Optimal Denial-of-Service Attack Scheduling With Energy Constraint

Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen

***Abstract*—Security of Cyber-Physical Systems (CPS) has gained increasing attention in recent years. Most existing works mainly investigate the system performance given some attacking patterns. In this technical note, we investigate how an attacker should schedule its Denial-of-Service (DoS) attacks to degrade the system performance. Specifically, we consider the scenario where a sensor sends its data to a remote estimator through a wireless channel, while an energy-constrained attacker decides whether to jam the channel at each sampling time. We construct optimal attack schedules to maximize the expected average estimation error at the remote estimator. We also provide the optimal attack schedules when a special intrusion detection system (IDS) at the estimator is given. We further discuss the optimal attack schedules when the sensor has energy constraint. Numerical examples are presented to demonstrate the effectiveness of the proposed optimal attack schedules.**

***Index Terms*—DoS attack, energy constraint, state estimation.**

I. Introduction

Recently, Cyber-Physical Systems (CPS), in which information and physical elements are closely integrated, have gained much research interest from various aspects [3]–[5]. Applications of CPS have a wide spectrum, such as battle field, smart grid, smart building, intelligent transportation, etc. CPS are vulnerable to different types of malicious attacks which make the security a fundamental issue for reliable services [3]. A famous example is that in June 2010 a cyber worm named "stuxnet" attacked an Iranian nuclear facility at Natanz, which resulted in 60% hosts damaged [6].

Researchers have investigated security issues in CPS from different perspectives recently [7], [8]. Teixeira *et al.* [8] summarized the characteristics of network attacks and defined an attack space with the adversary's priori knowledge of the system model, its disclosure, and disruption resources. Typical attacks can be categorized into Denial-of-Service (DoS) attack, replay data attack, and false data injection attack [8]. *DoS attack* that blocks the communication between the system components has been well studied, since it is the most reachable attack pattern in the attack space [9]. Besides the theoretical research on DoS attack, some experiments were also conducted to demonstrate the effect of DoS attacks [10].

In practice, energy constraint is a natural concern for various types of attackers, which will affect their attack policies [11]–[13]. Law *et al.* [11] pointed out that jammers may run out of energy very fast when their energy budget is limited. Kavitha *et al.* [12] introduced a random DoS attacker who randomly decides to jam the channel or sleep in order to save the energy.

Most existing works mainly investigate the system performance for given attack patterns. The study of the adversary's optimal attack schedules and the corresponding consequences is an important aspect in CPS security as pointed out in [14]. Motivated by this, we aim to answer how to optimally schedule the attack so as to maximize the attacking effect on a CPS. Specifically, we consider a system where one sensor processes the measurements and sends the data to a remote estimator through a wireless channel. An attacker has a limited attacking energy budget, and decides at each sampling time whether or not to jam the channel in order to degrade the remote estimation quality. To the best of our knowledge, this is the first work on the DoS attack schedules against remote state estimation. The main contributions of this technical note are summarized as follows:

1) We construct the optimal DoS attack schedules, which maximize the expected average estimation error.
2) We present the optimal attack schedules when a special IDS in the estimator is given.
3) We further present the optimal attack schedules when both the sensor and the attacker have energy constraints.

The remainder of the technical note is organized as follows. In Section II, we formulate the attack schedule problems. In Section III, we construct the optimal DoS attack schedules for maximizing the expected average estimation error. In Section IV, we present the optimal attack schedules for avoiding a given intrusion detection system. In Section V, we study the optimal attack schedules when the sensor also has energy constraint. In Section VI, numerical examples are shown to illustrate the results. Finally, Section VII concludes the technical note.

Notations: $\mathbb{S}_+^n$ stands for the set of $n \times n$ positive semi-definite matrices. $\mathbb{Z}^+$ stands for the set of positive integers. $\mathbb{E}[X]$ is the mean of random variable X, and $\mathbb{E}[X|Y]$ is the mean of random variable X conditioned on Y, respectively. $\|\gamma\|_0$ is used to denote the zero norm of γ, which is the number of nonzero entries of the vector γ. $Tr(\cdot)$ represents the trace of matrix.

II. Problem Formulation and Preliminaries

A. Problem Formulation

Consider the following system (Fig. 1):

$$\begin{aligned} x_{k+1} &= Ax_k + w_k \\ y_k &= Cx_k + v_k \end{aligned} \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$ is the system state with $n_x \in \mathbb{Z}^+$, $y_k \in \mathbb{R}^{n_y}$ is the sensor measurement with $n_y \in \mathbb{Z}^+$, $w_k \in \mathbb{R}^{n_x}$ is the process noise, $v_k \in \mathbb{R}^{n_y}$ is the measurement noise, and w_k and v_k are uncorrelated

Manuscript received June 9, 2014; revised October 19, 2014, February 1, 2015, and February 11, 2015; accepted February 14, 2015. Date of publication March 4, 2015; date of current version October 26, 2015. This work was supported in part by the NSFC under Grant U1401253, the National Program for Special Support of Top-Notch Young Professionals, Fundamental Research Funds for the Central Universities 2014XZZX003-25, NCET-11-0445, and by an HKUST Caltech Partnership FP004. This work was presented in part at the IEEE CDC 2013, Florence, Italy, December 2013. Recommended by Associate Editor W. X. Zheng. *(Corresponding author: Peng Cheng.)*

H. Zhang, P. Cheng, and J. Chen are with State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China (e-mail: ezhangheng@gmail.com; pcheng@iipc.zju.edu.cn; jmchen@iipc.zju.edu.cn).

L. Shi is with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong, China (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/TAC.2015.2409905

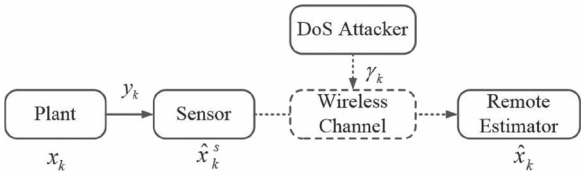

Fig. 1. Schematic of attack on the network.

zero mean Gaussian noises with covariance Σ_w and Σ_v, respectively. The pair (A, C) is assumed to be observable and $(A, \Sigma_w^{1/2})$ is controllable.

After y_k is obtained, the sensor pre-estimates the state x_k, and then sends its minimum mean squared error (MMSE) estimate $\hat{x}_k^s = \mathbb{E}[x_k|y_1, \ldots, y_k]$ to a remote estimator through a wireless channel.

We consider the scenario that there is an attacker which degrades the remote estimation quality by jamming the wireless channel. The attacker has a limited energy budget and has to determine whether to jam the channel or not at each sampling time. It is assumed that the packet will arrive at the remote estimator if there is no DoS attack during the transmission.

Denote $\gamma_k = 1$ or 0 as the attacker's decision variable at time k, and γ as a schedule that defines γ_k at each k. When the attacker launches an attack and jams the channel, the sensor data packet will be dropped with probability α. Denote $\theta_k = 1$ or 0 as the indicator function whether the data packet drops or not. We assume that θ_k's are i.i.d. Bernoulli random variables with $\mathbb{E}(\theta_k) = \alpha$.[1]

Denote all the data packets received at the estimator until time k as $D(\gamma_{1:k})$. The remote estimator then computes its own MMSE estimate $\hat{x}_k$ and its corresponding estimation error covariance P_k based on $D(\gamma_{1:k})$, i.e., $\hat{x}_k(\gamma_{1:k}) = \mathbb{E}[x_k|D(\gamma_{1:k})]$ and $P_k(\gamma_{1:k}) = \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)'|D(\gamma_{1:k})]$. For simplicity, we write $\hat{x}_k(\gamma_{1:k})$ as $\hat{x}_k$, etc., when the schedule $\gamma_{1:k}$ is given.

Consider a finite horizon T. Due to the finite energy constraint, we assume that the attacker can only launch n attacks from $k = 1$ to $k = T$, i.e., $\|\gamma\|_0 = n$.

Average Error: For a given attack schedule γ, define $J_a(\gamma)$ as the average expected estimation error covariance matrix, i.e.,

$$J_a(\gamma) = \frac{1}{T}\sum_{k=1}^{T} \mathbb{E}\left[P_k(\gamma_k)\right].$$

In this technical note, we aim to solve the following problem in the viewpoint of the attacker:

Problem 2.1:

$$\max_{\gamma\in\Gamma} Tr\left[J_a(\gamma)\right]$$
$$s.t.\ \|\gamma\|_0 = n,$$

where $\Gamma = \{0, 1\}^T$ is the set of all possible attack schedules.

III. Optimal Attack Schedule Analysis

A. State Estimation Under DoS Attack

In this section, we present some properties of the estimation error at the remote estimator under a DoS attack.

The MMSE estimate $\hat{x}_k^s$ is obtained from a standard Kalman filter. Let P_k^s be the estimation error covariance matrix of $\hat{x}_k^s$. Standard Kalman filtering analysis shows that P_k^s converges exponentially to its steady-state value $\overline{P}$[16]. For brevity, we assume $\Pi_0 = \overline{P}$, then it can be easily obtained that $P_k^s = \overline{P}$ for all $k \in [1, T]$. Define $h, h^k : \mathbb{S}_+^{n_x} \to \mathbb{S}_+^{n_x}$ as $h(X) \triangleq AXA' + \Sigma_w$, and $h^k(X) \triangleq \underbrace{h \circ h \circ \cdots \circ h}_{k \text{ times}}(X)$.

From [17], the following result holds.

Lemma 3.1: The function h has following property:

$$\overline{P} \le h(\overline{P}) \le h^2(\overline{P}) \le \cdots \le h^k(\overline{P}) \le \cdots, \quad \forall k \in \mathbb{Z}^+.$$

It is straightforward to show that at the remote estimator, $\hat{x}_k$ and P_k are obtained as follows [18]:

$$(\hat{x}_k, P_k) = \begin{cases} \left(A\hat{x}_{k-1}, h(P_{k-1})\right), & \text{if } \gamma_k = 1 \text{ and } \theta_k = 1; \\ \left(\hat{x}_k^s, \overline{P}\right), & \text{otherwise.} \end{cases}$$

Assume that the data packet is delivered to the remote estimator successfully at time s, and the attacker launches m consecutive attacks from time $s+1$ to $s+m$. The state space of the error covariance matrix P_k in this period is $\{\overline{P}, h(\overline{P}), \ldots, h^m(\overline{P})\}$.

We can see that the error covariance matrix P_k during the consecutive attack period $[s+1, s+m]$ is a stationary Markov chain, and the transition probability matrix (p_{ij}) is given by

$$p_{ij} = Pr\left\{P_k = h^j(\overline{P}) | P_{k-1} = h^i(\overline{P})\right\} = \begin{cases} \alpha, & j = i+1; \\ 1-\alpha, & j = 0; \\ 0, & others \end{cases} \quad (2)$$

$i, j = 0, 1, 2, \ldots, m$. Moreover, we have the following properties for $P_k, k \in [s+1, s+m]$.

Property 3.1: During the consecutive attack period $[s+1, s+m]$:

1) the distribution of the error covariance matrix P_{s+k} can be computed as

$$Pr\left\{P_{s+k} = h^i(\overline{P})\right\} = \begin{cases} \alpha^i - \alpha^{i+1}, & i = 0, 1, \ldots, k-1; \\ \alpha^k, & i = k. \end{cases}$$

2) the conditional probability can be computed as follows:

$$Pr\left\{P_{s+k} = h^j(\overline{P}) | P_s = h^i(\overline{P})\right\} = \begin{cases} \alpha^j - \alpha^{j+1}, & j = 0, \ldots, k-1; \\ \alpha^k, & j = i+k. \end{cases}$$

This property can be easily obtained from (2) by mathematical induction method. Due to the space limitation, the proof is omitted.

Property 3.2: 1) If the packet is not received at the remote estimator at time s, then $\mathbb{E}[P_{s+m}|P_s \ge \overline{P}] \ge \mathbb{E}[P_{s+m}|P_s = \overline{P}]$.

2) Consider two different consecutive attacking periods, n_1 and n_2, where $n_1 \ge n_2$. Then $\mathbb{E}[P_{s+n_1}] \ge \mathbb{E}[P_{s+n_2}]$.

An attack scheme with given attacking number n can be divided into the following consecutive attacking sequences, $k_1, k_2, \ldots, k_s$, i.e.,

$$(0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_1 \text{ times}}, 0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_2 \text{ times}}, 0, \cdots, 0, \underbrace{1, \cdots, 1}_{k_s \text{ times}}, 0, \cdots, 0),$$

where $\sum_{i=1}^{s} k_i = n$. Note that each neighboring sequences are divided by at least one zero. Using *Property 3.1*, we have

$$J_a(\gamma) = \frac{1}{T}\sum_{k=1}^{T} \mathbb{E}\left[P_k(\gamma_k)\right] = \frac{1}{T}\sum_{i=1}^{s}\sum_{n_i=1}^{k_i} \mathbb{E}\left[P_{s_i+n_i}\right] + \frac{T-n}{T}\overline{P}$$

$$= \frac{1}{T}\sum_{i=1}^{s}\sum_{n_i=1}^{k_i}\left[\sum_{m=0}^{n_i-1} h^m(\overline{P})(\alpha^m - \alpha^{m+1}) + \alpha^{n_i} h^{n_i}(\overline{P})\right] + \frac{T-n}{T}\overline{P}. \quad (3)$$

Note that (3) is independent of the attack start sequence $s_i, i = 1, 2, \ldots, s$, which means that any permutation of the k_i's will lead to

[1] Since the bit error rate (BER) is fixed in every attack time when the attacker exploits the same energy to jam the channel [15], we assume that the rate of successful attacks follows a Bernoulli probability distribution.

the same average expected estimation error. Thus, for the consecutive attack sequences $k_1, k_2, \ldots, k_s$, we define $\gamma_{1:T}^{k_1\oplus k_2\oplus\cdots\oplus k_s}$ as the set of attack schedules which have the same performance $J_{a,1:T}^{(k_1\oplus k_2\oplus\cdots\oplus k_s)}$. For simplicity, we write $\gamma_{1:T}^{k_1\oplus k_2\oplus\cdots\oplus k_s}$ as $\gamma^{k_1\oplus k_2\oplus\cdots\oplus k_s}$, and write $J_{a,1:T}^{(k_1\oplus k_2\oplus\cdots\oplus k_s)}$ as $J_a^{(k_1\oplus k_2\oplus\cdots\oplus k_s)}$, when the time horizon $[1, T]$ is given. In particular, let γ^n be the set of attack schedules with a consecutive attack sequence n, which have the same performance $J_a^{(n)}$. From Property 3.2, we have following property.

Property 3.3: The following statements are true.

1) $J_a^{(n_1)} \le J_a^{(n_2)}$, where $n_1 \le n_2$.
2) $J_a^{(n_1\oplus n_2)} \le J_a^{(n)}$, where $n = n_1 + n_2$.
3) $J_a^{(n_1\oplus n_2\oplus\cdots\oplus n_s)} \le J_a^{(n)}$, where $n = n_1 + n_2 + \cdots + n_s$.
4) $J_a^{(m_1\oplus m_2)} \le J_a^{(n_1\oplus n_2)}$, where $m_1 + m_2 = n_1 + n_2$ and $\max\{m_1, m_2, n_1, n_2\}$ is n_1 or n_2.

From statements 1) and 4) in *Property 3.3*, we can see that the more the attack times are grouped together, the lager the system cost becomes. Statements 2) and 3) demonstrate that consecutive attack is much better than scattered attack from the viewpoint of attacker.

B. Optimal Attack Schedule Design

Now we are ready to present the optimal attack schedule for *Problem 2.1*.

Theorem 3.1: The optimal attack schedule that solves *Problem 2.1* is anyone that belongs to γ^n, and the corresponding cost is given by

$$Tr(J_a)_{\max} = \frac{1}{T}\sum_{i=1}^{n} Tr\left[h_i(\alpha, \overline{P})\right] + \frac{T - n\alpha}{T} Tr(\overline{P}), \quad (4)$$

where $h_i(\alpha, \overline{P}) = [(n-i)(\alpha^i - \alpha^{i+1}) + \alpha^i]h^i(\overline{P})$.

Proof: A direct result from *Property 3.3* 2) and 3). ■

As a byproduct, we can obtain the worst attack strategy which minimizes the expected average error covariance.

Problem 3.1:

$$\min_{\gamma\in\Gamma} Tr\left[J_a(\gamma)\right]$$
$$s.t.\ \|\gamma\|_0 = n.$$

The solution of *Problem 3.1* is given by the following theorem.

Theorem 3.2: 1) If $n \le (1/2)T$, an optimal solution for *Problem 3.1* is anyone in $\gamma^{1\oplus 1\oplus\cdots\oplus 1}$, and the corresponding cost is given by

$$Tr(J_a)_{\min} = \frac{T - n\alpha}{T} Tr(\overline{P}) + \frac{n\alpha}{T} Tr\left[h(\overline{P})\right]. \quad (5)$$

2) If $n > (1/2)T$, an optimal solution for *Problem 3.1* is

$$\underbrace{(\underbrace{1\cdots1}_{z\text{ times}}0)\cdots(\underbrace{1\cdots1}_{z\text{ times}}0)}_{r_1\text{ times}}(\underbrace{1\cdots1}_{m_1\text{ times}}\ 0\ \underbrace{1\cdots1}_{m_2\text{ times}})\underbrace{(0\underbrace{1\cdots1}_{z\text{ times}})\cdots(0\underbrace{1\cdots1}_{z\text{ times}})}_{r_2\text{ times}}$$

where $r_1 + r_2 = T - n - 1$, $z = \lfloor n/(T-n)\rfloor$,[2] and $m_1 = m_2 = m/2$ if m is even, $m_1 = \lfloor m/2\rfloor, m_2 = m - m_1$ or $m_1 = \lfloor m/2\rfloor + 1, m_2 = m - m_1$ if m is odd, with $m = z + [n\ mod\ (T-n)]$.[3] The resulting cost is

$$Tr(J_a)_{\min} = \frac{1}{T}Tr\Bigg\{(T-n-1)\sum_{i=1}^{z} h_i(\alpha, \overline{P}) + \sum_{i=1}^{m_1} h_i(\alpha, \overline{P}) + \sum_{i=1}^{m_2} h_i(\alpha, \overline{P}) + [(T-n) + m(1-\alpha) + z(1-\alpha)(T-n-1)]\,\overline{P}\Bigg\}, \quad (6)$$

where $h_i(\alpha, \overline{P}) = [(n-i)(\alpha^i - \alpha^{i+1}) + \alpha^i]h^i(\overline{P})$.

Proof: A direct result from *Property 3.3* 3) and 4). ■

From the above two theorems, one can see that grouping the attacks together leads to maximal attacking effect, while separating the attacks as uniformly as possible leads to the minimal degradation. Thus the results can be viewed as the upper and lower bound of the damage an arbitrary attack schedule can make.

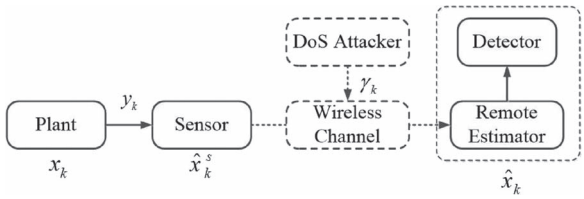

Fig. 2. Schematic of attack on the network against state estimation with an intrusion detector.

IV. Optimal Attack Schedules Against a Given IDS

The aforementioned problems are discussed under the assumption that the channel is perfect and there is no defensive measure. In practical applications, when the estimator considers unknown factors from environment changes or adversary's intrusion, which may lead to data drops, a detector is often designed at the receiver side as a first step to reduce the effectiveness of these factors (Fig. 2). For example, packet reception rate (PRR) at the receiver side is proposed as the criteria for intrusion detection in [19]. PRR is the rate of packets reception that are successfully delivered to the estimator compared to the number of packets that have been sent out by the sensor.

In practice, the PRR can be computed for a given length of a time window τ, i.e., $PRR = \sigma/\tau$, where σ is the packet reception numbers in the time window. If the PRR is too small, the detector will deduce that there may exist an attacker, which triggers an alarm to alert the sensor. Then the sensor can use channel hopping technology to guarantee the packet can be received by the remote estimator [20]. In this technical note, we assume that the alarm is triggered if $PRR \le PRR_0$, where PRR_0 is a given alarm bound.[4]

Before introducing the attack schedule against the IDS mechanism, we present a property to help formulate the attack optimization problem.

Property 4.1: The alarm triggering condition $PRR \le PRR_0$ is equivalent to $P_k \nleq h^d(\overline{P}), k = 1, 2, \ldots, T$, where $d = \tau - \sigma_0$, $\sigma_0 = \max\{\sigma | (\sigma/\tau) \le PRR_0\}$.

Proof: See the Appendix. ■

[2] $\lfloor x\rfloor$ is floor function, which is defined as the largest integer that is less than real number x.

[3] mod is defined as modulo operation, i.e., $n\ \mod\ m$ is the remainder in division n/m, where n and m are two positive integer.

[4] By utilizing the pseudo-random sequence, the sensor and estimator may implement channel hopping once the alarm is triggered [21]. However, the attacker can detect such channel switch by detecting the alarm signal, and search the new communication channel by scanning the wireless spectrum. In this way, the attacker can learn the alarm bound through statistical analysis, and follow the design against such IDS mechanism.

Remark 4.1: From *Property 4.1*, any attack schedule with at most d times consecutive attack, i.e., $\sum_{i=k+1}^{k+\tau}\gamma_i \le d, k=0,1,\ldots,T-\tau$, can guarantee that the attack action will not be detected by the estimator. In fact, time window τ and threshold PRR_0 can be evaluated by the attacker when he eavesdrops the transmission channels before taking attack actions.

In order not to be detected by IDS, we consider *Problem 2.1* with an additional constraint, i.e.,

Problem 4.1:

$$\begin{aligned}\max_{\gamma\in\Gamma}\quad & Tr\left[J_a(\gamma)\right]\\ s.t.\quad & \|\gamma\|_0 = n,\\ & \sum_{i=k+1}^{k+\tau}\gamma_i \le d,\ k\in[0,T-\tau].\end{aligned}\tag{7}$$

The following result presents the optimal solution to *Problem 4.1*.

Theorem 4.1: Consider *Problem 4.1*. Let $d=\tau-\sigma_0$, where $\sigma_0=\max\{\sigma|(\sigma/\tau)\le PRR_0\}$.

1) If $d\ge n$, any n times consecutive attack is optimal, and the corresponding cost is (4).
2) If $d<n$, the optimal attack schedule has the structure of (8), see equation at the bottom of the page, where $z_0+z_1+z_2+z_3+(s_1+s_2)\sigma_0=T-n$, and $s_1+s_2=m$, where m is the quotient of n/d and r is the remainder. The corresponding cost is

$$Tr(J_a)^{PRR}_{\max}=\frac{1}{T}\left\{m\sum_{i=1}^{d}Tr\left[h_i(\alpha,\overline{P})\right]+\sum_{i=1}^{r}Tr\left[h_i(\alpha,\overline{P})\right]\right\}+\frac{T-n\alpha}{T}Tr(\overline{P}).$$

Proof: See the Appendix. ■

Remark 4.2: In *Problem 4.1*, the attacker can completely avoid the given IDS mechanism. However, this attack schedule seems too cautious from an adventurous attacker's point of view. If the adventurous attacker still decides to use an attack schedule proposed in *Theorem 3.1*, the probability of being detected is $\sum_{k>d}C_\tau^k\alpha^{\tau-k}(1-\alpha)^k$ if $n>\tau$, and is $\sum_{k>d}C_n^k\alpha^{n-k}(1-\alpha)^k$ if $n\le\tau$.

V. Optimal Attack Schedules With Sensor's Energy Constraint

The aforementioned problems are discussed under the assumption that the sensor has sufficient energy to transmit throughout the entire time horizon. When the sensor's energy is also limited and cannot transmit all the time, the attacker needs to change the attacking schedule. Here we assume that the sensor and the estimator do not know the existence of the attacker.

Some literatures have focused on sensor scheduling and optimal state estimation in a lossy network environment [18], [22]–[25]. Sinopoli *et al.* studied the problem of state estimation using Kalman filtering in an i.i.d. packet-dropping network [22]. Reference [23] studied optimal state estimation and optimal LQG controller design over an intermittent packet-dropping network. Mo *et al.* provided a stochastic sensor selection scheme to minimize the asymptotic expected estimation error covariance due to the energy constraint [24]. You *et al.* investigated the stability of the mean estimation error over a network subject to Markovian packet losses [25]. However, these literatures have not considered the state estimation quality when a DoS attacker jams the wireless channel and this shortage motivates us to study the subsequent problem.

Denote $\vartheta_k=1$ or 0 as the sensor's transmission decision variable at time k, and ϑ as a scheduling scheme that defines ϑ_k at each k. Θ is the set of the sensor's transmission schedules. We assume that the sensor has energy constraint with $\|\vartheta\|_0=N$ and we consider the following problem in this section.

Problem 5.1:

$$\max_{\gamma\in\Gamma}\min_{\vartheta\in\Theta}\quad Tr\left[J_a(\vartheta,\gamma)\right]\tag{9}$$

$$s.t.\quad \|\vartheta\|_0=N,\tag{10}$$

$$\|\gamma\|_0=n.\tag{11}$$

From [18], we have the following property:

Property 5.1: Let $q=\lfloor T/N\rfloor$.

1) If $N<(1/2)T$, the optimal sensor schedule $\vartheta^*\in\Theta$ that minimizes the $Tr(J_a)$ has following structure:

$$(1\underbrace{0\ldots0}_{\tau_1\text{ times}})(1\underbrace{0\ldots0}_{\tau_2\text{ times}})\ldots(1\underbrace{0\ldots0}_{\tau_N\text{ times}})\tag{12}$$

in which there are $T-qN$ times $\tau_i=q$ and $(q+1)N-T$ times $\tau_i=q-1$ in $\{\tau_i,i=1,2,\ldots,N\}$.
2) If $N\ge(1/2)T$, ϑ^* has structure (12) with $T-N$ times $\tau_i=1$ and $2N-T$ times $\tau_i=0$ in $\{\tau_i,i=1,2,\ldots,N\}$.

Here, we assume that the attacker obtains the sensor's transmission strategy by eavesdropping the transmission channel over a long period before starting its attack action. We denote $t_{(i)},i=1,2,\ldots,N$ as the sensor's data transmission time. If $n\ge N$, it is obvious that optimal attack schedule is taking actions at full transmission time $t_{(i)},i=1,2,\ldots,N$. Thus we only need to consider *Problem 5.1* for $n<N$ hereinafter.

Theorem 5.1: Consider *Problem 5.1* with $n<N$.

1) When $N<(1/2)T$ and the sensor's schedule ϑ^* has the structure $(1\underbrace{0\ldots0}_{\tau\text{ times}})(1\underbrace{0\ldots0}_{\tau\text{ times}})\ldots(1\underbrace{0\ldots0}_{\tau\text{ times}})$, the optimal attack schedules are given by $\gamma_{t_{(k)}}=1,k=i+1,i+2,\ldots,i+n$, and $\gamma_k=0$ otherwise. The corresponding cost is given by

$$Tr(J_a)_{\max}=\frac{1}{T}\sum_{i=1}^{n}Tr\left[h_i(\alpha,\Delta_\tau)\right]+\frac{N-n\alpha}{T}Tr(\Delta_\tau),$$

where $h_i(\alpha,\Delta_\tau)=[(n-i)(\alpha^i-\alpha^{i+1})+\alpha^i]h^i(\Delta_\tau)$.
2) When $N\ge(1/2)T,\alpha=1$ and the sensor's schedule ϑ^* has the structure $(\underbrace{1\ldots1}_{\delta\text{ times}}0)(\underbrace{1\ldots1}_{\delta\text{ times}}0)\ldots(\underbrace{1\ldots1}_{\delta\text{ times}}0)$, the optimal attack

$$(\underbrace{0\cdots0}_{z_0\text{ times}})(\underbrace{\underbrace{1\cdots1}_{d\text{ times}}\underbrace{0\cdots0}_{\sigma_0\text{ times}}}_{s_1\text{ times}})\cdots(\underbrace{\underbrace{1\cdots1}_{d\text{ times}}\underbrace{0\cdots0}_{\sigma_0\text{ times}}}_{s_1\text{ times}})(\underbrace{0\cdots0}_{z_1\text{ times}}\underbrace{1\cdots1}_{r\text{ times}}\underbrace{0\cdots0}_{z_2\text{ times}})(\underbrace{\underbrace{0\cdots0}_{\sigma_0\text{ times}}\underbrace{1\cdots1}_{d\text{ times}}}_{s_2\text{ times}})\cdots(\underbrace{\underbrace{0\cdots0}_{\sigma_0\text{ times}}\underbrace{1\cdots1}_{d\text{ times}}}_{s_2\text{ times}})(\underbrace{0\cdots0}_{z_3\text{ times}})\tag{8}$$

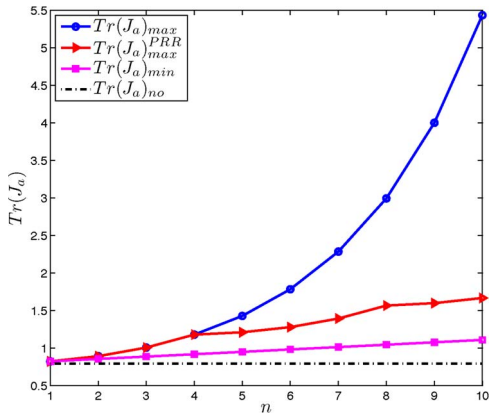

Fig. 3. Illustrating example on $Tr(J)$ under different attack schedules with varying attack times ($T = 100$, $\alpha = 1$).

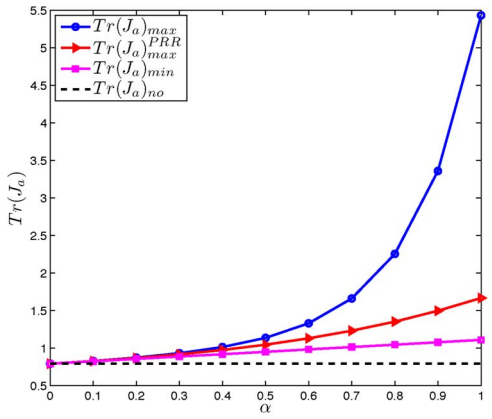

Fig. 4. Illustrating example on $Tr(J)$ under different attack schedules while successful attack probability is varying ($T = 100$).

schedules γ^* are given by $\gamma_{t_{(k)}} = 1, k = i+1, i+2, \ldots, i+n$, and $\gamma_k = 0$ otherwise. The corresponding cost is given by

$$Tr(J_a)_{\max} = \frac{1}{T} Tr\left[(N-n)\overline{P} + (T-N-b)h(\overline{P}) + \sum_{i=1}^{n+b} h^i(\overline{P})\right], \quad (13)$$

where $n = \delta b + b_0$ with $0 \le b_0 < b$.

Proof: 1) The proof is similar to that of *Theorem 3.1*. The only difference is that we replace $\overline{P}$ by Δ_τ.

2) One can easily obtain that the resulting cost under the attack schedule γ^* is (13). For an arbitrary attack schedule γ, we have

$$Tr\left(J_a(\gamma)\right) = \frac{1}{T} Tr\left[(N-n)\overline{P} + m_1 h(\overline{P}) + \sum_{i=1}^{m_2}\sum_{j=1}^{t_i} h^j(\overline{P})\right],$$

where t_i is the length of i-th $(i = 1, 2, \ldots, m_2)$ attack period $[s_i + 1, s_i + t_i]$ which satisfies $\vartheta_{s_i} = 1, \gamma_{s_i} = 0, \vartheta_{s_i+t_i} = 1, \gamma_{s_i+t_i} = 0$, and $\vartheta_k = 1, \gamma_k = 1$ or $\vartheta_k = 0, \gamma_k = 0$ for $k = s_i + 2, \ldots, s_i + t_i - 1$, $(N-n) + m_1 + \sum_{i=1}^{m_2} t_i = T$ and $\sum_{i=1}^{m_2} t_i \le n + b$. Then we have

$$\begin{aligned} &Tr\left(J_a(\gamma^*)\right) - Tr\left(J_a(\gamma)\right) \\ &= \frac{1}{T} Tr\left[\sum_{i=1}^{n+b} h^i(\overline{P}) - \sum_{i=1}^{m_2}\sum_{j=1}^{t_i} h^j(\overline{P}) - [m_1 - (T-N-b)]h(\overline{P})\right] > 0, \end{aligned}$$

which completes the proof. ■

Remark 5.1: In *Theorem 5.1* we study some special cases of *Problem 5.1*, and obtain the optimal attack schedules. Note that these schedules only depend on the sensor transmission schedule ϑ^* rather than on the system parameters. Thus the attacker can run his optimal attack schedules when he obtains the sensor's transmission schedule ϑ^*. The general cases of *Problem 5.1*, however, are complicated since the optimal attack schedules depend on sensor transmission schedule ϑ, the system parameters, and the attack successful probability. An example is given in Section VI (Fig. 5) to illustrate this.

VI. Examples

Consider system (1) with

$$A = \begin{bmatrix} 1.2 & 0.1 \\ 0 & 1 \end{bmatrix}, \; C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; \Sigma_w = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \; \Sigma_v = 0.5C.$$

TABLE I
Attack Schedules

attack schedule	1	2	3	4	5
i with $\gamma_{t_{(i)}} = 1$	1,2,3	2,3,4	3,4,5	1,2,4	1,2,5
attack schedule	6	7	8	9	10
i with $\gamma_{t_{(i)}} = 1$	1,3,4	1,3,5	2,3,5	2,4,5	1,4,5

The effects of different attack schedules are evaluated. In Fig. 3, where we examine the performance under different attack times from 1 to 10 with $T = 100$, $\alpha = 1$. It can be seen that the performance under the optimal attack schedules given by *Theorem 3.1*, i.e., $Tr(J_a)_{\max}$, increases rapidly with the allowable attack times. $Tr(J_a)_{\min}$, which is under the attack schedule obtained in *Theorem 3.2*, and $Tr(J_a)^{PRR}_{\max}$, which is under the attack schedule given in *Theorem 4.1* with $PRR \le (3/7)$, grow much slower than $Tr(J_a)_{\max}$. It also can be found that $Tr(J_a)_{\max}$ and $Tr(J_a)^{PRR}_{\max}$ are overlapping since they have the same optimal attack schedule set γ^n when $n \le 4$. But if $n > 4$, $Tr(J_a)^{PRR}_{\max}$ grows much slower than $Tr(J_a)_{\max}$ as the attack schedules need to be re-designed under the given intrusion detection mechanism. It also can been seen that the attack effectiveness is significantly reduced by this detection constraint.

In Fig. 4, we examine the estimation quality with different successful attack probabilities. In this example, the adversary can attack 10 times in the time horizon [1,100]. From Fig. 4, we can see that $Tr(J_a)_{\max}$ increases rapidly when the success probability α increases. On the other hand, $Tr(J_a)_{\min}$ grows much slower when α increases, which also demonstrates the attack effectiveness of our designed attack schedule. $Tr(J_a)^{PRR}_{\max}$ also grows slower due to the constraint of avoiding being detected.

In Fig. 5, we examine the estimation quality under different attack schedules when the sensor has energy constraint. Here $T = 14$, $N = 5$, $n = 3$. The sensos transmission schedule is chosen as $\vartheta^* = (100)(100)(10)(100)(100)$. There are 10 attack schedules which has been listed in Table I. We assume $\vartheta_{-1} = 1, \vartheta_0 = 0$ for the time $t = -1$,0, respectively. The effectiveness of the attack is studied with attack successful probability $\alpha = 0.8$ and $\alpha = 0.1$ in Fig. 5(a) and (b), respectively. In Fig. 5(a), it can be seen that attack schedule 2 $(\gamma_{t_{(2)}} = \gamma_{t_{(3)}} = \gamma_{t_{(4)}} = 1)$ and attack schedule 3 $(\gamma_{t_{(3)}} = \gamma_{t_{(4)}} = \gamma_{t_{(5)}} = 1)$ are optimal when the attack successful probability $\alpha = 0.8$. However, when $\alpha = 0.1$, from Fig. 5(b) we can see that attack schedule 5 $(\gamma_{t_{(1)}} = \gamma_{t_{(2)}} = \gamma_{t_{(5)}} = 1)$, attack schedule 8 $(\gamma_{t_{(2)}} = \gamma_{t_{(3)}} = \gamma_{t_{(5)}} = 1)$, and attack schedule 9 $(\gamma_{t_{(2)}} = \gamma_{t_{(4)}} = \gamma_{t_{(5)}} = 1)$ are optimal which is different from $\alpha = 0.1$. In general, it is difficult to find these optimal attack schedules explicitly. On the other hand, the

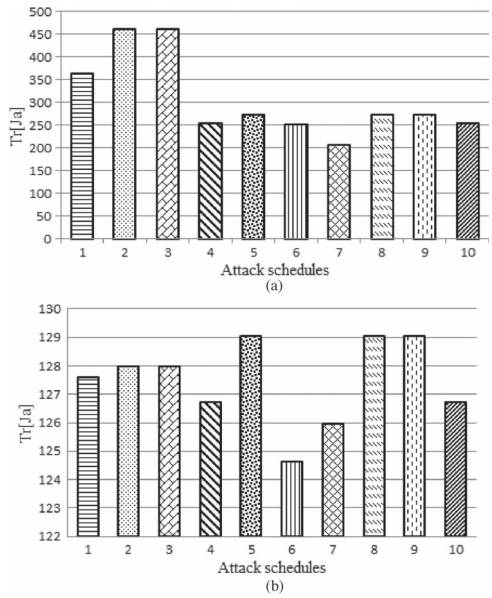

Fig. 5. Illustrating example on trace of average expected error covariance under different attack schedules when the sensor has energy constraint. (a) $\alpha = 0.8$. (b) $\alpha = 0.1$.

suboptimal attack schedules 1, 2, 3 only depend on sensor transmission schedule ϑ, and can be easily obtained.

VII. Conclusion

In this technical note, we considered optimal attack scheduling against remote state estimation through a wireless channel. We proved that consecutive attacks maximize the expected average error covariance. We also showed that when the attacks are separated uniformly, the attack effect on the estimation quality is minimum. We further proposed the optimal attack schedules when a special intrusion detection mechanism in the estimator is available. We finally studied the optimal attack schedules when both the sensor and the attacker have energy constraints. It is interesting but challenging to find a closed-form solution for optimal attack scheduling over packet lossy network environment. This will be left as a future work. We will also formulate the infinite-horizon attack model and study the optimal attack schedule in the future. It is also interesting to consider optimal defensive strategies assuming that the sensor knows the existence of the attacker. We will further validate our results using some physical experiments, and consider optimal attack scheduling against feedback control and evaluating the corresponding effectiveness.

Appendix

A. Proof of Property 4.1

Proof: Alarm triggering condition $PRR \leq PRR_0$ is equivalent to $\sigma \leq \sigma_0$. Thus it is also equivalent to that the packets drop number d_{num} in any time window is larger than $d = \tau - \tau_0$, i.e., $d_{num} > d$.

In order to obtain the result, we prove by contradiction, i.e., $d_{num} \leq d$ is equivalent to $P_k \leq h^d(\overline{P})$, which clearly holds. ■

B. Proof of Theorem 4.1

Proof: If $d \geq n$, any n times consecutive attack schedules satisfy the conditions $P_k \leq h^d(\overline{P}), k = 1, 2, \ldots, T$. Thus these schedules are optimal for *Problem 4.1* when $d \geq n$. From *Remark 4.1* and statements 1) and 3) of *Property 3.3*, we can obtain that optimal attack schedule has the structure (8) if $d < n$. ■

References

[1] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in *Proc. IEEE Conf. Decision and Control (CDC)*, 2013, pp. 5444–5449.

[2] H. Zhang, P. Cheng, L. Shi, and J. Chen, Optimal Denial-of-Service Attack Scheduling in Cyber-Physical Systems, Zhejiang University, Hangzhou, China, Tech. Rep. [Online]. Available: http://www.sensornet.cn/heng/Heng_estimation_Full.pdf

[3] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, no. 99, pp. 1–15, 2012.

[4] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water scada systems-part i: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, 2013.

[5] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Networks*.

[6] J. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[7] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[8] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st Int. Conf. High Confidence Networked Systems*, 2012, pp. 55–64.

[9] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *Hybrid Syst.: Comput. and Control*, pp. 31–45, 2009.

[10] M. Zuba, Z. Shi, Z. Peng, and J. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proc. 6th ACM Int. Workshop on Underwater Networks*, 2011, p. 12.

[11] Y. Law, M. Palaniswami, L. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," *ACM Trans. Sensor Netw.*, vol. 5, no. 1, p. 6, 2009.

[12] T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," *J. Inform. Assur. and Security*, vol. 5, no. 1, pp. 31–44, 2010.

[13] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal Denial-of-Service attack scheduling against linear quadratic gaussian control," in *Proc. American Control Conf. (ACC)*, 2014, pp. 3996–4001.

[14] A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proc. 3rd Conf. Hot Topics in Security*, 2008, pp. 1–6.

[15] R. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA: Artech House, 2011.

[16] G. Gu, X.-R. Cao, and H. Badr, "Generalized lqr control and kalman filtering with relations to computations of inner-outer and spectral factorizations," *IEEE Trans. Autom. Control*, vol. 51, no. 4, pp. 595–605, Apr. 2006.

[17] L. Shi, P. Cheng, and J. Chen, "Optimal periodic sensor scheduling with limited resources," *IEEE Trans. Autom. Control*, vol. 56, no. 9, pp. 2190–2195, 2011.

[18] 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, 2011.

[19] Y. Ponomarchuk and D.-W. Seo, "Intrusion detection based on traffic analysis in wireless sensor networks," in *Proc. Annu. Wireless and Optical Commun. Conf.*, 2010, pp. 1–7.

[20] M. Sha, G. Hackmann, and C. Lu, "Arch: Practical channel hopping for reliable home-area sensor networks," in *Proc. 17th IEEE Real-Time and Embedded Technology and Applications Symp.*, 2011, pp. 305–315.

[21] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proc. 26th IEEE Int. Conf. Computer Communications*, 2007, pp. 2526–2530.

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

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

[24] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "Stochastic sensor scheduling for energy constrained estimation in multi-hop wireless sensor networks," *IEEE Trans. Autom. Control*, vol. 56, no. 10, pp. 2489–2495, Oct. 2011.

[25] K. You, M. Fu, and L. Xie, "Mean square stability for kalman filtering with markovian packet losses," *Automatica*, vol. 47, pp. 2647–2657, 2011.