Jamming Attacks on Remote State Estimation in 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 remote state estimation of Cyber-Physical Systems (CPS). 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-theoretic framework and prove that the optimal strategies for both sides constitute a Nash equilibrium of a zero-sum game. To tackle the computation complexity issues, we present a constraint-relaxed problem and provide corresponding solutions using Markov chain theory.**

***Index Terms*—Cyber-physical systems (CPS), DoS jamming attack, game theory, Markov chain, remote state estimation.**

I. Introduction

Cyber-Physical Systems (CPS) are systems with a close integration of sensing, control, communication, computation and physical process. CPS usually consist of a group of networked agents, including sensors, actuators, control processing units, and communication devices [1] (see Fig. 1). CPS have a wide spectrum of applications in areas such as aerospace, smart grids, civil infrastructure, and transportation.

The increasing connection of CPS to many safety-critical applications brings a high risk of cyber-attacks by adversaries around the globe. As the operation and communication of CPS are mainly through a shared network, such systems are quite vulnerable to cyber security threats. Any severe attack on large CPS, such as the power grids of the nation, may have significant impact on the environment, national economy, national security or may even lead to the loss of human life [2]. Therefore, designing CPS taking into account security issues is of fundamental importance to ensure the safe operation of CPS. Not surprisingly, security issue in CPS has been a hot research area in recent years.

Cardenas *et al.* [3] studied two possible types of attacks on CPS: Denial of Service (DoS) attacks and deception attacks. These correspond to the traditional security goals *availability* and *integrity*, respectively. The DoS attack blocks the exchange of information including sensor measurement data or control inputs between each part of the CPS, while the integrity attack focuses on the integrity of the data by modifying the data packets. In the present note, we mainly focus on DoS attacks as these are the most reachable attack patterns in a shared network.

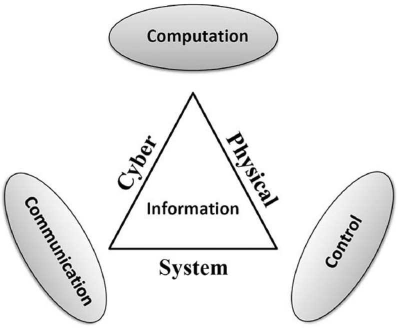

Fig. 1. Architecture of Cyber-Physical Systems.

Though some fundamental frameworks have been proposed in the previous literature, such as [4]–[6], these works have focused only on one side, i.e., either the attacker or the defender. However, if attackers have knowledge of system parameters, then both parties (defender and attacker) may involve in an interactive decision making process. To study such a situation, one requires a more comprehensive description about CPS security. The game-theoretic approach provides such a framework to handle these interactive decision issues (see [7]–[10]). In [11] a zero-sum game on multiple-input multiple-output (MIMO) Gaussian Rayleigh-fading channels is studied where both the jammer and the encoder are subject to power constraints. Gupta *et al.* [12] considered a dynamic game between a controller for a discrete-time LTI plant and an attacker who can jam the communication between the controller and the plant; the equilibrium control and jamming strategies for both players are provided. Agah *et al.* in [13] 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 can be made more reliable.

The work [14] studies a setup wherein the communication channels for transmitting system state information from a sensor to a remote controller can be partly jammed. Multiple channels can be chosen to avoid the attack. In that work, the payoff function of the stochastic game is in a quadratic form consisting of a weighted sum of the norms of the system state and an action vector with discount factors. The above objective (also used in [12]), and the assumption of availability of noiseless sensor measurements, however, are only of limited use for remote estimation scenarios. A preliminary version of parts of the present manuscript ([15]) investigated a jamming game where the data packet from the sensor always arrives at the remote estimator successfully without attack, and drops under attack. In the current work, we consider a more practical communication model which embeds [15] as a special case. Furthermore, as the computation complexity issue for finding the optimal solution is significant in [15], we propose a constraint-relaxed problem formulation and provide a corresponding closed-form expression which significantly reduces the calculation.

The main contributions of the present note can be summarized as follows:

1) We develop an integrated game-theoretic framework to investigate the interactive decision-making process between a sensor

Manuscript received February 17, 2014; revised July 25, 2014, November 2, 2014, and January 8, 2015; accepted February 9, 2015. Date of publication July 29, 2015; date of current version September 23, 2015. This work was supported by a Hong Kong RGC GRF funding 618612 and by NSFC under grant U1401253. Recommended by Associate Editor H. S. Chang.

Y. Li and L. Shi are with the Electronic and Computer Engineering Department, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (e-mail: yliah@ust.hk; eesling@ust.hk).

P. Cheng and J. Chen are with the Institute of Industrial Process Control, Department of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: pcheng@iipc.zju.edu.cn; jmchen@iipc.zju.edu.cn).

D. E. Quevedo is with the School of Electronic Engineering and Computer Science, The University of Newcastle, Callaghan, NSW 2308, Australia (e-mail: dquevedo@ieee.org).

Digital Object Identifier 10.1109/TAC.2015.2461851

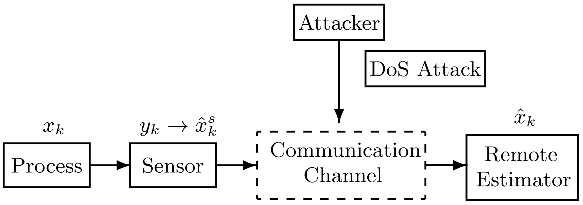

Fig. 2. CPS architecture studied: The communication channel is jammed by a malicious attacker. This affects the remote estimation performance.

node and an attacker who can launch DoS attacks. Our approach uses a novel payoff function and strategies set, which take into account the energy constraints on both sides.

2) We prove that the optimal strategies for both sides constitute a Nash equilibrium. For the case where the sensor and the attacker have on-line information about the previous transmission outcomes, we provide an algorithm (**Algorithm 1**) which performs the game dynamically.
3) We use Markov chain theory to address computation issues and solve an alternative relaxed problem.

The remainder of the note is organized as follows. Section II presents the system model and states the main problem of interest. Section III presents some game theory preliminaries and studies the optimal strategies for both sides. Section IV provides the dynamic updating algorithm. Section V proposes a constraint-relaxed problem formulation which reduces the computation complexity. Section VI draws conclusions.

Notations: $\mathbb{Z}$ denotes the set of all integers and $\mathbb{N}$ the positive integers. $\mathbb{R}$ 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 $f_1(f_2(x))$, and $f^n(x) \triangleq f(f^{n-1}(x))$, where $n \in \mathbb{N}$ and with $f^0(x) \triangleq x$. δ_{ij} is discrete-time Dirac delta function, i.e., δ_{ij} equals to 1 when $i = j$ and 0 otherwise. The notation $\mathbb{P}[\cdot]$ refers to probability and $\mathbb{E}[\cdot]$ to expectation. $T!$ stands for the factorial of T. We write C_T^M for $\binom{T}{M} = T!/(M!(T-M)!)$.

II. Problem Setup

Consider a general discrete linear time-invariant (LTI) process of

$$x_{k+1} = Ax_k + w_k$$
$$y_k = Cx_k + v_k$$

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 pair (A, C) is assumed to be observable and $(A, Q^{1/2})$ is controllable.

A. Local State Estimation

Our interest lies in security of remote state estimation, as depicted in Fig. 2. In CPS, sensors are often equipped with on-board processors [16]. Their capabilities can be used to improve system performance significantly. At each time k, the sensor first locally estimates the state x_k based on all the measurements it collects up to time k and then transmits its local estimate to the remote estimator. Let $\hat{x}_k^s$ and P_k^s be defined as the sensor's local Minimum Mean-Squared Error (MMSE) estimate of the state x_k and the corresponding error covariance. They are given by

$$\hat{x}_k^s = \mathbb{E}[x_k | y_1, y_2, \ldots, y_k]$$
$$\hat{P}_k^s = \mathbb{E}\left[(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)' | y_1, y_2, \ldots, y_k\right]$$

and can be calculated by a standard Kalman filter.

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

$$h(X) \triangleq AXA' + Q$$
$$\tilde{g}(X) \triangleq X - XC'[CXC' + R]^{-1} CX.$$

It is well-known that under suitable conditions the estimation error covariance of the Kalman filter converges to a unique value from any initial condition, thus the local estimation error covariance P_k^s will converge to a steady-state. Without loss of generality (similar assumptions can be found in [15], [17]), we assume that the Kalman filter at the sensor side has entered the steady state and simplify our subsequent discussion by setting

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

where $\overline{P}$ is the steady-state error covariance given in [18], which is the unique positive semi-definite solution of $\tilde{g} \circ h(X) = X$.

B. Communication Channel

Typical DoS attacks can jam the communication between components in CPS and degrade the overall system performance [4]–[6]. In our current work, the attacker is assumed to be capable to conduct DoS attack on the server to jam the communication channel between the sensor and the remote estimator, which may worsen the system performance. (See Fig. 2).

In practice, for both sensors and attackers, energy constraint is a natural concern, which affects the remote estimation performance and attacking policies. To encompass energy limitations, we will assume that, within a given 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.

The sensor's data-sending strategy is denoted as

$$\theta_S \triangleq \{\gamma_1, \gamma_2, \ldots, \gamma_T\} \tag{2}$$

where $\gamma_k = 1$ means that the sensor sends a data packet at time k, otherwise $\gamma_k = 0$. Consequently, we have the following constraint:

$$\sum_{k=1}^{T} \gamma_k \leqslant M. \tag{3}$$

Similarly, the attacker's strategy is denoted as

$$\theta_A \triangleq \{\lambda_1, \lambda_2, \ldots, \lambda_T\} \tag{4}$$

where $\lambda_k = 1$ means that the attacker launches a DoS attack at time k, otherwise $\lambda_k = 0$. The associated constraint is

$$\sum_{k=1}^{T} \lambda_k \leqslant N. \tag{5}$$

In practical communication systems, packet dropouts may occur due to different reasons, including signal degradation, channel fading and channel congestion. We assume the dropout probability of data packet from the sensor arrives at the remote estimator is β_1 in the absence of attack, and is $\beta_2 (> \beta_1)$ under the DoS attack. As noted above the strategies of the sensor and the attacker at time k are assumed to be γ_k and λ_k, respectively. Thus, the conditional probability of the remote estimator receiving the data packet from the sensor, denoted as p_k, is given by

$$p_k = \gamma_k \lambda_k (1 - \beta_2) + \gamma_k (1 - \lambda_k)(1 - \beta_1). \tag{6}$$

Remark 2.1: In [15], we studied the case where the data packet from the sensor will always arrive at the remote estimator successfully without an attack and drops under an attack. This is embedded in our current model as a special case when $\beta_1 = 0$ and $\beta_2 = 1$, in which case, (6) reduces to $p_k = \gamma_k(1 - \lambda_k)$.

C. Estimation Process

State estimation with dropouts has been well studied in recent literature on networked estimation [19], [20]. To quantify estimation performance, we introduce $\hat{x}_k$ and P_k which represent the remote estimator's MMSE state estimate (see Fig. 2) and the corresponding error covariance. The estimate $\hat{x}_k$ is calculated following a procedure similar to that adopted in [17]: once the sensor's local estimate packet arrives, the estimator synchronizes its own estimate with the sensor's; otherwise, the estimator just predicts x_k based on its previous optimal estimate

$$\hat{x}_k = \begin{cases} \hat{x}_k^s, & \text{if } \hat{x}_k^s \text{ arrives} \\ A\hat{x}_{k-1}, & \text{otherwise.} \end{cases} \tag{7}$$

As a result, the state estimation error covariance P_k obeys recursion

$$P_k = \begin{cases} \overline{P}, & \text{if } \hat{x}_k^s \text{ arrives} \\ h(P_{k-1}), & \text{otherwise.} \end{cases} \tag{8}$$

We assume that the remote estimator knows the system parameters A, C, Q, R. Thus based on (6) and (8), the expected state estimation error covariance can be easily written in a recursive way as

$$\mathbb{E}[P_k] = p_k\overline{P} + (1 - p_k)h\left(\mathbb{E}[P_{k-1}]\right). \tag{9}$$

D. Main Problem

To quantify the estimation quality over a finite time-horizon $T \in \mathbb{N}$, we introduce the cost function $J_\alpha(T)$ as

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

where $\alpha = 1$ or 0, corresponding to the overall performance and terminal performance, respectively.

The goal of the decision maker at the sensor's side is to minimize $J_\alpha(T)$, while the attacker tries to maximize the cost. Since the objective of the sensor is the opposite to the one of the attacker, for convenience, we define the objective functions of the attacker and the sensor

$$J_A(\theta_A) \triangleq J_\alpha(T) \tag{10}$$

and

$$J_S(\theta_S) \triangleq -J_A(\theta_A) = -J_\alpha(T) \tag{11}$$

where θ_A and θ_S are defined in (4) and (2). Thus, the goal of both sides is to maximize their respective objective functions.

We are interested in finding the optimal strategies for each side, subject to the energy constraints (3) and (5). Since more energy is always beneficial for improving performance, it is not difficult to show that the optimal strategies for each side remain the same if (3) and (5) are changed to $\sum_{k=1}^{T}\gamma_k = M$ and $\sum_{k=1}^{T}\lambda_k = N$, respectively (similar transformation can be found in [21]). Therefore, we consider the following optimization problem:

Problem 2.2: For the sensor

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

where $\theta_S \triangleq \{\gamma_1, \gamma_2, \ldots, \gamma_T\}$. For the attacker

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

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

III. Game-Theoretic Framework

In this section, we will model the decision-making process of the sensor and the attacker in a game-theoretic framework. Based on the objective functions of both sides, i.e., (10) and (11), the sensor and the attacker are regarded as the two players of a zero-sum game. The details of this game are discussed below.

A. Nash Equilibrium

In our work, for the case with energy constraint for both sides, i.e., $M < T$ and $N < T$, the tools provided in the existing literature which focus on only one side with energy constraint cannot be used. Since both sides have many different strategies and have to take the opponent's strategy into consideration, we shall investigate the problem from a game-theoretic point of view adopting the following definitions:

- *Player*: Two players: the sensor and the attacker.
- *Action*: θ_S and θ_A for the sensor and the attacker, respectively.
- *Payoff*: $J_S(\theta_S)$ and $J_A(\theta_A)$ for the sensor and the attacker, respectively.

If in a 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, constitutes a Nash equilibrium (defined in [22]). Nash defined a mixed strategy Nash Equilibrium for any game with a finite set of strategies and proved that at least one mixed strategy Nash Equilibrium must exist in such a game in [23].

Theorem 3.1: For any game with a finite set of strategies, there exists at least one mixed strategy Nash Equilibrium in the game.

Proof: Proved in [23]. ■

B. Existence of the Nash Equilibrium

To analyze the situation where both the sensor and the attacker have limited energy, we first note that the number of all the pure strategies (i.e., deterministic strategies) for the sensor is $K = C_T^M = \binom{T}{M}$. For future reference, those pure strategies are denoted as $\theta_S^{\mathrm{pure}}(1), \theta_S^{\mathrm{pure}}(2), \ldots, \theta_S^{\mathrm{pure}}(K)$. Though the number of pure strategies is finite, there are infinitely many mixed strategies for each side. Mixed strategies for the sensor can be written as: $\theta_S^{\mathrm{mixed}}(\pi_1, \pi_2, \ldots, \pi_K) = \{\theta_S^{\mathrm{pure}}(k) \text{ with probability } \pi_k\}$, $k = 1, 2, \ldots, K$, where $\sum_{k=1}^{K}\pi_k = 1, \pi_k \in [0, 1]$. Note that different combinations of $\{\pi_k\}$ constitute different mixed strategies. For the attacker, we use a similar notation: $\theta_A^{\mathrm{mixed}}(\mu_1, \mu_2, \ldots, \mu_L) = \{\theta_A^{\mathrm{pure}}(k) \text{ with probability } \mu_k\}$, $k = 1, 2, \ldots, L$, where $L = C_T^N = \binom{T}{N}$, $\sum_{k=1}^{L}\mu_k = 1, \mu_k \in [0, 1]$.

We now introduce the following result which together with Theorem 3.1 shows that a Nash equilibrium exists for the considered two-player zero-sum game between the sensor and the attacker.

Proposition 3.2: The optimal strategies for the sensor and the attacker constitute a Nash equilibrium of this two player's game.

Proof: The optimal strategies for each side are denoted as $\theta_S^\star$ and $\theta_A^\star$, respectively. 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 a similar conclusion. Since the objective functions $J_S(\theta)$ and $J_A(\theta)$ can be regarded as each side's payoff function, respectively, from the definition in [22], $\theta_S^\star$ and $\theta_A^\star$ constitute a Nash equilibrium. ■

Remark 3.3: Note that $\theta_S^\star$ and $\theta_A^\star$ are mixed strategies, which are only an assignment of probability to each pure strategy, thus although there is common knowledge of $\theta_S^\star$ and $\theta_A^\star$, both sides still do not know the exact following action taken by their opponent. This is indeed the reason why both sides can reach the Nash equilibrium.

C. Finding the Nash Equilibrium

We devote this subsection to finding the Nash equilibrium of the game. From Theorem 3.1, there exists at least one Nash equilibrium. $\theta_A^\star \triangleq \{\mu_1^\star, \mu_2^\star, \ldots, \mu_L^\star\}$ is assumed to be an equilibrium mixed strategy of the attacker.

Given $\theta_A^\star$, we can easily calculate the objective function $J_S(\theta_S^{\text{pure}}(k)) \triangleq M_k$ for each $\theta_S^{\text{pure}}(k)$ based on the recursion introduced in (8) and (9). Thus we can write the objective function of the mixed strategy θ_S^{mixed} of the sensor as

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

Based on the definition of Nash equilibrium, given $\theta_A^\star$, the equilibrium strategy of the sensor $\theta_S^\star = \{\pi_1^\star, \pi_2^\star, \ldots, \pi_K^\star\}$ is the one that maximizes $J_S(\theta_S^{\text{mixed}})$ under the constraint $\sum_{k=1}^{K} \pi_k^\star = 1$. Thus θ_S can be calculated easily using the Lagrange multipliers method [24]. This gives $\theta_S^\star = \{\pi_1^\star, \pi_2^\star, \ldots, \pi_K^\star\}$, where $\pi_k^\star$ is a function of $\theta_A^\star$, i.e., $\mu_1^\star, \mu_2^\star, \ldots, \mu_L^\star$. Then, for the attacker, we can run the same procedure and solve for $\theta_A^\star = \{\mu_1^\star, \mu_2^\star, \ldots, \mu_L^\star\}$, where $\mu_k^\star$ is a function of $\theta_S^\star$, i.e., $\pi_1^\star, \pi_2^\star, \ldots, \pi_K^\star$. By combining the two solutions to obtain both $\mu_k^\star$ and $\pi_k^\star$, one can then derive the optimal solutions for both sides.

IV. Dynamic Update Based on Online Information

In the game investigated in the previous section, though randomly chosen, the decisions of both sides are made before time $k = 0$ and thus can be regarded as an off-line schedule. In some practical situations, both sides may be able to monitor the status of the network environment. For example, after the attacker launches a jamming attack, the network server may be able to record the abnormality and inform the sensor about the attack [25]. The attacker can also detect whether the data packet is sent or not based on the network status. Thus, though each side is not sure what strategy will be taken by their opponent in the future, they can still detect (in a causal manner) the opponent's action and therefore narrow the scope of their opponent's action sets. In the present section we will study such scenarios.

As both sides can detect their opponent's past actions, at each time step after each observation, a new game with new constraints will arise. Let $\theta_S^\star(T, M, N, \Phi_0)$ and $\theta_A^\star(T, M, N, \Phi_0)$ denote the optimal mixed strategies for the sensor and the attacker, respectively, in the game with parameters T, M, N, Φ_0, where T is the time-horizon, M, N are the energy constraints, and $\Phi_0 = \overline{P}$ is the expected initial state estimate error covariance. $\theta_S^\star(T, M, N, \Phi_0)$ and $\theta_A^\star(T, M, N, \Phi_0)$ provide the action sequences for the whole time-horizon, but both sides only employ the actions for the first time step of the new game. After both sides move to the next step, the information, e.g., transmission outcomes, time-horizon and energy constraints, is updated, and thus a new game with new constraints will arise.

To update the whole decision-making process, a recursive algorithm (**Algorithm 1**) can be used. Following this algorithm, both sides are involved in a series of games with varying time horizon, energy constraints and initial states.

Algorithm 1 Updating algorithm for both sides

```
Process begins;
$\Phi_0 = \overline{P}$;
for $k = 1 : T$ do
    Solve for $\theta_S^\star(T, M, N, \Phi_0)$ and $\theta_A^\star(T, M, N, \Phi_0)$;
    Employ the actions of $\theta_S^\star(T, M, N, \Phi_0)$ and $\theta_A^\star(T, M, N, \Phi_0)$ designed for the first time step for the new game as the action of the current time step $k$;
    Observe the actions taken by both sides at time $k$;
    if $\gamma_k = 1$ then
        $M = M - 1$;
    else
        $M = M$;
    end if
    if $\lambda_k = 1$ then
        $N = N - 1$;
    else
        $N = N$;
    end if
    $T = T - 1$;
    $\Phi_0 = \mathbb{E}[P_k]$;
end for
```

Example 4.1: Consider a time-horizon $T = 3$ and the constraint for the sensor $M = 1$. After time $k = 1$, the attacker is assumed to observe that the sensor sent the data packet ($\gamma_1 = 1$). Since the mixed strategy for the sensor is chosen from $\{1, 0, 0\}$, $\{0, 1, 0\}$, and $\{0, 0, 1\}$, the attacker can deduce that the sensor's sending scheme is $\{1,0,0\}$. Then the attacker can make adjustments to his strategy and thus distribute the remaining energy more efficiently. A similar mechanism also applies to the sensor. ■

V. Relaxation: Average Energy Constraints

In this section, we will modify the constraints in Problem 2.2 and study an alternative problem formulation which can reduce the computational complexity significantly.

A. Constraint-Relaxed Problem Formulation

When using total energy constraints as considered in Problem 2.2, during the calculation of the optimal mixed strategy for each side, typically we need to consider $C_T^N \times C_T^M$ different combinations of the pure strategies from both sides to obtain closed-form expressions of the objective functions. Thus the order of computational complexity is $O((T!)^2)$, where T is the time-horizon. Thus, complexity issues must be taken into account when dealing with the general case in practice.

In the sequel, we will consider expected (average) energy constraints. Thus, the constraints in Problem 2.2 are relaxed to

$$\sum_{k=1}^{T} \mathbb{E}[\gamma_k] = M$$

and

$$\sum_{k=1}^{T} \mathbb{E}[\lambda_k] = N.$$

Remark 5.1: This type of constraint relaxation is attractive in some practical applications, where instead of only one time game, the estimation-jamming process will repeat many times under a total energy constraint. In view of a long time-horizon, the expected (average)

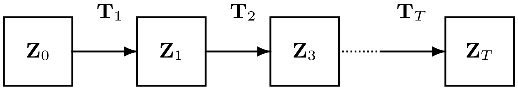

Fig. 3. Markov chain model of the estimation error covariance.

energy constraint on each short period is equivalent to the total energy constraint, thus is more flexible and practical. ■

Under the relaxed constraints, the pure strategies combinations are reduced from $C_T^M \times C_T^N$ to $2^T \times 2^T$, and the order of computation complexity is changed from $O((T!)^2)$ to $O(4^T)$. When considering the optimal mixed strategy, all the 2^T possible pure strategies are now feasible. Thus we can simplify the computation complexity even more and can express the mixed strategy of both sides in a more explicit way.

The sensor's data-sending mixed strategy now can be defined as

$$\tilde{\theta}_S^{\text{mixed}} \triangleq \{\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_T\}$$

where $\tilde{\gamma}_k \in [0,1]$ is defined as the probability of the sensor sending data packet at time k

$$\tilde{\gamma}_k = \mathbb{P}[\gamma_k = 1].$$

Similarly, the attacker's strategy can be expressed as

$$\tilde{\theta}_A^{\text{mixed}} \triangleq \{\tilde{\lambda}_1, \tilde{\lambda}_2, \ldots, \tilde{\lambda}_T\}.$$

Then at each time instant k, similar to (6), the probability of the sensor data packet arriving successfully at the remote estimator, denoted as $\tilde{p}_k$, can be written as

$$\tilde{p}_k = \tilde{\gamma}_k \tilde{\lambda}_k (1 - \beta_2) + \tilde{\gamma}_k (1 - \tilde{\lambda}_k)(1 - \beta_1). \tag{12}$$

Therefore, the constraints of the new problem become $\sum_{k=1}^T \tilde{\gamma}_k = M$ and $\sum_{k=1}^T \tilde{\lambda}_k = N$.

Interestingly, with average energy constraints, a closed-form expression for the objective functions $J_S(\tilde{\theta}_S^{\text{mixed}})$ and $J_A(\tilde{\theta}_A^{\text{mixed}})$ can be derived, by studying an underlying Markov chain, as discussed next.

B. Markov Chain Model

Based on the updating procedure of the error covariance P_k in (8) and the steady state assumption (1), it is easy to see that at any time instant $k_2 \geqslant k_1$, the error covariance at the remote estimator side can be written via iterated map as $P_{k_2} = h^{k_2 - k_1}(\overline{P})$, where k_1 is the latest time when the sensor data packet arrives successfully.

Definition 5.2: During the time-horizon T, if at time k, the state error covariance at the remote estimator $P_k = h^{i-1}(\overline{P})$, for some $i = 1, 2, \ldots, T+1$, then the state of the remote estimator is denoted as $S_k \triangleq z_{i,k}$. □

The state sets for time k is defined as

$$\mathbb{Z}_k = \{S_k | S_k = z_{i,k}, \quad 1 \leqslant i \leqslant T+1\}, \quad k = 1, 2, \ldots, T.$$

For convenience, as we already assumed that the remote estimator's error covariance is $\overline{P}$ before the process starts, i.e., $P_0 = \overline{P}$, $\mathbf{Z}_0 = \{z_{1,0}\}$ is the initialization state set before the process begins.

Due to the updating equation in (7), at any time $k+1$, the state S_{k+1} is only related to the previous state S_k. Thus the stochastic process $\{S_k\}, k = 1, 2, \ldots, T$, constitutes a Markov chain [26] (see Fig. 3). If $\mathbf{T}_k$ denotes the transition matrix from state set $\mathbf{Z}_{k-1}$ to $\mathbf{Z}_k$, then each entry of $\mathbf{T}_k$ can be expressed as

$$\mathbf{T}_k(i_1, i_2) = \mathbb{P}[z_{i_2,k} | z_{i_1,k-1}]. \tag{13}$$

Thus, the process is described by T transition matrices $\{\mathbf{T}_k\}_{k=1,2,\ldots,T}$ and each element can be easily computed as follows. If the sensor data packet arrives at the remote estimator, we have $P_k = \overline{P}$. Based on (13), this gives

$$\begin{aligned}\mathbf{T}_k(i_1, 1) &= \mathbb{P}[z_{1,k} | z_{i_1,k-1}] \\ &= \mathbb{P}[P_k = \overline{P} | z_{i_1,k-1}] \\ &= \tilde{p}_k, \quad \forall\, 1 \leqslant i_1 \leqslant T+1\end{aligned}$$

where $\tilde{p}_k$ is defined in (12). On the other hand, if the packet is dropped (even if the channel is not attacked), then $P_k = h(P_{k-1})$, and we have

$$\begin{aligned}\mathbf{T}_k(i_1, i_1 + 1) &= \mathbb{P}[z_{i_1+1,k} | z_{i_1,k-1}] \\ &= \mathbb{P}\left[P_k = h(P_{k-1}) | z_{i_1,k-1}\right] \\ &= \tilde{q}_k, \quad \forall\, 1 \leqslant i_1 \leqslant T\end{aligned}$$

where $\tilde{q}_k = 1 - \tilde{p}_k$ is the corresponding packet jamming probability.

Other entries of $\mathbf{T}_k$ are 0, since the corresponding state transitions are not possible. This gives

$$\mathbf{T}_k = \begin{bmatrix} \tilde{p}_k & \tilde{q}_k & & & \\ \tilde{p}_k & & \tilde{q}_k & & \\ \vdots & & & \ddots & \\ \tilde{p}_k & & & & \tilde{q}_k \end{bmatrix}_{(T+1)\times(T+1)}$$

where the missing entries are 0.

We define $\pi_{i,k}$ as the probability of state $z_{i,k}$ occurring at time k

$$\pi_{i,k} = \mathbb{P}[S_k = z_{i,k}] \tag{14}$$

then we can construct the probability matrix $\Pi = [\pi_{i,k}]_{(T+1)\times T}$.

From the definition of $\pi_{i,k}$, it is straightforward to show

$$\sum_{i=1}^{T+1} \pi_{i,k} = 1, \quad k = 1, 2, \ldots, T.$$

As we assumed $P_0 = \overline{P}$, at time $k = 1$, it follows that:

$$\begin{aligned}\pi_{1,1} &= \mathbb{P}[P_1 = \overline{P}] = \tilde{p}_1 \\ \pi_{2,1} &= \mathbb{P}\left[P_1 = h(\overline{P})\right] = \mathbb{P}\left[P_1 = h(P_0)\right] = \tilde{q}_1\end{aligned}$$

and

$$\pi_{i,1} = 0; \quad \forall i = 3, 4, \ldots, T+1.$$

To calculate an explicit form of Π, we first recall the definition of the transition matrix $\mathbf{T}_k$ in (13), from which the following relationship between $\mathbf{T}_k$ and Π can be established:

$$\Pi[k]^{\mathrm{T}} = \Pi[k-1]^{\mathrm{T}} \mathbf{T}_k \tag{15}$$

where $\Pi[k]$, $k = 1, \ldots, T$ is the k-th column of Π.

As we have already shown that $\Pi[1] = [\tilde{p}_1, \tilde{q}_1, 0, 0, \ldots, 0]^T$, following the recursion in (15), through some basic calculations, we can obtain the exact form of Π as a $T+1$ by T matrix:

$$\Pi = \begin{bmatrix} \tilde{p}_1 & \tilde{p}_2 & \tilde{p}_3 & \cdots & \tilde{p}_T \\ \tilde{q}_1 & \tilde{p}_1\tilde{q}_2 & \tilde{p}_2\tilde{q}_3 & \cdots & \tilde{p}_{T-1}\tilde{q}_T \\ 0 & \tilde{q}_1\tilde{q}_2 & \tilde{p}_1\tilde{q}_2\tilde{q}_3 & \cdots & \tilde{p}_{T-2}\tilde{q}_{T-1}\tilde{q}_T \\ 0 & 0 & \tilde{q}_1\tilde{q}_2\tilde{q}_3 & \cdots & \tilde{p}_{T-3}\tilde{q}_{T-2}\tilde{q}_{T-1}\tilde{q}_T \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \tilde{q}_1\tilde{q}_2\tilde{q}_3\cdots\tilde{q}_T \end{bmatrix}. \tag{16}$$

The above result significantly alleviates the computation issues. Once we have the probability matrix Π, we can easily obtain the closed-form expected error covariance for each time slot. In fact from (14), the definition of $\pi_{i,k}$, we have

$$\mathbb{E}[P_k] = \sum_{i=1}^{T+1} \pi_{i,k} h^{i-1}(\overline{P}).$$

Consequently, we can readily write $J_S(\tilde{\theta}_S^{\mathrm{mixed}})$ and $J_A(\tilde{\theta}_A^{\mathrm{mixed}})$ in a closed-form. Thus, following a similar procedure as in Section III-C, by using Lagrange multipliers, one can obtain the optimal solutions $\tilde{\theta}_S^\star$ and $\tilde{\theta}_A^\star$.

C. Comparison and Analysis

We will compare the constraint-relaxed problem formulation in Section V with the original one (Problem 2.2) using some examples.

Under the original energy constraints in Problem 2.2, when T increases, as the combinations number is $C_T^M \times C_T^N$ to $2^T \times 2^T$ with computation complexity $O((T!)^2)$, the calculation will become impractical. For example, when $T = 10$ and $M = N = 5$, one needs to consider $C_{10}^5 \times C_{10}^5 = 252 \times 252 = 63504$ different combinations of the pure strategies from both sides to obtain the closed-form expression of the objective functions. Under the constraint-relaxed problem formulation, however, computation complexity can be significantly reduced. This is due to the fact that the probability matrix can be obtained in a quite systematic way as shown in (16).

Now we use a simple example to illustrate the constraint-relaxed problem formulation where $T = 2$, $M = 1$, $N = 1$, $\alpha = 1$. The system parameters A, C, Q, R and the steady-state error covariance $\overline{P}$, are all scalars. Then one has the optimal solution

$$\begin{cases} \tilde{\gamma}_1^\star = \tilde{\gamma}_2^\star = \frac{1}{2} \\ \tilde{\lambda}_1^\star = \tilde{\lambda}_2^\star = \frac{1}{2} \end{cases}$$

i.e., the optimal strategy for the sensor under the relaxed constraints, is to send data packet with probability 0.5 at both time slots. One can interpret it as a mixed strategy which randomly chooses the pure strategies $\{0, 0\}$, $\{0, 1\}$, $\{1, 0\}$, $\{1, 1\}$, with the same probability 0.25. As a comparison, the optimal mixed strategies for the original Problem 2.2 are to randomly choose the pure strategies $\{0, 1\}$ and $\{1, 0\}$, each with probability 0.5.

When $T > 2$, the optimal strategy depends on the system parameters. For example, a process with parameters $A = 1.2$, $C = 0.7$, $Q = R = 0.8$, $\beta_1 = 0$, $\beta_2 = 1$, $T = 2$, $M = N = 1$ is considered. The optimal solution turns out to be $\mu_1^\star = 0.2748$, $\mu_2^\star = 0.4504$, $\mu_3^\star = 0.2748$ and $\pi_1^\star = 0.3626$, $\pi_2^\star = 0.2748$, $\pi_3^\star = 0.3626$.

VI. Conclusion

We have studied a CPS scenario where a malicious agent carries out jamming attacks on the communication channel between a sensor and a remote estimator. We first considered a situation where the sensor and the attacker fix their strategies *a priori*. For the case where the sensor and the attacker have on-line information about the previous transmission outcomes and the occurrence of attacks, we provided an algorithm which performs the game dynamically. We also introduced an alternative problem formulation which considers average energy constraints. By using a Markov chain model, we obtained a closed-form expression for the objective function. The associated optimization problem requires significantly less computation.

Possible extensions include studying the multi-sensor case with interferences between each sensor and attack from the attacker, and other types of attack including deception attack, which focuses on the integrity of the data by modifying the data packets.

Acknowledgment

The authors would like to thank the associate editor and the anonymous reviewers for their comments and suggestions which have helped to improve the presentation of the paper.

References

[1] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proc. 1st Int. Conf. High Confidence Networked Syst.*, 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," *Proc. 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 *Proc. 28th Int. Conf. Distrib. Comp. Syst. Workshops*, 2008, pp. 495–500.

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

[5] M. Zuba, Z. Shi, Z. Peng, and J. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proc. 6th ACM Int. Workshop Underwater Netw.*, 2011, p. 12.

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

[7] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[8] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, vol. 200. Philadelphia, PA, USA: SIAM, 1995.

[9] S. Bhattacharya and T. Başar, "Game-theoretic analysis of an aerial jamming attack on a uav communication network," in *Proc. IEEE Amer. Control Conf. (ACC'10)*, 2010, pp. 818–823.

[10] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proc. IEEE 43rd Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2010, pp. 1–10.

[11] A. Kashyap, T. Başar, and R. Srikant, "Correlated jamming on MIMO gaussian fading channels," *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 2119–2123, 2004.

[12] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decision Control (CDC)*, 2010, pp. 1096–1101.

[13] A. Agah, S. Das, and K. Basu, "A game theory based approach for security in wireless sensor networks," in *Proc. IEEE Int. Conf. Perform., Comp., Commun.*, 2004, pp. 259–263.

[14] H. Li, L. Lai, and R. C. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *Proc. IEEE 45th Annu. Conf. Inform. Sci. Syst. (CISS)*, 2011, pp. 1–6.

[15] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attack on cyber-physical systems: A game-theoretic approach," in *Proc. IEEE 3rd Annu. Int. Conf. Cyber Technol. Autom. Control Intell. Syst. (CYBER)*, 2013, pp. 252–257.

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

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

[18] B. Anderson and J. Moore, *Optimal Filtering*. Englewood Cliffs, NJ, USA: Prentice Hall, 1990.

[19] L. Shi and L. Xie, "Optimal sensor power scheduling for state estimation of Gauss-Markov systems over a packet-dropping network," *IEEE Trans. Signal Process.*, vol. 60, no. 5, pp. 2701–2705, 2012.

[20] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. Jordan, and S. Sastry, "Kalman filtering with intermittent observations," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1453–1464, 2004.

[21] L. Shi, P. Cheng, and J. Chen, "Sensor data scheduling for optimal state estimation with communication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693–1698, 2011.

[22] R. Gibbons, *A Primer in Game Theory*. Hemel Hempstead, U.K.: Harvester Wheatsheaf, 1992.

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

[24] M. Hazewinkel, *Encyclopaedia of Mathematics: Supplement*, vol. 3. New York, NY, USA: Springer-Verlag, 2002.

[25] L. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A network security monitor," in *Proc. IEEE Comp. Soc. Symp. Res. Security Privacy*, 1990, pp. 296–304.

[26] P. Brémaud, *Markov Chains*. New York, NY, USA: Springer-Verlag, 1999.