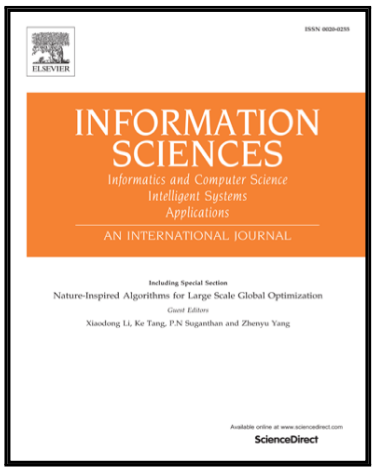
Accepted Manuscript



A Cooperative Detection and Compensation Mechanism against Denial-of-Service Attack for Cyber-Physical Systems

Lei Su, Dan Ye

PII: S0020-0255(18)30160-9
DOI: 10.1016/j.ins.2018.02.066
Reference: INS 13471

To appear in: *Information Sciences*

Received date: 5 December 2017
Revised date: 13 February 2018
Accepted date: 28 February 2018

Please cite this article as: Lei Su, Dan Ye, A Cooperative Detection and Compensation Mechanism against Denial-of-Service Attack for Cyber-Physical Systems, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.02.066

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

A Cooperative Detection and Compensation Mechanism against Denial-of-Service Attack for Cyber-Physical Systems ☆

Lei Su[a], Dan Ye[a,b,*]

[a]College of Information Science and Engineering, Northeastern University, Shenyang 110819, Liaoning, China.
[b]State Key Laboratory of Synthetical Automation of Process Industries, Northeastern University, Shenyang 110189, Liaoning, China.

Abstract

This paper is concerned with the detection and compensation co-design issue for cyber-physical systems against Denial-of-Service (DoS) attack. First, a novel supervisory strategy is proposed based on the concept of packet reception rate, which can detect the behavior of a DoS attacker during a given time window. A quantitative description of the relationship among attack times, time window, attack success rate and packet reception rate is analyzed. Based on the attack detection information, the current state under attack can be successfully reconstructed by some past available states. Then, a co-design compensation mechanism is also obtained, which can further guarantee the attacked system is stochastically stable (without the zero-mean Gaussian white noise) or mean square exponentially ultimately bounded (with the zero-mean Gaussian white noise). The corresponding design conditions are derived in terms of linear matrix inequalities. Finally, a numerical example and a practical example are given to show the effectiveness and superiority of the presented design method.

Keywords: Denial-of-Service attack; detection and compensation scheme; packet reception rate.

1. Introduction

Cyber-physical systems (CPSs) consist of a wide range of systems that firmly combine communication components with physical components. These systems have been applied in many areas ranging from aerospace, to traffic systems, medicine and to process automation systems since new developments in sensing and communication techniques [23, 30, 32, 36]. Meanwhile, several new challenges or problems are brought to CPSs since the control components are connected with network environment. Some traditional fault-tolerant and fault detection methods in a physical system will be unavailable when a malicious attacker destroys or injects false data to the communication networks. Therefore, many scholars devote themselves to developing new techniques to cope with the cyber attack issues in CPSs during the past few years [2, 18, 19, 21, 22, 24, 31].

Attacks against communication networks have become popular in recent years. In the past, most control networks were safe, notwithstanding, they are currently fragile to malicious attacks [34]. The influences brought by a triumphant attack on control networks can be worse than the attacks on other networks because control systems are the heart part of many infrastructures. Consequently, the security of control systems has received increasing attention [10, 16]. To date, some malicious attacks have been widely investigated, such as Denial-of-Service (DoS) attack [39, 41], deception attack [3, 8, 9], and replay attack [7, 43], etc. To name a few, a dynamic output feedback controller was synthesized to guarantee the prescribed security in probability under deception attacks [9]. In [8], the distributed filter has been designed to fuse the unreliable data corrupted by noises, quantization errors and possible deception attacks. Compared with the deception attack, a variable receding-horizon control law was proposed to cope with the replay attacks [43]. DoS attack

☆This work is supported by in part by National Natural Science Foundation of China (Grant No.61773097), the Fundamental Research Funds for the Central Universities (Grant No.N160402004), the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries (Grant No.2013ZCX01), and the Liaoning BaiQianWan Talents Program (201517).

*Corresponding author. Email: yedan@ise.neu.edu.cn
Email addresses: bhuyhj51@gmail.com (Lei Su), yedan@ise.neu.edu.cn (Dan Ye)

Download English Version:

https://daneshyari.com/en/article/6856529

Download Persian Version:

https://daneshyari.com/article/6856529

Daneshyari.com