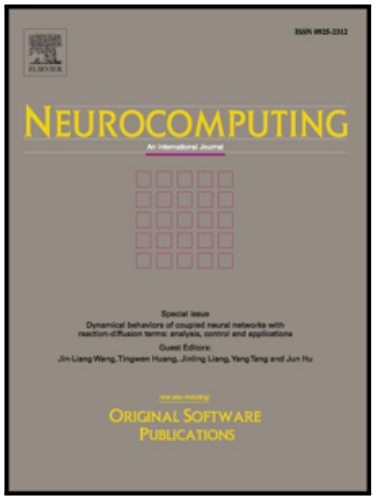
Communicated by Prof. Wei Guoliang

Accepted Manuscript



Energy Efficient Jamming Attack Schedule against Remote State Estimation in Wireless Cyber-Physical Systems

Lianghong Peng, Xianghui Cao, Changyin Sun, Yu Cheng, Shi Jin

PII: S0925-2312(17)31293-6
DOI: 10.1016/j.neucom.2017.07.036
Reference: NEUCOM 18724

To appear in: *Neurocomputing*

Received date: 28 November 2016
Revised date: 19 March 2017
Accepted date: 14 July 2017

Please cite this article as: Lianghong Peng, Xianghui Cao, Changyin Sun, Yu Cheng, Shi Jin, Energy Efficient Jamming Attack Schedule against Remote State Estimation in Wireless Cyber-Physical Systems, *Neurocomputing* (2017), doi: 10.1016/j.neucom.2017.07.036

Energy Efficient Jamming Attack Schedule against Remote State Estimation in Wireless Cyber-Physical Systems

Lianghong Peng[a,b], Xianghui Cao[a,b], Changyin Sun[a,b,*], Yu Cheng[c], Shi Jin[d]

[a]*School of Automation, Southeast University, Nanjing, Jiangsu, 210096, China*
[b]*Key Lab of Measurement and Control of Complex Systems of Engineering, Ministry of Education, Southeast University, Nanjing, Jiangsu, 210096, China*
[c]*Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616, USA*
[d]*National Mobile Communications Research Laboratory, Southeast University, Nanjing, Jiangsu, 210096, China*

Abstract

Recently, there has been a growing volume of literature on the security aspect of wireless Cyber-Physical Systems (CPS). Remote state estimation through wireless channels is a representative application of wireless CPS. However, such a system is exposed to various cyber security threats, such as replay attacks, jamming attacks and bad data injection attacks. In this paper, we focus on the wireless jamming attack and examine, from the standpoint of the attacker, the problem of optimal attack schedule that causes the largest performance degradation of the remote station estimation system, subject to attacker's energy constraint. Unlike some existing studies, we consider estimating multiple systems where sensors transmitting data to the remote estimator through multiple independent wireless channels. Due to the attacker's radio constraint, we assume that it can only launch jamming attack at one of the channels at any time. We start with the two-system case and formulate the energy efficient jamming attack schedule problem as a nonlinear program. The optimal energy efficient schedule is theoretically derived and is shown dependent on the wireless channels' properties, energy budget of the attacker and dynamics of the systems to

*Corresponding author
Email address: cysun@seu.edu.cn (Changyin Sun)