



网络化船舶自主航行系统安全技术研究进展

马勇^{1,2,3,4*}, 胡睿蝶^{1,2,3}, 胡松林⁵, 赵玉蛟⁶

1. 水路交通控制全国重点实验室, 武汉理工大学, 武汉 430063

2. 武汉理工大学航运学院, 武汉 430063

3. 内河航运技术湖北省重点实验室, 武汉 430063

4. 国家水运安全工程技术研究中心, 武汉 430063

5. 南京邮电大学碳中和先进研究院, 南京 210023

6. 济南大学信息科学与工程学院, 济南 250022

* E-mail: myongdl@whut.edu.cn

收稿日期: 2024-11-28; 接受日期: 2025-02-08; 网络版发表日期: 2025-03-31

国家自然科学基金(批准号: 52261160383, 62073251)、国家重点研发计划(编号: 2023YFB4302300)和湖北省重点研发计划(编号: 2024BCB099)资助项目

摘要 网络化船舶自主航行系统是指利用先进的信息技术和自主控制技术, 在无人或少人操作情况下实现船舶自主导航和远程监控管理。随着船-船、船-岸之间数字化连接日益增多, 网络安全已成为水路交通领域的研究热点。为掌握船舶自主航行系统的最新发展动态和技术趋势, 本文综述了其网络安全技术研究进展, 并介绍了船舶自主航行系统面临的5种主要网络安全威胁: 信息阻塞、时延、虚假数据、信息盗窃、权限提升。进而, 本文梳理并讨论了包括网络攻击数学建模技术、网络安全态势感知技术、威胁建模与风险评估技术、网络攻击检测技术和弹性安全防御技术的网络安全对策。最后, 本文分析了船舶自主航行系统在网络安全方面面临的机遇和挑战。

关键词 网络化船舶自主航行系统, 网络攻击, 攻击方式, 安全技术

1 引言

随着通信、物联网、大数据、云共享和人工智能等技术的迅猛发展, 以自主、智能为特征的网络化船舶自主航行系统在海洋科考、海事管理等领域的作用日益显著。网络化船舶自主航行系统通过先进的信息技术和自主控制技术, 在无人或少人操作的情况下实现船舶自主航行, 并通过网络与其他船舶、岸基设施以及相关管理机构进行通信和协作。

网络化船舶自主航行系统由船端自主航行系统、岸基支持模块和船岸通信模块共同构成, 其核心是搭载多源传感器感知船舶航行环境(如水文、气象、航道、他船动态等), 并通过船载或岸基智能航行控制单元做出航行决策; 同时, 利用船载通信设备传输船位信息、航行意图等指令和信息, 实现与其他船舶和岸基设施通信。

网络化船舶自主航行系统技术的应用显著降低了人为失误的影响, 提高了船舶航行的安全性和效率。然

引用格式: 马勇, 胡睿蝶, 胡松林, 等. 网络化船舶自主航行系统安全技术研究进展. 中国科学: 技术科学, 2025, 55: 698–716

Ma Y, Hu R D, Hu S L, et al. Research progress on cybersecurity technology for networked autonomous ship navigation systems (in Chinese). Sci Sin Tech, 2025, 55: 698–716, doi: [10.1360/SST-2024-0313](https://doi.org/10.1360/SST-2024-0313)

而, 当前该系统面临的网络安全问题愈加突出. 例如, 丹麦马士基公司在2017年遭遇了严重的安全事件, 这导致其被迫在10天内重建IT基础设施, 损失超过3亿美元, 船队陷入停滞, 港口被封锁, 货物被延误, 同时公司的声誉也受到严重损害^[1]. 此外, 刑事犯罪可能在海洋、陆地、沿海交界区域或网络空间中发生, 包括通过暗网进行的非法活动, 这对网络安全构成了进一步的威胁^[2].

开放接入的通信系统有效支持了网络化船舶自主航行系统在船-船、船-岸间的协作, 但使其更易遭受网络安全的威胁. 当传感器数据和执行器动作命令经由通信网络控制船舶时, 可能会遇到通信延迟、数据丢包等传统网络问题, 并且容易遭受欺骗攻击、重放攻击、中间人攻击和拒绝服务攻击等多种网络攻击. 操作系统或应用程序中的恶意软件以及通信网络中的恶意节点也威胁着自主航行系统的信息安全. 此外, 由于船上的船员经常轮换, 船员可能需要操作不熟悉的系统, 这增加了人为错误的潜在风险. 船载系统的设备维护通常由第三方公司和第三方设备管理, 追踪船只运营和网络安全方面的变化也变得更困难.

为掌握网络化船舶自主航行系统安全技术的研究动态和发展趋势, 本文简述了网络化船舶自主航行系统安全技术的研究进展. 第2节介绍了网络化船舶自主航行系统组成; 第3节分析了网络化船舶自主航行系统面临的威胁和分类; 第4节阐述了网络攻击数学建模、网络安全态势感知、威胁建模与风险评估、网络攻击检测和弹性安全防御5项关键技术的研究进展; 第5节探讨了网络化船舶自主航行系统的挑战与未来发展方向; 第6节对全文进行了总结.

2 网络化船舶自主航行系统组成

网络化船舶自主航行系统综合性较强, 关系到船舶航行的自主、安全水平, 涵盖了多个关键系统组件及模块. 为有效识别潜在的安全风险并采取相应措施, 有必要分析系统的结构及安全要素.

2.1 网络化船舶自主航行系统关键要素

网络化船舶自主航行系统主要包括岸端控制中心(shore control centre, SCC)、自主船舶控制器(autonomous ship controller, ASC)和自主导航系统(autono-

mous navigation system, ANS)^[3]. 图1所示, 各组件通过通信系统的连接、协调配合, 共同保障船舶安全、自主、高效航行.

2.1.1 岸端控制中心(SCC)

岸端控制中心用于远程监测和控制自主船舶. 未来, 岸端控制中心将作为国际海事组织定义的L2级和L3级自主水面船舶的关键组成部分. 在岸端控制中心, 操作人员可以通过远程控制全面监督船舶, 并在紧急情况下切换到人工驾驶模式以应对超出船舶自主能力的特定危险^[4]. 岸端控制中心配备有人机交互单元, 作为岸基与船舶之间的桥梁, 通过传感器数据分析、网络互联和必要时的主动控制, 远程监控和协同支持船舶水上作业^[5].

2.1.2 网络化船舶通信系统

网络化船舶通信系统支持船-船、船-岸间的监测、控制和协调^[6]. 与智能网联车系统中的路侧单元不同, 岸端控制中心距离船舶更远, 船-船之间的数据交换无法借助周边的静态数据锚点来完成, 只能通过建立动态自组网进行^[7]. 在动态自组网中, 自动识别系统(automatic identification system, AIS)和甚高频(very high frequency, VHF)在船-船通信中发挥关键作用, 可增强船舶的态势感知能力, 并与他船交换重要信息.

AIS以特定的时间间隔广播特定数据, 并接收该范围内其他船舶广播的数据. 交换的数据分为静态数据、动态数据和航次相关数据. 静态数据包括船舶的名称、类型、尺寸和吃水深度. 动态数据包括船舶的位置、速度、航向、时间戳等. 航次相关数据包括吃水、潜在危险货物类型、目的地和预计到达时间. 由于缺乏源身份验证, AIS容易受到船舶欺骗攻击. 虚拟船舶可能会广播虚假数据, 如虚假警报、虚假交通信息和虚假操纵信息. 目前, AIS被广泛应用于船舶监控、海上搜救、船舶避障、航海导航等实时工作场景^[8]. 为实现高效数据交换、远程控制, 在高流量的港口区需要使用5G及以上高级蜂窝网络以及Wi-Fi系统支持.

2.1.3 自主船舶控制器(ASC)

在自主船舶中, ASC担任虚拟船长的角色, 负责监督船舶的自主航行. ASC包含多个关键子系统, 如自动动力系统、锚泊和系泊系统以及状态监控和故障管理



图 1 网络化船舶自主航行系统

Figure 1 Networked vessel autonomous navigation systems.

系统. 其中, 自动动力系统与其他子系统集成, 确保船舶可靠推进并提供运行状况反馈; 锚泊和系泊系统支持船舶系留在预定位置, 保障船舶进出港安全; 状态监控和故障管理系统专注于实时监测船舶各系统的运行状态和性能参数, 识别潜在问题和异常情况, 及时发出警报或建议维护措施, 以预防和减少可能的设备故障, 提高网络化船舶自主航行系统的安全性.

2.1.4 自主导航系统(ANS)

自主导航系统是在没有持续人工控制或监督情况下负责操作船舶的集成硬件和软件, 基于多种传感器、处理器、算法感知环境, ANS分析导航复杂性, 规划无碰撞路线并相应地操纵船舶. 其中, 导航和态势感知系统是ANS关键子系统, 通过整合雷达、摄像机、自动识别系统、全球卫星导航系统(global navigation satellite system, GNSS)等传感器数据, 构建稳健的内部模型以重现自主船舶周边环境^[9]; 路线和速度优化系统负责规划最优航行路径和速度; 智能避碰系统作为ANS中重要组成部分, 负责在动态海洋环境

中探测障碍物并规划无碰撞机动方案.

2.2 船舶内部网络结构

船舶内部网络主要用于船舶各系统之间的通信^[10], 图2展示了船舶内部网络结构. 根据在网络安全中的重要性, 船舶内部网络自上而下分别为用户网络及一般应用层、综合管理监视层和船舶控制网络层, 各层连接之间分别设有防火墙^[11]. 用户网络及一般应用层为最上层, 连接外网, 提供船员邮件、电话和电脑等日常工作的网络服务, 最容易受到网络攻击. 综合管理监视层为中间层, 包含了AIS、电子海图显示与信息系统(electronic chart display and information system, ECDIS)等数字化设备, 保障船舶安全航行. 其中ECDIS包含电子海图和船舶航行状态实时信息, 集成了全球定位系统(global position system, GPS)、雷达、测深仪、AIS等系统信息. 攻击者可通过破坏GPS信号或访问ECDIS软件系统来干扰船舶的正常工作, 篡改船舶航行状态信息^[11]. 中间层是网络攻击的主要目标, 易遭受干扰、欺骗等攻击, 导致船舶电子设备

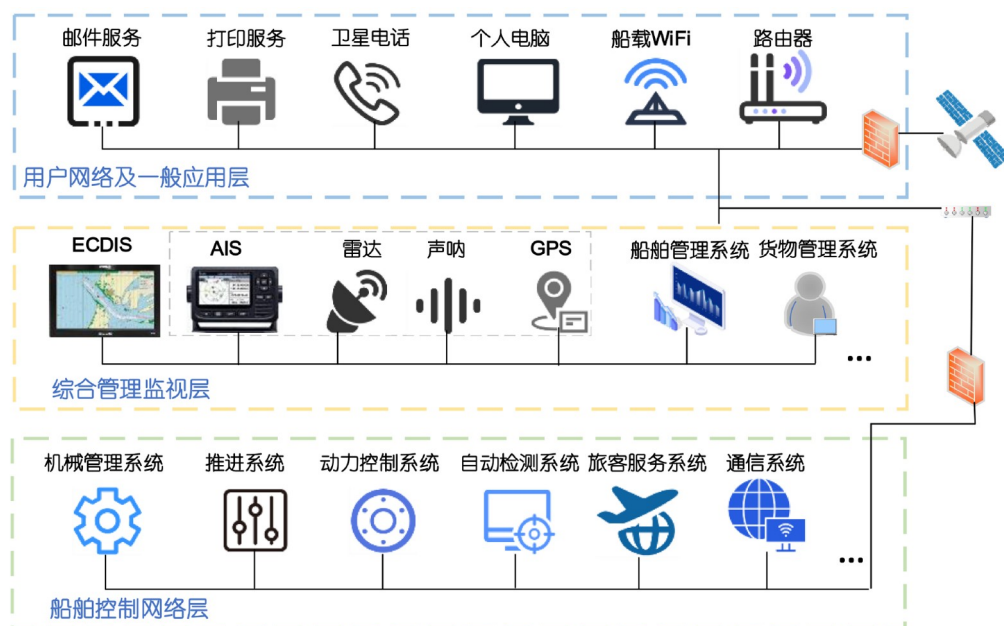


图 2 船舶内部网络结构示意图

Figure 2 Schematic diagram of vessel internal network structure.

失灵^[12]。船舶网络控制层为最底层, 包含最根本的动力、检测、管理等设备。网络控制层一旦被网络攻击者所控制, 船舶将失去自主权, 完全受攻击者操控^[13]。

3 网络化船舶自主航行系统的潜在网络安全威胁

随着网络技术在船舶自主航行系统中的广泛应用, 大量的通信需求潜藏着巨大的网络安全风险。如图3所示, 根据机密性、完整性和可用性的网络安全原则^[14], 本文将可能面临的网络安全威胁划分为五类: 信息阻塞、时延攻击、虚假数据注入、信息盗窃和非法权限提升。表1汇总了上述网络攻击类型。

3.1 信息阻塞

信息阻塞是指通过多种网络攻击技术来阻止船舶自主航行系统的通信, 以达到破坏船舶正常运行或控制的目的, 具体包括拒绝服务攻击、洪泛攻击和黑洞攻击。

(1) 拒绝服务攻击: 其原理是通过产生大量的访问请求使目标无暇响应或者通信链路超负荷。在拒绝服务攻击中, 攻击者通过不断发送无用的消息或在网络

节点上设置干扰, 使正确的消息无法及时到达目的地。分布式拒绝服务攻击是一种更高级的拒绝服务攻击形式, 可以从几个不同的系统向特定目标发起攻击, 并扰乱其功能。

(2) 洪泛攻击: 洪泛攻击是拒绝服务攻击的一种形式, 它在通信建立和使用期间恶意使用通信资源来阻止正常的通信活动。在船舶自主航行系统中, 洪泛攻击会影响船-船、船-岸通信网络和船舶内部网络的正常运行。攻击中使用的数据可以分为两种, 即通信协议规定的数据和无用的数据。前者将消耗通信计算能力, 后者将垄断通信信道资源^[15]。

(3) 黑洞攻击: 黑洞攻击是拒绝服务攻击的另一种形式, 其主要目的是破坏网络中节点或船舶之间的通信服务^[16]。其原理是利用恶意节点在网络通信中发送虚假的路由信息, 通常是具有虚假路径信息和高序列号的路由响应, 引导源节点选择通过恶意节点路径发送数据包, 然后有选择性地丢弃这些数据包, 从而导致通信中断或数据包丢失, 显著削弱网络的性能和可靠性^[17]。

3.2 时延攻击

时延的目的是延迟船舶信息的传递, 这种攻击尤

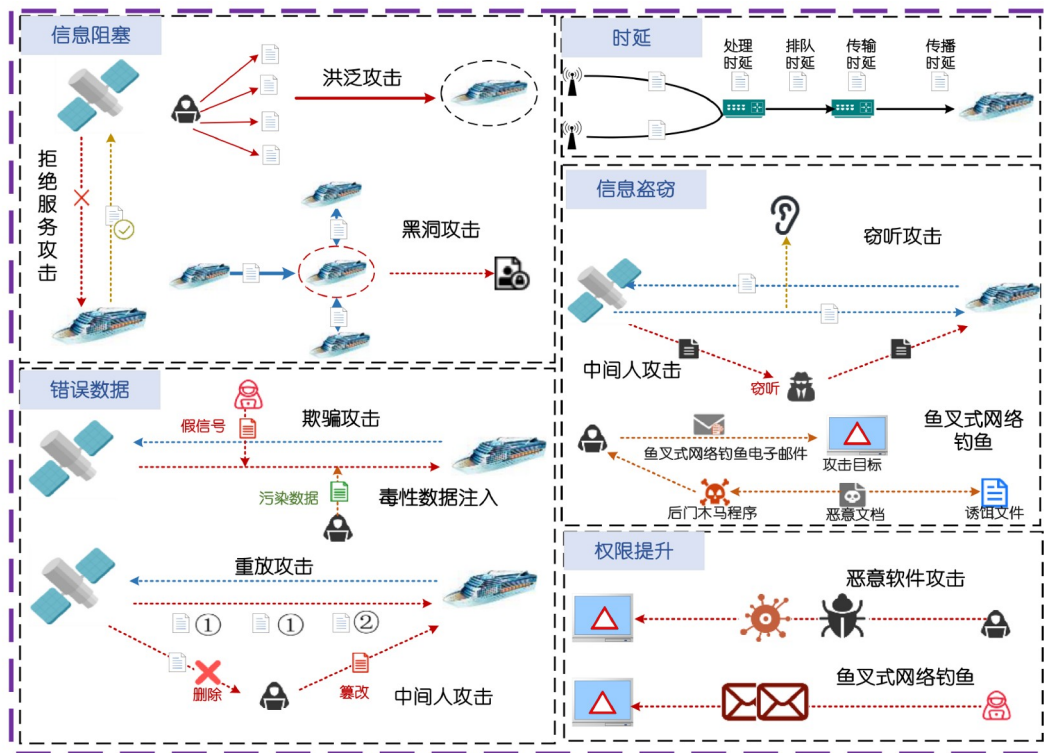


图 3 网络化船舶自主航行系统潜在网络安全威胁
Figure 3 Potential network security threat of networked vessel autonomous navigation system.

表 1 网络化船舶自主航行系统网络安全威胁概览
Table 1 Security threat summary of networked ship autonomous navigation system

可能遭受的安全威胁/攻击类型		攻击原理	攻击效果
信息阻塞	拒绝服务攻击	使用通信协议或物理脆弱性阻塞通信	导致网络资源对用户不可用
	洪泛攻击	占用通信资源	阻断正常通信
	黑洞攻击	利用恶意节点发送虚假路由信息	数据包丢失或通信中断
时延	—	不完全阻塞和阻塞后延迟释放消息	信息到达目标带有时延
虚假数据注入	毒性数据注入	发送错误数据给目标网络	干扰船舶的性能, 如增加碰撞风险
	欺骗攻击	诱使接收器从合法信号转移到欺骗信号	船舶进入错误位置
	重放攻击	发送记录的消息给通信网络	阻塞通信或误导船舶行为
	中间人攻击	拦截、篡改或伪造通信双方的数据, 向一方或双方传递错误信息	船舶接收错误的导航指令, 引发航行偏离、安全事故
信息盗窃	中间人攻击	中间节点窃听通信消息	发送给接收者的消息被丢弃或修改
	窃听攻击	攻击者分析船-船、船-岸通信中的内容, 获得私密的信息加以利用	窃取用户隐私和敏感信息
	鱼叉式网络钓鱼	伪造与船舶相关的可信通信, 诱导操作员或系统泄漏敏感信息	窃取私人信息
非法权限提升	恶意软件攻击	恶意软件获得了船舶、岸基设备的部分权限	侵犯隐私或攻击网络设备
	鱼叉式网络钓鱼	欺骗用户浏览恶意信息	发送恶意软件

其在需要高实时性能的定位信息时影响重大^[18]。船-船间通信网络中位置和速度信息的时延将导致交通减速、拥堵和吞吐量减少。船舶内部网络中传感器和控制信息的延迟传输可能导致船舶失控, 进而发生碰撞。

3.3 虚假数据注入

虚假数据在船舶自主航行系统中的传播, 违反了网络安全完整性要求。以毒性数据注入、欺骗攻击、重放攻击和中间人攻击为典型例子, 所有四种攻击都可以通过船舶内部网络和船-船、船-岸通信网络进行。以下是典型的虚假数据攻击路径、方法和攻击效果。

(1) 毒性数据注入: 构造虚假有害的信息投送到海事或船载系统的传感器, 使其做出错误决策从而导致不可预知后果^[19]。

(2) 欺骗攻击: 欺骗攻击主要通过注入虚假数据, 篡改控制器到执行器通道中的控制命令或传感器到控制器通道中的传感器测量。与DoS攻击相比, 欺骗攻击更复杂, 隐蔽性更强, 而且很难被一般的攻击检测机制检测^[20]。

(3) 重放攻击: 重放攻击的手段是截取有效的网络通信报文并重复向目标实体发送, 导致目标实体处理信息的状态紊乱或者无法接收最新信息^[20]。此类攻击无需修改新的数据信息, 只需将之前截取的数据包重新放入通信链路, 从而实现攻击。

(4) 中间人攻击: 其原理是通过在通信双方之间插入恶意第三方, 拦截并篡改有效的网络通信数据, 或伪造数据包后发送到目标实体, 从而破坏通信的完整性和保密性^[21]。

3.4 信息盗窃

信息窃取是一种利用漏洞和数据挖掘方法从船舶自主航行系统获取用户信息的网络攻击, 攻击方式包括中间人攻击、窃听攻击和鱼叉式网络钓鱼。

(1) 中间人攻击: 攻击者窃听通信, 然后试图删除或修改转发给接收方的信息内容^[7]。中间人攻击的前提是攻击者在两边的通信方之间放置一个恶意节点, 并在两边的通信中获得信任^[21]。

(2) 窃听攻击: 窃听攻击是通过监听无线媒体来实现, 此类攻击也被称为隐形攻击, 攻击者通过分析船-船、船-岸通信中的内容, 获得私密的信息加以利用^[22]。

(3) 鱼叉式网络钓鱼: 攻击者通过伪装成可信的实

体, 利用社交工程手段精心设计恶意邮件或消息, 引诱目标用户点击恶意链接或附件, 获取用户的敏感信息^[23]。

3.5 非法权限提升

非法权限提升是指攻击者试图获取比其正常权限更高级别的访问权限。这种攻击通常涉及利用系统或应用程序的漏洞, 获取对敏感数据或系统功能的未经授权访问, 攻击方式包括恶意软件攻击和鱼叉式网络钓鱼。

(1) 恶意软件攻击: 攻击者的主要目的是监控和窃取用户密码, 触发系统崩溃(如蓝屏)来干扰操作员, 从而获取进入系统或操作数据的非法权限^[23]。

(2) 鱼叉式网络钓鱼: 通过发送包含可疑链接的电子邮件来获取未经授权的访问权限。用户一旦点击这些链接, 黑客可能会安装键盘记录器以捕获登录名和密码, 进而识别每个工作人员的身份, 构建出系统端口状态的详细映射^[24]。

4 网络化船舶自主航行系统安全技术

为了有效抵御网络攻击带来的影响, 本文以网络攻击数学建模技术、网络安全态势感知技术、威胁建模与风险评估技术、网络攻击检测技术和弹性安全防护技术等关键内容为支撑, 全面保障船舶自主航行安全。如下简要概述上述关键技术进展情况。

4.1 网络攻击数学建模技术

网络攻击数学建模是理解并预测攻击行为的关键步骤, 能对攻击过程进行结构化和形式化描述, 有助于提高攻击检测和安全预警的效率。本文将详细介绍拒绝服务攻击、重放攻击和欺骗攻击等常见的网络攻击及其数学模型。

4.1.1 拒绝服务攻击数学建模

拒绝服务攻击(denial of service, DoS)通过干扰或占用系统资源, 使其无法提供正常的服务。典型的拒绝服务攻击包括间歇性拒绝服务攻击和随机拒绝服务攻击。

(1) 间歇性拒绝服务攻击

该类型攻击在特定时间间隔内发生^[25]。为了实施

间歇性DoS攻击, 攻击者必须访问船舶传感器和控制器之间的通信信道, 并发送干扰信号、洪泛数据包. 在实际攻击实施方面, 攻击者会受到硬件性能约束, 其硬件限制被建模为在特定时间间隔内的丢包调度^[26]. 攻击者依据数据包丢弃尝试的数量和连续数据包丢弃次数等条件来确定丢弃数据包的时隙.

(2) 随机拒绝服务攻击

由于DoS攻击而导致的数据包丢失也可以建模为随机过程. Qi等人^[27]考虑DoS攻击的随机性, 假设DoS攻击导致的丢包服从Bernoulli分布, 可用数据可表示为 $x(k) = \gamma \cdot x(k) + (1 - \gamma) \cdot x(k)$, 其中 γ 为服从Bernoulli分布的随机变量. 当 $\gamma = 1$ 时, 数据包传输成功(即未发生DoS攻击); 当 $\gamma = 0$ 时, 数据包传输失败(即发生DoS攻击). Wu等人^[28]考虑了能量有限约束的基本事实, 提出能量受限条件下的随机拒绝服务攻击. 在能量受限的随机拒绝服务攻击下, 采样数据包被阻断传输, 控制器无法获取当前采样数据, 这被看作是攻击引起的数据包丢失现象. Wu等人^[28]引入一组服从Bernoulli分布的随机变量, 描述攻击引起的丢包现象, 定义一个随机变量集 $\beta(s_k)$, 其中, $s_k \in S$, $S = \{s_0, s_1, s_2, \dots, s_k\}$ 为采样时刻. 当 $\beta(s_k) = 1$ 时, 表明没有攻击发生, 传感器采样数据成功传输到控制器; 反之, 当 $\beta(s_k) = 0$ 时, 采样数据包 $x(s_k)$ 由攻击者造成阻塞.

4.1.2 欺骗攻击数学建模

欺骗攻击也称为虚假数据注入攻击(false data injection, FDI), 主要通过注入虚假数据或重放历史数据等方式, 篡改控制命令或传感器测量值. 欺骗攻击数学建模分为以下三种情况.

(1) 针对控制器-执行器通道的欺骗攻击

该类攻击通过篡改控制命令直接影响系统正常运行. Zhang等人^[29]将欺骗攻击抽象为未知的加性信号, 那么由隐身欺骗性攻击建模的致动器输入信号为 $\tau_i^a = \tau_i^* + \zeta_i^\beta$, 其中 τ_i^* 为控制器输出指令, ζ_i^β 为虚假注入数据, 表示为 $\zeta_i^\beta = \delta_i^\beta \cdot \mu_i^\beta$, δ_i^β 是具有伯努利分布特性的攻击率伴随矩阵.

(2) 针对传感器-控制器通道的欺骗攻击

该类攻击通过操控传感器的测量值, 影响远程控制中心的观测性能, 并间接诱导错误的控制决策. Yao

等人^[30]假设欺骗攻击信号由非线性函数 $g(x(t))$ 表示, 引入伯努利随机变量 $\alpha(t)$ 描述随机发起的欺骗攻击, $\alpha(t) = 1$ 表示攻击者实施欺骗攻击, $\alpha(t) = 0$ 表示数据包正常传输.

(3) 针对控制器-执行器、传感器-控制器通道的欺骗攻击

与前面两种情形相比, 同时伪造控制命令和传感器测量值的欺骗攻击情形更具有破坏性. 针对装备水印检测模块的网络化水面无人航行器的隐身欺骗攻击设计问题, 为提高攻击性能, Kong和Yang^[31]设计了一种参数可调的指数欺骗信号模型, 并在不同条件下分析了其破坏性.

4.2 网络化船舶自主航行系统网络安全态势感知技术

网络安全态势感知(network security situational awareness, NSSA)是指通过收集和分析网络数据, 监测不同网络系统平台中的环境变化和网络内容, 对网络活动进行综合分析, 获得当前网络的安全态势. 从而, 及时发现网络威胁, 提高网络安全防范和响应能力, 确保网络系统稳定安全运行^[32]. 当前, 通常采用态势要素获取、态势评估和态势预测等三个功能模块来分类NSSA.

传统的网络安全态势感知技术模型通常包含三个核心过程: 感知、理解和预测(图4). 感知部分主要使用扫描工具、入侵检测系统(intrusion detection system, IDS)等工具来获取网络安全数据. 理解部分基于对海量数据的计算和处理, 从更高维度了解网络状况. 预测部分通过建立数学模型, 探索演化规律, 推理未来发展趋势. 当前大多数模型以传统模型的三层架构为基础, 进行了可视化补充, 实现对网络安全威胁的实时监控与分析.

尽管不同的研究者对如何划分NSSA的各个阶段持有不同的观点, 研究人员最常使用态势要素获取、态势评估和态势预测这三个功能模块来分类NSSA.

4.2.1 网络安全态势要素获取

态势要素获取是NSSA的基础. 通常, 情境要素主要包括网络的静态配置信息和动态信息. 前者包含网络拓扑结构、系统漏洞和当前状态等数据, 后者涉及通过网络收集的各种威胁数据和各种防御技术分析结

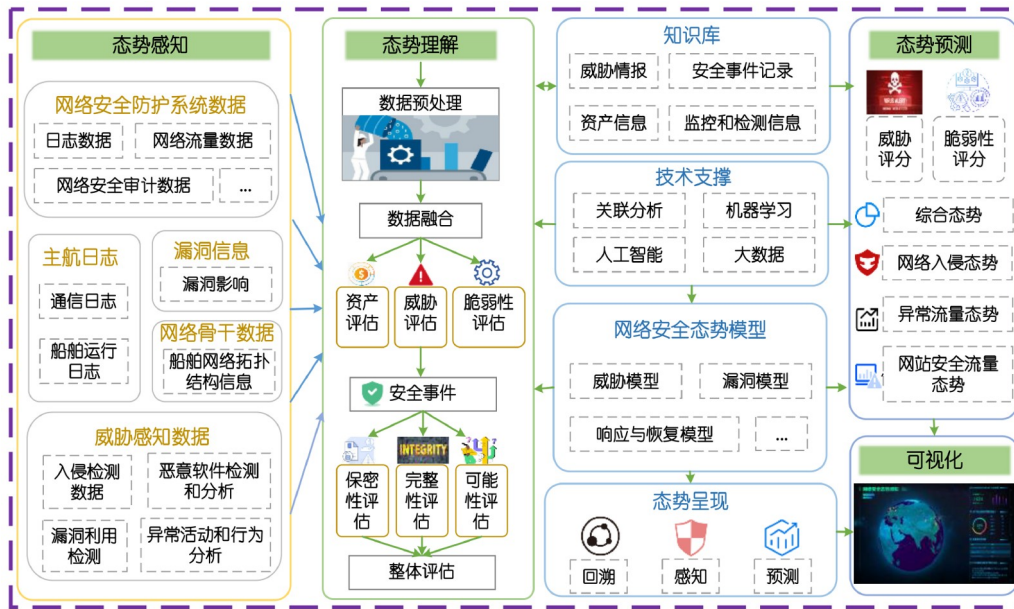


图 4 网络安全态势感知技术模型

Figure 4 Network security situational awareness technology model.

果。这些信息的有效整合为态势感知的高维抽象理解提供了基础。

安全数据的提取包括单元素和多源数据两个层次。从单个元素中提取主要用于漏洞信息、预警信息的特定数据。Barford等人^[33]使用从Honeynet中获得的攻击数据和威胁信息来评估网络状态,而Ning等人^[34]仅采集网络警报信息并检查警报信息的状态,就可以对网络的危险性进行评估。上述研究均收集、检查和研究了单个网络元素,难以获得完整的信息、了解整体情况或对复杂动态网络环境做出反应。

鉴于此,许多研究者的目标是从多个来源获取信息,从多个角度综合评估网络安全状况。Li等人^[35]提出了一种基于多源信息融合的异构网络嵌入方法,在非负矩阵分解框架下联合建模了结构邻近度、属性信息和标记信息。此外,对多源异构信息网络的安全性提取也开展了大量研究。Chang等人^[36]开发了一种基于概率神经网络的安全态势元素提取技术,解决了复杂网络环境下态势元素提取效率和准确性差的问题。

4.2.2 网络安全态势评估

网络安全态势评估是NSSA的关键环节,其最终目的是预测未来网络环境的变化,以提供管理框架,使网

络安全管理从被动变为主动。网络安全态势评估基于多个安全数据源,根据网络安全评估的具体要求,通过数学模型和形式逻辑推导出当前网络安全态势的评估值。典型的网络安全态势评估技术可分为三类:基于数学模型的技术、基于知识的推理技术和模式识别技术。

层次分析法(analytic hierarchy process, AHP)是最常用的基于数学模型的态势评估方法。代表性的研究成果是陈秀真等人^[37]提出的网络安全威胁态势定量评估模型,该模型从上到下分为四个级别:系统、主机、服务和攻击。但是,该模型存在一些不足:在评估方法中仅使用了IDS的报警信息。在真实的网络系统部署中,防火墙、系统日志等安全因素是不可或缺的。如果不包括来自多个来源的安全信息,则态势评估将丢失。为此,Wang等人^[38]对上述层次模型进行了优化,使更多来源的层次分析更加准确。

基于知识的推理方法是指在构建评估模型的过程中主要依靠专家的知识 and 经验对当前的网络安全态势进行分析。常见的基于知识的推理方法包括模糊逻辑推理、贝叶斯推理和证据理论。例如,为了评估网络安全状况,Alali等人^[39]提出利用模糊推理模型,根据脆弱性、威胁、可能性和影响四个风险因素生成

风险评估结果, 明确可能威胁任何实体的风险范围. 灰色关联方法、粗糙集理论和聚类分析方法是模式识别技术的例子. Zhuo等人^[40]将条件属性和决策规则相融合, 提出了一种基于粗糙集的网络安全态势评估模型.

4.2.3 网络安全态势预测

网络安全态势预测是根据历史信息和当前状况预测未来的发展趋势. 它是最高级别的全面态势感知, 在网络安全防御中起着至关重要的作用^[41]. 由于网络攻击具有随机性和不确定性, 网络安全态势的变化必然是一个复杂的非线性过程^[42]. Polatidis等人^[43]提出了一种利用海上供应链基础设施信息创建攻击图的方法, 该方法提供所有被网络攻击获取访问权限的可能路径.

博弈论方法试图确定玩家的最佳策略, 而不是历史数据中显示的最频繁的攻击进展, 与图形模型检查方法相反. Liu等人^[44]基于多源异构网络安全数据, 综合分析网络攻防状态下攻防双方的博弈过程, 提出攻防随机博弈模型的网络安全态势评估模型. Guo等人^[45]综合分析了安全态势要素的动态变化, 忽略了拓扑结构、服务信息等短期不会改变的态势要素, 提出了防御性随机博弈模型, 实验验证表明, 该预测方法能够提高预测精度, 更符合攻防场景.

4.3 网络化船舶自主航行系统威胁建模与风险评估技术

网络化船舶自主航行系统威胁建模与风险评估技术在海上活动的识别和早期缓解网络风险方面发挥着关键作用. 威胁建模是一种预防性方法, 能够识别海事系统内的潜在脆弱性. 威胁建模不仅仅是风险意识, 还提供了一个系统化的过程, 用于预测网络攻击可能发生的方式和地点^[46]. 而风险评估对这些已识别的网络威胁进行量化和优先排序, 为分配资源和实施保护措施提供战略依据^[47](图5).

4.3.1 威胁建模

威胁建模可以揭示船舶的GPS面临的潜在威胁, 如船舶被误导或导航中断, 通过预测船舶面临的威胁, 可以设计出更有针对性和更有效的网络安全措施. Enoch等人^[48]使用攻击树作为提出的海上船舶分层攻击表示模型的一部分, 以系统地识别海上船舶网络中的潜在攻击路径, 使用攻击图来可视化和分析海上网络安全中攻击向量的相互联系和相互依赖性. Sahay等人^[49]将STRIDE作为对潜在安全威胁进行深入分析的基本工具. 该方法使用数据流图创建系统模型, 全面审查压载水舱系统、发动机控制器和集成驾驶台控制器等关键系统组件. 此外, Bolbot等人^[50]通过流程图和安全评估矩阵, 分别分析了内河船舶导航系统和推进控

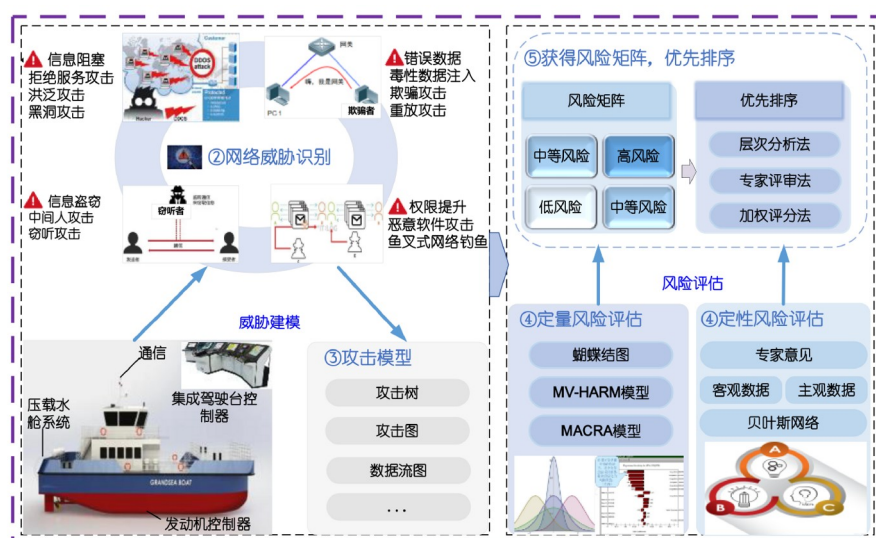


图5 网络威胁建模与风险评估流程图

Figure 5 Network threat modeling and risk assessment flow chart.

制系统的潜在网络攻击路径. Devkota和Dikshant^[51]利用STRIDE技术, 进行全面的威胁建模分析, 开发了针对海上自主水面舰艇的威胁建模框架.

4.3.2 风险评估

风险评估涉及将潜在的威胁和漏洞与系统的资产进行匹配, 评估其对系统安全的影响程度和可能造成的损失. 同时, 对不同的风险进行分类和排序, 确定优先处理的风险并采取相应的安全措施. 风险评估分为定量和定性两种.

(1) 定量风险评估

定量风险评估是指采用评分系统进行风险评估, 并为风险的概率和影响分配数值. Iphar等人^[52]利用专家知识进行AIS数据中的定量异常检测. 这项研究的优势在于, 独特地以AIS数据的完整性和真实性为中心, 利用专家知识和基于规则的分析来检测和评估海事数据中的网络威胁. 然而, 依赖专家意见可能导致冲突和忽视新的威胁. Bolbot等人^[53]提出了一种用于船舶系统网络安全风险评估的新方法, 通过使用经过调整的网络安全评估, 对已识别的危险进行排名, 从而量化了自主内河船舶的风险水平和不确定性. Papa-georgiou等人^[54]使用蝴蝶结图进行结构化定量海事安全风险评估. 与其他强调实际评估和特定船舶系统脆弱性扫描的方法不同, Svilicic等人^[55]结合了与船舶人员的直接接触和对船舶系统的技术分析, 评估网络风险. 与以往应用定量风险评估的研究不同, Amor和Gkioulos^[56]专门针对内河航道自动驾驶客船(APS)面临的独特挑战, 提出了相适应的网络风险管理策略. Tam和Jones^[57]提出了一种海上网络风险评估框架, 以应对任何可能的海上网络情景.

(2) 定性风险评估

定量风险评估的客观方法与依赖专家知识的定性风险评估形成对比, 突出了风险评估方法的差异. 定性风险评估是指使用专家意见和判断来确定航运业的网络安全风险, 根据风险的严重性和可能性确定高、中或低风险级别. 当面临复杂的网络威胁、没有太多可用数据或者理解风险需要人类的洞察力和经验时, 定性风险评估适用于应对新的和不断变化的网络威胁. Svilicic等人^[58]提出了一个风险评估框架, 用于评估影响船舶安全运行的网络风险. Chang等人^[59]提出的方法整合了客观数据和主观数据, 包括专家意见, 以解

决海事网络安全中不可靠的历史数据的挑战. Park等人^[60]构建了一个贝叶斯网络, 其中危害及其类别分别作为基础和约束元素, 最终将其结合起来形成最终的风险评估. Tusher等人^[61]有效地将BBWM整合到多标准决策框架中, 以解决网络安全问题. Amor和Gkioulos^[62]采用图论相关指标来确定已识别风险的影响, 结合故障模式、影响和关键性分析(FMECA)风险评估方法, 进行海事网络安全风险评估.

4.4 网络化船舶自主航行系统网络攻击检测技术

对网络化船舶自主航行系统, 日益复杂的网络威胁凸显了稳健的攻击检测和分类过程的重要性. 及时检测和分类网络攻击对于防止未经授权的访问、对关键系统的操纵以及可能危及这些自主船舶安全和功能的潜在中断至关重要^[63]. 网络攻击检测分为知识驱动和数据驱动两种, 表2列出了现有部分船舶自主航行系统网络攻击检测方法对比.

4.4.1 基于知识驱动的网络攻击检测技术

知识驱动的网络攻击检测技术是指利用领域知识、规则库和专家经验, 基于算法、统计学模型, 实现快速检测. Wu等人^[64]提出一种基于隐马尔可夫模型的船舶通信网络入侵信号识别方法, 对收集到的信道状态信息的特征值进行去噪和分类, 采用遗传算法对隐马尔可夫模型的初始参数进行优化, 解决模型对初始参数敏感的问题, 实验结果表明, 所提方法的最大识别准确率高达97.58%. Lan等人^[65]提出基于自适应模糊逻辑辅助的智能船舶网络脆弱性分析方法, 用于自主船舶入侵检测和信息管理. 结果表明, 与现有模型相比, 其提出的模型的数据传输率提高了99.2%, 攻击检测率提高了98.5%, 风险评估率提高了97.5%, 访问控制率提高了96.3%, 网络延迟率降低了11.4%. d'Afflisio等人^[66]提出了广义似然比检验和模型阶数选择方法, 用于从沿海雷达和星载卫星传感器等监测系统中获取可靠信息, 以支持检测AIS设备中异常、欺骗和隐身偏差.

4.4.2 基于数据驱动的网络攻击检测技术

数据驱动方法依托海量数据和人工智能技术, 强调从多源数据中提取特征, 利用深度学习和计算资源进行动态检测. 新一代人工智能技术的核心要素包括

表 2 网络攻击检测方法对比

Table 2 Comparison of network attack detection methods

主要技术	贡献	效果	缺点	文献
基于隐马尔可夫模型	解决了检测模型对初始参数敏感的问题	识别准确率高达97.58%	检测效率低	[64]
基于人工智能技术	为处理智能船舶网络中的不确定性和不精确性以及有效决策, 提供了一个框架	识别准确率高达98.5%	对复杂风险因素的综合评估仍然依赖于历史数据和已知攻击向量, 这可能限制了对新兴威胁的反应能力	[65]
基于广义似然比检验和模型顺序选择方法	可以从监控系统(海岸雷达和太空卫星传感器)中获取可靠信息	识别准确率高达90%	识别准确率低	[66]
基于深度学习算法	有效提高入侵数据位置判断准确性	识别准确率高达97.58%	检测效率低	[68]
基于深度学习算法	识别确切的威胁类型	识别准确率高达99%	对DLTIF框架评估时使用数据单一	[69]
基于边缘计算	实现渔船轨迹的实时异常检测	识别准确率高达92%	模型复杂度高、数据依赖性强	[70]
基于云计算	能够及时识别和应对船舶内外网络威胁	识别准确率达96.95%, 误报率2.56%	试验数量相对较少; 得出结论可能有些偏差; 用于检测的病毒样本类型不完整	[71]

数据、算法和计算能力^[67]. 网络攻击检测研究作为新一代人工智能技术在网络安全领域的应用之一, 分为数据、算法和计算能力三类. 数据层面的技术是多源数据融合方法; 算法层面的技术包括传统智能算法、深度学习、基于知识和数据驱动的集成; 计算能力层面的技术包括云计算和边缘计算.

数据驱动的网络攻击检测技术的核心在于对多源数据的融合和分析. 这些数据包括AIS、雷达、卫星传感器、通信信道状态信息以及网络日志等. 通过整合多源数据, 全面捕捉潜在的网络威胁, 为攻击检测提供更高的准确性和鲁棒性.

机器学习算法提供了一种动态和适应性强的方法来检测网络化船舶自主航行系统中的网络威胁, 实施有效的人工智能和机器学习技术对检测和缓解攻击至关重要. Xue^[68]将深度学习算法和云计算相结合, 有效提高入侵数据位置判断的准确性, 大大缩短数据特征提取所需的时间, 实现对入侵节点的准确识别和分类. Kumar等人^[69]开发了一个名为DLTIF的自动化框架, 用于建模网络威胁情报和识别威胁, DLTIF基于3种方案: 深度特征提取器、CTI驱动检测和CTI攻击类型识别, 结果表明, 该框架对病毒识别准确率高达99%.

计算能力是指设备处理数据以实现特定输出的能力, 并依赖于中央处理器、图形处理器和现场可编程门阵列等计算资源. Huang等人^[70]提出了一种基于边缘计算的渔船实时异常检测模型, 解决了通信延迟导致渔船异常预警不足的问题, 为传统渔船监控系统技

术升级提供了新途径. Guo和Guo^[71]在了解智能船舶网络运行模式的基础上深入研究了云计算技术的特点, 提出了一种基于云计算的智能船舶网络安全实时风险检测方法和防护策略, 结果表明, 提出的算法对病毒入侵的检测和防御率能够达到85%~95%, 有效提高了入侵检测的精度.

4.5 网络化船舶自主航行系统弹性安全防御技术

在攻击检测之后, 网络化船舶自主航行系统从控制和网络两个层面制定攻击处理和缓解策略, 以在攻击下提供可持续的服务. 网络化船舶自主航行系统弹性安全防护包括网络化船舶自主航行系统网络安全控制和网络管理, 如图6所示.

4.5.1 网络化船舶自主航行系统网络安全控制

随着计算技术的进步, 船舶自主航行系统可以处理控制输入信号和传感器测量, 其支持各种控制方法, 包括传感器测量和控制输入信号的非周期性控制和调制. 通过应用适当的控制方法, 网络化船舶自主航行系统可以抵抗一些已知的网络攻击. 如图6所示, 网络安全控制包含事件触发控制、协同控制及数据的编码和加密.

(1) 事件触发控制

事件触发控制(event-triggered control, ETC)是一种非周期性控制策略, 当特定事件发生时, 传输传感器测量值和控制输入信号^[72]. 在大多数情况下, 传感器

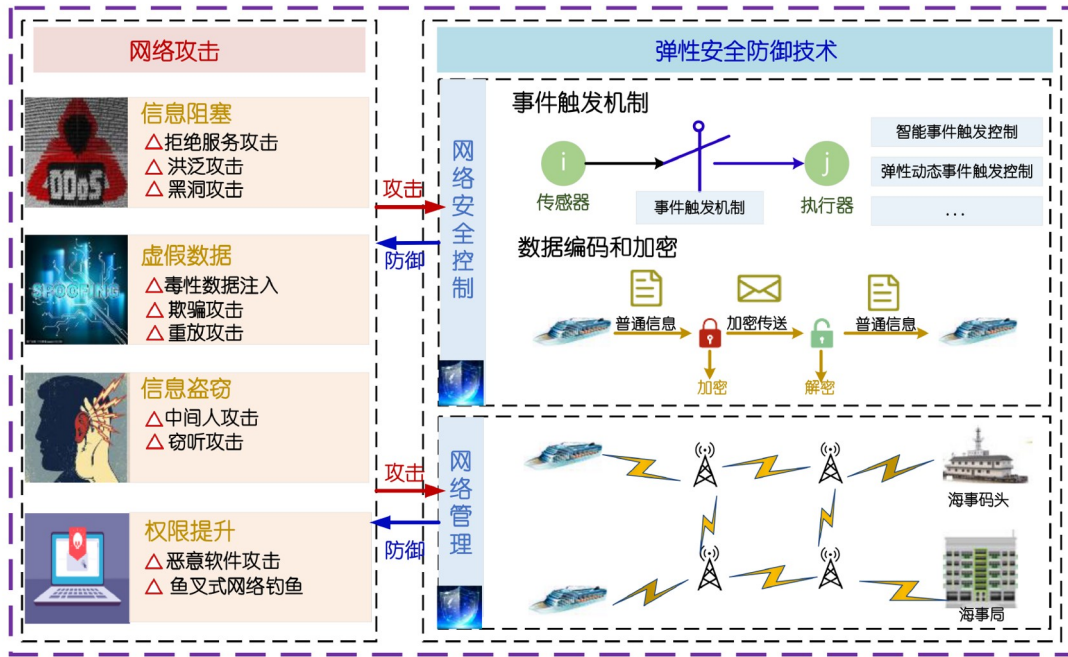


图 6 网络化船舶自主航行系统弹性安全技术图

Figure 6 Elastic safety technology diagram of networked vessel autonomous navigation system.

获得所有状态变量是困难的。因此, 将ETC策略应用于网络化船舶自主航行系统, 使其能够在网络化船舶自主航行系统中嵌入状态估计器以基于状态估计值触发事件。ETC仅在状态估计值满足触发函数中的稳定性条件时才交换传感器测量值和控制输入信号。以这种方式, ETC利用的网络资源明显少于周期性控制系统^[73]。

为有效利用有限的带宽资源, Chen等人^[74]提出了一种基于事件触发自适应滑模控制的新颖鲁棒分布式共识控制方案, 实现处理系统中的未知干扰同时避免Zeno行为。Song等人^[75]基于有限时间理论设计了模糊有限时间混合触发动态定位输出反馈控制器, 保证无人船舶控制系统在有限时间内稳定, 并达到 H_∞ 控制性能。李方昱等人^[76]设计了一种分布式事件触发优化控制方法, 使得多智能体在较好地完成任务的同时减少数据传输量, 达到优化通信机制、降低通信成本的目的。王涛等人^[77]利用变时域思想设计了自适应事件触发机制, 提出了多智能体系统跟踪一致的自适应事件触发分布式模型预测控制方法, 有效解决了在受扰多智能体系统跟踪问题中约束不满足和计算资源消耗问题。

从安全的角度来看, ETC为设计弹性网络化船舶

自主航行控制系统提供了优势。ETC策略在面对不可靠的通信信道和丢包时具有稳健性^[78]。Dong等人^[79]引入具有分段转换概率的分层半马尔可夫过程描述切换DoS攻击, 设计了一种带有对数量化器的自适应动态事件触发控制器, 提供更平滑的系统状态收敛, 更好地节省通信资源, 实现切换DoS攻击下船舶自主航行系统的有限时间动态定位。Ma等人^[80]提出了一种弹性动态事件触发控制器, 对抗DoS攻击, 减少不必要的数据传输, 提高有限资源的利用率, 保障船舶自主航行系统在传输延迟、外部干扰和非周期性DoS攻击存在的情况下达到稳定。Feng等人^[81]采用预测补偿器对网络攻击信号进行补偿, 减少网络攻击对系统的不利影响, 设计事件触发机制, 节省网络资源, 提出基于预测补偿器的事件触发控制策略, 使得船舶自主航行系统在外部分扰和DoS攻击下进行轨迹跟踪。Xu等人^[82]提出了一种周期事件触发自适应神经元跟踪控制方案, 降低了控制命令的传输频率, 缓解了重放攻击导致的芝诺问题。Ye等人^[83]建立了非线性无人船舶控制系统的随机切换T-S模糊系统模型, 提出了一种基于A3C算法的智能事件触发控制策略, 使得船舶自主航行系统在混合攻击下实现智能定位。

(2) 协同控制

当船舶自主航行系统出现故障, 如船舶主机故障后, 船舶自主航行系统控制性能下降. Ma等人^[84]提出一种基于事件触发的故障检测滤波器和事件触发控制器协同设计方案, 解决网络化船舶自主航行系统遭受通信延迟、外部干扰、执行器故障和拒绝服务攻击的问题. Liu等人^[85]提出了一种安全的协作路径跟踪控制方案, 使得即使在恶意的网络和物理攻击下多个自主水面航行器也可以成功地完成协作路径跟踪任务.

(3) 数据的编码和加密

先进的加密协议对于确保通信信道和数据的完整性也至关重要. 对自主航行船舶组件和外部系统之间传输的数据进行加密可以显著降低未经授权访问和数据操纵的风险^[86]. Yang等人^[87]提出了一种新的加密算法, 即改进的Hill加密算法, 解决了无人值守视频监控系统的的核心安全问题. Onishchenko等人^[88]提出了用于船舶信息系统的加密数据搜索引擎开发“危险”关键词识别的理论框架, 提高了船舶信息网络中机密数据的安全性. Liang等人^[89]提出了一种由安全和隐私保护的分布式脉冲估计器算法和局部非线性控制算法组成的信息物理框架, 解决了具有采样数据交互和外部干扰的网络化海洋水面航行器的协同编队跟踪问题. 张冲等人^[90]提出了一种具备隐私保护能力的多智能体系统弹性一致性算法, 在有效保护节点初始状态信息隐私的同时保证系统实现弹性一致性收敛.

4.5.2 网络管理策略

虽然网络攻击是以控制理论的方式检测到的, 但是实际恢复攻击是在满足来自船舶自主航行系统最后期限约束的网络上执行的. 因此, 网络化船舶自主航行系统的网络状态应该被实时监控, 并提供灵活的网络服务应对攻击.

软件定义网络(software defined network, SDN)是一种新的网络范例, 其将控制平面和数据平面与具有软件的传统网络设备分离, 如图7所示. 在SDN中, 控制平面和数据平面都是可编程的^[91]. SDN网络由集中式SDN控制器和多个SDN交换机组成. SDN控制器监控网络并提供各种网络服务. SDN交换机基于来自SDN控制器的转发规则进行转发分组. SDN控制器和SDN交换机之间的互连由诸如OpenFlow的应用程序接口支持. 控制平面上的SDN控制器周期性地收集网

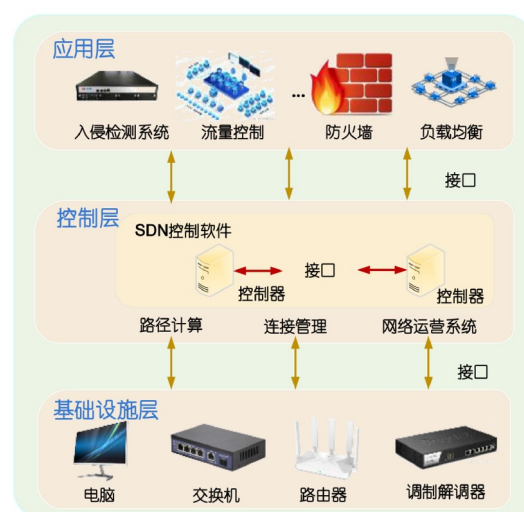


图7 软件定义网络结构

Figure 7 Software defined network structure.

络信息, 包括来自SDN交换机中每个链路的业务负载. SDN控制器还在数据平面上的每个SDN交换机上安装转发规则, 以提供诸如服务质量保证^[92]、灵活路由^[93]和负载均衡^[94]的网络服务. 数据平面上的SDN交换机将每个交换机的网络状态发送给集中式SDN控制器, 并根据SDN控制器的转发规则转发报文^[94]. SDN网络可以通过各种网络应用程序和SDN交换机编程来减轻恶意流量洪泛DDoS攻击的影响. Sahay等人^[95]提出了CyberShip-IoT框架, 为船舶系统的通信网络组件提供网络级防御. Yang等人^[96]提出了一种基于休眠调度和机会传输的优化分配方案, 实现在能耗和延迟间的最佳平衡.

5 网络化船舶自主航行系统安全技术的挑战与展望

船舶自主航行系统网络安全对于保护关键的海事基础设施至关重要. 在全球海上水面自主船舶快速发展的背景下, 尤其需要保护通信网络、导航系统和机载计算组件. 针对船舶自主航行系统的安全问题, 未来重点从以下五个方面开展进一步探索.

(1) 网络攻击数学建模技术

当前许多研究引入一些不合实际的特定假设, 如周期性、概率分布等, 与现实中的网络攻击实际情况不符. 这些假设违背了攻击通常是任意和隐蔽的事实.

例如, 由拒绝服务攻击引起的数据包丢失可能不遵循伯努利分布. 基于这种同实际有较大偏差的假设, 已有的部分结果难以应用到实践中去. 为此, 需要以更真实的方式, 对船舶航行系统遭遇到的网络攻击进行数学建模. 并考虑集成多种攻击模式的综合建模, 以更全面地理解网络安全威胁的变化, 能够实时反映网络环境的变化.

(2) 网络安全态势感知技术

网络安全态势提取所面临的数据源具有海量异构的特点, 亟需研究数据融合方法, 实现对海量异构数据高效、准确的处理. 同时, 应当开发面向船舶自主航行系统的网络安全态势感知软硬件系统, 以更直观、更清晰地了解网络安全每个环节, 掌握网络安全形式, 实现安全形势实时可视化. 此外, 应建立人机交互机制与人员辅助决策系统, 实现智能高效的自动响应与认知意识控制.

(3) 威胁建模与风险评估技术

随着信息技术的快速发展, 高度自动化的船舶将通过无线电频率或卫星通信传输大量数据, 这使其容易受到网络物理空间的各种现有威胁和风险的影响. 考虑到网络威胁具有复杂、动态的特点, 设计适用的动态方法对网络安全风险进行实时评估. 同时, 未来的海上网络安全风险评估将朝着统一化和结构化的方向发展, 通过明确威胁建模和风险评估过程, 定义清晰的目标和方法, 解决当前基于非结构化威胁列表导致的范围不完整问题, 提升海上网络安全环境的透明度和效率, 为复杂多变的船舶自主航行系统网络安全问题提供更加系统化的解决方案. 此外, 未来的海上网络安全研究将重点关注专家知识边缘的系统验证, 结合经验数据分析、同行评审, 以确保专家见解的可行度和有效性.

(4) 网络攻击检测技术

高级持续性威胁(advanced persistent threat, APT)攻击快速演变, 呈现出攻击工具更专业、攻击方式更

智能和攻击策略更多变的趋势, 使得现有检测方法难以应对. 为此, 为应对APT攻击中的未知特征, 需要引入迁移学习、元学习和度量学习等先进技术来检测具有未知特征的APT攻击. 同时, 结合零信任网络架构, 对船-船、船-岸通信的每个用户、设备 and 应用进行身份验证和访问控制, 降低内部攻击风险. 此外, 为检测来自网络内部或外部的未经授权的访问或恶意攻击, 有必要引入船舶内部网络的IDS. 未来将考虑用于船舶系统之间通信的NMEA协议, 检测由于自主船舶的高连接性而可能发生的恶意访问和外部攻击者的异常情况, 并考虑船舶网络的特性来保护网络.

(5) 弹性安全防御技术

在主动防御的背景下, 数据的稀疏性和传输间隔的不确定性严重影响了所开发方法的适用性. 同时, 在数字化环境下, 如何安全地存储、传输和处理船舶产生的大量数据是一个关键问题. 未来将深入研究量子安全加密技术和区块链技术, 以确保网络安全措施的持久弹性, 保护船舶自主航行系统免受基于量子的安全威胁, 加强自主航行系统关键数据和通信的可信度. 同时应用控制理论和通信网络安全技术, 支持网络化船舶自主航行系统的弹性功能, 保障系统稳定性. 此外, 如果无法精确获得系统模型参数, 则开展基于数据驱动的安全控制亦是值得探究的课题.

6 总结

随着物联网、大数据等新技术在航运业和船舶工业的广泛应用, 船舶自主化、无人化、网络化、信息化的进程快速发展, 网络化船舶自主航行系统的安全性成为关键. 通过研究网络攻击数学建模、网络安全态势感知、威胁建模和风险评估、网络攻击检测、弹性安全防护关键技术, 可以有效提升网络化船舶自主航行系统的安全技术水平, 推动更高等级的自主船舶研发和落地.

参考文献

- 1 Negenborn R R, Goerlandt F, Johansen T A, et al. Autonomous ships are on the horizon: Here's what we need to know. *Nature*, 2023, 615: 30–33
- 2 Witbooi E, Ali K D, Santosa M A, et al. Organized crime in the fisheries sector threatens a sustainable ocean economy. *Nature*, 2020, 588: 48–56
- 3 Cho S, Orye E, Visky G, et al. Cybersecurity considerations in autonomous ships. Technical Report. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2022

- 4 Kim M, Joung T H, Jeong B, et al. Autonomous shipping and its impact on regulations, technologies, and industries. *J Int Marit Saf Environ Aff Ship*, 2020, 4: 17–25
- 5 Veitch E, Andreas Alsos O. A systematic review of human-AI interaction in autonomous ship systems. *Saf Sci*, 2022, 152: 105778
- 6 Lynch K M, Banks V A, Roberts A P J, et al. What factors may influence decision-making in the operation of maritime autonomous surface ships? A systematic review. *Theor Issues Ergon Sci*, 2024, 25: 98–142
- 7 Wang Y, Ye T, Li T W, et al. Cyberspace security for autonomous ship navigation system: Challenges and explorations (in Chinese). *Huazhong Univ of Sci & Tech (Natural Science Edition)*, 2023, 51: 64–76 [汪洋, 叶挺, 李廷文, 等. 自主船舶航行系统信息空间安全: 挑战与探索. 华中科技大学学报(自然科学版), 2023, 51: 64–76]
- 8 Xia M H, Zhu Y M, Chen E H, et al. The state of the art and challenges of marine communications (in Chinese). *Sci Sin Inf*, 2017, 47: 677–695 [夏明华, 朱又敏, 陈二虎, 等. 海洋通信的发展现状与时代挑战. 中国科学: 信息科学, 2017, 47: 677–695]
- 9 Thombre S, Zhao Z, Ramm-Schmidt H, et al. Sensors and AI techniques for situational awareness in autonomous ships: A review. *IEEE Trans Intell Transp Syst*, 2020, 23: 64–83
- 10 Ma Y, Wang W Q, Yan X P. Research progress of vessel intelligent navigation technology for the new generation of waterborne transportation system (in Chinese). *Sci Sin Tech*, 2023, 53: 1795–1806 [马勇, 王雯琦, 严新平. 面向新一代航运系统的船舶智能航行技术研究进展. 中国科学: 技术科学, 2023, 53: 1795–1806]
- 11 Tsou M C. Multi-target collision avoidance route planning under an ECDIS framework. *Ocean Eng*, 2016, 121: 268–278
- 12 Su Y X, Liu Y J, Long F. Overview on ship cyber security (in Chinese). *Mar Electr Electron Eng*, 2018, 38: 11–14, 18 [苏义鑫, 刘宇杰, 龙飞. 船舶网络安全综述. 船电技术, 2018, 38: 11–14, 18]
- 13 Wu Z D, Han D Z, Jiang H B, et al. Review of marine ship communication cybersecurity (in Chinese). *J Comput Appl*, 2024, 44: 2123–2136 [吴中岱, 韩德志, 蒋海豹, 等. 海洋船舶通信网络安全综述. 计算机应用, 2024, 44: 2123–2136]
- 14 Khan M K, Quadri A. Augmenting cybersecurity in autonomous vehicles: Innovative recommendations for aspiring entrepreneurs. *IEEE Consumer Electron Mag*, 2020, 10: 111–116
- 15 Han J, Ju Z, Chen X, et al. Secure operations of connected and autonomous vehicles. *IEEE Trans Intell Veh*, 2023, 8: 4484–4497
- 16 Cherkaoui B, Beni-hssane A, Erritali M. Variable control chart for detecting black hole attack in vehicular ad-hoc networks. *J Ambient Intell Hum Comput*, 2020, 11: 5129–5138
- 17 Gurung S, Chauhan S. A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. *Wireless Netw*, 2020, 26: 1981–2011
- 18 Ma Y, Nie Z, Yu Y, et al. Event-triggered fuzzy control of networked nonlinear underactuated unmanned surface vehicle. *Ocean Eng*, 2020, 213: 107540
- 19 Luo Q, Cao Y, Liu J, et al. Localization and navigation in autonomous driving: Threats and countermeasures. *IEEE Wireless Commun*, 2019, 26: 38–45
- 20 Pang Z, Fu Y, Guo H, et al. Analysis of stealthy false data injection attacks against networked control systems: Three case studies. *J Syst Sci Complex*, 2023, 36: 1407–1422
- 21 Ahmad F, Kurugollu F, Adnane A, et al. MARINE: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet Things J*, 2020, 7: 3310–3322
- 22 Irshad A, Usman M, Ashraf Chaudhry S, et al. A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework. *IEEE Trans Ind Applicat*, 2020, 56: 4425
- 23 Parkinson S, Ward P, Wilson K, et al. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Trans Intell Transp Syst*, 2017, 18: 2898–2915
- 24 Kumari D, Sinha A, Dutta S, et al. Optimizing neural networks using spider monkey optimization algorithm for intrusion detection system. *Sci Rep*, 2024, 14: 17196
- 25 Feng S, Tesi P. Networked control systems under Denial-of-Service: Co-located vs. remote architectures. *Syst Control Lett*, 2017, 108: 40–47
- 26 Cetinkaya A, Ishii H, Hayakawa T. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, 2019, 21: 210
- 27 Qi W, Zhang N, Zong G, et al. Asynchronous sliding-mode control for discrete-time networked hidden stochastic jump systems with cyber attacks. *IEEE Trans Cybern*, 2023, 54: 1934–1946

- 28 Wu J, Peng C, Zhang J, et al. A sampled-data-based secure control approach for networked control systems under random DoS attacks. *IEEE Trans Cybern*, 2024, 54: 4841–4851
- 29 Zhang Q, Zhang S, Liu Y, et al. Adaptive terminal sliding mode control for USV-ROVs formation under deceptive attacks. *Front Mar Sci*, 2024, 11: 1320361
- 30 Yao L, Huang X, Wang Z, et al. Secure control of markovian jumping systems under deception attacks: An attack-probability-dependent adaptive event-triggered mechanism. *IEEE Trans Control Netw Syst*, 2023, 10: 1818–1830
- 31 Kong X Y, Yang G H. Anti-watermarking stealthy deception attacks against networked unmanned surface vehicles. *IEEE Trans Intell Transp Syst*, 2024, 25: 12835–12840
- 32 Bajracharya C. Performance evaluation for secure communications in mobile internet of vehicles with joint reactive jamming and eavesdropping attacks. *IEEE Trans Intell Transp Syst*, 2021, 23: 22563–22570
- 33 Barford P, Chen Y, Goyal A, et al. Employing Honeynets for Network Situational Awareness. Boston: Springer US, 2009. 71–102
- 34 Ning P, Cui Y, Reeves D S, et al. Techniques and tools for analyzing intrusion alerts. *ACM Trans Inf Syst Secur*, 2004, 7: 274–318
- 35 Li B, Pi D, Lin Y, et al. Multi-source information fusion based heterogeneous network embedding. *Inf Sci*, 2020, 534: 53–71
- 36 Li F W, Wang S, Zhu J, et al. Security situation element acquisition based on enhanced probabilistic neural network (in Chinese). *Telecom Eng*, 2017, 57: 64–71 [李方伟, 王森, 朱江, 等. 基于增强型概率神经网络的安全态势要素获取. 电讯技术, 2017, 57: 64–71]
- 37 Chen X Z, Zheng Q H, Guan X H, et al. Quantitative hierarchical threat evaluation model for network security (in Chinese). *J Software*, 2006, 17: 885–897 [陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法. 软件学报, 2006, 17: 885–897]
- 38 Wang H, Zhao D, Li X. Research on network security situation assessment and forecasting technology. *J Web Eng*, 2020, 19: 1239–1266
- 39 Alali M, Almogren A, Hassan M M, et al. Improving risk assessment model of cyber security using fuzzy logic inference system. *Comput Security*, 2018, 74: 323–339
- 40 Zhuo Y, He M, Gong Z. A rough set analysis model of network situation assessment (in Chinese). *Comput Eng Sci*, 2012, 34: 1–8 [卓莹, 何明, 龚正虎. 网络态势评估的粗糙集分析模型. 计算机工程与科学, 2012, 34: 1–8]
- 41 Wu S, Rendall J B, Smith M J, et al. Survey on prediction algorithms in smart homes. *IEEE Internet Things J*, 2017, 4: 636–644
- 42 Ebazadeh Y, Fotohi R. A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold. *Security Privacy*, 2022, 5: 183
- 43 Polatidis N, Pimenidis E, Pavlidis M, et al. From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. *Evolving Syst*, 2020, 11: 479–490
- 44 Liu J Y, Weng F Y, Zhang R, et al. A network security situation assessment method based on a random game model of attack and defense (in Chinese). CN Patent, 201710942981.5, 2024-05-24 [刘建毅, 翁芳雨, 张茹, 等. 一种基于攻防随机博弈模型的网络安全态势评估方法. 中国专利, 201710942981.5, 2024-05-24]
- 45 Guo X, Yang J, Gang Z, et al. Research on network security situation awareness and dynamic game based on deep Q learning network. *J Internet Technol*, 2023, 24: 549–563
- 46 Yu H, Meng Q, Fang Z, et al. Literature review on maritime cybersecurity: State-of-the-art. *J Navigation*, 2023, 76: 453–466
- 47 Huang X, Wen Y, Zhang F, et al. A review on risk assessment methods for maritime transport. *Ocean Eng*, 2023, 279: 114577
- 48 Enoch S Y, Lee J S, Kim D S. Novel security models, metrics and security assessment for maritime vessel networks. *Comput Netws*, 2021, 189: 107934
- 49 Sahay R, Estay D A S, Meng W, et al. A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. *Comput Security*, 2023, 128: 103179
- 50 Bolbot V, Theotokatos G, Wennersberg L A, et al. A novel risk assessment process: Application to an autonomous inland waterways ship. *Proc Inst Mech Eng O J Risk Reliab*, 2023, 237: 436–458
- 51 Dikshant D. Cybersecurity: Threat modeling of maritime autonomous surface ship. Dissertation for Master's Degree. Stavanger: University of Stavanger, 2024
- 52 Iphar C, Napoli A, Ray C. An expert-based method for the risk assessment of anomalous maritime transportation data. *Appl Ocean Res*, 2020, 104: 102337
- 53 Bolbot V, Theotokatos G, Boulougouris E, et al. A novel cyber-risk assessment method for ship systems. *Saf Sci*, 2020, 131: 104908
- 54 Papageorgiou P, Dermatis Z, Anastasiou A, et al. Using a proposed risk computation procedure and bow-tie diagram as a method for maritime

- security assessment. *Transp Res Record-J Transp Res Board*, 2024, 2678: 318–339
- 55 Svilicic B, Kamahara J, Rooks M, et al. Maritime cyber risk management: An experimental ship assessment. *J Navigation*, 2019, 72: 1108–1120
- 56 Amro A, Gkioulos V. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *Int J Inf Secur*, 2023, 22: 249–288
- 57 Tam K, Jones K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J Marit Affairs*, 2019, 18: 129–163
- 58 Svilicic B, Kamahara J, Celic J, et al. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU J Marit Affairs*, 2019, 18: 509–520
- 59 Chang C H, Kontovas C, Yu Q, et al. Risk assessment of the operations of maritime autonomous surface ships. *Reliab Eng Syst Saf*, 2021, 207: 107324
- 60 Park C, Kontovas C, Yang Z, et al. A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean Coast Manage*, 2023, 235: 106480
- 61 Tusher H M, Munim Z H, Notteboom T E, et al. Cyber security risk assessment in autonomous shipping. *Marit Econ Logist*, 2022, 24: 208–227
- 62 Amro A, Gkioulos V. Evaluation of a cyber risk assessment approach for cyber-physical systems: Maritime- and energy-use cases. *J Mar Sci Eng*, 2023, 11: 744
- 63 Tang D, Gao C, Li X, et al. A detection and mitigation scheme of LDoS attacks via SDN based on the FSS-RSR algorithm. *IEEE Trans Netw Sci Eng*, 2023, 10: 1952–1963
- 64 Wu W. Ship communication network intrusion signal identification based on Hidden Markov model. *J Coast Res*, 2018, 83: 868
- 65 Lan D, Xu P, Nong J, et al. Application of artificial intelligence technology in vulnerability analysis of intelligent ship network. *Int J Comput Intell Syst*, 2024, 17: 147
- 66 d’Afflisio E, Braca P, Willett P. Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Trans Aerosp Electron Syst*, 2021, 57: 2093–2108
- 67 Sadeeq M M, Abdulkareem N M, Zeebaree S R M, et al. IoT and cloud computing issues, challenges and opportunities: A review. *Qubahan Acad J*, 2021, 1: 1–7
- 68 Xue D. Research on identification of illegal intrusion in ship communication network based on depth learning algorithm. *J Coast Res*, 2020, 115: 127–129
- 69 Kumar P, Gupta G P, Tripathi R, et al. DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Trans Intell Transp Syst*, 2021, 24: 2472–2481
- 70 Huang J, Zhu F, Huang Z, et al. Research on real-time anomaly detection of fishing vessels in a marine edge computing environment. *Mobile Inf Syst*, 2021, 2021: 5598988
- 71 Guo J, Guo H. Real-time risk detection method and protection strategy for intelligent ship network security based on cloud computing. *Symmetry*, 2023, 15: 988
- 72 Peng C, Li F. A survey on recent advances in event-triggered communication and control. *Inf Sci*, 2018, 457: 113–125
- 73 Cuenca A, Antunes D J, Castillo A, et al. Periodic event-triggered sampling and dual-rate control for a wireless networked control system with applications to UAVs. *IEEE Trans Ind Electron*, 2018, 66: 3157–3166
- 74 Chen T, Zhuang X, Hou Z, et al. Event-triggered adaptive sliding mode control for consensus of multiagent systems with unknown disturbances. *Sci Rep*, 2022, 12: 17473
- 75 Song W, Li Y, Tong S. Fuzzy finite-time H_∞ hybrid-triggered dynamic positioning control of nonlinear unmanned marine vehicles under cyber-attacks. *IEEE Trans Intell Veh*, 2024, 9: 970–980
- 76 Li F Y, Liu J Y, Huang Y T, et al. Multi-agent distributed event-triggered optimization control based on deep reinforcement learning (in Chinese). *Sci Sin Tech*, 2024, 54: 1991–2002 [李方昱, 刘金溢, 黄琰婷, 等. 基于深度强化学习的多智能体分布式事件触发优化控制. 中国科学: 技术科学, 2024, 54: 1991–2002]
- 77 Wang T, Kang Y, Li P F. Adaptive event-triggered distributed model predictive control for tracking consensus of multiagent systems (in Chinese). *Sci Sin Tech*, 2023, 53: 1885–1894 [王涛, 康宇, 李鹏飞. 基于自适应事件触发分布式模型预测控制的多智能体系统跟踪一致性. 中国科学: 技术科学, 2023, 53: 1885–1894]
- 78 Cetinkaya A, Ishii H, Hayakawa T. Networked control under random and malicious packet losses. *IEEE Trans Automat Contr*, 2016, 62: 2434–2449

- 79 Dong J, Ye Z, Zhang D. Finite-time security control of networked unmanned marine vehicle systems subject to DoS attack. *IEEE Trans Intell Veh*, 2024, 9: 3464–3477
- 80 Ma Y, Qi X, Li Z, et al. Resilient control for networked unmanned surface vehicles with dynamic event-triggered mechanism under aperiodic DoS attacks. *IEEE Trans Veh Technol*, 2023, 73: 5824–5833
- 81 Feng N, Wu D, Yu H, et al. Predictive compensator based event-triggered model predictive control with nonlinear disturbance observer for unmanned surface vehicle under cyber-attacks. *Ocean Eng*, 2022, 259: 111868
- 82 Xu Z, Zhu G, Xu Y, et al. Periodic event-triggered adaptive neural control of USVs under replay attacks. *Ocean Eng*, 2024, 306: 118022
- 83 Ye Z, Zhang D, Wu Z G, et al. A3C-based intelligent event-triggering control of networked nonlinear unmanned marine vehicles subject to hybrid attacks. *IEEE Trans Intell Transp Syst*, 2021, 23: 12921–12934
- 84 Ma Y, Nie Z, Hu S, et al. Fault detection filter and controller co-design for unmanned surface vehicles under DoS attacks. *IEEE Trans Intell Transp Syst*, 2020, 22: 1422–1434
- 85 Liu Z Q, Ge X, Han Q L, et al. Secure cooperative path following of autonomous surface vehicles under cyber and physical attacks. *IEEE Trans Intell Veh*, 2023, 8: 3680–3691
- 86 Singh S, Sharma P K, Moon S Y, et al. Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *J Ambient Intell Hum Comput*, 2024, 15: 1625–1642
- 87 Yang T, Li Y, Lai C, et al. The improved hill encryption algorithm towards the unmanned surface vessel video monitoring system based on Internet of Things technology. *Wireless Commun Mob Comput*, 2018, 2018: 5183451
- 88 Onishchenko O, Shumilova K, Volyanskyy S, et al. Ensuring cyber resilience of ship information systems. *TransNav*, 2022, 16: 43–50
- 89 Liang C D, Ge M F, Xu J Z, et al. Secure and privacy-preserving formation control for networked marine surface vehicles with sampled-data interactions. *IEEE Trans Veh Technol*, 2021, 71: 1307–1318
- 90 Zhang C, Wu Y M, Xu M, et al. Resilient consensus control of multi-agent systems under privacy protection (in Chinese). *Sci Sin Inform*, 2024, 54: 927–943 [张冲, 伍益明, 徐明, 等. 隐私保护下的多智能体系统弹性一致性控制. 中国科学: 信息科学, 2024, 54: 927–943]
- 91 Hu F, Hao Q, Bao K. A survey on software-defined network and openflow: From concept to implementation. *IEEE Commun Surv Tutor*, 2014, 16: 2181–2206
- 92 Lee K, Kim M, Park T, et al. MC-SDN: Supporting mixed-criticality real-time communication using software-defined networking. *IEEE Internet Things J*, 2019, 6: 6325–6344
- 93 Yang H, Zhan K, Kadoch M, et al. BLCS: Brain-like distributed control security in cyber physical systems. *IEEE Netw*, 2020, 34: 8–15
- 94 Sood K, Yu S, Xiang Y. Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. *IEEE Internet Things J*, 2016, 3: 453–463
- 95 Sahay R, Meng W, Estay D A S, et al. CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Gener Comput Syst*, 2019, 100: 736–750
- 96 Yang T, Kong L, Zhao N, et al. Efficient energy and delay tradeoff for vessel communications in SDN based maritime wireless networks. *IEEE Trans Intell Transp Syst*, 2021, 22: 3800–3812

Research progress on cybersecurity technology for networked autonomous ship navigation systems

MA Yong^{1,2,3,4}, HU RuiDie^{1,2,3}, HU SongLin⁵ & ZHAO YuJiao⁶

¹ State Key Laboratory of Maritime Technology and Safety, Wuhan University of Technology, Wuhan 430063, China

² School of Navigation, Wuhan University of Technology, Wuhan 430063, China

³ Hubei Key Laboratory of Inland Shipping Technology, Wuhan 430063, China

⁴ National Engineering Research Center for Water Transport Safety, Wuhan 430063, China

⁵ Institute of Advanced Technology for Carbon Neutrality, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

⁶ School of Information Science and Engineering, University of Jinan, Jinan 250022, China

The networked autonomous ship navigation system utilizes advanced information technology and autonomous control technology to enable ship navigation, remote monitoring, and management with minimal or no human intervention. As digital connectivity between ships and between ships and the shore continues to expand, cybersecurity has become a key research topic in the maritime transport sector. To understand the current development trends and advancements in autonomous ship navigation systems, this review summarizes the progress in cybersecurity technology research. It introduces five key cybersecurity threats related to autonomous ship navigation systems: information blocking, latency, false data, information theft, and privilege escalation. It also discusses cybersecurity countermeasures, including network attack mathematical modeling technology, cybersecurity situational awareness technology, risk collaborative assessment technology, network attack detection technology, and resilient security defense technology. Furthermore, it examines the opportunities and challenges associated with cybersecurity in autonomous ship navigation systems.

networked autonomous ship navigation system, cyber attacks, attack mode, safety technology

doi: [10.1360/SST-2024-0313](https://doi.org/10.1360/SST-2024-0313)