Cybersecurity Frameworks for Enhancing the Resilience of Unmanned Surface Vehicles in Maritime Operations

Guangrui Bian

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

Abstract. The deployment of unmanned surface vehicles (USVs) in maritime environments has significantly advanced marine operations, including surveillance, logistics, and environmental monitoring. However, with the growing integration of these autonomous systems into critical maritime infrastructures, they face increasing exposure to cybersecurity threats. Vulnerabilities in communication channels, control systems, and data networks can lead to severe consequences, from operational failures to potential hijacking or unauthorized data access. This paper presents a comprehensive analysis of the cybersecurity challenges associated with USVs, outlines the potential attack vectors, and proposes a multi-layered defense framework tailored for maritime autonomous systems. By emphasizing the need for resilient cybersecurity measures, this study contributes to the safe and reliable deployment of USVs in real-world maritime environments.

Keywords: Unmanned surface vehicles, maritime cybersecurity, autonomous systems, cyber-physical security, maritime operations, intrusion detection, secure communication protocols.

Introduction:

Unmanned surface vehicles (USVs), a subset of autonomous marine vehicles, have become increasingly important in modern maritime operations. Whether for commercial, military, or scientific applications, USVs offer unparalleled flexibility and efficiency in tasks such as border surveillance, search and rescue, underwater mapping, and environmental monitoring. Their ability to operate autonomously for extended periods without human intervention has transformed how maritime operations are conducted. However, this same autonomy introduces significant cybersecurity risks that, if left unaddressed, could lead to catastrophic consequences.

USVs are equipped with complex communication systems, sensors, and control mechanisms that rely heavily on data exchange across networks. The open and distributed nature of these systems makes them attractive targets for cyberattacks. For instance, vulnerabilities in communication protocols can be exploited to intercept or alter commands, while weaknesses in onboard software could allow unauthorized access to sensitive operational data. The potential for cyberattacks is especially concerning in maritime contexts, where the consequences of compromised USVs could include navigational errors, loss of control, or even adversarial control over critical assets.

Given the increasing reliance on USVs for critical maritime operations, developing robust cybersecurity measures has become a priority. The challenge lies in the unique constraints and dynamic environments in which USVs operate. Unlike traditional cybersecurity systems that can rely on constant human oversight and intervention, USV defenses must be resilient, adaptive, and capable of responding to sophisticated threats autonomously. This paper examines the specific cybersecurity challenges facing USVs, identifies key vulnerabilities, and proposes a layered defense strategy that combines encryption, intrusion detection, and secure communication protocols. Through a detailed exploration of these strategies, this study aims to provide actionable insights for enhancing the cybersecurity of USVs in an increasingly connected and automated maritime world.