DoS Attack Energy Management Against Remote State Estimation

Heng Zhang[1], Yifei Qi[2], Junfeng Wu[3], Lingkun Fu[2], and Lidong He[2]

***Abstract*—This paper considers a remote state estimation problem, where a sensor measures the state of a linear discrete-time process and has computational capability to implement a local Kalman filter based on its own measurements. The sensor sends its local estimates to a remote estimator over a communication channel that is exposed to a Denial-of-Service (DoS) attacker. The DoS attacker, subject to limited energy budget, intentionally jams the communication channel by emitting interference noises with the purpose of deteriorating estimation performance. In order to maximize attack effect, following the existing answer to "when to attack the communication channel", in this paper we manage to solve the problem of "how much power the attacker should use to jam the channel in each time". For the static attack energy allocation problem, when the system matrix is normal, we derive a sufficient condition for when the maximum number of jamming operations should be used. The associated jamming power is explicitly provided. For a general system case, we propose an attack power allocation algorithm and show the computational complexity of the proposed algorithm is not worse than $\mathcal{O}(T)$, where T is the length of the time horizon considered. When the attack can receive the real-time ACK information, we formulate a dynamic attack energy allocation problem, and transform it to a Markov Decision Process to find the optimal solution.**

***Index Terms*—Cyber-Physical Systems, Estimation Theory, Sensor Networks, DoS attack.**

I. Introduction

As the next generation engineered systems, Cyber-Physical Systems (CPS), deeply integrate physical plants and cyber elements, significantly improving the system operating performances, e.g., efficiency, stability, and reliability [1]–[6]. CPSs have a variety of applications, including power systems, intelligent transportation, smart building, etc. However, due to the high degree openness of CPSs, they are prone to an increasing number of malicious attacks [7]–[11]. Thus, the security becomes a basic requirement and fundamental issue for CPSs.

[1] H. Zhang is with Huaihai Institute of Technology, Lianyungang, China Dr.Zhang.Heng@ieee.org

[2] Y. Qi, L. Fu, and L. He are with State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China {yifeiqi,lidonghe}@zju.edu.cn, lkfu@iipc.zju.edu.cn

[3] J. Wu is with ACCESS Linnaeus Center, Automatic Control, The Royal Institute of Technology (KTH), Sweden junfengw@kth.se

This work was supported by NSFC under Grant 61503147, 61503337, and 71401060, China Postdoctoral Science Foundation under Grant 2015M571870, Zhejiang Provincial Natural Science Foundation of China under Grant Y16F030011, University Science Research General Project of Jiangsu Province under Grant 15KJB510002, Science and Technology Project of Jiangsu Province under Grant BC2015166, and Lianyungang Science and Technology Project under Grant CG1413, CG1501.

Recent years many researchers have made great efforts to investigate the security issues from different perspectives. An important aspect of research in this field is to analyze and evaluate the vulnerabilities of CPSs to cyber attacks. Specifically, a great number of literatures focused on the the effect of given cyber attacks, including Denial-of-Service (DoS) attack [12], [13], false data injection attacks [14], [15], deception attack [16], [17], against particular systems. Among these typical cyber attacks, DoS attack has gained most attention since it is easy to accomplish and can lead to serious consequences. In fact, DoS attackers can block the communication between system elements by jamming the wireless transmission channel. An important hardware feature of DoS attacker is the limited energy/power budget. For example, the attacker can jam the wireless channels by a software defined radio (GNU Radio combined with USRP boards) or other hardware equipments [18], [19]. These hardware equipments often have limited energy budget.

Some of the literatures focused on effects of DoS attack against the open-loop performance of CPSs, e.g., state estimation error. A practical example is that DoS attack can significantly deteriorate the estimation quality of real-time state in smart grid [20]. Gupta et al. investigated the game between a jammer and a sender [21]. They provided a mixed strategy for the jammer with a limited number of attack actions in the given time horizon. Zhang et al. studied the optimal DoS attack strategy against remote state estimation when the attack energy budget is given [22]. Li et al. analyzed the effect of DoS attack against state estimation from the game-theoretic perspective [23]. Qi et al. considered the online DoS attack design against remote state estimation [24]. They proposed an intelligent event-based DoS attack mechanism, which leverages the real-time measurement, to degrade the mimimum mean square error(MMSE) estimation performance.

Some other literatures investigated close-loop performance of CPSs under DoS attacks. For example, Amin et al. studied the DoS attack against networked control systems, and formulated a semi-definite programming problem to analyze the effect of DoS attack on the stochastic control performance [13]. Claudio et al. studied the effect of energy-constraint DoS attack on the stability of the closed-loop system [25]. They have pointed out that the system is still asymptotically stable when the attack frequency is no more than a certain percentage of time on the average. Zhang et al. evaluated the effect of energy-constrained DoS attack against Linear Quadratic Gaussian (LQG) control and proposed the optimal DoS attack scheduling which can maximize the LQG cost [26]. From the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

viewpoint of DoS attacker, Lee et al. investigated DoS attack strategy against the control of network flow when the attacker has limited energy budget [27]. They designed a passivity-based dynamic DoS attack strategy to redirect the network flow. All these works pointed out that the energy constraint is the main concern when the DoS attacker launches a destructive activity.

In this work, we consider a remote state estimation problem. A sensor measures the state of a linear discrete-time process. The sensor has computational capability to implement a local Kalman filter based on its own measurements. It sends the local estimate to a remote estimator over a communication channel that is exposed to a DoS attacker. The DoS attacker deteriorates estimation performance by emitting interference signals and jamming the communication channel. Higher jamming power leads to larger packet loss probability over the communication channel, while on the other hand limited energy resource is a natural constraint for a DoS attacker. In order to maximize the attack effect, the DoS attacker needs to decide not only when to attack the communication channel but also how much energy the jamming operations should use. Following the work on investigating the optimal attack scheduling against open-loop performance of CPSs in [28], we continue to study the DoS attack strategy design problem against state estimation in this paper. We formulate a DoS attack optimization problem over a finite time horizon, where the trace of expected terminal estimation error covariance is to be maximized. Based the existing work [28] which only focused on "when to attack the communication channel" when the attack power level is given, this paper aims to answer "how much power the attacker should use to jam the channel". To simplify the analysis, we assume the attack energy is constantly used throughout the considered time horizon. Compared with the previous work, the main contributions of this paper are summarized as follows:

1) We prove that a higher jamming power leads to a larger terminal estimation error. When the system matrix is a normal one, we derive a sufficient condition of when the maximum number of jamming operations should be used. The associated jamming power is explicitly provided.
2) For a general case, we propose attack power allocation algorithm. Thanks to the optimality property of continuous jamming operations and the monotonicity property between the attack power and the expected terminal estimation error covariance, we show that the computational complexity of the proposed algorithm is not worse than $\mathcal{O}(T)$, where T is the length of the time horizon considered.
3) For the dynamic attack power allocation problem, we transform it to a Markov Decision Process problem, and present the backward recursive iteration algorithm to solve it.

The remainder of the paper is organized as follows: In Section II, we formulate the attack energy management problem. In Section III, we provide some preliminaries which will help to solve attack energy management problem. In Section IV, we present the optimal attack power for the special case and provide an algorithm to find the optimal power for a general case. In Section V, we study the attack energy allocation problem when the attacker can dynamically determine the attack energy in each time horizon. In Section VI, numerical examples are shown to illustrate the results. Finally, Section VII concludes the paper.

Notations: $\mathbb{R}^n$ is the set of n dimensional vectors with real value. $\mathbb{S}_+^n$ is the set of $n \times n$ positive semi-definite matrices. $\mathbb{Z}^+$ is the set of positive integers. $\mathbb{E}[X]$ stands for the mean of random variable X, and $\mathbb{E}[X|Y]$ stands for the mean of random variable X conditioned on Y, respectively. $Tr(X)$ represents the trace of matrix X. $X \preceq Y$ means that $Y - X$ is nonnegative-definite, i.e., $Y - X \succeq 0$.

II. Problem Statement

A. System model

Consider the system in Fig.1. The plant runs a linear time-invariant (LTI) process as follows

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

where $x_k \in \mathbb{R}^{n_x}, k = 1, 2, \ldots$ with $n_x \in \mathbb{Z}^+$ are the state vectors of the plant, $w_k \in \mathbb{R}^{n_x}$ are the process noises with Gaussian distribution $\mathcal{N}(0, \Sigma_w)$. The initial state is a Gaussian random variable with mean x_0 and covariance Π_0.

The sensor observes the plant and measures the state information with following equation

$$y_k = Cx_k + v_k, \tag{2}$$

where $y_k \in \mathbb{R}^{n_y}, k = 1, 2, \ldots$ with $n_y \in \mathbb{Z}^+$ are the measurement vectors, $v_k \in \mathbb{R}^{n_y}$ are the measurement noises with Gaussian distribution $\mathcal{N}(0, \Sigma_v)$. In addition, the initial state x_0, the process noises w_k, and the measurement noises v_k are uncorrelated with each other. It is assumed that the pair (C, A) is detectable and $(A, \Sigma_w^{\frac{1}{2}})$ is controllable.

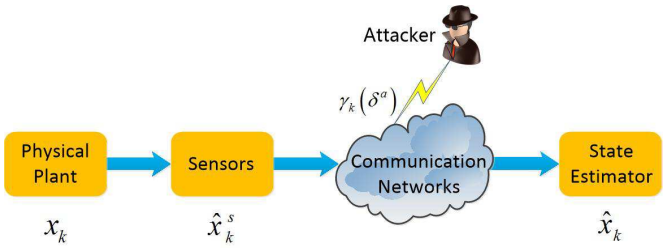


Fig. 1. Block diagram of the overall system.

Based on the obtained measurement y_k, the sensor generates a local estimate of the state x_k subject to the minimum mean squared error (MMSE) criterion, i.e., $\widehat{x}_k^s = \arg\min_{\widetilde{x}_k^s} \mathbb{E}[(e_k^s)(e_k^s)'|\mathcal{I}_k]$, where $e_k^s = \widetilde{x}_k^s - x_k$ is the corresponding estimation error, and $\mathcal{I}_k$ is the set of measurement data until time k [29].

Then the sensor transmits $\widehat{x}_k^s$ to a remote estimator over a wireless communication channel. The wireless communication network is vulnerable to DoS attack. For example, S. Bhattacharya et al. pointed out that it is easy to launch

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

DoS attack to interfere the communication between Unmanned Aerial Vehicles [30].

The remote estimator computes its own MMSE estimate $\widehat{x}_k$ based all the packets received until time k. Let $\mathcal{D}_k$ be the set of received data until time k. Then $\widehat{x}_k = \mathbb{E}[x_k|\mathcal{D}_k]$ and the corresponding estimation error covariance is denoted as $P_k = \mathbb{E}[(e_k)(e_k)'|\mathcal{D}_k]$ with $e_k = \widehat{x}_k - x_k$.

B. DoS attack model

In the remote estimation framework, the wireless channel is corrupted by a DoS attacker, which intentionally jams the sensor-to-estimator communication channel and deteriorates the remote estimation performance. The attacker can implement the jamming attack by a software defined radio (GNU Radio combined with USRP boards) or other hardware equipments [18], [19]. These hardware equipments often have limited energy budget. Different jamming power results in different packet drop probabilities [31].

In our scenario, the attacker itself has limited energy budget and needs to decide what attack strategy to use. The content of the attack strategy includes at which time the jamming operation should be implemented and which power level should be adopted. To simplify analysis, it is assumed that data packets can successfully arrive at the remote estimator if DoS attack is absent.

Formally, we denote δ_k^a as the attack power level at time k. Let γ_k be the attacker's decision at time k, i.e., $\gamma_k = 1$ indicates that attacker decides to jam the wireless channel at time k, $\gamma_k = 0$ the attacker does not implement jamming operation. Let $\theta_k(\gamma_k, \delta_k^a)$ be the indicator function whether the data packet drops or not, i.e., $\theta_k(\gamma_k, \delta_k^a) = 1$ if the packet is dropped, $\theta_k(\gamma_k, \delta_k^a) = 0$ otherwise. Note that when $\gamma_k = 0$, $\theta_k = 0$ always holds.

C. Problem of interest

Consider a finite time horizon T. The energy budget limitation of the attacker is denoted as Δ. From the viewpoint of the DoS attacker, it expects to deteriorate the expected terminal error covariance at the most degree provided a constrained energy budget Δ, which can be formulated as the following problem:

Problem 1:

$$\max_{\gamma\in\Theta,\delta_t^a} \; Tr\{\mathbb{E}[J(\gamma)]\} \tag{3}$$

$$\text{s.t.} \quad \sum_{t=1}^{T} \delta_t^a \gamma_t \le \Delta, \tag{4}$$

$$\underline{\delta} \le \delta_t^a \le \overline{\delta}, \tag{5}$$

where $J = P_T$ is the terminal error covariance at remote estimator side, $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_T)$ is the DoS attack decision vector on the time horizon $[1, T]$, and $\Theta = \{\gamma|\gamma_t \in \{0, 1\}, t = 1, 2, \ldots, T\}$ is the attack decision vector set, $\underline{\delta}$ and $\overline{\delta}$ are the low bound and upper bound of attack power, respectively.

Problem 1 aims to solve the problems "when to attack the communication channel", and "how much power the attacker should use to jam the channel in each time" so that the state estimation quality is deteriorated. We focus on the effect of jamming attack at the end of the time horizon. In fact, the terminal error covariance is an important index to measure the quality of remote estimation [32]. This kind of setup can also be seen in [28], [33], [34].

In Section IV, we consider the scenario that the attacker has to determine a time invariant attack power before the attack launches. When the attacker has more information on the real-time attack effect, i.e., the acknowledgement(ACK) information from the receiver (estimator) to the sender (sensor) [35], [36], we investigate the dynamic attack power allocation problem in each time in Section V.

III. Preliminaries

In this section, we present the relation between attack power and packet drop probability, and some properties of the remote state estimation under a DoS attack.

A. Attack power and packet drop probability

One property of wireless communication is that the packet is subject to random loss due to channel fading, interference, scattering, etc. The probability of successful and error-free packet reception primarily relies on the SNR (signal to noise ratio) at the receiver side [37]. Supposing that the sensor is transmitting a packet to the remote estimator with the power δ^s, the SNR of the remote estimator is defined by

$$\rho = \frac{\delta^s G^s}{\delta^a G^a + \sigma^2}, \tag{6}$$

where G^s is the channel gain from the sensor to remote estimator, G^a is the channel gain from the attacker to remote estimator, and σ^2 is the noise power.

We denote the packet length of the sensor by L and assume that the transmission error is of bit-to-bit independent. Only if every bit is received correctly, the packet is considered as successfully reception. The packet reception rate is therefore given by [31]

$$\mu = \left[1 - \mathcal{Q}(\sqrt{2\rho})\right]^L, \tag{7}$$

where $\mathcal{Q}(x) = 1/\sqrt{2\pi}\int_x^{+\infty} e^{-t^2/2}dt$. Then the packet drop probability α can be calculated by $\alpha = 1 - \mu$.

B. Remote estimation under DoS attack

At the sensor side, the local MMSE estimate $\widehat{x}_k^s$ can be obtained using a standard Kalman filter. According to [38], the corresponding error covariance P_k^s converges exponentially to a steady-state value $\overline{P}$. Thus, without loss of generality, it is assumed that $\Pi_0 = \overline{P}$. It is certain that $P_k^s = \overline{P}$ for all $k \in [1, T]$.

To simplify the notations, we define functions $h, h^k : \mathbb{S}_+^{n_x} \to \mathbb{S}_+^{n_x}$ as $h(X) \triangleq AXA' + \Sigma_w$, and $h^k(X) \triangleq \underbrace{h \circ h \circ \cdots \circ h}_{k \text{ times}}(X)$. Regarding to the function h, we have the following lemma.

Lemma 1 ([39], [40]): If $k_1 \le k_2, k_1, k_2 \in \mathbb{Z}^+$, then

$$h^{k_1}(\overline{P}) \preceq h^{k_2}(\overline{P}).$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

At the remote estimator side, the state estimate $\widehat{x}_k$ and corresponding error covariance P_k can be calculated by [41]

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

Similar to [22], [28], an attack decision vector with consecutive attacking sequence $k_1, k_2, \ldots, k_s$ can be formed as

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

According to [28], when the maximal attack times n is fixed, the optimal DoS attack strategy which maximizes the trace of expected terminal error covariance J arranges all the transmission consecutively for the last n time instants. This key result is mathematically stated in the following lemma.

Lemma 2: Consider the following problem

Problem 2:

$$\max_{\gamma \in \Theta} \; Tr\{\mathbb{E}[J(\gamma)]\}$$
$$s.t. \quad \sum_{t=1}^{T} \gamma_t \leq n.$$

The optimal solution of Problem 2 is

$$\gamma^*(n) = (0, 0, \cdots, \underbrace{1, 1, \cdots, 1}_{n \text{ times}}), \tag{8}$$

and the trace of corresponding expected terminal error covariance is

$$Tr[J]_{max} = Tr\left[\sum_{i=0}^{n-1}(\alpha^i - \alpha^{i+1})h^i(\overline{P}) + \alpha^n h^n(\overline{P})\right]. \tag{9}$$

IV. Optimal static attack energy allocation

In Section III, we have pointed out that the optimal attack scheduling scheme is to jam the wireless channel at the last n times if the static attack power is given. Therefore a further question is how to determine the static optimal attack power in the beginning. We focus on this problem in this section. First, we study a special case and present the close form of optimal attack power to maximize the trace of expected error covariance, which is an optimal solution to Problem 1. In this special case, A is confined as a normal matrix. Then we provide an algorithm to find an optimal attack power for a general case.

A. Special case study

Denote $\mathcal{S}_n = \{\alpha | \lfloor \Delta/\delta^a(\alpha) \rfloor = n\}$ as the set of the packet drop probability which is corresponding to n times attack capability. In order to deduce our main conclusion, the following two lemmas are needed.

Lemma 3: If $\alpha_1, \alpha_2 \in \mathcal{S}_n$, and $\alpha_1 > \alpha_2$, then the scheduling scheme (8) is optimal for α_1 and α_2. Moreover,

$$Tr[J]_{max}(\alpha_1) > Tr[J]_{max}(\alpha_2).$$

Proof: It can be easily deduced from (9). ■

Definition 1 (Normal matrix [42]): A square matrix A is normal if $A^*A = AA^*$, where A^* is the conjugate transpose of A.

Note that normal matrix plays an important role in matrix diagonalization. In fact, matrix A is normal if and only if it is unitarily similar to a diagonal matrix.

Lemma 4: Let $\overline{n} = \lfloor \Delta/\underline{\delta} \rfloor$. Suppose $\alpha \in \mathcal{S}_n, \beta \in \mathcal{S}_{n+1}$. If the following conditions are satisfied

1) matrix A is normal,
2) all the eigenvalues $\lambda = \lambda(AA')$ satisfy

$$1 < \lambda < \frac{1}{\underline{\alpha}}[1 - (\frac{\overline{\alpha} - \underline{\alpha}}{\underline{\alpha}^{\overline{n}+1}})]^{1/2}, \tag{10}$$

where $\underline{\alpha}$ and $\overline{\alpha}$ are the low bound and upper bound of packet drop probability, which are corresponding to the upper bound and low bound of attack power respectively, then we have

$$Tr[J]_{max}(\alpha) \leq Tr[J]_{max}(\beta). \tag{11}$$

Proof: See Appendix. ■

Now let us present the main conclusion.

Theorem 1: Let $\overline{n} = \lfloor \Delta/\underline{\delta} \rfloor$. If the matrix A is normal, and the condition (10) is satisfied, then an optimal attack power level, which is an optimal solution to Problem 1, is

$$\delta^{a*} = \min\left\{ \arg\max\{\delta^a | \lfloor \Delta/\delta^a \rfloor = \overline{n}\}, \overline{\delta} \right\}, \tag{12}$$

and the trace of corresponding expected terminal error covariance is

$$Tr[J]_{max} = Tr\left[\sum_{i=0}^{\overline{n}-1}(\alpha^{*i} - \alpha^{*i+1})h^i(\overline{P}) + \alpha^{*\overline{n}} h^{\overline{n}}(\overline{P})\right] \tag{13}$$

where $\alpha^* = 1 - \mu(\delta^{a*})$ is packet drop probability associated with optimal DoS attack power.

Proof: According to Lemma 3 and Lemma 4, the conclusion in this theorem can be readily deduced. ■

Notice that Theorem 1 provides a sufficient condition to optimize the DoS attack power. If the desired optimal attack power $\delta^a = \arg\max\{\delta^a | \lfloor \Delta/\delta^a \rfloor = \overline{n}\}$ is larger than the upper bound $\overline{\delta}$, the attacker will choose the upper bound power to jam the wireless channel when it launches the attack, from Theorem 1. According to [43], it can be seen that the packet reception rate μ is always monotonically increasing with respect to SNR ρ. We still can calculate optimal α, provided that the expression of μ is given with respect to ρ.

B. General case study

For a general case, the system matrix A is not always normal, and the condition (10) may not be satisfied. Therefore, the power level $\underline{\delta}$ is not always optimal. However, the attacker can find the optimal attack power level by exhaustion search method that is given in Algorithm 1.

Lemma 2 provides the maximal trace of expected terminal error covariance when the attack times and probability α are given. However, since the attack power is continuous, Problem 1 cannot use the exhaustion search method to find the optimal solution. According to Lemma 3, we see that the more attack power the larger trace of expected error covariance when the attack powers are in the same set $\mathcal{S}_n$. Then the attack power

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

can be discretized. The optimal attack power can be found in these discrete points.

Motivated by this, we design Algorithm 1 to find the optimal solution of Problem 1. In this algorithm, we first compute the difference between maximal attack times and minimal attack times, i.e., $m+1=\left\lfloor \frac{\Delta}{\underline{\delta}} \right\rfloor - \left\lfloor \frac{\Delta}{\overline{\delta}} \right\rfloor$. According to (6)(7)(8), we design the recursive process to exhaustively search the optimal attack power. In addition, we can obtain the maximum cost J_{max} from this algorithm.

When the time horizon T is fixed, it can be easily seen that the search steps are no more than T. In other words, the computational complexity of the proposed algorithm is not worse than $\mathcal{O}(T)$, where T is the length of the time horizon considered. In addition, this power allocation can be computed before the attack action begins and the number of cycles in Algorithm 1 only depends on the low bound $\underline{\delta}$, upper bound $\overline{\delta}$ and the constraint Δ of the attack power.

Algorithm 1 Optimal attack power allocation

1: Input: $\overline{P}; \underline{\delta}; \overline{\delta}; \Delta; J_{max}=0$;
2: Compute $m=\left\lfloor \frac{\Delta}{\underline{\delta}} \right\rfloor - \left\lfloor \frac{\Delta}{\overline{\delta}} \right\rfloor - 1$;
3: **for** $i=1:m$ **do**
4: Compute $n=\left\lfloor \frac{\Delta}{\overline{\delta}} \right\rfloor + i - 1$;
5: Construct attack schedule γ according to (8);
6: Compute attack energy

$$\delta^a = \max\{\delta | \left\lfloor \frac{\Delta}{\delta} \right\rfloor = n\} = \min\{\max\{\frac{\Delta}{n}, \underline{\delta}\}, \overline{\delta}\};$$

7: Compute $\alpha = 1-\mu$ where μ is calculated according to (6) and (7);
8: Compute the terminal error covariance cost (9) under attack schedule γ, i.e. $J=J(\gamma)$;
9: **if** $J > J_{max}$ **then**
10: $J_{max}=J, \delta^{a*}=\delta^a$, and $\gamma^*=\gamma$;
11: **end if**
12: **end for**
13: Output: optimal attack power allocation δ^{a*}, optimal attack schedule γ^*, and corresponding maximum cost J_{max}.

C. Discussion

Besides the terminal error covariance, the average error covariance is another important index in reflecting the state estimation quality [22]. The average error covariance in the time horizon T is defined as

$$J_{av} = \frac{1}{T}\sum_{k=1}^{T} P_k. \tag{14}$$

From the viewpoint of DoS attacker, the DoS attack energy allocation maximizing the average error covariance can be formulated as follows:

Problem 3:

$$\max_{\gamma\in\Theta, \delta^a} \; Tr\{\mathbb{E}[J_{av}(\gamma)]\} \tag{15}$$

$$\text{s.t.} \quad \sum_{t=1}^{T}\gamma_t \le \left\lfloor \frac{\Delta}{\delta^a} \right\rfloor, \tag{16}$$

$$\underline{\delta} \le \delta^a \le \overline{\delta}. \tag{17}$$

If the attack power δ^a is given and invariant, the optimal attack schedule, which aims to maximize the expected average error covariance, can be obtained from following conclusion.

Lemma 5: [22] Suppose that the attacker can at most launch n times attack with the same attack power δ^a. Then the optimal attack schedule which maximizes the expected average error covariance (14) is

$$(0,0,\cdots,0,\underbrace{1,1,\cdots,1}_{n \text{ times}},0,0,\cdots,0), \tag{18}$$

and the corresponding expected covariance is given by

$$J_{av}^{max} = \frac{1}{T}\sum_{i=1}^{n}[h_i(\alpha,\overline{P})] + \frac{T-n\alpha}{T}\overline{P}, \tag{19}$$

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

Since the form of the maximum expected average error covariance (19) is more complex than that of terminal error covariance (9), it is still a challenging work to provide the close form of optimal attack power for the average performance.

Similar to Algorithm 1, we can design an exhausting search method to find the optimal attack power for the average performance case. It only needs to change the step of calculating the estimation quality index in Algorithm 1, that is, replacing the line 8 by "Compute the trace of average error covariance cost (19) under attack schedule γ, i.e. $J=Tr[J_{av}^{max}(\gamma)]$".

V. Dynamic attack energy allocation

In Section IV, we investigate the optimal static attack energy allocation problem which destroys the estimation quality. In this scenario, the attacker does not know the real-time attack effect, and cannot switch the attack energy timely. In this section, we consider the scenario that the attacker has more capabilities,i.e., he can obtain the real-time ACK information from eavesdropping the estimator-to-sensor communication channel, and can dynamically adjust the attack power.

Let e be the unit attack energy. Without loss of generality, we suppose that the lower bound, upper bound and the constraint of the attack power are respectively denoted as $\underline{\delta}=p\cdot e$, $\overline{\delta}=q\cdot e$, $\Delta=r\cdot e$, where $p\le q<r$ are positive integers. Besides, we discrete the attack power as $\Phi=\{0,pe,(p+1)e,\ldots,qe\}$. Let δ_k^a be the attack power at time k and $\lambda=(\delta_1^a,\delta_2^a,\ldots,\delta_T^a)$ be an arbitrary attack power allocation scheme. Therefore, our interesting problem is to find the optimal scheme λ^* that maximizes the terminal error covariance.

Problem 4:

$$\max_{\lambda} \; Tr\{\mathbb{E}[J(\lambda)]\} \tag{20}$$

$$s.t. \quad \sum_{t=1}^{T}\delta_t^a \le \Delta, \tag{21}$$

$$\delta_t^a \in \{0,pe,(p+1)e,\ldots,qe\}. \tag{22}$$

To solve the above problem, one may leverage exhaustion method. However, as the T becomes larger, the computation complexity becomes higher. Therefore, we transform the Problem 4 into a Markov Decision Process (MDP) problem which can be solved by efficient numerical algorithm.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

Let $SP = \{\overline{P}, h(\overline{P}), h^2(\overline{P}), \ldots, h^T(\overline{P})\}$ and $SR = \{R^0, R^1, R^2, \ldots, R^r\}$, where $R^i = i \cdot e$ for $0 \leq i \leq r$. Thus, SP and SR include all the possible estimation error covariance and residue available attack power at each time horizon, respectively. Denote $\mathbb{S} = SP \times SR$ as the state space and $s_k = (P_k, E_k) \in \mathbb{S}, 0 \leq k \leq T$ as an arbitrary state at time k.

Furthermore, denote $\mathbb{A} = \Phi$ as the action space. Then the available action space for a given state $(h^i(\overline{P}), R^j)$ is

$$\mathbb{A}_{(h^i(\overline{P}),R^j)} = \{0, \max\{\underline{\delta}, R^j\}, \max\{\underline{\delta}, R^j\}+e, \ldots, \min\{\overline{\delta}, R^j\}\}.$$

Based on the remote estimation algorithm, the transition probabilities for given action $a \in \mathbb{A}_{(h^i(\overline{P}),R^j)}$ are

$$\begin{aligned}
&Pr\big((h^m(\overline{P}), R^n)|(h^i(\overline{P}), R^j), a\big) = \alpha_a,\\
&\text{when} \quad m = i+1, R^n = R^j - a;\\
&Pr\big((\overline{P}, R^n)|(h^i(\overline{P}), R^j), a\big) = 1-\alpha_a, \quad \text{when} \quad R^n = R^j - a;\\
&Pr\big((h^m(\overline{P}), R^n)|(h^i(\overline{P}), R^j), a\big) = 0, \quad \text{otherwise},
\end{aligned}$$

where $1 \leq i, m, \leq T$, $0 \leq n \leq r$ and α_a is the probability of packet loss which computed by (6) and (7).

Denote the immediate reward at each time horizon as follows:

$$RW_T\big((P_T, E_T)\big) = Tr(P_T), \tag{23}$$
$$RW_k\big((P_k, E_k), a\big) = 0, \quad 0 \leq k < T. \tag{24}$$

Therefore, the tuple $\{T, \mathbb{S}, \mathbb{A}, Pr, RW_k\}$ describes an MDP with the initial state $s_0 = (\overline{P}, \Delta)$.

Denote $\pi = (f_0, f_1, \ldots, f_{T-1})$ be a deterministic Markovian policy for the above MDP, where $f_k : \mathbb{S} \to \mathbb{A}_{s \in \mathbb{S}}$ is a deterministic decision function at time k. Then the objective function of Problem 4 can be rewritten as the following expected total reward within T times

$$V_T(s_0, \pi) = \sum_{k=0}^{T-1} \mathbb{E}_\pi^{s_0}[RW_k(s_k, a_k)] + \mathbb{E}_\pi^{s_0}[RW_T(s_T)]. \tag{25}$$

Thus, the Problem 4 can be modeled by the MDP problem whose objective is to find a policy π^* that generate the sequence action $(a_0^*, a_1^*, \ldots, a_{T-1}^*)$ and maximize the total cost (25). Note that, here $a_i^* = \delta_{i+1}^{a*}$.

Let

$$J_T^*(s_T) = Tr(P_T), \tag{26}$$
$$J_k^*(s_k) = \max_{a_k \in \mathbb{A}_{s_k}} \tag{27}$$
$$\left\{ \sum_{s_{k+1} \in \mathbb{S}} Pr(s_{k+1}|s_k, a_k) J_{k+1}^*(s_{k+1}),\ RW_k(s_k, a_k) \right\}. \tag{28}$$

Thus, according to [44], we have

$$J_0^*(s_0) = V_T^*(s_0, \pi^*), \tag{29}$$

and the backward recursive iteration Algorithm 2 within T times can be leveraged to solve the above MDP problem and give the optimal attack power allocation scheme λ^*.

Algorithm 2 Dynamic attack power allocation

1: Input: $\overline{P}; \underline{\delta}; \overline{\delta}; \Delta; e; T; \mathbf{S}; \mathbf{A}; Pr; RW$
2: Let $k = T$ and $J_T^*(s_T) = Tr(P_T)$ for all $s_T \in \mathbf{S}$;
3: **if** $k = 0$ **then**
4: $\pi^* = (f_0^*, f_1^*, \ldots, f_{T-1}^*)$ is the optimal Markovian policy and $V_T^*(s_0, \pi^*) = J_0^*(s_0)$ is the maximum trace of the terminal error covariance;
5: **else**
6: Let $k = k-1$, and for all $s_k \in \mathbf{S}$ compute

$$J_k^*(s_k) = \max_{a_k \in \mathbb{A}_{s_k}} \left\{ \sum_{s_{k+1} \in \mathbb{S}} Pr(s_{k+1}|s_k, a_k) J_{k+1}^*(s_{k+1}),\ RW_k(s_k, a_k) \right\}$$

$$f_k^*(s_k) = \arg\max_{a_k \in \mathbb{A}_{s_k}} \left\{ \sum_{s_{k+1} \in \mathbb{S}} Pr(s_{k+1}|s_k, a_k) J_{k+1}^*(s_{k+1}),\ RW_k(s_k, a_k) \right\}$$

7: **end if**
8: Output: Maximum trace of the terminal error covariance $V_T^*(s_0, \pi^*)$; Optimal deterministic Markovian policy π^*.

VI. Examples

In this section, we illustrate the effect of energy-constraint DoS attack with different attack power for the different scenarios.

A. The special case

We first consider the LTI system (1)(2) with

$$A = \begin{bmatrix} 1.01 & 0 \\ 0 & 1.01 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$\Sigma_w = \begin{bmatrix} 1 & 0 \\ 0 & 1.5 \end{bmatrix}, \Sigma_v = 0.5C.$$

It can be easily seen that A is normal. We assume that the sensor's transmission power is $\delta^s = 10$, the channel gain from sensor to estimator is $G^s = 1$. The noise power is $\sigma^2 = 0.1$. The attack power level $\delta^a \in [4+\tau, 4.4+\tau], \tau \in [0.1, 1]$, and the channel gain from the attacker to estimator is $G^a = 1$. Then we can easily verify that the condition (10) is true for this system.

The effects of the optimal DoS attack scheduling schemes with different attack power levels are evaluated by simulation. In Fig.2, we compare the packet drop probability under optimal attack scheduling schemes with different choices of the attack power. The top dash line in Fig.2 shows the variation of α under optimal attack scheduling schemes with low bound of attack power level $\underline{\delta}$. When the attacker chooses the low bound power to jam the wireless channel, the packet drop probability reaches the upper bound. The bottom line represents the variation of α under optimal attack scheduling schemes with upper bound of attack power level $\overline{\delta}$. The middle line shows the the variation of α when the attack strategy is (8) with our proposed power level in Theorem 1. One can see that the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

optimal attack power is the upper bound of attack power when $\tau < 0.6$. The reason is that the desired optimal attack power exceeds the upper bound. Then the attacker cannot launch the attach with the desired optimal attack power. When $\tau \geq 0.6$, it can be seen that the desired optimal attack power can be reached.

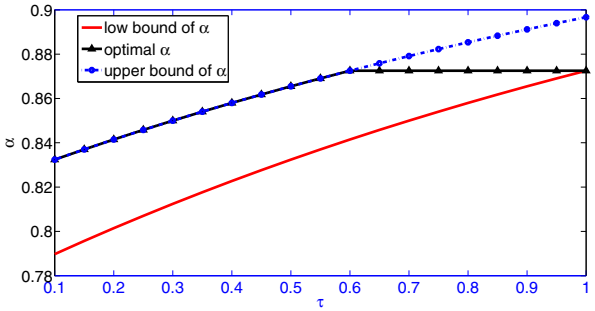


Fig. 2. Illustrative example on probability α under different attack power level when the conditions (10) are satisfied.

The top line in Fig.3 shows the variation of $Tr[\mathbb{E}(J)]$ under optimal attack scheduling schemes with our proposed attack power level in Theorem 1. The dash line presents the variation of $Tr[\mathbb{E}(J)]$ when the attacker launches the optimal attack schemes with the upper bound power level, while the remaining solid line is the variation of $Tr[\mathbb{E}(J)]$ under the optimal attack schemes with the low bound power level. Since the optimal attack power level is the upper bound when $\tau < 0.5$, the line with optimal attack power and the line with upper bound power are coincident. From Fig.3, we also can see that our proposed attack power can indeed maximize $Tr[\mathbb{E}(J)]$, which verifies our conclusion in Theorem 1.

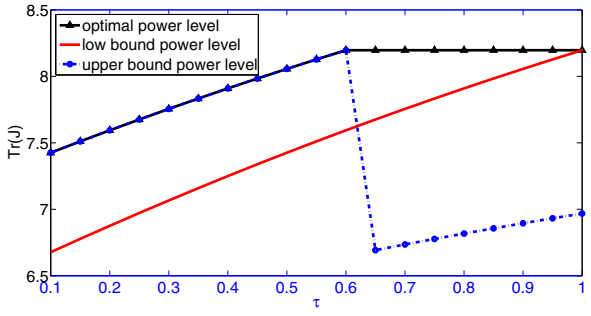


Fig. 3. Illustrative example on $Tr(J)$ under different attack power level when the conditions (10) are satisfied.

B. General case

In this subsection, we will verify the Algorithm 1 for a LTI system which is not satisfied condition (10) through numerical simulation.

Consider a unstable system with

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

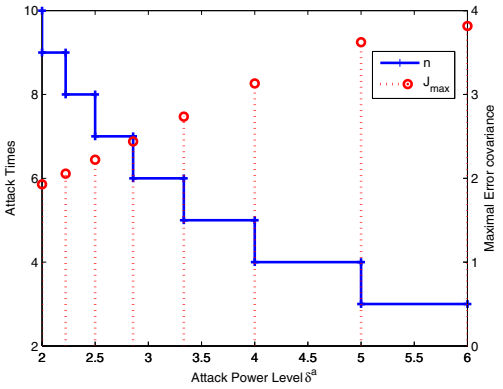


Fig. 4. Attack times and maximal terminal error covariance under different power level when $\underline{\delta} = 2, \overline{\delta} = 6, \Delta = 20$.

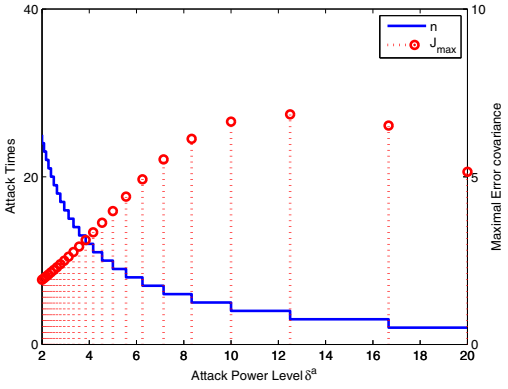


Fig. 5. Attack times and maximal terminal error covariance under different power level when $\underline{\delta} = 2, \overline{\delta} = 20, \Delta = 50$.

Let $\delta^s = 10$, $G^s = 1$, $G^a = 1$, $\sigma^2 = 2$, and $L = 20$. We solve the optimal power allocation problem 1 through Algorithm 1 and compare the maximal error covariance under different attack power level when the lower bound, upper bound and the constraint of the attack power are as the following three cases:

1) $\underline{\delta} = 2, \overline{\delta} = 6, \Delta = 20$,
2) $\underline{\delta} = 2, \overline{\delta} = 20, \Delta = 50$,
3) $\underline{\delta} = 20, \overline{\delta} = 50, \Delta = 200$.

Fig. 4, Fig. 5 and Fig. 6 plot the corresponding attack times and maximal error covariance under power $\delta^a = \max\{\delta \Big| \left\lfloor \frac{\Delta}{\delta} \right\rfloor = n\}$ where n is all possible number of attack, respectively. From the results of the algorithm and the the red stem line in three figures, we obtain the optimal power level, optimal attack times and optimal maximal error covariance for the above three cases are as follow:

1) $\delta^{a*} = 6$, $n^* = 3$, $J^*_{max} = 3.8160$,
2) $\delta^{a*} = 12.5$, $n^* = 4$, $J^*_{max} = 6.8607$,
3) $\delta^{a*} = 20$, $n^* = 10$, $J^*_{max} = 19.5153$.

According to the optimal solutions, one can find that the attacker tends to choose larger power to jam the communication when the upper bound of attack power is lower and he

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

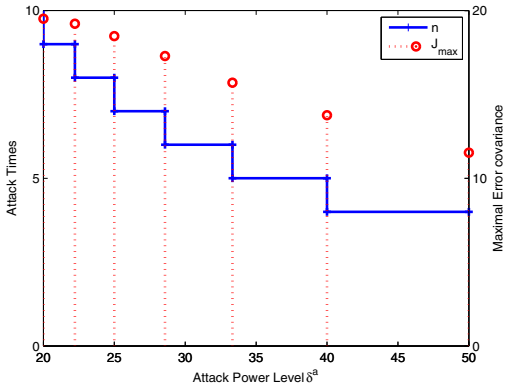


Fig. 6. Attack times and maximal terminal error covariance under different power level when $\underline{\delta} = 20, \overline{\delta} = 50, \Delta = 200$.

is inclined to choose lower power when the lower bound is larger.

We then study the optimal attack power allocation against the average error covariance in the time horizon $T = 100$. Consider three attack cases, in which the setup of attack, i.e., the lower bound, upper bound and the constraint of the attack power, is the same as the above for the terminal case. The simulation results are presented in Fig. 7, Fig. 8, and Fig. 9. It can be seen that the optimal attack times and optimal maximal error covariance for the above three cases are as follow:

1) $\delta^{a*} = 2,\ n^* = 10,\ J^*_{max} = 4.0923,$
2) $\delta^{a*} = 4.16,\ n^* = 12,\ J^*_{max} = 4.3020,$
3) $\delta^{a*} = 20,\ n^* = 10,\ J^*_{max} = 5.3193.$

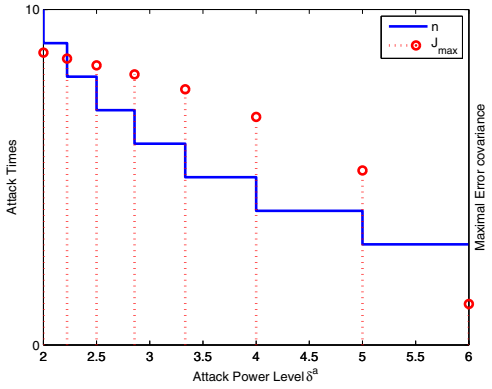


Fig. 7. Attack times and maximal average error covariance under different power level when $\underline{\delta} = 2, \overline{\delta} = 6, \Delta = 20$.

C. Dynamic attack energy allocation

Here we will verify the Algorithm 2 and compare the effectiveness between Algorithm 1 that uses constant attack power and Algorithm 2 that uses dynamic attack power.

Consider the same system in Section VI-B. First, for the case where $\underline{\delta} = 2, \overline{\delta} = 6, \Delta = 15$, we set $e = 1, T = 5$. By leveraging the Algorithm 2, the maximum trace of the terminal error covariance can be obtained as $V^*_T(s_0, \pi^*) = 3.6340$ and

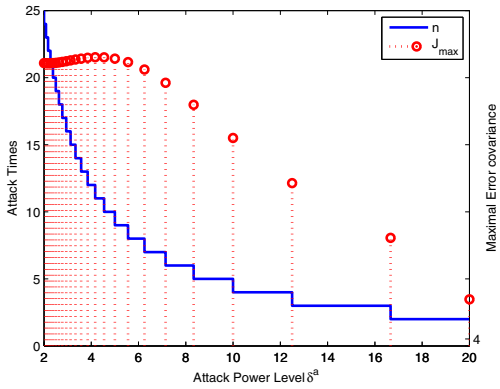


Fig. 8. Attack times and maximal average error covariance under different power level when $\underline{\delta} = 2, \overline{\delta} = 20, \Delta = 50$.

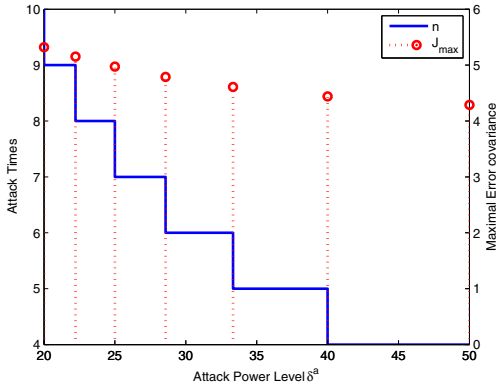


Fig. 9. Attack times and maximal average error covariance under different power level when $\underline{\delta} = 20, \overline{\delta} = 50, \Delta = 200$.

the optimal policy can be described by the following Figure 10.

Next, we fix $\underline{\delta} = 20, \overline{\delta} = 50$ and compare the maximum terminal error between two algorithms by changing the total available attack power $\Delta = 100, 150, 200, \ldots, 400$. Note that the unit energy and the maximum time are set to be $e = 1$ and $T = 100, 150, 200, \ldots, 400$ when using the Algorithm 2. Figure 11 plots the simulation results, from which one can find that the Algorithm 2 always performs better than Algorithm 1.

VII. Conclusion

In this paper, we investigated the optimal DoS attack power allocation against remote state estimation of a linear dynamic system. The objective of the attacker subject to limited energy budget is to maximize the terminal estimation error covariance by emitting interference signals with proper attack energy and jamming the communication channel. To this end, we first considered a special case where the system matrix is normal and found that using the maximum number of jamming operations is optimal under a derived sufficient condition. Furthermore, for the general case, an attack power allocation algorithm with low computation cost was proposed to figure

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

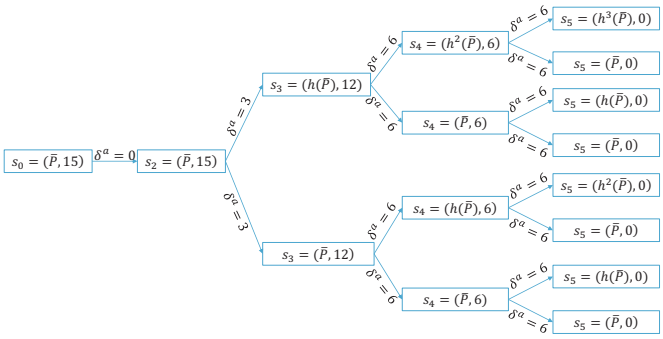


Fig. 10. Optimal decision tree when $\underline{\delta} = 2, \overline{\delta} = 6, \Delta = 15$.

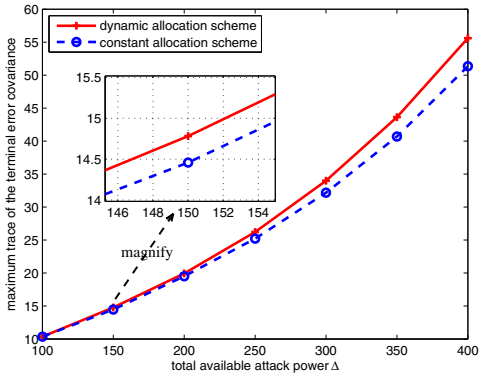


Fig. 11. Maximal trace of the terminal estimation error covariance under different total attack power Δ when $\underline{\delta} = 20, \overline{\delta} = 50$.

out the optimal attack power level as well as the attack strategy. We also investigate the dynamic attack energy allocation when the attacker can determine the attack power in each time horizon. Finally, some numerical simulations were presented to demonstrate the effectiveness of our results.

APPENDIX

PROOF OF THEOREM 4

Before proving Theorem 4, following lemma is needed.

Lemma 6: (Lagrange's Mean Value Theorem [45]) Suppose function $f : [a, b] \longrightarrow \mathbb{R}$ is continuous, and differentiable on (a, b). Then there exists $c \in (a, b)$ such that

$$f(a) - f(b) = f'(c)(a - b).$$

Now let us prove Theorem 4.

Proof of Lemma 4: According to (9), it can be seen that

$$\begin{aligned} Tr[J(\alpha)]_{max} &= Tr\Big[\sum_{i=0}^{n-1}(\alpha^i - \alpha^{i+1})h^i(\overline{P}) + \alpha^n h^n(\overline{P})\Big] \\ &= Tr\Big\{\sum_{i=1}^{n}\alpha^i[h^i(\overline{P}) - h^{i-1}(\overline{P})] + \overline{P}\Big\}. \end{aligned}$$

Then we have

$$\begin{aligned} &Tr[J(\alpha)]_{max} - Tr[J(\beta)]_{max} \\ &= Tr\Big\{\sum_{i=1}^{n}(\alpha^i - \beta^i)[h^i(\overline{P}) - h^{i-1}(\overline{P})] \\ &\quad -\beta^{n+1}[h^{n+1}(\overline{P}) - h^n(\overline{P})]\Big\}. \end{aligned}$$

From Lemma 6, there exists $\xi_i \in (\alpha, \beta)$ such that

$$\alpha^i - \beta^i = i\xi_i^{i-1}(\alpha - \beta).$$

Thus we have

$$\begin{aligned} &Tr[J(\alpha)]_{max} - Tr[J(\beta)]_{max} \\ &= Tr\Big\{\sum_{i=1}^{n} i\xi_i^{i-1}(\alpha - \beta)[h^i(\overline{P}) - h^{i-1}(\overline{P})] \\ &\quad -\beta^{n+1}[h^{n+1}(\overline{P}) - h^n(\overline{P})]\Big\}. \end{aligned}$$

Since

$$\begin{aligned} &h^i(\overline{P}) - h^{i-1}(\overline{P}) = Ah^{i-1}(\overline{P})A' - Ah^{i-2}(\overline{P})A' \\ &= A[h^{i-1}(\overline{P}) - h^{i-2}(\overline{P})]A' = \cdots = A^{i-1}[h(\overline{P}) - \overline{P}](A^{i-1})', \end{aligned}$$

then we can see that

$$\begin{aligned} &Tr[J(\alpha)]_{max} - Tr[J(\beta)]_{max} \\ &= Tr\Big\{\sum_{i=1}^{n} i\xi_i^{i-1}(\alpha - \beta)A^{i-1}[h(\overline{P}) - \overline{P}](A^{i-1})' \\ &\quad -\beta^{n+1}A^n[h(\overline{P}) - \overline{P}](A^n)'\Big\} \\ &= Tr\Big\{\sum_{i=1}^{n} i\xi_i^{i-1}(\alpha - \beta)(A^{i-1})'A^{i-1}[h(\overline{P}) - \overline{P}] \\ &\quad -\beta^{n+1}(A^n)'A^n[h(\overline{P}) - \overline{P}]\Big\} \\ &= Tr\Big\{\sum_{i=1}^{n}[i\xi_i^{i-1}(\alpha - \beta)(A^{i-1})'A^{i-1} \\ &\quad -\beta^{n+1}(A^n)'A^n][h(\overline{P}) - \overline{P}]\Big\}. \end{aligned}$$

Since $h(\overline{P}) - \overline{P} \succeq 0$, we only need to prove

$$\sum_{i=1}^{n} i\xi_i^{i-1}(\alpha - \beta)(A^{i-1})'A^{i-1} - \beta^{n+1}(A^n)'A^n \preceq 0. \quad (30)$$

Because $0 < \alpha - \beta < \overline{\alpha} - \underline{\alpha}$, the inequality (30) is established if

$$\sum_{i=1}^{n} i(\overline{\alpha} - \underline{\alpha})\xi_i^{i-1}(A^{i-1})'A^{i-1} - \beta^{n+1}(A^n)'A^n \preceq 0. \quad (31)$$

Since matrix A is normal, we can see that $AA' = A'A$, and then the left side of inequality (31) is a matrix polynomial with AA' as the independent matrix variable, i.e.,

$$\begin{aligned} &\sum_{i=1}^{n} i(\overline{\alpha} - \underline{\alpha})\xi_i^{i-1}(A^{i-1})'A^{i-1} - \beta^{n+1}(A^n)'A^n \\ &= \sum_{i=1}^{n} i(\overline{\alpha} - \underline{\alpha})\xi_i^{i-1}(AA')^{i-1} - \beta^{n+1}(AA')^n. \end{aligned} \quad (32)$$

Since $0 < \xi_i < \alpha < 1$, it can be seen that (32) is non-positive if

$$\sum_{i=1}^{n} i(\overline{\alpha} - \underline{\alpha})\alpha^{i-1}(AA')^{i-1} - \beta^{n+1}(AA')^n \preceq 0. \tag{33}$$

Furthermore, the inequality (33) is equivalent to

$$(I - \alpha AA')^2[\sum_{i=1}^{n} i(\overline{\alpha} - \underline{\alpha})(\alpha AA')^{i-1} - \beta^{n+1}(AA')^n] \preceq 0, \tag{34}$$

where I is the identity matrix.

Since

$$\begin{aligned}
&(I - \alpha AA')^2[\sum_{i=1}^{n} i(\overline{\alpha} - \underline{\alpha})(\alpha AA')^{i-1} - \beta^{n+1}(AA')^n] \\
&\preceq (I - \alpha AA')^2[(\overline{\alpha} - \underline{\alpha})\sum_{i=1}^{\infty} i(\alpha AA')^{i-1} - \beta^{n+1}(AA')^n] \\
&= (\overline{\alpha} - \underline{\alpha})I - \beta^{n+1}(I - \alpha AA')^2(AA')^n,
\end{aligned}$$

where

$$\begin{aligned}
&(I - \alpha AA')^2 \sum_{i=1}^{\infty} i(\alpha AA')^{i-1} \\
&= (I - \alpha AA')[(I - \alpha AA')\sum_{i=1}^{\infty} i(\alpha AA')^{i-1}] \\
&= (I - \alpha AA')\sum_{i=1}^{\infty}(\alpha AA')^{i-1} = I,
\end{aligned}$$

then we can see that the inequality (34) is established if

$$(\overline{\alpha} - \underline{\alpha})I - \beta^{n+1}(I - \alpha AA')^2(AA')^n \preceq 0. \tag{35}$$

The inequality (35) is equivalent to

$$(\overline{\alpha} - \underline{\alpha}) - \beta^{n+1}(1 - \alpha\lambda)^2\lambda^n \leq 0, \tag{36}$$

or

$$(1 - \alpha\lambda)^2\lambda^n \geq \frac{\overline{\alpha} - \underline{\alpha}}{\beta^{n+1}}, \tag{37}$$

for all the eigenvalue λ of matrix AA'.

Since $\lambda > 1$, and $\beta > \underline{\alpha}$, it can be seen that (37) is established if

$$(1 - \alpha\lambda)^2 \geq \frac{\overline{\alpha} - \underline{\alpha}}{\underline{\alpha}^{\overline{n}+1}}, \tag{38}$$

and (38) is established if $\lambda < \frac{1}{\overline{\alpha}}[1 - (\frac{\overline{\alpha} - \underline{\alpha}}{\underline{\alpha}^{\overline{n}+1}})]^{1/2}$, which finishes the proof. ■

REFERENCES

[1] K.-D. Kim and P. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. 13, pp. 1287–1308, 2012.

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

[3] S. H. Dau, W. Song, and C. Yuen, "On simple multiple access networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 2, pp. 236–249, 2015.

[4] H. Zhou, J. Chen, H. Zheng, and J. Wu, "Energy efficiency and contact opportunities tradeoff in opportunistic mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3723–3734, 2016.

[5] W. Meng, X. Wang, and S. Liu, "Distributed load sharing of an inverter-based microgrid with reduced communication," *IEEE Transactions on Smart Grid*, 2016,DOI:10.1109/TSG.2016.2587685.

[6] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, 2016.

[7] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

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

[9] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[10] S. H. Dau, W. Song, and C. Yuen, "Weakly secure mds codes for simple multiple access networks," in *Proceedings of IEEE International Symposium on Information Theory*, 2015, pp. 1941–1945.

[11] D. Shi, R. J. Elliott, and T. Chen, "On finite-state stochastic modeling and secure estimation of cyber-physical systems," *IEEE Transactions on Automatic Control*, DOI:10.1109/TAC.2016.2541919.

[12] X. Cao, L. Liu, W. Shen, A. Laha, J. Tang, and Y. Cheng, "Real-time misbehavior detection and mitigation in cyber-physical systems over wlans," *IEEE Internet of Things Journal*, DOI:10.1109/TII.2015.2499123.

[13] S. Amin, A. Cardenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *Hybrid Systems: Computation and Control*, pp. 31–45, 2009.

[14] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[15] C. Yang, H. Zhang, F. Qu, and Z. Shi, "Secured measurement fusion scheme against deceptive ecm attack in radar network," *Security and Communication Networks*, DOI: 10.1002/sec.1543.

[16] A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Proceedings of Workshop on Future Directions in Cyber-physical Systems Security*, 2009.

[17] H. Zhang, P. Cheng, J. Wu, L. Shi, and J. Chen, "Online deception attack against remote state estimation," in *Proceedings of World Congress of the International Federation of Automatic Control (IFAC)*, 2014.

[18] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of MOBIHOC*, 2005, pp. 46–57.

[19] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the Performance of IEEE 802.11 under Jamming," in *Proceedings of IEEE INFOCOM*, 2008, pp. 1265–1273.

[20] W.-T. Li, C.-K. Wen, J.-C. Chen, K.-K. Wong, J.-H. Teng, and C. Yuen, "Location identification of power line outages using pmu measurements with bad data," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3624–3635, 2016.

[21] A. Gupta, A. Nayyar, C. Langbort, and T. Basar, "A dynamic transmitter-jammer game with asymmetric information," in *Proceedings of IEEE Conference on Decision and Control*, 2012, pp. 6477–6482.

[22] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal Denial-of-Service Attack Scheduling with Energy Constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

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

[24] Y. Qi, P. Cheng, L. Shi, and J. Chen, "Event-based attack against remote state estimation," in *Proceedings of IEEE Conference on Decision and Control*, 2015.

[25] C. De Persis and P. Tesi, "Resilient control under denial-of-service," in *World Congress of IFAC*, vol. 19, no. 1, 2014, pp. 134–139.

[26] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843–852, 2016.

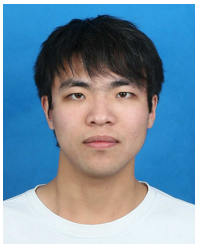
[27] P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, "Jamming-based adversarial control of network flow allocation: A passivity approach," in *Proceedings of American Control Conference*, 2015, pp. 4710–4716.

[28] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in *Proceedings of IEEE Conference on Decision and Control*, 2013, pp. 5444–5449.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2016.2614099, IEEE Transactions on Control of Network Systems

[29] X. Cao, P. Cheng, J. Chen, S. S. Ge, Y. Cheng, and Y. Sun, "Cognitive radio based state estimation in cyber-physical systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 489–502, 2014.
[30] S. Bhattacharya and T. Başar, "Game-theoretic analysis of an aerial jamming attack on a uav communication network," in *Proceedings of American Control Conference*, 2010, pp. 818–823.
[31] R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.
[32] L. Shi and L. Xie, "Optimal Sensor Power Scheduling for State Estimation of Gauss–Markov Systems Over a Packet-Dropping Network," *IEEE Transactions on Signal Processing*, vol. 60, no. 5, pp. 2701–2705, 2012.
[33] Q.-S. Jia, L. Shi, Y. Mo, and B. Sinopoli, "On optimal partial broadcasting of wireless sensor networks for kalman filtering," *IEEE Transactions on Automatic Control*, vol. 57, no. 3, pp. 715–721, 2012.
[34] J. Wu, Y. Li, D. E. Quevedo, V. Lau, and L. Shi, "Data-driven power control for state estimation: A bayesian inference approach," *Automatica*, vol. 54, pp. 332–339, 2015.
[35] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "Fake-acknowledgment attack on ack-based sensor power schedule for remote state estimation," in *Proceedings of IEEE Conference on Decision and Control*, 2015, pp. 5795–5800.
[36] Y. Qi, P. Cheng, and J. Chen, "Dynamic sensor data scheduling for remote estimation over gilbert-elliot channel," in *proceedings of IEEE/CIC International Conference on Communication in China (ICCC)*, Shanghai, China, Oct 2014, pp. 26–30.
[37] F. Xue, L.-L. Xie, and P. R. Kumar, "The transport capacity of wireless networks over fading channels," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 834–847, 2005.
[38] B. Anderson and J. Moore, *Optimal filtering*. Prentice-hall Englewood Cliffs, NJ, 1979, vol. 11.
[39] 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.
[40] ——, "Optimal periodic sensor scheduling with limited resources," *IEEE Transactions on Automatic Control*, vol. 56, no. 9, pp. 2190–2195, 2011.
[41] Z. Ren, P. Cheng, J. Chen, L. Shi, and Y. Sun, "Optimal periodic sensor schedule for steady-state estimation under average transmission energy constraint," *IEEE Transactions on Automatic Control*, DOI:10.1109/TAC.2013.2263651.
[42] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.
[43] D. Son, B. Krishnamachari, and J. Heidemann, "Experimental study of concurrent transmission in wireless sensor networks," in *Proceedings of the ACM international conference on Embedded networked sensor systems*, 2006, pp. 237–250.
[44] M. L. Puterman, *Markov decision processes: discrete stochastic dynamic programming*. John Wiley & Sons, 2014.
[45] P. Sahoo and T. Riedel, *Mean value theorems and functional equations*. World Scientific, 1998.

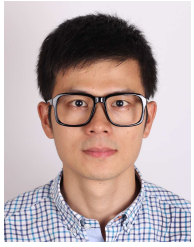
Heng Zhang received the Ph.D. degree in control science and engineering from Zhejiang University in 2015. He is currently an assistant professor at the School of Science, Huaihai Institute of Technology, Lianyungang, Jiangsu, China. His research interests include security and privacy in cyber-physical systems, control and optimization theory. He serves as a guest editor of Peer-to-Peer Networking and Applications and an active reviewer of IEEE TAC, IEEE TCNS, IEEE TIFS, and IEEE TWC.



Yifei Qi received the B.S. degree in Applied Mathematics from China University of Mining and Technology, Xuzhou, China, in 2011 and M.S. degree in Fundamental Mathematics from Wuhan University, Wuhan, China, in 2013, respectively. He is currently working toward the Ph.D. degree in the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His major research interests include sensor scheduling, security and application of remote estimation in cyber-physical system.

Junfeng Wu received the B.Eng. from the Department of Automatic Control, Zhejiang University, Hangzhou, China, in 2009 and the Ph.D. degree in Electrical and Computer Engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2013. From September to December 2013, he was a Research Associate in the Department of Electronic and Computer Engineering at the Hong Kong University of Science and Technology, Hong Kong. He is currently a Postdoctoral Researcher at ACCESS (Autonomic Complex Communication nEtworks, Signals and Systems) Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Sweden. His research interests include networked control systems, state estimation, and wirelesssensor networks, multi-agent systems. He received the Guan Zhao-Zhi Best Paper Award at the 34th Chinese Control Conference in 2015.

Lingkun Fu received the B.S. and Ph.D. degrees both in Control Science and Engineering from Zhejiang University in 2015. He is currently a postdoctoral research fellow at State Key Laboratory of Wind Power System at Zhejiang Windey Co., Ltd., joint with State Key Laboratory of Industrial Control Technology at Zhejiang University, working on industrial big data and control science & engineering. His research interests lie broadly in mobile computing, cyber-physical systems, wireless sensor networks and big data analysis.



Lidong He graduated from Zhejiang Ocean University in 2005 and received the Master's degree from Northeastern University, China, in 2008. After obtaining his Ph.D. degree in Control Science and Engineering from Shanghai Jiao Tong University in 2014, he has been a postdoctoral researcher in Zhejiang University. In the fall of 2010 and 2011, he was a visiting student in The Hong Kong University of Science and Technology for one year. His research interests include networked estimation and control, time/event-based scheduling of wireless sensor networks, as well as cyber security of control systems. He is an active reviewer of IEEE TAC, IEEE TCNS and Automatica.