面向算力网络的安全能力研究

Research on Security Capability for Computing Power Network

王蕴实[1,2]，傅　瑜[1,2]，徐　雷[1,2]（1. 中国联通研究院，北京 100048；2. 下一代互联网宽带业务应用国家工程研究中心，北京 100048）

Wang Yunshi[1,2], Fu Yu[1,2], Xu Lei[1,2] (1. China Unicom Research Institute, Beijing 100048, China; 2. Next Generation Internet Broadband Service Application National Engineering Research Center, Beijing 100048, China)

摘　要：

算力网络作为全新的网络基础设施，其新型网络架构、多样化的服务场景以及新技术的应用，给算力网络安全带来了新的风险和需求。介绍了算力网络的发展机遇，分析了算力网络新的安全挑战，提出了算力网络安全能力框架，并探讨了解决相关安全风险的算力网络安全能力部署建议。

关键词：

算力网络；安全；能力

doi：10.12045/j.issn.1007-3043.2024.06.004

文章编号：1007-3043（2024）06-0018-04

中图分类号：TP393.4

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract:

As a new network infrastructure, computing power networks have brought new risks and demands to their security due to their new network architecture, diversified scenarios, and the application of new technologies. It introduces the development opportunities and new challenges of computing power network, puts forward security capability architecture for the computing power network and discusses the deployment suggestions for computing power network security capabilities to address related security risks.

Keywords:

Computing power network; Security; Capability

引用格式：王蕴实，傅瑜，徐雷. 面向算力网络的安全能力研究[J]. 邮电设计技术，2024（6）：18-21.

0 引言

算力作为支撑数字经济持续向纵深发展的重要动力，已经成为全球战略竞争的新焦点，它将带动数字经济的创新发展迈向新台阶。算力网络是面向未来计算与网络深度协同的新型网络架构。以现有网络技术为基础，算力网络通过无所不在的网络连接分布式计算节点，实现服务的自动化部署、最优路由和负载均衡。从而构建连接+算力+服务的全新网络基础设施[1]。算力网络作为全新的网络基础设施，其新型网络架构、多样化的服务场景以及新技术的应用，给算力网络带来了新的安全需求和挑战，需要学术界、产业界的协作研究。

收稿日期：2024-04-01

1 算力网络发展机遇

当前新一轮科技革命和产业变革正在重塑全球经济结构，算力网络成为带动数字经济发展的主引擎，算力网络利好政策相继出台。2021年5月，国家发展改革委、中央网信办、工业和信息化部、国家能源局联合印发了《全国一体化大数据中心协同创新体系算力枢纽实施方案》，明确提出布局全国算力网络国家枢纽节点，启动实施“东数西算”工程，构建国家算力网络体系。2023年10月8日，工业和信息化部等6部门联合印发《算力基础设施高质量发展行动计划》。

2023年12月，国家发展改革委等部门发布《关于深入实施“东数西算”工程加快构建全国一体化算力网的实施意见》，进一步加快构建全国一体化算力网，以算力高质量发展支撑经济高质量发展。此外，国内三大运营商均已明确提出算力网络和云网融合发展的战略及举措，聚合计算与网络资源的能力，加快提供算网一体化服务。

2 算力网络安全新挑战

算力网络整合泛在、多源、多域的算力节点进行分布式计算，通过异构通信网络进行数据分发传输，按需为用户提供服务，算力和网络的融合打破了传统的安全域，为算力网络带来新的安全需求和挑战。

a）节点安全能力差异化。算力网络引入多样化算力节点，包括多形态终端、边缘算力节点、集中式云计算平台。节点安全属性等方面存在巨大差异。算力节点的可信评估与安全认证机制尚不成熟，算力节点可信度存在安全风险。

b）网算资源分布泛在化。算力网络中云、边、端各类算力节点泛在化分布，各算力节点间需要互联互通，将引入复杂多样的安全暴露面，攻击者也获得了更多的攻击路径。算力资源在泛在分布的网算资源间进行跨系统、跨域动态调度，海量分布式算力协同整合，也进一步提出了新的安全机制要求。

c）业务安全需求多样化。算力网络赋能数字经济中社会应用、生产应用和生活应用等多样化的业务场景，为多方算力节点提供算力对外输出平台，面向海量用户及节点提供算力交易服务。不同业务的形态也对算力网络提出了差异化的安全需求。

d）数据跨域流通规模化。数据在算力网络中跨节点、跨层级流通，加剧数据安全风险，需要对算力网络数据进行全生命周期安全管理，并根据上级监管要求，履行数据安全保护职责。重点保障跨域数据传输安全，构建针对用户隐私信息、算网业务数据、算力交易数据等安全保护机制，有效监测和处置各类数据安全风险和事件。

3 面向算力网络的安全能力架构体系

面对算力网络全新的安全需求和安全挑战，需要部署相应的安全能力来应对。面向算力网络的安全能力架构如图1所示，主要包括设备内生安全能力、网络韧性安全能力、编排管理安全能力、运营服务安全能力和数据安全能力等。

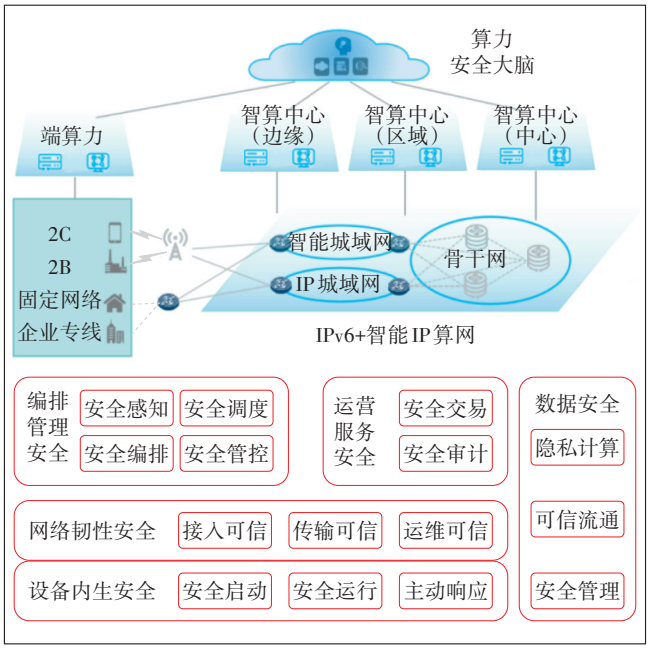

图1　算力网络的安全能力架构

3.1 设备内生安全能力

3.1.1 安全启动能力

安全启动是保护算力网络设备在启动阶段的安全性和完整性，防止系统程序被外部篡改的重要安全能力。它是基于硬件可信根的信任传递来验证后续加载固件、软件及应用的系统启动过程，其密码学基础是公钥加密算法、数字签名技术和哈希散列算法。安全启动应遵循“先校验，再执行”的原则，校验不过，则阻止系统继续启动，保障算力设备源头可信。

3.1.2 安全运行能力

安全运行是指通过安全隔离、权限控制、安全编译等安全手段，保障算力网络设备运行态安全的安全能力。可以通过对算网设备的内核态与用户态进行安全隔离，防止某个应用程序出错而影响操作系统的安全运行。通过对算网设备的不同进程进行隔离，避免某个进程被攻击，破坏其他进程。通过实施权限最小化原则，对算网设备系统关键文件、目录和运行的进程进行访问控制。通过安全编译加固算力网络设备系统软件的安全性，增加对应用内存数据的保护，阻断异常。

3.1.3 主动响应能力

算力网络设备除了保证自身启动、运行阶段安全，还应该具备安全主动响应能力，包括安全配置核查、入侵检测、攻击防御和安全态势感知等安全能力。

通过安全配置核查对安全配置项进行及时核查和风险提示,识别设备侧不安全配置,并进行安全加固。通过入侵检测能力对网络攻击、系统后门、异常操作行为进行动态分析检测,并通过攻击防御能力,主动提供对DDos攻击、ARP欺骗等攻击的响应处理能力。算力网络设备需要支持收集自身运行状态及所处环境等威胁情报源信息,并上报态势感知平台,支撑算力网络全域态势感知。

3.2 网络韧性安全能力

3.2.1 接入可信能力

算力网络接入可信体现在用户身份接入可信、互联设备接入可信和访问应用接入可信3个方面。算力网络用户包括消费互联网用户和产业互联网用户。需要建立用户身份统一标识,进行用户身份认证。可以基于运营商移动认证方法,以运营商基础网络资源作为统一开放的用户标识。另外,根据不同接入场景的需求,可以通过分级授权的方式,实现不同应用之间的业务接入[2]。针对算力网络归属权极度分散的分布式网络部署特点,对于规模化的算力节点的接入认证,可以结合区块链技术,屏蔽算力节点属性差异,构建统一的算力节点入网动态认证机制。

3.2.2 传输可信能力

算力节点间传输的安全可靠是算网安全的基本要求。算网安全传输需要根据计算类业务需求,结合实时网络状况和可服务的计算资源状况,动态灵活地将计算任务路由到合适的目标计算节点并保障业务的用户体验。算力网络为了满足“城域+骨干”端到端互联网业务差异化保障,通过应用SRv6技术,实现差异化业务需求的最优路径选择。攻击者通过窃取、定义SRv6路由扩展头,可实现网络拓扑窃取、安全防护被绕过、流量劫持、DDoS攻击等源路由威胁。需要通过定义SRv6信任域、SRv6扩展头校验等安全手段来防范,保障地址使用安全和转发路径安全[3]。

3.2.3 运维可信能力

算力网络需要对泛在分布的网算资源进行安全运维,对验证通信节点、访问身份、承载网络、共享资源的真实性的安全需求进一步提高。零信任技术是一种以资源保护为核心的网络安全范式,持续评估重要的算力资源、互联算力节点、重要上层应用的接入安全。采用零信任技术进行可信运维,从对算力网络用户访问主体的不信任开始,通过持续的身份鉴别和监测评估,动态调整访问策略和权限,实施精细化的访问控制和安全防护,有助于保障算力网络持续、健康、可靠的运行[4]。

3.3 编排管理安全能力

3.3.1 安全感知能力

算力网络安全感知的对象主要包括计算任务安全需求和计算节点的安全信息。计算任务安全需求包括计算节点的安全需求和安全服务的需求,可通过扩展IPv6协议字段携带或用户订阅等方式获得。感知计算节点安全信息包括计算节点的身份标识信息、安全配置情况、安全防护机制、安全服务能力等[5]。

安全感知信息作为安全资源编排的基础,在算力网络安全感知过程中,需要对算网节点身份进行统一标识,便于进行统一身份认证、安全风险溯源及安全事件及时处置。同时,可以考虑增加安全标识信息,便于算力资源的安全接入和安全分级分类管理。

3.3.2 安全编排能力

算力网络安全编排通过安全感知信息获取用户安全需求和计算节点安全信息,关联安全需求与安全能力,生成安全策略,对算力资源和网络资源进行统一的安全编排,实现安全策略与业务的协同。算力网络安全编排过程中,应该通过安全通道收集网络和算力资源信息数据,确保信息数据的机密性、完整性和真实性。对于用户信息、任务数据、算力资源分布信息等算力敏感数据,需时刻对其进行监控和防护,保障数据安全。另外,编排管理行为应受到授权和监控,对编排管理系统的访问权限应分级授权,防止非法用户越权调度算力网络资源。

3.3.3 安全调度能力

面对高度复杂的算网环境,针对多样化、定制化的算力需求,算力网络需要对算力资源和网络资源进行联合调度,调度过程中要充分考虑安全要素。算力和网络跨域拉通时,建立管理通道和控制通道应进行双向认证,加强访问控制。并根据任务需求,结合算力用户、算力任务、算力节点以及算力资源的安全等级标识,将任务调度到具有相应安全等级的资源节点处,实现算力的安全调度。在具体调度过程中,需要根据实际情况对用户信息和任务数据进行加密传输,采用动态监测和节点验证等手段保障安全[6]。

3.3.4 安全管控能力

算力安全管控主要对算力资源和业务行为进行安全监测和管理,确保算力资源的合法性,满足算力服务的可管理安全需求,对算力滥用、异常冲突、安全

攻击以及隐私泄露等安全问题及时处理解决。为加强算力网络的安全防御能力，安全管控需要从被动防御转变为自主检测和主动防御。可以通过对算力资源进行访问控制，来确保只有授权用户和程序能够使用所辖算力资源。对算力资源进行安全监控和审计，在检测到安全状态异常时应触发告警或其他自动响应机制。通过限制算力用量、拒绝算力请求或降低算力用户信用等措施对非法算力使能行为进行管控。

3.4 运营服务安全能力

3.4.1 安全交易能力

算力交易的主要目标是确保交易参与方的真实可信和交易过程的安全可控。算力交易参与方包括算力供需双方及交易平台运营商。算力交易过程包括用户注册、业务需求申请、交易订单签订、任务执行与计费、交易费用结算和服务评价与反馈等。对于中心式交易方式，由平台处理信息展示和交易流程，需要平台制定安全策略，保障交易安全。对于分布式交易方式，需要多方协作，实现分布式算力安全统一运营，可以通过区块链技术在链节点上进行信息展示和交易，保障交易安全。

3.4.2 安全审计能力

算力网络安全审计能力应支持在各层级数据访问节点对数据处理活动进行审计。尤其对算力网络中重要数据（包括系统数据、配置参数、业务数据和用户数据等）的处理活动进行记录和审计，对重要记录进行备份，追溯数据的各处理环节。

3.5 数据安全能力

3.5.1 隐私计算能力

算力节点间跨域、跨层级通信，可能会带来许多隐私暴露问题。隐私计算技术融合密码学、人工智能等多学科，技术路线主要的三大方向为：多方安全计算、联邦学习、可信执行环境。算力网络的数据安全方面需要具备隐私计算能力，确保在隐私数据保护的前提下进行分析应用，实现数据“可用不可见”，解决隐私信息的所有权和使用权分离时隐私泄漏等安全问题，可解决高安行业和算力并网后数据安全风险。

3.5.2 可信流通能力

数据在算力网络中跨节点、跨层级流通，加剧数据泄露安全风险，需要构建数据安全的共享管控能力，解决数据交易中敏感信息共享后被泄露的风险。需要具备数据标记能力，对数据出网和数据流转等行为进行管控。同时，可以考虑利用区块链技术去中心化和防篡改的特点，通过分布式共识算法及智能合约构建多方共识，通过基于区块链的分布式数据凭证构建跨系统、跨节点的数据流转标记能力和确权能力，可以实现数据出网可管控，数据流转可感知。

3.5.3 数据安全管理能力

算力网络处理大量的数据信息，包括节点标识信息、业务数据信息、资产信息和管理数据信息等。算力网络数据在采集、存储、传输、利用、销毁的处理环节都存在安全风险，算力网络需要具备对数据进行全生命周期安全防护和管理能力[7]，包括数据采集阶段的数据标识能力，数据传输阶段的数据加密和数据脱敏能力，数据存储阶段的数据存储加密和数据防勒索能力，以及数据计算阶段的隐私计算能力等，并能根据上级监管要求，具备数据分级分类管理能力，履行数据安全的保护职责。

4 结束语

算力网络作为将算力和网络深度融合，一体化服务的新型基础设施，成为全球战略竞争的新焦点，算力网络安全更是算力网络健康发展的重中之重。要以安全为基，筑牢算力网络屏障。全行业需要通过共同的算力网络安全理念、共识的算力网络安全框架及共建的算力网络安全能力，应对潜在的安全挑战。

参考文献：

[1] 姚惠娟，陆璐，段晓东. 算力感知网络架构与关键技术[J]. 中兴通讯技术，2021，27(3)：7-11.
[2] 中国移动. 算力网络安全白皮书[EB/OL]. [2024-03-22]. https://www.sgpjbg.com/bgdown/55126.html.
[3] CCSA. 基于SRv6的软件定义广域网络（SD-WAN）路由安全总体技术要求[EB/OL]. [2024-03-22] https://www. doc88. com/p-99939665338439.html
[4] 王蕴实，张曼君，徐雷，等. 天地一体化网络安全使能技术研究[J]. 邮电设计技术，2023(8)：1-4.
[5] CCSA. 算力网络安全参考框架[EB/OL]. [2024-03-22]. https://www.ccsa.org.cn/.
[6] 袁长卿，苏越，赵伟博. 面向算力网络的安全体系研究[J]. 信息通信技术与政策，2023，49(2)：82-86.
[7] 赵晨斌，王蕴实. 基于5G/5G-A的天地一体化网络安全风险及策略研究[J]. 通信世界，2023(12)：46-49.

作者简介：
王蕴实，毕业于北京邮电大学，高级工程师，主要从事网络与信息安全研究工作；傅瑜，毕业于北京邮电大学，首席研究员，主要从事网络与信息安全研究工作；徐雷，毕业于北京理工大学，教授级高级工程师，主要从事网络与信息安全研究工作。