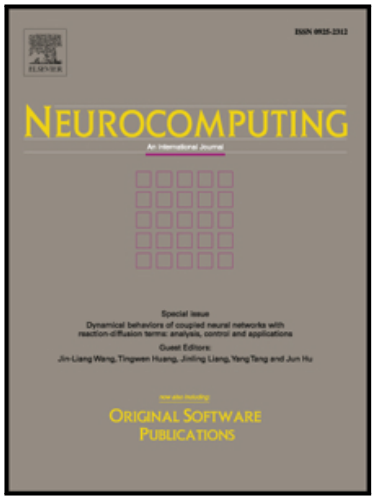
Communicated by Prof. Wei Guoliang

Accepted Manuscript



Security estimation under Denial-of-Service attack with energy constraint

Li Li, Huixia Zhang, Yuanqing Xia, Hongjiu Yang

PII: S0925-2312(18)30261-3
DOI: 10.1016/j.neucom.2018.02.086
Reference: NEUCOM 19391

To appear in: *Neurocomputing*

Received date: 10 November 2017
Revised date: 17 January 2018
Accepted date: 27 February 2018

Please cite this article as: Li Li, Huixia Zhang, Yuanqing Xia, Hongjiu Yang, Security estimation under Denial-of-Service attack with energy constraint, *Neurocomputing* (2018), doi: 10.1016/j.neucom.2018.02.086

Security estimation under Denial-of-Service attack with energy constraint

Li Li, Huixia Zhang, Yuanqing Xia and Hongjiu Yang

Abstract

This paper concentrates on security estimation of Cyber-Physical Systems subject to Denial-of-Service attack. A game framework is established to describe the interactive decision making process between the sensor and the attacker under energy constraint. A novel payoff function is used and the optimal strategies for both sides constituting a Nash equilibrium (NE) are obtained by using matrix game. Furthermore, the security issue on state estimation for CPS with multiple-subsystem is investigated based on game theory. To deteriorate the whole system performance, the attacker should decide when to attack and which subsystem to be chosen on account of limited energy. The existence conditions of NE strategies are given. Two numerical examples are provided to demonstrate the feasibility of the results.

Index Terms

State estimation, Cyber-Physical Systems, DoS attack, game theory, multiple-subsystem.

I. Introduction

Cyber-Physical Systems (CPS) are systems integrating computation, network and physical process which consists of sensors, actuators, control units and communication devices [1, 2], which have attracted considerable interest from both academic and industrial communities in the past few years, such as aerospace, smart grid, intelligent transportation, smart building, etc. However, with extensive use of widespread networking, wireless connection among sensors, estimators and actuators are more vulnerable to cyber security threats than wired sensors. The security issue caused by malicious attacks is of fundamental importance to ensure the safe operation of CPS [3–5], which have been investigated from different perspectives. The attack or the jamming is essentially a kind of methods, processes, or means which are utilized to maliciously reduce network reliability. In particular, deception attack and Denial-of-Service (DoS) are two typical attacks in reducing system performance. The former modifies the data packets in a malicious way [6–11], while the DoS attack blocks the information flow between the sender and the receiver to increase the packet drop rate [12–18]. Compared with deception attack, the DoS attack, which does not require comprehensive information about the system and the data, is a more reachable attack pattern in a shared network. Some critical systems which rely on real-time operation may become unstable and even be damaged under DoS attack.

Many scholars have acknowledged the importance of addressing the challenge of designing secure CPS. In the existing works, various efforts have been devoted to design estimators influenced by specific malicious attacks [12-21]. In [12], an optimal attack schedule has been investigated to maximize the expected average estimation error variance. To capture the strategic iteration between the sensor and the attacker, the game-theoretic approach provides such a framework to handle interactive decision issues (see [13–15]). In [16], a two-player zero-sum stochastic game is established to model the dynamic interaction between the defender and the DoS attacker. Due to energy constraint is inherent in almost all types of attacks, an integrated game-theoretic framework is proposed to investigate the interactive decision-making process under energy constraints in [17]. A multi-channel transmission schedule for remote state estimation under DoS attack is studied in [18, 19], in which a Nash Q-learning algorithm is proposed to reduce the

Li Li, Huixia Zhang and Hongjiu Yang are with the Institute of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China. Emails: lili@ysu.edu.cn; huixiaz0914@163.com; yanghongjiu@ysu.edu.cn. Yuanqing Xia is with the School of Automation, Beijing Institute of Technology, Beijing 100081, China. Email: xia_yuanqing@bit.edu.cn.