面向枢纽通航关基设施业务场景的安全防护技术研究综述

李宏宇[1]，李思帆[1]，王浩翔[1]，王昊天[1]，曹越[1]，陈龙[2]，张宇[3]
（1. 武汉大学国家网络安全学院，湖北 武汉 430072；2. 北京化工大学信息科学与技术学院，北京 100029；
3. 奇安信科技集团股份有限公司，湖北 武汉 430000）

摘 要：随着我国航运网络的智能化转型，以长江干线为代表的大型枢纽通航设施在数字化赋能下变得高度复杂化和异构化，其网络面临严峻的网络安全威胁，对航运乃至国家战略安全构成了挑战。为了应对这一挑战，基于大型枢纽通航关基设施网络不同安全域的安全需求，提出了一个面向跨域协同范式的安全防护框架，旨在整合不同安全域的防护技术与策略，实现紧密协同和高效响应。深入探讨了大型枢纽通航关基设施跨域联动安全防护技术的研究背景、体系架构、关键技术以及未来的研究重点，为提升大型枢纽通航关基设施的安全能力提供了可行的参考。

关键词：枢纽通航关基设施；跨域联动防护；物联网安全；工控网络
中图分类号：TP393.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.2026.00554

Review of research on security protection technologies for business scenarios in navigation hub infrastructure

Li Hongyu[1], Li Sifan[1], Wang Haoxiang[1], Wang Haotian[1], Cao Yue[1], Chen Long[2], Zhang Yu[3]
1. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
2. College of Information Science and Technology, Beijing University of Chemical Technology, Beijing 100029, China
3. Qi An Xin Technology Group Inc., Wuhan 430000, China

Abstract: With the intelligent transformation of China's shipping network, large navigation hub infrastructures, represented by the Yangtze River trunk line, have become highly complex and heterogeneous under the empowerment of digitalization. These networks face severe cybersecurity threats, posing a challenge to shipping and even national strategic security. To address this challenge, a security protection framework for cross-domain collaboration paradigm was proposed in this paper. The framework aimed to integrate protection technologies and strategies from different security domains to achieve tight collaboration and efficient response. The research background, architectural framework, key technologies, and future research priorities of cross-domain collaborative security protection technology for large navigation hub critical infrastructure were delved, providing feasible references for enhancing its security capabilities.

Key words: navigation hub infrastructure, cross-domain collaborative protection, Internet of things security, industrial control network

收稿日期：2026−01−28；**修回日期：**2026−02−04
通信作者：曹越，yue.cao@whu.edu.cn
基金项目：国家重点研发计划（No. 2024YFB3108400）；湖北省国际科技合作项目（No. 2024EHA048）；武汉市人工智能专项项目（No. 2023010402040020）
Foundation Items: The National Key Research and Development Program of China (No. 2024YFB3108400), the Hubei Province International Science and Technology Cooperation Program (No. 2024EHA048), the Wuhan Artificial Intelligence Special Project (No. 2023010402040020)

0　引言

枢纽通航关基设施是指在大型通航枢纽建设中，为水上交通运输、航道管理等业务职能提供关键技术支持的系统，通常包含船闸、升船机、航道水利、智能管理平台等设施。在我国的综合运输体系中，以长江干线为代表的航运网络已经成为新质生产力的发展重点，而通航枢纽作为航运网络的“咽喉”，更是成为事关航运安全、乃至国家战略安全的关键节点。2023年，《公路水路关键信息基础设施安全保护管理办法》正式施行，对通航枢纽的信息安全管理提出了明确要求，确立了运营者主体责任，鼓励充分发挥社会各方面作用，共同保护关键信息基础设施安全[1]。结合行业实际需求，近期制定的专业标准进一步细化了枢纽通航场景中的网络安全防护与运维技术规范[2-3]。

随着近年枢纽通航行业的智能化转型，枢纽通航关基设施处于高度复杂化与深度数字化进程，通过对物联网、大数据等技术的应用，实现了水运通航资源的协同调控，提升了枢纽通航管理与服务效率。具体而言，大型通航枢纽围绕提升效率、安全、环保3大核心目标，着力于船舶通航、枢纽设施、环境监测3个维度，通过广泛应用智能技术来全面提升通航的安全性和可持续性；同时，大型通航枢纽通过综合运营管理平台等渠道向运营人员和公众提供信息化服务。智能互联大型通航枢纽的应用场景如图1所示。

然而，鉴于关基设施规模急剧扩张、网络架构变得越加复杂，枢纽通航关基设施的网络安全逐渐成为一大挑战，对航运安全乃至国家战略安全产生了重要威胁。在数字化赋能的通航枢纽中，枢纽通航关基设施网络（NHI-Net, navigation hub infrastructure network）连接了通航工控设备、航运调度系统及其他网络基础设施，这些设施跨越不同工业领域，且在网络、应用、数据的技术上高度异构，因此，对NHI-Net的防护需要建立跨域协同的安全防护框架，基于模块化的理念整合各个安全域的不同防护技术与策略，从而实现不同安全域间的紧密协同和高效响应。

本文旨在基于NHI-Net不同安全域的安全需求，从跨域联动的角度总结枢纽通航关基设施的安全防护技术体系，并深入探讨研究背景、体系架构、关键技术、典型案例，以及未来的研究重点，为枢纽通航关基设施的安全能力升级提出可行的参考与见解。现有综述对比见表1，直观地展示了本文的研究定位与贡献，将本文与近年来国内外相关领域的综述文献进行了多维度对比。本文首次对船闸调度、水位调控等强物理耦合业务场景进行深入分析，并从跨域协同的视角探讨整体安全防护体系。

1　研究背景

现代NHI-Net应用数字孪生、区块链、人工智能（AI, artificial intelligence）等技术，通过全方位

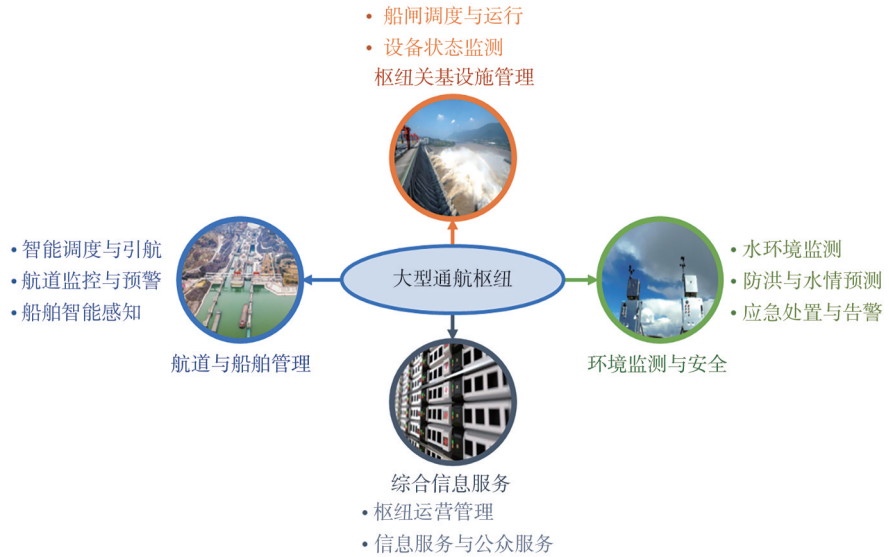


图1　智能互联大型通航枢纽的应用场景

表 1　现有综述对比

文献	年份	物联网	工控系统	枢纽通航场景	网络安全	跨域联动防护
[4]	2022	√	√		√	
[5]	2023	√			√	
[6]	2024		√	√		
[7]	2024	√	√	√		
本文	2026	√	√	√	√	√

感知、泛在互联、云边协同、智能服务与安全保障，实现水运枢纽通航场景中对泛在感知与智能调控的全面覆盖。然而，NHI-Net在大规模部署与数据驱动决策逐步渗透的同时，也暴露出一系列安全挑战与风险隐患。本节通过详细介绍研究背景，分析NHI-Net的体系结构与安全挑战，并介绍本文面向枢纽通航关基设施业务场景提出的跨域联动安全防护体系。

1.1　枢纽通航关基设施网络

1.1.1　体系结构

NHI-Net契合工业控制系统（ICS, industrial control system）网络架构，由运营技术（OT, operational technology）网络与信息技术（IT, information technology）网络组成，通常连接枢纽通航关基设施的传感与执行设备、控制网络，以及相关信息基础设施，强调跨系统的数据流通与功能协同，实现从物理世界到数字空间的映射、分析与反向控制。该网络可解构为设备层、控制层、监管层、IT层，其中，设备层、控制层、监管层共同组成了NHI-Net的OT网络。枢纽通航关基设施网络及威胁架构如图2所示。

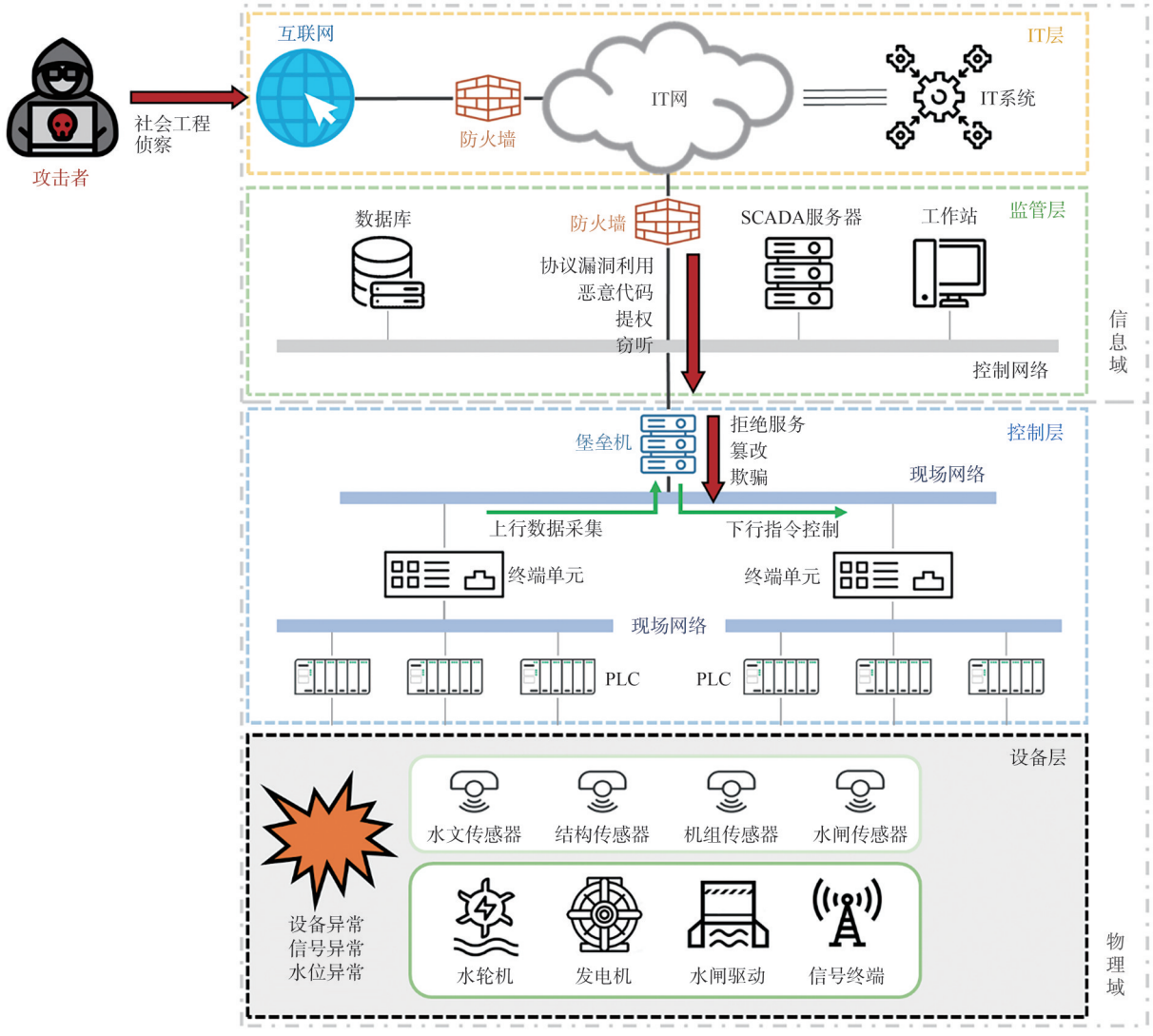


图2　枢纽通航关基设施网络及威胁架构

设备层是网络系统的最底层，包含执行物理操作的设备（如水轮机、发电机）和采集数据的传感器[8]。设备层作为全域状态感知和船舶调度的末梢，承担了航道感知、船舶感知、设施执行的功能。其中，水位计、流速传感器等组成的水文监测子系统实时采集航道与闸室的水位动态，为航道水位动态调控提供数据底座；信号终端（如船舶自动识别系统基站、无线射频识别）用于在船舶通航过程中支持船舶定位与识别；最后，驱动船闸启闭机、升船机承船厢等物理执行机构通过现场总线（如Modbus、PROFIBUS等）互联，执行上层下发的物理动作指令[9]。

控制层负责接收监管层指令并对设备层进行自动化控制，不仅执行单一设备的自动化逻辑，更承担着跨设施协同操作的核心职能。控制层包含多个控制单元，主要由主从可编程逻辑控制器（PLC, programmable logic controller）群组构成。控制单元通过现场总线网络连接到物理设备，并建立严密的逻辑互锁。根据预设的船舶调度逻辑，这些控制单元将上层的调度指令转化为针对阀门、电机等执行机构的时序控制信号，确保过闸流程（进闸、系缆、充泄水、出闸）的自动化运行。由于技术模式、通信目标、通信方式、传输要求的差异，控制层使用的协议是高度异构的，可能包含现场总线协议、工业以太网协议等。

监管层是OT网络的“指挥中心”，通过人机界面（HMI, human-machine interface）实现对基础设施的监控与管理。其核心是数据采集与监控（SCADA, supervisory control and data acquisition）系统，展示船舶排队态势图、闸室水位曲线及设备运行参数，从而提供宏观视图、实时监控和指令操作。当自动调度出现异常时，该层提供人工接管接口，允许操作员直接下发水位紧急调控或设备急停指令，保障通航安全底线。监管层的通信安全和数据安全是NHI-Net安全性的关键，通常通过网络隔离或防火墙进行安全控制[10]。

IT层作为NHI-Net的最顶层，负责宏观的业务管理、决策支持、数据分析和信息交互。该层将通过复杂调度算法生成的调度计划转化为数字指令，穿透IT/OT边界网关下发至监管层与控制层，驱动物理域的业务流转。由于涉及外网申报数据与内网控制指令的交互，该层也是网络安全风险渗透的主要入口[3]。

随着工业物联网（IIoT, industrial Internet of things）范式的发展，NHI-Net的架构发生了巨大变革[11]。例如，边缘计算提高了设备层的处理能力；LPWAN协议[12]和云计算[13]允许设备直接上传数据到云端；标准化工业协议（如，OPC UA[14]、MQTT[15]等）促进了数据扁平化传输，并形成统一的数字孪生模型[16]。上述技术增强了网络的复杂性和跨域性，也对NHI-Net的安全防护提出了新要求。

1.1.2　安全挑战

NHI-Net具有高度复杂的网络攻击面，使其面临着严峻的安全挑战。同时，传统的单一安全防护措施已难以应对跨域威胁。图2展示了常见的攻击者从渗透NHI-Net到漏洞利用的总体威胁架构。

1) 复杂跨域传播网络漏洞与威胁隐蔽性高

在新兴的高级持续威胁（APT, advanced persistent threat）场景中，NHI-Net安全风险具有隐蔽性、持久性、传播性，攻击者通常通过广泛的情报侦察手段以确立易被攻陷的攻击目标子系统与隐蔽的攻击方式，并在入侵成功之后的长周期内逐渐实现各个子系统的提权、数据收集与漏洞利用。ICS的典型APT攻击案例见表2，列举了针对ICS的典型APT攻击案例。以2015年乌克兰电力系统遭受BlackEnergy攻击事件为例，APT组织利用钓鱼邮件吸引电力公司员工在内网终端植入并传播BlackEnergy恶意程序，以获取凭证数据并渗透至内网。在充分侦察后，攻击者设法获取SCADA系统的控制权限，并造成当地大规模停电[18]。

对于枢纽通航关基设施场景，这种跨域攻击具有特殊的物理破坏性。由于NHI-Net的不同子系统采用不同的协议与技术标准，攻击者可利用IT层申报接口的漏洞获取权限，进一步横向移动渗透至OT工控系统。在枢纽通航的特有场景中，攻击者可能对底层水位传感器或流量计实施中间人欺骗，篡改关键的水文监测数据。例如，通过虚构“闸室内外水位已平”的信号，诱导PLC控制逻辑在存在巨大水头差（非等水位）的危险状态下错误开启闸门。这种“信息—物理”攻击将直接导致船只倾覆、闸门机械结构不可逆损毁等灾难性后果，造成航运业务瘫痪，从而对国家战略安全构成重大威胁。

表2　　ICS的典型APT攻击案例

攻击事件	年份	攻击类型	攻击目标	威胁传播范围
Stuxnet[17]	2010	间谍行动、篡改攻击	核设施PLC	监管、控制、设备层
BlackEnergy[18]	2015	网络钓鱼、篡改攻击、DDoS	电网设施SCADA HMI	IT、监管、控制层
Industryer[19]	2016	篡改攻击、DDoS	电网设施SCADA系统	监管、控制层
Triton[20]	2017	篡改攻击、欺骗攻击	石化设施SCADA仪表	监管、控制、设备层
GreyEnergy[21]	2018	网络钓鱼、窃听攻击	工控SCADA HMI	IT、监管层
Incontroller[22]	2022	篡改攻击、欺骗攻击	工控PLC	IT、监管、控制、设备层

2) 安全检测与防护机制相互孤立

在NHI-Net等类别的ICS网络的传统安全策略中，不同的安全设备和系统通常独立运行，针对特定威胁或特定系统执行单点防护，当攻击发生时，不同安全设备之间无法进行有效的协同响应[23]。例如，当入侵检测系统发现异常流量时，或将面临无法自动联动防火墙进行阻断，也无法通知其他系统进行防护策略调整等问题。这种孤立的防护模式使攻击者可以轻易绕过单一防御点，对整个系统造成危害。此外，上述单点防护方案各自产生安全日志和告警信息，而这些信息通常存储在不同的数据库中，缺乏统一的收集、分析和关联平台，形成“信息孤岛”，这使安全分析人员难以从海量的碎片化信息中发现跨域攻击的完整链条。

同时，枢纽通航业务对实时性与连续性有着极高的要求。由于安全检测与防护机制的孤立，安全事件响应流程复杂、效率低下。从发现威胁到采取有效防护措施，中间需要人工干预和跨部门协调，这大大延长了响应时间。在船闸运行等高风险场景中，响应滞后可能导致严重的后果。因此，针对NHI-Net的安全技术需要实现跨域协同，将威胁检测和防护融合，以确保及时有效的安全防御。

1.2　跨域联动安全防护体系

针对NHI-Net的安全防护，需要避免传统安全防御的局限性，不再将安全视为一系列孤立的工具或单点的防御工事，而是将其构建为一个有机的、自我强化的生态系统。防护方案应通过对自身脆弱性的深度认知和对外部威胁的精准感知，打破防御孤岛，实现从情报驱动、动态信任评估到协同防御与韧性恢复的全方位联动。因此，本文建立了枢纽通航关基设施的跨域联动安全防护技术体系，围绕跨域网络脆弱性与威胁精准自主识别、安全防御与防护响应多维度协同联动两大核心问题，形成了一个持续迭代、环环相扣的闭环防御机制。该体系涵盖了4个技术方向，即脆弱性分析、跨域威胁识别、跨域协同防御、防护联动。跨域联动安全防护技术体系如图3所示。

脆弱性分析技术作为防御体系的起点，核心在于全面且深入地理解枢纽通航关基设施自身的安全弱点。首先，通过威胁建模，从攻击者的视角系统性地识别潜在的攻击路径、威胁源与薄弱环节，这为后续的风险评估提供了精准的方向，确保不遗漏关键的攻击面；其次，在威胁建模的指引下，风险评估对这些潜在的威胁和已知的脆弱性进行量化或定性分析，评估其可能性与潜在影响，从而将有限的安全资源优先分配给最关键、风险最高的领域；同时，风险评估的结果会反向促进威胁建模更适配真实的系统架构，形成持续优化的认知循环；最终，漏洞发现技术依据风险评估的优先级，进行有针对性的主动探测，通过实测手段识别实际存在的安全缺陷。漏洞发现将直接反馈给风险评估，进一步修正和完善对风险的判断，确保对系统脆弱性的理解始终保持实时性与准确性。

当系统脆弱性被深度剖析后，跨域威胁识别技术则专注于实时且精准地感知和捕获正在发生的威胁与异常行为。这一过程以日志分析为基石，负责从海量、异构的系统和网络日志中聚合、规范化数据，为威胁识别提供全面的数据基础支持。基于这些基础数据，深度流量分析技术从数据中提取高价值威胁信息，继而识别出更隐蔽的恶意流量和攻击特征，弥补日志分析的不足。当威胁信息被识别时，监控告警系统会立即生成高优先级事件，并驱动自动化响应。跨域威胁识别技术各项措施应形成一个从数据汇聚到深度分析再到实时告警的动态感知链条。

威胁被精准识别后，跨域协同防御技术迅速启动，旨在将威胁感知转化为高效的防御行动。其核心在于通过威胁传播预测，利用事件关联分析，预

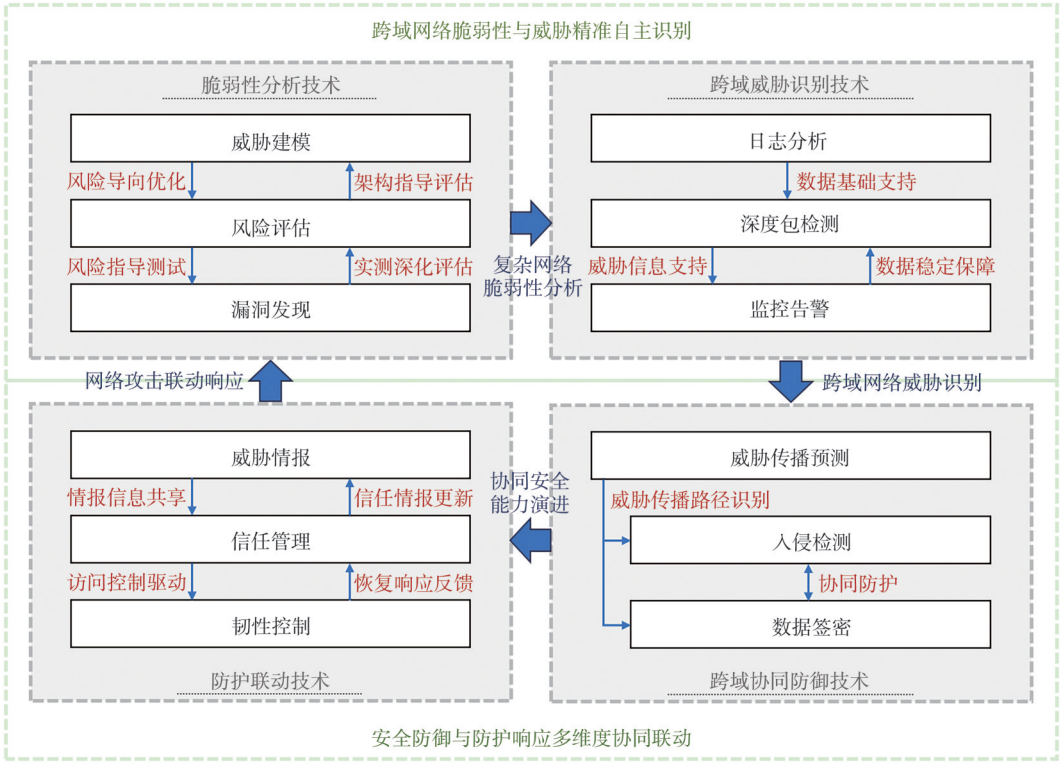


图3　跨域联动安全防护技术体系

判攻击可能在枢纽通航关基设施不同网络域中扩散的路径和方式，为后续防御提供关键的威胁传播指导。对攻击路径的预判完成后，入侵检测系统能更精准地在潜在的传播节点或关键业务区域部署监控与防御，及时发现并阻断入侵行为。与此同时，数据签密技术在数据传输和存储层面提供坚实的安全保障，它结合加密与数字签名，确保关键数据的机密性、完整性和真实性。入侵检测与数据签密实现对NHI-Net的协同防护：当入侵检测发现攻击行为时，可以联动数据签密系统，对受威胁的数据或通信进行加强保护；反之，数据签密对数据完整性的验证失败，也能反向作为入侵检测的重要信号，共同构建起立体化的防御屏障。

防护联动技术负责将防御成果和经验转化为持续优化的防御策略与系统韧性。它通过威胁情报的共享，获取外部最新的威胁态势、攻击方法等信息，为内部策略调整提供前瞻性的情报信息共享。这些情报信息被输入到信任管理体系中，信任管理会动态评估并调整系统内各实体的信任等级，并将最新的信任情报更新反馈给威胁情报系统，以优化情报的可靠性；基于信任评估的结果，信任管理将驱动韧性控制，动态调整资源访问权限，实现细粒度的安全控制，在攻击或故障发生时最大限度地限制影响范围；同时，韧性控制在应对攻击和进行业务恢复的过程中，产生的实际效果和经验将反馈给信任管理，进一步修正信任策略，形成一个从情报驱动、信任评估到动态控制与恢复的持续优化闭环，确保枢纽通航关基设施在面对挑战时具备强大的自适应性和业务连续性。

2　关键技术综述

本节将根据跨域联动安全防护技术体系涵盖的技术方向，分别对各个方向的关键技术及其研究现状进行梳理。安全防护技术见表3，总结了本文覆盖的安全防护技术及方案。

2.1　脆弱性分析技术

2.1.1　威胁建模

对NHI-Net架构执行脆弱性分析，并将网络架构安全性量化成威胁模型，是确保NHI-Net设计安全性的核心。在通航关基设施网络架构中，系统安全依赖于精准的机械控制和复杂的信息通信，并且如船闸、船运导航等子系统的控制与互相协作通常涉及多层次的协议与交互，因此，需要一种多层次的全面审视与综合建模方法，确保网络

表3　　安全防护技术

安全防护技术		研究内容	网络层级				文献
			设备	控制	监管	IT	
脆弱性分析	威胁建模	脆弱性分析、量化威胁模型	√	√	√	√	[24-27]
	风险评估	脆弱性优先级排序	√	√	√	√	[28-29]
	漏洞发现	配置审计、静态代码分析、模糊测试		√	√	√	[30-35]
跨域威胁识别	日志分析	设备监听、日志解析、数据聚合			√	√	[36-42]
	深度包检测	数据分析、行为异常识别			√	√	[43-45]
	监控告警	全流程监控、实时报警	√	√	√	√	[46-48]
跨域协同防御	威胁传播预测	关联识别、攻击路径预测			√	√	[49-58]
	入侵检测	流量特征处理、恶意检测		√	√	√	[59-66]
	数据签密	异构签密、数据安全传输		√	√	√	[67-71]
防护联动	威胁情报	网络实体归因、安全策略优化		√	√	√	[72-79]
	信任管理	身份认证、权限控制、信任评估		√	√	√	[80-87]
	韧性控制	容灾响应与恢复	√	√	√		[88-93]

在面对各种潜在威胁时具有足够的抵御能力和恢复韧性。

基于分层架构的威胁建模方法建构设备层、控制层、监管层和IT层实体、工作流程和连接模式，接下来对各层威胁向量的特征和潜在影响进行分析与抽象。常用的威胁建模方法是STRIDE（spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege）模型，该模型利用数据流图（DFD, data flow diagram）描述网络系统，随后整体分析网络各组件的威胁。STRIDE模型包含了对欺骗、篡改、否认、信息泄露、拒绝服务和特权提升6种威胁类型的建模理论。然而，原始的STRIDE模型未考虑ICS网络终端的物理环境，从而忽略了物理攻击对网络脆弱性的影响[24]。例如，升船机的PLC常处于强电磁干扰环境中，电磁噪声可能导致传输的控制指令出现误码或比特翻转，这种物理层面的信号完整性破坏若未被识别，可能导致设备执行错误的机械动作。为此，现有方法常在DFD中加入物理资产节点，并将物理破坏、阻断等物理行为纳入威胁框架[25-26]。混合建模也是一个可行的方案，Castiglione 和 Lupu[27]将STRIDE模型与关注系统物理安全的STPA-Sec分析相结合，通过构建“威胁—事故模型”将物理层面的攻击行为与物理系统的危险状态及所需特权直接关联。

2.1.2　风险评估

风险评估技术系统化地识别并量化网络系统中的潜在脆弱性及其可能引发的安全威胁，并对脆弱性的安全风险执行优先级排序，从而为制定有效的风险管理策略提供科学的依据。这里，对NHI-Net的风险评估不仅要求对网络资产的可见性，也需要利用安全经验或漏洞知识库作为评价依据。

通用漏洞评分系统（CVSS, common vulnerability scoring system）在IIoT脆弱性评估中被广泛应用，这是一个不断迭代的漏洞评估标准，最新版本CVSS v4建立了基础、威胁、环境、补充4个指标组，在每一个定性/定量指标下计算得分并合成脆弱严重性的最终分数[28]。由于CVSS的通用性质，部分概念和指标存在宽泛和模糊的问题，因此需要更精细的优化方法来契合NHI-Net的系统差异和统计粒度。Falco等[29]针对SCADA系统提出了一种风险评估框架，该方法从公开漏洞详情库和漏洞利用库中汇集脆弱性信息，利用余弦相似度测试比较SCADA系统和通用网络下的漏洞密度和分布，并基于CVSS和多变量回归模型改进了脆弱性优先级排序模式。

2.1.3　漏洞发现

NHI-Net的漏洞发现措施以增强系统配置安全性与分析脆弱性能力为目标，通过配置审计、静态代码分析和模糊测试等漏洞发现技术全面探查网络系统的脆弱性。

配置审计检查网络架构中操作系统、网络设备、应用程序和数据库等各种软硬件的相关配置信息，从而确保网络系统符合标准、规格说明和规程[30]。配置审计的核心任务是检查配置项的完备性、基线的完整性、技术文档的准确性、变更的正确性和合规性，以及配置管理人员的责任履行情况，同时评估配置信息安全的保护机制是否有效。

最新的研究提出了利用自动化技术优化配置审计流程的方法，从而最大限度地减少人为干预，提高敏捷性，并降低潜在的资源消耗。例如，Bringhenti等[31]采用了形式化验证的方法，开发了利用可满足性模理论的验证求解器，并基于网络流状态决策提出链式验证的并行范式，提高了验证效率。

静态代码分析是一种在不实际执行系统程序的条件下，基于安全开发规范解析源代码或编译后的中间代码，以识别潜在安全漏洞、逻辑缺陷及编码规范违规的自动化检测技术[32]。静态代码分析的检测对象包括源程序的语法、结构、过程、接口等，以检查并发现可能的歧义嵌套、参数不匹配、空指针应用等常见代码错误。一种通用的分析流程利用语法分析器对代码语法进行抽象建模，并规范化为中间表示。随后根据预定义的规则分析代码表示的语义或其中未定义的行为，从而识别各种漏洞及缺陷。

模糊测试立足于网络系统的运行阶段，基于缺陷注入的思想自动化地识别系统的安全异常。模糊测试的执行步骤可以分为预处理、测试用例生成，以及测试执行，即预先汇集源代码、数据结构等先决知识，并基于这些知识在下一步生成网络系统的测试数据用例输入系统，当出现异常时分析系统行为并溯源漏洞[33-35]。

2.2　跨域威胁识别技术

2.2.1　日志分析

网络日志分析技术系统化地监听、聚合定期产生的网络日志并执行分析处理，以研判网络入侵、数据泄露等安全威胁。NHI-Net的终端与网络设备（如通航工控设备、路由设备、服务器、网关等）产生海量的日志数据，因此通常需要自动化的日志解析方案用于辅助安全人员人工研判。然而，网络日志通常是非结构化的，且不同的设备日志规范可能不同，这驱动日志分析技术向多源一致性规范化的数据处理范式发展。

现有的自动化日志分析方案通常分为基于特征的日志分析与基于异常的日志分析[36]。基于特征的日志分析方法依赖已知攻击特征库，通过解析提取日志字段并匹配特征库中记录的攻击模式、恶意软件签名等攻击特征，以识别对网络的已知攻击。而基于异常的日志分析方法旨在识别潜在的新型攻击，通过比对同一数据流日志间的特定行为以筛选出存在显著异常的网络行为。后者大多运用机器学习方法进行异常识别，其中，常见的聚类算法方案将不同时段日志内容嵌入特征空间中进行聚类，并检测潜在的映射异常行为的离群点[37]；随着深度学习的发展，部分方案使用深度学习模型对非结构化的日志内容进行语义分析，并针对下游各类异常研判任务进行微调训练或提示词工程[38-40]。Le和Zhang[41]提出了一种基于BERT模型的异常检测方案，BERT模型直接从原始日志消息中编码语义表示，并馈送至下游分类任务。虽然异常检测方法能够识别未知攻击，但面临着误报率较高的挑战[42]。

2.2.2　深度包检测

深度包检测（DPI, deep packet inspection）作为跨域威胁识别中的一类新型关键检测技术，通过提取数据包信息，对包含特定数据或代码有效负载的数据包实施各类安全策略（如，识别、分类、重新路由等）。具体而言，DPI检查与单个数据包相关的数据和元数据，这不仅包含基于网络层的报头信息，还可能包含应用数据。DPI引擎通常内联部署在网关中的防火墙内以设置检查点。当数据包接近检查点时，DPI会分析提取信息以拦截任何协议违规、病毒、垃圾邮件和其他异常情况，或阻止数据包继续通过检查点。

DPI方案的技术方向可以分类为模式匹配和统计分析。依托已知恶意签名数据库，模式匹配方法借助正则匹配机制过滤恶意流量。模式匹配方案通常依赖已知签名，无法对未知恶意流量进行检测。此外，传统的自动机匹配方案检测效率低，易受计算资源的限制。因此，启发式算法也可以融入模式匹配方法中，通过优化数据流扫描机制来提高检测速度[43]。统计分析方法建立了一系列统计指标（如，均值、方差、熵），随后采集、监测这些指标并实施检测。例如，Piskac和Novotny[44]考虑流量的时序特征，对流量数据进行向量化，并使用均方根距离、欧几里得距离及向量间角度对流量进行分类。Chung等[45]将数据包内容转化成词向量嵌入向量空间，通过比较向量之间的余弦相似度以区分恶意流量。

2.2.3　监控告警

监控告警系统对NHI-Net的数据传输与处理的安全性执行实时监控，通常是由工控设备上的网络监测头与统一监控平台组成的网络架构。要保障实

时性，监测头及统一平台的数据传输协议须遵循轻量化原则，以兼顾低时延和低资源消耗的要求。例如，Liu 等[46]提出了一种综合性农业 IoT 监控框架，农业传感器基于 Zigbee 网络将数据传输至 Raspberry Pi 网关，最终以 MQTT 的传输形式上传至基于 AWS 的云计算监控告警平台。

然而，传统的集中式监控告警系统存在可用性和可扩展性的不足。监控数据集中传输显著地提高了对网络带宽的需求，这种带宽压力可能反过来影响监控平台的可用性，进而影响整个监控告警系统的运行。最近的研究从不同技术角度探讨了监控告警系统的分布式优化，将数据处理、存储等功能分散到各个节点协同工作[47]。例如，He 等[48]利用区块链技术对工控网络设备软件与文件系统的技术状态进行监控存储，其中，工控设备上的监控模块定期采集设备状态并生成快照，经验证后存储于可信分布式的区块链网络中。同时，监控模块根据可信快照生成软件访问白名单，从而监控并告警软件对文件系统的不正常调用。

2.3　跨域协同防御技术

2.3.1　威胁传播预测

威胁传播预测对 NHI-Net 中的攻击事件进行建模，以识别攻击路径并预测潜在的攻击事件与目标。具体而言，该环节通常通过多源数据来集成网络日志、告警数据等，并利用关联规则及关联矩阵，建立网络异构系统与设备间安全威胁的事件关联。之后，通常通过建模网络活动溯源图来识别攻击路径及预测潜在的威胁传播目标。

通常情况下，可以利用网络操作系统的内置审计功能或第三方工具收集网络活动信息，包括文件读写、网络与进程通信等[49-50]。为了追踪仅与攻击构成依赖关系的网络事件，需要设计精简方法对采集的信息流进行预处理。Ji 等[51]利用动态信息流追踪技术同步捕捉跨主机依赖关系，该方案建立网络数据流的标签映射，并解耦不同数据流标签的依赖关系以实现并行主机间的延迟同步。此外，分区追踪是一种更精简程序开销的技术，Yang 等[52]考虑用户侧可见程度与网络事件依赖粒度的关系，以省略不受关注的网络主机依赖。

在确立网络系统依赖关系并识别攻击的前提下，通常采用基于攻击图的预测方案，在当前状态下向后遍历依赖路径并执行算法来识别高概率的下一步攻击目标或完整的传播路径[53]。在攻击图的基础上，一些工作使用贝叶斯网络或马尔可夫链来构建概率图模型[54-55]。近年来，机器学习方法被广泛应用于威胁传播检测，从而接管了从攻击图建模到传播路径预测的一个或多个步骤[56-57]。Li 等[58]提出了一种攻击预测框架，利用 Transformer 模型分析网络日志语义以检测当前攻击序列，并使用 LSTM 预测潜在的攻击路径，最终构建完整的攻击链。

2.3.2　入侵检测

入侵检测系统（IDS, intrusion detection system）通过分析 NHI-Net 中的流量以识别网络中的恶意活动或违反安全策略的行为。根据实际场景，部署于 IIoT 中的 IDS 与通用 IDS 通常采取不同的计算和代理策略：首先，由于部署在 IIoT 中的大多数设备资源有限，很少存在具有高计算资源的网络节点，因此难以将 IDS 的计算功能部署于网络设备终端；其次，IIoT 多采用多跳通信的方式，且使用了独特的网络协议，这为 IDS 的数据源依据提出了新的要求。

与日志分析技术类似，IDS 也可以区分为基于已知特征和基于异常检测，后者被设计为可以识别未知的恶意攻击。其中，异常型 IDS 普遍使用机器学习方法，即提取流量特征后馈送至下游检测模型学习异常流量模式。此类 IDS 的完整部署周期包括流量数据收集、数据预处理、部署、训练和验证 5 个环节[59]。为了契合 IIoT 的网络架构，现有 IDS 方案大多将检测算法部署在中央平台或云端，部分方案采用了边缘计算的范式[60-62]。Abdel-Basset 等[63]基于雾计算架构在部署于 IIoT 节点上的雾节点执行分布式训练与检测，其检测模型使用局部门控递归单元模块来学习局部表征，并引入多头注意力层以捕捉全局表征。在数据源层面，相关工作依托拟真测试环境，构建并提出了专门的 IIoT 流量数据集[64-65]。这些数据集涵盖了工业网络架构中特有的流量模式和通信协议。例如，Zolanvari 等[66]搭建了一个真实水利设施 SCADA 架构测试台，并在该环境中模拟了后门、代码注入、SQL 注入 3 类攻击。该工作的网络架构将水处理设施控制子网与局域网通过逻辑控制器相连，子网间通信采用 Modbus 协议。

2.3.3　数据签密

NHI-Net 的数据签密是一种将数字签名和数据加密两种安全技术紧密结合的密码学操作。它旨在确保枢纽工业互联网中传输的敏感数据既具有机密

性，又具有不可否认性、完整性和真实性[67]。相较于传统数据安全方案，数据签密的优势在于它仅通过单个步骤或单个算法实现了双重安全目标，而无须先进行签名再进行加密的传统两步操作，不仅简化了流程，提高了运算效率，更重要的是确保了数据的发送方和接收方之间的端到端安全信任。

由于不同子系统之间的安全隔离需求，NHI-Net通常采用多密码体系。同时，由于传统的串行签密方案通常产生不必要的冗杂计算和通信开销，该传统方案可能会对系统实时性造成负面影响。因此，近期提出了若干种广播签密的方案，保证每个接收方都能独立地解密和验证消息，从而提高ICS数据签密的效率和实时性[68-69]。例如，Zhong等[70]使用基于身份的广播签密技术实现安全的数据共享，信任机构事先为已认证的参与实体群组生成固定长度的密文，新的参与实体须获取数据时，由代理服务器接收已认证实体的密文及生成的中间密钥，重加密后发送给新实体执行独立解密和验证。为了保障NHI-Net安全的同时允许子系统之间的互操作性，异构广播签密是一种可行的方向，它允许调度中心安全地向另一个不兼容的密码学体系中的多个接收方发送加密且带有签名的广播消息[71]。

2.4　防护联动技术

2.4.1　威胁情报

基于威胁情报的措施通过收集、分析和应用关于网络威胁、攻击者及其攻击方法的数据，以增强NHI-Net的安全态势。网络威胁情报是关于网络实体的多源安全线索，包括攻击源、攻击动机、攻击方式、系统漏洞、造成影响、补救措施等多维度的信息[72]。基于已有的威胁情报源，NHI-Net安全方案可通过实体识别技术分析情报主体并有条理地关联到本网络实体，随后执行防御系统响应、优化安全策略。

对威胁情报的实体分析包括对网络实体关键词的识别以及信息管理与归因。由于多源威胁情报的半结构化或非结构化特性，这一任务通常属于自然语言处理（NLP, natural language processing）领域。传统方案建立匹配规则规范化威胁情报，并对网络实体进行分类[73]。近年来深度学习被广泛应用于网络安全文本的实体识别，从而省去了人工语义建模和数据标注的过程[74-75]。作为必要的结构化步骤，构建知识图谱成为存储威胁情报并提高可用性的流行方法[76]。例如，Grigoriadis等[77]为网络物理系统设计了一种威胁情报本体法，随后利用Transformer架构编码情报文本并对本体缺失值进行逻辑回归或分类，最终构建机器可读的知识图谱。

在威胁情报采集分析的基础上，一些工作探讨了与防御技术自动化联动的可能性，包括对安全事件的响应和安全策略的控制。在响应层面，知识图谱可作为基于查询的威胁防御系统的数据源，从而对威胁传播检测、攻击检测与防御等安全方案进行增强[78]。在安全控制层面，Amthor等[79]提出了一种威胁情报管理与安全策略控制直接集成的规范模型，包括威胁响应策略、安全架构与机制、信息交换表示3个维度。自动化联动策略有潜力提高网络安全防御的态势感知和实时响应能力。

2.4.2　信任管理

NHI-Net通过一套综合安全信任管理框架，确保网络环境的真实性、合法性、可靠性和安全性，这一框架需要对所有参与实体（用户、设备、系统、数据）进行身份认证、授权、信任评估。目前的研究重点是基于零信任架构（ZTA, zero trust architecture），对内外实体的参与全程执行信任管理和动态授权[80]。

身份认证是在实体尝试访问资源时验证其身份的过程，这包括对用户和设备的认证。对用户而言，基础的口令验证方案容易遭到暴力破解，即使是强口令也会受到侧信道攻击的威胁，因此不适用于NHI-Net此类关键网络架构[81]。目前已有许多优化认证方案，如，生物因素识别、多因素认证等[82-83]。对设备而言，主流的认证方案包括对称密钥认证和公钥基础设施（PKI, public key infrastructure）。对设备的唯一性识别通常需要考虑其物理不可克隆特性、设备间关系等[84]。访问控制或授权则是确定已认证实体权限并相应地限制访问能力。访问控制架构通常采用基于策略（如XCAML[85]）、基于Token（如OAuth）或混合模式[86]。

ZTA的发展引导身份认证与访问控制方案与信任评估实现联动，从而通过参与实体的运行时信任指标动态，持续性地对其执行授权与认证过程。目前这一动态评估的能力主要通过采集实体状态元数据从而构建情境感知来实现，信任管理系统通过持续收集实体状态信息（如网络状态、地理位置、时间、行为等）来整体评估实体可信度[87]。

2.4.3 韧性控制

网络韧性是以操作持续性为目标，抵抗、响应灾害性事件（如网络攻击、物理故障等），并实现灾后恢复的能力[88]。网络韧性工程围绕着容错、可靠性、生存性、业务连续性、应急计划构建安全策略框架，并利用相关的网络安全技术来实现网络韧性控制。如 Al Maruf 等[89]使用各类韧性架构为 CPS 设计了基于时序的安全框架，该框架使用一种联合计算算法对韧性控制策略与时序参数做动态决策。

对于 NHI-Net 而言，韧性控制通常包括容灾响应和恢复，这一过程旨在最大化地保障网络正常运行，减少通航业务中断和损失。防御侧对灾害下网络系统的状态应保持一定的理解，从而基于可靠的状态信息识别灾害，并使用对应的韧性控制策略。这需要对系统执行韧性状态估计，主要基于时序模型从传感器收集的数据中动态估算系统状态[90-91]。在灾害期间，防御侧通常需要对系统修改配置（如，网络拓扑、设备配置、防火墙规则）以抵抗灾害。目前主流的方法是在系统中增添安全决策层，即通过控制器网络实现自动响应[92]。

为了在灾后恢复运行状态，网络系统（包括代码、配置、数据）通常被设计为可逆，即系统可以回溯到安全可信的映像。例如，Pradhan 等[93]设计的扩展架构对系统所有可达配置空间执行隐式编码，以便于在异常配置下计算有效配置点并向其迁移，从而实现了恢复韧性。

3 典型案例分析：船闸调度控制系统

为了进一步阐述跨域联动安全防护体系在枢纽通航业务场景中的应用逻辑，本文选取船闸调度控制系统作为典型案例。在枢纽通航关基设施中，船闸调度控制系统负责船闸运行的自动化、智能化管理与控制，通过集中调度、远程控制、信息服务、船舶自动排队与调度，保障船闸的通行能力和效率。同时，该系统连接了上层的航运调度管理平台和底层的现地控制单元，是高风险的跨域交互场景。船闸调度控制系统典型攻击场景与跨域联动安全防护如图 4 所示，展示了船闸调度控制系统的典型攻击场景，以及在该场景中基于上述技术构建的跨域联动安全防护框架。

3.1 攻击场景与威胁建模

在船闸调度控制系统攻击场景中，威胁源主要包括 APT 组织、网络犯罪团伙以及内部操作风险。由于航运调度管理平台连接到内部工控网络，同时借助为船民申报提供的 Web 服务连接到外部互联网。攻击者通过外部互联网收集线索以渗透航运调度管理平台，获取管理权限，并进一步实现跨域攻击。

1) 侦察与资产测绘

攻击者利用开源情报与网络空间测绘工具执行隐蔽侦察。由于船民申报系统面向公众开放，攻击者首先通过分析 Web 前端代码与应用程序接口（API, application program interface），识别后台中间件版本及数据库类型；同时，检索公开的工程招标

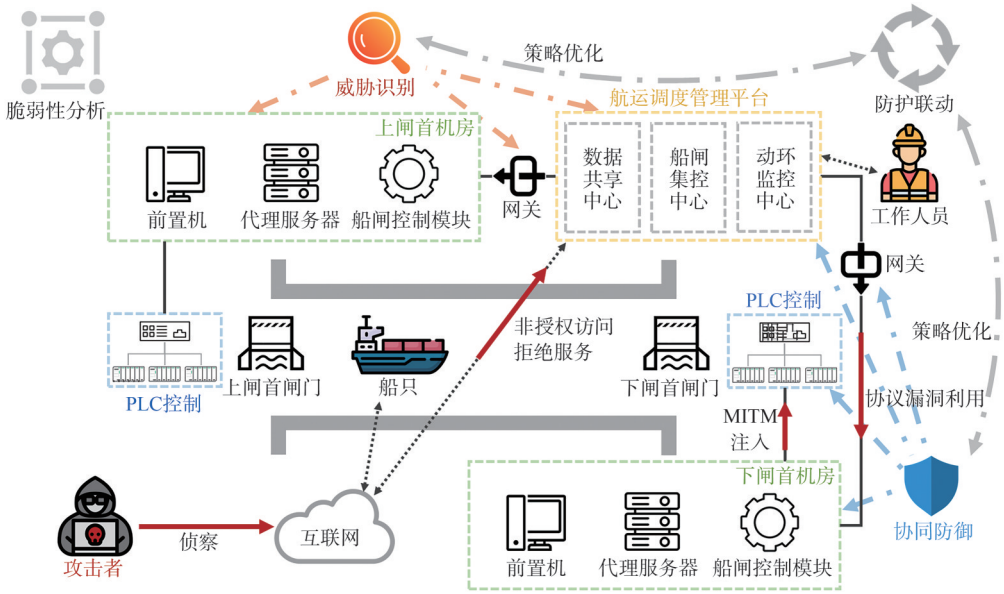


图 4　船闸调度控制系统典型攻击场景与跨域联动安全防护

文档、设备供应商维护手册或社交媒体泄露信息，精准地获取底层关键设备（如，PLC、变频器）的品牌型号、固件版本及默认口令策略。此外，攻击者利用网络扫描工具探测暴露在公网的远程维护端口或未授权访问服务，构建详细的网络拓扑与资产指纹库。

2) 跨域指令篡改

攻击者获取调度员权限后，利用IT/OT边界网关对私有协议解析的脆弱性，向OT层下发伪造指令，如排班确认指令。更进一步，攻击者利用工控协议缺乏认证的缺陷，对底层PLC执行中间人攻击（MITM, man in the middle），篡改水位传感器上传的数据。例如，将“闸室水位未平”的数据篡改为“水位已平”，诱骗控制逻辑打开闸门，导致船舶倾覆或闸门损毁。

3) 工控逻辑注入

攻击者针对船闸PLC注入恶意梯形图代码，其中包含逻辑炸弹，仅在特定时间（如汛期）或特定操作序列下触发，导致液压启闭机在超负荷状态下运行，造成物理设备的不可逆损坏。这种攻击方式与Stuxnet[17]病毒具有相同的攻击机制。

4) 服务拒绝与调度瘫痪

攻击者针对IT层的Web服务接口发动DDoS攻击，导致合法船舶无法申报过闸，造成航道严重拥堵。同时，攻击者可能向OT层的SCADA服务器发送高频畸形数据包，耗尽控制系统的处理资源，迫使系统进入故障安全模式，导致通航中断。

3.2　跨域联动安全防护技术的应用

上述攻击场景对防护体系覆盖IT层的身份与日志审计、边界的协议过滤，以及OT层的指令完整性校验提出了较高的要求。

在攻击发生前的脆弱性分析阶段，防护体系首先利用威胁建模技术对船闸复杂的业务流程进行解构，重点识别连接航运调度IT网络与现地控制OT网络的跨域边界。由于该边界涉及HTTP与Modbus TCP等异构协议的转换，极易成为攻击者横向移动的跳板，因此，系统通过针对性的模糊测试主动挖掘协议解析器中潜在的畸形包漏洞，提前加固高风险的协议转换网关，从源头上减少攻击面。

当攻击者尝试渗透时，跨域威胁识别技术开始发挥多维感知的效能。IT层的安全组件会实时审计业务日志，敏锐地捕捉到调度员账号在非工作时间登录等异常行为。与此同时，部署于OT层网关的DPI引擎深入工业协议载荷，监测到同一时间窗口内指向核心PLC的异常高频写操作指令。更关键的是，监控告警平台打破了IT与OT的信息孤岛，将上述账号异常与流量异常进行时序关联分析，从而能够精准地判定这不是单一的误操作，而是一次有预谋的跨域入侵行为。

一旦确认攻击特征，跨域协同防御机制立即响应，将被动发现转为主动阻断。IDS在识别威胁后，迅速联动加密组件。而异构广播签密机制要求所有下发至PLC的关键控制指令必须附带基于多因素认证的数字签名。虽然攻击者窃取了IT权限，但无法伪造有效的底层设备签名，所以其篡改后的船闸操作指令在到达PLC端时会因签名验证失败而被拒绝执行，从而有效地保障了数据的完整性与真实性。

最后，防护联动技术确保了系统的韧性与持续优化。基于ZTA的信任管理组件会根据检测到的入侵事件，动态地大幅降低受损调度终端的信任评分，自动剥离其对OT核心设备的访问权限，防止威胁进一步扩散。同时，韧性控制模块接管系统状态，在判定控制指令不可信的极端情况下，引导船闸系统自动切换至“安全失效”模式，即由远程自动控制转为就地人工确认模式，优先确保水利设施的物理安全与航运秩序的底线稳定。

4　问题与讨论

尽管现有的跨域联动安全防护体系为NHI-Net提供了一定的安全保障，但面对日益复杂的网络攻击手段与行业特有的业务连续性需求，相关技术仍面临诸多挑战。这一节根据枢纽通航行业的紧迫性与安全建设的优先级逻辑，分别从5个维度深入地探讨了当前面临的技术瓶颈与未来研究方向。

4.1　存量异构设备的非侵入式防护

作为当前枢纽通航行业面临的最紧迫挑战，枢纽通航关基设施中大量服役的存量OT设备面临着严峻的内生安全赤字。由于这些设备通常被设计用于特定的单一功能，且需要保障持续性不间断通航，导致其难以进行频繁的固件升级或停机安装补丁。未来的研究重点应聚焦于非侵入式防护技术，即在不改变原有网络拓扑与设备逻辑的前提下，研发能够深度解析私有异构工控协议的智能安全网络设备，最小化设备更新的影响。通过旁路监测或透

明代理的方式，防护方案能够实现对异构协议指令的深度威胁检测与异常行为阻断，从而为无法自我迭代的老旧设施构建一道有效的外置安全屏障[94]。

4.2　核心控制设备的自主可控

目前，部分枢纽通航设施的核心硬件及底层芯片仍依赖国外供应链，存在后门植入与远程断供的潜在风险。因此，未来的研究须重点关注基于自主可控硬件（如PLC）的可信运行环境构建。通过引入国产化可信计算芯片作为硬件信任根，建立从引导加载程序、操作系统内核到应用逻辑代码的完整信任链，实现对控制逻辑的实时度量与完整性校验。这种内生安全机制能够从根本上防御固件篡改攻击，确保关键控制指令在可信的计算环境中执行。

4.3　跨域联动响应的高实时性

随着船闸调度与航运管理自动化程度的提高，业务指令在IT与OT域间的交互频率呈指数级增长，对威胁响应的实时性提出了极高要求。现有的安全检测机制通常存在响应滞后，导致跨域攻击链难以在造成物理破坏前被切断。因此，提升跨域边界的实时防护能力是保障通航安全的关键，致使未来的研究须聚焦传统高时延检测瓶颈。应用边缘计算技术能够将计算能力下沉至设备层或接近数据源的节点，因此能够为跨域联动安全防护的实时性带来显著的增益[47]。

4.4　IT/OT网络防护一体化协同

过去的攻击事件证明了攻击者通常能够从IT网络突破传统上的隔离，对OT网络中的设备及系统执行攻击。因此，跨域联动安全防护范式要求对IT网络和OT网络实施一体化的安全防护，以实现跨领域的协同防御和统一管理。这包括将NHI-Net视为整体的脆弱性建模，以及贯穿IT与OT网络的联动威胁识别与防御。例如，为实现身份互信的跨域联动，需要建立适应多主体（如，航道管理、船闸管理、信息安全运维）协同的密钥管理与动态授权体系[3]。然而，现有的单一IT或OT网络安全防护方案普遍缺乏对另一网络的可扩展性，这为针对NHI-Net的一体化防护方案提出了新的要求：首先，需要解决协议转换和数据解析问题，确保来自OT网络的流量和日志能够被IT侧的安全分析工具理解和处理；其次，需要解决IT方案对OT环境中各类软硬件的兼容性和支持，考虑计算资源使用、延迟和抖动的差异[95]。

4.5　轻量化的AI应用及安全

在跨域联动安全防护的多数实践中，融合机器学习已成为安全行业的主流技术方向。然而，应用此类高度数据驱动的技术手段，需要使用海量的数据训练模型。其中，数据质量是模型性能的决定性因素，同时对于有标注数据而言还须注意平衡性，而这一因素往往限制了NHI-Net对机器学习的有效应用。从另一个角度而言，此类ICS有限的计算资源难以满足一些复杂机器学习方法的要求，相关研究需要在模型性能和资源之间找到平衡，为NHI-Net设计轻量化的机器学习方案[96]。

值得注意的是，机器学习本身也仍须引入新的攻击面。从数据的角度而言，攻击者可能在模型的训练数据中注入恶意或带有误导性的样本，这可能导致模型在学习过程中产生错误的认知，从而导致在实际部署后无法识别真正的威胁或产生误报。此外，攻击者可以通过分析模型的输入和输出来推断其内部结构和参数，使其可以复制模型的全部功能，甚至发现弱点以开发对抗性攻击。

5　结束语

本文全面梳理了NHI-Net基于不同安全域需求的跨域联动安全防护技术体系。通过深入剖析其研究背景、体系架构、典型案例以及关键技术，本文不仅为该设施的安全能力升级提供了可行的参考与见解，也为保障通航关键基础设施的韧性与安全奠定了理论基础。尽管如此，随着未来通航技术的快速发展与网络威胁的不断演变，相关安全防护体系仍须持续迭代与完善，以应对更复杂多变的威胁挑战，确保大型枢纽通航的持续安全与稳定运行。

参考文献：

[1] 中华人民共和国交通运输部. 公路水路关键信息基础设施安全保护管理办法[A]. (2023-05-06)[2025-06-24].
Ministry of Transport of the People's Republic of China, Measures for the Administration of the Protection of the Critical Information Infrastructure of Highways and Waterways[A]. (2023-05-06)[2025-06-24].

[2] JTS/T 161—2021 船闸信息系统设计规范[S].
JTS/T 161—2021 Design Code of Shiplocks Information System[S].

[3] JTS/T 185—2021 内河数字航道工程建设技术规范[S].
JTS/T 185—2021 Technical Specification of Inland Digital Waterway Engineering[S].

[4] Kayan H K, Nunes M, Rana O, et al. Cybersecurity of industrial

cyber-physical systems: a review[J]. ACM Computing Surveys, 2022, 54(11s): 1-35.

[5] Fei W, Ohno H, Sampalli S. A systematic review of IoT security: research potential, challenges, and future directions[J]. ACM Computing Surveys, 2024, 56(5): 1-40.

[6] 齐俊麟, 陈冬元, 吴澎, 等. 长江和西江大型船闸通航运行关键技术研究与展望[J]. 水运工程, 2024(1): 137-143.
Qi J L, Chen D Y, Wu P, et al. Key technology research and outlook for large ship lock navigationin Xijiang River and the Yangtze River[J]. Port & Waterway Engineering, 2024(1): 137-143.

[7] 马兰青, 张艳, 赵冲, 等. 智慧港口建设关键技术研究与应用综述[J]. 现代交通与冶金材料, 2024, 4(6): 16-30.
Ma L Q, Zhang Y, Zhao C, et al. A review of key technologies in the research and application of smart port development[J]. Modern Transportation and Metallurgical Materials, 2024, 4(6): 16-30.

[8] JTS 304-2—2019 航运枢纽安全检测与评估技术规范[S].
JTS 304-2—2019 Technical Specification for Safety Detection and Assessment of Navigation Junction[S].

[9] Drury B. Control techniques, drives and controls handbook[M]. Institution of Engineering and Technology, 2009.

[10] Tuptuk N, Hazell P, Watson J, et al. A systematic review of the state of cyber-security in water systems[J]. Water, 2021, 13(1): 81.

[11] 亓晋, 王微, 陈孟玺, 等. 工业互联网的概念、体系架构及关键技术[J]. 物联网学报, 2022, 6(2): 38-49.
Qi J, Wang W, Chen M X, et al. Concept, architecture and key technologies of industrial Internet[J]. Chinese Journal on Internet of Things, 2022, 6(2): 38-49.

[12] Shanmuga Sundaram J P, Du W, Zhao Z W. A survey on LoRa networking: research problems, current solutions, and open issues[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 371-388.

[13] Xia Y Q, Zhang Y, Dai L, et al. A brief survey on recent advances in cloud control systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(7): 3108-3114.

[14] Mahnke W, Leitner S H, Damm M. OPC unified architecture[M]. Berlin, Heidelberg: Springer, 2009.

[15] Yassein M B, Shatnawi M Q, Aljwarneh S, et al. Internet of things: survey and open issues of MQTT protocol[C]//Proceedings of the 2017 International Conference on Engineering & MIS (ICEMIS). Piscataway: IEEE Press, 2017: 1-6.

[16] DB32/T 4733—2024 数字孪生水网建设总体技术指南[S].
DB32/T 4733—2024 General technical guidelines of the digital twin water network construction[S].

[17] Langner R. Stuxnet: dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[18] Geiger M, Bauer J, Masuch M, et al. An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems[C]//Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). Piscataway: IEEE Press, 2020: 1537-1543.

[19] Cherepanov A. Win32/Industroyer: A new threat for industrial controls systems[R]. 2017.

[20] Johnson B, Caban D, Krotofil M, et al. Attackers deploy new ICS attack framework TRITON and cause operational disruption to critical infrastructure[EB]. (2017-12-14)[2025-06-24].

[21] Cherepanov A. Greyenergy A successor to BlackEnergy[R]. 2018.

[22] Brubaker N, Lunden K, Proska K, et al. INCONTROLLER: New state-sponsored cyber attack tools target multiple industrial control systems[EB]. (2022-04-13)[2025-06-24].

[23] Olaes T. The Top 8 IT/OT/IoT security challenges and how to solve them[EB]. (2025-03-25)[2025-06-24].

[24] Saßnick O, Rosenstatter T, Schäfer C, et al. STRIDE-based methodologies for threat modeling of industrial control systems: a review[C]//Proceedings of the 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS). Piscataway: IEEE Press, 2024: 1-8.

[25] Khan R, McLaughlin K, Laverty D, et al. STRIDE-based threat modeling for cyber-physical systems[C]//Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). Piscataway: IEEE Press, 2017: 1-6.

[26] Khalil S M, Bahsi H, Dola H O, et al. Threat modeling of cyber-physical systems - a case study of a microgrid system[J]. Computers & Security, 2023, 124: 102950.

[27] Castiglione L M, Lupu E C. Which attacks lead to hazards? combining safety and security analysis for cyber-physical systems[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 2526-2540.

[28] Lorenzo S F, Añorga J, Arrizabalaga S. A survey of IIoT protocols[J]. ACM Computing Surveys, 2020, 53(2): 1-53.

[29] Falco G, Caldera C, Shrobe H. IIoT cybersecurity risk modeling for SCADA systems[J]. IEEE Internet of Things Journal, 2018, 5(6): 4486-4495.

[30] Bringhenti D, Marchetto G, Sisto R, et al. Automation for network security configuration: state of the art and research trends[J]. ACM Computing Surveys, 2024, 56(3): 1-37.

[31] Bringhenti D, Marchetto G, Sisto R, et al. Improving the formal verification of reachability policies in virtualized networks[J]. IEEE Transactions on Network and Service Management, 2021, 18(1): 713-728.

[32] Gomes D, Felix E, Aires F, et al. Static code analysis for IoT security: a systematic literature review[J]. ACM Computing Surveys, 2026, 58(3): 1-47.

[33] Zuo F L, Luo Z X, Yu J Z, et al. Vulnerability detection of ICS protocols via cross-state fuzzing[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41(11): 4457-4468.

[34] Zong X J, Ning B W, Wang G G, et al. ICPGF: an industrial control protocol format-aware and feedback-guided fuzzing[C]//Proceedings of the 2023 International Conference on Automatics and Informatics (ICAI). Piscataway: IEEE Press, 2023: 65-70.

[35] Wanyan H, Lai Y X, Liu J, et al. NCMFuzzer: Using non-critical

field mutation and test case combination to improve the efficiency of ICS protocol fuzzing[J]. Computers & Security, 2024, 141: 103811.

[36] Svacina J, Raffety J, Woodahl C, et al. On vulnerability and security log analysis: a systematic literature review on recent trends[C]// Proceedings of the International Conference on Research in Adaptive and Convergent Systems. New York: ACM Press, 2020: 175-180.

[37] Landauer M, Skopik F, Wurzenberger M, et al. System log clustering approaches for cyber security applications: a survey[J]. Computers & Security, 2020, 92: 101739.

[38] Du M, Li F F, Zheng G N, et al. DeepLog: anomaly detection and diagnosis from system logs through deep learning[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1285-1298.

[39] Guo H X, Yuan S H, Wu X T. LogBERT: log anomaly detection via BERT[C]//Proceedings of the 2021 International Joint Conference on Neural Networks (IJCNN). Piscataway: IEEE Press, 2021: 1-8.

[40] Han X, Yuan S H, Trabelsi M. LogGPT: log anomaly detection via GPT[C]//Proceedings of the 2023 IEEE International Conference on Big Data (BigData). Piscataway: IEEE Press, 2023: 1117-1122.

[41] Le V H, Zhang H Y. Log-based anomaly detection without log parsing[C]//Proceedings of the 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE). Piscataway: IEEE Press, 2021: 492-504.

[42] Miranskyy A, Hamou-Lhadj A, Cialini E, et al. Operational-log analysis for big data systems: challenges and solutions[J]. IEEE Software, 2016, 33(2): 52-59.

[43] Liu R T, Huang N F, Chen C H, et al. A fast string-matching algorithm for network processor-based intrusion detection system[J]. ACM Transactions on Embedded Computing Systems, 2004, 3(3): 614-633.

[44] Piskac P, Novotny J. Using of time characteristics in data flow for traffic classification[M]//Managing the Dynamics of Networks and Services. Berlin, Heidelberg: Springer, 2011: 173-176.

[45] Chung J Y, Park B, Won Y J, et al. Traffic classification based on flow similarity[M]//IP Operations and Management. Berlin, Heidelberg: Springer, 2009: 65-77.

[46] Liu S B, Guo L Q, Webb H, et al. Internet of things monitoring system of modern eco-agriculture based on cloud computing[J]. IEEE Access, 2019, 7: 37050-37058.

[47] Liu G X, Shi H, Kiani A, et al. Smart traffic monitoring system using computer vision and edge computing[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(8): 12027-12038.

[48] He S, Ren W, Zhu T Q, et al. BoSMoS: a blockchain-based status monitoring system for defending against unauthorized software updating in industrial Internet of things[J]. IEEE Internet of Things Journal, 2020, 7(2): 948-959.

[49] Gehani A, Tariq D. SPADE: support for provenance auditing in distributed environments[M]//Middleware 2012. Berlin, Heidelberg: Springer, 2012: 101-120.

[50] Pasquier T, Han X Y, Goldstein M, et al. Practical whole-system provenance capture[C]//Proceedings of the 2017 Symposium on Cloud Computing. New York: ACM Press, 2017: 405-418.

[51] Ji Y, Lee S, Fazzini M, et al. Enabling refinable {cross-host} attack investigation with efficient data flow tagging and tracking[C]// Proceedings of the 27th USENIX Security Symposium. Baltimore: USENIX, 2018: 1705-1722.

[52] Yang R Q, Ma S Q, Xu H T, et al. UISCOPE: accurate, instrumentation-free, and visible attack investigation for GUI applications[C]//Proceedings of the 2020 Network and Distributed System Security Symposium. San Diego: Internet Society, 2020: 141.

[53] GhasemiGol M, Takabi H, Ghaemi-Bafghi A. A foresight model for intrusion response management[J]. Computers & Security, 2016, 62: 73-94.

[54] Huang K X, Zhou C J, Tian Y C, et al. Assessing the physical impact of cyberattacks on industrial cyber-physical systems[J]. IEEE Transactions on Industrial Electronics, 2018, 65(10): 8153-8162.

[55] Bar A, Shapira B, Rokach L, et al. Scalable attack propagation model and algorithms for honeypot systems[C]//Proceedings of the 2016 IEEE International Conference on Big Data (Big Data). Piscataway: IEEE Press, 2016: 1130-1135.

[56] Khosravi M, Ladani B T. Alerts correlation and causal analysis for APT based cyber attack detection[J]. IEEE Access, 2020, 8: 162642-162656.

[57] Wang W B, Yi P, Jiang J F, et al. Transformer-based framework for alert aggregation and attack prediction in a multi-stage attack[J]. Computers & Security, 2024, 136: 103533.

[58] Li T, Jiang Y, Lin C, et al. DeepAG: attack graph construction and threats prediction with bi-directional deep learning[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(1): 740-757.

[59] Nuaimi M, Fourati L C, Ben Hamed B. Intelligent approaches toward intrusion detection systems for Industrial Internet of things: a systematic comprehensive review[J]. Journal of Network and Computer Applications, 2023, 215: 103637.

[60] Yao H P, Gao P C, Zhang P Y, et al. Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection[J]. IEEE Network, 2019, 33(5): 75-81.

[61] Zolanvari M, Yang Z B, Khan K, et al. TRUST XAI: model-agnostic explanations for AI with a case study on IIoT security[J]. IEEE Internet of Things Journal, 2023, 10(4): 2967-2978.

[62] 丁凯, 黄宜都, 陶铭, 等. 基于联邦强化学习的面向边缘网络的入侵检测方法研究[J]. 物联网学报, 2024, 8(4): 140-155.
Ding K, Huang Y D, Tao M, et al. Research on intrusion detection method for edge networks based on federated reinforcement learning[J]. Chinese Journal on Internet of Things, 2024, 8(4): 140-155.

[63] Abdel-Basset M, Chang V, Hawash H, et al. Deep-IFS: intrusion detection approach for industrial Internet of things traffic in fog environment[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7704-7715.

[64] Al-Hawawreh M, Sitnikova E, Aboutorab N. X-IIoTID: a connectivity-agnostic and device-agnostic intrusion data set for in-

dustrial Internet of things[J]. IEEE Internet of Things Journal, 2022, 9(5): 3962-3977.

[65] Ferrag M A, Friha O, Hamouda D, et al. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning[J]. IEEE Access, 2022, 10: 40281-40306.

[66] Zolanvari M, Teixeira M A, Gupta L, et al. Machine learning-based network vulnerability analysis of industrial Internet of Things[J]. IEEE Internet of Things Journal, 2019, 6(4): 6822-6834.

[67] Hussain S, Ullah S S, Uddin M, et al. A comprehensive survey on signcryption security mechanisms in wireless body area networks[J]. Sensors, 2022, 22(3): 1072.

[68] 王利朋, 高健博, 李青山, 等. 应用区块链的多接收者多消息签密方案[J]. 软件学报, 2021, 32(11): 3606-3627.
Wang L P, Gao J B, Li Q S, et al. Blockchain-based multi-recipient multi-message signcryption scheme[J]. Journal of Software, 2021, 32(11): 3606-3627.

[69] Zhao Y N, Wang Y P, Liang Y H, et al. Identity-based broadcast signcryption scheme for vehicular platoon communication[J]. IEEE Transactions on Industrial Informatics, 2023, 19(6): 7814-7824.

[70] Zhong H, Zhang S, Cui J, et al. Broadcast encryption scheme for V2I communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2022, 71(3): 2749-2760.

[71] Hou Y Z, Cao Y, Xiong H, et al. Heterogeneous broadcast signcryption scheme with equality test for IoVs[J]. IEEE Transactions on Vehicular Technology, 2024, 73(12): 19550-19564.

[72] 李建华. 网络空间威胁情报感知、共享与分析技术综述[J]. 网络与信息安全学报, 2016, 2(2): 16-29.
Li J H. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space[J]. Chinese Journal of Network and Information Security, 2016, 2(2): 16-29.

[73] Zhu Z Y, Dumitras T. ChainSmith: automatically learning the semantics of malicious campaigns by mining threat intelligence reports[C]//Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2018: 458-472.

[74] Dionisio N, Alves F, Ferreira P M, et al. Cyberthreat detection from twitter using deep neural networks[C]//Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN). Piscataway: IEEE Press, 2019: 1-8.

[75] Zhao J, Yan Q B, Li J X, et al. TIMiner: automatically extracting and analyzing categorized cyber threat intelligence from social data[J]. Computers & Security, 2020, 95: 101867.

[76] Pingle A, Piplai A, Mittal S, et al. RelExt: relation extraction using deep learning approaches for cybersecurity knowledge graph improvement[C]//Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. New York: ACM Press, 2020: 879-886.

[77] Grigoriadis C, Berzovitis A M, Stellios I, et al. A cybersecurity ontology to support risk information gathering in cyber-physical systems[M]//Computer Security. ESORICS 2021 International Workshops. Cham: Springer International Publishing, 2022: 23-39.

[78] Gao P, Liu X Y, Choi E, et al. A system for automated open-source threat intelligence gathering and management[C]//Proceedings of the 2021 International Conference on Management of Data. New York: ACM Press, 2021: 2716-2720.

[79] Amthor P, Fischer D, Kühnhauser W E, et al. Automated cyber threat sensing and responding: integrating threat intelligence into security-policy-controlled systems[C]//Proceedings of the 14th International Conference on Availability, Reliability and Security. New York: ACM Press, 2019: 1-10.

[80] Syed N F, Shah S W, Shaghaghi A, et al. Zero trust architecture (ZTA): a comprehensive survey[J]. IEEE Access, 2022, 10: 57143-57179.

[81] Li M Y, Meng Y, Liu J Y, et al. When CSI meets public WiFi: inferring your mobile phone password via WiFi signals[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 1068-1079.

[82] Shah S W, Kanhere S S, Zhang J, et al. VID: human identification through vein patterns captured from commodity depth cameras[J]. IET Biometrics, 2021, 10(2): 142-162.

[83] 魏忠诚, 陈炜, 董延虎, 等. 基于Wi-Fi感知的多用户身份识别研究[J]. 物联网学报, 2024, 8(1): 111-121.
Wei Z C, Chen W, Dong Y H, et al. Research on multi-user identity recognition based on Wi-Fi sensing[J]. Chinese Journal on Internet of Things, 2024, 8(1): 111-121.

[84] Chen D J, Zhang N, Qin Z, et al. S2M: a lightweight acoustic fingerprints-based wireless device authentication protocol[J]. IEEE Internet of Things Journal, 2017, 4(1): 88-100.

[85] Riad K, Cheng J R. Adaptive XACML access policies for heterogeneous distributed IoT environments[J]. Information Sciences, 2021, 548: 135-152.

[86] Trabelsi R, Fersi G, Jmaiel M. Access control in Internet of things: a survey[J]. Computers & Security, 2023, 135: 103472.

[87] Carrera-Rivera A, Larrinaga F, Lasa G. Context-awareness for the design of Smart-product service systems: Literature review[J]. Computers in Industry, 2022, 142: 103730.

[88] Hausken K. Cyber resilience in firms, organizations and societies[J]. Internet of Things, 2020, 11: 100204.

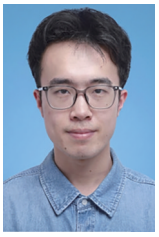
[89] Al Maruf A, Niu L Y, Clark A, et al. A timing-based framework for designing resilient cyber-physical systems under safety constraint[J]. ACM Transactions on Cyber-Physical Systems, 2023, 7(3): 1-25.

[90] Shoukry Y, Nuzzo P, Puggelli A, et al. Secure state estimation for cyber-physical systems under sensor attacks: a satisfiability modulo theory approach[J]. IEEE Transactions on Automatic Control, 2017, 62(10): 4917-4932.

[91] Alhelou H H, Nagpal N, Nagpal H, et al. Dynamic state estimation for improving observation and resiliency of interconnected power systems[J]. IEEE Transactions on Industry Applications, 2024,

60(2): 2366-2380.
[92] Li X, Zhou C J, Tian Y C, et al. A dynamic decision-making approach for intrusion response in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2019, 15(5): 2544-2554.
[93] Pradhan S, Dubey A, Levendovszky T, et al. Achieving resilience in distributed software systems via self-reconfiguration[J]. Journal of Systems and Software, 2016, 122: 344-363.
[94] Ding F, Li H D, Luo F, et al. DeepPower: non-intrusive and deep learning-based detection of IoT malware using power side channels[C]//Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. New York: ACM Press, 2020: 33-46.
[95] Bhole M, Kastner W, Sauter T. IT security solutions for IT/OT integration: identifying gaps and opportunities[C]//Proceedings of the 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA). Piscataway: IEEE Press, 2024: 1-8.
[96] Ericson A, Thar K, Forsström S. Enhancing intrusion detection in CPS and IIoT with lightweight explainable AI models[C]//Proceedings of the 2025 IEEE 21st International Conference on Factory Communication Systems (WFCS). Piscataway: IEEE Press, 2025: 1-8.

[作者简介]



李宏宇（2003– ），男，武汉大学国家网络安全学院硕士生，主要研究方向为入侵检测、物联网安全。

李思帆（1999– ），男，武汉大学国家网络安全学院博士生，主要研究方向为物联网入侵检测、车载安全以及空天地一体化安全。

王浩翔（2000– ），男，武汉大学国家网络安全学院博士生，主要研究方向为工控场景下时间序列异常检测。

王昊天（2002– ），男，武汉大学国家网络安全学院硕士生，主要研究方向为物联网网络设备攻击检测。

曹越（1984– ），男，博士，武汉大学国家网络安全学院教授、博士生导师，主要研究方向为网络通信、网络安全、交通决策优化。

陈龙（1988– ），男，博士，北京化工大学信息科学与技术学院教授、博士生导师，主要研究方向为网络安全、入侵检测。

张宇（1987– ），男，奇安信科技集团股份有限公司高级工程师，主要研究方向为网络安全。