Optimal DoS Attack Scheduling in Wireless Networked Control System

Heng Zhang, Peng Cheng, *Member, IEEE*, Ling Shi, *Member, IEEE*, and Jiming Chen, *Senior Member, IEEE*

***Abstract*— Recently, many literature works have considered the security issues of wireless networked control system (WNCS). However, few works studied how the attacker should optimize its attack schedule in order to maximize the effect on the system performance due to the insufficiency of energy at the attacker side. This paper fills this gap from the aspect of control system performance. We consider the optimal jamming attack that maximizes the Linear Quadratic Gaussian (LQG) control cost function under energy constraint. After analyzing the properties of the cost function under an arbitrary attack schedule, we derive the optimal jamming attack schedule and the corresponding cost function. System stability under this optimal attack schedule is also considered. We further investigate the optimal attack schedule in a WNCS with multiple subsystems. Different examples are provided to demonstrate the effectiveness of the proposed optimal denial-of-service attack schedule.**

***Index Terms*— Attack scheduling, Denial-of-Service (DoS) attack, energy constraint, Linear Quadratic Gaussian (LQG) control, system stability.**

I. Introduction

WIRELESS networked control systems (WNCSs), in which physical elements (plants, sensors, controllers, and actuators) communicate via wireless networks, have received increasing research interests [1]–[4]. WNCSs have a wide spectrum of applications in mobile sensor networks, remote surgery, intelligent transportation, unmanned aerial vehicles, mobile robots, and so on. Security issues in WNCSs have been investigated from different viewpoints in recent years due to the increasing amount of cyber attacks that make WNCSs more and more vulnerable [5]–[9].

Various efforts have been devoted to studying the influence of specific malicious attacks, e.g., Denial-of-Service (DoS) attacks [10], replay attacks [11], and data injection attacks [7], on particular systems. Thereinto, the *DoS attack*, which aims to prevent the communication between system components, has been widely studied since this attack pattern is the most accomplishable one and can result in serious consequences [10], [12], [13]. A typical DoS technique in WNCS is jamming attack, which can interfere with the radio frequencies on the communication channels [14].

Recently, researchers have studied the LQG problems under DoS attack [10], [15], [16]. A semidefinite programming-based solution was presented in [10] to find an optimal feedback controller that minimizes a cost function subject to safety and energy constraints in the presence of an attack with identical independent distributed actions. In [15], the optimal control law is designed against an intelligent jammer with limited actions. In [16], an event-trigger control strategy is derived in the presence of an energy-constrained periodic jamming attacker. The common characteristic of these related works is that they aim to find optimal defensive control law. Our work, however, is from the viewpoint of the attacker, i.e., we look for the optimal attack strategies to maximize the LQG cost function. This is equally important as one can design an effective defensive control law only when he knows how the attacker behaves.

In almost all types of attacks, energy constraint is inherent and will affect an attacker's strategies [17]–[19]. Kashyap *et al*. [17] studied a zero-sum game on Multiple Input Multiple Output (MIMO) Gaussian Rayleigh fading channels between an intelligent DoS jammer and a decoder with bilateral power constraints. Li *et al*. [18] investigated the optimal jamming attack strategies by controlling the probability of jamming and transmission range. Zuba *et al*. [19] studied the effect of jamming attack on underwater wireless sensor networks and investigated the minimal energy consumption and the probability of detection in order to launch an effective DoS jamming attack.

In this paper, we aim to design an optimal attack schedule to maximize the attacking effect on the WNCS. Specifically, we first consider a system where one sensor measures the system state and sends the data packets to a remote estimator through a wireless channel. The attacker has a limited energy budget in every active period and decides at each sampling time whether or not to jam the channel. Then, we extend it to the scenario with multiple subsystems. In this scenario, the

Manuscript received January 26, 2015; revised May 18, 2015; accepted July 8, 2015. Manuscript received in final form July 19, 2015. This work was supported in part by the National Natural Science Foundation of China under Grant U1401253 and Grant 61429301, in part by the National Program for Special Support of Top Notch Young Professionals, and in part by the Fundamental Research Funds for the Central Universities under Grant 2014XZZX001-03. The work of L. Shi was supported by The Hong Kong University of Science and Technology Caltech Partnership under Grant FP004. The work of H. Zhang was supported by the University Science Research General Project of Jiangsu Province under Grant 15KJB510002. Recommended by Associate Editor Y. Shi. *(Corresponding author: Jiming Chen.)*

H. Zhang is with the State Key Laboratory of Industrial Control Technology, Cyber Innovation Joint Research Center, Zhejiang University, Hangzhou 310027, China, and also with the Huaihai Institute of Technology, Lianyungang 222000, China (e-mail: ezhangheng@gmail.com).

P. Cheng, and J. Chen are with the State Key Laboratory of Industrial Control Technology, Cyber Innovation Joint Research Center, Zhejiang University, Hangzhou 310027, China (e-mail: pcheng@iipc.zju.edu.cn; jmchen@ieee.org).

L. Shi is with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: eesling@ust.hk).

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/TCST.2015.2462741

DoS attacker has to make the attack decision, i.e., when to attack and which channel to be chosen. The main contributions of this paper, which distinguish from the related literatures, are summarized as follows.

1) We formulate a novel DoS attack problem and seek the optimal attack schedule that maximizes the LQG control cost function with an energy constraint.
2) We obtain the analytical expression of LQG cost function under an arbitrary attack schedule.
3) We provide the optimal attack schedule and analyze the system stability under this schedule.
4) We study the optimal attack schedule in a networked control system with multiple subsystems.

The remainder of this paper is organized as follows. In Section II, we present the system model and problem formulation. In Section III, we introduce some basic properties of system performance under an arbitrary attack schedule. In Section IV, we construct optimal DoS jamming attack schedules that maximize the cost function and analyze the system stability. In Section V, we study the optimal attack schedule in a networked control system with multiple subsystems. In Section VI, numerical examples are shown to demonstrate the effectiveness of the proposed optimal attack schedule. Finally, Section VII concludes this paper.

Notations: $\mathbb{R}^n$ stands for the n-dimensional Euclidean space. $\mathbb{N}$ is a positive integer set. $(\cdot)'$ stands for the transposition of a matrix. $\mathrm{Tr}(\cdot)$ is the trace of a square matrix. $\Pr\{\cdot\}$ stands for the probability of a random event. $\mathbb{E}(\cdot)$ stands for the mathematical expectation of a random variable, and $\mathbb{E}(\cdot|\cdot)$ stands for the conditional mathematical expectation. $\mathrm{Var}(\cdot)$ stands for the variance of a random variable. $\lfloor x \rfloor$ stands for the floor function of x, i.e., the integer part of x.

II. Problem Formulation

A. System Model

Consider the following discrete linear system:

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

where $x_k \in \mathbb{R}^{n_x}$ is the state vector at time k, x_0 is the initial state vector, $u_k \in \mathbb{R}^{m_x}$ is the control input vector at time k, and $w_k \in \mathbb{R}^{n_x}$ is the zero-mean Gaussian with covariance $\mathrm{Cov}(w_i, w_j) = \delta_{ij}\,\Sigma_w$.[1] We assume that the pairs (A, B) and $(A, \Sigma_w^{1/2})$ are stabilizable [20].

The sensor measures the state x_k and sends it to the remote controller via a wireless channel (see Fig. 1). The controller has a built-in estimator to estimate the state in case the packet is lost. The controller then generates a control packet u_k based on all the received sensor measurements and historical control commands and sends u_k to the actuator through a reliable channel [21], [22].

We introduce $\theta_k = 1/0$ as the indicator function whether the data packet x_k is received or not by the controller at time k. Let $\mathcal{I}_k$ be the data set $\{\theta_1 x_1, \theta_2 x_2, \ldots, \theta_k x_k, u_1, u_2, \ldots, u_{k-1}\}$.

[1] δ_{ij} is the Kronecker delta function, i.e., $\delta_{ij} = 1$, if $i = j$, and $\delta_{ij} = 0$ otherwise.

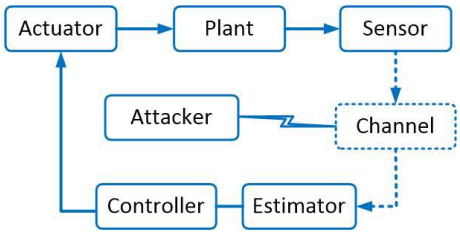

Fig. 1. System architecture.

We define $\hat{x}_k$ as the controller's minimum mean square error (MMSE) estimate of x_k at time k, i.e.,

$$\hat{x}_k = \mathbb{E}[x_k|\mathcal{I}_k], \tag{2}$$

where $\mathcal{I}_k$ denotes the controller's data at time k. The corresponding error covariance is

$$P_k = \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)'|\mathcal{I}_k]. \tag{3}$$

It is straightforward to obtain [22]

$$\hat{x}_k = \begin{cases} x_k, & \text{if } \theta_k = 1, \\ A\hat{x}_{k-1} + Bu_{k-1}, & \text{otherwise.} \end{cases} \tag{4}$$

We consider a linear static feedback controller of the form $u_k = L\hat{x}_k$, which is designed to minimize the following infinite-horizon LQG cost function [7], [22], [23]:

$$J = \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} \mathbb{E}[x_k' Q x_k + u_k' R u_k],$$

where $Q \geq 0$ and $R > 0$ are two weighting matrices and the expectation is taken over $\{w_k\}$. We will give the explicit form of L in Section III. We assume that the controller does not know the existence of the attacker.

B. Attack Model

It has been summarized that there are three types of attacks in an LQG control system, i.e., integrity attacks, DoS attacks, and direct physical attacks to the process (see [10, Fig. 1]). In this paper, we consider the case that the attacker performs DoS attack with the objective of increasing the cost function J as much as possible subject to an energy constraint. We assume that the attacker can attack only the communication channel n times in a given active period T_{ON}. After this period, he has to stop his attack actions and shift to an inactive period T_{OFF} to replenish the energy in order for the following attack period.

Let $\gamma(m) = (\gamma_{m,1}, \gamma_{m,2}, \ldots, \gamma_{m,T})$ be the attack schedule in the m-th period, where $\gamma_{m,t}, t = 1, 2, \ldots, T_{\mathrm{ON}}$ is the attack decision variable in active time, i.e., $\gamma_{m,t} = 1$ if he jams the transmission channel at time t of the m-th active period, and $\gamma_{m,t} = 0$ otherwise, and $\gamma_{m,t} = 0$ for inactive time $i = T_{\mathrm{ON}} + 1$, $T_{\mathrm{ON}} + 2, \ldots, T$ with $T = T_{\mathrm{ON}} + T_{\mathrm{OFF}}$. The consequence of attacking action $\gamma_{m,t} = 1$ is

$$\theta(\gamma_{m,t}) = \begin{cases} 1, & \text{with probability } 1 - \alpha, \\ 0, & \text{with probability } \alpha. \end{cases} \tag{5}$$

If he does not take action at time t, i.e., $\gamma_{m,t} = 0$, the data from the sensor can be received by the controller, i.e., $\theta(\gamma_{m,t}) = 1$.

From the attacker's viewpoint, it is of interest to design the optimal attack schedule that maximizes the expected cost function.

Problem 2.1:

$$\max_{\gamma\in\Theta} \mathbb{E}[J(\gamma)] \tag{6}$$

$$\text{s.t.} \sum_{t=1}^{T} \gamma_{m,t} \le n, \quad \forall m \in \mathbb{N}, \tag{7}$$

where $\gamma = [\gamma(m)]_{m=1}^{\infty}$ is the attack schedule on the infinite time horizon $[1,\infty)$ and $\Theta = \{\gamma\,|\gamma_{m,t} \in \{0,1\}, \forall m \in \mathbb{N}, t \in \{1,2,\ldots,T_{\text{ON}}\}\}$ is the attack schedule space.

III. Preliminaries

Before investigating the optimal attack schedule, we introduce some preliminary results.

Lemma 3.1 [7], [22]: The optimal static feedback controller is given by

$$u_k = -(B'SB+R)^{-1}B'SA\hat{x}_k,$$

where S is the unique solution to the following [24]:

$$S = A'SA + Q - A'SB(B'SB+R)^{-1}B'SA,$$

and the minimal cost is

$$J^* = J_c + J_e,$$

where

$$J_c = \text{Tr}[S\Sigma_w], \tag{8}$$

$$J_e = \lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}\text{Tr}[MP_k] \tag{9}$$

with $M = A'SB(B'SB+R)^{-1}B'SA$.[2]

Now, we present some properties of system performance under a given DoS attack schedule.

Lemma 3.2: Let $f(P) = \text{Tr}(MP)$, where P is an $n_x \times n_x$ positive definite symmetric matrix. If positive definite symmetric matrices P_1 and P_2 are $n_x \times n_x$ and satisfy $P_1 \ge P_2$, we have $f(P_1) \ge f(P_2)$.

Proof: See the Appendix. ∎

Remark 3.1: Note that J_c is the fixed part of J and J_e is the variable part that is affected by an attack schedule γ. Thus, we need only to find an optimal attack schedule to maximize $\mathbb{E}[J_e(\gamma)]$. From Lemma 3.2, maximizing $\mathbb{E}[J_e(\gamma)]$ is equivalent to maximize

$$\lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}\mathbb{E}[P_k(\gamma)].$$

Thus, we have to investigate $\mathbb{E}[P_k]$ under an arbitrary attack schedule γ.

From (3) and (4), one can see that

$$P_{k+1} = \begin{cases} \Sigma_w, & \text{if } \theta_{k+1}=0,\ P_k = 0,\\ AP_kA' + \Sigma_w, & \text{if } \theta_{k+1}=0,\ P_k \ne 0,\\ 0, & \text{otherwise.}\end{cases}$$

[2]It can be seen that M is a positive semidefinite matrix.

Then, we have

$$\mathbb{E}[P_{k+1}|P_k = 0] = \begin{cases}\alpha\Sigma_w, & \text{if } \gamma_{k+1}=1,\\ 0, & \text{otherwise,}\end{cases}$$

and

$$\mathbb{E}[P_{k+1}|P_k \ne 0] = \begin{cases}\alpha(AP_kA'+\Sigma_w), & \text{if } \gamma_{k+1}=1,\\ 0, & \text{otherwise.}\end{cases}$$

The following lemma shows how the consecutive attack actions affect the error covariance.

Lemma 3.3: For a given consecutive attack time interval $[s+1, s+t]$, i.e., $\gamma_s = 0, \gamma_{s+1} = \gamma_{s+2} = \cdots = \gamma_{s+t} = 1$, $\gamma_{s+t+1} = 0$, we have

$$\mathbb{E}[P_{s+j}] = \sum_{i=0}^{j-1}(\alpha^i - \alpha^{i+1})H_i + \alpha^j H_j, \tag{10}$$

where $H_i = \sum_{l=0}^{i-1}(A^l)\Sigma_w(A^l)'$ and $j = 1,2,\ldots,t$.

Proof: See the Appendix. ∎

From Lemma 3.3, for the given consecutive attack time interval $[s+1, s+t]$, $\mathbb{E}[P_{s+j}]$, $j = 1,2,\ldots,t$, does not depend on s. Thus, we denote $\Gamma_\alpha(t)$ by the sum of expected error covariance with any t times consecutive attack in the given active attack period $[s+1, s+t]$. Using the same method, any attack strategy with consecutive attack sequence $t_1, t_2, \ldots, t_s$ in a given period will lead to the same sum of expected error covariance. Then, we denote $\Gamma_\alpha(t_1 \oplus t_2 \oplus \cdots \oplus t_s)$ by the sum of expected error covariance with consecutive attack sequence $t_1, t_2, \ldots, t_s$ in the given attack period (Fig. 2). Note that $t_1, t_2, \ldots, t_s$ satisfy commutative law in $\Gamma_\alpha(t_1 \oplus t_2 \oplus \cdots \oplus t_s)$.

In fact

$$\begin{aligned}\Gamma_\alpha(t) &= \sum_{j=1}^{t}\mathbb{E}[P_{s+j}]\\ &= \sum_{j=1}^{t}\left[\sum_{i=0}^{j-1}(\alpha^i-\alpha^{i+1})H_i + \alpha^j H_j\right]\\ &= \sum_{i=0}^{t}\left[(t-i+1)\alpha^i - (t-i)\alpha^{i+1}\right]H_i,\end{aligned}$$

and

$$\Gamma_\alpha(t_1 \oplus t_2 \oplus \cdots \oplus t_s) = \sum_{i=1}^{s}\sum_{j_i=1}^{t_i}\mathbb{E}[P_{s_i+j_i}] = \sum_{i=1}^{s}\Gamma_\alpha(t_i).$$

Lemma 3.4: The following statements are true.

1) $\Gamma_\alpha(t_1) \le \Gamma_\alpha(t_2)$, where $t_1 \le t_2$.
2) $\Gamma_\alpha(t_1 \oplus t_2) \le \Gamma_\alpha(t)$, where $t = t_1 + t_2$.
3) $\Gamma_\alpha(t_1 \oplus t_2 \oplus \cdots \oplus t_s) \le \Gamma_\alpha(t)$, where $t = t_1 + t_2 + \cdots + t_s$.
4) $\Gamma_\alpha(t_1 \oplus t_2) \le \Gamma_\alpha(t_3 \oplus t_4)$, where $t_1 + t_2 = t_3 + t_4$ and $\max\{t_1,t_2,t_3,t_4\}$ is t_3 or t_4.

Proof: See the Appendix. ∎

Remark 3.2: From Lemma 3.4, one can see that more attack times (more energy) used in any given period lead to higher

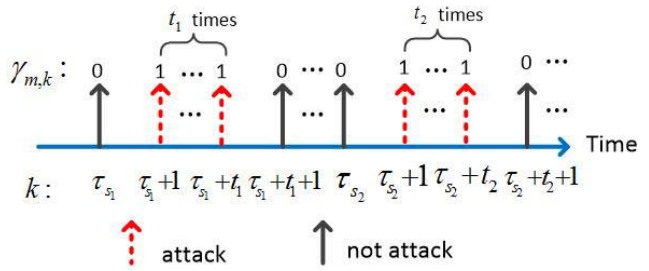

Fig. 2. Schematic of the attacker's schedule with consecutive attack sequences $t_1, t_2, \ldots, t_s$ in the same active period.

cost function. Thus, constraint (7) in Problem 2.1 can be replaced by

$$\sum_{t=1}^{T} \gamma_{m,t} = n, \quad \forall m \in \mathbb{N}. \tag{11}$$

IV. Optimal Attack Schedule Analysis

In this section, we first present the optimal attack schedule for Problem 2.1, and then analyze the system stability under the proposed attack schedule.

A. Optimal Attack Schedule

Theorem 4.1: The optimal attack schedule γ^* for Problem 2.1 is any n times consecutive attack at active periods, and the expected corresponding cost function can be calculated as follows:

$$\mathbb{E}[J(\gamma^*)] = J_c + \frac{1}{T}\mathrm{Tr}[M\Gamma_\alpha(n)]. \tag{12}$$

Proof: From Lemma 3.4, one can obtain that any n times consecutive attack at active periods is an optimal attack schedule.

Let $N = qT + m$ with $q, m \in \mathbb{N}$, and $0 \le m < T$. Then

$$\frac{1}{(q+1)T} < \frac{1}{N} \le \frac{1}{qT}.$$

If $0 \le m \le n$, we have

$$\sum_{k=1}^{N} \mathbb{E}[P_k] = qT\Gamma_\alpha(n).$$

If $n < m < T$, we have

$$\sum_{k=1}^{N} \mathbb{E}[P_k] = (qT+1)\Gamma_\alpha(n).$$

Then, it can be seen that

$$\frac{1}{(q+1)T}\sum_{k=1}^{N}\mathbb{E}[P_k] < \frac{1}{N}\sum_{k=1}^{N}\mathbb{E}[P_k] \le \frac{1}{qT}\sum_{k=1}^{N}\mathbb{E}[P_k].$$

Taking the limit $N \to \infty$ to this inequality, we can obtain

$$\lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}\mathbb{E}[P_k] = \frac{1}{T}[\Gamma_\alpha(n)]$$

which finishes the proof. ■

Example 4.1: Consider Problem 2.1 with $T_{\mathrm{ON}} = 5, n = 3$, and $T_{\mathrm{OFF}} = 5$. From Theorem 4.1, it can be seen that in any active period, the attack schedules $(1,1,1,0,0)$, $(0,1,1,1,0)$, and $(0,0,1,1,1)$ are optimal. The corresponding result on J can be calculated as

$$\mathbb{E}[J(\gamma^*)] = J_c + \frac{1}{10}\mathrm{Tr}[M\Gamma_\alpha(3)].$$

Remark 4.1: From Theorem 4.1, under an optimal attack schedule, the jamming instances are grouped together and this schedule does not depend on system parameters.

B. Stability Analysis Under Optimal Attack Schedule

Stability is critical in an LQG system. Before presenting results on stability of system (1) under an optimal attack schedule, we give the definition of system stability formally as follows.

Definition 4.1 [20], [25]: System (1) is stable if the covariance of the system state is bounded, i.e., $\mathrm{Var}(x_k) \le C^*$, where C^* is a constant matrix.

Theorem 4.2: Consider system (1) under an optimal attack schedule γ^*. When $T_{\mathrm{OFF}} > 0$, the system is stable in the sense of bounded covariance.

Proof: From Definition 4.1, one can see that

$$\begin{aligned}\mathrm{Var}(x_k) &= \mathbb{E}[\mathbb{E}((x_k - \mathbb{E}(x_k))(x_k - \mathbb{E}(x_k))'|\mathcal{I}_k)] \\ &= \mathbb{E}[\mathbb{E}((x_k - \hat{x}_k)(x_k - \hat{x}_k)'|\mathcal{I}_k)] = \mathbb{E}[P_k].\end{aligned}$$

Since $T_{\mathrm{OFF}} > 0$, from (10), we have

$$\mathrm{Var}(x_k) \le \sum_{i=0}^{n-1}(\alpha^i - \alpha^{i+1})H_i + \alpha^n H_n = C^*,$$

i.e., the covariance of state is bounded for a given n. ■

Remark 4.2: Theorem 4.2 shows that the optimal DoS attack cannot change the system stability if $T_{\mathrm{OFF}} > 0$. If $T_{\mathrm{OFF}} = 0$, the attacker has unlimited energy, and he can always attack the wireless channel. Thus, $\theta_k, k = 1, 2, \ldots$ become independent identically distributed Bernoulli random variable sequence with $\mathbb{E}(\theta_k) = 1 - \alpha$. Similar to [26], the system is stable if and only if $\alpha < 1 - \gamma_c$, where $\gamma_c = \inf_\gamma \{\gamma \,|X = A'XA + \Sigma_w - \gamma\, A'XB(B'XB + R)^{-1}B'XA\}$.

V. Multiple-Subsystem Case Study

In this section, we aim to optimize the attack schedule in a networked control system with multiple subsystems (see Fig. 3) [27], [28]. We assume that the attacker launches multichannel switch jamming in wireless networks. For example, DoS attacker can switch his jamming signals between target channels on 802.11 networks [29]. In our problem, the attacker has to make the attack decision, i.e., when to attack and which channel to be chosen.

A. WNCS Model With Multiple Subsystems

Similar to (1), we assume that the evolution of plants is as follows:

$$x_{i,k+1} = A_i x_{i,k} + B_i u_{i,k} + w_{i,k}, \quad i = 1, 2, \ldots, r, \tag{13}$$

where $x_{i,k} \in \mathbb{R}^{n_x}$ is the state vector of plant i at time k, $u_{i,k} \in \mathbb{R}^{m_x}$ is the control input vector of plant i at time k, $w_{i,k} \in \mathbb{R}^{n_x}$ is the zero-mean Gaussian with covariance

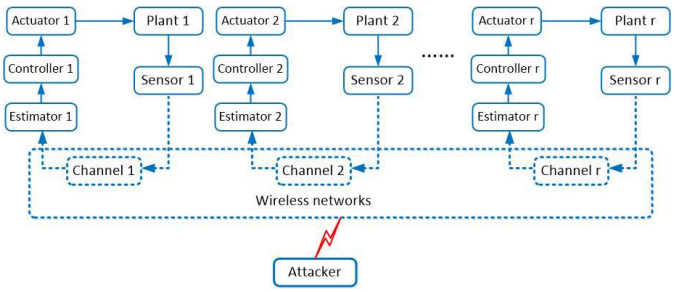

Fig. 3. Networked control system architecture with r subsystems. The attacker can jam one of the r channels during a time slot.

$\mathrm{Cov}(w_{i,k}, w_{i,t}) = \delta_{kt}\Sigma_{w_i}$, and $\mathrm{Cov}(w_{1,k}, w_{2,t}) = 0$. We assume that the pairs (A_i, B_i) and $(A_i, \Sigma_{w_i}^{1/2})$ are stabilizable.

Let $\hat{x}_{i,k}$ and $P_{i,k}$ be the MMSE estimates of $x_{i,k}$ and corresponding error covariance, respectively. They can be easily obtained from (2)–(4), respectively. The cost functions of these subsystems are

$$J_i = \lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}\mathbb{E}[x_{i,k}'Q_i x_{i,k} + u_{i,k}'R_i u_{i,k}], \quad i = 1, 2, \ldots, r.$$

From Lemma 3.1, we can obtain the optimal controller of system i as

$$u_{i,k} = -(B_i'S_iB_i + R_i)^{-1}B_i'S_iA_i\hat{x}_{i,k},$$

where S_i is the unique solution to the following equation:

$$S_i = A_i'S_iA_i + Q_i - A_i'S_iB_i(B_i'S_iB_i + R_i)^{-1}B_i'S_iA_i,$$

and the minimal cost is

$$J_i^* = J_{i,c} + J_{i,e}, \quad i = 1, 2, \ldots, r, \tag{14}$$

where

$$J_{i,c} = \mathrm{Tr}[S_i\Sigma_{w_i}],$$
$$J_{i,e} = \lim_{N\to\infty}\frac{1}{N}\sum_{k=1}^{N}\mathrm{Tr}[M_iP_{i,k}]$$

with $M_i = A_i'S_iB_i(B_i'S_iB_i + R_i)^{-1}B_i'S_iA_i$.

B. Optimal Attack Schedule

We assume that the attacker's energy budget is e_{total} in every active period and $T_{\text{OFF}} > 0$. Due to this energy constraint, the DoS attacker needs to make decisions when and which channel to jam in order to maximize the total cost

$$J_{\text{total}} = J_1 + J_2 + \cdots + J_r. \tag{15}$$

Let $\gamma_{m,t} = (\gamma_{m,t}^1, \gamma_{m,t}^2, \ldots, \gamma_{m,t}^r)$ be the attacker's decision vector at time t of m-th active period

$$\gamma_{m,t}^i = \begin{cases} 1, & \text{if the attacker jams channel } i, \\ 0, & \text{otherwise.} \end{cases}$$

We also assume that the attack action is successful with probability α_i when he jams the channel i with energy e_i for $i = 1, 2, \ldots, r$. From the viewpoint of DoS attacker, the optimization problem can be formulated as follows.

Problem 5.1:

$$\max_{\gamma\in\Theta}\mathbb{E}[J_{\text{total}}(\gamma)] \tag{16}$$
$$\text{s.t.}\ \sum_{i=1}^{r}\gamma_{m,t}^i \le 1, \quad \forall m \in \mathbb{N}, \tag{17}$$
$$\sum_{i=1}^{r}\left[e_i\left(\sum_{t=1}^{T}\gamma_{m,t}^i\right)\right] \le e_{\text{total}}, \quad \forall m \in \mathbb{N}, \tag{18}$$

where $\gamma = [\gamma(m)]_{m=1}^{\infty}$ is the attack schedule on the infinite time horizon $[1, \infty)$ and $\Theta = \{\gamma\,|\,\gamma_{m,t}^i \in \{0,1\}, \forall m \in \mathbb{N}, t \in \{1, 2, \ldots, T_{\text{ON}}\}\}$ is the attack schedule space. Constraint (17) shows that the attacker can only jam one channel or does not take action in any time. Equation (18) is the attacker's energy constraint in every active period.

From Lemma 3.4 and Theorem 4.1, one can see that if the attack times on channel i is limited to n_i, then consecutive attack n_i times with proper beginning attack time is the optimal decision. By unfolding (15) with (14), the objective function in Problem 5.1 can be replaced by

$$\sum_{i=1}^{r}J_{i,e} = \mathrm{Tr}\left[\sum_{i=1}^{r}M_i\Gamma_{\alpha_i}(n_i)\right],$$

since $J_{i,c}, i = 1, 2, \ldots, r$ are constants.

Therefore, Problem 5.1 can be converted to the following problem.

Problem 5.2:

$$\max \mathrm{Tr}\left[\sum_{i=1}^{r}M_i\Gamma_{\alpha_i}(n_i)\right] \tag{19}$$
$$\text{s.t.}\ \sum_{i=1}^{r}n_ie_i \le e_{\text{total}}, \tag{20}$$

where n_i denotes the consecutive attack times over channel i in the active periods for $i = 1, 2, \ldots, r$.

Note that this is an integer programming problem. Thus, the optimal solution $(n_1^*, n_2^*, \ldots, n_r^*)$ can be obtained by exhaustive search method.[3] From the above analysis, one can obtain the following theorem to solve Problem 5.1.

Theorem 5.1: The optimal attack schedule γ^* for Problem 5.1 is with any n_i^* times consecutive attack on channel i, respectively, at active periods, where

$$(n_1^*, n_2^*, \ldots, n_r^*) = \underset{\sum_{i=1}^{r}n_ie_i\le e_{\text{total}}}{\arg\max}\ \mathrm{Tr}\left[\sum_{i=1}^{r}M_i\Gamma_{\alpha_i}(n_i)\right]. \tag{21}$$

The expected corresponding cost function can be calculated as follows:

$$\mathbb{E}[J_{\text{total}}(\gamma^*)] = \sum_{i=1}^{r}J_{i,c} + \frac{1}{T}\mathrm{Tr}\left[\sum_{i=1}^{r}M_i\Gamma_{\alpha_i}(n_i^*)\right].$$

[3]The attacker needs only to run an exhaustive search method once before taking action. From constraint (20), we can see that the time complexity of exhaustive search method for Problem 5.2 is no more than $O(\bar{n}^{r-1})$, where $\bar{n} = \lfloor(e_{\text{total}}/e_{\min})\rfloor$ with $e_{\min} = \min\{e_1, e_2, \ldots, e_r\}$. Thus, it is not expensive to run the exhaustive search method.

Proof: First, if the DoS attacker assigns n_i times attack actions on channel i for $i = 1, 2, \ldots, r$, where $\sum_{i=1}^{r} n_i e_i \leq e_{\text{total}}$, then from Theorem 4.1, one can see that the optimal decision is any attack with consecutive attack n_i times on channel i.

Second, in order to find optimal attack assignment $(n_1^*, n_2^*, \ldots, n_r^*)$, from Problem 5.2, we just need to maximize

$$\text{Tr}\left[\sum_{i=1}^{r} M_i \Gamma_{\alpha_i}(n_i)\right].$$

■

An example is presented to illustrate Theorem 5.1 as follows.

Example 5.1: Consider Problem 5.1 with $T_{\text{ON}} = 4, n = 3$, and $T_{\text{OFF}} = 5$. If $(n_1^*, n_2^*) = (2, 1)$ is obtained from (21) for the given system parameters, it can be seen that in any active period, the attack schedules

$$\begin{pmatrix} \gamma_{m,1}^* \\ \gamma_{m,2}^* \\ \gamma_{m,3}^* \\ \gamma_{m,4}^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \text{or} \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}$$

are optimal.

If the subsystems are with identical parameters, we can get the optimal attack schedules for some special cases as follows.

Corollary 5.1: Consider the WNCS with identical subsystems, i.e., $A_1 = A_2 = \cdots = A_r$, $B_1 = B_2 = \cdots = B_r$, $\Sigma_{w_1} = \Sigma_{w_2} = \cdots = \Sigma_{w_r}$, $Q_1 = Q_2 = \cdots = Q_r$, and $R_1 = R_2 = \cdots = R_r$.

1) If the attacker uses the same energy to attack the channels, i.e., $e_1 = e_2 = \cdots = e_r$, then any consecutive attack $\hat{n} = \lfloor (e_{\text{total}}/e_1) \rfloor$ times over channel i^* is optimal, where $i^* = \arg\max_i \alpha_i$.
2) If the attack success probabilities over different channels are the same, i.e., $\alpha_1 = \alpha_2 = \cdots = \alpha_r$, then any consecutive attack $\tilde{n} = \lfloor (e_{\text{total}}/e_{j^*}) \rfloor$ times over channel j^* is optimal, where $j^* = \arg\min_j e_j$.

Proof: See the Appendix. ■

Similar to Section IV-B, we can see that the system is stable when $T_{\text{OFF}} > 0$. If $T_{\text{OFF}} = 0$, the attacker can always jam one of the wireless channels. Let $\gamma_{c,i} = \inf_\gamma \{\gamma \,|X = A_i' X A_i + \Sigma_{w_i} - \gamma\, A_i' X B_i (B_i' X B_i + R_i)^{-1} B_i' X A_i\}, i = 1, 2, \ldots, r$. From [26], it can be seen that the system is stable if and only if $\alpha_i < 1 - \gamma_{c,i}, \forall i$.

VI. Examples

A. Example I: Single System

We consider system (1) with $A = 2, B = 1, \Sigma_w = 1$, $Q = 1$, and $R = 1$. Assume that the length of the attacker's active period is $T_{\text{ON}} = 80$, inactive period is $T_{\text{OFF}} = 20$, and the attack energy constraint is $n = 20$. We use Monte Carlo method to illustrate the effects of different attack schedules on expected cost function $\mathbb{E}(J)$ and the system stability under optimal attacks. The simulation system runs 10 000 times for each illustration.

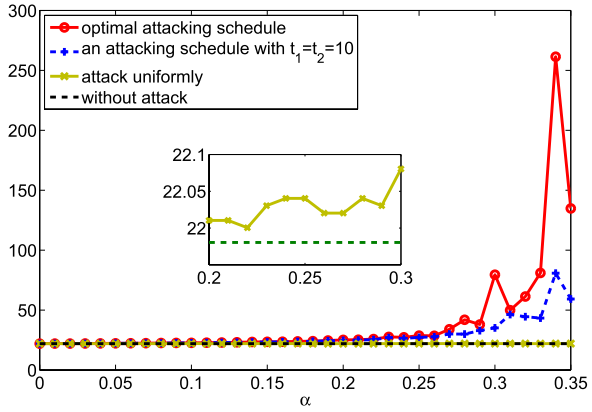

Fig. 4. Illustrating example on attacking effect of expected cost function $\mathbb{E}(J)$ with different attack schedules.

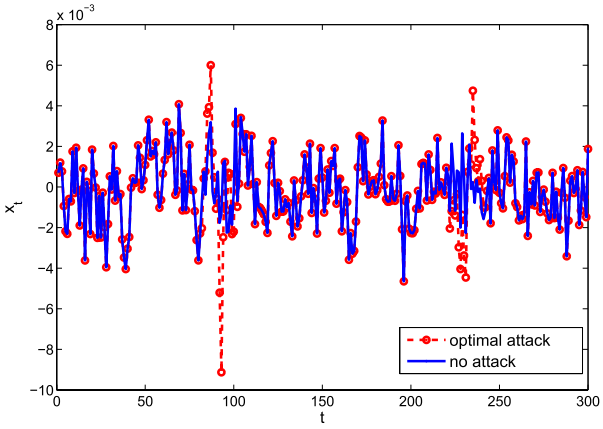

Fig. 5. System state under optimal attack schedule with and without attack, respectively. Here, the attacker can take action $n = 20$ times in any active period $T_{\text{ON}} = 100$ with successful probability $\alpha = 0.2$. $T_{\text{OFF}} = 40$.

1) Different Attack Schedules: Fig. 4 shows the variation of the expected cost function under different attack schedules when the sensor uses a deterministic channel for transmission. In Fig. 4, we examine the attack effect under different attack success probabilities from $\alpha = 0.01$ to $\alpha = 0.35$. The top curve of Fig. 4 stands for the performance under the attack schedule given by Theorem 4.1, i.e., $\mathbb{E}[J(\gamma^*)]$, which maximizes the expected cost function. It can also be seen that the expected cost function rapidly increases with α. The second line from the top shows the performance under a common attack schedule with consecutive attack sequence $t_1 = t_2 = 10$. It can be seen that the expected cost function grows much slower than $\mathbb{E}[J(\gamma^*)]$. We also can find that the performances under uniform attack with energy constraint in each active period are nearly the same as those without attack.

2) System Stability: Figs. 5 and 6 plot the evolution of the system state with different attack parameters T_{ON} and T_{OFF}. In Fig. 5, the attacker is working with $n = 20$, $T_{\text{ON}} = 80$, $T_{\text{OFF}} = 40$, and $\alpha = 0.2$. From Theorem 4.1, the attack schedule in Fig. 5 (attacking at time $[81, 100]$, $[221, 240]$, $[361, 380]$, and so on) is an optimal attack policy. In Fig. 5, the dashed line demonstrates that the system is still stable

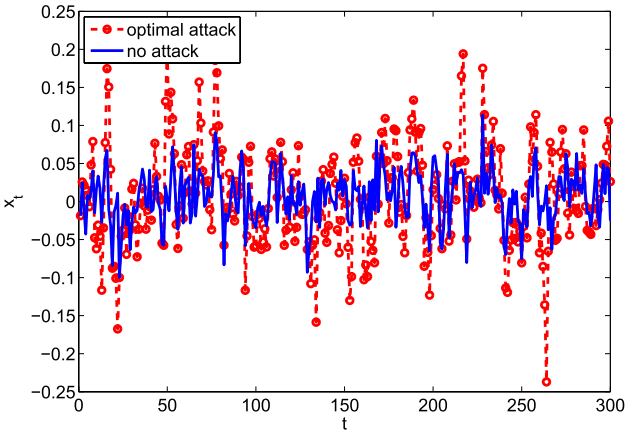

Fig. 6. System state under optimal attack schedule with and without attack, respectively. Here, the attacker can always take action in any active period $T_{\text{ON}} = 20$ with successful probability $\alpha = 0.2$. $T_{\text{OFF}} = 1$.

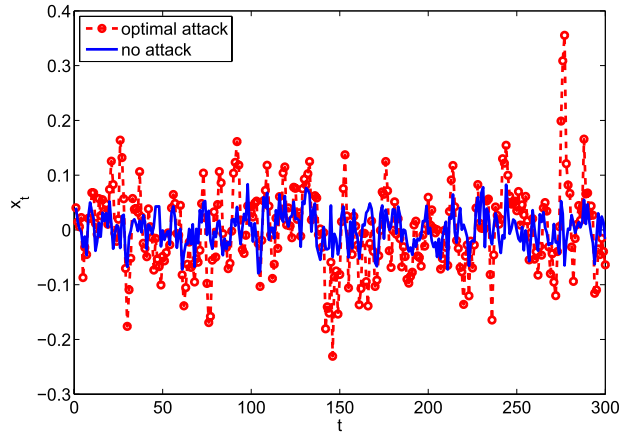

Fig. 7. System state under optimal attack schedule with and without attack, respectively. Here, the attacker can always take action in any active period $T_{\text{ON}} = 20$ with successful probability $\alpha = 0.2$. $T_{\text{OFF}} = 0$.

under this optimal attack schedule. The solid line shows the system's state without attack. In Fig. 6, the attacker is working with $T_{\text{ON}} = n = 20$ and $T_{\text{OFF}} = 1$. We can see that the state is still stable under this optimal attack.

Figs. 7 and 8 show the effectiveness of optimal attack schedule on the system state when there is no inactive period, i.e., $T_{\text{OFF}} = 0$ and $T_{\text{ON}} = n$. From Theorem 4.2, the stability depends on the attack successful probability α. In our example, the critical value can be calculated by $\gamma_c = 1 - (1/A^2) = 0.75$ [26]. From Fig. 7, one can see that the system is still stable when it suffers from the consecutive attack with successful probability $\alpha = 0.2 < 1 - \gamma_c = 0.25$. The system will become unstable, however, if the successful probability is $\alpha = 0.8 > 1 - \gamma_c$, which has been shown in Fig. 8.

B. Example II: Multiple Subsystems

We also consider WNCS with two subsystems (13) with $A_1 = 0.5, B_1 = 1, \Sigma_{w_1} = 1, Q_1 = 1, R_1 = 1$, $A_2 = 1.2, B_2 = 1, \Sigma_{w_2} = 0.5, Q_2 = 1$, and $R_2 = 1$. Assume that the length of attacker's active period is $T_{\text{ON}} = 80$ and $T_{\text{OFF}} = 20$. The attacker uses the same energy to jam

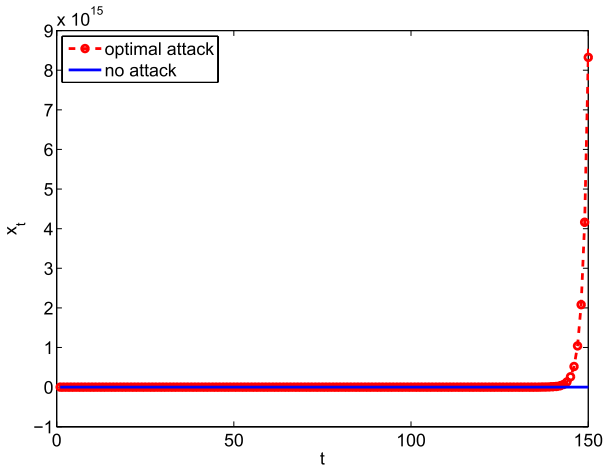

Fig. 8. System state under optimal attack schedule with and without attack, respectively. Here, the attacker can always take action in any active period $T_{\text{ON}} = 20$ with successful probability $\alpha = 0.8$. $T_{\text{OFF}} = 0$.

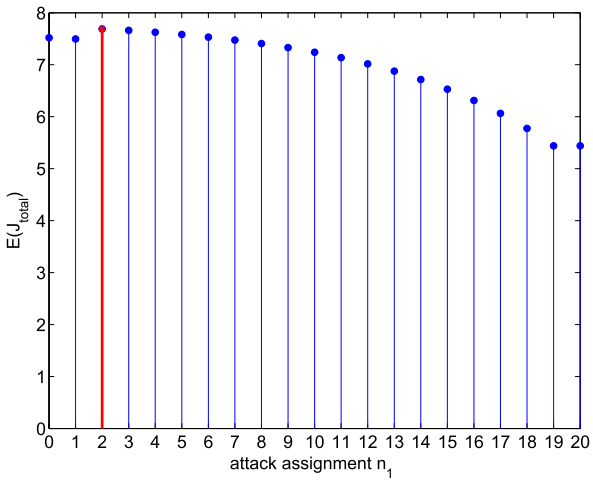

Fig. 9. Maximal value of cost $\mathbb{E}(J_{\text{total}})$ under different assignments (n_1, n_2) when $\alpha_1 = 0.1$ and $\alpha_2 = 0.6$. Here, $n_2 = 20 - n_1$ and $A_2 = 1.2$. The optimal assignment is $(n_1^*, n_2^*) = (2, 18)$.

channels 1 and 2, and the corresponding attack success probabilities are α_1 and α_2. Due to the energy constraint, he can at most attack $n = 20$ times in any active period.

Consider Problem 5.2 with given parameters. We can obtain the optimal attack assignment by exhaustive search method. Fig. 9 shows the variation of maximal value of $\mathbb{E}(J_{\text{total}})$ under different assignments (n_1, n_2) when $\alpha_1 = 0.1$ and $\alpha_2 = 0.6$. It can be seen that the optimal assignment is $(n_1^*, n_2^*) = (2, 18)$. Fig. 10 shows one optimal attack schedule in an active period. In this schedule, the attacker jams channel 1 in times 2 and 3 and jams channel 2 from time 11 to 28.

Table I shows the optimal attack assignment (n_1^*, n_2^*) under different attack success probabilities (α_1, α_2). Interestingly, in some cases, e.g., $(\alpha_1, \alpha_2) = (0.5, 0.2)$, though the probabilities satisfy the condition $\alpha_1 > \alpha_2$, the optimal assignment is opposite, i.e., $n_1^* < n_2^*$. The reason is that the optimal assignment also depends on the system parameters.

TABLE I
OPTIMAL ATTACK ASSIGNMENT (n_1^*, n_2^*) UNDER DIFFERENT ATTACK SUCCESS PROBABILITIES (α_1, α_2)

α_1 \ α_2	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.1	(8,12)	(6,14)	(5,15)	(4,16)	(3,17)	(2,18)	(0,20)	(0,20)	(0,20)
0.2	(9,11)	(7,13)	(6,14)	(5,15)	(4,16)	(3,17)	(0,20)	(0,20)	(0,20)
0.3	(10,10)	(8,12)	(7,13)	(5,15)	(4,16)	(3,17)	(2,18)	(0,20)	(0,20)
0.4	(11,9)	(9,11)	(7,13)	(6,14)	(5,15)	(3,17)	(2,18)	(0,20)	(0,20)
0.5	(11,9)	(9,11)	(8,12)	(6,14)	(5,15)	(4,16)	(3,17)	(0,20)	(0,20)
0.6	(12,8)	(10,10)	(8,12)	(7,13)	(6,14)	(4,16)	(3,17)	(0,20)	(0,20)
0.7	(12,8)	(10,10)	(9,11)	(7,13)	(6,14)	(5,15)	(3,17)	(0,20)	(0,20)
0.8	(13,7)	(11,1)	(9,11)	(8,12)	(7,13)	(5,15)	(4,16)	(2,18)	(0,20)
0.9	(13,7)	(11,9)	(10,10)	(8,12)	(7,13)	(5,15)	(4,16)	(2,18)	(0,20)

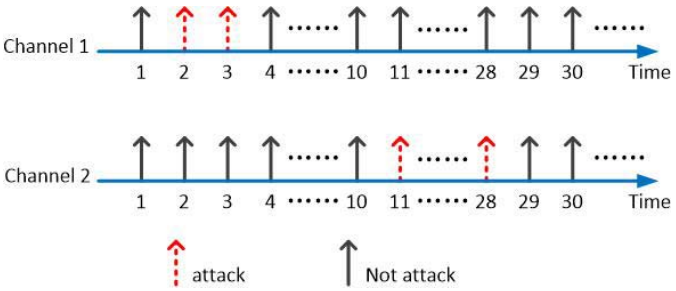

Fig. 10. Optimal attack schedule in an active period. Here, $\alpha_1 = 0.1$ and $\alpha_2 = 0.6$.

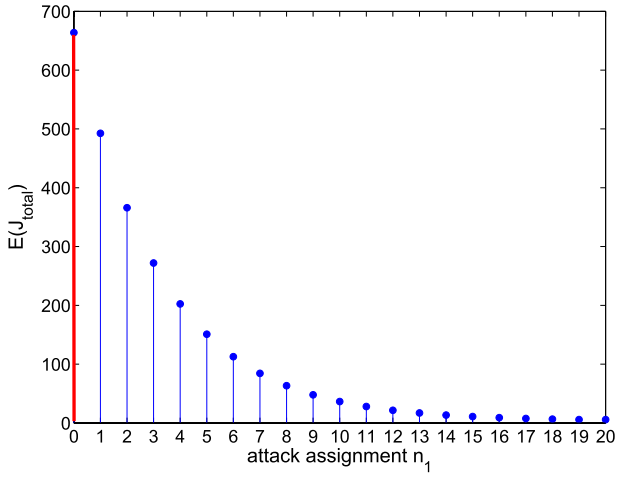

Fig. 11. Maximal value of cost $\mathbb{E}(J_{\text{total}})$ under different assignments (n_1, n_2) when $\alpha_1 = 0.1$ and $\alpha_2 = 0.6$. Here, $n_2 = 20 - n_1$ and $A_2 = 1.5$. The optimal assignment is $(n_1^*, n_2^*) = (0, 20)$.

From (19), we can see that the objective function is the polynomial function of α_1, α_2. The system parameters determine the coefficients of the polynomial function, and thus affect the optimal assignment (n_1^*, n_2^*). In order to show the impact of system parameters on the attack assignment, we change the parameter A_2 in subsystem 2 with $A_2 = 1.5$. Fig. 11 shows the variation of maximal value of $\mathbb{E}(J_{\text{total}})$ under different assignment (n_1, n_2) when $A_2 = 1.5$. We can see that the optimal attack assignment for this new WNCS is different from that in Fig. 9.

We also compare the effect of different attack schedules in Fig. 12. The top curve is the variation of $\mathbb{E}(J_{\text{total}})$ under

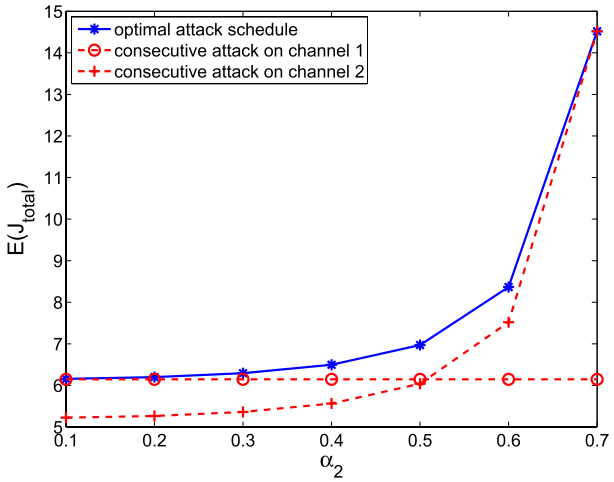

Fig. 12. Illustration of the effect on cost $\mathbb{E}(J_{\text{total}})$ under optimal attack schedule. Two reference curves are the cost $\mathbb{E}(J_{\text{total}})$ under consecutive attack $n_1 = n = 20$ times on channel 1 and consecutive attack $n_2 = n = 20$ times on channel 2, respectively. Here, $\alpha_1 = 0.2$.

optimal attack schedule with increasing α_2. Two reference curves are the cost $\mathbb{E}(J_{\text{total}})$ under consecutive attack on channel 1 and consecutive attack on channel 2, respectively. One can also see that when $\alpha_2 < 0.2$, the effect of optimal attack schedule and that of consecutive attack on channel 1 are very close. Thus, consecutive attack $n_1 = n = 20$ times on channel 1 is a suboptimal attack schedule when $\alpha_2 < 0.2$. Similarly, we can also see that consecutive attack $n_2 = n = 20$ times on channel 2 is a suboptimal attack schedule when $\alpha_2 > 0.6$.

VII. CONCLUSION

In this paper, we studied the optimal DoS attack policy with the energy constraint to maximize the LQG cost function. We first formulated an optimization problem from the perspective of a DoS attacker, in which the attacker can jam the transmission channel with limited actions in any active period. Then, we analyzed the properties of the LQG cost function under any given feasible attack schedule. The optimal attack schedules and corresponding expected cost are obtained, which demonstrate that grouping the limited attacks together in every active period is optimal. We further studied the system stability under optimal attack schedules. We also investigated the optimal attack schedule in WNCS with multiple subsystems.

Simulation examples demonstrate the effectiveness of the proposed optimal jamming attack policy.

APPENDIX

In this section, we prove Lemmas 3.2, 3.3, and 3.4 and Corollary 5.1.

Proof of Lemma 3.2: If $P_1 \geq P_2$, we have

$$\begin{aligned} f(P_1) - f(P_2) &= \mathrm{Tr}(MP_1) - \mathrm{Tr}(MP_2) \\ &= \mathrm{Tr}[M(P_1 - P_2)] \geq 0. \end{aligned}$$

■

Proof of Lemma 3.3: Since $\gamma_s = 0$ and $\gamma_{s+1} = 1$, we have $P_s = 0$ and $P_{s+1} = \mathbb{E}[w_s w_s'] = \Sigma_w$ with probability α, and $P_{s+1} = 0$ with probability $1-\alpha$. By the recursive method for time $s+k$, one has

$$\Pr\{P_{s+k} = H_i\} = \begin{cases} \alpha^i - \alpha^{i+1}, & i = 0, 1, \ldots, k-1, \\ \alpha^k, & i = k, \end{cases}$$

where $H_0 = 0$.

Then, we can see that

$$\begin{aligned} \mathbb{E}[P_{s+k}] &= \sum_{i=0}^{k} H_i \Pr\{P_{s+k} = H_i\} \\ &= \sum_{i=0}^{k-1} (\alpha^i - \alpha^{i+1}) H_i + \alpha^k H_k \end{aligned}$$

which finishes the proof. ■

Proof of Lemma 3.4:

1) According to the analysis in Section III, we have

$$\begin{aligned} \Gamma_\alpha(t_2) - \Gamma_\alpha(t_1) &= \sum_{k=0}^{t_1} (t_2 - t_1)(\alpha^k - \alpha^{k+1}) H_k + \sum_{k=t_1+1}^{t_2} \\ &\quad \times [(t_2 - k)(\alpha^k - \alpha^{k+1}) + \alpha^k] H_k \geq 0. \end{aligned}$$

2) It can be seen that

$$\begin{aligned} &\Gamma_\alpha(t) - \Gamma_\alpha(t_1 \oplus t_2) \\ &= \sum_{k=1}^{t_2} \left[\alpha^k (H_{t_1+k} - H_k) + \sum_{i=0}^{k-1} (\alpha^i - \alpha^{i+1})(H_{t_1+i} - H_i) \right] \geq 0. \end{aligned}$$

3) Since the proof of this result is similar to that of 2), it is omitted here.

4) It suffices to prove

$$\Gamma_\alpha(t_1 \oplus t_2) \leq \Gamma_\alpha((t_1 - 1) \oplus (t_2 + 1))$$

with $t_1 \leq t_2$. In fact

$$\begin{aligned} &\Gamma_\alpha((t_1 - 1) \oplus (t_2 + 1)) - \Gamma_\alpha(t_1 \oplus t_2) \\ &= \sum_{k=t_1}^{t_2} \alpha^{k+1} (H_{k+1} - H_k) \geq 0. \end{aligned}$$

■

Proof of Corollary 5.1:

1) From the definition of $\Gamma_\alpha(t)$, we have

$$\begin{aligned} \Gamma_\alpha(t) &= \sum_{j=1}^{t} \left[\sum_{i=0}^{j-1} (\alpha^i - \alpha^{i+1}) H_i + \alpha^j H_j \right] \\ &= \sum_{j=1}^{t} \left[H_0 + \sum_{i=1}^{j} \alpha^i (H_i - H_{i-1}) \right]. \end{aligned}$$

Then, it can be seen that $\Gamma_\alpha(t)$ is monotonically increasing with α when t is fixed. Thus, we have

$$\sum_{i=1}^{r} \Gamma_{\alpha_i}(n_i) \leq \sum_{i=1}^{r} \Gamma_{\alpha_i^*}(n_i) \leq \Gamma_{\alpha_i^*}(\hat{n}),$$

where $n_1 + n_2 + \cdots + n_r = \hat{n}$. It implies that consecutive attack $\hat{n}$ times over channel i^* in the active periods is optimal.

2) Since $e_{j^*} = \min e_j$, we have

$$\sum_{i=1}^{r} n_i e_{j^*} \leq \sum_{i=1}^{r} n_i e_i \leq e_{\text{total}},$$

which implies

$$\sum_{i=1}^{r} n_i \leq \tilde{n} = \left\lfloor \frac{e_{\text{total}}}{e_{j^*}} \right\rfloor.$$

From Lemma 3.4, we can see that $\Gamma_\alpha(t)$ is monotonically increasing with t when α is fixed. Then, it can be seen that

$$\begin{aligned} \sum_{i=1}^{r} \Gamma_{\alpha_i}(n_i) &= \sum_{i=1}^{r} \Gamma_{\alpha_{j^*}}(n_i) = \Gamma_{\alpha_{j^*}}(n_1 \oplus n_2 \oplus \cdots \oplus n_r) \\ &\leq \Gamma_{\alpha_{j^*}}(\tilde{n}). \end{aligned}$$

Thus, we can infer that the consecutive attack $\tilde{n}$ times over channel j^* in every active period is optimal. ■

REFERENCES

[1] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal Denial-of-Service attack scheduling against linear quadratic Gaussian control," in *Proc. Amer. Control Conf.*, 2014, pp. 3996–4001.

[2] P. Antsaklis and J. Baillieul, "Special issue on technology of networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 5–8, Jan. 2007.

[3] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Trans. Ind. Electron.*, vol. 57, no. 7, pp. 2527–2535, Jul. 2010.

[4] Y. Wang, S. X. Ding, D. Xu, and B. Shen, "An H_∞ fault estimation scheme of wireless networked control systems for industrial real-time applications," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 6, pp. 2073–2086, Nov. 2014.

[5] A. A. Cárdenas, S. Amin, and S. S. Sastry, "Research challenges for the security of control systems," in *Proc. 3rd Conf. Hot Topics Secur.*, 2008, Art. ID 6.

[6] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[7] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.

[8] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Syst.*, vol. 35, no. 1, pp. 24–45, Feb. 2015.

[9] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal Denial-of-Service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, doi: 10.1109/TAC.2015.2409905.

[10] 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*. Berlin, Germany: Springer-Verlag, 2009, pp. 31–45.
[11] M. Zhu and S. Martínez, "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.
[12] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, "Resilient control of cyber-physical systems against Denial-of-Service attacks," in *Proc. 6th Int. Symp. Resilient Control Syst.*, 2013, pp. 54–59.
[13] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in *Proc. IEEE 52nd Annu. Conf. Decision Control*, Dec. 2013, pp. 5444–5449.
[14] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA, USA: Artech House, 2011.
[15] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decision Control*, Dec. 2010, pp. 1096–1101.
[16] H. S. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic Denial-of-Service jamming attacks," in *Proc. IEEE 51st Annu. Conf. Decision Control*, Dec. 2012, pp. 2551–2556.
[17] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.
[18] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1119–1133, Aug. 2010.
[19] M. Zuba, Z. Shi, Z. Peng, and J.-H. Cui, "Launching Denial-of-Service jamming attacks in underwater sensor networks," in *Proc. 16th ACM Int. Workshop Underwater Netw.*, 2011, p. 12.
[20] V. Gupta, B. Hassibi, and R. M. Murray, "Optimal LQG control across packet-dropping links," *Syst. Control Lett.*, vol. 56, no. 6, pp. 439–446, 2007.
[21] K. Xin, X. Cao, J. Chen, P. Cheng, and L. Xie, "Optimal controller location in wireless networked control systems," *Int. J. Robust Nonlinear Control*, vol. 25, no. 2, pp. 301–319, Jan. 2015.
[22] L. Shi, Y. Yuan, and H. Zhang, "Sensor data scheduling for linear quadratic Gaussian control with full state feedback," in *Proc. Amer. Control Conf.*, 2012, pp. 2030–2035.
[23] Y. M. Cho and P. Gyugyi, "Control of rapid thermal processing: A system theoretic approach," *IEEE Trans. Control Syst. Technol.*, vol. 5, no. 6, pp. 644–653, Nov. 1997.
[24] P. Lancaster and L. Rodman, *Algebraic Riccati Equations*. Oxford, U.K.: Oxford Univ. Press, 1995.
[25] V. Gupta, R. M. Murray, L. Shi, and B. Sinopoli, "Networked sensing, estimation and control systems," Dept. Control Dyn. Syst., California Inst. Technol., Pasadena, CA, USA, Tech. Rep., 2009.
[26] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, and S. S. Sastry, "Optimal control with unreliable communication: The TCP case," in *Proc. Amer. Control Conf.*, 2005, pp. 3354–3359.
[27] A. Cervin and T. Henningsson, "Scheduling of event-triggered controllers on a shared network," in *Proc. IEEE Conf. Decision Control*, Dec. 2008, pp. 3601–3606.
[28] S.-L. Dai, H. Lin, and S. S. Ge, "Scheduling-and-control codesign for a collection of networked control systems with uncertain delays," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 1, pp. 66–78, Jan. 2010.
[29] 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.*, 2007, pp. 352–357.

Heng Zhang received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China.

He is currently a Faculty Member with the Huaihai Institute of Technology, Lianyungang, China. His current research interests include security and privacy in cyber-physical systems, control, and optimization theory.

Peng Cheng (M'10) received the B.E. degree in automation and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively.

He is currently an Associate Professor with the Department of Control Science and Engineering, Zhejiang University. His current research interests include networked sensing and control, cyber-physical systems, and robust control.

Prof. Cheng serves as an Associate Editor of *Wireless Networks* and the *International Journal of Communication Systems*. He served as a Guest Editor of the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He was the Publicity Co-Chair of the IEEE Mobile Adhoc and Sensor Systems in 2013, and the Local Arrangement Chair of ACM MobiHoc 2015.

Ling Shi (M'08) received the B.S. degree in electrical and electronic engineering from The Hong Kong University of Science and Technology, Hong Kong, in 2002, and the Ph.D. degree in control and dynamical systems from the California Institute of Technology, Pasadena, CA, USA, in 2008.

He is currently an Associate Professor with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology. His current research interests include networked control systems, wireless sensor networks, event-based state estimation and sensor scheduling, and smart energy systems.

Prof. Shi serves as a Subject Editor of the *International Journal of Robust and Nonlinear Control*. He served as a Guest Associate Editor of the Special Issue on Secure Detection, Estimation, and Control in Cyber-Physical Systems in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and a Guest Associate Editor of the Special Issue on Secure Control of Cyber Physical Systems in the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS in 2015.

Jiming Chen (M'08–SM'11) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2000 and 2005, respectively.

He was a Visiting Researcher with the French Institute for Research in Computer Science and Automation, Rocquencourt, France, in 2006, the National University of Singapore, Singapore, in 2007, and the University of Waterloo, Waterloo, ON, Canada, from 2008 to 2010. He is currently a Full Professor with the Department of Control Science and Engineering, and the Vice Director of the State Key Laboratory of Industrial Control Technology and the Institute of Industrial Process Control, Zhejiang University. His current research interests include sensor networks and networked control.

Prof. Chen serves as an Associate Editor of several international journals, including the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM, the IEEE NETWORK, and the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He was a Guest Editor of the IEEE TRANSACTIONS ON AUTOMATIC CONTROL.