面向智算融合网络的自主防御范式研究

刘 颖[1,2],夏 雨[1],于成晓[2*],张维庭[1],汪润虎[3],张宏科[1]
(1. 北京交通大学电子信息工程学院,北京 100044;2. 鹏城实验室,广东深圳 518055;
3. 中国电子科技集团有限公司第二十八研究所,江苏南京 210007)

摘 要: 随着数字经济时代算力供给模式的变革,以算力为核心的新型网络基础设施已成为实现算力资源共享、支撑数字经济转型的重要动力. 在算力网络中,多元异构用户终端通过多种方式高频接入网络以随时随地获取算力服务,网络的开放性和动态性增大,算力网络将面临更严峻的安全挑战. 然而,基于传统网络的安全防御模式通常针对具体安全问题静态式增补安全防护组件,无法主动适配用户需求灵活调整防御策略,难以应对算力网络中的安全风险. 因此,本文面向新型算力网络安全需求,将安全功能作为网络内部属性,基于智算融合网络提出一种多维协同自主防御范式. 结合智算融合网络"三层""三域"的设计思想,在"三层"中,以广义服务层定义安全固有服务,以映射适配层智慧适配安全功能,以融合组件层执行安全策略;在"三域"中,以实体域先导资源适配,以知识域驱动安全服务流程,以感控域实施具体安全技术,构建"检测""溯源""防御"三维一体的完整基础管控流程,其中安全策略与技术可根据场景扩展性与业务安全性进行灵活调整. 最终,通过仿真实验对所提范式有效性进行了验证,为未来智算融合安全的进一步研究和应用提供参考.

关键词: 智算融合网络;算力网络;自主防御;防御范式;网络攻击
基金项目: 鹏城实验室重大项目;国家重点研发计划(No.2022ZD0115301);国家自然科学基金(No.62201029);中国博士后科学基金(No.2022M710007,No.BX20220029)
中图分类号: TP303 **文献标识码:** A **文章编号:** 0372-2112(2024)05-1432-10
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230864

Research on Autonomous Defense Paradigm for Smart Computing Integration Networks

LIU Ying[1,2], XIA Yu[1], YU Cheng-xiao[2*], ZHANG Wei-ting[1], WANG Run-hu[3], ZHANG Hong-ke[1]
(1. *School of Electronic and Information Engineering*, *Beijing Jiaotong University*, *Beijing* 100044, *China*;
2. *Peng Cheng Laboratory*, *Shenzhen*, *Guangdong* 518055, *China*;
3. *The* 28*TH Research Institute*, *China Electronics Technology Group Corporation*, *Nanjing*, *Jiangsu* 210007, *China*)

Abstract: With the transformation of the computing power supply pattern in the digital economy era, the new network infrastructure with computing power as the core has become an important driving force to realize the sharing of computing power resources and support the digital economy transformation. In the computing power network, multiple heterogeneous user terminals access the network frequently in various ways to obtain computing power services anytime and anywhere, which increases the openness and dynamics of the network. Hence, the computing power network will face more severe security challenges. However, the traditional network-based security defense pattern usually statically supplements security protection components for specific security issues, which cannot actively adapt to user needs to adjust defense strategies flexibly, which is difficult to deal with security risks in computing-network integration scenarios. Therefore, facing the security requirements of the new computing power network, this paper regards security as the internal attribute of the network and proposes a multi-dimensional collaborative autonomous defense paradigm based on the smart computing integration networks, which combines the design of "three layers" and "three domains" of the network. In the "three layers", this paper defines the security inherent service at the generalized service layer, adapts the security function at the mapping adaptation layer, and executes the security strategy at the fusion component layer. In the "three domains", the resource adapta-

收稿日期:2023-09-15;修回日期:2024-04-03;责任编辑:朱梅玉
*通讯作者:于成晓

tion is guided by the entity domain, the security service process is driven by the knowledge domain, and the specific security technologies are implemented by the sense control domain. It constructs a basic management and control process that integrates “detection”, “trace”, and “defense”, in which security policies and technologies can be flexibly adjusted according to scenario scalability and business security. Finally, the proposed paradigm is verified through simulation experiments, and the results prove the effectiveness of the proposed paradigm and also provide a reference for further research and application of smart computing fusion security in the future.

Key words: smart computing integration networks; computing power network; autonomous defense; defense paradigm; network attack

Foundation Item(s): The Major Key Project of PCL; National Key Research and Development Program of China (No.2022ZD0115301); National Natural Science Foundation of China (No.62201029); China Postdoctoral Science Foundation (No.2022M710007, No.BX20220029)

1　引言

随着5G和人工智能等新技术的快速发展,用户对算力的需求大幅提升,算力已成为数字时代中极具战略价值的新型基础设施. 为保证算力互联互通、高效协同,需建立算网深度融合的算力网络,实现算力资源的智能弹性精准调度,满足未来社会泛在的算力需求[1]. 目前国家有关单位联合发布《全国一体化大数据中心协同创新体系算力枢纽实施方案》,以国家层次布局算力网络建设[2]. 此外,国内诸多单位和科研团队已开展相关研究,国内三大运营商和设备厂商已发布多个算力网络相关白皮书,并形成多个国际国家标准,推进算力网络进一步发展完善[3,4]. 算力网络现已成为建设新型基础设施的重要支撑,是未来加速信息技术创新的必然趋势[5].

随着对算网融合研究的不断深入,算力网络的典型特性逐渐凸显,为算力网络引入了新的安全风险. 在算力网络中,算力和网络相互感知、协调、调度,为不同类型用户任务统筹分配网、边、端算力资源,以充分利用算网资源,实现算网服务的随取随用[6]. 在此过程中,大量多源异构用户终端和算力节点可随时随地接入网络,网络的开放性增大. 同时,算力网络承担着大量动态变化的算力任务和算力资源,并通过敏捷调度各类算网资源提供服务,网络中将存在更为频繁的资源调度连接,因此,网络动态性加强,攻击暴露面进一步扩大. 此外,算力网络所蕴含的数据价值更为丰富,导致算力网络遭受攻击的概率大幅提高,算力网络的安全防护将面临更严峻的挑战.

面对算网融合场景下的安全风险,由于现有网络架构在设计之初未将安全功能作为主要考虑因素,其本身存在服务的“资源和位置的绑定”、网络的“控制和数据绑定”以及用户的“身份与位置绑定”“三重绑定”特征,使传统网络架构在数据传输、网络连接方面面临较大威胁[7]. 同时,基于传统网络的安全防御模式通常需要划分明确的网络边界,并面向具体安全问题构建边界安全附加组件来保护网络内部安全[8]. 这种补丁式的网络安全增强手段静态、僵硬,难以根据当前网络状态实时调整防御策略,无法有效应对算力网络中所面临的安全问题[9,10]. 因此,亟待提出一种新型网络架构,深度融合算力网络和安全功能,建立安全可靠的算网融合运行环境,在支持算力高效共享和灵活协作的同时保证算力资源安全.

在此背景下,智算融合网络应运而生,该网络通过“三层+三域”体系架构将网络纵向适配、横向解耦,并以算力服务需求为导向,通过动态感知网络状态,结合知识域中的经验知识智能适配网络族群以及网络组件,从根本上支持服务、网络以及算力间的动态适配调度,实现网络资源的高度优化利用,为用户需求提供定制化服务[11,12]. 本文基于算力网络的主动防御需求,以智算融合网络架构为基础,将安全防御服务作为智算融合网络体系内在属性,提出一种多维协同自主防御范式,以检测-溯源-防御为基础管控流程,根据场景扩展性与业务安全性需求采用适宜的相关技术,为网络提供智能防护能力. 具体来说,在“三层”中,以广义服务层定义安全固有服务,以映射适配层智慧适配安全功能,以融合组件层执行安全策略;在“三域”中,以实体域先导资源适配,以知识域驱动安全服务流程,以感控域实施具体安全技术. 此外,搭建仿真平台进行实验验证,结果表明,本文所提范式能够有效防御网络攻击,更好地服务于算力网络的安全需求,同时也为智算融合网络的安全防御研究提供参考.

2　多维协同自主防御范式总体设计

围绕智算融合网络体系,基于“三层+三域”设计架构,本文提出一种多维协同自主防御范式,其中包含“检测”“溯源”“防御”基础流程,共同构建了完整的攻击防御体系. 整体设计如图1所示. 以下将分别从“三层”和“三域”方面介绍相应设计.

在“三层”层面,本文将多维协同自主防御作为广义服务层的一个固有服务,如图2所示[11]. 服务中包含

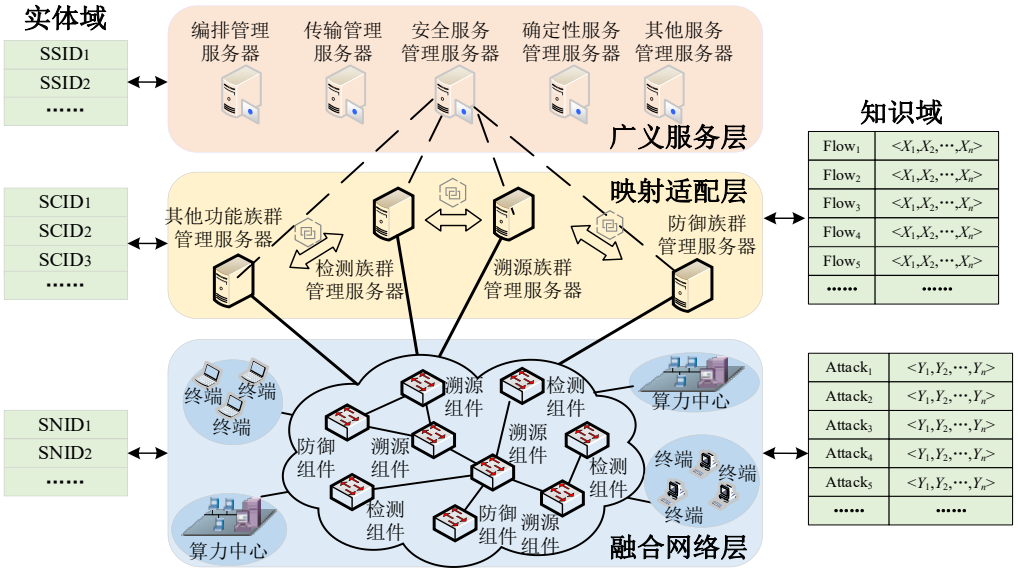


图1 多维协同自主防御范式整体设计

“检测”“溯源”“防御”等不同安全功能，通过广义服务层与映射服务层的上层映射，将各类安全功能在映射适配层以功能特有属性分类来构建相应功能族群，完成安全服务需求与安全功能的转换. 再基于不同安全功能族群，通过映射服务层与融合网络层的下层映射，将不同功能族群的安全策略部署到对应网络组件实体，以安全虚拟功能指导网络实体资源实时运行调度，完成虚拟安全服务到实体组件安全执行的最优适配.

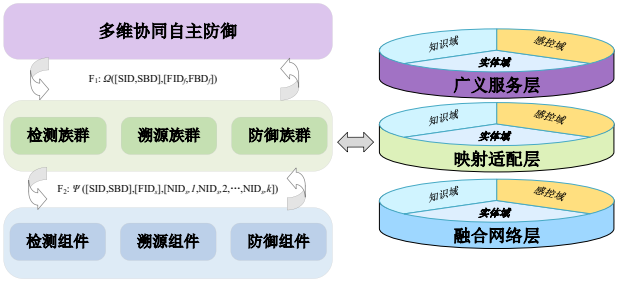


图2 多维协同自主防御范式在“三层”网络结构中对应关系

在“三域”层面，本文将多维协同自主防御范式的控制和运行分离，如图3所示[11]. 实体域统一管理融合网络组件和用户需求，知识域存储网络状态、网络拓扑等信息以驱动各类安全功能执行，感控域实施具体攻击检测、溯源和防御策略. 若感控域感知到网络出现异常信息，首先将异常信息映射至实体域内对应实体，然后以该实体为起点启动攻击溯源，并通过感控域执行溯源策略以快速定位攻击源头. 同时，协同更新知识域中网络状态以及拓扑信息，并构建或更新网络威胁知识库，为防御策略的制定以及二次攻击的及早发现提供数据支撑. 最后，感控域根据不同种类威胁，使能最佳安全防御策略以实现精准化自主防御服务，并同步更新知识域中相关信息，支持后续及时调整安全策略. 由于网络威胁知识库在检测、溯源和防御等环节流转过程中涉及大量信息共享操作，因此为确保网络威胁信息的完整性和可靠性，借助区块链技术在数据存储方面的不可篡改、高安全性的优势，保证知识域网络威胁知识库免受篡改和损坏，从而为智能安全决策提供可信数据基础.

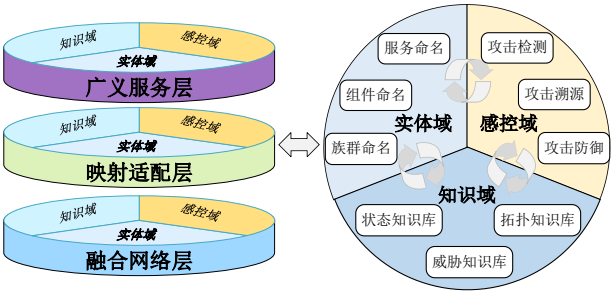


图3 多维协同自主防御范式在“三域”网络结构中对应关系

综上，本文将多维协同自主防御作为智算融合网络的内在安全服务. 一方面，通过“三层”中两层智慧映射，以映射适配层适配用户安全需求和底层融合网络资源，构建“检测”“溯源”“防御”功能族群，以功能隔离形式有效保障用户安全需求. 另一方面，通过“三域”管理、控制和知识的动态解耦，实体域管理和适配网络资源和用户安全需求，感控域感知和执行安全策略，知识域存储和共享网络状态和威胁等信息，三者相互协作实现安全功能的灵活调度和高效管控.

3 多维协同自主防御范式模块设计

3.1 安全服务定义

多维协同自主防御作为智算融合网络的一个内在

服务,需要统一标记服务,以提高服务兼容性和普适性. 因此,在实体域定义安全服务标识SSID(Secure Service ID)对安全服务进行唯一标识. 具体定义如式(1)所示:

$$\mathrm{SSID}=\psi\left(S_{\mathrm{data}}\right) \tag{1}$$

其中,ψ代表服务标识生成函数;S_{data}代表安全服务的关键词或内容,例如:"Security".

由于SSID仅为安全服务提供了一个统一对外标识,但未对安全服务的需求以及特点进行细粒度描述,难以为安全服务适配最佳融合网络组件. 因此,需要进一步多维度描述安全服务,以便融合网络组件资源更好地为安全服务提供适配支撑. 在安全服务描述中,本文从网络拓扑信息、安全服务性能要求以及安全服务可信要求等方面进一步描述安全服务,便于安全服务与网络资源的高效适配和查找. 由此,在感控域引入安全服务行为描述SSBD(Secure Service Behavior Description),具体定义如式(2)所示:

$$\mathrm{SSBD}=\begin{bmatrix}\mathrm{SBD}_{\mathrm{NT}}^{\mathrm{Loc}} & \mathrm{SBD}_{\mathrm{NT}}^{\mathrm{Cache}} & \\ \mathrm{SBD}_{\mathrm{SP}}^{\mathrm{QoS}} & \mathrm{SBD}_{\mathrm{SP}}^{\mathrm{BW}} & \mathrm{SBD}_{\mathrm{SP}}^{\mathrm{Delay}} \\ \mathrm{SBD}_{\mathrm{SF}}^{\mathrm{Cred}} & \mathrm{SBD}_{\mathrm{SF}}^{\mathrm{Ver}} & \mathrm{SBD}_{\mathrm{SF}}^{\mathrm{Sign}}\end{bmatrix} \tag{2}$$

其中,NT(Network Topology)、SP(Security Performance)、SF(Security Function)分别代表服务拓扑属性描述、网络安全性能属性描述以及网络安全功能属性描述. 服务拓扑属性描述包括服务位置以及数据缓存位置,网络安全性能属性描述包括服务质量需求、带宽需求和时延需求,网络安全功能属性描述包括传输信誉、版本号以及签名.

此外,知识库存储服务的唯一标识以及多维属性量化信息,如安全功能、安全等级、服务质量等级等,形成安全服务知识库,有效整合安全服务信息实现智能化管理,以支持上层安全服务需求和下层具体虚拟安全功能的高效适配.

3.2　安全功能映射

映射适配层作为智算融合网络的核心,将用户服务层的安全需求划分为具体安全功能,并映射形成不同安全功能族群. 同时每个族群感知当前所适配的网络组件状态,并根据上层的安全需求制定相应功能策略,下发至所适配的网络组件,协同构建完整的攻击防御体系.

在多维协同自主防御范式中主要提供攻击检测、攻击溯源和攻击防御等三个安全虚拟功能. 针对每一功能聚合完成同一功能的融合网络组件形成功能族群,实现虚拟安全功能与网络组件实体的快速适配和高效调度. 因此,本文在映射适配层设计三大安全族群,分别为攻击检测族群、攻击溯源族群以及攻击防御族群. 为保证族群信息的有效管理和快速查找,需要对不同族群进行统一标识. 因此,在实体域中引入族群标识SCID(Secure Cluster ID),具体定义如式(3)所示:

$$\mathrm{SCID}=\lambda(C_{\mathrm{data}}) \tag{3}$$

其中,λ代表族群标识生成函数;C_{data}代表不同族群所提供虚拟功能的内容或关键词,具体为"Detect""Traceability"和"Defense".

首先,在安全族群感控域中,需要制定相应功能策略,并向所适配的网络组件下发策略,使对应组件执行相应安全功能. 首先,攻击检测族群向网络组件下发监测策略实时获取网络流量状态,建立网络状态知识库,并通过检测策略实时判断当前网络是否存在异常. 若判断网络存在异常,则立刻驱动知识域建立或更新网络威胁知识库. 该知识库以区块链方式与其他族群共享相关信息,并向网络组件下发对应策略以采取溯源和防御动作. 在网络威胁知识库中,主要存储攻击行为信息:攻击类型AT(Attack Type)、攻击源地址ASA(Attack Source Address)、攻击目的地址ADA(Attack Destination Address)、攻击源端口ASP(Attack Source Port)、攻击目的端口ADP(Attack Destination Port)、攻击路径APS(Attack Paths)、传输协议AP(Attack Protocol)等,如式(4)所示. 其中,ASA、ADA、ASP、ADP、APS等信息由攻击溯源族群完善.

$$\mathrm{NAK}=\{\mathrm{AT},\mathrm{ASA},\mathrm{ADA},\mathrm{ASP},\mathrm{ADP},\mathrm{APS},\mathrm{AP}\} \tag{4}$$

其次,攻击溯源族群协同网络状态知识库和网络威胁知识库,通过感知域制定相应溯源策略进行溯源,并将结果同步更新至网络威胁知识库.

最后,攻击检测族群和攻击溯源族群共同构成的网络威胁知识库为攻击防御族群设计策略提供知识依据,支持在不同攻击场景下灵活设计针对性防御策略,实现多样化自适应的网络防御.

三大族群各司其职、相互独立、安全隔离,同时知识域将三大功能族群有机融合,并为不同族群制定策略提供可信知识基础. 三大族群协同构建完整的自主防御体系,实现对网络攻击的高效精准防护.

3.3　安全策略执行

在融合网络层中,融合网络组件实际执行每类族群所下发的安全策略. 首先,每个融合网络组件需在实体域中注册,方便族群感知网络资源,实现网络组件的可管可控. 然后,融合网络组件在感控域中按照所属功能族群实际执行相应安全策略,并将获得的组件状态信息、流量信息存储至对应知识库,为不同攻击场景下防御策略的设计提供依据. 下面将具体介绍融合网络组件的安全策略执行流程.

首先,攻击检测族群所适配的融合网络组件通过感控域执行网络状态实时监测策略,并建立网络状态知识库存储网络流量的幅度变化特征:流的数量

FC(Flow Count)、流的数据包个数FPC(Flow Packet Count)、流的持续时间FD(Flow Duration)、流的类型FT(Flow Type),如式(5)所示.同时,检测组件部署族群下发的攻击检测策略,依据当前网络状态信息进行异常判断.若任一组件发现异常,则将该结果上报给攻击检测族群,同时更新网络威胁知识库.

$$\mathrm{NTK}=\{\mathrm{FC},\mathrm{FPC},\mathrm{FD},\mathrm{FT}\} \tag{5}$$

然后,网络威胁知识库驱动攻击溯源族群和攻击防御族群设计相应策略,并将溯源和防御策略下发至所适配的网络组件.溯源组件将按照知识库中的威胁信息及溯源策略,追溯攻击源头,并将源头信息和攻击路径信息存储至网络威胁知识库,进一步完善攻击描述信息.同时,防御族群根据知识库中的攻击信息制定防御策略,并立刻向防御组件下发指令,快速抵御网络攻击.

通过三类组件的智慧协同和快速调配,构建实时检测、有效溯源、快速防御的一体化智能防御体系,有效增强网络主动抵御攻击的能力.同时,整合网络安全信息,建立可信共享的网络威胁知识库,为未来攻击检测研究与防御决策优化提供先备知识.

4 仿真验证与分析

多维协同自主防御范式的主要目标是在网络中快速检测攻击,通过自动追溯,准确找到攻击路径和源头,并根据攻击类型选取最佳防御策略.本节以泛洪攻击为例,实例化多维协同自主防御范式进行仿真实验,并对仿真结果进行总结.

4.1 安全策略执行

在多维协同自主防御范式中设计适宜的检测、溯源以及防御策略,以提供泛洪攻击的高效防御.首先,攻击检测族群采用灵活可扩展的攻击检测算法,快速探测注入到网络中的异常流量,为攻击溯源和防御提供合理的触发时机.然后,基于攻击检测结果,一方面攻击溯源族群启用概率性包标记机制实现对攻击路径和源头的追溯,同时借助区块链将网络威胁信息共享至其他族群,实现攻击信息安全协同共享;另一方面攻击防御族群部署基于流量管控的防御策略,各个防御组件结合网络威胁知识库和网络状态知识库协同缓解泛洪攻击流量,保障合法业务的正常运行.具体设计如图4所示.

具体来说,攻击检测采用基于信息熵的轻量级检测策略.通过在攻击检测组件中部署草图结构,实时统计网络流量特征数值情况,并计算时间窗口内网络流量特征的信息熵值.同时,基于滑动窗口计算发生攻击前所有正常状态时间窗口内的平均熵值.若当前时间窗口内任一特征熵值超出平均熵值,表明网络中存在异常流量,则立即触发溯源族群和防御族群,并更新网络威胁知识库.

攻击溯源采用基于源地址分片标记的高效溯源策略.通过网络溯源组件概率性地在异常流量数据包头中嵌入源地址信息,溯源族群汇总一定数量的标记数据包后进行路径重构.在嵌入源地址信息时,选择数据包头中较少使用的分片相关字段Identification(16 bit)、More Flag(1 bit)和Fragment Offset(13 bit)存储源地址信息.但由于3个字段无法直接存储完整源地址,因此将其划分为4个分片标记字段间接存储源地址,具体划分为源地址分片(Fragment)存储源地址分片后每片长度、分片偏移(Offset)存储分片插入位置、转发跳数(HopCount)存储数据包转发路径长度(最长为32跳)以及源地址哈希值(HashAdd)存储源地址摘要信息,用于验证溯源源地址的完整性和正确性.在重构路径时,首先将HopCount和HashAdd相同的数据报文分组,然后从HopCount=1的分片开始重组,将相同HashAdd的分片通过Offset重新拼接.当重组得到完整源地址时,再进行一次地址哈希计算,与分片中HashAdd进行比较,以验证重构信息是否正确.重复上述过程直至HopCount的所有分组计算完毕,最终构成完整的攻击路径.

攻击防御采用基于深度强化学习的智能流量缓解策略.通过在攻击防御族群中部署Deep Q-learning智能体,从网络状态知识库获取网络流量信息,处理形成状态空间输入到智能体中.智能体根据状态空间产生相应动作,以此决定网络组件端口分配到的带宽,并向防御组件下发指令,丢弃超过限制带宽的数据包,及时缓解网络泛洪流量.此外,综合考虑提高正常流量的经过比例和降低恶意流量的经过比例设计奖励函数,使动作根据网络状态自适应调整,以保证在缓解攻击流量的同时减少对正常流量的影响.

4.2 仿真环境设置

本文使用搭载Ubuntu16.04系统的虚拟机搭建Mininet仿真环境,族群功能由Python实现,网络组件由支持P4编程的软件交换机BMv2组成,族群与网络组件通信使用Thrift端口,并通过Scapy构造和发送数据包.此外,知识域使用InfluxDB数据库存储相关数据,并使用Remix和Ganache开发和维护区块链实现网络威胁信息共享.具体设置如表1所示,实验拓扑如图5所示,各主机IP地址及MAC地址由Mininet自动生成.其中,H_2和H_{11}为攻击主机,向受害主机H_5发起UDP泛洪攻击,其他用户向网络注入正常数据包.攻击流量和正常流量通过Scapy工具构造.其中,攻击数据包中使用随机函数随机生成虚假的源IP地址,目的地址指向H_5;正常数据包使用真实IP地址,目的地址指向任意主机.

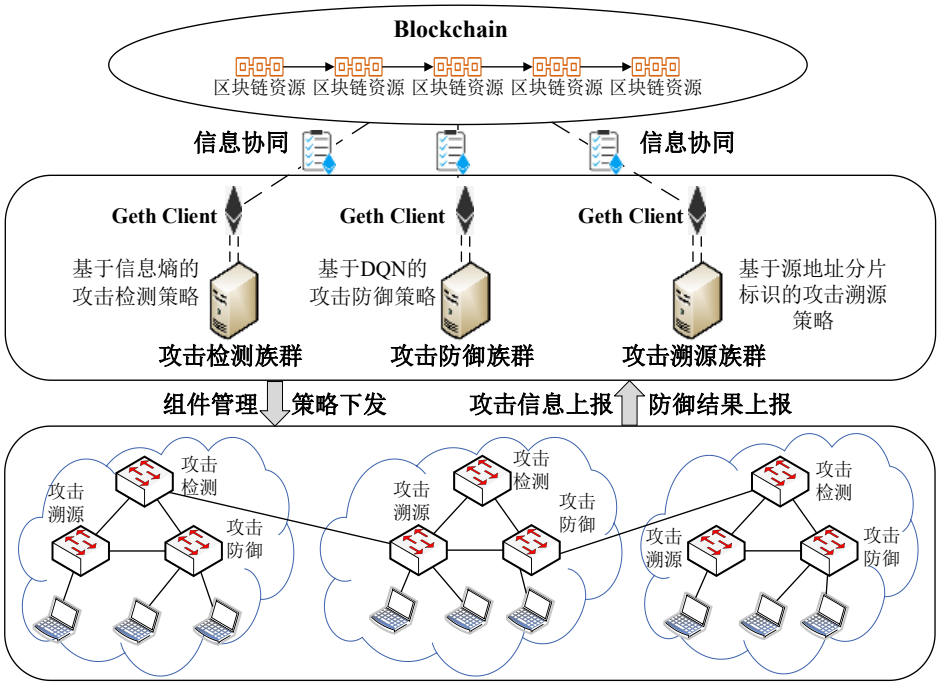


图4　实例设计示意图

表1　仿真环境设置

仿真工具	用途
Ubuntu 16.04	搭建仿真平台
Mininet	搭建仿真网络拓扑
BMV2	可编程交换机作为融合网络组件
Scapy	构造网络流量
InfluxDB	存储时序数据
Remix	开发智能合约
Ganache	维护区块链节点

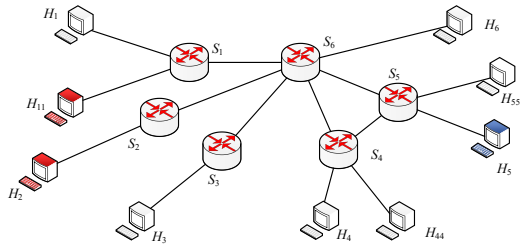


图5　实验拓扑图

4.3　仿真结果和分析

4.3.1　攻击检测性能

（1）　信息熵检测方案的参数确定

在攻击检测策略中，本文拟在检测网络组件中部署草图结构进行数据包特征统计，但由于草图大小占用网络组件有限的存储空间，因此需要合理设计草图大小，保证统计正确率的同时减少内存占用开销．本文构造随机IP地址、源端口数据包，向网络中发送10 000个数据包，设定统计草图的不同深度和计数表空间大小进行对比，以统计准确率作为评估标准．经过10轮重复测试取均值，结果如图6所示．

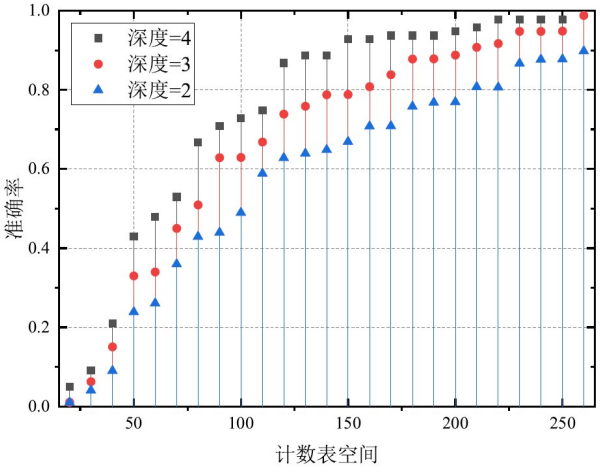


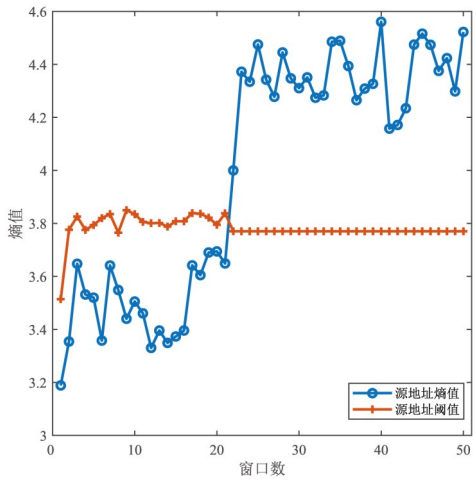
图6　在不同大小草图下的统计特征准确率比较

由图6可知，草图在相同计数表空间情况下，深度越高，统计准确率越高．在相同深度情况下，计数表空间越大，统计准确率越高．在准确率95%以上的情况下，深度为3和深度为4的草图统计准确率十分接近．由于网络组件需通过寄存器方式存储，寄存器寻址方式需选用32位的整数倍．因此，为兼顾统计正确率和内存开销，本文设定草图大小256×3.

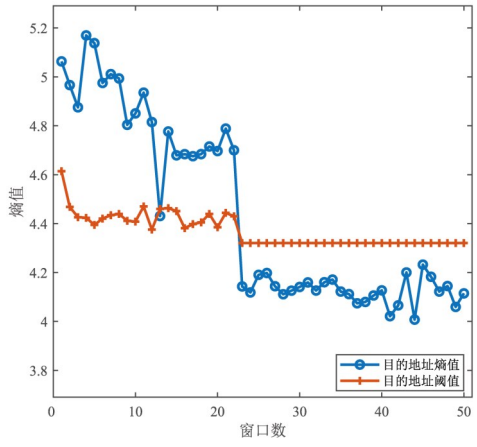
（2）　攻击检测有效性

在攻击检测中采用基于信息熵的检测策略．本文设定时间窗口为256个数据包，并在50个连续时间窗

口内观察交换机S_6上源地址和目的地址的熵值和阈值变化情况. 在0至20的时间窗口内,所有主机向目标主机发送正常流量,在第21个时间窗口,攻击者H_{11}和H_2发起攻击流量,结果如图7所示. 图7显示,在前20个时间窗口内,源地址和目的地址的熵值均在阈值范围内,表明网络中不存在异常流量,并且阈值动态变化;从第21个时间窗口开始,源地址和目的地址的熵值变化明显,表明交换机有效检测到泛洪攻击.



(*a*) 源地址的熵值和阈值变化



(*b*) 目的地址的熵值与阈值变化

图7 攻击检测测试结果

4.3.2 攻击溯源性能

(1)源地址分片标记溯源方案的参数选取

为模拟真实的网络环境并增强源地址分片算法的鲁棒性,本文使用CAIDA发布的The IPv4 Routed/24 Topology数据集2022年1月期间的数据进行溯源参数选取测试[13]. 数据集包含了从源节点157.92.44.100发出的到不同目的地址的数据流信息,其中包含了数据流途径的每一跳IP地址和TTL(Time To Live). 本文倒转这些路径形成不同主机节点对同一节点的访问以模拟分布式入侵攻击.

在源地址分片方案中,本文设计3种分片方式,即源地址分片大小分别为4 bit、8 bit、16 bit,并给出相应分片数量、偏移、转发跳数及源地址哈希的所占位数. 具体设置如表2所示. 通过统计3种分片方案溯源过程中所需要的数据包确定源地址分片方案,结果如图8所示.

表2 分片标记方案

源地址分片/bit	分片数量	分片偏移/bit	转发跳数/bit	源地址哈希值/bit
4	8	3	5	18
8	4	2	5	15
16	2	1	5	8

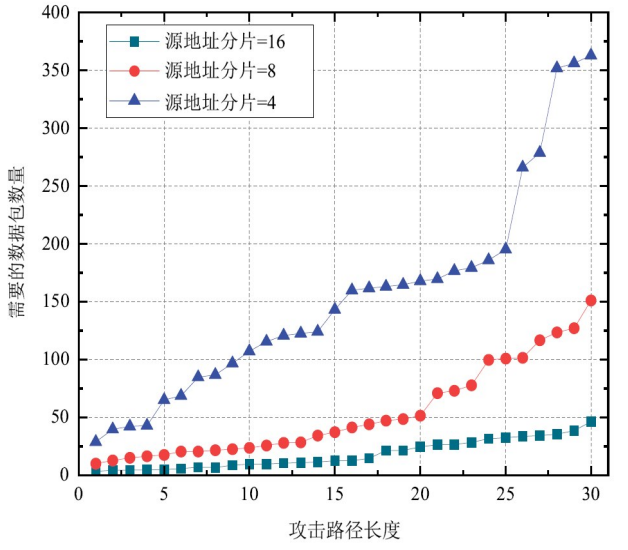


图8 不同分片方案在溯源过程中所需要的数据包个数

由图8所示,源地址分片的位数越多,溯源过程中所需的数据包越少. 而在分片时需要计算哈希值来验证重构源地址的正确性,位数过少会产生大量碰撞问题. 因此,为兼顾验证准确性及溯源效率,本文选取源地址分片大小为8 bit的方案.

另外,在此数据集中设计分别以5%和10%的概率标记数据包,并将其与基于概率标记的溯源方法PPM(Probabilistic Packet Marking)进行对比,统计在不同攻击路径跳数的情况下两种方法在路径重构时所使用的数据包个数. 结果如图9所示.

如图9所示,标记概率越大,路径重构所使用的数据包数量越小. 在标记概率相同时,本文方法在路径重构中所使用的数据包个数远小于PPM,所需数据包数量减少30%~50%. 其中,在标记概率为5%时,本文方法在路径重构中所使用的数据包个数与标记概率为10%的PPM的效果接近,表明本文方法不仅有效溯源攻击路径,同时效率更高.

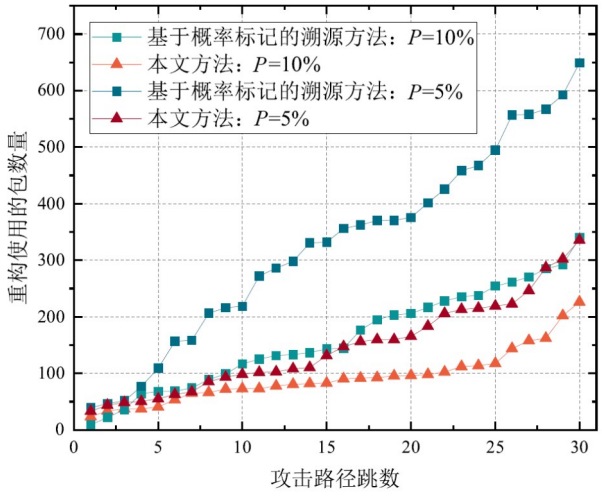


图9　两种方案在不同标记概率下路径重构所使用的数据包个数

(2)攻击溯源有效性

本文在攻击溯源中采用基于源地址分片的溯源策略. 基于上节的参数选择,设定溯源算法中的源地址分片大小为8 bit. 本文设定 H_{11} 和 H_2 向 H_5 发起UDP泛洪攻击,观察受害主机中所接收的分片数据包以及溯源情况,如图10所示.

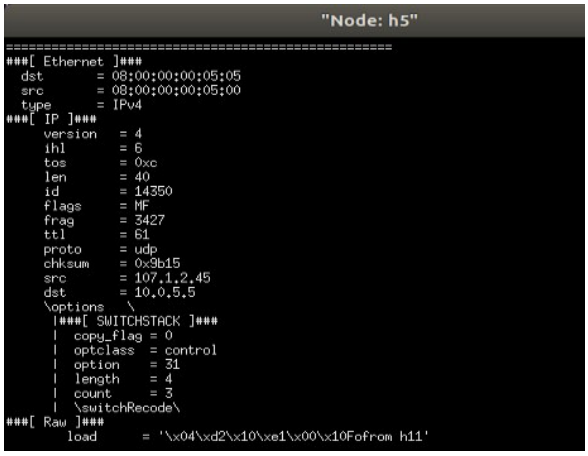
如图10(*a*)所示,受害主机 H_5 所接收的数据包中的tos字段为0xc,表明该数据包为源地址分片后的数据包,且标识字段Identification(Id)、标志位More Flag(Flags)和分片字段Fragment Offset(Frag)已被修改. 因此,H_5 通过收集大量这类分片数据包则可以进行攻击路径重构,路径重构结果如图10(*b*)所示,受害主机 H_5 可有效重构数据包在网络中的转发路径,以此找到攻击主机.

4.3.3　攻击防御性能

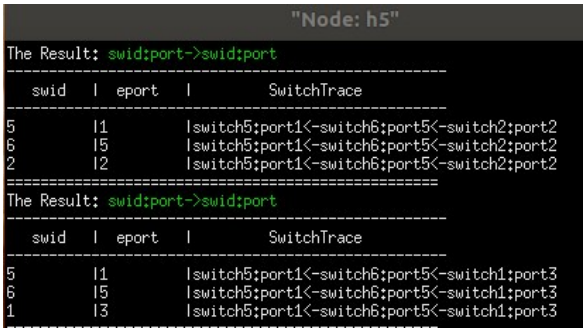
(1)攻击防御有效性

攻击防御采用基于深度强化学习算法Deep Q-Network的防御策略. 算法具体参数如表3所示. 本文设计一共经过100轮测试,每轮持续100 s. 在0~20轮中,所有主机向目标主机发送正常请求,当在第21轮时,攻击主机向目标主机发起攻击. 与此同时,深度强化学习模型中智能体根据学习到的经验调整网络组件端口分配到的带宽比例. 以通过正常流量的通过比例(pa)和恶意流量的通过比例(pb)作为评价标准. 结果如图11和图12所示.

由图11和图12可看出,在20轮之后,到达目标主机的攻击流量比例稳定在20%,到达目标主机的合法流量的比例保持在80%左右,表明基于Deep Q-Network的防御策略对泛洪攻击流量起到了明显的缓解效果,可尽可能压缩恶意流量通过率,同时减少对合法流量的影响,保证了网络带宽资源不被恶意流量占用.



(*a*) 受害主机收到的分片数据包信息



(*b*) 受害主机的重构溯源结果

图10　攻击溯源测试结果

表3　DQN算法参数设置

参数名称	参数设置
经验池	200
Batch_Size	8
学习率	0.000 5
经验数据大小	20
折扣因子	0.99
优化器	Adam

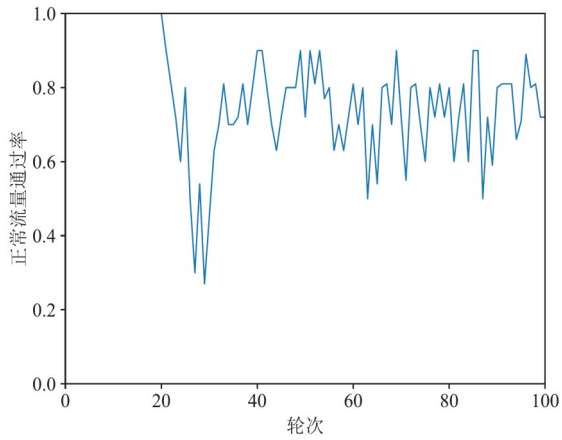


图11　正常流量到达比例

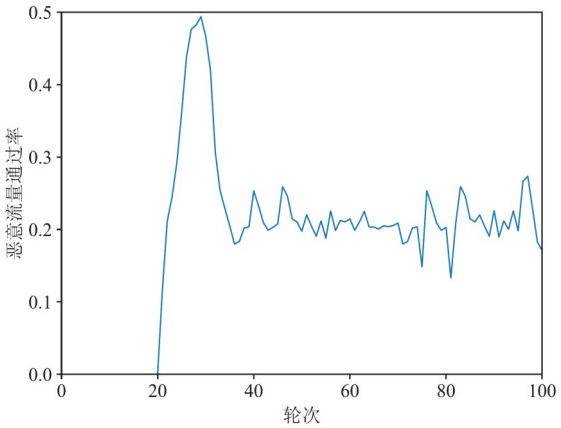
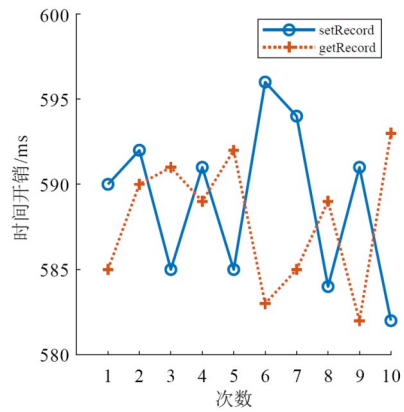


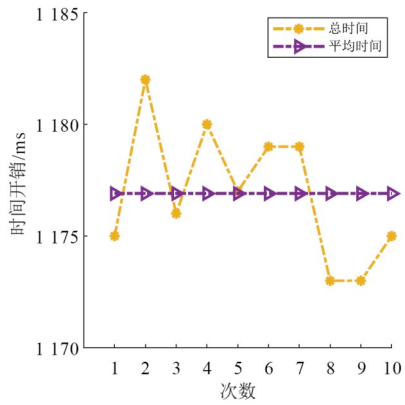
图 12 异常流量到达比例

(2)网络威胁知识库共享开销测试

网络威胁知识库通过区块链在攻击检测族群、攻击溯源族群和攻击防御族群中共享,为快速发现攻击和制定防御策略提供可信数据基础. 因此,区块链的开销主要取决于3个族群中部署的区块链节点完成存储交易和节点完成读取交易的时间. 本文使用以太坊Geth客户端搭建私有区块链,其中包括攻击检测族群、攻击溯源族群和攻击防御族群等3个族群内的对等区块账户节点. 区块链上所部署的智能合约用来在区块链节点间进行交互,并负责添加和获取攻击源地址和目的地址、攻击类型、攻击路径以及时间戳等相关信息. 本文选取区块链节点达成共识完成交易的场景,获取存储和读取交易数据两类主要时间作为系统引入区块链的开销,共测试10次,结果如图13所示.



(a) 10次测试存储和读取交易的时间



(b) 10次测试中完成交易时间与平均时间

图 13 网络威胁知识库共享开销测试结果

由图13测试结果表明,在10次测试中,族群节点存储和读取交易数据的时间大致在580~600 ms内,而一次交易完成时间最多不超过1 200 ms,其平均完成一次交易时间大约为1 176 ms. 虽然在族群中引入区块链共享网络威胁信息会引入少量的时间开销,但由于区块链存在反篡改、分布式的优势,不仅保证了网络威胁信息库的完整性以及正确性,提高了数据共享的安全性,并且可为跨域攻击以及重复攻击的快速发现和防御提供支撑.

5 结论

本文面向算力网络的安全需求,将安全因子作为算力网络架构的内在属性,基于智算融合网络新型架构提出一种多维协同自主防御范式,深度融合网络架构“三层”“三域”的设计,构建攻击检测-溯源-防御一体化基础管控流程,其中具体技术可根据场景扩展性与业务安全性需求进行灵活调整. 同时,本文以泛洪攻击为例,实例化攻击检测、溯源和防御技术,并进行仿真实验验证. 该范式为算网融合场景下的新型网络安全设计提供一种新的思路,未来将对算网融合场景下特有的安全问题进行研究,对所提方案进一步优化.

参考文献

[1] 李少鹤, 李泰新, 周旭. 算力网络:以网络为中心的融合资源供给[J]. 中兴通讯技术, 2021, 27(3): 29-34.
LI S H, LI T X, ZHOU X. Computing power network: A network-centric supply paradigm for integrated resources[J]. ZTE Technology Journal, 2021, 27(3): 29-34. (in Chinese)

[2] 邱勤, 徐天妮, 张智杰, 等. 算力网络安全应用需求与关键技术研究[J]. 信息技术与标准化, 2022(11): 19-24, 33.
QIU Q, XU T N, ZHANG Z J, et al. Research on security application requirements and key technologies of computing force network[J]. Information Technology & Standardization, 2022(11): 19-24, 33. (in Chinese)

[3] 曹畅, 唐雄燕. 算力网络关键技术及发展挑战分析[J]. 信息通信技术与政策, 2021, 47(3): 6-11.
CAO C, TANG X Y. Analysis of key technologies and de-

velopment challenges of computing power network[J]. Information and Communications Technology and Policy, 2021, 47(3): 6-11. (in Chinese)

[4] 贾庆民, 丁瑞, 刘辉, 等. 算力网络研究进展综述[J]. 网络与信息安全学报, 2021, 7(5): 1-12.
JIA Q M, DING R, LIU H, et al. Survey on research progress for compute first networking[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 1-12. (in Chinese)

[5] 段晓东, 姚惠娟, 付月霞, 等. 面向算网一体化演进的算力网络技术[J]. 电信科学, 2021, 37(10): 76-85.
DUAN X D, YAO H J, FU Y X, et al. Computing force network technologies for computing and network integration evolution[J]. Telecommunications Science, 2021, 37 (10): 76-85. (in Chinese)

[6] TANG X Y, CAO C, WANG Y X, et al. Computing power network: The architecture of convergence of computing and networking towards 6G requirement[J]. China Communications, 2021, 18(2): 175-185.

[7] 张宏科, 罗洪斌. 智慧协同网络体系基础研究[J]. 电子学报, 2013, 41(7): 1249-1252, 1254.
ZHANG H K, LUO H B. Fundamental research on theories of smart and cooperative networks[J]. Acta Electronica Sinica, 2013, 41(7): 1249-1252, 1254. (in Chinese)

[8] AHMAD I, NAMAL S, YLIANTTILA M, et al. Security in software defined networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2317-2346.

[9] ZHOU Y Y, CHENG G, YU S. An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 5366-5380.

[10] SAHAY R, MENG W Z, JENSEN C D. The application of Software Defined Networking on securing computer networks: A survey[J]. Journal of Network and Computer Applications, 2019, 131(C): 89-108.

[11] 张宏科, 于成晓, 权伟, 等. 融算网络体系基础研究[J]. 电子学报, 2022, 50(12): 2928-2934.
ZHANG H K, YU C X, QUAN W, et al. Fundamental research on computing integration networking[J]. Acta Electronica Sinica, 2022, 50(12): 2928-2934. (in Chinese)

[12] 张宏科, 权伟, 刘康. 算力网络研究与探索[J]. 中兴通讯技术, 2023, 29(1): 1-5.
ZHANG H K, QUAN W, LIU K. Research and exploration of computing power network[J]. ZTE Technology Journal, 2023, 29(1): 1-5. (in Chinese)

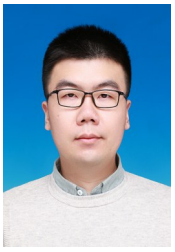
[13] The Center for Applied Internet Data Analysis. The CAIDA UCSD IPv4 Routed /24 topology dataset[EB/OL]. (2022)[2024]. https://www.caida.org/catalog/datasets/ipv4_routed_24_topology_dataset/.

作者简介

刘　颖　女,1978年8月生,山东寿光人. 北京交通大学电子信息工程学院教授、博士生导师. 主要研究方向为未来互联网体系架构、网络安全与确定性网络等.
E-mail: yliu@bjtu.edu.cn

夏　雨　女,1996年3月生,陕西咸阳人. 北京交通大学电子信息工程学院博士研究生. 主要研究方向为未来互联网体系架构、网络安全、算力网络等.
E-mail: xiaooyu@bjtu.edu.cn

于成晓　男,1993年生,辽宁大连人. 鹏城实验室助理研究员. 主要研究方向为新型网络传输协议理论与关键技术.
E-mail: yuchx@pcl.ac.cn



张维庭　男,1992年生,内蒙古巴彦淖尔人. 北京交通大学电子信息工程学院副教授、硕士生导师. 主要研究方向为工业互联网、算力网络和网络智能. 中国电子学会会员编号:E190029828M.
Email: wtzhang@bjtu.edu.cn

汪润虎　男,1999年生,江西吉安人. 中国电子科技集团有限公司第二十八研究所助理研究员. 主要研究方向为网络安全.
Email: 20120121@bjtu.edu.cn

张宏科　男,1957年9月生,山西大同人. 中国工程院院士,北京交通大学电子信息工程学院教授、博士生导师,移动专用网络国家工程研究中心主任. 主要研究方向为新一代信息网络理论与关键技术. 中国电子学会会员编号:E1900046895.
E-mail: hkzhang@bjtu.edu.cn