Automatica 93 (2018) 55–63

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

A hybrid stochastic game for secure control of cyber-physical systems[☆]

Fei Miao [a,*], Quanyan Zhu [c], Miroslav Pajic [d], George J. Pappas [b]

[a] *University of Connecticut, Storrs, CT, USA*
[b] *University of Pennsylvania, Philadelphia, PA, USA*
[c] *New York University, Brooklyn, NY, USA*
[d] *Duke University, Durham, NC, USA*

ARTICLE INFO

Article history:
Received 29 August 2016
Received in revised form 31 August 2017
Accepted 26 December 2017

Keywords:
Stochastic game
Secure control
Saddle-point equilibrium

ABSTRACT

In this paper, we establish a zero-sum, hybrid state stochastic game model for designing defense policies for cyber-physical systems against different types of attacks. With the increasingly integrated properties of cyber-physical systems (CPS) today, security is a challenge for critical infrastructures. Though resilient control and detecting techniques for a specific model of attack have been proposed, to analyze and design detection and defense mechanisms against multiple types of attacks for CPSs requires new system frameworks. Besides security, other requirements such as optimal control cost also need to be considered. The hybrid game model we propose contains physical states that are described by the system dynamics, and a cyber state that represents the detection mode of the system composed by a set of subsystems. A strategy means selecting a subsystem by combining one controller, one estimator and one detector among a finite set of candidate components at each state. Based on the game model, we propose a suboptimal value iteration algorithm for a finite horizon game, and prove that the algorithm results an upper bound for the value of the finite horizon game. A moving-horizon approach is also developed in order to provide a scalable and real-time computation of the switching strategies. Both algorithms aim at obtaining a saddle-point equilibrium policy for balancing the system's security overhead and control cost. The paper illustrates these concepts using numerical examples, and we compare the results with previously system designs that only equipped with one type of controller.

1. Introduction

Cyber-Physical Systems (CPS) feature a tight integration of embedded computation, networks, controlled physical processes, and provide the foundation of critical infrastructures such as transportation systems, smart grids, water service systems and so on (Kim & Kumar, 2012). However, the integration structures also result in vulnerability under malicious attacks (Cardenas, Amin, Sionpoli, Perrig, & Sastry, 2009). Recoded incidents caused by attacks show that CPS attacks can disrupt critical infrastructures and lead to undesirable, catastrophic consequences (Slay & Miller, 2007). While cyber security tools have focused on prevention mechanisms, there are still challenges on how to leverage the ability of control systems to keep system resilient under a smart adversary.

Detection methods for various types of attacks have been analyzed in the literature. Pasqualetti, Dorfler, and Bullo (2013) propose a framework for attacks and monitors of CPS perspectives. Mo et al. (2012) analyze security challenges and countermeasures in smart grids. Pajic et al. (2014) present resilient state estimators for systems with noise and modeling errors. Humphreys (2013) analyzes spoofing attacks against cryptographically-secured Global Navigation Satellite System (GNSS) signals and detection strategies. Miao, Zhu, Pajic, and Pappas (2016) design a coding scheme for sensor outputs to detect stealthy data injection attacks over the communication channel.

[☆] This material is based on research sponsored by DARPA under agreement number FA8750-12-2-0247. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government. This work was also supported in part by NSF CNS-1505701, CNS-1505799 grants, and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy. The material in this paper was partially presented at the 52nd IEEE Conference on Decision and Control, December 10–13, 2013, Florence, Italy and the 53rd IEEE Conference on Decision and Control, December 15–17, 2014, Los Angeles, CA, USA. This paper was recommended for publication in revised form by Associate Editor Bert Tanner under the direction of Editor Christos G. Cassandras.

[*] Corresponding author.
E-mail addresses: fei.miao@uconn.edu (F. Miao), quanyan.zhu@nyu.edu (Q. Zhu), miroslav.pajic@duke.edu (M. Pajic), pappasg@seas.upenn.edu (G.J. Pappas).

https://doi.org/10.1016/j.automatica.2018.03.012
0005-1098/© 2018 Elsevier Ltd. All rights reserved.

In general, attack models are used as parameters to design defense schemes. However, a specific detection approach alone is not sufficient, when the system does not have knowledge which attack will happen among various types of potential attacks. CPS are usually resource constrained systems, which prevents running all available modules at the same time. Besides security, other requirements like optimal cost need to be addressed during control systems design. Consequently, considering control and defense costs with the effects of multiple attacks, strategic methods that balance the system performance and security requirements are necessary. In this work, we consider the case that at each time instant, only one detector is active because of the limits of resources. Our approach can be generalized to more than one detector being active at every time instance.

The application of game theory to security problems has raised a lot of interest in recent years. Selected works that apply game-theoretic approaches in computer networks security and privacy problems are summarized by Manshaei, Zhu, Alpcan, Basar, and Hubaux (2013). Zhu and Martinez (2011) propose a receding-horizon dynamic Stackelberg game model for systems under correlated jamming attacks. Zhu and Basar (2015) propose game-theoretic methods for robust and resilient control of CPSs. However, none of these works have considered switching policies under multiple types of attacks, with payoffs as functions of system dynamics and probabilistic detection rate.

Building a framework that captures the hybrid system dynamics and interactions with attacks is pivotal for security analysis and design of CPS. To achieve this goal, our first step is to establish a zero-sum hybrid stochastic game model. The hybrid state of the game model contains a dynamic system state that captures the evolution of the physical processes, and discrete cyber modes that represent different security states of the CPS according to information provided by the detector. Then a suboptimal value iteration algorithm is developed for the finite horizon hybrid stochastic game. Compared with our previous game model (Miao, Pajic, & Pappas, 2013) that only switches between two controllers against replay attacks and needs strategy history to calculate a strategy, in this work the hybrid state stochastic game strategy calculation process does not depend on the strategy history.

We then propose a moving-horizon computation methodology to reduce the computational complexity of finding a saddle-point equilibrium for the hybrid stochastic game. This is a scalable and computationally efficient algorithm. At each stage, the system selects a window of finite length for the physical state, and computes the stationary saddle-point strategies for the associated finite stochastic game, with the game state reformulated as the joint cyber and physical states. A preliminary result of the moving-horizon algorithm appeared in the conference paper Miao and Zhu (2014); in this journal version, we have included more details about different types of attacks and each element of the game model, revised analysis of the moving horizon algorithm compared with the suboptimal algorithm, and added more simulation results. The cost comparison with the suboptimal algorithm shows that the real-time algorithm does not sacrifice system performance much. The contributions of this work are summarized as follows:

(1) We formulate a zero-sum, hybrid stochastic game framework for designing a switching policy for a system under various types of attacks.
(2) We design a suboptimal algorithm for the finite horizon hybrid stochastic game, and prove that the algorithm provides an upper bound for the optimal cost of the system.
(3) We develop a real-time algorithm to reduce the computation overhead of the game model.

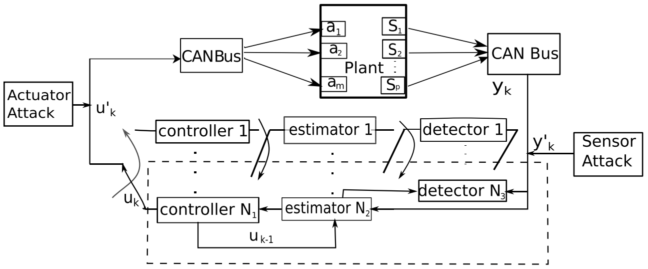

Fig. 1. Switching system diagram, where the system is equipped with N_1 controllers, N_2 estimators and N_3 detectors and switches among N subsystems. A subsystem (controller N_1, estimator N_2, and detector N_3) is chosen here.

This paper is organized as follows. We describe the system, attack models, and motivation of game-theoretic techniques for switching policies in Section 2. In Section 3, we formulate a zero-sum, hybrid stochastic game between the system and the attacker. A suboptimal algorithm for the finite horizon game is developed in Section 4. The moving horizon algorithm and its computational complexity are analyzed in Section 5. Section 6 compares the complexity and system performance of the finite horizon and the receding horizon algorithms. Finally, Section 7 provides concluding remarks.

2. Switched system and attack model

We consider the CPS security problem when both the system and attacker have limited knowledge about the opponent. The system is equipped with multiple controllers/estimators/detectors, such that each combination of these components constitutes a subsystem. A subsystem has a probability to detect specific types of attacks with different control and detection costs. To balance the security overhead and the control cost under various attacks, we consider switching among subsystems (choose a model for every component) according to the system dynamics and detector information. A switched system model is shown in Fig. 1, and the model of each component is described with a concrete example in the rest of this section. It is worth noting that the set of subsystems is not restricted and can be further generalized.

LTI plant and sensor attack model: Consider a class of LTI plants described by:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k + \mathbf{w}_k, \quad \mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{v}_k, \tag{1}$$

where $\mathbf{x}_k \in \mathbb{R}^n$, $\mathbf{u}_k \in \mathbb{R}^p$ and $\mathbf{y}_k \in \mathbb{R}^m$ denote the discrete time state, input and output vectors respectively, and $\mathbf{w}_k \sim \mathcal{N}(0, \mathbf{Q})$, $\mathbf{v}_k \sim \mathcal{N}(0, \mathbf{R})$ are independent and identically distributed (IID) Gaussian random noise. The initial state is $\mathbf{x}_0 \sim \mathcal{N}(\bar{\mathbf{x}}_0, \Sigma)$. Sensors or the communication between sensors and estimators are vulnerable, and attacker can change values $\mathbf{y}_k$ that sent from sensors of system (1), and the compromised sensor measurements are defined as $\mathbf{y}'_k$ according to the types of attacks we consider. For instance, if the attacker can inject arbitrary data $\mathbf{y}^a_k$ to sensors, $\mathbf{y}'_k = \mathbf{y}_k + \mathbf{y}^a_k$; for replay attacks, the attacker can choose the replay window size T_2, let $\mathbf{y}'_k = \mathbf{y}_{k-T_2}$ and decide whether to send the delayed plant outputs at k.

Estimators: The physical dynamical state of the system is provided by an estimator, for instance, attack resilient estimator (Pajic et al., 2014), l_1 norm state estimator (Pajic, Tabuada, Lee, & Pappas, 2015), fault detection filter (Zhong, Ding, Lam, & Wang, 2003), or the widely applied Kalman filter. When $(\mathbf{A}, \mathbf{B})$ is stabilizable, $(\mathbf{A}, \mathbf{C})$ is detectable, a steady state Kalman filter exists.

Controllers: A state feedback control law is described as $\mathbf{u}_k = L(\hat{x}_{k|k})$, where $L(\cdot)$ is a linear function, $\hat{x}_{k|k}$ is the estimated state. Mo