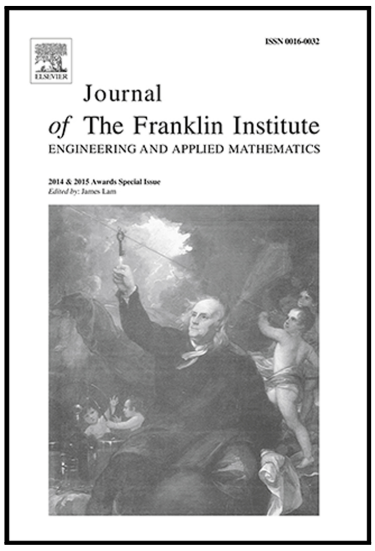

Towards Quantifying the Impact of Randomly Occurred Attacks on a Class of Networked Control Systems

Yuan Yuan, Peng Zhang, Lei Guo, Hongjiu Yang

PII: S0016-0032(17)30239-9
DOI: 10.1016/j.jfranklin.2017.05.016
Reference: FI 2990

To appear in: *Journal of the Franklin Institute*

Received date: 1 September 2016
Revised date: 11 February 2017
Accepted date: 1 May 2017

Please cite this article as: Yuan Yuan, Peng Zhang, Lei Guo, Hongjiu Yang, Towards Quantifying the Impact of Randomly Occurred Attacks on a Class of Networked Control Systems, *Journal of the Franklin Institute* (2017), doi: 10.1016/j.jfranklin.2017.05.016

HIGHLIGHTS

- a novel attack model is established which covers randomly occurred DoS attacks, deception attacks, and physical attacks;
- the so-called epsilon-NE is employed to quantify the maximum attack-induced impact, and the corresponding NE strategies are developed in delta-domain for the considered multi-tasking NCSs;
- an upper bound for the epsilon level is provided explicitly, and the corresponding convex optimization algorithm is given to compute such an upper bound.