# Stochastic DoS Attack Allocation Against Collaborative Estimation in Sensor Networks

Ya Zhang, *Member, IEEE*, Lishuang Du, and Frank L. Lewis, *Fellow, IEEE*

***Abstract*—In this paper, denial of service (DoS) attack management for destroying the collaborative estimation in sensor networks and minimizing attack energy from the attacker perspective is studied. In the communication channels between sensors and a remote estimator, the attacker chooses some channels to randomly jam DoS attacks to make their packets randomly dropped. A stochastic power allocation approach composed of three steps is proposed. Firstly, the minimum number of channels and the channel set to be attacked are given. Secondly, a necessary condition and a sufficient condition on the packet loss probabilities of the channels in the attack set are provided for general and special systems, respectively. Finally, by converting the original coupling nonlinear programming problem to a linear programming problem, a method of searching attack probabilities and power to minimize the attack energy is proposed. The effectiveness of the proposed scheme is verified by simulation examples.**

***Index Terms*—Attack allocation, denial of service (DoS) attack, packet loss, remote estimation, sensor networks.**

## I. Introduction

WIRELESS sensor networks (WSNs), which are interconnected by a large number of cooperative wireless sensor nodes, have been extensively applied in many areas [1]. The optimal estimation algorithms based on minimum mean square error, such as Kalman filtering and information filtering, are often used in WSN state estimation for obtaining accurate estimate [2]–[7]. However, due to the wireless communication characteristics of WSNs, attackers can easily monitor the channels in the task domain of the network, inject bitstream into the channel, and replay the previously captured packets [8]–[10]. It is important to conduct in-depth research on attacks in sensor networks.

The research on state estimation of networks under attacks can be classified into two categories: one is secure estimation against attacks, the other is to place the attacks from the standpoint of attackers. Secure estimation in centralized or distributed networks has been studied preliminarily. Chi-square detection and Euclidean detector were used to detect data anomalies caused by attacks [11]–[14]. Scheduling strategies including event triggering strategies were proposed out to mitigate the impact of attacks [15]–[17]. *K*-means algorithm for classifying trust nodes had also been studied [18]. In [19], a distributed secure estimation problem on GE F404 engine was researched. An efficient distributed resilient estimator and attack detection mechanism for sensor networks under deception attacks on both the system dynamics and sensor intercommunication links were proposed in [20]. A distributed finite-time filter was proposed for discrete time positive systems in sensor networks under random deception attacks [21]. Du *et al*. [22] studied distributed state estimation problem under deception attacks and denial of service (DoS) attacks, and proposed a novel alternating direction method of multipliers (ADMM)-based distributed state estimation method.

How to allocate attacks is another hot topic [23]–[29]. DoS attacks can cause network congestion and packet losses, which makes the remote estimator difficult to obtain uniformly bounded state estimation errors in the network. Qin *et al*. [23] studied the optimal attack scheduling scheme of the energy-constrained attacker in packet-dropping networks. The corresponding time-centralized attack strategies were given to maximize the trace of the average estimation error and the terminal estimation error. Similarly, using the Markov decision process, Ding *et al*. [24] proposed a two-player zero-sum stochastic game framework to investigate such a situation: sensors need to select a single channel to send data packets and reduce the possibility of being attacked; at the same time, attackers need to determine the attacked channel under the constraints of energy budget. Cao *et al*. [25] proposed a probabilistic DoS attack scheme against remote state estimator over a Markov channel in cyber-physical systems. Li *et al*. [26] designed an attack jamming approach on remote state estimation in cyber-physical systems by using a game theory. Zhang *et al*. [27], [28] studied a scenario, in which the optimal attack power allocation of energy-constrained DoS attackers to maximize the terminal estimation error was discussed. An attack power allocation mechanism with low cost was put forward. A dynamic attack

Manuscript received January 14, 2020; revised February 15, 2020; accepted March 17, 2020. This work was supported by the National Natural Science Foundation (NNSF) of China (61973082) and Six Talent Peaks Project in Jiangsu Province (XYDXX-005). Recommended by Associate Editor Giuseppe Franzè. *(Corresponding author: Ya Zhang.)*

Citation: Y. Zhang, L. S. Du, and F. L. Lewis, "Stochastic DoS attack allocation against collaborative estimation in sensor networks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1225–1234, Sept. 2020.

Y. Zhang and L. S. Du are with the School of Automation, Southeast University, and also with the Key Laboratory of Measurement and Control of Complex Systems of Engineering, Ministry of Education, Nanjing 210096, China (e-mail: realzhya@sina.com; beckydls@foxmail.com).

F. L. Lewis is with the University of Texas at Arlington Research Institute, Fort Worth, TX 76118 USA (e-mail: lewis@uta.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2020.1003285

energy disposal algorithm with ascertained attack capability in each period was also designed. In relevant works, most of the considerations focus on DoS attacks in single channel between the sensor and the remote estimator. Few researches have discussed DoS attack allocation in multiple channels of cooperative sensor networks. In [23] an attack scheduling approach was proposed to maximize the sum of the estimation errors of two remote estimators corresponding to two sensors, with the assumption that each sensor was completely observable. Yang *et al*. [29] studied DoS attack arrangement within an energy budget in centralized state estimation, and proposed a selection scheme of which sensor to be attacked under the assumption that different kinds of sensors are completely observable.

Although the DoS attack allocation problem has attracted wide attention [23]–[29], to the best of our knowledge, the problem of DoS attack scheduling in collaboratively working sensor networks has not been well addressed in the literature. The main difficulties may come from the following two aspects.

1) The network is composed of multiple heterogeneous sensors and single sensor is not necessarily observable. Unlike previous works [23], [27], [28], where the steady-state value is used to update estimation when there is no attack, in this paper each sensor transmits its measurement and the remote estimator uses the received measurements to update estimation. The existing attack scheduling schemes for remote estimator with one observable sensor cannot be applicable.

2) The attack probabilities and attack energy to be exerted by the attacker to the sensors can be different. The function of the packet dropout probability about attack energy is nonlinear and there is trade-off between collective observability and attack energy. Hence the attack scheduling problem is a nonlinear programming problem with high complexity and computation.

This paper focuses on designing a stochastic scheduling and attack power allocation scheme from the perspective of the energy-constrained DoS attacker, so as to influence the estimation of the collaboratively working sensor network with minimum attack energy cost. An allocation scheme consisting of three steps is proposed. The contributions of this paper contain the following.

1) Unlike attack allocation in single sensor's communication [23]–[28], in sensor networks, multiple sensors' channels should be attacked. The minimum number of channels needed to attack and how to select the channels are given.

2) A necessary condition and a sufficient condition on the packet loss probabilities of the attacked channels such that the mean square estimation error of the estimator is divergent are provided.

3) The optimal attack probabilities and attack power with minimum energy consumption to destroy the collective observability of the network are proposed.

The rest of this paper is arranged as follows. Section II formulates the filter in WSNs and DoS attack model, and states an overview of the problem. In Section III, the minimum number of channels needed to attack and how to select the channels are firstly given, and then the conditions of the packet loss probabilities making the estimation error divergent are provided for general and special systems respectively. In Section IV the optimal attack probability and power with minimum energy consumption are discussed. Finally, in Section V, the simulation results verify the effectiveness of the attack mechanism.

*Notations:* $\mathbb{R}^n$ denotes the set of $n$ dimensional vectors over real numbers and $\mathbb{R}^{m\times n}$ is the set of real matrices with $m$ rows and $n$ columns. $\mathbb{Z}^+$ denotes the set of positive integers. We write $X \geq 0$ to denote that $X$ is positive semi-definite. $\mathbb{E}\{\cdot\}$ represents the mathematical expectation. $\mathrm{tr}\,(\cdot)$ and $\rho(\cdot)$ stand for the trace and spectral radius of matrix, respectively. $\lfloor r \rfloor$ denotes the largest integer that does not exceed $r$, $r \in \mathbb{R}$. $\Pr(\cdot)$ means the probability. $|S|$ stands for the cardinality of set $S$. $\dim(\cdot)$ denotes the dimension of space. $x(i)$ denotes the $i$th element of vector $x$. $\mathrm{diag}\{R_i, i = 1,\ldots,n\}$ denotes a diagonal matrix with diagonal blocks $R_i, i = 1,\ldots,n$. $\mathrm{col}\{C_i, i = 1,\ldots,n\}$ is a short form of matrix $[C_1^T,\ldots,C_n^T]^T$.

## II. Problem Formulation

In this section, the target's system model, the sensor network, the impacts of DoS attacks, and the optimal attack allocation problem are formulated.

### *A. Target and Sensor Network*

Consider a linear time-invariant system to be monitored:

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

where $x_k \in \mathbb{R}^{n_x}$ is the state vector of the system at time $k$, $n_x \in \mathbb{Z}^+$, $k = 0,1,2,\ldots$. $A$ is the system matrix; $v_k \in \mathbb{R}^{n_x}$ is the process white Gaussian noise with covariance $Q > 0$. The initial state $x_0$ is a Gaussian random vector with zero mean and covariance $\Pi_0 \geq 0$.

A sensor network composed of $N$ sensors is used to measure the system. The sensor set is described as $\mathcal{V} = \{s_i \mid i = 1,2,\ldots,N\}$. These sensors have the ability to measure, calculate and communicate. The measurement of sensor $s_i$ at time step $k$ is obtained with the following form:

$$z_{i,k} = C_i x_k + w_{i,k} \tag{2}$$

where $z_{i,k} \in \mathbb{R}^{n_{z_i}}$ is a measurement vector for target system, $n_{z_i} \in \mathbb{Z}^+$; $C_i$ is the measurement matrix; $w_{i,k} \in \mathbb{R}^{n_{z_i}}$ is a zero-mean white Gaussian noise with covariance matrix $R_i > 0$, and $w_{1,k},\ldots,w_{N,k}$, $v_k$ are uncorrelated.

*Assumption 1:* The system matrix $A$ is known and the system is not necessarily Schur stable. $(A, Q^{\frac{1}{2}})$ is controllable. $(A, C_i)$ is not necessarily detectable but $(A, C)$ is detectable, where $C = [C_1^T, C_2^T,\ldots,C_N^T]^T$.

A centralized information Kalman filter is adopted in the remote estimator to estimate the state of the target. Sensors in the network transmit their innovation vectors $C_i^T R_i^{-1} z_{i,k}$ and innovation matrices $C_i^T R_i^{-1} C_i$ to the remote estimator, which updates the state estimate by the information received. Denote $\Omega_k^-$ and $\Omega_k^+$ as the a priori and a posteriori information matrices of the estimator, respectively, $P_k^-$ and $P_k^+$ as the a priori and a posteriori covariance matrices in Kalman filter, respectively. Then, $\Omega_k^- = (P_k^-)^{-1}$, $\Omega_k^+ = (P_k^+)^{-1}$. Similarly, the a priori and a posteriori estimation state vectors of the estimator are denoted as $x_k^-$ and $x_k^+$.

*Assumption 2:* All sensors are clock synchronized and there is no communication delay in the network. When there is no attack in the network, there is no packet dropout. The packet that each sensor transmits at each time instant consists of $L$ bits and the transmission error is of bit-to-bit independent.

The estimator firstly computes the a priori information matrix and vector as following:

$$\Omega_k^- = [A(\Omega_{k-1}^+)^{-1}A^T + Q]^{-1} \tag{3}$$

$$x_k^- = Ax_{k-1}^+. \tag{4}$$

Then, the information fusion center updates the a posteriori estimate by using the received information [5]

$$\Omega_k^+ = \Omega_k^- + \sum_{s_i \in \mathcal{V}_k^0} C_i^T R_i^{-1} C_i \tag{5}$$

and

$$x_k^+ = (\Omega_k^+)^{-1}(\Omega_k^- x_k^- + \sum_{s_i \in \mathcal{V}_k^0} C_i^T R_i^{-1} z_{i,k}) \tag{6}$$

where $\mathcal{V}_k^0$ denotes the set of sensors whose packets are successfully received at time $k$.

### *B. DoS Attack Model*

There exists an attacker in the network. The purpose of the attacker is to occupy the communication bandwidth by DoS attack, which jams some channels between sensors and the remote estimator and increases the packet loss probabilities. Under DoS attacks, the remote estimator may not estimate the system state successfully.

If the communication channel from sensor $s_i$ to the estimator is attacked by the attacker, from [30] its SNR (signal-to-noise ratio) is

$$\rho_i = \frac{\delta^s G^s}{\delta_i^a G^a + \sigma^2} \tag{7}$$

where $G^a$ is the channel gain from the attacker to the remote estimator and $G^s$ is that from a sensor to the estimator. $\delta^s$ is the transmission power of sensors. $\delta_i^a$ is the attack power statically assigned to the channel. $\sigma^2$ is the noise power and $\delta^s G^s \gg \sigma^2$.

The transmitted packet of each sensor consists of multiple bits, and only if every bit is received correctly, the packet is considered as successfully received. Then from Assumption 2, the probability of one packet reception is described as [28]

$$\mu_i = \left[1 - Q(\sqrt{2\rho_i})\right]^L \tag{8}$$

where $Q(x) = 1/\sqrt{2\pi}\int_x^\infty e^{-t^2/2}dt$. Therefore, under the DoS attack, the packet in sensor $s_i$'s communication channel is randomly dropped with probability

$$p_i = 1 - \mu_i. \tag{9}$$

When sensor $s_i$'s channel is not invaded, which means $\delta_i^a = 0$, the packet dropout probability is $p_i = 1 - \mu_i |_{\delta_i^a = 0}$, which is very close to zero. This fact conforms to Assumption 2 that when there is no attack, the packet loss probability is zero.

Considering a limited energy budget, there is no need for the attacker to keep implementing DoS attacks to one channel with high attack power at every time. Therefore, we consider the stochastic attack mechanism satisfying the following assumption.

*Assumption 3 (Attack Rule):* The attacker randomly exerts DoS attacks to part of transmission channels with certain fixed probabilities and power.

Under the stochastic DoS attack scheme, each channel is inflicted by attack with some probability. Define $\gamma_i$ $(0 \le \gamma_i \le 1,\ i = 1, 2, \ldots, N)$ as the probability that sensor $s_i$'s communication channel is attacked. Let $\theta_{i,k}$ denote the attacked status of sensor $s_i$'s channel. If the channel from sensor $s_i$ to the center suffers from jamming at time $k$, $\theta_{i,k} = 1$; otherwise, $\theta_{i,k} = 0$. Obviously, $\Pr(\theta_{i,k} = 1) = \gamma_i$. This paper focuses on allocating intruded channels by appropriate probabilities $\gamma_i$ and attack power $\delta_i^a$ $(i = 1, 2, \ldots, N)$ to destroy the estimation of the estimator with the minimum cost.

Being exposed to attack results in significantly increased packet loss probability. We define another variable $d_{i,k}$ to indicate whether the packet of sensor $s_i$ is successfully received by the remote estimator at time $k$, where if the packet on the channel from sensor $s_i$ to the estimator is not received successfully at time $k$, $d_{i,k} = 1$; otherwise, $d_{i,k} = 0$.

Due to the stochastic properties of the attacks and packet losses, $d_{i,k}$ can be modeled by a Bernoulli process with distribution

$$d_{i,k} = \begin{cases} 1, & \text{with probability } \gamma_i p_i \\ 0, & \text{with probability } 1 - \gamma_i p_i. \end{cases} \tag{10}$$

The block diagram for the sensor network under attack is shown in Fig. 1.

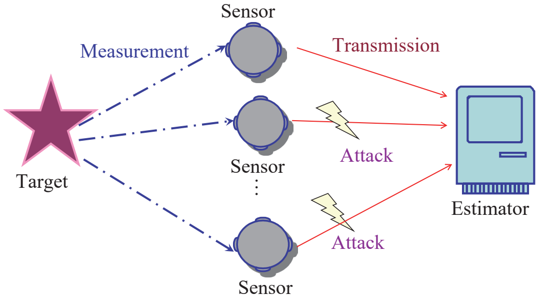


Fig. 1. The estimation network under attack.

### *C. Attack Allocation Problem*

The attacker's intention is to prevent the remote estimator from obtaining the effective state estimate with a bounded mean square estimation error. Since the packets of the sensors are lost randomly, the DoS attacker aims at making the trace of the mathematical expectation on a prior covariance matrix $P_k^-$ unbounded, and meanwhile, minimizing the attack energy consumed. During a long period $T$, the number of time steps that sensor $s_i$'s transmission channel is attacked can be approximated to $\gamma_i T$, and thus the attack power allocated in this channel is $\gamma_i T \delta_i^a$. Hence, the problem above can be summarized as follows:

*Problem 1:*

$$\begin{aligned}&\min \sum_{i=1}^{N} \gamma_i \delta_i^a\\ &\text{s.t.} \lim_{k\to\infty} \operatorname{tr} \mathbb{E}\left\{P_k^-\right\} \to \infty.\end{aligned}$$

In the following sections, we will investigate how to select $\gamma_i$ and $\delta_i^a$ $(i = 1,2,\ldots,N)$ to solve Problem 1.

*Remark 1:* It should be noted that considering a control input signal for the system does not affect the problem formulation if the control input is known to the estimator.

## III. Attack Placement and Probability Condition

To solve Problem 1, we can search the optimal attack probabilities and power by using the condition of $\lim_{k\to\infty} \operatorname{tr} \mathbb{E}\{P_k^-\} \to \infty$. It is a nonlinear programming problem with high complexity and computation. To reduce the complexity and computation, we will solve Problem 1 from three steps. The first step is to look for the minimum number and further the placement of channels to be attacked. Given the attacked node set, the second step is to investigate the conditions on the packet loss probabilities such that the covariance is unbounded. The last step is to search the attack probabilities and power based on the packet loss probability conditions to minimize the energy consumed. In this section, we will discuss the first and the second steps in order.

### *A. Mathematical Expectation of the Covariance Matrix*

To begin with, we give the equation of the expected covariance matrix.

Define $\mathcal{V}_k^0 = \{s_i | i \in \mathcal{V}, d_{i,k} = 0\}$ as the set of the sensors successfully sending information to the remote estimator at time $k$. Besides, $\mathcal{V}_k^d = \{s_i | i \in \mathcal{V}, d_{i,k} = 1\}$ denotes the set of sensors whose packets are dropped at time $k$. At any time $k$, $\mathcal{V} = \mathcal{V}_k^0 \cup \mathcal{V}_k^d$.

Define $z_k = \operatorname{col}\{z_{i,k}, s_i \in \mathcal{V}_k^0\}$ as the augmented vector collecting the sensors' measurements that are successfully transmitted to the processing center at time $k$, $\bar{C}_k = \operatorname{col}\{C_i, s_i \in \mathcal{V}_k^0\}$ as the collective measurement matrices of the corresponding sensors, and $\bar{R}_k = \operatorname{diag}\{R_i, s_i \in \mathcal{V}_k^0\}$.

Therefore, from (3), (5), and the Matrix Inversion Lemma, we obtain

$$\begin{aligned}P_{k+1}^- = {}& A P_k^- A^T + Q - A P_k^- \bar{C}_k^T\\ &\times (\bar{C}_k P_k^- \bar{C}_k^T + \bar{R}_k)^{-1} \bar{C}_k P_k^- A^T\end{aligned} \tag{11}$$

and its expected value is

$$\begin{aligned}\mathbb{E}\{P_{k+1}^-\} = {}& \mathbb{E}\{A P_k^- A^T + Q - A P_k^- \bar{C}_k^T\\ &\times (\bar{C}_k P_k^- \bar{C}_k^T + \bar{R}_k)^{-1} \bar{C}_k P_k^- A^T\}.\end{aligned} \tag{12}$$

Let $J_1, J_2, \ldots, J_{2^N}$ stand for all possible node sets $\mathcal{V}_k^0$, $\tilde{J} = \{J_t : t = 1,2,\ldots,2^N\}$ represent the set including all the possible sets $J_t$, $t = 1,2,\ldots,2^N$. For convenience, we denote $\bar{C}_k$ and $\bar{R}_k$ as $C_{J_t} = \operatorname{col}\{C_{j_l}, 1 \le l \le s\}$ and $\mathcal{R}_{J_t} = \operatorname{diag}\{R_{j_1}, R_{j_2}, \ldots, R_{j_s}\}$ respectively when $\mathcal{V}_k^0 = J_t = \{j_1, j_2, \ldots, j_s\}$. From the stochastic properties of $d_{i,k}$, we have

$$\Pr(\mathcal{V}_k^0 = J_t) = \prod_{i\in J_t} (1 - \gamma_i p_i) \prod_{j\notin J_t} \gamma_j p_j. \tag{13}$$

Then, the mathematical expectation expression of state error covariance satisfies the following equation:

$$\begin{aligned}\mathbb{E}\{P_{k+1}^- | P_k^-\} = {}& \prod_{j\in\mathcal{V}} \gamma_j p_j A P_k^- A^T + Q\\ &+ \sum_{J_t\in\tilde{J}\backslash\emptyset} \prod_{i\in J_t} (1 - \gamma_i p_i) \prod_{j\notin J_t} \gamma_j p_j [A P_k^- A^T + Q\\ &- A P_k^- C_{J_t}^T (C_{J_t} P_k^- C_{J_t}^T + \mathcal{R}_{J_t})^{-1} C_{J_t} P_k^- A^T)]\end{aligned} \tag{14}$$

where $\emptyset$ denotes the empty set.

For formulation convenience, we define operators $g(\cdot\,|_{J_t})$, $J_t \in \tilde{J}$ as follows: when $J_t \neq \emptyset$,

$$\begin{aligned}g(P_k^-|_{J_t}) = {}& A P_k^- A^T + Q - A P_k^- C_{J_t}^T (C_{J_t} P_k^- C_{J_t}^T\\ &+ \mathcal{R}_{J_t})^{-1} C_{J_t} P_k^- A^T\end{aligned} \tag{15}$$

when $J_t = \emptyset$,

$$g(P_k^-|_{J_t}) = A P_k^- A^T + Q. \tag{16}$$

Therefore,

$$\mathbb{E}\left\{P_{k+1}^- | P_k^-\right\} = \sum_{J_t\in\tilde{J}} \prod_{i\in J_t} (1 - \gamma_i p_i) \prod_{j\notin J_t} \gamma_j p_j g(P_k^-|_{J_t}). \tag{17}$$

### *B. Placement of Attacks*

To destroy the observability of the entire network for the sake of preventing the estimator from obtaining effective state estimation, at least a certain number of channels are required to attack. This subsection discusses the minimum number of attacked channels to destroy the collective observability of the network. An effective way to enhance the aggressivity and reduce the energy of the attacker is to select fixed channels to attack. For design simplicity, we consider the attack model satisfying the following assumption.

*Assumption 4:* The attacker is allocated to attack fixed sensors' channels.

In the following part, the existence of the minimum number of attacked channels is investigated by the concept of network collaborative observability. Before discussion, the concept of undetectable subspace should be introduced. Let the unstable subspace of system matrix $A$ be expressed as $U(A)$. In Assumption 1, $A$ is assumed to be not Schur stable. Consequently $U(A)$ is not empty. The undetectable subspace of sensor $s_i$ is defined by

$$\begin{aligned}U_i^- = {}& \left\{x \in \mathbb{R}^{n_x} \mid C_i A^l x = 0, l = 0,1,\ldots,n_x - 1\right\}\\ &\cap \{x \mid x \in U(A)\}.\end{aligned} \tag{18}$$

For any node subset $\mathcal{V}_s \subseteq \mathcal{V}$, the undetectable subspace of $\mathcal{V}_s$ is defined by

$$U_{\mathcal{V}_s}^- = \bigcap_{i\in\mathcal{V}_s} U_i^-. \tag{19}$$

*Proposition 1:* For system (1) and sensor networks satisfying Assumptions 1–4, there is a minimum number of channels needed to be attacked. Once the number of the attacked channels is less than it, the estimation error of the estimator must be bounded in mean square. The minimum number $m_{\min}$ is equal to

$$m_{\min} = \min\{|\mathcal{V}_s| : U^-_{\mathcal{V}/\mathcal{V}_s} \neq \emptyset\}. \tag{20}$$

*Proof:* Assume there are $m$ nodes' channels suffering from random attacks, whose set is denoted as $\mathcal{S}_a = \{s_{a_1}, s_{a_2}, \ldots, s_{a_m}\}$, and $m < m_{\min}$. Then from the form of (20), we have that $U^-_{\mathcal{V}/\mathcal{S}_a} = \emptyset$, which means that even all channels of nodes in $\mathcal{S}_a$ are attacked and the packets on them are dropped, the network is still collectively observable. Then, by applying the Kalman information filtering algorithm, the estimation error is bounded. So, the effective number of attacked channels $m$ should be larger than $m_{\min}$.

When $m = m_{\min}$, select one node set in $\{\mathcal{V}_s \subseteq \mathcal{V} : U^-_{\mathcal{V}/\mathcal{V}_s} \neq \emptyset, |\mathcal{V}_s| = m_{\min}\}$ to be attacked. Then, if sufficiently large attacks are allocated, the attacked channels are nearly always dropped, which can make the estimation error of the network unbounded. ■

*Remark 2:* We can search $m_{\min}$ by sorting the node sets according to the cardinality and bisection method. By verifying the condition $U^-_{\mathcal{V}/\mathcal{V}_s} \neq \emptyset$, we can also obtain an effective attacked node set with minimum cardinality. Single or multiple sets may satisfy the requirement after filtration. Here, we choose the set $\mathcal{V}^*$ to make $U^-_{\mathcal{V}/\mathcal{V}^*}$ have the worst stability, i.e., through structural decomposition, the unobservable part of system $(A, C_{\mathcal{V}/\mathcal{V}^*})$ has the maximum spectral radius, which represents the maximum value of the eigenvalues' modulus.

## *C. Probability Condition for General System*

To simplify the problem, in the following, we will fix the possible attacked node set as $\mathcal{V}^*$, which is designed according to Remark 2. Renumber the nodes in $\mathcal{V}^*$ as $1, 2, \ldots, m$, $m = m_{\min}$. Then, there are $M = 2^m$ possible node sets $J_1, \ldots, J_M$, in which each node successfully transmits its information to the center, and for any $J_s \in \tilde{J}$ $(1 \leq s \leq M)$, $\mathcal{V}/J_s \subset \mathcal{V}^*$. Correspondingly, $r_{J_s} = \prod_{i \in J_s}(1-\lambda_i)\prod_{j \notin J_s}\lambda_j$, $\lambda_i = \gamma_i p_i$ denotes the probability of packet loss on the communication channel of $s_i$, where $p_i$ is defined in (9).

In this subsection, we mainly investigate the condition of the packet loss probabilities on the channels of the nodes in $\mathcal{V}^*$ such that $\lim_{k\to\infty} \operatorname{tr} \mathbb{E}\{P^-_k\} \to \infty$. We firstly give an important lemma.

*Lemma 1:* The sequence

$$P_{k+1} = \sum_{s=1}^{M} r_{J_s} g(P_k|_{J_s}) \tag{21}$$

is convergent and bounded, if and only if there exist a symmetric positive definite matrix $X$ and matrices $Y_{J_s}$, $s = 1, 2, \ldots, M$, such that $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) < 0$, where $r_{J_s} = \prod_{i \in J_s}(1-\lambda_i)\prod_{j \notin J_s}\lambda_j$, $g(\cdot\,|_{J_s})$ is defined in (15), $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m)$ is defined in (22) (show at the bottom of this page).

*Proof:* According to the Schur complement lemma, $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) < 0$ is equivalent to that there exist positive definite matrix $\bar{P}$ and matrices $\bar{F}_{J_s}$ such that the following inequality holds

$$\bar{P} > \sum_{s=1}^{M} r_{J_s}[(A - \bar{F}_{J_s}C_{J_s})\bar{P}(A - \bar{F}_{J_s}C_{J_s})^T]. \tag{23}$$

*Necessity:* If the sequence (21) is convergent, there exists $\bar{P} > 0$ such that $\bar{P} = \sum_{s=1}^{M} r_{J_s} g(\bar{P}\,|_{J_s})$, which implies when $\bar{F}_{J_s} = A\bar{P}C^T_{J_s}(C_{J_s}\bar{P}C^T_{J_s} + \mathcal{R}_{J_s})^{-1}$, the inequality (23) holds.

*Sufficiency:* Firstly, we prove that when $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) < 0$ is feasible, the sequence is bounded.

Define linear operators

$$\begin{aligned} f(P) &= \sum_{s=1}^{M} r_{J_s}(A - \bar{F}_{J_s}C_{J_s})P(A - \bar{F}_{J_s}C_{J_s})^T \\ \phi(\overline{\boldsymbol{K}}, P) &= \sum_{s=1}^{M} r_{J_s}[(A - \bar{K}_{J_s}C_{J_s})P(A - \bar{K}_{J_s}C_{J_s})^T \\ &\quad + \bar{K}_{J_s}\mathcal{R}_{J_t}\bar{K}^T_{J_s}] + Q \end{aligned}$$

where $\bar{F}_{J_s}$ is the gain satisfying (23), $\bar{\boldsymbol{K}} = \{\bar{K}_{J_s}, 1 \leq s \leq M\}$, and $\bar{K}_{J_s}$ is the gain. Obviously, the operator $f$ is linear and non-decreasing with $P$. For any given $P_0 > 0$, there exists a positive constant $\alpha_1$ such that $P_0 \leq \alpha_1\bar{P}$. Choose $0 < \beta < 1$ such that $f(\bar{P}) \leq \beta\bar{P}$. Then

$$\begin{aligned} f(P_0) &\leq f(\alpha_1\bar{P}) \\ &= \alpha_1 f(\bar{P}) \\ &\leq \alpha_1\beta\bar{P} \end{aligned}$$

and thus

$$\begin{aligned} f^k(P_0) &\leq \alpha_1\beta f^{k-1}(\bar{P}) \\ &\leq \alpha_1\beta^2 f^{k-2}(\bar{P}) \\ &\leq \alpha_1\beta^k\bar{P}. \end{aligned}$$

Since when $\bar{K}_{J_s} = AP^-_kC^T_{J_s}(C_{J_s}P^-_kC^T_{J_s} + \mathcal{R}_{J_s})^{-1}$, $\phi(\bar{\boldsymbol{K}}, P_k)$ is minimum, we have

$$\begin{aligned} P_{k+1} &\leq \phi(\overline{\boldsymbol{F}}, P_k) = f(P_k) + U \\ &\leq f^k(P_0) + \sum_{t=0}^{k-1} f^t(U) \\ &\leq \alpha_1\beta^k\bar{P} + \sum_{t=0}^{k-1}\alpha_2\beta^t\bar{P} \\ &\leq (\alpha_1 + \frac{\alpha_2}{1-\beta})\bar{P} \end{aligned}$$

where $\bar{\boldsymbol{F}} = \{\bar{F}_{J_s}, 1 \leq s \leq M\}$, $U = \sum_{s=1}^{M} r_{J_s}\bar{F}_{J_s}\mathcal{R}_{J_s}\bar{F}^T_{J_s} + Q$, and $\alpha_2$ is a positive constant satisfying $U \leq \alpha_2\bar{P}$.

$$\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) = \begin{bmatrix} -X & \sqrt{r_{J_1}}(XA - Y_{J_1}C_{J_1}) & \sqrt{r_{J_2}}(XA - Y_{J_2}C_{J_2}) & \ldots & \sqrt{r_{J_M}}(XA - Y_{J_M}C_{J_M}) \\ * & -X & & & \\ * & & -X & & \\ \vdots & & & \ddots & \\ * & & & & -X \end{bmatrix} \tag{22}$$

Secondly, we prove its convergence. For sequence $\{\tilde{P}_k, k \geq 0\}$ satisfying (21), when $\tilde{P}_0 = 0$, we have $\tilde{P}_1 = Q \geq \tilde{P}_0$. And then by the fact that $g$ is a monotonically non-decreasing operator, $\tilde{P}_2 \geq \sum_{s=1}^{M} r_{J_s} g(\tilde{P}_0 |_{J_s}) \geq \tilde{P}_1$. From a simple inductive argument, we have that the sequence is monotonically non-decreasing and bounded. It is obvious that the sequence converges, i.e., $\lim_{k\to\infty} \tilde{P}_k = \bar{P}$, where $\bar{P}$ is a positive semi-definite solution of equation $\bar{P} = \sum_{s=1}^{M} r_{J_s} g(\bar{P} |_{J_s})$.

For sequence $\{\hat{P}_k, k \geq 0\}$ satisfying (21) and $\hat{P}_0 \geq \bar{P}$, $\hat{P}_1 = \sum_{s=1}^{M} r_{J_s} g(\hat{P}_0 |_{J_s}) \geq \hat{P}_0$. Similarly, for any $k \geq 0$, $\hat{P}_k \geq \hat{P}_0$. Let $\bar{F}_{J_s} = A\bar{P}C_{J_s}^T (C_{J_s}\bar{P}C_{J_s}^T + \mathcal{R}_{J_s})^{-1}$, we have

$$0 \leq \hat{P}_{k+1} - \bar{P} \leq \phi(\overline{\mathbf{F}}, \hat{P}_k) - \phi(\overline{\mathbf{F}}, \bar{P}) = f(\hat{P}_k - \bar{P}).$$

Since the operator is stable, i.e., $\lim_{k\to\infty} f(\hat{P}_k - \bar{P}) = 0$, when $\hat{P}_0 \geq \bar{P}$, the sequence $\{\hat{P}_k, k \geq 0\}$ also converges to $\bar{P}$.

Under any initial condition $P_0$, there exists $\hat{P} \geq \bar{P}$ such that $0 \leq P_0 \leq \hat{P}$. From the properties of operator $\phi$,

$$\begin{aligned}\tilde{P}_1 &= \sum_{s=1}^{M} r_{J_s} g(0|_{J_s}) \\ &\leq P_1 = \sum_{s=1}^{M} r_{J_s} g(P_0|_{J_s}) \\ &\leq \hat{P}_1 = \sum_{s=1}^{M} r_{J_s} g(\hat{P}_0|_{J_s})\end{aligned}$$

and similarly the sequences under these three initial conditions satisfy that $\tilde{P}_k \leq P_k \leq \hat{P}_k$. Since both $\tilde{P}_k$ and $\hat{P}_k$ converge to $\bar{P}$, under any initial condition the sequence $P_k$ converges to $\bar{P}$ as well. This lemma has been proved. ■

Lemma 1 gives a necessary and sufficient condition for the convergence of the algebraic Riccati equation (21). By using Lemma 1, we can obtain the following probability conditions making the estimation error unstable.

*Proposition 2:* For system (1) and sensor networks under Assumptions 1–4, fix the possible attacked node set as $\mathcal{V}^*$. The attacker can successfully destroy the estimation of the center, i.e., $\lim_{k\to\infty} \mathrm{tr}\mathbb{E}\left\{P_k^-\right\} \to \infty$, if the attack probabilities and attack power make $r_{J_1}\rho^2(A_{U_{J_1}^-}) \geq 1$, and only if the LMI $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) < 0$ is unfeasible, where $J_1 = \mathcal{V}/\mathcal{V}^*$, $A_{U_{J_1}^-}$ denotes the undetectable part of system matrix $A$ from observability structural decomposition of $(A, C_{J_1})$.

*Proof:*

*Sufficiency:* Define the node set $J_1 = \mathcal{V}/\mathcal{V}^*$. From the definition of $\mathcal{V}^*$, it is obvious that $U_{J_1}^- \neq \emptyset$. Since the channels of the sensors in $J_1$ are not attacked, from (17), we have

$$\mathbb{E}\left\{P_{k+1}^- \mid P_k^-\right\} \geq r_{J_1}(A - F_{J_1,k}C_{J_1})P_k^-(A - F_{J_1,k}C_{J_1})^T + Q$$

where $F_{J_1,k} = AP_k^-C_{J_1}^T(C_{J_1}P_k^-C_{J_1}^T + \mathcal{R}_{J_1})^{-1}$. If $r_{J_1}\rho^2(A_{U_{J_1}^-}) \geq 1$, then $\mathbb{E}\{P_{k+1}^-\}$ must be divergent, where $\rho(A_{U_{J_1}^-})$ denotes the spectral radius of the undetectable part $A_{U_{J_1}^-}$ of node set $J_1$, which can be obtained from observability structural decomposition. The sufficient condition has been proved.

*Necessity:* Since the operator $g(P_k^- |_{J_t})$ in (16) is concave, by using the Jensen's Inequality and (17) we have

$$\begin{aligned}\mathbb{E}\left\{P_{k+1}^-\right\} &= \sum_{J_t \in \tilde{J}} r_{J_t}\mathbb{E}\left\{g(P_k^-|_{J_t})\right\} \\ &\leq \sum_{J_t \in \tilde{J}} r_{J_t} g(\mathbb{E}\left\{P_k^-\right\}|_{J_t}).\end{aligned} \tag{24}$$

From Lemma 1 and the inequality (24), if $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) < 0$ is feasible, $\mathbb{E}\{P_{k+1}^-\}$ must be bounded. The necessity part has been proved. ■

*Remark 3:* Proposition 2 provides a necessary condition and a sufficient condition on the packet loss probabilities $\lambda_i$, $1 \leq i \leq m$, to solve Problem 1. We can directly obtain a suboptimal feasible probability set $\Lambda$ by verifying the sufficient condition $r_{J_1}\rho^2(A_{U_{J_1}^-}) \geq 1$ and decreasing $\lambda_1, \lambda_2, \ldots, \lambda_m$ in sequence by fixed step from $\lambda_1 = \lambda_2 = \ldots = \lambda_m = 1$. To propose a better feasible probability set, the idea of traversal and off-line verification can be used. Firstly, by verifying $r_{J_1}\rho^2(A_{U_{J_1}^-}) < 1$ we get a probability set $\overline{\Lambda}$. Secondly, for $(\lambda_1, \lambda_2, \ldots, \lambda_m) \in \overline{\Lambda}$, when $\Omega(\lambda_1, \lambda_2, \ldots, \lambda_m) < 0$ is unfeasible, the corresponding probability vector is recorded in the solution set $\underline{\Lambda}$. By using these two steps, we can narrow the scope of traversal in the third step, in which we implement Monte Carlo simulations of the estimation process by using the probability vectors in $\underline{\Lambda}$ in sequence. When the average estimation errors have tremendous variations around a probability vector, the corresponding probability vector is recorded in the critical solution set $\Lambda$.

### *D. Probability Allocation for Special System*

In this subsection, we consider a special case and give explicit probability conditions to solve Problem 1.

*Assumption 5:* The system state consists of $r$ modes with a corresponding diagonal form of the system matrix $A$

$$x_{k+1} = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{bmatrix} x_k + v_k \tag{25}$$

where $Q = \mathrm{diag}\{Q_s, 1 \leq s \leq r\}$, $\rho(A_s) \geq 1$, and $(A_s, Q_s^{\frac{1}{2}})$ is controllable. $r$ modes of the system are measured by $r$ different types of sensors. Each sensor belongs to only one type, which observes one mode of the system state vector. Denote $O_s, s = 1, 2, \ldots, r$, as the set of sensors that can detect the $s$th mode in the system. Define $|O_s| = n_s > 0$. For any $i \in O_s$, $(A_s, C_i)$ is observable.

Because the network is collaboratively observable, the absence of some key measurements will destroy the observability of the whole network. If we attack all the sensors of one type, the network will be intermittently unobservable, which may make it difficult to obtain a uniformly bounded mean square estimation error. Based on this idea, we can give the explicit minimum number of attackers.

*Proposition 3:* For system (25) and networks satisfying Assumptions 2–5, the minimum number of attacked communication channels is $m_{\min} = \min_{1\leq s\leq r}\{n_s\}$. Once the number of attacked channels is less than $m_{\min}$, the estimation error of the estimator must be bounded in mean square sense.

*Proof:* The proof is similar to that of Proposition 1. When $m < m_{\min}$, for any mode of the system there exists at least one sensor to measure it and the network is always collectively observable, which can ensure that the estimation error of the remote estimator is bounded. ■

From the proof of Proposition 3, to minimize the attack power, it is better to place the attacks to the nodes of the same type. In the following, we will give an explicit sufficient condition and necessary condition on the packet loss probabilities to solve Problem 1.

*Proposition 4:* For system (25) and networks satisfying Assumptions 2–5, the attacker can successfully destroy the estimation of the center, if there exists a system mode $s$ $(1 \leq s \leq r)$, fix the possible attacked node set as $O_s$, the attack probabilities and attack power make the packet loss probabilities satisfy that

$$\prod_{s_i \in O_s} \lambda_i \geq \frac{1}{\rho^2(A_s)} \tag{26}$$

and only if there exists a system mode $s, 1 \leq s \leq r$, such that

$$\prod_{s_i \in O_s} \lambda_i \geq \frac{1}{\prod |\lambda^u(A_s)|^2} \tag{27}$$

where $\lambda^u(A_s)$ stands for unstable eigenvalues of $A_s$.

*Proof:* For system (25), the equation of the covariance can also be decoupled. Assume the attacked node set is $O_s$, define $P_k^{-(s)}$ as the covariance matrix corresponding to the $s$th mode, then

$$\begin{aligned}\mathbb{E}\{P_{k+1}^{-(s)} | P_k^{-(s)}\} = &\prod_{j \in O_s} \lambda_j A_s P_k^{-(s)} A_s^T + Q_s \\ &+ \sum_{J_t \subset O_s} \prod_{i \in J_t} (1-\lambda_i) \prod_{j \notin J_t} \lambda_j \Big[ A_s P_k^{-(s)} A_s^T \\ &- A_s P_k^{-(s)} C_{J_t}^T (C_{J_t} P_k^{-(s)} C_{J_t}^T + \mathcal{R}_{J_t})^{-1} \\ &\times C_{J_t} P_k^{-(s)} A_s^T) \Big].\end{aligned} \tag{28}$$

*Sufficiency:* From (28) we have that $\mathbb{E}\{P_{k+1}^{-(s)}\} \geq \prod_{j \in O_s} \lambda_j A_s \mathbb{E}\{P_k^{-(s)}\} A_s^T + Q_s$. Similar to the proof of Proposition 2, if $\prod_{s_i \in O_s} \lambda_i \geq \frac{1}{\rho^2(A_s)}$, then $\mathbb{E}\{P_k^{-(s)}\}$ is divergent.

*Necessity:* Define $\bar{P}_k^{-(s)} = \mathbb{E}\{P_k^{-(s)}\}$. From (28) and the proof of Proposition 2, we have

$$\begin{aligned}\bar{P}_{k+1}^{-(s)} \leq &\prod_{j \in O_s} \lambda_j A_s \bar{P}_k^{-(s)} A_s^T + Q_s \\ &+ (1 - \prod_{j \in O_s} \lambda_j) [A_s \bar{P}_k^{-(s)} A_s^T - A_s \bar{P}_k^{-(s)} C_{o_s}^T \\ &\times (C_{o_s} \bar{P}_k^{-(s)} C_{o_s}^T + R_{o_s})^{-1} C_{o_s} \bar{P}_k^{-(s)} A_s^T)].\end{aligned}$$

where $o_s$ denotes any one node in $O_s$, and for any $i \in O_s$, $C_i = C_{o_s}$, $R_i = R_{o_s}$.

From [31] and [32], if $\prod_{j \in O_s} \lambda_j < \dfrac{1}{\prod |\lambda^u(A_s)|^2}$, the sequence $\bar{P}_k^{-(s)}$ will be bounded. ■

*Remark 4:* For all nodes in $O_s$, it is optimal to allocate uniform packet loss probability to minimize the sum of their probabilities and guarantee the necessary condition and the sufficient condition in Proposition 4. Define $o_s$ as one node in $O_s$ and assume for $i \in O_s$, $\lambda_i = \lambda_{o_s}$. From Proposition 4 we can obtain a lower bound $\underline{\lambda}_s$ and an upper bound $\bar{\lambda}_s$ of the optimal probability $\lambda_s^*$ to make the estimation error of the estimator divergent when the node set $O_s$ is attacked, i.e., $\underline{\lambda}_s = 1/\prod |\lambda^u(A_s)|^{\frac{2}{n_s}}$, $\bar{\lambda}_s = 1/(\rho(A_s))^{\frac{2}{n_s}}$. Then, we implement Monte Carlo simulations of the estimation process by using the probabilities in $[\underline{\lambda}_s, \bar{\lambda}_s]$ in sequence and look for the critical probability $\lambda_s^*$. Although placing attacks to the minimum number of channels can reduce the cost of attack energy to a certain extent, it is not necessarily the optimal solution since the probability condition depends on the system mode $A_s$ as well. We can search an attack node set $O_{s^*}$ to minimize the sum of the packet loss probabilities $n_s \lambda_s^*$, i.e., $s^* = \arg\min_{1 \leq s \leq r} \{n_s \lambda_s^*\}$. The critical probability vector corresponding to the node set is recorded as set $\Lambda$.

In this section, an attack node set $\mathcal{V}^*$ and a universally applicable approach to finding feasible probability set $\Lambda$ have been given. In the next section, we will discuss how to design the attack probabilities and power to minimize the overall attack energy.

## IV. Optimization of Attack Parameters

In the above section, we have solved the first two steps of the stepwise solution to Problem 1. In this section, the third step, which aims at finding the minimum of $\sum_{s_i \in \mathcal{V}^*} \gamma_i \delta_i^a$ based on the first two steps, will be discussed.

From Section II-B, the probability of the packet loss on the channel is positively correlated with the attack power. We use a function $\psi(\cdot)$ to briefly represent this relationship, i.e., $p_i = \psi(\delta_i^a)$, where the form of the function $\psi(\cdot)$ can be obtained by (7)–(9). Since the DoS attacker injects attacks to the communication channel of $s_i$ with a probability $\gamma_i$ at any time step, we obtain $\lambda_i = \gamma_i p_i = \gamma_i \psi(\delta_i^a)$ accordingly.

Provided that the placement of attacks $\mathcal{V}^*$ and the feasible packet loss probability set $\Lambda$ have been given by Remark 2 and Remark 3 (or by Remark 4 for special systems), in the following we investigate the optimal attack power $\delta_i^a$ and attack probability $\gamma_i$ in the feasible packet loss probability set $\Lambda$ to minimize the attack energy $\sum_{i \in \mathcal{V}^*} \gamma_i \delta_i^a$.

Replacing $\gamma_i$ by $\lambda_i / \psi(\delta_i^a)$, the cost function $\lambda_i \delta_i^a / \psi(\delta_i^a)$ just depends on $\delta_i^a$ and Problem 1 is simplified to the following problem.

*Problem 2:*

$$\min \sum_{s_i \in \mathcal{V}^*} \frac{\lambda_i \delta_i^a}{\psi(\delta_i^a)} \tag{29}$$

$$\text{s.t.} \quad 0 \leq \frac{\lambda_i}{\psi(\delta_i^a)} \leq 1 \tag{30}$$

$$\delta_1^a \geq 0, \ldots, \delta_m^a \geq 0 \tag{31}$$

$$(\lambda_1, \ldots, \lambda_m) \in \Lambda \tag{32}$$

where the attack sensor set $\mathcal{V}^*$ is obtained by Remark 2; the set of critical probability vector $\Lambda$ is obtained by Remark 3 or Remark 4.

The packet loss probability $\lambda_i$ and attack energy depend on both $\gamma_i$ and $\delta_i^a$. We firstly give an example to show the relationships among the packet loss probability $\lambda_i$, attack power $\delta_i^a$, attack probability $\gamma_i$, and energy $\gamma_i\delta_i^a$. Define the parameters in (7) and (8) as $G_s = G_a = 1, \delta_s = 10, \sigma = 0.1$, $L = 32$. The impact of attack parameters $\gamma_i$ and $\delta_i^a$ on attack energy and packet loss probability $\lambda_i$ is shown in contour overlap sketch map in Fig. 2. Here dotted lines represent the contours of packet loss probability and solid lines represent that of attack energy. The $x$-axis indicates attack possibility $\gamma_i$ within the range from 0 to 1; the $y$-axis indicates attack power $\delta_i^a$. In Fig. 2, both the packet loss probability and attack energy decline from upper-right to lower-left. Moreover, for fixed $\lambda_i$ (represented by a red dotted line), we can always find an optimal solution $\delta_i^a$ to minimize the energy under the condition that $0 \le \lambda_i/\psi(\delta_i^a) \le 1$.

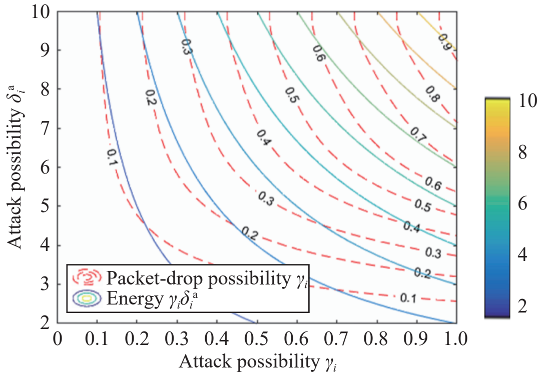


Fig. 2. Contour overlap sketch map.

*Remark 5:* To solve Problem 2, we can look for parameters to minimize $\lambda_i\delta_i^a/\psi(\delta_i^a)$ under condition (30) for fixed $\lambda_i$ and search the global optimal parameters by testing all feasible probabilities in $\Lambda$.

By solving Problem 2, the original nonlinear programming problem with high complexity and high coupling is simplified to a linear programming problem with largely reduced difficulties. Moreover, in Problem 1 two optimal coupled attack parameters for each channel should be searched while in Problem 2, just one parameter $\delta_i^a$ is required to be considered. This solution may be a suboptimal solution of Problem 1. However, the complexity in solving Problem 1 has been reduced considerably.

## V. Numerical Simulations

### A. General System

We firstly verify the effectiveness of the allocation mechanism for general systems. In this part, we consider a military gas turbine engine as the target model. In order to evaluate and monitor the state information of the engine, an on-board engine monitoring system [33] is used.

Three incompletely observable sensors send information to process center and the network parameters in (7) and (8) are given as $G_s = G_a = 1$, $\delta_s = 10$, $\sigma = 0.1$, $L = 32$. According to [33], a discrete-time model of the engine system is concerned as follows:

$$x(k+1) = \begin{bmatrix} 0.8673 & 0 & 0.2022 \\ 0.0145 & 0.9608 & -0.0316 \\ 0.0259 & 0 & 0.8032 \end{bmatrix} x(k) + \begin{bmatrix} 0.0165 \\ 0.0789 \\ -0.0177 \end{bmatrix} v_k.$$

The measurement matrices of sensors are $C_1 = [0\ 1\ 1]$, $C_2 = [1\ 1\ 0]$ and $C_3 = [0\ 0\ 1]$. Obviously, we get $\mathcal{V}^* = \{s_2\}$. The effect of attack is shown in Fig. 3. When the channel between sensor $s_2$ and the estimator is attacked by the attacker, the estimation error increases largely.

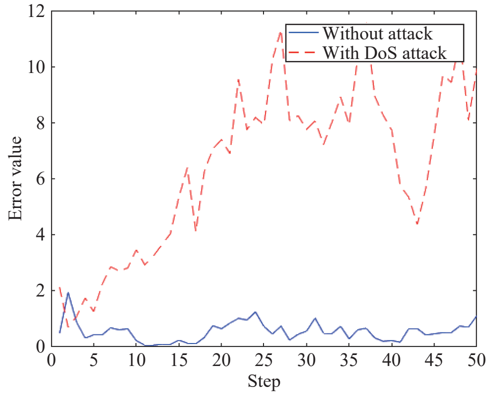


Fig. 3. Estimation errors with and without DoS attack: engine monitoring system.

When the system has an unstable eigenvalue, the same attack results in more lethal effect. When $A = \begin{bmatrix} 1.0890 & 0 & 0.2022 \\ 0.0145 & 0.9608 & -0.0316 \\ 0.0259 & 0 & 0.8032 \end{bmatrix}$, according to Proposition 2, $\lambda \ge 0.8234$ is obtained. The optimal solution for attack energy is then obtained with $\gamma = 1, \delta^a = 7.5325$. Meanwhile, the traces of the estimation error covariance matrices with and without DoS attack are shown in Fig. 4. Obviously, the attack strategy is effective.

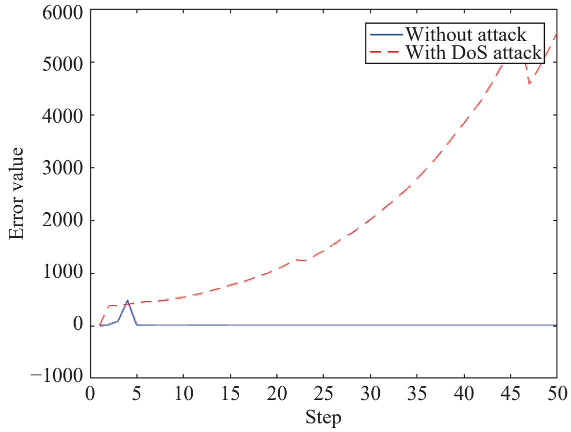


Fig. 4. Estimation errors with and without DoS attack: general unstable case.

### B. Special System

In this subsection, we consider a system with diagonal form and there are 4 incompletely observable sensors sending information to the process center through communication channels, where the monitoring process of the smart grid is studied. In the smart grid, some separate self-generating areas can be regarded as independent power agents ([21]). The system is $A=\begin{bmatrix}1.01 & 0.1136 & 0 & 0\\ 0 & 0.3825 & 0 & 0\\ 0 & 0 & 0.4237 & 0.5346\\ 0 & 0 & 0 & 1.5\end{bmatrix}$ and the sample time is $T=0.1$s. Each mode of the system state represents the power distribution of an agent, which is detected by a sensor, and there are couplings between agents. Sensor $s_i$ is only available to agent $i$. For simple expression, four state components $x_k(i), 1\le i\le 4$, respectively stand for the power distributions of agents 1, 2, 3 and 4.

The system has two diagonal blocks, thus we easily get $m_{\min}=2$ based on Proposition 3. $\mathcal{O}_1=\{s_1,s_2\}$ and $\mathcal{O}_2=\{s_3,s_4\}$.

From Proposition 4, we obtain the optimal packet loss probability $\lambda_3^*=\lambda_4^*=1/1.4692$ with $\mathcal{V}^*=\mathcal{O}_2$. By solving Problem 2, the optimal attack parameters are $\gamma_3=\gamma_4=1, \delta_3^a=\delta_4^a=7.6821$, respectively. It is noteworthy that if we choose $\mathcal{V}=\mathcal{O}_1$, more attack energy will be consumed with $\gamma_1=\gamma_2=1, \delta_1^a=\delta_2^a=8.4678$. The traces of the estimation error matrices with existence and absence of DoS attack are shown in Fig. 5. It is shown that the proposed attack scheme deteriorates the estimation performance.

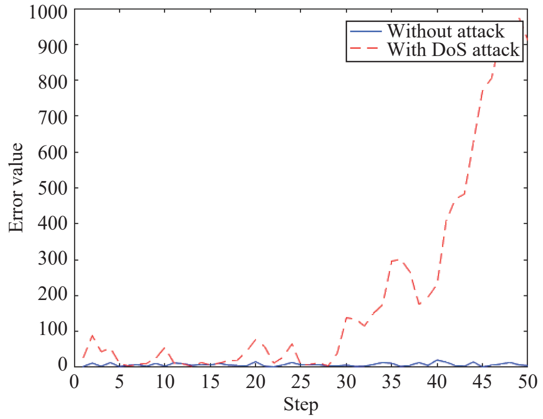


Fig. 5. Estimation errors with and without DoS attack: special case.

## VI. Conclusions

In this paper, a suboptimal stochastic DoS attack mechanism is designed to destroy the centralized state estimation in wireless sensor networks, which makes the estimation error of the system unbounded with minimum energy consumption. The mechanism is composed of three steps, where the attack node set, the feasible induced packet loss probability set, and the attack probabilities and power are proposed in sequence. This paper focuses on attack management in centralized estimation networks. How to place attacks in distributed estimation networks and delayed networks is of our research interest in future.

## References

[1] X. M. Zhang, Q. L. Han, X. H. Ge, D. R. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 1, pp. 1–17, Jan. 2020.

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

[3] I. Bahceci and A. K. Khandani, "Linear estimation of correlated data in wireless sensor networks with optimum power allocation and analog modulation," *IEEE Trans. Commun.*, vol. 56, no. 7, pp. 1146–1156, Jul. 2008.

[4] Y. L. Mo, R. Ambrosino, and B. Sinopoli, "Sensor selection strategies for state estimation in energy constrained wireless sensor networks," *Automatica*, vol. 47, no. 7, pp. 1330–1338, Jul. 2011.

[5] G. Battistelli, L. Chisci, G. Mugnai, A. Farina, and A. Graziano, "Consensus-based linear and nonlinear filtering," *IEEE Trans. Autom. Control*, vol. 60, no. 5, pp. 1410–1415, May 2015.

[6] X. X. Guo, A. S. Leong, and S. Dey, "Estimation in wireless sensor networks with security constraints," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 2, pp. 544–561, Apr. 2017.

[7] Y. Zhang and Y. P. Tian, "A fully distributed weight design approach to consensus Kalman filtering for sensor networks," *Automatica*, vol. 104, pp. 34–40, Jun. 2019.

[8] Y. L. Zou, J. Zhu, X. B. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[9] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*, R. Majumdar and P. Tabuada, Eds. Heidelberg, Germany: Springer, 2009, pp. 31-45.

[10] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.

[11] J. Milosevic, T. Tanaka, H. Sandberg, and K. H. Johansson, "Analysis and mitigation of bias injection attacks against a Kalman filter," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8393–8398, Jul. 2017.

[12] D. W. Shi, R. J. Elliott, and T. W. Chen, "On finite-state stochastic modeling and secure estimation of cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 65–80, Jan. 2017.

[13] B. Chen, D. W. C. Ho, G. Q. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE Trans. Cybern.*, vol. 48, no. 6, pp. 1862–1876, Jun. 2018.

[14] B. Chen, D. W. C. Ho, W. A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 49, no. 2, pp. 455–468, Feb. 2019.

[15] Q. Y. Liu, Z. D. Wang, X. He, and D. H. Zhou, "Event-based recursive distributed filtering over wireless sensor networks," *IEEE Trans. Autom. Control*, vol. 60, no. 9, pp. 2470–2475, Sep. 2015.

[16] W. Yang, L. Lei, and C. Yang, "Event-based distributed state estimation under deception attack," *Neurocomputing*, vol. 270, pp. 145–151, Dec. 2017.

[17] A. S. Leong, S. Dey, and D. E. Quevedo, "Transmission scheduling for remote state estimation and control with an energy harvesting sensor," *Automatica*, vol. 91, pp. 54–60, May 2018.

[18] F. X. Wen and Z. M. Wang, "Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks," *Digit. Signal Process.*, vol. 78, pp. 92–97, Jul. 2018.

[19] Y. P. Guan and X. H. Ge, "Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks," *IEEE Access*, vol. 5, pp. 10858–10870, Jun. 2017.

[20] X. H. Ge, Q. L. Han, M. Y. Zhong, and X. M. Zhang, "Distributed

Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, pp. 108557, Nov. 2019.

[21] S. Y. Xiao, Q. L. Han, X. H. Ge, and Y. J. Zhang, "Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 3, pp. 1220–1229, Mar. 2020.

[22] D. J. Du, X. Li, W. T. Li, R. Chen, M. R. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Trans. Syst.*, *Man*, *Cybern.*: *Syst.*, vol. 49, no. 8, pp. 1698–1711, Aug. 2019.

[23] J. H. Qin, M. L. Li, L. Shi, and X. H. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.

[24] K. M. Ding, Y. Z. Li, D. E. Quevedo, S. Dey, and L. Shi, "A multi-channel transmission schedule for remote state estimation under DoS attacks," *Automatica*, vol. 78, pp. 194–201, Apr. 2017.

[25] X. H. Cao and C. Y. Sun, "Probabilistic denial of service attack against remote state estimation over a Markov channel in cyber-physical systems," in *Proc. 11th Asian Control Conf.*, Gold Coast, Australia, 2017, 17–20.

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

[27] H. Zhang, P. Cheng, L. Shi, and J. M. Chen, "Optimal Denial-of-Service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[28] H. Zhang, Y. F. Qi, J. F. Wu, L. K. Fu, and L. D. He, "DoS attack energy management against remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 383–394, Mar. 2018.

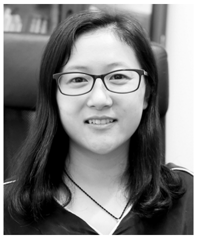
[29] C. Yang, W. Yang, and H. B. Shi, "DoS attack in centralised sensor network against state estimation," *IET Control Theory Appl.*, vol. 12, no. 9, pp. 1244–1253, Jun. 2018.

[30] R. A. Poisel, *Modern Communications Jamming: Principles and Techniques*. Norwood, USA: Artech House, 2011.

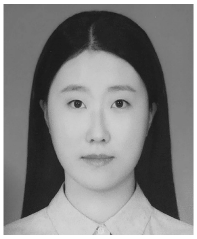
[31] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1453–1464, Sep. 2004.

[32] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[33] R. W. Eustace, B. A. Woodyatt, G. L. Merrington, and A. Runacres, "Fault signatures obtained from fault implant tests on an F404 engine," *J. Eng. Gas Turbines Power*, vol. 116, no. 1, pp. 178–183, Jan. 1994.



**Ya Zhang** (M'14) received the B.S. degree in applied mathematics from China University of Mining and Technology in 2004, and Ph.D. degree in control engineering from Southeast University, in 2010. Since 2010, she has been with Southeast University, where she is currently a Professor with the School of Automation. Her research interests include cooperative control and estimation, multi-agent systems, and network security.



**Lishuang Du** received her B.S. degree in automation from Southeast University in 2017. She is currently a graduate student at the School of Automation, Southeast University, Her major research interests include sensor networks and secure estimation.

**Frank L. Lewis** (F'94) received the bachelor degree in physics/electrical engineering and the master of electrical engineering degree at Rice University in 1971. He spent six years in the U.S. Navy, serving as Navigator aboard the frigate USS Trippe (FF-1075), and Executive Officer and Acting Commanding Officer aboard USS Salinan (ATF-161). In 1977 he received the master of science in aeronautical engineering from the University of West Florida. In 1981 he received the Ph.D. degree at the Georgia Institute of Technology in Atlanta, where he was employed as a Professor from 1981 to 1990. He is Moncrief-O'Donnell Endowed Chair Professor of Electrical Engineering at the University of Texas at Arlington. He is a Qian Ren Thousand Talents Consulting Professor with Northeastern University, Shenyang, China. His current interests include intelligent control, distributed cooperative control on graphs, nonlinear systems, reinforcement learning, process control, and neurobiological systems. Author of 7 U.S. patents, 420 journal papers, 52 chapters and encyclopedia articles, 420 refereed conference papers, and 20 books. Dr. Lewis is a member of the National Academy of Inventors, Fellow of the IEEE, Fellow of IFAC, Fellow of the U.K. Institute of Measurement & Control, Fellow American Association for the Advancement of Sciences, Member of the New York Academy of Sciences. Registered Professional Engineer in the State of Texas and Chartered Engineer, U.K. Engineering Council. Ranked at position 89 worldwide, 64 in the USA, and 3 in Texas of all scientists in Computer Science and Electronics, by Guide2Research (June 2019). 55 500 google citations, h-index 107. Charter Member (2004) of the UTA Academy of Distinguished Scholars. UTA Academy of Distinguished Teachers 2012. IEEE Control Systems Society Distinguished Lecturer 2012–1014. Founding Member of the Board of Governors of the Mediterranean Control Association. Served as Visiting Professor at Democritus University in Greece, Hong Kong University of Science and Technology, Chinese University of Hong Kong, City University of Hong Kong, National University of Singapore, and Nanyang Technological University Singapore.