Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 351 (2014) 4570–4583

Journal of The Franklin Institute

www.elsevier.com/locate/jfranklin

A stochastic game approach to the security issue of networked control systems under jamming attacks ☆

Shichao Liu[a], Peter X. Liu[a,*], Abdulmotaleb El Saddik[b]

[a]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada K1S 5B6
[b]School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada K1N 6N5

Received 8 August 2013; received in revised form 10 May 2014; accepted 14 June 2014
Available online 30 June 2014

Abstract

Securing networked control systems (NCSs) from cyber attacks has been a very important issue to keep NCSs reliable and stable. Most existing efforts tackling this issue treat cyber attacks as model-based disturbances to NCSs. But the reality is that intelligent attackers will not follow any prescribed models and in fact they are able to change their attack strategies dynamically and randomly. In this paper, we address this problem and present an optimal defense mechanism for the NCS under jamming attacks based on the stochastic game theory. A two-player zero-sum stochastic game is formulated to model the dynamic interactions between a jammer (attacker) and a sensor transmitter (defender) in the NCS. In this stochastic game, the cost function includes not only the resource costs used to conduct cyber-layer defense and attack actions, but also the possible degraded dynamic performance (indexed by a quadratic state error) of the NCS. With this cost function, the impacts of the interactions between the attacker and the defender on the dynamic performance of the NCS are taken into account when the two players design/change their cyber-layer strategies. The optimal defense mechanism is obtained by solving a stochastic dynamic programming (SDP) problem. Simulation and comparison studies show that the packet-loss rate of the communication channel of the NCS has been greatly reduced and the dynamic performance of the NCS being attacked by an intelligent jammer is much improved when the proposed defense mechanism is deployed.

☆This work is partially supported by the Natural Sciences and Engineering Research Council of Canada and Carleton University President 2010 Ph.D. Fellowship.

*Corresponding author.
E-mail addresses: lshchao@sce.carleton.ca (S. Liu), xpliu@sce.carleton.ca (P.X. Liu), abed@mcrlab.uottawa.ca (A. El Saddik).

http://dx.doi.org/10.1016/j.jfranklin.2014.06.010
0016-0032/

1. Introduction

Many critical infrastructures in our society, such as smart power grids and water resource management systems, are typical examples of networked control systems (NCSs), for which the control loops are closed via communication links [1]. While the communication links of these systems facilitate the aggregation and exchange of both system-wide information and local measurement data, they introduce new challenges as well, including time delays, packet losses, cyber attacks, etc. While problems associated with time delays and/or packet losses have been extensively studied in both system and network communication communities, such as [2–5], there are very few results dealing with cyber attacks and the security problem explicitly, especially from the system and control point of view.

There have been several reported attacks on power grids in U.S. [6,7]. In [8], the authors have pointed out that replacing proprietary networks by open communication infrastructures inevitably exposes these systems to cyber security risks. Regarding the cyber attacks on NCS systems, several critical challenges have been identified by Cardenas et al. [9]. In [10], different attack models and scenarios were considered for NCSs. In [11], robust controllers were designed for NCSs under Denial of Service (DoS) attacks. In [12], the effects of DoS attacks on load frequency control (LFC) in smart grids were analyzed. In [13], the authors studied false data attacks on a control system equipped with a Kalman filter.

While the above efforts are encouraging, most of these results formulate cyber attacks as model-based disturbances to NCSs. The reality, however, is that intelligent attackers will not follow any prescribed models and they are able to change their attack strategies dynamically and randomly. Therefore, it is unsuitable (also difficult) to characterize cyber attacks as model-based disturbances to NCSs. According to the results reported in [14–16], attackers and network defenders could dynamically design/change their attack and defense strategies, respectively. While many efforts to deal with cyber attacks and network security issues have been reported from the perspectives of networking and data communication, very few results have been reported from the system and control points of view [17–19], in particular there is so far no consideration of the effects of cyber attacks on the dynamic performances of NCSs.

In this paper, we address cyber attacks on NCSs explicitly from the control point of view and propose an optimal defense mechanism for the NCS under intelligent jamming attacks. The contributions of this work can be summarized as follows:

(1) Instead of using a model-based approach to the modeling of cyber attacks, a two-player zero-sum stochastic game is formulated to model the dynamic interactions between a jammer (as a attacker) and a sensor transmitter (as a defender) of the NCS. To our best knowledge, this is the first treatment of NCSs under jamming attacks by using stochastic game theories.
(2) An optimal defense mechanism is developed for the NCS to fight against intelligent jamming attackers, for which attacking strategies may be dynamic and random. Simulation and comparison studies demonstrate that the dynamic performance of the NCS being attacked by a jammer is much improved when the proposed defense mechanism is deployed, compared with those without such a mechanism.
(3) The cost function of the proposed stochastic game includes not only the resource costs used to conduct cyber-layer defense or attack actions, but also the dynamic performance (indexed by quadratic state errors) of the NCS. Therefore, when the two players (attacker and defender) in the cyber layer design/change their strategies, the impacts of their interactions on the dynamic performance of the NCS can be well taken into account.