Optimal Jamming Attack Scheduling of Interactive Channels

LAN WU, SHEYAN SU, AND JINGJING YAN
College of Electrical Engineering, Henan University of Technology, Zhengzhou 450001, China
Corresponding author: Lan Wu (wulan@haut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61973103 and Grant 61773154, and in part by the Henan Province Thousand Talents Plan - Top Young Talents.

ABSTRACT

Recently, public attention is thoroughly aroused as to the security threats of Cyber-Physical Systems (CPS), which can seriously disrupt the system operation. In order to analyze the impact of potential cyber-attacks, one needs to investigate the attack scheduling strategy from the attacker’s perspective. In this paper, we investigate the optimal attack schedules to degrade the system performance through multiple interactive channels against remote state estimation, which is different from the studies through multiple independent channels. Specifically, a channel is affected when the attacker launches an attack on another one, causing two different loss rates of the data package. Based on this, we represent the estimation error covariance of the remote estimator. Then we give the optimal jamming attack schedule theoretically. Finally, the effectiveness of the theoretical results is shown by numerical simulations.

INDEX TERMS

Cyber-physical systems, jamming attack schedule, interactive channels, remote state estimation.

I. INTRODUCTION

Cyber-Physical Systems are agents with integrated control, communication, computation. CPS have a wide application in many areas, such as aerospace, chemical processes, manufacturing, civil infrastructure, energy, intelligent transportation and battle field [1]–[3], [5], [10], [23]. The emergence of cyber-attacks has made wireless CPS more and more vulnerable. Take a very famous example, in June 2010 “Stuxnet” attacked an Iranian nuclear facility at Natanz, which damaged 60 percent hosts [4]–[6]. It is the first time that physical devices have been damaged by malicious computer programs.

Based on the attacker’s model knowledge, disclosure and disruption resources, cyber-attacks can be categorized into Denial-of-Service (DoS) attack, replay attack, false data injection attack, zero dynamics attack, covert attack and eavesdropping attack [7], [10]. Common malicious attacks are DoS attack [8], replay attack [9] and false data injection attack [7]. DoS attack aims to cause random loss of transmitted data by jamming the wireless communication channels to block the exchange of information between the system components, which is the most reachable attack [11]–[13]. Such attack can ignore protocols normally used and continuously transmit on a wireless channel with a set of frequency bands [14]. Jamming attack may be regarded as a special form of DoS attack [15]. In the present note, we focus on jamming attack.

Jamming attack in CPS has been well studied in recent literature [16], [17], [19]. Document [17] gives four different models of jamming attack and evaluates the properties in sending and receiving data packets of a wireless node. Literature [19] describes the transmission between sensors and estimator with a binary random process. In order to understand the behavior of potential attackers, one needs to investigate malicious attacks from the viewpoint of an attacker [13]. Therefore, the optimal attack scheduling strategy and the corresponding attack effect are urgently to be studied for CPS security [20]. Document [5] is the first work on DoS attack schedules against remote state estimation. On the condition that the attacker’s energy is limited, the authors consider a system where only one sensor processes the measurements and sends the data to a remote estimator through a wireless channel. The research purpose of document [5] is to determine when the attacker should perform an attack to maximize the average error of the remote estimation. With energy constraints for both the sensor and the attacker, the research shows that the optimal attack scheduling strategy is continuous attacks during the activation period when there

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.
is only one channel to transmit data [23]. Expand to scenario with multiple systems, there are some interesting results have been studied against DoS attack [16, 18, 21, 22]. For multiple systems, most existing works which investigate the optimal attack schedules mainly focus on multiple independent wireless channels. Paper [23] firstly uses two sensors to observe a system, and transmits data to remote estimator through two independent wireless channels. The optimal attack scheduling strategy is to continuously attack one channel when the total states of the system are observed. Reference [10] assumes that the system has two sensors to observe two states, and the energy of the attacker is limited. When the measurements are transmitted through two independent channels, the optimal attack scheduling strategy is to continuously attack one of the channels.

In the actual physical environment, due to the similar channel frequency bands or signal crosstalk, an interactive relationship will occur between channels. That is, when an attacker launches jamming attack on one of the channels, packet loss also occurs to the other channels. Reference [10] doesn’t fully integrate with physical reality, only study the case of transmitting through independent channels. Motivated by this, we investigate the optimal attack schedules to degrade the system performance through multiple interactive channels, which is different from the above studies through multiple independent channels. Specially, we assume that there are two sensors transmitting data packets to a remote estimator through two interactive channels. The transmission success rate is adopted to characterize the coupling relationship between the channels. The attacker with limited attack energy budget decides whether to block the channel to deteriorate the remote estimation quality at each sampling time. The main contribution of this paper is to construct the optimal jamming attack schedules when data packets are transmitted through two interactive wireless channels.

The rest of this paper is organized as follows. Section II presents the system model and attack model, and formulates the optimal jamming attack scheduling problem. Section III constructs the optimal jamming attack schedules when data packets are transmitted through two interactive wireless channels. In Section IV, we provide several numerical examples to validate our theoretical results. Section V draws conclusions.

Notations: In the whole paper, Z and Z_+ are the sets of all integers and nonnegative integers, respectively. R^n represents the Euclidean space with n-dimensional. S^n_+ is the set of the positive semi-definite matrices with n-by-n dimension. For simplicity, we denote X ≥ 0 for X ∈ S^n_+. While X > 0, it means that X is a positive definite matrix. In terms of functions f, f_1, f_2 : S^n_+ → S^n_+, define f_1 ∘ f_2(X) = f_1(f_2(X)), and f^T(X) = f ◦ f ◦ ⋯ ◦ f(X). P[X] and E[X] refer to probability and expectation for a random variable X, whose spectral radius is presented by ρ(X). The notation ⋄ refers to the floor function.

II. PROBLEM FORMULATION
A. SYSTEM MODEL
As shown in Fig.1, we consider a general discrete linear time-invariant (LTI) process in wireless CPS:

\[ x_i(k + 1) = A_i x_i(k) + \omega_i(k) \]
\[ y_i(k) = C_i x_i(k) + \nu_i(k) \]

where \( x_i(k) \in \mathbb{R}^n \) denotes the state of the ith plant \( i = 1, 2 \), \( \omega_i(k) \) is the process noise which is assumed to be white Gaussian with covariance \( Q_i \geq 0 \). \( \nu_i(k) \) is the measurement noise which is also assumed to be white Gaussian with covariance matrix \( R_i > 0 \). We assume that the initial state of the plant is zero-mean white Gaussian followed its covariance matrix \( P_i(0) > 0 \). Moreover, \( x_i(0) \) and \( \omega_i(k) \) are assumed to be independent with each other. The pair \((A_i, \sqrt{Q_i})\) is stabilizable. To make the problem tractable, we assume that \((A_1, C_1), (A_2, C_2)\) are both observable [10].

Kalman filter is an optimal linear filter. In remote state estimation, each sensor gets a local state estimation by Kalman filter firstly. We use \( \tilde{x}_i(k) \) and \( \tilde{P}_i(k) \) to represent the local state estimation and its corresponding estimation error covariance matrix, i.e.,

\[ \tilde{x}_i(k) = E[\tilde{x}_i(k)|y_i(1), y_i(2), \ldots, y_i(k)] \]
\[ \tilde{P}_i(k) = E[(\tilde{x}_i(k) - \tilde{x}_i(k))(\tilde{x}_i(k) - \tilde{x}_i(k))^T | y_i(1), y_i(2), \ldots, y_i(k)] \]

The standard Kalman filter process is as follows:

\[ \tilde{x}_i(k|k - 1) = A_i \tilde{x}_i(k - 1) \]
\[ \tilde{P}_i(k|k - 1) = A_i \tilde{P}_i(k - 1) A_i^T + Q_i \]
\[ \tilde{K}_i(k|k - 1) = \tilde{P}_i(k|k - 1) C_i^T [C_i \tilde{P}_i(k|k - 1) C_i^T + R_i]^{-1} \]
\[ \tilde{x}_i(k) = \tilde{x}_i(k - 1) + \tilde{K}_i(k)(y_i(k) - C_i \tilde{x}_i(k - 1)) \]
\[ \tilde{P}_i(k) = \tilde{P}_i(k|k - 1) - \tilde{K}_i(k) C_i \tilde{P}_i(k|k - 1) \]

where

\[ \tilde{x}_i(k|k - 1) = E[\tilde{x}_i(k)|y_i(1), y_i(2), \ldots, y_i(k - 1)] \]
\[ \tilde{P}_i(k|k - 1) = E[(\tilde{x}_i(k) - \tilde{x}_i(k|k - 1))(\tilde{x}_i(k) - \tilde{x}_i(k|k - 1))^T | y_i(1), y_i(2), \ldots, y_i(k - 1)] \]
that the steady value of $\bar{P}_i(k)$ converges quickly to a steady-state value in an exponential speed. Without any performance loss, we assume that the steady value of $\{\bar{P}_i(k)\}$ is represented by $\bar{P}_i(i \in 1, 2)$, which reaches the steady state at a time $k$.

**B. ATTACK MODEL**

We suppose that there is only one jamming attacker in the system. The attacker can launch jamming attack on only one of the channels because the wireless communication radio can only act upon one of the channels at each time step [25]. On condition that the attacker’s energy is limited, the attacker decides which channel to attack at every moment. If there is no jamming attacker in the wireless channels, the data packets will arrive at remote estimator successfully.

For any $k$, $\lambda(k) = i(i \in 1, 2)$ represents that the channel $i$ is under the jamming attack, and $\lambda(k) = 0$ denotes that none of the channels is under the jamming attack launched by the jamming attacker. Because only one of the channels can be jammed by the attacker at every moment, it follows that $1_{\lambda(k)=1} + 1_{\lambda(k)=2} \leq 1, \forall k \in Z_+$, in which $1_{\text{cond}}$ is an indicator function, i.e., $1_{\text{cond}} = 1$ if cond holds and $1_{\text{cond}} = 0$ otherwise.

In this paper, we research on the case where transmission channels interact with each other, that is, there is a coupling relationship between channels. The transmission success probability satisfying $\Pr[\gamma_2|y_2(k) = 1] = \gamma_2$ is used to reflect the coupling relationship between channels. More specifically, when the attacker launches an attack on channel 1, the probability of successful transmission of channel 1 is $\gamma_1$, and the probability of successful transmission of channel 2 is $\gamma_2$; when the attacker attacks channel 2, the probability of successful transmission of channel 1 is $\gamma_1$, and the probability of successful transmission of channel 2 is $\gamma_2$.

**C. PROBLEM FORMULATION**

For a time horizon $T$, the attacker’s schedule can be denoted as $s = (\lambda(1), \lambda(2), \ldots, \lambda(T))$. Denote $\hat{x}_i(k)$ and $P_i(k)$ as the state estimation of the remote estimator and the corresponding estimation error covariance matrix, respectively, i.e., $\hat{x}_i(k) = E[x_i(k)|P_i(k) = [x_i(k) - \hat{x}_i(k)](x_i(k) - \hat{x}_i(k))^T, i = 1, 2$.

**Average Error:** For a given attack schedule, the average expectation of the estimation error covariance is defined as $J_i(s)$, i.e.,

$$J_i(s) = \frac{1}{T} \sum_{k=1}^{T} E[P_i(k, \lambda(k))], \quad i = 1, 2 \tag{11}$$

**Problem 2.1:** Find out the optimal energy efficient attack schedule which maximizes the whole estimation error, that is

$$\max_{s \in S} \text{Tr}[J_1(s)] + \text{Tr}[J_2(s)] \tag{12}$$

s.t. $\sum_{k=1}^{T} (1_{\lambda(k)=1}\Psi_1 + 1_{\lambda(k)=2}\Psi_2) \leq \Psi$

$$\leq \max\{(T + 1)\Psi_1, (T + 1)\Psi_2\} \tag{13}$$

in which $S = \{0, 1, 2\}^T$ is the set of all the possible jamming attack schedules. Constraint (13) means that the total energy of the attacker is limited to $\Psi$, where $\Psi$ represents the consumed energy that the attacker launches jamming attack on channel $i$ once. Constraint (14) shows that only one channel is under jamming attack at a time $k$. Constraint (15) shows that each channel is attacked at least once during the period $T$. Constraint (16) means the remaining energy, which is equal to the total energy minus the spent energy, to attack on any channel. In other words, the attacker uses enough energy to attack more times on the wireless channels, which can degrade the estimation performance at a much higher level. (See Lemma 4 for detailed proof).

**III. OPTIMAL ENERGY EFFICIENT JAMMING ATTACK SCHEDULE**

The optimal estimation $\hat{x}_i(k)$ and its corresponding error covariance matrix $P_i(k)$ can be calculated using the following formulas:

$$\hat{x}_i(k) = \begin{cases} A_i\hat{x}_i(k - 1), & \text{if } 1_{\lambda(k)=i}(1 - \gamma_i(k)) \leq 1; \\ \hat{x}_i(k), & \text{otherwise} \end{cases} \tag{17}$$

$$P_i(k) = \begin{cases} h_i(P_i(k - 1)), & \text{if } 1_{\lambda(k)=i}(1 - \gamma_i(k)) \leq 1; \\ P_i, & \text{otherwise} \end{cases} \tag{18}$$

in which $h_i(X) = A_iX_iA_i^T + Q_i, i = 1, 2$.

In the following, we aim to find out the optimal energy efficient jamming attack schedule to solve Problem 2.1.

**Lemma 1:** $h_i^k(P_i)$ is monotonically increasing with $k(\forall k \in Z_+, i = 1, 2)$ [19].

**Lemma 2:** $h_i(X) = AX_iA_i^T + Q$ is monotonically increasing for any $X$.

Proof: Assume $X_1 > X_2$, then $X_1 - X_2 > 0$, and thus $A(X_1 - X_2)A_i^T > 0$. However,

$$A(X_1 - X_2)A_i^T = AX_iA_i^T - AX_iA_i^T + Q - Q$$

$$= AX_iA_i^T + Q - [AX_iA_i^T + Q]$$

$$= h(X_1) - h(X_2) > 0$$

Thus, $h(X)$ is monotonically increasing for any $X$.

Paper [10] has proved that the optimal energy efficient jamming attack schedule is continuously jamming one of the channels until the attacker runs out of its total energy. For our problem, according to the interaction of the two physical systems and the results in [10], without loss of generality, we suppose that the form of the optimal energy efficient attack schedule is as follows:

$$s_{r_1, r_2} = (1, 1, \ldots, 1, 2, 2, \ldots, 2, 0, 0 \ldots 0) \tag{19}$$

for $r_1 \times r_2 \times (T - r_1 + r_2)$.
in which \( \tau_1 \Psi_1 + \tau_2 \Psi_2 \leq \Psi, \tau_i \in \mathbb{Z}_+, i = 1, 2 \). Denote \( E[P_i(k)] = M_i(k) \) and its initial value of error covariance as:

\[
E[P_i(0)] = M_i(0) = \hat{P}_i, \quad i = 1, 2 \tag{20}
\]

For simplicity, it is assumed that \( \frac{\Psi_1}{\Psi_2} = \frac{\alpha}{\beta} \), where \( \alpha \) and \( \beta \) denote two co-prime integers. It means that the energy of launching \( \beta \) times consecutive attack on channel 1 equals to that of launching \( \alpha \) times consecutive attack on channel 2. Thus, according to (18), we have

\[
\begin{align*}
M_1(k) &= \gamma_1 \tilde{P}_1 + (1 - \gamma_1) h_1(M_1(k - 1)) \\
M_2(k) &= \gamma_2 \tilde{P}_2 + (1 - \gamma_2) h_2(M_2(k - 1)) \\
&\text{for } k = 1, \ldots, \tau_1 \\
M_1(k) &= \gamma_1 \tilde{P}_1 + (1 - \gamma_1) h_1(M_1(k - 1)) \\
M_2(k) &= \gamma_2 \tilde{P}_2 + (1 - \gamma_2) h_2(M_2(k - 1)) \\
&\text{for } k = \tau_1 + 1, \ldots, \tau_1 + \tau_2
\end{align*} \tag{21}
\]

and

\[
\begin{align*}
M_1(k) &= \gamma_1 \tilde{P}_1 + (1 - \gamma_1) h_1(M_1(k - 1)) \\
M_2(k) &= \gamma_2 \tilde{P}_2 + (1 - \gamma_2) h_2(M_2(k - 1)) \\
&\text{for } k = 1, \ldots, \tau_1 \\
M_1(k) &= \gamma_1 \tilde{P}_1 + (1 - \gamma_1) h_1(M_1(k - 1)) \\
M_2(k) &= \gamma_2 \tilde{P}_2 + (1 - \gamma_2) h_2(M_2(k - 1)) \\
&\text{for } k = \tau_1 + 1, \ldots, \tau_1 + \tau_2
\end{align*} \tag{22}
\]

that is

\[
\begin{align*}
M_1(k) &= \gamma_1 \sum_{q=0}^{k-1} (1 - \gamma_1)^q h_1^q(\tilde{P}_1) + (1 - \gamma_1)^k h_1^k(\tilde{P}_1) \\
M_2(k) &= \gamma_2 \sum_{q=0}^{k-1} (1 - \gamma_2)^q h_2^q(\tilde{P}_2) + (1 - \gamma_2)^k h_2^k(\tilde{P}_2) \\
&\text{for } k = 1, \ldots, \tau_1 \\
M_1(k) &= \gamma_1 \sum_{q=0}^{k-1} (1 - \gamma_2)^q h_1^q(\tilde{P}_1) + (1 - \gamma_1)^k h_1^k(\tilde{P}_1) \\
M_2(k) &= \gamma_2 \sum_{q=0}^{k-1} (1 - \gamma_2)^q h_2^q(\tilde{P}_2) + (1 - \gamma_2)^k h_2^k(\tilde{P}_2) \\
&\text{for } k = \tau_1 + 1, \ldots, \tau_1 + \tau_2
\end{align*} \tag{23}
\]

in which

\[
\begin{align*}
\tilde{P}_{11} &= M_1(\tau_1) = \gamma_1 \sum_{q=0}^{\tau_1-1} (1 - \gamma_1)^q h_1^q(\tilde{P}_1) \\
&\quad + (1 - \gamma_1)^{\tau_1} h_1^{\tau_1}(\tilde{P}_1) \\
\tilde{P}_{22} &= M_2(\tau_1) = \gamma_2 \sum_{q=0}^{\tau_1-1} (1 - \gamma_2)^q h_2^q(\tilde{P}_2) \\
&\quad + (1 - \gamma_2)^{\tau_1} h_2^{\tau_1}(\tilde{P}_2)
\end{align*} \tag{24}
\]

Define \( J \) as the total expectation of the estimation error covariance, then

\[
TJ(s_{\tau_1, \tau_2}) = TJ_1(s_{\tau_1, \tau_2}) + TJ_2(s_{\tau_1, \tau_2}) + (T - \tau_1 - \tau_2)(\tilde{P}_1 + \tilde{P}_2) = \sum_{k=1}^{\tau_1} M_1(k) + \sum_{j=\tau_1+1}^{\tau_1+\tau_2} M_1(j) + \sum_{k=1}^{\tau_1} M_2(k) + \sum_{j=\tau_1+1}^{\tau_1+\tau_2} M_2(j) + (T - \tau_1 - \tau_2)(\tilde{P}_1 + \tilde{P}_2)
\]

where the inequality is due to Lemma 1.

**Lemma 3:** For \( \tilde{P}_{11} \) and \( \tilde{P}_1 \) defined by (25) and (20), respectively, it holds that \( \tilde{P}_{11} \geq \tilde{P}_1 \).

**Proof:** In fact,

\[
\begin{align*}
\tilde{P}_{11} &= \gamma_1 \sum_{q=0}^{\tau_1-1} (1 - \gamma_1)^q h_1^q(\tilde{P}_1) + (1 - \gamma_1)^{\tau_1} h_1^{\tau_1}(\tilde{P}_1) \\
&\geq \gamma_1 [(1 - \gamma_1)^0 h_1^0(\tilde{P}_1) + (1 - \gamma_1)^1 h_1^1(\tilde{P}_1)] + \ldots \\
&\quad + (1 - \gamma_1)^{\tau_1-1} h_1^{\tau_1-1}(\tilde{P}_1)] + (1 - \gamma_1)^{\tau_1} h_1^{\tau_1}(\tilde{P}_1) \\
&\geq \gamma_1 [(1 - \gamma_1)^0 h_1^0(\tilde{P}_1) + (1 - \gamma_1)^1 h_1^1(\tilde{P}_1)] + \ldots \\
&\quad + (1 - \gamma_1)^{\tau_1-1} h_1^{\tau_1-1}(\tilde{P}_1)] + (1 - \gamma_1)^{\tau_1} h_1^{\tau_1}(\tilde{P}_1) \\
&= \gamma_1 \frac{1 - (1 - \gamma_1)^{\tau_1}}{1 - (1 - \gamma_1)} \tilde{P}_1 + (1 - \gamma_1)^{\tau_1} \tilde{P}_1 = \tilde{P}_1
\end{align*}
\]

Similarly, \( M_i(n) - \tilde{P}_i > 0 \) due to Lemma 3. Therefore, \( J_1 > J_2 \). We can get the conclusion that the more attacks result in the greater degradation of system performance.

Based on the above analysis, we have the following theorem which gives the optimal energy efficient jamming attack schedule.

**Theorem 1:** Consider the system with two sensors which is formed as (1). \( s_{\tau_1^*, \tau_2^*} \) is the optimal energy efficient jamming attack schedule for Problem 2.1, in which \( \tau_1^*, \tau_2^* \in \mathbb{Z}_+ \) can be calculated as follows when

\[
\gamma_2 \leq \frac{[h_2^{\tau_1-1}(\tilde{P}_2 - h_1^{\tau_1}(\tilde{P}_{11}))]}{h_2^{\tau_1-1}(\tilde{P}_{11}) - h_1^{\tau_1}(\tilde{P}_1)} \quad \gamma_2 \leq \frac{[h_2^{\tau_1-1}(\tilde{P}_2 - h_1^{\tau_1}(\tilde{P}_{22}))]}{h_2^{\tau_1-1}(\tilde{P}_{22}) - h_1^{\tau_1}(\tilde{P}_{11})}
\]

(1) \( \tau_1^* = \frac{\tau_1 - 1}{\Psi_1} \text{, } \tau_2^* = \frac{\tau_2 - 1}{\Psi_2} \text{, if } g_1 \geq g_2 \)

(2) \( \tau_1^* = \frac{\tau_1 - 1}{\Psi_1} \text{, } \tau_2^* = \frac{\tau_2 - 1}{\Psi_2} \text{, if } g_1 \geq g_2 \)

**Proof:** Consider that

\[
TJ(s_{\tau_1 + \beta, \tau_2 - \alpha}) - TJ(s_{\tau_1, \tau_2}) = \sum_{k=1}^{\tau_1} [M_1(k) + M_2(k)] + \sum_{j=\tau_1+1}^{\tau_1+\beta} [M_1(j) + M_2(j)] + (T - (\tau_1 + \beta)) (\tilde{P}_1 + \tilde{P}_2)
\]
\[- (\tau_2 - \alpha)(\hat{P}_1 + \hat{P}_2) - \sum_{k=1}^{\tau_1} [M_1(k) + M_2(k)] \]
\[- \sum_{j=\tau_1+1}^{\tau_2} [M_1(j) + M_2(j)] - (T - \tau_1 - \tau_2)(\hat{P}_1 + \hat{P}_2) \]
\[= \sum_{k=1}^{\tau_1} [M_1(\tau_1 + k) + M_2(\tau_1 + k)] - \sum_{k=1}^{\tau_2} [M_1(\tau_2 - \alpha + k) + M_2(\tau_2 - \alpha + k)] + (\alpha - \beta)(\hat{P}_1 + \hat{P}_2) \]  \hspace{1cm} (28)

in which \( \tau_2 = \left\lfloor \frac{\tau_1 - \Psi_1}{\Psi_2} \right\rfloor. \)

Denote
\[G(\tau_1, \tau_2) = \sum_{k=1}^{\tau_1} [M_1(\tau_1 + k) + M_2(\tau_1 + k)] \]
\[+ \sum_{k=1}^{\tau_2} [M_1(\tau_2 - \alpha + k) + M_2(\tau_2 - \alpha + k)] \]  \hspace{1cm} (29)

It holds that
\[G(\tau_1 + \beta, \tau_2 - \alpha) - G(\tau_1, \tau_2) \]
\[= \sum_{k=1}^{\tau_1 + \beta} [M_1(\tau_1 + \beta + k) + M_2(\tau_1 + \beta + k)] \]
\[- \sum_{k=1}^{\tau_2 - \alpha} [M_1(\tau_2 - 2\alpha + k) + M_2(\tau_2 - 2\alpha + k)] \]
\[- \sum_{k=1}^{\tau_1} [M_1(\tau_1 + k) + M_2(\tau_1 + k)] \]
\[+ \sum_{k=1}^{\tau_1} [M_1(\tau_2 - \alpha + k) + M_2(\tau_2 - \alpha + k)] \]
\[- \sum_{k=1}^{\tau_2} [M_1(\tau_2 - \alpha + k) + M_2(\tau_2 - \alpha + k)] \]
\[= \sum_{k=1}^{\tau_1} [M_1(\tau_1 + \beta + k) - M_1(\tau_1 + k)] \]
\[+ M_2(\tau_1 + \beta + k) - M_2(\tau_1 + k)] \]
\[- \sum_{k=1}^{\tau_2} [M_1(\tau_2 - 2\alpha + k) - M_1(\tau_2 - \alpha + k)] \]
\[+ M_2(\tau_2 - 2\alpha + k) - M_2(\tau_2 - \alpha + k)] \]

and
\[M_1(\tau_1 + k) - M_1(\tau_1 + k - 1) \]
\[= \sum_{q=0}^{k-1} (1 - \gamma_21)^q h_1^{k-1}(\hat{P}_{11}) + (1 - \gamma_21)^k h_1^{k-1}(\hat{P}_{11}) \]
\[- \sum_{q=0}^{k-2} (1 - \gamma_21)^q h_1^{k-1}(\hat{P}_{11}) - (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \]
\[= \gamma_21 \sum_{q=0}^{k} (1 - \gamma_21)^q h_1^{k-1}(\hat{P}_{11}) - \sum_{q=0}^{k-2} (1 - \gamma_21)^q h_1^{k-1}(\hat{P}_{11}) \]
\[+ (1 - \gamma_21)^k h_1^{k-1}(\hat{P}_{11}) - (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \]
\[= \gamma_21 (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) - (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \]
\[+ (1 - \gamma_21)^k h_1^{k-1}(\hat{P}_{11}) \]  \hspace{1cm} (30)

For any \( k \geq 1 \), we know that
\[M_1(\tau_1 + k) - M_1(\tau_1 + k - 1) \geq 0 \]
\[\Leftrightarrow \gamma_21 (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \geq 0 \]
\[\Leftrightarrow (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \geq 0 \]
\[\Leftrightarrow \gamma_21 (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \geq 0 \]
\[\Leftrightarrow \gamma_21 (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \geq 0 \]
\[\Leftrightarrow \gamma_21 (1 - \gamma_21)^{k-1} h_1^{k-1}(\hat{P}_{11}) \geq 0 \]
\[\Rightarrow \gamma_21 \leq \frac{h_1^{k-1}(\hat{P}_{11}) - h_1^{k-1}(\hat{P}_{11})}{h_1^{k-1}(\hat{P}_{11})} \]  \hspace{1cm} (31)

Thus, \( M_1(\tau_1 + k) - M_1(\tau_1 + k - 1) \geq 0 \), which means \( M_1(k) \) is monotonically increasing with \( k \leq \tau_1 \). For the time \( k = \tau_1 + 1 \), \( M_1(k) \) is still monotonically increasing if
\[M_1(\tau_1 + 1) \geq M_1(\tau_1) \]
\[\Leftrightarrow \gamma_21 \hat{P}_1 + (1 - \gamma_21) h_1^{k-1}(\hat{P}_{11}) \geq \hat{P}_{11} \]
\[\Leftrightarrow \gamma_21 \leq \frac{h_1^{k-1}(\hat{P}_{11}) - \hat{P}_{11}}{h_1^{k-1}(\hat{P}_{11}) - \hat{P}_{11}} \]  \hspace{1cm} (32)

which is a special case of (30) that \( k = 1 \). In combination with (30), (31) and (32), we have \( M_1(k) - M_1(k - 1) \geq 0, \forall k \in T \). Thus, \( M_1(\tau_1 - \alpha + k) - M_1(\tau_1 - 2\alpha + k) \geq 0 \). Similarly, we can get that \( M_2(\tau_1 - \alpha + k) - M_2(\tau_1 - 2\alpha + k) \geq 0 \). Hence, \( G(\tau_1 + \beta, \tau_2 - \alpha) - G(\tau_1, \tau_2) \geq 0 \). It is obvious that \( \tau_1 \in [1, \frac{\Psi_1}{\Psi_2}], \tau_2 = \frac{\Psi_1 - \Psi_1}{\Psi_2} \). We can draw a conclusion that \( J(s_{\tau_1, \tau_2}) \) can be maximized at both endpoints, i.e.,
\[\max \left\{ J(s_{\tau_1, \tau_2}), J(s_{\Psi_1, \Psi_2}) \right\} \geq J(s_{\tau_1, \tau_2}) \]  \hspace{1cm} (33)
all \( \tau_1 \in [0, 1], \tau_2 = \left[ \Psi_{\tau_1} \Psi_{\tau_2} \right], \) where \( z_1 = \Psi - \left[ \Psi_{\tau_1} \Psi_{\tau_2} \right] \Psi_2, z_2 = \Psi - \left[ \Psi_{\tau_1} \Psi_{\tau_2} \right] \Psi_1. \) It can be seen that

\[
TJ(s_1 \mid s_2) = \sum_{k=1}^2 [M_1(k) + M_2(k)] + \sum_{j=1}^2 [M_1(j) + M_2(j)] + (T - \left[ \frac{z_1}{\Psi_{\tau_1}} \right] - \left[ \frac{z_2}{\Psi_{\tau_2}} \right]) (P_1 + P_2) = g_1
\]

\[
TJ(s_1 \mid s_2) = \sum_{k=1}^2 [M_1(k) + M_2(k)] + \sum_{j=1}^2 [M_1(j) + M_2(j)] + (T - \left[ \frac{\Psi}{\Psi_{\tau_1}} \right] - \left[ \frac{z_2}{\Psi_{\tau_2}} \right]) (P_1 + P_2) = g_2
\]

Consequently, we can get that

\[
(\tau_1^*, \tau_2^*) = \begin{cases} 
\left[ \frac{z_1}{\Psi_{\tau_1}}, \frac{\Psi}{\Psi_{\tau_2}} \right], & \text{if } g_1 \geq g_2 \\
\left[ \frac{\Psi}{\Psi_{\tau_1}}, \frac{z_2}{\Psi_{\tau_2}} \right], & \text{if } g_1 < g_2 
\end{cases}
\]

IV. ILLUSTRATIVE EXAMPLES

In this section, some numerical simulations are provided to show the optimal energy efficient jamming attack schedule for Problem 2.1. Consider the system (1) with

\[
A_1 = \begin{pmatrix} 1.5 & 0.1 \\ 0.8 & 1 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0.2 & 0.4 \\ 0 & 0.3 \end{pmatrix},
\]

\[
A_2 = \begin{pmatrix} 1 & 0.2 \\ 0.5 & 1.2 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 0.5 \\ 0 & 0.1 \end{pmatrix}
\]

\( \omega_k, \nu_k^1 \) and \( \nu_k^2 \) have zero mean and variance \( Q_1 = I_{2 \times 2}, Q_2 = 2I_{2 \times 2}, R_1 = 2I_{2 \times 2}, R_2 = I_{2 \times 2} \) respectively. Take \( \Psi = 10, \Psi_1 = 0.8, \Psi_2 = 0.9, \Psi_3 = 0.5, \) and \( T = 20. \) Obviously, \( (A_i, C_i) \) is observable, \( i = 1, 2. \) Fig.2. provides the state trajectory of \( Tr[\mathcal{J}(s_{\tau_1, \tau_2})] \) with \( \gamma_1 = 0.2, \gamma_2 = 0.3, \gamma_1 = 0.4, \gamma_2 = 0.1. \) It is observed from that \( Tr[\mathcal{J}(s_{\tau_1, \tau_2})] \) gets the maximum when \( \tau_1^* = 11, \tau_2^* = 1. \) Therefore, the optimal energy efficient jamming attack schedule for Problem 2.1 is \( (1, \ldots, 1, 2, 0, \ldots, 0). \)

Fig.3. provides the state trajectory of \( Tr[\mathcal{J}(s_{\tau_1, \tau_2})] \) with \( \gamma_1 = 0.3, \gamma_2 = 0.2, \gamma_1 = 0.4, \gamma_2 = 0.1. \) Compared with
the result of Fig.2, we can find that our proposed theorem still holds the maximum with the value of $y_{ij}$.

Fig.4 provides the response trajectory of $Tr\{J(s_1, r_2)\}$ varying with $r_2$. Combining Fig.2 and Fig.3, the theorem we mentioned is still feasible to find the optimal scheduling strategy.

V. CONCLUSIONS

In this paper, we consider the case where the data packets are transmitted through two interactive wireless channels. Specifically, one channel can be affected when attacker jammed another channel, which causes two different loss rates of the data package. We propose a theorem to find out the optimal jamming attack schedule and proved its correctness by some simulations. Future works include investigating the case of multiple channels eorect method and considering the attacker is equipped with energy constraints and studying the case where there is an constraint with sensors.

REFERENCES

[1] H. Li, L. Lai, and H. V. Poor, “Multicast routing for decentralized control of cyber physical systems with an application in smart grid,” IEEE J. Sel. Areas Commun., vol. 30, no. 6, pp. 1097–1107, Jul. 2012.

[2] K.-D. Kim and P. R. Kumar, “Cyber–physical systems: A perspective at the centennial,” Proc. IEEE, vol. 100, no. Special Centennial Issue, pp. 1287–1308, May 2012.

[3] P. Derfer, E. A. Lee, and A. S. Vincentelli, “Modeling cyber-physical systems,” Proc. IEEE, vol. 100, no. 1, pp. 13–28, Aug. 2012.

[4] J. P. Farwell and R. Rhozinski, “Stuxnet and the future of cyber war,” Survival, vol. 53, no. 1, pp. 23–40, Feb. 2011.

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

[6] J. Markoff, “A Silent Attack, but not a Subtle One,” The New York Times, Sep. 2010.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” Automatica, vol. 51, pp. 135–148, Jan. 2015.

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

[9] M. Zhu and S. Martinez, “On the performance analysis of resilient networked control systems under replay attacks,” IEEE Trans. Autom. Control, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[10] L. Peng, X. Cao, C. Sun, Y. Cheng, and S. Jin, “Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems,” Neurocomputing, vol. 272, pp. 571–583, Jan. 2018.

[11] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal DoS attack scheduling in wireless networked control system,” IEEE Trans. Control Syst. Technol., vol. 24, no. 3, pp. 843–852, May 2016.

[12] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal DoS attack policy against remote state estimation,” in Proc. 52nd IEEE Conf. Decis. Control, Dec. 2013, pp. 5444–5449.

[13] F. Li, C. Yang, and Y. Tang, “Optimal linear attack on cyber physical systems with multiplicative noise,” IEEE Access, vol. 6, pp. 33318–33328, 2018.

[14] L. Peng, X. Cao, H. Shi, and C. Sun, “Optimal jamming attack schedule for remote state estimation with two sensors,” J. Franklin Inst., vol. 355, no. 14, pp. 6859–6876, Sep. 2018.

[15] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[16] L. Peng, L. Shi, X. Cao, and C. Sun, “Optimal attack energy allocation against remote state estimation,” IEEE Trans. Autom. Control, vol. 63, no. 7, pp. 2199–2205, Jul. 2018.

[17] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. MobiHoc, 2005, pp. 46–57.

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

[19] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, “SINR-based DoS attack on remote state estimation: A game-theoretic approach,” IEEE Trans. Control Netw. Syst., vol. 4, no. 3, pp. 632–642, Sep. 2017.

[20] A. A. Ç Shields, S. Amin, and S. Sastry, “Research challenges for the security of control systems,” in Proc. 3rd USENIX Workshop Hot Topics Secure, San Jose, CA, USA, vol. 29, Jul. 2008, pp. 1–6.

[21] J. Qin, M. Li, L. Shi, and X. 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.

[22] Q. Li, Z. Wang, W. Sheng, F. E. Alsaadi, and F. E. Alsaadi, “Dynamic event-triggered mechanism for $H_\infty$ non-fragile state estimation of complex networks under randomly occurring sensor saturations,” Inf. Sci., vol. 509, pp. 304–316, Jan. 2020.

[23] 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. Autom. Control, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

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

[25] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, “Multi-channel jamming attacks using cognitive radios,” in Proc. 16th Int. Conf. Comput. Commun. Netw., Aug. 2007, pp. 352–357.