Security Control and Intrusion Detection Systems for Unmanned Maritime Vehicles: A Multi-Layered Approach

Guangrui Bian

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

Abstract. Unmanned maritime vehicles (UMVs) play a critical role in modern maritime operations, spanning a wide range of applications from defense to commercial purposes. Despite their advantages, the increased autonomy and network connectivity of UMVs expose them to significant cybersecurity risks. This paper proposes a multi-layered security control framework combined with real-time intrusion detection systems (IDS) to protect UMVs from cyberattacks. We focus on key vulnerabilities in communication channels, navigation systems, and sensor networks while introducing machine learning-based detection techniques capable of identifying both known and zero-day attacks. The study also evaluates the performance of these systems in dynamic maritime environments through simulation and real-world testing, highlighting the trade-offs between security, latency, and operational efficiency.

Keywords: Unmanned maritime vehicles, cybersecurity, intrusion detection systems, attack detection, multi-layered security, machine learning, autonomous systems

Introduction:

Unmanned maritime vehicles (UMVs), encompassing both unmanned surface vehicles (USVs) and unmanned underwater vehicles (UUVs), have become indispensable tools in various maritime sectors, including defense, environmental monitoring, and offshore industries. The autonomy and versatility of these systems allow them to perform complex tasks in remote or hazardous environments without human intervention. However, the shift toward autonomous operations and increased connectivity has introduced substantial cybersecurity concerns that, if left unaddressed, could lead to mission failure, data breaches, or even loss of control.

One of the key challenges in securing UMVs lies in their reliance on interconnected networks for command, control, and data transmission. These communication systems are susceptible to various forms of cyberattacks, ranging from jamming and spoofing to sophisticated malware attacks targeting control software. Traditional security measures, such as firewalls and encryption, are often insufficient in protecting UMVs from evolving threats in dynamic and adversarial maritime environments.

This paper aims to bridge the gap by proposing a comprehensive security control framework for UMVs that integrates multi-layered defenses with advanced intrusion detection systems (IDS). The approach combines signature-based detection for known threats with anomaly detection techniques powered by machine learning algorithms, capable of identifying novel attack patterns. By simulating realistic attack scenarios and conducting field tests, this study evaluates the effectiveness of the proposed framework, providing insights into the optimal configuration of security measures for different operational contexts.