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.

The remainder of this paper is organized as follows. The model of the NCS with jamming attacks is built in Section 2. The two-player zero-sum stochastic game is formulated for the NCS in Section 3. The stochastic game is solved for the optimal defense mechanism in Section 4. A linear NCS is used to illustrate the proposed stochastic game formulation for the NCS with jamming attacks and comparison studies are also conducted in Section 5. Finally, conclusions are made in Section 6.

Notation: $\mathbb{R}^n$, $\mathbb{R}^m$ denotes the n dimensional and m dimensional Euclidean space, respectively. The superscript 'T' denotes the transposition of a vector or matrix.

2. Modeling of the networked control system under jamming attacks

The following discrete-time linear system is considered here:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k \tag{1}$$

where, $\mathbf{x}_k \in \mathbb{R}^m$ is the state vector, $\mathbf{u}_k \in \mathbb{R}^n$ is the control input. $\mathbf{A}$ and $\mathbf{B}$ are system constant matrices with appropriate dimensions.

The state feedback controller is

$$\mathbf{u}_k = \mathbf{K}\mathbf{x}_k. \tag{2}$$

In the networked control system (NCS) shown in Fig. 1, feedback measurements are transmitted over wireless communication networks. Generally, wireless communication networks are extremely vulnerable to physical-layer attacks such as jamming attacks. According to [20], jamming attacking strategies are usually implemented by introducing radio noise signals on wireless mediums to overwhelm the reception of useful signals at the receiver sides. The jamming attack is successful when the power levels of noise signals sent by the jammer are greater than that of transmitting signals from transmitter sides. Since adversaries can launch jamming attacks by jamming the communication channels, the feedback measurements will be lost. Without the information feedback from the other side, the NCS becomes an open-loop system, which may not be stable any more.

In order to properly model the jamming attack, let us define the state of the feedback communication channel $\gamma_k \in \{0, 1\}$. While $\gamma_k = 0$ indicates the failure state, $\gamma_k = 1$ is the normal state of the feedback communication channel. Thus, the closed-loop networked control system is described by the following stochastic equation:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \gamma_k \mathbf{B}\mathbf{K}\mathbf{x}_k. \tag{3}$$

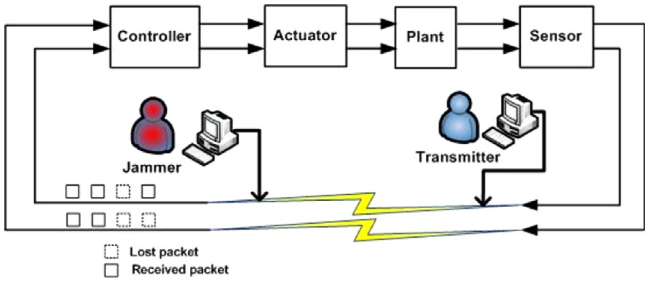

Fig. 1. The networked control system (NCS) with a jamming attacker.

While most work in the literature considers that γ_k follows random processes, such as Markov chain process and Bernoulli process, those processes are not able to model the jamming-anti-jamming (attack–defense) situations when the NCS is under jamming attacks. Here, the state of γ_k depends on the result of the attack–defense game between the jammer and the sensor transmitter. In this paper, a two-player zero-sum stochastic game is formulated for the NCS under jamming attacks. Our main objective in this work to design an optimal defense mechanism for the sensor transmitter with limited network resources.

3. Formulation of the stochastic attack–defense game in the NCS

In this section, we formulate the attack–defense game between the sensor transmitter and the jammer in the NCS as a two-player zero-sum stochastic game. We consider the sensor transmitter as the defender P^D, while the jammer as the attacker P^J. The two-player zero-sum stochastic game considered here is defined by the following elements.

3.1. States

Being different from existing stochastic games, every state in this stochastic game for the NCS is composed of two parts. One part is composed of the elements of the state of the NCS $\mathbf{x}_k = [x_k^1, \ldots, x_k^i, \ldots, x_k^m]^T$, while the other element is the state of the wireless network γ_k. The collection of these elements $(x_k^1, \ldots, x_k^i, \ldots, x_k^m, \gamma_k)$ makes the state $s_k = (x_k^1, \ldots, x_k^i, \ldots, x_k^m, \gamma_k)$ of this stochastic game at the kth time slot. The set of γ_k is $\{0, 1\}$. Each element of the state of the NCS x_k^i is considered to be within the range $[\underline{l}, \bar{l})$. Therefore, the state space of this stochastic game is $\mathcal{S} = \{0, 1\} \times [\underline{l}, \bar{l}) \times \cdots \times [\underline{l}, \bar{l}) \times \cdots \times [\underline{l}, \bar{l})$. A stochastic game is also called a competitive Markov decision process (MDP) [21]. It is usually solved by using stochastic dynamic programming approaches, such as value iteration and policy iteration [22]. However, a continuous-state stochastic game is difficult to be solved by these approaches which are essentially discrete-state and discrete-time iterations. Therefore, discretization of the continuous state space of a MDP has been used to approximate the value functions of a continuous MDP or a stochastic game [23,24]. In this paper, the range $[\underline{l}, \bar{l})$ is divided into discrete intervals and represented by discrete numbers [25]. For instance, if the range is $[0, 10)$, it can be divided into ten intervals, such as $[0, 1), [1, 2), \ldots, [9, 10)$. These intervals can be represented by discrete integers, such as $\{1, 2, \ldots, 10\}$. Therefore, the continuous state space of the stochastic game is estimated by a discrete state space.

We assume the two players both have access to the model of the NCS a priori and the state of the wireless network at the beginning of each time slot. By sensing the NCS, both the sensor transmitter and the jammer know the state of the stochastic game at the beginning of each time slot.

Remark 1. Here, we consider that the state of the NCS is bounded. This could be guaranteed by adding a saturation unit when we design a controller [26,27].

3.2. Actions

The objective of the attacker P^J is to bring down the dynamic performance of the NCS such as convergence rates and state errors by sending noisy signals with a certain power level to jam the

wireless network. The objective of the defender P^D is to guarantee the dynamic performance of the NCS by transmitting signals with higher power levels than that of jammer's noisy signals.

The actions for P^J and P^D at time slot k are power levels to transmit signals denoted by a_k^J and a_k^D, respectively. For the simplicity of calculations, we consider a fixed power level case $a_k^J \in \mathcal{A}^J = \{0, J\}$ and $a_k^D \in \mathcal{A}^D = \{0, D\}$, where $\mathcal{A}^J$ and $\mathcal{A}^D$ are two action sets. Each player can either transmit a signal with the fixed power level (J or D) or not at any time slot.

3.3. State transitions

The stochastic game proceeds from one state to the other according to transition probabilities controlled jointly by the actions of the defender and the attacker, and also the current state of the game at the beginning of each time slot, denoting by the mapping: $\mathcal{M} : \mathcal{S} \times \mathcal{A}^D \times \mathcal{A}^J \longrightarrow \mathcal{S}$. At the beginning of time slot k, the current state and the next possible state are denoted by S_k and S_{k+1}, respectively. The transition probability is defined as follows:

$$p(s'|s, a_k^J, a_k^D) = \mathbb{P}\{S_{k+1} = s'|S_k = s, a_k^J, a_k^D\} \tag{4}$$

where, s' and s are within the state space $\mathcal{S} = \{0, 1\} \times [\underline{l}, \bar{l}) \times \cdots \times [\underline{l}, \bar{l}) \times \cdots \times [\underline{l}, \bar{l})$, $a_k^J \in \mathcal{A}^J$, $a_k^D \in \mathcal{A}^D$.

The transitions among the states of the stochastic game in a scalar NCS are illustrated in Fig. 2. In Fig. 2, p_{00}, p_{01}, p_{10}, p_{11} are transition probabilities between the states, while X_k^0, X_{k+1}^0 are the states of the scalar NCS at kth and (k+1)th time slots, respectively, when the state of the wireless network is 0, X_k^1, and X_{k+1}^1 are the states of the scalar NCS at kth and (k+1)th time slots, respectively, when the state of the wireless network is 1.

3.4. Cost functions and strategies

Each player has a cost function consisting of two parts. One part comes from the cost of sending signals with the fixed power level. The other part is the degraded dynamic performance of the NCS. These two parts are both converted into monetary costs here. For example, considering the state of the networked control system is $\mathbf{x}_k$ and the defender transmits a signal with a power level D which needs network resource M, the cost function of the defender has the following form:

$$c_1 M + c_2 \mathbf{x}_k^T Q \mathbf{x}_k$$

where, the parameters c_1 and c_2 are monetary parameters which are related to the needed network resources and the system state, Q is a weighting matrix.

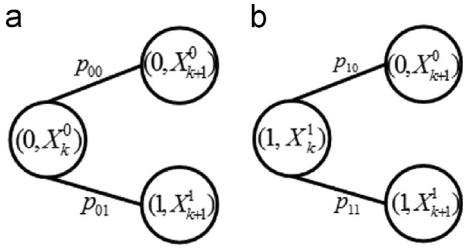

Fig. 2. Transitions of state pairs.

In this paper, strategies of two players are state dependent and mixed strategies. According to [16], mixed strategies ensure that there exists a saddle-point equilibrium at each stage of the game. The mixed strategy of P^D,

$$f^D(s) := [f_1^D(s), f_2^D(s)]^T, \tag{5}$$

is defined as a probability distribution on the set of defense actions $\mathcal{A}^D$ for a given state $s \in S$, $\sum_{i=1}^{2} f_i^D(s) = 1$.

The mixed strategy of P^J is

$$g^J(s) := [g_1^J(s), g_2^J(s)]^T,$$
$$\sum_{i=1}^{2} g_i^J(s) = 1. \tag{6}$$

We denote immediate game values at the *kth* time slot with the state s for the defender and the attacker by game matrices $R_k^D(s)$ and $R_k^J(s)$ for all possible defense–attack action pairs. In zero-sum games, $R^J(s) = -R^D(s)$. Thus, we only show the defender game matrices in the following sections. The defender game matrices have the following structure:

$$R_k^D(s) = \begin{bmatrix} c_1 M_1 + c_2 \mathbf{x}_k^T Q \mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k \geq \overline{b}\}} & c_1 M_2 + c_2 \mathbf{x}_k^T Q \mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k \geq \overline{b}\}} \\ -c_1 M_3 + c_2 \mathbf{x}_k^T Q \mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k \geq \overline{b}\}} & 0 \end{bmatrix} \tag{7}$$

where c_1, c_2, M_1, M_2 and M_3 are monetary parameters by investing recourses to defend for different attack actions. In this game matrix, numerical values are only representative and have no units. We assume that the attacker gets some payoffs for bringing down the dynamic performance of the NCS only when the system state error is over given lower bound $\overline{b}$.

Remark 2. The game matrix (7) specifies both players' action spaces and cost functions. For example, as rows of the matrix are the defender's actions, row 1 corresponds to defend and row 2 corresponds to do nothing. As columns of the matrix are the attacker's actions, column 1 corresponds to attack and column 2 corresponds to do nothing. The elements of the matrix are costs/benefits that correspond to the action pairs. By bringing in $\mathbb{1}$ in (7), we mean that every control system has a certain tolerance to the deviation from its operating equilibrium. Only when the state of the control system is above its tolerance $\overline{b}$, it begins to result in costs or benefits for the defender and attacker.

For any time slot k, the one-stage value of the stochastic game r_k^D, being only one scale element of the game matrix (7), has the following form:

$$r_k^D(s) = g^J(s)^T(s) R_k^D(s) f^D(s). \tag{8}$$

For an N-stage stochastic games, we define the action history information set until the kth time slot by $I_k^J = \{a_0^J, a_1^J, \ldots, a_{k-1}^J\}$ for the attacker, $I_k^D = \{a_0^D, a_1^D, \ldots, a_{k-1}^D\}$ for the defender. The expected sum of the discounted cost of the defender is given by

$$V^D(s) := E\{\sum_{k=0}^{N} \alpha^k r_k^D(s, I_k^J, I_k^D)\} \tag{9}$$

where s is the initial state, and α^k is the discounted factor at time slot k.

Remark 3. A discounted factor α^k is used to capture the practical situation that a cost/benefit of 1 unit at time slot $k+1$ is worth only $\alpha < 1$ of what it was worth at time k.

4. Solving stochastic game for optimal defense policy

In the previous section, we formulated the two-player zero-sum stochastic game. In this stochastic game, the defender aims to minimize his expected total cost, $V^D(s)$, while the attacker wants to maximize his expected payoff $V^J(s)$. For zero-sum games, $V^D(s)+V^J(s)=0$. Thus, we give details on how to solve this stochastic game only from the defender point of view to get the optimal defense policy by a value iteration method in this section. We also denote the expected total value of the stochastic game by $V_k(s)$ at kth stage for simplicity and one-stage value $r_i(s)$ as a simplified form of $r_k^D(s)$

The expected total value of this stochastic game at time instant k, with state $s\in\mathcal{S}$ is defined by

$$V_k(s)=E\left\{\sum_{i=k}^{N}\alpha^i r_i(s)\right\} \tag{10}$$

where, α^i is the discounted factor, $r_i(s)$ is the stochastic game value for one stage.

At a given stage k, we define a Q-function $Q_k(a,d,s)$ as an expected discounted cost when the attacker takes action a, and the defender takes action d, when the current state is s. Then, the optimal value with state $s\in\mathcal{S}$ in the stochastic game is

$$V_k(s)=\min_{f^D(s)}\max_{g^J(s)}E\left\{\sum_{d\in A^D(s)}g^J(s)^T Q_k(a,d,s)f^D(s)\right\}, \tag{11}$$

where $Q_k(a,d,s)$ is updated by

$$Q_k(a,d,s)=r_k(a,d,s)+\alpha\sum_{s'\in\mathcal{S}}p(s'|s,a,d)V_{k+1}(s') \tag{12}$$

where $r_k(a,d,s)$ is the game value at kth stage, $V_{k+1}(s')$ is the total expected cost from the next stage with state s'.

The value of the stochastic game can be described as

$$V_k(s)=\min_{f^D(s)}\max_{g^J(s)}g^J(s)^T Q_k(a,d,s)f^D(s). \tag{13}$$

In order to solve the problem in Eq. (13), we assume the defender's strategy $f^D(s)$ is fixed, then it becomes

$$\max_{g^J(s)} g^J(s)^T Q_k(a,d,s)f^D(s). \tag{14}$$

Since $Q_k(a,d,s)f^D(s)$ is a vector, and $g^J(s)$ is a probability distribution, the solution of the problem in Eq. (13) is to find the maximal element of the vector $Q_k(a,d,s)f^D(s)$. Then, the problem in Eq. (13) is simplified as

$$\min_{f^D(s)}\max_i[Q_k(a,d,s)f^D(s)]_i. \tag{15}$$

By defining $z=\max_i[Q_k(a,d,s)f^D(s)]_i$, we have $[Q_k(a,d,s)f^D(s)]_i\le z$. Thus, the original min–max problem becomes the following linear programming (LP) problem with constraints,

$$\begin{aligned}&\min_{f^D(s)} \quad z\\ &s.t. \qquad [Q_k(a,d,s)f^D(s)]_i\le z,\\ &\qquad\quad f^D(s)\ge\mathbf{0},\\ &\qquad\quad \mathbf{1}^T f^D(s)=1.\end{aligned} \tag{16}$$

By defining augmented variable vectors $\pi = [f^D(s)^T, z]^T$, $\mathbf{1} = [1, 1, 0]^T$, $\mathbf{0} = [0, 0, 1]^T$, and $\overline{Q} = [Q_k(a, d, s), -\mathbf{1}]$, the LP problem in Eq. (16) is turned to the following LP problem:

$$\begin{aligned} \min_{\pi} \quad & \mathbf{0}^T \pi \\ s.t. \quad & \overline{Q}\pi \le \mathbf{0}, \\ & f^D(s) \ge \mathbf{0}, \\ & \mathbf{1}^T \pi = 1. \end{aligned} \tag{17}$$

The value of the stochastic game can be obtained after solving the above LP problem.

5. Simulations

In this section, we demonstrate the formulation of the proposed stochastic security game for a linear NCS under jamming attacks and evaluate the dynamic performance of the NCS under jamming attacks. With the proposed defense mechanism, the packet-loss rate of the communication channel in the NCS is sharply reduced and the dynamic performance of the NCS under jamming attacks is much improved.

A Phantom Premium 1.5A robotic arm with 3 degrees of freedoms (DOFs) is used as the plant of the NCS. Since our main purpose is to demonstrate the formulation and effectiveness of the proposed stochastic security game, we take only the modeling and control of the first joint of the robotic arm into consideration for simplicity. It is described by the following model:

$$m\ddot{q}(t) + c\dot{q}(t) = \tau(t) \tag{18}$$

where $q(t)$ and $\dot{q}(t)$ are the actuator motor position and velocity, respectively, m is the inertia, and c is the Coriolis forces (torques) parameter.

According to the setup of the Phantom Premium 1.5A robotic arm, we get the model parameters as follows: $m = 0.107\ \mathrm{kg \cdot m^2}$ and $c = 0.08$ Nms. Let $x(t) = [\dot{q}(t), q(t)]^T$, $u(t) = \tau(t)$ be the system state and input. Its state space model is given by

$$\dot{x}(t) = \begin{bmatrix} -0.75 & 0 \\ 1 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 9.35 \\ 0 \end{bmatrix} u(t). \tag{19}$$

The sampling period is $h = 0.01$ s. A LQR controller is designed for this NCS without jamming attacks, shown as follows.

$$\mathbf{u}_k = -[0.9777, 0.9533]\mathbf{x}_k.$$

The discretization is used for the two elements of the state of this NCS x_k^1, x_k^2. The two elements of the state of this NCS are considered to be within the range [0, 1) and [0, 10), respectively. To discretize the continuous state space of the stochastic game, the range of x_k^1 is divided into 10 discrete intervals $[0, 0.1), [0.1, 0.2), \ldots, [0.9, 1)$ and represented by 10 discrete numbers $\{0.1, 0.2, \ldots, 1\}$. The range of x_k^2 is also divided into 10 discrete intervals $[0, 1), [1, 2), \ldots, [9, 10)$ and represented by 10 discrete numbers $\{1, 2, \ldots, 10\}$. The set of γ_k is $\{0, 1\}$. Thus, the state of this stochastic game at k time slot is $s_k = (x_k^1, x_k^2, \gamma_k)$. Its state space is $\mathcal{S} = \{0.1, 0.2, \ldots, 1\} \times \{1, 2, \ldots, 10\} \times \{0, 1\}$.

Two matrix games at k time slot are considered for both $\gamma_k = 0$ and $\gamma_k = 1$ cases, to indicate different extents of the difficulty to attack and defend the communication channel. They are shown in Tables 1 and 2. The transition probabilities are in the brackets. For the indicator function $\mathbb{1}_{\{Tr(P_{k+1|k})\} \ge \overline{b}} = 1$, we choose $\overline{b} = 1.5$ here.

Table 1
The matrix game at k time slot when $\gamma_k = 0$.

Defender	Attacker	
	J	0
D	$5c_1 + c_2\mathbf{x}_k^T\mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k^T\mathbf{x}_k \geq \bar{b}\}}$	$2c_1 + c_2\mathbf{x}_k^T\mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k^T\mathbf{x}_k \geq \bar{b}\}}$
	(0.2, 0.8)	(0.3, 0.7)
0	$-c_1 + c_2\mathbf{x}_k^T\mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k^T\mathbf{x}_k \geq \bar{b}\}}$	0
	(0.9, 0.1)	(0.5, 0.5)

Table 2
The matrix game at k time slot when $\gamma_k = 1$.

Defender	Attacker	
	J	0
D	$3c_1 + c_2\mathbf{x}_k^T\mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k^T\mathbf{x}_k \geq \bar{b}\}}$	$c_1 + c_2\mathbf{x}_k^T\mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k^T\mathbf{x}_k \geq \bar{b}\}}$
	(0.1, 0.9)	(0.2, 0.8)
0	$-2c_1 + c_2\mathbf{x}_k^T\mathbf{x}_k \mathbb{1}_{\{\mathbf{x}_k^T\mathbf{x}_k \geq \bar{b}\}}$	0
	(0.8, 0.2)	(0.5, 0.5)

We define the cost function parameters in the game matrix as $c_1 = 0.85$ and $c_2 = 0.08$, and the discounted factor $\alpha = 0.9$. According to the proposed method for solving the stochastic game in the previous section, we get optimal defense and attack strategies for all the possible states. The strategies at four states are shown in Figs. 3 and 4. From these two figures, it can be seen that the convergence rates for this stochastic game at the four states are very fast. Also, it can be observed that optimal strategies could be either deterministic (such as at state (0, 2, 1) for both the defender and the attacker) or stochastic (such as at states (0, 3, 1) and (0, 3, 0) for both the defender and the attacker). The optimal defense strategies can give suggestions to the sensor transmitter how to choose its defense actions. For instance, according to the obtained optimal defense strategies, the sensor transmitter should always send its measurement signal with high power level when the state is (0, 2, 1) and should send its measurement signal with high power level with the probability 0.09 when the state is (0, 3, 0).

Then, in order to evaluate the effect of the proposed defense mechanism on the communication channel state, the following two cases are considered.

- *Case* 1: There is no defense mechanism for the sensor transmitter of the NCS under jamming attacks.
- *Case* 2: The proposed defense mechanism is adapted by the sensor transmitter of the NCS under jamming attacks.

The simulations run 100 times in the Matlab R2012a environment. Packet-loss rate is used as the metric for the communication channel performance comparison between Case 1 and Case 2. For the total 100 simulations, the average packet-loss rate of the communication channel in

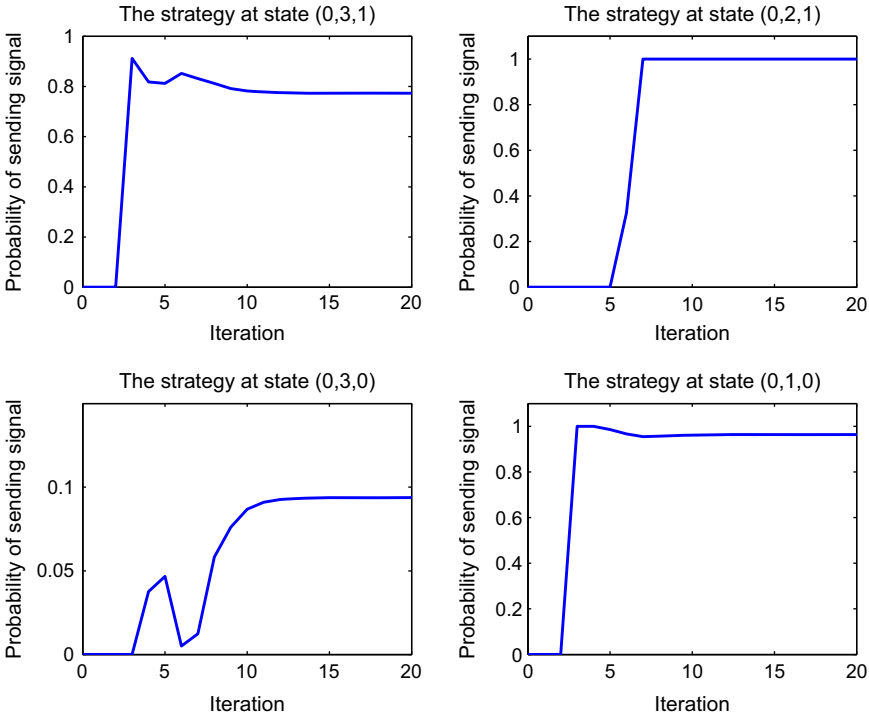

Fig. 3. Optimal defense strategies when $c_1=0.85$, $c_2=0.08$ and $\alpha=0.9$.

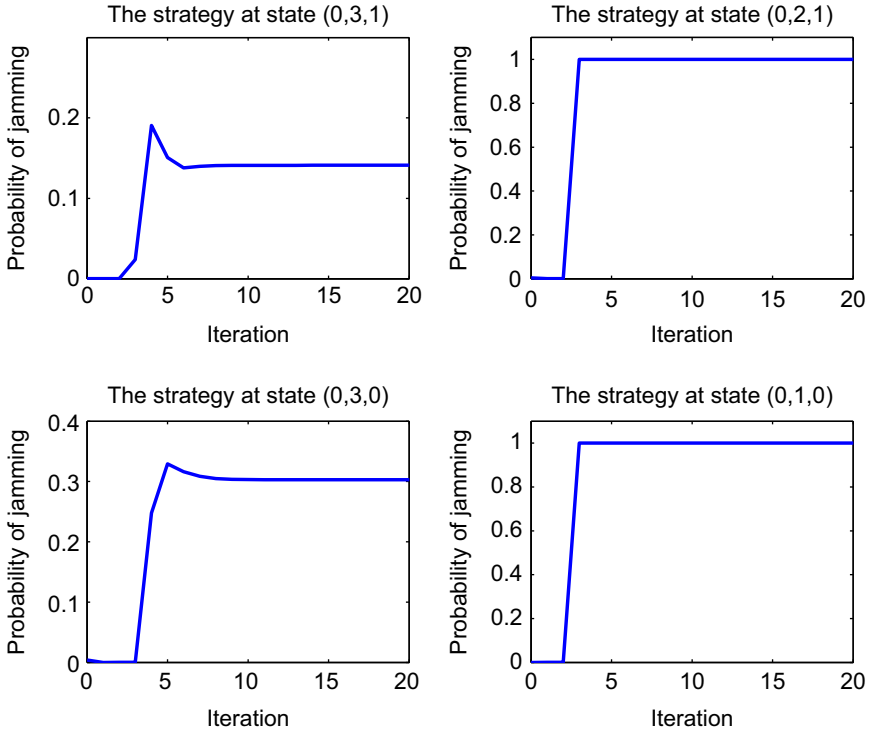

Fig. 4. Optimal attack strategies when $c_1=0.85$, $c_2=0.08$ and $\alpha=0.9$.

Case 1 (without the proposed defence mechanism) is 51.34%, while the average packet-loss rate of the communication channel in Case 2 (with the proposed defence mechanism) is reduced to 25.67%. Fig. 5 shows a typical sample of the communication channel state jumping between 0 and 1 in Case 1. Without the proposed defense mechanism, its packet-loss rate is 42.66% (the ratio of the communication channel state being 0). Fig. 6 shows a typical sample of the communication channel state jumping process in Case 2. With the proposed defense mechanism, its packet-loss rate is reduced to 24.33%. From the above observations, it can be seen that the proposed defense mechanism improves the network performance quite significantly when there is a random jamming attacker.

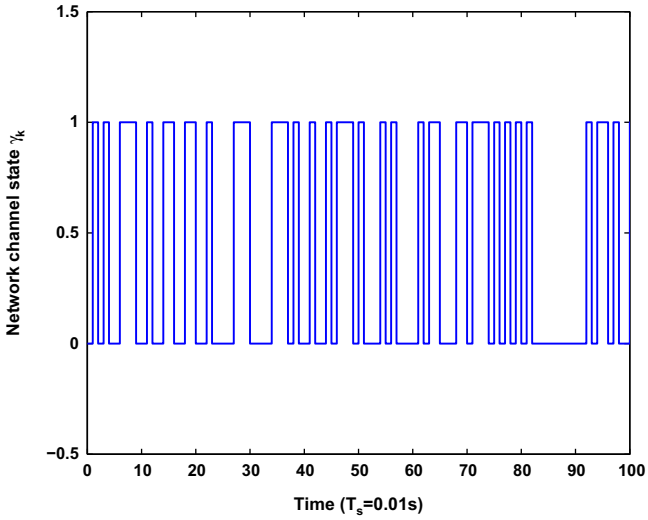

Fig. 5. One sample of the network state without a defense mechanism.

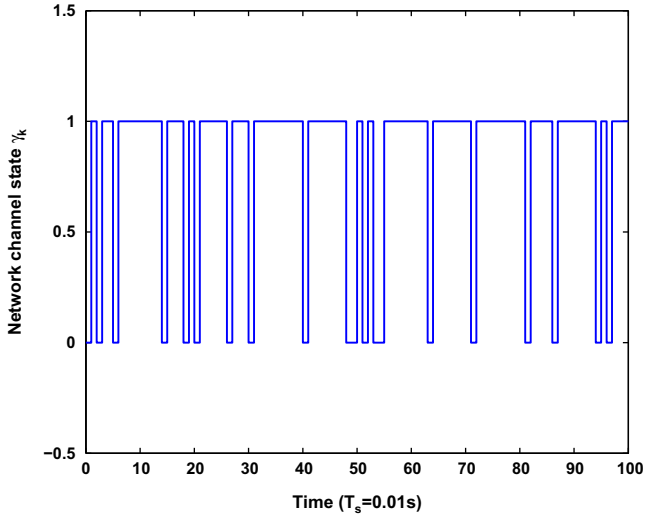

Fig. 6. One sample of the network state with the proposed defense mechanism.

Finally, two initial states ($\mathbf{x}_0 = [0, 3]^T$ and $\mathbf{x}_0 = [0, 2]^T$) are considered to evaluate the effectiveness of the proposed defense mechanism in improving the dynamic performance of the robotic arm. The mean square error (MSE) of the state vector $\mathbf{x}_k = [x_k^1, x_k^2]^T$ of the NCS is chosen as the dynamic performance metric for the NCS. The state trajectory of the original NCS with the LQR controller is used as the reference for calculating the mean square errors. The simulations run 100 times in Matlab R2012a environment. The MSEs of the state vectors are shown in Figs. 7 and 8. The comparison results from these two figures demonstrate that the dynamic performance of the NCS is much improved when it is under randomly jamming attacks.

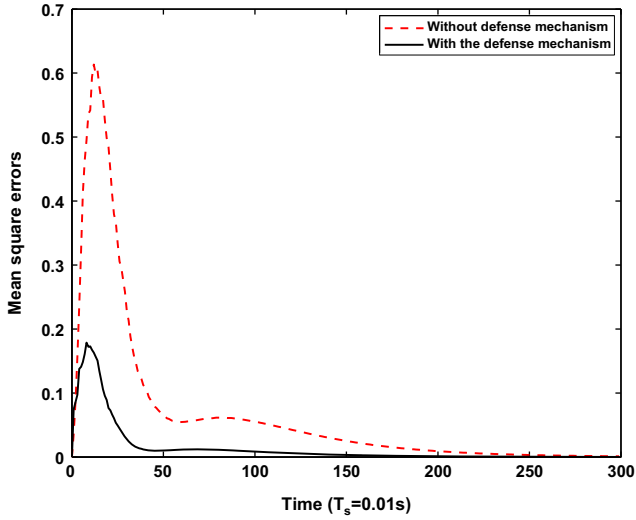

Fig. 7. The mean square errors of the NCS state $\mathbf{x}_k$ with the initial state $\mathbf{x}_0 = [0,\ 3]^T$.

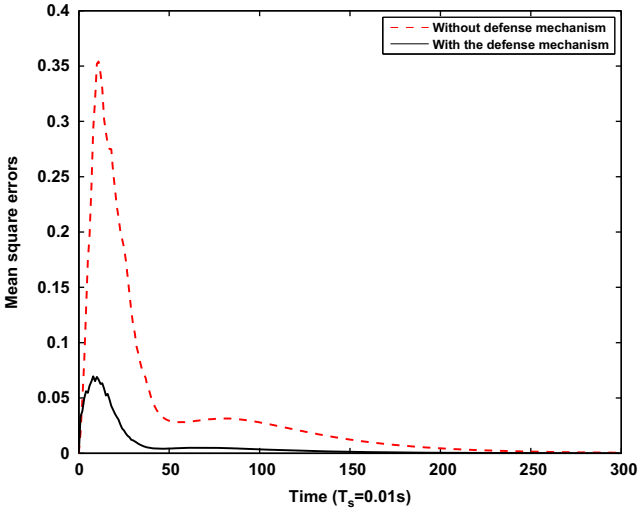

Fig. 8. The mean square errors of the NCS state $\mathbf{x}_k$ with the initial state $\mathbf{x}_0 = [0,\ 2]^T$.

6. Conclusions and future work

In this work, we have designed an optimal defense mechanism for the NCS to deal with intelligent jamming attackers, for which the attacking strategies may be changed dynamically or randomly. Compared with existing work, an important difference lies on the fact that we do not assume a pre-defined model for the attack. Instead, a two-player zero-sum stochastic game is proposed to describe the dynamic interactions between the defender (i.e. the sensor transmitter) and the attacker (i.e. the jammer) in the NCS. Simulation and comparison results show that the proposed optimal defense mechanism reduces the packet-loss rate of the communication channel in the NCS and improves the dynamic performance of the NCS when it is under randomly jamming attacks.

Several interesting research directions for future work are listed as follows:

- A zero-sum stochastic game is formulated in this paper. It can be extended to general-sum stochastic games in future. In general-sum games, the existence of multiple Nash equilibriums also needs to be investigated.
- Only two players are considered in this work. It will be interesting to consider one defender and multiple-attacker scenarios.

Acknowledgments

The authors would like to thank Professor Minyi Huang in the School of Mathematics and Statistics at Carleton University for helpful and encouraging discussions.

References

[1] W. Zhang, M.S. Branicky, S.M. Phillips, Stability of networked control systems, IEEE Control Syst. Mag. 21 (1) (2001) 84–99.
[2] Y. Xu, H. Su, Y.-J. Pan, Z.G.W. adn Weihua Xu, Stability analysis of networked control systems with round-robin scheduling and packet dropouts, J. Frankl. Inst. 350 (8) (2013) 2013–2027.
[3] X. Ye, S. Liu, P.X. Liu, Modeling and stabilization of networked control system with packet loss and time-varying delays, IET Control Theory Appl. 4 (6) (2010) 1094–1100.
[4] Y. Shi, B. Yu, Robust mixed h_2/h_∞ control of networked control systems with random time delays in both forward and backward communication links, Automatica 47 (4) (2012) 754–760.
[5] Y. Song, J. Wang, Y. Shi, C. Li, h_∞ control of networked control systems with time delay and packet disordering, J. Frankl. Inst. 350 (6) (2013) 1596–1616.
[6] S. Gorman, Electricity grid in U.S. penetrated by spies, The Wall Street Journal (2009) A1.
[7] J. Vijayan, Stuxnet renews power grid security concerns, Computer World (2010).
[8] E. Byres, J. Lowe, The myths and facts behind cyber security risks for industrial control systems, in: the VDE Kongress 2004, Berlin, Germany, 2004.
[9] A.A. Cardenas, S. Amin, S. Sastry, Research challenges for the security of control systems, in: Proceedings of the 3rd conference on Hot topics in security, Berkeley, CA, USA, 2008, pp. 1–6.
[10] A. Teixeira, D. Perez, H. Sandberg, K.H. Johansson, Attack models and scenarios for networked control systems, in: Proceeding of the HiCoNS'12, Beijing, China, 2012, pp. 55–64.
[11] S. Amin, A. Cardenas, S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, Berlin/Heidelberg, 2009, pp. 31–45.
[12] S. Liu, X.P. Liu, A.E. Saddik, Denial-of-service (dos) attacks on load frequency control in smart grids, in: Proceedings of the IEEE PES 4th Innovative Smart Grid Technologies (ISGT) Conference, Washington, DC, 2013, pp. 1–6.

[13] Y. Mo, T.H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure, Proc. IEEE 100 (1) (2012) 195–209.
[14] T. Alpcan, T. Basar, Network Security: A Decision and Game-Theoretic Approach, Cambridge University Press, Cambridge, UK, 2011.
[15] B. Wang, Y. Wu, K.J.R. Liu, T.C. Clancy, An anti-jamming stochastic game for cognitive radio networks, IEEE J. Sel. Areas Commun. 29 (2011) 877–889.
[16] M.L. Littman, Markov games as a framework for multi-agent reinforcement learning, in: Proceedings of the 11th International Conference on Machine Learning, 1994, pp. 157–163.
[17] M. Zhu, S. Martinez, Stackelberg-game analysis of correlated attacks in cyber-physical systems, in: Proceedings of the 2011 American Control Conference, San Francisco, CA, USA, 2011, pp. 4063–4068.
[18] Q. Zhu, T. Basar, Robust and resilient control design for cyber-physical systems with an application to power systems, in: Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), Orlando, FL, USA, 2011, pp. 4066–4071.
[19] S. Liu, X.P. Liu, A.E. Saddik, A stochastic security game for kalman filtering in networked control systems (ncss) under denial of service (dos) attacks (invited paper), in: the 3rd IFAC International Conference on Intelligent Control and Automation Science (ICONS 2013), Chengdu, China, 2013, pp. 106–111.
[20] A.D. Wood, J.A. Stankovic, Denial of service in sensor networks, Computer 35 (10) (2011) 54–62.
[21] J. Filar, K. Vrieze, Competitive Markov Decision Process, Springer, New York, USA, 1997.
[22] M.L. Puterman, Markov Decision Processes: Discrete Stochastic Dynamic Programming, John Wiley and Sons, Inc., New Jersey, USA, 2005.
[23] G.J. Gordon, Approximate solutions to Markov decision processes (Ph.D. thesis), Carnegie Mellon University, 1999.
[24] Y. Xue, D. Beltran-Villegas, M. Bevan, M. Grover, Mdp based optimal control for a colloidal self-assembly system, in: American Control Conference (ACC), 2013, pp. 3397–3402.
[25] M. Karamouz, F. Szidarovszky, B. Zahraie, Water Resources Systems Analysis, Lewis publishers in CRC Press, New York, USA, 2003.
[26] Control System Toolbox: For Use With MATLAB R2012a, MathWorks, 2012.
[27] G. Grimm, J. Hatfield, I. Postlethwaite, A. Teel, M. Turner, L. Zaccarian, Antiwindup for stable linear systems with input saturation: an lMI-based synthesis, IEEE Trans. Autom.Control 48 (9) (2003) 1509–1525.