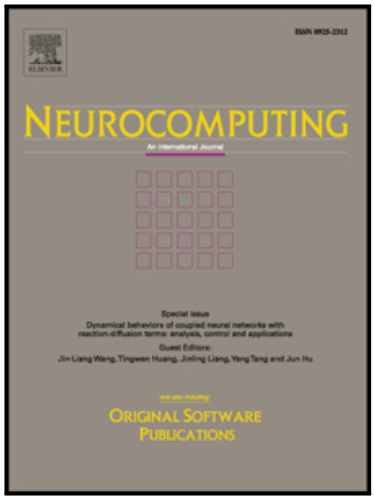
Communicated by Prof. Wei Guoliang

Accepted Manuscript



Security estimation under Denial-of-Service attack with energy constraint

Li Li, Huixia Zhang, Yuanqing Xia, Hongjiu Yang

PII: S0925-2312(18)30261-3
DOI: 10.1016/j.neucom.2018.02.086
Reference: NEUCOM 19391

To appear in: *Neurocomputing*

Received date: 10 November 2017
Revised date: 17 January 2018
Accepted date: 27 February 2018

Please cite this article as: Li Li, Huixia Zhang, Yuanqing Xia, Hongjiu Yang, Security estimation under Denial-of-Service attack with energy constraint, *Neurocomputing* (2018), doi: 10.1016/j.neucom.2018.02.086

Security estimation under Denial-of-Service attack with energy constraint

Li Li, Huixia Zhang, Yuanqing Xia and Hongjiu Yang

Abstract

This paper concentrates on security estimation of Cyber-Physical Systems subject to Denial-of-Service attack. A game framework is established to describe the interactive decision making process between the sensor and the attacker under energy constraint. A novel payoff function is used and the optimal strategies for both sides constituting a Nash equilibrium (NE) are obtained by using matrix game. Furthermore, the security issue on state estimation for CPS with multiple-subsystem is investigated based on game theory. To deteriorate the whole system performance, the attacker should decide when to attack and which subsystem to be chosen on account of limited energy. The existence conditions of NE strategies are given. Two numerical examples are provided to demonstrate the feasibility of the results.

Index Terms

State estimation, Cyber-Physical Systems, DoS attack, game theory, multiple-subsystem.

I. Introduction

Cyber-Physical Systems (CPS) are systems integrating computation, network and physical process which consists of sensors, actuators, control units and communication devices [1, 2], which have attracted considerable interest from both academic and industrial communities in the past few years, such as aerospace, smart grid, intelligent transportation, smart building, etc. However, with extensive use of widespread networking, wireless connection among sensors, estimators and actuators are more vulnerable to cyber security threats than wired sensors. The security issue caused by malicious attacks is of fundamental importance to ensure the safe operation of CPS [3–5], which have been investigated from different perspectives. The attack or the jamming is essentially a kind of methods, processes, or means which are utilized to maliciously reduce network reliability. In particular, deception attack and Denial-of-Service (DoS) are two typical attacks in reducing system performance. The former modifies the data packets in a malicious way [6–11], while the DoS attack blocks the information flow between the sender and the receiver to increase the packet drop rate [12–18]. Compared with deception attack, the DoS attack, which does not require comprehensive information about the system and the data, is a more reachable attack pattern in a shared network. Some critical systems which rely on real-time operation may become unstable and even be damaged under DoS attack.

Many scholars have acknowledged the importance of addressing the challenge of designing secure CPS. In the existing works, various efforts have been devoted to design estimators influenced by specific malicious attacks [12-21]. In [12], an optimal attack schedule has been investigated to maximize the expected average estimation error variance. To capture the strategic iteration between the sensor and the attacker, the game-theoretic approach provides such a framework to handle interactive decision issues (see [13–15]). In [16], a two-player zero-sum stochastic game is established to model the dynamic interaction between the defender and the DoS attacker. Due to energy constraint is inherent in almost all types of attacks, an integrated game-theoretic framework is proposed to investigate the interactive decision-making process under energy constraints in [17]. A multi-channel transmission schedule for remote state estimation under DoS attack is studied in [18, 19], in which a Nash Q-learning algorithm is proposed to reduce the

Li Li, Huixia Zhang and Hongjiu Yang are with the Institute of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China. Emails: lili@ysu.edu.cn; huixiaz0914@163.com; yanghongjiu@ysu.edu.cn. Yuanqing Xia is with the School of Automation, Beijing Institute of Technology, Beijing 100081, China. Email: xia_yuanqing@bit.edu.cn.

computation complexity when solving the optimal strategies for both players. Besides, the paper [20] is applied a novel acknowledgement-based cheating scheme for the sensor to confuse the DoS attacker. In [21], multiple channels are used to defense the attacker when system is attacked and the attacker and anti-attacker are modeled as a zero-sum stochastic game.

Besides, it is common that many system components share a common communication network (like a communication bus or a wireless local area network) [23]. A great of correlative results on remote state estimation in multi-systems can be found in [12, 22–24]. For example, some event-triggered control loops are closed over a shared medium communication in [24]. In this situation, attackers need to decide when to launch attack and which target system to be chosen for achieving the purpose of jamming signals, and sensors face a tradeoff between consuming more energy to increase link reliability thereby ensuring an accurate remote estimation performance, and consuming less energy to meet the energy constraints. In [12], an optimal attack schedule for the attacker has been designed in a networked control system with multiple-subsystem. Due to dynamic nature of the systems, when the attacker and the sensors choose actions, they should take consideration of the actions their opponent may take. Therefore, instead of a static analysis focusing on only one side of the security issues, a more comprehensive game-theoretic framework to model the interactive action making process between the sensors and the attack is needed for the scenario with multiple-subsystem, which motivates the present study.

In this article, the security estimation for CPS subject to DoS attack is considered under game framework. Both the sensor and the attacker have limited energy budget. Firstly, a system in which one sensor measures the state and sends the data packets to a remote estimator through a wireless channel is considered. The interactions between the sensor and the DoS attacker is studied based on game theory. A novel pay-off function is proposed and optimal strategies for both sides are obtained by using matrix game. Then, we extend it to the scenario with multiple-subsystem. In this scheme, the DoS attacker has to decide when to attack and which subsystem to be attacked. An integrated game-theoretic framework is developed to investigate the interactive decision-making process between the sensors and the attacker. Moreover, existence conditions of NE strategies are presented. Finally, two numerical examples are provided to illustrate the effectiveness of the proposed design techniques. The main contributions of this paper are summarized as below:

i Under energy constraint, the interactions between the sensor and the DoS attacker is studied based on game theory. A novel pay-off function is proposed and the optimal strategies for both sides are obtained by using matrix game.

ii A game-theoretic framework for multiple-subsystem under DoS attack with energy constraint is established instead of a static analysis focusing on only one side, and the existence of NE solution for multiple-subsystem is proved.

The rest of this paper is organized as follows: In Section II, the system model and problem formulation is presented. Some game theory preliminaries and the optimal strategies for both sides is studied in Section III. The game for multiple-subsystem under DoS attack is proposed in Section IV. Numerical simulations are given to demonstrate the validity of the results in Section V. Section VI concludes this paper.

Notation: Some standard notations are used throughout this paper. For a matrix A, A^T and A^{-1} represent its transpose and inverse, respectively. $A > 0$ (resp. $A < 0$) means that A is positive definite (resp. negative definite). $A \geq 0$ (resp. $A \leq 0$) means that A is a semi-positive definite (resp. semi-negative definite). $\mathbb{E}\{x\}$ stands for the expectation of random variable x. $P\{x|y\}$ stands for the probability of x on condition of y. $\mathbb{R}^n$ denotes n-dimensional Euclidean space and $\mathbb{N}$ is the set of nonnegative integers. $\text{diag}\{x\}$ is a diagonal matrix with diagonal entries given by elements of x. I is an identity matrix with the appropriate dimension. $T!$ represents the factorial of T. For functions h, g, $g \circ h$ is defined as the function composition $g(h(\cdot))$. $Tr(\cdot)$ is the trace of a square matrix. C_T^M stands for $T!/(M!(T-M)!)$ and r^N is $\underbrace{r \cdots r}_{N \text{ times}}$.

II. Problem Statement and Preliminaries

Consider the following discrete linear time-invariant (LTI) system:

$$x_{k+1} = Ax_k + w_k \tag{1}$$

$$y_k = Cx_k + v_k \tag{2}$$

where $k \in \mathbb{N}$, $x_k \in \mathbb{R}^{n_x}$ is the 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 uncorrelated zero-mean Gaussian white noises with covariances Q and R, respectively. The pair (A, C) is assumed to be observable and $(A, Q^{1/2})$ is controllable.

A. Local state estimation

The system under DoS attack is shown in Fig. 1.

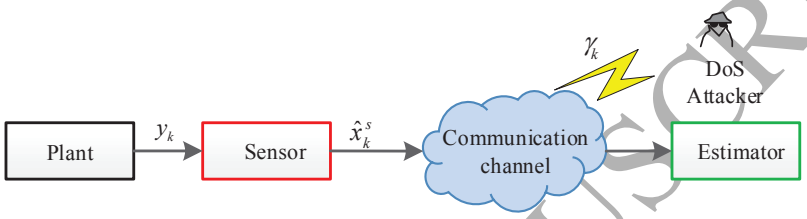


Fig. 1. The system under DoS attack

In order to improve the estimation performance, a smart sensor with storage and computing capabilities is used for the system under DoS attack [17]. On the other hand, the smart sensor is also able to collect information by conducting some simple recursive algorithms. With the use of the smart sensor, a local estimation $\hat{x}_k^s$ of the state x_k is obtained by running a Kalman filter after taking measurement y_k and then $\hat{x}_k^s$ is transmitted to the remote estimator. The local minimum mean-squared error (MMSE) estimate $\hat{x}_k^s$ of the process x_k is denoted by

$$\hat{x}_k^s = \mathbb{E}\{x_k | y_1, y_2, \ldots, y_k\} \tag{3}$$

The estimation error covariance matrix $\hat{P}_k^s$ is given by

$$\hat{P}_k^s = \mathbb{E}\{(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)^T | y_1, y_2, \ldots, y_k\} \tag{4}$$

The standard Kalman filter [8] adopted by the sensor is as follows:

$$\begin{aligned}
\hat{x}_{k|k-1} &= A\hat{x}_{k-1}^s \\
P_{k|k-1} &= AP_{k-1}^s A^T + Q \\
K_k &= P_{k|k-1}C^T[CP_{k|k-1}C^T + R]^{-1} \\
\hat{x}_k^s &= A\hat{x}_{k-1}^s + K_k[y_k - C\hat{x}_{k|k-1}] \\
P_k^s &= (I - K_k C)P_{k|k-1}
\end{aligned}$$

For convenience of analysis, define the following matrix functions h and g:

$$h(X) \triangleq AXA^T + Q \tag{5}$$

$$g(X) \triangleq X - XC^T[CXC^T + R]^{-1}CX \tag{6}$$

It is generally known that the estimation error covariance of the Kalman filter converges to a unique value from any initial condition. In order to simplify the subsequent discussion, the Kalman filter at the sensor side is assumed to enter the steady state. Thus, we have

$$P_k^s = \bar{P}, \ k \geq 1$$

where $\bar{P}$ is the steady-state error covariance given in [25, 26], which is the unique fixed solution of $g \circ h(X) = X$. When the Kalman filter is in the steady state, the Kalman gain become a constant K which can be computed offline [27]. Then the sensor merely calculates the state as following:

$$\hat{x}_k^s = A\hat{x}_{k-1}^s + K[y_k - C\hat{x}_{k|k-1}]$$

.

B. Communication network

Communication between components of CPS is influenced by a typical DoS attack which blocks the information flow between the sensor and the receiver to increase packet drop rate. And performance of the system subject to packets dropout will be deteriorated [28, 29]. In practice, due to limited energy, the remote estimation performance and strategies corresponding to the sensor and the attacker will be affected. Within a given time frame T, the data packet is transmitted at most M times from the sensor to the remote estimator, where M meets $M \leq T$. On the other hand, the attacker can launch attack at most N times, where N meets $N \leq T$.

The transmission strategy of the sensor is represented as

$$\vartheta_S \triangleq \{\lambda_1, \lambda_2, \cdots, \lambda_T\}$$

where $\lambda_k = 1$ indicates that the sensor transmits the estimation to the remote estimator at time k and $\lambda_k = 0$ otherwise. Then, the following constraint is obtained

$$\sum_{k=1}^{T} \lambda_k \leq M \tag{7}$$

Similarly, the attack strategy is represented as

$$\vartheta_A \triangleq \{\gamma_1, \gamma_2, \cdots, \gamma_T\}$$

where $\gamma_k = 1$ indicates that the attacker launches a DoS attack at time k and $\gamma_k = 0$ otherwise. Then, the following constraint is obtained

$$\sum_{k=1}^{T} \gamma_k \leq N \tag{8}$$

In this article, the network is supposed to be reliable without attacker appearing. In other words, there is no packet dropout between the sensor and the remote estimator. What's more, the packet loss rate under the DoS attack is defined by θ.

C. Remote estimation process

For facilitating the following description, $\hat{x}_k$ and P_k are defined to represent the remote estimator's MMSE state estimate and error covariance of the process x_k . At time k, the estimation is $\hat{x}_k = \hat{x}_k^s$ only when $\hat{x}_k^s$ is successfully received by the remote estimator; otherwise, the estimation is predicted based on the estimation of the previous step. Thus, the estimation is obtained as

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

Similarly, the error covariance P_k is derived as

$$P_k = \begin{cases} \bar{P}, & \text{if packet arrives} \\ h(P_{k-1}), & \text{otherwise} \end{cases}$$

Assume that the initial value of the error covariance is $\bar{P}$, i.e., $P_0 = \bar{P}$, which indicates a local state estimate at time $k = 0$. According to [12], P_k can only take values in the finite set $\{\bar{P}, h(\bar{P}), \cdots, h^k(\bar{P})\}$ at a given time k.

D. Main Problem

For a given attack strategy ϑ_A, define $J_\theta(\gamma_k)$ as the average expected estimation error covariance matrix. θ is packet loss rate under DoS attack. Then $J_\theta(\gamma_k)$ is described by

$$J_\theta(\gamma_k) = \frac{1}{T}\sum_{k=1}^{T}\mathbb{E}[P_k(\gamma_k)] \tag{9}$$

In order to analyze performance of the sensor and the attacker, the packet loss rate $\theta(\vartheta_A)$ is defined as cost function for the attacker. $J_S(\vartheta_S)$ is defined as pay-off function for the sensor as following

$$J_S(\vartheta_S) \triangleq -Tr\{J_\theta(\gamma_k)\} \tag{10}$$

Remark 1. *Estimation error covariance is an index to evaluate performance of the state estimation. In this article, a system under DoS attack with energy constraint is studied. Consider a finite horizon T and a given attack schedule γ_k, due to the finite energy constraint, a typical pay-off function: the average expected estimation error covariance, is adopted to analyze performance of the sensor and the attacker in this article. Similar definitions can be found in[17, 18, 26].*

The purpose of the sensor and the attacker is to maximize their pay-off function, respectively. Due to the energy for both sides is constrained, we are interested in finding the optimal strategies for each side. It is obvious that more energy is beneficial for improving performance. The optimal strategies for both sides are not changed if the conditions change from (7) and (8) to $\sum_{k=1}^{T}\lambda_k = M$ and $\sum_{k=1}^{T}\gamma_k = N$, respectively. (similar transformation can be found in [17], [30]).

Based on the above analysis, similar to [17], a new optimization problem is raised as follows:

Problem 1. *For the sensor*

$$\max_{\vartheta_S} \quad J_S(\vartheta_S)$$
$$s.t. \sum_{k=1}^{T}\lambda_k = M$$

For the attacker

$$\max_{\vartheta_A} \quad \theta(\vartheta_A)$$
$$s.t. \sum_{k=1}^{T}\gamma_k = N$$

Remark 2. *It should be pointed out that $J_A(\vartheta_S) \triangleq Tr\{J_\theta(\gamma_k)\}$ is adopted as a pay-off function of the attacker in [17]. While in the above problem, the pay-off function for the attacker is defined as $\theta(\vartheta_A)$ which is convenient for analysis in game framework. Furthermore, the relation between $J_A(\vartheta_S)$ and $\theta(\vartheta_A)$ will be given in the following.*

It is easy to know that $J_A(\vartheta_S)$ is a function of the packet loss rate θ. Next, the relation between $J_A(\vartheta_S)$ and $\theta(\vartheta_A)$ will be given. A lemma is introduced to facilitate the proof. It can be seen that the error covariance matrix P_k during the consecutive attack period $[s+1, s+m]$ is a stationary Markov chain:

Lemma 1. *1) the distribution of error covariance matrix P_{s+k} is represented as*

$$Pr\{P_{s+k} = h^{\zeta}(\bar{P})\} = \begin{cases} \theta^{\zeta} - \theta^{\zeta+1}, & \zeta = 0, 1, \cdots, k-1 \\ \theta^{k}, & \zeta = k \end{cases}$$

2) the conditional probability is represented as follows:

$$Pr\{P_{s+k} = h^{j}(\bar{P}) | P_s = h^{\zeta}(\bar{P})\} = \begin{cases} \theta^{j} - \theta^{j+1}, & j = 0, 1, \cdots, k-1 \\ \theta^{k}, & j = \zeta + k \end{cases}$$

Attacking times n is given by an attack strategy with following attacking sequences, $k_1, k_2, \cdots, k_s, i.e.$,

$$(0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_1 \text{ times}}, 0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_2 \text{ times}}, 0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_s \text{ times}}, 0, \cdots, 0) \tag{11}$$

where $\sum_{\zeta=1}^{T} = N$, 1 indicates that the attacker launches an attack and 0 otherwise. Note that each neighboring sequences are divided by at least one zero. Then we have

$$\begin{aligned} J_{\theta}(\gamma_k) &= \frac{1}{T}\sum_{k=1}^{T}\mathbb{E}[P_k(\gamma_k)]\} = \frac{1}{T}\sum_{\zeta=1}^{s}\sum_{n_\zeta=1}^{k_\zeta}\mathbb{E}[P_{s_\zeta+n_\zeta}] + \frac{T-n}{T}\bar{P} \\ &= \frac{1}{T}\sum_{\zeta=1}^{s}\sum_{n_\zeta=1}^{k_\zeta}\left[\sum_{m=0}^{n_\zeta-1} h^m(\bar{P})(\theta^m - \theta^{m+1}) + \theta^{n_\zeta}h^{n_\zeta}(\bar{P})\right] + \frac{T-n}{T}\bar{P} \end{aligned} \tag{12}$$

Lemma 2. *$J_A(\vartheta_A)$ is a monotonically increasing function about θ.*

Proof. Define $\Psi = \sum_{m=0}^{n_\zeta-1} h^m(\bar{P})(\theta^m - \theta^{m+1}) + \theta^{n_\zeta}h^{n_\zeta}(\bar{P})$. Then the monotonicity of $J_\theta(\gamma_k)$ and Ψ is consistent.

$$\begin{aligned} \Psi' &= \left[\sum_{m=0}^{n_\zeta-1} h^m(\bar{P})(\theta^m - \theta^{m+1}) + \theta^{n_\zeta}h^{n_\zeta}(\bar{P})\right]' \\ &= \sum_{m=0}^{n_\zeta-1} h^m(\bar{P})\{m\theta^{m-1} - (m+1)\theta^m\} + n_\zeta\theta^{n_\zeta-1}h^{n_\zeta}(\bar{P}) \\ &= h(\bar{P}) - h^0(\bar{P}) - 2\theta[h(\bar{P}) - h^2(\bar{P})] - 3\theta^2[h^2(\bar{P}) - h^3(\bar{P})] + \cdots + n_\zeta\theta^{n_\zeta-1}h^{n_\zeta}(\bar{P}) \\ &= \sum_{m=0}^{n_\zeta-1}(m+1)\theta^m[h^{m+1}(\bar{P}) - h^m(\bar{P})] \end{aligned} \tag{13}$$

According to the Property 3.3 of reference [12], $h^m(\bar{P})$ is an increasing function. Therefore we can obtain $\Psi' > 0$, which is the same to $J'_\theta(\gamma_k) > 0$. $J_A(\vartheta_S)$ is also an increasing function. Therefore, maximizing packet loss rate is equivalent to maximizing the error covariance for the attacker. □

III. Game Framework

Depending on the targets of the attacker and the sensor, the adopted game may take different strategies. In a game, the sensor and the attacker are two players where ϑ_S and ϑ_A are their respective actions. No player is able to benefit from changing his own strategy while the other players keep theirs benefit unchangeable. Therefore the current strategy profile, i.e., the current set of strategy choices, constitutes a

Nash equilibrium (defined in [31]). A series of processes are described for convenience of the later narrative in which several definitions are introduced. For example, the pure strategy: Participants choose only one specific strategy under the given information. The mixed strategy: Participants make a combination of pure strategies with different probabilities. Both sides do not know the exact following action taken by their opponent in the game and any side does not use a single strategy to reach the NE. Further, there exists at least one mixed strategy NE for any game with a finite set of strategies, which is proved in [31, 32].

In this section, the matrix game framework is adopted to solve the problem 1. Define the attack strategy set as $\{a_1, a_2, \ldots, a_n\}$, and the mixed strategy $\Phi_A(a_p)$ is a probability of the DoS attacker choosing attack behavior $a_p, p = 1, 2, ...n$. On the other hand, define the defensor strategy set as $\{d_1, d_2, \ldots, d_m\}$, and the mixed strategy $\Phi_S(d_q)$ is a probability of the sensor choosing defensive behavior $d_q, q = 1, 2, ...m$. Moreover, there exist the following equalities

$$\sum_{q=1}^{n} \Phi_S(d_q) = 1 \quad q = 1, 2, \cdots, m \tag{14}$$

$$\sum_{p=1}^{m} \Phi_A(a_p) = 1 \quad p = 1, 2, \cdots, n \tag{15}$$

For simplicity, $\Phi_S(d_q)$ and $\Phi_A(a_p)$ are represented as $\Phi_S(q)$ and $\Phi_A(p)$, respectively. Let Φ_S and Φ_A be

$$\Phi_S := [\Phi_S(d_1), \Phi_S(d_2), \cdots, \Phi_S(d_m)]^T$$
$$\Phi_A := [\Phi_A(a_1), \Phi_A(a_2), \cdots, \Phi_A(a_n)]^T$$

NE for the problem 1 is defined in the following. For the convenience, we define $J = Tr\{J_S(\vartheta_S)\}$.

Definition 1. *If the following inequalities*

$$\begin{aligned} \theta(\Phi_S{}^*, \Phi_A) &\leq \theta(\Phi_S{}^*, \Phi_A{}^*) \\ J_S(\Phi_S, \Phi_A{}^*) &\leq J_S(\Phi_S{}^*, \Phi_A{}^*) \end{aligned}$$

set up simultaneously, strategy set (Φ_S^*, Φ_A^*) is called the NE strategy of the game model.

Considering the above definition, the optimal strategies for each side are Φ_S^* and Φ_A^*, respectively. The sensor is to maximize the benefit $J_S(\Phi_S, \Phi_A)$ given the optimal strategy Φ_S^*. The DoS attacker is to maximize the packet loss rate $\theta(\Phi_S, \Phi_A)$ given the optimal strategy Φ_A^*. Under the framework of the game model, there exists only one optimal allocation strategy in the form of an NE strategy. Any game players in the NE point do not get any benefit by altering its strategy unilaterally.

Next, the optimal strategy for the game will be designed. Firstly, the objective pay-off matrices $\mathbf{F}_\theta$ and $\mathbf{F_J}$ of the attacker and the sensor are defined as following

$\mathbf{F}_\theta :=$

	a_1	a_2	$\cdots$	a_n
d_1	θ_{11}	θ_{12}	$\ldots$	θ_{1n}
d_2	θ_{21}	θ_{22}	$\ldots$	θ_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
d_m	θ_{m1}	θ_{m2}	$\ldots$	θ_{mn}

(16)

$$\mathbf{F_J} := \begin{array}{|c|c|c|c|c|} \hline & a_1 & a_2 & \cdots & a_n \\ \hline d_1 & J_{S,11} & J_{S,12} & \cdots & J_{S,1n} \\ \hline d_2 & J_{S,21} & J_{S,22} & \cdots & J_{S,2n} \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline d_m & J_{S,m1} & J_{S,m2} & \cdots & J_{S,mn} \\ \hline \end{array} \tag{17}$$

In the pay-off matrices (16) and (17), the element θ_{qp}, $q = 1, 2, \cdots, m$, $p = 1, 2, \cdots, n$ is used to express benefit of the DoS attacker when the attacker uses behavior a_p and the defender uses defensive behavior d_q. Similarly, the element $J_{S,qp}$, $p = 1, 2, \cdots, n, q = 1, 2, \cdots, m$ is used to express benefit of the sensor when the sensor uses defensive behavior d_q and the DoS attacker uses attack behavior a_p. The following Theorem provides the conditions for the existence and uniqueness of NE, while the expression of NE strategy is given.

Theorem 1. *Denote matrices* $\mathbf{R_J}, \mathbf{R}_\theta, \mathbf{v_J}$ *and* $\mathbf{v}_\theta$ *as follows*

$$\mathbf{R_J} = \begin{bmatrix} J_{S,11} - J_{S,12} & J_{S,21} - J_{S,22} & \cdots & J_{S,m1} - J_{S,m2} \\ \vdots & \vdots & \ddots & \vdots \\ J_{S,11} - J_{S,1n} & J_{S,21} - J_{S,2n} & \cdots & J_{S,m1} - J_{S,mn} \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

$$\mathbf{R}_\theta = \begin{bmatrix} \theta_{11} - \theta_{12} & \theta_{21} - \theta_{22} & \cdots & \theta_{m1} - \theta_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{11} - \theta_{1n} & \theta_{21} - \theta_{2n} & \cdots & \theta_{m1} - \theta_{mn} \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

$$\mathbf{v_J} = \underbrace{\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^T}_{n} \quad \mathbf{v}_\theta = \underbrace{\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^T}_{m}$$

If matrices $\mathbf{F_J}$ *and* $\mathbf{F}_\theta$ *are invertible, meanwhile, the following equalities*

$$\mathbf{R_J}\Phi_S^* = \mathbf{v_J}, \quad \mathbf{R}_\theta\Phi_A^* = \mathbf{v}_\theta, \ n = m$$

have solutions with $\Phi_S(p), \Phi_A(q) > 0, \forall p \in \{1, 2, \cdots, m\}, \forall q \in \{1, 2, \cdots, n\}$*, then there exists a unique NE solution. The NE strategy* (Φ_S^*, Φ_A^*) *is given by*

$$\Phi_S^* = \mathbf{R_J^{-1}}\mathbf{v_J} \tag{18}$$

$$\Phi_A^* = \mathbf{R}_\theta^{-1}\mathbf{v}_\theta \tag{19}$$

Proof. Similar proof can be found in [33]. □

IV. CPS WITH MULTIPLE-SUBSYSTEM

In this section, the security estimation is considered for CPS with multiple-subsystem as in Fig. 2. Our purpose is to gain the optimal estimate strategy subject to DoS attack under a game framework. An assumption is proposed that the attacker launches a attack on multiple-subsystems in the wireless transmission networks. For example, DoS attacker is able to switch strategy between target subsystems, which achieves the purpose of jamming signals. In this situation, the attacker has to make the attack decision, i.e., when to attack, which subsystem and what to be chosen. While the sensors face a tradeoff between consuming more energy to increase link reliability and meeting the energy constraints.

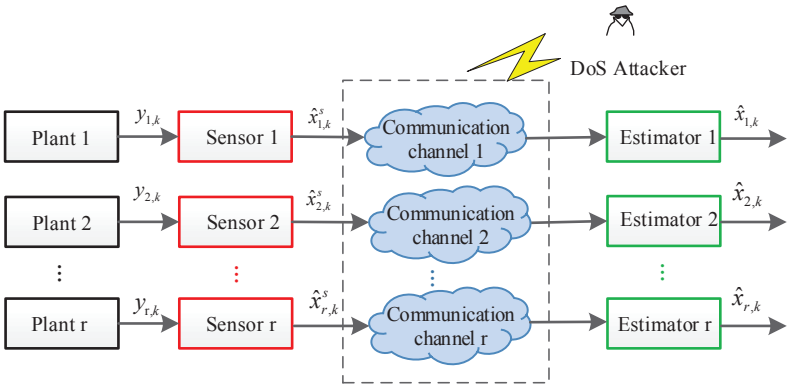


Fig. 2. The system with multiple-subsystem under DoS attack

The system model with multiple-subsystem is described in the following:

$$x_{i,k+1} = A_i x_{i,k} + w_{i,k} \tag{20}$$

$$y_{i,k} = C_i x_{i,k} + v_{i,k} \tag{21}$$

where $k \in \mathbb{N}$ and i stands for the ith subsystem, $x_{i,k} \in \mathbb{R}^{n_x}$ is the process state vector at time k for the ith subsystem. $y_{i,k} \in \mathbb{R}^{n_y}$ is the measurement taken by the sensor for the ith subsystem, $w_{i,k} \in \mathbb{R}^{n_x}$ and $v_{i,k} \in \mathbb{R}^{n_y}$ are uncorrelated zero-mean Gaussian noises with covariances Q_i and R_i for the ith subsystem, respectively. For different subsystems, $\mathbb{E}\{\omega_{i,k}\omega_{j,k}^T\} = 0$, $\mathbb{E}\{\nu_{i,k}\nu_{j,k}^T\} = 0, (i \neq j)$. The pair (A_i, C_i) is assumed to be observable and $(A_i, Q_i^{1/2})$ is controllable.

A. *Communication network*

In this section, due to limited energy, the remote estimation performance and strategies corresponding to the sensors and the attacker will be affected. Within a given time frame T, the data packet is transmitted at most M_i times for the ith subsystem from the sensor i to the remote estimator i. And the sensor's energy constraint meets $M_i \leq T$. On the other hand, the attacker can only jam one channel or does not take action in any time. And the attacker's energy constraint meets $N \leq T$. The transmission strategies of the sensors are represented as

$$\vartheta_S' \triangleq \left\{ \begin{array}{cccc} \lambda_{1,1}, & \lambda_{1,2}, & \cdots, & \lambda_{1,T} \\ \lambda_{2,1}, & \lambda_{2,2}, & \cdots, & \lambda_{2,T} \\ \cdots, & \cdots, & \cdots, & \cdots \\ \lambda_{r,1}, & \lambda_{r,2}, & \cdots, & \lambda_{r,T} \end{array} \right\} \tag{22}$$

where r is the number of subsystems. $\lambda_{i,k} = 1, (i = 1, 2, ...r, k = 1, 2, ...T)$ indicates that the sensor i transmits the estimation successfully to the remote estimator i at time k and $\lambda_{i,k} = 0$ otherwise. Then, the following constraint is obtained

$$\sum_{k=1}^{T} \lambda_{i,k} \leq M_i \quad (i = 1, 2, \cdots, r) \tag{23}$$

Similarly, the attack strategy is represented as

$$\vartheta_A' \triangleq \left\{ \begin{array}{cccc} \gamma_{1,1}, & \gamma_{1,2}, & \cdots, & \gamma_{1,T} \\ \gamma_{2,1}, & \gamma_{2,2}, & \cdots, & \gamma_{2,T} \\ \cdots, & \cdots, & \cdots, & \cdots \\ \gamma_{r,1}, & \gamma_{r,2}, & \cdots, & \gamma_{r,T} \end{array} \right\} \tag{24}$$

where $\gamma_{i,k} = 1, (i = 1, 2, ...r, k = 1, 2, ...T)$ indicates that the attacker launches a DoS attack at time k for the ith subsystem and $\gamma_{i,k} = 0$ otherwise. It is assumed that the packet loss rate is θ_i when the attacker jams the ith system. Due to energy constraint, we suppose that the attacker can only jam one channel or does not take action in any time. Then, the following constraint is obtained

$$\sum_{i=1}^{r}\sum_{k=1}^{T}\gamma_{i,k} \leq N \tag{25}$$

B. State estimation

Firstly, for the sensor, the smart sensor is also used to collect information by conducting some simple recursive algorithms in the single system. An estimation of the state $x_{i,k}$ is obtained by running a Kalman filter after taking measurement $y_{i,k}$ by using the smart sensor, where i stands for the ith subsystem. Thus, it is unnecessary to transmit the measurement $y_{i,k}$ to the remote estimator i. The local MMSE estimate $\hat{x}^s_{i,k}$ of the process $x_{i,k}$ for the ith subsystem is denoted by

$$\hat{x}^s_{i,k} = \mathbb{E}[x_{i,k}|y_{i,1}, y_{i,2}, \cdots, y_{i,k}] \tag{26}$$

The estimation error covariance matrix $\hat{P}^s_{i,k}$ is given by

$$\hat{P}^s_{i,k} = \mathbb{E}[(x_{i,k} - \hat{x}^s_{i,k})(x_{i,k} - \hat{x}^s_{i,k})'|y_{i,1}, y_{i,2}, \cdots, y_{i,k}] \tag{27}$$

Without loss of generality, it is considered that the Kalman filter for ith subsystem is convergent from any initial condition. That is the error covariance $P^s_{i,k}$ is assumed to enter the steady-state at the sensor side.

$$P^s_{i,k} = \bar{P}_i, k \geq 1 \tag{28}$$

where the error covariance $P^s_{i,k}$ converges exponentially to a unique fixed point $\bar{P}_i$.

Secondly, for the remote estimator, to quantify estimation performance, $\hat{x}_{i,k}$ and $P_{i,k}$ are defined to represent the remote estimator's MMSE state estimate and error covariance of the process $x_{i,k}$. At time k, the estimation is $\hat{x}_{i,k} = \hat{x}^s_{i,k}$ only when $\hat{x}^s_{i,k}$ is successfully received by the remote estimator; otherwise, the estimation is predicted based on the estimation of the previous step for the ith subsystem. Thus, the estimation is obtained as

$$\hat{x}_{i,k} = \begin{cases} \hat{x}^s_{i,k}, & \text{if packet arrives} \\ A\hat{x}_{i,k-1}, & \text{otherwise} \end{cases}$$

Similarly, the error covariance $P_{i,k}$ is derived in the following

$$P_{i,k} = \begin{cases} \bar{P}_i, & \text{if packet arrives} \\ h(\bar{P}_{i,k-1}), & \text{otherwise} \end{cases}$$

Specially, when the system parameters of all subsystems are the same, the initial value of the error covariance P_0 for every remote estimator starts from $\bar{P}$, that is, $\bar{P}_i = P_0 = \bar{P}$.

C. Problem setup

For a given attack strategy ϑ'_A, define $J_{i,\theta_i}(\gamma_{i,k})$ as the average expected estimation error covariance matrix for the ith subsystem. Then $J_{i,\theta_i}(\gamma_{i,k})$ is described by

$$J_{i,\theta_i}(\gamma_{i,k}) = \frac{1}{T}\sum_{k=1}^{T}\mathbb{E}[P_{i,k}(\gamma_{i,k})] \tag{29}$$

From the viewpoint of sensors, the purpose is to maximize their total pay-off function

$$J_S(\vartheta'_S) = \sum_{i=1}^{r} J_{i,S}(\vartheta'_S) \tag{30}$$

$$J_{i,S}(\vartheta'_S) \triangleq -Tr\{J_{i,\theta_i}(\gamma_{i,k})\} \tag{31}$$

Due to energy constraint, the DoS attacker needs to make decisions when and which channel to jam in order to maximize the pay-off function

$$J_A(\vartheta'_A) = -J_S(\vartheta'_S) \tag{32}$$

We are interested in finding the optimal strategies for each side, subject to the energy constraints (24) and (25). Similarly, more energy is always beneficial for improving performance, the energy constraints (24) and (25) are changed to $\sum_{k=1}^{T} \lambda_{i,k} = M_i$, $\sum_{i=1}^{r}\sum_{k=1}^{T} \gamma_{i,k} = N$, respectively. Both the sensors and the attacker want to achieve their maximum cost, which raises the following optimal problem.

Problem 2. *For the sensors*

$$\max_{\vartheta'_S} \quad J_S(\vartheta'_S)$$
$$s.t. \sum_{k=1}^{T} \lambda_{i,k} = M_i \qquad (i = 1, 2, \cdots, r)$$

For the attacker

$$\max_{\vartheta'_A} \quad J_A(\vartheta'_A)$$
$$s.t. \sum_{i=1}^{r}\sum_{k=1}^{T} \gamma_{i,k} = N$$

Remark 3. *The attacker focuses more on the packet loss rate θ for the single system. While the attacker pays more attentions on overall performance of the system, that is, the error covariance of all subsystems. Therefore, $J_A(\vartheta'_A) = -\sum_{i=1}^{r} J_{i,S}(\vartheta'_S)$ is adopted as the pay-off function in problem 2 .*

D. Existence of the Nash equilbrium

In this section, for the situation with energy constraint for the attacker and the sensors. Both sides have many strategies and take the opponent's strategy into consideration, we shall investigate the problem from a game-theoretic point. As far as the sensors, the number of all the pure strategies is $U = C_T^{M_1} C_T^{M_2} ... C_T^{M_r}$. For future reference, those pure strategies are denoted as ${\vartheta'_S}^{\text{pure}}(1)$, ${\vartheta'_S}^{\text{pure}}(2)$, $\cdots$, ${\vartheta'_S}^{\text{pure}}(U)$. Mixed strategies for the sensors are able to be written as: ${\vartheta'_S}^{\text{mixed}}(\pi_1, \pi_2, \ldots, \pi_U)$ = $\{{\vartheta'_S}^{\text{pure}}(u)$ with probability $\pi_u\}$ and where $\pi_u \in [0, 1]$, $u = 1, 2, ..., U$ and $\sum_{u=1}^{U} \pi_u = 1$. Similarly, for the attacker, the number of all the pure strategies is $L = r^N C_T^N$, and the pure strategies are denoted as ${\vartheta'_A}^{\text{pure}}(1)$, ${\vartheta'_A}^{\text{pure}}(2)$, $\cdots$, ${\vartheta'_A}^{\text{pure}}(L)$. ${\vartheta'_A}^{\text{mixed}}(\mu_1, \mu_2, ..., \mu_L)$ =$\{{\vartheta'_A}^{\text{pure}}(l)$ with probability $\mu_l\}$,where $\mu_l \in [0, 1]$, $l = 1, 2, ..., L$, and $\sum_{l=1}^{L} \mu_l = 1$.

Firstly, Nash defined a mixed strategy NE for any game with a finite set of strategies and proved that at least one mixed strategy Nash must exist in such a game. Then, every side once chooses a strategy and no player is able to obtain benefit by changing his own strategy while the other players keep theirs unchanged. Finally, the two sides still do not know what exact action for the opponent is taken. Based the analysis above, the reason why both sides can achieve the NE is obtained.

Theorem 2. *For any game with a finite set of strategies, there exists at least one mixed strategy NE in the game.*

Proof. Proved in [31]. □

Lemma 3. *The lagrange multipliers can be used to obtain the solution of function* $f(\pi_1, \pi_2, ...\pi_l)$

Proof. According to [34], a multi-variate function $f(\pi_1, \pi_2, ...\pi_l)$ is set and $g(\pi_1, \pi_2, ...\pi_l) = \Omega$ is introduced. And f and g are both function that have continuous first partial derivatives and $\Omega = 1$ in this section. Next, one new variable ϖ is introduced and the lagrange function $\Delta(\pi_1, \pi_2, ...\pi_l, \varpi)$ is set as

$$\Delta(\pi_1, \pi_2, ...\pi_l, \varpi) = f(\pi_1, \pi_2, ...\pi_l) + \varpi[g(\pi_1, \pi_2, ...\pi_l) - \Omega]$$

We need the partial derivative of function $\Delta(\pi_1, \pi_2, ...\pi_l, \varpi)$ about all variables to obtain the solution $\Delta(\pi_1, \pi_2, ...\pi_l, \varpi)$. In the above, given ϑ'_A, we can obtain $f(\pi_1, \pi_2, ...\pi_l) = J_S(\vartheta'^{\text{mixed}}_S)$ and $g(\pi_1, \pi_2, ...\pi_l) = \sum_{l=1}^{U} \pi_l = 1$. Given ϑ'_S, it will have the following

$$\Delta(\mu_1, \mu_2, ...\mu_u, \varpi') = f(\mu_1, \mu_2, ...\mu_l) + \varpi'[g(\mu_1, \mu_2, ...\mu_u) - \Omega]$$

where $f(\mu_1, \mu_2, ...\mu_l) = J_A(\vartheta'^{\text{mixed}}_A)$ and $g(\mu_1, \mu_2, ...\mu_u) = \sum_{l=1}^{U} \pi_l = 1$ □

Theorem 3. *Consider the interactive decision making in the multiple subsystems subject to the malicious attack. The optimal strategies for the sensors and the attacker achieve the NE of the player's game.*

Proof. Define the optimal mixed strategies for the sensors and the attacker as $\vartheta'^*_S = (\pi^*_1, \pi^*_2, \ldots, \pi^*_U)$ and $\vartheta'^*_A = (\mu^*_1, \mu^*_2, \ldots, \mu^*_L)$, respectively. Then

$$\begin{aligned} J_A(\vartheta'^*_S, \vartheta'_A) &\leq J_A(\vartheta'^*_S, \vartheta'^*_A) \\ J_S(\vartheta'_S, \vartheta'^*_A) &\leq J_S(\vartheta'^*_S, \vartheta'^*_A) \end{aligned}$$

Next, the NE solution of the game will be given. Define $J_S(\vartheta'^{\text{pure}}_S(u)) \triangleq G_u$ for each $\vartheta'^{\text{pure}}_S(u)$. The objective function $J_S(\vartheta'^{\text{mixed}}_S)$ of the $\vartheta'^{\text{mixed}}_S$ is written as follows:

$$J_S(\vartheta'^{\text{mixed}}_S) = \sum_{u=1}^{U} \pi_u G_u, \qquad \sum_{u=1}^{U} \pi_u = 1 \tag{33}$$

where $J_S(\vartheta'^{\text{pure}}_S(u)) = \sum_{u=1}^{r} J_{u,S}(\vartheta'^{\text{pure}}_S(u))$. Assuming that ϑ'^*_A is given, the equilibrium strategy of the sensors $\vartheta^*_S = (\pi^*_1, \pi^*_2, \ldots, \pi^*_U)$ is the one that maximizes $J_S(\vartheta'^{\text{mixed}}_S)$ under the constraint $\sum_{u=1}^{U} \pi^*_u = 1$ by the definition of the NE. Thus ϑ'^*_S can be calculated easily using the Lagrange multipliers method. Then, for the attacker, there is a similar process to find the optimal solution $\vartheta'^*_A = (\mu^*_1, \mu^*_2, \ldots, \mu^*_L)$. Finally, we are able to combine the two solutions to obtain the NE of the two player's game. □

V. Numerical Examples

A. Example 1: Single System

In this section, we use a scalar system to illustrate the effectiveness of the results for single linear time-invariant system under attack. The system parameters are set as $A = 0.5$, $C = 1$, $Q = 0.05$, $R = 0.001$. The sensor and the attacker are assumed to be limited to only one chance to send date or launch attack, that is $T = 2, M = 1, N = 1$. Then there exist two kinds of attack strategies a_1 and a_2 to be chosen by the attacker. For the sensor, d_1 and d_2 are its defensive strategies. Pay-off matrices are given as follows

$\mathbf{F}_\theta :=$

	a_1	a_2
d_1	0.39	0.18
d_2	0.12	0.48

, $\mathbf{F_J} :=$

	a_1	a_2
d_1	0.0195	0.0090
d_2	0.0060	0.0240

According to Theorem 1, the optimal mixed strategy for the sensor is calculated as follows

$$\Phi^*_S = \begin{bmatrix} 0.5263 & 0.4737 \end{bmatrix}^T$$

and the optimal mixed strategy for the attacker is

$$\Phi_A^* = \left[\begin{array}{cc} 0.6316 & 0.3684 \end{array} \right]^T$$

Therefore, the packet loss rate $\theta^* = \Phi_S^{*T} \mathbf{F}_\theta \Phi_A^* = 0.2842$ is gotten. Simulation results are shown in the following.

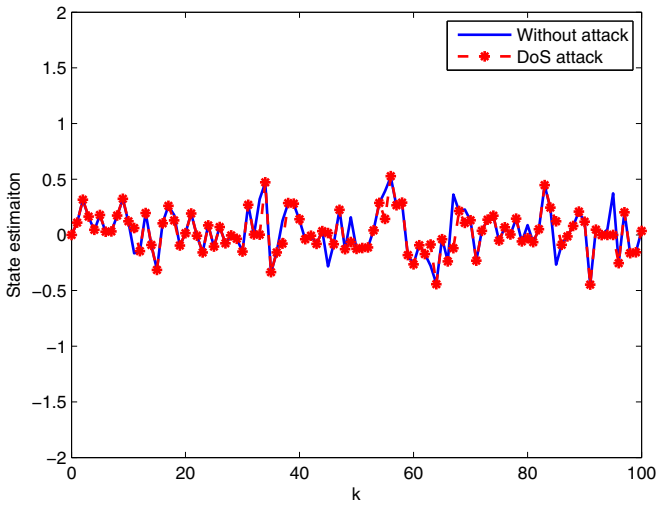


Fig. 3. State estimation with and without attack

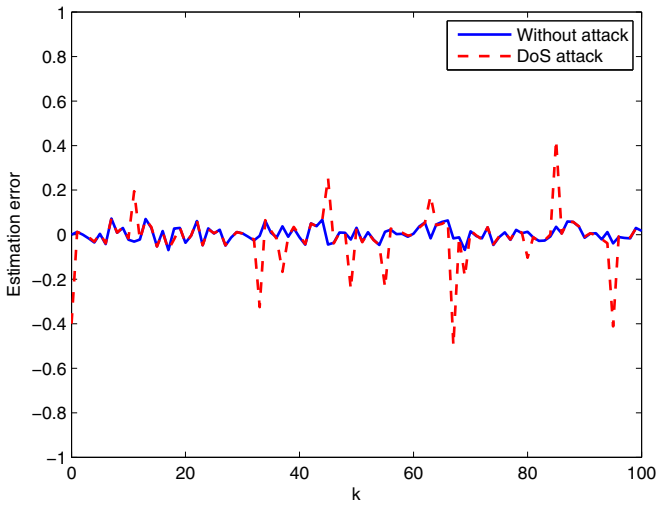


Fig. 4. Estimation error with and without attack

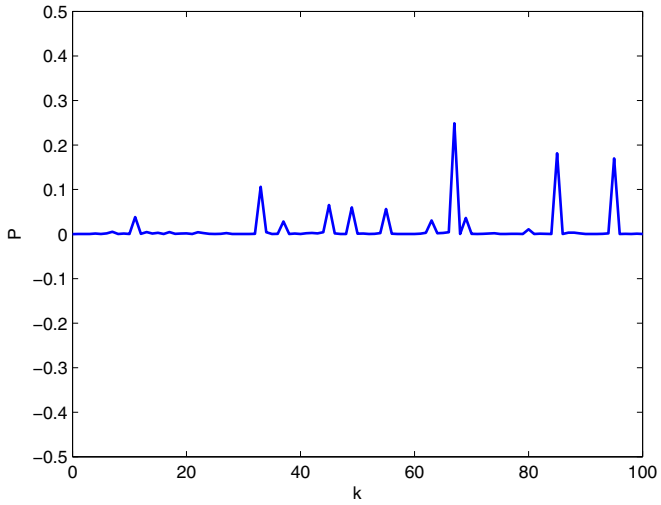


Fig. 5. The estimation error covariance

From Fig. 3-Fig. 5, it can be seen that the system is still stable under this attack. And the state estimation is basically consistent under attacker and without attacker. The estimate error covariance fluctuates around the steady state value $\bar{P}$. (The value of $\bar{P}$ will not affect the convergence of the filter. So it is assumed to be zero in this example.)

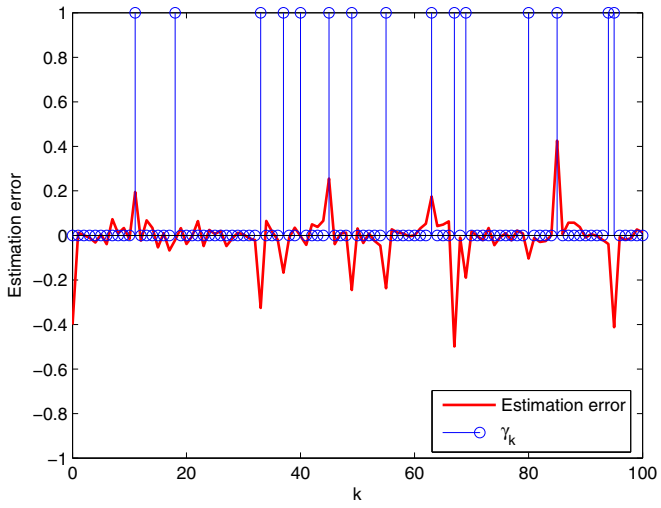


Fig. 6. Estimation error VS dynamic attack

In Fig. 6, the estimation error and the packet loss sequence based on the NE solution is illustrated, where γ_k=1 represents packet loss, and 0 represents no packet loss. It can be seen that the estimation error fluctuates greatly when the data packet loss occurs. From the above analysis, it is concluded that the transmission strategy for the sensor provides a more accurate state estimation.

B. Example 2: Multiple-subsystem

An example with two subsystems is given to illustrate the security estimation for CPS with multiple-subsystem under DoS attack. The system parameters are set as: $T = 2, M_1 = 1, M_2 = 1, N = 1$ and $A_1 = 0.6, A_2 = 0.8, C_1 = 1, C_2 = 1.1, Q_1 = 0.05, Q_2 = 0.02, R_1 = 0.001, R_2 = 0.004$. The pure strategies

for the attacker are

$$\vartheta_A'^{\text{pure}}(1)=\left\{\begin{array}{cc}1&0\\0&0\end{array}\right\},\vartheta_A'^{\text{pure}}(2)=\left\{\begin{array}{cc}0&0\\1&0\end{array}\right\},\vartheta_A'^{\text{pure}}(3)=\left\{\begin{array}{cc}0&1\\0&0\end{array}\right\},\vartheta_A'^{\text{pure}}(4)=\left\{\begin{array}{cc}0&0\\0&1\end{array}\right\}.$$

The pure strategies for the sensor are Similar, for the sensors, we can also obtain as following:

$$\vartheta_S'^{\text{pure}}(1)=\left\{\begin{array}{cc}1&0\\1&0\end{array}\right\},\vartheta_S'^{\text{pure}}(2)=\left\{\begin{array}{cc}0&1\\1&0\end{array}\right\},\vartheta_S'^{\text{pure}}(3)=\left\{\begin{array}{cc}0&1\\0&1\end{array}\right\},\vartheta_S'^{\text{pure}}(4)=\left\{\begin{array}{cc}1&0\\0&1\end{array}\right\}.$$

According to Theorem 3, the Nash equilibrium solution is obtained as $\vartheta_S^*=(0.1901,0.3386,0.2553,0.2160)$ and $\vartheta_A^*=(0.0620,0.2787,0.3813,0.2780)$.

VI. Conclusion

In this paper, the problem of remote state estimation under DoS attack has been studied. Firstly, a system where one sensor communicated with a remote estimator through a wireless channel was considered. The DoS attacker can jam the transmission channel with limited actions in any time. A novel game framework was proposed and the optimal strategies for both sides have been obtained by using matrix game. Further, we extended it to the scenario with multiple-subsystem. An integrated game-theoretic framework was developed to investigate the interactive decision-making process between the sensors and the attacker. Moreover, existence conditions of NE strategies were presented. Simulation examples demonstrate the effectiveness of the provided techniques.

VII. Acknowledgment

The authors would like to thank the anonymous reviewers for their detailed comments that helped to improve the quality of the paper. The work was supported by the National Natural Science Foundation of China (61773334, 61403330, 61773063 and 61573301), the Natural Science Fund of Hebei Provincial (F2015203163), and the Science Fund for Distinguished Young Scholars of Hebei Province (F2016203148).

References

[1] D. Ding, Q. Han, Y. Xiang, X. Ge, X. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, DOI: 10.1016/j.neucom.2017.10.009, 2017.

[2] H. Fawzi, P. Tabuada, S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454-1467, 2014.

[3] Zhang Y, Qiu M, Tsai C W, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88-95, 2017.

[4] Y. Mo, B. Sinopoli, "Integrity attacks on cyber-physical systems," *Proceedings of the 1st International Conference on High Confidence Networked Systems*, pp. 47-54, 2012.

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

[6] L. Hu, Z. Wang, Q. Han, X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176-183, 2018.

[7] D. Ding, Z. Wang, D. Ho, G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231-240, 2017.

[8] Z. Guo, D. Shi, K. Johansson, L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 4-13, 2017.

[9] Y. Li, L. Shi, T. Chen, "Detection against linear deception attacks on multi-sensor remote state estimation," *Proceedings of the IEEE Transactions on Control of Network Systems*, DOI: 10.1109/TCNS.2017.2648508, 2017.

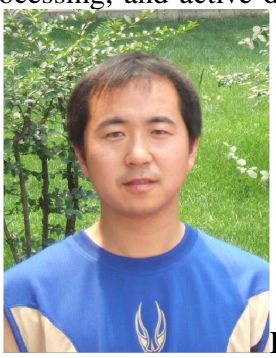
[10] D. Ding, G. Wei, S. Zhang, "On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors," *Neurocomputing*, vol. 219, pp. 99-106, 2017.
[11] H. Yuan and Y. Xia, "Secure filtering for stochastic nonlinear systems under multiple missing measurements and deception attacks," *IET Control Theory and Applications*, DOI: 10.1049/iet-cta.2017.0868, 2017.
[12] H. Zhang, L. Shi, P. Cheng, J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023-3028, 2015.
[13] T. Alpcan, T. Basar, "Network security: A decision and game-theoretic approach," *Automatica*, vol. 78, pp. 194-201, 2010.
[14] T. Basar, G. Olsder, "Dynamic noncooperative game theory," *Siam*, vol. 19, no. 2, pp. 139-152, 1982.
[15] S. Bhattacharya, T. Basar, "Game-theoretic analysis of an aerial jamming attack on a UAV communication network," *Proceedings of the IEEE American Control Conference*, pp. 818-823, 2010.
[16] S. Liu, X. Liu, A. Saddik, "A stochastic security game for Kalman filtering in networked control systems (NCSs) under denial of service (DoS) attacks," *IFAC Proceedings Volumes*, vol. 46, no. 20, pp. 106-111, 2013.
[17] Y. Li, L. Shi, P. Cheng, J. Chen, D. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831-2836, 2015.
[18] K. Ding, Y. Li, D. Quevedob, S. Dey, L. Shi, "A multi-channel transmission schedule for remote state estimation under DoS attacks," *Automatica*, vol. 78, pp. 194-201, 2017.
[19] K. Ding, D. Quevedo, S. Dey, "A secure cross-layer design for remote estimation under DoS attack: When multi-sensor meets multi-channel," *Proceedings of the Decision and Control*, pp. 6297-6302, 2016.
[20] K. Ding, X. Ren, L. Shi, "Deception-based sensor scheduling for remote estimation under DoS attacks," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 169-174, 2016.
[21] H. Li, L. Lai, R. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," *Proceedings of the Conference on Information Sciences and Systems*, pp. 1-6, 2011.
[22] X. Ren, J. Wu, S. Dey, L. Shi, "Attack allocation on remote state estimation in multi-systems: Structural results and asymptotic solution," *Automatica*, vol. 87, pp. 184-194, 2018.
[23] Y. Song, J. Hu, D. Chen, Y. Liu, F. Alsaadi, G. Sun, "A resilience approach to state estimation for discrete neural networks subject to multiple missing measurements and mixed time-delays," *Neurocomputing*, vol. 272, pp. 74-83, 2018.
[24] A. Cervin, T. Henningsson, "Scheduling of event-triggered controllers on a shared network," *Proceedings of the IEEE Conference on Decision and Control*, pp. 3601-3606, 2008.
[25] G. Gu, X. Cao, H. Badr, "Generalized LQR control and kalman filtering with relations to computations of inner-outer and spectral factorizations," *IEEE Transactions on Automatic Control*, vol. 51, no. 4, pp. 595-605, 2006.
[26] H. Zhang, P. Cheng, L. Shi, J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843-852, 2016.
[27] Y. Li, F. Zhang, D. Quevedo, V. Lau, S. Dey, and L. Shi, "Power control of an energy harvesting sensor for remote state estimation," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 277-290, 2017.
[28] L. Wang, Z. Wang, Q. Han, G. Wei, "Synchronization control for a class of discrete-time dynamical networks with packet dropouts: A coding-decoding-based approach," *IEEE Transactions on Cybernetics*, DOI: 10.1109/TCYB.2017.2740309, 2017.
[29] L. Wang, Z. Wang, Q. Han, G. Wei, "Event-based variance-constrained H_∞ filtering for stochastic parameter systems over sensor networks with successive missing measurements," *IEEE Transactions on Cybernetics*, DOI: 10.1109/TCYB.2017.2671032, 2017.
[30] L. Shi, P. Cheng, J. Chen, "Sensor data scheduling for optimal state estimation with communication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693-1698, 2011.

[31] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, no. 2, pp. 286-295, 1951.
[32] Y. Yuan, F. Sun, "Data fusion-based resilient control system under DoS attacks: A game theoretic approach," *International Journal of Control Automation Systems*, vol. 13, no. 3, pp. 513-520, 2015.
[33] S. Amin, G. Schwartz, S. Sastry, "On the interdependence of reliability and security in networked control systems," *Proceedings of the Conference on Decision and Control and European Control*, pp. 4078-4083, 2011.
[34] M. Hazewinkel, "Encyclopaedia of Mathematics: Supplement," *Springer*, 2002.

Li Li received the B.S.degree in Mathematics and Applied Mathematics from the Hebei Normal University, Shijiazhuang, China, in 2006,the M.S.degree in Applied Mathematics from Hebei University of Science and Technology, Shijiazhuang, China, in 2009 and the Ph.D.degree in Control Science and Engineering in Beijing Institute of Technology, Beijing, China, in 2013. She is currently an Associate Professor with the Department of Automation, Institute of Electrical Engineering, Yanshan University, Qinhuangdao, China. Her current research interests are in the fields of networked control systems, cyber-physical system security, and nonlinear filtering.

Huixia Zhang received the B.S. degree in measurement and control technology and instrumentation from Hebei University of Science and Technology, Shijiazhuang, China, in 2015. She is currently pursuing the M.S. degree in control theory and control engineering in Yanshan University. Her current research interests include cyber-physical system security and networked state estimation.

Yuanqing Xia (M15SM16) was born in Anhui, China, in 1971. He received the M.S. degree in fundamental mathematics from Anhui University, Hefei, China, in 1998, and the Ph.D. degree in control theory and control engineering from the Beijing University of Aeronautics and Astronautics, Beijing, China, in 2001.From 2002 to 2003, he was a Post-Doctoral Research Associate with the Institute of Systems Science, Academy of Mathematics and System Sciences, Chinese Academy of Sciences, Beijing. From 2003 to 2004, he was with the National University of Singapore, Singapore, as a Research Fellow, where he researched on variable structure control. From 2004 to 2006, he was with the University of Glamorgan,Pontypridd, U.K., as a Research Fellow. From 2007 to 2008, he was a Guest Professor with Innsbruck Medical University, Innsbruck, Austria. Since 2004, he has been with the School of Automation, Beijing Institute of Technology, Beijing, first as an Associate Professor, then, since 2008, as a Professor. His current research interests include networked control systems, robust control and signal processing, and active disturbance rejection control.



Hongjiu Yang received the B.S. degree in mathematics and applied mathematics and the M.S. degree in applied mathematics from the Hebei University of Science and Technology, Shijiazhuang, China, in 2005 and 2008, respectively, and the Ph.D. degree in control science and engineering from the Beijing Institute of Technology, Beijing, China. He is currently an Associate Professor with the Department of Automation, Institute of Electrical Engineering, Yanshan University, Qinhuangdao, China. His current research interests include robust control/filter theory, delta operator systems, networked control systems, and active disturbance rejection control.