Securing Unmanned Surface Vehicles: Addressing Cyber-Physical Threats in Maritime Autonomy

Guangrui Bian

School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
15151818811@163.com

Abstract. The growing use of unmanned surface vehicles (USVs) in maritime operations has introduced new efficiencies but also exposed significant cybersecurity risks. As autonomous vessels increasingly rely on interconnected networks for navigation, communication, and decision-making, they become prime targets for cyberattacks. This paper investigates the vulnerabilities of USVs, emphasizing the cyber-physical threats that could lead to navigational errors, data breaches, and even adversarial control of vessels. We propose a cybersecurity framework designed to safeguard the operational integrity of USVs by integrating resilient communication protocols, real-time threat detection, and autonomous response mechanisms.

Keywords: Unmanned surface vehicles, cyber-physical security, maritime autonomy, GPS spoofing, encrypted communication, autonomous defense systems.

Introduction:

As unmanned surface vehicles (USVs) take on more critical roles in maritime operations, their cybersecurity has emerged as a pressing concern. Whether deployed for environmental monitoring, cargo transport, or military applications, USVs operate within complex cyber-physical environments that rely heavily on interconnected systems. These systems include onboard sensors, communication networks, navigation tools, and automated decision-making algorithms, all of which can be vulnerable to cyberattacks. The unique operating conditions of USVs—ranging from harsh maritime environments to remote, data-intensive missions—further complicate their security needs.

Cybersecurity for USVs is particularly challenging because their systems are often exposed to multiple attack vectors. These vehicles rely on GPS for navigation, wireless communication for control, and cloud-based data platforms for mission updates. If any of these components are compromised, the USV's mission can be disrupted or redirected, potentially with disastrous consequences. Additionally, the remote and autonomous nature of USVs makes them difficult to monitor in real time, requiring sophisticated, automated defense mechanisms that can detect and mitigate threats without human intervention.

This paper explores the multi-faceted cybersecurity threats that target USVs and proposes a defense-in-depth strategy tailored to their unique needs. Our approach combines proactive threat detection, encrypted communications, and autonomous response systems to ensure the secure operation of USVs in diverse maritime environments. By addressing both existing and emerging threats, our research provides a roadmap for enhancing the resilience of autonomous maritime systems, supporting their safe integration into global maritime infrastructures.