A Risk-Based Approach to Cybersecurity for Autonomous Maritime Systems: Challenges and Solutions for Unmanned Surface Vehicles

Guangrui Bian

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

Abstract. Unmanned surface vehicles (USVs) are increasingly being adopted in maritime operations, driven by their potential to enhance efficiency, reduce human risk, and support complex missions in hostile environments. However, the increased reliance on these autonomous systems introduces new cybersecurity challenges, as they become attractive targets for malicious actors. This paper presents a risk-based approach to cybersecurity for USVs, identifying key threat vectors and proposing adaptive strategies to mitigate them. By integrating advanced risk assessment techniques with real-time monitoring and threat response, the study highlights best practices to enhance the resilience of USV systems in dynamic maritime environments.

Keywords: unmanned surface vehicles (USVs), cybersecurity, risk-based approach, threat assessment, maritime security, autonomous systems

Introduction:

The advent of unmanned surface vehicles (USVs) marks a transformative shift in maritime operations, offering new capabilities for both civilian and military applications. From search and rescue missions to maritime surveillance and cargo transport, USVs are becoming indispensable tools across a wide array of maritime sectors. However, as these systems become more sophisticated and interconnected, they also become more vulnerable to cyber threats. The complex communication networks, sensor systems, and autonomous decision-making algorithms that drive USV operations present multiple entry points for cyber-attacks. In particular, these threats can compromise mission-critical functions, disrupt communication channels, and even lead to hostile takeovers of USV platforms. Given the critical roles USVs play in strategic maritime operations, the need for robust cybersecurity measures has never been more urgent. This paper investigates the primary cybersecurity challenges faced by USVs and proposes a risk-based framework to enhance their defense mechanisms. By examining various risk scenarios and leveraging cutting-edge security solutions, the research provides actionable insights to safeguard the operational integrity of USVs in an increasingly contested maritime environment.

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.