Proceedings of the 2013 IEEE International Conference on
Cyber Technology in Automation, Control and Intelligent Systems
May 26-29, 2013, Nanjing, China

Jamming Attack on Cyber-Physical Systems: A Game-theoretic Approach

Yuzhe Li*, Ling Shi*, Peng Cheng†, Jiming Chen† and Daniel E. Quevedo‡

***Abstract*—We consider security issues in Cyber-Physical Systems (CPSs). A sensor node communicates with a remote estimator through a wireless channel which may be jammed by an external attacker. With energy constraints for both the sensor and the attacker, the interactive decision making process of when to send and when to attack is studied. We formulate a game-theoretical framework and prove that the optimal strategies for both sides constitute a Nash equilibrium. The derivation of the optimal strategies for both sides is also provided with examples.**

***Index Terms*—Cyber-Physical Systems, Security, Game Theory, Networked estimation.**

I. Introduction

Cyber-Physical Systems (CPSs) are systems with a close integration of sensing, control, communication, computation and physical process. CPSs usually consist of a group of networked agents, including sensors, actuators, control processing units, and communication devices [1] (See Fig. 1). The rapid development of CPSs in recent years has brought significant advances in terms of efficiency, reliability, adaptability and autonomy. Thus CPSs have a wide spectrum of applications in areas such as energy, aerospace, smart grids, civil infrastructure, transportation, etc.

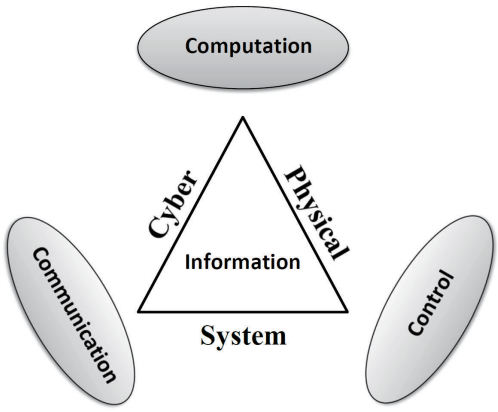

Fig. 1. Architecture of Cyber-Physical Systems

*: Electronic and Computer Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. Email: {yliah, eesling}@ust.hk.

†: State Key Lab. of Industrial Control Technology, Zhejiang University, China. Email: {pcheng, jmchen}@iipc.zju.edu.cn.

‡: School of Electronic Engineering and Computer Science, The University of Newcastle, Australia, Email: dquevedo@ieee.org.

The work by Y. Li and L. Shi is supported by an HKUST grant DAG12EG09S.

The increasing connection of CPSs to many safety-critical aspects of our nation and society brings the high risk of cyber-attacks by adversaries around the globe. For example, the future electric power grids, i.e., the smart grids, will be the largest and most complex Cyber-Physical Systems in each country. Since the operation and communication are mainly through the shared public network with the strong opening-up characteristic, such systems are quite vulnerable to cyber security threats. Any severe attack on the power grids of the nation may have significant impact on the environment, national economy, national security or even the loss of human life [2]. Therefore, the security issues of CPSs is of fundamental importance to ensure the safe operation of CPSs.

Security of CPSs has been a hot research area in recent years. Cardenas *et al.* [3] studied two possible types of attacks on CPSs: Denial of Service (DoS) attack and deception (integrity) attack, which corresponds to the traditional security goals *availability* and *integrity*, respectively. The DoS attack block the exchange of information including sensor measurement data or control inputs between each part of the CPSs, while the integrity attack focus on the integrity of the data by modifying the data packets. Liu *et al.* [4] proposed a new class of attacks against state estimation in electric power grids, namely false data injection attacks. With the configuration and parameters of the power system, the attacker can launch such attacks to inject arbitrary errors into certain state variables without triggering the existing bad measurement detection alarm. Mo *et al.* [1] described the CPS model as a discrete linear time-invariant system running a Kalman filter, an LQG controller and a χ^2 failure detector, which is under the the integrity attack. The authors presented a quantitative index of the system resilience by investigating the feasible set of the the adversary's attack strategies without being detected and the corresponding state estimation error under certain attacks.

Though some fundamental frameworks have been proposed in the previous literatures, most of the traditional solutions to CPSs security focus on only one side of the CPSs security issues, i.e., either the attacker or the defender. In practice, both parties (defender and attacker) involve in this interactive action making process, and each side chooses the optimal action based on all the information they have, including the understanding and prediction of the actions their opponent may taking. Thus we need a more comprehensive description about the CPSs security scenario rather than a static one side analysis. Due to the limitation of recent frameworks and the complexity of such problem, we consider a game-theoretic approach which provides an alternative way to handle these interactive decision issues.

978-1-4799-0612-3/13/$31.00 © 2013 IEEE

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers, i.e., the interactive decision theory [5]. Though game theory was widely used in economics at the beginning, it has developed in a wide range of practical application areas. Roy *et al.* [6] investigated the existing results about enhancing network security under the game-theoretic framework and provided a classification of recent results based on the types of the corresponding games. Agah *et al.* [7] formulated a cooperative game between sensor nodes in mobile wireless sensor networks and showed that through cooperation between two nodes the data communication between them will be more reliable.

Different from the works above, in the present paper, we consider the interactive decision making process between the sensor node and the attacker who can launch jamming attack on the communication channel between the sensor and the remote estimator. With energy constraints for both sides, we prove that the optimal strategies for both sides constitute a Nash equilibrium under game theoretical framework which enables us to derive the optimal strategies for both sides.

The remainder of this paper is organized as follows. Section II presents the system model and states the main problem of interest. In Section III, we provide some game theory preliminaries. Section IV presents the general case for the optimal strategies for both sides. Numerical examples are included in Section V. Section VI concludes the paper.

Notation: $\mathbb{Z}$ denotes the set of all integers. $\mathbb{N}$ are the positive integers, $n \in \mathbb{N}$. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is the n-dimensional Euclidean space. $\mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$) is the set of n by n positive semi-definite matrices (and positive definite matrices). When $X \in \mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$), we write $X \geqslant 0$ (and $X > 0$). $X \geqslant Y$ if $X - Y \in \mathbb{S}_+^n$. $\mathrm{Tr}(\cdot)$ is the trace of a matrix. The superscript $'$ stands for transposition. For functions f, f_1, f_2 with appropriate domains, $f_1 f_2(x)$ stands for the function composition $f_1\big(f_2(x)\big)$, and $f^n(x) \triangleq f\big(f^{n-1}(x)\big)$ with $f^0(x) \triangleq x$. δ_{ij} is Dirac delta function, i.e., δ_{ij} equals to 1 when $i = j$ and 0 otherwise. The notation $\mathbb{P}[\cdot]$ refers to probability, $\mathbb{E}[\cdot]$ to expectation.

II. Problem Setup

A. System Model

Consider a general discrete linear time-invariant (LTI) process in CPSs:

$$x_{k+1} = Ax_k + w_k, \tag{1}$$
$$y_k = Cx_k + v_k, \tag{2}$$

where $k \in \mathbb{N}$, $x_k \in \mathbb{R}^{n_x}$ is the process state vector at time k, $y_k \in \mathbb{R}^{n_y}$ is the measurement taken by the sensor, $w_k \in \mathbb{R}^{n_x}$ and $v_k \in \mathbb{R}^{n_y}$ are zero-mean i.i.d. Gaussian noises with $\mathbb{E}[w_k w_j'] = \delta_{kj} Q$ ($Q \geqslant 0$), $\mathbb{E}[v_k (v_j)'] = \delta_{kj} R$ ($R > 0$), $\mathbb{E}[w_k (v_j)'] = 0$ $\forall j, k \in \mathbb{N}$. The initial state x_0 is a zero-mean Gaussian random vector with covariance $\Pi_0 \geqslant 0$ and is uncorrelated with w_k and v_k. The pair (A, C) is assumed to be observable and $(A, \sqrt{Q})$ is controllable.

In the cyber-physical systems, sensors are typically equipped with on-board processor [8] and utilization of these capabilities improves the system performance significantly. At each time k, the sensor first locally runs a Kalman filter to estimate the state x_k based on all the measurements it collects up to time k and then transmit its local estimate to the remote estimator.

Denote $\hat{x}_k^s$ and P_k^s as the sensor's local state estimate and the corresponding error covariance, which are given by

$$\hat{x}_k^s = \mathbb{E}[x_k | y_1, y_2, ..., y_k], \tag{3}$$
$$\hat{P}_k^s = \mathbb{E}[(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)' | y_1, y_2, ..., y_k]. \tag{4}$$

Based on the fundamental linear estimation method, $\hat{x}_k^s$ and P_k^s can be calculated by standard Kalman filter as follows:

$$\hat{x}_{k|k-1}^s = A\hat{x}_{k-1}^s, \tag{5}$$
$$P_{k|k-1}^s = AP_{k-1}^s A' + Q, \tag{6}$$
$$K_k^s = P_{k|k-1}^s C' [CP_{k|k-1}^s C' + R]^{-1}, \tag{7}$$
$$\hat{x}_k^s = A\hat{x}_{k-1}^s + K_k^s (y_k - CA\hat{x}_{k-1}^s), \tag{8}$$
$$P_k^s = (I - K_k^s C) P_{k|k-1}^s, \tag{9}$$

where the recursion starts from $\hat{x}_0^s = 0$ and $P_0^s = \Pi_0 \geqslant 0$.

For notational ease, we introduce the functions $h, \tilde{g} : \mathbb{S}_+^n \to \mathbb{S}_+^n$ as:

$$h(X) \triangleq AXA' + Q, \tag{10}$$
$$\tilde{g}(X) \triangleq X - XC'[CXC' + R]^{-1} CX. \tag{11}$$
$$h^k(X) \triangleq \underbrace{h \circ h \circ \cdots \circ h \circ h}_{\text{k times}}(X) \tag{12}$$

It is well known (see, e.g., [9]) that the estimation error covariance P_k^s in (9) will converge to a steady-state value exponentially fast. Without loss of generality, we assume that the Kalman filter at the sensor side has entered the steady state and simplify our subsequent discussion by setting:

$$P_k^s = \overline{P}, \ k \geqslant 1, \tag{13}$$

where $\overline{P}$ is the steady-state error covariance, which is the unique positive semi-definite solution of $\tilde{g} \circ h(X) = X$. From [10], $\overline{P}$ has the following property.

Lemma 2.1: For $0 \leqslant t_1 \leqslant t_2$, the following inequality holds:

$$h^{t_1}(\overline{P}) \leqslant h^{t_2}(\overline{P}). \tag{14}$$

In addition, if $t_1 < t_2$, then

$$\mathrm{Tr}\left(h^{t_1}(\overline{P})\right) < \mathrm{Tr}\left(h^{t_2}(\overline{P})\right). \tag{15}$$

B. Communication Channel

The communication between the sensor and the remote estimator in the CPSs is mainly through wired or wireless network, which makes Denial-of-Service (DoS) attack becomes the most reachable attack pattern for the attacker [11]. Typical DoS attack can jam the communication between each components in CPSs and degrade the total system performance [12]–[14]. In our work, the attacker is assumed capable to conduct DoS attack on the sever to jam the communication channel between the sensor and the remote estimator, therefore causing the data packet drop. Fig. 2 shows the overall system

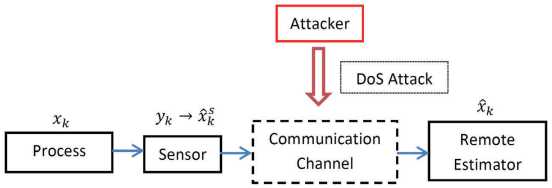

Fig. 2. System Architecture

architecture. Besides, we assume that the data packet from the sensor can arrive at the remote estimator perfectly without the DoS attack, otherwise will be dropped.

C. Estimation Process

Due to the energy limitation, suppose that within a time horizon T, the sensor can send the data packet at most $M \leqslant T$ times to the remote estimator while the attacker can launch jamming attack at most $N \leqslant T$ times.

Denote $\theta_S \triangleq \{\gamma_1, \gamma_2, ..., \gamma_T\}$ as the sensor's data-sending strategy, where $\gamma_k = 1$ means the sensor sends data packet at time k, otherwise $\gamma_k = 0$. Consequently we have

$$\sum_{k=1}^{T} \gamma_k \leqslant M. \tag{16}$$

Similarly we denote $\theta_A \triangleq \{\lambda_1, \lambda_2, ..., \lambda_T\}$ as the attacker's attack strategy, where $\lambda_k = 1$ means the attacker launch jamming attack at time k, other wise $\lambda_k = 0$. Similarly we also have

$$\sum_{k=1}^{T} \lambda_k \leqslant N. \tag{17}$$

Define I_k as all the sensor data packets collected by the remote estimator from time 1 to time $k \leqslant T$, i.e.,

$$\begin{aligned} I_k = &\{\gamma_1(1-\lambda_1), \gamma_2(1-\lambda_2), ..., \gamma_k(1-\lambda_k)\} \\ &\bigcup \{\gamma_1(1-\lambda_1)\hat{x}_1^s, \gamma_2(1-\lambda_2)\hat{x}_2^s, ..., \gamma_k(1-\lambda_k)\hat{x}_k^s\}. \end{aligned} \tag{18}$$

At the remote estimator's side, similar to [15], once the sensor's local estimate packet arrives, the estimator synchronizes its own estimate with the sensor. Otherwise, the estimator just predicts x_k based on its previous optimal estimate.

Denote $\hat{x}_k$ and P_k as the remote estimator's state estimate and the corresponding error covariance based on I_k, i.e.,

$$\hat{x}_k = \mathbb{E}[x_k | I_k], \tag{19}$$

$$P_k = \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k^s)' | I_k]. \tag{20}$$

Then $\hat{x}_k$ is given by

$$\hat{x}_k = \begin{cases} \hat{x}_k^s, & \text{if } \hat{x}_k^s \text{ arrives,} \\ A\hat{x}_{k-1}^s, & \text{otherwise.} \end{cases} \tag{21}$$

As a result, the state estimation error covariance P_k satisfies

$$P_k = \begin{cases} \overline{P}, & \text{if } \hat{x}_k^s \text{ arrives,} \\ h(P_{k-1}), & \text{otherwise.} \end{cases} \tag{22}$$

Based on (18) and the description of the communication channel, $\hat{x}_k^s$ arrives at the remote estimator perfectly if and only if $\gamma_k(1-\lambda_k) = 1$.

D. Problem Setup

Given the time-horizon $T \in \mathbb{N}$, we define $J_\alpha(T)$ as:

$$J_\alpha(T) \triangleq \alpha \frac{1}{T} \sum_{k=1}^{T} \mathrm{Tr}\{\mathbb{E}[P_k]\} + (1-\alpha)\mathrm{Tr}\{\mathbb{E}[P_T]\}, \tag{23}$$

where $\alpha = \{0, 1\}$.

It is easy to see that when $\alpha = 1$, $J_1(T)$ is the trace of the average expected estimation error covariance at the estimator's side, while when $\alpha = 0$, $J_0(T)$ is the trace of the terminal expected estimation error covariance at the estimator's side.

The goal of the decision maker at the sensor's side is to minimize $J_\alpha(T)$, while at the attacker's side is to maximize that.

We define the objective function of the attacker as:

$$J_A(\theta_A) \triangleq J_\alpha(T). \tag{24}$$

Since the objective of the sensor is opposite to the one of the attacker, for convenience, we can define the objective function of the sensor as:

$$J_S(\theta_S) \triangleq -J_A(\theta_A) = -J_\alpha(T). \tag{25}$$

Thus, the goal of both sides is to maximize their objective function.

We are interested in finding the optimal strategies for each side subject to the constraints (16) and (17). Denote the optimal strategies for each side as $\theta_S^\star$ and $\theta_A^\star$, respectively.

To be more specific, we consider the following optimization problem:

Problem 2.2: For the sensor,

$$\begin{aligned} \max_{\theta_S} \quad & J_S(\theta_S), \\ \text{s.t.} \quad & \sum_{k=1}^{T} \gamma_k \leqslant M, \end{aligned}$$

where $\theta_S \triangleq \{\gamma_1, \gamma_2, ..., \gamma_T\}$.

For the attacker,

$$\begin{aligned} \max_{\theta_A} \quad & J_A(\theta_A), \\ \text{s.t.} \quad & \sum_{k=1}^{T} \lambda_k \leqslant N, \end{aligned}$$

where $\theta_A \triangleq \{\lambda_1, \lambda_2, ..., \lambda_T\}$.

It is not difficult to show that the optimal strategies for each side remain the same if the constraint of Problem (2.2) is changed to $\sum_{k=1}^{T} \gamma_k = M$ and $\sum_{k=1}^{T} \lambda_k = N$. Thus we will focus on the following problem:

Problem 2.3: For the sensor,

$$\begin{aligned} \max_{\theta_S} \quad & J_S(\theta_S), \\ \text{s.t.} \quad & \sum_{k=1}^{T} \gamma_k = M, \end{aligned}$$

where $\theta_S \triangleq \{\gamma_1, \gamma_2, ..., \gamma_T\}$.

For the attacker,

$$\max_{\theta_A} \quad J_A(\theta_A),$$
$$\text{s.t.} \quad \sum_{k=1}^{T} \lambda_k = N,$$

where $\theta_A \triangleq \{\lambda_1, \lambda_2, ..., \lambda_T\}$.

III. Game Theory Preliminaries

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers, i.e., the interactive decision theory. At the beginning, game theory was widely used in economics, political science, as well as psychology. Today, has found a growing number of application including communication, control and network protocol design.

In our work, for the case with energy constraint for both sides, i.e., $M < T$ and $N < T$, which is much general situation in practice, the tools provided in existing literature can not be used. Since both sides have many different strategies and have to take the opponent's strategy into consideration, we will investigate the problem from a game-theoretic point of view.

To utilize the mature tools from the game theory, we need some basic and necessary assumptions:

Assumption 3.1: Both the senor and the attacker are intelligent rational decision makers, pursuing the maximization of their utilities, i.e., their payoff function (objective function) (25) and (24), respectively.

Remark 3.2: This "rational maximizing behavior" is a basic assumption in game theory, while it does not necessarily mean that people always make "100% perfect decisions", due to that people may be limited by the amount of information they have.

Definition 3.3: The common knowledge p in a group of players G is that all the players in G know p, they all know that they know p, they all know that they all know that they know p, and so on and so forth.

Assumption 3.4: The decision maker at each side acts simultaneously or, at least, without knowing the actions of the other. But they know the objective function and the possible actions set of each other, which is common knowledge among them.

Assumption 3.4 is straightforward.

We now give some basic definition in game theory [5].

Definition 3.5: A game consists of a set of players, a set of strategies available to those players, and a specification of payoffs for each players on the condition of each combination of strategies.

Definition 3.6: A player's *strategy* refers to one of all the options he can choose in the game, which will determine all the actions to take at any stage of the game.

A *pure strategy* provides a complete definition of how a player will play a game.

A player's *strategy set* is the set of all the pure strategies available to that player.

A *mixed strategy* is an assignment of probability to each pure strategy in the strategy set, which allows the player to randomly select a pure strategy.

A *strategy profile* (strategy combination) is a set of strategies for each player which fully specifies all actions in a game.

Remark 3.7: We can regard the pure strategy as a degenerate case of the mixed strategy, where the particular pure strategy is selected with probability 1 and every other strategy with probability 0.

If in the game, each player has chosen a strategy and no player can benefit by changing his own strategy while the other players keep theirs unchanged, then the current strategy profile, i.e., the current set of strategy choices constitute a Nash equilibrium. We can express the definition in an analytical way.

Definition 3.8: Given a game with n players. Denote S_i as player i's strategy set and $S = S_1 \times S_2 \times \cdots \times S_n$ as the strategy profile set. Define $F \triangleq (f_1(x), f_2(x), ..., f_n(x)), x \in S$ as the whole payoff function, where $f_i(x)$ is the payoff function of player i. Each player $i \in \{1, 2, ..., n\}$ chooses strategy x_i in strategy profile $x = (x_1, x_2, ..., x_n)$ and obtains payoff $f_i(x)$. A strategy profile $x^\star \in S$ is a Nash equilibrium (NE) if:

$$f_i(x_i^\star, x_{-i}^\star) \geqslant f_i(x_i, x_{-i}^\star), \quad \forall i, x_i \in S_i. \tag{26}$$

where x_{-i} is the strategy profile of all players except for player i.

When the inequality (26) holds strictly (with $>$ instead of $\geqslant$) for all players and all feasible strategies, then the equilibrium is classified as a strict Nash equilibrium.

If for some player, there exists exact equality between $x_i^\star$ and some other strategy in S , then the equilibrium is classified as a weak Nash equilibrium.

Theorem 3.9: Consider the interactive decision making process in the CPSs with the sensor and the attacker under the game-theoretic framework. The optimal strategies for both sides constitutes a Nash equilibrium of this two player's game.

Proof: We denote the optimal strategies for each side as $\theta_S^\star$ and $\theta_A^\star$ respectively. Based on the assumption (3.1) and (3.4), the decision makers at both sides will choose $\theta_S^\star$ and $\theta_A^\star$, respectively, which is common knowledge (see Remark 3.10).

Given the optimal strategy $\theta_A^\star$ chosen by the attacker, the optimal strategy $\theta_S^\star$ for the sensor is the one that maximizes $J_S(\theta)$, i.e.,

$$J_S(\theta_S^\star | \text{given } \theta_A^\star) \geqslant J_S(\theta_S | \text{given } \theta_A^\star), \ \forall \theta_S.$$

For the attacker, we have similar conclusion.

Since the objective function $J_S(\theta)$ and $J_A(\theta)$ can be regarded as each side's payoff function, respectively, from (26), $\theta_S^\star$ and $\theta_A^\star$ constitutes a Nash equilibrium. ■

Remark 3.10: The common knowledge of $\theta_S^\star$ and $\theta_A^\star$ is from the Assumption 3.4, which does not mean that both sides know each other's exact action but keep unchanged. From (3.6), the mixed strategy is only an assignment of probability to each pure strategy, which is indeed the reason why both sides can reach the Nash equilibrium and keep unchanged.

Nash [16] in 1951 defines a mixed strategy Nash Equilibrium for any game with a finite set of strategies and proves that at least one mixed strategy Nash Equilibrium must exist in such a game based on Kakutani's generalized fixed point theorem and the Brouwer theorem.

Theorem 3.11: [16] For any game with a finite set of strategies, there exists at least one mixed strategy Nash Equilibrium in the game.

From Theorems 3.9 and 3.11, we conclude that the solution to problem 2.3, i.e., the optimal strategy for both sides, always exists as a Nash Equilibrium of the two player's game.

IV. General case: with energy constraints for both sides

It is easy to see that the number of all the pure strategies for the sensor is

$$C_T^M = \binom{T}{M} \triangleq K$$

and we denote those pure strategies as $\theta_S^{\text{pure}}(1), \theta_S^{\text{pure}}(2), ..., \theta_S^{\text{pure}}(K)$. Though the number of the pure strategy is finite, there are infinitely many mixed strategies for each side. Thus the mixed strategy for the sensor can be write as:

$$\theta_S^{\text{mixed}}(\pi_1, \pi_2, ..., \pi_K) = \{\theta_S^{\text{pure}}(k) \text{ with probability } \pi_k\},$$
$$k = 1, 2, ..., K,$$

where

$$\sum_{k=1}^{K} \pi_k = 1, \quad \pi_k \in [0, 1]. \tag{27}$$

Note that different combinations of $\{\pi_k\}$ constitute different mixed strategies.

For the attacker, we have similar notations as:

$$\theta_A^{\text{mixed}}(\mu_1, \mu_2, ..., \mu_L) = \{\theta_A^{\text{pure}}(k) \text{ with probability } \mu_k\},$$
$$k = 1, 2, ..., L,$$

where

$$C_T^N \triangleq L,$$

and

$$\sum_{k=1}^{L} \mu_k = 1, \mu_k \in [0, 1].$$

The optimal solution $\theta_S^\star$ and $\theta_A^\star$ for the special case in section III is the so-called "pure strategy" and is indeed a special form of our general mixed strategy.

Now we will find the Nash equilibrium of the game.

From Theorem 3.11, there exists at least one Nash equilibrium point. Suppose that $\theta_A^\star \triangleq \{\mu_1^\star, \mu_2^\star, ..., \mu_L^\star\}$ is one equilibrium mixed strategy of the attacker.

Given $\theta_A^\star$, we can easily calculate the objective function $J_S\left(\theta_S^{\text{pure}}(k)\right) \triangleq M_k$ for each $\theta_S^{\text{pure}}(k)$. Thus we can write the objective function of the mixed strategy θ_S^{mixed} of the sensor as:

$$J_S(\theta_S^{\text{mixed}}) = \sum_{k=1}^{K} \pi_k M_k, \quad \sum_{k=1}^{K} \pi_k = 1.$$

Based on the definition of Nash equilibrium, given $\theta_A^\star$, the equilibrium strategy of the sensor $\theta_S^\star = \{\pi_1^\star, \pi_2^\star, ..., \pi_K^\star\}$ is the one that maximize $J_S(\theta_S^{\text{mixed}})$ under the constraint (27).

Lemma 4.1 provides the method to find $\theta_S^\star$.

Lemma 4.1: [17], [18] Consider a multi-variate function $f(x_1, x_2, ..., x_n)$ subject to the constraints

$$g(x_1, x_2, ..., x_n) = c,$$

where f and g are functions with continuous first partial derivatives. Lagrange multipliers can be used to find the critical point (local extremum) of function f. The procedure is as follows:

Introduce a new variable λ_L, called Lagrange multiplier, and study the Lagrange function defined by:

$$\Lambda(x_1, x_2, ..., x_n, \lambda_L) = f(x_1, x_2, ..., x_n) + \lambda_L[g(x_1, x_2, ..., x_n) - c]. \tag{28}$$

The critical points of f can be obtained by solving:

$$\nabla\Lambda(x_1, x_2, ..., x_n, \lambda_L) = 0, \tag{29}$$

where ∇ denotes the gradient. The extremum of the function f is within the critical points (local extremum) and the points on the closed set's boundary. □

By using Lagrange multiplier method, we can calculate $\theta_S^\star = \{\pi_1^\star, \pi_2^\star, ..., \pi_K^\star\}$, where $\pi_k^\star$ is a function of $\theta_A^\star$, i.e., $\mu_1^\star, \mu_2^\star, ..., \mu_L^\star$.

Then for the attacker, we can run the same procedure given $\theta_S^\star$, and solve $\theta_A^\star = \{\mu_1^\star, \mu_2^\star, ..., \mu_L^\star\}$, where $\mu_k^\star$ is a function of $\theta_S^\star$, i.e., $\pi_1^\star, \pi_2^\star, ..., \pi_K^\star$.

In the end we can combine the two solutions to obtain both $\mu_k^\star$ and $\pi_k^\star$ and we have the optimal solutions for both sides: $\theta_S^\star$ and $\theta_A^\star$.

V. Numerical Example

In this section, we provide an example to show how to obtain the optimal strategies for both sides.

We consider a simple scenario where the time-horizon is 2 and both sides are limited to only one chance to send data or launch attack, i.e., $T = 2$, $M = 1$, $N = 1$. We investigate the average cost, namely, $\alpha = 1$.

We consider a one dimensional process, i.e., the system parameters A, C, Q, R and the steady-state error covariance $\overline{P}$, are all scalar.

The attacker has two pure strategies: $\theta_A^{\text{pure}}(1) = \{1, 0\}$ and $\theta_A^{\text{pure}}(2) = \{0, 1\}$.

Similarly, for the sensor, we also have $\theta_S^{\text{pure}}(1) = \{1, 0\}$ and $\theta_S^{\text{pure}}(2) = \{0, 1\}$.

The following example shows the calculation of the objective function $J_S\left(\theta_S^{\text{pure}}(1)\right)$ for the pure strategy $\theta_S^{\text{pure}}(1)$ given $\theta_A^\star$.

Step 1:

Assume that the attacker's optimal strategy is $\theta_A^\star = \{\mu_1^\star, \mu_2^\star\}$.

If the attacker's pure strategy is $\theta_A^{\text{pure}}(1) = \{1, 0\}$, from (13), we get:

$$\begin{aligned} P_1 &= h(\overline{P}), \\ P_2 &= h^2(\overline{P}), \\ J_S &= -\frac{1}{2}(P_1 + P_2) = -\frac{1}{2}[h(\overline{P}) + h^2(\overline{P})]. \end{aligned}$$

If the attacker's pure strategy is $\theta_A^{\text{pure}}(2) = \{0, 1\}$, similarly we have:

$$\begin{aligned} P_1 &= \overline{P}, \\ P_2 &= h(\overline{P}), \\ J_S &= -\frac{1}{2}[\overline{P} + h(\overline{P})]. \end{aligned}$$

Thus given $\theta_A^\star$, we have:

$$J_S\left(\theta_S^{\text{pure}}(1)\right) = -\mu_1^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] - \mu_2^\star \frac{1}{2}[\overline{P} + h(\overline{P})]. \quad (30)$$

Step 2:

Following the procedure in Step 1, we get:

$$J_S\left(\theta_S^{\text{pure}}(2)\right) = -\mu_1^\star \frac{1}{2}[\overline{P} + h(\overline{P})] - \mu_2^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})]. \quad (31)$$

Thus the objective function of the sensor for a mixed strategy given $\theta_A^\star$ can be written as:

$$\begin{aligned} J_S\left(\theta_S^{\text{mixed}}\right) &= \pi_1 J_S\left(\theta_S^{\text{pure}}(1)\right) + \pi_2 J_S\left(\theta_S^{\text{pure}}(2)\right) \\ &= -\pi_1 \left\{ \mu_1^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] + \mu_2^\star \frac{1}{2}[\overline{P} + h(\overline{P})] \right\} \\ &\quad - \pi_2 \left\{ \mu_1^\star \frac{1}{2}[\overline{P} + h(\overline{P})] + \mu_2^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] \right\}. \end{aligned}$$

Similarly the objective function of the attacker for a mixed strategy given $\theta_S^\star$ can be written as:

$$\begin{aligned} J_A\left(\theta_A^{\text{mixed}}\right) &= \mu_1 J_A\left(\theta_A^{\text{pure}}(1)\right) + \mu_2 J_A\left(\theta_A^{\text{pure}}(2)\right) \\ &= \mu_1 \left\{ \pi_1^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] + \pi_2^\star \frac{1}{2}[\overline{P} + h(\overline{P})] \right\} \\ &\quad + \mu_2 \left\{ \pi_1^\star \frac{1}{2}[\overline{P} + h(\overline{P})] + \pi_2^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] \right\}. \end{aligned}$$

Step 3:

From Lemma 4.1 we will find the maximum value of $J_S(\theta_S^{\text{mixed}})$ and $J_A(\theta_A^{\text{mixed}})$ under the constraint $\pi_1 + \pi_2 = 1$ and $\mu_1 + \mu_2 = 1$ with Lagrange multiplier.

First denote that

$$f(\pi_1, \pi_2, \lambda_L) \triangleq J_S(\theta_S^{\text{mixed}}) - \lambda_L(\pi_1 + \pi_2 - 1). \quad (32)$$

By solving following equation set:

$$\begin{cases} \partial f(\pi_1, \pi_2, \lambda_L)/\partial \pi_1 = 0, \\ \partial f(\pi_1, \pi_2, \lambda_L)/\partial \pi_2 = 0, \\ \partial f(\pi_1, \pi_2, \lambda_L)/\partial \lambda_L = 0, \end{cases} \quad (33)$$

we have

$$\begin{cases} -\left\{\mu_1^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] + \mu_2^\star \frac{1}{2}[\overline{P} + h(\overline{P})]\right\} - \lambda_L = 0, \\ -\left\{\mu_1^\star \frac{1}{2}[\overline{P} + h(\overline{P})] + \mu_2^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})]\right\} - \lambda_L = 0, \\ \pi_1 + \pi_2 - 1 = 0, \end{cases} \quad (34)$$

For the attacker, we have similar equation set:

$$\begin{cases} \left\{\pi_1^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})] + \pi_2^\star \frac{1}{2}[\overline{P} + h(\overline{P})]\right\} - \lambda_L' = 0, \\ \left\{\pi_1^\star \frac{1}{2}[\overline{P} + h(\overline{P})] + \pi_2^\star \frac{1}{2}[h(\overline{P}) + h^2(\overline{P})]\right\} - \lambda_L' = 0, \\ \mu_1 + \mu_2 - 1 = 0, \end{cases} \quad (35)$$

Combine (34) and (35) we find the only solution:

$$\begin{cases} \pi_1^\star = \pi_2^\star = \frac{1}{2} \\ \mu_1^\star = \mu_2^\star = \frac{1}{2} \end{cases}. \quad (36)$$

Thus the optimal strategy for the sensor is $\{\pi_1^\star, \pi_2^\star\} = \{\frac{1}{2}, \frac{1}{2}\}$, i.e., randomly choose pure strategies $\{1, 0\}$ or $\{0, 1\}$ with same probability 0.5. For the attacker we have similar conclusion.

VI. Conclusion

We have considered the security issues in Cyber-Physical Systems (CPSs) in this paper. The interactive decision making process between the sensor node and the attacker was investigated. We formulated game-theoretical framework and proved that the optimal strategies for both sides constitute a Nash equilibrium. We also showed how to derive the optimal strategies with examples.

References

[1] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 47–54.

[2] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[3] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.

[4] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[5] R. Gibbons, *A primer in game theory*. Harvester Wheatsheaf Hemel Hempstead, 1992.

[6] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–10.

[7] A. Agah, S. Das, and K. Basu, "A game theory based approach for security in wireless sensor networks," in *Performance, Computing, and Communications, 2004 IEEE International Conference on*. IEEE, 2004, pp. 259–263.

[8] P. Hovareshti, V. Gupta, and J. Baras, "Sensor scheduling using smart sensors," in *Decision and Control, 2007 46th IEEE Conference on*. IEEE, 2007, pp. 494–499.

[9] B. D. O. Anderson and J. B. Moore, "Detectability and stabilizability of time-varying discrete-time linear systems," *SIAM Journal on Control and Optimization*, vol. 19, no. 1, pp. 20–32, Jan. 1981.

[10] L. Shi, K. Johansson, and L. Qiu, "Time and event-based sensor scheduling for networks with limited communication resources," in *World Congress of the International Federation of Automatic Control (IFAC)*, 2011.

[11] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack policy against remote state estimation," in *12th European Control Conference*, Zurich, Switzerland, July 2013 (submitted).

[12] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *Internet Computing, IEEE*, vol. 10, no. 1, pp. 82–89, 2006.

[13] S. Amin, A. Cardenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *Hybrid Systems: Computation and Control*, pp. 31–45, 2009.

[14] M. Zuba, Z. Shi, Z. Peng, and J. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*. ACM, 2011, p. 12.

[15] L. Shi, M. Epstein, and R. Murray, "Kalman filtering over a packet-dropping network: A probabilistic perspective," *Automatic Control, IEEE Transactions on*, vol. 55, no. 3, pp. 594 –604, march 2010.

[16] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, 1951.

[17] T. M. Apostol, *Mathematical analysis*, 2nd ed. Addison-Wesley Pub. Co., 1974.

[18] M. Hazewinkel, *Encyclopaedia of mathematics: Supplement*. Springer, 2002, vol. 3.