融合神经与免疫机理的信息系统仿生免疫模型

A Bionic Information System Immune Model Integrating Neural and Immune Mechanisms

胡爱群/HU Aiqun，李涛/LI Tao，卞青原/BIAN Qingyuan
（东南大学，中国 南京 210096）
(Southeast University, Nanjing 210096, China)

DOI：10.12142/ZTETJ.202206009
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221207.1153.002.html
网络出版日期：2022-12-07
收稿日期：2022-10-20

摘要：针对现有信息系统缺乏有效主动防御模型、安全体系与信息系统融合不充分的问题，提出一种融合神经与免疫机理的仿生免疫模型。模仿人体神经控制系统与免疫系统高效的安全防御机理，借鉴其独特的“感知-策略-效应-反馈”工作机制与自适应的免疫算法，从整体架构入手，将安全体系和信息系统高度融合。通过各仿生安全组件的高效联动，实现信息感知分布性、控制适应性、防御主动性。实验结果表明，提出的融合神经与免疫机理的仿生免疫模型面对安全风险能够主动防御，自适应调整安全策略，维持系统任务的稳态运转。融合神经与免疫机理的仿生免疫模型为信息系统仿生免疫的实现提供了理论架构支撑。

关键词：信息系统安全；计算机免疫系统；仿生安全；安全模型

Abstract: A bionic immune model adapted from human immune mechanisms and neural control mechanisms is proposed in response to the problem of inadequate design and insufficient fusion in the current computer immune system. By imitating the unique working mechanism including the adaptive immune strategy and the pipeline of "perception-strategy-effect-feedback" from the human immune control system, our model allows for an improved security defense design with flexible control and active defense capabilities. Meanwhile, the efficient linkage of bionic safety components enables a heightened architectural integration of safety systems and information systems in our model. The experimental results show that the proposed bionic immune model integrating human immune and neural control mechanisms can achieve active defense against security risks and adaptive adjustment of security policies while maintaining the steady operation of the system, which provides a theoretical framework for the realization of the computer immune system.

Keywords: information system security; computer immune system; biometric security; security model

随着通信技术的飞速发展,运行在开放网络环境中的信息系统日趋复杂。承载数据量呈指数级增长,数据来源变得更加丰富,内容也更加细化。网络空间安全面临越来越多的新挑战。传统的安全防御体系在面对安全威胁时无法及时对承载巨大流量的信息系统进行细粒度地、深层次地主动安全防御。

为了解决传统网络安全防御体系存在的静态不变缺陷问题，全球科研团队相继开展了主动式防御研究工作。其中，生物免疫机理与计算机科学技术相融合的人工免疫系统[1-5]，为网络安全的相关研究提供了新思路。相较于传统的被动式防御技术，人工免疫网络攻击检测技术具有显著的智能监控、快速响应、主动防御等特点，因此在网络攻击检测领域得到了较好的应用。然而，受限于现有的信息系统架构，免疫系统中免疫细胞的动态游走等特性难以在信息系统中实现。目前的人工免疫系统往往只是在防御体系的某一个环节融入仿生免疫元素（例如在入侵检测中融入免疫算法），仍缺乏一种有效的体系架构作为支撑，并未实现真正意义上的免疫体系。

为解决上述问题，本文提出一种融合神经与免疫机理的仿生安全模型，借鉴人体神经系统的“感知-策略-控制-反馈”体系架构和免疫系统的自适应分层免疫思想，将安全体系与信息系统深度融合，构建具有自主防御能力的新型仿生免疫系统。

1 相关研究背景

仿生学是一门古老而又新兴的学科，主要研究生物体的

基金项目：东南大学移动信息通信与安全前沿科学中心项目（2242022k30007）

结构与功能机理，并将这种结构和功能应用到各类工程系统和现代技术的研究与设计中。目前，网络空间安全中的仿生技术应用主要体现在仿生自愈、拟态防御、计算机免疫等方面。

近年来，许多学者开始致力于仿生自愈的研究，以提高信息系统的主动防御能力。P. JAIN 等[6]提出一种网络安全自修复模型，将生物免疫系统中自监控、自适应、自修复的防御机制应用到网络攻击防御中。 DAI Y. S. 等[7-11]提出一种仿生自主神经系统（BANS）。该系统借鉴生物神经系统，结合模糊测试、神经网络、信息熵等技术，实现了信息系统的自我保护能力。系统能够识别拒绝服务攻击（DoS）、间谍软件、恶意软件和病毒等已知/未知攻击，并进行有效的自我防御。

邬江兴院士提出拟态防御理论[12-13]，通过动态异构冗余架构利用不可信软硬构件,组成高可靠、高安全等级信息系统，实现了对功能组件的主动隐匿，在较大程度上增加了攻击难度。近年来，众多研究者对拟态防御进行了深入研究。丁绍虎等[14]提出基于拟态防御的软件定义网络（SDN）控制层安全机制，使用多个异构的等价控制器同时处理数据层的请求，通过对比它们的流表项来检测主控制是否存在恶意行为，解决了 SDN 控制层的单点脆弱性问题。仝青和张铮等[15-16]基于动态冗余架构构建了拟态防御 Web 服务器，提出了适用于拟态防御架构的 Web 服务器测试方法，验证了拟态防御技术在 Web 服务器上的有效性和可行性。任权等[17]利用离散时间马尔可夫链模型对采用动态冗余架构的拟态防御系统进行建模，并对动态冗余架构的抗干扰性能进行分析，证明目标系统在攻击扰动条件下的稳态可用性和感知安全性。DAI W. B. 等[18]提出基于拟态防御的安全系统结构，通过数字孪生技术构建拟态防御模型的执行实体，提高安全系统的动态性与冗余性，进而提高系统的安全防御能力，增加攻击难度。

基于人工免疫系统（AIS）的入侵检测模型通过模拟人体免疫机制来进行网络入侵检测，在入侵检测方面拥有天然的适应性和鲁棒性。J. KIM 等[19-20]提出一种用于检测网络攻击行为的 AIS 系统模型。该模型结合了克隆选择过程、否定选择过程和基因库进化三大机制，同时应用了小生境否定选择算法。这是一套较为完善的、基于人工免疫技术的网络入侵检测模型。它具有良好的自适应性和学习能力。P. NESPOLI 等[21]提出一种新型的基于人工免疫系统的网络安全防御模型。该模型采用遗传算法等免疫算法来防御网络入侵，有效地降低了受保护系统的网络安全风险。罗娅等[22]提出一种基于核熵和人工免疫的网络异常检测方法。在基于入侵检测标准数据集 KDD Cup99 上的对比实验中，该方法有效地改进了网络异常检测的性能。于全等[23]提出基于人体免疫机理的网络安全防护体系设计原则，并基于该原则设计一种免疫启发式网络安全防护架构，模拟人体免疫系统的非特异性免疫与特异性免疫机制，构建分层网络安全防护体系。

从目前的研究情况来看，仿生自愈、拟态防御、计算机免疫等主动防御技术都是围绕生物的局部安全防御机制展开的，缺乏完整的免疫体系设计。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与免疫系统的工作机理，提出一种新型的仿生免疫模型。

2 免疫系统和神经控制的基本机理

2.1 人体免疫系统机理

人体免疫系统是一种具有高度分布性自适应免疫系统，具有完善的机制来抵御外来病原体的入侵。通过对人体免疫过程模型分析可知，免疫系统可以分为自然免疫（非特异性免疫）层和适应性免疫（特异性免疫）层，自然免疫层主要由补体和吞噬细胞等所组成，而适应性免疫层则包含抗体、T-细胞和B-细胞等。

自然免疫层是人体抵抗外来病原体入侵的第一道防线。在自然免疫过程中，免疫系统能够利用血液和组织中存在的各种白细胞来检测病原体，以便将其与自身细胞区分开。虽然这种方法不具有高度特异性，不能形成免疫记忆，但其能够迅速对感染做出反应。相对于自然免疫，适应性免疫过程较为缓慢，但其能够通过淋巴细胞的协作发挥作用，包括T-细胞、B-细胞等。在它们的共同作用下，使用专门的抗体来特异性检测病原体，并将病原体标记为威胁，能够放大反应并摧毁入侵者。该过程的重要特点之一，就是可以形成病原体的长久记忆。这使得免疫系统能够应对未来的挑战，以便更快速、更容易地对抗相同病原体。

面对微生物或外来病原体的入侵，免疫系统的这种自然免疫和适应性免疫的分层免疫机制与网络安全存在一定的相似性。自然免疫通过专家库形成防御能力，适应性免疫则是在动态对抗中形成新的防御方法。这对于构建新型计算机防御模型具有重要的借鉴作用。

2.2 人体神经控制系统机理

在面临威胁时，人体往往能够做出有效、适度的反应，以维持机体的高效运转。在人体防御过程中，神经控制系统既能使我们有效避开威胁，又可以不断提高应对威胁的能力。

在人体神经系统中，中枢神经系统是主体部分，其内部

聚集了大量神经细胞，主要负责信息的传导、储存、处理等工作。神经系统最基本的活动方式为反射。反射过程可以抽象为感受器、传入神经、反射中枢神经、传出神经、效应器、反馈六大基本环节。在反射过程中，人体通过感受器不断感受机体内外环境变化产生的刺激，然后将其转换成神经冲动并通过传入神经传至中枢，最终经过中间神经元的轴突所构成的感觉传导通路传至大脑皮质以产生感觉。大脑皮质对感觉信息进行分析与整合，然后通过传出神经构成的运动传导通路将整合好的信息传递出去，并通过运动神经元到达各类效应器产生效应。该效应行为会再次反馈至感受器。

此外，反射可以分为非条件反射和条件反射。其中，非条件反射是人体长期进化形成的本能反射，不需要大脑皮层等高级神经中枢的参与；而条件反射是人通过后天学习逐渐形成的高级神经活动，需要大脑皮层等高级神经中枢的参与。

2.3 仿生机理总结

通过对人体免疫系统和神经控制系统工作机理的研究分析，我们可以发现维持人体稳态运转、趋利避害的两大系统有许多可供仿生免疫系统借鉴的地方：

（1） 神经控制系统与免疫系统中均存在“感知–策略–反馈”机制。该机制能够对系统调节情况进行实时反馈，通过组件的联动配合应对环境变化，保证机体的生理平衡。

（2） 免疫系统的免疫过程能够区分“自我”与“非我”，对自体抗原呈现出特异性无应答状态，而对异体抗原能够保持免疫记忆、快速应答和及时清除。

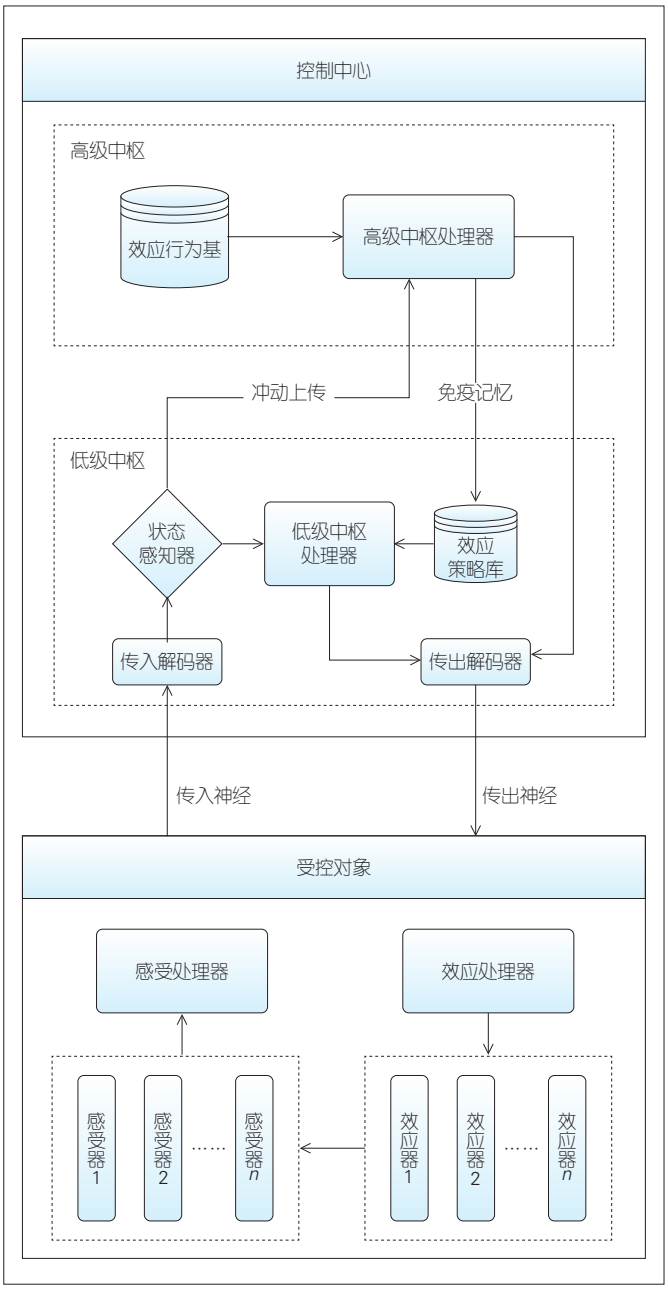
（3） 神经系统的体系架构实现了信息感知分布性、控制适应性、整体协调性，在架构设计方面为安全体系与信息系统的融合提供参考，有助于构建具有智能监控、快速响应、主动防御特点的仿生免疫系统。

3 融合神经与免疫机理的安全模型

3.1 仿生安全系统模型

结合生物免疫的应答过程和人体神经控制反射过程的工作机理，本文设计了融合神经与免疫机理的仿生安全模型。该模型以人体神经控制系统中的“感知–策略–效应–反馈”工作机制为基本架构，研究和部署类神经系统的细粒度威胁感受器和传导机制，实时监测系统内外参数变化，全面掌握系统的安全态势，以便对外部入侵进行合理反制，对内部入侵进行免疫式防御。借鉴人体免疫系统中的自然免疫与适应性免疫的免疫思想，构建分层安全防御体系，建立各种机制之间关联与分析方法，可使得各安全组件能够高效联动，在面对已知安全威胁时能够依据预定义策略库进行快速反制，在面对未知安全威胁时能够在动态对抗中形成新的防御方法。

如图1所示，仿生安全模型宏观分为受控对象与控制中心两部分。受控对象为仿生安全系统中保护的目标对象，其业务功能组件与仿生安全组件高度融合，并内置了海量细粒度感受器与效应器等安全组件。在受控对象进行正常业务的同时，感受器感知系统运行状态并将其上传至控制中心，效



▲图1 仿生免疫模型

应器根据控制中心的决策产生效应行为，对系统的异常状态进行及时调整，以保证受控对象业务功能的稳定运转。控制中心是仿生安全系统的核心，它可以根据受控对象上传的感受向量来研判系统当前的安全态势，通过两级安全控制中枢的联动配合生成对应的效应策略，实现对安全威胁的快速反制，并在对抗中进行自我学习、自我适应。

3.2 模型关键组件描述

3.2.1 受控对象

受控对象为仿生安全系统的底层组件，除常规的业务功能组件之外，还包含感受器R、感受处理器P_R、效应器E以及效应处理器P_E等仿生安全组件，以实现仿生安全系统控制架构中的感知与效应功能。

（1） 感知层面

为实现对受控对象的细粒度状态感知，仿生安全系统结合受控对象业务功能模块的特异性，在受控对象中部署若干定制化感受器R。感受器负责感知系统运行过程中的各种状态参数，如中央处理器（CPU）使用率、内存使用率、网络连接状况、函数参数、程序执行流以及效应器行为等，实现对受控对象运行状态的细粒度掌握。

感受器采集的原始状态参数错综复杂，若直接上传控制中心，不仅会增加传输神经的数据传输负担，还会给控制中心造成数据处理困难。受控对象中因此设置了感受处理器P_R，以负责对各感受器R_i采集的原始感受向量$r_i(t)$进行融合汇聚，并通过处理操作生成感受向量$V_R(t)$，如公式（1）所示。最后感受处理器将感受向量经传入神经上传至控制中心。至此，系统感知工作完成。

$$V_R(t) = pre\_process\left(r_1(t), r_2(t), \cdots, r_n(t)\right)。 \tag{1}$$

预处理操作的具体流程需要依据系统的具体业务场景需求进行设计，总体可以概述为如下几方面：

（a）感受向量分类。为了便于归一化、融合处理，感受处理器需要对接收到的初始感受向量（依据感受向量的属性）进行分类处理。

（b）感受向量融合。感受处理器会对分类后的感受向量进行融合汇聚。借鉴人体神经冲动上传机制中存在的“水潭效应”，感受处理器会结合特异性感受阈值σ_i来生成感受向量。其中，由于系统的各项状态参数指标会随系统业务的进行而发生变化，感受处理器需要依据状态参数的变化动态更新感受阈值，以实现感受层面的自适应。

融合汇聚操作可以抽象描述为：

$$x_i(t) = f\left(r_j(t),\ y_j(t)\right),\ j \in 1, 2, \cdots n\ 。 \tag{2}$$

感受向量生成操作可以简单描述如下：

$$R_i(t) = g\left(x_i(t),\ \sigma_i(t)\right),\ i \in 1, 2, \cdots k, \tag{3}$$

其中，$f(\cdot)$表示感受向量融合策略，依赖于类别i中的原始感受向量$r_j(t)$、向量权重$y_j(t)$；$g(\cdot)$表示感受向量生成策略，依赖于聚合向量$x_i(t)$和特异性阈值σ_i。$f(\cdot)$和$g(\cdot)$的具体形式要依据实际需求来设计。

（c）感受向量编码。为了便于数据传输和控制中心分析处理，感受处理器最后会对感受向量进行进一步的编码处理，如公式（4）所示：

$$V_R(t) = encode\left(R_1(t), R_2(t), \cdots, R_k(t)\right)。 \tag{4}$$

（2） 效应层面

为了实现受控对象对安全威胁的快速反制，我们在受控对象中设置了效应安全组件：效应处理器P_E和效应器E。结合受控对象的具体业务，若干效应器被放置在仿生安全系统中受控对象的安全薄弱处与业务核心区。当系统面对安全威胁时，效应器能依据控制中心的效应向量执行具体的效应行为，调整受控对象运行状态，抵御外来安全威胁。

类似于感知安全组件设计，效应安全组件中还设置了效应处理器，以负责解析处理控制中心下发的效应向量。这种做法有利于效应器专注自身效应行为的执行。效应处理器的功能具体包括两个方面：

（a）效应向量译码。为了便于数据的传输，控制中心会对效应向量进行编码整合。在接收到效应向量后，效应处理器首先需要对效应向量进行译码分析，并将其映射为类似效应器的效应行为。

（b）效应指令分发。根据译码结果，唤醒受控对象中相应效应器并执行正确的效应行为，可实现对系统的调控和对安全威胁的快速反制。

3.2.2 控制中心

控制中心是仿生安全系统的核心安全组件，它通过分析受控对象上传的感受向量来感知系统当前的运行状态，下发效应策略以指导受控对象反制安全威胁。借鉴人体免疫系统和神经系统的工作机理，控制中心采用分层结构，包含低级中枢和高级中枢两个安全策略中枢。

（1） 低级中枢

低级中枢包含编/解码器、状态感知器SA、效应策略库P和低级中枢处理器L等仿生安全组件，主要负责态势感知及

已知异常状态的应对处理。其中编/解码器负责对传输神经上的数据进行编/解码操作；状态感知器通过细粒度感受器采集的感受向量来感知受控对象运行状态，并分发异常状态参数至对应的中枢处理器；低级中枢处理器L负责处理系统已知异常状态，依据效应策略库中专家预定义或免疫记忆形成的策略生成效应向量，实现对已知安全威胁的快速反制。低级中枢的工作流程可概述如下：

（a）低级中枢接收到受控对象上传的感受向量$V_R(t)$后，传入解码器D，并对其进行如公式（4）所示的逆操作进行解码，以便后续状态的感知分析。

（b）状态感知器SA利用解码后的感受向量进行态势感知。当前状态$s(t)$若为已知异常状态，则将交由低级中枢处理器L处理；若为未知异常状态，则状态及相关参数均会被上传至高级中枢处理。

$$s(t) = state\_detect\left(R_1(t), R_2(t), \cdots, R_k(t)\right)。 \tag{5}$$

（c）对于已知异常状态$s(t)$，低级中枢处理器L首先通过效应策略库匹配获取相应的策略信息，然后调用免疫函数生成效应策略，最后通过编码器编码生成效应向量$V_E(t+1)$。该过程可描述为：

$$V_E(t+1) = encode\left(low\_immu\left(s(t), \{policy(s(t))\}, \cdots\right)\right), \tag{6}$$

其中，$policy(\cdot)$为策略匹配函数，$low_immu(\cdot)$为初级免疫函数，相关参数包含但不限于系统状态$s(t)$、策略信息$p(t)$。

（2） 高级中枢

高级中枢负责应对系统的未知异常状态。通过仿生安全系统的免疫函数和“内反馈”机制，高级中枢在动态对抗中形成面向未知威胁的新型防御策略，包含效应行为基A和高级中枢处理器H等仿生安全组件。

效应行为基是映射到效应器效应行为的一组预定义效应行为集合，是高级中枢处理器生成效应策略的基础。其目的是保证受控对象在遭受未知安全威胁时，高级中枢处理器生成的效应策略不会危害业务的正常运转。若效应行为基$A = \{a_1, a_2, \cdots, a_m\}$包含$m$个预定义效应行为，则高级中枢做出的效应策略$p(t)$可抽象表示为：

$$p(t) = \sum_{i=1}^{m} x_i \cdot a_i, \tag{7}$$

其中，x_i为效应行为a_i的权重系数。

高级中枢处理器H为高级中枢的核心，负责生成应对未知威胁的效应策略。按照功能划分，高级中枢可以分为异常分析模块、策略生成模块以及免疫记忆模块。

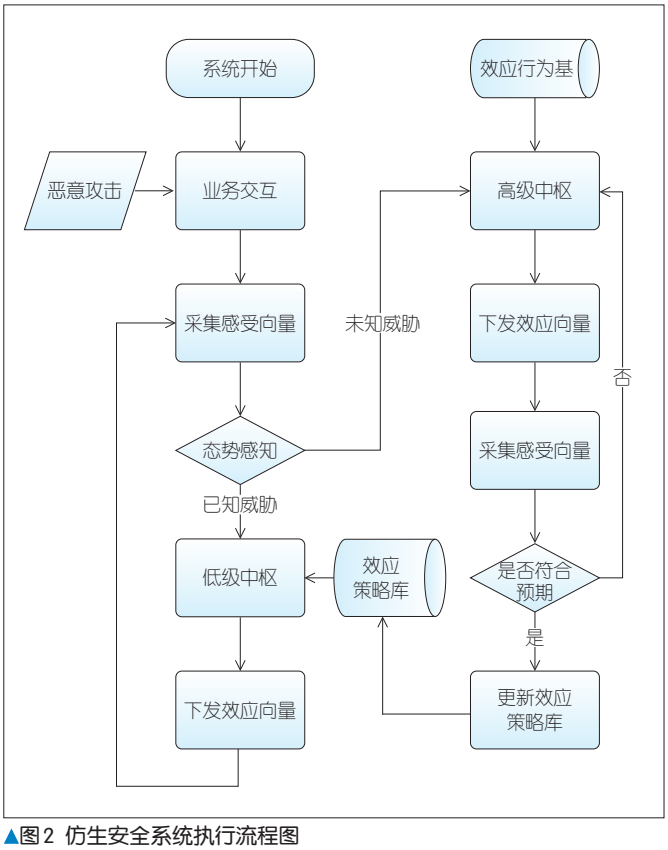
（a）在高级中枢接收到由低级中枢上传的异常状态数据后，异常分析模块会对感受器采集的状态参数进行分析，以寻找异常状态参数之间的关联，推断系统异常根源。

（b）结合异常分析的结果，策略生成模块可调用免疫策略函数生成效应策略，修正系统未知异常状态，反制未知安全威胁。其中，免疫策略函数的核心在于能够基于效应行为基生成有效的效应策略，并能够依据受控对象的反馈不断优化策略。

（c）免疫记忆模块负责效应策略的缓存与更新下发。抵御未知攻击是一个动态对抗的过程。缓存反制过程中的效应策略非常有利于更新工作。此外，对于能够有效反制当前未知安全威胁的安全策略，免疫记忆模块会将其下放至低级中枢，形成免疫记忆，当系统再次受到该威胁时能够实现快速反制。

3.3 模型动态描述

为了更好地描述仿生安全组件之间的关系和仿生免疫系统的工作机制，我们给出了相关系统的运行流程图，如图2所示。



▲图2 仿生安全系统执行流程图

在系统业务交互过程中，仿生安全感受器持续对系统运行情况进行感知。与异常状态信号对应的感受器感知到异常状态后，系统将原始参数传递到感受处理器。经过感受处理器预处理、编码后生成的感受向量，会经传入神经传至控制中枢。在接收到感受向量后，控制中枢首先对其进行解码与分析，并通过态势感知组件对系统安全状况进研判：若为已知风险，低级中枢就会依据效应策略库直接采取应对措施，下发效应向量；若为未知威胁，高级中枢会进行处理。高级中枢处理器根据异常情况并基于效应行为基采取安全策略，下发效应向量，根据反馈持续优化安全策略。当系统恢复稳态时，高级中枢更新效应策略库，产生免疫记忆。

4 原型系统实现与验证

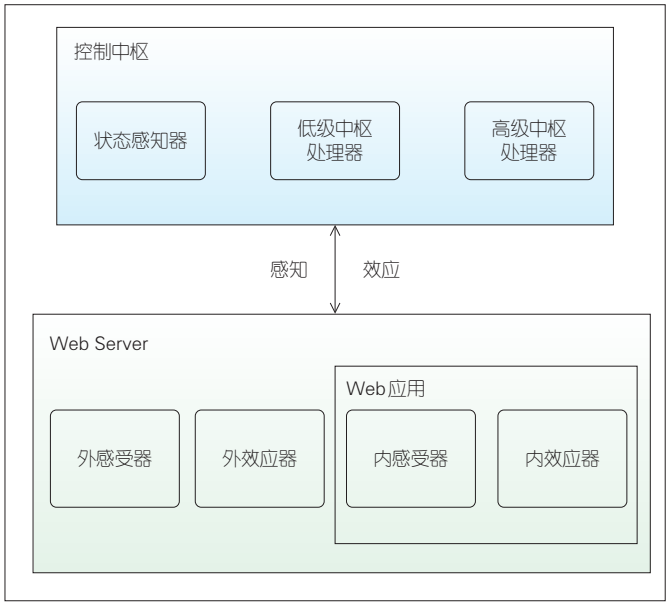
4.1 原型系统实现

为验证理论模型的有效性和可行性，我们基于Web Server设计构建了仿生安全原型系统，如图3所示。该系统不仅在业务功能层面上支持常规的Web应用部署，还融合了仿生安全元素，即在业务功能模块与系统模块中加入了仿生安全组件，以感知、调控系统运行状态。

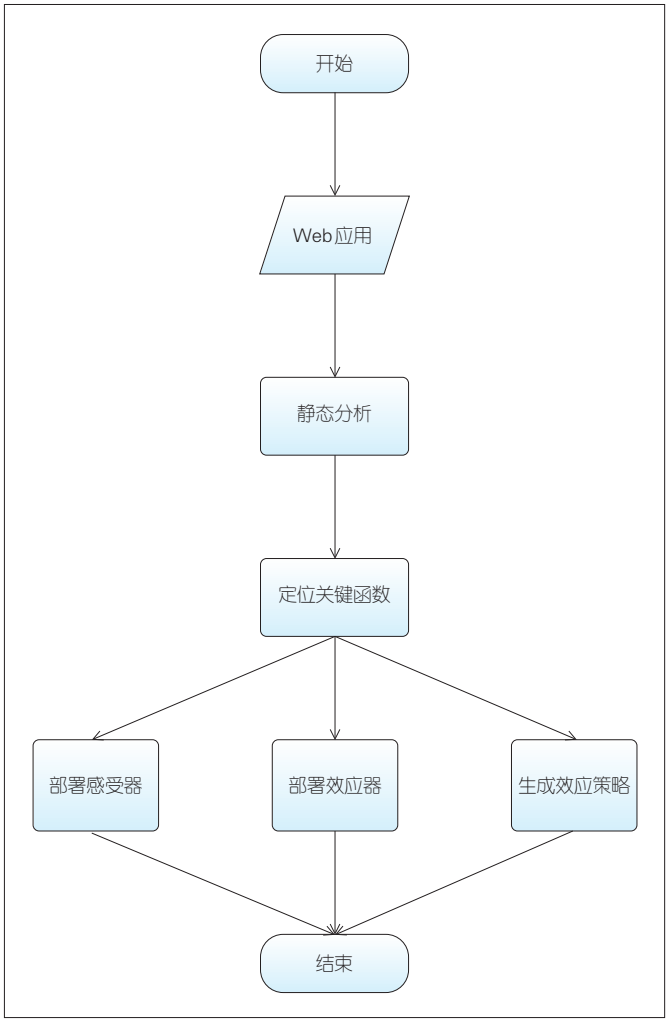
（1）受控对象层面

为了实现对系统运行期间的应用执行参数、系统运行状态的感知，原型系统在业务功能层面和系统层面分别部署了内感受器/效应器与外感受器/效应器。

内感受器与业务功能耦合，能够结合业务应用的静态分析结果，定位业务组件中具有安全隐患的关键函数，安插定制化感受器/效应器，生成对应效应安全策略，如图4所示。在业务运行期间，内感受器在程序执行流层面进行感知，当监测到关键函数执行“非我”的异常指令时，及时上报控制中心并结合策略库的安全策略进行处置。外感受器负责感知宏观层面的系统运行状态，如CPU用量、内存用量、线程池状态、网络请求参数等。结合控制中心下达的效应策略，外效应器在系统层面进行调控，以保证系统稳态运行、业务功能正常交互。



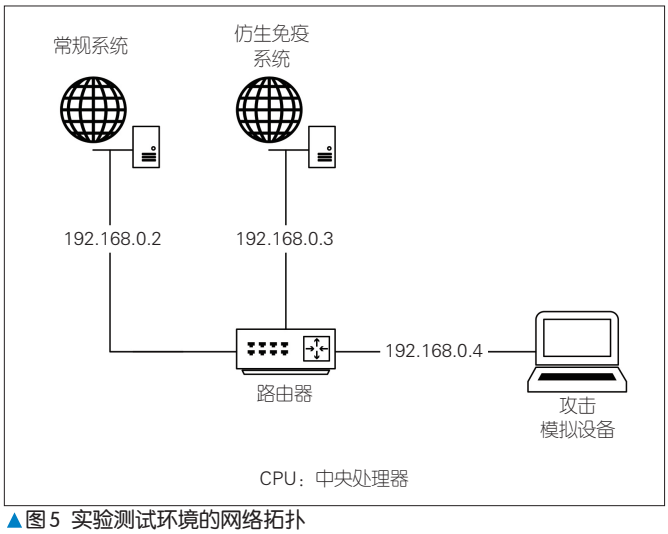
▲图3 仿生免疫系统框架



▲图4 内感受器的部署流程

（2）控制中心层面

结合内感受器的设计，控制中心层面实现了相应的执行流处理器，可负责解析内感受器采集的感受向量，分析关键函数的调用参数、报错等信息，调用静态分析阶段结合Web漏洞相关先验知识生成的效应策略，在执行流层面对非法的函数执行进行快速拦截，阻止已知安全威胁的攻击进程。



▲图5 实验测试环境的网络拓扑

4.2 系统测试

4.2.1 测试环境

实验测试环境的网络拓扑如图5所示。常规系统与仿生免疫系统的硬件配置相同，均为Ubuntu 20.04操作系统、8核Intel Core 2 Duo T7700处理器、8 GB内存。其中，仿生免疫系统是以常规系统为基础改造而成的，两系统均运行相同的Web业务应用。攻击模拟设备为MacBook Pro（14-inch，2021），该设备配有Apple M1 Pro处理器、32 GB内存。

4.2.2 性能开销

融合神经与免疫机理的仿生安全系统会在业务系统中部署感受器和效应器等仿生安全组件。相较于常规系统，仿生安全系统会造成额外的性能开销。为了探究仿生安全组件对业务的影响，我们测试了运行相同业务的常规系统和仿生安全系统的平均性能开销，结果如表1所示。可以看出，相较于常规系统，仿生安全系统的CPU占用率、内存用量以及业务响应时间均有所增加，但没有对系统业务造成影响。

▼表1 两种系统的性能开销对比

	CPU占用率/%	内存用量/MB	响应时间/ms
常规业务系统	5.1	251.5	153
仿生安全系统	6.3	278.5	171

CPU：中央处理器

4.2.3 已知威胁反制

仿生安全系统的效应策略库记录了一些安全威胁的反制措施。当受控对象受到这些已知安全威胁入侵时，仿生安全系统能够快速应对，保证业务的正常运行。为了检测仿生安全系统对于已知威胁的防御效果，我们在系统中部署了漏洞靶场WebGoat和一些存在已知漏洞的业务，漏洞清单如表2所示。此外，我们还部署了一些无漏洞的业务，用于测试系统的误报率。经过攻击脚本的攻击测试后，仿生安全系统对已知安全威胁的防护效果如表3所示。

4.2.4 未知威胁反制

面对效应策略库未曾记录的未知安全威胁，仿生安全系统的高级中枢能够基于效应行为基做出效应策略，并根据感受器的反馈信息不断调整优化。结合原型系统的Web业务场景，我们通过压力测试软件JMeter来模拟业务系统DoS攻击，检验仿生安全系统的未知安全威胁防御能力。

▼表3 已知安全威胁测试结果

漏洞类型	检出率/%	误报率/%
SQL注入漏洞	100	0
OGNL注入漏洞	100	0
JNDI注入漏洞	100	6
XXE 漏洞	100	0
SSRF漏洞	78	11
反序列化漏洞	87	28
远程代码执行漏洞	88	0

JNDI：Java命名和目录接口　SSRF：服务端请求伪造
OGNL：对象导航图语言　XXE：XML外部实体注入
SQL：结构化查询语言

▼表2 测试漏洞清单

漏洞类型	漏洞编号	漏洞描述
OGNL注入漏洞	CVE-2017-5638	Apache Struts2 S2-045代码执行漏洞
OGNL注入漏洞	CVE-2020-17530	Apache Struts2 S2-062代码执行漏洞
反序列化漏洞	CVE-2020-9548	Jackson 反序列化漏洞
反序列化漏洞	CVE-2022-25845	Fastjson反序列化漏洞
远程代码执行漏洞	CVE-2022-21350	Oracle WebLogic 远程代码执行漏洞
JNDI注入漏洞	CVE-2021-44228	Log4j2 JNDI注入漏洞

CVE：通用漏洞披露　JNDI：Java 命名和目录接口　OGNL：对象导航图语言

我们采用不同的压力测试线程数来模拟不同的DoS攻击强度，分别对运行有相同业务组件的常规系统和仿生安全系统进行每组100 s的压力测试。业务系统的平均响应时间如表4所示。当测试线程数为40时，请求强度处于系统的正常业务范围中，仿生安全系统的响应相较于常规系统有所延迟。这是由于安全组件会造成一定的性能损耗。当测试线程数达到80时，业务系统处于异常状态，常规系统的业务功能受到影响，响应时间大幅增加，而仿生安全系统的业务功能未受到明显影响。这说明高级中枢做出了有效的效应策略，纠正了系统的异常状态。

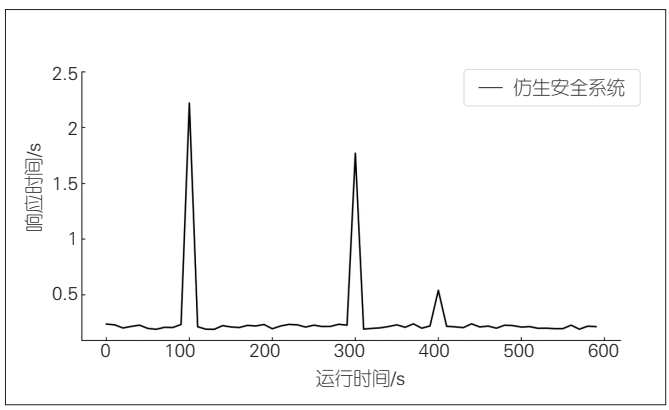
压力测试过程中，仿生安全系统的业务功能响应时间变化如图6所示。从图中可以看出，当系统遭受未知攻击并处于异常状态时，控制中心的效应策略存在调整优化过程。此过程中系统的业务功能会受到攻击的影响。当效应策略行而有效时，高级中枢会将其下放到效应策略库中，以便当再次面对此攻击时，能够更快速地采取正确的效应措施，保证系统的稳态运转。

4.3 实验结论

依据仿生安全理论模型的设计思想，我们构建了具有Web Server功能的仿生安全原型系统，并结合相关测试样例对系统的性能开销、已知威胁反制能力以及未知威胁反制能力进行了测试。实验结果验证了融合神经与免疫机理的仿生安全模型的可行性、安全性，在性能开销方面该模型仍然具有改进空间。

▼表4 系统平均响应时间

压力测试线程数	常规系统响应时间/s	仿生安全系统响应时间/s
40	0.15	0.17
80	13.04	0.19
120	55.17	0.21
160	54.81	0.19
200	54.16	0.19
240	54.47	0.20



▲图6 仿生安全系统响应时间

5 结束语

借鉴神经系统中“感知–策略–效应–反馈”的体系架构以及免疫系统的免疫机制，本文提出了一种融合神经与免疫机理的仿生安全理论模型，将安全体系与信息系统深度融合，构建了具有自主防御能力的新型仿生免疫系统，并基于该模型设计实现了仿生安全原型系统。相关实验验证了融合神经与免疫机理的仿生安全理论模型的有效性与可行性。

本文提出的仿生安全模型是一种宏观的主动安全框架。后续的研究工作还需要结合具体的场景，构建更加细化的组件设计与系统实现。此外，归纳总结免疫算法、引入人工智能方法均有助于实现系统安全策略的自适应配置与优化。

参考文献

[1] GHOSH D. Self-healing systems—survey and synthesis [J]. Decision support systems, 2007, 42(4): 2164-2185. DOI: 10.1016/j.dss.2006.06.011
[2] 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. DOI: 10.1109/ACCESS.2020.2973608
[3] ALIYU F, SHELTAMI T, DERICHE M, et al. Human immune-based intrusion detection and prevention system for fog computing [J]. Journal of network and systems management, 2022, 30(1): 11. DOI: 10.1007/s10922-021-09616-6
[4] LI D. Continual learning classification method with new labeled data based on the artificial immune system [J]. Applied soft computing, 2020, 94: 106423. DOI: 10.1016/j.asoc.2020.106423
[5] 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. DOI: 10.3321/j.issn: 0023-074X.2005.17.020
[6] JAIN P, SINGH P K, ABRAHAM A. Intrusion detection and self healing model for network security [C]//Proceedings of 2011 7th International Conference on Next Generation Web Services Practices. IEEE, 2011: 320-325. DOI: 10.1109/NWeSP.2011.6088198
[7] DAI Y S, XIANG Y P, PAN Y. Bionic autonomic nervous systems for self-defense against DoS, spyware, malware, virus, and fishing [J]. ACM transactions on autonomous and adaptive systems, 2014, 9(1): 1-20. DOI: 10.1145/2567924
[8] DAI Y S, XIANG Y P, LI Y F, et al. Consequence oriented self-healing and autonomous diagnosis for highly reliable systems and software [J]. IEEE transactions on reliability, 2011, 60(2): 369-380. DOI: 10.1109/TR.2011.2136490
[9] SUN P, DAI Y S, QIU X W. Optimal scheduling and management on correlating reliability, performance, and energy consumption for multiagent cloud systems [J]. IEEE transactions on reliability, 2017, 66(2): 547-558. DOI: 10.1109/TR.2017.2678480
[10] DAI Y S, HINCHEY M, MADHUSOODAN M, et al. A prototype model for self-healing and self-reproduction in swarm robotics system [C]// Proceedings of 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. IEEE, 2006: 3-10. DOI: 10.1109/DASC.2006.10
[11] DAI Y S, HINCHEY M, QI M R, et al. Autonomic security and self-protection based on feature-recognition with virtual neurons [C]// Proceedings of 2006 2nd IEEE International Symposium on Dependable,

Autonomic and Secure Computing. IEEE, 2006: 227–234. DOI: 10.1109/DASC.2006.24
[12] 邬江兴. 网络空间拟态安全防御 [J]. 保密科学技术, 2014(10): 4–9+1
[13] 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. DOI: 10.19363/j.cnki.cn10–1380/tn.2016.04.001
[14] 丁绍虎, 李军飞, 季新生. 基于拟态防御的SDN控制层安全机制研究 [J]. 信息安全学报, 2019, 4(4): 84–93. DOI: 10.19363/J. cnki. cn10–1380/tn.2019.07.06
[15] 仝青, 张铮, 张为华, 等. 拟态防御Web服务器设计与实现 [J]. 软件学报, 2017, 28(4): 883–897. DOI: 10.13328/j.cnki.jos.005192
[16] 张铮, 马博林, 邬江兴. web服务器拟态防御原理验证系统测试与分析 [J]. 信息安全学报, 2017, 2(1): 13–28. DOI: 10.19363/j. cnki. cn10–1380/tn.2017.01.002
[17] 任权, 贺磊, 邬江兴. 基于离散马尔可夫链的不同抗干扰系统模型分析 [J]. 网络与信息安全学报, 2018, 4(4): 30–37. DOI: 10.11959/j. issn. 2096–109x.2018035
[18] DAI W B, LI S Y, LU L, et al. Research on application of mimic defense in industrial control system security [C]//Proceedings of 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA). IEEE, 2022: 573–577. DOI: 10.1109/ICIBA52610.2021.9688212
[19] KIM J, BENTLEY P J. Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection [C]// Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600). IEEE, 2002: 1015–1020. DOI: 10.1109/CEC.2002.1004382
[20] KIM J, BENTLEY P. Immune memory and gene library evolution in the dynamic clonal selection algorithm [J]. Genetic programming and evolvable machines, 2004, 5(4): 361–391. DOI: 10.1023/B: GENP.0000036019.81454.41
[21] NESPOLI P, MÁRMOL F G, VIDAL J M. A bio–inspired reaction against cyberattacks: AIS–powered optimal countermeasures selection [J]. IEEE access, 2021, 9: 60971–60996. DOI: 10.1109/ACCESS.2021.3074021
[22] 罗娅, 陈文. 一种基于核熵和人工免疫的网络异常检测方法 [J]. 西南师范大学学报(自然科学版), 2016, 41(6): 119–124. DOI: 10.13718/j. cnki.xsxb.2016.06.019
[23] YU Q, REN J, ZHANG J Y, et al. An immunology–inspired network security architecture [J]. IEEE wireless communications, 2020, 27(5): 168–173. DOI: 10.1109/MWC.001.2000046

作 者 简 介

胡爱群，东南大学网络空间安全学院教授；主要研究领域为信息系统安全、物理层安全、内生安全等；主持和参与国家“863”计划、国家自然科学基金、国家支撑计划、国家发展改革委信息安全专项、企业合作项目数十项；发表学术论文100余篇，获授权国家发明专利40余项。

李涛，东南大学网络空间安全学院副教授；主要研究领域为信息系统安全、内生安全、智能安全。

卞青原，东南大学网络空间安全学院在读硕士研究生；主要研究方向为内生安全。

➡上接第35页

在超过百家的大型政企机构的“十四五”网络安全规划、3—5年中长期网络安全规划设计、重点领域的网络安全专项设计与建设当中，包括大型部委、能源央企、制造业央企、大型民营智能制造企业、银行与金融机构、数字城市等的数字化新型网络安全体系的构建。

在2022年北京冬奥会的网络安全保障工作中，内生安全也发挥了重要作用。人们基于内生安全框架，系统性、全局性地设计了冬奥会网络安全保障体系，统筹部署了整体安全运行工作。通过基于内生安全的“联合作战、精准防护、深度运营”，在冬奥会期间，分析日志的数据总量超过1 850亿条，修复中高危漏洞5 800余个，累计监测网络攻击尝试超3.8亿次，跟踪、研判、处置重点网络安全事件105件，最终实现了奥运网络安全保障历史上第一次“零事故”的成果。

未来内生安全的理念、框架，以及配套的能力体系模型、工具、参考架构、纲要库等，也会继续为中国重要政企机构网络安全保障、关键信息基础设施保护、重大活动网络安全保障贡献更多的力量。

参考文献

[1] 奇安信战略咨询规划部. 内生安全 新一代网络安全框架体系与实践 [M]. 北京: 人民邮电出版社, 2021
[2] 钱学森. 论系统工程 [M]. 长沙: 湖南科学技术出版社, 1982
[3] 朱一凡. NASA系统工程手册 [M]. 北京: 电子工业出版社, 2012
[4] ZACHMAN J A. A framework for information systems architecture [J]. IBM systems journal, 26(3): 276–292. DOI: 10.1147/sj.263.0276
[5] LEE M R. The sliding scale of cyber security [R]. SANS Institute, 2015

作 者 简 介

韩永刚，奇安信科技集团副总裁、战略咨询规划业务负责人，中国计算机学会计算机安全专业委员会委员、中国计算机行业协会数据安全专业委员会数据安全产业专家委委员；有近20年的网络安全领域经验，专注于数字化转型中的新一代网络安全体系规划设计与构建、内生安全体系、态势感知与大数据安全分析、数据安全、城市安全运营等方向；曾带领团队开展中石化“十四五”网络安全规划，南方电网“十四五”网络安全规划，中国人民银行业务网网络安全三年规划等多个大型部委、央企、数字城市的网络安全规划与体系设计。