Optimal Hybrid Attacks Scheduling on Remote State Estimation with Energy Constraint

Shilin Xu[1], Ying Wan[1(✉)], Guohua Liu[1], and Mengfei Niu[2]

[1] School of Mathematics, Southeast University, Nanjing 211189, China
wan_ying@seu.edu.cn
[2] School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China

Abstract. This paper investigates optimal scheduling for hybrid attacks on remote state estimation in the sense of maximizing system average error with energy constraint. Hybrid attacks considered are composed of DoS (Denial-of-Service) attack and stealthy attack. After analyzing average error under several particular types of strategies, optimal hybrid attacks scheduling is determined theoretically. The numerical results are presented to verify our theoretical results.

Keywords: Stealthy attack · DoS attack · Optimal attack scheduling · Remote state estimation · Energy constraint

1 Introduction

Cyber-Physical System (CPS) is a practical but complex system integrating networking, computing, sensors and physical environment. Application scenarios of CPS have broad prospects, such as smart grid, intelligent transportation, healthcare system, industrial process, etc. However, in CPS, sensors and wireless channels are vulnerable to malicious attacks. CPS security problem has become a hot research topic in recent years [1–5].

Generally, common malicious attacks include DoS attacks and stealthy attacks. DoS attacks degrade system performance by blocking packets in wireless transmission channels. In [6], security estimation subject to DoS attack was considered in CPS. To mitigate the impact of DoS attack for cyber-physical system, a resilient model predictive control (MPC) framework was provided in [7]. In [8,9], authors were concerned with information fusion of the remote estimator under DoS attack.

On the other hand, stealthy attacks degrade system estimation performance by tampering with packets. In [10], the optimal deception attack was investigated. The Kullback-Leibler divergence is adopted to detect system abnormalities and a linear attack plan was considered in [11]. Further, an encryption-based counter-measure against stealthy attack was proposed in [12].

Z. Ren et al. (Eds.): *Proceedings of 2021 5th Chinese Conference on Swarm Intelligence and Cooperative Control*, LNEE 934, pp. 802–812, 2023.
https://doi.org/10.1007/978-981-19-3998-3_77

In practice, malicious attackers have only limited energy, which will affect their attack policies. Authors in [13,14] studied the optimal DoS attack schedules in the case of energy constraints. In [15], the optimal stealthy attack schedule was also considered. However, as far as we know, the existing literature did not consider hybrid attacks to evaluate the optimal attack schedule, which mainly motivates this paper. The main contributions are summarized as follows:

(1) The impacts of different scheduling of hybrid attacks on system performance are analyzed.
(2) Based on the detailed analysis for several scheduling of stealthy attacks and DoS attacks, we give the optimal hybrid attacks scheduling theoretically.

The remainder of this paper is organized as follows: Sect. 2 introduces the system model and attack strategies. Section 3 derives the optimal hybrid attacks scheduling. Section 4 presents simulations to verify the effectiveness of the derived results. Finally, conclusions are drawn in Sect. 5.

2 Problem Formulation

2.1 System Model

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

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

where $k \in \mathbb{N}$ is the time index, $x_k \in \mathbb{R}^{n_x}$ is the vector of system state, $y_k \in \mathbb{R}^{n_y}$ represents sensor measurement, $w_k \in \mathbb{R}^{n_x}$ and $v_k \in \mathbb{R}^{n_y}$ are zero-mean i.i.d Gaussian noises with covariances $\mathbb{E}[w_i w_j^T] = \delta_{ij} Q \geq 0$, $\mathbb{E}[v_i v_j^T] = \delta_{ij} R > 0$ and $\mathbb{E}[w_i v_j^T] = 0$ for $\forall i, j$, respectively. The initial state x_0 is zero-mean Gaussian with covariance matrix $\Pi_0 \geq 0$, and is independent of w_k and v_k for all $k \geq 0$. Besides, the pair (A, C) is detectable and $(A, \sqrt{Q})$ is stabilizable.

2.2 Attack Strategy

Two common attack types, DoS attacks and stealthy attacks, are considered respectively.

Type 1 (Stealthy Attack): The smart sensor provides computation function in CPS, which has the ability to process the measurement y_k at each time step and sends its innovation term to the remote state estimator via a wireless network. In order to accurately estimate the actual state of the system, a standard Kalman filter equipped at the remote estimator to estimate system state, the specific form is as follows

$$\begin{aligned}
\hat{x}_k^- &= A\hat{x}_{k-1} \\
P_k^- &= AP_{k-1}A^T + Q \\
K_k &= P_k^- C^T (CP_k^- C^T + R)^{-1} \\
\hat{x}_k &= \hat{x}_k^- + K_k z_k \\
P_k &= (I - K_k C)P_k^-
\end{aligned} \tag{3}$$

where $\hat{x}_k^-$ and $\hat{x}_k$ represent a priori and a posterior estimations of the real system state, respectively. P_k^- and P_k are the corresponding error covariances for $\hat{x}_k^-$ and $\hat{x}_k$, respectively. The recursion starts from $\hat{x}_0^-$ and $P_0^- = \Omega_0 \geq 0$. The innovation term z_k is expressed as

$$z_k = y_k - C\hat{x}_k^- \tag{4}$$

For notation brevity, define the Lyapubov and Riccati operators h, $\tilde{g}$: $\mathbb{S}_+^n \to \mathbb{S}_+^n$ as

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

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

As we all know, the convergence rate of the Kalman filter is exponential under any initial conditions. Since the steady-state error covariance is defined as

$$\bar{P} = \lim_{k \to +\infty} P_k^- \tag{7}$$

where $\bar{P}$ is the unique positive semi-definite solution of $h \circ \tilde{g}(X) = X$. For convenience, we assume that Kalman filter starts from a steady state, i.e., $\Omega_0 = \bar{P}$, which results in a steady-state Kalman filter with fixed gain

$$K = \bar{P}C^T(C\bar{P}C^T + R)^{-1} \tag{8}$$

At every time step k, the general attack strategy can be expressed as

$$\tilde{z}_k = f_k(z_k) \tag{9}$$

where $z_k \in \mathbb{R}^{n_y}$ is the real innovation term in the current system, $\tilde{z}_k \in \mathbb{R}^{n_y}$ is the innovation term modified by the attacker, and $f_k : \mathbb{R}^{n_y} \longrightarrow \mathbb{R}^{n_y}$ is an arbitrary function designed by the attacker for specific attack aims. However, for any nonlinear function f_k, it is hard for us to analyze the statistical characteristics of $\tilde{z}_k$, so it is complicated for the attacker to keep the attack signals stealthy. Hence, we focus on linear stealthy attack scenario, i.e., $\tilde{z}_k = T_k z_k + b_k$.

To facilitate the subsequent analysis, the following lemmas are first given.

Lemma 1 ([10]). *If the considered system (1) and (2) under the linear stealthy attack, the optimal stealthy attack strategy is $T_k = -I$ and $b_k = 0$ at every time instant k, which yields the largest estimated error covariance.*

Lemma 1 illustrates how to design linear attacks that can evade detectors while maximizing the estimated performance of the system.

Lemma 2 ([15]). *When the attacker did not launch a stealthy attack, i.e., $\tilde{z}_k = z_k$, the error covariance has the following recursive form*

$$P_k = AP_{k-1}A' + Q - \Theta \tag{10}$$

Otherwise, i.e., $\tilde{z}_k = -z_k$, the corresponding error covariance follows the recursion as

$$P_k = AP_{k-1}A' + Q + 3\Theta \tag{11}$$

where $\Theta = \bar{P}C'(C\bar{P}C' + R)^{-1}C\bar{P}$.

From Lemma 2, we can obtain the recursive rules for estimated error covariance with or without stealthy attacks.

Type 2 (DoS Attack): Consider the existence of DoS attacks in wireless networks, attackers obtain and intercept the innovation term z_k. Denote $\mathscr{D}_k^d$ as the DoS attacker's decision at time k, i.e.,

$$\mathscr{D}_k^d = \begin{cases} 1, & \text{system is attacked by the DoS attack at time } k \\ 0, & \text{otherwise} \end{cases}$$

At the same time, variable $\theta_k = 1$ or 0 is defined to indicate whether the remote estimator receives the innovation term successfully or not at every time instant k. It is well known that θ_k only depends on whether the DoS attack occur at the current time since we assume θ_k satisfies an independent Bernoulli process with

$$\mathbb{E}[\theta_k = 1|\mathscr{D}_k^d = 1] = 1 - \alpha \ \ , \mathbb{E}[\theta_k = 1|\mathscr{D}_k^d = 0] = 1 \tag{12}$$

where $\alpha \in [0, 1]$. For simplicity, it is assumed that as long as the DoS attack is launched, the innovation term z_k must be intercepted, i.e., $\mathbb{E}[\theta_k = 0|\mathscr{D}_k^d = 1] = 1$.

Remark 1. In some existing literatures, a posteriori estimation is sent from the smart sensor to the remote estimator, and it is easy to model error covariance at the remote estimator as MDP. However, in this work, the smart sensor only sends the innovation term z_k, and remote estimator needs to do both the Kalman filter prediction step and the correction step. Therefore, the MDP method commonly used in existing literature is not applicable to this paper.

2.3 Problems of Interest

Consider the optimal hybrid attacks scheduling in a finite horizon T, which aim to degrade the remote estimator's estimated performance. Denote $\mathscr{D} \triangleq [\mathscr{D}_1, \mathscr{D}_2, \cdots, \mathscr{D}_T]$ as the attacker's decision schedule, that is,

$$\mathscr{D}_k = \begin{cases} 1, & \text{attacker decides to launch a DoS attack or stealthy attack at time } k \\ 0, & \text{otherwise} \end{cases}$$

Obviously, if there is no energy limit, the attacker can choose to attack the system all the time, thereby reducing the estimated performance of the system. Whereas, in a real attack environment, the attacker only has limited energy due to various factors, such as computing power, battery power, etc. Then, the attacker has to choose the optimal scheduling to attack the system under limited energy. Therefore, we assume that stealthy attacks and DoS attacks have the same attacks times n.

Next, for a given attack schedule $\mathscr{D}$, average error is introduced to reflect system performance, i.e.,

$$\mathcal{J}_a(\mathscr{D}) = \frac{1}{T}\sum_{k=1}^{T} P_k(\mathscr{D}) \tag{13}$$

where $P_k(\mathscr{D})$ represents the estimated error covariance of the remote state estimator at every time k under a given stealthy attack strategy $\mathscr{D}$.

From the perspective of the attacker, due to the limitation of its own energy, attacker has to design optimal hybrid attacks scheduling in the sense that it yields the largest estimated error covariance, which could be formulated as the following optimization problem.

Problem 1

$$\max_{\mathscr{D}\in\mathcal{D}} Tr[\mathcal{J}_a(\mathscr{D})]$$
$$s.t. \begin{cases} \sum\limits_{k=1}^{T} \mathscr{D}_k = 2n \\ \sum\limits_{k=1}^{T} \mathscr{D}_k^s = \sum\limits_{k=1}^{T} \mathscr{D}_k^d = n \end{cases}$$

where binary variable $\mathscr{D}_k^s$ denotes whether the attacker launch a stealthy attack at time k and $\mathcal{D}$ is the set of all possible attack schedules, i.e., $\mathcal{D} = \underbrace{\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}}_{T\ times}$.

3 Optimal Hybrid Attacks Schedules Analysis

In this section, the optimal hybrid attacks scheduling for maximizing the trace of the average error is explored.

3.1 Preliminaries

Firstly, some useful lemmas are given for the subsequent analysis.

Lemma 3. *For any initial error covariance P^s and the total attack interval length M, assume that the number of stealthy attack and DoS attack are M_1 and M_2 respectively, where $M_1 + M_2 = M$ and $M_1 = M_2$. Then, performing stealthy attacks first and then DoS attacks will result in a larger average error.*

Proof. Assume that the initial time T_0 and corresponding error covariance is P^s. The following two cases will be analyzed.

Case 1): When $T_0 < k \leq T_0 + M_1$, the attacker launchs stealthy attacks. When $T_0 + M_1 < k \leq T_0 + M_1 + M_2$, the attacker launchs DoS attacks.

Case 2): When $T_0 < k \leq T_0 + M_2$, the attacker launchs DoS attacks. When $T_0 + M_2 < k \leq T_0 + M_1 + M_2$, the attacker launchs stealthy attacks.

For case 1, when $T_0 < k \leq T_0 + M_1$, the error covariance at time k is

$$P_k = A^{k-T_0} P^s (A')^{k-T_0} + \sum_{i=0}^{k-T_0-1} A^i Q (A')^i + 3 \sum_{i=0}^{k-T_0-1} A^i \Theta (A')^i \tag{14}$$

When $T_0 + M_1 < k \leq T_0 + M_1 + M_2$, the error covariance at time k is

$$P_k = A^{k-T_0-M_1} P_{T_0+M_1} (A')^{k-T_0-M_1} + \sum_{i=0}^{k-T_0-M_1-1} A^i Q (A')^i \tag{15}$$

where $P_{T_0+M_1} = A^{M_1} P^s (A')^{M_1} + \sum_{i=0}^{M_1-1} A^i Q (A')^i + 3 \sum_{i=0}^{M_1-1} A^i \Theta (A')^i$.

For case 2, when $T_0 < k \leq T_0 + M_2$, the error covariance at time instant k is

$$P_k = A^{k-T_0} P^s (A')^{k-T_0} + \sum_{i=0}^{k-T_0-1} A^i Q (A')^i \tag{16}$$

when $T_0 + M_2 < k \leq T_0 + M_1 + M_2$, the error covariance at time instant k is

$$P_k = A^{k-T_0-M_2} P_{T_0+M_2} (A')^{k-T_0-M_2} + \sum_{i=0}^{p} A^i Q (A')^i + 3 \sum_{i=0}^{p} A^i \Theta (A')^i \tag{17}$$

where $p = k - T_0 - M_2 - 1$, $P_{T_0+M_2} = A^{M_2} P^s (A')^{M_2} + \sum_{i=0}^{M_2-1} A^i Q (A')^i$.

According to the conditions of Lemma 3,

$$P_{T_0+M_1} - P_{T_0+M_2} = 3 \sum_{i=0}^{M_1-1} A^i \Theta (A')^i$$

Hence, we have

$$\begin{aligned} \mathcal{J}_a(case1) - \mathcal{J}_a(case2) &= \tfrac{1}{M} [\sum_{i=1}^{M_2} A^i (P_{T_0+M_1} - P^s)(A')^i \\ &\quad + \sum_{i=1}^{M_1} A^i (P^s - P_{T_0+M_2})(A')^i] \\ &= \tfrac{1}{M} \sum_{i=1}^{M_1} A^i (P_{T_0+M_1} - P_{T_0+M_2})(A')^i \end{aligned} \tag{18}$$

Note that $\Theta = \bar{P}C'(C\bar{P}C' + R)^{-1} C\bar{P} \geq 0$ and $P_{T_0+M_1} - P_{T_0+M_2} \geq 0$, then we get $J_a(case1) - J_a(case2) \geq 0$. The proof is thus completed.

Next, we consider the characteristics of the following attack strategies

$$\begin{cases} \phi = (\mathcal{F}^{d}, \mathcal{A}^{k_1^s}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s}, ..., \mathcal{A}^{k_s^s}, \mathcal{F}^{d_s}). \\ \phi_0 = (\mathcal{F}^{d}, \mathcal{A}^{k_1^s+1}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s-1}, ..., \mathcal{A}^{k_s^s}, \mathcal{F}^{d_s}). \\ \phi_1 = (\mathcal{F}^{d-1}, \mathcal{A}^{k_1^s}, \mathcal{F}^{d_1+1}, \mathcal{A}^{k_2^s}, ..., \mathcal{A}^{k_s^s}, \mathcal{F}^{d_s}). \\ \phi_2 = (\mathcal{F}^{d}, \mathcal{A}^{k_1^d+1}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^d-1}, ..., \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s}). \\ \phi_3 = (\mathcal{F}^{d-1}, \mathcal{A}^{k_1^d}, \mathcal{F}^{d_1+1}, \mathcal{A}^{k_2^d}, ..., \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s}). \end{cases} \tag{19}$$

where $\mathcal{A}^{k_i^s}$ is the ith continuous stealthy attacks sequence of length $k_i^s > 0$, $i = 1, 2, \cdots, s$, $\mathcal{A}^{k_i^d}$ is the ith continuous DoS attacks sequence of length $k_i^d > 0$, $i = 1, 2, \cdots, s$. $\mathcal{F}^{d}$ and $\mathcal{F}^{d_j}$, respectively, denote the first and the $(j+1)$th consecutive sequence, in which no attack of length d_j is launched, where $d_j \geq 1, j = 1, 2, ..., s-1, d \geq 0$ and $d_s \geq 0$.

Lemma 4 [15]**.** *For the definition $\mathcal{J}_a$ in (13), and the definition ϕ, ϕ_0, ϕ_1 in (19), we can obtain*

$$(1)\ \mathcal{J}_a(\phi) \leq \mathcal{J}_a(\phi_0); \quad (2)\ \mathcal{J}_a(\phi) \leq \mathcal{J}_a(\phi_1)$$

Lemma 5. *For the definition $\mathcal{J}_a$ in (13), and the definition ϕ, ϕ_2, ϕ_3 in (19), we can obtain*

$$(1)\ \mathcal{J}_a(\phi) \leq \mathcal{J}_a(\phi_2); \quad (2)\ \mathcal{J}_a(\phi) \leq \mathcal{J}_a(\phi_3)$$

Proof. Similar to the proof of Lemma 3, omitted.

3.2 Optimal Hybrid Attacks Scheduling

An attack scheme with $2n$ launched DoS and stealthy attacks, can be denoted by

$$(\mathcal{F}^{d}, \mathcal{A}^{k_1^s}, \mathcal{A}^{k_1^d}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s}, \mathcal{A}^{k_2^d}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s}) \tag{20}$$

where $\sum_{i=1}^{s}(k_i^s) = \sum_{i=1}^{s}(k_i^d) = n$, $k_i^s = k_i^d$ and $d + \sum_{j=1}^{s} d_j = T - 2n$. Obviously, when $d_1 = 0$, a continuous attack sequence of length $k_1 + k_2$ can be obtained. Hence, $d_j \geq 1, j = 1, 2, .., s-1$ are needed, i.e.

$$(\underbrace{0, \cdots, 0}_{d\ times}, \underbrace{1, \cdots, 1}_{k_1^s\ times}, \underbrace{1, \cdots, 1}_{k_1^d\ times}, 0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_s^s\ times}, \underbrace{1, \cdots, 1}_{k_s^d\ times}, \underbrace{0, \cdots, 0}_{d_s\ times}),$$

For Problem 1, We constructed three special types of attack strategies as

$$\begin{cases} \pi = (\mathcal{F}^{d}, \mathcal{A}^{k_1^s}, \mathcal{A}^{k_1^d}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s}, \mathcal{A}^{k_2^d}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s}) \\ \pi_1 = (\mathcal{F}^{d}, \mathcal{A}^{k_1^s+1}, \mathcal{A}^{k_1^d+1}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s-1}, \mathcal{A}^{k_2^d-1}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s}) \\ \pi_2 = (\mathcal{F}^{d-1}, \mathcal{A}^{k_1^s}, \mathcal{A}^{k_1^d}, \mathcal{F}^{d_1+1}, \mathcal{A}^{k_2^s}, \mathcal{A}^{k_2^d}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s}) \end{cases} \tag{21}$$

Then, Theorem 1 is given to compare average error $\mathcal{J}_a$ under different attack strategies π, π_1 and π_2.

Theorem 1. *For the definition $\mathcal{J}_a$ in (13), and the definition π, π_1, π_2 in (21), we can obtain*

(1) $\mathcal{J}_a(\pi) \leq \mathcal{J}_a(\pi_1)$
(2) $\mathcal{J}_a(\pi) \leq \mathcal{J}_a(\pi_2)$

Proof. A direct result from Lemma 3, Lemma 4 and Lemma 5.

In Theorem 2, optimal hybrid attacks scheduling is provided.

Theorem 2. *The optimal hybrid attacks scheduling in the sense of maximizing average error, i.e., the solution to Problem 1, is*

$$\mathscr{D}_* = (\underbrace{1,1,\cdots 1}_{n \text{ times stealthy attacks}}, \underbrace{1,1,\cdots 1}_{n \text{ times Dos attacks}}, \underbrace{0,0,\cdots 0}_{T-2n \text{ times}}) \tag{22}$$

Proof. For any attack strategy, which can be expressed by (20), where d, k_i^s, k_i^d, d_i, $i = 1, 2, \cdots, s$ are determined by $\mathscr{D}$. By (1) of Theorem 1, we have

$$\begin{aligned}
&\mathcal{J}_a(D)\\
&\leq \mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{k_1^s+1}, \mathcal{A}^{k_1^d+1}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s-1}, \mathcal{A}^{k_2^d-1}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s})\\
&\leq \mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{k_1^s+2}, \mathcal{A}^{k_1^d+2}, \mathcal{F}^{d_1}, \mathcal{A}^{k_2^s-2}, \mathcal{A}^{k_2^d-2}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s})\\
&\leq \cdots\\
&\leq \mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{k_1^s+k_2^s}, \mathcal{A}^{k_1^d+k_2^d}, \mathcal{F}^{d_1+d_2}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s})\\
&\leq \cdots\\
&\leq \mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{k_1^s+k_2^s+k_3^s}, \mathcal{A}^{k_1^d+k_2^d+k_3^d}, \mathcal{F}^{d_1+d_2+d_3}, \cdots, \mathcal{A}^{k_s^s}, \mathcal{A}^{k_s^d}, \mathcal{F}^{d_s})\\
&\leq \cdots\\
&\leq \mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{\sum_{i=1}^s k_i^s}, \mathcal{A}^{\sum_{i=1}^s k_i^d}, \mathcal{F}^{\sum_{i=1}^s d_i})
\end{aligned} \tag{23}$$

Next, according to (2) of Theorem 1, we can further obtain

$$\begin{aligned}
&\mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{\sum_{i=1}^s k_i^s}, \mathcal{A}^{\sum_{i=1}^s k_i^d}, \mathcal{F}^{\sum_{i=1}^s d_i})\\
&\leq \mathcal{J}_a(\mathcal{F}^{d-1}, \mathcal{A}^{\sum_{i=1}^s k_i^s}, \mathcal{A}^{\sum_{i=1}^s k_i^d}, \mathcal{F}^{\sum_{i=1}^s d_i+1})\\
&\leq \cdots\\
&\leq \mathcal{J}_a(\mathcal{A}^{\sum_{i=1}^s k_i^s}, \mathcal{A}^{\sum_{i=1}^s k_i^d}, \mathcal{F}^{\sum_{i=1}^s d_i+d}) = J_a(\mathscr{D}_*)
\end{aligned} \tag{24}$$

Combining (23) and (24) yields that

$$\begin{aligned}
\mathcal{J}_a(\mathscr{D}) &\leq \mathcal{J}_a(\mathcal{F}^d, \mathcal{A}^{\sum_{i=1}^s k_i^s}, \mathcal{A}^{\sum_{i=1}^s k_i^d}, \mathcal{F}^{\sum_{i=1}^s d_i})\\
&\leq \mathcal{J}_a(\mathcal{A}^{\sum_{i=1}^s k_i^s}, \mathcal{A}^{\sum_{i=1}^s k_i^d}, \mathcal{F}^{\sum_{i=1}^s d_i+d})
\end{aligned} \tag{25}$$

Therefore, $\mathscr{D}_*$ defined in (22) is the optimal hybrid attacks scheduling maximizes the system error covariance. The proof of Theorem 2 is completed.

4 Simulations

In this section, the theoretical results of this paper are verified through some examples.

Consider system (1) and (2) and set system parameters as: $A = 0.8, C = 1.2, Q = R = 0.8$. Set the finite time horizon $T = 100$, and stealthy attacks and DoS attacks times $n = 15$. Then, the steady error covariance can be obtained as $\bar{P} = 1.0311$. From Theorem 2, the optimal hybrid attacks scheduling to maximize average error defined (13) is $(\mathcal{A}_s^{15}, \mathcal{A}_d^{15}, \mathcal{F}^{70})$. We simulate average error under different hybrid attack strategies and compare average error in Table 1. According to Table 1, it can be observed that the optimal attacks scheduling proposed in this work achieves the maximum attack effect.

To illustrate the impact of our proposed optimal hybrid attacks scheduling on the system, we simulate the remote state estimate for following scenarios: 1) The optimal hybrid attacks scheduling; 2) The standard Kalman filter; and depict them in Fig. 1. From Fig. 1, we see that when the attack occurs, the state estimate quickly diverges and deviates from the system state, and when the attack ends, it can converge to the true value in a short time. Besides, we also

Table 1. Comparison of average error under different schedules

Attack schedules	Average error
$(\mathcal{A}_s^{15}, \mathcal{A}_d^{15}, \mathcal{F}^{70})$	316.0735
$(\mathcal{A}_d^{15}, \mathcal{A}_s^{15}, \mathcal{F}^{70})$	109.3482
$(\mathcal{A}_s^{15}, \mathcal{F}^{70}, \mathcal{A}_d^{15})$	184.6129
$(\mathcal{A}_s^{10}, \mathcal{A}_d^{10}, \mathcal{F}^{30}, \mathcal{A}_s^{5}, \mathcal{A}_d^{5}, \mathcal{F}^{50})$	19.3039

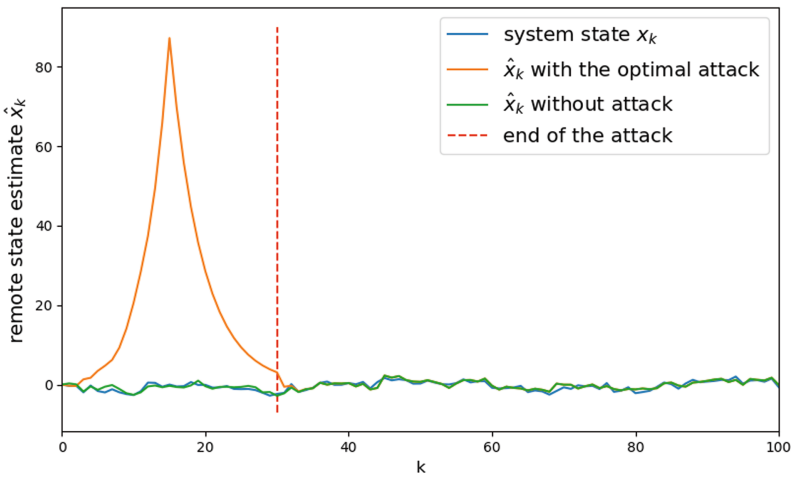

Fig. 1. Remote state estimate

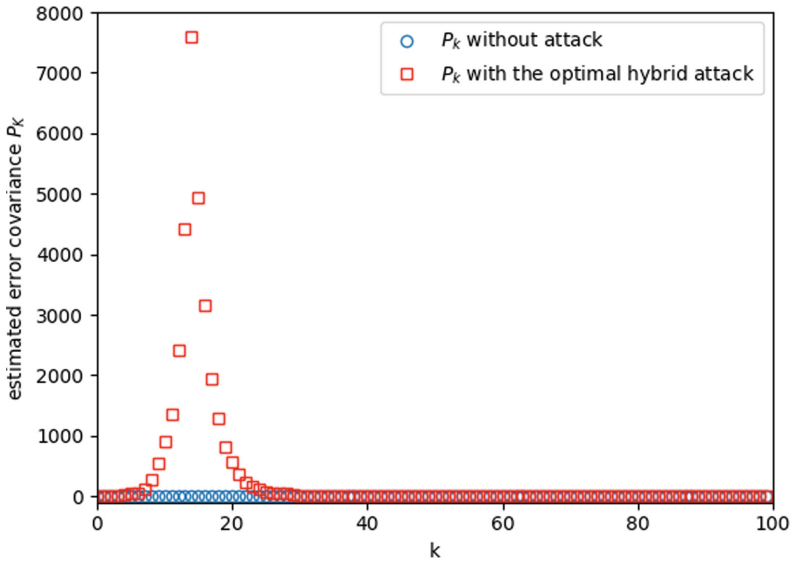

Fig. 2. Remote estimated error covariance

simulate the estimated error covariance under above two cases in Fig. 2. From Fig. 2, it can be seen that error covariance without attack will keep the steady error covariance. However, error covariance under the optimal hybrid attacks schedules will deviate from the steady error covariance at the attack period and then it will keep convergence.

5 Conclusion

In this paper, we have investigated optimal DoS attack and stealthy attack scheduling with energy constraint. Firstly, the attack order of stealthy attacks and DoS attacks with same attacks times have been derived. Then, the main results reveal the interesting fact that the optimal hybrid attacks scheduling for average error is the strategy where stealthy attacks launched at the beginning of system running until energy exhaustion and then launchs DoS attacks. Finally, simulations have been presented to verify the derived results. Future works will include the investigations of optimal attack scheduling for terminal errors, or the related explorations for multiple transmission channels.

Acknowledgements. This work was supported in part by the National Natural Science Foundation of China under Grant 62106042, and in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20210211.

References

1. Wen, G., Yu, W., Yu, X., Lü, J.: Complex cyber-physical networks: from cybersecurity to security control. J. Syst. Sci. Complexity **30**(1), 46–67 (2017). https://doi.org/10.1007/s11424-017-6181-x
2. Wen, G., Wang, P., Huang, T., Lu, J., Zhang, F.: Distributed consensus of layered multi-agent systems subject to attacks on edges. IEEE Trans. Circuits Syst. I Regul. Pap. **67**, 3152–3162 (2020). https://doi.org/10.1109/TCSI.2020.2986953
3. Wan, Y., Long, C., Deng, R., Wen, G., Yu, W., Huang, T.: Distributed event-based control for thermostatically controlled loads under hybrid cyber attacks. IEEE Trans. Cybern. **51**(11), 5314–5327 (2020). https://doi.org/10.1109/TCYB.2020.2978274
4. Wan, Y., Wen, G., Yu, X., Huang, T.: Distributed consensus tracking of networked agent systems under denial-of-service attacks. IEEE Trans. Syst. Man Cybern. Syst. **51**, 6183–6196 (2021). https://doi.org/10.1109/TSMC.2019.2960301
5. Zhou, J., Lv, Y., Wen, G., Yu, X.: Resilient consensus of multiagent systems under malicious attacks: appointed-time observer-based approach. IEEE Trans. Cybern. (2021). https://doi.org/10.1109/TCYB.2021.3058094
6. Li, L., Zhang, H., Xia, Y., Yang, H.: Security estimation under denial-of-service attack with energy constraint. Neurocomputing **292**, 111–120 (2018). https://doi.org/10.1016/j.neucom.2018.02.086
7. Sun, Q., Zhang, K., Shi, Y.: Resilient model predictive control of cyber-physical systems under DoS attacks. IEEE Trans. Industr. Inf. **16**, 4920–4927 (2020). https://doi.org/10.1109/TII.2019.2963294
8. Zhu, D., Chen, B., Hong, Z., Yu, L.: Networked nonlinear fusion estimation under DoS attacks. IEEE Sens. J. **21**, 7058–7066 (2021). https://doi.org/10.1109/JSEN.2020.3039918
9. Chen, J., Dou, C., Xiao, L., Wang, Z.: Fusion state estimation for power systems under DoS attacks: a switched system approach. IEEE Trans. Syst. Man Cybern. Syst. **49**, 1679–1687 (2019). https://doi.org/10.1109/TSMC.2019.2895912
10. Guo, Z., Shi, D., Johansson, K.H., Shi, L.: Optimal linear cyber-attack on remote state estimation. IEEE Trans. Control Netw. Syst. **4**, 4–13 (2017). https://doi.org/10.1109/TCNS.2016.2570003
11. Guo, Z., Shi, D., Johansson, K.H., Shi, L.: Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica **89**, 117–124 (2018). https://doi.org/10.1016/j.automatica.2017.11.018
12. Shang, J., Chen, M., Chen, T.: Optimal linear encryption against stealthy attacks on remote state estimation. IEEE Trans. Autom. Control **66**, 3592–3607 (2021). https://doi.org/10.1109/TAC.2020.3024143
13. Zhang, H., Cheng, P., Shi, L., Chen, J.: Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans. Autom. Control **60**, 3023–3028 (2015). https://doi.org/10.1109/TAC.2015.2409905
14. Qin, J., Li, M., Shi, L., Yu, X.: Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. IEEE Trans. Autom. Control **63**, 1648–1663 (2018). https://doi.org/10.1109/TAC.2017.2756259
15. Zhang, J., Sun, J.: Optimal stealthy linear-attack schedules on remote state estimation. IEEE Trans. Signal Process. **69**, 2807–2817 (2021). https://doi.org/10.1109/TSP.2021.3078624