19th International Conference on Innovative Computing, Information and Control (ICICIC2025)
August 26-29, 2025, Kitakyushu, Japan

PS-20: ICICIC2025-079

ET-WTOD Protocol Based Sliding Mode Control under False Data Injection Attacks

Xinyu Xie, Xinran Chen and Hongtao Sun*

College of Engineering, Qufu Normal University, Rizhao 276826, P. R. China
*Corresponding author: huntsun@qfnu.edu.cn

Introduction

Networked control systems (NCSs) have emerged as a critical infrastructure in modern industrial automation and cyber-physical systems, enabling remote monitoring through shared communication channels. However, the integration of network infrastructure introduces fundamental challenges that demand systematic investigation.

From the perspective of communication resource optimization, contemporary NCSs employ multiple sensors to enhance system reliability and response efficiency. The inherent limitations of bandwidth-constrained networks, however, may induce communication delays and packet dropouts that degrade transmission efficiency and control performance. From the cybersecurity perspective, wireless communication networks introduce vulnerabilities to malicious attacks despite their connectivity advantages.

Contributions

1) To save limited communication resources, an ET-WTOD co-design framework is developed. At the same time, the probability distribution of the network induced delay is considered. Besides, the proposed discrete-time period ET-WTOD can naturally exclude Zeno behaviours because the period samplings and time delay are easily characterized by the well-known input delay approach.

2) Due to the inherent robustness of the sliding mode control method to uncertainties and external disturbances, a scheduling-signal-dependent sliding mode control strategy is devised to ensure that the state trajectories are driven into the domain of the specified sliding surface while improving the communication efficiency.

Results

The system's actuator is injected with malicious attack signals and no additional auxiliary security is designed for the controller under the ETWTOD protocol. As can be seen from Figure 1, the state response fails to eventually reach a steady state when there is an injected actuator attack. The number of data transfers is 277.

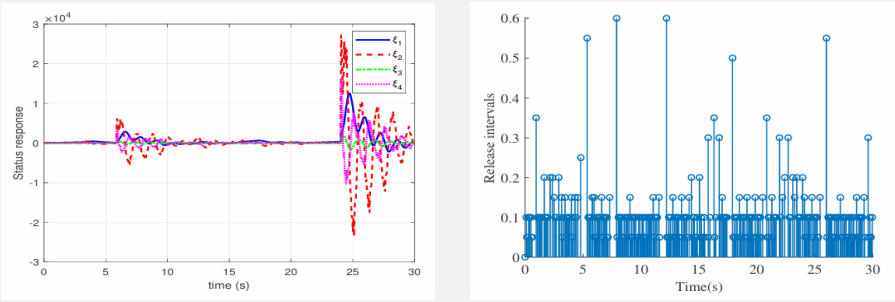

Figure 1. State responses and release intervals with equivalent controller under actuator attacks

The integrated sliding mode controller is used to defend the system against FDI attacks. From Figure 2, the state of the system quickly reaches stability under the effect of FDI attack, indicating that the sliding mode security control strategy based on the ET-WTOD protocol can well resist the effect of FDI attack. The number of data transfers is 259.

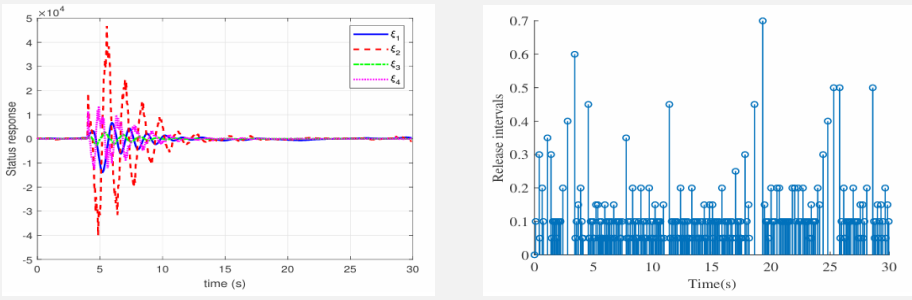

Figure 2. State responses, and release intervals with switching controller under actuator attacks