Asynchronous Fault Detection for Unmanned Marine Vehicles Under Deception attacks

Fuxing Wang
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China
wfx614328@163.com

***Abstract*—This paper addresses the challenge of thruster fault detection in Unmanned Marine Vehicles (UMVs) subjected to deception attacks, a sophisticated type of cyber threat where adversaries manipulate sensor data to mislead fault detection systems. Deception attacks pose significant risks by introducing erroneous data, which can obscure genuine faults and disrupt the reliability of detection mechanisms. To tackle this issue, the study proposes a novel detection framework that integrates an advanced asynchronous switched filter designed specifically to counteract the effects of deception attacks. This approach combines adaptive filtering techniques with robust model-based methods to enhance the accuracy and reliability of fault detection. The framework employs model-dependent average dwell time (MDADT) and piecewise Lyapunov functions (PLF) to derive rigorous conditions that ensure global stability and optimal performance under the influence of deceptive data. Additionally, the research introduces a dynamic adjustment mechanism to adapt the filter parameters in real-time, based on evolving attack patterns and system conditions. Extensive simulations demonstrate the effectiveness of the proposed framework in maintaining high levels of detection accuracy and system reliability despite the presence of deceptive attacks. The findings underscore the critical need for innovative and adaptive strategies to address the challenges posed by sophisticated cyber threats in unmanned marine systems, providing valuable insights and practical solutions for enhancing the operational integrity and security of UMVs.**

***Index Terms*—Unmanned marine vehicles, Deception Attacks, Asynchronous Fault Detection, Stability Analysis.**

I. Introduction

In recent years, unmanned marine vehicles (UMVs) have become integral to a wide array of marine applications, including environmental monitoring, resource exploration, and military operations. Their ability to operate autonomously and perform complex tasks in challenging maritime environments has made them invaluable assets in modern maritime operations. However, the reliance of UMVs on wireless communication networks and advanced sensor systems exposes them to a growing spectrum of cyber threats, among which deception attacks pose a particularly insidious risk. Deception attacks, characterized by the intentional manipulation of sensor data, undermine the integrity of fault detection systems by injecting misleading information that can obscure genuine faults and disrupt system performance.

The challenge of detecting thruster faults in UMVs becomes increasingly complex in the presence of deception attacks. Traditional fault detection methods, which rely on accurate sensor data to diagnose system health, are often inadequate when confronted with data deliberately corrupted by adversaries. These attacks can cause significant operational issues by masking real faults, leading to erroneous diagnostics and potentially catastrophic failures. As such, there is a critical need for advanced fault detection strategies that can effectively handle the unique challenges posed by deception attacks.

To address this pressing issue, this paper introduces an innovative framework for thruster fault detection designed specifically to counteract the effects of deception attacks. The proposed approach integrates an advanced asynchronous switched filter methodology with adaptive filtering techniques and robust model-based strategies. This novel framework is tailored to manage the distortions introduced by deceptive data, ensuring that the fault detection system remains accurate and reliable even in the face of sophisticated cyber threats.

Central to the framework is the use of model-dependent average dwell time (MDADT) and piecewise Lyapunov functions (PLF), which provide a rigorous basis for establishing conditions that ensure global system stability and optimal performance despite the presence of manipulated data. Additionally, the study incorporates a dynamic adjustment mechanism that enables real-time adaptation of filter parameters based on evolving attack patterns and system performance metrics. This adaptability enhances the resilience of the fault detection system, allowing it to maintain high levels of accuracy and reliability.

Extensive simulations validate the effectiveness of the proposed framework, demonstrating its ability to sustain robust fault detection in the presence of deception attacks. The results highlight the necessity of developing innovative and adaptive strategies to address the multifaceted challenges posed by modern cyber threats. By advancing the state-of-the-art in fault detection for UMVs, this research offers valuable insights and practical solutions that enhance the operational integrity and security of unmanned marine systems. The findings contribute significantly to the broader fields of cybersecurity and autonomous systems, providing a comprehensive approach to safeguarding critical maritime operations against sophisticated cyber threats.