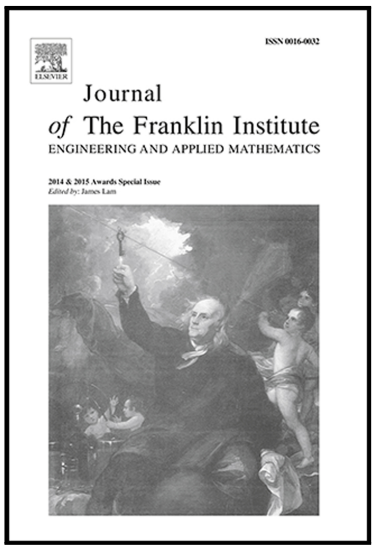

A Data-driven Covert Attack Strategy in the Closed-loop Cyber-physical Systems

Zhe Li, Guang-Hong Yang

PII: S0016-0032(18)30375-2
DOI: 10.1016/j.jfranklin.2018.05.046
Reference: FI 3482

To appear in: *Journal of the Franklin Institute*

Received date: 19 September 2017
Revised date: 28 March 2018
Accepted date: 28 May 2018

Please cite this article as: Zhe Li, Guang-Hong Yang, A Data-driven Covert Attack Strategy in the Closed-loop Cyber-physical Systems, *Journal of the Franklin Institute* (2018), doi: 10.1016/j.jfranklin.2018.05.046

Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 00 (2018) 1–14

Journal of The Franklin Institute

A Data-driven Covert Attack Strategy in the Closed-loop Cyber-physical Systems

Zhe Li[a], Guang-Hong Yang[a,b,*]

[a] *College of Information Science and Engineering, Northeastern University, Shenyang, China*
[b] *State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang, China*

Abstract

In this paper, a data-driven covert attack strategy is proposed for a class of closed-loop cyber-physical systems. Without the parameters of the system plant and the nominal controller, the attacker can only use the intercepted input and output data of the nominal system. The injected input attack signals are designed based on the subspace predictive control method, which can deviate the real outputs to the expected attack references in a future time horizon. Meanwhile, by injecting the designed output attack signals for compensation, the attack cannot be detected by the anomaly detector. The simulation results of an irrigation canal system illustrate the effect of the proposed strategy with satisfactory performances.

Keywords: Data-driven, covert attack, closed-loop cyber-physical systems

1. Introduction

With the intelligentization and informatization of the modern industrial systems, the application of the cyber-physical systems (CPSs) is becoming more and more extensive. Examples of application of CPS include smart transportation networks, power generation and distribution networks, water and gas distribution networks, and advanced communication systems [1–3]. The CPS integrates physical processes, computational resources and communication capabilities, which makes the entire system complex and vulnerable to attacks despite of its advantages.

Although the research on CPS is still in the primary stage, there are still various constructive results to provide enlightment. In particular, many researchers pay more attention to the security problems of the CPS [3–5]. In [5], a comprehensive introduction of the related control theories about the typical security problems in CPS is presented with some benchmark examples. In general, the security problems in CPS can be characterized by how to defend and how to attack, from the opposite standpoints of the defender (or controller) and the attacker, respectively.

From the viewpoint of the defender, the concerning studies are mainly about the secure estimation and control, attack detection and identification for anticipated attack patterns [7–10]. Paper [9] investigates the attack-resilient state estimation problem for continuous-time linear systems with sparse actuator attacks and process noises. Paper [10] proposes a switched Luenberger observer for the secure state estimation for CPS under disturbances and sparse sensor attacks.

*Corresponding author: yangguanghong@ise.neu.edu.cn