Asynchronous Fault Detection for Unmanned Marine Vehicles under Aperiodic DoS Attacks and Stochastic 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 focuses on asynchronous thruster fault detection for unmanned marine vehicles (UMVs) in the presence of multiple cyber threats, external disturbances, and thruster failures. A novel detection model is developed utilizing an asynchronous switched method, specifically addressing aperiodic Denial-of-Service (DoS) attacks and stochastic Deception attacks. The proposed approach employs the Lyapunov–Krasovskii functional method combined with model-dependent average dwell time to derive a set of sufficient conditions that ensure the system achieves global mean-square exponential stability with a guaranteed H_∞ performance. Furthermore, the research determines the tolerable upper and lower bounds for constrained DoS attacks, enhancing the system's robustness against such cyber threats. Solvable conditions for the design of fault detection filters are derived using decoupling techniques, ensuring the efficacy of the detection mechanism. Finally, extensive simulations on a UMV validate the proposed method's feasibility and effectiveness, demonstrating its capability to maintain reliable fault detection under complex and evolving cyber attack scenarios.**

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

I. Introduction

In the rapidly advancing field of autonomous maritime operations, unmanned marine vehicles (UMVs) have become integral to a wide range of applications. These vehicles are crucial for activities such as environmental monitoring, deep-sea exploration, resource management, and military reconnaissance. The autonomous capabilities of UMVs enable them to operate in remote and often hostile marine environments, where human presence is either impractical or impossible. Their ability to gather and relay data in real-time, monitor vast oceanic areas, and execute complex tasks with minimal human intervention has significantly transformed maritime operations. However, the increasing reliance on these vehicles also brings about substantial challenges, particularly in terms of ensuring their operational reliability and security.

One of the most pressing challenges faced by UMVs today is their vulnerability to cyber-attacks, which can severely compromise their functionality and safety. As UMVs depend heavily on wireless communication networks and sophisticated sensor systems for navigation, control, and data transmission, they are exposed to a wide array of cyber threats. Among these, denial-of-service (DoS) attacks and deception attacks have been identified as particularly dangerous due to their potential to disrupt UMV operations in ways that are difficult to detect and mitigate.

DoS attacks aim to overwhelm a system's resources, rendering it unable to perform critical tasks by flooding it with excessive requests or by blocking legitimate communication channels. In the context of UMVs, such attacks can lead to a loss of communication between the vehicle and its control center, which may result in the UMV becoming inoperable or deviating from its mission parameters. On the other hand, deception attacks involve the injection of false data into the system, misleading the UMV's decision-making processes by providing incorrect information. These attacks can manipulate sensor readings or communication data, causing the UMV to make erroneous judgments about its environment, which could lead to navigation errors, operational failures, or even catastrophic accidents.

The dual threat posed by DoS and deception attacks makes it imperative to develop robust fault detection mechanisms that can effectively identify and respond to such cyber threats in real-time. Traditional fault detection methods, which are often designed to handle more straightforward system malfunctions, are typically ill-equipped to address the sophisticated nature of cyber-attacks. These conventional methods tend to assume that faults are isolated and occur in predictable patterns, whereas cyber-attacks, especially deception attacks, are engineered to exploit system vulnerabilities in unpredictable ways. This gap in detection capabilities necessitates the development of more advanced strategies that are specifically tailored to counteract the dynamic and covert nature of cyber threats.

In response to this critical need, the present study introduces a novel approach to thruster fault detection in UMVs that is capable of addressing the complexities introduced by multiple cyber threats, particularly DoS and deception attacks. The proposed framework employs an asynchronous switched method, which is specifically designed to handle the irregular and unpredictable timing of these attacks. By incorporating an asynchronous switching mechanism, the detection system

can dynamically adjust to the changing conditions of the UMV's operational environment, allowing for more accurate and timely identification of faults even under continuous cyber assault.

Central to the effectiveness of the proposed method is the integration of the Lyapunov–Krasovskii functional approach with model-dependent average dwell time (MDADT) analysis. This combination provides a mathematically rigorous foundation for ensuring the global mean-square exponential stability of the UMV system. The Lyapunov–Krasovskii functional offers a robust framework for analyzing the stability of systems subject to time delays and stochastic disturbances, which are common in scenarios involving cyber-attacks. Meanwhile, MDADT analysis is used to derive sufficient conditions that guarantee the UMV's stability and performance in the presence of aperiodic DoS attacks and stochastic deception attacks.

Moreover, the research extends its contribution by determining the tolerable upper and lower bounds for constrained DoS attacks. These bounds are crucial for defining the operational limits within which the UMV can function safely while under attack. By establishing these parameters, the study provides clear guidelines for maintaining system resilience, ensuring that the UMV can continue its mission even when subjected to severe cyber threats. This aspect of the research addresses a significant gap in existing literature, where the focus has often been on either the detection or the mitigation of attacks, with less emphasis on defining the operational boundaries within which systems can remain effective during an ongoing attack.

The proposed framework also employs decoupling techniques to derive solvable conditions for the design of fault detection filters. Decoupling in this context allows the system to isolate and address individual faults or attack impacts without being overwhelmed by the complexity of multiple, simultaneous threats. This methodological innovation ensures that the detection filters are not only effective but also computationally feasible, making them suitable for real-time applications in UMVs.

Finally, the effectiveness of the proposed method is rigorously validated through extensive simulations. These simulations replicate various attack scenarios, including combinations of DoS and deception attacks, to test the resilience and accuracy of the fault detection system. The results demonstrate that the proposed asynchronous switched method significantly enhances the UMV's ability to detect and respond to faults, even in highly complex and dynamic environments. The simulations underscore the importance of adopting advanced detection strategies that are capable of dealing with the multifaceted challenges posed by modern cyber threats.

In conclusion, this study makes a substantial contribution to the field of autonomous marine vehicles by providing a comprehensive and innovative solution to the problem of thruster fault detection under cyber-attack conditions. The integration of advanced mathematical techniques with practical engineering solutions offers a robust framework for enhancing the reliability and security of UMVs. As cyber threats continue to evolve, the development of such adaptive and resilient detection systems will be crucial in ensuring the safe and effective operation of UMVs across all domains of maritime activity. This research not only advances the current state of knowledge in fault detection but also sets the stage for future work in developing even more sophisticated strategies to safeguard UMVs against the ever-increasing threats of the cyber landscape.