

基于免疫系统控制机理的仿生安全模型研究

李涛, 王昕皖, 胡爱群

(东南大学网络空间安全学院, 江苏 南京 210000)

摘要: 随着信息系统架构的日益复杂, 传统的外壳式防御弊端逐渐显现, 主要表现为集中于外部边界的防御难以应对渗透网络内部的威胁和新型未知的高级威胁、边界被攻破易出现单点故障、缺乏综合性和全面性的安全保障。要从根本上解决这些问题, 需要变被动为主动, 采取更多层次和更综合的防御策略。基于免疫系统控制机理的仿生安全模型被提出, 其基于人体免疫系统的控制机理, 借鉴分布于人体各处的树突状免疫细胞捕获病原体、遍布于人体结构的血管以血液承载信息实现信息的传递与互通、具有中枢效应的淋巴系统综合处理和分析信息并进行决策, 构建具有自主防御功能的系统。以任务为导向, 将系统划分为任务组件、转发组件和分布式控制组件3部分, 并实现各部分的高度链接与融合。调用任务组件执行基本任务, 在执行过程中感知并提取安全数据。安全数据经转发组件初步处理和判断后, 被转发至控制组件。控制组件基于安全决策树生成决策进行校准, 从而实现针对异常情况的主动防御。实验结果表明, 此模型对系统异常攻击的防御成功率达98.9%, 并基本实现仿生免疫模型从捕获、提呈、传递、分析、决策到效应的全链路机制。

关键词: 仿生安全; 免疫; 系统安全模型; 主动防御

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025017

Biomimetic security model based on immune system control mechanism

LI Tao, WANG Xinwan, HU Aiqun

School of Cyber Science and Technology, Southeast University, Nanjing 210000, China

Abstract: The limitations of traditional perimeter-based defense mechanisms have gradually become apparent as information system architectures have become increasingly complex, with defense concentrated on the external boundary becoming difficult to deal with threats that penetrate into the network interior, new and unknown advanced threats, the breach of the boundary being prone to a single point of failure, and a lack of comprehensive and all-round security guarantees. A biomimetic security model based on the control mechanisms of the immune system was pro-

收稿日期: 2024-09-12; 修回日期: 2015-01-08

通信作者: 王昕皖, 220215273@seu.edu.cn

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)

Foundation Item: Project of Frontiers in Mobile Information, Communication, and Security Science Center at Southeast University (2242022k30007)

引用格式: 李涛, 王昕皖, 胡爱群. 基于免疫系统控制机理的仿生安全模型研究[J]. 网络与信息安全学报, 2025, 11(2): 50-60.

Citation Format: LI T, WANG X W, HU A Q. Biomimetic security model based on immunesystem control mechanism[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 50-60.

posed to address these problems. The model was designed to achieve information learning by mimicking the functions of dendritic immune cells distributed throughout the human body to capture pathogens, the blood vessels that carry information transmission and intercommunication, and the lymphatic system that comprehensively analyzes and processes information and makes decisions. A system with autonomous defense functions was thus built. Task-oriented, the system was divided into three components: task component, forwarding component, and distributed control component, with all parts being highly interconnected and integrated. The task component was designed to perform basic tasks and extract security information during execution. The security information was initially processed and judged by the forwarding component and then forwarded to the control component. The control component generated decisions based on the security decision tree for calibration, thereby achieving active defense against abnormal situations. The experimental results showed that the success rate of the proposed model in defending against system anomaly attacks reached 98.9%. Furthermore, the model fundamentally realized the full-chain mechanism of the biomimetic immune model, from capture, presentation, and transmission to analysis, decision-making, and effectuation.

Keywords: biomimetic security, immunity, system security model, proactive defense

0 引言

随着信息技术的不断发展和进步,信息系统的数字化、多应用化程度逐渐提升,针对信息系统的网络攻击也愈加隐蔽和复杂化,传统外壳防御的弊端逐渐显现,具体表现为:①无法有效应对高级持续性威胁和零日漏洞攻击;②难以主动、高效地检测和防止内部威胁;③无法满足物联网安全需求;④过度集中于外部边界保护;⑤无法全面防御人为因素引起的攻击。因此,采取更加综合和多层次的防御策略,变被动防御为主动防御成为目前的研究方向。

主动防御提倡在攻击者发动攻击之前,为系统构建防御体系,达到及时预警和防护、降低攻击破坏力的目的。Farmer等^[1]早期基于Jerne的网络假设提出的免疫系统动态模型为计算机免疫学的发展奠定了重要基础,其基于免疫网络、复制选择原理等算法动态适应网络环境变化,实现有效检测与预防未知攻击。但受信息系统架构的限制,目前免疫防御技术多用于入侵检测,未能与基本信息系统进行融合。可信计算是主动防御的另一代表性技术。该技术通过构建信任根,并沿着可信链将信任关系延伸至系统应用,实现可信环境中的系统安全。但目前的可信验证机制多依赖于硬件设备,若根用户身份验证信息泄露,将导致整个机制失效。

现有的主动防御(如免疫防御、可信计算等)由于缺乏与基本信息系统的内在融合,信息系统难以在保证运行性能的基础上进行安全防

控。因此,需要在原有信息系统的基础上,构建基础功能与防御功能高度融合的内生安全防御体系。

本文借鉴人体免疫系统(artificial immune system, AIS)控制机理,提出了一种适用于信息系统的仿生免疫安全模型。该模型模拟人体“内生”的特性,将安全元素纳入功能模块,通过在信息系统部署海量感知器感知任务的执行情况,并通过组件间的联动与配合实现对信息系统运行环境与执行状态的监测与调控,使系统可以按照预期正确、安全地运行,达到仿生免疫机制的效果。

本文主要贡献如下。

1) 提出一种基于人体免疫系统的多层次仿生安全模型,突破传统外壳式防御的被动性,通过模块化重构实现安全功能与基础系统的内生融合。

2) 构建分布式协同的主动防御体系,设计多个分布式安全中心,动态分配资源并基于安全决策树生成自适应策略,形成“感知-传递-分析-决策-效应”的全链路闭环防御机制。

3) 通过docker容器化部署实现组件间物理隔离与功能联动,搭建仿生安全的信息系统。测试结果表明,模型在安全增强的同时维持了基础性能。

1 相关研究

仿生学是一门跨学科的科学,主要研究自然界中的生物结构、功能、行为和进化机制,并将原理应用于工程技术等领域。目前,在网络安全

领域, 仿生学的应用主要有拟态防御、人工免疫系统、仿生安全防护系统等。

拟态防御是一种主动防御机制, 最早由邬江兴^[2]院士团队提出, 通过类比生物在色彩、纹理、形状等方面模仿另一生物或环境的方式, 主动隐匿目标对象的系统架构、运行方式及核心算法, 以实现主动防御。Malik 等^[3]通过改变系统的运行状态、配置或组件, 有效地减少了攻击者利用漏洞的时间窗口。此后, 相关研究在更多应用场景融入了拟态防御思想, 如三模冗余异构拟态 Web 服务器、拟态化 SaaS 云内生安全架构、基于机器学习与拟态防御融合的动态互联网防御策略、基于拟态防御的物联网终端安全防护^[4-7]。

人工免疫系统将免疫系统的结构和功能抽象为计算系统。1997 年, Forrest 等^[8]设计了首个计算机免疫系统。后来, 该系统吸引了越来越多的学者投入研究。在免疫学与入侵检测结合的方向, Ou^[9]通过模拟免疫系统中的树突状细胞检测并分类危险信号来设计自适应代理系统。Zhang 等^[10]提出基于抗体浓度变化的入侵检测方法, 建立了抗原和抗体的动态进化模型。此外, 在免疫算法方向, 基于免疫系统行为, 多目标复制选择优化算法、动态多模式复制选择算法、基于垂直距离的复制选择机制^[11-13]相继被提出。

仿生安全防护系统借鉴生物系统的自适应、自组织、自学习和自修复能力, 构建全新的网络安全防护架构。Liang 等^[14]受生物系统可靠性维护机制的启发, 提出具有进化能力的下一代网络可靠性设计模型。Jain 等^[15]提出一种生物入侵检测和自愈模型, 能够检测攻击并自动修复系统。于全等^[16]提出一种类生物免疫机制的网络安全架构, 通过模拟人体非特异性和特异性免疫机制, 实现可用性与安全性的平衡。胡爱群等^[17]将神经与免疫机理进行融合, 提出宏观的信息系统仿生免疫模型, 为后续研究提供了理论支撑。

从目前的研究情况来看, 网络安全的仿生技术多基于生物防御机制的局部展开, 或多停留在理论层面。为了将安全功能与系统架构高度融合, 构建各部分紧密配合的信息系统, 本文深入分析并类比了人体免疫系统机理, 构建了新型仿

生免疫体系架构, 基于模块化、面向任务的思想对信息系统进行重建并测试, 实现实时检测并校正程序异常的基本效果。

2 人体免疫系统机理

对于生物而言, 免疫系统是维持自身生命体并延续物种所必需的生存机制。这一机制帮助生物迅速适应周围环境, 进行机体识别并清除抗原性异物, 维持机体内环境稳定。

免疫系统具有调节机制。在日常机体运作过程中, 生物免疫系统会持续监测机体环境的变化。一旦发现异常情况, 免疫应答系统会被启动, 此时免疫细胞间、免疫细胞与免疫分子间、免疫系统和机体的其他系统间会产生相互作用^[18], 使免疫应答系统维持在适度水平, 保持有效的免疫应答, 隔离有害入侵物, 同时防止或减少免疫过激对自身器官、组织造成损伤。

图 1 为免疫系统的调节机制, 免疫系统通过对病原体、免疫细胞膜分子及其他细胞分泌物的感知来获取多元信号, 在此基础上进行综合分析并采取与之对应的免疫措施。当应答水平较低时, 免疫系统会进行正向免疫调节, 通过增强抗原提呈细胞 (antigen presenting cell, APC)、淋巴细胞等的活化与分化产生免疫分子, 促进免疫应答的进行。若应答水平较高, 免疫系统会适时采取负向免疫调节, 通过多种机制抑制细胞免疫, 下调免疫应答水平。

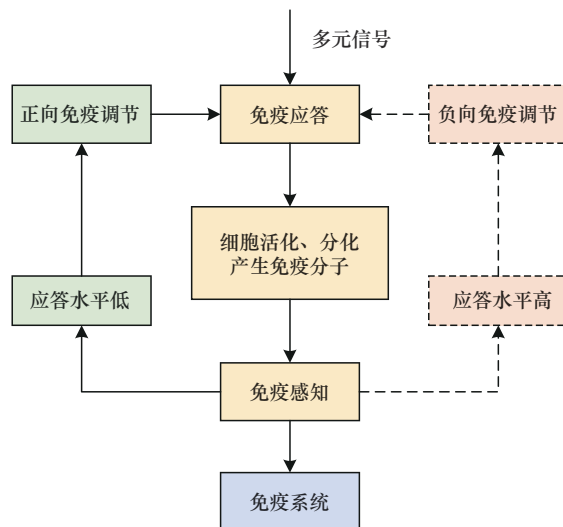


图 1 免疫系统的调节机制

Figure 1 Regulatory mechanisms of the immune system

免疫系统具有防御体系。人体免疫系统可以分为先天性免疫系统和适应性免疫系统。先天性免疫系统包括机体的天然组织屏障，如皮肤、黏膜、体内的血-脑屏障及固有的免疫细胞和免疫分子^[19]。病原体进入机体时，首先接触的是机体的皮肤、黏膜等保护屏障。这些屏障不仅可以阻止外来物的侵入，还可以通过其表面存在的抑菌或杀菌物质清除病原体。适应性免疫系统则更加复杂。图2为适应性免疫系统的防御机制。首先，APC中的树突状细胞在识别出抗原后将其向上提呈。其次，在血管中巡视的巨噬细胞发现异常后，捕获抗原并形成抗原肽-MHC复合物表达在细胞膜上。然后，特异性淋巴细胞（B细胞、T细胞）在识别出抗原肽-MHC复合物后将与之结合，并启动细胞抗原特异性识别及细胞活化的共刺激信号，同时分泌IL-2等多种细胞因子参与T细胞的活化与增殖^[20]。最后，T细胞在这些信号与因子的共同调控下，分化为不同的效应T细胞来介导不同的免疫反应。以其中的Th1细胞为例，Th1细胞通过分泌细胞因子，趋化单核/巨噬细胞定向迁移、富集与活化^[21]，从而对炎症部位的病原生物进行吞噬和清除。除此之外，在淋巴细胞特异性识别阶段，B细胞会与T细胞相互作用而进一步活化，分化为可以产生抗体的浆细胞和记忆B细胞，而后抗体分子亲和力成熟并进行类比转换^[22]，生成大量抗体。这些抗体存在于血清和体液，本身不具有杀伤和清除病原体的能力，但在下一次病原体等相应抗原入侵时，可以中和细菌毒素并与病原体结合使之凝集、沉淀，从而有效阻止病原体入侵。

综上所述，人体免疫机制的主要特点如下。

- 1) 拥有分布在各处的树突状细胞，动态监测机体的健康状况，感知、加工状态信息并向上提呈。
- 2) 以遍布机体的血管为传输通道、以血液为载体转发信息，确保细胞间信息互通。
- 3) 拥有作为中枢控制的淋巴细胞，其负责综合处理和分析信息并进行决策。
- 4) 细胞之间物理隔离又功能交互，淋巴细胞分散式分布，共同构成免疫系统的内部环境。

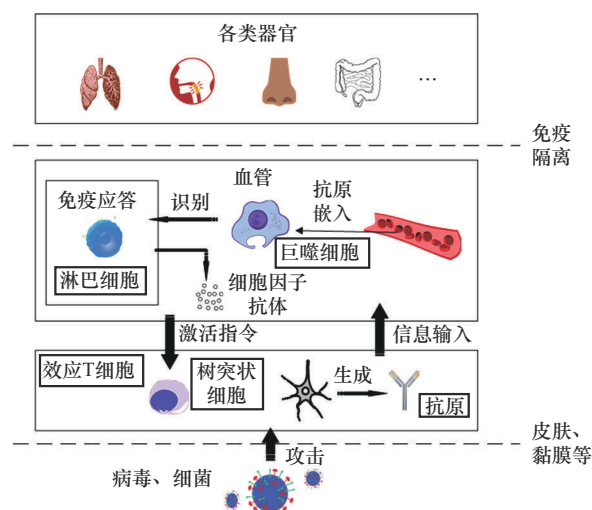


图2 适应性免疫系统的防御机制
Figure 2 Defense mechanisms of the adaptive immune system

3 仿人体的内生免疫系统

3.1 以任务为导向的控制机制

仿照人体免疫系统的工作机理，通过研究免疫系统发现并防御入侵异物的过程，本文构建了多层次的类免疫系统控制架构。

类免疫系统控制架构如图3所示，分为任务组件、转发组件和控制组件3个模块。

任务组件主要负责感知、校准和反馈。所有位于终端的树突状细胞不断监控系统的任务执行情况（包括系统内存和CPU占用、线程、函数调用等），感知各项可能影响系统正常运作的参数，并对参数进行加密。一旦发现执行异常，效应T细胞将根据上层下发的校准决策采取相应校准策略，如终止进程、降低模块负载等。

转发组件作为连接任务组件与控制组件的中转站，负责各类信息的处理和转发。转发组件接收到安全信息后，血管中的巨噬细胞将对获取的原始安全参数进行特性分类和预处理，并向上传递。血管在接收到控制组件下发的决策因子时，会将策略下达至出现异常的任务处，并收集校准效果将其反馈给控制组件。

控制组件是整个架构的核心，类似于免疫系统中管控免疫应答的淋巴细胞。其接收下层传递的安全参数并进行安全校验，生成自适应的校准决策并下发；同时，经过不断地学习和迭代，完善校准决策并形成规则，优化规则库。

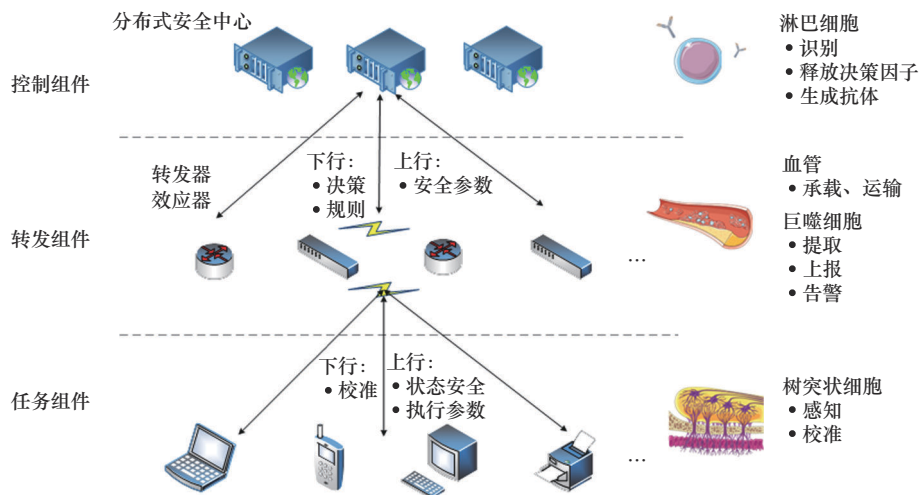


图3 类免疫系统控制架构

Figure 3 Immunomodulatory system control architecture

人体免疫系统和仿生免疫系统的具体类比如表1所示。

表1 人体免疫系统与仿生免疫系统类比

Table 1 The analogy between the human immune system and an endogenous immune system

人体免疫系统	仿生免疫系统
皮肤、黏膜	网络边界隔离
人体各器官	任务组件
抗原	功能性输入数据
树突状细胞	感受器
血管	传输通道
巨噬细胞	转发组件
淋巴细胞	控制组件
效应T细胞	效应器
细胞因子	安全决策
抗体	规则库
免疫应答	识别调控入侵物的过程

基于规则库的决策机制如图4所示，主要包含行为特征的监控（监控机制）、决策的匹配和优化（修复机制）两个方面。

在初始监控机制中，系统提取行为特征动态监控系统的环境和任务的执行情况信息。在修复机制中，首先在规则库中搜索相匹配的校准规则，这一过程类似于生物免疫中抗体自主凝集病原生物。若不存在相匹配的规则，通过状态数据分析生成相应的校准策略，并对系统异常状态进

行校准。与此同时，对有效的校准策略进行学习形成既定规则，将其添加到规则库中，促使系统对同质异常情况进行快速响应，提高系统异常处理的效率。

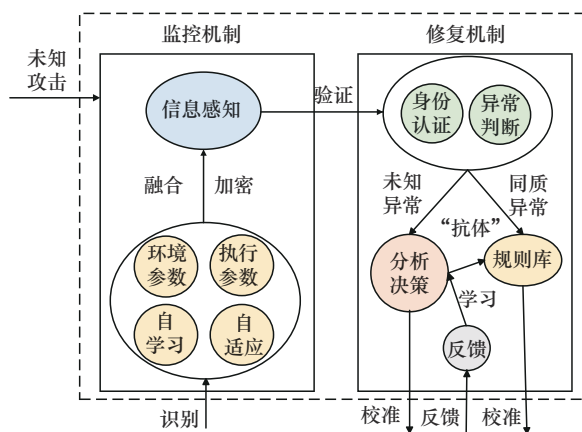


图4 基于规则库的决策机制

Figure 4 Decision mechanism based on rule base

3.2 重构系统架构

对具有基本功能模块的信息系统进行类人体免疫系统的重构，基于任务导向，系统需要明确可执行的任务，在任务的基础上设计模块，实现模块之间相互通信，构成紧密、高效的安全系统模型。仿生免疫系统的功能架构如图5所示。

整个系统包含任务组件、转发组件和分布式控制组件3个部分。任务组件感知进程中的安全信息，输出加密的安全参数。转发组件进行信息的处理和转发。控制组件负责认证、管理、判别

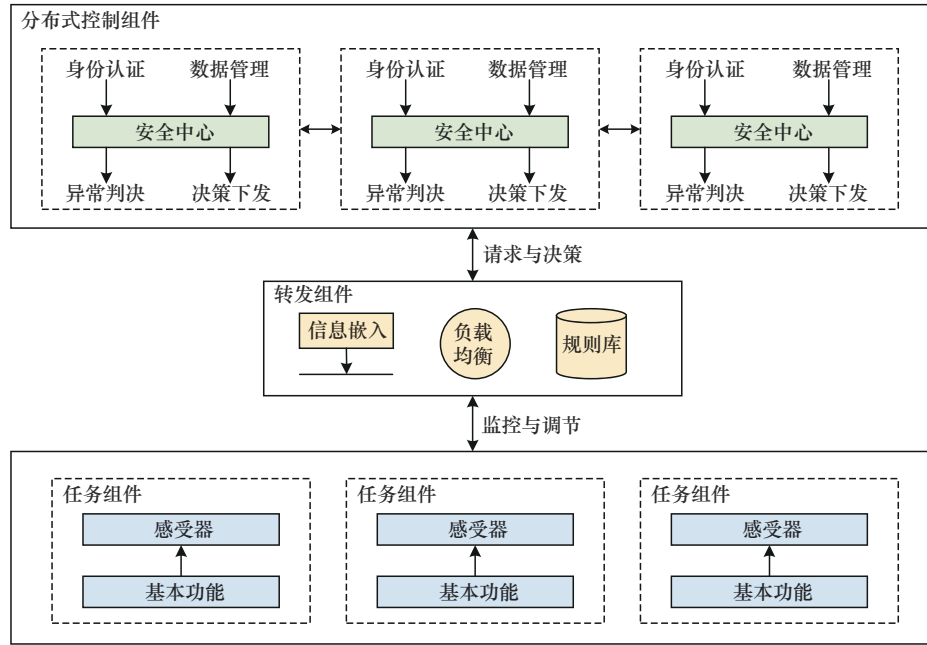


图5 仿生免疫系统的功能架构

Figure 5 Functional architecture of biomimetic immune system

和决策。

类比淋巴细胞分布于全身各处并在免疫过程中采取就近应答的特性，控制组件中部署多个分布式的安全中心，转发组件根据负载均衡机制将安全信息传递给其中一个安全中心，以缓解安全中心集中处理的压力，提高安全中心抗风险能力。

4 基于任务导向的仿生免疫模型分析

为了易于理解仿生免疫模型中各组件及系统的运行机制，对模型进行了抽象描述，整个系统动态执行过程如图6所示。

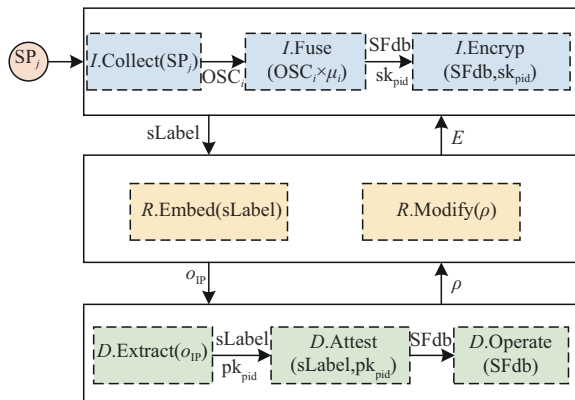


图6 系统动态执行过程

Figure 6 System dynamic execution process

(1) 任务组件部分

任务组件部分需要对系统的状态数据进行采集和加工。

1) $I.Collect(SP_j) \rightarrow OSC_i$: 采集算法以多维安全特性 SP_j ($j \in J$ 特性总数) 为输入，输出感受器标识符 $i \in I$ 的系统安全参数 OSC_i 。

2) $I.Fuse(OSC_i \times \mu_i) \rightarrow SFdb$: 融合算法以多个系统的安全参数 OSC_i 为输入 (μ_i 为第 i 个感受器)，输出一个安全融合数据 $SFdb$ 。

3) $I.Encrypt(SFdb, sk_{pid}) \rightarrow sLabel$: 加密算法以安全融合数据 $SFdb$ 和私钥 sk_{pid} (pid 为进程) 为输入，输出加密后的系统安全标签 $sLabel$ 。

(2) 转发组件部分

转发组件部分需要将安全标签嵌入IP请求报文，向上转发至控制组件。同时，接收控制组件传输过来的决策信息，并对相应任务组件进行任务调整。

1) $R.Embed(sLabel) \rightarrow o_{IP}$: 以系统安全标签 $sLabel$ 为输入，输出嵌入安全信息的IP请求报文 o_{IP} 。

2) $R.Modify(\rho) \rightarrow E$: 以控制组件传输过来的决策指令 ρ 为输入，输出效应 E 。

(3) 控制组件部分

控制组件部分首先需要对安全数据进行身份

认证, 认证通过后根据融合数据生成决策, 并将决策传输给转发组件。

1) $D.Extract(o_{IP}) \rightarrow sLabel$: 以 IP 请求报文 o_{IP} 为输入, 输出安全标签 $sLabel$ 。

2) $D.Attest(sLabel, pk_{pid}) \rightarrow (\alpha, SFdb)$: 认证算法以系统安全标签 $sLabel$ 和公钥 pk_{pid} 为输入, 输出认证结果 α 和解密后的安全融合数据 $SFdb$ 。若 $\alpha = 1$, 则表明身份认证成功; 若 $\alpha = 0$, 则表明身份认证失败。

3) $D.Operate(SFdb) \rightarrow \rho$: 以安全融合数据 $SFdb$ 为输入, 输出决策指令 ρ 。

下面对模型的安全性进行分析和证明。

定义 1 正常报文。应用程序的合法进程按照正常状态流程执行任务时, 发出的带有安全标签的报文称为正常报文。

定义 2 异常报文。非法进程执行任务时, 或合法进程执行任务状态流程发生偏移时, 发出的带有安全标签的报文称为异常报文。

定理 1 模型的安全性包括两点: ①非法进程执行任务时, 将被系统检测出来并终止任务; ②任务执行状态发生异常时, 将被系统检测出来并进行控制调整。

定理 1.1 非法进程 n ($n \neq pid$) 执行任务时, 采用 sk_n 私钥进行加密 $I.Encrypt(SFdb, sk_n) \rightarrow sLabel$; 终端输出带有安全标签的报文 o_{IP} 给安全中心后, 在安全中心进行身份认证。从密钥库中提取公钥 pk_{pid} , 由于 $n \neq pid$, 此时解密失败, 输出 $\alpha = 0$, 则系统判定报文为异常报文, 并执行相应的安全措施阻止非法进程的继续执行。

定理 1.2 合法进程 n ($n = pid$) 执行任务时, 终端输出带有安全标签的报文 o_{IP} 给安全中心后, 在安全中心进行身份认证。从密钥库中提取公钥 pk_{pid} , 由于 $n = pid$, 此时解密成功, 输出 $\alpha = 1$, 即身份认证成功。对安全标签携带的安全状态数据进行判决, 判决异常输出 $\beta = 0$, 则报文为异常报文, 并执行相应的安全措施对进程进行校准。

综合定理 1.1 与定理 1.2, 可得本模型满足定理 1, 即当非法进程获取任务执行控制权时, 会因公私钥匹配不一致而被检测出来并被终止任

务; 当合法进程在任务执行过程中出现异常时, 会因状态异常而被检测出来并进行调整, 因此系统是安全可信的。

5 系统原型实现与分析

5.1 系统框架实现

本文实验基于 socket 编程实现基本文件传输系统, FTP 系统界面如图 7 所示。

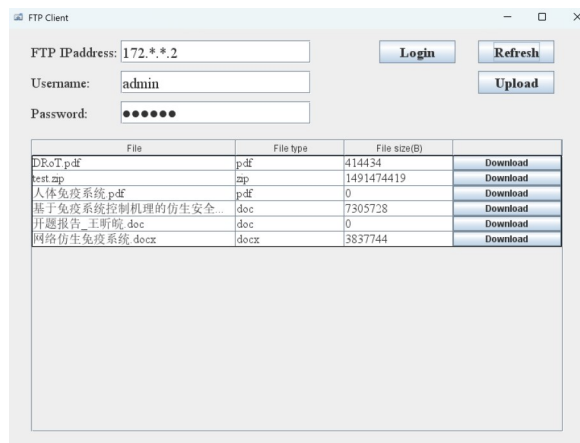


图 7 FTP 系统界面

Figure 7 FTP system interface

在 Linux (Ubuntu 20.04) 系统的实验环境下, 依赖 docker、Nacos 等组件对 FTP 应用程序进行改造。系统原型框架如图 8 所示, 整体分为任务组件 (FTP APP 及 ASP)、转发组件 (docker 网关和 ASE)、控制组件 (多个分布部署的安全中心及负责统筹管理多个安全中心的 Nacos)。每个模块部署在单个独立的 docker 容器中, 同时这些 docker 容器处于相同的网络环境中, 通过 docker 网关 (转发组件) 实现容器间的通信互联。

系统工作时序如图 9 所示。用户 admin 在使用 FTP App 的过程中会产生具有时效性的多维安全数据, 这些安全数据首先会被 ASP 针对性地进行提取和处理, 之后经过网络提交至控制组件的安全中心。安全数据在进入安全中心之前, 由 Nacos 进行统一的管理和分发, 为其分配一个指定的安全中心。该安全中心对接收到的安全数据进行安全性分析, 生成决策 (policy) 并将决策响应至 ASE 中, 对 FTP App 采取针对性的调节措施。

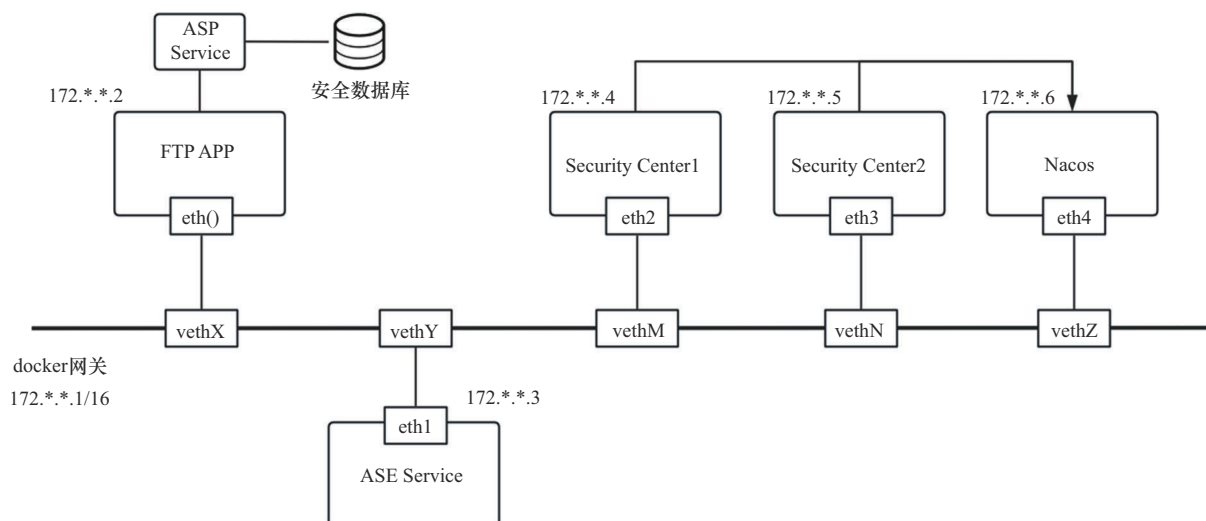


图8 系统原型框架

Figure 8 System prototype framework

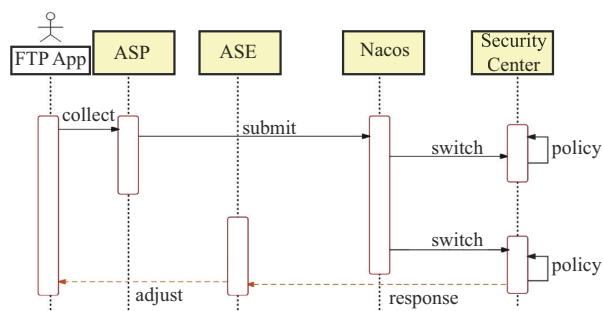


图9 系统工作时序

Figure 9 System workflow

5.2 系统基本功能实现

在FTP App中植入感受器，用来对系统运行过程中的底层资源和事件执行情况进行监控与采集。下面以应用的CPU占用率和内存(Memory)使用量为例，在应用正常运行时，每隔一段时间向应用传输相同大小的文件，采集到的内存使用量和CPU占用率如图10所示。

从图10中可以看出，应用的CPU占用率随传输任务的进行呈现周期性地增加，当传输任务结束时，CPU占用率会逐渐恢复为静默状态。应用的内存使用量随着每次传输任务的进行而不断增加，当达到临界值(约62 MB)时，JVM自动进行内存回收，将无引用链相连(不可用)的对象回收，确保系统正常运行。

为验证系统检测并处理异常的基本功能，通过JMeter暴力请求程序模拟简单的DDoS攻击，监测应用的CPU、内存、类、线程的使用

情况，采集到一系列特征数据，其中self(自我)状态的数据255组，noself(非我)状态的数据128组。

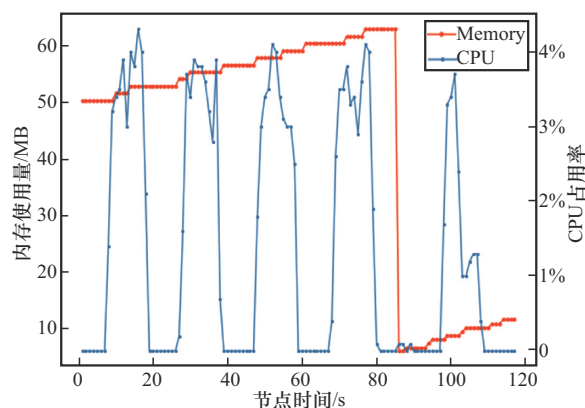


图10 FTP App运行期间的内存使用量和CPU占用率

Figure 10 Memory usage and CPU utilization during FTP App runtime

之后，控制中心将进行异常判决。在确定异常判决算法时，选取KNN、贝叶斯和决策树这3种常见的监督学习算法对采集的数据进行训练和预测，并计算预测的准确率。预测准确率 P 的计算式如下。

$$P = \frac{N_{\text{self}} + N_{\text{noself}}}{N} \quad (1)$$

其中， N 为样本总数， N_{self} 和 N_{noself} 分别为预测成功的正常和异常样本总数。各算法的准确率和响应时间如表2所示。

表2 算法的效果评估

Table 2 Evaluation of the effectiveness of the algorithm

算法	TrainSet准确率	TestSet准确率	响应时间/ms
KNN	99.012%	97.076%	483
贝叶斯	96.013%	92.895%	112
决策树	99.024%	97.812%	175

从表2中可以看出,相比贝叶斯算法,KNN算法与决策树算法的预测准确率较高。但由于KNN算法的空间复杂度高,处理数据的响应时间更长,因此选用决策树算法。

安全数据经决策树算法判决后,可以得到“自我”和“非我”两种状态。若为“非我”(即出现异常),此时调用程序shutdown()丢弃缓存中未完成数据,强制关闭TCP连接,如图11所示。

```
ip is 172.*.*.2
port is 5***
STOR 人体免疫系统.pdf
execute Store command @@@StoreCommand
Unsafe factors, forcing connection closure Connection closed ...
connection closed
```

图11 强制关闭TCP连接

Figure 11 Forceful termination of a TCP connection

5.3 防御能力和性能测试

在此基础上,构建如图12所示的实验环境,测试仿生免疫系统的防御能力与性能开销。

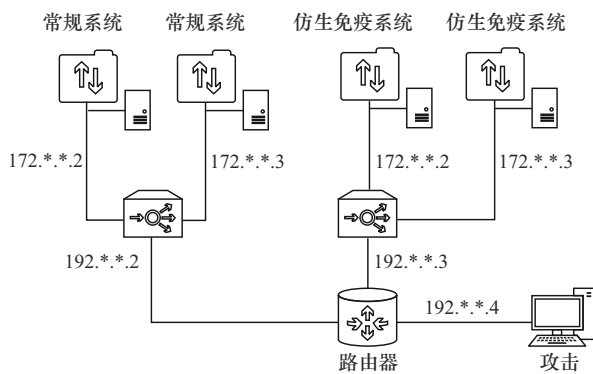


图12 对比实验网络拓扑

Figure 12 Network topology of comparative experiments

为了验证防御能力,首先模拟DDoS、中间人(man in the middle, MITM)、服务器端请求伪造(server-side request forgery, SSRF)攻击生成混合攻击测试集,如表3所示,对仿生免疫系统

和常规系统发动攻击。模拟攻击设备为MacBook(Apple M1处理器、16 GB内存)。

表3 混合攻击测试集

Table 3 Hybrid attack test set information

攻击	测试集
DDoS	143
MITM	65
SSRF	55
合计	263

混合攻击实验结果如表4所示,其中,TP表示系统检测漏洞数量,TPR表示系统检测漏洞数量占总漏洞的比例。在几种不同类型的攻击下,仿生免疫系统相较于常规系统在检测并捕捉漏洞方面的表现更佳,漏洞的检测率提升了52.5%。

表4 混合攻击实验结果

Table 4 Hybrid attack experimental results

攻击类型	仿生免疫系统		常规系统	
	TP	TPR	TP	TPR
DDoS	143	100%	79	55.2%
MITM	62	95.4%	14	21.5%
SSRF	55	100%	29	52.7%
合计	260	98.9%	122	46.4%

为了评估性能开销,使用Apache JMeter分别设置1、25、50、100、500、1 000、2 500的并发数来模拟不同用户的请求,从内存负载和响应时间两个角度评估系统性能。仿生免疫系统与常规系统的性能对比如图13所示,从图13中可以看出,相较于常规系统,仿生免疫系统虽在内存负载方面的开销有所增加,但响应时间与常规系统相差甚微,对性能的影响较小。

综上所述,实验搭建的仿生免疫安全模型具有监测并拦截异常的基本功能。相较于常规系统,仿生免疫系统可以在保证较好的运行性能的同时提升对攻击的检测能力,从而更好地维护系统安全。

6 结束语

本文针对传统外壳式防御难以应对日益复杂的信息系统攻击的问题,借鉴人体免疫系统识别并清除抗原性异物的免疫机制,提出一种基于免

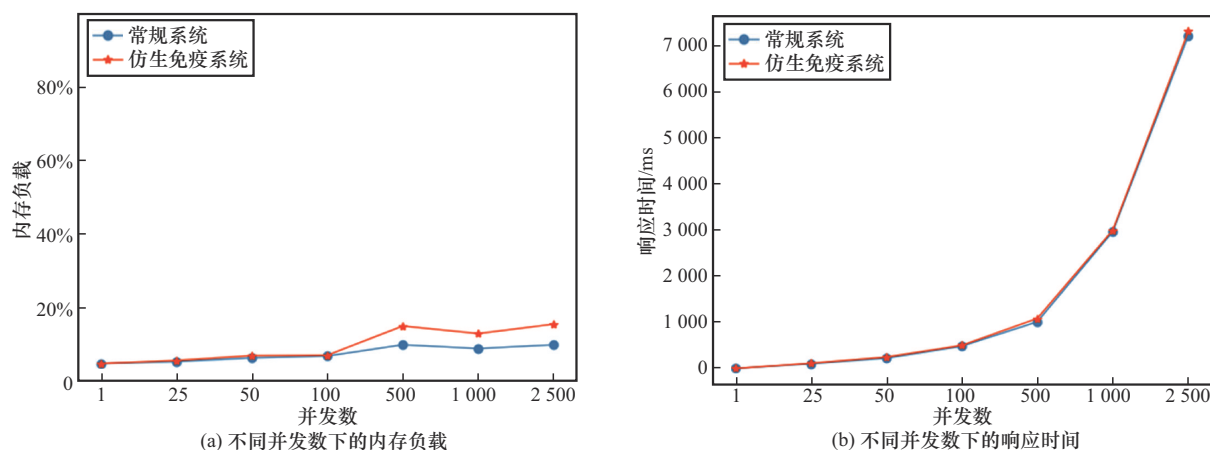


图13 仿生免疫系统与常规系统的性能对比

Figure 13 Comparison performance of the bionic immune system with conventional systems

疫控制的仿生安全模型。

参考人体免疫系统树突状细胞、巨噬细胞和淋巴细胞等的协调配合机制，对信息系统的基础架构进行重构。在确保系统基本功能模块正常运行的前提下，嵌入安全模块并耦合，构建自维稳的仿生安全模型。通过分析，该模型在满足双向验证和无干扰的情况下可以保证安全性。系统实验验证了该模型具有与免疫系统类似的针对异常威胁的检测与防御功能。

在此模型的基础上，未来可以考虑增加或嵌套更多模块，实现针对更加复杂攻击的防御机制；同时，在底层数据感知层面可以采用更加精密的感知方法，感知更多维度的安全数据，帮助提高决策的针对性和准确性。

参考文献：

- [1] FARMER J D, PACKARD N H, PERELSON A S. The immune system, adaptation, and machine learning[J]. Physica D: Nonlinear Phenomena, 1986, 22,2(1-3): 187-204.
- [2] 郭江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(2): 189-204.
- [3] MALIK J, MUTHALAGU R, PAWAR P M. A systematic review of adversarial machine learning attacks, defensive controls and technologies[J]. IEEE Access, 2024.
- [4] 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.
- [5] SIYUAN N, HONGCHAO H, WENYAN L, et al. Security levels oriented deployment algorithm for mimic SaaS cloud[C]// Proceedings of the 6th International Conference on Computer and Communications (ICCC 2020). Piscataway: IEEE Press, 2020: 2409-2414.
- [6] WANG L, ZHAO Z, LIU H. AI-driven mimic defense systems: opportunities and Challenges[J]. Journal of Intelligent Cybersecurity, 2022, 15(6): 50-63.
- [7] 顾天晟, 曾福康, 邵思思, 等. 基于拟态防御和 Paillier 加密的智能物联网终端安全防护方法[J]. 网络与信息安全学报, 2024, 10(6): 164-176.
- [8] GU T S, ZENG F K, SHAO S S, et al. Security protection method based on mimic defense and Paillier encryption for smart IoT terminals[J]. Chinese Journal of Network and Information Security, 2024, 10(6): 164-176.
- [9] FORREST S, SOMAYAJI A, ACKLEY D H. Building diverse computer systems[C]// Proceedings of the 6th Workshop on Hot Topics in Operating Systems, HotOS-VI, Cape Cod. Piscataway: IEEE Press, 1997: 67-72.
- [10] OU Z M. Host-based intrusion detection systems inspired by machine learning of agent-based artificial immune systems[C]// Proceedings of 2019 IEEE International Symposium on INnovations in Intelligent Systems and Applications (INISTA). Piscataway: IEEE Press, 2019: 1-5.
- [11] ZHANG R, XIAO X. An intrusion detection method based on changes of antibody concentration in immune response[J]. Journal of Information Processing Systems, 2019, 15(1): 137-150.
- [12] ZAREIZADEH Z, HELFROST M S, RAHIDEH A, et al. A robust gene clustering algorithm based on clonal selection in multi-objective optimization framework[J]. Expert Systems with Applications, 2018, 113: 301-314.
- [13] LUO W, LIN X, ZHU T, et al. A clonal selection algorithm for dynamic multimodal function optimization[J]. Swarm and Evolutionary Calculation, 2019, 50: 100459.
- [14] LI L, LIN Q, LI K, et al. Vertical distance-based clonal selection mechanism for the multiobjective immune algorithm[J]. Swarm and

- Evolutionary Computation, 2021, 63: 100886.
- [14] LIANG Z X, DING Y S, FANG J, et al. Reliability design model research of next-generation network based on bio-network[C]//Proceedings of 2009 Asia-Pacific Conference on Information Processing. Piscataway:IEEE Press, 2009: 509-512.
- [15] JAIN P, SINGH P K, ABRAHAM A. Intrusion detection and self healing model for network security[C]//Proceedings of the 7th International Conference on Next Generation Web Services Practices. Piscataway:IEEE Press, 2011: 320-325.
- [16] 于全,任婧,李颖,等.类生物免疫机制的网络安全架构[J].网络空间安全, 2020, 11(8): 6-10+22.
- YU Q, REN J, LI Y, et al. Network security architecture of biological immune mechanisms[J]. Cyber Space Security, 2020, 11(8): 6-10+22.
- [17] 胡爱群, 方兰婷, 李涛. 基于仿生机理的内生安全防御体系研究[J]. 网络与信息安全学报, 2021, 7(1): 11-19.
- HU A Q, FANG L T, LI T. Research on bionic mechanism based endogenous security defense system[J]. Chinese journal of network and information security, 2021, 7(1): 11-19.
- [18] BRODIN P, DAVIS M M. Human immune system variation[J]. Nature Reviews Immunology, 2017, 17(1): 21-29.
- [19] CHEN S, SAEED A F U H, LIU Q, et al. Macrophages in immunoregulation and therapeutics[J]. Signal Transduction and Targeted Therapy, 2023, 8(1): 207.
- [20] SUO C, DANN E, GOH I, et al. Mapping the developing human immune system across organs[J]. Science, 2022, 376(6597).
- [21] 彭伟涛,任玥,吴晓牧.固有免疫和适应性免疫在病毒性脑炎发病中的作用机制[J].中国神经免疫学和神经病学杂志, 2020, 27(6): 466-469.
- PENG W T, REN Y, WU X M. The role of innate and adaptive immunity in the pathogenesis of viral encephalitis[J]. Chinese Journal of Neuroimmunology and Neurology, 2020, 27(6): 466-469.
- [22] CYSTER J G, ALLEN C D C. B cell responses: cell interaction dynamics and decisions[J]. Cell, 2019, 177(3): 524-540.

[作者简介]



李涛 (1984-), 男, 江苏镇江人, 博士, 东南大学副教授, 主要研究方向为内生安全、信息系统安全。



王昕皖 (1999-), 女, 安徽合肥人, 东南大学硕士生, 主要研究方向为内生安全、信息系统安全。



胡爱群 (1964-), 男, 江苏南通人, 博士, 东南大学教授、博士生导师, 主要研究方向为内生安全、信息系统安全。