Asynchronous Fault Detection for Unmanned Marine Vehicles Under False Data Injection 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 (FD) in Unmanned Marine Vehicles (UMVs) under the threat of False Data Injection (FDI) attacks. FDI attacks can corrupt sensor data, leading to erroneous fault detection and impaired system performance. To tackle this issue, the study proposes a robust detection framework that integrates an advanced asynchronous switched filter specifically designed to counteract the effects of FDI attacks. The proposed framework employs a combination of adaptive filtering techniques and model-based approaches to effectively identify and isolate faults despite the presence of manipulated data. The analysis utilizes a model-dependent average dwell time (MDADT) and piecewise Lyapunov functions (PLF) to establish stability and performance criteria under the influence of FDI attacks. Additionally, the study derives conditions for filter design and performance guarantees, ensuring accurate fault detection even in the presence of data corruption. Simulation results demonstrate the framework's efficacy in maintaining high detection accuracy and system reliability. The findings underscore the importance of incorporating adaptive and resilient strategies to enhance fault detection capabilities in the face of sophisticated cyber threats.**

Index Terms—**Unmanned marine vehicles, False Data Injection (FDI) Attacks, Asynchronous Fault Detection,Stability Analysis .**

I. Introduction

In the rapidly evolving field of unmanned marine vehicles (UMVs), ensuring their reliable operation amidst increasingly sophisticated cyber threats is a pressing and paramount concern. UMVs play a critical role in a range of applications including environmental monitoring, resource exploration, and military operations, where their autonomous capabilities and data-gathering functions are of immense value. However, the inherent reliance of UMVs on wireless communication networks makes them highly vulnerable to a spectrum of cyber threats, with False Data Injection (FDI) attacks emerging as a particularly severe and complex challenge. FDI attacks involve the deliberate injection of misleading data into the system, which can severely compromise the integrity of sensor readings and thus lead to erroneous fault detection and impaired operational effectiveness.

The intricacy of detecting faults in UMVs is significantly heightened by the nature of FDI attacks. Unlike traditional faults, which can often be identified using established diagnostic techniques, FDI attacks are engineered to obscure the true state of the system through deliberate data manipulation. This deliberate falsification of data introduces considerable difficulty in distinguishing between genuine faults and attack-induced anomalies, thereby rendering conventional fault detection methods inadequate. Traditional approaches may struggle to maintain accuracy and reliability when faced with the intentional distortions introduced by FDI attacks, thereby necessitating innovative solutions to address this challenge effectively.

To address these pressing issues, this paper presents a groundbreaking approach to thruster fault detection that is specifically designed to tackle the complexities introduced by FDI attacks. The proposed solution leverages an advanced asynchronous switched filter framework that is adept at managing the distortions and uncertainties associated with FDI attacks. This innovative framework integrates adaptive filtering techniques with model-based methodologies to significantly enhance the robustness and accuracy of fault detection systems. By employing a combination of model-dependent average dwell time (MDADT) and piecewise Lyapunov functions (PLF), the research establishes rigorous conditions that ensure the global stability of the system and its optimal performance despite the presence of manipulated data.

Moreover, the study makes a substantial contribution to the field by deriving comprehensive conditions for the design and performance of fault detection filters, thus addressing a critical gap in current research. These conditions encompass the necessary parameters to sustain system stability and maintain high detection accuracy in the face of data corruption. The incorporation of adaptive filtering techniques allows for real-time adjustments based on evolving attack patterns and system performance metrics, thereby enhancing the system's resilience to dynamic and sophisticated cyber threats.

The proposed framework's effectiveness is validated through extensive simulation studies, which confirm its ability to achieve high levels of fault detection accuracy and system reliability even when confronted with complex and evolving cyber threats. These findings underscore the crucial importance of developing adaptive, resilient fault detection strategies capable of countering the multifaceted challenges posed by modern cyber threats. By advancing the state-of-the-art in fault detection for UMVs, this research provides valuable insights and practical solutions that enhance the safety, reliability, and operational integrity of unmanned marine systems. This contri-

bution is significant for the broader fields of cybersecurity and autonomous systems, offering a novel approach to ensuring the operational integrity of critical unmanned maritime operations.