Resilient Security Strategies for Autonomous Maritime Systems: Detecting and Mitigating Cyberattacks in UMVs

Guangrui Bian

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

Abstract. As autonomous maritime systems become increasingly integrated into commercial and military operations, the need for resilient cybersecurity solutions grows. Unmanned maritime vehicles (UMVs) face unique challenges due to their remote and often isolated deployment environments, making them attractive targets for cyberattacks. This paper presents a resilient security strategy focused on real-time attack detection and automated response mechanisms for UMVs. By leveraging a hybrid approach combining rule-based and behavior-based detection, the proposed system is capable of identifying complex attack vectors while minimizing false positives. Additionally, the study discusses techniques for secure communication, encryption, and redundancy measures to enhance the robustness of UMV operations in adversarial settings.

Keywords: UMV security, resilient cybersecurity, attack detection, secure communication, autonomous systems, maritime operations

Introduction:

Autonomous maritime systems, specifically unmanned maritime vehicles (UMVs), have gained significant traction in recent years due to their potential to carry out critical missions with minimal human involvement. These systems are widely deployed across various sectors, including naval defense, underwater exploration, and resource management. However, the increasing reliance on UMVs introduces new cybersecurity challenges that must be addressed to ensure mission success and protect sensitive information.

Unlike traditional manned vessels, UMVs operate independently over extended periods and in often remote, high-risk environments. Their autonomy is supported by sophisticated onboard control systems and communication networks that allow for remote monitoring and adjustments. However, this connectivity exposes UMVs to a wide range of cyber threats, from GPS spoofing and denial-of-service (DoS) attacks to more complex malware and signal interception techniques. Given the potentially catastrophic consequences of a successful attack, robust security mechanisms are essential.

This paper proposes a comprehensive strategy to enhance the resilience of UMVs against cyberattacks. The approach integrates real-time detection techniques, including signature-based and anomaly-based methods, with adaptive response strategies that can isolate compromised components and maintain operational continuity. Moreover, secure communication protocols and redundancy designs are explored to mitigate the impact of potential breaches. The proposed solutions are tested through simulation and real-world scenarios to validate their effectiveness, focusing on minimizing detection latency and optimizing resource utilization.