的 IASM 处于平等地位,是一种协作关系,可以进行交互以完成检测任务,包括请求协查、通报协查结果以及对异常事件作出响应等.

4.2　MSMIDS 中各“软件人”间的协调控制

由于“软件人”具有移动的特性,各“软件人”可以位于不同的网络或主机上. 由于网络的动态性和不确定性,以及存在网络传输中的延迟,过多地依赖通讯来完成“软件人”群的协调一致会出现很多困难,在“软件人”系统中不宜采取完全集中的控制方式,而应采取分散控制的方式,它具有以下特点:

1) “软件人”对自身进行控制以达到自身的平衡稳定;

2) “软件人”之间能够相互感知和通信,以便快速及时地进行交互;

3) “软件人”对于整个系统的全局状态在结构上是不可直接观测和控制的,但它们能够感知外界环境,并动态地修改或调整系统变量和参数以协调系统的平衡.

4.3　MSMIDS 协调控制的策略

当“软件人”群系统采用分散弹性控制方式时,由于没有上级协调器,各“软件人”只能通过各自对外界环境的感知及信息交换来自发地调节和控制自身的行为,并按照其目的和需求采取行动,动态地协调系统的平衡. 为此,“软件人”之间的协调控制采用部分 —全局规划(PGP) 策略,它是一种典型的分布式协商技术,其特点是每个“软件人”都能收集目前的状态,又能收集其他“软件人”的目标信息. 因此,PGP 提供了“软件人”之间的灵活协调,保证了各“软件人”之间的交互. PGP 通过不同局部计划间的交互,可以避免“软件人”之间的任务冗余,特别是当多个“软件人”计划具有相同的中间目标时会发出告警通知. 每个“软件人”都维护自身的 PGP,独立且异步地使用 PGP 来协调各自的行为,从而实现全局任务.

5　Multi-SoftMan 在 IDS 中的强大优势

“软件人”的自治性、移动性、智能性、协作性等特性为解决传统 IDS 中存在的问题提供了条件. 将“软件人”技术应用于 IDS 具有以下优势:

1) 降低网络负载. 以往的 IDS,大多是分散收集各种数据源,将这些原始数据按照一定的格式作本地处理,再交由控制中心分析是否有异常出现,这样就会产生相当大的网络负载.“软件人”系统的特征是将计算移往数据,而不是将数据移往计算. 只需派遣“软件人”在主机上直接对数据进行分析处理,从而大大降低了网络负载.

2) 负载平衡. 如果在某一个中心节点分析数据包,将会大大增加该中心节点的计算工作量,是 IDS 的一个瓶颈,效率降低,检测处理时间增多. 而应用“软件人”技术可将较大的计算工作分布在多个处理器上并行执行,从而避免了瓶颈问题的出现.

3) 动态可扩展性. 一个高效的 IDS 必须具有可扩展性,跟踪入侵方法和入侵技术,及时扩充对应的检测技术.“软件人”是自治的,在一定程序上是松散捆绑的,虽然句柄之间有一定的联系,但它们之间是可以相互独立操作的. 因此,即使系统很复杂,在不影响其他“软件人”正常工作的情况下,单个功能模块也能够被删除、更改,甚至改进. 可见,这种系统也内涵一种容错机制.

4) 克服网络延时. 当某个检测节点需要对一个网络事件进行响应时(比如详细记录一个连接的通讯情况,或是对某个攻击进行阻断),检测模块无需和远端的中央服务器进行通讯,而是通过驻留在该节点的“软件人”来完成相应操作,缩短了响应时间.

5) 计算的异步性和自治性. 传统的入侵检测体系结构需要在中央服务器和检测模块之间建立一个可靠的连接,这使得系统很容易受到攻击. 如果中央服务器受到攻击,整个系统将处于单点失效状态. 基于分布式的“软件人”群框架允许 IDS 在通信连接中断或者中央服务器暂时失效的情况下继续工作,这是由“软件人”自主性的特征决定的.

6) 平台无关性.“软件人”平台允许“软件人”在异构的环境中移动,这就允许各个不同区域的 IDS 之间通过“软件人”迁移实现数据共享.

7) 动态适应性.“软件人”使得系统能够进行安全策略的动态配置. 这种动态配置通过向那些正受到攻击的主机派遣一些特定的“软件人”来完成,这些“软件人”能够修改主机的安全策略(比如限制某个用户的登录等).

8) 静态适应性. 对于一个 IDS 来说,维护攻击特征库以及检测算法的及时更新是非常重要的. 采用"软件人"技术可以避免在系统进行攻击特征库或是检测算法更新时必须重新启动整个 IDS,仅仅需要激活一个更新"软件人"并将它派遣到各个检测模块即可实现特征库和算法更新.

由此可见在入侵检测领域,"软件人"技术有着其他技术所不可比拟的优势.

6 结 论

本文通过对现有网络入侵检测系统、人工智能和"软件人"技术的深入研究,提出了基于"软件人"群的分布式入侵检测系统协调控制模型. 该模型充分利用各个"软件人"之间相互协作却又相互独立的特性,使系统结构具有很好的伸缩性、灵活性、扩展性、容错能力、分布式控制和攻击预防能力等. 它有效地解决了传统入侵检测技术对异构系统和大规模高速网络检测的明显不足以及不同的入侵检测系统之间不能协同工作等问题. 随着研究的深入,基于"软件人"群的分布式入侵检测系统会得到不断的完善,它的应用也将更为广泛.

参考文献(References)

[1] Snapp S, Brentano J, Dias G, et al. DIDS (distributed intrusion detection system) —Motivation, architecture, and an early prototype[C]. Proc of the 14th National Computer Security Conf. Washington, 1999: 67-76.

[2] Chen S S, Cheung S, Crawford R, et al. GrIDS-A graph-based intrusion detection system for large networks[C]. The 19th National Information Systems Security Conf. Baltimore, 1996: 361-370.

[3] Porras P A, Neumann P G. Event monitoring enabling responses to anomalous live disturbances[C]. Proc of the 20th National Information Systems Security Conf. Maryland, 1997: 353-365.

[4] Spafford E, Zamboni D. Intrusion detection using autonomous agents[J]. Computer Networks, 2000, 34 (4): 547-570.

[5] 曾广平, 涂序彦. 软件人[C]. 中国人工智能学会第 10 届全国学术年会论文集. 北京:北京邮电大学出版社, 2003: 677-682.
(Zeng G P, Tu X Y. SoftMan[C]. Proc of the 10th CAAI National Conf. Beijing: Beijing University of Posts and Telecommunications Publishing House, 2003: 677-682.)

[6] Tu Xuyan, Zeng Guangping, Tang Tao. Humanized autonomous decentralized systems[C]. Proc of the Int Symposium on Autonomous Decentralized Systems. Sichuan, 2005: 593-598.

[7] Lu Qingling, Zeng Guangping, Zhang Wei, et al. SoftMan and agent [C]. Proc of the Int Conf on Networking, Sensing and Control. Tucson, 2005: 904-907.

[8] Ma Zhonggui, Ye Bin, Ban Xiaojuan, et al. The study on model and architecture of SoftMan group based on intelligent autonomous decentralized systems[C]. Proc of the Int Conf on Autonomous Decentralized Systems. Chengdu, 2005: 641-646.

[9] Pang Jie, Ning Shurong, Li Guizhi, et al. Research on scheduling in multi-SoftMan system with the learning mode based on genetic algorithms[C]. Proc of the Int Con on Networking, Sensing and Control. Lauderdale, 2006: 1026-1029.

[10] Zaki M, Tarek S Sobh. Attack abstraction using a multiagent system for intrusion detection[J]. J of Intelligent & Fuzzy Systems, 2005, 16: 141-150.

[11] Dasgupta D, Gonzalez F, Yallapu K, et al. An agent-based intrusion detection system[J]. Computers & Security, 2005, 24: 387-398.

[12] Azzedine B, Renato B M, Kathia R L, et al. An agent-based and biological inspired real-time intrusion detection and security model for computer network operations[J]. Computer Communications, 2007, 1: 1-14.