Enhancing Thruster Fault Detection in Unmanned Marine Vehicles Under Denial of Service Attacks Using Asynchronous Switched Filters

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 critical issue of thruster fault detection (FD) in Unmanned Marine Vehicles (UMVs) under Denial of Service (DoS) attacks. Due to the inherent complexity of UMV operations and their reliance on wireless networks, these vehicles are vulnerable to cyber threats that can lead to system failures. The study proposes an asynchronous switched filter to improve fault detection accuracy, considering the delays in detecting DoS attacks. By employing model-dependent average dwell time (MDADT) and piecewise Lyapunov functions (PLF), the research establishes parameters that limit the impact of DoS attacks, and simulation results validate the method's effectiveness in enhancing UMV reliability and security.**

***Index Terms*—Unmanned marine vehicles, Asynchronous fault detection filters, Thruster failures, DoS attacks.**

I. Introduction

In recent years, Unmanned Marine Vehicles (UMVs) have increasingly drawn significant attention in the fields of marine science and technology due to their wide-ranging applications across various critical domains. These domains include, but are not limited to, marine exploration, environmental monitoring, and the development of marine resources. As technology advances, UMVs are being deployed more extensively and are undertaking increasingly complex missions within these fields. However, the operational environment for UMVs is inherently complex and unpredictable, which adds layers of challenges to their effective deployment and operation.

A key factor in the operation of UMVs is their heavy reliance on wireless communication networks to maintain contact with shore-based control centers. This reliance is essential for the remote control and monitoring of these vehicles, but it also introduces significant vulnerabilities. Specifically, UMVs are exposed to a range of potential disruptions, including external disturbances, equipment malfunctions, and particularly cyber-attacks, which can exploit the open nature of their communication networks. These vulnerabilities can have serious consequences, compromising the operational integrity and safety of the UMVs, and potentially leading to severe accidents or even catastrophic failures.

The unpredictability of the potential harm caused by such disturbances or faults to UMVs has been widely recognized in the field. This unpredictability is exacerbated by the openness of cyberspace, which leaves UMV systems particularly susceptible to various forms of cyber threats, especially cyber-attacks. These threats are not merely hypothetical; they represent real and present dangers that can lead to significant system failures. Such failures not only disrupt the intended missions of UMVs but also pose substantial risks to the safety of the vehicle, the environment, and potentially human lives.

Given these risks, enhancing the reliability and security of UMVs has become an increasingly urgent and critical area of research and development. Addressing these challenges requires innovative solutions that can effectively mitigate the risks associated with both physical disturbances and cyber threats. In response to these challenges, this paper specifically investigates the issue of thruster fault detection (FD) for UMVs under the condition of Denial of Service (DoS) attacks, which are a common and particularly dangerous form of cyber-attack that UMVs may face.

The study introduces an asynchronous switched method as a novel approach to improving the reliability and security of fault detection mechanisms in UMVs. One of the primary challenges in detecting faults in the presence of DoS attacks is the difficulty in promptly identifying these attacks. In the context of this challenge, an asynchronous switched filter is proposed for the specific purpose of detecting thruster faults in UMVs. This approach differs from most existing research, which often operates under the assumption that DoS attacks can be detected immediately and that the switching of filters corresponding to each subsystem occurs synchronously with the subsystem switching. However, the reality of practical applications is that DoS attacks are notoriously difficult to detect in a timely manner.

This delay in the detection of DoS attacks creates a scenario where the filter requires additional time to select the appropriate control mode that corresponds to the current subsystem mode. This delay leads to asynchronous switching between the filter and the subsystem, which poses a significant challenge to achieving optimal fault detection in real-world scenarios. Filters designed under the assumption of synchronous switching may fail to provide effective detection due to the inherent delays introduced by undetected DoS attacks. Recognizing and

addressing this asynchronous nature of switching is thus of great practical importance for improving the fault detection capabilities of UMVs.

To address these challenges, the paper employs advanced techniques, including model-dependent average dwell time (MDADT) and piecewise Lyapunov functions (PLF), to derive critical parameters. These parameters include the tolerable lower limit of the sleep interval and the upper limit of the attack interval for DoS attacks. By deriving these limits, the study effectively constrains the impact of DoS attacks, ensuring that the UMV system can continue to operate within safe boundaries even in the presence of such attacks. Additionally, the study utilizes decoupling techniques to establish the solvability conditions for the designed fault detection filter, which are crucial for determining the optimal filter gains.

Finally, the effectiveness of the proposed method is rigorously validated through a series of simulation experiments. These simulations are designed to replicate real-world conditions and demonstrate the practical applicability of the asynchronous switched filter in enhancing the reliability and security of UMV operations under the threat of DoS attacks. The results of these simulations provide strong evidence that the proposed method offers significant advancements in the field of marine vehicle fault detection and cybersecurity, contributing to safer and more reliable UMV operations in increasingly challenging environments.