第 7 卷 第 2 期 信 息 安 全 学 报 Vol. 7 No. 2
2022 年 3 月 Journal of Cyber Security March 2022

基于仿生控制机理的信息系统内生免疫体系研究

李　涛[1,2], 胡爱群[1,2], 方兰婷[1,2]

[1]东南大学 网络空间安全学院 南京 中国 210000
[2]网络通信与安全紫金山实验室 南京 中国 210000

摘要　随着信息通信系统的架构日益复杂, 承载的数据量呈指数级增长, 现有的安全防护体系存在严重缺陷: 先建网络、后做防护导致安全防护难以到位; 集中式防御模式导致信息系统对外服务能力下降严重; 防御机制与信息系统的安全状况关联不大导致防御效能低下。如何从根源上突破以上瓶颈成为未来信息系统安全的核心问题, 需要改变被动式防御方式, 实施主动式防御。本文提出一种基于仿生控制机理的内生免疫体系, 通过研究人体的高效神经控制特征: 遍布系统并与功能器官高度融合的海量神经元、由一系列基本动作为基础要素进行任务的执行、实时反馈并对偏差动作进行校准、具有大脑这样的综合分析处理中心进行分析和决策。基于上述特征构建了信息系统类神经系统控制架构, 通过全方位部署安全神经元, 将功能和安全融入到基本功能模块中, 构建一种以任务为导向的执行动作细粒度监控机制, 根据任务执行条件调用基本模块执行操作, 在执行过程中感知执行路径, 通过反馈发现错误, 根据策略进行校准。通过对构建的仿生控制模型分析表明, 这种基于仿生控制的机制能够维持信息系统的安全状态。通过构建原型系统对任务在不同策略下的运行模式进行了分析, 系统包含通信模块与加解密模块, 模块中融入了安全监测与控制部分, 基于模糊认知图进行控制校准, 实验结果表明提出的仿生控制机制能够根据运行环境的变化调整策略, 维持任务的有效运行。基于仿生控制的机理为内生免疫系统的实现提供了基础理论支撑。

关键词　信息系统安全; 内生安全; 内生免疫; 安全模型; 主动安全
中图法分类号　TP309　DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.03.06

Bionic Control Mechanism Based Research of Endogenous Immune Architecture for Information System

LI Tao[1,2], HU Aiqun[1,2], FANG Lanting[1,2]

[1] School of Cyber Science and Engineering, Southeast University, Nanjing 210000, China
[2] Purple Mountain Laboratories, Nanjing 210000, China

Abstract　The architecture of information system is becoming more and more complicated, and the generated data is also growing exponentially. Facing the rapid transformation of information system, existing security architecture exposes some serious flaws: protection mechanisms are deployed after network constructing, which leads to some security policies are hard to implement protecting mechanisms efficiently; centralization protection model leads to serious decline of service capacity; small relevance between protection mechanisms and security statement results in decline of defense efficiency. How to solve above problems from original base is the core problem of future information system. The protection method must be changed from passive to initiative method. This paper proposes an endogenous immune architecture based on bionic control mechanism. Through study of human being's efficient neural control mechanisms, which include a mass of neurons throughout the system and highly integrated with functional organs, a task is executed with a series of basic actions, action's executing effects are monitored and deviations are calibrated in real time, a brain acts as a comprehensive analytical processing center for analysis and decision making. Based on the above characteristics, this paper constructs a neural control architecture for information system. Our architecture fully deploys security neurons in system. Functions and security are deeply involved in basic module. Based on proposed architecture, system includes some basic tasks which can be decomposed into a series of actions. When the system executes a task, executing path and actions' running data are monitored. Executing errors can be detected through feedback mechanism. Then the adjusting policy is executed to correct flaws. We also construct a bionic control model for proposed architecture. The analysis of model shows that security mechanism based on bionic control mechanism can maintain security state. By constructing prototype system, we analyzed task's running modes under different policies. The prototype system includes communication module and encryption and decryption module. Each module integrates security monitor and control parts. The control calibration mechanism is carried out by fuzzy cognitive map. Experimental results show that the proposed bionic control mechanism can adjust the

---

通讯作者: 李涛, 博士, 副教授, lit@seu.edu.cn。
本课题得到至善青年学者支持计划、移动信息通信与安全前沿科学中心、自然科学基金基于量化可信模型的信息系统智能安全机制研究(No. 61601113)、网络通信与安全紫金山实验室资助。
收稿日期: 2020-11-26; 修改日期: 2021-01-11; 定稿日期: 2022-01-06

executing strategy according to the changes of operating environment and maintain the effective operating of task. The mechanism based on bionic control provides basic theoretical support for the realization of endogenous immune system.

Key words information system security; endogenous security; endogenous immune; security model; initiative security

1 引言

信息通信系统正在朝大流量、富应用方向发展,对现有的“外壳式”安全防御体系提出严峻挑战, 通过在网络节点和终端部署防火墙、防病毒软件、入侵检测系统来保障信息系统安全性的弊端日益显现。未来, 信息通信网络架构日趋复杂, 数据量呈指数级增长, 数据来源更加丰富, 内容更为细化, 网络数据分析的维度更广泛。同时随着终端设备性能的增长, 数据源发送速率更快, 对安全信息采集的速度要求越来越高, 漏洞日益增多, 影响也更加广泛。这些变化使得外壳式防御体系面临问题: (1)防火墙来不及深度过滤; (2)入侵检测系统来不及检测入侵; (3)防病毒来不及发现病毒。这些问题导致了外壳式的安全防御系统无法保证逐渐一体化的巨流量通信服务的信息网络安全, 如何突破被动防御的瓶颈, 构建主动防御体系是当前信息保障技术面临的重大问题。

在信息系统中构造类似人体的免疫机制是理想的主动防御措施, 最早由 Forrest 等人[1]提出并在计算机上建立了一个人工免疫系统, 由此逐步发展形成了计算机免疫学的概念, 作为一个新兴的研究领域吸引了众多研究者的参与, 并提出了一系列免疫模型与系统[2-4]。但由于信息系统现有体系架构的限制, 免疫防御的研究缺乏应用环境的支撑, 并不能在实际系统上实现真正理想的免疫机制。可信计算是构建主动防御体系的另一个重要思路, 其基于现有的应用环境构建, 目标是利用信息系统中有限的信任条件构建一套相对可信可控的安全环境, 从体系架构上建立恶意代码攻击免疫机制[5], 能及时识别“自己”和“非己”成分, 使漏洞不被攻击者利用。在我国自主提出的可信 3.0 中, 明确提出了可信免疫的思想, 使用双系统双体系的架构, 构建基本的可信免疫机制, 实现计算机体系结构的主动免疫[6]。但目前可信免疫机制并不等于安全, 而是用来支撑安全, 确保安全机制的运行符合预期, 在系统纵深上缺乏更细致的监控, 没有描述如何针对动态运行环境进行主动式防御。

在现有构建主动式防御体系的过程中, 缺少与原有信息系统的高度融合, 使得计算机免疫、可信计算在实际应用过程中难以做到系统运行效率和安全防护的统一。在这种困境下, 内生安全的概念近年来成为热点, 通过构建全新的内生安全防御体系, 首先解决融合问题, 在信息系统设计的时候就考虑安全功能的部署, 将安全体系和信息系统高度融合, 以期能够解决现有通信网络防御效率低下、无法处理高速率数据、不能应对未知威胁等问题。通过使网络具有“与生俱来、自主成长”的安全防御能力, 满足“业务高可用、安全高效率”的通信网络发展需求。从目前的研究情况来看, 内生安全还没有明确的定义, 没有整体上明确其内涵, 借鉴生物安全防护机制是大致的思路, 但是现有的免疫、拟态、智能都是从生物的安全防御局部机制获得启发展开的研究, 需要深入分析生物防御机制构造内生安全的体系, 充分借鉴生物的神经、免疫系统可以在不影响生物其它功能的情况下完成安全防御的特性。

本文提出一种基于仿生控制机理的安全防护机制, 借鉴人体面对内外安全威胁的防御机理, 这种安全防御能力是与生育来, 与人体自身高度融合的, 是一种“内生”的安全机制, 与信息系统安全防御从系统的目标、结构及工作模式上具有高度相似性。通过在信息系统中部署海量的神经元, 完成对执行动作的感知和控制, 使得任务能够按照预期效果完成, 从而构造出类似人体的内生免疫机制。

2 相关研究

内生安全是一种主动式安全防护方法, 在现有的研究中, 主动式安全防护方法主要包括可信计算、智能安全自动计算、拟态防御和计算机免疫。

可信计算由 TCG(Trusted Computing Group)系统的提出并应用在信息系统中。可信计算首先通过物理防护方式构建一个可信根, 再通过密码方法构建一条可信链, 将信任关系从可信根延伸到操作系统、应用以及网络实体[7]。TCG 提的可信计算架构最大的问题在于只能构建静态可信链, 应用启动后的动态可信性无法保证。针对系统运行过程中信任的管理成为众多学者研究的重点, Zheng Yan 等长期从事可信管理方面的工作, 提出了一系列系统运行过程中的动态可信评估和管理的方法[8-9], 通过实时评估和动态管理维持了应用运行的可信性。沈昌祥院士提出了我国的可信计算标准—可信计算 3.0, 通过主动免疫原理构建可信免疫架构, 以双系统体系架构

的模式实现可信计算[10]。Liu 等人[11]通过研究电力监控系统的安全状况, 提出了一种基于可信强制访问控制的 TMAC 模型, 该模型具有自学习特征, 可以实现基于智能代理的全局安全策略的自动升级, 从而建立了安全的可信免疫能力和主动防御系统。动态可信管理和可信免疫都是针对系统运行过程提出的可信机制, 但在实施过程中缺少应用程序支撑, 需要进一步提出更为细致的规范化架构。

智能安全使用人工智能的方法对威胁进行分析, 以期达到人脑一样对威胁能够主动判别的效果。近年来, 人工智能在网络安全领域的应用初显端倪, 已成为下一代安全解决方案的核心思路[12-13]。MIT 的 CSAIL 实验室与初创公司 PatternEX 共同开发的一个端到端系统“AI2”, 可以不断学习来自安全分析员的反馈来对新发生的事件进行预测, 其准确率是当今类似的自动化网络攻击检测系统的 2.92 倍, 误报率比同类的安全解决方案小 5 倍[14-15]。一些国内的知名安全厂商也已开始了以签名为基础的反病毒和反恶意软件产品到不再依赖现有恶意软件定义的机器学习模式来检测威胁的转变。Zhou 等人[16]提出了一种内生主动防御机制, 通过对整个网络的安全数据进行采集和综合分析来实现智能化的防御。人工智能在安全方面的应用提高了恶意软件的分析效率, 然而目前的智能安全研究大多数仍是基于现有防护体系构建的, 主要应用在对恶意代码进行自动识别方面, 本质上仍然是对被动式防御方式的改进, 并没有从基础上去构建一种主动式防御架构。

自动计算最早是由 IBM 研究院提出, 旨在构建一种具有自我认知、自我优化、自我修复、自我防御的系统[17-18], IBM 开展了一个 Eliza 项目, 从操作系统层面进行了改造以支持自动化部署和调配资源的能力, 以期实现主动式防御。但由于没有对应用进行改造, 自我优化和修复缺少细粒度的联动机制, 目前自动计算的思路只应用在了云计算[19]和物联网[20]中, 主要用于对计算资源进行优化和动态适配, 并没有形成真正的主动式防御能力。

生物的一种规避风险的行为是通过伪装来躲避攻击, 这就是“拟态现象”, 即一种生物在色彩、纹理和形状等特征上模拟另一种生物或环境, 从而使一方或双方受益的生态适应现象[21]。一些研究者根据拟态现象提出相应的安全防御方法, 代表性的是邬江兴院士提出的“拟态防御”[22], 该方法基于生物的拟态现象, 提出了一种通过类似拟态伪装的方式进行主动隐匿, 较大程度上增加了攻击的难度。姚东等人结合性能和兼容性问题提出一种基于多变体执行架构的软件安全主动防御架构[23]。拟态防御旨在隐藏受保护目标, 使得攻击行为难以实施[24-25]。

计算机免疫学的研究旨在信息系统中构造类似人体的免疫机制, 主要包括三部分研究内容: (1)将免疫机制应用到入侵检测中, 进行自动入侵恢复、攻击特征提取以及改进基于行为的检测潜力[26-27], 基于生物免疫的入侵检测方法能够有效提高入侵检测的效率[28]; (2)将人体免疫架构应用到计算机系统中, 提出受免疫启发的安全体系结构, 其中包括类似抗原和抗体的分布式 multi-agent 检测器, 以及检测器的生成和分配机制[29-32]; (3)针对免疫算法的研究, 而免疫算子又是通过接种疫苗和免疫选择两个步骤来完成免疫算子的构造, 其中波动现场和收敛速度是衡量免疫算法效果的主要指标[33-34]。计算机免疫是一种理想的主动防御方法, 但由于信息系统现有体系架构的限制, 构建的免疫防御机制缺乏应用环境的支撑, 通常应用在检测系统内部的病毒攻击方面。

从目前的研究情况来看, 免疫、拟态、智能安全等都是从生物的安全防御局部机制获得启发展开的研究, 主动式防御的机制需要信息系统各部分紧密配合, 需要安全和系统原生功能的高度融合。本文从整体架构上入手, 充分分析和借鉴人体神经控制系统的原理, 提出一种新型的内生免疫体系。

3 人体神经控制系统机理

人体在面临威胁时, 往往能够做出有效、适度的反应, 维持机体的高效运转。在人体防御过程中, 既能使我们有效的避开威胁, 又不会影响我们正常的日常生活, 同时还可以不断调整和提高应对威胁的能力。例如, 当人体的手接触到蜡烛的火焰时, 人往往只会移开手, 而不是反应过度的从此不再接触火。这是一种基于自身认识对外部攻击的适度响应。此外, 人体体内拥有的强大免疫系统能够抵御病毒的内部入侵, 这是一种内部攻击发生后的免疫行为。

遇到未知的威胁时, 人体会通过自我学习, 逐渐地具备防备此类威胁的能力。例如, 婴儿可以通过对外界的不断感知, 学习走路, 防止摔倒, 自身的免疫力也能够通过“免疫记忆”的方式逐渐提高, 这是一种“自我生长”的能力。

人体的这种安全防御能力是与生育来, 与人体自身高度融合的, 是一种“内生”的安全机制, 与信息系统安全防御从系统的目标、结构及工作模式上具有高度相似性, 研究人体的这种内生免疫机制具有重要意义, 在信息系统中构造类似人体的安全机制是理想的主动防御措施, 通过研究人体对外界威胁

的智能反应对信息系统安全具有重要意义。

通过研究发现，正是人体的神经控制系统提供了这种高效的防御能力，人体具有无意识和有意识的控制自身输入与输出的功能特性。基于人体神经的控制系统时刻进行自我调节，指导心脏跳动速度、调节瞳孔、监控温度调节血液流动速度和皮肤功能来维持体温，甚至在受到惊吓时候能让头发竖起。这是一种面对复杂多变的外部环境，维持内部稳定的能力，使人体能够应对处理各种任务。

在人体神经控制系统下，并不需要有意识的去组织任务的完成方法，即“需要思考要做什么，不需要去思考怎么做”。典型的例子是在追赶汽车时，不需要计算呼吸和心跳有多快，由神经控制系统自动地调节并调动身体的各个元素协同工作，完成追赶任务。

人体神经控制系统不但可以进行外在调节，还可以进行内在调节，人体内的免疫系统也受到神经系统影响。传统观点认为免疫系统不受神经系统的调节，但是自 2010 年以来兴起的心理神经免疫学(Psychoneuroimmunology)的研究表明[35]，在神经、内分泌系统与免疫系统之间有着密切的关系和复杂的交互作用。免疫反应可以形成条件反射，通过条件反射的方法可使动物的免疫系统功能发生变化。

从神经控制系统的组成来看，人体的控制系统主要包括控制单元和受控对象两部分[36]，如图 1 所示。控制单元主要由控制器、感受器和效应/执行器组成，核心是控制器，受控对象即为生命体或其不同的生理和代谢过程等。

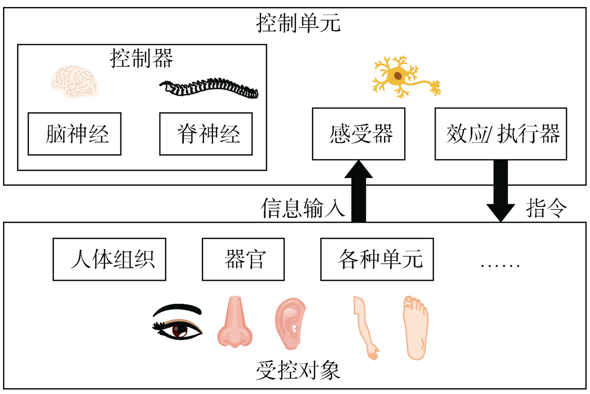


图 1 人体神经控制系统

Figure 1 Human nervous control system

控制器即为人类脑神经、颈神经、胸神经、腰神经、骶神经和尾神经等神经系统，在种种调节控制中发挥主导作用。实现控制首要的是信息的输入，信息的来源是内外环境条件的种种刺激和干扰，根据接受信息来源的不同包括外感受器和内感受器。感受器接受到的刺激或干扰，作为输入信息传输到控制器，经控制器加工处理后，变为输出信息，再作为指令使效应器执行既定动作。其中一个显著的特点是人体的效应器和感受器是统一的，例如人体四肢是效应器也是感受器，既可以完成既定动作，也能感受外界的环境变化。

在神经系统的组成架构上进行控制的主要原理是内反馈[36]。如图 2 所示，控制器接收由感受器感知的内外界信息后，由控制器输出到效应器，使受控对象动作。其执行的实际状态还会通过反馈器再汇报给控制器，控制器对输送来的信息经过比较分析、判断处理后，即按实际效应与预期目标间偏差，指令效应器采取进一步调整措施，以对外来干扰给予正确反应。这是一种负反馈控制调节过程。

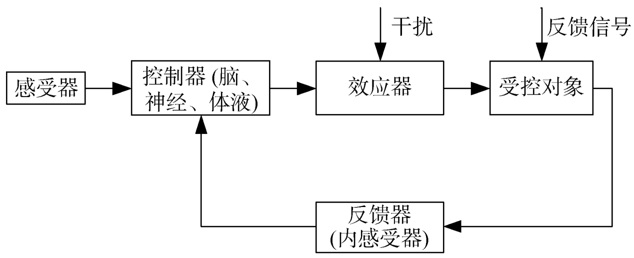


图 2 神经控制反馈原理

Figure 2 Feedback principle of neural control

神经控制系统的另一个特征是分层次的多级控制系统，存在不同水平的控制中心，高级控制中心可控制和修正低级控制中心的活动[37]。时时刻刻进行自控调节，应答生境中多变的刺激和干扰，保持自身内部条件的平衡和对生境的高度协调。

综上所述，人体神经控制系统实现的主要要素为:

(1) 遍布系统的海量神经元，神经元与功能器官高度融合，功能器官既是功能部件，也是感知和效应部件;

(2) 以任务为导向，明确任务后，由一系列的基本动作为要素，自发组合动作，执行任务;

(3) 具有反馈系统，对任务执行情况进行实时反馈，通过系统的联动来应对，对偏差动作进行校准，保证任务按照预期完成;

(4) 具有大脑这样的综合分析处理中心进行分析和决策，拥有自主学习能力。

4 仿人体的内生免疫信息系统

仿造人体的神经控制系统，在信息系统中构建

一种以任务为导向的执行动作细粒度监控机制，整体控制流程如图 3 所示。

控制流程分为静态分析和动态防御两部分，静态分析是基础，分析一个任务的正常执行特征。例如动作执行过程中对系统产生影响的参数、动作本身向外发送的证明自身正确执行的参数等。通过对参数的自学习，刻画出任务的执行特征，并生成正常执行过程中的行为库，这些特征是识别“自我”的基础，是系统对任务安全执行进行判断的预期参数。

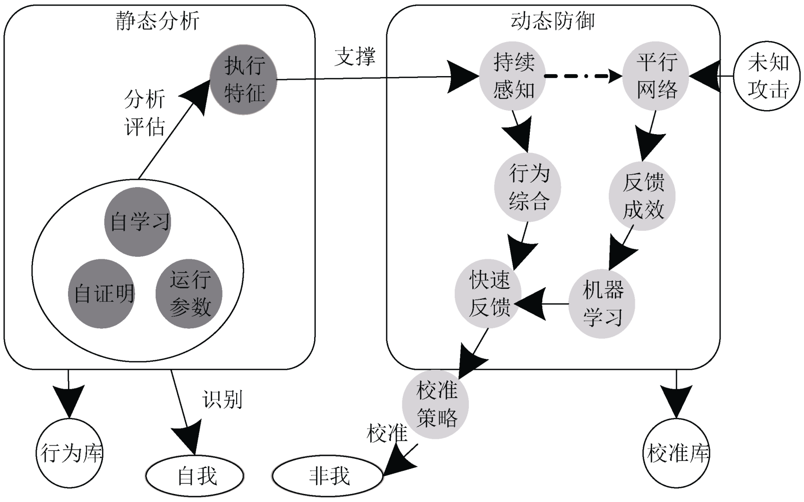


图 3　信息系统类神经控制流程

Figure 3　Neural control flow of information system

在分析了任务安全执行的行为特征后，在实际系统运行过程中进入到动态防御阶段。系统通过遍布各个功能模块的神经元感知动作执行效果，并与预期行为参数进行对比，反馈执行效果。一旦发现执行偏差就进行校准，下达校准策略，将“非我”动作校准到预期执行路径上。校准策略依据已有的校准库下达，如果出现未知攻击导致的执行偏差，机器学习算法将根据监控参数和系统预期进行最优化策略的制定，并根据校准的效果不断优化策略，实现自主进化的功能。

基于上述控制流程，构造了贯穿通信信息系统终端、网络和核心网层的内生免疫系统架构，如图 4 所示。

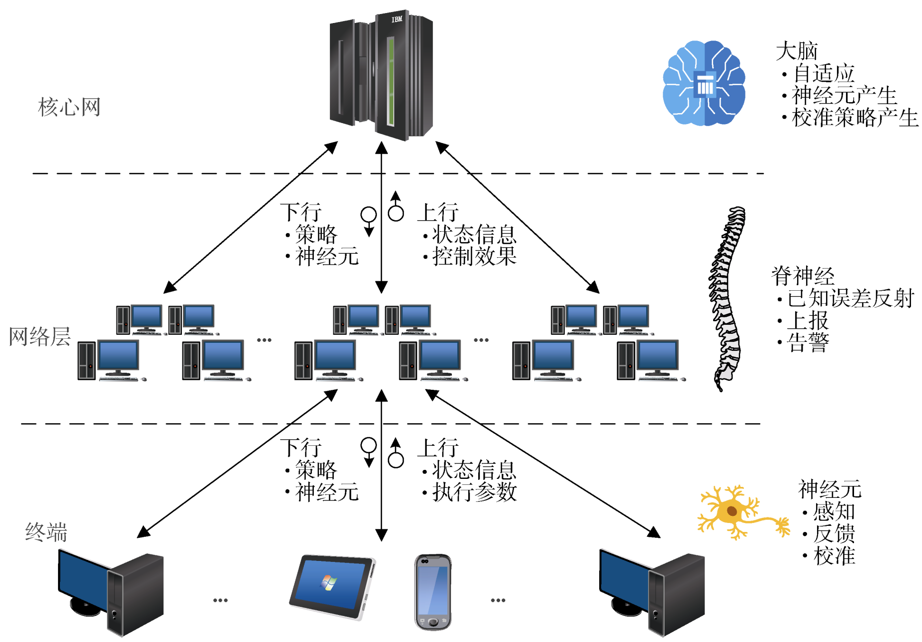


图 4　类神经系统控制架构

Figure 4　Neural control architecture

每层的功能描述如下:

终端: 遍布终端的神经元感知并控制每个终端系统的活动, 监控并维持应用任务的正常进行。终端运行的各种应用就是效应部件, 神经元延伸到每个效应部件, 为了尽可能降低终端的负担, 神经元仅仅执行策略下达、环境感知和动作校准的功能, 不进行大量的计算。

终端的应用以任务的方式执行, 对应用进行模块化划分, 根据事先规定的策略调用相应的模块执行任务。模块的执行有一定的次序, 并在执行的过程中感知各种运行参数, 这些执行参数将作为反馈信息上传给脊神经。

一旦出现执行偏差, 终端神经元将根据校准策略指挥效应器进行校准。校准功能包含传统的安全机制, 例如加密、访问控制、阻断等, 也包含一些功能性措施, 例如替换异常模块、降低负载、提高运行速率等。

神经元起到感知和执行作用, 它的运行依赖于和上层脊椎层和大脑层的交互作用。神经元进行一些低功耗的操作(搜集信息, 下达指令), 更复杂的功能(行为判定、反馈策略制定、神经元升级等)由更高层执行。把所有搜集到的信息传递给关联的网络层脊椎神经, 接收来自脊椎神经的信息, 校准指令也由神经元接收, 这些校准指令将触发并更改模块运行方式。

网络层: 网络层包含了在更高层有交互需求的终端节点, 这些节点具有一定的共性: 共享大量的资源, 由一个本地或者广域的网络连通, 并且支撑同一个组织网络。在网络层面, 有些任务可能需要多个节点共同协调才能完成, 并且如果一个节点中毒, 可能会快速扩散到网络中。因此, 需要网络层脊椎神经来协调网络内终端神经元的工作。此外, 颈椎神经也是终端和大脑信息传输的通道。

颈椎神经的主要功能包括: 行为分类, 当脊椎神经接收到神经元传输上来的执行信息后, 会判断任务执行效果, 并对执行效果尝试进行分类。这将由执行流信息和行为库进行匹配, 一旦发现执行流出现偏差, 就在脊椎神经查找是否有对应的校准策略, 并将策略下达到终端神经元。这一过程相当于神经反射, 也类似于一种识别自我和非我的疫苗库。如果无法在现有校准策略里进行匹配, 就将信息上传到大脑, 由大脑进行校准策略的下达。

总体来看, 脊椎神经把校准策略反馈给终端神经元, 并搜集校准效果, 形成度量报告, 把控制策略和效果上报给大脑。大脑根据校准效果报告不断进行进化, 提高校准效率。

核心网层: 架构的顶端是核心网层, 相当于大脑。这一层的活动主要包括: 生成并自适应校准策略资源, 将资源下载到网络层; 通过不断学习、自我完善, 使得安全防御的各个结构和功能相互合作又互不影响。大脑是所有资源的仓库, 并且有一些进化算法的应用, 进行资源的自适应, 通过类脑安全控制并行处理整体体系的数据, 实现多任务整合、归纳和决策。通过自主进化决策对潜在的风险自主学习, 实现安全性能的自我提升。

基于以上架构, 如表 1 所示, 可以对人体神经控制系统与内生免疫系统进行类比。

表 1 人体神经控制与内生免疫对比

Table 1 Contrast between human neural control and endogenous immunity

人体神经系统	内生免疫系统
手、脚等	模块
外感受器	功能部件调用外部资源监控
内感受器	功能部件自身输出
神经传导	安全参数传输通道
大脑	安全控制中心
效应器	功能部件
反馈	任务完成度参数反馈
预期目标	系统任务
实际效应	任务执行情况
校准	调正策略
分层级多级控制	不同的系统层级, 不同的控制中心
干扰	安全威胁

总体上看, 人体实现不同功能的器官在信息系统中以不同功能的模块对应, 完成不同的动作。在系统层面监控功能部件调用外部资源、与外部交互情况类似于外感受器的作用, 而功能部件自身主动发送的一些状态输出类似于内感受器的作用。在信息系统中构建的安全状态传输通道类似神经传导, 用来传输安全状态相关的信息。安全控制中心相当于大脑, 进行决策和策略下发。功能部件类比于效应器, 完成信息系统的各种基础功能。对任务的执行情况进行监控并反馈, 构建了信息系统内的负反馈机制。系统的任务相当于预期目标, 有其要达到的效果和执行的路径。任务的最终执行情况就是实际效应, 执行过程中根据反馈进行策略调整是校准的过程。在不同的信息规模层面部署不同的安全部件, 相当于构建了一个多级分层的控制机制。安全威胁就是任务执行过程中的干扰。

5 以任务为导向的控制机理

在内生免疫信息系统框架下，需要构建类人体的高效控制机理。人体神经控制的重要特征是以任务为导向，仿造这种自主神经控制原理，具有内生免疫特征的信息系统也需要明确执行的任务、划分功能模块，根据任务执行条件调用功能模块执行操作。在执行过程中感知执行路径，通过反馈发现错误，根据策略进行校准。构成这些操作的要素包括:

(1) 信息系统的每个任务分解成基本动作，其中包含动作的实施序列;

(2) 每个动作是否完成有预期的证明参数，当所有参数都符合时，表明动作已经按照预期实施完成;

(3) 任务执行过程中将实时获得监控参数，通过任务执行过程中监控得到的参数进行效果反馈;

(4) 动作不符合预期就进行校准，总体目标是保障任务的顺利完成。

为了实现以上要素，需要对信息系统的体系架构进行重新构建，总体架构如图 5 所示。

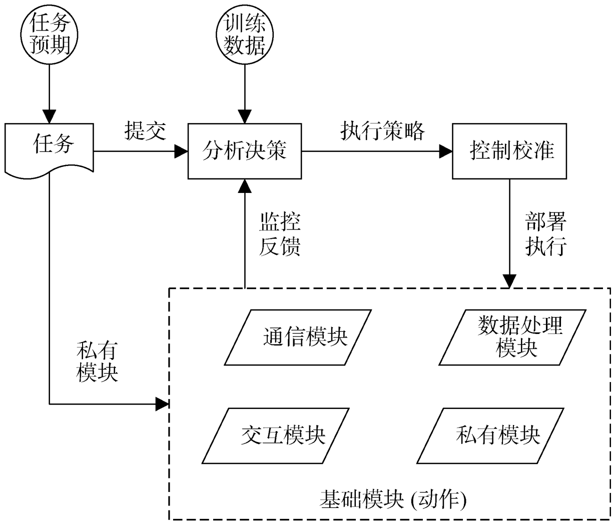


图 5 以任务为导向的执行架构

Figure 5 Task-oriented execution architecture

信息系统包含有基础功能模块，每个模块对应一个基本的动作，模块的执行效果由动作产生的输出体现。例如与网口进行交互通信、对数据进行加解密、与显示器进行交互等。除了公有模块，完成一些任务可能还需要特有的功能模块，称为私有模块。在模块化的基础上，对提交的任务进行分析，确定完成任务需要的模块以及执行的次序，在执行过程中对基础模块的执行效果进行监控，实时反馈并对执行偏差进行校准。

基础的监控和校准功能由神经元实现，为了构建上述神经控制的机制，如图 6 所示，在划分的功能模块中融入安全部分，实现类似神经元的感知和校准的功能。功能部分实现模块原有的功能，例如无线网络通信。在开发功能部分的同时，需要融入安全部分，实现对功能运行的监控以及配置调整，相当于融入功能部分的神经元。

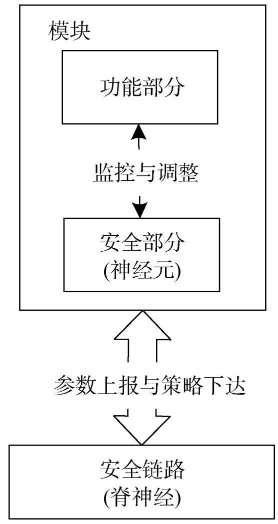


图 6 模块基本结构

Figure 6 Module's basic structure

按照模块的基本结构对功能模块进行改造。例如无线网络通信模块，原有的功能部分实现无线网卡的数据收发，安全部分可以监控的参数包括通信开始到结束的时间、信息传输速率、占用的内存、网络带宽等。通过策略配置实现模块功能调整，包括占用的带宽、内存、端口、数据块大小等。安全部分通过接口与外部通信，将监控参数上报，并接受下达的调整策略对功能进行配置。在此机制下，模块封装成一个黑盒子，通过对应接口进行上下行通信。

通过对模块的安全改造，使其具有了安全感知和策略调整的功能。在任务的运行过程中，基于感知参数进行安全性判断，通过策略配置进行调整。具体的决策控制流程如图 7 所示。

步骤 1. 任务开始运行，附带参数包括需要的模块和任务的预期。其中任务的预期包含对各个安全相关属性的期望值，并且具有主观性，例如偏向加密强度或者处理速度。

步骤 2. 根据预期属性值和先验知识，设置初始参数，使用判决算法(本文在原型系统中使用了基于模糊认知图的判决方法)对不同配置策略下任务的运行安全性进行预测，由此选择出一个最优化的策略组合，并将其应用到系统中。

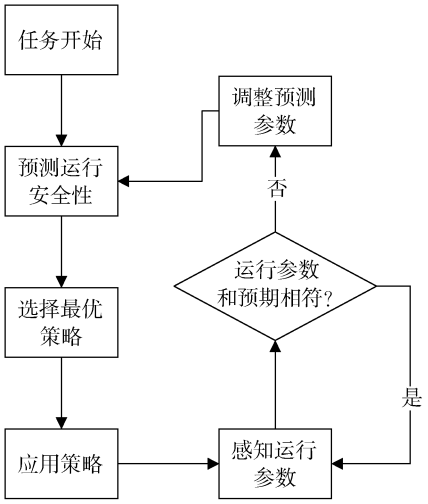


图 7　决策控制流程
Figure 7　Decision and control process

步骤 3. 任务在实际系统运行过程中, 实时感知运行的属性值, 并与预期值相比较。如果相符合则继续感知, 不进行调整。如果不符合, 则说明初始设置的预测参数和实际运行环境有偏差, 或者运行过程中遇到攻击等引起了运行环境发生变化, 下一步进入到调整阶段。

步骤 4. 根据实际属性值的反馈对预测判决算法的参数进行调整, 使得在当前策略下的预测值与实际感知到的值一致。

步骤 5. 根据新调整的参数对不同配置策略进行重新预测, 选择最优化策略, 进入新的感知流程。

在此仿生控制机制下, 通过监控任务执行过程中功能部件的输出对任务执行过程进行识别, 系统正常执行的过程就是“自我”, 一旦发现偏差就是“非我”, 通过策略配置将偏差校准, 以按照预期把任务执行完成。

6　基于仿生控制机理的模型分析

通过无干扰模型的方法构建本文描述的仿生控制模型, 无干扰理论模型从动作和运行结果的角度建立系统安全策略模型[38], 模型强调输出结果和预期的一致, 在排除非期望干扰的情况下, 执行当前动作的结果应该与预期是一致的。无干扰模型以动作为基本元素、观察执行动作输出的思路与本文仿生控制机理的基本要素具有相似性。

定义 1. 系统 $M(S, O, T, A, F)$包含如下元素。

S: 系统状态集合, 包含一个初始状态 $s_0 \in S$;

O: 输出集合;

T: 任务集合;

A: 动作集合, 其中$\alpha, \beta, \ldots$表示动作序列;

F: 一些函数:

step: $S \times A \rightarrow S$, 执行单个动作的状态转移;

output: $S \times A \rightarrow O$, 执行单个动作的实际输出;

except: $S \times A \rightarrow O$, 执行单个动作的预期输出;

run: $S \times A^* \rightarrow S$, 执行动作序列的状态转移;

task: $a \rightarrow t$, 动作的归属任务。

定义 2. 关于任务动作序列的清除函数。对于$t \in T$ 和一个动作序列α, purge(α,t): $A^* \times T \rightarrow A^*$定义为:

$$\mathrm{purge}(\Lambda,t) = \Lambda$$

$$\mathrm{purge}(a \circ \alpha, t) = \begin{cases} a \circ \mathrm{purge}(\alpha, t), & \text{if } \mathrm{task}(a) \sim> t \\ \mathrm{purge}(\alpha, t), & \text{otherwise} \end{cases}$$

清除函数排除了对指定任务不存在干扰的动作, 说明了一种干扰关系。无干扰模型不限制任务间的干扰, 而是不允许非预期的干扰, 实质上强调了动作执行效果的预期。进一步由无干扰模型可以得到任务安全运行的条件。

定义 3. 任务 t 运行安全, 当满足:

$$\begin{aligned} &\mathrm{output}(\mathrm{run}(s_0, \alpha), a) = \\ &\mathrm{output}(\mathrm{run}(s_0, \mathrm{purge}(\alpha, \mathrm{task}(a))), a) \end{aligned} \tag{1}$$

其中 t=task(a), 该定义说明任务执行过程与结果预期性的符合, 与仿生控制机理中强调结果与预期的符合一致。系统从初始状态 s_0 开始, 执行了动作序列$\alpha \in A^*$后, 经历一系列状态转化, 产生一系列输出, 到达状态 run(s_0,α)。此时, 由任务 t 发起动作 a, 并观察动作 a 执行后的输出。如果能够区分动作序列α和动作序列 purge(α,task(a))执行后的状态, 则说明任务 t 被干扰了, t 是不安全的。

定义 4. 系统满足观察等价性质, 对于一个任务 $t \in T$, 存在观察等价状态 $r, s \in S, r \overset{t}{\sim} s$, 即从任务 t 的角度观察, 系统状态 r 和 s 等价, 系统视图是一样的。

定义 5. 系统满足结果隔离性质, 系统存在等价关系$\overset{t}{\sim}$, 该等价关系满足:

$$r \overset{t}{\sim} s \Rightarrow \mathrm{output}(r, a) = \mathrm{output}(s, a) \tag{2}$$

其中 t=task(a)。该性质说明, 如果两个状态对于 t 是等价的话, 则执行相同的动作将产生相同的输出。

定义 6. 输出验证函数 verify: $A \times O \rightarrow$\{true, false\}, 描述了动作产生的输出和预期输出是否相符:

$$\mathrm{verify}(a, o) = \begin{cases} \text{true}, & \text{if } \mathrm{output}(s, a) = \mathrm{except}(s, a) \\ \text{false}, & \text{otherwise} \end{cases}$$

由输出验证函数可以看出, 如果动作产生的输出验证通过, 则说明系统视图改变在预期范围。

进一步, 系统可以看成是一系列的状态转移, 转移是以执行动作为基础, 在任意时刻, 动作、执行动作的任务和系统状态是相关联的。为了简化分析, 本文忽略任务发起动作执行的时间, 只考虑执行结果, 系统运行过程就是串行的动作执行序列。

定义 7. 系统状态 $s\in S$ 为一个二元组(t, α), 其中 t 为当前系统状态下执行的任务, 序列α表示系统到达当前状态 s 时所有执行的历史动作, 包括当前 t 发出的动作。

定义 8. 一个系统具有初始状态 s_0, 称 s_0 为系统的安全根。

安全根是一种无条件安全, 其安全性可以由类似可信计算的方法保证。

定义 9. 系统可达状态 $s\in S$。设 s_0 是系统的初始状态, 则$\exists\alpha\in A^*$, 使得 $\mathrm{run}(s_0,\alpha)=s$。

由此建立了系统状态和任务、动作之间的关系, 在任意时刻, 由当前正在执行任务角度观察系统状态等同于当前系统状态。任意时刻只有一个任务在执行, 当前系统执行的任务是安全的, 就认为当前系统状态是安全的。由文献[39]可知在无干扰模型下系统安全的充分条件。

定义 10. 一个系统 M 满足下列条件, 则称 M 是安全系统。

(1) 系统运行的初始状态 s_0 是安全的;

(2) s 是系统可达状态, 且 s 是安全状态;

(3) 系统状态转移是安全的。

由以上定义, 可得系统安全运行的定理。

定理. 一个系统 M, 满足下列条件时, 系统是安全的。

(1) M 从安全根启动;

(2) 动作执行序列中的每个动作都满足输出验证;

(3) 系统满足结果隔离性质和观察等价性质。

证明. 需要证明系统M满足定义 10 的三个条件。

由 M 从安全根启动可知, 定义 10 的条件(1)满足。

下面证明条件(2)满足。任取 s 是一个可达状态, 证明 $s=(t,\alpha)$是安全状态, 即要证明 s 时刻的任务 t 是安全的, 由定义 5 的条件, 要证明式(1)成立。

由结果隔离性质和观察等价性质, 即要证明:

$$\mathrm{run}(s_0,\alpha)\overset{t}{\sim}\mathrm{run}(s_0,\mathrm{purge}(\alpha,t)) \tag{3}$$

对动作序列α长度作归纳。

当$\alpha=\Lambda$, 式(3)成立。

假设动作序列长度为 n 时, $\mathrm{run}(s_0,\alpha)\overset{t}{\sim}\mathrm{run}(s_0,\mathrm{purge}(\alpha,t))$, 则长度为 n+1 时, 记$\alpha'=a\circ\alpha$。

此时, 式子左边为:

$$\mathrm{run}(s_0,\alpha')=\mathrm{run}(s_0,a\circ\alpha)=\mathrm{run}(\mathrm{step}(s_0,a),\alpha)$$

式子右边为:

$$\mathrm{run}(s_0,\mathrm{purge}(\alpha',t))=\mathrm{run}(s_0,\mathrm{purge}(a\circ\alpha,t))$$

若 $\mathrm{task}(a)\sim>t$, 则

$$\mathrm{run}(s_0,\mathrm{purge}(a\circ\alpha,t))=\mathrm{run}(s_0,a\circ\mathrm{purge}(\alpha,t))$$

$$=\mathrm{run}(\mathrm{step}(s_0,a),\mathrm{purge}(\alpha,t))$$

由假设条件可知式(3)成立。

若$\mathrm{task}(s)\sim>t$, 则动作 a 对 t 无干扰, 不改变 t 的系统视图, 因此: $\mathrm{step}(s_0,a)\overset{t}{\sim}s_0$。

此时:

$$\mathrm{run}(s_0,\mathrm{purge}(\alpha',t))=\mathrm{run}(s_0,\mathrm{purge}(a\circ\alpha,t))$$

$$=\mathrm{run}(s_0,\mathrm{purge}(\alpha,t))\overset{t}{\sim}\mathrm{run}(\mathrm{step}(s_0,a),\alpha)$$

式(3)成立。

因此定义 10 的条件(2)满足。

最后证明条件(3)满足。

设状态 $s_2=\mathrm{step}(s_1,a)$此时 $s_1=(s_0,\alpha)$, $s_2=(s_0,\alpha\circ a)$。

系统从状态s_1转移到了状态s_2, 由(2)可知动作a验证是安全的, 且由前面的证明过程可知状态 s_1 和 s_2是安全的, 因此状态转移安全的。证毕。

系统运行的安全定理给出了一个系统满足什么样的条件才是运行安全的。系统初始状态必须安全, 这是安全的基础。动作满足输出验证实际上保证了每个执行动作是符合预期的, 这是构成任务安全的基本要素。结果隔离性质和观察等价要求任务之间相互隔离, 输出参数要能够分辨由哪个任务动作的输出。该定理也反映了设计内生免疫系统要遵循的一些基本原则, 因为系统由任务构成, 如果系统在设计中能够提供某些机制来支持任务达到运行安全所具备的上述条件, 则可达到系统运行安全。

7 原型系统实现与分析

7.1 系统实现框架

原型系统构建的框架如图 8 所示。在系统内核层构建仿神经控制的运行环境。安全管理部分进行运行机制的管理, 任务管理部分对系统的任务进行分解, 根据任务的预期选择模块和参数配置。运行监控部分对模块的运行过程进行感知, 执行调整根据反馈参数进行策略的重新配置。此外, 资源管理对系统的底层资源进行统一管理, 上层连接与上层进行安全方面的通信。

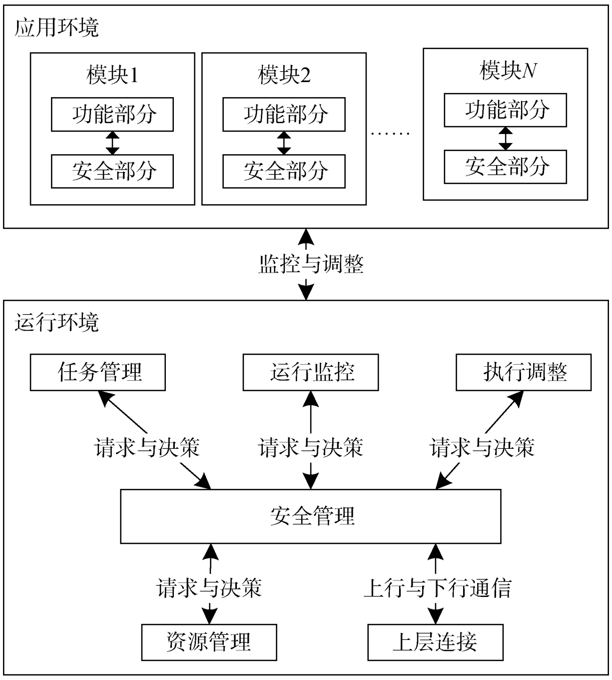


图8 系统构建框架

Figure 8 System construction framework

在现有单机系统上进行系统实现时，需要对应用进行模块化改造，使得模块包含原有的功能部分和增加的安全部分。

本文改造一个对数据加密并传输的通信应用，在Linux(Ubuntu 16.04)系统实现，使用Erlang语言编写模块，Erlang语言模块化以及支持热更新的特性使得模块可以实时调整[40]。应用中实现了两个模块：通信模块和加解密模块。两个模块在完成原有的收发数据、加解密操作功能的同时，融入对运行的参数进行感知和运行策略进行调整的功能。模块的具体功能、完成动作的输出参数和可供调整的策略如表2和表3所示，表格中功能部分表示模块原有的功能，输出参数和调整策略表示安全相关的部分。

表2 通信模块

Table 2 Communication module

功能	收发数据
动作输出参数	传输速率
	占用CPU
调整策略	传输数据块大小
	传输带宽

表3 加解密模块

Table 3 Encryption and decryption module

功能	加解密操作
输出参数	占用CPU
	加解密速度
调整策略	加密强度

在判断决策方面使用模糊认知图的方法构造自动判决和策略调整机制。对数据进行处理和发送的任务进行感知，监控保密性、CPU占用率和处理速度三个参数。构造的模糊认知图结构如图9所示。

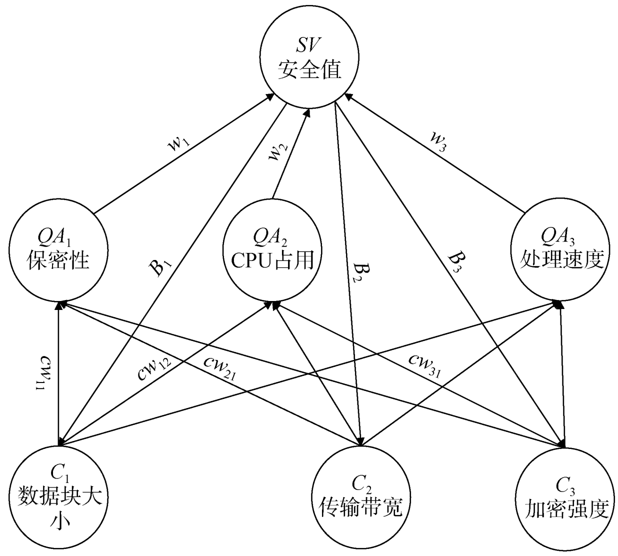


图9 模糊认知图结构

Figure 9 Structure of fuzzy cognitive map

顶层为安全值 SV，受中间层参数 $QA_{1,2,3}$ 的影响，分别为保密性、CPU占用和处理速度，$QA_{1,2,3}$ 对可信性影响的大小由任务主观预期来决定，满足 $QA_1+QA_2+QA_3=1$ 的限定条件。最底层节点 $C_{1,2,3}$ 表示调整策略，和模块构建的数据块大小、传输带宽和加密强度对应。$B_{1,2,3}$ 表示调整策略的具体程度，例如强加密策略设置 $B_1=1$，中加密策略 $B_1=0.5$，不加密策略 $B_1=0$。各种调整策略可以组成各种策略模式，不同策略对监控参数的影响由 cw_{ij} 决定。

7.2 系统测试与分析

该任务使用通信模块和加密模块完成数据加密和发送的任务，可配置的策略选项如下：每次传输的数据块大小，包括 1×10^6 Bytes 和 5×10^6 Bytes；传输带宽可设置为900Kb和11Mb；使用AES加密，可以设置为不加密、128位加密和256位加密。在可配置参数下，可以组合成12组策略模式：

- M_1(1×10^6 Bytes, 900Kb, 不加密);
- M_2(1×10^6 Bytes, 11Mb, 不加密);
- M_3(1×10^6 Bytes, 900Kb, 128位);
- M_4(1×10^6 Bytes, 11Mb, 128位);
- M_5(1×10^6 Bytes, 900Kb, 256位);
- M_6(1×10^6 Bytes, 11Mb, 256位);
- M_7(5×10^6 Bytes, 900Kb, 不加密);
- M_8(5×10^6 Bytes, 11Mb, 不加密);

- M_9(5×10^6 Bytes, 900Kb, 128 位);
- M_{10}(5×10^6 Bytes, 11Mb, 128 位);
- M_{11}(5×10^6 Bytes, 900Kb, 256 位);
- M_{12}(5×10^6 Bytes, 11Mb, 256 位)。

任务可以监控的参数包括每次发送任务的处理时间、任务总体的 CPU 占用率和数据传输速率。不同的策略模式下的监控参数如表 4 和图 10 所示，实验选取了 10 次运行结果的平均值。

表 4　监控参数表

Table 4　Monitor parameters table

选择模式	处理时间(*10^{-1}s)	CPU 占用率(%)	传输速率(*10^6Bytes/s)
模式 1	4.75	4	4.2105
模式 2	4.75	18	4.2105
模式 3	8.013	8	4.2105
模式 4	8.013	22	4.2105
模式 5	12.226	11	4.2105
模式 6	12.226	25	4.2105
模式 7	8.948	5	7.6069
模式 8	8.948	19	7.6069
模式 9	12.211	9	7.6069
模式 10	12.211	23	7.6069
模式 11	16.424	12	7.6069
模式 12	16.424	26	7.6069

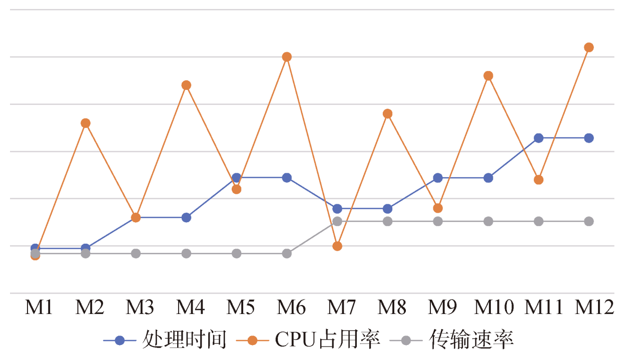


图 10　监控参数图

Figure 10 Monitor parameters diagram

由上述图表可以看出，首先，每次传输的数据块增大，处理时间会增大，CPU 占用增加不明显，但是数据传输速率会显著增大。其次，由于设置的两个数据块的传输速率都显著低于设置的两个带宽，因此带宽增大并没有带来传输效果的提升，却增加了 CPU 占用。最后，提高加密强度会增大任务处理时间和 CPU 占用率，这是实施高安全性的代价。

下面通过决策控制流程对策略进行自动化调整，设置 w_1=0，w_2=0.1，w_3=0.9。首先通过预测判决算法选出最优模式 12，计算出预期的预期参数值如表 5 所示。

表 5　预测参数值

Table 5　Predictive parameter value

QA_1	QA_2	QA_3
0.9659	0.9013	0.9598

在运行过程中监控三个属性参数，对参数进行归一化处理，得到的实际运行参数如表 6 所示。

表 6　实际运行参数值

Table 6　Actual running parameter value

QA_1	QA_2	QA_3
0.9	0.5	0.5

可以看出由于系统环境发生变化，监控的属性参数出现偏差，此时模糊认知图中的权重系数 cw_{ij} 已经不能反映实时环境变化，需要进行调整。通过对所有权值进行迭代调整的方法进行计算，得到新的权值，再进行模式的选择，选择出模式 1。此时计算出预期的参数值如表 7 所示。

表 7　调整后的预期参数值

Table 7　Predictive parameter value after adjusting

QA_1	QA_2	QA_3
0.9015	0.4998	0.5004

通过实验可以看出，当系统环境发生改变时，参数会偏离预期值，此时通过调整权重 cw_{ij} 使得参数预期值与运行时参数一致，使得系统可以正确反映运行环境。在此基础上，再对配置策略进行调整优化。通过细粒度的监控任务执行的参数可以感知系统环境的变化，在系统受到攻击导致系统环境发生改变时，可以通过配置策略进行调整优化。

在内置安全神经元的模块架构下，根据任务的主观预期，可以进行模块策略的定制，通过更改权重 w_1、w_2 和 w_3 来控制任务的主观预期。例如，某次任务对于保密性要求较高，可以将 w_1 设定为较大值，使安全值 SV 主要受保密性影响，基于此来选择最优的策略模式。

为了测试任务的主观预期性，实验定制了两个任务，任务一对保密性要求比较高，权重设置为 w_1=0.8, w_2=0.1, w_3=0.1, 此时模式 5 的安全值最大，策略定制为数据块大小 1×10^6 Bytes，传输带宽 900Kb，使用 256 位的 AES 加密。任务二对处理时间要求较高，则将权重设置为 w_1=0.1, w_2=0.1, w_3=0.8, 此时模式 1 的安全值最大，模式策略定制为数据块大小为 1×10^6 Bytes，传输带宽为 900Kb，不加密。可以看出通过设置 $w_{1,2,3}$ 的权重，能够选出符合主观预期的策略配置。

通过将安全部分结合到功能部件中，使得安全与信息系统体系高度融合，这是计算机免疫、拟态、可信计算等其它架构不具备的特征。在融合架构基础上能够细粒度的感知系统环境和系统任务的运行情况，通过遍布的类神经元安全部件可以对相应的功能部分进行细粒度的调控，通过策略的调整抵消攻击的影响，保证任务的预期执行。与可信计算、计算机免疫直接杀死异常进程相比，这是一种具有较高鲁棒性的自我调整修复过程。最终，在类人脑的安全决策中心的整体控制下，能够进行自主决策和联动的防御，抵御未知攻击，提高防御效率。

8 总结

本文针对现有“外壳式”防御体系无法应对信息系统大流量、富应用带来的安全挑战，研究并总结了人体神经控制系统的基本原理，提出一种基于仿生控制机理的内生免疫安全体系。该体系将神经元、脊神经、人脑的元素引入到信息系统网络的各个层次中，安全体系与系统功能高度融合，在基于系统基本功能元素模块化的基础上，以任务为导向进行细粒度的安全控制。通过对构建的模型进行分析表明，在满足单步安全转移、动作唯一性的条件下，本文提出的控制机理能够维持系统的安全性。

本文提出的内生免疫体系模型是一种全新的主动式安全框架，在后续的研究工作中，构建模块更多、更复杂的任务进行系统实现，以此观察任务和面对复杂攻击的效果。进一步，需要对基础功能模块进行组合和调整，引入人工智能的方法完善自主判断和策略配置的功能，实现自适应的安全策略配置和优化。

参考文献

[1] Forrest S, Somayaji A, Ackley D H. Building Diverse Computer Systems[C]. *The Sixth Workshop on Hot Topics in Operating Systems* (*Cat. No.97TB100133*), 1997: 67-72.

[2] Hofmeyr S A, Forrest S. Architecture for an Artificial Immune System[J]. *Evolutionary Computation*, 2000, 8(4): 443-473.

[3] Harmer P K, Williams P D, Gunsch G H, et al. An Artificial Immune System Architecture for Computer Security Applications[J]. *IEEE Transactions on Evolutionary Computation*, 2002, 6(3): 252-280.

[4] Liang Y W. Immune model for network information security [D]. Wuhan: Wuhan University, 2002.
(梁意文. 网络信息安全的免疫模型[D]. 武汉: 武汉大学, 2002.)

[5] Feng D G, Qin Y, Wang D, et al. Research on Trusted Computing Technology[J]. *Journal of Computer Research and Development*, 2011, 48(8): 1332-1349.
(冯登国, 秦宇, 汪丹, 等. 可信计算技术研究[J]. *计算机研究与发展*, 2011, 48(8): 1332-1349.)

[6] Shen C X. Using active immunity trusted computing to establish network security protection architecture for new infrastructure[J]. *Civil-Military Integration on Cyberspace*, 2020(4): 10-13.
(沈昌祥. 用主动免疫可信计算构筑新型基础设施网络安全保障体系[J]. *网信军民融合*, 2020(4): 10-13.)

[7] TCG TSS 2.0 Overview and Common Structures Specification. https://trustedcomputinggroup.org/resource/tss-overview-common-structures-specification. Oct. 2019.

[8] Yan Z, Govindaraju V, Zheng Q H, et al. IEEE Access Special Section Editorial: Trusted Computing[J]. *IEEE Access*, 2020, 8: 25722-25726.

[9] Wu Y L, Yan Z, Choo K K R, et al. IEEE Access Special Section Editorial: Internet-of-Things Big Data Trust Management[J]. *IEEE Access*, 2019, 7: 65223-65227.

[10] Hu J, Shen C X, Gong B. *Trusted computing 3.0 engineering fundamentals*[M]. Beijing: Posts & Telecom Press, 2017.
(胡俊, 沈昌祥, 公备. 可信计算 3.0 工程初步[M]. 北京: 人民邮电出版社, 2017.)

[11] Liu W, Yao Y Y, Zhao B H, et al. Active Defense Technology of Power Monitoring System with Adaptive Features[J]. *IEEE Access*, 2018, 6: 57778-57786.

[12] Buczak A L, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection[J]. *IEEE Communications Surveys & Tutorials*, 2016, 18(2): 1153-1176.

[13] Harel Y, Gal I B, Elovici Y. Cyber Security and the Role of Intelligent Systems in Addressing Its Challenges[J]. *ACM Transactions on Intelligent Systems and Technology*, 2017, 8(4): 1-12.

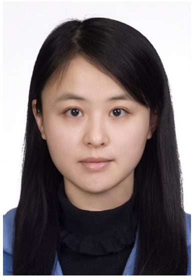
[14] Yue D, Han Q L. Guest Editorial Special Issue on New Trends in Energy Internet: Artificial Intelligence-Based Control, Network Security, and Management[J]. *IEEE Transactions on Systems*, *Man*, *and Cybernetics*: *Systems*, 2019, 49(8): 1551-1553.

[15] Jeschke S, Brecher C, Meisen T, et al. Industrial Internet of Things and Cyber Manufacturing Systems[J]. *Industrial Internet of Things*, 2017: 3-19.

[16] Zhou Z, Kuang X H, Sun L M, et al. Endogenous Security Defense Against Deductive Attack: When Artificial Intelligence Meets Active Defense for Online Service[J]. *IEEE Communications Magazine*, 2020, 58(6): 58-64.
[17] Horn P. Autonomic Computing: IBM\'s Perspective on the State of Information Technology[J]. *Computing Systems*, 2001, 2007(Jan): 1-40.
[18] Kapoor V. Services and Autonomic Computing: A Practical Approach for Designing Manageability[C]. *2005 IEEE International Conference on Services Computing*, 2005: 41-48.
[19] Coutinho E F, Gomes D G, de Souza J N. An Autonomic Computing-Based Architecture for Cloud Computing Elasticity[C]. *2015 Latin American Network Operations and Management Symposium*, 2015: 111-112.
[20] Tahir M, Mamoon Ashraf Q, Dabbagh M. Towards Enabling Autonomic Computing in IoT Ecosystem[C]. *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress*, 2019: 646-651.
[21] Mimic octopus. https://en.wikipedia.org/wiki/Mimic_octopus. Mar. 2020.
[22] Wu J X. Research on Cyber Mimic Defense[J]. *Journal of Cyber Security*, 2016, 1(4): 1-10.
(邬江兴. 网络空间拟态防御研究[J]. *信息安全学报*, 2016, 1(4): 1-10.)
[23] Yao D, Zhang Z, Zhang G F, et al. MVX-CFI: A Practical Active Defense Framework for Software Security[J]. *Journal of Cyber Security*, 2020, 5(4): 44-54.
(姚东, 张铮, 张高斐, 等. MVX-CFI: 一种实用的软件安全主动防御架构[J]. *信息安全学报*, 2020, 5(4): 44-54.)
[24] Hu H C, Wu J X, Wang Z P, et al. Mimic Defense: A Designed-in Cybersecurity Defense Framework[J]. *IET Information Security*, 2018, 12(3): 226-237.
[25] Hu H C, Wang Z P, Cheng G Z, et al. MNOS: A Mimic Network Operating System for Software Defined Networks[J]. *IET Information Security*, 2017, 11(6): 345-355.
[26] De Paula F S, de Castro L N, de Geus P L. An Intrusion Detection System Using Ideas from the Immune System[C]. *The 2004 Congress on Evolutionary Computation*, 2004: 1059-1066.
[27] Dutt I, Borah S, Maitra I K. Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model[J]. *IEEE Access*, 2020, 8: 34929-34941.
[28] Wei W H, Chen S, Lin Q Z, et al. Feature Selection Using an Improved Multi-Objective Immune Algorithm for Intrusion Detection[C]. *2019 IEEE Symposium Series on Computational Intelligence*, 2019: 1922-1927.
[29] Mohamed Y A, Abdullah A B. Immune Inspired Framework for Ad Hoc Network Security[C]. *2009 IEEE International Conference on Control and Automation*, 2009: 297-302.
[30] Li T. Dynamic Detection for Computer Virus Based on Immune System[J]. *Science in China Series F: Information Sciences*, 2008, 51(10): 1475-1486.
[31] Hou C Z, Zhang Y J. Biologically Inspired Immunity Based on Multi-Agent: A New Idea of Research on Computer Anti-Virus Measures[J]. *Journal of Beijing Institute of Technology*, 2002, 22(3): 270-273, 296.
(侯朝桢, 张雅静. 基于 multi-agent 的仿生物免疫: 计算机抗病毒研究新思路[J]. *北京理工大学学报*, 2002, 22(3): 270-273, 296.)
[32] Li T. Idid: a Immune Based Dynamic Intrusion Detection Model[J]. *Chinese Science Bulletin*, 2005, 50(17): 1912-1919.
(李涛. Idid: 一种基于免疫的动态入侵检测模型[J]. *科学通报*, 2005, 50(17): 1912-1919.)
[33] Gao M, Chen M X, Liu A, et al. Optimization of Microservice Composition Based on Artificial Immune Algorithm Considering Fuzziness and User Preference[J]. *IEEE Access*, 2020, 8: 26385-26404.
[34] Ye X M, Yang X F. SIRS Model of Computer Virus Propagation Based on Two-Stage Immunization[J]. *Journal of Computer Applications*, 2013, 33(3): 739-742.
(叶晓梦, 杨小帆. 基于两阶段免疫接种的 SIRS 计算机病毒传播模型[J]. *计算机应用*, 2013, 33(3): 739-742.)
[35] Jorge H Daruna. Introduction to Psychoneuroimmunology [M]. Salt Lake City: Academic Press, 2012: 15.
[36] Nicholls J G. From Neuron to Brain[M]. Cary: Sinauer Associates, 2001.
[37] Ren L Q, Liang Y H. *Introduction of bionics*[M]. Beijing: Science Press, 2016.
(任露泉, 梁云虹. 仿生学导论[M]. 北京: 科学出版社, 2016.)
[38] Rushby J. Noninterference, Transitivity, and Channel-Control Security Policies[M]. CSL-92-02, Menlo Park: Stanford Research Institute, 1992.
[39] Zhang X, Chen Y L, Shen C X. Non-Interference Trusted Model Based on Processes[J]. *Journal on Communications*, 2009, 30(3): 6-11.
(张兴, 陈幼雷, 沈昌祥. 基于进程的无干扰可信模型[J]. *通信学报*, 2009, 30(3): 6-11.)
[40] What is an Erlang. https://www.erlang.com/what-is-an-erlang/. Sep. 2020.

李涛 于 2012 年在东南大学信号与通信工程专业获得博士学位。现任东南大学网络空间安全学院副教授。研究领域为信息系统安全、内生安全。研究兴趣包括: 智能安全、内生安全。Email: lit@seu.edu.cn

胡爱群 于 1993 年在南京工学信号处理专业获得博士学位。现任东南大学网络空间安全学院教授。研究领域为信息系统安全、物理层安全。研究兴趣包括: 内生安全、物理层安全。Email: aqhu@seu.edu.cn



方兰婷 于 2018 年在东南大学信号与通信工程专业获得博士学位。现任东南大学网络空间安全学院讲师。研究领域为内生安全、人工智能。研究兴趣包括: 智能安全、数据挖掘。Email: 101012508@seu.edu.cn