Resilient-Learning Control of Cyber-Physical Systems Against Mixed-Type Network Attacks

Ximing Yang
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu 611731, China
yxm961115123@163.com

***Abstract*—This article develops a novel resilient-learning control strategy for cyber-physical systems (CPSs) to mitigate the impact of mixed-type network attacks. These attacks combine false-data-injection (FDI) and replay attacks, which are modeled using Markov jump processes. The attacks are assumed to be uncertain, and a three-layer neural network is employed to learn and approximate them. Based on these approximations, a resilient controller is designed, integrating adaptive laws to estimate the neural network weights in real-time. The proposed control strategy ensures the system's ultimate boundedness and asymptotic stability under attack conditions. To validate the efficacy of the approach, a vertical take-off and landing (VTOL) helicopter model is used for simulation, demonstrating the controller's robustness and effectiveness in maintaining system stability despite the presence of mixed-type network attacks.**

***Index Terms*—Cyber-Physical Systems (CPSs), Mixed-Type Network Attacks, Resilient Control, Neural Networks, Markov Jump Processes, Adaptive Control, False-Data-Injection Attack, Replay Attack**

I. Introduction

The integration of advanced technologies such as intelligent sensing, mobile communication, and automation has revolutionized modern industrial control systems, giving rise to cyber-physical systems (CPSs). These systems, which tightly couple computational algorithms with physical processes, have become pivotal in a range of applications, including smart grids, autonomous vehicles, healthcare systems, and industrial automation. The seamless interaction between the cyber and physical components in CPSs enables real-time data exchange and decision-making, significantly enhancing efficiency and reliability in these applications.

However, the increasing reliance on networked communication within CPSs also exposes them to a new array of vulnerabilities. The openness and connectivity that are central to CPS operations make them prime targets for a variety of cyber-attacks, which can have devastating effects on both the cyber infrastructure and the physical processes they control. Among these cyber threats, false-data-injection (FDI) attacks, replay attacks, and Denial-of-Service (DoS) attacks are particularly notorious. Each of these attack types can independently disrupt system operations, but when combined into a mixed-type attack, their impact can be exponentially more harmful, posing significant challenges to existing security measures.

FDI attacks involve the malicious alteration of data as it is transmitted through the network, leading to incorrect decision-making and control actions. Replay attacks, on the other hand, involve intercepting and then re-sending legitimate data packets at a later time, causing the system to operate on outdated or misleading information. DoS attacks focus on overwhelming the network with traffic, rendering communication channels unavailable and thus incapacitating the system's ability to respond to real-time changes. While these attacks have been studied extensively in isolation, the growing trend of combining these tactics into sophisticated, mixed-type attacks presents a new frontier of challenges for CPS security.

The complexity of defending against mixed-type attacks lies in their ability to exploit multiple vulnerabilities simultaneously, often evading traditional security mechanisms that are designed to address singular threats. This necessitates the development of more resilient and adaptive control strategies that can not only detect and mitigate individual attack types but also respond effectively to their combinations. Moreover, the uncertainty associated with the nature and timing of these attacks adds another layer of difficulty, requiring controllers to be both robust and flexible in their operation.

To address these challenges, this paper proposes a novel resilient-learning control strategy specifically designed to safeguard CPSs against mixed-type network attacks. The approach leverages the powerful approximation capabilities of neural networks to learn and estimate the characteristics of FDI attacks in real-time, even when the exact attack model is unknown. Additionally, the use of Markov jump processes to model replay attacks allows the controller to anticipate and respond to these threats dynamically. The proposed control framework integrates these elements into a unified adaptive strategy, enhancing the system's ability to withstand and recover from complex, multi-faceted cyber threats.

The effectiveness of the proposed resilient-learning controller is demonstrated through its application to a vertical take-off and landing (VTOL) helicopter model-a scenario that exemplifies the critical need for robust control in the face of cyber threats. The VTOL helicopter, like many CPS applications, relies heavily on precise control and real-time data processing, making it particularly vulnerable to the types of attacks considered in this study. Through rigorous simulation studies, the proposed method is shown to maintain system stability and performance, even under severe attack conditions, highlighting its potential as a practical solution for enhancing

CPS security.

In conclusion, as CPSs continue to play an increasingly vital role in critical infrastructure and industry, the need for advanced security mechanisms that can address the evolving landscape of cyber threats becomes paramount. The resilient-learning control strategy presented in this paper represents a significant step forward in this direction, offering a robust, adaptive approach to protecting CPSs against the growing threat of mixed-type network attacks. This work not only contributes to the theoretical foundations of CPS security but also provides actionable insights for the design and implementation of secure control systems in practice.