2016 IEEE 55th Conference on Decision and Control (CDC)
ARIA Resort & Casino
December 12-14, 2016, Las Vegas, USA

A Secure Cross-Layer Design for Remote Estimation under DoS Attack : When Multi-sensor meets Multi-channel

Kemi Ding, Daniel E. Quevedo, Subhrakanti Dey and Ling Shi

Abstract— **This paper considers security issues of a cyber-physical system (CPS) under denial-of-service (DoS) attacks. The measurements of multiple sensors are transmitted to a remote estimator over a multi-channel network, which may be congested by an intelligent attacker. Aiming at improving the estimation accuracy, we first propose a novel aggregation scheme for the estimator to produce accurate state estimates, from which we obtain a closed-form expression of the expected estimation error covariance. We further develop a sensor-attacker game to design the cooperative and defensive channel-selection strategy, which avoids the sensors being attacked in an energy-efficient way. Numerical examples are provided to illustrate the developed results.**

I. Introduction

As the next generation of engineering systems, cyber-physical systems (CPSs), which synthesize physical processes, communication networks and control systems (i.e., 3C), have aroused wide attentions from different areas [1], such as aerospace engineering, smart grid, transportation system and ubiquitous health care systems, etc. The 3C structure provides CPSs with prominent stability, robustness and efficiency. However, the tight integration of 3C brings additional security issues to the design of CPSs. The vulnerability of computational and communication components exposes the control systems to many potential threats, like operation abnormality and system destruction. These may be conducted by malicious adversaries with economic or terrorism-based motivations. Two typical classes of attack on CPSs discussed in the work of Cardenas *et al.* [2] are deception (integrity) attacks and denial-of-service (DoS) attacks. The former modifies the data packets in a malicious way, while DoS attacks block the information flow between the sender (sensor) and the receiver to increase the packet-drop rate. The latter is common and ease of implementation in practical systems. For example, cyber attackers blocked the information flow from the physical plant in the recent incident on Ukrainian power grid [3], in which the power supply to hundreds of thousands of homes in Ukraine was brought down. In the present work, we mainly deal with a defence-strategy design to assure safe operations of CPSs in the presence of DoS attacks.

The work by K. Ding and L. Shi is supported by a HK RGC theme-based project T23-701/14N.

K. Ding and L. Shi are with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. {kdingaa, eesling}@ust.hk

D. Quevedo is with the Department of Electrical Engineering, Paderborn University,Germany. dquevedo@ieee.org

S. Dey is with the Department of Engineering Science, Uppsala University, Sweden. subhrakanti.dey@angstrom.uu.se

Several recent studies investigating CPS security under DoS attacks have been carried out in [4]–[7]. The latest work by Senejohnny *et al.* studied a modified consensus protocol to avoid DoS attacks. The survey conducted by Zhang *et al.* [4] has investigated the energy-constrained attack policy taken by a DoS attacker to degrade the system performance. These works about designing optimal strategies only focus on one side, i.e., the sensors or the attacker. To capture the strategic iterations between a sensor and an intelligent attacker, Liu *et al.* [5] applied a game-theoretic approach. Under energy constraints, Li *et al.* [7] analyzed an interactive decision-making process between a sensor and a remote estimator and obtained the equilibrium solution via an updating algorithm.

Unfortunately, these existing DoS-defence strategies cannot fully handle the new challenges brought by the large-scale wireless sensor networks (WSNs) in CPSs. In practice, CPSs accomplish diverse applications (e.g., timely environmental monitoring) by utilizing an enormous number of sensors with high-rate data collection ability, which may measure the same/different physical processes (e.g., temperature/humidity fluctuation). Moreover, to alleviate bursty communication traffic in this competitive environment (i.e., numerous sensors with high data transmission rate), CPSs utilize the multi-channel technology and it is supported by some MAC protocols, WSN hardware and commercially available communication radios [8]. Motivated by this, we consider a novel multi-channel multi-sensor system in our CPS-security study. Specifically, for the multi-sensor issue (when sensors measure the states of the same physical process), to avoid heavy computational overhead, we adopt the information fusion method to process the aggregated data. Sun and Deng [9] described an optimal information fusion criterion weighted by matrices for Kalman filter. Lack of considering the unreliability of the remote transmission, this criterion may not apply to the worst-case when the fusion center receives nothing. To overcome it, this work presents a linear combination method, in the minimum-error-variance sense, to aggregate the available information (involving the received data and the prediction information based on previous estimate). Meanwhile, the sensors, provided with the multi-channel networks, will utilize the public resource in general cases, and this competition situation will be broken if there is a malicious attacker. Compared with previous works, the main contributions of our current work are summarized as follows:

- Online information: to improve the estimation accuracy,

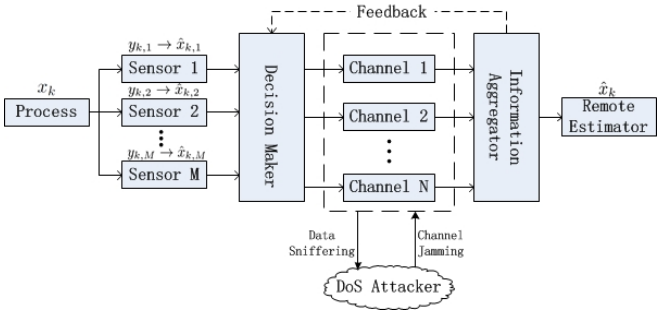

Fig. 1: System Model

we propose an optimal linear combination among the received information and previous estimates. We also prove the existence of a fix point, which enables us to obtain a closed form of the expected state estimation error covariance.

- Cooperative strategy: to model the interactive decision-making process among the multiple agents, we first group the sensors together due to their same purpose and introduce a sensor-attacker game for the cooperative strategy design.
- Cross-Layer design: the proposed aggregation scheme for the remote estimator guides the design of the defensive channel-selection strategies for the sensors, which links the sensor layer with the estimator layer. Furthermore, an extension model with $N > 2$ channels and $M > 2$ sensors can be easily obtained via this framework.

The remainder of the paper is organized as follows. Section II contains the mathematical models of the multi-sensor multi-channel system. Section III demonstrates the dynamic parameter design for the proposed data aggregation scheme. Section IV introduces the cooperative channel-selection scheme for sensors via a game-theoretical approach. Some examples and concluding remarks are presented in Section V and Section VI, respectively.

Notations: $\mathbb{N}$ is the set of positive integers. $\mathbb{R}^n$ is the n dimensional Euclidean space. We write $X \geq 0$ (or $X > 0$) when X is positive semi-definite (or positive definite). $\mathbb{T}r(\cdot)$ denotes the trace of a matrix. For functions h, g, $h \circ g$ is defined as the function composition $h(g(\cdot))$. $\mathbb{E}[\cdot]$ is the expectation of a random variable and $\Pr(\cdot)$ refers to the probability. The notation $\vec{\cdot}$ is the representation of vectors. $y_{0,i}^k$ stands for the sequence $\{y_{0,i}, y_{1,i}, \ldots, y_{k,i}\}$.

II. System Model

A general multi-sensor multi-channel system is shown in Fig. 1.As a baseline, we start by a simple model with two sensors and two channels, and introduce the mathematical models for each components in this section.

A. Local Kalman Filtering

We consider the following process model:

$$x_{k+1} = Ax_k + w_k,\ \ y_{k,i} = C_i x_k + v_{k,i}, i = 1, 2, \qquad (1)$$

where $x_k \in \mathbb{R}^{n_x}$ and $y_{k,i} \in \mathbb{R}^{m_{y,i}}$ denote the process state vector and the i-th sensor's observation vector, respectively. The process noise $w_k \in \mathbb{R}^{n_x}$ and the observation noise $v_{k,i} \in \mathbb{R}^{m_{y,i}}$ are independent zero-mean Gaussian random vectors with

$$\mathbb{E}[\Delta_k \Delta_j'] = \begin{pmatrix} \delta_{kj} Q & 0 & 0 \\ 0 & \delta_{kj} R_1 & \delta_{kj} R_0 \\ 0 & \delta_{kj} R_0' & \delta_{kj} R_2 \end{pmatrix},\ \forall j, k \in \mathbb{Z} \quad (2)$$

in which $\Delta_k = [w_k\ v_{k,1}\ v_{k,2}]'$, $Q \geq 0$ and $R_i > 0,\ i = \{1, 2\}$. Assume that the initial state x_0 is a zero-mean Gaussian random vector with covariance $\Pi_0 \geq 0$ and is uncorrelated with the noises w_k and $v_{k,i},\ \forall i \in 1, 2$. In addition, the pair (A, C_i) is assumed to be detectable for all i and $(A, \sqrt{Q})$ is stabilizable.

To improve the estimation/control performance of the system, CPSs adopt the "smart sensors" [10]. Precisely, the sensors in Fig. 1, after taking measurements at time step k, run local Kalman filters to estimate the state x_k based on the overall collected measurements.The obtained minimum mean-squared error (MMSE) estimate of x_k for the $i-$th sensor is denoted by $\hat{x}_{k,i} = \mathbb{E}[x_k | y_{0,i}^k]$. Correspondingly, the estimation error for the i-th sensor denoted by $\varepsilon_{k,i}$ and the error covariance matrix $P_{k,i}$ are defined as

$$\varepsilon_{k,i} \triangleq x_k - \hat{x}_{k,i},\ P_{k,i} \triangleq \mathbb{E}[(\varepsilon_{k,i})(\varepsilon_{k,i})' | y_{0,i}^k]\ i = 1, 2. \quad (3)$$

By employing a local Kalman filter, these terms are computed as

$$\begin{aligned} \tilde{x}_{k,i} &= A\hat{x}_{k-1,i},\ \tilde{P}_{k,i} = AP_{k-1,i}A' + Q, \\ K_{k,i} &= \tilde{P}_{k,i} C_i' [C_i \tilde{P}_{k,i} C_i' + R_i]^{-1}, \\ \hat{x}_{k,i} &= A\hat{x}_{k-1,i} + K_{k,i}(y_{k,i} - C_i A\hat{x}_{k-1,i}), \\ P_{k,i} &= (I - K_{k,i} C_i)\tilde{P}_{k,i}, \end{aligned}$$

in which the recursion starts from $\hat{x}_0 = 0$ and $P_0 = \Pi_0$.

For convenience, we define the Lyapunov and Riccati operators h and $\tilde{g}_i : \mathbb{S}_+^n \to \mathbb{S}_+^n$ for each sensor as

$$h(X) \triangleq AXA' + Q,$$
$$\tilde{g}_i(X) \triangleq X - XC_i'[C_i X C_i' + R_i]^{-1} C_i X.$$

Due to the detectability assumption on (A, C_i), the error covariance matrix $P_{k,i}$ for each sensor will converge exponentially to a unique fixed point $\overline{P}_i$ of $h \circ \tilde{g}_i$ [11]. For simplicity, we assume that the initial state of the Kalman filter at each sensor has entered steady state, i.e., $P_{k,i} = \overline{P}_i,\ k \geq 0,\ i = 1, 2$.

B. Communication Model

As a data packet, the obtained local estimate $\hat{x}_{k,i}$ for each sensor are transmitted to the remote estimator (see Fig. 1) through two channels, which are assumed to have independent Additive White Gaussian Noise (AWGN). Each sensor is required to decide through which channel to send data, and evidently a channel-scheduling problem arises with the consideration of improving the remote estimation accuracy.

Transmitted through the unreliable communication channel, the data packets will contain uncertain errors when arriving at the receiver as a consequence of channel noise, multi-path fading and so on. The packets containing transmission

errors will be detected by the cyclic redundancy check (CRC) and abandoned before uploading to the data aggregator. In this point-to-point communication, we measure the packet arrival reliability by the packet-error-rate (PER) and for any modulation scheme, it is closely related to the signal-to-noise-ratio (SNR). In this multi-sensor system, if the sensors select the same channel for transmission, the two transmitted packets may interfere with each other. Additionally, the malicious attacker will obstruct the communication channel by launching DoS attacks, which also perturbs the packet transmission in the selected channel. Under this case, the SNR is replaced by SINR (signal-to-interference-plus-noise-ratio) [12]. Assume that the channel selection for the three agents (the two sensors and the attacker) are denoted by (l, j, s), then

$$SINR_i(l,j,s) = \begin{cases} \frac{e_{l,1}}{\tau\delta_{lj}e_{j,2}+\delta_{ls}n_s+\sigma_l}, & i=1, \\ \frac{e_{j,2}}{\tau\delta_{lj}e_{l,1}+\delta_{js}n_s+\sigma_j}, & i=2, \end{cases} \tag{4}$$

in which $l, j, s \in \{1, 2\}$, and $e_{l,i}$ represents the transmission power on the l-th channel for the i-th sensor. The coefficient τ indicates the degree of the simultaneous-transmission interference between the transmitted packets $\hat{x}_{k,1}$ and $\hat{x}_{k,2}$. The interference power used by the attacker to jam the s-th channel is denoted by n_s. Moreover, σ_l is the additive white noise power for the l-th channel. We describe the packet-arrival-rate for the l-channel, which depends on channel characteristics, in a general form, i.e., $f_l(SINR_i(l, j, s))$. It is an increasing function on $SINR$ since low $SINR$ leads to an undesirably poor communication performance. We characterize the arrival of packets by two independent binary random processes, denoted by $\gamma_{k,1}$ and $\gamma_{k,2}$. $\gamma_{k,1} = 0$ represents the occurrence of packet ($\hat{x}_{k,1}$) loss. We assume that the arrivals of the two packets are independent even if they are transmitted in the same channel, e.g., $\mathbb{P}r(\gamma_{k,1} = 1, \gamma_{k,2} = 1) = \mathbb{P}r(\gamma_{k,1} = 1)\mathbb{P}r(\gamma_{k,2} = 1)$. This scenario is reasonable, for example, simultaneous transmission in frequency-nonselective channels. If the packet-arrivals are related, we can still use a formula on SINR to express the probability $\mathbb{P}r(\gamma_{k,1} = 1, \gamma_{k,2} = 1)$ and other cases.

C. Remote Estimation

We denote $\hat{x}_k$ as the estimate generated by the remote estimator. After receiving the data packets, the remote estimation of the state x_k is described as follows: once receiving $\hat{x}_{k,1}$ and/or $\hat{x}_{k,2}$ correctly (i.e., $\gamma_{k,1} = 1$ or $\gamma_{k,2} = 1$), the remote estimator synchronizes its estimate $\hat{x}_k$ with them based on a linear combination; otherwise, simply predicts the estimate with its previous estimate $\hat{x}_{k-1}$ by using the system model (1). Then, we write $\hat{x}_k$ in the following simple equation:

$$\hat{x}_k = \alpha_{k,1}\gamma_{k,1}\hat{x}_{k,1} + \alpha_{k,2}\gamma_{k,2}\hat{x}_{k,2} + \alpha_{k,3}\gamma_{k,3}A\hat{x}_{k-1}, \tag{5}$$

in which $\gamma_{k,3} = \gamma_{k,1} \oplus \gamma_{k,2} \triangleq (\gamma_{k,1} + \gamma_{k,2})\ mod\ 2$, i.e., a binary addition[1]. Note that when the two packets are received successfully, the predict item $A\hat{x}_{k-1}$ contains no more effective information and its weight $\gamma_{k,3}$ equals to zero.

Under this scheme (5), the estimate $\hat{x}_k$ are required to be unbiased if the packet-arrival statuses $\gamma_{k,1}$ and $\gamma_{k,2}$ are known. That is, $\mathbb{E}[\hat{x}_k|\gamma_{k,1}, \gamma_{k,2}] = \mathbb{E}[x_k],\ \forall k \geq 1$. Hence, we have the following constraint for the parameters,

$$\alpha_{k,1}\gamma_{k,1} + \alpha_{k,2}\gamma_{k,2} + \alpha_{k,3}\gamma_{k,3} = 1, \tag{6}$$

which can be easily obtained from the mathematical induction and the following derivation:

$$\begin{aligned} &\mathbb{E}[\hat{x}_k|\gamma_{k,1}, \gamma_{k,2}] \\ =&\alpha_{k,1}\gamma_{k,1}\mathbb{E}[\hat{x}_{k,1}] + \alpha_{k,2}\gamma_{k,2}\mathbb{E}[\hat{x}_{k,2}] + \alpha_{k,3}\gamma_{k,3}A\mathbb{E}[\hat{x}_{k-1}] \\ \overset{(a)}{=}&(\alpha_{k,1}\gamma_{k,1} + \alpha_{k,2}\gamma_{k,2} + \alpha_{k,3}\gamma_{k,3})\mathbb{E}[x_k] \\ =&\mathbb{E}[x_k], \end{aligned} \tag{7}$$

The derivation of (a) relies on the fact that $\mathbb{E}[\mathbb{E}[X|Y]] = \mathbb{E}[X]$ and $\mathbb{E}[x_k] = A\mathbb{E}[x_{k-1}]$. Apparently, the parameters are required to be bounded; however, it is unnecessary to require the parameters to be positive, which will be analyzed later.

Similar to (3), the estimation error ε_k and the error covariance matrix P_k for the remote estimator are introduced to describe the estimation performance.

$$\varepsilon_k \triangleq x_k - \hat{x}_k,,\ P_k \triangleq \mathbb{E}[(\varepsilon_k)(\varepsilon_k)'|\mathcal{I}_0^k], \tag{8}$$

in which $\mathcal{I}_k \triangleq \{\gamma_{k,1}\hat{x}_{k,1}\gamma_{k,2}\hat{x}_{k,2}\}$ represents the received information at time k.

D. Problem of Interest

We study the following two questions:

1) how to obtain an optimal aggregation and compute the remote estimation error covariances;
2) how to design secure channel-selection strategies for the multi-sensor in the existence of DoS attacks.

III. Estimation Accuracy for Data Fusion

In this section, we introduce the parameter design for the aggregation scheme and provide a closed-form recursion for the error covariance P_k with the optimal parameters.

A. Preliminaries

Before designing the optimal parameters, we study some properties of the information available to the remote estimator. First, we introduce the incremental innovation in the local state estimate of the i-th sensor $\hat{x}_{k,i}$, denoted by $z_{k,i} = \hat{x}_{k,i} - A\hat{x}_{k-1,i}$.

From [13], some properties about the estimation error $\varepsilon_{k,i}$ as defined in (3) are summarized in the following lemma.

Lemma 3.1: The following statements about $\varepsilon_{k,i}, i = 1, 2$ hold:

1) $\varepsilon_{k,i}$ is zero-mean Gaussian and is independent of the innovation $z_{k,i}$;
2) $\varepsilon_{k,i}$ is independent of w_l and $v_{j,i}$ for any $l, j \in \mathbb{Z}$ and $l \geq k, j \geq k+1$;

The prove is simple and we omit the details here. For different sensors, their estimation errors are cross-correlated and the relationship is summarized in the following theorem.

[1]Since this modular in the operation can be any positive number, the aggregation scheme can be extended to include $M > 2$ estimates sent by M sensors.

Theorem 3.2: For the two Gaussian processes $\varepsilon_{k,1}$ and $\varepsilon_{k,2}$, their cross-covariance at time k, denoted by $\Gamma_k = \mathbb{E}[\varepsilon_{k,1}\varepsilon'_{k,2}]$, follows the iteration:

$$\begin{aligned} \Gamma_k &= \mathrm{T}(\Gamma_{k-1}) : \mathbb{R}^{n_x \times n_x} \longrightarrow \mathbb{R}^{n_x \times n_x} \\ \mathrm{T}(\Gamma_k) &\triangleq (I - K_1C_1)h(\Gamma_k)(I - K_2C_2)' + K_1R_0K_2', \end{aligned} \tag{9}$$

in which $R_0 = \mathbb{E}[v_{k,1}v'_{k,2}]$. The cross-covariance matrix Γ_k converges exponentially to a unique fixed point $\overline{\Gamma}$ of the mapping T.

Proof: The iteration (9) is obvious. We focus on the proof of the fixed point of the cross-covariance matrix. For any $X, Y \in \mathbb{R}^{n_x \times n_x}$, we have

$$\begin{aligned} &\| \mathrm{T}(X) - \mathrm{T}(Y) \|^2 \\ &= \mathbb{T}r[(X-Y)'A_1'A_1(X-Y)A_2'A_2] \\ &\overset{(a)}{\leq} \mathbb{T}r[(X-Y)'(X-Y)]\mathbb{T}r[A_1'A_1] \parallel A_2 \parallel^2 \\ &\overset{(b)}{\leq} \rho^2 \parallel X - Y \parallel^2, \end{aligned} \tag{10}$$

where $\| \cdot \|$ represents the Frobenius norm and $A_i = (I - K_iC_i)A, i = 1, 2$. The inequality (a) is derived from the fact that $\mathbb{T}r(AB) \leq \mathbb{T}r(A)\mathbb{T}r(B)$ if A and B are positive semi-definite. Because of the detectability assumption, we have $\| A_i \| \leq \rho < 1$ and then the inequality (b) is obvious. The inequality (10) illustrates that T is a contraction mapping and a unique fixed point point exists for the mapping T according to the Banach fixed point theorem. ■

Furthermore, we can obtain the relationship between the estimation error and the innovation from different sensors.

Lemma 3.3: The zero-mean Gaussian random process $\varepsilon_{k,i}$ and $z_{k,j}$, in which $i, j \in \{1, 2\}$, $i \neq j$, are cross-correlated and their cross co-variance are independent of time k.
It is easy to obtain this lemma and we omite the details here.

B. Parameter Design for Remote Estimation

The information aggregation scheme (5) aims at producing an estimate based on the available information and simultaneously minimizes its mean square error (MSE). Thereupon, with the received information $\mathcal{I}_k = (\gamma_{k,1}\hat{x}_{k,1}, \gamma_{k,2}\hat{x}_{k,2})$ at time k, we look for a triple $\overrightarrow{\alpha_k} \triangleq (\alpha_{k,1}, \alpha_{k,2}, \alpha_{k,3})$ which solves the following optimization problem:

$$\min_{\overrightarrow{\alpha_k}} \ \mathbb{T}r[P_k|\mathcal{I}_k] \quad s.t. \ \gamma_{k,1}\alpha_{k,1} + \gamma_{k,2}\alpha_{k,2} + \gamma_{k,3}\alpha_{k,3} = 1. \tag{11}$$

The optimal parameter design is summerized in the following theorem.

Theorem 3.4: For the linear combination scheme (5), the dynamic optimal parameter triple under different realizations of $\overrightarrow{\gamma_k} \triangleq (\gamma_{k,1}, \gamma_{k,2})$ and the corresponding error covariance are as follows:

$$\overrightarrow{\alpha_k}/\mathbb{T}r[P_k] = \begin{cases} (1 - \alpha^\star_{k,2}, \alpha^\star_{k,2}, 0)/\beta_{k,0} & \text{if } \overrightarrow{\gamma_k} = (1,1), \\ (\alpha^\star_{k,1}, 0, 1 - \alpha^\star_{k,1})/\beta_{k,1} & \text{if } \overrightarrow{\gamma_k} = (1,0), \\ (0, 1 - \alpha^\star_{k,3}, \alpha^\star_{k,3})/\beta_{k,2} & \text{if } \overrightarrow{\gamma_k} = (0,1), \\ (0,0,1)/\mathbb{T}r[h(P_{k-1})] & \text{otherwise.} \end{cases} \tag{12}$$

where $\alpha^\star_{k,1}$, $\alpha^\star_{k,2}$ and $\alpha^\star_{k,3}$ are given in (14), (18) and (20); $P_{k,0}$, $P_{k,1}$ and $P_{k,2}$ are given in (15), (13) and (16).

Proof: We analyze the optimization problem in different cases.

Case 1: If the two packets $\hat{x}_{k,1}$ and $\hat{x}_{k,2}$ are all received successfully, the estimate is $\hat{x}_k = \alpha_{k,1}\hat{x}_{k,1} + \alpha_{k,2}\hat{x}_{k,2}$. Then, we have

$$\begin{aligned} P_k &= \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)'] \\ &\overset{(a)}{=} {\alpha_{k,2}}^2(\overline{P}_1 + \overline{P}_2 - \overline{\Gamma} - \overline{\Gamma}') + \alpha_{k,2}(\overline{\Gamma} + \overline{\Gamma}' - 2\overline{P}_1) + \overline{P}_1, \end{aligned} \tag{13}$$

in which $\overline{\Gamma}$ is the fix point defined in Lemma 3.2.

To solve the minimization problem (11), we substitute the equality constraint $\alpha_{k,2} = 1 - \alpha_{k,1}$ into the objective function (see (a) in (13)), and the symmetric axis of the quadratic objective function is obtained to be

$$\alpha^\star_{k,2} = \frac{\mathbb{T}r[\overline{P}_1 - \overline{\Gamma}]}{\mathbb{T}r[\overline{P}_1 + \overline{P}_2 - 2\overline{\Gamma}]}. \tag{14}$$

Hence, we have the minimum error covariance:

$$\beta_{k,0} \triangleq \mathbb{T}r[P_k|\gamma_{k,1}, \gamma_{k,2} = 1] = \frac{\mathbb{T}r[\overline{P}_1]\mathbb{T}r[\overline{P}_2] - \mathbb{T}r[\overline{\Gamma}]^2}{\mathbb{T}r[\overline{P}_1 + \overline{P}_2 - 2\overline{\Gamma}]} \tag{15}$$

Case 2: If the remote estimator only receives the packet $\hat{x}_{k,1}$ at time k, the linear combination is $\hat{x}_k = \alpha_{k,1}\hat{x}_{k,1} + \alpha_{k,3}A\hat{x}_{k-1}$. Then, we have

$$\begin{aligned} P_k = {\alpha_{k,1}}^2\overline{P}_1 + \alpha_{k,1}\alpha_{k,3}(\mathbb{E}[(x_k - \hat{x}_{k,1})(x_k - A\hat{x}_{k-1})'] \\ + {\alpha_{k,3}}^2\mathbb{T}r[h(P_{k-1})] + \mathbb{E}[(x_k - A\hat{x}_{k-1})(x_k - \hat{x}_{k,1})']) \end{aligned} \tag{16}$$

To obtain the cross covariance between $\varepsilon_{k,1} = x_k - \hat{x}_{k,1}$ and $z_k = x_k - A\hat{x}_{k-1}$, we define $W_k \triangleq \mathbb{E}[\varepsilon_{k,1}z'_k]$ ($W_1 = \overline{P}_1$) which satisfies the following iteration:

$$\begin{aligned} W_k = \tilde{\alpha}_{k-1,1}(A - K_1C_1A)\overline{P}_1A' + \tilde{\alpha}_{k-1,2}(A - K_1C_1A) \\ \cdot \overline{\Gamma}A' + \tilde{\alpha}_{k-1,3}(A - K_1C_1A)W_{k-1}A' + (I - K_1C_1)Q, \end{aligned} \tag{17}$$

in which $\tilde{\alpha}_{k-1,i} = \gamma_{k-1,i}\alpha_{k-1,i}$. $\varepsilon_{k-1,i}$ is a linear function of $\varepsilon_{k-2,i}$, w_{k-2} and $v_{k-1,i}$ from Lemma 3.1. Hence it is independent of w_{k-1} and $v_{k,i}$, $\forall i \in 1, 2$. Furthermore, x_{k-1} is independent of w_{k-1} and $v_{k,i}, \forall i$, and $\hat{x}_{k-2}$ only depends on $x_0, w_0, \ldots, w_{k-3}$ and $v_{0,i}, \ldots, v_{k-2,i}$, $i = 1, 2$. As a consequence, z_{k-1} is also independent of w_{k-1} and $v_{k,i}$ for $i \in \{1, 2\}$. Similar to **Case 1**, we can obtain the optimal parameters and its corresponding P_k:

$$\alpha^\star_{k,1} = \frac{\mathbb{T}r[h(P_{k+1}) - W_k]}{\mathbb{T}r[\overline{P}_1 + h(P_{k-1}) - 2W_k]}. \tag{18}$$

and

$$\begin{aligned} \beta_{k,1} &\triangleq \mathbb{T}r[P_k|\gamma_{k,1} = 1, \gamma_{k,2} = 0] \\ &= \frac{\mathbb{T}r[\overline{P}_1]\mathbb{T}r[h(P_{k-1})] - \mathbb{T}r[W_k]^2}{\mathbb{T}r[\overline{P}_1 + h(P_{k-1}) - 2W_k]}. \end{aligned} \tag{19}$$

Besides that, based on the Cauchy-Schwarz inequality, we can obtain the bound of W_k, i.e., $|\mathbb{T}r[W_k]| \leq (\mathbb{T}r(P_1)\mathbb{T}r(h(P_{k-1})))^{\frac{1}{2}}$, $\forall k \in \mathcal{N}$, hence $\alpha^\star_{k,1}$ is bounded.

The discussion of the case $(\gamma_{k,1} = 0, \gamma_{k,2} = 1)$ is same as the aforementioned analysis. We omit the details and present that

$$\alpha^\star_{k,3} = \frac{\mathbb{T}r[h(\overline{P}_2 - \hat{W}_k]}{\mathbb{T}r[\overline{P}_2 + h(P_{k-1}) - 2\hat{W}_k]}. \tag{20}$$

and

$$P_{k,2} = \frac{\mathbb{T}r[\overline{P}_2]\mathbb{T}r[h(P_{k-1})] - \mathbb{T}r[\hat{W}_k]^2}{\mathbb{T}r[\overline{P}_2 + h(P_{k-1}) - 2\hat{W}_k]}, \tag{21}$$

where $\hat{W} \triangleq \mathbb{E}[\varepsilon_{k,2} z_k']$ and its iteration is similar to (17). ■

IV. Cooperative Channel Selection for DoS Attacks

As depicted in Fig. 1, the remote estimator explicitly informs the sensors whether the data packets are received successfully or not via a feedback mechanism. Thus, the sensors can obtain full knowledge of the estimation error covariance P_k from (12) developed in the previous section. Meanwhile, the attacker can also infer P_k by intercepting the feedback signals. Based on this real-time information, at each time, the agents will make efficient decisions among the multiple communication paths. To model this interactive decision-making process among the sensors and the attacker, we introduce a game-theoretic framework and design the defensive/offensive strategies for the sensors/attacker, respectively.

A. Game Formulation

Define a game as $\mathcal{G} =< \mathcal{I},\ \mathcal{S},\ \mathcal{J} >$, where $\mathcal{I}$ represents the set of two players; $\mathcal{S} = (\mathcal{S}_1,\ \mathcal{S}_2)$ is the action set for each player in $\mathcal{I}$; and the payoff function $\mathcal{J} : \mathcal{S}_1 \times \mathcal{S}_2 \to \mathbb{R}^{\mathcal{I}}$ denotes the payoff of each player $i \in \mathcal{I}$. In this game framework, we have the following specifications.

1) Player: Since two sensors have the same objective to improve the estimation accuracy, they can be regarded as a team; in contrast, the attacker aims at degrading the system performance. The sensor team denoted by $\mathcal{I}_s$ and the attacker $\mathcal{I}_a$ are assumed to be two rational players; i.e., each player makes the best choice among the action set $\mathcal{S}$.

2) Strategy: At every time step k, the sensor team needs to choose through which channel to send the two estimates $\hat{x}_{k,1}$ and $\hat{x}_{k,2}$; analogously, the attacker selects a channel to launch DoS attacks. Consequently, the strategy of the attacker, denoted by $\overrightarrow{\lambda_k} = \{\lambda_s\} \in \mathbb{R}^3$ with $s = 0, 1, 2$, is composed of different probabilities for choosing corresponding channels. Note that the subscript $s = 0$ stands for the inactive state of the attacker, which means that no DoS attack are launched for the sake of energy saving. Differently, the pure strategies (actions) for the sensor team are $\mathcal{S}_1 = \{(l, j) : l, j = 0, 1, 2\}$ and its mixed strategy is denoted by $\overrightarrow{\rho_k} = (\rho_{00}, \rho_{01}, \ldots, \rho_{lj}, \ldots, \rho_{22})' \in \mathbb{R}^9$, i.e., a probability distribution over the corresponding actions (l, j). Hence, the mixed strategies satisfy that $\sum_{s=0}^{2} \lambda_s = 1,\ \sum_{l=0}^{2}\sum_{j=0}^{2} \rho_{lj} = 1$.

3) Arrival Rate: To analyze this relationship between the packet-arrival-rate and $SINR_i$ under the multi-sensor multi-channel framework, we introduce two matrices describing the packet-arrival-rate for each sensor.Let the arrival rate of packet $\hat{x}_{k,1}$ denoted by $q_1 \triangleq \tilde{f}_1(l, j, s) = f_l(SINR_1(l, j, s))$ (in which (l, j, s) indicates the selected channels). Similarly, the packet $\hat{x}_{k,2}$ is received by the remote estimator with probability $q_2 \triangleq \tilde{f}_2(l, j, s) = f_j(SINR_2(l, j, s))$. Consider the constructed matrixes $Q_i, i \in \{1, 2\}$, defined as

$$Q_i = \begin{pmatrix} \tilde{f}_i(0,0,0) & \tilde{f}_i(0,0,1) & \tilde{f}_i(0,0,2) \\ \vdots & \vdots & \vdots \\ \tilde{f}_i(l,j,0) & \tilde{f}_i(l,j,1) & \tilde{f}_i(l,j,2) \\ \vdots & \vdots & \vdots \\ \tilde{f}_i(2,2,0) & \tilde{f}_i(2,2,1) & \tilde{f}_i(2,2,2) \end{pmatrix} \in \mathcal{R}^{9\times 3},$$

in which (l, j) has the same order as $\overrightarrow{\rho_k}$. According to the independence assumption on $\gamma_{k,1}$ and $\gamma_{k,2}$, we obtain the probability matrix for the no-packet-loss case, denoted by $M_0 = Q_1 \circ Q_2$, in which $\circ$ represents the Hadamard product. Analogously, the probability matrix M_1 for the case $(\gamma_{k,1} = 1, \gamma_{k,2} = 0)$ is $M_1 = (\mathbf{1} - Q_1) \circ Q_2$ where $\mathbf{1} \in \mathcal{R}^{9\times 3}$ refers to a matrix of all ones. Additionally, we have $M_2 = Q_1 \circ (\mathbf{1} - Q_2)$ and $M_3 = (\mathbf{1} - Q_1) \circ (\mathbf{1} - Q_2)$. With these probability matrices, we can obtain the expected packet-arrival-rate at time k: $R_t(M_t, \overrightarrow{\lambda_k}, \overrightarrow{\rho_k}) = \overrightarrow{\rho_k}' M_t \overrightarrow{\lambda_k}, t \in \{0, 1, 2, 3\}$. Consequently, based on (12) the trace of the expected error covariance at time k is $\mathbb{T}r\left[\mathbb{E}(P_k)\right] = \sum_{t=0}^{3} R_t(M_t, \overrightarrow{\lambda_k}, \overrightarrow{\rho_k})\beta_{k,t}$, where $\beta_{k,3} = \mathbb{T}r[h(P_{k-1})]$.

4) Energy: Energy constraints are common in CPS study due to limited batteries and inconvenience of recharging, etc. One of the most important goals of CPS design is to achieve a desired tradeoff between the energy cost and the system performance. The attacker may also have energy limitations on its attack scheme. The expected energy for the sensor and the attacker is $\overline{E_k^s} = \overrightarrow{\rho_k}' \cdot \overrightarrow{E^s}$ and $\overline{E_k^a} = \overrightarrow{E^a}' \cdot \overrightarrow{\lambda_k}$.

5) Payoff: With the sensors aiming to improving the estimation performance without too much energy expenditure, we model the one-stage payoff function for the sensor team: $r_k(P_{k-1}, \overrightarrow{\rho_k}, \overrightarrow{\lambda_k}) \triangleq -\mathrm{Tr}\left[\mathbb{E}(P_k)\right] - \delta_s \overline{E^s} + \delta_a \overline{E^a}$, where the parameters δ_a, δ_s represent the proportions of the energy term in the payoff. For the attacker, its payoff function is $-r_k(P_{k-1}, \overrightarrow{\rho_k}, \overrightarrow{\lambda_k})$.

B. Rational Strategies Design

Based on the characteristics of the payoff functions, players will process the following one-step zero-sum game at every time k:

Problem 4.1: For the sensor team and the attacker,

$$\begin{aligned} \mathcal{J}_S^\star(m) &= \max_{\overrightarrow{\rho_k} \in \mathcal{S}_2} \min_{\overrightarrow{\lambda_k} \in \mathcal{S}_1} r_k(m, \overrightarrow{\rho_k}, \overrightarrow{\lambda_k}), \\ \mathcal{J}_A^\star(m) &= \max_{\overrightarrow{\lambda_k} \in \mathcal{S}_2} \min_{\overrightarrow{\rho_k} \in \mathcal{S}_1} -r_k(m, \overrightarrow{\rho_k}, \overrightarrow{\lambda_k}) \\ & s.t. \sum_s \lambda_s = 1,\ \sum_l \sum_j \rho_{lj} = 1. \end{aligned}$$

To solve Problem 4.1, we first introduce the equilibria of the one-step game [14]. Then, we prove the existence of the optimal strategies, which are deployed by the sensor and the attacker; i.e., we show that a Nash Equilibrium (NE) exists for this game.

Definition 4.2 (NE): In the two-player zero-sum game with the initial state P_0, a strategy profile $\pi^{s,\star}$ (or $\pi^{a,\star}$)

TABLE I: Dynamics of the optimal parameters

$\overrightarrow{\alpha_k}$ \ k	1	2	3	4	5	6	7
$\alpha_{k,1}$	0	0	0	0	0	0.8905	0
$\alpha_{k,2}$	0.8172	0.8175	0.8193	0	0	0	0
$\alpha_{k,3}$	0.1828	0.1825	0.1807	1	1	0.1095	1

TABLE II: Summary for parameters

Parameters for dynamic system						Weight	
A	C_1/C_2	Q	R_1/R_2	$\overline{P}_1/\overline{P}_2$	$\overline{\Gamma}$	δ_1	δ_2
1.2	0.7/0.8	0.8	0.8/0.8	0.92/0.75	0.18	0.15	0.15
Parameters for multi-channel							
c_1/c_2	L_1/L_2	$\{e_{l,1}\}$	$\{e_{j,2}\}$	$\{n_s\}$		σ_1/σ_2	τ
4/4	1/1	(4, 5)	(4, 5)	(2.5, 2.5)		0.1/0.15	0.1

for the sensor team (or the attacker) is a NE if

$$\mathcal{J}_S^\star(P_0) \doteq \mathcal{J}_S(P_0, \pi^{s,\star}, \pi^{a,\star}) \geq \mathcal{J}_S(P_0, \pi^s, \pi^{a,\star}), \forall \pi^s,$$
$$\mathcal{J}_A^\star(P_0) \doteq \mathcal{J}_A(P_0, \pi^{s,\star}, \pi^{a,\star}) \geq \mathcal{J}_A(P_0, \pi^{s,\star}, \pi^a), \forall \pi^a.$$

To explain the existence of NE in the sensor-attacker game, recall the theorem that the two-player zero-sum game with finite pure strategies for each player, has at least one NE. Note that, the reward function can be described as: $r_k = -\overrightarrow{\rho_k}'[\sum_{t=0}^{3}\beta_{k,t}M_t]\overrightarrow{\lambda_k} - \delta_s\overrightarrow{\rho_k}'\overrightarrow{E^s} + \delta_a\overrightarrow{E^a}'\overrightarrow{\lambda_k}$. Apparently, this objective function is convex on $\overrightarrow{\rho_k}$ and $\overrightarrow{\lambda_k}$ and we have $\min\max r_k = \max\min r_k$. Hence, the NE exists based on the minmax theorem in [14, Appendix 2]. By employing the convex tools, we are able to solve this minmax problem and some examples are illustrated in Section V.

V. Examples

In this section, we illustrate the results developed via some examples. For simplicity, we consider a scalar dynamic system with parameters shown in Tab. II. We adopt a general form of $f_l(SINR)$ from [12], that is, $f_l(SINR) = 1 - c_l \cdot (SINR)^{-L_l}$, $l = 1, 2$. After simulating the sensor-attacker game and the aggregation 50 times using Matlab, we obtain the following results. For each time, we obtain the optimal parameter triple $\{\alpha_{k,1}, \alpha_{k,2}, \alpha_{k,3}\}$ based on Theorem 3.4, and its dynamics for the first 7 times are illustrated in Tab. I. From this, we can infer the arrival of estimates, for example, the packets are lost at time 4 and 5 since $\overrightarrow{\alpha_k} = (0,\ 0,\ 1)$ when $k = 4, 5$. With the feedback information, the sensors have a knowledge of the latest system performance P_{k-1} and send their estimates following the optimal defensive strategy (see Fig. 2), and simultaneously the intelligent attacker will congest a channel following its offensive strategy, the specifics of which are presented in Fig. 3. From the simulation results, the possible actions for the sensor team are in the set $\{(l, j) : (0, 0), (0, 1), (0, 2), (1, 2), (2, 1)\}$ (and the probabilities of others equal to zero). Since $\mathbb{P}r(j = 0) < \mathbb{P}r(l = 0)$, we can conclude that the sensor team is inclined to send the more accurate estimate $\hat{x}_{k,2}$ rather than $\hat{x}_{k,1}$ (note that $\overline{P}_1 > \overline{P}_2$ and $e_{l,1} = e_{j,2}$ if $l = j$) when the transmission energy is limited. Moreover, they avoid sending $\hat{x}_{k,1}$ and $\hat{x}_{k,2}$ in a same channel to eliminate the interference.

VI. Conclusion

This work proposed an optimal aggregation scheme to operate the received information and a cooperative channel-selection strategy for the sensors via a game-theoretic approach.

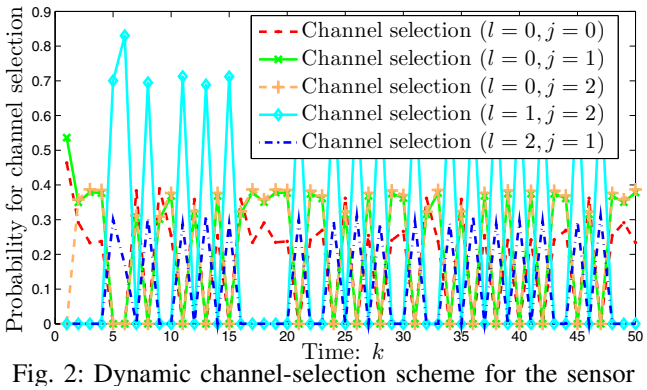

Fig. 2: Dynamic channel-selection scheme for the sensor

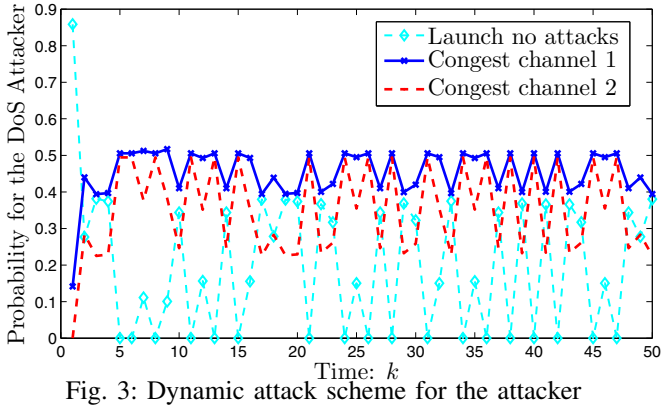

Fig. 3: Dynamic attack scheme for the attacker

References

[1] K.-D. Kim and P. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, May 2012.

[2] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *ICDCS Workshops*. IEEE, 2008, pp. 495–500.

[3] Ics.sans.org. (2016, Jan.) Sans industrial control systems security blog—current reporting on the cyber attack in ukraine resulting in power outage—sans institute.

[4] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, Nov 2015.

[5] S. Liu, P. X. Liu, and A. El Saddik, "A stochastic game approach to the security issue of networked control systems under jamming attacks," *Journal of the Franklin Institute*, vol. 351, no. 9, pp. 4570–4583, 2014.

[6] H. Li, L. Lai, and R. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *Proc. IEEE Conf. Information Sciences and Systems*, March 2011, pp. 1–6.

[7] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[8] O. D. Incel, "A survey on multi-channel communication in wireless sensor networks," *Computer Networks*, vol. 55, no. 13, pp. 3081–3099, 2011.

[9] S.-L. Sun and Z.-L. Deng, "Multi-sensor optimal information fusion kalman filter," *Automatica*, vol. 40, no. 6, pp. 1017–1023, 2004.

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

[11] B. Anderson and J. B. Moore, "Optimal filtering," *Englewood Cliffs, NJ: Prentice-Hall, 1979*, vol. 1, 1979.

[12] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[13] J. Wu, Y. Yuan, H. Zhang, and L. Shi, "How can online schedules improve communication and estimation tradeoff?" *Signal Processing, IEEE Transactions on*, vol. 61, no. 7, pp. 1625–1631, 2013.

[14] R. Luce and H. Raiffa, *Games and Decisions: Introduction and Critical Survey*. Dover Publications, 1957.