Multi-SoftMan 入侵防御系统模型的智能弹性架构*)

马占飞[1,2] 郑雪峰[1] 曾广平[1] 涂序彦[1]

(北京科技大学信息工程学院 北京 100083)[1] (内蒙古科技大学包头师范学院 包头 014030)[2]

摘 要 "软件人"(SoftMan,SM)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,它为解决当前网络入侵检测中存在的诸多问题提供了新的思路。本文在深入研究入侵检测与防护技术的基础上,受"软件人"技术的启示,提出了基于群体"软件人"(Multi-SoftMan,MSM)入侵防御系统的智能协商控制模型及相应的算法。模型采取无控制中心的群体"软件人"结构,充分利用"软件人"本身的独立性、自主性、自学习、自适性、遗传和变异等特性,尽量降低各检测部件间的相关性,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,这有助于解决目前入侵检测系统普遍存在的智能化程度不高、系统不易维护、检测效率低下等问题。

关键词 群体"软件人",入侵检测,入侵防御,协商控制,智能弹性架构,代理

Intelligent Resilient Framework of Multi-SoftMan Intrusion Prevention System Model

MA Zhan-fei[1,2] ZHENG Xue-feng[1] ZENG Guang-ping[1] TU Xu-yan[1]

(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]

(Baotou Teachers College, Inner Mongolia University of Science and Technology, Inner Mongolia Baotou 014030, China)[2]

Abstract "SoftMan" is a new concept based on production of distributed technique, agent, intelligent robot and artificial life, and its corresponding theory and technology fruits provide a good foundation and reference for studying the present intrusion detection systems (IDS). Inspired by the intelligence recognition capability of "SoftMan", a novel Multi-SoftMan intrusion prevention system (MSMIPS) negotiation control model and relevant algorithm are presented and researched deeply for network security systems, which model is adopted distributed intelligence architecture. 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 is adopted the non-control center Multi-SoftMan architecture, which is used to "SoftMan" attributes, such as independence, activity, self-learning, self-adaptation, inheritance and variation, and so on. All of the components in model, such as data collection units, intrusion detection and analysis units, are independent, which has realized successfully the distributing data collection and the real-time detection and response. Therefore, the robustness of the system is enhancing, the distributing detection idea is realized really, and helps to improve intrusion detection efficiency, intelligentization and maintainability.

Keywords Multi-softman, Intrusion detection, Intrusion prevention, Negotiation control, Intelligent resilient framework, Agent

1 引言

入侵检测是指通过从计算机系统或网络中的若干关键点收集并分析信息,从中发现系统或网络中是否有遭到攻击的迹象并作出响应。根据采用检测技术的不同可以分为基于误用的入侵检测和基于异常的入侵检测。早期的开发主要集中在对单机入侵检测系统(intrusion detection system,IDS)的检测技术研究。网络技术的进步为黑客技术的发展提供了条件,出现了分布式攻击、典型的拒绝服务(Denial-of-Service,DoS)攻击和在其上演变而成的分布式拒绝服务(Distributed Denial-of-Service,DDoS)攻击,它们都是通过向网络发送海量数据包,消耗系统资源,导致系统无法对合法用户提供正常的服务,进而使整个网络瘫痪。单机入侵检测系统已经不能有效防范这种攻击。于是,研究人员开始对分布式入侵检测系统进行研究和开发。分布式入侵检测系统通过分布采集、协同工作的方式,彼此交互网络信息,进行关联分析,从而达到检测分布式攻击的目的。目前已经开发出来的典型分布式入侵检测系统有:(1)美国加州大学 Davis 分校于 20 世纪 90 年代提出来的 DIDS(Distributed Intrusion Detection System)[1],该系统采用分布采集、集中处理的方式,所有采集到的网络或主机数据将被传送到中心节点集中处理,判断是否存在攻击行为,这时导致中心处理节点可能会成为系统瓶颈,在出现大量攻击时存在失效的威胁。(2)为了克服 DIDS 集中分析的缺点,美国 Texas A&M 大学于 1996 年提出了 CSM

*)国家自然科学基金(60375038, 60503024);北京市自然科学基金(4072018)。**马占飞** 副教授,博士生,主要研究方向为计算机网络技术与信息安全、人工智能;**郑雪峰** 教授,博士生导师,主要研究方向为计算机网络技术与信息安全;**曾广平** 教授,博士生导师,研究方向为计算机软件、网络与人工智能;**涂序彦** 教授,博士生导师,研究方向为人工智能、人工生命、大系统控制等。

(Cooperating Security Managers)系统[2]。该系统采用对等体来组织系统,每个CSM就是一个入侵检测系统,各CSM之间通过交换信息来合作检测分布式入侵。但是,该系统在CSM数量大的情况下存在交互信息量大和综合判断能力不强的问题。(3)由日本IPA(Information Technology Promotion Agency)开发的IDA(Intrusion Detection Agent System)[3]是一个多主机检测系统,该系统采用两层的系统框架,其最大特点就是采用移动代理技术自动收集信息。但是,该系统只定义了某类特定事件,因此只适用于检测某一类分布式入侵,扩展性不强。(4)在国内,对于分布式入侵检测系统的研究也有了一定的成果,如大规模分布式入侵检测系统(Large-scale Distributed Intrusion Detection System, LDIDS)[4]采用分布采集、动态协调、集中管理的思想,采用树型的分层体系结构设计了一种大规模的分布式入侵检测系统。该系统具有很大的灵活性和可扩展性。但是,这些传统的分布式入侵检测系统由于处理数据量大且集中,负载不均衡,从而导致系统整体处理速率较慢,不能满足实时处理的要求。

"软件人"(SoftMan,SM)技术[5]的提出为入侵检测系统提供了新的研究思路,并成为计算机网络入侵检测与防御领域的一个新的研究亮点。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)。而群体"软件人"(Multi-SoftMan,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"不能够解决的复杂问题,由多个"软件人"协调合作形成的自律分散系统[6]。为了使群体"软件人"之间能够合理高效地进行工作,各"软件人"之间采用协作、协调、协商机制。因此,本文采用群体"软件人"的方法研究和探索大规模高速网络的入侵检测与防御,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,实现分布式的检测和负载均衡,有效地提高入侵检测效率。

本文第2节介绍"软件人"的基本概念、状态描述和科学基础;第3节分析"软件人"的体系结构及工作机理;第4节构建基于Multi-SoftMan入侵防御系统的智能协商控制模型及相应的算法,并对其进行详尽的分析和论述;最后总结我们的研究工作,并且指出了未来的研究方向和基本思路。

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[5]。

2.2 "软件人"的状态属性描述

软件人的状态属性: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、机动性和社会性等;

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

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等。

拟人结构 $S=\{S_b,S_w,F_w\}$,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)等。

"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,$F_W=\{W_i \mid i=1,2,3,\cdots,N\}$,$N$ 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导出的六元组表示:

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

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,同时应具人类的某些特征,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的反应并且完成特定的任务。"软件人"还可以充当网上"安全警察"、网上"垃圾清洁工"、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(Distributed Artificial Intelligence,DAI)、智能机器人(Intelligent Robot,IR)、智能网络(Intelligent Net,INet)、广义人工生命(Generalized Artificial Life,GAL)和软件技术与软件工程学(Software Technology and Engineering)等。

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、自进化能力,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,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。

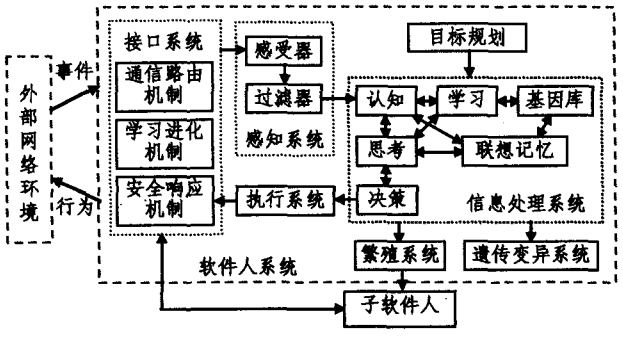

图1 "软件人"体系结构

"软件人"的最外层接口系统是由通信路由机制、安全响应机制、学习进化机制组成。其中,通信与路由部分是"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，并且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)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的变化，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、联想记忆以及决策等职能。它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，并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”，因而构成繁殖系统。子“软件人”继承了“软件人”的所有特征，同时在其生命周期中可以通过在变化的环境中学习，以提高自己的适应能力、处理问题的能力。

“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、基因变异产生丰富的变异现象。

因此，“软件人”具有拟人智能、拟人行为和功能，而且具有环境识别、自由意志以及自主决策能力。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[7]。

4 Multi-SoftMan 入侵防御系统的体系结构及分析

“软件人”是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、服务和监控等工作。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”群引入到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，我们提出了基于群体“软件人”入侵防御系统(Multi-SoftMan Intrusion Prevention System，MSMIPS)的智能协商控制模型，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。MSMIPS 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[8-11]。

4.1 MSMIPS 智能协商控制模型

MSMIPS 模型以自治“软件人”为组织单元，主要有 5 类自治“软件人”：通信路由“软件人”(Communication Route SoftMan，CRSM)、数据采集“软件人”(Data Collection SoftMan，DCSM)、入侵检测“软件人”(Intrusion Detection SoftMan，IDSM)、入侵分析“软件人”(Intrusion Analyse SoftMan，IASM)和安全防御“软件人”(Security Prevention SoftMan，SPSM)。如图 2 所示。

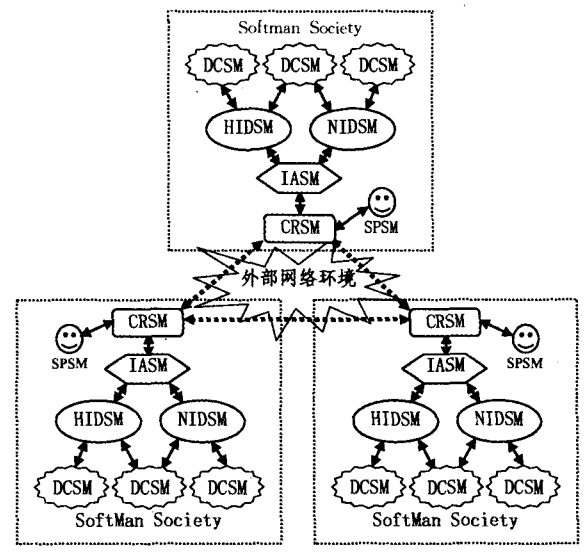

图 2 Multi-SoftMan 入侵防御系统的智能协商控制模型

4.1.1 通信路由“软件人”(CRSM)

CRSM 是“软件人”与外界通信的中介，采用“软件人”的通信协议，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；CRSM 能够实现自治“软件人”之间在各个平台之间自主移动，并根据当前网络负载和服务器负载等外界环境，按照一定的路由策略规划出“软件人”的迁移路径；同时，CRSM 也能够执行、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，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 是专门用于数据采集的“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。如 DCSM 与 IDSM 不在同一机器上，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 独立地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。IDSM 分布在各个网络节点和通讯设备中，并时刻保持警戒状态。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，对网络运行环

境变化、数据包发送情况、异常或可疑行为进行实时检测；同时要与特定意图(如查找功能失常、缺陷、异常等)的设备进行通信，以监视不同层次上的多个参数。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，从而提高检测效率。DCSM、IDSM与IASM可以位于同一台主机上，也可以位于不同的主机上，IDSM需要把检测到的可疑或异常信息向本地IASM汇报。

根据IDSM所处理的数据源不同，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是对入侵事件进行分析、响应的"软件人"。每个检测区域内包含一个唯一的IASM，每个IASM独立承担一定的事件分析任务，并负责系统或网络某一方面的安全问题。IASM与IDSM之间是一种层次型的从属关系，IDSM负责检测可疑或异常行为，并向所属的IASM汇报，IASM则对IDSM上报的事件进行聚合分析，并依据基因库的规则对入侵事件做出相应的防御措施。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行为作出响应等。

4.1.5 安全防御"软件人"(SPSM)

SPSM是专门进行自身保护和验证的"软件人"。它能够防止外部环境对本区域内部"软件人"的非法访问，以保证数据的正确性和合法性；也能完成对数据的加密/解密、数字签名等任务；同时定时检查本主机和相邻主机的CRSM以及本主机或网段内的IASM的状态，并向系统管理员报告异常。另外，由它提供用户接口，用户可以通过它察看主机中IASM的状态，也可以通过它动态地配置某些IASM和CRSM。

4.2 MSMIPS协商控制的特点

"软件人"的协商控制是指"软件人"能够根据自身内部的状态和外界环境自发地调节和控制自己的行为，并按照其目的和需求采取行动，动态地协调系统的平衡。由于"软件人"具有迁移的特性，因此各"软件人"可以位于不同的网络或主机上。对于网络的动态性和不确定性、网络传输中存在的延迟以及过多地依赖通讯来完成"软件人"群的协调一致等都可能存在很多问题。因此，在MSMIPS中"软件人"不宜采取完全集中的控制方式，而应采取分散弹性控制的方式。它具有以下特点：

1)"软件人"对自身进行控制，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，进而达到系统的协调。

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，但是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 MSMIPS协商控制的形式

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。为此根据"软件人"之间相互通信的方式及信息通道结构的不同，可采用导引协调、循环协调、分组协调和全息协调四种形式[12]，这四种协调模式可视系统规模大小而灵活运用。当系统规模比较大时，应先采用分组协调模式将系统分为若干组，组内可采用导引协调、循环协调、全息协调，或其中几种协调模式的不同组合。本模型主要采用分层组合导引协调的混合模式。

根据系统中各"软件人"之间所处的位置、耦合的强弱、相互通信的难易以及对协调需求的差异等具体情况，将"软件人"群划分为若干组，每组由主导子系统对各从属子系统的运行状态进行观测、评价，发出导引协调信号，从而对各从属子系统进行导引协调控制。各组可以采用不同的协调方案，并行地、独立地进行协调，并且在主导子系统的引导下共同实现系统的总目标和总任务。如图3所示：选取某一个SM为主导"软件人"——SM_1，由SM_1对其所属各SM的状态进行观测、评价，发出导引协调信号，从而对各SM进行导引协调，实现"软件人"群的协作，共同完成所求解的问题。

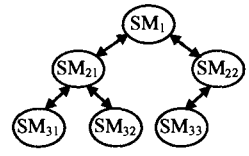

图3 Multi-SoftMan分层组合导引协调控制模式

4.4 MSMIPS协商控制的算法

如图3所示，"软件人"群以树状结构表示。设该树的度为k，深度为h，"软件人"群的规模为n。由图3可知：

$$n\leqslant\sum_{i=1}^{h}k^{i-1}=\frac{k^h-1}{k-1} \tag{1}$$

则，"软件人"群(分组)的协调代价可表示为

$$\cos t(SM_1)=\cos t_1+\cos t_2 \tag{2}$$

其中：$\cos t_1$——SM_1向其他SM广播导引协调信号的代价；$\cos t_2$——其他SM响应SM_1的协调结果的代价之和。

若以树的每个分支表示一个单位代价，则

$$\cos t_1=\sum_{i=2}^{h}(i-1)k^{i-1}=\frac{k}{k-1}\left(k\frac{k^{h-1}-1}{k-1}-h+1\right)$$

$$=\frac{k}{k-1}\left(\frac{k^h-1}{k-1}-h\right) \tag{3}$$

为计算$\cos t_2$，给每个(分组)"软件人"$SM_i(i=2,3,\cdots,n)$赋予权值W_{ij}，权值越大表示协调难度越大。由此，计算每个叶子结点到根结点的带权路径长度，然后取其最大值，即为$\cos t_2$：

$$\cos t_2=\mathrm{Max}\left\{\sum_{i=h}^{h-1}(i-1)W_{ij}\right\} \tag{4}$$

所以

$$\cos t(SM_1)=\cos t_1+\cos t_2=\frac{k}{k-1}\left(\frac{k^h-1}{k-1}-h\right)+\mathrm{Max}$$

$$\left\{\sum_{i=h}^{h-1}(i-1)W_{ij}\right\} \tag{5}$$

将式(3)代入式(1)，得：

$$\cos t_1\geqslant\frac{k}{k-1}(n-h) \tag{6}$$

由于$\cos t_2$主要受权值W_{ij}的影响，而权值W_{ij}主要取决于问题本身的影响，所以当问题确定后，权值W_{ij}就可以确定。故$\cos t_2$在这里可以近似看作常量C。因此，合并式(5)和式(6)，得

$$\cos t(SM_1)\geqslant\frac{k}{k-1}(n-h)+\mathrm{C} \tag{7}$$

由k叉树的性质可知：具有n个结点的k叉树的最小深度为

$$h=\log_k[n(k-1)+1] \tag{8}$$

因此，以式(6)为目标函数，式(1)和式(8)为约束条件，式

(下转第66页)

系统相对于全部样本的平均检测率、误报率分别为 60.47% 和 30.65%(表 3)。

表 3 各类攻击事件检测统计结果

攻击类别	检测率	平均检测率	误报率
DoS	69.23%		
Probing	41.67%	60.47%	30.65%
R2L	83.33%		

表 4 DARPA 入侵检测系统评测大会评测结果

系统	检测率
Forensics	55.56%
Expert1	50.30%
Expert2	46.83%
Dmine	40.20%

表 4 为 1999 年美国 DARPA 入侵检测系统运用 KDD-Cup99 中的网络入侵检测数据包的非抽样数据的评测结果。

比较不难发现,本文设计的基于免疫学原理的混合入侵检测系统在检测性能方面较美国 DARPA 入侵检测系统稍好,有进一步完善之必要。

参 考 文 献

[1] 刘克胜,曹先彬,郑浩然,等. 基于免疫算法的 TSP 问题求解. 计算机工程,2000,26(1):1-2

[2] 陈波,于怜. 基于人工免疫的网络入侵检测[J]. 计算机工程与应用,2002,22:165-167

[3] Dipankar D, Yu S, Majumdar N S. MILA-Multilevel Immune Learning Algorithm// the Proceedings of GECCO. 2003

[4] Kim, Bentley. Immune Memory in the Dynamic Clonal Selection Algorithm// 1st International Conference on Artificial ImmuneSystems (ICARIS-2002). University of Kent at Canterbury, UK, 2002.9

[5] Xie Gang, Xu Xingying, Xie Kerning, et al. Clone mind evolution algorithm. Lecture Notes in Computer Science, v 3611, n PART II, Advances in Natural Computation // First International Conference, ICNC 2005. Proceedings, (EI: 05439427285, SCI: 000232222500132),2005: 945-950

(上接第 49 页)

(5)为检验条件,通过分析各参数之间的关系,从而确定合理的"分层组合导引协调树"的结构。

4.5 MSMIPS 协商控制的策略

"软件人"之间的协商控制采用部分——全局规划(Partial Global Planning,PGP)策略,它是一种典型的分布式协商技术,其特点是每个 SM 都能收集目前的状态,又能收集其他 SM 的目标信息。因此,PGP 提供了 SM 间的灵活协调,保证了各 SM 间的交互。PGP 通过不同局部计划间的交互,可以避免 SM 间的任务冗余,特别是当多个 SM 计划具有相同的中间目标时会发出告警通知。每个 SM 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。

结束语 本文研究的目的在于,将群体"软件人"智能检测技术和先进的分布式体系结构相结合,构建一种新型的入侵防御系统体系结构。为了实现此目的,提出了基于群体"软件人"入侵防御系统的智能协商控制模型及相应的算法。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,系统结构具有很好的伸缩性、灵活性、扩展性、自学习能力、容错能力、分布式控制和攻击预防能力等。它能有效地解决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,以及在不同的入侵检测系统之间数据量大且集中、负载不均衡、不能协同工作等。本课题下一步的研究方向包括:1)将"软件人"技术与入侵检测系统结合,利用其优势互补设计基于群体"软件人"的智能入侵防御系统;2)针对群体"软件人"的检测分析算法及自身的安全进行更深入地研究,使入侵防御系统的智能化程度、检测性能、可操作和维护性将有大幅度提升。相信随着研究的深入,基于群体"软件人"的智能入侵防御系统会得到不断地完善,它的应用也将更为广泛。

参 考 文 献

[1] Snapp S R, Brentano J, Dias G V, et al. DIDS (Distributed Intrusion Detection System)-Motivation, Architecture, and An Early Prototype// Proc. of the 14th National Computer Security Conf. Vol 10. Washington, 1991:167-176

[2] White G B, Fisch E A, Pooch U W. Cooperating Security Managers: A Peer-based Intrusion Detection System. IEEE Network, 1996, 10(1):20-23

[3] Asaka M, Taguchi A, Goto S. The Implementation of IDA: An Intrusion Detection Agent System// Proc. of the 11th FIRST Conf. 1999. Brisbane, 1999

[4] 褚永刚. 大规模分布式入侵检测系统关键技术研究. 博士学位论文. 北京:北京邮电大学, 2005:65-72

[5] 曾广平,涂序彦. 软件人[A]// 中国人工智能学会第 10 届全国学术年会论文集[C]. 北京:北京邮电大学出版社, 2003:677-682

[6] Tu X Y, Zeng G P, Tang T. HADS: Humanized Autonomous Decentralized Systems [A]// Proc. of the International Symposium on Autonomous Decentralized Systems (ISADS'2005) [C]. 2005:593-598

[7] Lu Q L, Zeng G P, Tu X Y. SoftMan and Agent [A]// Proc. of the International Conference on Networking, Sensing and Control (ICNSC'2005) [C]. Tucson, AZ, USA, March 2005

[8] Zaki M, Sobh T S. Attack Abstraction Using a Multiagent System for Intrusion Detection [J]. Journal of Intelligent & Fuzzy Systems, 2005,16:141-150

[9] Dasgupta D, Gonzalez F, Yallapu K, et al. CIDS: An Agent-based Intrusion Detection System [J]. Computers & Security, 2005,24:387-398

[10] Dasgupta D, Rodriguez J, Balachandran S. Mining Security Events in a Distributed Agent Society [A]// Proc. of the Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, part of SPIE Defense and Security Symposium-2006 [C]. Orlando, Florida, April 2006

[11] 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

[12] Zeng G P, Tu X Y, Zhang S M. Study on the Organization Models of SoftMan Group [A] // Proc. of the International Conference on Networking, Sensing and Control (ICNSC'2005) [C]. 2005