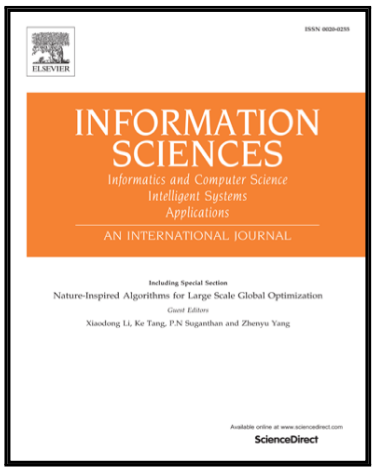

Stability Analysis of Token-based Wireless Networked Control Systems under Deception Attacks

Dajun Du, Changda Zhang, Haikuan Wang, Xue Li, Huosheng Hu, Taicheng Yang

PII: S0020-0255(18)30355-4
DOI: 10.1016/j.ins.2018.04.085
Reference: INS 13628

To appear in: *Information Sciences*

Received date: 15 February 2018
Revised date: 13 April 2018
Accepted date: 30 April 2018

Please cite this article as: Dajun Du, Changda Zhang, Haikuan Wang, Xue Li, Huosheng Hu, Taicheng Yang, Stability Analysis of Token-based Wireless Networked Control Systems under Deception Attacks, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.04.085

Stability Analysis of Token-based Wireless Networked Control Systems under Deception Attacks

Dajun Du[a], Changda Zhang[a,*], Haikuan Wang[a], Xue Li[a], Huosheng Hu[b], Taicheng Yang[c]

[a]*Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200072, P.R. China*

[b]*Department of Computer Science, University of Essex, Wivenhoe Park, Colchester CO3 4SQ, UK*

[c]*Department of Engineering and Design, University of Sussex, Brighton BN1 9QT, UK*

Abstract

Currently cyber-security has attracted a lot of attention, in particular in wireless industrial control networks (WICNs). In this paper, the stability of wireless networked control systems (WNCSs) under deception attacks is studied with a token-based protocol applied to the data link layer (DLL) of WICNS. Since deception attacks cause the stability problem of WNCSs by changing the data transmitted over wireless network, it is important to detect deception attacks, discard the injected false data and compensate for the missing data (i.e., the discarded original data with the injected false data). The main contributions of this paper are: 1) With respect to the character of the token-based protocol, a switched system model is developed. Different from the traditional switched system where the number of subsystems is fixed, in our new model this number will be changed under deception attacks. 2) For this model, a new Kalman filter (KF) is developed for the purpose of attack detection and the missing data reconstruction. 3) For the given linear feedback WNCSs, when the noise level is below a threshold derived in this paper, the maximum allowable duration of deception attacks is obtained to maintain the exponential stability of the system. Finally, a numerical example based on a linearized model of an inverted pendulum is provided to

*Corresponding author. Tel.: +086-021-56331634.
Email address: silenceupdown@hotmail.com (Changda Zhang).