信息通信领域产学研合作特色期刊　十佳皖刊
第三届国家期刊奖百种重点期刊　中国科技核心期刊

ISSN 1009-6868
CN 34-1228/TN

中兴通讯技术

ZTE TECHNOLOGY JOURNAL

http://tech.zte.com.cn

2022 年 12 月 · 第 6 期

专题：网络内生安全

（封面图片详解见 P66）

ISSN 1009-6868
9 771009 686229 12>

《中兴通讯技术》第 9 届编辑委员会成员名单

目　次

中兴通讯技术（ZHONGXING TONGXUN JISHU）
总第167期　第28卷　第6期　2022年12月

信息通信领域产学研合作特色期刊　第三届国家期刊奖百种重点期刊　中国科技核心期刊　工信部优秀科技期刊　十佳皖刊　中国五大文献数据库收录期刊　1995年创刊

热点专题 ▶ 网络内生安全

《中兴通讯技术》2022年热点专题名称及策划人

1. 新型网络技术
中国联通研究院副院长　唐雄燕

2. 自然语言处理预训练模型
中国工程院院士　郑纬民

3. 智能超表面技术
中兴通讯技术预研总工　赵亚军
北京理工大学教授　费泽松

4. 多频段协同通信
电子科技大学教授　李少谦
中国联通研究院副院长　唐雄燕
中兴通讯首席科学家　向际鹰

5. 通信感知一体化技术
中国科学技术大学副教授　陈力
中国科学技术大学教授　卫国

6. 网络内生安全
北京航空航天大学教授　刘建伟

MAIN CONTENTS

ZTE TECHNOLOGY JOURNAL
Vol. 28 No. 6 Dec. 2022

期刊基本参数：CN 34-1228/TN*1995*b*16*100*zh*P*¥20.00*6500*15*2022-12

网络内生安全专题导读

专题策划人 >>>

刘建伟，北京航空航天大学网络空间安全学院教授、博士生导师、院长，享受国务院政府特殊津贴，现任国务院学位委员会第八届学科评议组成员、教育部高等学校网络空间安全专业教学指导委员会委员、中国密码学会常务理事、中国指挥与控制学会常务理事、中国电子学会网络空间安全专委会副主任委员、中国指挥与控制学会网络空间安全专委会副主任委员、中关村智能终端操作系统联盟副理事长；曾获国家技术发明一等奖、国防技术发明一等奖、中国指挥与控制学会科技进步一等奖等，所编写的教材获全国普通高校优秀教材一等奖、国家网络安全优秀教材、国家精品教材、全国优秀科普作品奖、第四届中国科普作家协会优秀科普作品金奖等；出版教材7部、专著2部、译著1部。

在网络架构融合开放的发展趋势下，网络安全已从过去的“静态被动式安全”，发展到当前的“动态主动式安全”，并正在向“内生智能安全”演进。网络安全领域已逐步达成共识——“架构决定安全”，因此利用系统架构、算法、机制、场景、规律等内在因素获得安全功能或属性的“内生安全”便应运而生。本期专题以网络内生安全为主题，邀请内生安全领域学者和专家撰写了10篇文章。

《网络内生安全研究现状与关键技术》综述了内生安全的概念与演进阶段，梳理总结了包括拟态防御、可信计算、零信任、DevSecOps等路线在内的主流内生安全路线的研究现状、技术路线和关键技术；《主动免疫可信计算综述》阐述了主动免疫可信计算的基本思想、主要特征，介绍了主动免疫可信计算工作原理，并分析了主动免疫可信计算与可信计算组织（TCG）可信计算的区别；《安全可信的互联网体系结构与端到端传送关键技术》提出了具备安全可信和主动防御能力的互联网端到端传送关键技术，实现了分组数据从可靠生成到安全传输，再到可信应用3个阶段的安全闭环，有效增强了互联网的整体安全性；《零信任平台方案及关键技术》介绍了零信任架构（ZTA）平台的3个组成部分及零信任平台各模块的功能，深入阐述了第三代单包授权（SPA）、新一代沙箱、动态访问控制列表（ACL）、三层转四层隧道等关键技术；《基于内生安全框架的面向数字化转型的网络安全防御体系》提出了一种新的全体系设计、建设与运营思路，将网络安全能力与数字化环境进行融合内生，实现安全与信息化的深度融合与全面覆盖；《零信任架构在医疗物联网安全建设中的应用》提出一种基于零信任架构的医疗物联网融生安全框架，构建业务安全访问、持续风险评估和动态访问控制的安全能力；《代码疫苗技术在DevSecOps体系下的实践》介绍了已成功应用于交互式应用安全测试（IAST）工具和运行时应用自保护（RASP）工具的代码疫苗技术，并阐述了代码疫苗技术在DevSecOps体系下的实践；《融合神经与免疫机理的信息系统仿生免疫模型》提出一种融合神经与免疫机理的仿生免疫模型，模仿人体的安全防御机理，将安全体系和信息系统高度融合实现内生安全；《网络空间拟态防御建模与量化评估技术研究》归纳总结了现有拟态防御理论系统建模方法，对比分析了不同模型的适用场景，展望了拟态防御理论在应用场景中的定性和定量评估方法；《安全平行切面：面向企业数字生命体的安全基础设施》阐述了安全平行切面的内涵，并总结了网络与信息安全形势面临的3个趋势。

本期作者均为知名高校和网络安全龙头企业的专家，专题文章汇聚了他们最新的研究成果。希望本期的内容能给读者朋友提供有益的参考，并在此对所有作者和专家的大力支持和辛勤工作表示衷心感谢！

刘建伟

2022年11月20日

DOI：10.12142/ZTETJ.202206001
收稿日期：2022-11-21

网络内生安全研究现状与关键技术

Research Status and Key Technologies of Network Endogenous Security

王瀚洲/WANG Hanzhou，刘建伟/LIU Jianwei
（北京航空航天大学，中国 北京 100191）
(Beihang University, Beijing 100191, China)

DOI：10.12142/ZTETJ.202206002
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221129.0829.002.html
网络出版日期：2022-11-30
收稿日期：2022-10-15

摘要：网络正处于融合开放的发展趋势中，传统的由安全事件和等保合规驱动的外挂式、被动式的安全机制已无法满足业务的需求。认为以“架构决定安全”为核心理念的内生安全已成为下一阶段网络安全领域的发展方向。从现有安全技术出发，分析了前内生安全技术的缺陷及发展内生安全技术的必要性，介绍了内生安全的概念与演进阶段，梳理总结了包括拟态防御、可信计算、零信任、DevSecOps等路线在内的主流内生安全路线的研究现状，并从原理层面介绍了各路线的关键技术。

关键词：内生安全；拟态防御；可信计算；零信任；DevSecOps；物理层安全

Abstract: The network is in the development trend of integration and opening. The traditional external and passive security mechanism driven by security events and equal guarantee compliance cannot meet the needs of business. The endogenous security with "architecture determines security" as the core concept has become the development direction of the network security field in the next stage. Starting from the existing security technology, this paper analyzes the defects of the former endogenous security technology and the necessity of developing endogenous security technology, introduces the concept and evolution stage of endogenous security, and summarizes the research status of mainstream endogenous security routes including mimicry defense, trusted computing, zero trust, DevSecOps, etc. The key technologies of each route are introduced from the principle level.

Keywords: endogenous security; mimicry defense; trusted computing; zero trust; DevSecOps; physical layer security

随着信息通信技术的迅猛发展，信息网络系统已成为不可或缺的基础设施。然而，与网络发展相伴而生的网络安全问题也被急剧推到前所未有的高度。网络安全已经成为社会发展、国家安全的基础需求，也成为决定网络能否发挥最大化潜能和价值的关键因素[1]。

在网络架构融合开放的发展趋势下，网络安全从过去主要由安全事件驱动的静态被动式安全，到当前主要由等保合规驱动的动态主动式安全，正在向着下一阶段由具体场景需求驱动的内生智能安全演进。网络安全领域逐步达成共识——“架构决定安全”。也就是说，安全能力应在网络顶层设计构建时就做出充分考虑。对此，以网络系统的架构、机制、场景、规律等先天构建安全能力，并可后天自成长、自适应的“内生安全”理念应运而生。

基金项目：国家重点研发计划（2021YFB2700200）；国家自然科学基金（U21B2021、61972018、61932014）

1 前内生安全技术评析

网络安全技术的发展具有明显的代际发展效应。在内生安全技术之前的网络安全发展主要经历了3个阶段：以阻止入侵为目的的系统加固阶段、以限制破坏为目的的检测响应阶段、以系统顽存为目的的网络容侵阶段[2]。每一阶段的安全技术都呼应了其所面临的安全问题。在网络规模化部署中，这对已知特征和固化模式的攻击具有重要防护意义，但各阶段均以网络攻防对抗为核心思路，缺乏安全的顶层结构化设计，难以逃脱“道高一尺，魔高一丈”的安全困境[3]。

第1阶段的安全技术主要通过划分明确的网络边界，利用各种保护和隔离技术手段，例如用户鉴权与认证、访问控制、信息加解密、网络隔离等，在网络边界上部署，防止外部非法入侵与信息泄露，达到系统加固的目的。此类技术在确保网络系统的正常访问、鉴别合法用户身份和权限管理、机密数据信息安全方面有较强的防护作用，但这一阶段技术对部分攻击行为如用户身份假冒、系统漏洞后门攻击等显得

无能为力。

第2阶段的安全防护融合了保护、检测、响应、恢复四大技术。此阶段主要采用特征扫描、模式匹配等手段对系统状态进行检测与报警，寻找被植入的恶意代码并进行查杀，找出导致恶意代码可被植入的原因并用补丁的方式进行修补，发现不规范的蓄意行为和特征并加以抑制。此阶段技术高度依赖检测能力，且攻击方发展出对应的伪装欺骗技术，导致不可能发现全部攻击。

第3阶段的安全防护在前两阶段的基础上叠加了信息生存技术。此阶段网络在假设漏洞后门不可避免，攻击和意外事故已然、必然发生的条件下，通过实时状况感知与响应，实时调整安全策略，采用自我诊断隔离、还原重构等手段，仍可在限定时间内完成全部关键使命。容侵技术可以作为网络系统的最后一道防线，使攻击侵犯的影响降到最低。但目前容侵技术主要基于门限密码秘密共享理论的容侵模型设计，尚未达到规模化实用的程度，并且模型的建立依赖大量先验知识与实际经验，对于未定义的攻击行为仍然较难防范。

2 内生安全概念

2.1 定义及特征

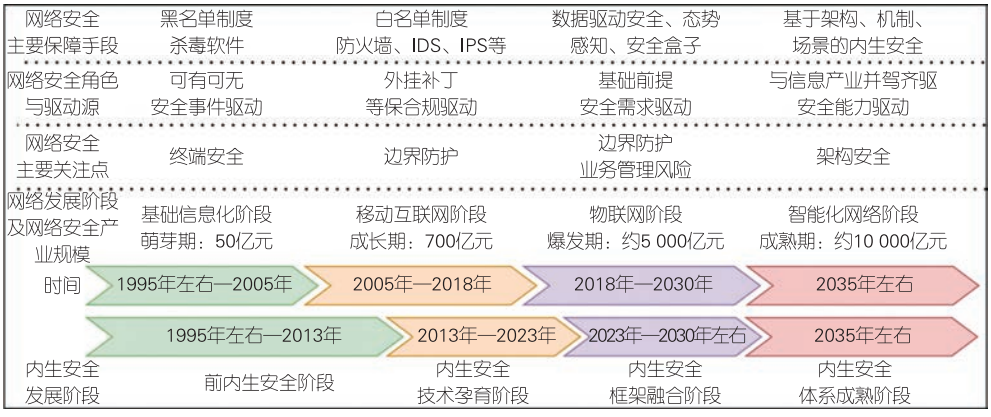
内生安全最早于2013年由邬江兴院士提出。经过学术界、产业界的持续关注，内生安全概念与愿景逐步清晰——内生安全是以网络中各类网元设备自身的安全能力为基础，利用系统架构、算法、机制或场景等内部因素获得安全功能或安全属性，协同配合构建的综合安全体系。内生安全系统至少具有以下基本特征：（1）先天构建。安全能力需要与网络系统的设计与建设同步进行、同步建成，同时安全能力应与网络业务功能全面、紧密耦合。（2）后天成长。系统能够通过与运行环境的交互作用，使自己能够适应环境，应对安全事件，随网络环境变化动态提升安全能力[1,4]。

2.2 演进阶段

在技术层面如何实现内生安全，目前仍未形成统一的技术框架与构建方案。内生安全的演进需经历3个阶段的技术与产品革新（如图1所示），才能使真正具备内生安全的网络系统实现落地[1]。

在内生安全发展的初级阶段——技术孕育阶段，基于不同技术路线的内生安全方案逐渐涌现。多样的内生安全方案被提出，并初步实现积累、融合。此阶段的目标是构建一个基本完备的、融合的内生安全体，逐步由分散式的建设转向统一架构的、可规划的建设。在网络层面，该阶段网络架构特征为端到端、分层网络，但未形成统一的安全构架。在技术层面，该阶段基于拟态防御、零信任、可信计算等技术，初步构建网络内生安全能力；基于DevSecOps、软件安全开发周期等框架，初步实现网络中软件应用安全；基于改良互联网协议（IP）协议、软件定义安全、网络功能虚拟化（NFV）等技术，初步实现具备原子化安全能力的网元；基于密码、量子密钥分发（QKD）等技术，初步实现数据安全能力；基于安全管理、人工智能、威胁模型、关联分析模型等，初步进行免疫能力构建。

在内生安全发展的中级阶段——框架融合阶段，内生安全发展的主要形式是架构的健全化与智能化。随着对未来融合网络架构的研讨，人们将形成内生安全架构的共识方案。在孕育期发展产生的各项成熟的安全技术之间并非竞争择优的关系，而是联合协作的关系。单一封闭的技术实现方案将不适用于未来智能、融合、开放的网络体系，各项安全技术将封装为原子化安全能力。借助人工智能调配，为业务量身打造最适合、最安全的网络，将有助于实现网络适配业务。在网络层面，该阶段初步形成了功能开放的架构底座，可为上层原子化安全能力提供支撑。在技术层面，原子化安全能力逐渐成熟，人工智能会逐步与网络安全能力相结合以提升网络免疫能力，此时边界、网元、应用、数据等安全能力将



▲图1 网络安全代际发展特征[5]与内生安全发展阶段

向智能化、协同化的方向发展。

在内生安全发展的高级阶段——体系成熟阶段，网络已具备健全的先天内生安全体系和全网一体化的后天免疫。随着与人工智能的进一步结合，网络将实现安全的弹性自治。网络的安全能力将形成高共识度的安全度量标准，网络也将形成泛在的、系统化的内生安全保障体系。

3 内生安全研究现状

解决现有网络内生安全问题的思路包含重新设计网络架构与进行增量式修补两种鲜明路线，并兼存寻求折中的演进路线。总体而言，目前已提出的解决方案均在某种程度上具备内生安全特性，实现内生安全的技术方案处于“多强并进”的状态。但目前内生安全研究在硬件、软件或协议层面均未达成足够共识，缺乏将不同技术路线下的内生安全解决方案整合起来的统一框架。各种内生安全路线及其特征如表1所示。

3.1 基于拟态防御的内生安全路线

基于拟态防御的内生安全最早由邬江兴院士提出。他认为带来安全问题的漏洞与后门是未知且不可避免的，同时一切技术都存在内生安全问题（包含伴生的显式副作用或隐式暗功能）。例如，可信计算在目标对象行为不都是可知或可预期的情况下难以保证安全可信，零信任架构难以消除分布式认证节点系统中的漏洞和后门威胁等。因此他提出一种结构或算法。该算法能在不依赖先验知识的条件下，将针对目标对象内生安全的网络威胁归一化为由可靠性和鲁棒性控制理论与方法能够处理的未知扰动。拟态防御通过条件规避的方法让攻击者无法形成有效的攻击，使必然存在的内生安全问题不会成为系统的安全威胁[6]。拟态防御作为一种通用安全技术正在逐步实现应用落地与产品化。基于拟态防御的云基础设施、网络切片防护方案、区块链安全增强方案等层出不穷。拟态构造的域名服务器、Web服务器等已经部署投入使用。以拟态服务器为例，图2展示了拟态防御与传统安全技术相结合的部署架构。

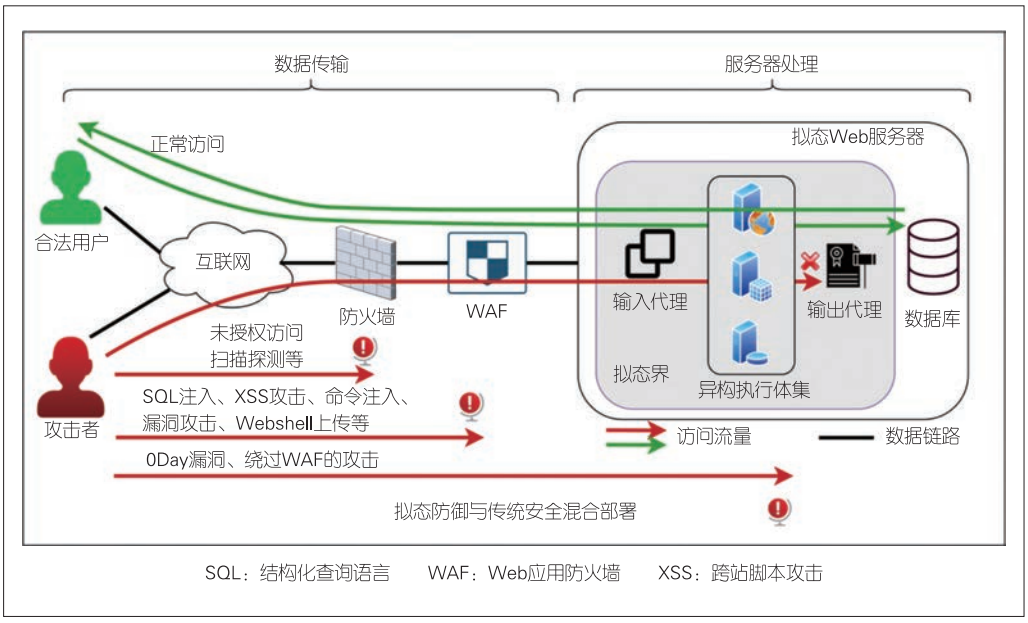
3.2 基于可信计算的可信网络内生安全路线

可信从行为预期的角度被可信计算组织（TCG）定义为：可信实体的行为总是以预期的方式，朝着预期的目标进行，产生的结果总是与预期一致。可信计算中存在一个由底层硬件确保安全性的信任根和一个在系统硬件层面上独立于原宿主系统的可信子系统。可信节点以监控者的身份，主动逐级从可信根向上层执行安全策略，实施行为控制，并返回审计信息，建立由硬件结构到操作系统、应用系统的信任链。上层只有获取底层信任后才能正常运行[7]。

▼表1 各种内生安全路线特征

序号	技术路线	基本思想	关键技术/架构	技术优势	适用场景
1	拟态防御	通过执行体异构性使攻击者很难同时多点攻破；通过策略性的动态变化扰乱攻击链的构造和生效过程	动态异构冗余架构	能非特异性地免疫未知的安全威胁	理论上适用于全部软硬件信息化产品，但因其与现有架构差异较大、部署成本较高，常用于高安全需求的场景
2	可信计算/可信网络	通过规定限制接入终端的身份、状态、行为获取可信身份，通过可信传输、可信连接、身份认证等手段，将单个终端网元的可信状态扩展形成多个节点互联的可信网络	可信连接架构TCA	技术成熟、规模化部署基础较好、国产自主可控	主要应用于安全等级较高的集中管理场合，如局域网办公自动化环境、工控系统、云计算、物联网等领域
3	零信任	“永不信任，始终验证”；缩小到单个资源组的网络防御边界；动态认证授权+精细化的访问控制	软件定义边界、身份和访问控制、微隔离	契合企业服务上云后的安全需求、不依赖边界安全	目前常应用于企业网络，实现远程访问等，未来有望规模应用至物联网
4	DevSecOps	安全左移，源头风险治理；敏捷右移，安全运营敏捷化；人人为安全负责，安全嵌入开发整体流程体系中	CNAPP、RASP、IAST、BAS等	注重人员安全意识培训、安全运维更高效、安全可度量	目前多应用于软件供应链安全、云原生安全，实现应用级、软件级的安全
5	物理层安全	利用物理信道特征、终端制造容差、目标用户地理位置等物理特征，增强数据传输、鉴权认证、数据完整性保护等能力	物理层身份认证；物理层密钥生成；物理层安全传输	轻量化、安全与通信过程绑定、“一次一密”	多数技术应用于无线通信，未来有望大规模应用于6G通信
6	改进IP协议	针对现行IP协议存在的安全性问题，通过在扩展报头中增加身份标识、服务标识等通过改进协议增强网络内生安全性	IPv6、New IP等	在网络层提供安全增强服务、技术上部署难度小	面向宏观、全面的互联网，并借助5G和AI等构建一个智能化的全新互联网
7	伴生网络对抗学习	构建真实网络的1∶1平行数字伴生网络，通过对抗学习生成“网络疫苗”，并依靠智能化预测增强真实网络的安全能力	数字孪生网络、人工智能	降低试错成本、可进行预测性运维	易于建模的网络，可为单一网络域（如接入网、传输网、核心网、承载网等）子网，也可以是端到端的跨域网络

AI：人工智能
BAS：入侵与攻击模拟
CNAPP：云原生应用程序保护平台
IAST：交互式应用安全测试
IP：互联网协议
RASP：应用运行自我保护
TCA：可信网络连接架构



▲图2 拟态防御与传统安全技术相结合的部署架构

可信计算仅提供设备层面的可信，在网络层面以某个或多个可信网元为基础，通过可信传输、身份认证、可信网络连接等手段，构建可信网络连接架构，将单个终端、网元的可信状态，扩展到多个节点互联的可信状态。其核心的思路是对访问者的身份、状态、行为加以规定限制，以接入的自由性换取网络其他节点的信任[8]。2004年TCG提出可信网络连接（TNC）[9]。如图3所示，2007年中国可信计算标准网络组提出可信网络连接架构（TCA），并于2013年将其正式发布为国家标准GB/T 29828–2013《信息安全技术 可信计算规范 可信连接架构》[10]。

3.3 基于零信任架构的内生安全路线

零信任架构最早由Forrester首席分析师J. KINDERVAG提出，是一种基于“永不信任，始终验证”与最低权限原则的网络安全体系，如图4所示。它将网络防御的边界缩小到单个资源组，不再依据用户所处网络位置来决定是否安全可信，而是在对行为的精细化安全风险评估的基础上，强制性地通过动态认证和授权来重构访问控制的信任基础，实现网络系统内生安全。零信任执行以下3个基本原则：（1）所有用户均需要基于访问主体身份、网络环境、终端状态等尽可能多的信任要素进行持续验证和动态授权；（2）所有授权的访问均应遵循最低权限原则按需授权；（3）所有的访问请求都应当被记录和跟踪[11]。零信任安全是安全策略从静态向动态转化的结果，对现有网络安全架构进行了改良。相比于拟态防御，零信任架构对网络架构的改动较少，得到了较为广泛的应用。

零信任是近年来互联网、网络安全企业研究推进的热点技术，并在发展中产生了不同的技术路线，例如Google的Beyond Corp模型、Beyond Prod模型，Gartner的持续自适应风险与信任评估（CARTA）模型、零信任网络访问（ZTNA）模型，Forrester的零信任架构等[12]。远程访问是实施零信任的主要驱动与优先选择。零信任在企业专网安全保障场景下有较为广泛的应用，例如远程办公、远程运维、远程分支机构接入、第三方协作等场景[13]。

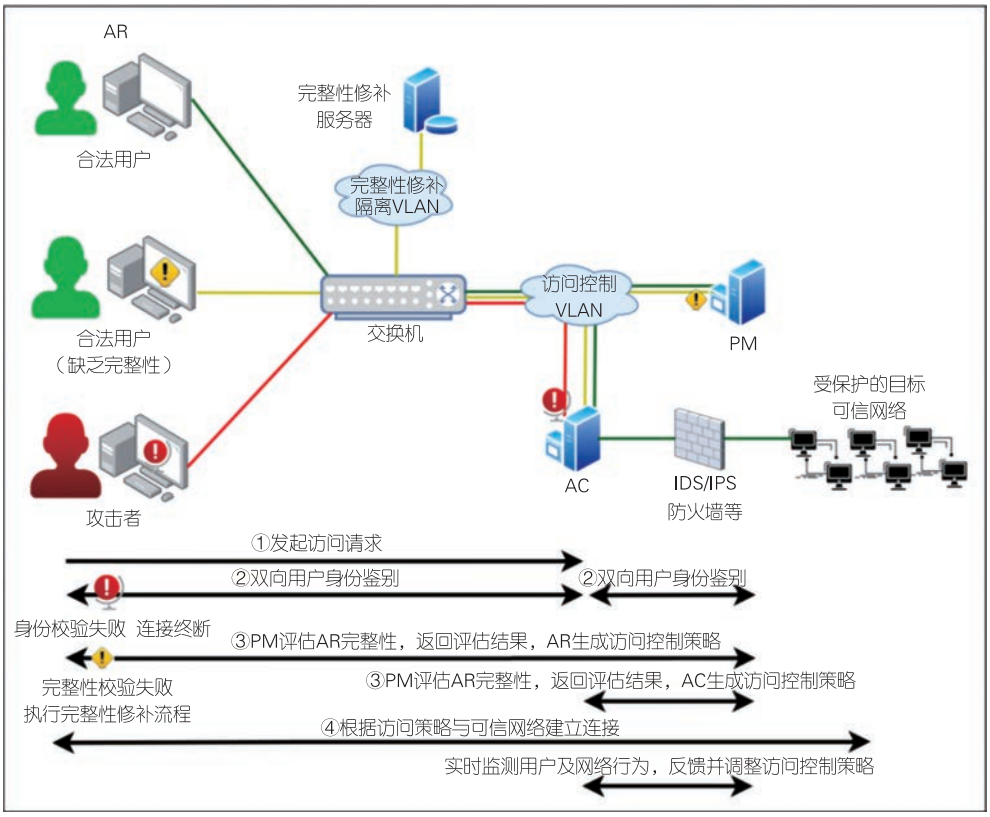
3.4 基于DevSecOps的内生安全路线

DevOps是一套将开发、运维、质量保障相结合，通过实施自动化流程与高效沟通合作，使软件开发整体过程更加快捷可靠的理念，如图5所示。DevSecOps是DevOps概念的延续，它将安全无缝集成到软件开发运维过程中，要求软件开发团队和运营团队与安全团队密切合作，人人参与软件的安全治理，对DevOps周期中每个阶段的安全负责。

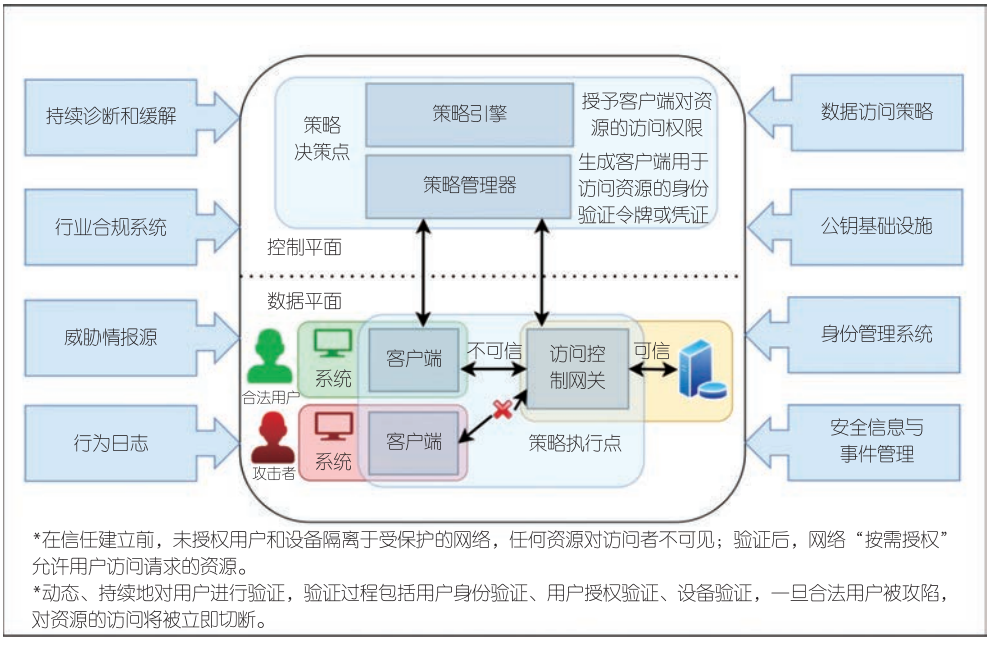
DevSecOps是一种基于安全治理的应用级内生安全实施方案，在两个层面上保障软件开发全流程的内生安全：（1）基于安全左移的理念，在软件架构设计阶段充分考虑安全因素，并基于应用运行自我保护（RASP）技术、软件成分分析（SCA）技术、交互式应用安全测试（IAST）技术等，在开发环节使软件“天生”安全；（2）基于敏捷安全的理念，在运维过程中积极实施入侵与攻击模拟（BAS）以及安全度量，通过自动化技术实现敏捷自适应、软件与网络环境的共生进化。目前DevSecOps的应用场景主要为软件供应链与云原生的安全保障。因能够契合当前互联网行业产品迭代的需求，该技术已在微软、谷歌、腾讯等实现规模化应用[14]。

3.5 基于物理层安全技术的内生安全路线

随着5G网络的规模化发展，移动通信的网络安全问题成为研究的重点。物理层安全技术的本质是利用通信双方无线信道的特征、无线终端的制造容差、目标用户的地理位置



▲图3 TCA可信连接架构部署示例



▲图4 零信任安全架构[11]

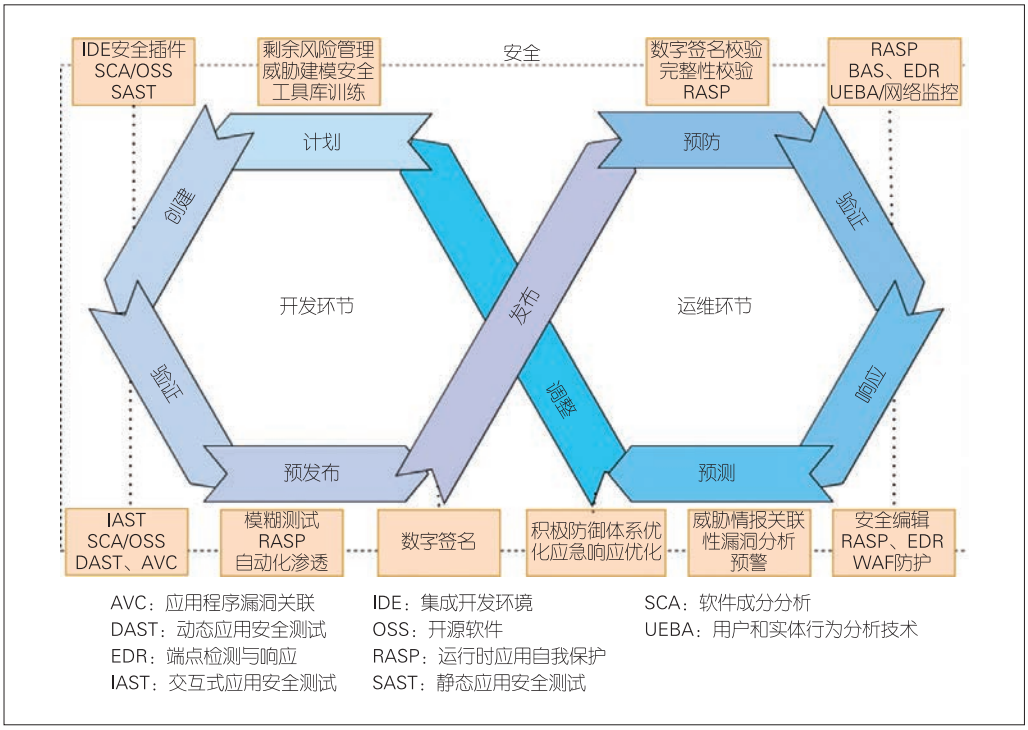
等物理特征，经过信号处理后，提取物理特征指纹，实现绑定于设备自身、通信信道上的身份识别、密钥生成、安全传输。与上层安全技术相比，物理层安全技术由于具备轻量级、难复制的特点，可以解决高速率数据传输加密、鉴权认证增强、数据完整性保护等多方面的难题。

目前不少学者针对Wi-Fi、ZigBee、LoRa、长期演进（LTE）等常见的无线通信协议进行了设备指纹提取的研究，典型的研究方法包括信号功率谱方法、差分星座轨迹图方法等，但物理层安全技术并未得到规模化应用[15-16]。

3.6 基于改进IP协议的内生安全路线

现有的IP协议围绕着开放、互联、安全、可信的核心使命，具备无连接性、分组交换、尽力而为的转发、基于IP地址的寻址等特点，并且经过超半个世纪的补充与完善，形成了IPv6、IPsec、信息中心网络（ICN）、命名数据网络（NDN）等改进方案。这些方案以数千条请求评论（RFC）文档的形式，为IP协议打补丁或增加附加功能。

当前人们对IP协议的具体批判主要针对尽力而为的转发与基于IP地址的寻址，认为IP协议虽然完美地完成了开放与互联的使命，但是在安全与可信上有所欠缺。这是因为：IP协缺乏内生的可信和安全机制，无法保证



▲图5 将安全集成于开发运维的DevSecOps流程框架

用户信息的完整性和不可篡改性；IP协议缺乏内生的资源感知和管控能力。在B5G/6G、工业互联网等场景下，现有基于IP协议的网络体系已经很难适应未来的业务需求。因此，针对下一代网络架构的设计，如何在开放与互联主题不变的条件下，实现安全与可信是IP协议的改进方向。IPv6、NewIP是两项改进IP内生安全性的热门方案。

IPv6的初衷是为了解决IPv4地址枯竭的问题。相比于IPv4，IPv6的头部长度从32位扩容到128位。地址扩容使得IPv6的安全性得到极大提升，这主要体现在以下几方面：

（1）可溯源与防扫描。攻击者若要实现像在IPv4条件下的网段主机地址扫描是极其困难的。同时IPv6终端之间可建立点对点连接，无需地址转换，在攻击发生后易于及时处置，因而系统能够实现高效的信息安全治理。

（2）IPv6默认支持IPsec协议。IPv6通过扩展认证报头（AH）和封装安全载荷报头（ESP）实现加密和验证功能，不需要额外对IPSec扩展包头进行处理。

（3）IPv6支持真实源地址验证体系结构（SAVA）[17]（RFC5210）。相比于IPv4协议只基于目标地址进行路由选择的转发机制，IPv6可通过SAVA体系识别并阻止伪造的源地址报文被转发，使每一个转发分组的IP源地址都是真实的。与IPv4相比，IPv6在安全性方面进行了预先设计与考虑，但仍然存在一些难以解决的安全风险。虽然使网络的安全性有一定的提升，但IPv6的改进仍然是增量式的，内生安全机制仍然是不完备的[18]。

New IP由华为网络技术实验室于2019年提出，旨在提供万网互联、万物互联的新连接能力、确定性传输及大吞吐量传输的新服务能力、安全可信及用户可定义的新内生安全能力，在保留原IP协议高生存性、高可达性、尽力而为的核心优势的前提下，提升确定性转发、高互联、内生安全等新能力，实现能力的增强与扩展，满足更高要求、更复杂的应用业务需求。其基本实现思路是在包头中增加服务标识与身份标识，使得网络可以根据标识优先级，实现更适配业务特征的资源调配及安全保障[19]。在内生安全能力提升方面，New IP架构主要提升了端到端通信业务安全与网络基础设施安全两大方面。New IP基于可信身份管理、真实身份认证、审计溯源、访问控制、密钥管理等安全模块，构建了由可信节点参与的、可审计的安全域。同时，New IP采用去中心化技术构建网络基础设施，提供不依赖于根节点的证明，从而解决了美国根节点权限过大、单点失效等问题[20]。

3.7 基于伴生网络对抗学习的内生安全路线

伴生网络是基于数字孪生技术将物理网络在数字空间中映射出1∶1平行运行的数字化虚拟网络。伴生网络通过采集网络设备实时数据，利用模型构建、修正与融合技术，构建与物理网络一致的数据模型，进而可以实现低成本试错与智能化预测。于全等提出类生物免疫机制的网络安全架构。该网络架构搭载了其自身的数字孪生体——平行伴生网络，并在伴生网络中加载高强度的人工智能攻击，通过攻防对抗学习生成“网络疫苗”，依靠强于攻击者的超级算力动态构成先于攻击的防御策略，从而获得网络空间的对抗优势[21]。

然而，在机理上网络空间的安全防护与生物体的免疫是否可以类比，目前仍然存在疑问。此外，基于目前人工智能的发展水平，人们尚未能构建可以发现创造性的、超出现有人类认知的攻击方式的框架，只能就某一维度的攻击方式进行挖掘。

因此，基于伴生网络对抗学习的安全能力并不具有完备性，不能完全取代其他安全工具，而是起到相辅相成的作用。

4 内生安全关键技术

当前网络内生安全仍处于技术孕育阶段，因此梳理各发展路线上的关键技术，开展未来网络内生安全的关键技术识别，将有利于技术的融合与统一架构的形成。本章将从技术层面对拟态防御、可信计算、零信任等路线的关键技术及其在内生安全领域的作用加以介绍。

4.1 拟态防御关键技术

邬江兴院士等将移动目标防御（MTD）技术的动态性与*N*-变体系统的异构冗余特性相结合，提出了基于动态异构冗余的拟态防御模型[22]，如图6所示。系统通过分发器将输入复制*N*份，并通过动态选择算法将相同或相异的组件组合成*N*个异构执行体（每个异构执行体分别独立处理输入），之后将*N*份执行结果交给表决器处理。当至少有*K*个执行体正常工作时（*N*=3、*K*=2的三模冗余架构最为普遍），我们就可以认为整个系统是正常运行的。同时，系统具有动态切换机制，可根据运行过程中产生的告警/报错信息（或在固定时间后），将旧的异构执行体替换为可信的新重构的异构执行体，从而实现更高的动态性[23]。

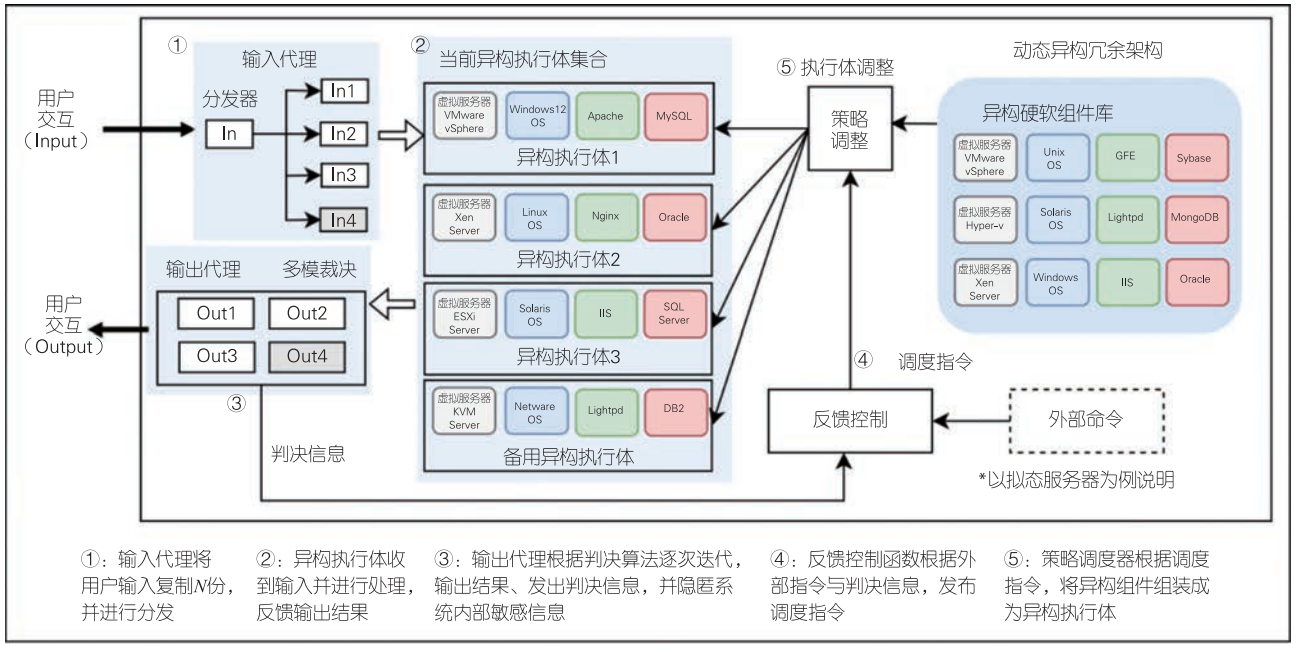
将动态异构冗余架构应用于网络内生安全的构件后，邬江兴院士等提出全维可定义多模态智慧网络[24]。该网络系统的异构资源池由平台、系统、部件、模块多层面上的网络功能组成，包括异构的网络拓扑、寻址路由、交换模式、网元形态、传输协议等。网络通过人工智能技术、智慧化网络管理机制，从异构资源池中选取不同层面上的网络技术，组成不同模态的网络执行体集，实现网络层面上的拟态防御。

4.2 可信网络关键技术

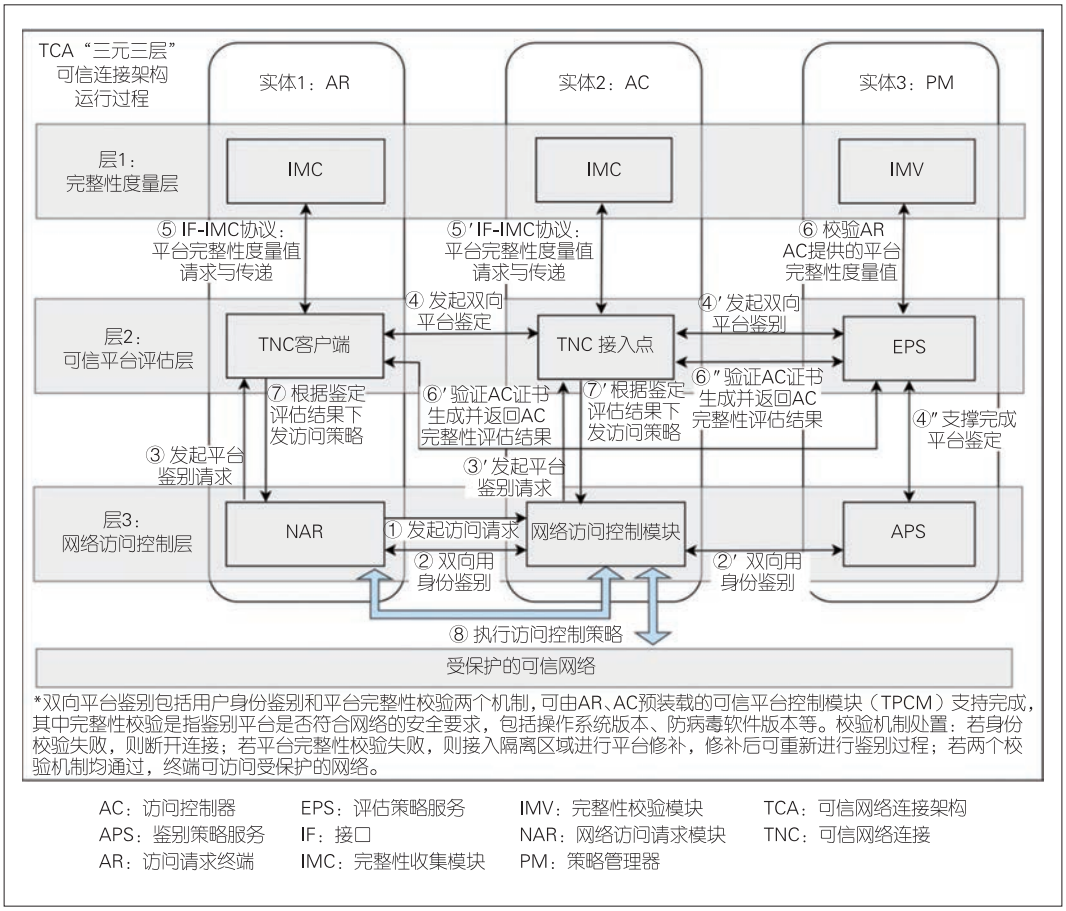
在可信计算与可信网络架构TNC基础上[9]，中国提出了具备主动免疫机制的TCA，如图7所示。TCA三元三层网络架构由实体、层、组件和组件间接口组成。通过多步骤的鉴别、认证，TCA可以实现身份鉴别、平台鉴别、完整性度量、策略管理、保密通信等功能。在鉴别身份、判断被授权允许访问网络的基础上，TCA还要检查终端当前的完整性及其他安全属性是否与网络要求的安全策略一致，从而为网络环境提供稳定可靠的保证[10]。

4.3 零信任关键技术

美国国家标准与技术研究院（NIST）将零信任的核心



▲图6 动态异构冗余架构



▲图7 可信网络连接架构关键流程

技术归纳为软件定义边界（SDP）、身份和访问管理、微隔离[11]，如图8所示。

SDP基于安全策略可灵活创建边界，用于将服务与不安全的网络隔离开，提供按需、动态的网络安全。区别于传统传输控制协议（TCP）/IP网络的默认允许连接，在没有经过身份验证和授权之前，受保护的资源对于终端用户是完全不可见。SDP主要由SDP控制器、SDP安全网关、SDP客户端三大组件构成。其中，SDP控制器用于认证和授权SDP客户端，并配置SDP网关的连接；SDP网关与控制器通信并强制执行策略，控制客户端的访问流量。

身份和访问管理可确认访问者身份的合法性，并为合法用户在规定时间内按照访问权限来要求受保护资源提供一种安全的方法。身份和访问管理技术的发展经历了从粗粒度到细粒度的转变，实现了设备内部不同端口之间的流量控制。此外，基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）、基于任务的访问控制（TBAC）等均各有侧重。对于零信任网络的身份与访问控制（IAM），目前人们正在提升策略的动态性，并尝试将已有技术的优势加以融合。

微隔离是一种细粒度的边界安全管理策略，是边界隔离不断向受保护资源靠近的结果，主要以软硬件结合的方式，通过虚拟化环境中划分逻辑域来形成逻辑上的安全边界，实现细粒度的流量监测、访问控制和安全审计功能。目前微隔离的实现方法主要分为物理安全设备（防火墙、IPS、IDS等）、主机代理、软交换（Softswitch）和虚拟机监视器（Hypervisor）等方式[25]。

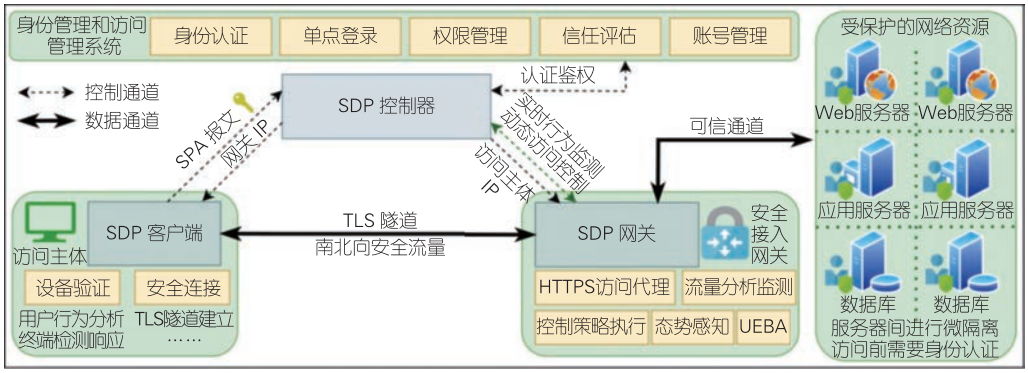
4.4 DevSecOps关键技术

DevSecOps将多项安全技术集成于软件开发的整体流程中，其基本技术架构如图9所示。其中，云原生应用程序保护平台（CNAPP）是一个整合了安全和合规方法的功能集，作为云原生应用安全开发的基础设施保障与框架；应用运行自我保护（RASP）内置于应用内部，通过钩子（Hook）关键函数，实时监测应用在运行时与其他系统的交互过程，可根据上下文环境识别并阻断攻击；交互式应用安全测试技术（IAST）通过在软件代码运行的中间件上插入探针，自动识别和判断应用中的安全漏洞；软件成分分析（SCA）通过对二进制软件的组成部分进行分析，清点开源软件的组件及其构成和依赖关系，识别已知的安全漏洞或者潜在的许可证授权问题，并把这些风险排查在应用系统投产之前，也适用于应用系统运行中的诊断分析；入侵与攻击模拟（BAS）通过持续模拟针对企业资产进行攻击的剧本及payload，验证企业安全防御的有效性[14]。

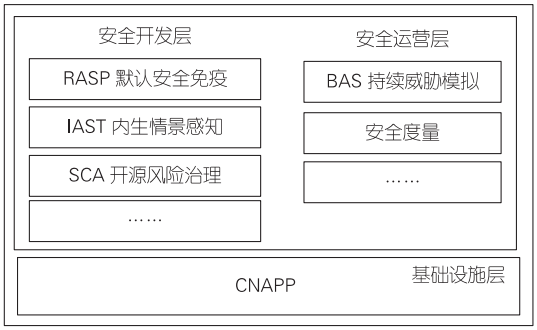
4.5 其他内生安全技术

4.5.1 增强的密码技术

密码技术是安全领域的基础，主要基于传统数学难题的诸多公钥密码体系。由于量子计算正面临严峻的安全威胁，



▲图 8 基于软件定义边界、身份和访问管理、微隔离三大关键技术的零信任网络架构



▲图 9 DevSecOps 安全技术栈架构

传统密码学又发展为两种：利用量子力学性质来保护数据的量子密码学和能够抵抗量子算法攻击的经典密码学，其中后者又被称为后量子密码学。

量子密码协议目前正处于量子密钥分配协议遥遥领先、其他协议有待突破的状态。量子密钥分配是一种通信双方通过传输量子态来建立密钥的协议。最著名的 BB84 和 E91 协议通过量子态纠缠协商安全密钥。如果攻击者试图读出基于纠缠的量子态中的信息，量子态将不再处于叠加态，通信双方将意识到攻击者可能存在，即抛弃本次协商并重新进行新的协商[26]。

后量子密码学算法的实现方法主要有 4 种：基于格、基于编码、基于多变量、基于哈希。当参数选取适当时，目前还没有已知的经典算法和量子算法可以快速求解这些问题。

4.5.2 物理层安全关键技术

物理层安全技术是十分有前景的上层密码学技术的替代/增强方案，主要包括物理层身份认证、物理层密钥生成、物理层安全传输。

物理层身份认证技术利用无线终端设备在生产过程中不可避免的容差，针对设备发射信号的瞬态、稳态部分，提取设备特异性的“指纹”，进而实现对海量终端的认证。物理层密钥生成技术利用通信双方私有的信道特征，提供实时生成、无需分发的快速密钥更新手段，实现一次一密的完美加密效果。物理层安全传输技术则利用无线信道的差异设计与位置强关联的信号传输和处理机制，使得只有在期望位置上的用户才能正确解调信号，其他位置上的用户解调后只能得到置乱加扰、不可恢复的信息[15-16]。

4.5.3 数字孪生网络关键技术

数字孪生网络是物理网络的虚拟表示，基于数据和模型与物理网络实时交互映射，从而提供诊断评估、决策分析、预测性运维等能力，新的安全技术可以更容易地在数字孪生网络中得到测试与验证。

数字孪生网络架构可以分为物理网络层、孪生网络层、网络应用层。物理网络层主要包含构成端到端网络的物理实体，包括移动接入网、移动核心网、骨干网、数据中心网或端到端的跨域网络等。物理网络层通过接口实现与网络孪生体的网络数据和控制信息交互。孪生网络层包含 3 个关键子系统：数据共享仓库、服务映射模型和网络孪生体管理，分别提供网络数据采集和存储及统一接口服务、数据模型实例、全生命周期管理和可视化呈现服务。网络应用层通过接口将需求输入至孪生网络层，同时进行业务部署。充分验证后，孪生网络层将控制更新下发至物理网络层，以实现网络创新技术和应用低成本、高效率的快速部署[27]。

5 结束语

未来网络应具备内生安全属性已成为网络安全领域的共识，但目前内生安全概念的明确内涵（建设什么样的内生安全）与内生安全的技术路线（如何建设内生安全）尚未形成一致性方案。为此，本文从网络发展的角度分析了网络内生

安全建设的必要性，讨论了从当前多强并立状态到网络内生安全完全建成的演进阶段，简要介绍了当前包括拟态防御、可信计算、零信任、物理层安全在内的多条技术路线齐头并进的研究现状，并从架构的层面概述了各路线的关键技术，尝试梳理总结网络内生安全的现状。

参考文献

[1] 中兴通讯股份有限公司. 2030+网络内生安全愿景白皮书 [R]. 2021
[2] 吴礼发, 洪征, 李华波. 网络攻防原理与技术 [M]. 2版. 北京: 机械工业出版社, 2017
[3] 邬江兴. 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
[4] WU J X. Cyberspace mimic defense: generalized robust control and endogenous security [EB/OL]. [2022–09–25]. https://www.doc88.com/p–9009953314809.html. DOI: 10.1007/978–3–030–29844–9
[5] 中国信息通信研究院. 2021年中国网络安产业白皮书 [R]. 2022
[6] 邬江兴. 网络空间内生安全(上册): 拟态防御与广义鲁棒控制 [M]. 北京: 科学出版社, 2020
[7] SHEN C X, ZHANG H G, WANG H M, et al. Research on trusted computing and its development [J]. Science China information sciences, 2010, 53(3): 405–433. DOI: 10.1007/s11432–010–0069–x
[8] MA J F, WANG C G, MA Z. Architecture of trusted network connect [M]// Security Access in Wireless Local Area Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 401–423. DOI: 10.1007/978–3–642–00941–9_11
[9] 吕润璞, 郝福珍. TNC可信网络架构与元数据存取点研究 [J]. 计算机工程与设计, 2010, 31(2): 243–248. DOI: 10.16208/j.issn1000–7024.2010.02.037
[10] 李明, 李琴, 张国强, 等. 可信网络连接架构TCA的实现及其应用 [J]. 信息安全研究, 2017, 3(4): 332–338. DOI: 10.3969/j.issn.2096–1057.2017.04.007
[11] ROSE S, BORCHERT O, MITCHELL S, et al. Zero trust architecture [R]. 2020
[12] 张泽洲, 王鹏. 零信任安全架构研究综述 [J]. 保密科学技术, 2021, (8): 8–16
[13] 郭雪, 吴倩琳, 孔松. 零信任的行业应用场景分析研究 [J]. 中国信息安全, 2022, (2): 36–38. DOI: 10.3969/j.issn.1674–7844.2022.02.012
[14] 子芽. DevSecOps敏捷安全 [M]. 北京: 机械工业出版社, 2022
[15] 厉东明, 杨旋. 6G物理层安全技术综述 [J]. 移动通信, 2022, 46(6): 60–63
[16] 黄开枝, 金梁, 钟州. 5G物理层安全技术: 以通信促安全 [J]. 中兴通讯技术, 2019, 25(4): 43–49. DOI: 10.12142/ZTETJ.201904008
[17] WU J P, BI J, LI X, et al. A source address validation architecture (sava) testbed and deployment experience [R]. 2008
[18] DURDAĞI E, BULDU A. IPV4/IPV6 security and threat comparisons [J]. Procedia – social and behavioral sciences, 2010, 2(2): 5285–5291. DOI: 10.1016/j.sbspro.2010.03.862
[19] CHEN Z, WANG C, LI G W, et al. NEW IP framework and protocol for future applications [C]//Proceedings of NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2020: 1–5. DOI: 10.1109/NOMS47738.2020.9110352
[20] 郑秀丽, 蒋胜, 王闯. NewIP: 开拓未来数据网络的新连接和新能力 [J]. 电信科学, 2019, 35(9): 2–11. DOI: 10.11959/j.issn.1000–0801.2019208
[21] 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] 秦俊宁, 韩嘉佳, 周升, 等. 基于异构冗余架构的拟态防御建模技术 [J]. 电信科学, 2020, 36(5): 31–38
[23] 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. DOI: 10.1049/iet–ifs.2017.0086
[24] 邬江兴. 多模态智慧网络与内生安全 [J]. 网信军民融合, 2018, (11): 11–14
[25] 王群, 袁泉, 李馥娟, 等. 零信任网络及其关键技术综述 [EB/OL]. (2022–06–23) [2022–09–25]. https://kns.cnki.net/kcms/detail/51.1307.TP.20220622.0934.006.html
[26] 张雪, 高飞, 秦素娟, 等. 量子密码协议研究现状与未来发展 [J]. 中国工程科学, 2022, 24(4): 145–155. DOI: 10.15302/J–SSCAE–2022.04.015
[27] 孙滔, 周敏, 段晓东, 等. 数字孪生网络(DTN): 概念、架构及关键技术 [J]. 自动化学报, 2021, 47(3): 569–582. DOI: 10.16383/j.aas.c210097

作 者 简 介

王瀚洲，北京航空航天大学在读硕士研究生；主要研究领域为信息网络安全、网络体系结构。

刘建伟，北京航空航天大学网络空间安全学院教授、博士生导师、院长，享受国务院政府特殊津贴，现任国务院学位委员会第八届学科评议组成员、教育部高等学校网络空间安全专业教学指导委员会委员、中国密码学会常务理事、中国指挥与控制学会常务理事、中国电子学会网络空间安全专委会副主任委员、中国指挥与控制学会网络空间安全专委会副主任委员、中关村智能终端操作系统联盟副理事长；曾获国家技术发明一等奖、国防技术发明一等奖、中国指挥与控制学会科技进步一等奖等，所编写的教材获全国普通高校优秀教材一等奖、国家网络安全优秀教材、国家精品教材、全国优秀科普作品奖、第四届中国科普作家协会优秀科普作品金奖等；出版教材7部、专著2部、译著1部。

主动免疫可信计算综述

A Survey on Active Immune Trusted Computing

张建标/ZHANG Jianbiao[1,2]，黄浩翔/HUANG Haoxiang[1,2]，胡俊/HU Jun[1,2]
（1. 北京工业大学，中国 北京 100124；
2. 可信计算北京市重点实验室，中国 北京 100124）
(1. Beijing University of Technology, Beijing 100124, China;
2. Beijing Key Laboratory of Trusted Computing, Beijing 100124, China)

DOI:10.12142/ZTETJ.202206003
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.tn.20221209.1035.002.html
网络出版日期：2022-12-10
收稿日期：2022-10-25

摘要：对主动免疫可信计算的基本思想及特征进行了重点阐述，并从标准体系、解决方案及产业发展3个方面对主动免疫可信计算进行详细介绍。认为随着等级保护2.0标准的实施，主动免疫可信计算技术已在保障重要信息系统的安全可信中发挥了重要的作用。

关键词：可信计算；主动免疫；主动防御；双体系结构；网络安全

Abstract: The basic ideas and characteristics of active immune trusted computing are expounded, and active immune trusted computing is then introduced in detail from three aspects of the standard system, solution, and industrial development. It is believed that with the implementation of level protection 2.0 standard, the active immune trusted computing technology has played an important role in ensuring the security and credibility of important information systems.

Keywords: trusted computing; active immune; active defense; dual system structure; cyber security

网络空间已成为继陆、海、空、天之后的第五大主权领域空间，没有网络安全就没有国家安全。提供安全可信的网络产品和服务是国家法律（《中华人民共和国网络安全法》[1]）、战略（网络空间安全战略[2]）和等级保护制度的要求。为配合网络安全法的实施，新修订的网络安全等级保护（简称等级保护2.0）标准[3]，突出了主动免疫可信计算支撑的一个中心三重防护的安全框架，通过可信验证确保各个环节的安全可信，保障国家重要信息系统的安全。

1 主动免疫可信计算介绍

1.1 基本思想

信息安全问题由图灵计算模型缺少攻防理念、冯·诺依曼架构缺少防护部件、工程应用无安全管控服务三大原始缺陷而引起[4]。传统的计算机体系结构专注于计算功能的实现，缺乏对安全防护的考虑。这就相当于一个人没有免疫系统，只能生活在无菌状态下。此外，人类对事物的认知存在局限性，而系统设计过程中所具有的逻辑组合无法穷尽，必然会存在逻辑不全的缺陷，而当前大部分网络安全系统主要是由防火墙、入侵监测和病毒防范等“老三样”组成，消极被动的封堵查杀不仅难以应对利用逻辑缺陷的攻击，且只能被动抵御已知病毒[5]。

相较于“老三样”，主动免疫可信计算能够实现计算机体系结构的主动免疫，其基本思想为：在计算机系统中建立一个可信根，可信根的可信性由物理安全、技术安全、管理安全共同确保；再建立一条可信链，从可信根开始到硬件平台、操作系统、应用，一级测量认证一级，一级信任一级，把这种信任扩展到整个计算机系统中，从而确保整个计算机系统的可信[6]。

主动免疫可信计算就是要为计算平台建立起免疫系统，是一种在运算的同时进行安全防护的新计算模式。该模式以密码为基因实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏并排斥进入机体的有害物质。这相当于为网络信息系统培育了免疫能力[7]。

1.2 主要特征

（1）新计算模式：计算同时进行安全防护

计算机最初的设计目标是为了解决复杂计算问题，因此其体系结构在设计时要解决的核心问题即是提高计算速度，但却忽略了安全问题，如系统任务难以隔离、内存无越界保护等。这直接导致网络化环境下的计算服务存在很多安全问

基金项目：北京市自然科学基金（M21039）

题，如源配置可被篡改、恶意程序被植入执行、利用缓冲区（栈）溢出攻击、非法接管系统管理员权限等[6]。主动免疫可信计算是一种运算时进行安全防护的新计算模式，该模式采用计算和防护并行的双体系结构，在计算的同时进行安全防护，使计算结果总是符合预期，计算全程可测可控，不被干扰。

（2）双体系结构：计算部件+防护部件

如图1所示，主动免疫可信计算采用计算部件和防护部件并行的双体系结构。其中，计算部件即为通用计算系统，防护部件则是负责实施主动免疫可信计算的部件。主动免疫可信计算保持通用计算系统功能流程不变的同时，通过逻辑独立的防护部件，能够主动实施对计算部件（计算组件、系统固件、系统软件、应用软件）的可信监控，从而实现对计算部件全生命周期的可信保障。

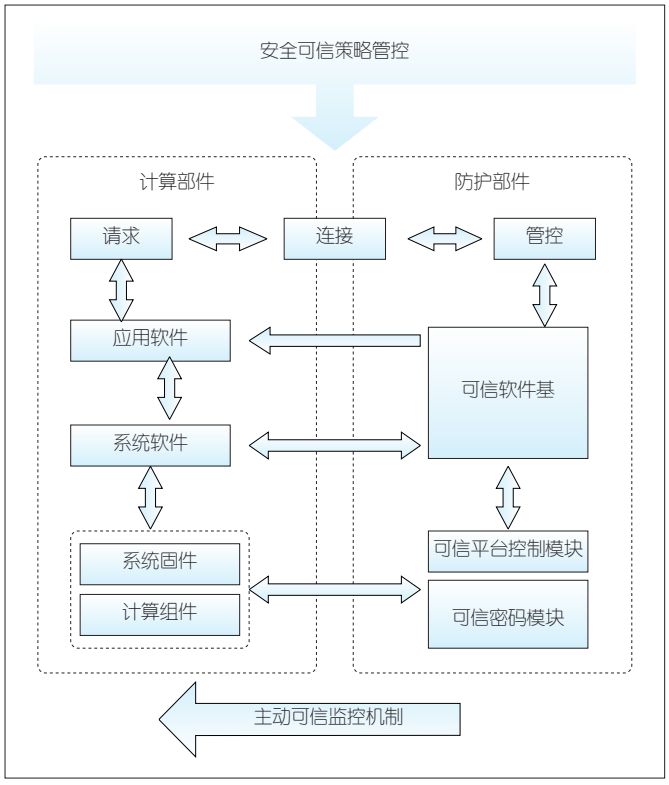
防护部件以并接于计算部件的可信平台控制模块（TPCM）作为可信根。TPCM在连接可信密码模块（TCM）的基础上增添对计算部件和外设的总线级控制功能，成为系统可信的源头。TPCM融合密码机制与控制机制，先于计算部件中央处理器（CPU）启动，主动对计算部件进行度量并实施控制。之后，可信软件基构建，对上承接可信管理机制，在安全策略规则的支配下实施主动监控；对下调度管理TPCM等可信硬件资源，协调完成主动度量及控制。

针对集中控管的网络环境安全需求，我们提出了三元三层对等可信网络连接架构，通过安全管理中心集中管理，对网络通信连接的双方资源实施可信度量和判决，有效防范内外合谋攻击。

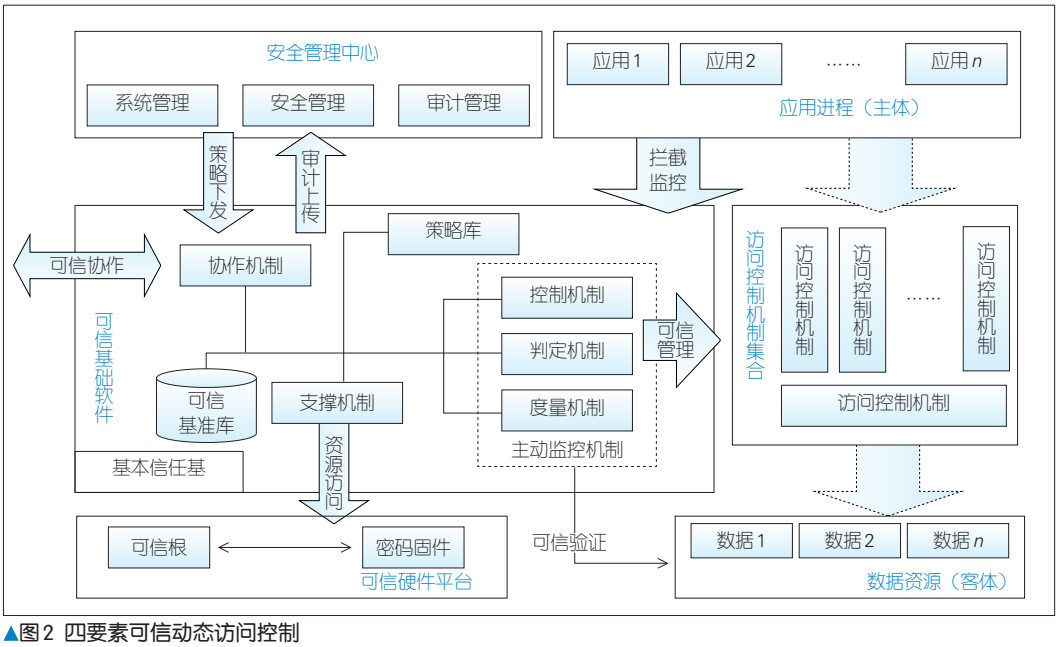
（3）四要素可信动态访问控制

传统访问控制机制是实现系统安全的有效措施，它基于主体、客体和操作三要素，控制主/客体的操作行为，保证系统访问的安全。但传统无计算环境要素的访问控制策略模型只基于授权标识属性进行操作，不作可信验证。这带来了难防篡改的安全缺陷，如恶意用户假冒合法实体进行资源访问、合法实体被篡改导致越权访问资源破坏、破坏被授权客体的完整性、计算环境的重要配置文件被篡改[8]等，访问控制过程的可信性无法保障。

因此，我们必须对访问控制过程中的“主体、客体、操作、环境”四要素进行动态可信度量、识别和控制，如图2所示。



▲图1 计算+防护的双体系结构



▲图2 四要素可信动态访问控制

（4）三重防护框架

一个中心三重防护，就是针对安全管理中心和安全计算环境、安全区域边界、安全通信网络的安全合规进行方案设计，建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障体系。2019年12月实施的国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019）更加强调了安全通信网络、安全区域边界和安全计算环境的可信验证要求，即实现以可信验证为支撑的一个中心三重防护，如图3所示。

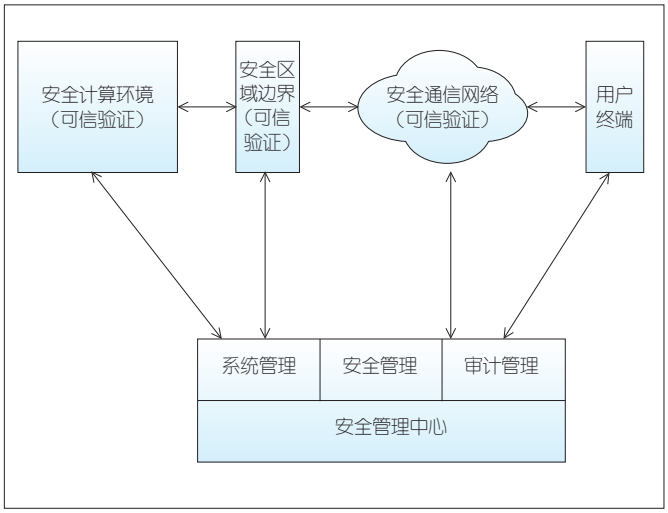
2 主动免疫可信计算研究进展

2.1 标准体系

2006年中国进入可信计算规范和标准的制定阶段，国家密码管理局制定了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》。2007年在国家信息安全标准化委员会的主持下，北京工业大学可信计算实验室牵头，联合几十家单位，开始“可信平台控制模块”等4个主体标准和“可信计算体系结构”等4个配套标准的研究工作，构建了中国可信计算标准的体系框架，为后续制定一系列的可信计算国家标准奠定了基础。目前中国已经发布的可信计算相关标准如表1所示。

2.2 解决方案

TPCM作为构建主动免疫可信计算体系的信任锚点，具备主动控制和度量功能。当前，根据应用平台的不同，TPCM主要有3种构建形式：计算部件主板上增加TPCM；多核CPU的一个核作为TPCM；通过外部设备互连（PCI）插卡接入TPCM。



▲图3 可信验证支撑的一个中心三重防护

▼表1 可信计算国家标准

标准编号	名称
GB/T 29827—2013	信息安全技术 可信计算规范 可信平台主板功能接口
GB/T 29828—2013	信息安全技术 可信计算规范 可信连接架构
GB/T 29829—2022	信息安全技术 可信计算密码支撑平台功能与接口规范
GB/T 36639—2018	信息安全技术 可信计算规范 服务器可信支撑平台
GB/T 37935—2019	信息安全技术 可信计算规范 可信软件基
GB/T 38638—2020	信息安全技术 可信计算 可信计算体系结构
GB/T 40650—2021	信息安全技术 可信计算规范 可信平台控制模块

1）TPCM结构有两种主流的呈现方式。

（1）独立TPCM芯片：多用于以嵌入式系统为代表的计算资源有限的平台中，能够降低计算平台资源开销，且具备较高的物理可信性。文献[9]所述基于TPCM芯片的三阶三路可信平台主动防护架构方案表明，实验芯片通过直接存储器访问（DMA）协议或CPU共享总线交换数据，降低了系统开销，具备较高的安全性。

（2）基于基板管理控制器（BMC）构建TPCM：BMC具有独立处理器、内存和存储空间的服务器度量器件，能够实现对服务器硬件设备的主动监测和控制，成为构建“计算”与“防护”并行的主动免疫双体系结构的理想方案。北京工业大学可信计算重点实验室基于BMC构建服务器启动及运行过程，对“计算”和“防护”并行主动免疫架构进行了较为丰富的研究。随着TPCM相关的产、学、研、用多领域深度融合以及相应接口标准的完善，TPCM软硬生态建设及工程应用已趋于成熟。

2）随着多核CPU计算平台/服务器在实际中应用，基于其多核特性，构建计算核、安全核并行的主动免疫可信架构成为一种高效的解决思路。以海光、申威为代表的国产服务器生产商均研发了多核可信服务器，有效提高了国产服务器的安全性。在文献[10]中，安全防御机制由与普通处理器并行运行的安全处理器来充当，实现硬件级别的物理隔离，具备较高的安全性。但是由于物理隔离导致安全处理器对主机内存语义信息的获取较为困难，因此主动可信度量的结果较为粗粒度，且该方案只是对静态代码段进行周期性度量，度量有效性较低。文献[11]提出了一种改进的针对飞机硬件的攻击免疫超级监控可信架构。该架构基于轻量级精简指令集计算机（RISC）CPU来独立运行可信监控系统（TMS），实现TMS与主处理器系统（MPS）的安全隔离，使得对手很难

通过软件进行攻击。

3）外接可信插卡：通过外接可信插卡的方式实现防护部件，能实现对旧计算系统改造，降低了实现难度和工程成本。如华虹设计推出的高速串行计算机扩展总线标准（PCIE）可信加固卡提供了一组串行外设（SPI）Master接口，用于对计算平台主机基本输入输出系统（BIOS）进行主动度量，并可用来控制计算机主板上电时序的多组隔离输入/出开关控制系统，从而实现芯片层面的主动控制要求。文献[12]通过在异构计算网络加速卡上设置控制逻辑芯片、安全可信芯片及PCIE总线开关，构造了一种基于异构计算的安全可信卡。文献[13]提出了一种PCIE和MINIPCIE双接口的通用安全可信接口卡，能够通过TCM芯片与主板复杂可编程逻辑器件（CPLD）和CPU之间的信号传递及控制实现主动度量及端口主动控制功能。

TrustZone的快速发展为防护部件提供了隔离受保护的可信运行环境，同时防护部件为系统、应用提供丰富的可信度量、监控等功能，这种构建模式契合双系统体系架构的核心思想，成为构建主动免疫可信方案的一种改造思路[14]。文献[15]从控制流的角度提出了一种动态度量方案，该方案基于TrustZone构建内核飞地，从而确保监控度量模块无法被攻击者篡改或绕过，最终确保动态度量过程的可信性。文献[16]中的TrustZone架构实现了一种双系统体系架构下的主动度量机制，使得位于安全世界的防护部件能够主动对非安全世界的计算部件进行度量。

2.3 产业发展

2014年4月16日，由中国工程院沈昌祥院士提议，中国电子信息产业集团、北京工业大学、中国电力科学研究院等60家单位发起的中关村可信计算产业联盟正式成立。目前，该联盟成员包括国有企业、民营企业、上市公司、研究院所、大专院校等网络安全领域各种单位200多家，涉及中国可信计算产业链的各个环节，覆盖了产、学、研、用、测各界，有效推动了可信计算的产业化和市场化。2020年10月28日，国家网络安全等级保护制度2.0与可信计算3.0攻关示范基地在北京工业大学揭牌成立。目前，基于TPCM国家标准，主板并加可信SoC、多核CPU可信核及外接可信插卡3种产品形态已被研发并大量推广应用[4]。“白细胞”等可信软件基产品的发布标志着中国自主创新的基于可信技术的新一代网络安全技术路线实现产业化。

3 对比分析

1999年，IBM、HP、Intel和微软等著名IT企业发起并成立了可信计算平台联盟（TCPA），2003年TPCA改组为可信计算组织（TCG），这标志着可信计算开始向泛计算领域应用扩展。TCG可信计算技术是以可信赖平台模块（TPM）芯片来增强计算平台的安全性。这种可信计算技术防护部件的安全性依赖于计算部件，因此存在着被旁路或篡改的风险。此外，TCG采用被动调用的外挂式体系结构，这种结构不仅缺乏主动防御能力，且计算和防护串行执行，难以符合等级保护2.0标准中对重要信息系统实施主动、动态安全防护的要求。

主动免疫可信计算提出了“计算+防护”的双体系结构，防护部件逻辑独立于计算平台。该结构不仅有效防止源于通用计算系统的广泛攻击，而且有效提高了性能。TPCM作为可信根，能够先于主机计算部件上电启动，实现对计算平台的主动控制。无须修改应用软件，TPCM上运行的可信软件基接管系统软件的内核层系统调用，实现主动、动态防护。表2给出了可信计算技术对比分析。

4 结束语

提供安全可信的网络产品和服务是国家网络安全法律、国家网络空间安全战略和国家等级保护制度的要求。2021年9月施行的关键信息基础设施安全保护条例，强调运营者应当优先采购安全可信的网络产品和服务。随着等级保护2.0标准的实施，主动免疫可信计算技术已在保障重要信息系统的安全可信中发挥了重要的作用。但在面对云计算、移动互联、物联网和工业控制系统等应用场景，我们还需要深入进行主动免疫可信计算关键技术研究、相关标准制定、产品研制、适配测试和推广应用。

▼表2 可信计算技术对比

	技术机制	可信根	体系架构	技术手段	安全强度	对业务影响/性能
TCG可信计算	被动可信	TPM	串行	TPM串接于外总线，可信软件栈作为子程序库被动调用	能够实现对计算系统的串行静态检测保护	需要对应用、系统进行适配更改/低
主动免疫可信计算	主动免疫可信	TPCM	计算+防护并行双体系结构	密码为基因，主动识别、主动度量、主动保密存储	能够主动抵御未知病毒、漏洞，能够对重要信息系统动态防护	不修改应用，计算与防护并行进行/高

TCG：可信计算组织　TPCM：可信平台控制模块　TPM：可信平台模块

参考文献

[1] 中华人民共和国网络安全法 [N]. 人民公安报, 2016-11-08(3)
[2] 中国网信网. 国家网络空间安全战略(全文) [J]. 中国信息安全, 2017(1): 26-31
[3] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求: GB/T 22239—2019 [S]. 2019
[4] 沈昌祥, 田楠. 主动免疫可信计算打造安全可信网络产业生态体系 [J]. 信息通信技术与政策, 2022(8): 1-6. DOI: 10.12267/j.issn.2096-5931.2022.08.001
[5] 李刚. 创新驱动 构筑网络强国安全保障——沈昌祥院士谈技术可信计算的创新与发展 [J]. 中国信息安全, 2015(2):46-51
[6] 沈昌祥. 用可信计算构筑网络安全 [J]. 求是, 2015(20):33-34
[7] 沈昌祥. 用主动免疫可信计算3.0筑牢网络安全防线营造清朗的网络空间 [J]. 信息安全研究, 2018, 4(4): 282-302. DOI: 10.3969/j. issn. 2096-1057.2018.04.001
[8] VERC. 美国国家安全局(NSA)"酸狐狸"漏洞攻击武器平台技术分析报告 [EB/OL].[2022-10-22].https://www.cverc.org.cn/head/zhaiyao/news20220629-FoxAcid.htm
[9] 黄坚会, 沈昌祥, 谢文录. TPCM三阶三路安全可信平台防护架构 [J]. 武汉大学学报(理学版), 2018, 64(2): 109-114. DOI: 10.14188/j. 1671-8836.2018.02.002
[10] JIA X Q, HE Y, WU X Y, et al. Performing trusted computing actively using isolated security processor [C]//Proceedings of the 1st Workshop on Security-Oriented Designs of Computer Architectures and Processors. ACM, 2018: 2-7. DOI: 10.1145/3267494.3267498
[11] CHENG D X, ZHANG C, LIU J W, et al. An attack-immune trusted architecture for supervisory aircraft hardware [J]. Chinese journal of aeronautics, 2021, 34(11): 169-181. DOI: 10.1016/j.cja.2021.03.004
[12] 毕革新, 刘铁军, 张晶威, 等. 一种基于异构计算的安全可信卡及安全可信方法: CN111737698A [P]. 2020
[13] 邹武, 张鲁峰, 周魏. 一种PCIE和MINIPCIE双接口的通用安全可信接口卡: CN109739791A [P]. 2019-05-10
[14] 董攀, 丁滟, 江哲, 等. 基于TEE的主动可信TPM/TCM设计与实现 [J]. 软件学报, 2020, 31(5): 1392-1405. DOI: 10.13328/j.cnki.jos.005953
[15] 张英骏, 冯登国, 秦宇, 等. 基于Trustzone的强安全需求环境下可信代码执行方案 [J]. 计算机研究与发展, 2015, 52(10): 2224-2238. DOI: 10.7544/issn1000-1239.2015.20150582
[16] 尹超, 周霆, 黄凡帆. 一种基于TrustZone架构的主动可信度量机制设计 [J]. 信息通信, 2020, 33(9): 17-20

作 者 简 介

张建标，北京工业大学教授、博士生导师；主要研究领域为可信计算、系统安全和区块链；先后主持和参加科研项目20余项；获北京市科学技术进步二等奖；已发表论文80余篇，授权专利20余项。

黄浩翔，北京工业大学在读博士研究生；主要研究领域为可信计算、云安全、可信访问控制；已发表论文4篇，申请专利10余项。

胡俊，北京工业大学讲师；主要研究领域为可信计算、云安全、工控安全；获2项科研成果奖；负责通用可信软件基、可重构TCM模拟器等可信计算开源软件项目；出版可信计算专著2本，申请专利10余项。

安全可信的互联网体系结构与端到端传送关键技术

Secure and Trusted Internet Architecture and Key Technologies of End-to-End Transmission

徐恪/XU Ke，冯学伟 /FENG Xuewei，
李琦/LI Qi，朱敏/ZHU Min

（清华大学，中国 北京 100084）
(Tsinghua University, Beijing 100084, China)

DOI：10.12142/ZTETJ.202206004
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221128.1433.002.html
网络出版日期：2022-11-28
收稿日期：2022-10-16

摘要：围绕无连接网络中安全可信的端到端传送关键问题，从互联网的工作原理出发，提出了具备安全可信和主动防御能力的互联网端到端传送关键技术，包括层间交互、语义一致的协议栈安全漏洞检测与防御，随机标识、层次验证的分组转发正确性检测，以及频域分析、交互图构造的传送连接可信检测，实现了分组数据可靠生成、安全传输、可信应用3个阶段全生命周期的安全闭环，有效增强了互联网的整体安全性。在实际网络环境中进行规模化应用及部署的结果表明，所提出的技术方法能够有效抵御拒绝服务（DoS）、流量劫持、身份欺骗、路由篡改等针对互联网的各种攻击威胁。

关键词：互联网体系结构；端到端传送；语义一致性；路径验证；恶意流量检测

Abstract: The key issues of secure and trusted end-to-end transmissions in connectionless are addressed. Aiming to ensure the consistency between network policies and the end-to-end transmission behavior, a new technique based on the working principles of the Internet is presented, i.e., identifying and mitigating vulnerabilities in protocol stacks by leveraging cross-layer interactions and semantic consistency analysis, detecting the correctness of packets forwarding path by leveraging random labels and hierarchical verification, as well as identifying the reliability of transmission connections by leveraging frequency domain analysis and interaction graph construction. Our technique can ensure the reliable generation, safe transmission and trusted application of IP packets in the three-stage life cycle, thus enhancing the security of the Internet. Through large-scale applications and deployments in the real world, experimental results show that our technique can effectively mitigate the threats of denial of service (DoS), traffic hijacking, identity spoofing, and route tampering.

Keywords: Internet architecture; end-to-end transmission; semantic consistency; path verification; malicious traffic detection

互联网已经成为国民经济赖以发展的重要信息基础设施。与此同时，互联网安全也是国家能源、交通、国防、教育等关键领域安全的重要保证。近些年，美国Colonial Pipeline输油管道网络勒索停服、委内瑞拉电网异常断电、乌克兰电信运营商Ukrtelecom服务中断、Log4j远程代码执行等大量网络安全事件表明，当前的互联网存在严重的安全缺陷和风险，可被攻击者所利用，从而对基础设施服务造成破坏，严重影响人们的日常生活[1]。

总的来说，网络应用的破坏和服务安全性的攻击主要来自3个方面：首先，在分组生成过程中，利用协议栈漏洞实施攻击破坏[2-6]；其次，在分组传输过程中，利用网络路由协议与转发机制设计的缺陷实施攻击破坏[7-10]；最后，在分组应用过程中，利用传送连接不可信开展大规模隐蔽攻击[11-12]。产生上述3个方面攻击威胁的根本原因在于：互联网体系结构在设计之初假设了通信双方和通信过程是真实可信的，无连接的网络状态也没有设计保障端到端传送安全可信的相关技术。这导致恶意攻击者有机会针对网络空间中的特定目标发起地址欺骗、流量劫持、分布式拒绝服务等多种类型的网络攻击，最终严重破坏网络中关键基础设施、服务等的安全性[13]。

本文围绕无连接网络中安全可信的端到端传送这一关键问题，从互联网的功能和原理出发，深入分析了分组数据生命周期中不同阶段面临的攻击威胁，然后从网络规范策略与端到端传送行为一致性保证出发，提出了基于语义一致性的

基金项目：国家自然科学基金（61825204、61932016、62132011）；北京卓越青年科学家计划项目（BJJWZYJH01201910003011）

协议栈漏洞发现与修复机制、随机协作的分组恶意转发检测机制、基于频域特征和图结构的传送连接可信机制，实现了分组数据的可靠生成、安全传输、可信应用3个不同阶段的安全闭环，增强了网络向用户提供正常、有序、可信的端到端传送服务能力，有效提高了互联网的整体安全性。

1 互联网端到端传送基本原理和关键安全问题

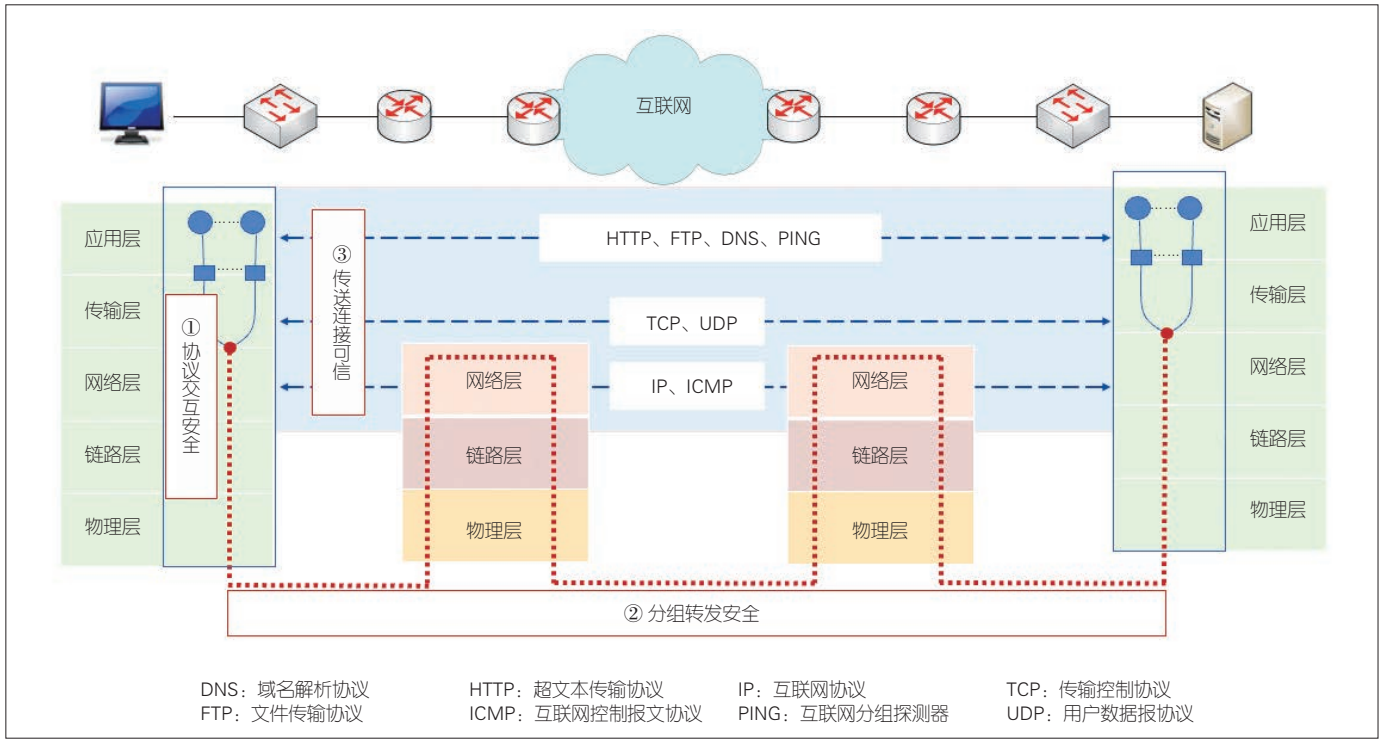
网络协议、系统及应用服务在设计和实现过程中不可避免地存在缺陷。为了增强网络的安全性，本文从互联网的工作原理出发，依据分组数据的不同生命周期，将分组数据在端到端传送过程中面临的安全威胁，归纳为以下3个方面，具体如图1所示。

（1）在分组数据生成过程中，协议栈交互安全问题引起的攻击威胁。终端协议栈承担分组数据的可靠生成和安全接收任务。协议栈安全直接关系到分组数据源的安全。我们发现经典的传输控制协议（TCP）/互联网协议（IP）的协议栈模型存在着一种隐蔽的共性缺陷模式。协议栈在跨层交互过程中会产生安全问题，这在当前被严重忽略。诸如二义性、信息泄露、语义缺失、身份欺骗等安全漏洞可被攻击者远程触发利用，对分组数据的可靠生成造成严重威胁和破坏[2-6]。

（2）在分组数据传输过程中，路由转发安全问题引起的攻击威胁。路由劫持、数据拦截和篡改、流量窃听等攻击行为会给分组数据的安全传输带来极大威胁。因此，如何保证分组数据能够按照预期的路由配置进行正常转发，使路由节点和目的节点能够验证数据包的来源并过滤恶意流量，是保证分组数据安全转发的关键[7-10]。

（3）在分组数据应用过程中，传送连接不可信问题引起的攻击威胁。随着互联网用户规模和应用复杂性的不断上升，以及新型攻击技术的不断出现，保证海量异构分组数据中没有隐蔽恶意分组的混淆嵌入，实现高精度、低延迟的恶意分组识别和检测，是实现传送连接不可信条件下分组数据可信应用的关键[11-12]。

为了提高整个网络空间的协同防御能力，有效解决分组数据生命周期中3个阶段的安全问题，本文提出了无连接网络中安全可信的端到端传送体系结构，具体包括：面向分组数据可靠生成的协议栈安全，提出基于语义一致性的终端协议栈漏洞发现与修复机制，整体上揭示并解决协议层间交互的深层安全问题，增强了协议栈的鲁棒性和安全性；面向分组数据安全传输的路由转发安全，提出通过安全边界网关协议（BGP）和真实路径验证为互联网提供数据转发真实可信保障能力，从控制平面和数据平面杜绝流量被恶意劫持、重定向或恶意丢弃；面向分组数据可信应用的传送连接安全，提出基于频域特征和图结构的恶意分组流量检测识别技术，对抗加密低速等逃逸手段，实现泛化性，适应多场景，为分



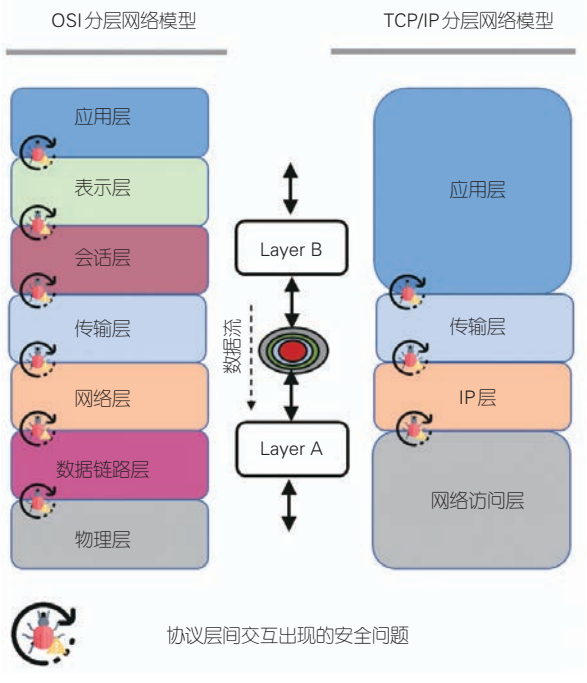
▲图1 互联网端到端传输基本原理和关键安全问题

组数据的可信应用提供保证。

通过上述3个有机协作的组成部分，本文提出的无连接网络中安全可信的端到端传送体系结构，整体上增强了互联网的安全性和鲁棒性，使分组数据具备了全生命周期的安全可信和主动防御能力，从而有效对抗多样化的攻击威胁。

2 面向分组数据可靠生成的协议栈安全

协议栈是网络空间数据生成的基础。在生成和解析分组数据过程中，不同层次间的协议需要动态跨层交互和协同。如图2所示，在这一过程中，虽然单层协议足够安全鲁棒，但将它们组合在一起进行跨层交互，则可能会出现严重的安全问题，例如协议跨层交互二义性问题、信息泄露问题、语义缺失问题、身份欺骗问题等。这些问题一旦被攻击者触发利用，将会对数据分组的可靠生成（即数据源）造成严重的破坏和威胁。当前，协议跨层交互安全问题并未引起足够的重视。本文通过对网络协议跨层交互的共享变量及资源进行特征分析，发现并形式化定义了协议在交互过程中存在的5种典型安全问题。在此基础之上，我们还提出了链式验证的防御机制，有效解决了协议层间交互安全问题，并通过热修复机制为异构平台提供统一的漏洞自动修复方法，实现了漏洞发现、防御和修复的安全闭环。



IP：互联网协议　OSI：开放系统互联　TCP：传输控制协议

▲图2 分层网络模型跨层交互安全问题

2.1 TCP/IP分层网络模型的交互式安全性分析方法

我们发现了TCP/IP协议栈模型中存在的5种典型跨层交互式安全问题，并提出了形式化的方法以便对这5种安全问题进行归纳概括，抽象出各类安全问题的共性范式。在TCP/IP网络协议栈中，我们假设层A和层B在交换数据（以层B向层A write数据为例），将这一过程简化为两个实体间的数据传递模型。这里我们揭示了5种跨层交互式漏洞范式：

（1）同步问题引起的二义性。B.write ! = A.read，即在层B对内核中某字段进行状态更新后，层A并没有完整读取到该更新。这将导致层A读取的字段值不完整或者不正确，致使层间由于状态不同步而出现安全漏洞[5]。

（2）封装不完备引起的信息泄露。A.field = f (B.key) and observable (A.field) == Ture，即层B中的关键字段key属于隐私受保护信息，不可被攻击者探测到。但层A中某个可观测字段值field的计算方法依赖于层B中的关键字段key，它可以直接由层B中的关键字段key计算获得，也可以根据层B中的关键字段key进行判断，然后筛选相应的计算方法。封装不完备将导致攻击者通过A的字段值field推理出B的关键字段key，进而导致信息泄露[2-3]。

（3）语义缺失引起的误操作。A.write = f(B.payload) && trace (B.payload) ==False，即层A将根据层B的载荷来执行写操作。但是由于层A无法对层B的载荷进行溯源，即无法验证其是否伪造或者包含错误，因此会默认层B的载荷正确合法。这导致层A会潜在地执行错误操作，形成恶意攻击[4]。

（4）输入源缺乏验证引起的身份欺骗。A.read==X.write and X!=B，即层A所读取到的字段来自X，而非来自其所期待的B。由于协议栈中层A的协议缺乏对其输入来源进行验证的安全措施，层A可能接收到伪造信息进而引发身份欺骗漏洞[6]。

（5）语义过载引起的误操作。A.read == B.write and A.$write_1$ = f_1(A.read) and A.$write_2$ = f_2(A.read)，即层A能够正常读取层B所写内容，同时层A的某个写操作$write_1$紧密依赖于从层B读取到的内容。但是，在进行其他不同的写操作$write_2$时，该操作也会依赖从层B所读取到的内容。这将可能导致层B所写的内容语义过载，进而导致内核发生误操作漏洞[2-3]。

描述每类安全问题的共性特征和漏洞规则，然后借鉴经典的程序分析方法，如污点分析、模型检验、符号执行等，能够自动化地挖掘协议栈跨层交互式安全漏洞，提高协议栈安全漏洞的分析效率和协议栈的鲁棒性。

2.2 基于轻量级链式验证的协议栈安全性增强

为了增强协议栈的安全性，我们提出了一种基于轻量级链式验证的传输层安全性增强方法。基于哈希验证的方式，该方法使TCP连接双方能够对传输层报文形成彼此可验证的共识，避免攻击者或中间人窃取和伪造类似敏感信息，从而消除网络协议栈面临的典型安全威胁。我们重新设计了传输层报文的校验和机制，采用链式哈希计算的方式，生成报文中可验证的checksum字段。每一个传输层报文校验和的计算，是根据当前报文数据和上一个报文的校验和计算获得的。这有助于形成一个完整的校验链，从而能够对抗攻击者的伪造和破坏。这种新型的传输层报文验证方式，使传统报文的校验和字段信息不再孤立，具备了链式完整性传递和验证的功能，可以有效抵御攻击者针对报文的破解、伪造等威胁，实现了协议栈安全能力的增强。

2.3 基于语义的异构平台协议栈漏洞热修复

为了有效应对不同系统和平台的异构性，提高协议栈防御方法的自动化部署能力和防御效果，我们提出并实现了一种通用的漏洞热修复机制RapidPatch[14]。该机制支持在不修改原始代码的情况下，通过实时注入扩展的伯克利数据包过滤器（eBPF）字节码实现通用的Patch。该Patch可以适配所有不同软件、硬件异构系统上相同的漏洞，在不重启系统的情况下进行动态加载并实现热修复。同时，自动验证和软件错误隔离机制可有效减少人工测试工作量，确保通过验证的Patch能在各个平台上安全地运行。

3 面向分组数据安全传输的路由转发安全

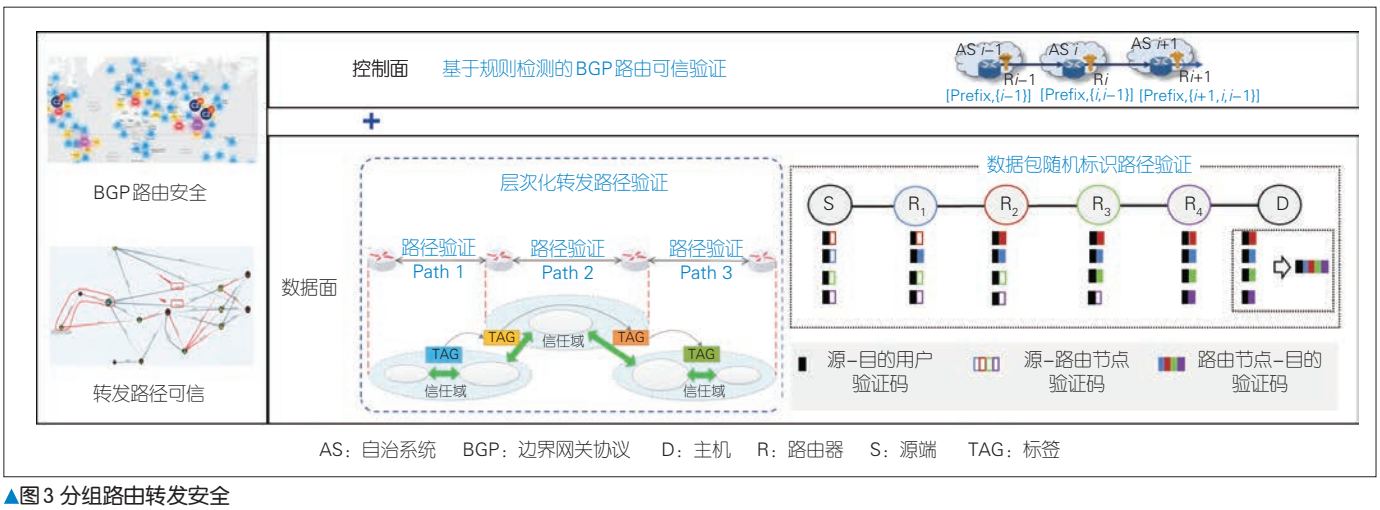
协议栈安全保证了数据分组的可靠生成，确保了数据源的真实可信。但在分组传输过程中，攻击者可能会在中间链路上进行数据拦截与篡改、流量窃听、分组恶意转发和错误路由等。如图3所示，为应对分组传输过程中的恶意攻击行为，我们从网络层控制面、数据面两个层次设计安全检测机制，实现了分组的路由转发安全[15-16]。基于规则检查的BGP路由信息验证机制能够保障控制面真实有效。同时，针对数据面域间高吞吐、高扩展性要求，我们设计了层次化的可扩展路径验证方法，实现了规模化路径验证的技术基础，保证了分组传输路径的真实可信。使用随机标识方法可进一步降低路径验证开销。为此，我们提出了更高效的基于随机标识的路径验证机制，实现了灵活可扩展、安全收益明确且可支持域间大吞吐的高效验证能力。

3.1 基于规则检测的BGP路由信息验证

BGP易产生错误配置或者受到路由攻击。由于误配置或者路由攻击，任何自治系统（AS）都可以通告自己是每一个前缀源的所有者，即实施前缀劫持攻击，或者通告一个不存在的AS路径，即伪造路径攻击。因而，目的网络会被劫持并产生路由黑洞。对此，我们提出了基于规则检测的BGP（TBGP）路由验证方案，通过在路由器上检测路由是否符合BGP路由通告的规范来验证路由，并实现了一种自动路由过滤机制。在TBGP中，如果一个BGP路由器在出口过滤器中成功验证路由通告（即符合路由验证规则），则路由器签名这个路由。邻居路由器通过在入口过滤器验证路由签名的有效性，可以确定这个路由通告是否符合BGP的路由通告规范。通过这个机制，TBGP路由器可以在每个路径中建立一个可传递的信任关系[17]。

3.2 层次化的可扩展转发路径验证机制设计

为了简化控制平面的设计，降低分组转发路径验证的复



▲图3 分组路由转发安全

杂度，实现可扩展的分段转发路径验证，我们通过在AS之间建立信任联盟，实现了层次化的可扩展分组转发路径验证机制。AS按照位置可以划分为3种角色，即主域、边界域以及非主非边界域。这里的主域是指子信任联盟的代表节点，用于同其他子信任联盟的主域建立联系。这样信任联盟之间最后形成的是树状关系，不在同一分支下的AS之间不会有直接建联的关系。边界域是位于子信任联盟边界的域。数据包从该域发出，即发往其他子信任联盟或者发出信任联盟。非主非边界域是指既不是主域也不是边界域的域。上述信任域的构建能够实现层次化的分段转发路径验证，有助于将端到端的完整路径验证拆分成分段的信任传递，达到基于层次化和分段机制的可扩展路径验证能力[7]。

3.3 基于数据包随机标识的高效真实性路径验证

在层次化的路径验证机制基础之上，我们提出了数据包标识的随机添加及验证机制，进一步实现低开销、高效率的域间转发路径验证能力[8-9]。从流的角度出发，我们提出基于数据包随机标识的高效真实性路径验证机制。该机制使源、目的节点能够有效验证数据包经过的自治域路由节点是否和预期一致。基于层次化信任，高效真实性路径验证共享各自治域路由节点之间的动态标签；使用动态标签为每个数据包生成验证码，并将其作为源、目的节点与路由节点验证数据包的标识；结合随机标识技术降低路由节点开销和网络通信开销，从而实现基于数据包随机标识的高效真实性路径验证。

4 面向分组数据可信应用的传送连接安全

在协议实现与分组转发安全可信的基础上，攻击者也可能会利用安全可信的基础设施进行攻击，发送恶意的数据包到合法流量中，危害互联网端到端通信安全，破坏应用服务的可用性。因此，传送连接不可信条件下的分组数据的可信应用是另一个关键安全需求。然而，分组数据流中恶意分组的检测与剔除目前仍存在很大的挑战。主要原因在于传统的恶意流量检测方案通常仅针对少数已知的攻击和低速网络设计，而且无法应对流量动态变化的特征，即没有考虑攻击者的逃逸行为。如图4所示，我们提出了基于频域特征的恶意流量实时检测方案和基于图结构的高效隐蔽恶意行为检测方案，两组检测方案可以分别识别短期与长期恶意数据行为。

4.1 基于频域特征的恶意流量实时检测

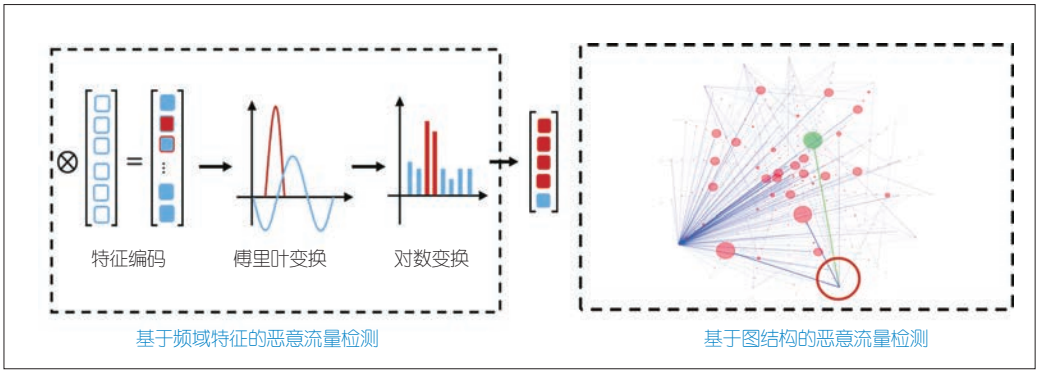
基于频域的检测方案针对短时恶意行为，解决了传统恶意流量检测系统中检测速度和鲁棒性不可兼得的难题，最终实现了在高带宽环境下对抗逃逸行为的实时鲁棒性检测。

基于频域特征的恶意流量实时检测主要包含两个模块：频域特征抽取和轻量级的机器学习。频域特征抽取模块首先对观测到的高速流量进行解析，以获取原始的细粒度逐包特征，对逐包特征进行压缩编码；随后对于编码后的特征进行频域特征抽取，并将频域变换作为特征增强方法来进一步降低特征冗余性，提升特征有效性；最后利用对数变换，防止检测过程中机器学习算法的数值出现不稳定。该方法采用轻量级无监督机器学习算法，来学习流量的频域特征向量，在检测阶段将聚类损失率大的流量标注为异常流量。通过真实世界实验证实，采用频域分析的方法能精准检测拒绝服务（DoS）、侧信道等42种典型恶意流量，并保证单核1.65 Gbit/s的吞吐量和毫秒级延迟[11]。

4.2 基于图结构的高效隐蔽恶意行为检测

基于图结构的检测方案针对长期恶意行为，解决了传统检测方案不能应对低速加密且隐蔽的恶意流量问题，最终实现了多场景通用的低速隐蔽恶意流量检测。流量交互图可有效表示网络用户的长期交互信息，能够挖掘异常的交互模式，检测出隐蔽的加密恶意流量。

在构建出流量交互图之后，我们使用四步轻量级图学习方法，利用图结构上维护的丰富历史交互信息来检测加密的恶意流量。（1）通过提取强连通分量来分析图的连通性，并通过对粗粒度统计特征进行聚类来识别图上异常的强联通分量。其中，排除正常的联通分量可显著降低图学习算法的开



▲图4 传送连接不可信条件下的恶意流量检测

销。（2）由于边特征具备局部邻接性，使用图学习算法对边进行预先聚类，可以显著降低特征处理开销，保证检测的效率。（3）使用Z3 SMT（指一种求解器）求解顶点覆盖问题，以提取关键顶点，然后逐一分析关键节点就可以分析全部的边。（4）对连接到相同的关键节点的边特征进行聚类，从正常交互模式相关的边当中区分异常的交互模式相关的边，即识别表示加密恶意流量的边。在80个场景下，该方法能高精度地检测各类异常流量，包括传统暴力洪范攻击流量、低速率探测流量、加密的洪范流量、代表性恶意软件流量。相比于传统方案，基于图结构的检测方案可以实现17.5%～31.2%的检测准确度提升[12]。

5 结束语

针对无连接网络中安全可信的端到端传送这一关键问题，我们基于互联网的工作原理，从分组数据的可靠生成、安全传输和可信应用3个阶段出发，提出了基于语义一致性的协议栈漏洞发现与修复机制、随机协作的分组恶意转发检测机制、基于频域特征和图结构的传送连接可信机制，改善了互联网现有协议实现不安全、分组转发不安全和传送连接不可信的现状，整体增强了互联网提供正常、有序服务的能力。同时，本文所提出的技术方法已在奇安信、新华三等实现产业化和规模化应用。

参考文献

[1] LIGHTFOOT L. The top 10 biggest cyber attacks of 2021 [EB/OL]. (2022-06-24) [2022-08-25]. https://expertinsights. com/insights/10-high-profile-attacks-2021/

[2] FENG X W, FU C P, LI Q, et al. Off-path TCP exploits of the mixed IPID assignment [C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2020: 1323-1335

[3] FENG X W, LI Q, SUN K, et al. Off-path TCP hijacking attacks via the side channel of downgraded IPID [J]. IEEE/ACM transactions on networking, 2022, 30(1): 409-422. DOI: 10.1109/TNET.2021.3115517

[4] FENG X W, LI Q, SUN K, et al. Off-path network traffic manipulation via revitalized ICMP redirect attacks [C]//Proceedings of the 31st USENIX Security Symposium (USENIX Security 22). USENIX, 2022: 2619-2636

[5] FENG X W, LI Q, SUN K, et al. PMTUD is not panacea: revisiting IP fragmentation attacks against TCP [C]//Proceedings 2022 Network and Distributed System Security Symposium. IEEE, 2022: 1-18. DOI: 10.14722/ndss.2022.24381

[6] FENG X W, LI Q, SUN K, et al. Man-in-the-middle attacks without rogue AP: when WPAs meet ICMP redirects [C]//Proceedings of the 2023 IEEE Symposium on Security and Privacy. IEEE, 2023: 1-16

[7] FU S T, XU K, LI Q, et al. MASK: practical source and path verification based on multi-AS-key [C]//Proceedings of 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS). IEEE, 2021: 1-10. DOI: 10.1109/IWQOS52092.2021.9521345

[8] WU B, XU K, LI Q, et al. Enabling efficient source and path verification via probabilistic packet marking [C]//Proceedings of 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS). IEEE, 2019: 1-10. DOI: 10.1109/IWQoS.2018.8624169

[9] WU B, XU K, LI Q, et al. Robust and lightweight fault localization [C]//Proceedings of 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC). IEEE, 2018: 1-8. DOI: 10.1109/PCCC.2017.8280428

[10] FU S T, LI Q, WANG X L, et al. D3: lightweight secure fault localization in edge cloud [C]//Proceedings of 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2022: 515-525. DOI: 10.1109/ICDCS54860.2022.00056

[11] FU C P, LI Q, SHEN M, et al. Realtime robust malicious traffic detection via frequency domain analysis [C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2021: 3431-3446. DOI: 10.1145/3460120.3484585

[12] FU C P, LI Q, XU K. Detecting unknown encrypted malicious traffic in real time via flow interaction graph analysis [C]//Proceedings of the 2023 Network and Distributed System Security (NDSS) Symposium. 2023: 1-18

[13] 徐恪, 李琦, 沈蒙, 等. 网络空间安全原理与实践 [M]. 北京: 清华大学出版社, 2022

[14] HE Y, ZOU Z H, SUN K, et al. RapidPatch: firmware hotpatching for real-time embedded devices [C]//Proceedings of the 31th USENIX Security Symposium (USENIX Security 22). USENIX, 2022

[15] 徐恪, 付松涛, 李琦, 等. 互联网内生安全体系结构研究进展 [J]. 计算机学报, 2021, 44(11): 2149-2172. DOI: 10.11897/SP.J.1016.2021.02149

[16] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展 [J]. 计算机学报, 2021, 44(1): 55-83. DOI: 10.11897/SP.J.1016.2021.00055

[17] LI Q, XU M W, WU J P, et al. Enhancing the trust of Internet routing with lightweight route attestation [J]. IEEE transactions on information forensics and security, 2012, 7(2): 691-703. DOI: 10.1109/tifs.2011.2177822

作 者 简 介

徐恪，清华大学教授；主要研究领域为计算机网络体系结构、网络安全和区块链系统；主持和承担重点研发项目5项，近5年发表论文100余篇，出版专著10余部，获授权中国及国际发明专利70余项。

冯学伟，清华大学在读博士生；主要研究领域为网络安全及程序分析技术。

李琦，清华大学副教授；主要研究领域为互联网与云计算安全。

朱敏，清华大学高级工程师；主要研究领域为互联网体系结构及安全。

零信任平台方案及关键技术

Zero Trust Architecture Platform Construction and Security Technology

严波/YAN Bo，王小伟/WANG Xiaowei
（深信服科技股份有限公司，中国 深圳 518055）
(Sangfor Technologies Inc, Shenzhen 518055, China)

DOI：10.12142/ZTETJ.202206005
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221209.0854.001.html
网络出版日期：2022-12-09
收稿日期：2022-10-19

摘要：零信任平台由“中心+组件+服务”三大部分构成，以平台形式充分融合软件定义边界（SDP）、身份与访问管理（IAM）、微隔离（MSG）的技术方案优势，通过关键技术的创新，实现最佳可信访问控制和安全隔离，为用户在业务层、数据层、终端层的访问达到“从不信任，始终验证”的安全效果，提升整体安全水平的同时降低了安全复杂性和运营开销。

关键词：零信任平台；SDP；IAM；MSG

Abstract: The zero-trust platform is composed of three major parts: "center + component + service", which fully integrates the technical advantages of Software Defined Perimeter (SDP), Identity and Access Management (IAM), and Micro-Segmentation Gatekeeper (MSG) as a platform. Through key technological innovation, this platform achieves the best-trusted access control and security isolation, and achieves the effect of "never trust, always verify" for user access at the business layer, data layer, and terminal layer, improving the overall security level while reducing security complexity and operating expenses.

Keywords: zero-trust platform; SDP; IAM; MSG

随着数字化进程的深入演进，网络边界已逐渐模糊，基于“外网危险、内网安全”理念构建的安全防御体系已不再适用。在网络威胁不断变化和网络攻击日益猖獗的形势下，以“零信任”为代表的白环境分析手段也逐渐出现，从而逐渐替代基于威胁特征“一刀切”的黑名单机制。

2010 年，著名研究机构 Forrester 的首席分析师 J. KINDERVAG 首次提出零信任，核心思想是“从不信任，始终验证”。此后，零信任开始得到业界关注。零信任发展至今，主流三大技术方案分别是：软件定义边界（SDP）、身份和访问管理（IAM）和基于身份的微隔离（MSG）。不同技术方案各有特点，适用于不同的业务场景需求。SDP 重点在于按需定义业务访问边界，仅为合法请求提供业务资源的访问支持；IAM 重点在于用户的身份管理与权限分配，与业务深度结合；MSG 重点在于数据中心内部东西向流量的控制[1-4]。

对于跨国、跨地区的庞大业务规模、资源类别繁多的企业，仅依靠某一个技术路线而开发的单一产品，难以应对企业发展过程中面临的不同业务挑战，如远程办公、混合云环境、数据中心数据保护等安全问题。基于上述需求，融合各技术方案特色的零信任平台应运而生。从企业环境的关键业务需求出发，结合三大技术方案的防护思路与功能，统一规划、统一建设，可以打造安全与业务融合的零信任闭环[5]。

1 零信任平台方案

零信任平台（以下简称“ZTA 平台”）是以 SDP 为核心，融合其他零信任技术产品、功能组件的方案。在零信任平台方案中，各个产品和安全组件实现灵活解耦，在充分发挥各自功能特性的同时，还实现了“统一策略”“统一管理”的平台联动机制，达到“1+1>2”的效果。组件的解耦，可实现不同业务场景下的灵活组合：一是可解决单一产品覆盖场景不全的问题；二是可以在整体规划之下，按阶段选择需要的组件，实现安全防御强需求，并同步实现建设成本可控的要求，具体如图 1 所示。

▲图 1 零信任建设阶段

基金项目：深圳市云安全关键技术研究重点实验室项目（ZDSY20200811143600002）

ZTA平台分为3个部分：零信任中心、零信任组件、服务支撑，它们分别承担不同的功能职责，彼此联动，互相支撑。ZTA平台具体如图2所示。

零信任中心部分位于ZTA平台的控制平面，是ZTA平台的核心和关键所在。该部分包括两个子中心：分析中心和控制中心。分析中心基于多源数据对访问主体的信任等级进行持续分析、评估，并将评估结果发送至控制中心，用于访问策略的选择和应用。除此之外，分析中心还肩负实时风险展示、权限梳理、应用识别、办公安全行为可视等多种职责。控制中心是根据分析中心的评估结果，动态匹配访问控制策略，并将策略下发至数据平面的执行组件。

零信任组件部分位于ZTA平台的数据平面（或业务平面）。作为访问控制策略的执行点，该组件主要与控制平台联动，兼顾情报点、自身安全防护等职能。执行点主要负责访问策略的执行，即控制中心对具体的访问请求进行分析评估，并下发选定的执行策略，并负责执行[6]。在平台化中，执行类设备被称为网关，所有业务流量均由网关设备转发；情报点主要用于访问请求中的信息收集、分析和传输，包括认证登录、业务访问行为信息等。该类信任一方面用于优化使用体验，另一方面则为分析中心提供数据分析的来源[7]。

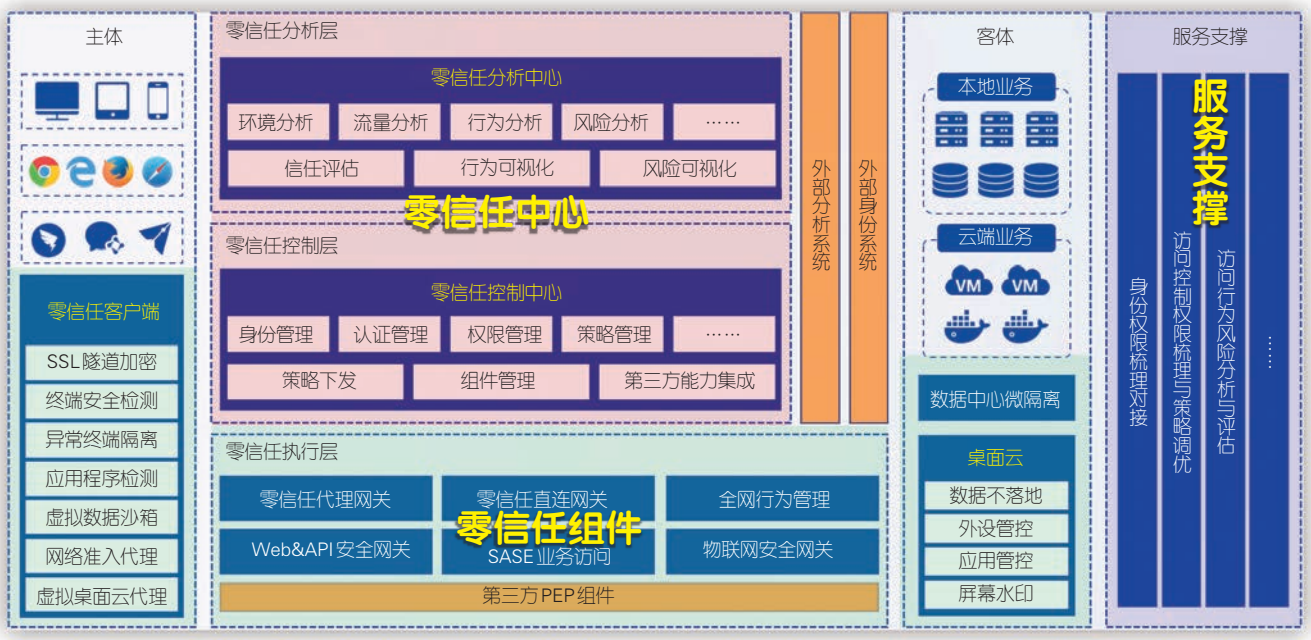
服务支撑部分是ZTA平台持续迭代、安全防御能力优化、业务保障的重要组成部分。通过交付阶段的业务梳理，服务支撑部分完成基础能力的建设，并进行动态策略调整，在业务运行平稳后，逐步扩大零信任的覆盖和使用范围，最终达成业务的全部迁移；在运营阶段，通过安全运营，持续完善业务白名单，建立、优化访问控制关系和策略调整，确保业务访问的合规化、合理化，达到安全自适应的闭环。

2 功能组成

2.1 零信任控制中心

零信任控制中心在ZTA平台中占具核心地位，与信任分析中心、零信任组件进行控制联动，提供的管理功能包括：身份管理、认证管理、权限管理、策略管理、策略下发、组件管理、第三方能力集成等。本文中，我们主要介绍身份认证管理、应用管理、策略管理三大内容。

身份认证管理主要通过与统一身份管理平台对接或由控制器自身提供认证服务，实现身份的认证和权限管理。身份认证的对象包括用户（人）、终端、设备、程序等。控制中心根据用户登录信息、终端环境信息等内容动态调整访问策略，例如，用户首次使用账户信息登录或在非常用地区登录时可能触发增强认证，即触发多因子认证，保障接入安全；在终端已被设置为授信终端或登录环境安全时，进行认证豁



API：应用程序编程接口　PEP：策略执行点　SASE：安全访问服务边缘　SSL：安全套接层

▲图2 零信任平台

免，免除二次认证过程或实现离线客户端一键上线，以提升用户的使用体验[8]。

应用管理部分主要围绕业务系统的访问需求，确定合适的安全发布机制和访问模式。例如，当用户的访问环境为内网时，应用管理触发直连网关（DGW）的访问模式；当用户的访问环境为互联网时，自动调整为SDP代理网关访问模式。

策略管理部分主要为不同环境下的访问需求，能够提供多类型的动态控制策略，常见的包括：安全策略、客户端接入策略等。动态策略选定主要来源于零信任分析中心，控制中心通过与分析中心联动，完成风险分析和持续信任评估，最终确定并生成动态的访问控制策略，下发给安全组件后完成执行。

为了更清晰地展现以上原理，我们以图3为例进行说明。由“客户端及用户”侧向“业务系统”发起业务访问，会经历以下几个阶段：首先客户端及用户需要与零信任控制中心完成身份验证，身份验证可以由控制器自身或统一身份管理平台来实现；认证成功后，控制中心检查与之相匹配的策略和该用户所具备的业务资源列表，判定满足访问条件后，下发放通或拒绝的策略到网关设备节点，网关设备来完成该策略执行。在以上过程中，控制中心还会持续接收来自分析中心的分析结果，辅助策略决策。

2.2 零信任分析中心

零信任分析中心主要为控制中心提供决策依据输入，并基于用户访问行为或访问环境等信息进行综合风险分析。例如，用户的客户端登录源IP地址在授信IP地址范围内时，在提供正确的身份信息后，即可访问业务系统；当源IP地址在非授信IP地址范围内时，即使提供了正确的身份信息，也可下发策略阻止本次访问。分析中心可以周期性检测客户端的源IP地址的变化情况，并将分析结果及时传递给控制器，以供决策参考。

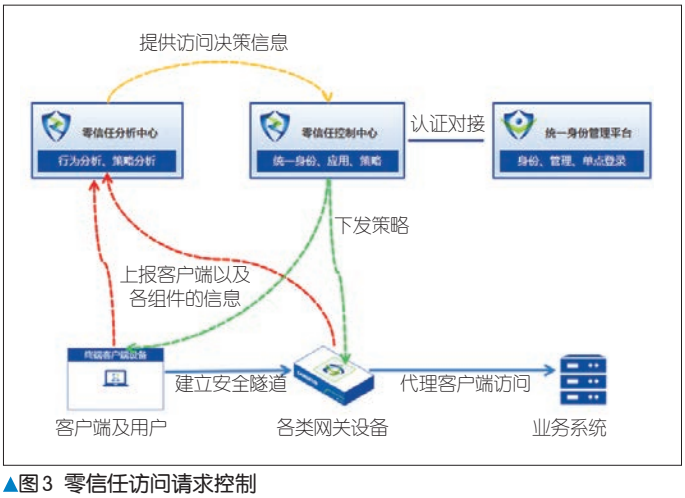
分析中心的情报数据采用的是多源并行的方式，不仅汇集客户端的数据信息，还可汇集其他安全组件或日志分析平台的数据，例如：终端安全环境检测的风险分析数据、用户认证和访问流量的风险分析数据，以及第三方策略信息点（PIP）分析中心分析数据。零信任分析中心对多源输入的情报信息进行统一聚合处理，控制中心将参考分析中心的具体分析结果做出访问决策，并匹配、下发具体的访问控制策略，如图4所示。

2.3 零信任组件

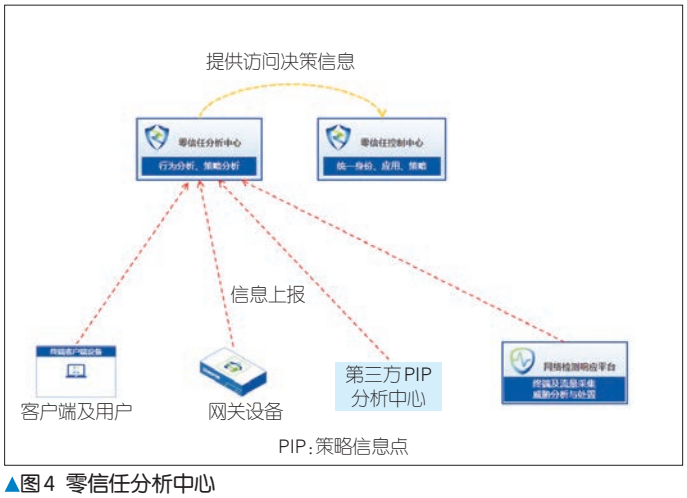
零信任组件主要指各类场景下负责策略执行处的安全管控组件，例如：SDP代理网关、DGW、安全访问服务边缘（SASE）类网关、物联网安全网关等。根据实际的业务场景和安全需求设置不同的安全组件，远程接入办公可选择SDP代理网关，内网办公场景可以选择DGW，物联网可选择物联网安全网关，互联网云上业务访问场景使用安全访问服务边缘–专用访问（SASE–PA）。

在ZTA平台中，常见的网关分为三大类：SDP代理网关、DGW、SASE–PA网关。

SDP代理网关适用于互联网接入和远程办公场景，如图5所示。SDP采用的是代理转发模式，即与终端建立连接，再与业务系统建立连接。SDP代理网关工作在“内外”网的逻辑边界处，业务系统隐藏在SDP代理网关之后。这样能够实现暴露面的收缩（仅剩余SDP代理网关本身对外暴露），而SDP代理网关的安全可通过其他的安全措施加以防护，例如单包授权（SPA）技术。



▲图3 零信任访问请求控制



▲图4 零信任分析中心

DGW适用于内网办公场景，因业务访问由内部网络承载，所以又被称为直连网关，如图6所示。DGW采用防火墙架构设计，用于放通/禁止内网客户端对于业务的访问。对于客户端发起的访问，DGW仍然会对客户端做应用级的校验，校验通过后才会放通本次访问请求。

SASE-PA网关适用于跨地区分支需要访问总部业务的办公场景，如图7所示。该模式是将网关组件以云化的方式部署在云端，通过终端客户端与SASE-PA网关建立加密隧道，实现业务数据引流。当客户端发起业务访问请求，流量会被“抓”取并放入隧道，通过云上SASE-PA网关实现代理访问。同时，客户端的非业务流量会自动过滤分流。相比于传统的SDWAN组网，SASE-PA网关模式极大地实现了企业跨地区灵活组网、高性价的安全业务访问需求。

以上3类网关各具特点。对于SDP代理网关模式，当网关出现故障时，通常需要通过修改域名或者映射配置来恢复业务访问；对于DGW模式，在网关故障发生时，可以通过透明模式部署来实现业务访问的快速逃生；相比于SDP代理网关与DGW，SASE-PA网关模式天生具备易部署、易扩展、访问健壮的特点，主要应用于云托管场景。

2.4 ZTA平台落地与服务支撑

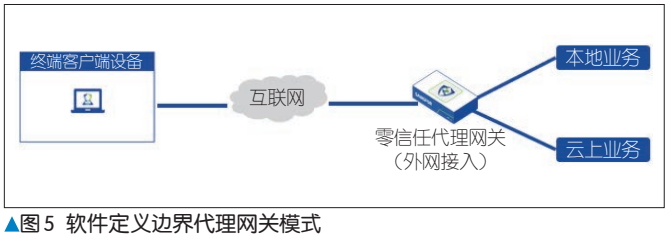
传统的网络安全防御体系与被保护的业务系统属于分割、松耦合关系，在计算环境、网络边界、传输网络中以设定“黑名单”为主的安全策略。ZTA平台作为一种全新的安全架构，与业务需求、安全能力动态持续融合，增强“白环境”检测逻辑，以场景化、阶段化的方式，逐步构建完整的业务安全防御体系，所以ZTA平台方案落地可分为三大阶段，分步实施。

第1阶段，优先实现通过互联网或广域网（类似政务外网等专网）进行远程接入访问的业务场景部分，通过零信任架构，收缩业务对外的暴露面。

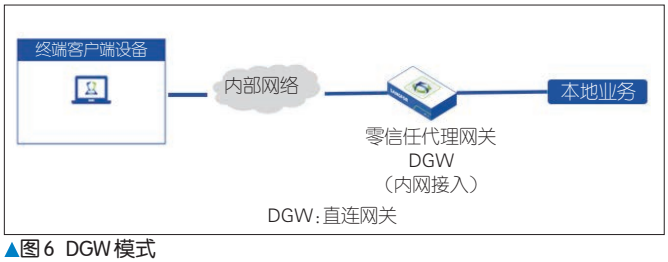
第2阶段，优先考虑内网访问和分支机构接入访问的业务场景部分，可将传统网络安全升级为零信任架构体系，实现内外网统一、无差别的安全访问办公体验。

第3阶段，深入组织数据中心内部访问场景，主要解决数据中心主机、虚拟机、容器、服务之间相互访问调用的安全访问控制逻辑。

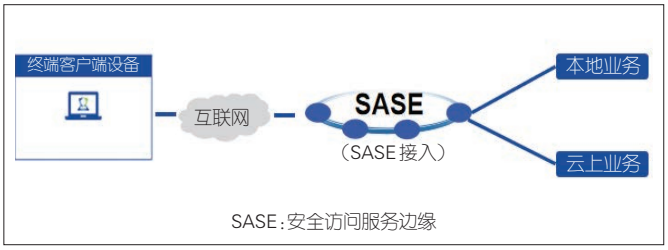
在平台的运营阶段，还需专业团队以安全运营服务的方式，持续提升企业的“白”化能力。通过可视化报表和自动化技术的辅助，主动挖掘和发现未知风险，实现动态、自进化式的安全策略调整。



▲图5 软件定义边界代理网关模式



▲图6 DGW模式



▲图7 SASE-PA网关模式

3 关键技术

ZTA平台是通过在多个层面，以多种安全控制技术，实现以下的一些安全目标：正确的人利用可信的终端，通过安全的通道，使用适当的权限，访问重要的业务，从而保护敏感的数据。

3.1 第3代SPA技术

零信任核心能力之一是实现基于身份的安全访问控制。这需要两个必要条件：一是实现流量身份化；二是在通过身份认证之前，要充分缩小业务的暴露面，做到先认证后访问。

在传统的远程办公场景中，客户端需要先与业务系统建立连接，再进行用户身份认证，认证通过后即可获取相应的业务资源列表。先连接的前提条件是业务端口保持开放，但这种开放先天就存在被攻击的风险，例如：端口扫描、分布式拒绝服务攻击（DDOS）等。

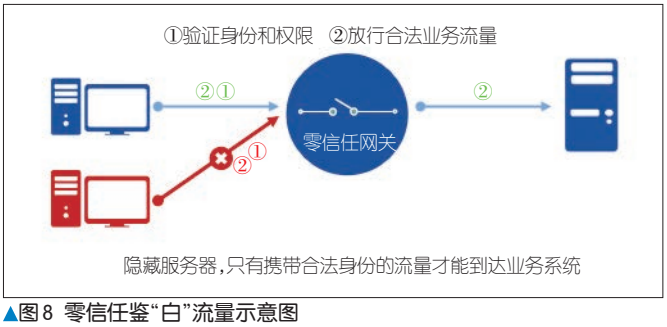
在ZTA平台中，客户端在正式发起连接前，需要完成身份验证，验证通过后才能进行正式连接，同时实现对设备自身的安全防护。未通过身份验证的客户端，无法得知业务端口，更无法与之建立连接。整个过程包括两个阶段：第1个阶段，通过控制平面的身份校验后，控制平台通过策略配置，打开业务连接端口；第2个阶段，客户端与打开的端

口，在数据平面建立业务连接，实现业务访问。零信任鉴“白”流量示意如图8所示。

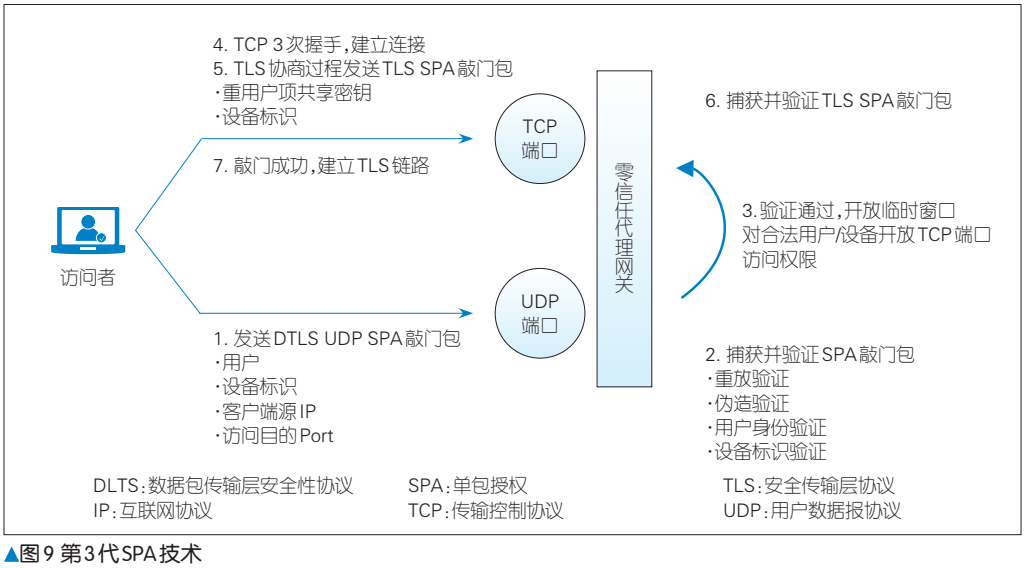
在互联网访问的具体场景中，SDP代理网关通过第3代SPA技术和隧道技术，实现暴露面隐藏和流量身份化。由于安全网关采用代理的方式替代了客户端进行业务访问，所以在隧道头部中以插入字段的方式，传递身份验证所需内容。

零信任系统默认隐藏所有服务端口，仅开放所需的用户数据报协议（UDP）端口。在正常用户访问前，客户端发送含有身份凭证的UDP SPA“敲门”包，验证通过后会临时打开一个时间窗口，且仅允许指定源IP地方访问的443端口（即TCP SPA敲门端口）。后续的传输控制协议（TCP）连接过程遵循第2代TCP SPA流程，在安全传输层协议（TLS）协商过程中完成TCP敲门，具体如图9所示。

由于非代理模式下不能修改数据包内容，所以DGW访问场景无法直接使用SDP来实现业务端口隐藏。该场景以使用前置验证包的方式来实现应用级鉴权。客户端在每一次发起会话连接时，需要先通过一个前置验证包来完成验证，验证通过后才能建立会话；验证失败，则会拒绝建立会话。



▲图8 零信任鉴“白”流量示意图



▲图9 第3代SPA技术

3.2 新一代沙箱技术

在零信任方案中，数据安全也需要重点考虑。实现数据安全保护的技术主要包括：桌面云（VDI）、虚拟浏览器（SBC）、沙箱（SandBox）。桌面云和虚拟浏览器技术能实现数据云端存储，可见、可用，但不可得；沙箱技术能实现数据落地，但不泄密。

沙箱技术是通过在终端上创建与当前终端环境逻辑隔离的安全工作空间，来实现数据隔离保护。该技术通常是以插件的形态来实现轻量化、简洁化的应用。沙箱技术使用驱动层的文件透明加解密技术，在文件系统添加一个加解密过滤层。所有软件的磁盘写入操作最终都会经过这个加解密模块，再进入磁盘。加解密模块会对写入操作的进程进行判断，属于工作空间的进程则写加密、读解密，属于终端空间的进程读写均不做额外操作。沙箱技术在应对勒索病毒方面也具有一定优势。勒索病毒主要是通过磁盘文件遍历的方式来获取对应格式的文件并实行加密。写入沙箱文件系统的文件被隔离保护，在个人桌面无法搜索找到对应文件，也就无法实现对其加密勒索。与此同时，沙箱技术还可以实现对数据导入和传出的控制，避免数据失控、外泄。

3.3 动态访问控制列表（ACL）技术

传统网络安全的ACL策略是静态制定、规则匹配的模式，无法实现动态、细粒度、差异化管控，无法实现主动防御和响应。ZTA平台中以动态ACL技术来评估终端接入的风险，从而实现动态策略控制。

零信任的策略引擎主流模式有两种：一种是信任评分机制，一种是规则机制。

信任评分机制又分为配置评分和智能评分两种模式。配置评分模式是管理员为不同安全缺陷情况预设分值，并对整体评估结果设定一个“及格线”分值；智能评分则是通过平台引擎进行统计、学习从而完成判断和赋值，整个过程无须人员参与，所以智能评分机制的弊端是如何设定合理的“及格线”。

规则机制是通过在不同的板面上分别设定安全策略基线，以“短板”效应的方式，达到设定目标。相比于

信任评分机制，规则机制更有利于保障安全的底线和原则，不会单方面通过得分情况做出策略判断。

在ZTA平台方案中，我们采用规则+评分的混合模式，以规则机制为主，评分机制为辅，共同完成安全分析判定。ZTA平台的理念是："安全有原则，管理有灰度，信任有智慧"。"安全有原则"是指策略引擎以规则为主；"管理有灰度"是指在动态ACL规则方面可配置二次认证或告警，或提供过渡期整改再处置，以保证业务优先，而非"一刀切"的统一策略；"信任有智慧"是指在规则基础上引入智能评分机制，辅助决策。

ZTA平台中的动态ACL涵盖时间、位置、可信应用程序等多种维度，可根据实际场景需求进行细粒度设置。在智能评分模式下，零信任中心联动终端安全设备，实现客户端的环境评估赋值，辅助决策；在规则模式下，通过对发起访问请求的终端程序进程的使用情况、签名信息等内容进行安全评估，与预置的可信进程和不可信进程标签进行动态匹配，以支撑不同策略的差异化选择。

3.4 三层转四层隧道技术

隧道技术是在传输层面实现安全控制，主要包括3个关键内容：引流、传输和代理。引流是精准"抓"取业务访问流量，传输是指以加密后传输给隧道代理网关，代理是由网关代理客户端完成业务访问。

传统的三层引流技术主要是通过虚拟网卡和路由完成引流，兼容性较好。其原理是通过在终端本地安装虚拟网卡，并下发路由的方式，实现引流进入隧道，同时通过虚拟域名系统（DNS）配合，实现域名资源的访问。由于工作在三层，也被称为是三层隧道。当客户端存在多个客户端/服务端模式（C/S）的应用程序时，会通过一条传输控制协议（TCP）长连接与代理网关实现数据交互。长连接的传输受网络波动、切换的影响较大，用户感知明显。

三层转四层技术是在三层虚拟网卡处，通过IP路由表引流获取到终端的请求流量，之后以轻量级IP协议栈转换成四层数据包，再将数据包通过客户端私有隧道代理的方式发送至网关。这种模式使用TCP的短连接，客户端与代理网关之间会为每个隧道均建立一个TCP短连接。当数据传输完成后，立即释放该短连接资源。由于短连接对应用层（四层以上）流量不做改写，在数据包被加密封装的payload部分长度要比长连接更短，因此在大文件传输和下载场景中，传输效率高于长连接方式。

4 结束语

零信任是内生安全模型的代表之一，以强调业务"白"化能力的方式，与被保护的业务深度融合。依托零信任平台方案和可行技术的应用，零信任构建了安全与生产力的平衡发展态势，优先保障业务可用性，并以系统化思维全面提升业务自身的安全免疫力，为数字化、智能化社会的安全建设指明了方向，奠定了的"可信"基石。零信任架构旨在加强安全性以保护企业资产的系统和操作设计指南，它本身并不是一个单一的架构。零信任平台通过融合软件定义边界、身份与访问管理、微隔离的技术优势，为企业提供业务与安全同行的网络环境，是保障企业数字化良好发展的重要路径。

致谢

本文的撰写得到深信服科技股份有限公司游建舟、王琦然的帮助，在此表示感谢。

参考文献

[1] 潘吴斌, 任国强. 软件定义边界SDP: 概念、技术及应用研究综述 [J]. 数字通信世界, 2021, (3): 192-195. DOI: 10.3969/J.ISSN.1672-7274.2021.03.084
[2] 田由辉. 基于零信任架构的网络安全防护思路 [J]. 信息技术与信息化, 2020(5): 154-157. DOI: 10.3969/j.issn.1672-9528.2020.05.048
[3] 魏小强. 基于零信任的远程办公系统安全模型研究与实现 [J]. 信息安全研究, 2020, 6(4): 289-295. DOI: 10.3969/j.issn.2096-1057.2020.04.002
[4] 朱良海, 张义超, 袁震. 构建基于SDP技术的网络安全体系 [J]. 网络安全和信息化, 2019, (12): 109-112
[5] 王刚, 张英涛, 杨正权. 基于零信任打造封闭访问空间 [J]. 信息安全与通信保密, 2020, 18(8): 78-86
[6] 江伟玉,刘冰洋, 王闯. 内生安全网络架构 [J]. 电信科学, 2019(9). 20-28
[7] 訾然, 刘嘉. 基于精益信任的风险信任体系构建研究 [J]. 信息网络安全, 2019, (10): 32-41. DOI: 10.3969/j.issn.1671-1122.2019.10.005
[8] 王琦然, 王金红, 卢艺, 等. 零信任助力数字化办公安全高效: 深信服零信任安全解决方案 [C]//2021年国家网络安全宣传周"网络安全产业发展论坛"论文集. 西安, 2021: 189-192

作 者 简 介

严波，深信服科技股份有限公司产业教育中心教学教研部主任、安全服务认证专家、网络安全等级保护体系专家、网络安全高级咨询顾问；长期从事零信任、云安全、数据安全方向的技术研究工作；曾参与多项国家标准的研究和编写工作。

王小伟，深信服科技股份有限公司产业教育中心教学教研部资深讲师、深信服安全技术认证专家；长期从事零信任、云安全方向的技术研究工作；曾多次主导及参与媒体、能源、金融等行业数据中心网络安全实战项目的规划、交付和研究工作。

基于内生安全框架的面向数字化转型的网络安全防御体系

A Network Security Defense System for Digital Transformation Based on Intrinsic Security Framework

韩永刚/HAN Yonggang
（奇安信科技集团股份有限公司，中国 北京 100044）
(QI-ANXIN Technology Group Inc. , Beijing 100044, China)

DOI：10.12142/ZTETJ.202206006
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221219.1325.002.html
网络出版日期：2022-12-20
收稿日期：2022-10-10

摘要：提出了网络空间安全领域的一种新安全体系设计、建设与运营思路方法。所阐述的内生安全，指通过内生安全框架方法，将网络安全能力与数字化环境进行融合内生，达到安全与信息化的深度融合与全面覆盖。以系统工程与企业架构的方法，结合内生安全理念，从体系化、全局化的视角，以能力为导向，可以构建动态综合的新型网络安全防御体系。

关键词：内生安全；系统工程；企业架构；网络安全能力

Abstract: A new method of design, construction, and operation of security systems in the field of cybersecurity is proposed. Through the intrinsic security framework, the cybersecurity capabilities and the digital environment are integrated, to achieve deep integration and comprehensive coverage with information technology. With the method of system engineering and enterprise architecture, combined with the endogenous security concept, and from a systematic and global perspective, a new dynamic and comprehensive network security defense system can be built.

Keywords: intrinsic security; system engineering; enterprise architecture; cybersecurity capability

1 数字化时代的网络安全体系需求演进

全球经济已全面进入数字化时代，中国在“十四五”规划中也明确提出了“加快数字化发展，建设数字中国”的战略规划。近年来，“网络强国”“加快培育数据要素市场”“加强数字政府建设”等一系列与数字化转型紧密相关的战略部署，都将数字化转型作为重要的发展战略与核心经济驱动力。数字化的核心不仅在于云计算、大数据、5G、物联网、人工智能、智能制造、卫星互联网这些新技术的应用，更在于将信息技术与政企机构业务运营、管理流程融合在一起，形成新的业务运营模式，从而显著提升业务运营效率和效益，为政企机构带来巨大的创新红利。与此同时，信息技术与业务的深度融合也将增加网络安全方面的风险，使得网络安全问题对业务产生破坏性乃至灾难性的影响。在这种情况下，网络安全风险将会等效于业务运营风险。政企机构信息系统一旦被入侵或被破坏，将会直接危害业务运营，进而危害生产安全、社会安全，甚至国家安全。这也是国家在数字化转型期从战略与法律法规角度，频繁推出《网络安全法》《数据安全法》《个人信息保护法》《网络安全等级保护制度》等一系列法律、法规、制度、标准的原因。

近年来，随着数字化环境的变化，网络空间威胁也发生了新的变化：各类新型的威胁如勒索攻击、大规模数据泄漏、供应链攻击、高级威胁高级持续性威胁（APT）攻击、内部威胁、国家网络空间对抗等相继出现，并带来了一系列影响。数字化转型对政企机构运营模式的转变是颠覆性的、不可逆转的，传统的信息化模式也将无法支撑目前经济环境下的业务运行要求。因此，政企机构必须立足于数字化业务运营的安全、高效、可靠运行，建设具有动态、综合、可持续等特点的适应于数字化业务的新型网络安全保障体系。

2 内生安全的理念

“内生安全”是指面向数字化业务，将网络安全能力内置到数字化环境中，并通过信息化系统和安全系统的聚合、业务数据和安全数据的聚合、IT人才和安全人才的聚合，让网络安全系统像人的免疫系统一样，实现自适应、自主和自成长，从体系化全局视角构建出动态综合的网络安全防御体系[1]。

从内生安全理念的产生到框架设计方法的形成与落地，相关实践指引了中国大量的大型政企机构的网络安全体系设计、建设、运行。这些实践与系统工程及企业架构（EA）方法论的结合与应用，起了关键作用。

系统工程产生于20世纪50年代，被广泛地用于航空、航天、机械制造、电子工程等各个领域，并由钱学森院士在中国积极倡导并开拓创新。系统工程是看待复杂系统（SoS）时的一种逻辑思维方法，是组织、管理“系统”规划、研究、设计、制造、试验和使用的科学方法[2]。系统工程专注于复杂系统的整体设计，从问题的全局视角来审视，为系统整体而非单一子系统设计方案，将所有变量都考虑在内，并梳理其相互关系。从系统化的视角来看，系统作为整体所产生的价值主要来自各组成部分的相互联系和相互作用关系，而且远远超过各组成部分的单独贡献的和[3]，这也就是所谓系统工程的“涌现”效果。

如果将日益复杂的数字化环境也视为一个复杂系统，那么EA就是系统工程在信息化领域的应用。在过去的20～30年，EA方法论在引导与推动大规模、体系化、高效整合的信息化建设、支撑各行各业科学地展开业务运营等方面都起到至关重要的作用，而内生安全框架亦有很多思路来源于EA方法论。通过创建、沟通、提高等方法，EA可以描述企业未来状态和发展的关键原则，进而把商业远景和战略转化成有效的企业变革。EA方法主要用于维护信息技术（IT）体系，或引入新的信息技术体系，从而实现组织的战略目标和信息资源管理目标。

1987年，J. ZACHMAN在《A Framework for Information Systems Architecture》中首次提出了“信息系统架构框架”的概念，从“信息、流程、网络、人员、时间、基本原理”6个视角来分析信息系统架构，由此奠定了EA的理论基础[4]。美国的一些机构率先使用EA：美国国家技术标准研究所（NIST）于1989年发布企业架构模型（NIST EA Model），于1999年发布联邦企业架构框架（FEAF），于2003年发布国防部体系架构框架（DoDAF）。同时，在企业机构和一些标准化组织中，也涌现出一些具有影响力的框架，例如开放标准组织体系结构框架（TOGAF）。

EA是企业业务战略与IT战略之间的接口，是企业顶层设计的图纸，决定企业结构、组成部分、各部功能、空间关系等元素。一般来说，EA可以分为两大部分：业务架构和IT架构。目前大部分EA方法都是从IT架构发展而来的。业务架构是把企业的业务战略转化为日常运作的渠道。业务战略决定业务架构，它包括业务的运营模式、流程体系、组织结构、地域分布等内容。而IT架构，是指导IT投资和设计决策的IT框架，是建立企业信息系统的综合蓝图，包括数据架构、应用架构和技术架构3部分。其中，业务架构的重点是流程和数据，而IT架构的重点是应用和技术。前者增加了企业愿景和任务目标驱动，后者增加了可落地的实施策略和计划。

作为系统工程思想在信息化领域的应用，EA方法打破了零散式的规划与建设，系统性地构建信息化体系，从而推动了大规模、体系化、高效整合的信息化建设。在很长一段时间里，网络安全在方法论上都缺乏这种体系化与全局视角。我们要做的就是从EA的方法体系与各种框架中，找到适合中国网络安全状况的方法，并结合具体国情，加以开发与利用，并结合内生安全理念，形成适用于网络安全的框架、方法与配套工具等。

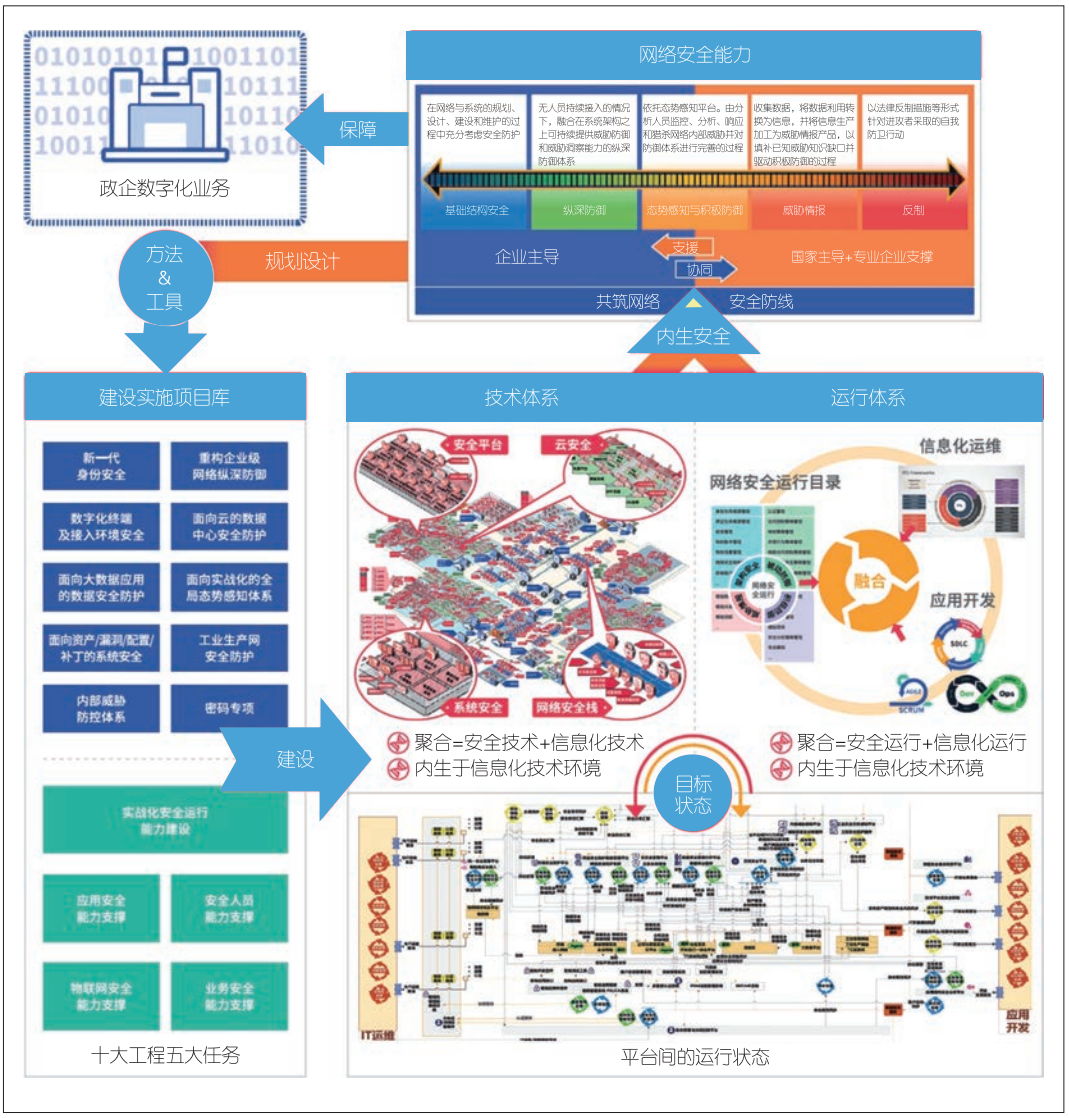
在网络空间安全领域对EA方法论的使用，是为了帮助政企大型机构理清并实现所需的“网络安全能力体系”，而不是为了建设某种具体的系统或产品。我们需要从全局视角了解大型政企机构所需的网络安全能力体系是什么？包含什么？应该如何有序地构建，并真正运行起来。我们要做的是进行合理恰当的选取与应用，从全局视角以系统性的方法进行整体的设计、建设与运行。我们应当综合考虑业务现状与信息化环境的未来发展，规划设计与之相匹配的网络安全能力体系，并像信息化的建设一样，将网络安全的能力与数字化融合内生，做到与信息化环境全面覆盖以及深度融合，从而保障政企核心业务的顺畅运行。

根据政企机构信息化与网络安全建设的实践经验，我们总结了一套适合于中国政企机构，特别是大中型政企机构信息化发展的、系统性的网络安全建设框架。新框架即是对网络安全模式升级新方法的探索，也是“内生安全”理念的有效落地。

3 内生安全框架与体系设计方法

借鉴EA方法论，以“网络安全能力体系”建设为中心，内生安全框架可以识别出在信息化的各个层面构成网络安全能力的能力组件，并将这些安全能力组件全面覆盖至政企普遍存在的信息化各领域，进而规划出网络安全建设实施“项目纲要库”（需要逐步实施的项目的集合）。随着这些项目的实施，安全防护体系将逐步融入信息化环境，进而共同实现全面的安全能力。最终，安全技术体系与安全运行体系的建立完善，可以实现“内生安全”的全面落地，并使政企机构能够具备体系化的安全防御能力。

内生安全框架（具体如图1所示）涉及的安全能力应全面覆盖云、终端、服务器、通信链路、网络设备、工控、人



▲图1 内生安全框架[1]

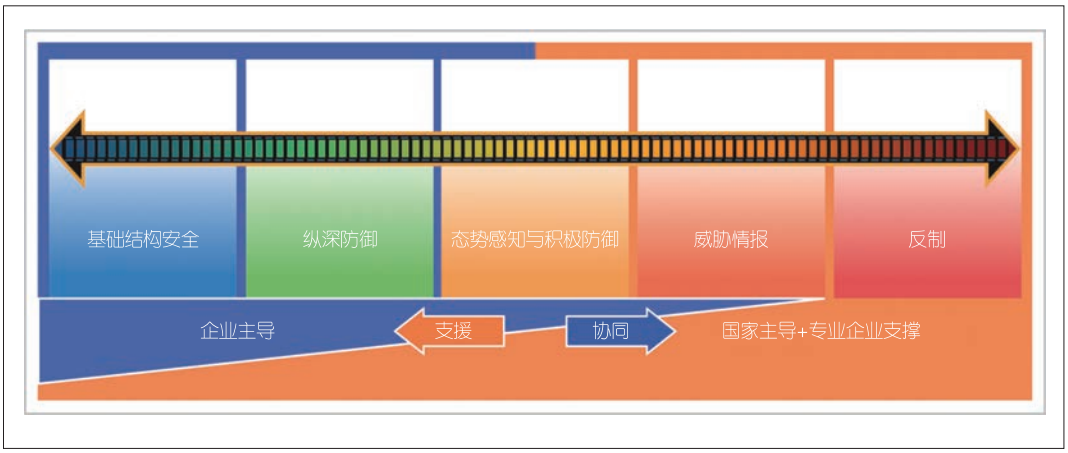
员等IT要素，避免因局部盲区而导致的防御体系失效；还需要将安全能力深度融入物理、网络、系统、应用、数据与用户等各个层次，确保安全能力能在IT的各层次有效集成。

内生安全框架为大型政企机构在数字化转型的快速发展期开展整体的网络安全规划与体系设计提供了思路与建议。我们通过该框架，从“甲方视角、信息化视角、网络安全顶层视角”展现出政企网络安全体系全景，通过以能力为导向的网络安全体系设计方法，规划出面向中长期的建设实施项目纲要库（即重点工程与任务，其进一步的扩展与细化可以形成网络安全相关重点领域的参考架构），并设计出将网络安全与信息化相融合的目标技术体系和目标运行体系，供政企机构参考、借鉴。

通过“叠加演进的能力分类方法”，内生安全框架形成面向政企信息化全领域的网络安全能力体系。政企可结合自身情况，采用框架中包含的方法工具，对每个安全领域的安全能力进行组合，重点设计能力间的逻辑关系以形成能力逻辑架构，并规划出覆盖网络安全全领域的建设实施项目库。在规划周期内，项目库中的工程和任务依据路线图确定的时间开展研究、立项、建设。随着项目和任务的落地，政企将逐步建成目标技术体系架构与目标运行体系架构。体系化的网络安全能力也会随之达成，从而保障了数字化业务。

网络安全能力体系是保障政企机构数字化业务运营所必须的网络安全能力的集合。只有政企机构具备了这些必须的安全能力，才能真正有效地保障数字化业务安全。在框架的组成中，网络安全能力体系通过结合全球安全领域的规范标准、最佳实践、新安全技术，枚举出了保障政企机构数字化业务安全运行所需的能力集合。借鉴国际网络安全研究机构（SANS）提出的网络安全“滑动标尺”模型[5]，我们对安全能力进行分类，并结合中国政企机构信息化普遍存在的安全领域，规划、设计并形成了适合具有中国特色的“叠加演进”的网络安全能力体系。

如图2所示，网络安全能力体系包含五大类，即基础结构安全（Architecture）、纵深防御（Defense in Depth）、态势感知与积极防御（Active Defense）、威胁情报（Intelligence）和反制（Counter）。其中，基础结构安全、纵深防御、积极防御、威胁情报这4类能力是一个完备的政企业级网络空间安全防御体系所需的，而反制能力主要由国家级网络安全防御体系来提供。



▲图2 叠加演进的网络安全能力模式

• 基础结构安全：在系统规划、建设和维护的过程中，我们应该充分考虑安全要素，确保这些安全要素被设计到系统中，从而构建一个安全要素齐全的基础架构。

• 纵深防御：该能力体系是建立在架构安全基础上的，并能在多道网络防线上提供持续的威胁防御或威胁洞察力。该能力就像是给整个机构构建了战场防御的“纵深”，并在阵地的不同层次、不同区域上进行不同技术类型的层层设防，并保证其防御策略行之有效。

• 积极防御：在该能力体系中，主动防御、数据分析被充分利用，分析人员开始介入，形成人机互动，并对网络内的威胁进行监控、响应、学习和理解。积极防御把攻防过程从看似离散的告警，进化成一个有时空关联的完整过程；把攻击发生时的瞬间防御，变成了日常的监测、分析和学习的过程；把对单次攻击本身的检测，延伸到对攻击者和攻击者持续行为的关注。

• 威胁情报：该阶段的主要任务是收集和分析内部数据，并使用外部第三方威胁情报数据。更多来源的威胁情报的利用，能够使防御体系有更广泛的视角。这样能够综合了解行业、区域，甚至全球的网络攻击的现状、方法与相关攻击指标（IOC），从而通过可机读情报的处理过程来大大提升防御系统的告警准确性与效率。

• 反制：该能力指在友好网络之外，对攻击者采取直接的压制或打击行动。不过，按照中国网络安全法律、法规的要求，对于一般的政企机构来说，在进攻反制阶段所能做的，主要是通过法律手段对攻击者进行反击或借助国家力量进行网络安全监管。

从叠加演进的视角来看，网络安全防御能力体系中的基础结构安全与纵深防御能力具有与信息基础设施“深度结合、全面覆盖”的综合防御特点，而积极防御与威胁情报能力具有“掌握敌情、协同响应”的动态防御特点。这些能力间彼此关联、相互促进。

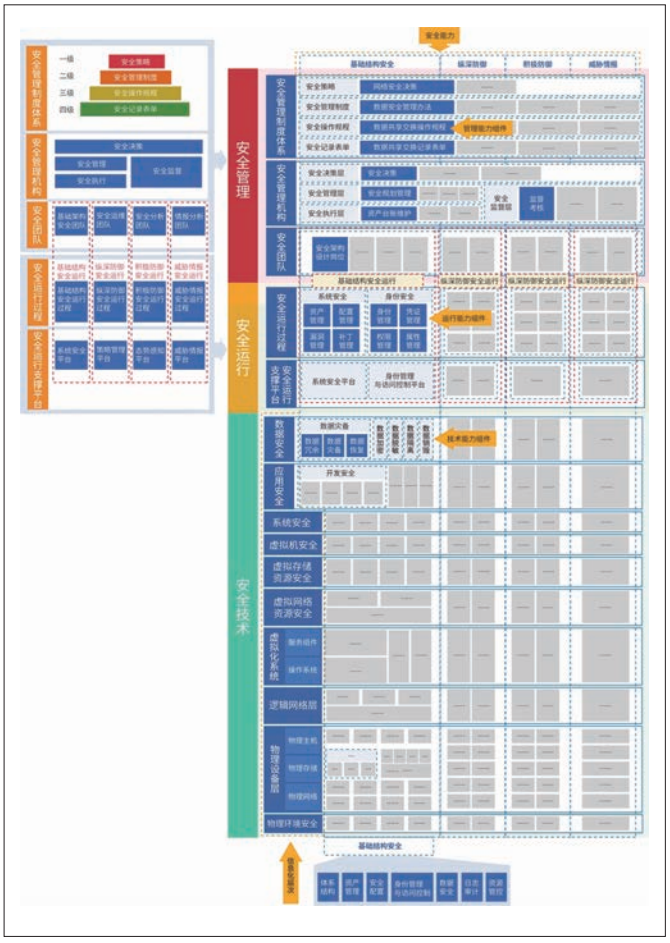
对于数字化的系统来说，IT与业务是密不可分的。从EA方法论出发，上述网络安全能力应当与信息化相融合，以保障业务安全、有序地发展。通过识别、设计构成网络安全防御体系的基础设施、平台、系统和工具集，围绕可持续的安全运行体系进行集成整合，可以构建出动态综合的网络安全防御体系。需要注意的是，我们要避免“以偏概全”的传统模式，以全覆盖、层次化的思路进行规划、设计。以网络的纵深防御体系为基础，进一步以数据确定防御重点，开展实战化安全运行，规划、建设动态综合的网络安全防御体系，以确保安全能力在IT的各层次有效内生。

通过组件化安全能力，内生安全框架将网络安全能力映射为可执行、可建设的网络安全能力组件，具体如图3所示。安全能力组件是安全能力的实现载体，具体包括安全管理、安全技术、安全运行相关内容。在政企机构信息化的所有层面，把安全能力组件与信息化组件相结合，保证了安全能力对信息化的覆盖与融合。通过对安全组件的组合，能够定义出要建设的项目，并清晰地表达项目的建设内容。

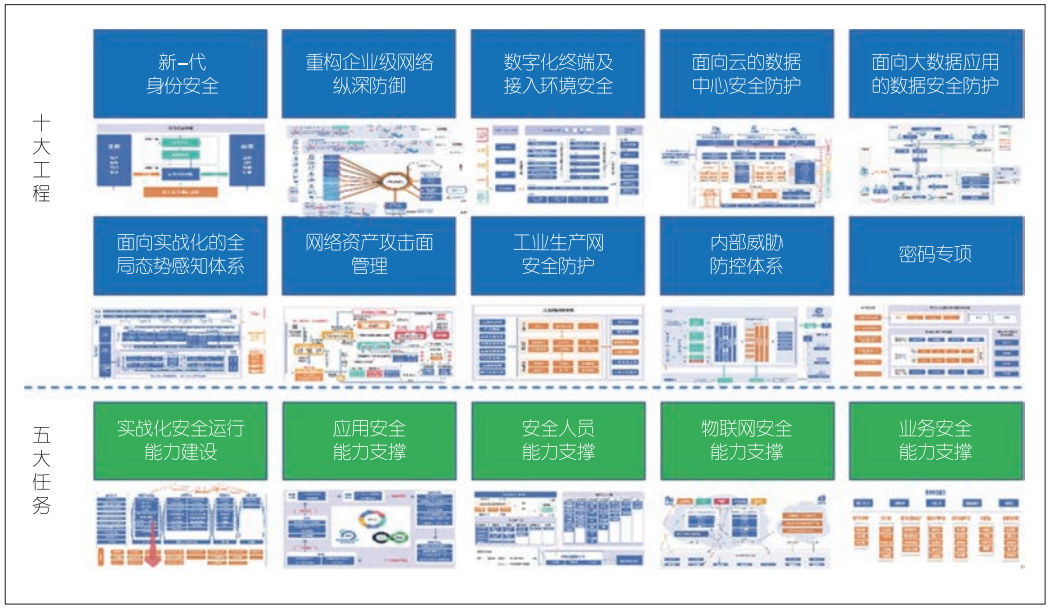
在政企机构网络安全的实际规划、设计、建设、运行、落地的过程中，项目是推行安全管理思想、强化安全管控、提升安全能力的重要抓手。在安全规划中，项目设置的科学性、合理性、可落地性是决定安全体系建设成效的关键因素。通过使用基于“能力导向”的EA方法论，内生安全框架将政企的网络安全防御体系作为一个整体复杂系统进行设计，并在此过程中识别出了15个“构成子系统”，即“十大工程、五大任务”，具体如图4所示。进一步地，内生安全框架以系统工程的方式将这15个构成子系统分别作为“复杂系统”进行设计，从而梳理清晰其全景与相互依赖关系。

在框架的工具集中，我们面向这15个子系统设计了项目规划纲要。项目规划纲要是项目库的核心。从项目建设与实施的视角出发，项目规划纲要高度概括了项目的目标、覆盖范围、预期效果、协同领域以及多个项目之间的作用关系，强调项目规划、可研、立项与设计阶段的关键要点。

政企机构在网络安全规划时可参考项目规划纲要模板，



▲图3 组件化安全能力



▲图4 项目实施纲要库

并根据政企现状规划项目，向信息化领导和网络安全领导阐述项目的重要意义、必要性、建设内容等，以得到充分的资源配给和政策支持。在规划的全周期内，政企参考项目规划纲要进行可研、立项、招标、初步设计、概要设计、建设和运行，明确项目执行中每个系统须达到的预期能力、关键指标和协同关系，确保安全能力的完整性、体系性和可落地性，进而以一个可实现、一贯秉承的整体视角持续建设，以达成网络安全防御目标。

4 内生安全“构成系统”的技术要点与参考架构

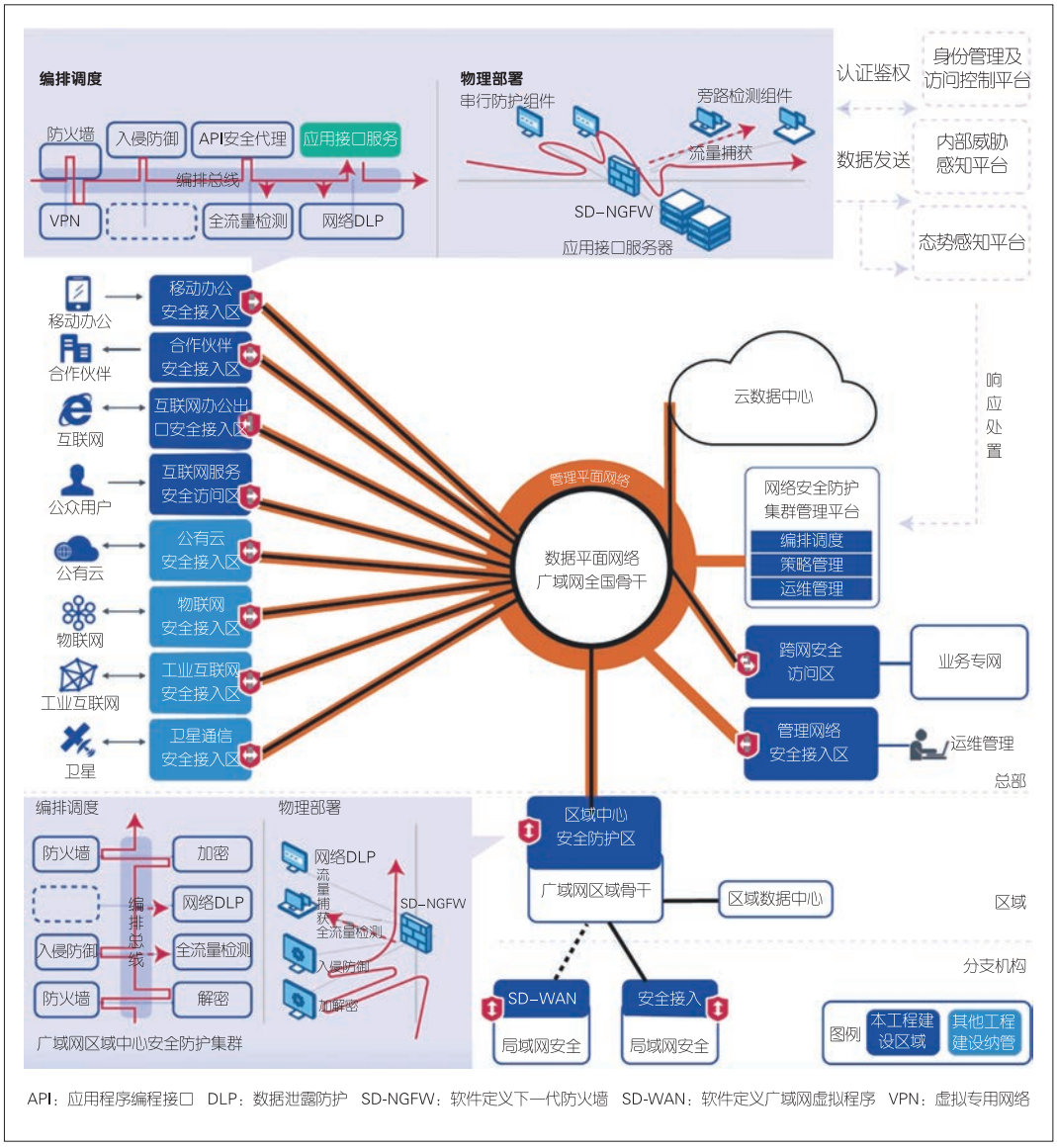
在内生安全框架的每一个项目纲要库中，通过进一步的扩展，能够间接起到构建该领域的“参考架构”的作用。“参考架构”一般不会具体明确实现该领域能力体系的具体方案或服务细节，而是会从该领域（子系统）的能力体系出发，给出子系统网络安全的能力要求与技术要点。而具体采用何种落地方案、产品、服务，则不受限制。这样也能够在保证网络安全防御目标达成的同时，采用多样的技术路线来灵活实现。下面，我们从两个角度进行说明：最基础的网络纵深防御和目前最受关注的数据安全。

网络纵深防御是网络安全体系中最基础的子系统，其整体架构如图5所示。在数字化转型进一步升级、网络变得越来越开放与复杂的情况下，网络纵深防御已不再是简单的边界防护，而是有了更多的具体要求。在这种挑战下，“重构企业级网络纵深防御”工程给出了设计的参考架构与样例库。

从设计原则上，该工程给出了“最小攻击面设计”“面向失效的设计”“能力导向的设计”3个原则。在总体架构上，通过在大型政企网络中构建多级网络纵深，并在纵深与各安全域上进行威胁模型分析，建立纵深防御策略矩阵。

网络纵深防御最终遵循8个方面的技术建设要点，具体包括：

（1）设计标准化、模块化的各类网络安全防护集群，提供流量清洗、网络访问控制、加/解密、入侵防范、恶意代码防范、应用安全防护、安全代理、数据泄漏检测、全流量检测、攻击诱捕等安全能力，通过软件定义



API：应用程序编程接口　DLP：数据泄露防护　SD-NGFW：软件定义下一代防火墙　SD-WAN：软件定义广域网虚拟程序　VPN：虚拟专用网络

▲图5 网络纵深防御整体架构

网络等技术实现安全能力服务化、弹性扩展和灵活调度编排，适配各节点的安全防护需求。

（2）规整网络外部边界，收敛应用服务及接口的协议类型，分别部署网络安全防护集群：建设合作伙伴安全接入区，保障对外接口及数据安全；建设互联网安全接入区，保障互联网服务访问安全；建设互联网办公出口安全接入区，保障用户上网行为安全；纳管其他工程建设的公有云安全接入点、物联网安全接入区、工业互联网安全接入区、卫星通信安全接入区。

（3）在业务专网、涉密网等不同密级的网络间集中建设跨网安全访问区，部署网络安全防护集群，提供网络访问控制、应用程序编程接口（API）安全代理、数据隔离与交换等能力，确保用户跨网访问及数据交换的安全。

（4）在广域网各区域中心节点建设区域中心安全防护区，部署网络安全防护集群，以增加广域网安全防护纵深，形成多层次、协同联动的广域网纵深防御能力，全面缩小广域网暴露面，从而降低横向移动的可能性。

（5）在广域网各分支节点建设分支机构安全接入点，通过软件定义广域网（SD-WAN）技术，实现网络访问控制、传输加密、入侵防范等能力，保障大量分支机构节点的安全接入，优化广域网线路成本，提高部署和运维工作效率。

（6）建设独立的管理网络，以实现数据平面与管理平面分离，收敛硬件管理接口，从而确保运维管理通道资源的可用性。建设、管理网络安全接入区，部署网络安全防护集群，基于零信任架构和基于属性的访问控制模型，与身份管理及访问控制平台对接，实现运维特权账号管理，从而对运维管理操作实施动态细粒度访问控制，最小化对资源的访问权限。

（7）将各安全防护集群的安全数据接入安全运行与态势感知平台，为安全分析提供全局网络安全数据支撑。

（8）面向各节点的网络安全防护集群，建设统一的运行管理平台，以实现安全策略全生命周期自动化管理，从而支撑态势感知平台安全事件的响应处置。

根据具体的网络环境场景，上述建设要点完整地呈现了系统架构中的组件要素及它们相互之间的逻辑关系，能够帮助政企机构在该领域形成更准确的项目定义，而不仅仅是简单的产品堆砌。因此我们需要瞄准一个可实现、有依据的目

标，进行全景设计。对于这其中所涉及到的技术要点，我们并不会强制地规定具体的实现方式，而是更为关注其所需要的安全能力，以及实现这些能力所必要的组件、子系统、模块，以及它们之间的逻辑关系和集成关系。这些内容的进一步细化与扩展，就能够起到“参考架构”的作用。

另外一个例子是数据安全。与最为基础的网络纵深防御相比，数据安全领域则更加能够体现了“内生”的重要性。为了描述得更清晰，我们会用到系统工程中的一个工具ConOps，具体如图6所示。

数据安全运行构想图共有4层：

（1）数据安全策略层。该层的重点是健全数据安全管理制度，能根据数据安全治理的结果，构建相应的数据安全策略，从而帮助机构明确数据安全所需的组织、规范、制度、流程等。从业务场景、应用逻辑出发，基于数据安全治理阶段的成果（数据脉络、数据标签、数据分类分级等）构建需要基于属性的数据安全策略，以向下面的3层进行分发。这一层更多的是与数据安全的管理相关。

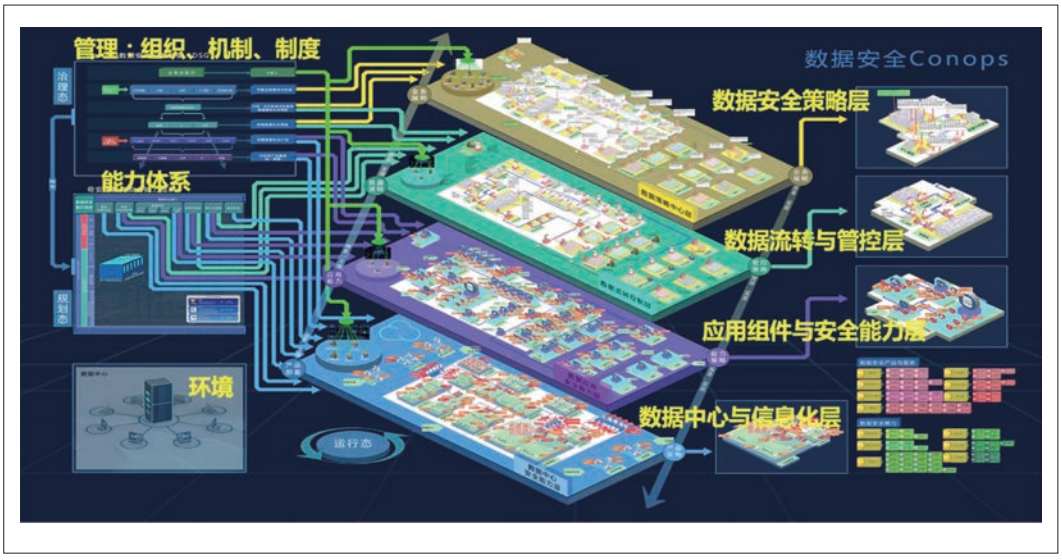
（2）数据流转与管控层。该层的重点是确保数据的流转有序合规、数据使用的行为规范，并实现对数据的全面梳理和有效防护。在这一层中，我们要全面梳理数据资产，确定适当的数据安全等级，并设定多样化的属性标签，从而全方位描述与数据安全管控可能相关的数据信息；通过明确管控数据的流转，并结合数据流转监测，发现非法用户窃取数据等异常行为；根据数据流转与管控策略，以“权限最小化”原则进行授信。未来，我们可通过零信任体系进行动态评估，从而实现对数据的动态、细粒度访问控制；对数据使用行为留痕，从而为实时的监测响应和审计提供支撑。

（3）应用组件和安全能力层。该层用于描述新型数据中心中业务应用的运行态，并基于业务系统的逻辑和应用架构，将各个应用组件和各组件之间的逻辑关系呈现出来，同时将每个组件和应用所需要的安全能力嵌入到组件中，从而将安全能力与应用内生融合。进一步地，根据数据安全治理的成果做相关的安全保护（如加密、脱敏、去标识化等）。同时，应用安全策略的落地会集中在这一层，“身份与访问控制、信息保护、监测与响应、审计与定责”为之提供能力支撑。

（4）数据中心和信息化层。该层的重点是保障数据的载体和业务运行环境的安全，包括数据中心安全区域划分、边界网络安全栈防护、服务器加固、系统与资产安全的保障等。该层是数据的载体和业务运行的基础环境，是数据安全的基础保障。

数据中心安全能力层是以体系化的方式，保障数据运行环境的安全。数据中心安全区域的划分，保证了不同安全等级业务在适合的区域运行，以及不同安全等级数据的有效隔离；数据中心网络安全栈防护，是为了做好边界安全的防护抵御外部攻击；服务器加固与防护，是对应用和中间件进行持续监控保护，防止服务器遭受APT和0DAY攻击；而面向资产、配置、漏洞、补丁的系统安全，可以解决资产不清、配置不明、漏洞分布不知、补丁修复缓慢等问题。

我们可以看到，在数据安全运行构想图中，各层级之间可以实现有效连接和运转。自上而下看，这是策略的逐层实现与落地；自下而上看，这是从产品部署到应用能力，再到业务流转及逻辑规则的支撑与提炼。尤其是最上面的两层，说明了与传统的网络安全相比较，要想做好完整的数据安全保障，一定会介入数据流转、应用逻辑、管理策略，这就更加体现了“内生”的思想。在数字化时代的新应用与数据安全体系中，安全能力不仅仅要内生于信息化环境，甚至要内生于应用与业务逻辑，以及数据流转与管理策略当中。



▲图6 数据安全ConOps运行构想图

5 结束语

迄今为止，内生安全框架在近3年已经被应用

下转第56页➡

零信任架构在医疗物联网安全建设中的应用

Application of Zero Trust Architecture in Security Construction of Internet of Medical Things

景鸿理/JING Hongli，屈伟/QU Wei，刘治平/LIU Zhiping
（天融信科技集团股份有限公司，中国 北京 100193）
(Topsec Technology Group Inc., Beijing 100193, China)

DOI：10.12142/ZTETJ.202206007
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221208.1448.001.html
网络出版日期：2022-12-09
收稿日期：2022-10-16

摘要：提出了一种基于零信任架构和技术的医疗物联网（IoMT）融生安全框架。该安全框架利用零信任控制平台、物联网安全接入网关、医疗终端、医疗业务系统、相关辅助支撑系统等组件，实现访问主体、运行环境、访问客体的融合共生，能够形成以身份可信管理为中心，全面融合业务安全访问、持续风险评估和动态访问控制的安全能力，支撑IoMT的设备统一管理、安全准入控制、设备行为分析、终端安全检测、动态可信接入、安全加密通道等安全应用。

关键词：IoMT；智能医疗设备；零信任架构；融生安全框架

Abstract: A security framework for the Internet of Medical Things (IoMT) based on zero trust architecture and technology is proposed. Using the zero trust control platform, Internet of Things security access gateway, medical terminal, medical business system, and relevant auxiliary support system components, the security framework realizes the access subject, operating environment, and access object fusion symbiosis, which can form a security capability that takes identity trusted management as the center, fully integrate business security access, continuous risk assessment and dynamic access control, and support IoMT equipment unified management, security access control, device behavior analysis, terminal security detection, dynamic trusted access, secure encryption channel, and other security applications.

Keywords: IoMT; intelligent medical equipment; zero trust architecture; fusion-symbiosis security framework

医疗物联网是物联网技术在医疗行业的重要应用。医疗物联网模糊了传统的网络边界，通过可穿戴设备、传感器和专业工具等智能医疗设备，实时感知环境信息（包括人和物理环境等），或将数据传输数据给用户，并在网络中完成数据加密、数据传输和数据分析等，从而协助人们完成医疗物联网平台数据采集和数据分析等工作[1]。但大量支持物联网技术的智能医疗设备数量激增,容易受到未经授权访问和其他恶意活动的攻击[2]；物联网技术的异构性和设备的动态管理特点，使得医疗物联网系统容易受到不同的动态环境攻击者的数据窃取和篡改[3]。从某种意义上讲,基于物联网的医疗行业应用放大了安全边界，带来了访问控制和数据资源的安全风险。因此，加强医疗物联网的身份管理和边界防护，提高医疗物联网平台、用户、设备等资产的身份认证和访问控制安全能力，保护医疗物联网环境下的应用和数据资源安全,是当前亟待解决的问题。

随着数字化转型的不断深入，以信任为核心的安全理念迎来发展机遇，零信任机制成为一种有前景的解决方法，可有效应对行业数字化转型过程中医疗物联网系统的各种隐私、安全和认证挑战。医疗物联网与零信任机制的融合，能够打破网络边界位置和信任间的默认关系，解决在不可信环境中可能出现的智能医疗设备身份可信和业务数据动态管理问题，提升医疗物联网对基础网络层和数据中心层的安全管控力度，隐藏被攻击区域，减少攻击面，最大限度保证资源被可信访问。

本文中，我们主要对医疗物联网建设中的可信安全防护进行详细研究，融合新兴的零信任架构和技术，结合医疗物联网的安全风险，分析适用于医疗物联网的动态身份管理机制设计，提出零信任-医疗物联网融生安全框架，并解决以下问题：

（1）医疗物联网边界模糊带来的安全性问题。随着移动办公、万物互联等技术的广泛采用，医疗物联网的网络边界越来越模糊，安全防护边界逐步被打破，已无法清晰定义安全的网络。工作方式移动化、数据资源集中化、资源访问云

化等，进一步导致业务数据的访问超出了传统的物理边界，增加威胁暴露面。

（2）医疗物联网传统安全架构缺陷问题。医疗物联网仍然按照传统网络安全架构将网络划分为内部网络和外部网络。内部网络受信任，外部网络则不受信任，整体安全防护通过静态配置来实现。在受信任区域，大量的移动用户和设备接入导致业务暴露面扩大，一旦被渗透，受信任区域所有数据资产无法进行有效隔离和防护；内部网络部署的大量设备缺少信息共享和安全联动，受信任区域实质上处于割裂状态下的静态安全防护。在不受信任区域，随着数据资源集中，价值增加，存在大量绕过或攻破网络访问权限的内部横向攻击破坏行为；以高级可持续威胁（APT）为代表的高级攻击层出不穷，大型组织甚至国家的攻击者可以利用大量的漏洞“武器”，对重要目标进行攻击，这类攻击往往防不胜防[4]。

1 医疗物联网架构和安全概述

中国信息通信研究院将医疗物联网定义为 Internet of Medical Things（IoMT），是指面向医疗机构全方位的运营和管理，将传感器、近距离通信、互联网、云计算、大数据、人工智能等物联网相关技术与医学健康领域技术相融合，实现医疗健康服务智能化的综合系统。IoMT 通过结合广域网、局域网、无线网络等网络领域，使得物联网技术越来越广泛地应用于医院信息系统，如人体传感技术、医疗装备定位、移动医疗技术、精准疫情防控等，已形成基于医疗信息平台的，具有创新应用模式、系统高度集成、数据资源高度整合的医院管理应用生态链[5]。

1.1 医疗物联网架构

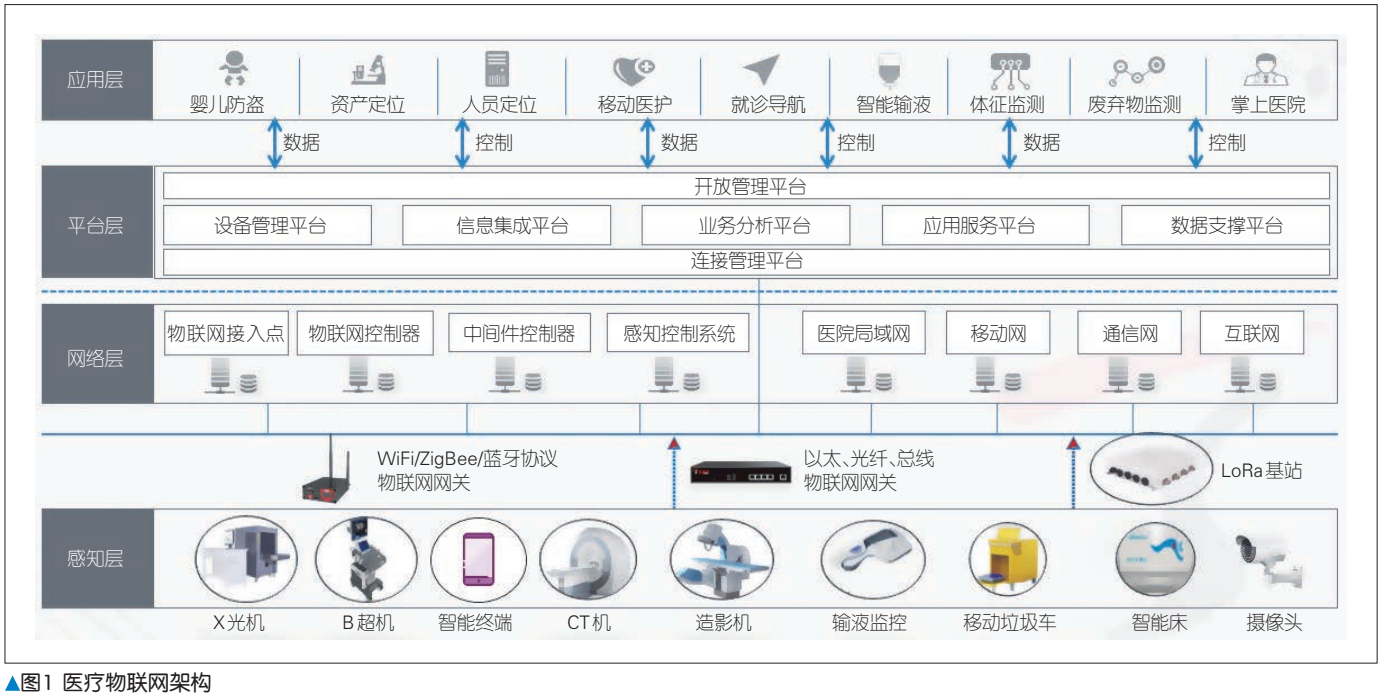
IoMT 架构一般沿用通用物联网的感知、网络、应用 3 层体系，结合大数据、云计算等医疗实际环境，把管理和业务平台建设独立出来，形成了 IoMT 的感知层、网络层、平台层和应用层 4 层体系架构，如图 1 所示。

感知层主要通过医疗健康感知设备和信息采集设备，对 IoMT 中的医患人员设备节点进行感知识别，并利用多种生理信号采集方式，协同完成对医疗信息的采集和数据传输。

网络层实现物联组网和控制，利用以太网技术、移动通信技术、机器通信（M2M）技术等，以无线或者有线的通信方式，将感知采集的数据信息进行实时、无障碍、高可靠的传送。

平台层主要通过设备管理平台、信息集成平台、应用服务平台、业务分析平台、数据支撑平台等，实现终端设备和资产的“管理、控制、运营”一体化，向下通过连接管理平台连接感知层，向上通过开放管理平台提供面向医疗应用服务的开发能力和统一接口管理。

应用层面向医院业务管理、个人健康管理、网络运营管控、辅助决策支撑等提供具体的业务应用[6]，如婴儿防盗、资产定位、人员定位、移动医护、智能输液、体征监测、废弃物监测、掌上医院、就诊导航、数据支撑平台等。



▲图 1 医疗物联网架构

1.2 医疗物联网安全防护现状

IoMT安全防护一般参考物联网安全架构有关标准要求进行建设，主要包括对资产标识与配置管理、数据加密与保护、逻辑访问控制、设备安全状态等安全基线控制要求[7]。经过多年的信息化建设，IoMT基本实现了环境数据感知采集、业务过程全周期控制、医疗全程跟踪追溯、医院体系化安全管理等[8]。物联网技术给医疗行业带来网络化、智能化、自动化的同时，也存在着物理感知节点控制伪装、医疗信息数据可能被破坏或用户隐私泄露等安全隐患[9]。

目前，IoMT安全防护建设主要基于网络安全等级保护的物联网安全扩展要求，采用传统网络隔离的安全模型，用防火墙、入侵检测系统（IDS）/入侵预防御系统（IPS）、虚拟专用网（VPN）、行为审计等边界防护设备划分出医疗内网和外网，形成以账户管理和边界防护为核心的防御体系。从防范外部攻击的角度，防火墙和VPN的模式形成了深度防御态势，增加了黑客攻击的难度，但是对内部人员实施的窃密行为无法管控，存在内部人员攻击和绕过边界防护的APT等攻击行为；同时，IoMT也模糊了内外网的边界，存在逻辑外部人员实际已在内网进行操作，以及逻辑内网设备实际已在外网存在的可能。随着IoMT对云计算、移动互联网、大数据、人工智能等技术的融合应用，IoMT联网设备一般无法配备足够的存储空间和计算能力，不能通过部署安全防护软件来保障自身安全；大量智能设备不间断收集数据并存储到云端，会带来医疗数据泄露、非授权访问、隐私泄露等新的安全隐患。医疗行业用户需要面临医疗数据泄露、应用账号密码泄露、特权账号共享、网络终端木马、内部员工违规操作等内部风险，以及APT攻击、网络钓鱼邮件等外部威胁。现有安全防护手段与业务结合不紧密，资产管理、户身份认证、访问控制、数据资源保护以及终端安全状态等安全措施缺乏统一融合管理，亟需优化和重构。

2 零信任架构和关键技术

零信任是一种建立安全战略的理念、方法和框架，代表着当前正在演进的网络安全最佳实践，力求通过全新的去中心化安全架构，应用更细粒度的规则来解决网络中特定数据的安全威胁[10]。2020年8月，美国国家标准与技术研究院（NIST）发布的《零信任架构》指出了传统安全架构基于边界安全的问题，并将零信任架构确定为一种包含身份、凭证、访问控制、操作、互联基础设施等所有网络要素的端对端安全体系方案[11]。经过多年发展，数字化时代网络安全威胁比以往任何时候都更加复杂和险恶，安全架构的薄弱环节正是身份安全基础设施的缺失。建设以身份为基石的零信任网络安全体系，成为覆盖云环境、大数据中心、微服务、万物互联等众多场景的新一代安全解决方案。

2.1 零信任架构

零信任架构本质就是以身份为中心，根据受限资源访问需求，在访问主体和访问客体之间，实现临时、动态、可信的安全访问体系，如图2所示。

基于零信任建立的网络以受限资源安全保护需要为出发点，将安全能力抽象为可信代理、动态访问控制、身份管理、权限管理及身份分析等功能组件，形成主客体间的动态可信安全访问平台，同时与其他安全分析平台协同联动，保障主体对客体业务、数据访问的安全可信闭环[4]。

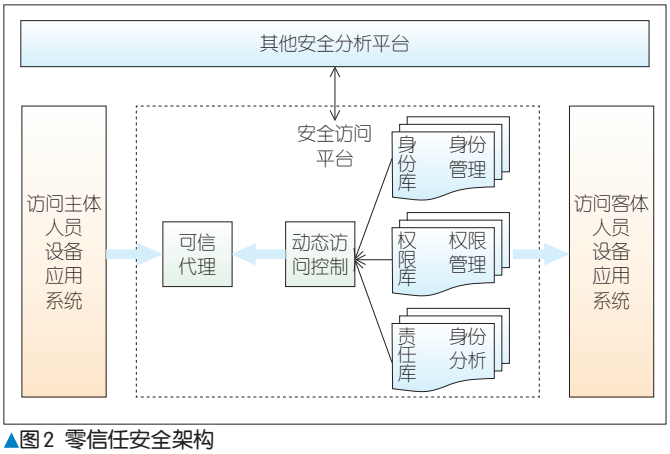
2.2 零信任关键技术

零信任关键技术包括身份管理、终端环境感知、主体行为分析、信任推断、动态控制等。

（1）身份管理。身份管理分为认证和授权两大组件，可为零信任体系提供身份认证服务和安全授权服务。身份管理可以将用户身份和访问权限做到细粒度对应，确定用户最小访问权限。对主客体的身份认证可以为业务系统提供统一的身份认证服务，支持多种常用认证协议，建立多权限模型，从而满足不同业务场景[12]。

（2）终端环境感知。终端环境感知需要针对业务终端进行统一管理和分组，查看所有终端的状态，对终端的操作系统版本、核心进程号、指定文件、木马、蠕虫、病毒等指定监测因子进行持续监控与检查，并针对终端进行安全策略集中下发等，为零信任体系提供终端风险状态的判定。

（3）主体行为分析。主体行为分析是指对主体的日常访问行为进行持续审计和监控，构建行为模型和综合评分机制，以形成主体行为访问基线，对主体访问偏离基线的程度



▲图2 零信任安全架构

进行上报，从而为零信任体系提供主体行为偏离度的判定。

（4）信任推断。信任判断是指综合多种判定因子，实现基于身份、权限、主客体安全等级模型的关联；建立主体访问客体的信任模型，为动态访问模块提供可信访问的判断依据；实时接收、统计终端环境风险的评估数据，判断当前用户风险状态。

（5）动态访问控制。动态访问控制与信任推断联动，将网络安全等级与业务安全策略进行自动匹配，将最小权限下发到相应的策略执行点。主体行为分析系统提供的风险评估等级，可以提供多因子认证方式的访问控制策略和执行，实现动态决策授权。基于访问主体和访问客体安全属性的风险评估结果可以进行动态决策。

3 基于零信任架构的医疗物联网融生安全框架

3.1 零信任–医疗物联网融合解决思路

结合 IoMT 架构和安全风险，融合零信任架构和技术，以身份为中心，建立访问主体（合法设备、合法用户等）、运行环境（通信网络和计算环境）、访问客体（业务应用及数据资源）之间的安全可信关系，能够持续验证主体的访问权限信任度。基于设备代理/网关部署隐藏互联访问交互，可以实现对医疗终端到业务系统的主体访问、应用访问、访问控制 3 个阶段的持续动态评估，从而能够确保访问主体安全可信和业务访问动态安全，达到零信任和医疗物联网融合共生安全的效果。零信任–医疗物联网融合解决思路如图 3 所示。

3.2 零信任–医疗物联网融生安全框架

我们按照零信任–医疗物联网融合解决思路，设计了零信任–医疗物联网融生安全框架，具体如图 4 所示。

零信任–医疗物联网融生安全框架包括零信任控制平台、物联网安全接入网关、医疗终端、医疗业务系统、相关辅助支撑系统 5 部分，分别部署于医疗物联网的控制平面和数据平面。

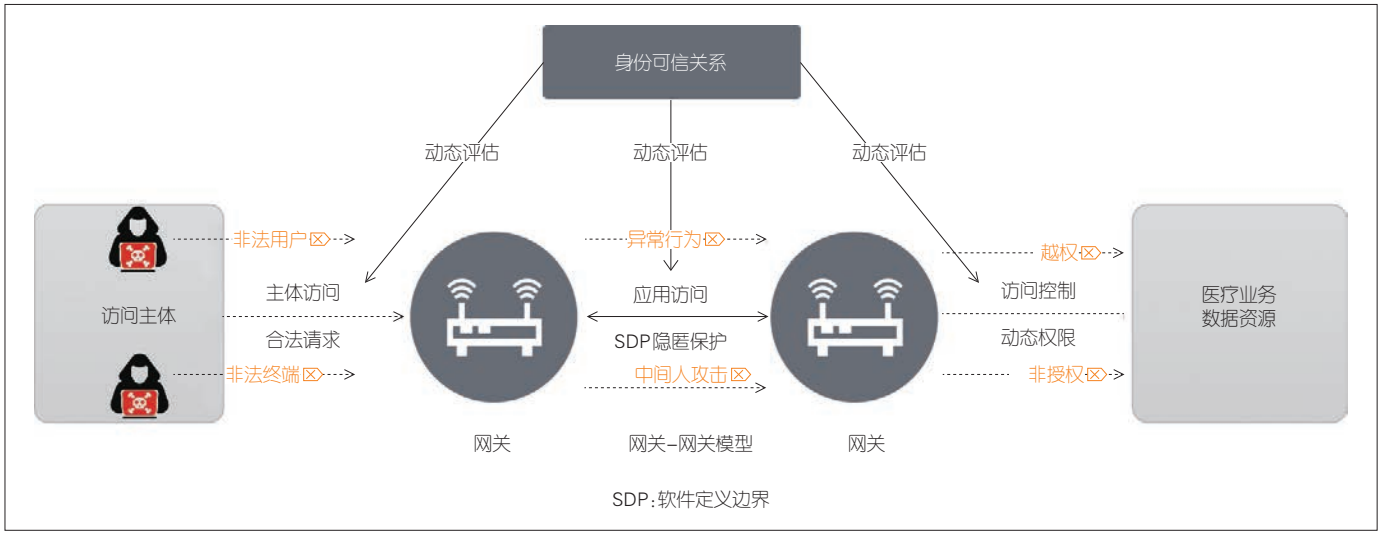
（1）零信任控制平台

零信任控制平台是整个框架的“大脑”和中心控制点，包括信任策略引擎、策略控制中心、物联环境感知、智能身份分析等组件。零信任控制平台负责医疗终端身份验证方的通信，统一协调身份验证和授权分发，定义和评估相应的访问策略，动态调整医疗终端的接入权限。零信任控制平台通过策略控制中心对用户和设备建立或关闭资源连接，进行自动配置、动态授权和策略决策；通过信任策略引擎为给定的主体授予访问权限，对策略控制中心下达信任指令和收集评估状态；通过物联环境感知识别环境和设备，进行风险通报；通过智能身份分析实现访问控制的日志上报和持续评估。

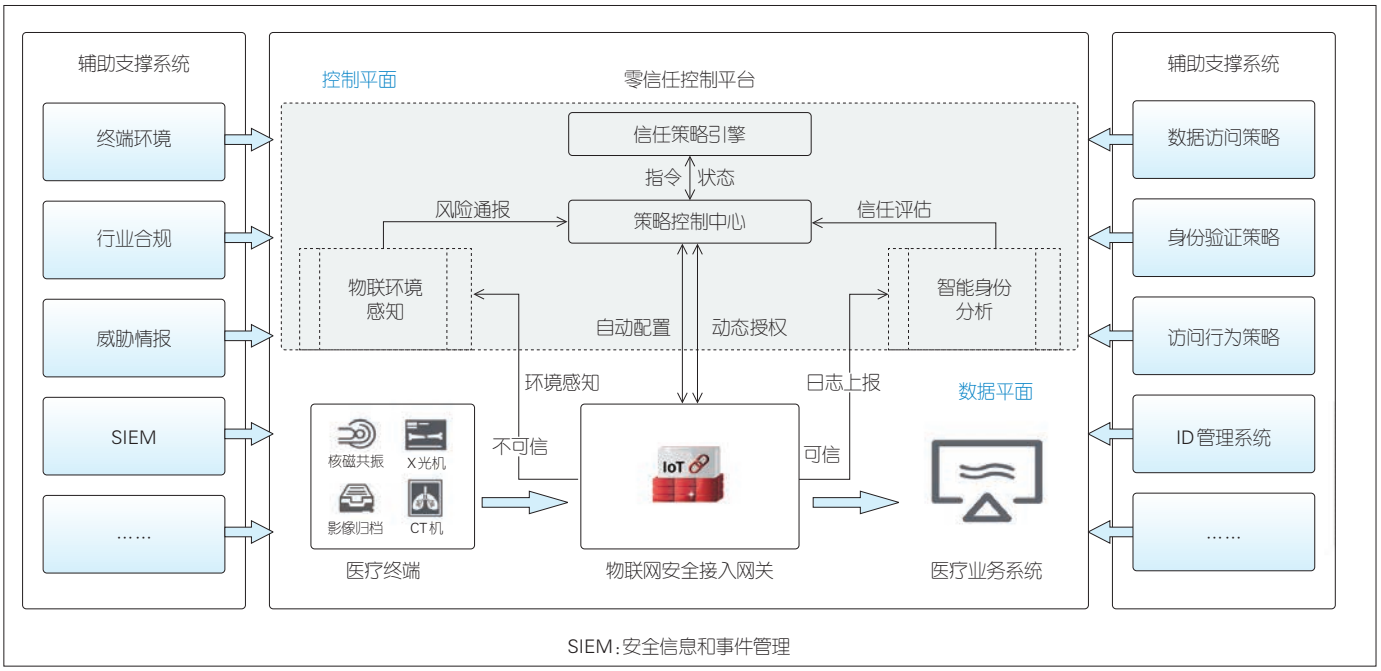
（2）物联网安全接入网关

物联网安全接入网关是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。物联网安全接入网关主要负责监视主客体间的访问连接，建立安全传输通道，从零信任控制平台接收控制信息，并只接受经过零信任控制平台确认的医疗终端的用户访问连接请求，保证只有经过授权的主机才能访问到受保护的医疗业务系统。

（3）医疗终端



▲图 3 零信任–医疗物联网融合解决思路



▲图4 零信任–医疗物联网融生安全框架

医疗终端是访问主体，在主体实施信任评估前均处于不信任状态，通过策略引擎和策略控制中心实施信任评估。

（4）医疗业务系统

医疗业务系统是访问客体，初始的资源隔离、策略发现和自动化配置使得医疗业务系统始终处于受保护资源的资源访问状态。

（5）相关辅助支撑系统

除上述核心组件外，还需要引入辅助支撑系统，包括数据访问、身份验证、行为分析、ID管理、威胁情报、终端环境、行业合规、安全事件等。这样能够为零信任控制平台的策略生成及安全态势提供决策依据，从而达到安全联动效果。

4 零信任–医疗物联网融生安全框架的应用

基于零信任–医疗物联网融生安全框架的网络安全体系建设模糊了传统基于边界的物理或网络位置，而授予用户或设备认证和授权的隐式信任，符合网络安全应用趋势，能够在IoMT安全建设中支持设备统一管理、安全准入控制、设备行为分析3项安全基线应用，并实现终端环境安全检测、动态可信接入、安全加密通道3项安全创新应用。

（1）设备统一管理

设备统一管理需要对所有医疗终端进行统一分组管理，查看所有医疗终端的状态，并针对终端进行安全策略集中下发等，为零信任控制平台提供终端风险状态判定依据。

（2）安全准入控制

安全准入控制网络支持在边缘接入层采用安全隔离技术，对不同主客体之间建立物联网安全通道，设定必要的分布式安全访问控制措施，并利用先进的设备指纹、智能画像、精准识别等技术，对接入的设备进行安全准入控制，基于预设安全策略对接入节点进行安全访问控制，避免非法仿冒设备入侵。

（3）设备行为分析

物联网医疗终端形态多样化，地理位置分散，缺少值守，且一般携带敏感数据，因此容易发生设备盗用并以此为跳板侵入到医疗内部核心网络，从而造成重大损失。我们可通过智能学习和行为关联分析，构建医疗终端的正常行为模型，以达到安全管控的目标。

（4）终端环境安全检测（创新点）

IoMT终端环境安全检测具体包括对感知层网关自身环境检测、文件感知、容器感知、通信感知、状态感知、设备感知等，主要从终端环境出发，划分不同的终端安全等级，用于安全探测物联感知终端设备连接状态，监控设备数据传输安全，对终端的控制实现细粒度控制，改变以往的粗放式管理。

（5）动态可信接入（创新点）

动态可信接入可以融合零信任技术和IoMT接入的安全管控能力，将原有的静态防御改为动态防御，全面、动态、持续感知医疗终端和网关进程，能够实时度量和控制资源访

问行为，实现双向身份鉴别机制，支撑与业务的紧密结合，从而保证人员和医疗设备接入时身份的可信任。

（6）安全加密通道（创新点）

安全加密通道可以将零信任主客体间的动态可信安全访问能力赋能到IoMT中，建立医疗终端和医疗业务系统间的安全可信连接，改变传统的“先连接后认证”方式，向基于零信任的“先认证后连接”方式转变，实现对IoMT专用传输通道的安全加密，从而保障数据的传输安全。

5 结束语

零信任–医疗物联网融生安全框架提供了一种全新的安全访问思路，形成了一种与网络位置无关的动态访问控制方案，支持用户建立全局的安全控制策略。根据被访问客体的安全信任状态对访问主体进行授权，持续监测评估访问过程安全性和信任状态，自动编排更新身份访问策略配置，动态调整访问权限，实现基于身份/属性/权限等级策略的细粒度访问控制，满足医疗物联网创新技术应用安全需求。零信任的深度应用将会催生策略智能调优的手段。如何针对目标资产、组件、访问实体等实现智能化的动态安全风险评估和策略配置，仍然需要我们在自动化系统、深度学习、智能控制等领域进行深入研究，从而应对零信任安全访问网络建设中的策略自动发现、有限访问控制、缺乏高效检测防御的应用挑战。

参考文献

[1] 杨惠杰, 周天祺, 桂梓原. 区块链技术在物联网中的身份认证研究 [J]. 中兴通讯技术, 2018, 24(6): 3–40. DOI: 10.19729/j.cnki.1009–6868.2018.06.007
[2] 蒋昆. 西京医院: 医疗物联网安全的思考与实践 [J]. 科技新时代, 2018, (4): 38–40
[3] 陈庆龙, 石春花, 郝文延. 物联网医疗系统安全和隐私保护方法研究 [J]. 医学信息学杂志, 2022, 43, (1): 67–72. DOI: 10.3969/j.issn.1673–6036.2022.01.013
[4] 田由辉. 基于零信任架构的网络安全防护思路 [J]. 信息技术与信息化, 2020, (5): 154–157. DOI: 10.3969/j.issn.1672–9528.2020.05.048
[5] 戴家刚, 杨胜利, 周玉宝. 医院物联网体系结构和关键技术研究 [J]. 中国新通信, 2015, 17(21): 20. DOI: 10.3969/j.issn.1673–4866.2015.21.016
[6] 张程. 医院物联网方兴未艾 [J]. 检察风云, 2022, (5): 72–73
[7] NIST. IoT device cybersecurity capability core baseline: NISTIR 8259A [EB/OL]. (2020–05–29) [2022–11–28]. https://csrc. nist. gov/publications/detail/nistir/8259a/final
[8] 郭丽娜, 路杰, 郭玮娜. 浅谈物联网在智慧医院建设中的应用 [J]. 中国卫生信息管理杂志, 2016, 13(3): 299–302. DOI: 10.3969/j. issn. 1672–5166.2016.03.016
[9] 沈志强. 医疗物联网的安全问题及策略 [J]. 信息与电脑, 2017, (21): 178–179, 183. DOI: 10.3969/j.issn.1003–9767.2017.21.069
[10] KINDERVAG J. Build security into your network´s DNA: the Zero Trust network architecture [EB/OL]. (2010–11–05) [2022–08–23]. https://www.yumpu. com/en/document/view/17914587/build–security–into–your–networks–dna–the–zero–trust–ndmnet
[11] NIST. Zero Trust architecturel: NIST special publication 800–207 [EB/OL]. (2020–08–10) [2022–08–23]. https://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST.SP.800–207.pdf
[12] 张宇, 张妍. 零信任研究综述 [J]. 信息安全研究, 2020, 6(7): 608–614

作 者 简 介

景鸿理，天融信科技集团高级副总裁；主要研究领域为安全操作系统、网络安全、密码理论及工程应用；曾获国家科技进步二等奖2次、军队科技进步一等奖1次、党政密码科技进步一等奖1次。

屈伟，天融信科技集团资深战略咨询顾问，高级工程师；主要研究领域为数字化安全体系规划、智慧城市安全运营、健康医疗安全、电子政务安全、教育安全等。

刘治平，天融信科技集团CSA零信任专家；参与多项零信任及商用密码安全领域的标准规范编写，成功交付多个大型零信任及商用密码项目。

代码疫苗技术在DevSecOps体系下的实践

Practice of Code Vaccine Technology Under DevSecOps System

董毅/DONG Yi
（北京安普诺信息技术有限公司，中国 北京 100193）
(Beijing Anpro Information Technology Co. ,Ltd. , Beijing 100193, China)

DOI:10.12142/ZTETJ.202206008
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221221.1419.001.html
网络出版日期：2022-12-23
收稿日期：2022-10-17

摘要：安全工具在帮助开发人员构建安全软件方面发挥着至关重要的作用。然而，在不影响DevOps部署速度或交付频率的情况下，引入和充分利用安全工具是具有挑战性的。通过分析当下传统安全工具存在的问题，提出了目前已成功应用于交互式应用安全测试（IAST）工具和运行时应用自保护（RASP）工具的代码疫苗技术。阐述了代码疫苗技术在DevSecOps体系下的实践，并以Log4j2组件的远程代码执行漏洞的防护为例，梳理了代码疫苗技术的防护流程。

关键词：DevSecOps；代码疫苗技术；RASP；IAST；DevOps

Abstract: Security tools play a vital role in helping developers build secure software. However, it is challenging to introduce and fully utilize security tools without compromising the speed or frequency of DevOps deployments. By analyzing the current problems of traditional security tools, the code vaccine technology covering interactive application security testing (IAST) technology and runtime application self-protection (RASP) technology is proposed. The practice of code vaccine technology under the DevSecOps system is expounded. Taking the remote code execution vulnerability protection of Log4j2 component as an example, the protection process of code vaccine technology is summarized.

Keywords: DevSecOps; code vaccine technology; RASP; IAST; DevOps

DevOps的兴起打破了开发与运营之间的壁垒，帮助企业快速地将新产品或服务推向市场。然而，随着交付效率的提升，传统的“外挂式”安全和合规检测工具无法跟上快速迭代的步伐，已成为开发运营效能提升的瓶颈。内生安全的概念在DevOps实践中随即被提出[1]。DevSecOps的核心理念是将安全嵌入DevOps工作流程中，通过在软件生命周期的不同阶段加入相对应的安全工具，赋能软件内生的安全性，有效保障软件系统的正常上线发布和稳定运行[2]。

传统的安全检测工具，如静态应用程序安全测试（SAST）工具[3]、动态应用程序安全测试（DAST）工具[4]，经常会输出一些不准确的结果（误报或漏报），因此需要工程师手动评估输出结果的准确性。这与DevSecOps的自动化理念背道而驰。此外，防火墙、Web应用防火墙（WAF）、下一代WAF、入侵检测系统（IDS）、入侵防御系统（IPS）等都是基于边界防护手段[5]。随着“云大物移智”等技术的到来，“无界防护”需求的产生给企业的安全防护带来了新的考验。基于边界的传统网络安全防护远不能应对当下的网络攻击[6]。

新时代下的软件安全开发运营既要实现“安全左移”，又要实现“敏捷右移”。这一理念催生出代码疫苗技术。代码疫苗技术是指把某项技术像疫苗一样注入应用服务器内部，在内部清晰看到解析后的流量，感知业务运行过程的情境上下文。该技术可被应用到软件成分分析（SCA）、交互式应用安全测试（IAST）、运行时应用自保护（RASP）以及入侵和攻击模拟（BAS）等工具中[7]。这样一来，系统既能诊断应用自身存在的漏洞和缺陷，也能积极防御外部危险，进行自主检测和响应。本文主要分析当前传统应用安全防护面临的问题，阐述当前已成功应用于IAST和RASP工具中的代码疫苗技术，并对代码疫苗技术在DevSecOps体系下的实践展开深入研究。

1 代码疫苗技术相关理论概述

1.1 研究背景及现状

国际著名咨询调查机构Gartner制定了一个较为全面的DevSecOps工具链实践清单，并将DevSecOps生命周期分成计划、创建、验证、预发布、发布、预防、检测、响应、预测和改进10个环节。其中，每个环节都具有相应的安全工

具和安全活动，如图1所示。验证阶段应用的IAST技术来自2012年Gartner提出的一种新的应用程序安全测试方案。检测响应阶段应用的RASP技术是2014年被Gartner在应用安全报告里列为应用安全领域的关键技术。IAST和RASP技术已连续数年被Gartner列入“十大安全技术”[8]。

DevSecOps的根本目标是使企业组织内部拥有不断进化的安全能力，让安全变成一种内在属性嵌入企业数字化应用的全生命周期中。这样可以使企业具备持续安全的开发和运营能力，而不是单纯地保障业务和业务系统的安全[2]。在DevSecOps中，安全工具起到了关键作用。安全活动工具化是组织在DevOps基础上实现安全敏捷化的前提条件。只有将具体的安全活动工具化，追求安全的敏捷化，安全的“敏捷的价值交付”才能成为可能。建立“端到端”的、完整的安全工具链是DevSecOps安全活动工具化的内在需求和关键目标。近年来，用于改进软件构建和交付方式的工具越来越成熟，如持续集成（CI）/持续部署（CD）平台、微服务、容器等，但针对安全的工具开发还相对滞后。DevSecOps每个阶段集成了不同的安全工具。每个安全工具只能发现应用程序中存在的所有漏洞的部分子集。检测出的结果在很大程度上是不同的，甚至是混乱的。另外，通过人工手动对检测出来的漏洞信息进行筛查整理的方式，会影响开发效率，致使DevSecOps难以实现自动化。

针对上述问题，本文提出当前已成功应用于IAST工具和RASP工具的代码疫苗技术。其中，相较于SAST白盒安全测试技术和DAST黑盒安全测试技术，IAST技术具有更高的漏洞检出率和更多的适配场景，同时也更加适用于目前流行的DevOps场景[9]。相较于传统的WAF或IDS在流量层的检测，RASP技术更多的是与应用耦合在一起，通过运行时插桩技术，对应用的运行环境进行检测。这样的方式有助于拦截从应用程序到系统的所有调用，确保应用程序的安全，从而实时检测和阻断各式各样的安全攻击。在2021年底爆发的“核弹级”Apache Log4j2安全漏洞事件[10]后，RASP的能力得到了更为广泛的认可。

1.2 代码疫苗技术基本概述

代码疫苗技术是一种能够通过运行时插桩技术进行风险自发现及威胁自免疫的新一代安全技术。该技术可将IAST技术的漏洞检测能力与RASP技术的攻击防护能力进行合并，形成一个统一的IAST和RASP探针，实现IAST技术与RASP技术的集成，发挥各自技术的最大优势，进而形成统一的从漏洞检测到漏洞防护全生命周期的检测与防护解决方案，如图2所示。代码疫苗技术得核心内涵主要包含4个方面：

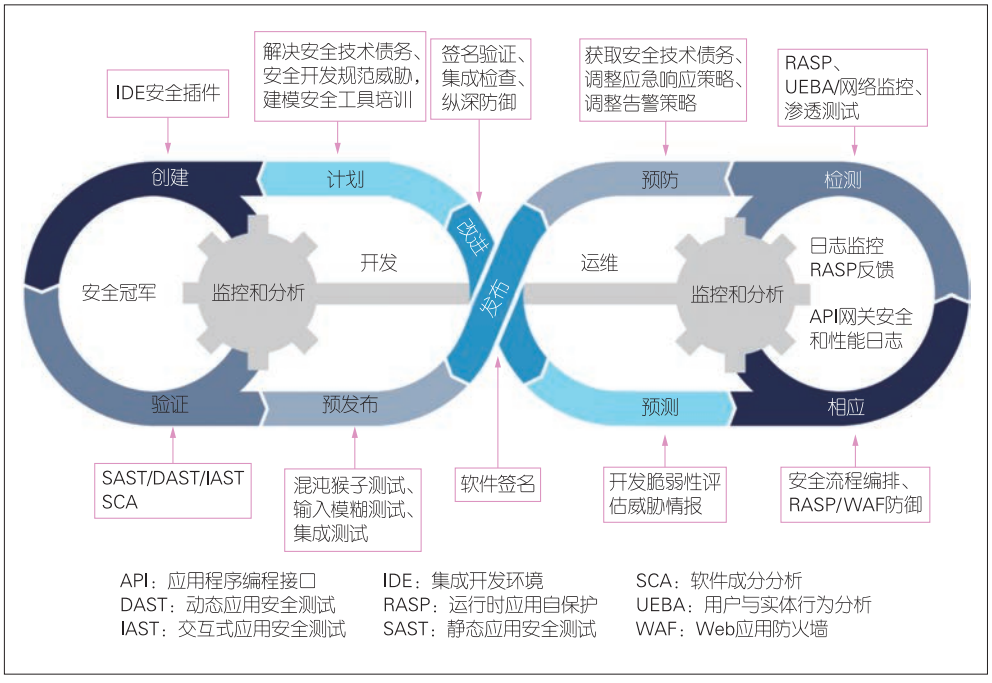
（1）不需要代码安全专家逐行分析源代码；

（2）不需要对原有代码逻辑进行修改调整；

（3）不需要维护复杂流量过滤策略及规则；

（4）实时监测应用程序中由第三方组件引入的风险。

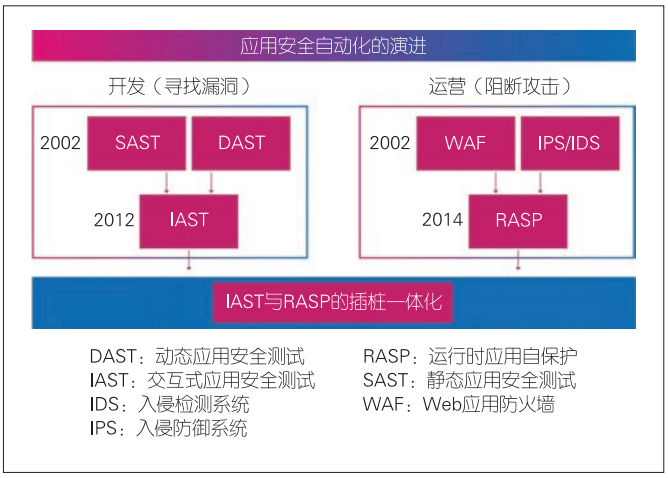
与医学界对疫苗的定义相似，代码疫苗技术并不是传统的外挂式安全技术，其侧重点是在软件应用的内部构筑安全屏障，以便搭建更加有效的内生安全防御体系。



▲图1 Gartner DevSecOps工具链

1.3 代码疫苗技术实现原理

无论是IAST技术还是RASP技术，都依赖以代码疫苗技术为内核的运行时插桩组件。在应用层运行时插桩是通过应用启动后替换函数体或在函数前后插入检测代码来实现的。通过插桩代码，记录应用程序运行时的堆栈数据可获得应用运行在关键点的数据信息。需要注意的是，由于不同语言间存在运行时的环境差异，因此不同语言实现插桩的方式也有所区别。以Java为例，由于Java拥有Instrument的特性，因此在



▲图2 统一的应用安全探针

类加载的过程中，需要首先对所关注的关键类与方法的字节码进行修改，然后才能够达到插入检测逻辑的目的。

运行时插桩技术和流量代理技术是IAST最具代表性的两种技术。其中，流量代理技术通过对镜像流量、日志等数据进行重放和分析来达到检测目的，对研发测试人员等完全透明，无流程侵入，也不依赖应用编程语言，如图3所示。

运行时插桩技术通过插桩帮助研发测试人员快速完成业务安全测试，精准定位漏洞细节并进行修复指导。运行时插桩技术又分为交互式缺陷定位（主动式插桩技术）和动态污点追踪（被动式插桩技术）。其中，动态污点分析技术能够基于运行时插桩跟踪外部可控数据对应用的影响，分析外部数据在应用内部的流转情况，从而确定应用是否存在漏洞。动态IAST拥有无重放数据、无脏数据、可应对加密签名接口、可适配复杂场景等优点，因此目前的适用面比较广泛。

在动态污点分析技术中，污点传播过程包括污点输入、污点传播、污点汇集3个阶段，如图4所示。

• 污点输入阶段。所有外部数据都被默认为不可信数据，因此需要在外部数据进入应用的时候，对其添加污点标记。

• 污点传播阶段。此阶段的主要目标为跟踪污点数据的传播过程。由于外部数据在进入应用程序时已被污点标记，因此当被标记数据进行运算或字符串拼接等操作时，所产生的新数据也将会携带污点标记。

• 污点汇集阶段。此阶段需要对可能触发漏洞的函数进行关注，即确定携带污点标记的数据是否会汇聚到敏感函数之上。若该过程发生，则意味着在应用程序中的这些函数执行流程中可能存在着漏洞。在污点传播阶段，如果携带污点标记的数据遇到清洁函数，并被成功执行过滤操作或其他安全操作，则该数据所携带的污点标记将被消除，以此来确认这条链路的安全性。

RASP的核心是通过插桩技术将防护逻辑与防护功能注入应用程序，深入应用运行时的环境内部，通过分析与了解上下文数据流及事件流，依据自有的安全规则列表，检测和防护无法预见的安全威胁与攻击事件（如0day攻击）。这种运作模式使得RASP能够解决一些难题，包括WAF所存在的检测规则与功能无法对应、服务端防御方式无法知晓、变形及未知威胁防御乏力、微服务场景难适配等。

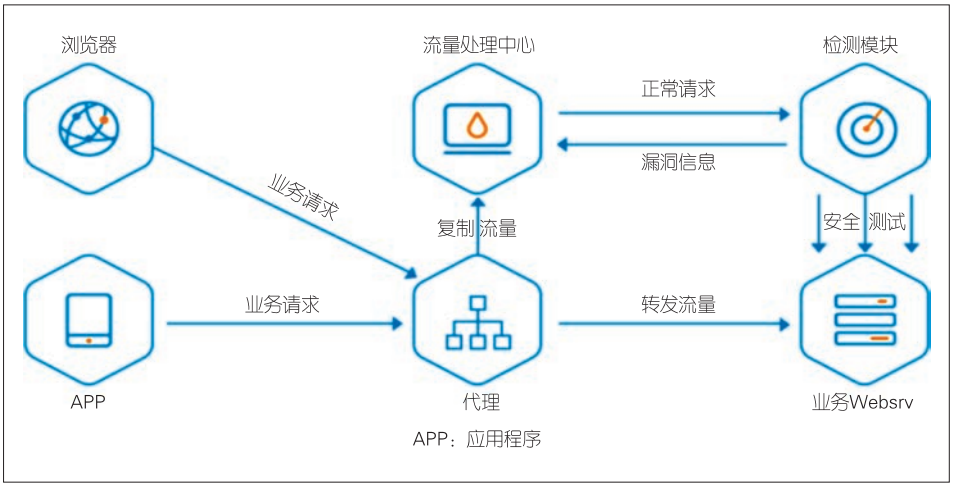
RASP主要获取以下4种运行时的上下文数据：

（1）超文本传输协议（HTTP）请求与响应数据，以及各种远程调用协议（RPC），例如Dubbo的请求与响应数据、gRPC等各式RPC框架。

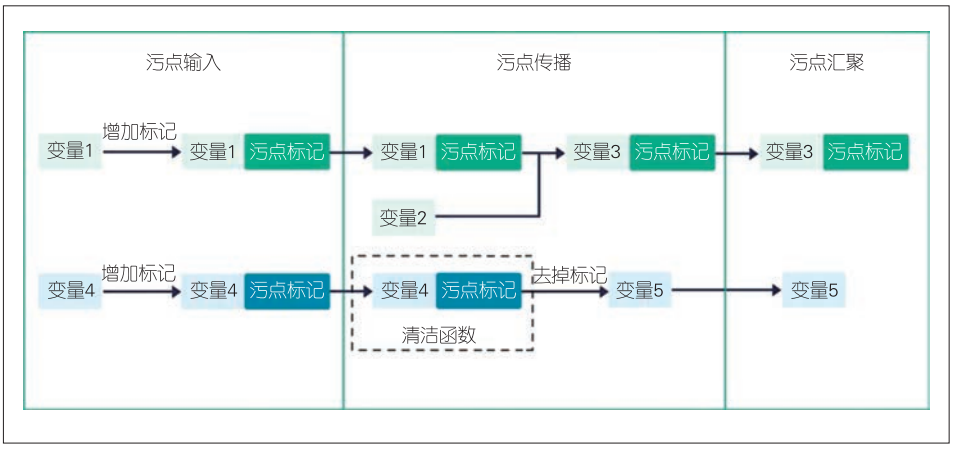
（2）所关注函数的执行数据，包括动态运行时函数所接收到的完整参数、调用函数的对象实例以及函数执行的返回值。获取运行时过程中的函数整体执行状态，就能够判断运行函数在执行过程中是否存在所关注的数据。

（3）函数执行过程中的调用栈。获取完整的函数调用栈不仅有助于进行漏洞分析与攻击分析，还有助于分析攻击者的行为。常用的一些反序列化的攻击手段都可以通过函数调用栈进行分析。

（4）应用配置信息。获取应用的各类安全配置、代码内属性配置等信息，可以完整得知该应用是否执行安全策略。



▲图3 流量代理模式



▲图4 污点数据流

通过对上述4种运行时的上下文数据进行分析和运用，RASP可实现应用运行时的自我防护。根据采用的算法或者检测逻辑，基于运行时上下文的防护逻辑包括以下4类：

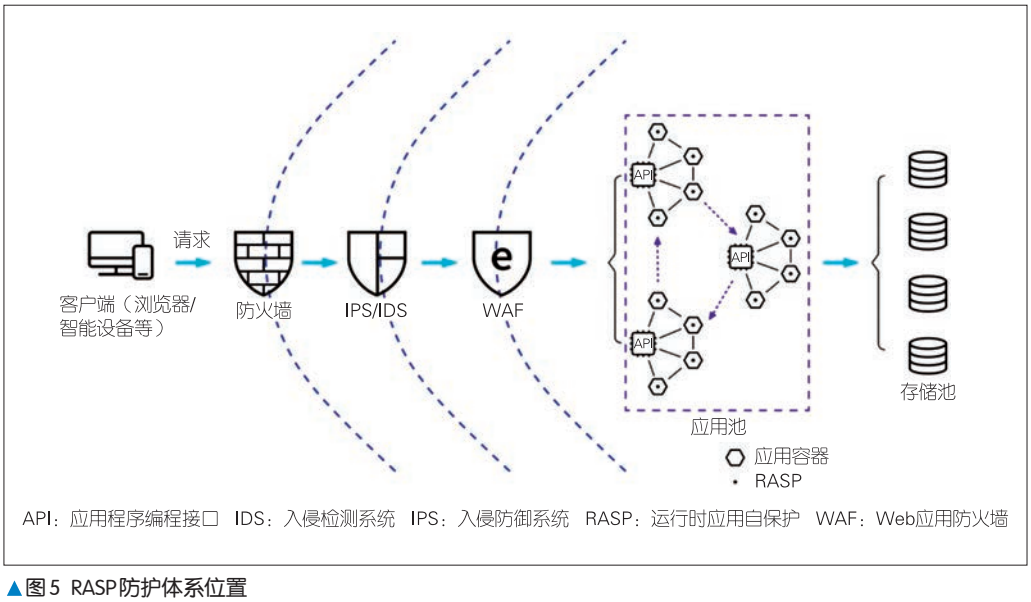
第1类是规则方式，即对获取的参数或者HTTP请求进行规则匹配。

第2类是基于词法的分析。由于RASP所获取的数据更加全面，RASP能够针对完整的输入信息（如SQL等）进行词法分析，以判断关键函数执行点上的数据是否存在异常。

第3类是行为及运行堆栈检测，该检测主要用来检测敏感函数的执行。例如，WebShell在植入系统后会通过变形等方式绕过检测，但在执行系统命令或文件操作的过程中，其必定会调用底层运行时的应用程序编程接口（API）。此时借助行为及运行堆栈分析能够获取执行调用的函数或函数调用栈信息。

第4类是应用运行配置检测，即对代码中的动态安全配置及其他配置检测。例如，当增加某些安全配置后，部分漏洞就无法被再利用了。这其中就包括预编译这类防范SQL注入的方式，以及XML外部实体注入（XXE）的关闭外部实体访问方式等。这样便能够完整地了解目前应用所存在的安全防护情况。

在整体防护体系中，RASP会与每个应用耦合，但其与WAF、IDS/IPS、防火墙等并不冲突。RASP适用于现代开发或应用架构，与应用、微服务是相伴相生的。因此，每个安全解决方案都是纵深防御体系中的一个环节。图5为RASP防护体系位置。



▲图5 RASP防护体系位置

2 代码疫苗技术在DevSecOps体系下的应用

代码疫苗技术可以应用到多个不同的场景中。相关应用场景主要分为以下4类：

（1）应对DevOps的检测防护一体化。探针是比较轻量级的，可以随流水线一同上线发布。在开发和测试环节，IAST可被用于漏洞检测。在上线后，RASP则会被开启进行漏洞防护，以实现全流程的检测防护一体化，提高DevOps的效率。

（2）红蓝对抗。在这一场景下，RASP充当高级漏洞攻击防护工具的角色。目前红蓝对抗会更多地应用0day、1day或一些未公开的漏洞利用程序（EXP）进行攻防。这对于传统的流量手段而言是难以防护的，而RASP有能力应对一些高级攻击。

（3）应对突发漏洞。RASP能够提供针对基于行为与调用栈位置威胁的检测。这可以在一定程度上缓解0day或1day攻击，为漏洞修复争取时间；也可以利用RASP提供的热补丁功能，通过一些简单配置，先进行第一波漏洞攻击的防护。

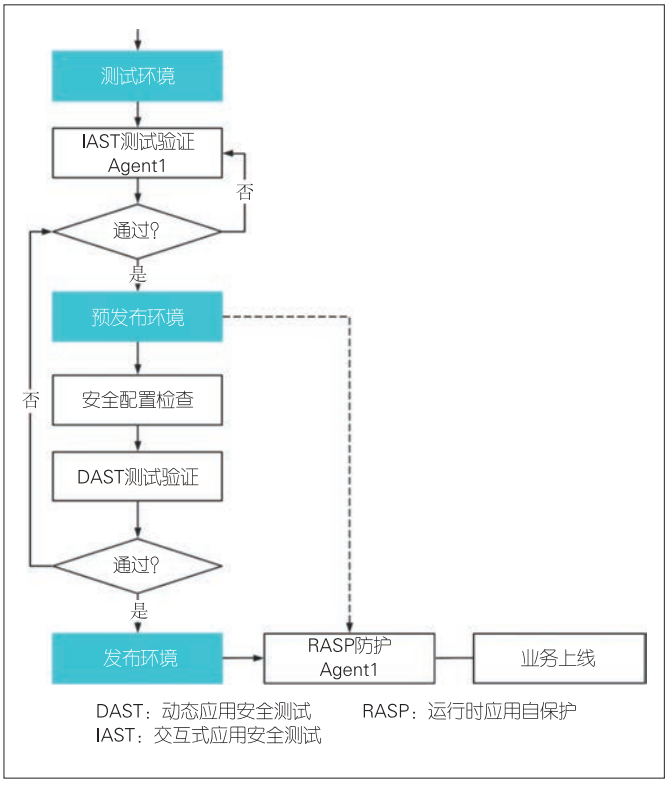
（4）应用上线的自免疫。在容器化的环境之中，将探针

和应用进行打包可使应用在上线之后能够自带攻击防护效果。

应对DevOps的检测防护一体化场景是代码疫苗技术应用最为重要的场景。代码疫苗技术实现安全工具链自动化，与DevOps的核心需求（高效和自动）高度一致。在开发流程中同步实现安全，确保应用安全上线，实现DevSecOps，不仅能为企业业务提供更加及时、可靠的服务支持，还能使企业在数字化转型中持续占据身位优势与竞争优势。代码疫苗技术与DevSecOps流水线集成流程如图6所示。系统在测试阶段采用IAST工具来检测识别漏洞，在预发布和发布阶段利用同一Agent获取的函数堆栈信息，并采用RASP技术对识别出来的漏洞进行热补丁修复，从而实现对应用程序的实时防护。

DevOps大多在容器虚拟化环境中进行软件的开发交付。IAST的安全融合可充分利用DevOps的自动化特性，在构建测试环境的同时引入代码疫苗技术插桩，即IAST和RASP的同一探针。这里我们使用修改容器配置文件（如DockerFile）的方式进行插桩。由于代码疫苗技术依赖软件的运行环境，在简单修改测试环境的环境变量或启动参数后，我们就可以应用该插桩对软件的运行时内存和数据流进行全面监控。当流水线运行到测试阶段时，软件需要进行全面的自动化功能测试，或者根据测试用例进行人工测试。对此，IAST可依托污点追踪完成软件每个功能点的安全漏洞风险和敏感数据泄露风险验证；RASP可依据同一Agent获取代码执行流程，对应用进行防护。

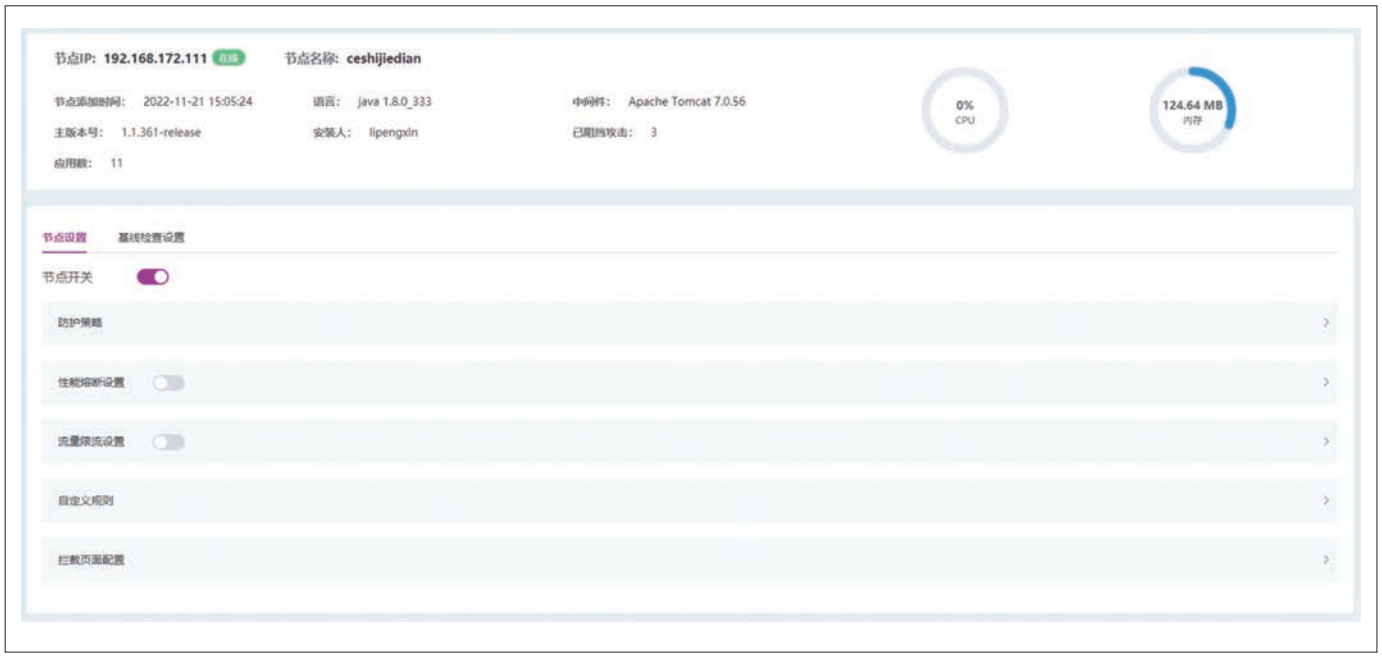
如图7和图8所示，代码疫苗技术成功应用到IAST工具和RASP工具中，在不影响企业现有开发流程的同时，实现



▲图6 代码疫苗技术与DevSecOps流水线集成流程图

了真正透明无感知的深度漏洞检测与防护。代码疫苗技术使业务和安全充分融合同时又相互解耦，使数字化业务出厂即带有默认安全能力，实现跨维检测、响应与防护，安全能力可编程、可扩展，与业务各自独立演进，让业务按照自身需求敏捷运转并进行迭代。

▲图7 代码疫苗技术应用到交互式应用安全测试工具中



▲图8 代码疫苗技术应用到运行时应用自保护工具中

3 结束语

安全工具和软件交付工具之间的技术创新差距是DevOps安全性落后的主要原因之一。IAST与RASP技术的兴起可逐渐满足DevOps的快速交付需求，有助于应对DevOps面临的安全挑战。然而，在DevOps流程中仅仅使用合适的安全工具还远远不够。将安全成功地集成到DevOps中将对安全工具的集成提出更高要求。代码疫苗技术的出现实现了IAST技术与RASP技术的集成。该技术可以将探针布控在软件生命周期的各个环节，在应用程序运行时识别并应对可能的安全风险事件，为应用搭建更加有效的内生积极防御体系。

代码疫苗技术拥有广阔的应用空间。除IAST和RASP外，代码疫苗技术还可以用来实现运行时SCA、API模糊测试、应用性能管理（APM）等工具。在未来，这一技术的应用范围会变得更加广泛，软件生命周期各阶段中不同的安全工具都将能更好地集成到一个通用的安全解决方案中，以实现真正的DevSecOps。

致谢

本文的撰写得到北京安普诺信息技术有限公司子芽、宁戈、陈超的帮助，在此表示感谢！

参考文献

[1] GoUpSec. DevSecOps自动化的九大优点 [EB/OL]. [2022-10-15]. https://www.secrss.com/articles/43793.2022-06-21
[2] 敏捷小智. DevSecOps软件研发安全实践——设计篇 [EB/OL]. [2022-10-15]. https://bbs.huaweicloud.com/blogs/349101
[3] GSA. DevSecOps Guide [EB/OL]. [2022-10-15]. https://tech. gsa. gov/guides/dev_sec_ops_guide/
[4] LIETZ S. What is DevSecOps? [EB/OL]. [2022-10-15]. https://www.devsecops.org/blog/2015/2/15/what-is-devsecops
[5] LIETZ S. Principles of DevSecOps [EB/OL]. [2022-10-15]. https://www.devsecops.org/blog/2015/2/21/Principles of DevSecOps
[6] 陈杨. 从被动防御到主动出击，网络安全的智能进化 [EB/OL]. [2022-10-15]. https://baijiahao.baidu.com/s?id=1680323118631685292.2020-10-12
[7] 宁戈. 内生安全免疫，代码疫苗关键技术剖析 [EB/OL]. [2022-10-15]. https://baijiahao.baidu.com/s?id=1733885397350294816.2022-05-26
[8] 廖翰晖. 浅谈在DevSecOps流程中融合RASP安全防护 [EB/OL]. [2022-10-15]. https://view.inews.qq.com/a/20220216A06XDX00.2022-02-16
[9] DOD Enterprise DevSecOps Strategy Guide [EB/OL]. [2022-10-15]. https://dodcio. defense. gov/Portals/0/Documents/Library/DoD% 20Enterprise% 20DevSecOps% 20Strategy% 20Guide_DoD-CIO_20211019. pdf. 2021-10-19.
[10] 阿里云云原生. Apache Log4j2, RASP防御优势及原理 [EB/OL]. [2022-10-15]. https://developer.aliyun.com/article/836012.2021-12-17

作 者 简 介

董毅，北京安普诺信息技术有限公司COO；全面负责公司运营中心的管理工作，拥有超过10年的网络安全产品设计、研发及运营管理全栈经验，对网络安全行业有深刻的洞察和理解；主导撰写《DevSecOps行业洞察报告》《软件供应链安全治理与运营白皮书》《软件供应链安全白皮书》等，拥有多项发明专利。

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。

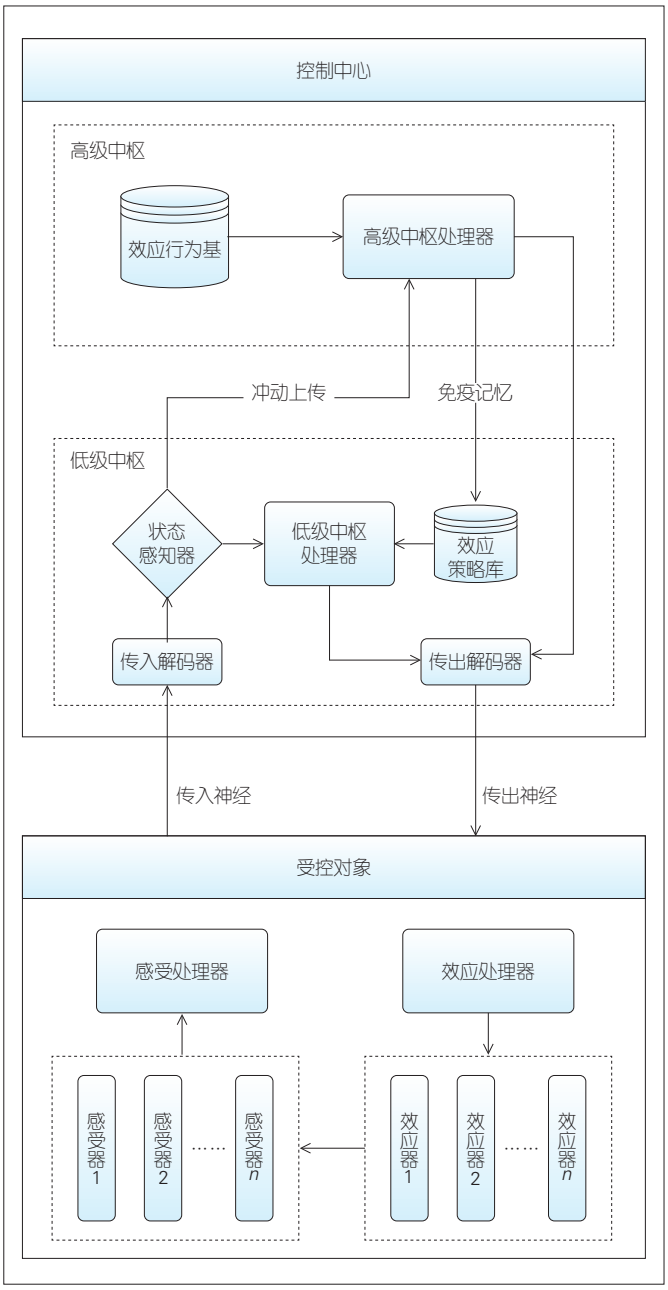
（3） 神经系统的体系架构实现了信息感知分布性、控制适应性、整体协调性，在架构设计方面为安全体系与信息系统的融合提供参考，有助于构建具有智能监控、快速响应、主动防御特点的仿生免疫系统。

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。

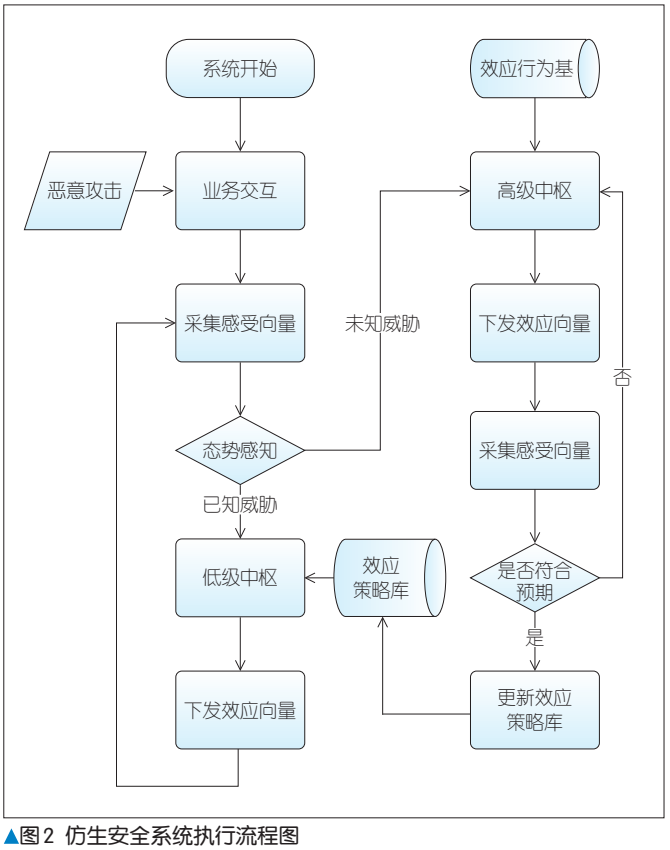
（a）在高级中枢接收到由低级中枢上传的异常状态数据后，异常分析模块会对感受器采集的状态参数进行分析，以寻找异常状态参数之间的关联，推断系统异常根源。

（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

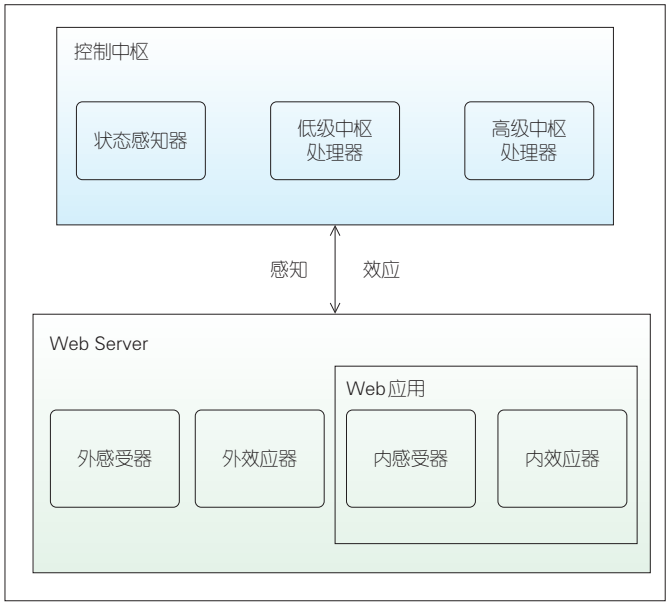
4.1 原型系统实现

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。

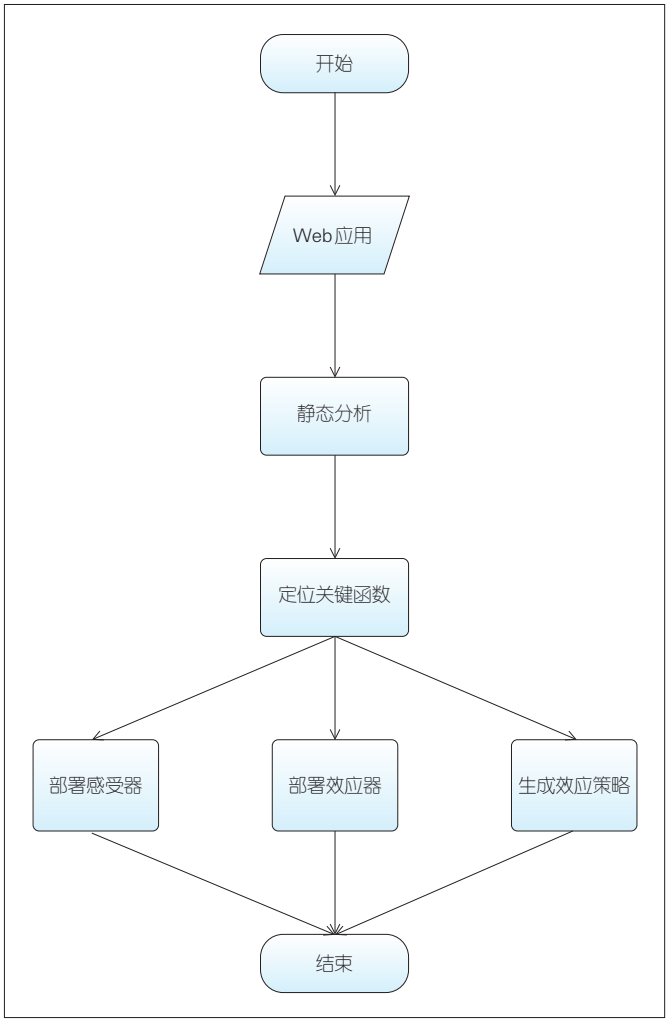
（1）受控对象层面

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。



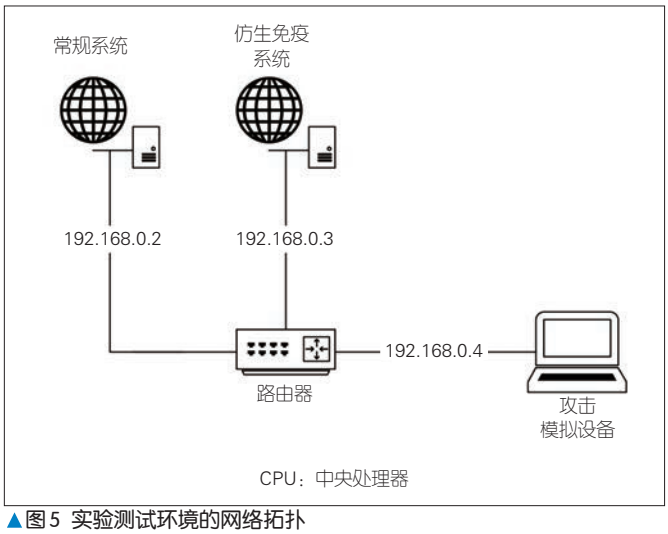
▲图3 仿生免疫系统框架



▲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。

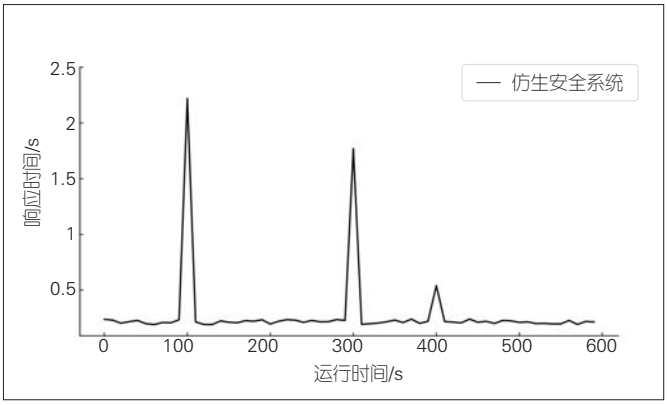
压力测试过程中，仿生安全系统的业务功能响应时间变化如图6所示。从图中可以看出，当系统遭受未知攻击并处于异常状态时，控制中心的效应策略存在调整优化过程。此过程中系统的业务功能会受到攻击的影响。当效应策略行而有效时，高级中枢会将其下放到效应策略库中，以便当再次面对此攻击时，能够更快速地采取正确的效应措施，保证系统的稳态运转。

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。

网络空间拟态防御建模与量化评估技术研究

Modeling and Quantitative Evaluation of Cyberspace Mimic Defense

马海龙/MA Hailong，任权/REN Quan，伊鹏/YI Peng
（中国人民解放军战略支援部队信息工程大学，中国 郑州 450001）
(Information Engineering University, Zhengzhou 450001, China)

DOI：10.12142/ZTETJ.202206010
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221221.1450.005.html
网络出版日期：2022-12-23
收稿日期：2022-10-17

摘要：针对网络空间未知漏洞后门等不确定性扰动问题，拟态防御技术基于动态异构冗余架构与拟态伪装机制实现了对随机或非随机扰动的有效管控。针对上述内生安全问题，首先采用Petri网、鞅以及概率论等理论与技术来评估与仿真系统的安全性，并对评估结果与实际部署进行了策略分析，同时对比了不同理论工具在量化可用性、攻击成功概率以及逃逸概率等指标时存在的优缺点。最后，针对现有理论与技术在不同场景适用性存在的不足以及实际部署量化问题，展望了后续拟态防御系统在定性与定量分析研究的主要方向。

关键词：网络空间内生安全；拟态构造；建模方法；评估

Abstract: For uncertain disturbances such as unknown vulnerabilities and backdoors in cyberspace, the mimic defense technology realizes effective control of random or non-random disturbances based on dynamic heterogeneous redundancy architecture and mimicry camouflage mechanism. For the above endogenous security problems, the Petri nets, martingales, probability theory, and other theories and technologies are used to evaluate and simulate the security of the system, and the evaluation results and actual deployment strategies are analyzed. At the same time, the advantages and disadvantages of different theoretical tools are compared in quantifying availability, attack success probability, escape probability, and other indicators. Finally, in view of the shortcomings of the applicability of the existing theories and technologies in different scenarios and the quantitative problems of the practical deployment, the main direction of the subsequent mimicry defense system in qualitative and quantitative analysis is discussed.

Keywords: cyberspace endogenous security; mimic structure; modeling methods; evaluation

随着信息化和工业化的高度融合，各类信息安全事件层出不穷，网络空间安全问题成为信息时代日益严峻的挑战[1]。为了应对各类网络安全事件，传统的网络防御是在系统上，通过防火墙、恶意检测等附加式防御手段来提高系统的抗攻击能力。尽管上述防护技术能在一定程度上减少网络攻击造成的危害，但逐年递增的网络安全事件却表明现有网络安全防御架构难以应对基于未知的漏洞后门发动的未知攻击，总体表现为：工程技术手段的局限性，任何软硬件厂家都无法确保网络设备中不存在任何设计缺陷；在全球开放式产业链条件下，任何厂商都不能确保生产链等环节未被蓄意植入后门；开源模式已经成为技术开发的主流趋势，现有的科技理论和方法尚不能彻查系统中的漏洞与后门；修补式的被动网络防御策略难以应对日新月异的网络攻击方法[2]。

为改变网络空间攻防不对称性的格局，提高网络系统应对攻击的能力，网络空间拟态防御[3]被提议作为网络安全“改变游戏规则”的研究主题之一。拟态防御技术是通过动态异构冗余构造与拟态伪装机制来规避网络空间广义不确定性扰动问题。2008年，邬江兴教授受生物界拟态现象启发，提出了“结构决定效能”的拟态计算，又从“结构决定功能与安全”思路入手，将动态异构冗余架构与广义鲁棒控制机制融合，创立拟态防御理论体系，逐步开辟了网络空间拟态防御（CMD）研究方向，期望通过架构设计赋予信息系统内生安全能力。内生安全是指借助系统本身的构造、机制、运行场景以及规律等内部属性，达成的安全功能或属性。拟态防御是基于功能等价的多个执行单元，以提供目标环境的动态性、非确定性、异构性、非持续性为目的，动态地构建网络、平台、环境、软件、数据等多样化的拟态环境。拟态防御基于动态异构冗余架构与拟态伪装机制实现了将随机或

基金项目：国家自然科学基金资助项目（61872382）

非随机扰动转化为概率可控的可靠性事件。

因此，本文将对网络空间拟态防御理论与技术发展展开研究，主要贡献包括：（1）对网络空间内生安全问题进行阐述，针对该问题探讨了现有防御架构存在的问题；（2）介绍拟态防御系统的基本要素与关键技术；（3）给出了现有拟态防御理论的系统建模方法，对比分析了不同模型的适用场景；（4）对拟态防御理论方向研究进行展望。

1 问题提出与解决

1.1 内生安全问题

“矛盾存在于一切事物之中，矛盾双方在一定条件下可以转化”。在信息网络空间中，如果一个软硬件实体的暗功能和副作用能被某种因素触发而影响到实体服务功能的可信性，这些副作用和暗功能则被称为“内生安全”问题[3]，即系统内部本征功能的内在性矛盾。以典型技术为例，大数据技术能够根据算法和数据样本发现未知的规律或特征，而被人为污染的数据样本以及恶意利用的算法缺陷同样可使人误解，结果的不可解释性是其内生安全问题。区块链技术采用了大于等于51%的共识机制，该机制却不能避免市场占有率大于51%的商用级产品中的漏洞后门问题。这是区块链1.0时代的内生安全问题。当前，计算技术的快速发展使人类步入了辉煌的信息时代，但计算技术本身的缺陷也使得网络空间充满了不确定性。因此，本文所提的内生安全问题主要是指网络空间各类信息服务功能实体中存在的未知漏洞后门等问题。显然，该类问题是系统内部本征功能所衍生出的副作用或暗功能，是伴随本征功能产生和发展的，因此无法从根本上彻查或者消除。

1.2 解决思路

从哲学原理上说，内生安全问题不可能彻底消除，只能在时空约束前提下实现条件规避或危害控制。传统的网络安全思维模式和技术路线主要采取挖漏洞、打补丁、查毒杀马或是设蜜罐、布沙箱等堆叠的附加式防护手段。该方式在引入安全功能的同时会不可避免地引入新的内生安全问题。内生安全问题源自系统结构本身，那么在功能等价条件下变换系统结构本身无疑能成为内生安全问题的解决之道。

2 拟态防御架构

动态异构冗余（DHR）架构以非相似余度架构为基础，融合了多模表决与策略裁决、负反馈控制策略、多维动态重构机制三大核心机理，实现了将广义不确定扰动管控在有效范围之内，从而确保DHR架构相对攻击方具有“熵不减”的广义鲁棒控制能力。

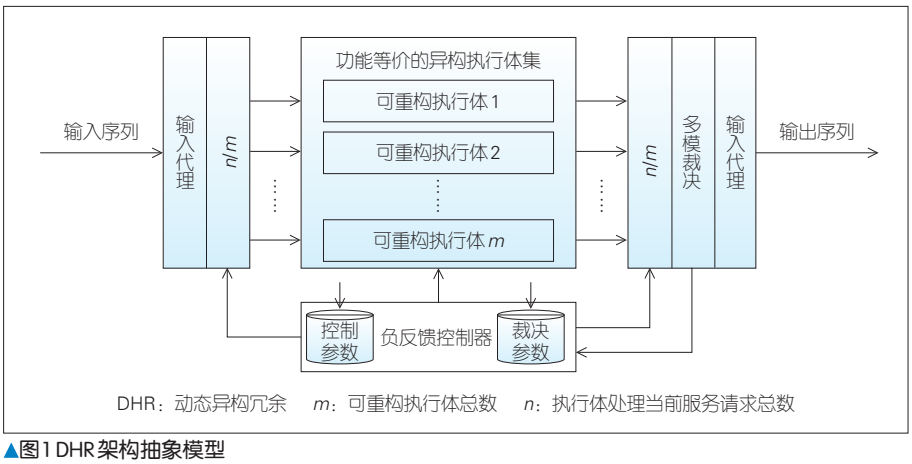
DHR架构抽象模型如图1所示，主要包括输入输出代理、功能等价的可重构执行体集、输出裁决模块以及负反馈控制器。输入代理模块负责接收负反馈控制器的指令，并将输入请求复制、分发到多个功能等价的可重构异构体；功能等价异构执行体集合中的可重构执行体能独立完成指定功能属大概率事件；输出裁决模块策略选取合适算法判决输出矢量，并将满足要求的输出响应转发给输出代理，若裁决结果不一致或未达要求则激活负反馈控制器；负反馈控制器通常会依据自身策略主动激活或受裁决结果被动激活，反馈控制器被激活后会依据控制参数和裁决参数执行功能等价的重组/重构/重配等操作。

3 拟态防御理论系统建模

拟态防御基于DHR架构与拟态伪装机制，将攻击造成的随机或非随机扰动转化为概率可控的可靠性事件，这使得定量分析架构的抗攻击能力成为可能。本节中，针对现有系统可用概率、攻击成功概率等通用指标，以及拟态构造特有逃逸概率指标，我们探讨拟态防御模型的抗攻击性。抗攻击性是系统在受到外部攻击出现不可见故障时，连续提供有效服务并在规定时间内恢复所有服务的能力。关于抗攻击性模型的假设与定义如下：

假设1：目标系统是3余度DHR系统，执行体中不包括入侵检测、防火墙等特异性感知和防御手段；

假设2：通过拟态裁决机制可以发现输出矢量与多数执



▲图1 DHR架构抽象模型

行体不同的情况，并能够对其进行包括动态重构等在内的恢复操作；

假设3：对于拟态裁决机制未能发现的错误，系统仍然能以一定的概率进行定期或不定期恢复。

定义1：可用概率。系统处于正常服务状态的概率。在3余度拟态防御系统中，可用概率是指系统全部执行体处于漏洞休眠状态或单个执行体处于故障状态的概率。

定义2：逃逸概率。攻击方通过协同多个执行体使输出结果出现一致错误，从而实现判决逃逸。

定义3：攻击成功概率。攻击成功执行的概率，如系统组件（或防御者）被破坏导致出错或目标被攻击者成功访问的概率。

下面我们主要针对集中式与分布式裁决场景、随机与非随机攻击场景对3个模型进行阐述。

3.1 基于广义随机Petri网的拟态构造评估模型

19世纪60年代，德国学者C. A. PETRI提出了Petri网的概念。Petri网适用于在逻辑层次上对事件离散的动态系统进行建模和分析。Petri网可用来描述系统中进程或部件的顺序、并发、冲突以及同步等关系。为了准确地描述整个拟态防御系统的结构、不同攻击扰动与拟态系统动态重构与负反馈控制防御特性，文献[4]和[5]以3余度动态异构冗余系统为例，依据拟态系统针对不同扰动表现出不同的行为，建立包括24个状态、42个变迁的广义随机Petri网（GSPN）模型（具体如图2所示）。

拟态构造扰动异常情况下的GSPN模型：

$$GSPN=(S,T,F,K,W,M_0,\Lambda), \tag{1}$$

其中，库所$S=\{P_1,P_2,\cdots,P_{24}\}$表示系统中状态元素的集合，变迁$T=\{T_1,T_2,\cdots,T_{42}\}$表示系统中状态迁移集合，$F$为模型中库所与变迁之间的有向弧集合，$W$是弧的权重集合，各弧的权重为1，$K=\{1,1,1,0,\cdots,0\}$定义了$S$中各元素的容量，状态标识$M=\{M_0,M_1,\cdots,M_{12}\}$。其中$M_0=\{1,1,1,0,\cdots,0\}$定义了模型的初始状态，$\Lambda=\{\lambda_1,\lambda_2,\cdots,\lambda_{15}\}$定义了与时间变迁相关联的平均实施速率集合。

设i，j表示马尔科夫链中任意实存状态，$i,j\in M_T$，r,s表示马尔科夫链中任意消失状态，$r,s\in M_v$。系统实存状态之间的转移概率矩阵为：

$$u_{ij}=f_{ij}+\sum_{r\in M_v}P_r\{r\to j\}, \tag{2}$$

其中，f_{ij}表示实存状态间的转移概率，$P_r\{r\to j\}$表示沿着一条全部由消失状态构成的中间状态的路径，从消失状态r转移到实存状态j的概率。其中，路径可以包括任意步数。

由马尔可夫链的转移概率建立转移速率矩阵如下：

$$q_{ij}=\begin{cases}\lim\limits_{\Delta t\to 0}\dfrac{u_{ij}(\Delta t)}{\Delta t}, i\neq j\\ \lim\limits_{\Delta t\to 0}\dfrac{u_{ij}(\Delta t)-1}{\Delta t}, i=j\end{cases}, \tag{3}$$

q_{ij}为由实存状态M_i到实存状态M_j的转移速率，其中$i,j\in[1,l],l=M_T$。Q矩阵是以q_{ij}为元素的转移速率矩阵。概率向量$P(t)=(P_1(t),P_2(t),\cdots,P_i(t),\cdots,P_l(t))$，其中$P_i(t)$为系统处于实存状态$M_i$的瞬时概率，则有微分方程（4）成立：

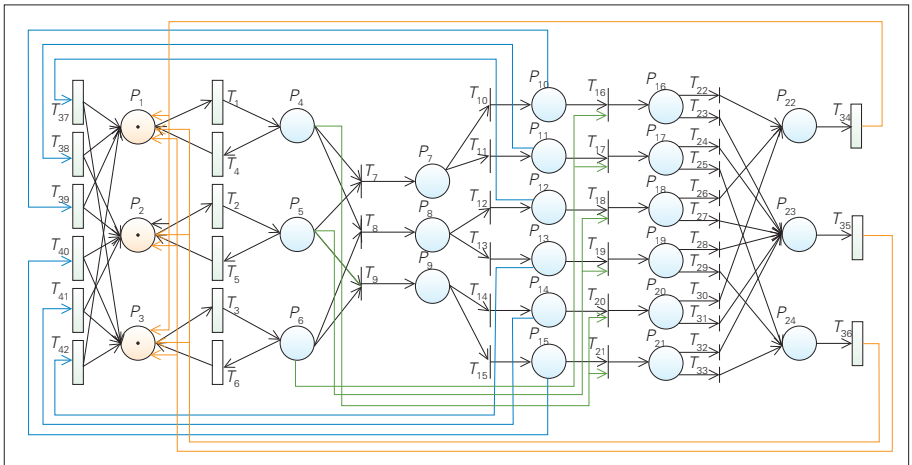
$$\begin{cases}P'(t)=P(t)Q\\ P(0)=(P_1(0),P_2(0),\cdots,P_l(0))。\end{cases} \tag{4}$$

通过上述方程组可求解可达标识的可用概率和逃逸概率。

文献[4]给出了各种防御策略所对应的安全性指标，因此可针对不同安全需求采用不同策略部署与系统构建来实现。

3.2 融合鞅与GSPN的二维拟态构造评估模型

拟态防御系统在联合判决和重配置过程中带来的资源消耗将大幅增加防御成本。存在判决时延的分布式拟态系统亟



▲图2 拟态构造扰动异常GSPN模型

需一种分析系统安全性的方法。文献[6]在单节点攻击层，根据博弈论思想对攻击者和防御者的行为分别建立模型，利用广义随机PN描述攻防动作对系统的影响，进而分析系统的安全性。在链路攻击层，使用马尔科夫链来刻画攻击者在链路中的位置变化，并结合随机过程的鞅理论，计算出攻击难度和网络配置间的量化关系。

假定攻击单个节点成功的概率为μ，攻击链的节点总数为Θ，节点被随机扰动的概率为ω。假设当前时刻攻击者停留在第k个节点，即已攻击成功k个节点，则攻击转移如图3。

定理1：构建一个随机序列$M_0,M_1,M_2,\cdots,M_n$，其中，$M_i=X_i-[(1-\omega)\mu-\omega]*i$，则$M_n$序列是关于$X_0,X_1,X_2,\cdots,X_n$的鞅。

为了求解攻击Θ步到达目标节点的步数，我们引入了鞅停时定理。在随机过程中，停时被定义为具有某种与将来无关性质的随机时刻。鞅停时满足：

（1）$P\{S<\infty\}=1$；

（2）$E[|M_S|]<\infty$；

（3）$\lim\limits_{n\to\infty}E[|M_S|I_{\{S>n\}}]=0$。

则有：

$$E[M_S]=E[M_0]。\tag{5}$$

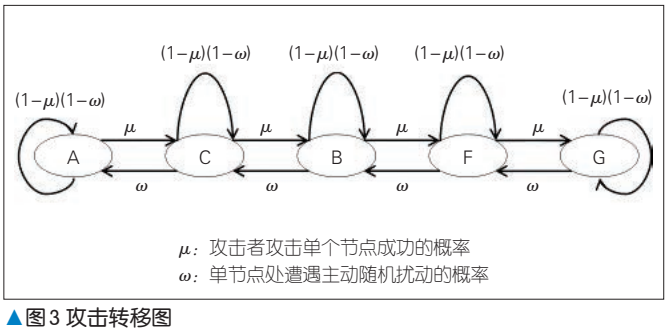
定理2：对于一条长度为Θ个节点的攻击链，如果攻击者攻击单个节点成功的概率为μ，单节点处遭遇主动随机扰动的概率为ω，那么攻击者成功攻击目标节点（即Θ点）需要的步数期望为：

$$E[S]=\frac{\theta}{(1-\omega)\mu-\omega}。\tag{6}$$

下面我们计算到达Θ点的步数期望。根据停时定理得：$E[M_S]=E[M_0]=E[X_0]=0$，

$$E[M_S]=E[X_S-[(1-\omega)\mu-\omega]S]=E[X_S]-[(1-\omega)\mu-\omega]E[S]。\tag{7}$$

又因为$E[X_S]=\Theta$，所以等式（6）成立。



▲图3 攻击转移图

根据上文，运算得到的攻击逃逸的稳态概率即为下一部分马尔科夫链的下行概率，攻击成功概率即为马尔科夫链的上行概率，即：$\mu=P(P_E)$，$\omega=\lambda(T_{E0})$。

该模型给出了二维拟态构造评估模型，在实际部署过程中可以通过改善动态清洗与重构能力来增大修复速率，通过改善节点品质等因素来改变单个节点的攻击成功概率[7-10]。

3.3 基于概率论与数理统计的拟态构造评估模型

针对系统的未知安全防范，大多数安全评估模型首先基于随机性攻击假设，进而基于攻击路径和漏洞分析方法来量化攻击难度。尽管这类攻击模型能有效反映攻防双方在随机条件下的博弈策略，但缺乏针对系统整体安全的有效性证明，即从理论上论证在一定的攻击条件，存在一种防御方案可保证任意小的系统差错概率。

文献[7]给出了一种证明方法，针对非随机扰动且执行体有记忆情况，DHR架构引入了反馈函数$f(t)$，在部署差模异构执行体（即在共模同构率ω可忽略）后，拟态构造执行体出错概率：

$$\forall t>0,P_e^i(t)\in[0,\max\{\frac{\lambda_{i+1}}{\lambda_{i+1}+\mu_{i+1}}(1-e^{-(\lambda_{i+1}+\mu_{i+1})T'_{i+1}}),e^{-\mu_{i+1}T'_{i+1}}\}]<1。\tag{8}$$

由此可见，执行体出错概率值随时间递增并处于与时刻T_{i+1}相关的确定范围（T_{i+1}在非随机扰动条件下为确定值），即执行体在DHR架构中出错概率$P_e^i(t)$随时间变化不趋于1。当引入反馈可控消记忆动作$f(t)$后，DHR构造信道容量C将处于防御方可控范围$[C_s,C_0]$。若非随机扰动到达与动态反馈修复时间服从负指数分布，那么整个DHR构造信道有可控的稳态分布。DHR构造信道稳态信道容量为C_s，初始信道容量为C_0，执行体i稳态信道容量记作C_s^i。

我们设DHR构造信道在t时刻的输入请求为$\boldsymbol{x}(t)$，$\boldsymbol{x}(t)\in X^n$，$\boldsymbol{x}(t)=(x_1(t),x_2(t),\cdots,x_n(t))$，输出响应为$\boldsymbol{y}(\boldsymbol{x}(t))\in Y^n$，$\boldsymbol{y}(\boldsymbol{x}(t))=(y_1(x_1(t)),y_2(x_2(t)),\cdots,y_n(x_n(t)))$。从编码空间$X^n$中随机选取$M=2^{nR(t)}$个编码序列作为请求发送，设$X$中所有元素以独立、等概率形式出现，那么就可以满足随机编码条件。给定与时刻t对应的输出响应$\boldsymbol{y}(\boldsymbol{x}(t))$，若存在唯一的$k\in[1,2^{nR(t)}]$，则有：

$$(\boldsymbol{x}_k(t),\boldsymbol{y}(\boldsymbol{x}(t)))\in T_{XY}(n,\varepsilon)。\tag{9}$$

$\boldsymbol{y}(\boldsymbol{x}(t))$判决为$\boldsymbol{x}_k(t)$，即$F(\boldsymbol{y}(\boldsymbol{x}(t)))=\boldsymbol{x}_k(t)$。其中，$T_{XY}(n,\varepsilon)$表示输入输出序列对$(\boldsymbol{x}(t),\boldsymbol{y}(\boldsymbol{x}(t)))$是联合$\varepsilon$典型序列。

若发送请求为$\boldsymbol{x}_m(t)$，响应序列为$\boldsymbol{y}(\boldsymbol{x}_m(t))$，则判决出错概率为：

$$P_{em}=P(\boldsymbol{x}_k(t)\neq\boldsymbol{x}_m(t)|\boldsymbol{y}(\boldsymbol{x}_m(t)))。\tag{10}$$

我们设发送端的第一个请求消息为$\boldsymbol{x}_1(t)$，令事件：

$$E_m(t)=\{(\boldsymbol{x}_m(t),\boldsymbol{y}(\boldsymbol{x}_m(t)))\in T_{XY}(n,\varepsilon)\},m\in[1,2^{nR(t)}]。\tag{11}$$

于是，判决出错可分为两种情况：

（1）发送编码序列$\boldsymbol{x}_1(t)$与响应序列$\boldsymbol{y}(\boldsymbol{x}_1(t))$不构成联合$\varepsilon$典型序列，令事件为$E_1^C(t)$；

（2）编码序列$\boldsymbol{x}_k(t),k\neq1$与响应序列$\boldsymbol{y}(\boldsymbol{x}_1(t))$构成联合$\varepsilon$典型序列，令事件为$E_k(t)$。

于是则有攻击成功概率：

$$P_e(t)=P(E_1^C(t)\cup E_2(t)\cdots\cup E_M(t))\leqslant P(E_1^C(t))+\sum_{k=2}^{M}P(E_k(t))。\tag{12}$$

第1部分攻击成功概率：

$$P(E_1^C(t))=1-P(E_1(t))\leqslant\varepsilon。\tag{13}$$

第2部分攻击成功概率：

$$\sum_{k\neq1}P(E_k(t))\leqslant2^{n[R(t)-C(t)+3\varepsilon]}。\tag{14}$$

我们取t时刻的DHR构造信道容量$C(t)=\min\{C_s^1,C_s^2,\cdots C_s^n\}$，于是：

$$\forall\eta=3\varepsilon>0,R(t)<C(t)-\eta,n\to\infty,\tag{15}$$

那么：

$$\sum_{k\neq1}P(E_k(t))\to0,$$

$$P_e(t)\leqslant\varepsilon,\tag{16}$$

即攻击成功概率$P_e(t)$为任意小。

该模型给出了内生安全构造具有任意小安全需求的存在性证明。在实际部署过程中，我们可通过编码与冗余度设计、执行体扰动消除以及反馈控制构造等来尽可能地接近该模型求解结果。

3.4 评估指标分析

表1比较了上述3个模型的优缺点。当前，拟态防御理论模型主要针对集中式与分布式裁决、扰动随机与非随机场景进行量化评估。GSPN模型在面向集中判决场景时能通过多个量化指标可以有效评估系统的抗攻击能力。然而，在面向分布式场景时，该模型需要进一步完善。文献[7]所提的模型则是通过优化资源与构造来仿真系统攻击可用性，该方法同样在一定余度与随机性攻击扰动条件下进行的。针对分布式裁决系统，文献[8]建立了融合鞅与GSPN的系统安全评估方法，该方法对裁决延时判决问题进行了进一步研究。针对基于拟态防御的云科学计算流，文献[9]提出了一种攻击评估模型。上述的可用性与攻击成功概率指标模型相关研究存在两方面不足：一方面，GSPN模型在执行体数量增多时会出现指数爆炸问题；另一方面，上述模型均是在攻击随机到达的情况下分析的系统安全性。在逃逸概率指标方面，文献[4]在GSPN模型的基础上提出用大系统拆分成小系统的方案来解决状态爆炸问题，从而实现逃逸概率的一般性求解。针对攻击非随机到达展开建模，文献[10]量化分析了拟态构造将非随机攻击转化为随机可靠性事件，从而借助概率论与数理统计方法对余度足够大的情况进行探讨，实现了对拟态构造安全的有效性论证。该论证过程主要以攻击成功概率指标进行推理，简化了攻防细节。由于文献[4]和[10]对攻击扰动与防御动作特性进行了整合与抽象，简化了量化指标。

因此，上述模型均能有效量化评估系统抗攻击能力，所

▼表1 现有拟态防御理论量化评估模型的优缺点

指标	优点	缺点
可用性	基于GSPN模型，文献[5]和[7]准确地描述拟态防御系统结构、不同攻击扰动与负反馈控制防御特性，量化分析攻击可用性和感知安全性；文献[8]提出一种感知调度算法与失效概率最小化模型来保证系统可用性最大化。	仅考虑扰动随机表现形式，均未分析非随机扰动情况；GSPN在多余度架构下状态复杂，抗攻击性评估也将异常复杂；失效概率最小化模型则是在一定余度下进行仿真分析，未考虑一般性。
攻击成功概率	针对存在判决时延的分布式拟态系统，文献[6]提出一种基于鞅与GSPN的系统安全评估方法，量化分析攻击扰动概率和逃逸概率。针对拟态构造的云科学计算流；文献[9]提出了一种攻击评估模型，能有效反应攻击次数与攻击成功率的关系。	仅考虑了扰动随机表现形式，且现有模型对多余度系统架构下的抗攻击性分析同样难以适用。
逃逸概率	针对大余度拟态防御系统提出了组合模型，文献[4]可将大规模复杂系统拆分成多个子系统，再对整个系统采用GSPN理论进行一般性求解；文献[10]基于概率论与数理统计方法，论证了系统整体的安全性，该论证具有一般性，适用多余度与非随机攻击场景。	通过组合子系统GSPN模型来建立系统整体模型，可以实现逃逸概率分析，但难以覆盖任意余度，因此具有一定局限性；概率与数理统计模型则是针对攻防动作特性进行整合与抽象，对安全防御有效性进行一般论证，简化了量化指标。

GSPN：广义随机Petri网

提数学模型在解决各自场景问题时均表现出一定的优越性。同时，现有的模型在应对不同拟态场景时仍有待进一步优化，如GSPN模型在面临大余度分布式网络场景[11]时如何量化分析，针对不同场景的非随机攻击评估量化指标如何选取等。此外，现有模型在针对异构性[12]量化评估方面仍存在不足，有待进一步研究。因此，后续拟态防御理论的发展将会进一步面向系统异构性与共模扰动的量化、面向系统裁决与异构归一化的量化、面向负反馈控制的动态重构与清洗策略制定等方面，从而有效解决拟态防御理论与实际部署结合存在的难题[12]。

4 结束语

作为未知漏洞后门等不确定性威胁的解决方案，网络空间拟态防御得到广泛应用。文章中，我们研究了网络空间拟态防御理论模型，阐述了网络空间内生安全以及现有防御架构所存在的问题，并指出了拟态防御系统的基本要素与关键技术。同时，我们对3种典型的建模方法进行了比较分析。随着拟态防御技术与各类技术的融合，拟态防御理论存在的挑战也逐步彰显，如拟态防御理论在攻防对抗定性分析方面有待完善；在网络通信理论方面如何研究基于概率论与数理统计的拟态构造安全可控性；对拟态构造的防御极限进行量化评估；如何研究拟态构造执行体的信息并行处理方式，构造高容量的执行体，减少裁决时延，实现高效的处理能力等。在网络计算理论方面，如何研究网络信息处理过程中存储、计算与控制单元存在的内生安全问题，并从整体上量化分析网络计算的安全可控性。因此，拟态防御的发展仍需大力推进理论与技术创新。

参考文献

[1] CONTEH N Y, SCHMICK P J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks [J]. International journal of advanced computer research, 2016, 6(23): 31–38. DOI: 10.19101/ijacr.2016.623006

[2] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense [M]. Springer, New York, 2012

[3] 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

[4] 任权, 邬江兴, 贺磊. 基于GSPN的拟态DNS构造策略研究 [J]. 信息安全学报, 2019, 4(2): 37–52. DOI: 10.19363/J.cnki.cn10–1380/tn.2019.03.05

[5] REN Q, WU J X, HE L. Performance modeling based on GSPN for cyberspace mimic DNS [J]. Chinese journal of electronics, 2020, 29(4): 738–749. DOI: 10.1049/cje.2020.05.001

[6] 杨昕, 李挥, 邬江兴, 等. 融合广义随机Petri网的二维拟态安全评估模型 [J]. 中国科学: 信息科学, 2020, 50(12): 1944–1960

[7] REN Q, HU T, WU J, et al. Multipath resilient routing for endogenous secure software defined networks [J]. Computer networks, 2021, 194(2): 108134

[8] QI C, WU J X, CHENG G Z, et al. An aware–scheduling security architecture with priority–equal multi–controller for SDN [J]. China communications, 2017, 14(9): 144–154. DOI: 10.1109/CC.2017.8068772

[9] WANG Y W, WU J X, GUO Y F, et al. Scientific workflow execution system based on mimic defense in the cloud environment [J]. Frontiers of information technology & electronic engineering, 2018, 19(12): 1522–1536. DOI: 10.1631/FITEE.1800621

[10] 邬江兴. 网络空间内生安全: 拟态防御与广义鲁棒控制(下册) [M]. 北京: 科学出版社, 2020

[11] REN Q, GUO Z H, WU J X, et al. SDN–ESRC: a secure and resilient control plane for software–defined networks [J]. IEEE transactions on network and service management, 2022, 19(3): 2366–2381. DOI: 10.1109/TNSM.2022.3163198

[12] TONG Q, GUO Y F. A comprehensive evaluation of diversity systems based on mimic defense [J]. Science China information sciences, 2021, 64 (12): 1–2. DOI: 10.1007/s11432–020–3008–1

作 者 简 介

马海龙，中国人民解放军战略支援部队信息工程大学副研究员；主要研究领域为网络空间内生安全与智能威胁感知；先后主持和参加国家重点研发计划和自然基金项目10余项，获得6项科技进步奖；已发表论文40余篇，出版专著2部，授权专利10项。

任权，中国人民解放军战略支援部队信息工程大学助理研究员；主要研究领域为软件定义网络与网络内生安全架构。

伊鹏，中国人民解放军战略支援部队信息工程大学研究员；主要研究领域为网络空间内生安全与多模态网络。

安全平行切面:面向企业数字生命体的安全基础设施

Aspect-Oriented Security: Security Infrastructure for Enterprises as Digital Lifeforms

韦韬/WEI Tao,顾为群/GU Weiqun,刘宇江/LIU Yujiang
(蚂蚁集团,中国 杭州 310013)
(Ant Group, Hangzhou 310013, China)

DOI:10.12142/ZTETJ.202206011
网络出版地址:https://kns.cnki.net/kcms/detail//34.1228.TN.20221209.1058.003.html
网络出版日期:2022-12-10
收稿日期:2022-10-16

摘要: 现代数字化企业是一种不断演变进化的生命体。它的架构复杂性会爆炸性增长,不断引入的外部数字化产品服务和行业技术体系演化,会推动其形成内部数字化基因的代差积累。为了应对严峻的网络安全攻击威胁,符合严格的数据安全合规要求,保障企业数字生命体的健康发展,现代企业安全基础设施必须更加适应这种动态复杂性。阐述了安全平行切面,其核心思路是把安全能力融入企业基础设施中并与业务解耦,使安全能力深入业务逻辑,同时实现双方的独立高速发展,在更高维度上实现持续的动态安全防护。

关键词: 安全平行切面;内生安全;原生安全;企业安全架构;企业数字生命体

Abstract: A modern digital enterprise is a living organism that is constantly evolving. The complexity of its architecture will grow explosively, and the continuous introduction of external digital products and services and the evolution of industrial technologies will promote the accumulation of internal digital genes. In order to deal with severe threats of network security attacks, comply with strict data security compliance requirements, and ensure the healthy development of enterprise digital lifeforms, modern enterprise security infrastructure must be more adaptable to this dynamic complexity. The aspect-oriented security is described. The core idea is to integrate security capabilities into enterprise infrastructure and decouple them from business, so that security capabilities can penetrate into business logic, and at the same time both parties can achieve independent and rapid development, and ensure continuous dynamic security in a higher dimension.

Keywords: aspect-oriented security; endogenous security; security-native; enterprise security architecture; enterprise as digital lifeforms

随着“十四五”规划的发布,中国正式提出“加快建设数字经济、数字社会、数字政府,以数字化转型整体驱动生产方式、生活方式和治理方式变革”的发展目标。这标志着中国“加快数字化发展,建设数字中国”的目标正式启航。习近平总书记指出,没有网络安全就没有国家安全,就没有经济社会稳定运行,广大人民群众利益也难以得到保障。当今世界,以互联网为代表的新兴技术日新月异,对人类社会的发展进程产生深刻影响。同时,网络安全问题也相伴而生。世界范围内的个人隐私侵犯、知识产权侵犯、网络犯罪等时有发生,网络监听、网络攻击、网络恐怖主义活动等成为全球公害。网络安全已经成为中国面临的最复杂、最现实、最严峻的非传统安全问题之一。网络安全是经济与社会发展的基础保障。如何通过创新架构、创新理念和创新技术等方式突破现有困境,成为当前网络和信息安全建设的重要工作。

安全架构是网络和信息安全建设成果的重要体现。虽然近几年零信任、纵深防御、网络安全滑动标尺等安全架构和理念相继产生,但并没有根本性地改变安全建设与业务发展之间的生产关系:长期以来,安全架构建设由安全团队独立完成,被认为与企业架构及企业经营业务流程相对独立;因为安全架构需要建立在企业架构相关可用信息之上,所以安全架构建设常常滞后于企业架构的动态演进。经历数字化转型后的企业架构就像复杂的企业数字生命体(以下简称数字生命体)一样,会为了适应竞争环境而不断“进化”。每一次进化都可能会给安全架构带来巨大冲击。静态安全架构无法适应企业架构的动态变化,最终导致传统架构下的安全能力无法动态贴近业务,应对更深层的复杂性安全风险。面对数字生命体的不断进化,本文尝试将数字生命体与“人类复杂有机体”(以下简称有机体)进行比较,思考安全架构建设的困境与愿景,探究数字生命体在进化过程中,如何通过创新技术来实现安全架构与企业架构的常态化融合,并保持安全架构的一致性、连续性、低侵入性、有效性、稳定性和

友好性。

数字生命体中众多面向公网开放的互联网业务就像有机体的呼吸系统一样。当前开源软件的大规模引用和软件供应链安全威胁的加剧，使得类似新冠病毒这样的未知0day攻击日趋常态化，并通过“呼吸系统”感染数字生命体内部。结合外部风险态势和蚂蚁集团自身的安全需求，我们看到：随着业务复杂度的提升，已有的安全架构建设及单点安全能力显得力不从心，在面对内外部环境时不断爆出漏洞，在对抗、溯源、治理方面仍面临巨大挑战。因此，蚂蚁集团对安全理念和安全架构进行了全面升级。其中，安全平行切面与平行舱是安全理念和架构的具体体现。安全平行切面是中国在国际安全领域首创的创新安全理念及技术。

1 安全建设的困境与愿景

据统计，2022年网络与信息安全产业共包含94个细分安全领域[1]，比2021年增加7个。近几年，安全产业细分领域的快速增加在某种程度上表明，企业架构和业务逻辑复杂性的急剧增加也不断催生新的安全需求。为满足前期业务快速发展的需求，安全能力大多采用外挂式的架构模型保障业务发展。这种外挂式安全架构的部署成本和对业务的侵入性都较低，所以被各类企业所接受。但是在高强度对抗与复杂治理场景下，外挂式安全架构的业务效果受限于可观测能力，已经无法满足更深层次的对抗和治理需求。例如，在数据安全治理领域，过往对抗和治理的对象往往是内部结构化数据的非法泄漏风险。但如今数据已成为生产要素，数据要素的流动会潜藏数据非授权共享、个人隐私泄漏、敏感数据违规扩散等重大经营风险。企业不仅仅要在边界层查看数据流出的一跳链路，更需要将整条数据传输链路及传输内容进行精细化审计和实质性管控。外挂式安全架构在高强度对抗与复杂治理场景下已显得力不从心。

随着网络安全、数据安全、个人隐私保护等监管要求的加强，安全能力与业务逻辑相融合所产生的价值愈发凸显，但彼此融合后又面临严峻挑战：融合升级后的安全防护效果优于外挂式安全架构，但在对抗方面基本无法发挥作用。其中，融合的形式包括安全团队为满足防护需求而开发的各种软件开发工具包（SDK），以及需要与中间件深度集成的安全组件。受限于业务方的研发集成、发布和升级等工作，安全与业务相互间制约着各自的发展。例如，安全团队需要小时级甚至分钟级的止血响应，而大型业务团队经常面临着十几个版本的碎片化测试和稳定性灰度上线压力，无法满足安全应急要求；更有甚者，安全团队辛苦推动各基础设施和应用服务集成一个关键安全增强组件，但基础设施的一个小缺陷或者业务的一个需求变更回滚，导致安全团队前功尽弃。

当前企业架构和业务逻辑呈现复杂性爆炸态势。作为企业经营战略的组成部分，安全架构应以低侵入而非捆绑的方式集成到企业架构中，以改变企业经营发展受到安全架构发展滞后影响的现状，为业务提供体验友好的原生化安全服务。这既是未来企业架构与安全架构共同的演进趋势，也是安全架构建设的愿景。

面对数字生命体的进化和安全建设愿景，如何在动态过程中实现安全架构与业务架构的无缝融合，是蚂蚁集团在新形势下面临的挑战。蚂蚁集团逐渐形成了以数据要素为中心的网络安全架构。业务云化、数字化转型等技术变革带来了企业服务和数据要素的动态访问需求，而动态访问需求又产生了更为复杂的安全业务场景和需求，例如员工在任意空间对企业内网的安全访问、在线数据要素的实时共享和确权、个人隐私信息保护、生产网访问流量鉴权、多类型移动应用漏洞检测等。面向复杂和动态的业务场景，灵活、快速地部署安全能力和响应安全需求，既是对已有安全架构和单点安全产品的挑战，也是蚂蚁集团新安全架构的建设诉求。蚂蚁集团在2019年提出了安全平行切面的理念和技术体系[2]，安全平行切面技术能够在高强度对抗和复杂治理背景下，将安全能力深入到业务内部，从根本上解决问题。该技术不仅可以确保安全逻辑和业务逻辑各自独立、平稳演进，避免出现绑腿走路的困境，还可以让企业快速具备精准的感知和干预能力，同时实现安全能力和效率的跨越式提升。

2 安全平行切面的定义

我们通过类比的方式来描述什么是安全平行切面。在新冠病毒防控过程中，佩戴口罩和接种疫苗是非常重要的。（1）佩戴口罩的作用是防止空气中的病毒通过呼吸系统进入体内。理想情况下，如果每个人都佩戴了口罩就相当于达到了微隔离的效果。但口罩不是完全封闭的状态，病毒总会绕过口罩进入体内。（2）经过科学论证，接种疫苗是抗击新冠病毒的最佳途径。但在应对新冠病毒全面爆发这样的突发事件时，疫苗的有效性、疫苗自身的安全性、与体内其他疫苗的兼容性、疫苗的规模化接种等变得非常关键。可以想象，对于不同国家来说，为1 000万人口、1亿人口和14亿人口大规模接种疫苗的难度是完全不同的。

上述两个阶段恰好与企业在高强度对抗与安全治理的过程十分相似。企业首先通过入侵防御系统（IPS）/Web应用防火墙（WAF）/防火墙等对企业边界进行防护。有效的边界防护非常重要，它能够防护大部分的外部攻击。但防护能力始终存在被绕过的可能，所以企业开始考虑通过运行时插

桩手段对正在运行的业务进行像疫苗一样的保护。这种技术方式将安全逻辑注入到业务内容，形成一种以上下文分析和异常行为检查为基础的“抗疫”能力。这种植入“安全疫苗”的方式在蚂蚁集团内部多个0day应急场景中被证明是有效的。因此，蚂蚁集团自研了诸如运行时应用自我保护（RASP）、交互式应用安全测试（IAST）等安全疫苗产品。但在应急响应过程中，这同时也带来了诸多问题：

• “安全疫苗”本身也是由代码构成的，如何快速验证疫苗能够发挥预期的安全作用？

• 如何确保疫苗自身足够安全，不会被攻击绕过或被动失效？

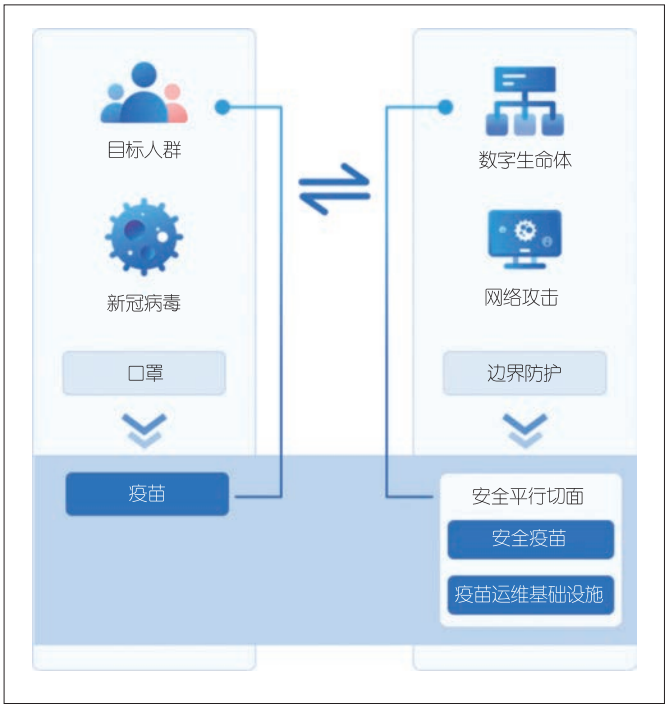
• 如何确保疫苗自身足够稳定，不会在出现异常的情况下影响宿主正常运转？

• 企业可能拥有几万甚至几十万台机器，那么如何在短时间内为每台机器都注入疫苗？

• 每台机器不会只注入一种疫苗，那么疫苗和疫苗之间如何进行有效的隔离，以确保不存在兼容性异常？

解决上述问题是蚂蚁集团提出并打造安全平行切面架构的初心。我们发现：为安全疫苗在业务空间内提供一个可持续进化的安全平行空间，是未来高强度对抗与安全治理背景下安全能力建设的普遍需求和唯一方向。这样的平行空间需要完备的稳定性、有效性、安全性、隔离性保障，不仅能够帮助安全疫苗快速部署到离业务会话最近的地方，还能够随着业务的动态扩/缩容而动态部署，实现中心化安全能力向分布式安全资源的演进。

那么什么是安全平行切面？安全平行切面是一套由安全疫苗和疫苗运维基础设施组成的安全架构。它首先在移动应用程序（APP）、云端应用、操作系统等应用与基础设施中注入安全疫苗，形成端-管-云立体安全防护架构，通过安全逻辑与业务逻辑解耦实现网络安全、数据安全的微观和宏观感知覆盖，满足应急响应、漏洞止血、数据安全、隐私保护等高强度对抗和安全治理需求。疫苗运维基础设施则从研发、测试、验证、监测与控制、稳定性保障等方面确保安全疫苗产品符合各类准入要求，并帮助各类安全疫苗实现全生命周期运维和大规模覆盖。所以，安全疫苗（例如RASP、IAST或其他具备运行时安全特性的产品）与疫苗运维基础设施共同构成了安全平行切面，如图1所示。



▲图1 安全平行切面为数字生命体提供疫苗保障

3 安全平行切面架构与平行舱

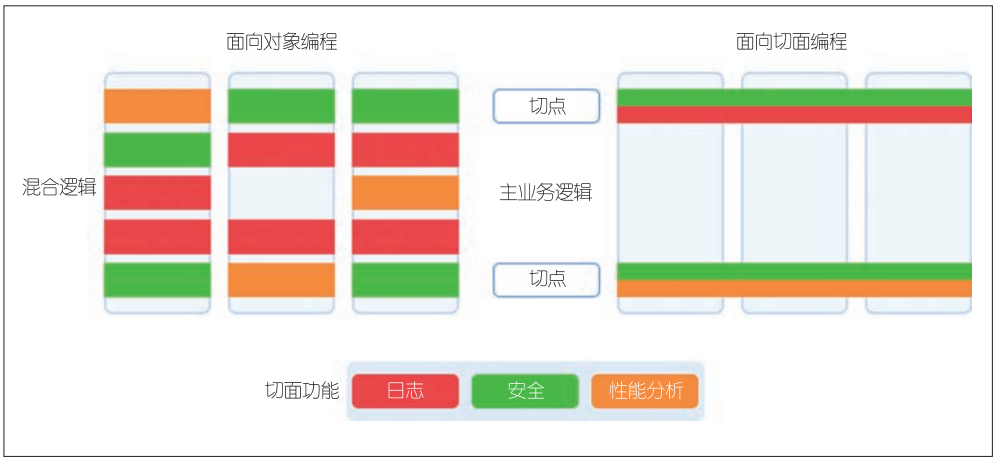
3.1 面向切面编程（AOP）与安全平行切面

1997年施乐帕洛阿尔托研究中心的Gregor等学者在著名的欧洲面向对象编程（ECOOP）会议上提出AOP的概念[3]。研究发现，面向对象编程（OOP）不能解决所有的问题，特别是涉及大量类的横切系统性功能问题很难用OOP来解决。而AOP能够很好地解决这一问题，它可通过预编译、运行时动态代理、注入等方式，在不修改原码的情况下，给程序的正常业务逻辑动态添加或修改功能，如图2所示。AOP已在AspectJ和Spring等项目中得到应用。

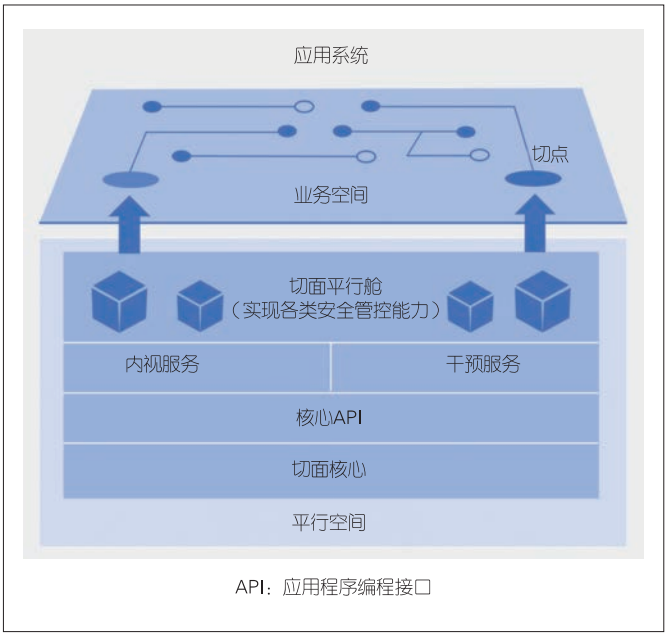
安全平行切面的核心思想是：将编程语言环境下的AOP推广应用到安全架构建设中，构建与业务正交融合的安全平行空间，在不修改业务正常逻辑的情况下，将安全能力系统化地融入到技术基础设施和应用服务的内部，从而实现更高维度的安全防护，在保持安全响应能力和复杂业务逻辑解耦的同时，通过标准化的接口为安全业务提供内视和干预能力。安全平行切面是一种创新的安全架构，是低成本实现“原生安全”、快速增强应用服务内在“安全体质”的一条可行路径。

3.2 安全平行切面基本架构

图3是安全切面的基本结构，上方是业务空间，下方是平行空间。在平行空间里面，安全平行切面通过注入、代理等技术，可以在不修改源代码的情况下动态添加新的（或修改程序原有的）逻辑。这部分动态逻辑称为切面应用。切面应用的作用位置（切点）是应用原有运行逻辑中的某一代码



▲图2 面向对象编程与面向切面编程



▲图3 安全切面的基本结构

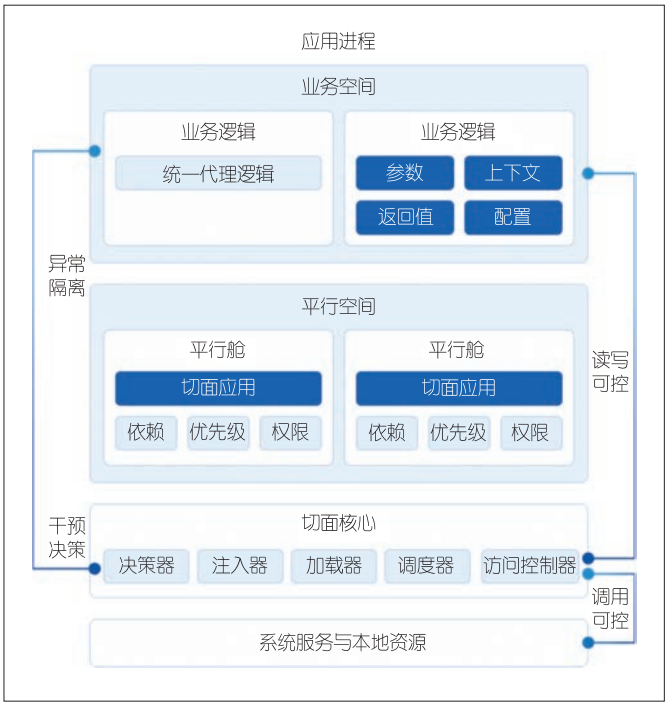
位置。一个切面应用可以作用于一个或者一组切点。类似于AOP的机制，安全切面可以将切点位置的代码执行流程引至切面应用中，并对其原有逻辑进行观测或干预。安全团队可以通过研发部署各种作用于不同切点的切面应用，来为应用服务动态扩展出各种丰富的安全增强能力。这就像如同通过应用注射各种疫苗来提升应用服务自身应对安全风险的“抵抗力”。

切面应用的动态扩展能力能够很好地降低日常安全治理成本，实现高效的安全响应能力。对切面应用模块化的管理方式，不仅能使各类安全能力实现独立开发，还可使不同的切面应用研发人员之间相互解耦，互不影响。但是便捷是一把双刃剑，其背后隐藏着巨大的隐患。例如，随着各类切面应用的不断增多，切面应用的质量参差不齐导致各类系统故障，不同切面应用之间的相互影响导致功能异常。如果被恶意人员所利用，切面应用反而会成为应用服务的安全短板。因此，如果不加以合理管控，安全切面会成为安全和稳定性的短板，无法被大规模推广使用。

3.3 平行舱：安全平行切面的稳定保障

为了保障平行空间内各种切面应用能够平稳、有序、可控、安全地运行，在系统运行时我们对切面应用进行了一层封装，即切面平行舱。这就像给疫苗加上一层“胶囊”一样，能够控制其在何时、何处、以何种规模生效。平行舱有三大特性：隔离性、可调度性和可管控性。借助平行舱可以对切面应用的作用和影响范围、组件依赖、可执行动作等进行相应的隔离与管控，如图4所示。

切面应用通过切面核心的加载器加载到平行空间中，在属于其自身的平行舱中运行，并通过各平行舱命名空间的隔离，来确保其依赖作用域只限于自身，不会污染业务空间。切面核心通过统一注入的代理逻辑接管切点的处理流程，并根据各种切面应用的优先级进行统一的调度管理。当最终各



▲图4 平行舱与切面应用

切面应用的处置逻辑执行完成之后，根据不同切面应用的执行结果，决策器会给出对业务逻辑所需要执行的干预行为。当切面应用出现异常时，切面核心可作为异常缓冲；而当切面核心出现异常时，统一的代理逻辑可提供异常兜底机制，避免对业务产生影响。这极大地提高了切面基础设施对切面应用和业务应用的运行保障能力。

此外，由于切面应用可以对业务执行流的上下文等数据进行修改，并且能和应用服务一样访问系统资源和服务，如果不加以限制，一旦被恶意利用，切面应用自身将成为安全短板。平行舱的访问控制能力可以限制切面应用对业务上下文的读写，默认其只有只读权限。这对于大部分观测类的切面应用来说已经足够使用。此外，对系统资源和服务的访问，也可以通过平行舱限定在有限的范围内。每个切面应用默认只能访问属于自身的资源目录和提供有限的系统服务。只有经过许可的切面应用，才能执行额外的操作。

安全平行切面是一套安全基础设施。通过提供统一的干预与内视能力，安全平行切面可实现丰富的安全能力。同时平行舱可确保整个架构平稳、可靠地运行，进一步提升了整个架构的安全性和稳定性，为各类切面应用与应用服务之间和谐有序共存提供了必要的基础保障，为安全平行切面的大规模应用奠定了基础。

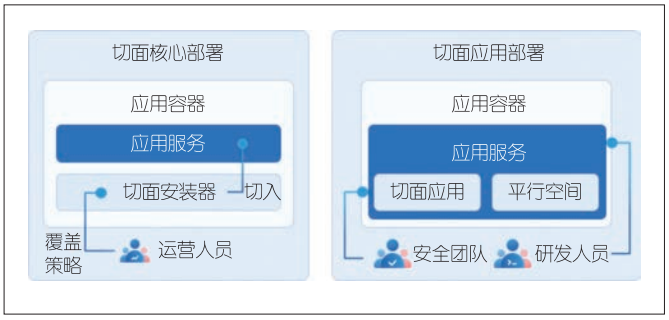
4 安全平行切面的规模化应用

4.1 基本部署结构

在安全平行切面大规模落地的过程中，为了降低推进成本，减少不同语言、框架应用带来的差异性，我们将安全平行切面的部署结构分为3个基本组成部分：切面安装器、切面核心和切面应用。切面安装器在接收到安装指令后，会将指定版本的切面核心包下载，并在应用启动阶段，对应用执行注入动作，进而完成切面核心的部署。切面核心部署与切面应用部署如图5所示。不同领域的安全团队，比如数据安全、系统安全、攻防对抗等，可以各自独立地对平行空间内的切面应用进行维护，从切面应用仓库中，选择并部署它们所需要的能力。整个过程不需要应用做任何提前准备和代码修改。在这种解耦的工作模式下，各个团队的效率都可以得到跨越式的提升。

4.2 切面规模化部署

安全平行切面是一个面向多语言、多框架异构应用的安全基础设施。不同语言和框架的差异性使切面核心的注入方式、启动方式等有所不同。为了尽可能降低由碎片化场景带来的运维交付成本，满足大规模部署要求，我们必须对适用于各类异构应用的切面进行运维操作统一化处理。因此，切面安装器应运而生。



▲图5 切面核心部署与切面应用部署

切面安装器是一个纯系统软件，可广泛应用于各类操作系统。在切面大规模部署之前，切面安装器需要先安装在所有目标应用容器之内。整个过程所需要的仅仅是系统软件的批量安装能力（在绝大多数云和企业中，这是一个比较常规的能力），并且这一过程通常是一次性的，成本相对可控。

在当下复杂的企业环境中，往往运行着各种基于不同语言和框架开发的应用服务。由于需要针对不同的应用服务决策下发不同的部署策略，因此切面管控管控端需要有足够的信息依据，以便判定一个应用是什么语言类型、适合部署什么版本的切面。由此可见，在切面安装器部署完成之后，首先要解决的是应用资产信息的收集问题。通过切面安装器自带的进程和环境信息上报能力，云端可以快速获取每个容器中运行服务的基本情况。结合配置管理数据库（CMDB）、代码仓库、平台即服务（PaaS）等，我们可以很方便地识别出容器内运行应用服务的基本信息，例如所属应用、开发语言、服务框架和负责人等，自动化地完成应用服务摸底任务。当然，对于一些元数据缺失的应用，我们也可以通过人工打标的方式完成资产判定。但是这对于存量应用的覆盖是有限的，无法实现增量应用服务的自动识别与覆盖，会产生一定的维护成本。

不同语言应用在切面核心注入逻辑上的原理与实现方式是有差别的。为了消除不同语言（或框架）切面核心的差异性，切面安装器定义了一套统一的安全平行切面部署执行标准。无论哪种语言类型的切面核心，都使用同一个安装包格式。安装包内除了有切面核心具体代码之外，还包含相对应的初始化脚本、注入脚本和启动脚本等。针对不同语言类型的切面核心，切面安装器只需要进行统一解压、校验，并按流程依次执行相应的脚本即可。标准化的运维操作可以让我们很方便地实现面向任意语言切面的统一部署流水线，配合

相应的监控、变更防御策略等，可以稳定、高效、自动化地完成大规模切面部署。

经过我们的实践测算，在确保稳定性的情况下，平均每1 000个应用服务在完成日常安全能力升级时仅需要10人日（紧急情况下，甚至可以在小时级时间内完成），而传统的强耦内嵌式的安全能力升级往往需要以月为单位计算。安全切面带来的效能和安全敞口收敛效果的提升是跨越式的。在整个体系验证完成后，蚂蚁集团就很快完成了全站95%以上应用的接入，并完成了核心业务全覆盖。整个系统非常稳定，至今未发生过故障，具有很好的推广价值和借鉴意义。

5 安全平行切面架构的收益

安全平行切面给企业数字生命体带来的最大收益是：能够在企业动态进化的架构中构建与业务逻辑平行的原生安全空间，将“疫苗”快速、稳定、高效地注入给受保护的目标。安全平行切面架构能够将安全逻辑深入到应用服务内部，天然具备更细粒度且更为精准的感知和干预能力。同时由于安全平行切面架构具有与业务解耦的特性，因此在效率与成本方面，优于很多传统的内嵌安全架构。使用不断扩展的切面应用可以实现各种丰富的安全能力。经过不断探索，蚂蚁集团目前已经拥有40多种切面应用，包括负责对抗和漏洞感知的切面应用（RASP、IAST等），以及和数据与隐私保护相关的切面应用（隐私数据的流转和血缘分析、敏感接口的确权控制等）。

5.1 运行时安全防护

2021年底，Log4j被爆出存在命令执行漏洞，影响范围广泛。因攻击难度低、变种多、内网穿透强性，log4j危险性极大。一方面，当时蚂蚁集团正处于双十二购物狂欢节（以下简称“双十二”）大促业务稳定性保障的关键时期。在大促封网的关键时期，启动全局范围的修复阻力非常大，会耽误最佳的应急时间。另一方面，由于log4j的攻击变种比较多且具有相当强的内网穿透性，所以边界层Web应用防护系统（WAF）的止血效果也十分有限。而基于安全平行切面实现的、大规模部署的RASP应用，可以很好地防御此次漏洞攻击：只需要在漏洞执行链的关键切点进行阻断即可，精准且高效。借助安全平行切面的快速部署能力，安全团队在小时级的时间内就完成了全站数千个应用、几十万容器的防护升级，最终阻止了40多万次真实外部攻击，实现了0漏报和0误报，使应急人力投入从预期的6 000人日降到30人日，大大提升了安全防护效率，缩短了安全风险的暴露时间，顺利抗住了“双十二”的流量洪峰。这个案例很好地体现了安全切面应用的精准感知和管控能力，即安全切面应用可以在非常细粒度的关键点上进行布防。不管外层如何变化和隐藏，都绕不过最终的执行点。同时，整套架构和业务自身是解耦的，不需要业务感知，极大提升了整体的应急效率。

5.2 数据要素流转治理

在业务运转过程中，数据就像血液一样流动。敏感数据伴随着普通数据在应用及数据存储间快速流转。基于敏感数据传输的上下文最终呈现数据血缘关系。基于切面体系实现的数据采集能力发挥其与业务融合又相对解耦的巨大优势，大大提升了数据安全治理的可观测性。可观测性是指对海量、异构、复杂数据的采集、分析和展示能力，即不仅能够在流转的复杂结构数据中识别敏感数据，还能够对敏感数据进行准确分类和分级。基于安全平行切面的数据安全应用能够按照数据类型和采集需求动态下发采集规则，实现对指定接口读写数据的行为采集。后继结合图分析技术，将信息进行融合分析，可以还原整个数据处理流程，构建完善的数据链路血缘。通过安全平行切面架构对数据要素共享治理体系进行升级后，数据要素的分类分级识别能力、数据采集的可达范围均可产生显著提升，并将风险感知和处置的时效提升至分钟级以内。

5.3 移动应用隐私风险治理

移动应用特别是平台型APP存在大量第三方SDK、小程序、H5页面等。由于缺少运行时的监测和管控技术，线上实际调用行为无法被观测到。这导致APP的行为记录、解释和追溯变得极为困难。当出现问题之后，系统很难进行紧急阻断。传统方式下，应用的安全风险治理主要通过APP上架前的安全研发生命周期管理（SDL）和上架后的APP发版对漏洞进行修复。这种方式存在一些问题：

（1）难以枚举应用的输入与输出。静态分析可以枚举出一部分，但误报率高，且无法检测动态加载的行为；动态检测可以模拟的环境有限，只能触发有限的业务场景。

（2）难以复现。应用的某些行为仅在特殊场景下才会触发。而安全分析人员难以了解每个业务的细节。因此，这些仅在特殊场景下触发的行为难以被发现和评估。

（3）难以修复。从发现问题到发布修复版本往往耗时数个月（3～4个版本），这给研发带来巨大负担。

利用代码植入技术、运行时函数信息监测技术、风险行为检测算法和运行时函数行为管控技术，移动端安全平行切面架构可以提供移动应用数据内视、行为刻画和业务干预能

力，实现针对运行时的威胁发现和恶意收集用户隐私行为的监测和防护。目前通过对安全平行切面获取的数据进行收集和挖掘，我们已经发现多个日活跃用户数达到亿级的移动应用的数十项隐私合规风险，包括隐私泄漏、后台调用异常、超频次使用、未授权调用等。这些风险可通过动态下发切面管控配置进行修复，不需要通过APP进行重新发版。

6 结束语

本文中我们将当前企业信息架构类比为数字生命体，将数字生命体的网络攻击防护与新冠病毒的防护进行类比，阐述了安全平行切面的内涵，并总结了网络与信息安全形势面临的3个趋势：企业数字生命体持续动态进化、业务规模及业务逻辑复杂性爆炸、高强度攻防对抗及安全治理日趋常态化。在这样的背景与趋势下，传统静态安全架构已显得力不从心，原生安全架构比“口罩”的静态安全架构有更加理想的安全效果。安全逻辑与业务逻辑紧密结合所带来的巨大收益逐渐被人们重视。我们认为安全架构与企业架构实质性融合的时代即将到来。如何将安全逻辑像疫苗一样安全、稳定、可靠、大规模地注入到应用内部是安全平行切面需要应对的挑战。此外，本文还介绍了蚂蚁集团安全平行切面架构和平行舱技术，阐述了如何通过疫苗运维基础设施对安全疫苗实施全生命周期的运维保障。蚂蚁集团应用安全平行切面所取得的收益或许能够为安全行业带来新的建设思路。

致谢

在本文撰写过程中，蚂蚁集团郑旻、王少宇、李婷婷给予了大力支持，特此感谢！

参考文献

[1] FreeBuf 咨询 . CCSIP 2022 中国网络安全产业全景图（第四版）[EB/OL]. (2022-07-21)[2022-10-15]. https://www.freebuf.com/articles/339788.html
[2] 蚂蚁科技集团股份有限公司, 中国电子科技集团第十五研究所(信息产业信息安全测评中心). 安全平行切面白皮书 [R]. 2021
[3] KICZALES G, LAMPING J, MENDHEKAR A, et al. Aspect-oriented programming [EB/OL]. [2022-10-15]. https://www. cs. ubc. ca/~gregor/papers/kiczales-ECOOP1997-AOP.pdf

作 者 简 介

韦韬，蚂蚁集团副总裁、首席技术安全官，浙江省科学技术协会委员，北京大学客座教授；20多年来一直致力于让各种复杂系统变得更加安全可靠，牵头和推动了多项知名开源项目的研发工作，在全球首创了安全平行切面、可信密态计算等重要安全技术体系，在安全攻防、隐私保障、合规治理等领域有着丰富的实战经验，2022年入选IDC“中国CSO名人堂（十大人物）”。

顾为群，蚂蚁集团安全平行切面产品经理；深耕网络与信息安全产品领域10余年，致力于通过产品与解决方案链接创新技术和复杂业务场景，主导和参与蚂蚁集团在安全平行切面、生产网零信任、应用安全、威胁对抗、数据安全等多个领域的产品体系建设。

刘宇江，蚂蚁集团安全平行切面架构师；长期从事企业基础安全领域的体系架构与建设工作，具备丰富的大型互联网企业安全建设实践经验，先后负责蚂蚁集团的安全感知、威胁对抗、零信任与安全切面等安全体系的设计与落地，深度参与了蚂蚁集团历代基础安全能力的架构演进升级工作。

5G网络赋能物联网安全

5G Enables Internet of Things Security

林美玉/LIN Meiyu
（中国信息通信研究院安全研究所，中国 北京 100191）
(China Academy of Information and Communications Technology, Security Research Institute, Beijing 100191, China)

DOI：10.12142/ZTETJ.202206012
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221013.1427.006.html
网络出版日期：2022-10-13
收稿日期：2022-08-25

摘要：分析了物联网（IoT）安全需求，并梳理了5G网络的安全能力。认为5G网络能够满足物联网应用的安全需求。5G网络自身安全能力的增强，有助于满足物联网应用对网络安全性的需求。5G网络可以通过安全组网、能力开放的方式，利用自身安全能力、切片特有的安全能力以及运营商网络中部署的其他安全能力，向不同的物联网应用场景提供差异化安全服务，以赋能物联网安全。

关键词：5G网络；物联网安全；切片；能力开放

Abstract: The security requirements of the Internet of Things (IoT) are analyzed, and the security capabilities of 5G networks are introduced. It is believed that 5G networks can meet the security requirements of IoT. The enhancement of the 5G networks security capabilities helps meet the needs of IoT applications for network security. The 5G networks can also use the security capabilities to enable IoT security through providing customized virtual private network or security capability exposure. The security capabilities include 5G network security capabilities, slice-specific security capabilities, and other security capabilities deployed in the network by the operators.

Keywords: 5G network; Internet of Things security; slice; capability exposure

目前，5G已经成为全球最瞩目的热门技术之一。相比于4G和之前的蜂窝移动网络，5G融合了很多新技术，可提供极端差异化的性能以满足多样化场景的业务应用需求。5G网络主要支持三大应用场景：增强移动宽带（eMBB）、海量机器类通信（mMTC）和超可靠低时延通信（URLLC）。其中，mMTC面向的就是物联网应用场景，例如海量终端高密度连接的智慧城市应用场景。实际上，自动驾驶、工业控制等对可靠性和时延高度敏感的URLLC场景，也是物与物之间的通信。因此，从5G网络支持的应用场景来看，5G是为物联而生的。

与此同时，业界对5G网络安全的重视程度显著提高。5G安全问题甚至已成为世界各国在5G网络方面的主要博弈点。欧美国家纷纷出台了相关法律、政策，并制定了相关技术指导文件，将5G安全上升到国家战略层面。事实上，5G安全问题的重要性之所以能够引发全球的共鸣，其根本原因是在5G与物联网[1]应用深度融合后，人们对5G网络所承载的物联网应用安全有所担忧。5G网络本身的安全与4G之前网络的安全并没有本质区别，但是其承载的物联网应用的安全却关系着国计民生的各行各业，甚至关系着国家安全。因此5G安全问题的重中之重，就是如何解决5G网络与物联网应用融合的安全问题。

1 5G融合物联网应用的安全风险

物联网应用对5G网络的安全疑虑主要体现在两方面：一方面是能否消除5G网络自身面临的安全风险，以确保所承载的物联网应用的安全；另一方面是能否解决5G网络与物联网应用融合所带来的新风险问题。

5G网络自身的安全风险主要来自5G网络所引入的新技术[1]。网络功能虚拟化（NFV）、多接入边缘计算/移动边缘计算（MEC）、网络能力开放、网络切片等多种新技术的引入，确实给5G网络带来了一些新的安全风险。但是随着隔离等安全技术的逐渐成熟，以及5G网络增强安全机制的产生[1]，5G网络自身的安全风险基本可控。

5G网络与物联网应用之间的边界融合泛化后，其安全风险也会互相影响。从物联网应用的角度来看，5G网络的引入打破了某些物联网应用领域通过物理边界保护的封闭性。这容易引发越权访问，造成安全后果。例如，无线接口劫持可能会导致合法终端接入非法网络，泄露敏感信息。如果5G网络身份认证能力不足，非法物联网终端可能接入业务系统，泄露或篡改业务数据，并导致物联网业务失效。从

1. 本文所指物联网，主要关注物联网业务应用层面，而非联通万物的网络本身；本文仅适用于5G网络承载物联网应用的场景。

5G网络的角度来看，物联网应用的安全风险，也可能会给5G网络带来灾难性后果。例如，在mMTC应用场景中，大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被操控向网络发起分布式拒绝服务（DDoS）攻击，就可能带来网络中断、系统瘫痪等安全风险。

2 物联网应用对5G网络的安全需求

目前5G网络的安全问题被广泛关注甚至被无限扩大。这与不同行业之间存在较大的认知差异密切相关。物联网垂直行业在安全性方面对移动通信网不够信任，对通信网络的安全能力也不够了解；而通信行业对物联网领域的安全需求也尚未充分了解，无法发挥5G网络的最大价值。本文首先从物联网的业务特征出发，分析物联网安全需求。这些需求主要包括：

（1）对敏感数据保护的需求。物联网应用场景中包含重要的行业信息和个人隐私，因此数据泄露和篡改会带来严重的后果。尤其是利用感知数据进行应用决策的物联网应用场景，一旦感知数据被篡改，就可能导致决策错误。这不仅会关系到企业经营和生产安全，甚至关乎国家安全。

（2）差异化安全需求。物联网应用涉及千行百业，其安全需求也各不相同。例如，工业互联网主要关注数据不能出园区，智慧医疗更关注隐私数据加密。

（3）对海量终端的安全管理需求。众所周知，物联网终端安全能力普遍较低，物联网应用服务商的安全技术水平良莠不齐。操控物联网终端向网络发起DDoS攻击会导致物联网应用平台瘫痪。非法终端接入网络和物联网应用平台会导致数据泄露或被篡改。这些案例比比皆是，带来的后果也是非常严重的。

（4）对无线接口安全性的需求。物联网应用与5G网络融合后，开放的无线网络可能会成为物联网应用安全的薄弱点，例如网络攻击者可能会通过无线接口进行窃听、数据篡改等。

结合5G网络特点，上述安全需求映射到5G网络中，具体可体现为以下技术需求[2]：

（1）安全隔离技术。针对不同安全等级的物联网应用，5G网络需要采用网络安全分域方式或安全隔离技术手段来实现网络资源、数据传输通道的隔离。

（2）终端身份安全和访问授权技术。该技术可防范非法终端接入网络和物联网应用平台。

（3）5G网络无线接口通信安全技术。为满足物联网应用的安全需求，无线接口需要具备防窃听、防篡改、防无线接口劫持等通信安全能力。对安全要求较高的场景，甚至还需要具备无线接口DDoS攻击防御、无线接口抗干扰等能力。

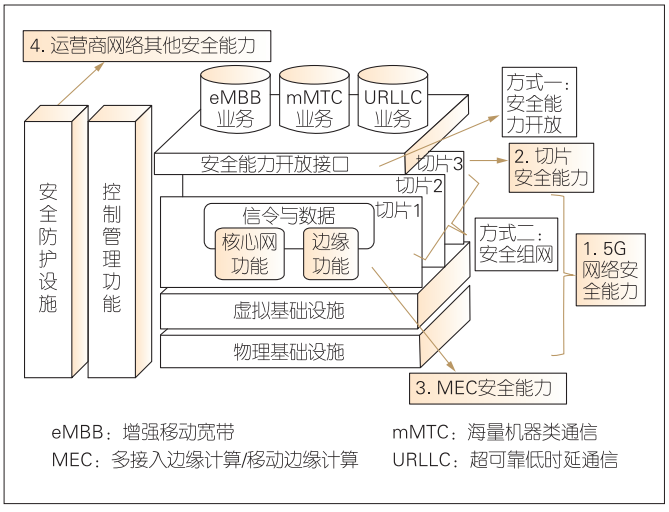
（4）数据机密性和完整性保护技术。该技术主要是用于防范5G网络所传输的数据被泄露或篡改。

3 5G赋能物联网安全的解决方案

作为支撑未来万物互联的基础设施，5G网络对物联网应用的安全保障能力是各个行业完成数字化转型的关键。事实上，5G网络在安全架构设计方面，已充分考虑了上层应用的安全需求。针对物联网应用的安全需求，一方面5G网络本身的安全能力须不断增强，以打消物联网应用对5G网络安全性的疑虑；另一方面通过安全组网、能力开放等新技术，5G网络可以整合自身及外在的各种安全能力，为物联网应用提供差异化的安全服务，直接赋能物联网应用安全。

3.1 可赋能的安全能力

5G网络可用于物联网安全赋能的安全能力主要体现在4个方面：5G网络自身安全能力、网络切片技术特有的安全能力、MEC的数据安全保护能力以及运营商网络中部署的其他外在安全能力，具体如图1所示。



▲图1 5G赋能物联网安全

3.1.1 5G网络自身安全能力

（1）终端身份认证和访问授权

用户设备（UE）接入5G网络需要进行主认证（Primary认证）。在认证机制方面，5G继承了4G成熟的认证与密钥协商（AKA）认证机制，并对AKA机制进行了增强，强化了归属网络对认证的控制。此外，5G还引入了灵活的扩展认证协议（EAP）认证框架，以实现统一认证。这样网络一

方面既可支持各物联网应用场景中已使用的多种认证协议（例如扩展认证协议–传输层安全协议等），又可根据物联网应用所需要的认证能力需求进行扩展适配；另一方面，还可以支持不同接入网络方式的认证，例如无线局域网（WLAN）等非第3代合作伙伴计划（3GPP）接入方式。

在主认证的基础上，5G网络还可支持针对应用的次认证，即用户在通过5G网络访问外部数据网络时，由承载数据网络的第三方（例如物联网服务商）对用户进行身份认证。次认证的过程中需要使用终端中预存的认证凭证。认证过程会使用5G网络的EAP认证框架。

（2）5G网络无线接口通信安全

对于无线接口的通信安全，5G网络进行了一系列的安全增强[3]。一是空口采用加密身份标识，提供增强的用户隐私保护。为了解决4G网络中由使用用户国际移动用户识别码（IMSI）接入网络而导致的用户标识在空口的泄露问题，5G引入了用户隐藏标识（SUCI）。通过一系列的算法和机制设计，在5G响应身份请求消息时，UE永远不发送用户的永久标识（SUPI）。由于每次产生的SUCI并不相同，因此攻击者无法根据SUCI计算出SUPI。这能够起到保护用户隐私的作用。二是5G网络无线接口支持接入层（AS）和非接入层（NAS）的机密性和完整性保护。在用户面的完整性保护方面，之前的蜂窝移动网络在应对业务时效性的要求时均未设计完整的保护机制。考虑到有些物联网应用场景对控制数据传递的准确性要求比时效性要求更高，5G网络引入了灵活的数据完整性保护机制。设置完整性保护策略可以使5G网络灵活地决定是否开启用户面数据完整性保护，以更好地适应不同应用场景的差异化需求。

（3）数据机密性和完整性保护

在无线接口机密性和完整性保护算法方面，5G网络支持高级加密标准（AES）、祖冲之算法（ZUC）或者Snow 3G 128 bit的密码算法。考虑到未来量子计算对算法的破解，5G网络将支持256 bit的密钥。

除了无线接口外，5G网络还在运营商网间增加了安全边界保护代理（SEPP）设备，可支持在运营商之间建立传输层安全（TLS）的安全传输通道，或者基于共同认同的安全策略对传输的信息进行机密性和完整性保护，以防止重要敏感数据在传输过程中被篡改和窃听。

（4）网络功能（NF）之间的安全隔离

5G网络的服务化架构使NF之间的相互访问更加便利，但是也为攻击者伪造成合法NF进行攻击带来了便利。针对服务化架构，5G网络设计了一套授权认证机制，以确保只有授权的NF才能访问特定服务，实现服务化架构下NF之间的安全隔离。这主要包括：（a）引入网络仓储功能（NRF）提供NF服务能力的注册、发现、授权，来保障服务化安全；（b）NF与NRF、NF之间进行交互时都需要进行双向认证，具体可采用传输层安全机制（例如TLS协议）的认证机制或者网络域安全机制，例如网络域安全/互联网协议（NDS/IP）；（c）引入授权机制，即NRF采用互联网工程任务组（IETF）定义的OAuth 2.0授权框架[4]对NF进行显式授权，或者基于5G网络的服务发现流程向NF进行隐式授权。

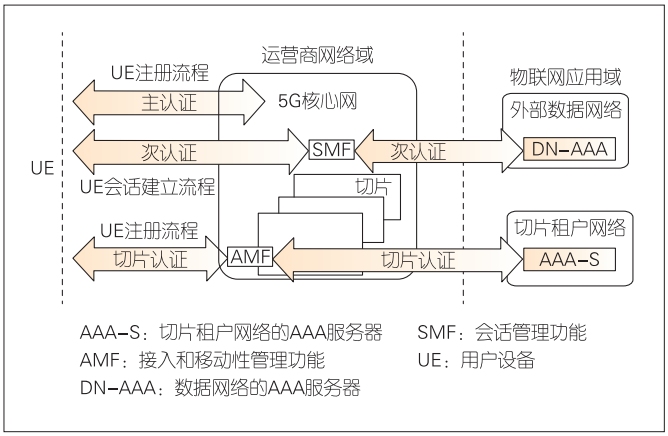
3.1.2 网络切片技术的安全能力

除了5G网络本身的安全能力之外，网络切片还支持一系列特有的安全机制。

（1）网络切片认证

UE接入切片时，其注册过程除了可以通过5G网络进行主认证之外，还可以使用网络切片认证[3,5]，进一步防止未授权用户访问切片。网络切片认证可以由切片使用者（例如物联网应用的服务提供商）自行进行管理。这增强了切片使用者对用户的控制能力和灵活度。

主认证、次认证和切片认证共同构成了5G网络保障物联网应用安全的三级认证体系。三者之间的关系如图2所示[6]。



▲图2 主认证、次认证和切片认证的关系

物联网应用可根据自身的安全需求，在主认证基础之上，叠加次认证和/或切片认证来增强安全能力。

（2）切片的安全隔离机制

切片技术安全性的核心是切片的隔离能力。5G网络从无线接入网隔离、承载网隔离、核心网隔离、数据隔离4个方面引入隔离机制，构建了切片之间、切片网络与用户之间、切片内网元之间的三级隔离体系。无线接入网隔离机制包括：为不同的切片分配专用频谱可实现无线频谱资源的物

理隔离，或者不同切片按需使用相同的频谱以实现逻辑隔离[7]；为不同的切片分配不同的硬件、虚拟机或容器以及对应的虚拟局域网/虚拟可扩展局域网（VLAN/VxLAN）可实现网元隔离。承载网隔离机制包括VLAN逻辑隔离，以及以太网分片技术（如灵活以太网）实现时隙层面的物理隔离[8]。核心网的隔离机制包括独立的物理资源隔离、基于虚拟机或容器的逻辑隔离、通过划分不同的安全域并在安全域之间配置安全策略（例如认证、授权等）而实现的隔离、通过账号权限控制实现不同切片管理维护之间的隔离等。数据隔离机制包括使用独立的密钥而实现的不同数据的隔离、通过身份认证和细粒度授权进行数据访问控制、不同安全级别采用不同的加密机制等。

（3）切片的安全监控

切片管理系统可以实时掌握切片的运行情况（包括故障和受攻击情况），并可通过联动其他安全设备进行威胁处置、故障修复等。双向认证、访问授权以及管理接口的安全保护，可保障切片管理功能的安全。

3.1.3 MEC技术的安全能力

MEC技术可降低时延和网络传输压力，其自身并不具备安全能力。但是由于需要指定用户面功能（UPF）处理数据、阻断对外的N9接口、不开放面向公网的N6接口，事实上MEC技术可以达到敏感数据的流向可管可控、数据不出园区的效果，能够满足某些物联网应用场景下更高的数据安全需求。

当然，如前所述，MEC技术会给5G网络带来一定的安全风险。因此，我们还需要对边缘计算采取必要的安全防护方案，例如：对使用MEC的操作进行认证、授权和审计，对引入的第三方应用执行严格的评估管控流程，加强数据访问控制，对MEC内部边界进行安全隔离等。

3.1.4 运营商网络部署的其他安全能力

除了5G网络和切片的安全能力之外，为保障相关网络和业务系统的安全，运营商网络通常会部署很多其他的安全能力，包括认证、授权、审计、入侵检测、漏洞扫描、入侵检测、威胁情报共享、恶意流量清洗等。

3.2 赋能方式

5G网络可以通过安全组网和安全能力开放两种方式，为物联网应用提供差异化的安全服务，直接赋能物联网应用安全。

3.2.1 安全组网

5G网络可通过“切片+边缘计算”的方式进行组网，为不同物联网应用提供不同安全等级的定制化虚拟专网。显然，安全的虚拟专网可满足不同物联网应用之间的安全隔离要求。

除此之外，我们还可以根据各物联网应用的安全需求，为虚拟专网设计定制化的安全机制，提供差异化的安全服务。5G网络自身的安全能力、切片的安全能力，MEC技术，甚至包括运营商部署的入侵检测、安全防护等能力，都可以作为虚拟专网的安全定制选项。例如，对安全等级和资源保障要求高的重点应用，可将切片部署于专用的物理资源实现物理隔离并部署MEC；对数据准确性要求高的应用，可开启数据的完整性保护；对可用性要求高的应用，可以通过流调度的方式，让应用的流量经过抗DDoS攻击、异常流量监测等安全模块进行防御。

3.2.2 安全能力开放

5G网络支持的网络能力开放技术为5G网络赋能物联网安全提供了一种新的方式。

为了更好地支持物联网行业应用，5G标准中引入网络开放功能（NEF），支持将5G网络的基础能力对外转换为标准的应用编程接口（API），以便第三方应用服务提供商调用。目前3GPP已经完成服务质量（QoS）能力等业务能力开放的标准化工作。5G网络的安全能力开放目前正处于研究当中。

安全能力开放的方式[9]包括：由5G网络构建安全能力开放平台，实现网络即服务（NaaS），形成一系列安全服务能力，并通过API进行开放以赋能物联网安全。物联网行业应用可根据自身的安全需求，直接调用运营商网络的安全服务能力和安全资源，可以节省更多的财力和精力，实现行业共赢。

前述5G网络自身的安全能力、切片的安全能力，甚至运营商部署的入侵检测、安全防护等能力都可以考虑以适当的服务方式进行开放。例如，3GPP R16就提出了一种面向应用的认证和密钥协商（AKMA）[10–11]能力开放的解决方案，即利用5G网络的认证凭证和安全机制，为第三方应用提供认证和应用层通信加密服务。该方案尤其适合物联网应用的调用场景。在物联网场景下，由于终端难以进行密钥接收和配置，而AKMA无须在终端预置安全凭证，物联网应用也无须建立自身密钥管理体系进行密钥分发，使用5G的AKMA能力就可以实现认证和密钥管理能力。由于第三方应用可通过标准的能力开放接口接入并使用AKMA功能，因此该方案可适用于所有协议的物联网设备。

4 结束语

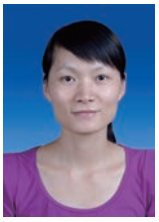
目前，5G对物联网安全赋能的各种实践已崭露头角。5G网络结合MEC和切片技术进行安全组网并提供定制化安全能力的方案，业界已有较多试验应用场景，但还不够成熟，尚未进行规模化复制。而5G网络安全能力开放的方案，目前尚处于方案探索阶段，实践案例很少。这主要是由于通信行业与垂直应用行业彼此了解不够，5G网络难以结合行业需求并对自身丰富的相关安全能力进行充分地挖掘和开放。

5G网络让万物互联成为可能，促进了产业的跨界融合，但也引发了业界对安全问题的担忧。如前所述，5G网络蕴含的丰富的安全能力有待释放，未来5G网络与物联网应用在安全方面的深度融合还有无限的可能，尤其是5G安全能力开放，将成为未来5G和物联网融合发展的一个重要方向。后续运营商与物联网应用服务商应加强沟通合作，形成跨行业共识，共同推动5G赋能物联网安全，更好地发挥5G在推动社会数字化转型过程中的作用。

参考文献

[1] 中国信息通信研究院, IMT-2020(5G)推进组. 5G安全报告 [R].2020
[2] IMT-2020(5G)推进组. 面向行业的5G安全分级白皮书 [R].2020
[3] 3GPP. Security architecture and procedures for 5G system: 3GPP TS 33.501 [S]. 2019
[4] RFC. The oauth 2.0 authorization framework: RFC 6749 [S]. 2020
[5] 3GPP. System architecture for the 5G system (5GS): 3GPP TS 23.501 [S]. 2019
[6] 杨志强，栗栗，杨波，等. 5G安全技术与标准 [M]. 北京: 人民邮电出版社, 2020: 195-196
[7] 毛玉欣，陈林, 游世林. 5G网络切片安全隔离机制与应用 [J]. 移动通信, 2019, 43(10): 31-37
[8] 李晗. 面向5G的传送网新架构及关键技术 [J]. 中兴通讯技术, 2018,24(1): 53-57
[9] 杨红梅, 林美玉. 5G网络及安全能力开放技术研究 [J]. 移动通信, 2020, 44(4): 65-68
[10] 3GPP. Study on authentication and key management for applications based on 3GPP credential in 5G: 3GPP TR 33.835 [S].2020
[11] 3GPP. Authentication and key management for applications (AKMA) based on 3GPP credentials in the 5G System (5GS): 3GPP TS 33.535 [S]. 2021

作　者　简　介



林美玉，中国信息通信研究院安全研究所副所长、中国通信标准化协会ST6组长；长期从事网络交换、网络与信息安全方面的研究工作；牵头完成多项国家重大专项，并多次获得中国通信标准化协会科技进步奖一等奖、二等奖、三等奖，中国通信学会科技奖二等奖、三等奖，以及国家安全部科技进步奖二等奖等奖项；已发表论文10余篇，累计完成相关领域标准40余项。

深度学习的10年回顾与展望

Deep Learning: Past Decade and Future

韩炳涛/HAN Bingtao[1,2]，刘涛/LIU Tao[1,2]，唐波/TANG Bo[1,2]
（1. 中兴通讯股份有限公司，中国 深圳 518057；
2. 移动网络和移动多媒体技术国家重点实验室，中国 深圳 518055）
(1. ZTE Corporation, Shenzhen 518057, China;
2. The State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055, China)

DOI：10.12142/ZTETJ.202206013
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221221.1442.003.html
网络出版日期：2022-12-23
收稿日期：2022-10-15

摘要：过去10年深度学习在算法、算力、数据方面获得了长足发展，使人工智能（AI）技术突破商用限制，行业应用场景日益广泛，产业规模持续扩大。在基础模型方面出现了卷积、注意力机制等关键突破；在学习方法方面，强化学习、自监督学习、大模型并行训练等使模型学习能力大大加强。新型AI计算芯片不断涌现，使计算能效提升百倍。未来10年，深度学习若要保持可持续的指数增长态势，绿色、高效、安全将成为新的核心要素。空间计算、近似计算等技术有望使AI芯片效能继续获得百倍提升。一系列生态融合工具的出现将解决目前日趋严峻的生态碎片化问题。AI安全、可信将成为AI技术应用的基本要求。

关键词：深度学习；AI芯片；推理加速；可信AI；开源

Abstract: In the past ten years, deep learning has made great progress in algorithm, computing power, and data, which has enabled artificial intelligence (AI) technology to meet commercial requirements, and has an increasingly wide range of application in various kinds of business, and the scale of the industry has continued to expand. In terms of basic models, there have been key breakthroughs such as convolution and attention mechanisms; in terms of learning methods, technologies such as reinforcement learning, self-supervised learning, and parallel training of large-scale model have greatly enhanced performance. New AI chips continue to emerge, and computing energy efficiency has increased by a hundredfold. In the next ten years, deep learning will maintain a sustainable exponential growth trend, and green, efficient, and safe will become the new core elements. Spatial computing, approximate computing and other technologies are expected to continue to improve the performance of AI chips by a hundredfold. Some integration tools will appear to solve the increasingly severe ecological fragmentation problem. AI security and trustworthiness will become the basic requirements for the application of AI technology.

Keywords: deep learning; AI chip; inference accelerating; trusted AI; open source

1 第1个10年回顾

2012年AlexNet[1]横空出世，掀起第3次人工智能（AI）浪潮。从此AI进入深度学习时代。在深度学习的第1个10年，数据、算法、算力三大要素得到迅速发展。与前两次浪潮不同的是，在第3次浪潮中AI技术一举突破商用限制，拥有日益广泛的行业应用场景，产业规模持续扩大，打消了人们对于第3次浪潮何时终结的疑虑。

1.1 算法长足发展

深度学习的特点是可以将基础算子以层层叠加的方式组成复杂的神经网络，并使用反向传播算法统一实现神经网络的训练。使用如此的简单方法即可构建任意复杂模型。这种能力使深度学习成为一种适用于多种任务的通用算法。

在过去10年中，基础模型经历了两次跨越式发展。第1次跨越是以AlexNet为代表的卷积神经网络。2015年ResNet[2]的出现使得这一阶段的发展达到高峰。在这一阶段人们普遍认为，更深的神经网络将具备更强的表征能力。因此，研究者主要思考如何增加神经网络的深度。ResNet通过引入跨层shortcut连接，成功将网络深度提升至150层以上。之后的研究虽将网络深度提升至1 000层以上，但模型性能提升幅度越来越小，因此百层左右的网络成为应用的主流选择。此外，这一阶段发展了大量基于卷积计算的算子，在提取空间和时间局部特征方面取得了很好的效果，使得图像、语音模式识别准确率大幅提升，产生了诸如语音输入、人脸识别等第一批可商业化的技术，为第三次AI浪潮创造了一个良好的开端。

第2次跨越是以2016年出现的以Transformer[3]为代表的注意力机制神经网络。注意力机制此前在神经网络中仅是辅助性算子，但Transformer创造性地将其作为网络核心算子，引发了一系列重大创新。Transformer最初解决了长短期记忆网络（LSTM）[4]等循环神经网络计算效率低、训练容易过拟合等问题。2017年基于Transformer的预训练语言模型

BERT[5]利用海量样本的无监督预训练大幅提升下游任务表现能力，使大规模样本预训练和少量样本精调成为模型训练新范式。此后，自监督预训练[6]更是将这一范式推向高潮。研究人员很快发现语言模型规模越大，表现就越好。模型规模在短短的两年内迅速突破了千亿参数级别。2019年，拥有1 700亿参数的GTP-3[7]模型在对话、知识问答、吟诗作赋等多项任务中展示出的能力令人印象深刻。深度学习从此迈入大模型时代。现如今相关模型规模已经达到百万亿级别[8]。此外，研究人员发现Transformer具备跨模态通用性。2018年，ViT[9]模型证明Transformer除了适用于处理自然语言相关任务外，在处理图像任务方面也不输于卷积神经网络。最新的DALL.E、紫东太初、M6[10-12]等多模态模型更是可以同时处理文本、语音、图像多模态数据。自监督预训练、大模型、多模态等创新Transformer成为当今最重要的深度学习模型，为深度学习的发展带来无限可能。

除了基础模型，过去10年在学习方法上也取得了重大进展。学习方法主要包括监督学习和无监督学习两大类。监督学习比较容易，但需要对数据进行标注，这个过程通常需要耗费大量人力。强化学习是一种特殊的监督学习，它只需要一个回报信号而无须对每条数据进行标注。在强化学习过程中，算法以一种“试错”的方式对问题空间进行探索，从而找到一种最优（获取最大回报）的策略。深度学习模型和强化学习方法相结合，产生多项重要成果，大幅拓展了深度学习的应用边界。2016年AlphaGo[13]战胜九段专业棋手，AI进入大众视野，第3次AI浪潮开始井喷。2017年AlphaGo Zero[14]完全不依赖人类的围棋知识，仅从最基本的围棋规则开始，经过72 h的训练，棋力就可远超AlphaGo。2018年AlphaZero[15]使用同一个模型和算法，同时掌握国际象棋、将棋、围棋，显示出强化学习有实现通用AI的潜力。强化学习在德州扑克、DOTA、星际争霸等视频游戏[16-18]中也达到顶尖人类玩家的水平。在真实环境中使用强化学习的研究也取得很大进展。使用强化学习算法不仅可以对机械臂实现适应性控制，可以完成诸如网线插拔等灵巧型任务[19]，甚至还可以操作复杂的可控核聚变托卡马克装置，实现对装置中高温等离子体形状、位置的跟踪和控制[20]。最近，强化学习在科学领域也取得不小进展。例如，AplhaTensor[21]可以发现各种大小的矩阵乘法的速算方法，而人类科学家还没能发现任何一种大于3×3规模矩阵的速算方法。强化学习在多种任务中体现出通用性，使其成为实现“通用AI”一条重要技术路线，不断吸引更多学者参与到研究中来。

难度最大同时也是最具发展潜力的无监督学习方法，特别是在生成式模型领域，在过去10年产生了两个重大的方法创新。一个是在2014年，Goodfellow提出的生成对抗网络（GAN）模型及其创新的对抗训练方法[22]，被LeCun认为是过去10年中机器学习领域中最有趣的想法。对抗训练方法通过同步优化生成器、判别器，使两者达到纳什均衡。这种方法可以生成更加清晰的图片，但训练过程不稳定。此后对GAN的改进成为研究热点，特别是在2019年BigGAN[23]改进了大规模网络下对抗训练不稳定的问题，使batch size增大至2 048，模型参数达到1.7亿，在生成图像的真实性和多样性上取得巨大进步，生成了可以假乱真的图像。另一个是自监督学习，以变分自动编码器（VAE）[24]为代表的自动编码器通过将模型分割为编码器、解码器两个部分，先将数据编码到隐变量空间，再从隐变量空间解码恢复数据。这种方法使数据自身成为标签，在不使用任何人工标注的情况下从大规模无标签数据中学习数据特征。除了以原始数据作为标签外，其他多种建立自标签的方法也陆续被发现。2021年Diffusion Model[25]则是将向原始图像添加的高斯噪音作为标签，让模型从加噪的图像中预测噪音，从而学习得到降噪编码器。将这样多个降噪编码器层层叠加，就可以从噪音中得到图像。这种方法可以使深度学习模型生成前所未有的高清、逼真图像。2022年潜在扩散模型（LDM）[26]大幅提升了高分辨率图像的效率，使AI内容生成技术更加实用化。AI在未来音乐、视频、游戏、元宇宙内容生成中有广阔的应用前景。

正是由于过去10年中深度学习算法的长足发展，如今AI已在千行百业中拥有广泛的应用场景[27-36]，产业规模持续扩大，成为数字经济下不可或缺通用基础技术，对经济增长意义重大。

1.2 算力需求驱动芯片迅速发展

J. SEVILLA等[37]对AI主要算法所需要的算力进行了汇总。过去10年在模型训练方面，模型所需的算力增长超过了100万倍。深度学习对算力的巨大需求推动了AI芯片快速发展。在这10年中，主流AI芯片架构经历了3代进化。

第1代（2012—2016年）AI芯片架构是通用图形处理器（GPGPU）。这一时期深度学习刚刚起步，网络规模并不大。这一代芯片架构没有针对神经网络计算进行加速的特殊设计，而是利用GPGPU已有的单指令多线程（SIMT）计算核心来提升向量、矩阵并行计算效率。SIMT架构特点是硬件根据数据自动分支，既可以像单指令多数据（SIMD）一样高效，又可以像多指令多数据（MIMD）一样灵活。但SIMT是为通用计算设计的，依赖共享内存交换中间数据，功耗大，算力并不高。

第2代AI芯片架构从2016年开始出现，时至今日仍是主流。这一时期卷积神经网络成为最主流的算法。AI芯片以加速卷积神网络为首要目标。ResNet成为AI芯片性能测试标准。这一代架构以谷歌张量处理器（TPU）[38]为代表，其主要特点是将AI计算抽象为标量、向量、矩阵3类计算。计算核心包含对应的3种专用计算单元，可以提供很高的峰值算力。同时核心内置容量较大的静态随机存取存储器（SRAM）作为本地存储。因此，第2代AI芯片架构在算力和功耗上相对于第1代架构有了巨大的提升。但是这一代架构在通用性上较差，在应对各种尺寸的神经网络时难以表现出很好的计算效率，同时在可编程、灵活性上不如第1代架构，面对不断涌现的新算法和新场景，日益显示出应用场景的局限性和软件开发的高成本弊端。

同一时期，GPGPU在计算核心中增加专门的矩阵计算单元Tensor Core[39]，这样既拥有高性能，又拥有强大的可编程性和灵活性，依靠完备的工具链和成熟的生态，具有突出的市场竞争力。因此，对于第2代AI芯片架构，从数量上看是百花齐放，从市场占有率上看却是一枝独秀。拥有Tensor Core的GPGPU，例如NVIDIA Volta、Ampare系列，成为这一代AI芯片的最终赢家。

第3代AI芯片架构产生于2019年，这一时期出现了Transformer模型。该模型迅速发展，并与卷积神经网络形成了分庭抗礼的局面。特别是随着大规模预训练模型和多模态的进展，Transformer很可能会最终取代卷积神经网络（CNN）。摆在芯片架构设计面前的挑战有两个：（1）需要对Transformer进行优化设计。相对于CNN，同等算力的Transformer模型对带宽的要求更高，这增加了芯片设计的难度。（2）系统需要具备优秀的水平扩展能力，以满足急速增长的大模型训练算力需求。这一代架构以GraphCore[40]、Tenstorrent[41]为代表，其特点是在单一芯片拥有上百甚至上千个计算核心。同时芯片间具备良好的水平扩展能力，可以实现从单核到百万核的无缝扩展。为保证如此大规模并行计算高效运行，需要采用软硬件协同设计，特别是需要图编译器对多核上的计算任务派发和数据路由做出优化调度，以便隐藏数据传输等额外开销，实现一加一等于二的并行计算效果。然而，这一代架构大幅增加了编译器的开发难度，芯片可编程性和灵活性相对上一代架构并未得到明显的提升，工具链和生态建设难度大。与此同时，GPGPU的TensorCore已具备专用的Tensformer加速引擎。第3代AI芯片架构中谁是最终胜利者，仍需要时间来给出答案。

算法的不断发展对AI芯片架构提出越来越高的要求。我们认为未来AI芯片架构必须要具备如下综合能力：在性能方面，对Transformer模型有优秀的加速能力；在功耗方面，8位整数（INT8）等效算力达到10 TOPS/W以上；在通用性方面，对各种规模的模型都可以达到较高的硬件利用率；在可编程性方面，可以通过编程支持新的算法且容易开发，具备完整的工具链，能够快速完成模型的开发和部署。

2 第2个10年展望

在深度学习的第2个10年，数据、算法、算力三大要素依旧占据核心地位。但随着AI的应用越来越广泛和深入，绿色、生态、可信将成为AI可持续发展新的核心要素。

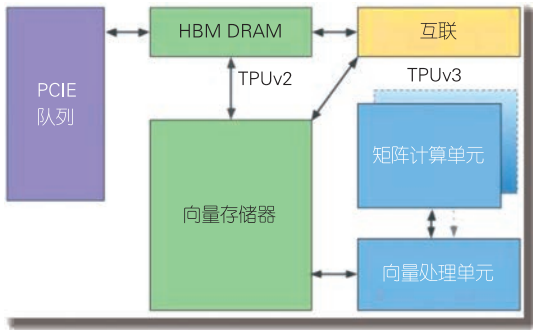
2.1 AI芯片创新实现绿色节能

2019年一项研究表明，完成一次Trasformer（Big）模型训练所排放的二氧化碳高达282吨，相当于5辆汽车整个生命周期的CO_2排放量[42]。目前，全世界1%的发电量被用于AI计算。全球AI计算能耗年增长率为37%。据此估算，下一个10年，AI计算将消耗全世界发电量的15%左右，将为环境带来沉重的负担。为了实现绿色可持续发展，必须不断研究更有效率的AI芯片。

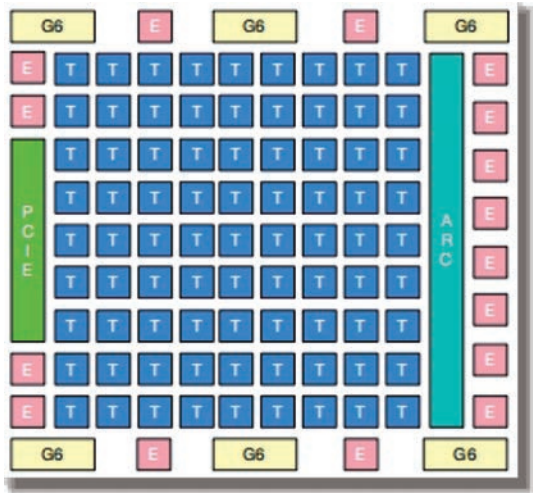
提升AI芯片效率的一个方向是空间计算。众所周知，AI芯片功耗与数据在芯片内搬运的距离正相关。借助创新的芯片架构设计，减少完成每次操作数据在芯片内需要移动的距离，就可以大幅降低芯片的能耗。

这里我们对Google TPUv3和Tenstorrent Wormhole两个AI芯片进行对比。如图1（a）所示，TPU计算核心设计是采用一个较大的向量和矩阵计算单元同本地SRAM相连接，完成一个神经网络算子的计算，需要将数据从Vector Memory搬移到Matrix Multiply Unit完成矩阵乘计算，然后再搬移到Vector Unit完成Element-wise计算。这种大计算、大存储单元的设计导致每次计算数据平均移动距离达到毫米级别，因此芯片功耗高，以至于必须采用水冷才能使TPU集群系统正常运行。在图1（b）中，每颗Wormhole芯片包含80个Tensix计算核心。每个计算核心拥有约5 TOPS的算力以及1.5 MB的本地存储。由于大多数计算能够在单核心内完成，因此更小的核心能够缩短数据移动距离。只有少数的跨核心计算才需要将数据搬运到更远的地方。据估算，Wormhole芯片每次操作数据的平均移动距离只有TPUv3的1/10左右。因此，Wormhole芯片功效比要高得多，达到3 TOPS/W@INT8，而TPUv3的为0.6 TFOPS/W@BF16。

将一个包含大计算、大存储单元的计算核心拆分为多个包含小计算、小存储单元的计算核心，可以有效降低每次计算数据移动的平均距离，从而降低芯片能耗。这也成为新一



（a）Google TPUv3



（b）Tenstorrent Wormhole

ARC：一种嵌入式微处理器　　PCIE：一种高速串行计算机扩展总线标准
DRAM：动态随机存取存储器　　TPU：张量处理器
HBM：高带宽内存

▲图1 Google TPUv3和Tenstorrent Wormhole架构示意图

代AI芯片的设计趋势。然而，这种多核并行计算会引入额外的开销，导致计算效率降低。相应的解决方案是通过软硬件架构协同设计，将一个计算任务拆分为多个子任务，然后将子任务指派到不同的计算核心上，并规划任务之间数据传输路径，最优匹配芯片的算力、存储、数据传输带宽、互联拓扑结构，减少数据移动距离，从而实现性能最优、功耗最低。这种将多个计算任务在空间（多核）上进行调度的计算方式被称为“空间计算”。

实现多核空间计算需要软硬件协同设计。在硬件方面，为提升并行计算效率，计算核心可以增加对AI并行计算常用通信模式的硬件支持，如Scatter、Gather、Broadcast等，对数据包进行封装、压缩等，在核间互联上优化片上网络拓扑结构和动态路由能力。在软件方面，由于空间计算的优化非常复杂，非开发人员所能负担，需要编译器自动实现任务的拆分、指派、路由规划，在运行时需要完成计算过程控制，特别是对空间计算过程中产生的各种异常（如丢包、乱序、拥塞）进行处理。

未来空间计算的一条演进路线是在存计算（At-Memory）。在存计算可以把一个大的计算核心拆分为上万个微型计算核心，而不仅仅是上百个小核心。在这种架构下，每个计算数据平均移动距离将进一步降低至微米级，功效比可以超过10 TOPS/W@INT8。例如Untether AI公司的Bo-queria[43]芯片拥有上万个处理引擎（PE）。每个PE配置6 kB本地内存，整个芯片的内存带宽高达PB/s级。PE与本地内存之间的数据移动距离仅有几微米，功效比高达30 TFOPS/W@FP8。然而，由于存在面积限制，每个PE功能简单、灵活性差，只适用于一些特定算法，目前只能进行推理，无法进行训练。此外，将计算任务部署在上万个PE上，对编译器的优化能力提出了更高的要求。

空间计算技术的另一条演进路线是确定性设计。编译器优化能力对空间计算的性能至关重要，但只能利用静态信息对计算进行调度。因此，重新设计系统的软件-硬件界面、静态-动态界面，使编译器能够利用更多的静态信息，成为一个新的技术演进方向。例如，Groq公司的张量流处理器（TSP）[44]芯片采用确定性硬件设计，芯片中没有Arbiter、Crossbar、Cache等“响应型”组件，允许编译器进行时钟级的调度。编译器可以精确地调度每个核上的计算、内存访问和数据传输，使得指令流在运行期内完全避免共享资源的访问冲突，因此可以实现无锁，系统极为高效。但是，这种确定性设计需要编译器接管到硬件状态机级别，复杂度很高。实现系统级硬件确定性非常复杂，需要实现全局时钟、链路延迟补偿、时钟漂移补偿等机制，引入硬件对齐计数器、软件对齐计数器、指令集。

随着3D封装技术的日趋成熟，空间计算还可以向3D的方向发展。将一颗大计算核心拆分为多个小核心，并在3D方向堆叠起来，可以进一步缩短数据移动的距离，从而进一步降低芯片功耗，提升能效比。此外，相对于传统2D芯片，经由3D封装技术，3D Mesh、3D torus等片上网络（NOC）拓扑更有效率，从而给编译器留下更大的调度优化空间，进一步提升空间计算性能。

提升AI芯片效率的第2个方向是近似计算。深度学习模型的一个特征是对精度要求不高。计算过程中出现的误差并不会显著影响模型的最终判定结果。近似算法可以减少内存使用和计算复杂度，使计算更加高效。

低精度计算是深度学习近似计算一个重要的技术方向。使用低精度的数据类型，可以有效减少芯片面积和功耗。例

如，INT8的乘法和加法运算所消耗的能量仅为32位浮点数（FP32）的1/30和1/15[45]。目前混合精度训练技术可以使用FP16位半精度浮点数和FP32单精度浮点数配合完成模型训练。Transformer模型的训练则可以使用更低的精度浮点数。例如，NVIDA在其最新的Hopper架构中实现了FP16和FP8混合精度训练Transformer模型[46]。未来仍有可能出现更低精度的训练算法。

由于推理对精度的要求更低，因此在完成模型训练之后，我们可以将模型转化为更低精度的数据类型表示，这个技术称之为模型量化。目前，INT8量化技术已经相当成熟，INT4量化技术仍然面临一些困难。特别是在模型中使用了非线性激活函数时，模型准确率下降很多。对此，一种思路是使用INT8和INT4自适应混合精度量化，另一种思路是将模型量化为FP8。FP8的面积和功耗仅有INT8的一半，但模型判定准确率没有明显下降。

近似计算的另一个演进路线是稀疏计算。研究发现，深度学习模型的权重存在一定的稀疏性，即部分权重值为零或者非常接近于零，特别是Transformer模型的稀疏度更大。利用模型的稀疏性可以省略不必要的计算，从而提升模型计算的效率。例如，NVIDIA A100 GPGPU中的4选2稀疏加速可以将芯片等效算力提升一倍[47]，同时功耗保持不变。Tenstorrent Wormhole芯片更是可以在模型稀疏度90%的情况下，将芯片等效算力提升100倍。未来软硬件协同下稀疏计算仍然会是一个非常有前景的技术方向。新模型的稀疏化算法、稀疏加速计算核心仍然是研究的热点。

未来10年，依靠制程提升能效比的难度越来越大，而空间计算、近似计算在提升芯片能效比方面存在巨大潜力。相对于目前的主流AI芯片，未来的芯片效能将有数十倍的提升，是AI产业实现双碳目标的有力保障。

2.2 生态融合实现降本增效

深度学习模型的研发和应用可以分为两个阶段，一是模型的训练，二是模型的应用服务。完成训练并达到业务性能要求的模型，最终形成各种形式的模型应用服务，产生商业价值。当前，从模型训练完成到部署的过程，还存在诸多痛点，无法很好的满足规模化部署的要求。

首先，目标硬件多种多样，如X86/ARM中央处理器（CPU）、GPGPU、现场可编程门阵列（FPGA）、专用集成电路（ASIC）芯片等。随着新的AI芯片层出不穷，各厂商芯片之间架构、指令集、软件工具链互不兼容，缺乏统一标准，容易引起生态碎片化问题。上层算法和应用与底层硬件紧耦合。跨硬件部署同一模型需要大量移植工作，这大幅增加了深度学习模型的研发成本和应用难度。其次，部署阶段的场景主要分为云侧、边缘侧、端侧，有基于容器化部署场景，也有基于嵌入式硬件部署的场景。不同部署场景对模型推理的性能需求、计算资源、App调用方式等要求不同。因此不同部署方案需要具备不同的技术。再次，模型开发使用的训练框架各不相同，如TensorFlow、PyTorch、Paddle - Paddle、Caffe、Keras、OneFlow。不同框架训练后保存的模型格式均不相同，在部署时需要做针对性处理，即需要一一转换到目标硬件支持的模型格式。但转换路径较为繁杂，用户需要付出较多的学习成本。

性能优化也是深度学习模型在落地时经常遇到的问题，例如计算时延高、吞吐量低、内存占用大等。在不同的应用场景和部署环境下，模型的优化目标不完全相同。例如，在端侧部署中，内存和存储空间均非常有限，模型的优化目标是减小模型的大小；在自动驾驶场景下，由于计算平台算力有限，对模型的优化侧重于在有限的算力下，尽可能提升吞吐量，降低时延。模型优化技术包括模型压缩和硬件执行优化，涉及模型剪枝、量化、稀疏化、模型中间表示（IR）、可执行文件的编译器，以及基于硬件架构的高性能计算等多项关键技术点。

为应对上述挑战，中兴通讯主导了Adlik开源项目[48]。Adlik是将深度学习模型部署至特定硬件并提供模型应用服务的端到端工具链，能够与多种推理引擎协作，提供灵活的模型加速、部署、推理方案，助力用户构建高性能AI应用。

Adlik的整体架构包括模型优化器、编译器和引擎模块。它支持各类模型在云、边、端侧多种硬件上的灵活部署和高效执行。

Adlik模型优化器支持多种结构化剪枝方法，能够有效降低模型参数量和算力需求，支持多节点、多GPU并行剪枝以提升系统效率，同时支持自动剪枝方法。用户只需要指定神经网络类型（如ResNet-50）和限制条件（如算力、延迟），模型优化器会自动决定模型每一层的通道数，得到在限制条件下最优的模型结构[49-50]。在模型量化方面，Adlik模型优化器支持8 bit量化，可以利用少量校准数据快速实现8 bit训练后量化（PTQ）；也支持量化感知训练（QAT）算法，提升量化模型精度。Adlik模型优化器提供不同的蒸馏方法，能够应用于各种深度学习任务（如图像分类、目标检测等）。如表1所示，针对ResNet-50模型优化研究，在执行剪枝、蒸馏和INT8量化后，Adlik模型推理吞吐量提升13.82倍，同时模型准确率没有降低[51]。

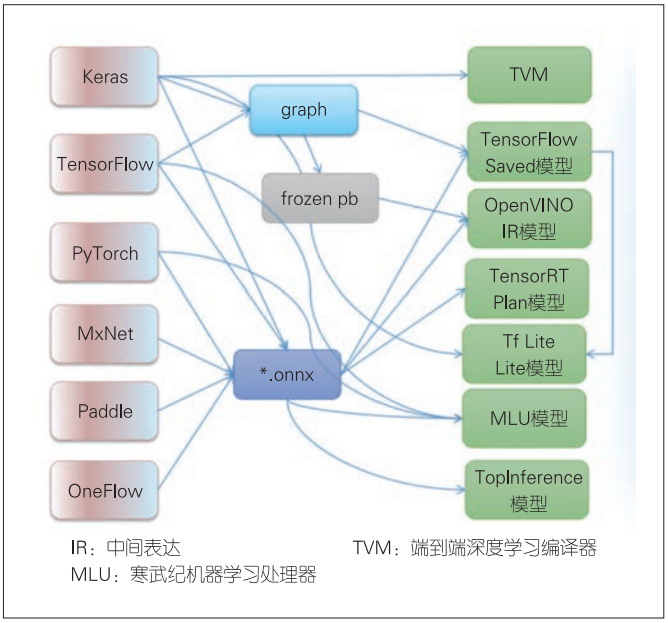
Adlik模型编译器支持不同的训练框架模型格式和推理框架模型格式之间的转换，并易于扩展，如图2所示。因

▼表1 Adlik模型优化器性能测试结果

模型优化方法	吞吐量（OpenVINO）	精度/%
基线	432	76.80
自动剪枝	1 615	73.30
自动剪枝+蒸馏	1 615	77.50
自动剪枝+蒸馏+INT8量化	6 401	77.00

INT8：8位整数　　OpenVINO：开放视觉推理及神经网络优化

此，在设计上Adlik模型编译器采用自动构建有向无环图（DAG）的方式生成源模型格式和目标模型格式的转换路线。用户只需要给出源和目标模型格式，Adlik模型编译器就可以使用最优转换路线，端到端地完成模型格式的转换[52]。目前，除了业界常用的TensorFlow和PyTorch之外，Adlik还引入了国产训练框架PaddlePaddle和OneFlow，并支持国产推理芯片厂商（寒武纪、燧原等）的推理模型格式。



▲图2 Adlik模型编译依赖图

Adlik模型应用服务存在Serving和Embedding两种方式。Adlik Serving以独立的微服务部署，支持多个客户端的推理请求服务。支持表述性状态转移（REST）和远程过程调用（RPC）接口，相关模型的版本控制和管理，可以在保持业务不中断的情况下完成模型的滚动升级。Adlik Serving的特色是以插件的方式部署和隔离各种运行时的环境，如TensorFlow、OpenVINO、Tf Lite、TensorRT、Paddle Inference等，使应用可按需加载。Serving SDK提供模型推理开发的基础类库。用户可扩展实现推理运行时的自定义开发，如实现多模型在进程内协作的推理服务、低时延嵌入式设备的推理服务等。Serving SDK提供模型上载、模型升级、模型调度、模型推理、模型监控、运行时隔离等基础模型管理功能，以及用户定制与开发推理服务的C++应用程序编程接口（API）。应用根据自身的需求，定制开发自己的模型和运行时。Serving SDK提供标准的扩展点，方便用户高效地定制新的模型和运行时环境。

Adlik支持云、边缘、端3种部署场景并提供相应的特性支持[53]：（1）在云侧，支持原生容器化部署方案、优化和编译完成的模型，可以和Adlik Serving Engine镜像一起打包，发布为应用服务镜像，并在指定硬件的容器云上运行；（2）在边缘侧，支持在启动的Adlik Serving Engine服务上加载优化和编译完成的模型，支持多模型实例调度功能，减少边缘侧计算资源的占用；（3）在端侧，支持用户优化和编译完成的模型，结合特定的计算引擎依赖库和交叉编译工具链，可编译为运行在指定硬件上的可执行文件。同时Adlik可以提供C/C++的API接口，用来提供模型编排能力，为用户提供低延时、小体积并可在指定硬件上运行的模型应用。

Adlik是对生态融合的一次尝试，用一套统一的工具链打通不同框架和硬件供应商相互割裂的生态，从而实现深度学习部署应用降本增效，为下一个10年更大规模的深度学习应用打下良好基础。未来Adlik将进一步围绕深度学习端到端性能优化、AI应用在异构平台上的部署与运行、高性能计算、模型运维等技术方向发展，持续构建社区生态，推动产业推动数字化变革，为用户打通深度学习应用的全流程，真正实现高效率、低成本的AI应用落地，助力不同行业实现智慧化转型，为数字经济发展提供强劲动力。

2.3 安全可信任实现深度应用

随着AI广泛应用于金融、交通、医疗等诸多领域，AI自身的脆弱性、黑盒等导致的安全问题和可信危机逐渐突显。例如，以色列科研人员生成的9张万能人脸可以冒充超40%的人[54]，微软聊天机器人Tay发表歧视女性相关言论[55]，没有任何犯罪记录的黑人被AI判定为更具危险性，自动驾驶汽车引发多起交通事故等。

在此背景下，世界主要国家和组织，纷纷出台AI安全和可信的法律法规、道德伦理规范和标准，用于规范和引导AI的安全生产和应用，并将AI的安全使用上升到国家战略高度。例如，中国将“促进公平、公正、和谐、安全，避免偏见、歧视、隐私和信息泄露等问题”写入《新一代AI伦理规范》[56]总则。

综合AI安全、可靠、可解释、可问责等方面的需求，

可信AI的概念被提出[57]。可信AI被业界归结为4个方面。（1）可靠性：AI系统在面临恶意攻击和干扰的情况下，能够提供正确决策和正常服务的能力；（2）隐私安全性：AI的开发和应用不能造成个人或者群体隐私信息的泄露；（3）可解释性（透明性）：AI系统的决策能够被人类用户理解，并能提供相应的解释；（4）公平性（包含个体公平性和群体公平性）：AI系统不因个体或群体差异而给出不公正的输出。因此，我们应该规范、安全地开发和使用AI，在享受技术发展带来红利的同时避免技术自身缺陷带来的负面影响。

发展可信AI意义重大，其价值主要体现在以下两个方面：

（1）有助于打破数据孤岛，充分释放数据要素价值，决定AI未来发展应用的广度和深度。一方面数据要素作为重要的战略资源，需要充分流通和共享才能释放巨大的价值，加速社会的数字化转型；另一方面数据使用过程中的隐私保护已经成为法律、法规的基本要求，例如一般数据保护条例（GDPR）[58]、《中华人民共和国网络安全法》[59]等。在此背景下发展以联邦学习[60]为代表的隐私安全机器学习方法、隐私安全计算[61]就显得尤为重要。这对打破因隐私安全造成的数据孤岛、挖掘各行各业的数据价值具有重大意义。

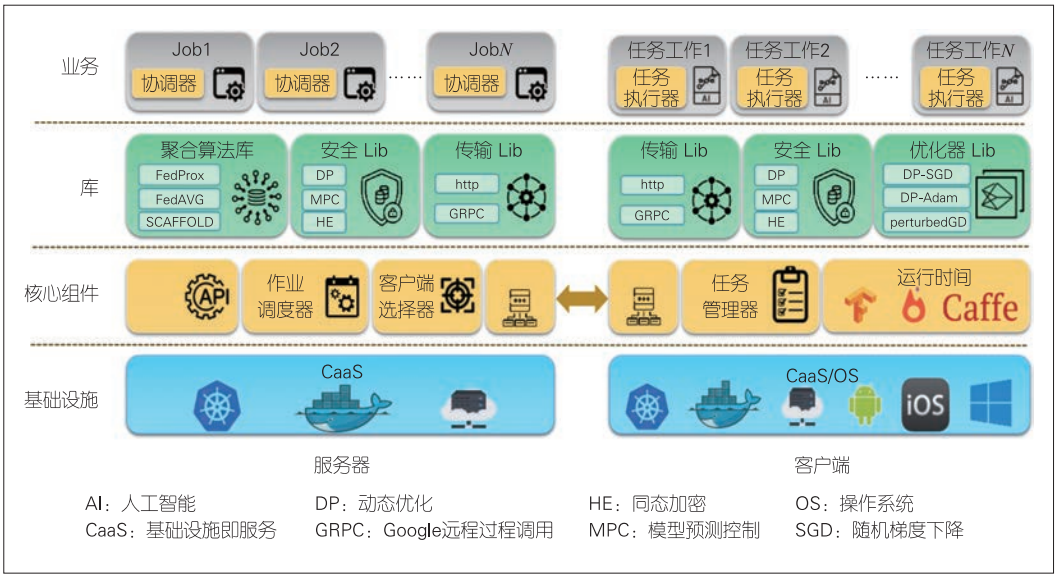
（2）安全、可靠、透明、合乎伦理规范的AI能消除人们对AI的疑虑，从而释放产业价值。AI的内生安全[62]已经引发人们的担忧，具体表现在：（a）贯穿AI生命周期、种类繁多的攻击会引起人们对可靠性的担忧，相关攻击包括对抗样本攻击、投毒攻击、后门攻击、模型窃取等[63-66]；（b）AI的黑盒特点使系统难以给出决策依据，导致在安全关键领域的决策难以被采纳；（c）AI在某些应用场景中表现出来的公平性缺失[67]，引发人们对其道德伦理的担忧。解决上述问题，构建公众对AI的信心，才能让AI被广泛接纳和使用，从而进一步扩大产业规模和价值。

综上所述，可信AI决定和影响着AI发展的可持续性和未来产业规模，而规范、法律、标准的出台更让其成为发展AI的必选项和基本准入门槛。

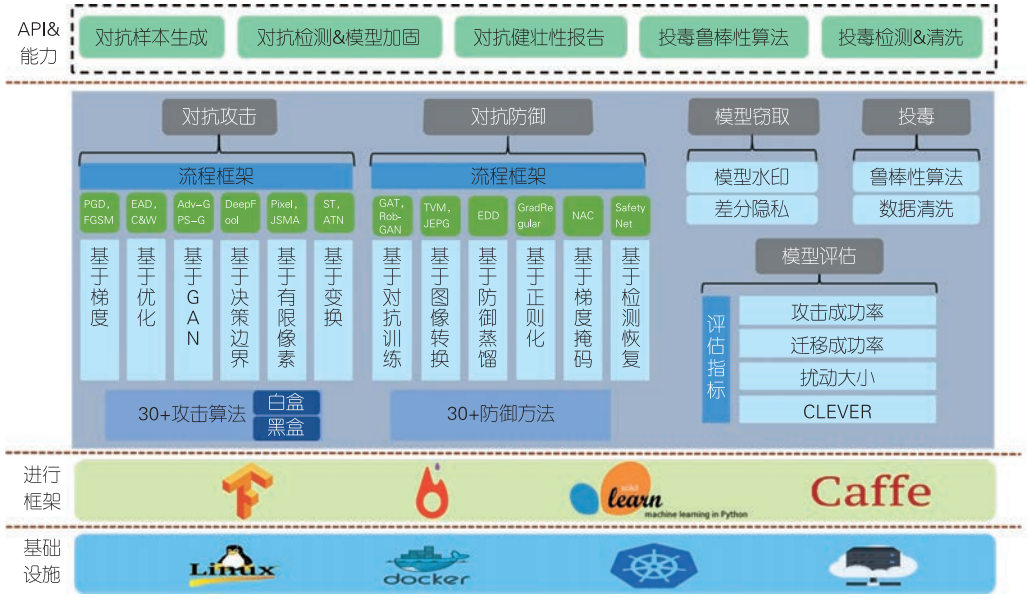
中兴通讯在可信AI方面积极投入，创建了Nuersafe开源社区（https://github.com/neursafe）。Nuersafe开源社区包含联邦学习、AI安全、AI公平和AI可解释4个平台，覆盖可信AI的4个要素。目前我们重点研究了联邦学习（Neursafe-FL[68]）和AI安全工具（Neursafe-Security）。下面我们将针对这两个方面做详细介绍。

（1）Neursafe联邦学习。该平台的目标是在隐私安全的前提下，打造可靠、高效、易用的联邦学习解决方案，如图3所示。为了实现这一目标，在设计和实现中我们应做出如下几个方面的考虑：（a）进行微服务架构设计，以满足系统灵活部署的需求，提供单机、Cross-Silo、Cross-Device 3种部署模式，并可满足科研验证、跨企业数据孤岛、海量设备联合训练等多种场景的需求。（b）拥有完备的框架能力，可提供分布式资源管理和作业调度能力，通过调度算法最大化联邦学习性能。（c）通过核心组件的高可用设计和作业级的容错处理机制，保证系统持续可服务性。（d）支持Tensorflow和Pytorch两种主流底层机器学习框架，并支持框架扩展；通过用户层极简的联邦API设计，最大程度上保留底层框架编程习惯，降低原机器学习算法向联邦学习迁移的成本。（e）封装基于差分隐私和安全多方计算等隐私算法库，并标准化算法接口，支持算法扩展。（f）提供多种算法（FedAvg、Scaffold、FedProx、FedDC等[69-72]）构成的聚合和优化算法库，满足不同数据异构场景下的收敛效率需求。

（2）Neursafe AI安全。如图4所示，该平台以工具化的方式，提供AI对抗攻击、模型鲁棒性检测以及模型加固和对



▲图3 Neursafe联邦学习架构



Adv-G：对抗生成对抗网络
API：应用程序接口
ATN：对抗变换网络
C&W：基于优化的攻击
EAD：弹性网络攻击
EDD：扩展防御蒸馏
FGSM：快速梯度符号下降法
GAN：生成对抗网络
GAT：生成对抗训练
JPEG：JPEG Compression，JPEG压缩
JSMA：基于雅克比的显著图攻击
NAC：噪声增强分类器防御
PGD：投影梯度下降法
PS-G：感知敏感生成对抗网络
Rob-GAN：一种基于GAN的防御方法
ST：空间变换攻击
TVM：总体方差最小防御

▲图4 Neursafe 人工智能安全架构

抗样本检测等能力。该平台可以实现：（a）统一服务入口，屏蔽底层算法实现，支持命令行、API和SDK 3种接口形式，一键完成对模型的对抗攻击、鲁棒性检测、安全防御加固等功能使用。（b）支持30+的黑、白盒攻击算法，其中30+的防御算法涵盖了当前主流且经典的攻防算法。（c）对当前主流的攻击和防御算法进行分类，如基于梯度的攻击、基于遗传算法的攻击、基于对抗训练的防御等，提取同类算法共性，在算法基类中实现框架代码，简化后续算法创新开发工作量。（d）支持Auto Attack，自学习攻击参数；支持多种攻防算法的正交组合，增强综合攻防能力。（e）攻防算法一次编码，兼容Tensorflow和Pytorch，解决了主要当前攻防工具支持底层框架单一问题。（f）支持模型鲁棒性检测功能，能进行模型鲁棒性的综合评估，生成界面优化的评估报告。（g）支持模型加固、对抗样本检测、对抗样本恢复3种防御手段，满足不同场景下的安全防御需求，在模型已经上线运行的情况下可以通过增加前置检测网络来实现安全防御。

可信AI的研究进展对AI的可持续发展至关重要。中兴通讯将继续关注可信AI，对未来可信AI的研究工作有如下规划：（1）将坚持开源运作，和业界一起共筑可信AI未来；（2）补齐当前在公平和可解释方面的缺失，构建可信AI的全方位能力；（3）针对可信AI中的问题，如联邦学习中的性能问题、AI安全中的碎片化问题，跟踪业界最新进展，对算法进行创新研究，逐步扫除解决方案的落地障碍；（4）坚持产品化的思维，站在用户角度，提供简单、用户友好的解决方案。

3 结束语

经过3次发展浪潮，AI已经快速走出低谷期。在第2个10年学术研究、产业落地的双轮驱动下，研究者数量、论文数量、数据量、算力、产业规模等维度将保持指数增长态势。绿色、高效、安全是下一个10年深度学习维持可持续指数增长的3个新的核心要素，是实现中国新一代AI发展规划三步走[73]、2030年AI核心产业突破十万亿元的关键。

参考文献

[1] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[C]//Proceedings of the 25th International Conference on Neural Information Processing Systems-Volume. ACM, 2012: 1097-1105. DOI: 10.5555/2999134.2999257
[2] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition [C]//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2016: 770-778. DOI: 10.1109/CVPR.2016.90
[3] VASWANI A, SHAZEER N, PARMAR N, et al. 2017. Attention is all you need [EB/OL]. [2022-10-12]. https://arxiv.org/abs/1706.03762
[4] HOCHREITER S, SCHMIDHUBER J. Long short-term memory [J]. Neural computation, 1997, 9(8): 1735-1780. DOI: 10.1162/neco.1997.9.8.1735
[5] DEVLIN J, CHANG M W, LEE K, et al. BERT: pre-training of deep bidirectional transformers for language understanding [EB/OL]. [2022-10-12]. https://aclanthology.org/N19-1423/
[6] LIU X, ZHANG F J, HOU Z Y, et al. Self-supervised learning: generative or contrastive [J]. IEEE transactions on knowledge and data engineering, 2022, 35(1): 857-876. DOI: 10.1109/TKDE.2021.3090866
[7] BROWN T B, MANN B, RYDER N, et al. Language models are few-shot learners [EB/OL]. [2022-10-12]. https://arxiv.org/abs/2005.14165
[8] 马子轩, 翟季, 韩文弢, 等. 高效训练百万亿参数预训练模型的系统挑战和对策[J]. 中兴通讯技术, 2022, 28(2): 51-58
[9] DOSOVITSKIY A, BEYER L, KOLESNIKOV A, et al. An image is worth 16x16 words: transformers for image recognition at scale [EB/OL]. [2022-10-12]. https://arxiv.org/abs/2010.11929
[10] RAMESH A, PAVLOV M, GOH G, et al. Zero-shot text-to-image generation [EB/OL]. [2022-10-12]. https://arxiv.org/abs/2102.12092
[11] LIU J, ZHU X, LIU F, et al. OPT: omni-perception pre-trainer for cross-

modal understanding and generation [EB/OL]. [2022−10−12]. https://arxiv.org/abs/2107.00249
[12] LIN J, MEN R , YANG A, et al. M6: a Chinese multimodal pretrainer [EB/OL]. [2022−10−12]. https://arxiv.org/abs/2103.00823
[13] SILVER D, HUANG A, MADDISON C J, et al. Mastering the game of Go with deep neural networks and tree search [J]. Nature, 2016, 529(7587): 484−489. DOI: 10.1038/nature16961
[14] SILVER D, SCHRITTWIESER J, SIMONYAN K, et al. Mastering the game of Go without human knowledge [J]. Nature, 2017, 550(7676): 354−359. DOI: 10.1038/nature24270
[15] SILVER D, HUBERT T, SCHRITTWIESER J, et al. Mastering chess and shogi by self−play with a general reinforcement learning algorithm [EB/OL]. [2022−10−12]. https://arxiv.org/abs/1712.01815
[16] BROWN N, SANDHOLM T. Safe and nested subgame solving for imperfect−information games [EB/OL]. [2022−10−12]. https://arxiv. org/abs/1705.02955
[17] BERNER C, BROCKMAN G, CHAN B, et al. Dota 2 with large scale deep reinforcement learning [EB/OL]. [2022−10−12]. https://arxiv. org/abs/1912.06680
[18] VINYALS O, BABUSCHKIN I, CZARNECKI W M, et al. Grandmaster level in StarCraft II using multi−agent reinforcement learning [J]. Nature, 2019, 575(7782): 350−354. DOI: 10.1038/s41586−019−1724−z
[19] WU Z, LIAN W Z, UNHELKAR V, et al. Learning dense rewards for contact−rich manipulation tasks [EB/OL]. [2022−10−12]. https://arxiv. org/abs/2011.08458
[20] DEGRAVE J, FELICI F, BUCHLI J, et al. Magnetic control of tokamak plasmas through deep reinforcement learning [J]. Nature, 2022, 602(7897): 414−419. DOI: 10.1038/s41586−021−04301−9
[21] FAWZI A, BALOG M, HUANG A, et al. Discovering faster matrix multiplication algorithms with reinforcement learning [J]. Nature, 2022, 610 (7930): 47−53. DOI: 10.1038/s41586−022−05172−4
[22] GOODFELLOW I, POUGET−ABADIE J, MIRZA M, et al. Generative adversarial networks [J]. Communications of the ACM, 2020, 63(11): 139−144. DOI: 10.1145/3422622
[23] BROCK A, DONAHUE J, SIMONYAN K. Large scale GAN training for high fidelity natural image synthesis [EB/OL]. [2022−10−12]. https://arxiv. org/abs/1809.11096
[24] KINGMA D P, WELLING M. Auto−encoding variational bayes [EB/OL]. [2022−10−12]. https://arxiv.org/abs/1312.6114
[25] HO J, JAIN A, ABBEEL P. Denoising diffusion probabilistic models [EB/OL]. [2022−10−12]. https://arxiv.org/abs/2006.11239
[26] ROMBACH R, BLATTMANN A, LORENZ D, et al. High−resolution image synthesis with latent diffusion models [C]//Proceedings of 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2022: 10674−10685. DOI: 10.1109/CVPR52688.2022.01042
[27] 熊先奎, 袁进辉, 宋庆春. 面向分布式AI的智能网卡低延迟Fabric技术 [J]. 中兴通讯技术, 2020, 26(5): 23−28
[28] SHI W Q, SUN Y X, HUANG X F, et al. Scheduling policies for federated learning in wireless networks networks: an overview [J]. ZTE communications, 2020, 18(2): 11−19
[29] 曹晓雯, 莫小鹏, 许杰. 面向边缘智能的空中计算 [J]. 中兴通讯技术, 2020, 26 (4): 31−37. DOI: 10.12142/ZTETJ.202004007
[30] YANG H H, ZHAO Z Y, QUEK T Q S. Enabling intelligence at network edge: an overview of federated learning [J]. ZTE communications, 2020, 18 (2): 2−10. DOI: 10.12142/ZTECOM.202002002
[31] 朱近康. 知识+数据驱动学习: 未来网络智能的基础 [J]. 中兴通讯技术, 2020, 26(4): 46−49. DOI: 10.12142/ZTETJ.202004011
[32] LIU W C, SHEN M Q, ZHANG A D, et al. Artificial intelligence rehabilitation evaluation and training system for degeneration of joint disease [J]. ZTE communications, 2021, 19(3): 46−55. DOI: 10.12142/ZTECOM.202103006
[33] 程强, 刘姿杉. 数据驱动的智能电信网络 [J]. 中兴通讯技术, 2020, 26(5): 53−56. DOI: 10.12142/ZTETJ.202005010
[34] ZHANG C C, ZHANG N, CAO W, et al. AI−based optimization of handover strategy in non−terrestrial networks [J]. ZTE Communications, 19(4): 98−104, DOI: 10.12142/ZTECOM.202104011
[35] YANG K, ZHOU Y, YANG Z P, et al. Communication−efficient edge AI inference over wireless networks [J]. ZTE communications, 2020, 18(2): 31−39
[36] 李高, 王威, 吴启晖. 面向低轨卫星的频谱认知智能管控 [J]. 中兴通讯技术, 2021, 27(5): 7−11. DOI: 10.12142/ZTETJ.202105003
[37] SEVILLA J, HEIM L, HO A, et al. Compute trends across three eras of machine learning [C]//Proceedings of 2022 International Joint Conference on Neural Networks (IJCNN). IEEE, 2022: 1−8. DOI: 10.1109/IJCNN55064.2022.9891914
[38] JOUPPI N P, YOUNG C, PATIL N, et al. In−datacenter performance analysis of a tensor processing unit [C]//Proceedings of 2017 ACM/IEEE 44th Annual International Symposium on Computer Architecture (ISCA). IEEE, 2017: 1−12
[39] NOVID. Nvida tesla V100 GPU architecture [EB/OL]. [2022−10−12]. https://images. nvidia. com/content/volta−architecture/pdf/volta−architecture−whitepaper.pdf
[40] JIA Z, TILLMAN B, MAGGIONI M, et al. Dissecting the graphcore IPU architecture via microbenchmarking [EB/OL]. [2022−10−12]. https://arxiv.org/abs/1912.03413
[41] PATEL, D. Tenstorrent wormhole analysis: a scale out architecture for machine learning that could put Nvidia on their back foot [EB/OL]. [2022−10−12]. https://www. semianalysis. com/p/tenstorrent−wormhole−analysis−a−scale
[42] STRUBELL E, GANESH A, MCCALLUM A. Energy and policy considerations for deep learning in NLP [EB/OL]. https://arxiv. org/abs/1906.02243
[43] BEACHLER R, SNELGROVE M. Untether ai: boqueria [C]//Proceedings of 2022 IEEE Hot Chips 34 Symposium (HCS). IEEE, 2022: 1−19. DOI: 10.1109/HCS55958.2022.9895618
[44] ABTS D, KIM J, KIMMELL G, et al. The Groq Software−defined Scale−out Tensor Streaming Multiprocessor: from chips−to−systems architectural overview [C]//Proceedings of 2022 IEEE Hot Chips 34 Symposium (HCS). IEEE, 2022: 1−69. DOI: 10.1109/HCS55958.2022.9895630
[45] HOROWITZ M. 1.1 Computing's energy problem (and what we can do about it) [C]//Proceedings of 2014 IEEE International Solid−State Circuits Conference Digest of Technical Papers (ISSCC). IEEE, 2014: 10−14. DOI: 10.1109/ISSCC.2014.6757323
[46] ANDERSCH M. Nvidia Hopper architecture in−depth [EB/OL]. [2022−10−12]. https://developer. nvidia. com/blog/nvidia−hopper−architecture−in−depth
[47] POOL J. Accelerating inference with sparsity using the Nvidia ampere architecture and NVIDIA TENSORRT [EB/OL]. [2022−10−12]. https://developer. nvidia. com/blog/accelerating−inference−with−sparsity−using−ampere−and−tensorrt
[48] GITHUB. Lfai−landscape [EB/OL]. [2022−10−12]. https://github. com/lfai/lfai−landscape
[49] 王成灿. Adlik 在模型剪枝量化上的实践 [EB/OL]. [2022−10−12]. https://zhuanlan.zhihu.com/p/197837122
[50] 潘佳懿. 模型优化算法 [EB/OL]. [2022−10−12].https://zhuanlan.zhihu.com/p/543576964
[51] 中兴通讯, 英特尔. 英特尔联手中兴优化深度学习模型推理 实现降本增效[EB/OL]. [2022−10−12]. https://wiki. lfaidata. foundation/display/ADLIK/Discussion+materials
[52] 韩雪微. Adlik 深度学习模型编译器介绍[EB/OL]. [2022−10−12]. https://zhuanlan.zhihu.com/p/368595113
[53] 刘涛. 异构计算系列(三): Adlik 在深度学习异构计算上的实践 [EB/OL]. [2022−10−12]. https://www.infoq.cn/article/eg4kwzd1uofwjssuzfgt
[54] SHMELKIN R, FRIEDLANDER T, WOLF L. Generating master faces for dictionary attacks with a network−assisted latent space evolution [C]// Proceedings of 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021). IEEE, 2022: 1−8. DOI: 10.1109/FG52635.2021.9666968
[55] Wikipedia. Tay [EB/OL]. [2022−10−12]. https://en.wikipedia.org/wiki/Tay
[56] 中华人民共和国科学技术部. 新一代 AI 治理原则 [EB/OL]. [2022−10−12]. https://www.safea.gov.cn/kjbgz/202109/t20210926_177063.html
[57] 中国信息通信研究院, 京东探索研究院. 可信AI白皮书 [R]. 2021
[58] VOIGT P, BUSSCHE A V D. The EU general data protection regulation (GDPR): a practical guide [M]. Cham: Springer International Publishing, 2017
[59] 中华人民共和国网络安全法 [EB/OL]. [2022−10−12]. http://www.cac.gov.cn/2016−11/07/c_1119867116.htm
[60] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning: concept and applications [J]. ACM transactions on intelligent systems and technology, 2019, 10(2): 1−19. DOI: 10.1145/3298981
[61] LI F H, LI H, NIU B, et al. Privacy computing: concept, computing framework, and future development trends [J]. Engineering, 2019, 5(6): 1179−1192. DOI: 10.1016/j.eng.2019.09.002
[62] 方滨兴, 崔翔, 顾钊铨. 人工智能安全论述[EB/OL]. [2022−10−12]. https://tx.pcl.ac.cn/CN/article/openArticlePDF.jsp?id=15

[63] SZEGEDY C, ZAREMBA W, SUTSKEVER I, et al. Intriguing properties of neural networks [EB/OL]. [2022-10-12]. https://arxiv.org/abs/1312.6199
[64] JAGIELSKI M, OPREA A, BIGGIO B, et al. Manipulating machine learning: poisoning attacks and countermeasures for regression learning [C]// Proceedings of 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018: 19-35. DOI: 10.1109/SP.2018.00057
[65] GAO Y S, DOAN B G, ZHANG Z, et al. Backdoor attacks and countermeasures on deep learning: a comprehensive review [EB/OL]. [2022-10-12]. https://arxiv.org/abs/2007.10760
[66] TRAMÈR F, ZHANG F, JUELS A, et al. Stealing machine learning models via prediction APIs [C]//Proceedings of the 25th USENIX Conference on Security Symposium. ACM, 2016: 601-618. DOI: 10.5555/3241094.3241142
[67] MEHRABI N, MORSTATTER F, SAXENA N, et al. A survey on bias and fairness in machine learning [J]. ACM computing surveys, 2022, 54(6): 1-35. DOI: 10.1145/3457607
[68] TANG B, ZHANG C M, WANG K W, et al. Neursafe-FL: a reliable, efficient, easy-to-use federated learning framework [EB/OL]. [2022-10-12]. http://kns.cnki.net/kcms/detail/34.1294.TN.20220826.1322.001.html
[69] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data [EB/OL]. [2022-10-12]. https://arxiv.org/abs/1602.05629
[70] KARIMIREDDY S P, KALE S, MOHRI M, et al. Scaffold: stochastic controlled averaging for federated learning [EB/OL]. [2022-10-12]. https://arxiv.org/abs/1910.06378v3
[71] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks [EB/OL]. [2022-10-12]. https://arxiv. org/abs/1812.06127
[72] GAO L, FU H Z, LI L, et al. FedDC: federated learning with non-IID data via local drift decoupling and correction [C]//Proceedings of 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2022: 10102-10111. DOI: 10.1109/CVPR52688.2022.00987
[73] 国务院. 国务院关于印发新一代AI发展规划的通知 [EB/OL]. [2022-10-12]. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

作 者 简 介

韩炳涛，中兴通讯股份有限公司数据智能平台中心总工程师、移动网络和移动多媒体技术国家重点实验室多媒体研究中心副主任、Linux深度学习基金会Adlik项目负责人；研究方向为机器学习平台技术和网络智能化，以及相关核心系统架构和AI算法；拥有发明专利多项，出版专著多部。

刘涛，中兴通讯股份有限公司资深算法专家、Adlik开源项目首席架构师、AI预研项目经理；主要研究领域为AI模型并行训练、模型推理优化、高性能计算、异构硬件模型部署等；拥有多项发明专利。

唐波，中兴通讯股份有限公司资深系统架构师；主要研究领域为深度学习技术、异构资源调度、隐私安全机器学习、AI安全攻防等；主导中兴通讯公司AI平台、联邦学习、AI安全工具的设计和研发工作；拥有多项发明专利，发表论文多篇。

综合信息

《中兴通讯技术》2023年热点专题预告

期 次	专题名称	策划人
1	云网安全新挑战及智能防护技术	中国电信研究院教授级高工 解冲锋 北京邮电大学教授 杨义先
2	语义通信	清华大学教授 陶晓明 中国科学院院士 陆建华
3	数字孪生	重庆邮电大学教授、副校长 陈前斌
4	算力网络和东数西算	工业和信息化部通信科技委专职常委 赵慧玲
5	6G网络技术	北京邮电大学教授 王文东
6	面向双碳的新一代无线通信网络	华中科技大学教授 葛晓虎 西安电子科技大学教授 李建东

5G/5G-Advanced/6G接入网安全技术演进及内生安全

Security Technology Evolution and Intrinsic Security of 5G/5G-Advanced/6G Access Network

陆海涛/LU Haitao[1,2,3]，陈一喆/CHEN Yizhe[4]，
娄笃仕/LOU Dushi[1,3]
（1. 中兴通讯股份有限公司，中国 深圳 518057；
2. 深圳市无线移动技术重点企业研究院（中兴），中国 深圳 518055；
3. 深圳市5G接入网安全技术研究及应用重点实验室，中国 深圳 518055；
4. 南京邮电大学，中国 南京 210003）
(1. ZTE Corporation, Shenzhen 518057, China;
2. Shenzhen Key Enterprise R&D Institute of Wireless Mobile Technology (ZTE), Shenzhen 518055, China;
3. Shenzhen Key Laboratory of 5G RAN Security Technology Research and Application, Shenzhen 518055, China;
4. Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

DOI：10.12142/ZTETJ.202206014
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221219.1255.001.html
网络出版日期：2022-12-20
收稿日期：2022-10-08

摘要：网络安全技术在无线通信技术的演进中不断增强。介绍了现有5G网络的安全技术方案，并结合5G行业应用需求，探讨了5G-Advanced增强安全技术。立足于万物智能互联愿景，从海量设备连接、智能运维、人工智能/机器学习、区块链方面分析了内生安全技术。认为内生安全是6G网络安全研究的热点，轻量化是6G内生安全的主要特征之一。

关键词：内生安全；行业应用；物联网；海量连接；轻量化

Abstract: Network security technologies are constantly enhanced in the evolution of wireless communication technology. The security technology solutions of the existing 5G networks are introduced, and the 5G-advanced enhanced security technologies are discussed in combination with the 5G industry application requirements. Based on the vision of intelligent interconnection of everything, the intrinsic security technologies are analyzed from the aspects of massive equipment connection, intelligent operation and maintenance, artificial intelligence/machine learning, and blockchain. It is considered that intrinsic security is the focus of 6G network security research, and lightweight is one of the main features of 6G intrinsic security.

Keywords: intrinsic security; industry application; Internet of Things; massive connections; lightweight

第3代合作伙伴计划（3GPP）定义了5G的三大应用场景：增强移动宽带（eMBB）、超可靠低时延通信（URLLC）和海量机器类通信（mMTC）。3GPP在制定5G网络标准时已把安全性作为核心问题来考虑，并在5G的第一个标准R15里提出5G网络安全架构[1]，从访问域、网络域、服务化架构（SBA）域等方面分别定义了安全功能和组件。3GPP R15标准于2018年6月被冻结，该标准主要规定了eMBB和URLLC两大场景。基于3GPP R15的网络安全架构，文献[2]针对5G接入网和基站设备，从基础设施、新空口（NR）、核心网接口和网管接口4个方面提出了安全解决方案。

基金项目：广东省重点领域研发计划（2020B0101120003）

2020年7月3GPP R16标准被冻结，该标准完善了URLLC技术特性。该技术特性使得5G可以应用于工业、港口、地铁等物联网中，为5G面向企业（ToB）垂直行业应用打下基础。此时业界开始意识到：传统的网络安全防护机制是“外挂式”“补丁式”的，难以应对未来万物互联所面临的安全挑战，因此需要改变传统的安全防御思想，不再使用独立安全解决方案来应对安全问题，需要重新设计安全协议和机制，建立一套完备的信息系统安全体系，使系统具备自我免疫、内外兼修、自我进化的特点，从网络内部增强安全防范能力，从源头上抵制攻击的产生[3]，即实现内生安全。

2022年6月3GPP R17标准被冻结。该标准支持增强的工业物联网、精准授时、高精度定位和车联网（V2X），并

引入了面向较低复杂度物联网终端的RedCap，将5G扩展至几乎全部终端和用例，为实现5G万物互联提供了重要支撑。

3GPP在2022—2026年进行5G-Advanced标准（R18/R19/R20）的研究，并将在2027—2030年开展6G标准（R21/R22/R23）的研究，继续在移动宽带、固定无线接入、工业物联网、V2X、扩展现实（XR）、无人机与卫星接入等用例方面进行空口协议演进与增强，研究和制定更高频段的相关标准。另外，6G通信标准的服务范围将从陆地扩展到卫星、海底、地下，真正实现海、地、天三位一体通信。

1 5G接入网安全技术

5G通信网络由终端、接入网、承载网和核心网组成。其中，接入网是指用户终端和骨干承载网之间的设备和链路，可实现无线信号的接入和转换。5G接入网的关键设备是5G基站（gNB），可实现3GPP定义的5G协议规范，具有大带宽、高可靠低时延、多连接的特性。相关核心指标包括无线频谱效率、峰值速率、用户体验速率、流量密度、连接密度、时延和移动性等。5G接入网安全技术主要包括终端安全、空口安全、基础设施安全、安全日志和公钥基础设施（PKI）系统等，如图1所示。这些技术是5G基站为数据处理、协议转换、访问控制和管理功能提供的安全支撑和重要保障。

（1）终端安全

终端安全是指在用户接入网络时做认证和鉴权的控制，对用户身份进行确认。长期演进技术（LTE）/5G使用了全新的双向认证方式和配有用户识别模块（UIM）的全球用户识别卡（USIM）。只有都完成网络对终端认证和终端对网络认证后，用户才可接入网络。5G增加了5G认证与密钥协商协议（5G-AKA）认证，并通过向归属网络提供用户设备（UE）从访客网络成功认证的证明，来增强演进分组系统（EPS）-AKA的安全性[1]。

对5G基站而言，终端安全更侧重于用户隐私数据的保护。例如，欧盟的《通用数据保护条例》和中国的《中国个人信息保护法》都严格要求在收集个人数据之前要征得用户同意，并规定了收集和处理数据的义务和责任。

5G基站数据处理所涉及的用户隐私数据有两种：一是执行3GPP协议处理所涉及的协议消息内容，如用户永久标识（SUPI）/国际移动用户标识（IMSI）、用户匿名标识（SUCI）、5G全球唯一临时标识（5G-GUTI）/临时移动用户识别码（TMSI）、国际移动设备标识（IMEI）、用户互联网地址（UE IP）及位置区标识（LAI）定位信息等；二是操作维护管理所涉及的管理消息内容，如SUPI/IMSI、UE IP等。对于所涉及的用户隐私数据，5G基站通过采取数据加密、系统加固、数据脱敏等措施来保护隐私数据的安全。

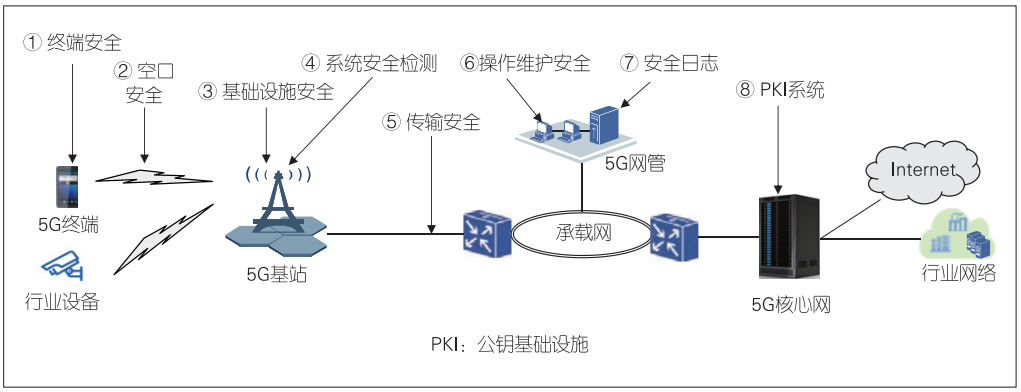
（2）空口安全

空口安全主要解决终端和基站之间无线通道的安全传输问题。由于无线信号覆盖在空间各处，非法用户可以随意截取，因此需要对空口数据进行加密和完整性保护，防止数据泄露或被篡改。

5G基站的空口安全处理包括数据加密和完整性保护。其中，数据加密是指发送方通过加密算法将明文数据转换为密文数据，保证数据不泄露；完整性保护是指发送方通过完整性算法计算出完整的消息认证码（MAC-I），接收方通过完整性算法计算预期的消息身份验证代码（X-MAC），并比较MAC-I和X-MAC是否一致，以保证数据不被篡改。5G基站在分组数据汇聚协议（PDCP）层实现数据加密和完整性保护功能，根据核心网发送的安全策略激活安全功能。加密算法由5G基站通过无线资源控制（RRC）信令发送给终端，密钥由终端和5G基站生成。

（3）基础设施安全

5G基站的基础设施安全包括多个方面。（a）物理设备安全：对基站以及周围设施保证安全，如设置门禁、监控，配备烟雾、温度传感器等；（b）操作系统安全：定期对软硬件进行安全威胁分析和评估，每发布一个软件版本，都需要经过第三方软件的安全扫描和评估，对于发现的漏洞和风险能够及时解决；（c）禁用不安全的服务和协议：与基站应用无关的操作系统（OS）服务和协议需要被关闭或移除，不使用的端口缺省也要被关掉，提供对外开放的端口/协议列表，支持端口/协议可关闭；



▲图1 5G接入网安全技术架构

（d）存储安全：本地存储的机密信息都需要加密，其中特别敏感的信息还要存放在保护区内；（e）不使用无支持的硬件和软件模块：在基站产品开发过程中，可选择硬件模块或者第三方软件模块，但不能选用已经没有支持和不再升级的产品，因为这类产品往往存在安全缺陷。如果没有支持来修补安全漏洞，基站就会暴露安全问题。

（4）系统安全检测

系统安全检测可保护基站正常运行，在软硬件异常或故障时能够快速恢复，避免基站服务中断。资源监控、回收、复位、告警、日志等手段可保证业务软件服务与硬件资源的可用性。（a）中央处理器（CPU）监控与死锁检测：通过线程切换等关键点的时刻记录来获取运行时间，计算线程在一个周期内的CPU占用率，结合线程的CPU/核占用率和主动切换次数，判断线程是否进入死循环或处于死锁状态，记录现场日志并恢复服务；（b）内存泄露检测：限定具体进程的内存使用量，结合申请者信息和一些使用策略对内存泄露做出判定，在监控到这些问题发生时记录详细的异常日志；（c）孤岛监控与自救：当各种故障与核心网、网管等连接设备断链出现孤岛状态时，系统会监控孤岛状态，实施自救，传输参数回滚等以保障基站服务的可用性。

（5）传输安全

传输安全主要指5G基站数据传输的安全协议保障，涉及5G基站之间、5G基站与LTE基站间的Xn/X2接口，5G基站与5G核心网及LTE核心网间的下一代5G（NG）/4G（S1）接口连接。传输网络协议涉及物理层到应用层之间的安全协议。如果这些接口的物理网络非可信，则需要通过连接安全网关（SeGW）建立端对端的安全通信隧道，支持Internet安全协议（IPSec），保证5G基站数据传输的安全。另外，基站和网管间的传输链路也要支持传输层安全（TLS）协议，保证管理数据的安全。

由于是一个多层次的需求，在某些特定场景中数据传输安全还需要支持更底层的业务，例如实现链路层的额外保护。相关协议包括电气与电子工程师协会（IEEE）制定的基于端口的访问控制和认证协议（IEEE 802.1x）、媒体访问控制安全（MACSec）协议等。

（6）操作维护安全

5G基站的操作维护安全涉及配置、版本、告警、诊断操作等。维护用户是指对基站进行配置、操作和维护的使用者，用户必须唯一识别。基站的操作维护系统功能包括SSH、SFTP和Web服务。授权用户可以通过基站的本地管理口从外部远程访问，非授权用户不能接入系统。用户接入系统后还需要进行权限控制，即用户能够读取/修改/执行系统文件是否在授权范围内。系统需要对用户分组，不同等级的用户分组有不同的用户权限。

系统支持集中账户管理和本地账户管理。其中，集中账户是指通过轻量目录访问协议（LDAP）等集中管理分布网元的账户，本地账户用于设备近端的操作维护管理。系统的用户访问控制是指对用户授权可以访问的对象和执行的操作，通常通过基于角色的权限分配来实现。

（7）安全日志

5G基站提供安全日志，记录用户登录和登出、用户权限变更等安全事件以供审计，提供有效证据防止人员或实体否认执行过的活动。同时基站实时反馈5G网络系统的安全势态，让运营商了解无线系统的整体安全情况，提供日志查询、安全事件关联分析和报告等。当分析结果有潜在和可疑的活动时，系统会产生告警并调查可疑活动。

（8）PKI系统

5G规范引入了基于PKI的安全体系结构。3GPP 33.310协议定义了基站数字证书的注册机制，以及应用数字证书与核心网建立安全通信链路的过程。PKI采用非对称密码算法技术实现可提供安全服务的具有通用性的安全基础设施，能够为所有网络应用提供采用加密和数字签名等密码服务所需要的密钥和证书管理，并提供创建、颁发、查询证书的功能。

设备商为基站提供出厂生成的公私钥对。基站会预装由设备商签名的数字证书、登记授权（RA）/证书授权（CA）服务器预装设备商根证书、核心网SEG预装运营商根证书。然后基站向核心网注册并使用证书管理协议版本2（CMPv2）协议向RA/CA发起证书申请。RA/CA则使用设备商根证书和设备商签名证书对基站进行身份验证。验证通过后基站会获得签发的运营商证书并返回证书响应。基站证书替换为运营商签名证书，则表明基站注册完成。随后基站使用运营商签名证书与核心网建立IPSec安全连接。

2 5G-Advanced安全增强技术

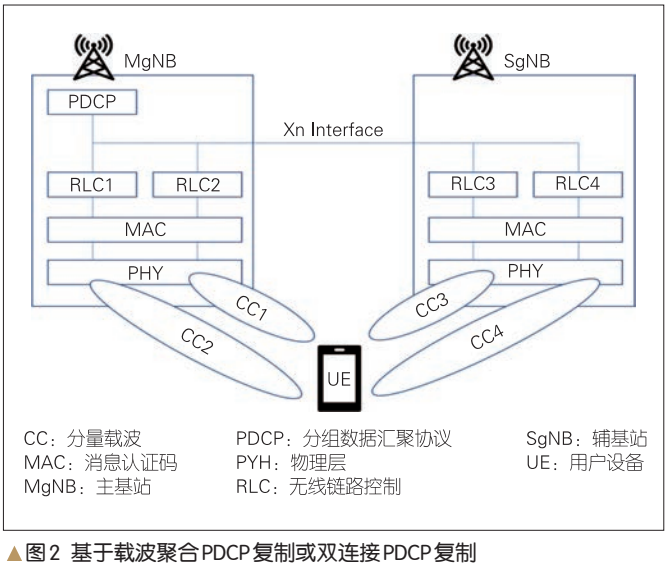
5G发展的关键是应用。2021年7月，工业和信息化部等十部门联合发布了《5G应用“扬帆”行动计划（2021—2023年）》，从5G应用标准体系、面向行业需求的5G产品、5G应用创新生态、5G应用安全能力四大领域打造5G融合应用新产品、新业态、新模式，为经济社会各领域的数字转型、智能升级、融合创新提供坚实支撑。中国5G应用市场发展空间巨大，根据行业互联网数据中心（IDC）研究预测，到2025年全球物联网市场将达到1.1万亿美元，其中中国市场占比将提升到25.9%，物联网市场规模全球第一。大部分市场增长来自企业市场，这说明5G发展将

从传统面向个人（ToC）消费市场向ToB企业应用转变。5G赋能各行各业，带动行业数字化、智能化转型升级。

5G-Advanced是5G技术的演进版本，其目标是实现万兆体验、千亿物联、智能感知的网络能力。3GPP于2021年12月将R18作为5G-Advanced第一个版本。R18的27个项目涵盖5G传统的eMBB、URLLC、V2X等场景，同时定义了新场景、新业务，如上行大容量、空口人工智能（AI）、虚拟现实增强业务XR、高精度定位等。相比于先前的5G版本，5G-Advanced面向ToB垂直行业应用，在现有网络能力的基础上，进一步提升网络能力，增强支持大上行（1 Gbit/s峰值速率）、极低时延（毫秒级）、更高可靠性（99.9999%）、更高可用性、更高精准授时、更高精度定位，以及通信感知、空天一体的服务保障能力。相应地，5G-Advanced网络的安全技术也要进行增强，以适应在ToB行业的应用推广。

2.1 高可靠性安全

随着5G技术的广泛部署，行业应用普遍对网络可靠性提出确定性要求，如电网差动保护、港口岸桥远程控制、桥式起重机远程操纵等。5G-Advanced的高可靠性增强技术包括PDCP复制、混合自动重传请求（HARQ）重传、智能自适应调制编码（AMC）控制重传和低码率MCS调整等。涉及的安全增强技术主要是PDCP复制安全，即确保PDCP数据和复制数据均使用相同的加密完保策略和密钥，如图2所示。这也是跨站CA和切换场景的密钥一致性解决方案。

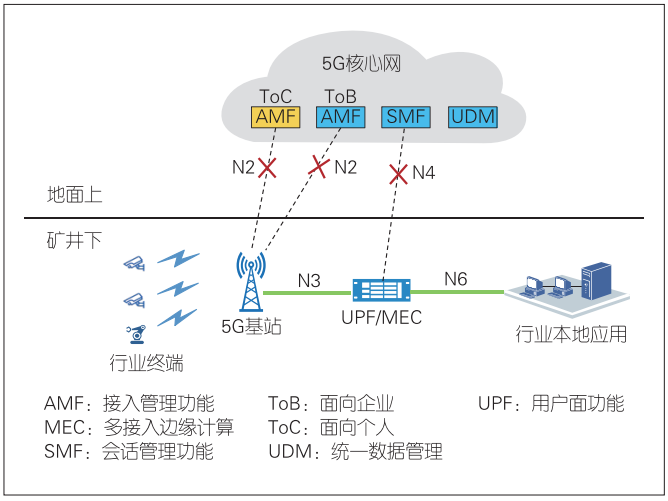


▲图2 基于载波聚合PDCP复制或双连接PDCP复制

2.2 高可用性安全

高可用性是行业应用的基本要求：一方面通过设备和链路冗余提高可用性，例如基站热备支持节点级和网络级的容灾保护，前传光口双上联合环组网，均能保障传输的高可用性；另一方面，要确保在通信链路断开后，仍能继续保持业务连接，例如在矿山场景中，当井下基站和地面核心网链路因事故中断后，基站要支持断链保持功能，使井下用户终端业务不中断。

如图3所示，当矿山场景的井下基站与地面核心网的连接（N2、N4）断链时，为了保持业务连贯运行，井下用户终端的正常业务不受影响，基站需要启动5G控制面（NG-C）断链业务保持功能，并且要求业务不断、安全不断。由于对用户的安全控制管理是在核心网进行的，因此当基站启动断链保持时，基站也要增强对用户的安全控制管理。



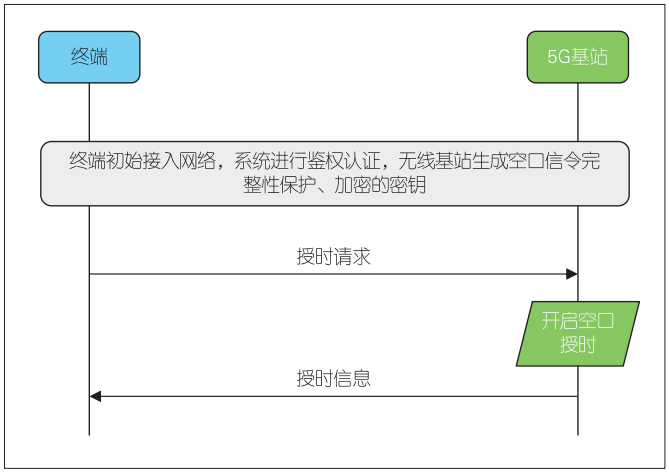
▲图3 5G控制面断链业务保持功能示意

2.3 5G精准授时安全

工业控制、电力差动保护/精密测量单元（PMU）等业务需要严格的业务同步。由于工业控制有线化成本高、布放受限，工业控制网络无线化是一个重点发展方向。特别是随着5G工业互联网产业需求的迅猛发展，5G+垂直行业产业发展迅速，通过5G空口实现业务到UE侧高精度时间同步成为业务系统的基础性需要。5G基站通过空口把网络同步时间传送给UE，同时系统对处理时延进行相应的误差校准，从而实现全网UE的高精度时间同步。

5G空口授时的安全性增强主要是对系统信息模块（SIB）广播消息的增强处理。5G空口授时有两种模式：RRC单播信令、SIB9广播。其中，RRC单播方式拥有空口安全协商接入准入机制，并采用加密的信令对UE进行授时，具有较高的安全性。

图4为5G空口授时的RRC单播方式。基站在发送授时信息时使用安全协商后得到的密钥进行加密和完保，以保证授时信息通过空口传输时的机密性和完整性。



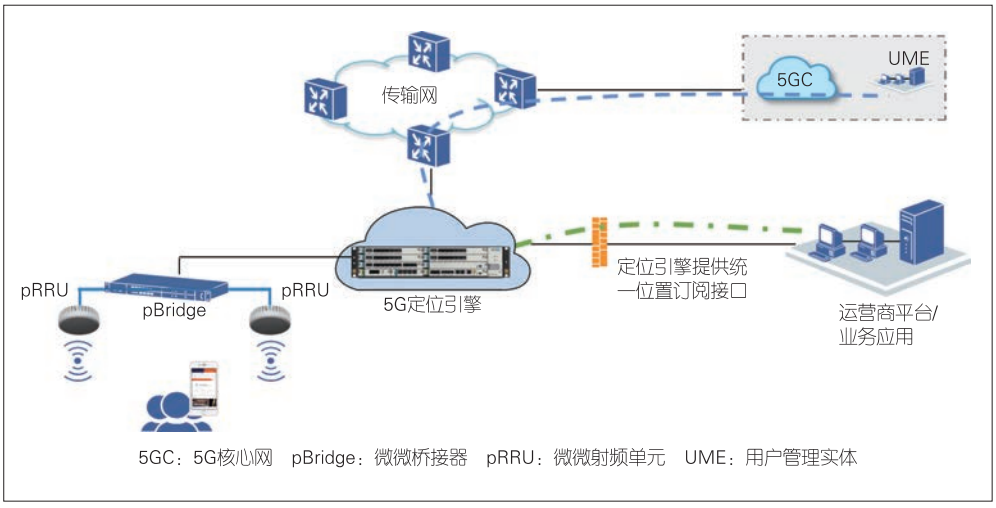
▲图4 5G空口授时的无线资源控制单播方式

而广播方式SIB9消息不需要接入认证就可获取，安全性差，容易受到伪基站攻击。因此，我们需要先考虑增强终端流程安全，确保终端收到的SIB9广播消息的合法性，再重新获取时间信息和使用时钟。

2.4 5G高精度定位安全

位置服务是未来新兴产业的重要驱动力，包括商场、车站、医院的室内导航，移动电子商务、个性化广告的商品引导，救灾抢险的特殊行业人员定位等。传统的卫星定位由于受覆盖和通信能力限制，难以满足未来数字化社会的高精度定位服务需求。5G大规模天线、大带宽的关键技术和算法突破，使得厘米级的高精度定位成为可能，不仅能保障室内室外的无缝覆盖，还具有强大的通信能力。因此，5G高精度定位是未来位置服务的主要手段。

5G空口定位的安全性增强主要是对定位数据的保护，需要严格定义数据访问权限，防止非法访问、防DDOS攻击等。同时位置计算的定位引擎是高精度定位的核心。连接基站、网管和业务平台需要采用不同的网络平面进行隔离，以保证网络安全，如图5所示。



▲图5 5G空口定位结构

2.5 数据分流安全

5G行业应用中数据安全是保障企业开展生产经营活动的重要前提。各类技术资料可能含有重要的商业机密，一旦泄露将导致企业失去核心竞争力。此外，生产控制指令、工况状态等信息若被不法分子篡改，将引发系统设备故障甚至生产安全事故，影响企业生产运行。企业客户普遍提出5G网络的引入需要保证数据不出园的安全需求。

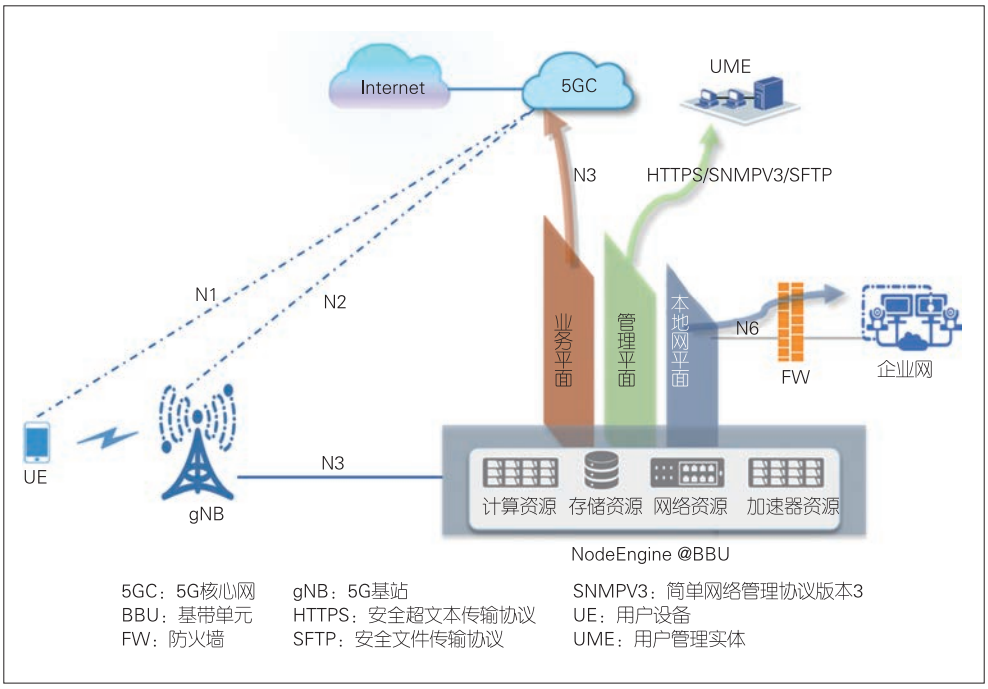
由于ToB业务本地处理需求强烈，我们可通过下沉部署园区专用的本地分流网关来解决数据在本地处理的问题，也可根据业务场景的需要选择基站内置分流功能产品或UPF产品来作为本地分流网关，例如中兴通讯的NodeEngine基站引擎就可实现数据分流，如图6所示。

5G基站集成的数据处理引擎NodeEngine可实现园区业务的本地分流。这不仅使园区业务就近得到处理，提高业务处理的实时性，还可满足园区业务不出园的安全需求。NodeEngine可以根据业务部署的需要灵活支持IP五元组/域名服务器（DNS）域名、切片标识以及公共陆地移动网络（PLMN）的数据分流机制。

NodeEngine采用虚拟本地网（VLAN）隔离和隐藏UE IP等安全隔离措施，满足智简园区的组网安全。NodeEngine在对接基站、网管、企业专网时采用不同的网络平面，各网络平面采用VLAN隔离，以保证网络安全；在企业专网内部UE IP与运营商传输网络IP不同的情况下，支持对专网UE IP进行网络地址转换（NAT），以对外隐藏UE IP。

3 6G内生安全

6G网络设计将在很多方面和5G有着显著的不同。首先，6G可以实现网络自动化和网络即服务（NaaS），用户可



▲图6 5G行业应用数据分流示意图

以定制网络；其次，核心/无线网络组件的云化网络和开源软件的快速应用表明，未来6G将是“完全开放”的网络。因此，6G安全架构需要适应变化，支持新的应用和太空-空中-地面-海洋网络模型的集成[4]。中国的6G相关科研工作启动比较早。2019年6月工业和信息化部牵头成立中国IMT-2030（6G）推进组，标志着中国6G研发正式启动。IMT-2030（6G）推进组认为：6G将实现人与人、人与物、物与物的高效智能互联，打造泛在精细、实时可信、有机整合的数字世界，实时精确地反映和预测物理世界的真实状态，助力人类走进人机物智慧互联、虚拟与现实深度融合的全新时代，最终实现“万物智联、数字孪生”的美好愿景[5]。在6G给社会经济生活带来变革的同时，安全性显得至关重要。网络安全技术需要实现颠覆性的突破。传统“外挂式”、“补丁式”的安全机制将向内生安全演进。

IMT-2030（6G）推进组把内生安全列为6G潜在的十大关键技术之一，同时定义网络内生安全的四大特征：（1）主动免疫，为网络基础设施、软件等提供主动防御功能；（2）弹性自治，实现安全能力的动态编排和弹性部署；（3）虚拟共生，实现物理网络与虚拟网络安全的统一与进化；（4）泛在协同，通过端、边、网、云的智能协同来准确感知整个网络的安全态势[6]。本文中我们认为，轻量化也是6G内生安全的主要特征之一，而传统的接入安全技术无法满足海量设备连接和实时传输，需要有轻量化的安全机制来满足6G万物智联、数字孪生的应用场景需求。

3.1 主动免疫

网络安全攻击的目的与攻击手段在不断变化，所以安全的风险也会持续不断变化。与传统5G安全被动式地应对安全攻击和风险不同，6G内生安全提供了一种主动免疫的解决思想，赋予网络以类似人体免疫的安全能力。因此，内生安全也被称为新的网络安全范式。

（1）AI/机器学习（ML）安全

AI/ML将全方位赋能6G网络安全。基于AI/ML的安全内生机制使得6G网络具备主动免疫、自我演进、按需提供安全服务的能力。具体来说，使用深度强化学习和深度神经网络进行入侵检测和预防，可以有效防御网络中的伪基站攻击、IP欺骗攻击、DDoS攻击、控制平面饱和攻击和主机位置劫持攻击等；使用AI预测分析可以在攻击发生之前预测攻击，例如基于强化学习（RL）的智能波束成形技术可提供针对6G太赫兹和可见光通信系统中窃听者攻击的最佳波束成形策略；基于边缘的联邦学习能够在6G分布式网络的海量设备和数据机制中执行网络安全任务。

未来基于AI/ML的主动免疫内生安全演进过程分为3个阶段。（a）初级阶段：基于AI/ML、威胁模型、关联分析模型等，按规划进行安全能力建设，初步形成免疫能力；（b）中级阶段：进一步基于AI/ML和网络空间灾害模型等提升网络免疫能力，仅需要部分人工干预，使网络安全建设具备一定的可控和收敛能力；（c）高级阶段：网络的主动免疫能力能够量化，安全能够弹性自治，基本不再需要人为干预[7]。

（2）区块链技术

区块链是一种以密码学算法为基础的分布式账本技术，可在去中心和多中心的系统中实现不可篡改和防伪，并保证各个节点账本的动态一致性，其本质是一种互联网共享数据库，具有主动免疫特性，能够帮助6G网络构建安全可信的通信环境。区块链在中国受到高度重视。2021年中国的“十四五”规划明确提出：区块链是新兴数字产业之一，需要“以联盟链为重点发展区块链服务平台和金融科技、供应链管理、政务服务等领域应用方案”。可以预见，区块链将是6G时代数字化经济形态所覆盖的数千万甚至数以亿计的资

产单位或机器（物联网）的分布式、安全交易模式，并有望成为6G网络内生安全的关键技术。文献[8]研究了区块链技术与6G频谱管理融合发展（特别是共识机制、合约机制技术）的深入应用，有效提高频谱利用率，实现动态、高效的频谱资源管理，为6G网络营造一个安全、智能、可行的动态频谱共享环境。文献[9]面向6G零信任网络的通信需求，以区块链为“信任桥梁”，研究了6G车联网边缘计算中的可信可靠接入管理方法。该方法在不泄露车辆隐私的前提下显著提升了车辆验证效率，降低了基站能耗，具有更高的安全性。

6G时代的mMTC场景将实现去中心化转变，以支持海量设备连接。这和区块链的去中心化特征非常适配。区块链具有不可篡改、全程留痕、可追溯、集体维护、公开透明等特点，可以很好地满足内生安全设计需求，是6G内生安全的候选关键技术。区块链可能是最具颠覆性的万物互联技术之一[10]。当然，区块链要成为6G内生安全技术，需要关注自身部署形态，尤其是在工业物联网等ToB行业应用中，区块链+边缘计算的部署形态，以保障链上链下数据的可信交互；还需要关注高可靠低时延的区块链链上链下通信方式，以支持在多类型终端大数据容量和复杂网络环境下数据的高效安全传输，以及区块链系统与其他系统之间的数据交换。

3.2 弹性自治

6G网络的行业应用场景，例如增强现实（AR）、虚拟现实（VR）等，对网络时延、传输速率、连接数等需求差异巨大。传统5G网络受限于网络架构、交付方式、运维模式等，难以满足不同行业的应用需求。因此，6G网络安全应具备内生弹性可伸缩的框架。基础设施应具备安全服务灵活拆分与组合的能力，通过软件定义安全、虚拟化等技术，构建随需取用、灵活高效的安全能力资源池，实现安全能力的按需定制、动态部署和弹性伸缩，适应云化网络的安全需求。

文献[11]设计了一种6G网络内生安全架构。该架构包括安全管理中心、安全智能中心、安全策略控制单元、安全能力层（网元设备自身安全能力、专用安全能力资源池）4层，并结合信任共识设施、资源编排与调度能力、人工智能分析能力，形成体系化安全架构，如图7所示。

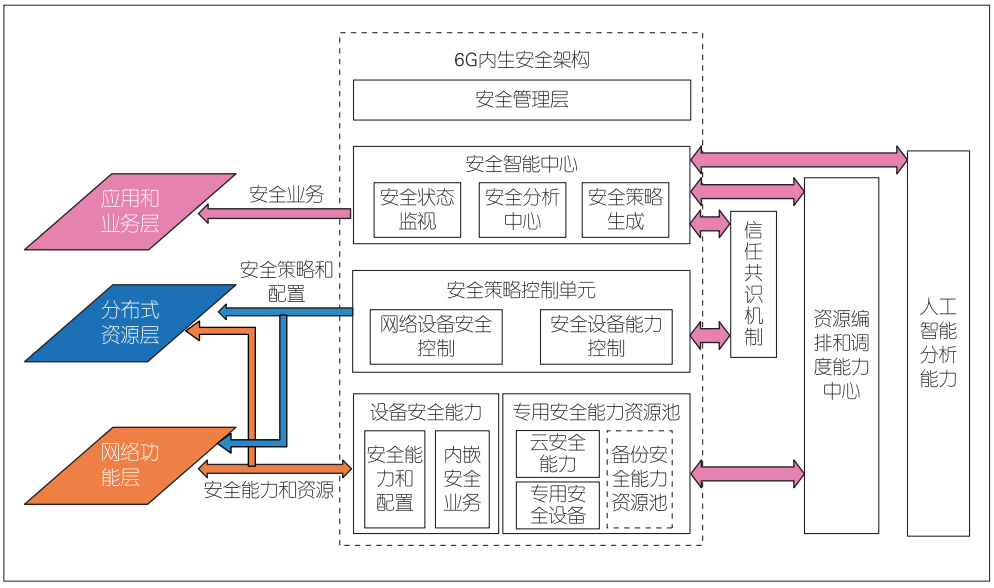
在图7所示的6G内生安全架构中，设备安全能力可保障设备基础安全功能应由设备自身提供，还可有效保障设备在其他安全机制失效时仍能维持基本的安全能力；专用安全能力资源池提供实现共性安全能力，其目标是保障安全能力高效执行，避免系统中安全能力的重复建设与部署；安全策略控制单元执行安全智能中心的安全策略下发，包括网元设备的安全策略、安全专用设备的安全策略；安全智能中心是安全协同的大脑，基于AI能力，与管理中心、资源编排与调度能力联动；安全管理中心提供系统管理、审计管理、安全管理、集中管控等能力，并能呈现安全态势等。

在安全管理中心的指导下，以6G网络安全能力为基础，配合柔性安全能力资源池，协同智能分析与编排机制，可构建弹性自治的安全防护体系。这样的体系具备对外安全服务能力，能够达到主动免疫、信任共识、协同弹性的目标。

3.3 虚拟共生

相比于传统5G网络，6G网络将打通物理世界和虚拟世界，形成物理网络与虚拟网络相结合的数字孪生网络，在工业控制、体育场馆、新闻媒体、社交娱乐等领域有着广泛的应用前景。XR技术利用硬件设备并结合多种技术手段，将虚拟的内容和真实场景融合，通过计算机技术和可穿戴设备产生一个真实与虚拟组合的、可人机交互的环境，包括VR、AR、混合现实（MR）等多种形式，不仅可以实现数字和物理世界的社交属性的充分放大，还可基于共同的物理空间和虚拟空间分享信息。

个人数据的管理是XR应用必须考虑的安全要素。通过



▲图7 6G内生安全参考架构

6G网络进行的数据收集、存储、保护和共享必须遵守相应的数据保护规范和条例。文献[12]认为超低时延网络的可靠性是解决网络动态的关键，同时发现一些网络攻击过于复杂、无法防御，因此敏感和机密数据仍可以被公开。为此，文献[13]提出一种高效的物理层安全技术——正交频分复用（OFDM）及子载波索引选择，通过开发联合优化子载波索引选择（IS）和自适应交织（AI）设计，最大限度地提高仅在合法接收机处的信噪比，来保护基于OFDM的波形在无线网络之外免遭窃听。该技术适用于URLLC场景的安全保护。

文献[14]提出一个3D系统，针对许多XR系统的隐私数据威胁进行风险建模。另外，文献[15]提出一种基于Delta正交多址接入（D-OMA）的物理层安全方案。该方案可增强上下行无线接入网的安全性，能够应用于XR的安全解决方案，扩展6G XR设备的访问能力，如图8所示。

D-OMA的安全方案是基于拼图概念实现的。在上行链路中，每个XR设备都有代表最终簇密钥（CK）的特定部分密钥（PK）。在接收端，将来自同一群集中不同XR设备的PK部分组合，可最终形成完整的CK。这与多因素并行身份验证过程类似。组合CK被视为所有设备从该集群中接收的数据的解密密钥。在未完全确认该密钥的情况下，系统将不会重构来自所有设备的数据。也就是说，窃听器需要以相同的时间和顺序解码所有用户的数据。而当大量XR终端设备传输到单一上行链路接收器时，这是比较难以实现的。只有接收基站知道运行期间所需的解码顺序以及每个XR群集的内容，从而确保XR设备的数据安全。

3.4 泛在协同

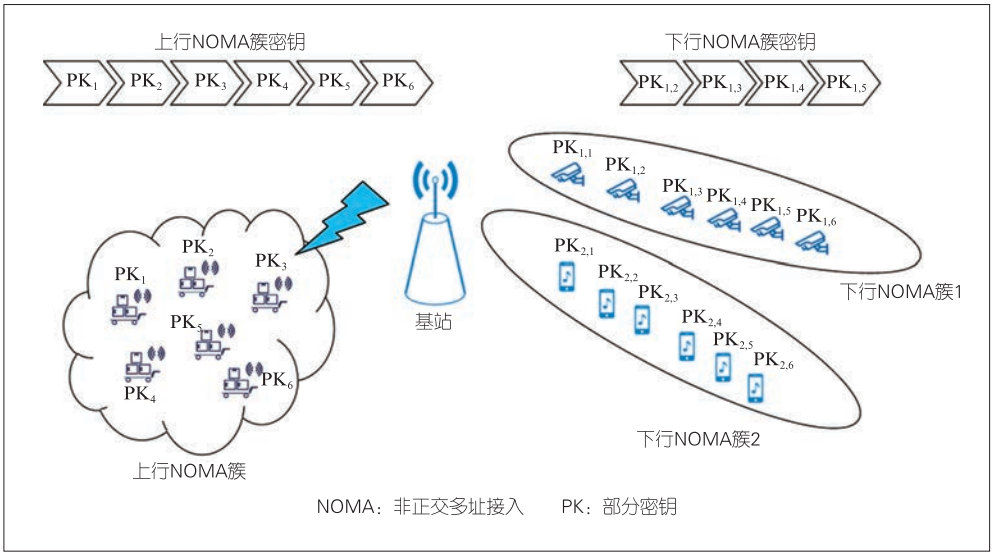
6G时代网络赋能各行各业，将传统封闭的通信技术（CT）领域融入信息技术（IT）领域。在这个变革的过程中我们可以发现，不同于传统5G通信网络的特性，6G网络更多地面对ToB领域。在确保有足够的专业维护手段来保障网络核心效果的同时，面对千行百业存在的特异性差别，行业间的技术壁垒和巨大的学习成本衍生出对端、边、网、云泛在协同的智能运维的诉求。各行业在安全生产、传输高可靠性、生产长连接保障、网络建设成本控制等方面存在刚性需求。在智慧内生的6G网络中，ML和大数据分析技术在安全方面将得到广泛应用。在AI技术的赋能下，6G网络能够建立端、边、网、云智能主体间的泛在交互和协同机制，准确感知网络安全态势并预测潜在风险，进而通过智能共识决策机制完成自主优化演进，实现主动纵深安全防御和安全风险自动处置[6]。

例如，中兴通讯的智能数字化运维服务系统（iDOS），通过关联端侧、无线、传输等各域数据，以业务精准识别端到端体验建模为核心，运用AI数据挖掘算法，实现对企业网络和业务指标的异常识别、故障的业务详单和信令级回溯、端到端问题定界，关联同时间、同维度、同域数据分析，进行故障的最终定位，协助客户监控业务整体运行状况、定位故障，从而提升对整个网络的运维支撑能力[16]，如图9所示。

iDOS从运维出发，提供智能化安全态势感知和主动故障预防机制，通过AI引擎持续在线进行ML和迭代更新，训练生成网络健康度量模型，并应用于实时的设备和网络健康监控，快速发现可能导致业务质量下降的网络风险、设备故障、外部环境风险等，提供最佳处理建议，真正做到防患于未然。通过长期监控数据，iDOS可提前识别设备、链路和环境等网络平稳运行的影响因素，对健康度进行评估，精准识别潜在的风险并预测故障发生的时间，在故障发生之前提示用户。此外，iDOS还可通过主动预防，提前识别并更换存在隐患的硬件，指导运维人员针对环境风险进行整改，从而极大降低网络故障发生率，确保企业业务所需要的高可靠性[16]，如图10所示。

3.5 轻量化

未来6G应用场景的通信技术将从人的通信转变为物的



▲图8 基于Delta正交多址接入提供的安全方法

通信、以下行为主转变为上行为主、以基站为中心转变为去中心化。传统的接入技术无法满足物理网等海量设备接入和实时传输，会引发网络拥塞问题。另外，mMTC场景在满足物联网、工业现场网络、智慧城市等应用同时，也会面临网络安全挑战，例如在终端、接入和数据方面的安全威胁：

（1）终端安全威胁。mMTC场景下的终端具有低功耗、低成本的特点，但海量终端的计算资源和存储资源有限，难以支持复杂的安全防护机制和强安全加密算法，因此安全防护能力较弱，容易成为攻击者的主要目标。

（2）接入安全威胁。mMTC场景下的设备数量庞大，海量的终端设备接入网络后同时触发接入认证流程，容易引起信令风暴，导致网络拥塞并加大终端设备的能源消耗。因此，针对这类设备的认证机制需要进行简化。采用高效而轻量化的认证机制，可减少认证时间，减轻网络拥塞程度。

（3）数据安全威胁。在mMTC业务场景中，网络服务、功能及数据的开放共享增加了对用户隐私和敏感数据的完整性和机密性保护难度。如未采取必要的数据保护措施，则可能会引发数据泄露风险。采取用户权限管理、安全认证、安全隔离、网络安全加固、审计等措施，可有效提升数据安全能力。

因此，传统5G接入技术无法满足mMTC场景海量设备连接和实时传输需求，需要演进为轻量化的接入和认证技术，实现极简无连接和高过载传输的海量设备互联。例如，多用户共享接入（MUSA）技术就实现了简化传输交互流程和去中心化，以支持海量设备互联。经过实测，MUSA可实现每平方公里9 000万次的连接，这是国际电信联盟（ITU）定义的90倍。相应的安全保护机制也是mMTC场景的安全关键技术，具体可从轻量级接入认证、轻量级密钥管理及加解密、隐私数据保护等来寻求安全解决方案。

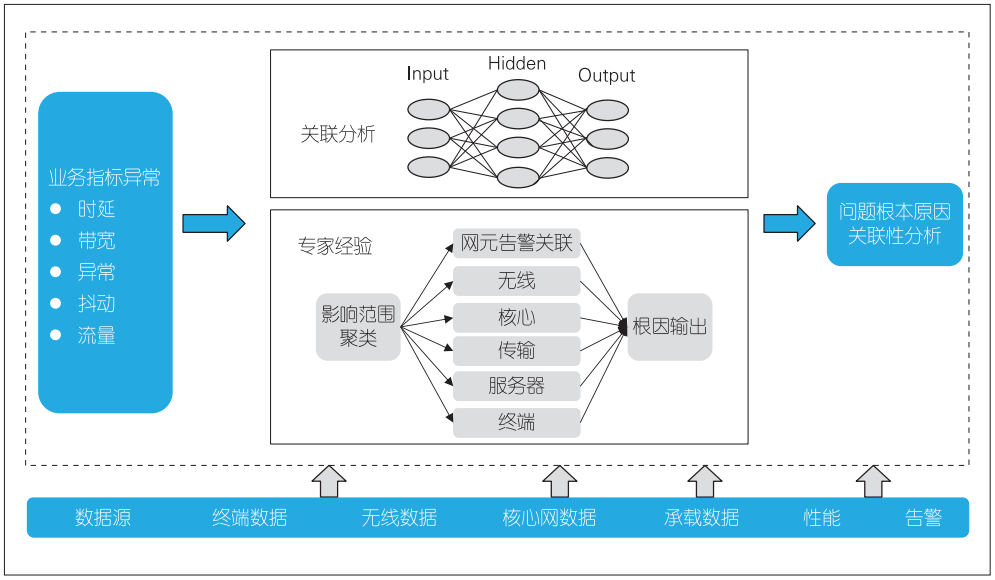
（1）轻量级接入认证

针对mMTC场景的MUSA技术简化了接入信令交互流程，有时甚至只需要1条信令就能实现用户接入，因此有必要建立支持大规模设备的、灵活可靠的认证机制。简化算法和运算逻辑，完成海量设备和网络侧的认证，既能保证连接的安全性，又能降低对资源的使用。

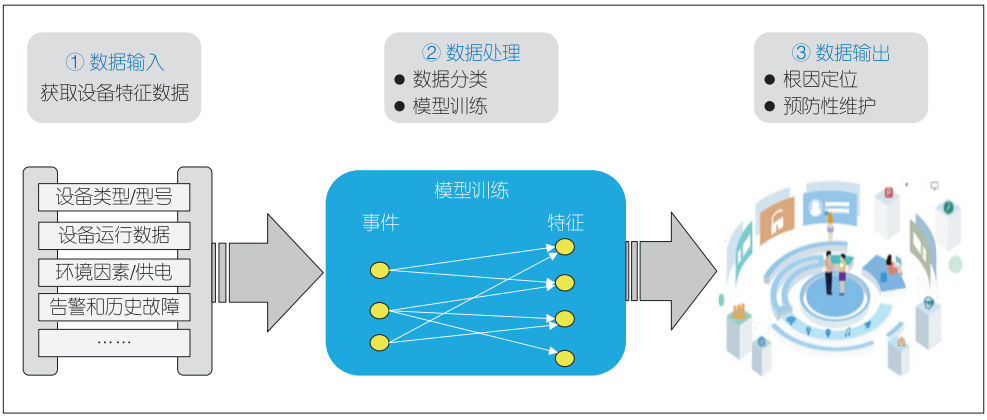
物理层认证是实现轻量级接入认证的关键技术之一。利用无线网络物理层的私有信道特征实现的低复杂度、高安全性的安全方案，分为基于设备指纹的认证和基于信道指纹的认证两种。前者利用硬件设备的电特性差异提取设备独有的特征，将唯一标识作为设备的认证指纹；后者不需要额外的信号提取设备，从无线信道特征入手，利用不同位置设备的信道特征之间存在的不相干性进行认证。文献[17]提出一种在认证过程中可以使用的非监督式学习方法，来增强物理层的安全性。

（2）轻量级密钥管理及加解密

传统密码学技术的核心是依靠密钥强度来保护系统安



▲图9 泛在协同智能运维系统



▲图10 人工智能赋能安全态势感知

全，使得攻击者在有限的时间和算力条件下无法破解密钥。而海量终端设备由于能力受限，无法提供复杂的密钥管理和密钥存储条件，导致传统密码学技术难以使用，因此需要引入轻量级的密钥管理和加解密技术。

物理层密钥生成技术也是实现轻量级密钥管理和加解密的解决方案。其原理是利用发射和接收信道中的随机熵来生成用于通信的保密密钥[18]。通过信道的互易性、时变性、唯一性等特征，基站与用户对信道进行探测，得到共同随机性以生成对称密钥，进行轻量级的加解密处理。物理层密钥生成可以做到一次一密（OTP），实现最强的密码安全保护。

（3）隐私数据保护

终端数据传输保护技术包括空口加密和完整性保护、非接入层（NAS）信令加密和完整性保护、无线资源控制（RRC）信令加密和完整性保护、空口业务数据加密和完整性保护等。在mMTC场景中，诸如自动驾驶、可穿戴设备、远程医疗终端等物联网设备在日常使用中会收集、存储和传输大量个人隐私数据。个人数据可以是与已识别或可识别人员直接或间接相关的任何信息，如姓名、身份证号码、用户位置和社交身份[19]。我们需要根据不同的业务场景和用户对象提供差异化的隐私数据保护能力，对用户隐私数据的请求、存储、传输等各个环节采取隐私保护措施。

4 结束语

在5G之前，甚至在5G-Advanced阶段，安全技术都不是内生的，而是对业务功能的补充和增强。随着6G颠覆性技术应用（如太赫兹和可见光通信、智能表面技术、通信感知一体化等）的发展，6G网络架构和形态将发生系统性变化。网络安全不再是传统的“外挂式”和“补丁式”，而是内生的。这也是人们进行6G安全研究的共识。

本文中，我们回顾了5G的基础安全能力和技术，以及5G-Advanced的安全技术演进，并分析了6G内生安全特征和内生安全关键技术，希望为后续6G安全技术研究提供参考。

参考文献

[1] 3GPP. Security architecture and procedures for 5G system (release 15): 3GPP TS 33.501 [S]. 2019
[2] 陆海涛, 李刚, 高旭昇. 5G网络的设备及其 接入安全 [J]. 中兴通讯技术, 2019, 25(4): 19-24+55. DOI: 10.12142/ZTETJ.201904004
[3] 聂凯君, 曹傧, 彭木根. 6G内生安全:区块链技术 [J]. 电信科学, 2020, 36(1): 21-27
[4] ABDEL HAKEEM S A, HUSSEIN H H, KIM H. Security requirements and challenges of 6G technologies and applications [J]. Sensors, 2022, 22(5): 1969. DOI: 10.3390/s22051969
[5] IMT-2030(6G)推进组. 6G总体愿景与潜在关键技术白皮书 [R]. 2021
[6] IMT-2030(6G)推进组. 6G网络安全愿景技术研究报告 [R]. 2021
[7] 中兴通讯. 2030+网络内生安全愿景白皮书 [R]. 2021
[8] 牛娇红, 黄何, 王卫斌, 等. 区块链技术及其6G网络中应用探析 [J]. 信息通信, 2020, 33(11): 37-39
[9] 郝敏, 叶东东, 余荣, 等. 区块链赋能的6G零信任车联网可信接入方案 [J]. 电子与信息学报, 2022, 44(9): 3004-3013
[10] SAAD W, BENNIS M, CHEN M Z. A vision of 6G wireless systems: applications, trends, technologies, and open research problems [J]. IEEE network, 2020, 34(3): 134-142. DOI: 10.1109/MNET.001.1900287
[11] 粟栗, 庄小君, 杜海涛, 等. 6G网络内生安全架构研究. 中国科学: 信息科学, 2022, 52(2): 12. DOI: 10.1360/SSI-2021-0257
[12] CHEN R Q, LI C H, YAN S H, et al. Physical layer security for ultra-reliable and low-latency communications [J]. IEEE wireless communications, 2019, 26(5): 6-11. DOI: 10.1109/MWC.001.1900051
[13] HAMAMREH J M, BASAR E, ARSLAN H. OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services [J]. IEEE access, 2017, 5: 25863-25875. DOI: 10.1109/ACCESS.2017.2768558
[14] YAMAKAMI T. A privacy threat model in XR applications [M]//Advances in Internet, Data and Web Technologies. Cham: Springer International Publishing, 2020: 384-394. DOI: 10.1007/978-3-030-39746-3_40
[15] AL-ERYANI Y, HOSSAIN E. The D-OMA method for massive multiple access in 6G: performance, security, and challenges [J]. IEEE vehicular technology magazine, 2019, 14(3): 92-99. DOI: 10.1109/MVT.2019.2919279
[16] 中兴通讯. ToBeEasy极简运维技术白皮书 [R]. 2021
[17] SATTIRAJU R, WEINAND A, SCHOTTEN H D. AI-assisted PHY technologies for 6G and beyond wireless networks [EB/OL]. [2022-10-16]. https://arxiv.org/abs/1908.09523
[18] TANG J, JIAO L, ZENG K, et al. Physical layer secure MIMO communications against eavesdroppers with arbitrary number of antennas [J]. IEEE transactions on information forensics and security, 2021, 16: 466-481. DOI: 10.1109/tifs.2020.3015548
[19] European-Union. General data protection regulation [R]. 2016

作 者 简 介

陆海涛，中兴通讯股份有限公司5G研发安全总监，高级工程师，CISSP；主要从事无线网络架构、无线产品安全、大规模天线、动态频谱共享等技术研究；牵头和参与10多项国家科技重大专项、“863”计划课题，获广东省科技进步奖；发表论文8篇，申请发明专利60多项。

陈一喆，南京邮电大学在读本科生；研究方向为物联网、网络安全、机器视觉、深度学习等；参与多个科研项目，其中两个项目分别获得“互联网+竞赛”江苏省一等奖和“双创大赛”江苏省二等奖。

娄笃仕（通信作者），中兴通讯股份有限公司5G研发总工、高级工程师；主要从事CDMA/WiMAX/LTE/5G移动通信技术方面的研究工作；拥有丰富的无线系统产品设计和研发经验，牵头中兴通讯5G基站产品总体方案设计和研发管理；申请发明专利15项，发表论文多篇。

基于Spark的自适应蚁群算法对CVRP问题的求解

Spark-Based Adaptive Ant Colony Algorithm for Solving CVRP Problems

徐涛/XU Tao[1]，孙鉴/SUN Jian[1,2]，刘陈伟/LIU Chenwei[1]
（1. 北方民族大学，中国 银川 750021；
2. 图像图形智能处理国家民委重点实验室，中国 银川 750021）
(1. North Minzu University, Yinchuan 750021, China;
2. The Key Laboratory of Images and Graphics Intelligent Processing of State Ethnic Affairs Commission, Yinchuan 750021, China)

DOI:10.12142/ZTETJ.202206015
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.tn.20221223.1314.001.html
网络出版日期：2022-12-27
收稿日期：2022-10-08

摘要：为解决大规模带容量限制的车辆路径问题（CVRP），提出一种基于Spark平台的自适应蚁群算法。该算法利用改进的自适应状态转移规则和动态的信息素更新策略，减轻固定参数的弊端；结合2-opt进行局部搜索优化；在Spark集群上分布式并行实现该算法，利用Spark提供的应用程序编程接口（API）实现对蚁群弹性分布式数据集（RDD）的各种操作，实现蚁群分布式计算。在标准数据集CVRPLib的实验结果表明，该算法使得大规模算例问题求解速度有显著提升。

关键词：Spark；车辆路径问题；蚁群算法；2-opt；并行计算

Abstract: An adaptive ant colony algorithm based on Spark platform is proposed to solve the large-scale capacitated vehicle routing problem (CVRP). First, the algorithm uses improved adaptive state transfer rules and dynamic pheromone update strategy to alleviate the drawbacks of fixed parameters; then, it combines 2-opt for local search optimization; finally, the algorithm is implemented in distributed parallel on Spark cluster, using the application programming interface (API) provided by Spark to realize various operations on ant colony resilient distributed datasets (RDDs) to achieve ant colony distributed computation. The experimental results on the standard dataset CVRPLIB show that the algorithm has a significant improvement in the speed of solving the large-scale arithmetic problem.

Keywords: Spark; vehicle routing problem; ant colony algorithm; 2-opt; parallel computing

作为车辆路径问题（VRP）的一个分支，带有容量限制的车辆路径问题（CVRP）和旅行商问题（TSP）相比，约束条件复杂，问题规模大，求解难度高。VRP在物流配送中具有至关重要的作用，是运筹学和组合优化领域的研究热点，受到业界广泛关注。

VRP[1]是一种NP-hard问题，主要的解决方法有精确式算法、元启发式算法、机器学习算法等。分支限界法[2-3]及动态规划法[4-5]是精确式算法[6]的代表，可以有效求解小规模的CVRP问题。例如，对于数据集CVRPLIB①中A类（set A）的27个实例，其节点规模在32~80之间[7]。但面对大规模问题，如数据集CVRPLIB中X类（Uchoa et al）的99个实例，节点规模在101~1 001之间[8]，计算复杂度较高，计算资源受限。强化学习[9-12]和深度学习[13-14]是机器学习算法的代表，但面对大规模CVRP的求解时间较长。蚁群算法[15]、模拟退火算法[16]、遗传算法[17]是元启发式算法的代表。此类算法更适用于大规模客户点的场景，能够在一个可接受的时间内得到一个相对可以接受的解。而蚁群算法由于具有蚂蚁搜索路径过程中并行的特点，结合分布式计算框架，可以有效提高解的效率。

蚁群算法本质上是一种并行算法，其中每只蚂蚁搜索路径的过程彼此独立。黄震华等[18]利用图形处理器（GPU）多线程并发的优势，提出中央处理器-图形处理器（CPU-GPU）异构环境。该环境由CPU负责控制，同时由GPU完成大部分计算任务。每只蚂蚁被分配到统一计算设备架构

基金项目：国家自然科学基金项目（62062002）；宁夏自然基金（2022AAC03289）北方民族大学中央高校基本科研业务费专项资金（FWNX09）；北方民族大学校级一般项目（2021XYZJK01）

① http://vrp.atd-lab.inf.puc-rio.br/index.php/en/

（CUDA）的不同线程上。虽然能实现蚂蚁并行，但是这种异构环境依旧是单GPU多线程的单机环境。吴昊等[19]提出基于大数据环境MapReduce框架的蚁群算法。该算法用Map函数并行每只蚂蚁求解过程，用Reduce函数表达求得较优解和改变信息素过程，同时应用云计算的管道能力，把Reduce函数的输出信息作为下一代Map函数的输入，以进行下一代循环。这种蚁群算法在求解大规模的TSP问题上取得较好的结果。与MapReduce平台蚁群优化算法相比，王诏远等[20]提出的基于Spark平台的蚁群优化算法在解决TSP问题上的执行速度提升了10倍以上。

虽然上述并行算法能较好地解决CVRPLIB中A类及X类的VRP，但这些算法仍存在求解时间长、精度不高、平台架构限制大、扩展性差等缺陷。为此，本文中我们提出一种基于Spark平台的自适应蚁群算法（SPAMACO）。

本文中，我们首先针对蚁群算法信息素导向和启发信息权重进行自适应变化设计，摆脱固定参数的弊端；分段设计信息素强度变化，及时跳出局部最优解；针对求解精度差的问题，在产生局部解时利用2–opt算子增强算法局部搜索能力；针对大规模数据集执行时间过长问题，在Spark平台实现该并行算法，将蚁群封装成弹性分布式数据集（RDD），实现蚁群在分布式集群环境下的并行构造可行解，在减少算法执行时间的前提下保证了算法的求解精度。

1 技术介绍

1.1 CVRP问题描述

在图 $G=(V,E)$ 中，顶点 $V=\{v_0,v_1,\cdots,v_n\}$，边 $E=\{(v_i,v_j),i\neq j\}$。其中，v_0 表示仓库，v_n 为第 n 个客户点。每个客户的需求为 c_i，d_{ij} 表示 (v_i,v_j) 的欧几里得距离，每辆车的最大载重为 D。约束条件如下：

（1）每辆车都必须从仓库出发，并且返回仓库；

（2）每个客户点有且只有一辆车可以进行配送服务；

（3）一条线路上客户的总需求不能超过车辆的容量限制。

CVRP的目标是在这些节点当中确定一条最短的路径。集合 $K=\{1,2,3,\cdots,k\}$ 表示运输车辆，车辆总数为 k。集合 $P=\{p_i=\{v_{i1},v_{i2},\cdots,v_{ir\,i}\}|r\in K\}$，使 P 中的 k 条路径距离和最小。其中，r_i 为由车辆 i 配送的客户节点数，v_{ij} 为车辆 i 经过的第 $j+1$ 个节点。建立模型的目标使车辆路径总长度最短。

$$\min z=\sum_{i=0}^{n}\sum_{j=0}^{n}\sum_{l=0}^{k}d_{ij}x_{ij}^{l},i\neq j \quad (1)$$

$$\text{s.t.}\sum_{i=1}^{n}\sum_{j=0}^{n}c_i x_{ij}^{l}\leqslant D \quad (2)$$

$$p_1\cup p_2\cup\ldots\cup p_n=V, \quad (3)$$

$$p_i\cap p_j=\varnothing,\forall i,j\in K,i\neq j, \quad (4)$$

其中，公式（1）为目标函数。x_{ij}^{l} 的取值为1或0，表示序号为 l 的车辆是否经过 (i,j) 边，1为经过，0为经过。公式（2）表示单量车货运量不能超过最大载重量。公式（3）和公式（4）约束每客户节点有且仅有一辆车送货。

1.2 蚁群算法

蚁群算法是M. DORIGO教授于1992年提出的。该算法源于蚂蚁觅食行为。蚂蚁在寻找食物时，会在经过的路径上释放一种信息素，并且能够感知其他蚂蚁释放的信息素。信息素浓度的大小表明路径的远近。信息素浓度越高，对应的路径距离越短。通常蚂蚁会以较大的概率优先选择信息素浓度高的路径，并且释放一定的信息素，使该条路径上的信息素浓度增高，进而使自己能够找到一条由巢穴到食物源最近的路径。但是路径上的信息素浓度会随着时间推移而逐渐衰减。

在基本蚁群算法中，人工蚂蚁在寻找路径时也会像真实蚂蚁一样，根据路径上信息素的浓度选择方向。浓度越高，选择该方向的的概率就越大。在 t 时刻，蚂蚁 k 从城市 i 到城市 j 的转移概率 $p_{ij}^{k}(t)$ 如公式（5）所示：

$$p_{ij}^{k}(t)=\begin{cases}\dfrac{\left[\tau_{ij}(t)\right]^{\alpha}\left[\eta_{ij}(t)\right]^{\beta}}{\sum\limits_{u\in Q_k(i)}\left[\tau_{ij}(t)\right]^{\alpha}\left[\eta_{ij}(t)\right]^{\beta}}, & j\in Q_k(i)\\ 0, & \text{否则}\end{cases}, \quad (5)$$

其中，$Q_k(i)=\{1,2,\cdots,n\}-\tau_k$ 表示蚂蚁 k 下一步允许选择的城市；列表 τ_k 记录这此次迭代中蚂蚁 k 的已访问城市，在接下来的遍历中不能再次访问列表 τ_k 中的城市；$\tau_{ij}(t)$ 表示 t 时刻路径 (i,j) 上信息素的数量；η_{ij} 表示启发因子，一般取路径 (i,j) 距离的倒数；α 和 β 分别表示路径上的信息素累积量和启发信息的权重比例。

当所有蚂蚁均完成遍历任务后，各条路径上的信息素数量根据公式（6）和公式（7）进行更新。

$$\tau_{ij}(t+n)=(1-\rho)\tau_{ij}(t)+\Delta\tau_{ij}(t), \quad (6)$$

$$\Delta\tau_{ij}(t)=\sum_{k=1}^{m}\Delta\tau_{ij}^{k}, \quad (7)$$

其中，$\rho(0<\rho<1)$表示路径上信息素的蒸发比例，$1-\rho$表示信息素的残余量比例；$\Delta\tau_{ij}^{k}$表示此次迭代中蚂蚁k在路径(i,j)上的信息素残余量，即增加量；$\Delta\tau_{ij}(t)$表示此次迭代中o只蚂蚁在路径(i,j)上的信息素累计增加量。

$\Delta\tau_{ij}^{k}$有3种更新模型，分别是蚁周模型、蚁量模型和蚁密模型。本文采用的是蚁周模型，如公式（8）所示。

$$\Delta\tau_{ij}^{k}=\begin{cases}\dfrac{Q}{L_k}, & \text{当蚂蚁}k\text{在本次寻找路径中经过路径}(i,j)\text{时}\\ 0, & \text{否则}\end{cases}\tag{8}$$

其中，Q为常数，L_k表示蚂蚁k在此次迭代中所走过的路径长度。

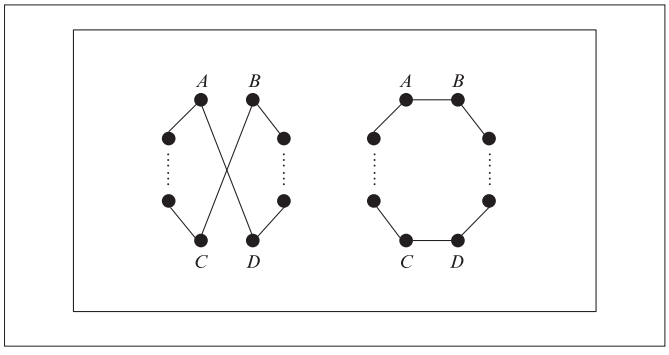
在蚁群算法求解CVRP方面，WANG X.[21]等提出一种新的ACO算法来求解CVRP。该算法允许蚂蚁多次进出仓库，直到它们访问所有客户。这简化了构建可行解的过程。LIN N.[22]等针对CVRP提出一种有效的顺序感知混合遗传算法。该算法的特征为改进的初始化策略和特定问题的交叉算子。前者结合了扫描算法，后者结合了邻域搜索启发式。S. AKPINAR[23]提出一种新的混合算法。该算法结合蚁群优化的解构造机制，执行大邻域搜索（移除和插入算子）方法来求解CVRP。R. GOEL[24]提出用蚁群和萤火虫算法（HAFA）的混合算法来求解CVRP，并在CVRP和带时间窗车辆路径问题（VRPTW）上做了验证。

1.3 局部搜索算子2-opt

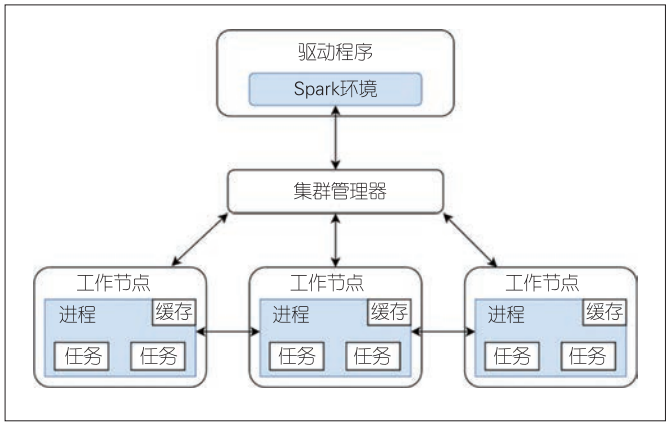
2-opt算法是一种随机性算法，其基本思想是随机取两个元素进行优化，在路径问题求解上得到广泛应用。如图1所示，路径AD、BC。如果满足$AD+BC>AB+DC$，则删除AD、AC并连接AB、DC，生成更短的路径。

1.4 Spark计算框架

Spark是Apache软件基金会三大分布式计算系统开源项目，是基于内存的分布式计算平台。与MapReduce相比，Spark可以将计算中间结果存储在内存中，不需要反复读写分布式文件系统（HDFS），提高了计算速度，因此适合需要迭代处理的算法。Spark运行架构如图2所示。



▲图1 2-opt算法优化过程



▲图2 Spark运行架构

Spark运行架构包括集群资源管理器、执行作业任务的工作节点、每个应用的任务控制节点和每个工作节点的执行进程。Spark所采用的进程有两个优点：一是用多线程执行具体任务，减少了启动开销；二是在执行进程中，会把内存和磁盘共同作为存储设备，有效减少了输入/输出（I/O）开销，提高了读写性能。

2 基于Spark框架的自适应蚁群算法设计

2.1 转移概率$p_{ij}^{k}(t)$的改进

本文采用自适应调整选择概率来提高收敛性能。公式（9）中先进行的状态转换的选择操作，使得搜索个体倾向选择信息素浓度较高且路径长度较短的城市f。

$$f=\begin{cases}\dfrac{\left[\tau_{ij}(t)\right]^{\alpha}\left[\eta_{ij}(t)\right]^{\beta}}{\sum\limits_{u\in Q_k(i)}\left[\tau_{iu}(t)\right]^{\alpha}\left[\eta_{iu}(t)\right]^{\beta}}, & q<q_0\\ \left\langle p_{ij}^{k}(t)\right\rangle, & \text{否则}\end{cases},\tag{9}$$

其中，q是$[0,1]$区间的均匀分布的随机数；$q_0=2-\arctan(ni+2)$，$(ni=1,2,\cdots,iterations)$，$iterations$为最大迭代次数。

由公式（9）可知，在开始搜索进行城市f的选择时，系统先产生一个随机数$(0\leqslant q\leqslant 1)$，以判断$q$和$q_0$的大小，然后确定转移方向。当$q<q_0$时，根据公式（9）选择最好路径，

否则采用公式（10）的自适应转移概率$\left\langle p_{ij}^{k}(t)\right\rangle$进行更新。

$$\left\langle p_{ij}^{k}(t)\right\rangle=\begin{cases}\dfrac{\left[\tau_{ij}(t)\right]^{\delta}\left[\eta_{ij}(t)\right]^{\gamma}}{\sum\limits_{u\in Q_k(i)}\left[\tau_{iu}(t)\right]^{\delta}\left[\eta_{iu}(t)\right]^{\gamma}}, & j\in Q_k(i)\\ 0, & \text{否则}\end{cases} \tag{10}$$

其中，信息素积累$\delta=\dfrac{2\alpha ni}{iterations}+\alpha$，启发信息$\gamma=\dfrac{\beta ni}{iterations}+\alpha$。随着迭代次数增加，权重比例不断变化。这样可实现自适应变化，消除固定参数的弊端。

2.2 信息素强度的动态调整

在前期，算法收敛比较慢；在后期，路径信息素浓度过大（容易造成局部最优）。对此，本文采用公式（11）中的分段函数代替常数Q。

$$Q_i=\begin{cases}Q, & iterations/3 > ni\\ \dfrac{Q}{2}, & iterations/2 > ni > iterations/3\\ \dfrac{Q}{4}, & iterations > ni > iterations/2\end{cases}。 \tag{11}$$

当最优解在一段时间内不变化时，搜索过程可能陷入局部最优困境。此时，分段的信息素设定可以增加或者减少信息素的数量影响。这使系统可以跳出局部最优困境。

2.3 自适应蚁群算法的并行化实现

用Spark平台可以完成自适应蚁群算法的并行实现。我们采用RDD进行操作，实现蚁群并行构建求解过程。

具体的SPAMACO步骤如下：

1）读取CVRPLIB数据文件，初始化车辆数量k、车辆容量D，构建坐标点（x,y）、客户点需求$demand$，计算各点距离，初始化信息素矩阵；

2）初始化参数；

3）封装蚂蚁为Ant类，利用Spark的.parallelize()操作将蚂蚁装换为分布式的RDD；

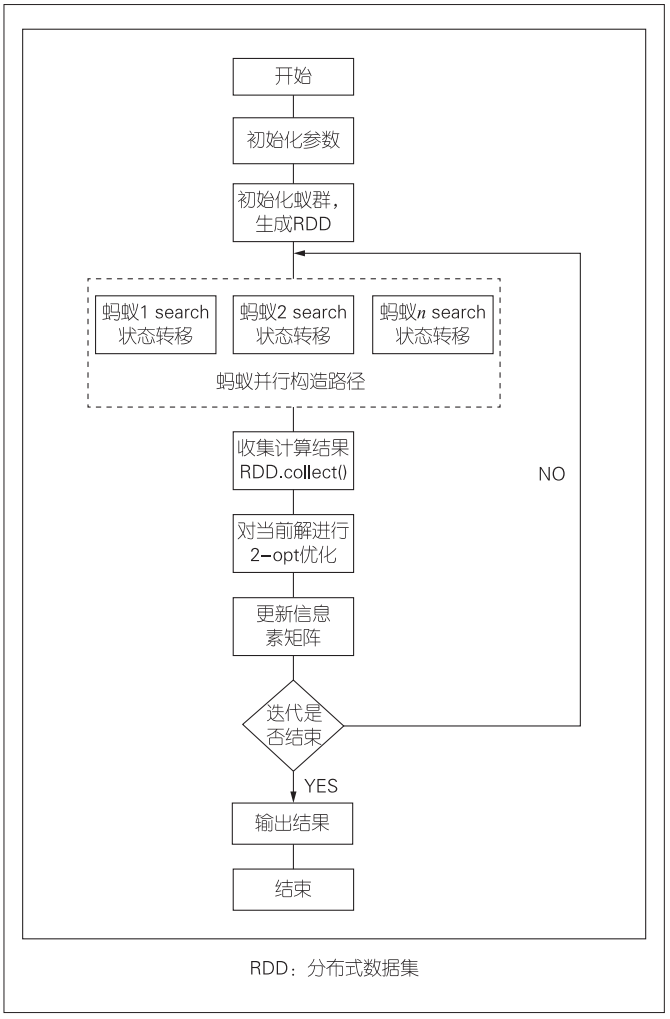
4）在每轮迭代中通过Spark的.map()方法实现并行求解过程；

5）每轮迭代结束后通过Spark的.collect()方法收集计算结果，对其进行2-opt局部优化；

6）更新信息素并广播；

7）判断迭代是否结束，结束输出全局最优解，否则返回步骤4继续并行计算求解。

综上所述，算法流程如图3所示。



▲图3 基于Spark的自适应蚁群算法求解CVRP流程图

3 数值实验

3.1 实验设计

本文基于Spark分布式集群实现SPAMACO。实验环境由8台虚拟机组成，其中包括1台master主节点（负责任务控制节点的运行和管理），7台执行节点。

硬件配置：每台虚拟机CPU为四核四线程，内存为4 GB，磁盘容量为40 GB。操作系统是64位的Ubuntu18.04。

软件配置：Spark2.4.0、hadoop3.1.3、java1.8.0_162。实验中，我们采用具有函数式编程特性的python语言，同时为验证SPAMACO算法的有效性，采用自适应动态搜索蚁群算法（ADACO）[25]和自适应贪婪蚁群算法（GSACO）[26]作为对比实验。其中，为了保证公平性，GSACO和ADACO的参

数选用原文中的参数设置。3个算法的迭代次数均为200次。

3.2 小规模算例实验结果

对于小规模算例，本文采用CVRPLIB中的A类数据集（SET A Benchmark），并选取A-n60-k9、A-n61-k9、A-n62-k9、A-n62-k10、A-n63-K9、A-n64-k9、A-n65-k9、A-n69-k9、A-n80-k10进行求解。实验结果如表1所示，其中*V*表示当前算法最优解，*T*表示程序运行时间。

▼表1 小规模算例实验结果

算例	ADACO		GSACO		SPAMACO	
	V	*T*/s	*V*	*T*/s	*V*	*T*/s
A-n60-k9	1 505.99	70.51	1 490.72	63.36	1 434.19	77.37
A-n61-k9	1 193.36	76.67	1 181.34	66.16	1 107.43	77.64
A-n62-k9	1 432.71	81.84	1 395.79	66.85	1 381.43	74.59
A-n62-k10	1 819.90	81.29	1 784.36	70.17	1 769.49	80.28
A-n63-k9	1 413.09	82.00	1 463.69	69.93	1 388.44	81.78
A-n64-k9	1 581.80	85.21	1 511.13	74.18	1 445.88	81.77
A-n65-k9	1 359.61	92.16	1 348.06	76.75	1 320.60	84.86
A-n69-k9	1 354.16	105.92	1 240.56	96.01	1 305.17	87.38
A-n80-k10	2 098.46	160.89	1 898.82	138.18	1 833.32	114.72

ADACO：自适应动态搜索蚁群算法　　GSACO：自适应贪婪蚁群算法
SPAMACO：基于Spark平台的自适应蚁群算法

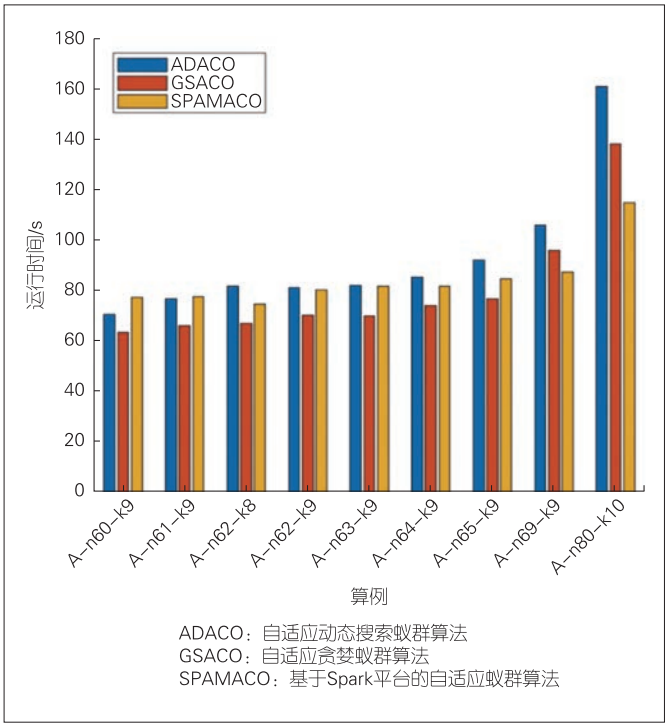
从表1可以看出，和ADACO、GSACO相比，SPAMACO在求解精度上有所提升。但是由于受到Spark集群初始化时间、广播时间和组间通信等的影响，在小规模算例上，SPAMACO的运行时间优势并不明显。在客户点大于65后，并行的执行时间优势逐渐体现。在执行A-n80-k10算例时，本文算法执行时间比ADACO低28.8%，比GSACO低17%。

由图4可以看出，对于小规模算例，随着客户点数的增加，3个算法的执行时间会逐步增加。其中，除A-n80-k10以外，这种增加比例几乎相同。

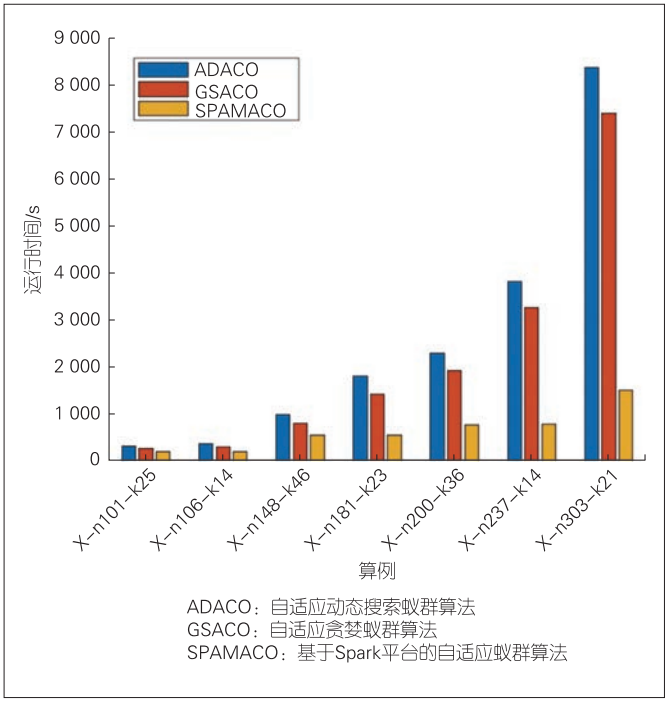
3.3 大规模算例实验结果

对于大规模算例，本文采用CVRPLIB中的X类数据集（Uchoa et al. Benchmark），选取X-n101-k25、X-n106-k14、X-n148-k46、X-n181-k23、X-n200-k36、X-n237-k14、X-n303-k21，并进行求解，结果如表2所示。

从图5可以看出，在大规模算例上（n>100），随着客户点数的增加，ADACO和GSACO的执行时间呈指数增长，而本文所提算法的时间增加比率几乎不变。这是因为此时程序运行的大部分时间都是算法执行时间，同时Spark初始化、广播时间和组间通信所用时间占比也变小了。因此Spark基



▲图4 小规模算例运行时间



▲图5 大规模算例运行时间

于内存的并行计算优势逐步体现出来。

在101个点时，本文所提算法的执行时间比ADACO快39.7%，比GSACO快29.0%。当客户点数增加时，如在200个点时，本文所提算法的执行时间比ADACO快66.6%，比GSACO快60.1%。在300个点时，本文所提算

法的执行时间比ADACO快82.1%，比GSACO快79.7%。因此，SPAMACO更适合处理大规模算例，并且随着算例规模的增加，时间提升效果明显增加。

4 结束语

本文提出了一种基于Spark框架的自适应蚁群算法SPAMACO，结合2-opt局部优化算子，在解决大规模CVRP上效果明显。数值实验表明，该算法在大规模算例应用上具有明显优势。在保证时间优势的条件下，未来我们将进一步探讨最优解。

参考文献

[1] 庞燕, 罗华丽, 邢立宁, 等. 车辆路径优化问题及求解方法研究综述 [J]. 控制理论与应用, 2019, 36(10): 1573-1584. DOI: 10.7641/CTA.2019.90120
[2] LU D. The robust vehicle routing problem with time windows: solution by branch and price and cut [J]. European journal of operational research, 2019, 275(3): 925-938. DOI: 10.1016/j.ejor.2018.12.019
[3] REIHANEH M. A branch-and-price algorithm for a vehicle routing with demand allocation problem [J]. European journal of operational research, 2019, 272(2): 523-538. DOI: 10.1016/j.ejor.2018.06.049
[4] SOYSAL M, et al. A simulation based restricted dynamic programming approach for the green time dependent vehicle routing problem [J]. Computers & operations research, 2017, 88: 297-305. DOI: 10.1016/j.cor.2017.06.023
[5] ÇIMEN M. Time-dependent green vehicle routing problem with stochastic vehicle speeds: an approximate dynamic programming algorithm [J]. Transportation research part D: transport and environment, 2017, 54: 82-98. DOI: 10.1016/j.trd.2017.04.016
[6] SAVITRI H, KURNIAWATI D A. Sweep algorithm and mixed integer linear program for vehicle routing problem with time windows [J]. Journal of advanced manufacturing systems, 2018, 17(4): 505-513. DOI: 10.1142/s0219686718500282
[7] COSSIO E, HERNANDEZJ A, OCHOA-ZEZZATT C A, et al. Comparison between instances to solve the CVRP [J]. International journal of combinatorial optimization problems and informatics, 2018, 9(2): 41.
[8] BONILHA I S, MAVROVOUNIOTIS M, MÜLLER F M, et al. Ant colony optimization with heuristic repair for the dynamic vehicle routing problem [C]//Proceedings of 2020 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, 2021: 313-320. DOI: 10.1109/SSCI47803.2020.9308156
[9] 牛鹏飞, 王晓峰, 芦磊, 等. 强化学习在车辆路径问题中的研究综述 [J]. 计算机工程与应用, 2022, 58(1): 41-55. DOI: 10.3778/j.issn.1002-8331.2108-0467
[10] XU Y, FANG M, CHEN L, et al. Reinforcement learning with multiple relational attention for solving vehicle routing problems [J]. IEEE transactions on cybernetics, 2022, 52(10): 11107-11120. DOI: 10.1109/tcyb.2021.3089179
[11] PENG B, WANG J H, ZHANG Z Z. A deep reinforcement learning algorithm using dynamic attention model for vehicle routing problems [M]// Communications in computer and information science. Singapore: Springer Singapore, 2020: 636-650.. DOI: 10.1007/978-981-15-5577-0_51
[12] XIN L, SONG W, CAO Z G, et al. Multi-decoder attention model with embedding glimpse for solving vehicle routing problems [J]. Proceedings of the AAAI conference on artificial intelligence, 2021, 35(13): 12042-12049. DOI: 10.1609/aaai.v35i13.17430
[13] BDEIR A, BOEDER S, DERNEDDE T, et al. RP-DQN: an application of Q-learning to vehicle routing problems [EB/OL]. [2022-10-16]. https://arxiv.org/abs/2104.12226
[14] ZHAO J X, MAO M J, ZHAO X, et al. A hybrid of deep reinforcement learning and local search for the vehicle routing problems [J]. IEEE transactions on intelligent transportation systems, 2021, 22(11): 7208-7218. DOI: 10.1109/TITS.2020.3003163
[15] 李奕颖, 秦刚. 基于Spark的改进蚁群算法对带时间窗车辆路径问题的求解 [J]. 计算机系统应用, 2019, 28(7): 9-16. DOI: 10.15888/j.cnki.csa.007000
[16] 孙鉴, 刘淞佐, 武晓晓, 等. 基于Spark的并行模拟退火算法求解TSP [J]. 电子测量技术, 2022, 45(4): 53-58. DOI: 10.19651/j.cnki.emt.2108429
[17] 唐坤. 车辆路径问题中的遗传算法设计 [J]. 东华大学学报(自然科学版), 2002, 28(1): 66-70. DOI: 10.3969/j.issn.1671-0444.2002.01.015
[18] 黄震华, 赵振岐, 林培裕, 等. 基于异构平台的并行最大最小蚁群算法 [J]. 同济大学学报(自然科学版), 2016, 44(12): 1949-1955. DOI: 10.11908/j.issn.0253-374x.2016.12.021
[19] 吴昊, 倪志伟, 王会颖. 基于MapReduce的蚁群算法 [J]. 计算机集成制造系统, 2012, 18(7): 1503-1509. DOI: 10.13196/j.cims.2012.07.162.wuh.019
[20] 王诏远, 王宏杰, 邢焕来, 等. 基于Spark的蚁群优化算法 [J]. 计算机应用, 2015, 35(10): 2777-2780+2797. DOI: 10.11772/j.issn.1001-9081.2015.10.2777
[21] WANG X Y, CHOI T M, LIU H K, et al. Novel ant colony optimization methods for simplifying solution construction in vehicle routing problems [J]. IEEE transactions on intelligent transportation systems, 2016, 17(11): 3132-3141. DOI: 10.1109/TITS.2016.2542264
[22] LIN N, SHI Y J, ZHANG T L, et al. An effective order-aware hybrid genetic algorithm for capacitated vehicle routing problems in Internet of Things [J]. IEEE access, 2019, 7: 86102-86114. DOI: 10.1109/ACCESS.2019.2925831
[23] AKPINAR S. Hybrid large neighbourhood search algorithm for capacitated vehicle routing problem [J]. Expert systems with applications, 2016, 61: 28-38. DOI: 10.1016/j.eswa.2016.05.023
[24] GOEL R. A hybrid of ant colony and firefly algorithms (HAFA) for solving vehicle routing problems [J]. Journal of computational science, 2018, 25: 28-37. DOI: 10.1016/j.jocs.2017.12.012
[25] 贺智明, 郑丽, 梁文. 基于自适应动态搜索蚁群算法的车辆路径规划 [J]. 计算机工程与设计, 2021, 42(2): 543-551. DOI: 10.16208/j.issn1000-7024.2021.02.036
[26] LI W, XIA L, HUANG Y, et al. An ant colony optimization algorithm with adaptive greedy strategy to optimize path problems [J]. Journal of ambient intelligence and humanized computing, 2022, 13(3): 1557-1571. DOI: 10.1007/s12652-021-03120-0

作 者 简 介

徐涛，北方民族大学在读硕士研究生、CCF会员；主要研究方向为大数据技术等。

孙鉴，北方民族大学讲师、CCF会员；主要研究方向为大数据、存储与管理等。

刘陈伟，北方民族大学在读硕士研究生、CCF会员；主要研究方向为云计算、任务调度等。

《中兴通讯技术》第28卷总目次

通信感知一体化技术

网络内生安全

卷·期·页

专家论坛

企业视界

技术广角

《中兴通讯技术》杂志（双月刊）投稿须知

一、杂志定位

《中兴通讯技术》杂志为通信技术类学术期刊。通过介绍、探讨通信热点技术，以展现通信技术最新发展动态，并促进产学研合作，发掘和培养优秀人才，为振兴民族通信产业做贡献。

二、稿件基本要求

1. 投稿约定

（1）作者需登录《中兴通讯技术》投稿平台：tech.zte.com.cn/submission，并上传稿件。第一次投稿需完成新用户注册。

（2）编辑部将按照审稿流程聘请专家审稿，并根据审稿意见，公平、公正地录用稿件。审稿过程需要 1 个月左右。

2. 内容和格式要求

（1）稿件须具有创新性、学术性、规范性和可读性。

（2）稿件需采用 WORD 文档格式。

（3）稿件篇幅一般不超过 6 000 字（包括文、图），内容包括：中、英文题名，作者姓名及汉语拼音，作者中、英文单位，中文摘要、关键词（3 ~ 8 个），英文摘要、关键词，正文，参考文献，作者简介。

（4）中文题名一般不超过 20 个汉字，中、英文题名含义应一致。

（5）摘要尽量写成报道性摘要，包括研究的目的、方法、结果 / 结论，以 150 ~ 200 字为宜。摘要应具有独立性和自明性。中英文摘要应一致。

（6）文稿中的量和单位应符合国家标准。外文字母的正斜体、大小写等须写清楚，上下角的字母、数据和符号的位置皆应明显区别。

（7）图、表力求少而精（以 8 幅为上限），应随文出现，切忌与文字重复。图、表应保持自明性，图中缩略词和英文均要在图中加中文解释。表应采用三线表，表中缩略词和英文均要在表内加中文解释。

（8）所有文献必须在正文中引用，文献序号按其在文中出现的先后次序编排。常用参考文献的书写格式为：

- 期刊 [序号] 作者 . 题名 [J]. 刊名 , 出版年 , 卷号 (期号): 引文页码 . 数字对象唯一标识符
- 书籍 [序号] 作者 . 书名 [M]. 出版地 : 出版者 , 出版年 : 引文页码 . 数字对象唯一标识符
- 论文集中析出文献 [序号] 作者 . 题名 [C]// 论文集编者 . 论文集名 (会议名). 出版地：出版者 , 出版年 (开会年): 引文页码 . 数字对象唯一标识符
- 学位论文 [序号] 作者 . 题名 [D]. 学位授予单位所在城市名：学位授予单位，授予年份 . 数字对象唯一标识符
- 专利 [序号] 专利所有者 . 专利题名 : 专利号 [P]. 出版日期 . 数字对象唯一标识符
- 国际、国家标准 [序号] 标准名称 : 标准编号 [S]. 出版地 : 出版者 , 出版年 . 数字对象唯一标识符

（9）作者超过 3 人时，可以感谢形式在文中提及。作者简介包括：姓名、工作单位、职务或职称、学历、毕业于何校、现从事的工作、专业特长、科研成果、已发表的论文数量等。

（10）提供正面、免冠、彩色标准照片一张，最好采用 JPG 格式（文件大小超过 100 kB）。

（11）应标注出研究课题的资助基金或资助项目名称及编号。

（12）提供联系方式，如：通讯地址、电话（含手机）、Email 等。

3. 其他事项

（1）请勿一稿多投。凡在 2 个月（自来稿之日算起）以内未接到录用通知者，可致电编辑部询问。

（2）为了促进信息传播，加强学术交流，在论文发表后，本刊享有文章的转摘权（包括英文版、电子版、网络版）。作者获得的稿费包括转摘酬金。如作者不同意转摘，请在投稿时说明。

（3）编辑部地址：安徽省合肥市金寨路 329 号凯旋大厦 1201 室，邮政编码：230061。

（4）联系电话：0551-65533356，联系邮箱 : magazine@zte.com.cn。

（5）本刊只接受在线投稿，欢迎访问本刊投稿平台：tech.zte.com.cn/submission。

中兴通讯技术

(ZHONGXING TONGXUN JISHU)

办刊宗旨：

以人为本，荟萃通信技术领域精英
迎接挑战，把握世界通信技术动态
立即行动，求解通信发展疑难课题
励精图治，促进民族信息产业崛起

双月刊　1995 年创刊　总第 167 期
2022 年 12 月　第 28 卷 第 6 期

主管：安徽出版集团有限责任公司
主办：时代出版传媒股份有限公司
　　深圳航天广宇工业有限公司
出版：安徽科学技术出版社
编辑、发行：中兴通讯技术杂志社

总编辑：王喜瑜
主编：蒋贤骏
执行主编：黄新明
编辑部主任：卢丹
责任编辑：徐烨
编辑：杨广西、朱莉、任溪溪
设计排版：徐莹
发行：王萍萍
编务：王坤

《中兴通讯技术》编辑部
地址：合肥市金寨路 329 号凯旋大厦 1201 室
邮编：230061
网址：tech.zte.com.cn
投稿平台：tech.zte.com.cn/submission
电子信箱：magazine@zte.com.cn
电话：(0551)65533356

发行方式：自办发行
印刷：合肥添彩包装有限公司
出版日期：2022 年 12 月 20 日
中国标准连续出版物号：ISSN 1009-6868
CN 34-1228/TN
定价：每册 20.00 元