

On the Complexity and Approximability of Optimal Sensor Selection and Attack for Kalman Filtering

Lintao Ye, Nathaniel Woodford, Sandip Roy and Shreyas Sundaram

Abstract—Given a linear dynamical system affected by stochastic noise, we consider the problem of selecting an optimal set of sensors (at design-time) to minimize the trace of the steady state *a priori* or *a posteriori* error covariance of the Kalman filter, subject to certain selection budget constraints. We show the fundamental result that there is no polynomial-time constant-factor approximation algorithm for this problem. This contrasts with other classes of sensor selection problems studied in the literature, which typically pursue constant-factor approximations by leveraging greedy algorithms and submodularity (or supermodularity) of the cost function. Here, we provide a specific example showing that greedy algorithms can perform arbitrarily poorly for the problem of design-time sensor selection for Kalman filtering. We then study the problem of attacking (i.e., removing) a set of installed sensors, under predefined attack budget constraints, to maximize the trace of the steady state *a priori* or *a posteriori* error covariance of the Kalman filter. Again, we show that there is no polynomial-time constant-factor approximation algorithm for this problem, and show specifically that greedy algorithms can perform arbitrarily poorly.

I. INTRODUCTION

In large-scale control system design, the number of sensors or actuators that can be installed is typically limited by a design budget constraint. Moreover, system designers often need to select among a set of possible sensors and actuators, with varying qualities and costs. Consequently, a key problem is to select an appropriate set of sensors or actuators in order to achieve certain objectives. This problem has recently received much attention from researchers (e.g., [1]–[9]). One specific instance of this problem arises in the context of linear Gauss-Markov systems, where the corresponding Kalman filter (with the chosen sensors) is used to estimate the states of the systems (e.g., [10], [11]). The problem then becomes how to select sensors dynamically (at run-time) or statically (at design-time) to minimize certain metrics of the corresponding Kalman filter. The former scenario is known as the sensor scheduling problem, where different sets of sensors can be chosen at different time steps (e.g., [12]–[14]). The latter scenario is known as the design-time sensor selection problem, where the set of sensors is chosen *a priori* and is not allowed to change over time (e.g., [15]–[17]).

Since these problems are NP-hard in general (e.g., [18]), approximation algorithms that provide solutions within a certain factor of the optimal are then proposed to tackle them.

This research was supported by NSF grants CMMI-1635014 and CMMI-1635184. The work of the second author was also supported by the Purdue Military Research Initiative. Lintao Ye, Nathaniel Woodford and Shreyas Sundaram are with the School of Electrical and Computer Engineering at Purdue University, West Lafayette, IN 47906 USA. Email: {ye159,nwoodfor,sundara2}@purdue.edu. Sandip Roy is with the School of Electrical Engineering and Computer Science at Washington State University, Pullman, WA 99164 USA. Email: sroy@eecs.wsu.edu.

Among these approximation algorithms, greedy algorithms have been widely used (e.g., [19], [20]), since such algorithms have provable performance guarantees if the cost function is submodular or supermodular (e.g., [21], [22]).

Additionally, in many applications, the sensors that have been selected and installed on the system are susceptible to a variety of potential attacks. For instance, an adversary (attacker) can inject false data to corrupt the state estimation, which is known as the false data injection attack (e.g., [23]–[25]). Another type of attack is the Denial-of-Service (DoS) attack, where an attacker tries to diminish or eliminate a network’s capacity to achieve its expected objective [26], including, for example, wireless jamming (e.g., [27], [28]) and memory exhaustion through flooding (e.g., [29]). One class of DoS attacks corresponds to removing a set of installed sensors from the system, i.e., the measurements of the attacked sensors are not used. This was also studied in [30] and [31], and will be the type of attack we consider in this work.

In this paper, we consider the sensor selection problem and the sensor attack problem for Kalman filtering of discrete-time linear dynamical systems. First, we study the problem of choosing a subset of sensors to install (under given selection budget constraints) to minimize the trace of either the steady state *a priori* or *a posteriori* error covariance of the Kalman filter. We refer to these problems as the *priori* and *posteriori Kalman Filtering Sensor Selection (KFSS)* problems, respectively. Second, we study the problem of attacking the installed sensors (by removing a subset of them, under given attack budget constraints) to maximize the trace of either the steady state *a priori* or *a posteriori* error covariance of the Kalman filter associated with the surviving sensors. These problems are denoted as the *priori* and *posteriori Kalman Filtering Sensor Attack (KFSA)* problems, respectively.

Contributions

Our contributions are as follows. First, we show that for the *priori* and *posteriori* KFSS problems, *there are no polynomial-time constant-factor approximation algorithms for these problems* (unless $P = NP$) *even* for the special case when the system is stable and all sensors have the same cost. In other words, there are no polynomial-time algorithms that can find a sensor selection that is always guaranteed to yield a mean square estimation error (MSEE) that is within any constant finite factor of the MSEE for the optimal selection. More importantly, our result stands in stark contrast to other sensor selection problems studied in the literature, which leveraged submodularity of their associated cost functions to provide greedy algorithms with constant-factor approximation ratios (e.g., [19], [32]). Second, we show that the same results hold

for the priori and posteriori KFSA problems. Our inapproximability results directly imply that greedy algorithms cannot provide constant-factor guarantees for our problems. Our third contribution is to explicitly show how greedy algorithms can provide arbitrarily poor performance even for very small instances (with only three states) of the priori and posteriori KFSS (resp., KFSA) problems.

A portion of the results pertaining to only the priori KFSS problem appears in the conference paper [33].

Related work

The authors in [11] and [32] studied the design-time sensor selection problem for discrete-time linear time-varying systems over a finite time horizon. The objective is to minimize the estimation error with a cardinality constraint on the chosen sensors (or alternatively, minimize the number of chosen sensors while guaranteeing a certain level of performance in terms of the estimation error). The authors analyzed the performance of greedy algorithms for this problem. However, their results cannot be directly applied to the problems that we consider here, since we aim to optimize the steady state estimation error.

The papers [16] and [18] considered the same design-time sensor selection as the one we consider here. In [16], the authors expressed the problem as a semidefinite program (SDP). However, they did not provide theoretical guarantees on the performance of the proposed algorithm. The paper [18] showed that the problem is NP-hard and provided upper bounds on the performance of any algorithm for the problem; these upper bounds were functions of the system matrices. Although [18] showed via simulations that greedy algorithms performed well for several randomly generated systems, the question of whether such algorithms (or other polynomial-time algorithms) could provide constant-factor approximation ratios for the problem was left open. We resolve this question in this paper by showing that there does not exist any polynomial-time constant-factor approximation algorithm for this problem.

In [30], the authors studied the problem of attacking a given observation selection in Gaussian process regression [34] to maximize the *posteriori* variance of the predictor variable. It was shown that this problem is NP-hard. Moreover, they also gave an instance of this problem such that a greedy algorithm for finding an optimal attack will perform arbitrarily poorly. In [35], the authors considered the scenario where the attacker can target a different set of sensors at each time step to maximize certain metrics of the error covariance of the Kalman filter at the final time step. Some suboptimal algorithms were provided with simulation results. Different from [30] and [35], we study the problem where the attacker removes a set of installed sensors to maximize the trace of the steady state error covariance of the Kalman filter associated with the surviving sensors, and provide fundamental limitations on achievable performance by any possible algorithm for this problem.

Notation and Terminology

The sets of integers and real numbers are denoted as \mathbb{Z} and \mathbb{R} , respectively. The set of integers that are greater than

(resp., greater than or equal to) $a \in \mathbb{R}$ is denoted as $\mathbb{Z}_{>a}$ (resp., $\mathbb{Z}_{\geq a}$). Similarly, we use the notations $\mathbb{R}_{>a}$ and $\mathbb{R}_{\geq a}$. For any $x \in \mathbb{R}$, let $\lceil x \rceil$ be the least integer greater than or equal to x . For a square matrix $P \in \mathbb{R}^{n \times n}$, let P^T , $\text{rank}(P)$, $\text{rowspace}(P)$ and $\text{trace}(P)$ be its transpose, rank, rowspace and trace, respectively. We use P_{ij} (or $(P)_{ij}$) to denote the element in the i th row and j th column of P . A diagonal matrix $P \in \mathbb{R}^{n \times n}$ is denoted as $\text{diag}(P_{11}, \dots, P_{nn})$. The set of n by n positive definite (resp., positive semi-definite) matrices is denoted as \mathbb{S}_{++}^n (resp., \mathbb{S}_+^n). The identity matrix with dimension $n \times n$ is denoted as I_n . The zero matrix with dimension $m \times n$ is denoted as $\mathbf{0}_{m \times n}$. In a matrix, let $*$ denote elements of the matrix that are of no interest. For a vector v , let v_i be the i th element of v and define the support of v to be $\text{supp}(v) = \{i : v_i \neq 0\}$. The Euclidean norm of v is denoted by $\|v\|_2$. Define \mathbf{e}_i to be a row vector where the i th element is 1 and all the other elements are zero; the dimension of the vector can be inferred from the context. Define $\mathbf{1}_n$ to be a column vector of dimension n with all the elements equal to 1. The set of 0-1 indicator vectors of dimension n is denoted as $\{0, 1\}^n$. For a random variable ω , let $\mathbb{E}[\omega]$ be its expectation. For a set \mathcal{A} , let $|\mathcal{A}|$ be its cardinality.

II. PROBLEM FORMULATION

Consider the discrete-time linear system

$$x[k+1] = Ax[k] + w[k], \quad (1)$$

where $x[k] \in \mathbb{R}^n$ is the system state, $w[k] \in \mathbb{R}^n$ is a zero-mean white Gaussian noise process with $\mathbb{E}[w[k](w[k])^T] = W$, and $A \in \mathbb{R}^{n \times n}$ is the system dynamics matrix. The initial state $x[0]$ is assumed to be a Gaussian random vector with mean $\bar{x}_0 \in \mathbb{R}^n$ and covariance $\Pi_0 \in \mathbb{S}_+^n$.

Consider a set \mathcal{Q} that contains q sensors. Each sensor $i \in \mathcal{Q}$ provides a measurement of the system of the form

$$y_i[k] = C_i x[k] + v_i[k], \quad (2)$$

where $C_i \in \mathbb{R}^{s_i \times n}$ is the measurement matrix for sensor i , and $v_i[k] \in \mathbb{R}^{s_i}$ is a zero-mean white Gaussian noise process. We further define $y[k] \triangleq [(y_1[k])^T \dots (y_q[k])^T]^T$, $C \triangleq [C_1^T \dots C_q^T]^T$ and $v[k] \triangleq [(v_1[k])^T \dots (v_q[k])^T]^T$. Thus, the output provided by all sensors together is given by

$$y[k] = Cx[k] + v[k], \quad (3)$$

where $C \in \mathbb{R}^{s \times n}$ and $s = \sum_{i=1}^q s_i$. Denote $\mathbb{E}[v[k](v[k])^T] = V$. We assume that the system noise and the measurement noise are uncorrelated, i.e., $\mathbb{E}[v[k](w[j])^T] = \mathbf{0}_{s \times n}$, $\forall k, j \in \mathbb{Z}_{\geq 0}$, and $x[0]$ is independent of $w[k]$ and $v[k]$, $\forall k \in \mathbb{Z}_{\geq 0}$.

A. The Sensor Selection Problem

Consider the scenario where there are no sensors initially deployed on the system. Instead, the system designer must select a subset of sensors from \mathcal{Q} to install. Each sensor $i \in \mathcal{Q}$ has a cost $b_i \in \mathbb{R}_{\geq 0}$; define the cost vector $b \triangleq [b_1 \dots b_q]^T$. The designer has a budget $B \in \mathbb{R}_{\geq 0}$ that can be spent on choosing sensors from \mathcal{Q} .

After a set of sensors is selected and installed, the Kalman filter is applied to provide an optimal estimate of the states

using the measurements from the installed sensors (in the sense of minimizing the MSEE). Define $\mu \in \{0, 1\}^q$ to be the indicator vector of the selected sensors, where $\mu_i = 1$ if and only if sensor $i \in \mathcal{Q}$ is installed. Let $C(\mu)$ denote the measurement matrix of the installed sensors indicated by μ , i.e., $C(\mu) \triangleq [C_{i_1}^T \cdots C_{i_p}^T]^T$, where $\text{supp}(\mu) = \{i_1, \dots, i_p\}$. Similarly, let $V(\mu)$ be the measurement noise covariance matrix of the installed sensors, i.e., $V(\mu) = \mathbb{E}[\tilde{v}[k](\tilde{v}[k])^T]$, where $\tilde{v}[k] = [(v_{i_1}[k])^T \cdots (v_{i_p}[k])^T]^T$. Let $\Sigma_{k|k-1}(\mu)$ (resp., $\Sigma_{k|k}(\mu)$) denote the *a priori* (resp., *a posteriori*) error covariance matrix of the Kalman filter at time step k , when the sensors indicated by μ are installed. Take the initial covariance $\Sigma_{0|-1}(\mu) = \Pi_0$, $\forall \mu$. We will use the following result [36].

Lemma 1: Suppose that the pair $(A, W^{\frac{1}{2}})$ is stabilizable. For a given indicator vector μ , $\Sigma_{k|k-1}(\mu)$ (resp., $\Sigma_{k|k}(\mu)$) will converge to a finite limit $\Sigma(\mu)$ (resp., $\Sigma^*(\mu)$), which does not depend on the initial covariance Π_0 , as $k \rightarrow \infty$ if and only if the pair $(A, C(\mu))$ is detectable. \square

The limit $\Sigma(\mu)$ satisfies the *discrete algebraic Riccati equation (DARE)* [36]:

$$\begin{aligned} \Sigma(\mu) &= A\Sigma(\mu)A^T + W - \\ &A\Sigma(\mu)C(\mu)^T(C(\mu)\Sigma(\mu)C(\mu)^T + V(\mu))^{-1}C(\mu)\Sigma(\mu)A^T. \end{aligned} \quad (4)$$

The limits $\Sigma(\mu)$ and $\Sigma^*(\mu)$ are coupled as

$$\Sigma(\mu) = A\Sigma^*(\mu)A^T + W. \quad (5)$$

The limit $\Sigma^*(\mu)$ of the *a posteriori* error covariance matrix satisfies the following equation [37]:

$$\begin{aligned} \Sigma^*(\mu) &= \Sigma(\mu) - \\ &\Sigma(\mu)C(\mu)^T(C(\mu)\Sigma(\mu)C(\mu)^T + V(\mu))^{-1}C(\mu)\Sigma(\mu). \end{aligned} \quad (6)$$

Note that we can either obtain $\Sigma^*(\mu)$ from $\Sigma(\mu)$ using Eq. (6) or by substituting Eq. (5) into Eq. (6) and solving for $\Sigma^*(\mu)$. The inverses in Eq. (4) and Eq. (6) are interpreted as pseudo-inverses if the arguments are not invertible.

For the case when the pair $(A, C(\mu))$ is not detectable, we define $\Sigma(\mu) = +\infty$ and $\Sigma^*(\mu) = +\infty$. Moreover, for any sensor selection μ , we note from Lemma 1 that the limit $\Sigma(\mu)$ (resp., $\Sigma^*(\mu)$), if it exists, does not depend on \bar{x}_0 or Π_0 . Thus, we can assume without loss of generality that $\bar{x}_0 = \mathbf{0}$ and $\Pi_0 = I_n$ in the sequel. The priori and posteriori Kalman Filtering Sensor Selection (KFSS) problems are then defined as follows.

Problem 1: (Priori and Posteriori KFSS Problems). Given a system dynamics matrix $A \in \mathbb{R}^{n \times n}$, a measurement matrix $C \in \mathbb{R}^{s \times n}$ containing all of the individual sensor measurement matrices, a system noise covariance matrix $W \in \mathbb{S}_+^n$, a sensor noise covariance matrix $V \in \mathbb{S}_+^s$, a cost vector $b \in \mathbb{R}_{\geq 0}^q$ and a budget $B \in \mathbb{R}_{\geq 0}$, the priori Kalman filtering sensor selection problem is to find the sensor selection μ , i.e., the indicator vector μ of the selected sensors, that solves

$$\begin{aligned} \min_{\mu \in \{0, 1\}^q} \quad & \text{trace}(\Sigma(\mu)) \\ \text{s.t.} \quad & b^T \mu \leq B \end{aligned}$$

where $\Sigma(\mu)$ is given by Eq. (4) if the pair $(A, C(\mu))$ is detectable, and $\Sigma(\mu) = +\infty$ if otherwise. Similarly, the posteriori Kalman filtering sensor selection problem is to find the sensor selection μ that solves

$$\begin{aligned} \min_{\mu \in \{0, 1\}^q} \quad & \text{trace}(\Sigma^*(\mu)) \\ \text{s.t.} \quad & b^T \mu \leq B \end{aligned}$$

where $\Sigma^*(\mu)$ is given by Eq. (6) if the pair $(A, C(\mu))$ is detectable, and $\Sigma^*(\mu) = +\infty$ if otherwise. \square

B. The Sensor Attack Problem

Now consider the scenario where the set \mathcal{Q} of sensors has already been installed on the system. An adversary desires to attack a subset of sensors (i.e., remove a subset of sensors from the system), where each sensor $i \in \mathcal{Q}$ has an attack cost $\omega_i \in \mathbb{R}_{\geq 0}$; define the cost vector $\omega \triangleq [\omega_1 \cdots \omega_q]^T$. We assume that the adversary has a budget $\Omega \in \mathbb{R}_{\geq 0}$, which is the total cost that can be spent on removing sensors from \mathcal{Q} .

After a subset of sensors are attacked (i.e., removed), the Kalman filter is then applied to estimate the states using the measurements from the surviving sensors. We define a vector $\nu \in \{0, 1\}^q$ to be the indicator vector of the attacked sensors, where $\nu_i = 1$ if and only if sensor $i \in \mathcal{Q}$ is attacked. Hence, the set of sensors that survive is $\mathcal{Q} \setminus \text{supp}(\nu)$. Define $\nu^c \in \{0, 1\}^q$ to be the vector such that $\text{supp}(\nu^c) = \mathcal{Q} \setminus \text{supp}(\nu)$, i.e., $\nu_i^c = 1$ if and only if sensor $i \in \mathcal{Q}$ survives. Similarly to the sensor selection problem, we let $C(\nu^c)$ and $V(\nu^c)$ denote the measurement matrix and the measurement noise covariance matrix, respectively, corresponding to ν^c . Furthermore, let $\Sigma_{k|k-1}(\nu^c)$ and $\Sigma_{k|k}(\nu^c)$ denote the *a priori* error covariance matrix and the *a posteriori* error covariance matrix of the Kalman filter at time step k , respectively. Denote $\lim_{k \rightarrow \infty} \Sigma_{k|k-1}(\nu^c) = \Sigma(\nu^c)$ and $\lim_{k \rightarrow \infty} \Sigma_{k|k}(\nu^c) = \Sigma^*(\nu^c)$ if the limits exist, according to Lemma 1. Note that Eq. (4)-(6) also hold if we substitute μ with ν^c .

For the case when the pair $(A, C(\nu^c))$ is not detectable, we define $\Sigma(\nu^c) = +\infty$ and $\Sigma^*(\nu^c) = +\infty$. Recall that we have assumed without loss of generality that $\bar{x}_0 = \mathbf{0}$ and $\Pi_0 = I_n$. The priori and posteriori Kalman Filtering Sensor Attack (KFSA) problems are defined as follows.

Problem 2: (Priori and Posteriori KFSA Problems). Given a system dynamics matrix $A \in \mathbb{R}^{n \times n}$, a measurement matrix $C \in \mathbb{R}^{s \times n}$, a system noise covariance matrix $W \in \mathbb{S}_+^n$, a sensor noise covariance matrix $V \in \mathbb{S}_+^s$, a cost vector $\omega \in \mathbb{R}_{\geq 0}^q$ and a budget $\Omega \in \mathbb{R}_{\geq 0}$, the priori Kalman filtering sensor attack problem is to find the sensor attack ν , i.e., the indicator vector ν of the attacked sensors, that solves

$$\begin{aligned} \max_{\nu \in \{0, 1\}^q} \quad & \text{trace}(\Sigma(\nu^c)) \\ \text{s.t.} \quad & \omega^T \nu \leq \Omega \end{aligned}$$

where $\Sigma(\nu^c)$ is given by Eq. (4) if the pair $(A, C(\nu^c))$ is detectable, and $\Sigma(\nu^c) = +\infty$ if otherwise. Similarly, the posteriori Kalman filtering sensor attack problem is to find the sensor attack ν that solves

$$\begin{aligned} \max_{\nu \in \{0, 1\}^q} \quad & \text{trace}(\Sigma^*(\nu^c)) \\ \text{s.t.} \quad & \omega^T \nu \leq \Omega \end{aligned}$$

where $\Sigma^*(\nu^c)$ is given by Eq. (6) if the pair $(A, C(\nu^c))$ is detectable, and $\Sigma^*(\nu^c) = +\infty$ if otherwise. \square

Note that although we focus on the optimal sensor selection and attack problems for Kalman filtering, due to the duality between the Kalman filter and the Linear Quadratic Regulator (LQR) [38], all of the analysis in this paper will also apply if the priori KFSS and KFSA problems are rephrased as optimal actuator selection and attack problems for LQR, respectively. We omit the details of the rephrasing in the interest of space.

Remark 1: Our goal in this paper is to show that for the priori and posteriori KFSS problems and the priori and posteriori KFSA problems, the optimal solutions cannot be approximated within any constant factor in polynomial time. To do this, it is sufficient for us to consider the special case when $C_i \in \mathbb{R}^{1 \times n}$, $\forall i \in \{1, \dots, q\}$, i.e., each sensor provides a scalar measurement. Moreover, the sensor selection cost vector and the sensor attack cost vector are considered to be $b = [1 \ \dots \ 1]^T$ and $\omega = [1 \ \dots \ 1]^T$, respectively, i.e., the selection cost and the attack cost of each sensor are both equal to 1. By showing that the problems are inapproximable even for these special subclasses, we obtain that the general versions of the problems are inapproximable as well. \square

III. INAPPROXIMABILITY OF THE KFSS AND KFSA PROBLEMS

In this section, we analyze the approximability of the KFSS and KFSA problems. We will start with a brief overview of some relevant concepts from the field of computational complexity, and then provide some preliminary lemmas that we will use in proving our results. That will lead into our characterizations of the complexity of KFSS and KFSA.

A. Review of Complexity Theory

We first review the following fundamental concepts from complexity theory [39].

Definition 1: A *polynomial-time algorithm* for a problem is an algorithm that returns a solution to the problem in a polynomial (in the size of the problem) number of computations. \square

Definition 2: A *decision problem* is a problem whose answer is “yes” or “no”. The set P contains those decision problems that can be solved by a polynomial-time algorithm. The set NP contains those decision problems whose “yes” answers can be verified using a polynomial-time algorithm. \square

Definition 3: An *optimization problem* is a problem whose objective is to maximize or minimize a certain quantity, possibly subject to constraints. \square

Definition 4: A problem \mathcal{P}_1 is *NP-complete* if (a) $\mathcal{P}_1 \in \text{NP}$ and (b) for any problem \mathcal{P}_2 in NP, there exists a polynomial-time algorithm that converts (or “reduces”) any instance of \mathcal{P}_2 to an instance of \mathcal{P}_1 such that the answer to the constructed instance of \mathcal{P}_1 provides the answer to the instance of \mathcal{P}_2 . \mathcal{P}_1 is *NP-hard* if it satisfies (b), but not necessarily (a). \square

The above definition indicates that if one had a polynomial-time algorithm for an NP-complete (or NP-hard) problem, then one could solve *every* problem in NP in polynomial time. Specifically, suppose we had a polynomial-time algorithm to

solve an NP-hard problem \mathcal{P}_1 . Then, given any problem \mathcal{P}_2 in NP, one could first reduce any instance of \mathcal{P}_2 to an instance of \mathcal{P}_1 in polynomial time (such that the answer to the constructed instance of \mathcal{P}_1 provides the answer to the given instance of \mathcal{P}_2), and then use the polynomial-time algorithm for \mathcal{P}_1 to obtain the answer to \mathcal{P}_2 .

The above discussion also reveals that to show that a given problem \mathcal{P}_1 is NP-hard, one simply needs to show that any instance of some other *NP-hard* (or *NP-complete*) problem \mathcal{P}_2 can be reduced to an instance of \mathcal{P}_1 in polynomial time (in such a way that the answer to the constructed instance of \mathcal{P}_1 provides the answer to the given instance of \mathcal{P}_2). For then, an algorithm for \mathcal{P}_1 can be used to solve \mathcal{P}_2 , and hence, to solve all problems in NP (by NP-hardness of \mathcal{P}_2).

The following is a fundamental result in computational complexity theory [39].

Lemma 2: If $P \neq \text{NP}$, there is no polynomial-time algorithm for any NP-complete (or NP-hard) problem. \square

For NP-hard optimization problems, polynomial-time approximation algorithms are of particular interest. A constant-factor approximation algorithm is defined as follows.

Definition 5: A *constant-factor approximation algorithm* for an optimization problem is an algorithm that always returns a solution within a constant (system-independent) factor of the optimal solution. \square

We will discuss the notion of a constant-factor approximation algorithm in greater depth later in this section. As described in the Introduction, the KFSS problem was shown to be NP-hard in [18] for two classes of systems and sensor costs. First, when the A matrix is unstable, it was shown in [2] that the problem of selecting a subset of sensors to make the system detectable is NP-hard, which implies that KFSS is NP-hard using Lemma 1 as shown in [18]. Second, when the A matrix is stable (so that all sensor selections cause the system to be detectable), [18] showed that when the sensor selection costs can be arbitrary, the knapsack problem can be encoded as a special case of the KFSS problem, thereby again showing NP-hardness of the latter problem.

In this paper, we will show that the hardness of KFSS (resp., KFSA) does not solely come from selecting (resp., attacking) sensors to make the system detectable (resp., undetectable) or the sensor selection (resp., attack) costs. To do this, we will show a stronger result that there is no polynomial-time constant-factor approximation algorithm for KFSS (resp., KFSA) *even* when the corresponding system dynamics matrix A is *stable* (which guarantees the detectability of the system), and all the sensors have the same selection (resp., attack) cost. Specifically, we consider a known NP-complete problem, and show how to reduce it to certain instances of KFSS (resp., KFSA) with stable A matrices in polynomial time such that hypothetical polynomial-time constant-factor approximation algorithms for the latter problems can be used to solve the known NP-complete problem. Since we know from Lemma 2 that if $P \neq \text{NP}$, there does not exist a polynomial-time algorithm for any NP-complete problem, we conclude that if $P \neq \text{NP}$, there is no polynomial-time constant-factor approximation algorithm for KFSS (resp., KFSA), which directly implies that the KFSS (resp., KFSA) problem is NP-hard even under

the extra conditions described above. We emphasize that our results do not imply that there is no polynomial-time constant-factor approximation algorithm for *specific* instances of KFSS (resp., KFSA). Rather, the result is that we cannot have such an algorithm for *all* instances of KFSS (resp., KFSA).

B. Preliminary Results

The following results characterize properties of the KFSS and KFSA instances that we will consider when proving the inapproximability of the KFSS and KFSA problems. The proofs are provided in Appendix A.

Lemma 3: Consider a discrete-time linear system defined in (1) and (3). Suppose the system dynamics matrix is of the form $A = \text{diag}(\lambda_1, \dots, \lambda_n)$ with $0 \leq |\lambda_i| < 1$, $\forall i \in \{1, \dots, n\}$, the system noise covariance matrix $W \in \mathbb{S}_+^n$ is diagonal, and the sensor noise covariance matrix $V \in \mathbb{S}_+^q$. Then, the following hold for all sensor selections μ .

(a) For all $i \in \{1, \dots, n\}$, $(\Sigma(\mu))_{ii}$ and $(\Sigma^*(\mu))_{ii}$ satisfy

$$W_{ii} \leq (\Sigma(\mu))_{ii} \leq \frac{W_{ii}}{1 - \lambda_i^2}, \quad (7)$$

and

$$0 \leq (\Sigma^*(\mu))_{ii} \leq \frac{W_{ii}}{1 - \lambda_i^2}, \quad (8)$$

respectively.

(b) If $\exists i \in \{1, \dots, n\}$ such that $W_{ii} \neq 0$ and the i th column of C is zero, then $(\Sigma(\mu))_{ii} = (\Sigma^*(\mu))_{ii} = \frac{W_{ii}}{1 - \lambda_i^2}$.

(c) If $V = \mathbf{0}_{q \times q}$ and $\exists i \in \{1, \dots, n\}$ such that $\mathbf{e}_i \in \text{rowspace}(C(\mu))$, then $(\Sigma(\mu))_{ii} = W_{ii}$ and $(\Sigma^*(\mu))_{ii} = 0$. \square

Lemma 4: Consider a discrete-time linear system defined in Eq. (1) and Eq. (3). Suppose the system dynamics matrix is of the form $A = \text{diag}(\lambda_1, 0, \dots, 0) \in \mathbb{R}^{n \times n}$, where $0 < |\lambda_1| < 1$, and the system noise covariance matrix is $W = I_n$.

(a) Suppose the measurement matrix is of the form $C = \begin{bmatrix} 1 & \gamma \end{bmatrix}$ with sensor noise variance $V = \sigma_v^2$, where $\gamma \in \mathbb{R}^{1 \times (n-1)}$ and $\sigma_v \in \mathbb{R}_{\geq 0}$. Then, the MSEE of state 1, denoted as Σ_{11} , satisfies

$$\Sigma_{11} = \frac{1 + \alpha^2 \lambda_1^2 - \alpha^2 + \sqrt{(\alpha^2 - \alpha^2 \lambda_1^2 - 1)^2 + 4\alpha^2}}{2}, \quad (9)$$

where $\alpha^2 = \|\gamma\|_2^2 + \sigma_v^2$.

(b) Suppose the measurement matrix is of the form $C = \begin{bmatrix} \mathbf{1}_{n-1} & \rho I_{n-1} \end{bmatrix}$ with sensor noise covariance $V = \mathbf{0}_{(n-1) \times (n-1)}$, where $\rho \in \mathbb{R}$. Then, the MSEE of state 1, denoted as Σ'_{11} , satisfies

$$\Sigma'_{11} = \frac{\lambda_1^2 \rho^2 + n' - \rho^2 + \sqrt{(\rho^2 - \lambda_1^2 \rho^2 - n')^2 + 4n' \rho^2}}{2n'}, \quad (10)$$

where $n' = n - 1$.

Moreover, if we view Σ_{11} and Σ'_{11} as functions of α^2 and ρ^2 , denoted as $\Sigma_{11}(\alpha^2)$ and $\Sigma'_{11}(\rho^2)$, respectively, then $\Sigma_{11}(\alpha^2)$ and $\Sigma'_{11}(\rho^2)$ are strictly increasing functions of $\alpha^2 \in \mathbb{R}_{\geq 0}$ and $\rho^2 \in \mathbb{R}_{\geq 0}$, with $\lim_{\alpha \rightarrow \infty} \Sigma_{11}(\alpha^2) = \frac{1}{1 - \lambda_1^2}$ and $\lim_{\rho \rightarrow \infty} \Sigma'_{11}(\rho^2) = \frac{1}{1 - \lambda_1^2}$, respectively. \square

C. Inapproximability of the KFSS Problem

In this section, we characterize the achievable performance of algorithms for the priori and posteriori KFSS problems. For any given algorithm \mathcal{A} (resp., \mathcal{A}') of the priori (resp., posteriori) KFSS problem, we define the following ratios:

$$r_{\mathcal{A}}(\Sigma) \triangleq \frac{\text{trace}(\Sigma_{\mathcal{A}})}{\text{trace}(\Sigma_{opt})}, \quad (11)$$

and

$$r_{\mathcal{A}'}(\Sigma^*) \triangleq \frac{\text{trace}(\Sigma_{\mathcal{A}'}^*)}{\text{trace}(\Sigma_{opt}^*)}, \quad (12)$$

where Σ_{opt} (resp., Σ_{opt}^*) is the optimal solution to the priori (resp., posteriori) KFSS problem and $\Sigma_{\mathcal{A}}$ (resp., $\Sigma_{\mathcal{A}'}^*$) is the solution to the priori (resp., posteriori) KFSS problem given by algorithm \mathcal{A} (resp., \mathcal{A}').

In [18], the authors showed that there is an upper bound for $r_{\mathcal{A}}(\Sigma)$ (resp., $r_{\mathcal{A}'}(\Sigma^*)$) for any sensor selection algorithm \mathcal{A} (resp., \mathcal{A}'), in terms of the system matrices. However, the question of whether it is possible to find an algorithm \mathcal{A} (resp., \mathcal{A}') that is guaranteed to provide an approximation ratio $r_{\mathcal{A}}(\Sigma)$ (resp., $r_{\mathcal{A}'}(\Sigma^*)$) that is *independent* of the system parameters has remained open up to this point. In particular, it is desirable to find polynomial-time *constant-factor* approximation algorithms for the priori (resp., posteriori) KFSS problem, where the ratio $r_{\mathcal{A}}(\Sigma)$ (resp., $r_{\mathcal{A}'}(\Sigma^*)$) is upper-bounded by some (system-independent) constant.¹ We provide a negative result by showing that there are no polynomial-time algorithms that can always yield a solution that is within any constant factor of the optimal (unless P = NP), i.e., for all polynomial-time algorithms \mathcal{A} (resp., \mathcal{A}') and $\forall K \in \mathbb{R}_{\geq 1}$, there are instances of the priori (resp., posteriori) KFSS problem where $r_{\mathcal{A}}(\Sigma) > K$ (resp., $r_{\mathcal{A}'}(\Sigma^*) > K$).

Remark 2: Note that the “constant” in “constant-factor approximation algorithm” refers to the fact that the *cost* of the solution provided by the algorithm is upper-bounded by some (system-independent) constant times the cost of the optimal solution. The algorithm can, however, use the system parameters when finding the solution. For example, an optimal algorithm for the KFSS problem will be a 1-factor approximation, and would use the system matrices, sensor costs, and budget to find the optimal solution. Similarly, a polynomial-time K -factor approximation algorithm for KFSS would use the system parameters to produce a solution whose cost is guaranteed to be no more than K times the cost of the optimal solution. As indicated above, we will show that no such algorithm exists for any constant K (unless P = NP). \square

To show the inapproximability of the priori KFSS problem, we relate it to the EXACT COVER BY 3-SETS (X3C) problem described below [39].

Definition 6: (X3C) Given a finite set $D = \{d_1, \dots, d_{3m}\}$ and a collection $\mathcal{C} = \{c_1, \dots, c_\tau\}$ of 3-element subsets of D , an *exact cover* for D is a subcollection $\mathcal{C}' \subseteq \mathcal{C}$ such that every element of D occurs in exactly one member of \mathcal{C}' . \square

We will use the following result [39].

¹Polynomial-time constant-factor approximation algorithms have been widely studied for NP-hard problems, e.g., [39].

Lemma 5: Given a finite set $D = \{d_1, \dots, d_{3m}\}$ and a collection $\mathcal{C} = \{c_1, \dots, c_\tau\}$ of 3-element subsets of D , the problem of determining whether \mathcal{C} contains an exact cover for D is NP-complete. \square

As argued in Remark 1, in order to show that the priori KFSS problem cannot be approximated within any constant factor in polynomial time, it is sufficient for us to show that certain special instances of this problem are inapproximable. Specifically, consider any instance of the $X3C$ problem. Using the results in Lemma 3-4, we will first construct an instance of the priori KFSS problem in polynomial time such that the difference between the solution to KFSS when the answer to $X3C$ is “yes” and the solution to KFSS when the answer to $X3C$ is “no” is large enough. Thus, we can then apply any hypothetical polynomial-time constant-factor approximation algorithm for the priori KFSS problem to the constructed priori KFSS instance and obtain the answer to the $X3C$ instance. Since we know from Lemma 5 that the $X3C$ problem is NP-complete, we obtain from Lemma 2 the following result; the detailed proof is provided in Appendix B.

Theorem 1: If $P \neq NP$, then there is no polynomial-time constant-factor approximation algorithm for the priori KFSS problem. \square

The following result is a direct consequence of the above arguments; the proof is also provided in Appendix B.

Corollary 1: If $P \neq NP$, then there is no polynomial-time constant-factor approximation algorithm for the posteriori KFSS problem. \square

D. Inapproximability of the KFSA Problem

In this section, we analyze the achievable performance of algorithms for the priori and posteriori KFSA problems. For any given algorithm \mathcal{A} (resp., \mathcal{A}') for the priori (resp., posteriori) KFSA problem, we define the following ratios:

$$r_{\mathcal{A}}(\tilde{\Sigma}) \triangleq \frac{\text{trace}(\tilde{\Sigma}_{opt})}{\text{trace}(\tilde{\Sigma}_{\mathcal{A}})}, \quad (13)$$

and

$$r_{\mathcal{A}'}(\tilde{\Sigma}^*) \triangleq \frac{\text{trace}(\tilde{\Sigma}_{opt}^*)}{\text{trace}(\tilde{\Sigma}_{\mathcal{A}'}^*)}, \quad (14)$$

where $\tilde{\Sigma}_{opt}$ (resp., $\tilde{\Sigma}_{opt}^*$) is the optimal solution to the priori (resp., posteriori) KFSA problem and $\tilde{\Sigma}_{\mathcal{A}}$ (resp., $\tilde{\Sigma}_{\mathcal{A}'}^*$) is the solution to the priori (resp., posteriori) KFSA problem given by algorithm \mathcal{A} (resp., \mathcal{A}'). It is worth noting that using the arguments in [18], the same (system-dependent) upper bounds for $r_{\mathcal{A}}(\tilde{\Sigma})$ and $r_{\mathcal{A}'}(\tilde{\Sigma}^*)$ can be obtained as those for $r_{\mathcal{A}}(\Sigma)$ and $r_{\mathcal{A}'}(\Sigma^*)$ in [18], respectively. Nevertheless, we show that (if $P \neq NP$) there is again no polynomial-time constant-factor approximation algorithm for the priori (resp., posteriori) KFSA problem, i.e., for all $K \in \mathbb{R}_{\geq 1}$ and for all polynomial-time algorithms \mathcal{A} (resp., \mathcal{A}'), there are instances of the priori (resp., posteriori) KFSA problem where $r_{\mathcal{A}}(\tilde{\Sigma}) > K$ (resp., $r_{\mathcal{A}'}(\tilde{\Sigma}^*) > K$). To establish this result, we relate the priori KFSA problem to the $X3C$ problem described in Definition 6 and Lemma 5. Similarly to the proof of Theorem 1, given any instance of $X3C$, we will construct an instance of the priori

KFSA problem and show that any hypothetical polynomial-time constant-factor approximation algorithm for the priori KFSA problem can be used to solve the $X3C$ problem. This leads to the following result; the detailed proof is provided in Appendix C.

Theorem 2: If $P \neq NP$, then there is no polynomial-time constant-factor approximation algorithm for the priori KFSA problem. \square

The arguments above also imply the following result whose proof is provided in Appendix C.

Corollary 2: If $P \neq NP$, then there is no polynomial-time constant-factor approximation algorithm for the posteriori KFSA problem. \square

IV. FAILURE OF GREEDY ALGORITHMS

Our results in Theorem 1 and Theorem 2 indicate that no polynomial-time algorithm can be guaranteed to yield a solution that is within any constant factor of the optimal solution to the priori (resp., posteriori) KFSS and KFSA problems. In particular, these results apply to the greedy algorithms that are often studied for sensor selection in the literature (e.g., [18], [30]), where sensors are iteratively selected (resp., attacked) in order to produce the greatest decrease (resp., increase) in the error covariance at each iteration. In this section we will focus on such greedy algorithms for the priori (resp., posteriori) KFSS and KFSA problems, and show explicitly how these greedy algorithms can fail to provide good solutions even for small and fixed instances with only three states; this provides additional insight into the factors that cause the KFSS and KFSA problems to be challenging.

A. Failure of Greedy Algorithms for the KFSS Problem

It was shown via simulations in [18] that greedy algorithms for KFSS work well in practice (e.g., for randomly generated systems). In this section, we provide an explicit example showing that greedy algorithms for the priori and posteriori KFSS problems can perform arbitrarily poorly, even for small systems (containing only three states). We consider the greedy algorithm for the priori (resp., posteriori) KFSS problem given in Algorithm 1, for instances where all sensors have selection costs equal to 1, and the sensor selection budget $B \in \{1, \dots, q\}$ (i.e., up to B sensors can be chosen). For any such instance of the priori (resp., posteriori) KFSS problem, define $r_{gre}(\Sigma) = \frac{\text{trace}(\Sigma_{gre})}{\text{trace}(\Sigma_{opt})}$ (resp., $r_{gre}(\Sigma^*) = \frac{\text{trace}(\Sigma_{gre}^*)}{\text{trace}(\Sigma_{opt}^*)}$), where Σ_{gre} (resp., Σ_{gre}^*) is the solution of Eq. (4) (resp., Eq. (6)) corresponding to the sensors selected by Algorithm 1.

Algorithm 1 Greedy Algorithm for Problem 1

Input: An instance of priori (resp., posteriori) KFSS

Output: A set \mathcal{S} of selected sensors

- 1: $k \leftarrow 1, \mathcal{S} \leftarrow \emptyset$
 - 2: **for** $k \leq B$ **do**
 - 3: $j \in \arg \min_{i \notin \mathcal{S}} \text{trace}(\Sigma(\mathcal{S} \cup \{i\}))$ (resp., $j \in \arg \min_{i \notin \mathcal{S}} \text{trace}(\Sigma^*(\mathcal{S} \cup \{i\}))$)
 - 4: $\mathcal{S} \leftarrow \mathcal{S} \cup \{j\}, k \leftarrow k + 1$
 - 5: **end for**
-

Example 1: Consider an instance of the priori (resp., posteriori) KFSS problem with matrices $W = I_3$ and $V = \mathbf{0}_{3 \times 3}$, and A, C defined as

$$A = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & h & h \\ 1 & 0 & h \\ 0 & 1 & 1 \end{bmatrix},$$

where $0 < |\lambda_1| < 1$, $\lambda_1 \in \mathbb{R}$, and $h \in \mathbb{R}_{>0}$. In addition, we have the selection budget $B = 2$, the cost vector $b = [1 \ 1 \ 1]^T$ and the set of candidate sensors $\mathcal{Q} = \{1, 2, 3\}$, where sensor i corresponds to the i th row of matrix C , for $i \in \{1, 2, 3\}$. \square

Based on the system defined in Example 1, we have the following result whose proof is provided in Appendix D.

Theorem 3: For the instance of the priori (resp., posteriori) KFSS problem defined in Example 1, the ratios $r_{gre}(\Sigma) = \frac{\text{trace}(\Sigma_{gre})}{\text{trace}(\Sigma_{opt})}$ and $r_{gre}(\Sigma^*) = \frac{\text{trace}(\Sigma_{gre}^*)}{\text{trace}(\Sigma_{opt}^*)}$ satisfy

$$\lim_{h \rightarrow \infty} r_{gre}(\Sigma) = \frac{2}{3} + \frac{1}{3(1 - \lambda_1^2)}, \quad (15)$$

and

$$\lim_{h \rightarrow \infty} r_{gre}(\Sigma^*) = \frac{1}{1 - \lambda_1^2}, \quad (16)$$

respectively. \square

Examining Eq. (15) (resp., Eq. (16)), we see that for the given instance of the priori (resp., posteriori) KFSS problem, we have $r_{gre}(\Sigma) \rightarrow \infty$ (resp., $r_{gre}(\Sigma^*) \rightarrow \infty$) as $h \rightarrow \infty$ and $\lambda_1 \rightarrow 1$. Thus, $r_{gre}(\Sigma)$ (resp., $r_{gre}(\Sigma^*)$) can be made arbitrarily large by choosing the parameters in the instance appropriately. To explain the result in Theorem 3, we first note that the only nonzero eigenvalue of the diagonal A defined in Example 1 is λ_1 , and so we know from Lemma 3(a) that state 2 and state 3 of the system defined in Example 1 each contributes at most 1 to $\text{trace}(\Sigma(\mu))$ (resp., $\text{trace}(\Sigma^*(\mu))$) for all μ . Hence, in order to minimize $\text{trace}(\Sigma(\mu))$ (resp., $\text{trace}(\Sigma^*(\mu))$), we need to minimize the MSEE of state 1. Moreover, the measurements of state 2 and state 3 can be viewed as measurement noise that corrupts the measurements of state 1. It is then easy to observe from the form of matrix C defined in Example 1 that sensor 2 is the single best sensor among the three sensors since it provides measurements of state 1 with less noise than sensor 1 (and sensor 3 does not measure state 1 at all). Thus, the greedy algorithm for the priori (resp., posteriori) KFSS problem defined in Algorithm 1 selects sensor 2 in its first iteration. Nonetheless, we notice from C defined in Example 1 that the optimal set of two sensors that minimizes $\text{trace}(\Sigma(\mu))$ (resp., $\text{trace}(\Sigma^*(\mu))$) contains sensor 1 and sensor 3, which together give us exact measurements (without measurement noise) on state 1 (after some elementary row operations). Since the greedy algorithm selects sensor 2 in its first iteration, no matter which sensor it selects in its second iteration, the two chosen sensors can only give a noisy measurement of state 1 (if we view the measurements of state 2 and state 3 as measurement noise), and the variance of the measurement noise can be made arbitrary large if we take $h \rightarrow \infty$ in C defined in Example 1. Hence, the greedy algorithm fails to perform well due to its myopic choice in the first iteration.

It is also useful to note that the above behavior holds for any algorithm that outputs a sensor selection that contains sensor 2 for the above example.

B. Failure of Greedy Algorithms for the KFSA Problem

In [30], the authors showed that a simple greedy algorithm can perform arbitrarily poorly for an instance of the observation attack problem in Gaussian process regression. Here, we consider a simple greedy algorithm for the priori (resp., posteriori) KFSA problem given in Algorithm 2, for instances where all sensors have an attack cost of 1, and the sensor attack budget $\Omega \in \{1, \dots, q\}$ (i.e., up to Ω sensors can be attacked). For any such instance of the priori (resp., posteriori) KFSA problem, define $r_{gre}(\tilde{\Sigma}) = \frac{\text{trace}(\tilde{\Sigma}_{opt})}{\text{trace}(\tilde{\Sigma}_{gre})}$ (resp., $r_{gre}(\tilde{\Sigma}^*) = \frac{\text{trace}(\tilde{\Sigma}_{opt}^*)}{\text{trace}(\tilde{\Sigma}_{gre}^*)}$), where $\tilde{\Sigma}_{gre}$ (resp., $\tilde{\Sigma}_{gre}^*$) is the solution to the priori (resp., posteriori) KFSA problem given by Algorithm 2. We then show that Algorithm 2 can perform arbitrarily poorly for a simple instance of the priori (resp., posteriori) KFSA problem described below.

Algorithm 2 Greedy Algorithm for Problem 2

Input: An instance of priori (resp., posteriori) KFSA

Output: A set \mathcal{S} of targeted sensors

- 1: $k \leftarrow 1, \mathcal{S} \leftarrow \emptyset$
 - 2: **for** $k \leq \Omega$ **do**
 - 3: $j \in \arg \max_{i \notin \mathcal{S}} \text{trace}(\Sigma(\mathcal{Q} \setminus (\mathcal{S} \cup \{i\})))$ (resp., $j \in \arg \max_{i \notin \mathcal{S}} \text{trace}(\Sigma^*(\mathcal{Q} \setminus (\mathcal{S} \cup \{i\})))$)
 - 4: $\mathcal{S} \leftarrow \mathcal{S} \cup \{j\}, k \leftarrow k + 1$
 - 5: **end for**
-

Example 2: Consider an instance of the priori (resp., posteriori) KFSA problem with matrices $W = I_3$, $V = \mathbf{0}_{4 \times 4}$, and A, C defined as

$$A = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & h & h \\ 1 & 0 & h \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where $0 < |\lambda_1| < 1$, $\lambda_1 \in \mathbb{R}$ and $h \in \mathbb{R}_{>0}$. In addition, the attack budget is $\Omega = 2$, the cost vector is $\omega = [1 \ 1 \ 1 \ 1]^T$, and the set of sensors $\mathcal{Q} = \{1, 2, 3, 4\}$ has already been installed on the system, where sensor i corresponds to the i th row of matrix C , for $i \in \{1, 2, 3, 4\}$. \square

We then have the following result, whose proof is provided in Appendix D.

Theorem 4: For the instance of the priori (resp., posteriori) KFSA problem defined in Example 2, the ratios $r_{gre}(\tilde{\Sigma}) = \frac{\text{trace}(\tilde{\Sigma}_{opt})}{\text{trace}(\tilde{\Sigma}_{gre})}$ and $r_{gre}(\tilde{\Sigma}^*) = \frac{\text{trace}(\tilde{\Sigma}_{opt}^*)}{\text{trace}(\tilde{\Sigma}_{gre}^*)}$ satisfy

$$\lim_{h \rightarrow 0} r_{gre}(\tilde{\Sigma}) = \frac{2}{3} + \frac{1}{3(1 - \lambda_1^2)}, \quad (17)$$

and

$$\lim_{h \rightarrow 0} r_{gre}(\tilde{\Sigma}^*) = \frac{1}{1 - \lambda_1^2}, \quad (18)$$

respectively. \square

Inspecting Eq. (17) (resp., Eq. (18)), we observe that for the given instance of the priori (resp., posteriori) KFSA problem, we have $r_{gre}(\tilde{\Sigma}) \rightarrow \infty$ (resp., $r_{gre}(\tilde{\Sigma}^*) \rightarrow \infty$) as $h \rightarrow 0$ and $\lambda_1 \rightarrow 1$. Thus, $r_{gre}(\tilde{\Sigma})$ (resp., $r_{gre}(\tilde{\Sigma}^*)$) can be made arbitrarily large by choosing the parameters in the instance appropriately. Here, we explain the results in Theorem 4 as follows. Using similar arguments to those before, we know from the structure of matrix A defined in Example 2 that in order to maximize $\text{trace}(\Sigma(\nu^c))$ (resp., $\text{trace}(\Sigma^*(\nu^c))$), we need to maximize the MSEE of state 1, i.e., make the measurements of state 1 “worse”. Again, the measurements of state 2 and state 3 can be viewed as measurement noise that corrupts the measurements of state 1. No matter which of sensor 1, sensor 2, or sensor 3 is attacked, the resulting measurement matrix $C(\nu^c)$ is full column rank, which yields an exact measurement of state 1. We also observe that if sensor 4 is targeted, the surviving sensors can only provide measurements of state 1 that are corrupted by measurements of states 2 and state 3. Hence, the greedy algorithm for the priori (resp., posteriori) KFSA problem defined in Algorithm 2 targets sensor 4 in its first iteration, since it is the single best sensor to attack from the four sensors. Nevertheless, sensor 1 and sensor 2 form the optimal set of sensors to be attacked to maximize $\text{trace}(\Sigma(\nu^c))$ (resp., $\text{trace}(\Sigma^*(\nu^c))$), since the surviving sensors provide no measurement of state 1. Since the greedy algorithm targets sensor 4 in its first iteration, no matter which sensor it targets in the second step, the surviving sensors can always provide some measurements of state 1 with noise (if we view the measurements of state 2 and state 3 as measurement noise), and the variance of the noise will vanish if we take $h \rightarrow 0$ in matrix C defined in Example 2. Hence, the myopic behavior of the greedy algorithm makes it perform poorly.

Furthermore, it is useful to note that the above result holds for any algorithm that outputs a sensor attack that does not contain sensor 1 or sensor 2 for the above example.

Remark 3: Using similar arguments to those in the proof of Theorem 3 (resp., Theorem 4), we can also show that when we set $V = \varepsilon I_3$ (resp., $V = \varepsilon I_4$), where $\varepsilon \in \mathbb{R}_{>0}$, the results in Eqs. (15)-(16) (resp., Eqs. (17)-(18)) hold if we let $\varepsilon \rightarrow 0$. This phenomenon is also observed in [11], where the approximation guarantees for the greedy algorithms provided in that paper get worse as the sensor measurement noise tends to zero. \square

V. CONCLUSIONS

In this paper, we studied sensor selection and attack problems for (steady state) Kalman filtering of linear dynamical systems. We showed that these problems are NP-hard and have no polynomial-time constant-factor approximation algorithms, even under the assumption that the system is stable and each sensor has identical cost. To illustrate this point, we provided explicit examples showing how greedy algorithms can perform arbitrarily poorly on these problems, even when the system only has three states. Our results shed new insights into the problem of sensor selection and attack for Kalman filtering and show, in particular, that this problem is more difficult than other variants of the sensor selection problem that have

submodular (or supermodular) cost functions. Future work on extending the results to Kalman filtering over finite time horizons, characterizing achievable (non-constant) approximation ratios, identifying classes of systems that admit near-optimal approximation algorithms, and investigating resilient sensor selection problems under adversarial settings would be of interest.

VI. ACKNOWLEDGMENTS

The authors thank the anonymous reviewers for their insightful comments that helped to improve the paper.

APPENDIX A

Proof of Lemma 3:

Since A and W are diagonal, the system represents a set of n scalar subsystems of the form

$$x_i[k+1] = \lambda_i x_i[k] + w_i[k], \forall i \in \{1, \dots, n\},$$

where $x_i[k]$ is the i th state of $x[k]$ and $w_i[k]$ is a zero-mean white Gaussian noise process with variance $\sigma_{w_i}^2 = W_{ii}$. As A is stable, the pair $(A, C(\mu))$ is detectable and the pair $(A, W^{\frac{1}{2}})$ is stabilizable for all sensor selections μ . Thus, the limits $\lim_{k \rightarrow \infty} (\Sigma_{k|k-1}(\mu))_{ii}$ and $\lim_{k \rightarrow \infty} (\Sigma_{k|k}(\mu))_{ii}$ exist for all i and for all μ (based on Lemma 1), and are denoted as $(\Sigma(\mu))_{ii}$ and $(\Sigma^*(\mu))_{ii}$, respectively.

Proof of (a): Since A and W are diagonal, we know from Eq. (5) that

$$(\Sigma(\mu))_{ii} = \lambda_i^2 (\Sigma^*(\mu))_{ii} + W_{ii},$$

which implies $(\Sigma(\mu))_{ii} \geq W_{ii}$, $\forall i \in \{1, \dots, n\}$. Moreover, it is easy to see that $(\Sigma(\mu))_{ii} \leq (\Sigma(\mathbf{0}))_{ii}$, $\forall i \in \{1, \dots, n\}$. Since $C(\mathbf{0}) = \mathbf{0}$, we obtain from Eq. (4) that

$$\Sigma(\mathbf{0}) = A\Sigma(\mathbf{0})A^T + W.$$

which implies that $(\Sigma(\mathbf{0}))_{ii} = \frac{W_{ii}}{1-\lambda_i^2}$ since A is diagonal. Hence, $W_{ii} \leq (\Sigma(\mu))_{ii} \leq \frac{W_{ii}}{1-\lambda_i^2}$, $\forall i \in \{1, \dots, n\}$. Similarly, we also have $(\Sigma^*(\mu))_{ii} \leq (\Sigma^*(\mathbf{0}))_{ii}$, and we obtain from Eq. (6) that

$$\Sigma^*(\mathbf{0}) = A\Sigma^*(\mathbf{0})A^T + W.$$

Thus, $0 \leq (\Sigma^*(\mu))_{ii} \leq \frac{W_{ii}}{1-\lambda_i^2}$, $\forall i \in \{1, \dots, n\}$.

Proof of (b): Assume without loss of generality that the first column of $C(\mu)$ is zero, since we can simply renumber the states to make this the case without affecting the trace of the error covariance matrix. We then have $C(\mu)$ of the form

$$C(\mu) = \begin{bmatrix} \mathbf{0} & C_1(\mu) \end{bmatrix}.$$

Moreover, since A and W are diagonal, we obtain from Eq. (4) that $\Sigma(\mu)$ is of the form

$$\Sigma(\mu) = \begin{bmatrix} \Sigma_1(\mu) & \mathbf{0} \\ \mathbf{0} & \Sigma_2(\mu) \end{bmatrix},$$

where $\Sigma_1(\mu) = (\Sigma(\mu))_{11}$ and satisfies

$$(\Sigma(\mu))_{11} = \lambda_1^2 (\Sigma(\mu))_{11} + W_{11},$$

which implies $(\Sigma(\mu))_{11} = \frac{W_{11}}{1-\lambda_1^2}$. Furthermore, we obtain from Eq. (6) that $\Sigma^*(\mu)$ is of the form

$$\Sigma^*(\mu) = \begin{bmatrix} \Sigma_1^*(\mu) & \mathbf{0} \\ \mathbf{0} & \Sigma_2^*(\mu) \end{bmatrix},$$

where $\Sigma_1^*(\mu) = (\Sigma^*(\mu))_{11}$ and satisfies

$$(\Sigma^*(\mu))_{11} = \lambda_1^2(\Sigma^*(\mu))_{11} + W_{11},$$

which implies $(\Sigma^*(\mu))_{11} = \frac{W_{11}}{1-\lambda_1^2}$.

Proof of (c): We assume without loss of generality that $\mathbf{e}_1 \in \text{rowspace}(C(\mu))$. If we further perform elementary row operations on $C(\mu)$, which does not change the solution to Eq. (4) (resp., Eq. (6)), we obtain a measurement matrix $\tilde{C}(\mu)$ of the form

$$\tilde{C}(\mu) = \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \tilde{C}_1(\mu) \end{bmatrix}$$

with $\tilde{V}(\mu) = \mathbf{0}$. Moreover, since A and W are diagonal, we obtain from Eq. (4) that $\Sigma(\mu)$ is of the form

$$\Sigma(\mu) = \begin{bmatrix} \Sigma_1(\mu) & \mathbf{0} \\ \mathbf{0} & \Sigma_2(\mu) \end{bmatrix},$$

where $\Sigma_1(\mu) = (\Sigma(\mu))_{11}$ and satisfies

$$(\Sigma(\mu))_{11} = \lambda_1^2(\Sigma(\mu))_{11} + W_{11} - \lambda_1^2(\Sigma(\mu))_{11},$$

which implies $(\Sigma(\mu))_{11} = W_{11}$. Furthermore, we obtain from Eq. (6) that $\Sigma^*(\mu)$ is of the form

$$\Sigma^*(\mu) = \begin{bmatrix} \Sigma_1^*(\mu) & \mathbf{0} \\ \mathbf{0} & \Sigma_2^*(\mu) \end{bmatrix},$$

where $\Sigma_1^*(\mu) = (\Sigma^*(\mu))_{11}$ and satisfies $(\Sigma^*(\mu))_{11} = (\Sigma(\mu))_{11} - (\Sigma(\mu))_{11} = 0$. ■

Proof of Lemma 4:

Proof of (a): We first note from Lemma 1 that the limit $\Sigma(\mu)$ exists for all μ (since A is stable). Since $A = \text{diag}(\lambda_1, 0, \dots, 0)$, we have $x_i[k+1] = w_i[k]$, $\forall i \in \{2, \dots, n\}$ and $\forall k \in \mathbb{Z}_{\geq 0}$. Moreover, we have from Eq. (3) that

$$y[k] = [1 \ \mathbf{0}_{1 \times (n-1)}]x[k] + v[k] + v'[k] = x_1[k] + \tilde{v}[k], \quad \forall k \in \mathbb{Z}_{\geq 0},$$

where $v'[k] = \sum_{i=1}^{n-1} \gamma_i x_{i+1}[k]$ and $\tilde{v}[k] \triangleq v[k] + v'[k]$. Recall that we have assumed without loss of generality that $\bar{x}_0 = \mathbf{0}$ and $\Pi_0 = I_n$. Moreover, noting that $W = I_n$ and that $x[0]$ is independent of $w[k]$ and $v[k]$ for all $k \in \mathbb{Z}_{\geq 0}$, where $w[k]$ and $v[k]$ are uncorrelated zero-mean white Gaussian noise processes (as assumed), we have that $\tilde{v}[k]$ is a zero-mean white Gaussian noise process with $\mathbb{E}[(\tilde{v}[k])^2] = \|\gamma\|_2^2 + \sigma_v^2$. Thus, to compute the MSEE of state 1 of the Kalman filter, i.e., Σ_{11} , we can consider a scalar discrete-time linear system with $A = \lambda_1$, $C = 1$, $W = 1$ and $V = \alpha^2$, and obtain from Eq. (4) the scalar DARE

$$\Sigma_{11} = \lambda_1^2 \left(1 - \frac{\Sigma_{11}}{\alpha^2 + \Sigma_{11}}\right) \Sigma_{11} + 1, \quad (19)$$

where $\alpha^2 = \|\gamma\|_2^2 + \sigma_v^2$. Solving for Σ_{11} in Eq. (19) and omitting the negative solution lead to Eq. (9).

To show that Σ_{11} is strictly increasing in $\alpha^2 \in \mathbb{R}_{\geq 0}$, we can use the result of Lemma 6 in [18]. For a discrete-time linear system defined in Eq. (1) and Eq. (3), given $A = \lambda_1$ and $W = 1$, suppose we have two sensors with the measurement matrices as $C_1 = C_2 = 1$ and the variances of the (Gaussian) measurement noise as $V_1 = \alpha_1^2$ and $V_2 = \alpha_2^2$. Define $R \triangleq C^T V^{-1} C$ to be the sensor information matrix corresponding to a sensor with measurement matrix C and measurement noise covariance matrix V . The sensor information matrix of these two sensors are denoted as R_1 and R_2 . We then have $R_1 = \frac{1}{\alpha_1^2}$ and $R_2 = \frac{1}{\alpha_2^2}$. If $\alpha_1^2 > \alpha_2^2$, we know from Lemma 6 in [18] that $\Sigma_{11}(\alpha_1^2) < \Sigma_{11}(\alpha_2^2)$. Hence, $\Sigma_{11}(\alpha^2)$ is a strictly increasing function of $\alpha^2 \in \mathbb{R}_{\geq 0}$. For $\alpha > 0$, we can rewrite Eq. (9) as

$$\Sigma_{11}(\alpha^2) = \frac{2}{\sqrt{(1 - \lambda_1^2 - \frac{1}{\alpha^2})^2 + \frac{4}{\alpha^2}} + 1 - \lambda_1^2 - \frac{1}{\alpha^2}}. \quad (20)$$

We then obtain from Eq. (20) that $\lim_{\alpha \rightarrow \infty} \Sigma_{11}(\alpha^2) = \frac{1}{1 - \lambda_1^2}$.

Proof of (b): Using similar arguments to those above, we obtain from Eq. (3) that

$$y[k] = \mathbf{1}_{n-1} x_1[k] + v'[k],$$

where $v'[k] = \rho [x_2[k] \cdots x_n[k]]^T$ is a zero-mean white Gaussian noise process with $\mathbb{E}[v'[k](v'[k])^T] = \rho^2 I_{n-1}$. Hence, to compute the MSEE of state 1 of the Kalman filter, i.e., Σ'_{11} , we can consider a system with $A = \lambda_1$, $C = \mathbf{1}_{n-1}$, $W = 1$ and $V = \rho^2 I_{n-1}$. Solving Eq. (4) (using the matrix inversion lemma [40]) yields Eq. (10). Similarly, we have Σ'_{11} is strictly increasing in $\rho^2 \in \mathbb{R}_{\geq 0}$ and $\lim_{\rho \rightarrow \infty} \Sigma'_{11}(\rho^2) = \frac{1}{1 - \lambda_1^2}$. ■

APPENDIX B

We will use the following result in the proof of Theorem 1.

Lemma 6: Consider an instance of X3C: a finite set D with $|D| = 3m$, and a collection $\mathcal{C} = \{c_1, \dots, c_\tau\}$ of τ 3-element subsets of D , where $\tau \geq m$. For each element $c_i \in \mathcal{C}$, define a column vector $g_i \in \mathbb{R}^{3m}$ to encode which elements of D are contained in c_i , i.e., for $i \in \{1, 2, \dots, \tau\}$ and $j \in \{1, 2, \dots, 3m\}$, $(g_i)_j = 1$ if element j of set D is in c_i , and $(g_i)_j = 0$ otherwise. Denote $G \triangleq [g_1 \ \cdots \ g_\tau]^T$. For any $l \leq m$ ($l \in \mathbb{Z}$) and $\mathcal{L} \triangleq \{i_1, \dots, i_l\} \subseteq \{1, \dots, \tau\}$, define $G_{\mathcal{L}} \triangleq [g_{i_1} \ \cdots \ g_{i_l}]^T$ and denote $\text{rank}(G_{\mathcal{L}}) = r_{\mathcal{L}}$.² If the answer to the X3C problem is “no”, then for all \mathcal{L} with $|\mathcal{L}| \leq m$, there exists an orthogonal matrix $N \in \mathbb{R}^{3m \times 3m}$ such that

$$\begin{bmatrix} \mathbf{1}_{3m}^T \\ G_{\mathcal{L}} \end{bmatrix} N = \begin{bmatrix} \gamma & \beta \\ \mathbf{0} & \tilde{G}_{\mathcal{L}} \end{bmatrix}, \quad (21)$$

where $\tilde{G}_{\mathcal{L}} \in \mathbb{R}^{l \times r}$ is of full column rank, $\gamma \in \mathbb{R}^{1 \times (3m-r)}$ and at least $\kappa \geq 1$ ($\kappa \in \mathbb{Z}$) elements of γ are 1's, and $\beta \in \mathbb{R}^{1 \times r}$. Further elementary row operations on $\begin{bmatrix} \gamma & \beta \\ \mathbf{0} & \tilde{G}_{\mathcal{L}} \end{bmatrix}$ transform it into the form $\begin{bmatrix} \gamma & \mathbf{0} \\ \mathbf{0} & \tilde{G}_{\mathcal{L}} \end{bmatrix}$. □

Proof: Assume without loss of generality that there are no identical subsets in \mathcal{C} . Since $\text{rank}(G_{\mathcal{L}}) = r$, the

²We drop the subscript \mathcal{L} on r for notational simplicity.

dimension of the nullspace of $G_{\mathcal{L}}$ is $3m - r$. We choose an orthonormal basis of the nullspace of $G_{\mathcal{L}}$ and let it form the first $3m - r$ columns of N , denoted as N_1 . Then, we choose an orthonormal basis of the columnspace of $G_{\mathcal{L}}^T$ and let it form the rest of the r columns of N , denoted as N_2 . Clearly, $N = [N_1 \ N_2] \in \mathbb{R}^{3m \times 3m}$ is an orthogonal matrix. Furthermore, since the answer to the $X3C$ problem is “no”, for any union of $l \leq m$ ($l \in \mathbb{Z}$) subsets in \mathcal{C} , denoted as \mathcal{C}_l , there exist $\kappa \geq 1$ ($\kappa \in \mathbb{Z}$) elements in D that are not covered by \mathcal{C}_l , i.e., $G_{\mathcal{L}}$ has κ zero columns. Let these denote the j_1 th, ..., j_κ th columns of $G_{\mathcal{L}}$, where $\{j_1, \dots, j_\kappa\} \subseteq \{1, \dots, 3m\}$. Hence, we can always choose $\mathbf{e}_{j_1}, \dots, \mathbf{e}_{j_\kappa}$ to be in the orthonormal basis of the nullspace of $G_{\mathcal{L}}$, i.e., as columns of N_1 . Constructing N in this way, we have $G_{\mathcal{L}}N_1 = \mathbf{0}$ and $G_{\mathcal{L}}N_2 = \tilde{G}_{\mathcal{L}}$, where $\tilde{G}_{\mathcal{L}} \in \mathbb{R}^{l \times r}$ is of full column rank since the columns of N_2 form an orthonormal basis of the columnspace of $G_{\mathcal{L}}^T$ and $r \leq l$. Moreover, we have $\mathbf{1}_{3m}^T N_1 = \gamma$ and $\mathbf{1}_{3m}^T N_2 = \beta$, where at least κ elements of γ are 1's (since $\mathbf{1}_{3m}^T \mathbf{e}_{j_s} = 1, \forall s \in \{1, \dots, \kappa\}$). Combining these results, we obtain Eq. (21). Since $\tilde{G}_{\mathcal{L}}$ is of full column rank, we can perform elementary row operations on $\begin{bmatrix} \gamma & \beta \\ \mathbf{0} & \tilde{G}_{\mathcal{L}} \end{bmatrix}$ and obtain $\begin{bmatrix} \gamma & \mathbf{0} \\ \mathbf{0} & \tilde{G}_{\mathcal{L}} \end{bmatrix}$. ■

Proof of Theorem 1:

Assume that there exists such an approximation algorithm \mathcal{A} , i.e., $\exists K \in \mathbb{R}_{\geq 1}$ such that $r_{\mathcal{A}}(\Sigma) \leq K$ for all instances of the priori KFSS problem, where $r_{\mathcal{A}}(\Sigma)$ is defined in Eq. (11). We will show that \mathcal{A} can be used to solve the $X3C$ problem, which will lead to a contradiction.

Given an arbitrary instance of the $X3C$ problem described in Definition 6 and Lemma 5, for each element $c_i \in \mathcal{C}$, we define $g_i \in \mathbb{R}^{3m}$ to encode which elements of D are contained in c_i . Specifically, for $i \in \{1, 2, \dots, \tau\}$ and $j \in \{1, 2, \dots, 3m\}$, $(g_i)_j = 1$ if $d_j \in D$ is in c_i , and $(g_i)_j = 0$ otherwise. Denote $G \triangleq [g_1 \ \dots \ g_\tau]^T$. Thus $G^T x = \mathbf{1}_{3m}$ has a solution $x \in \{0, 1\}^\tau$ such that x has m nonzero entries if and only if the answer to the $X3C$ instance is “yes” [41].

Given the above instance of $X3C$, we then construct an instance of the priori KFSS problem as follows. Denote $Z = \lceil K \rceil(m+1)(\sigma_v^2 + 3)$, where we set $\sigma_v = 1$. Define the system dynamics matrix as $A = \text{diag}(\lambda_1, 0, \dots, 0) \in \mathbb{R}^{(3m+1) \times (3m+1)}$, where $\lambda_1 = \frac{Z-1/2}{Z}$. Note that $Z \in \mathbb{Z}_{>1}$ and $0 < \lambda_1 < 1$. The set \mathcal{Q} is defined to contain $\tau+1$ sensors with collective measurement matrix

$$C = \begin{bmatrix} 1 & \varepsilon \mathbf{1}_{3m}^T \\ \mathbf{0} & G \end{bmatrix}, \quad (22)$$

where G is defined based on the given instance of $X3C$ as above. The constant ε is chosen as $\varepsilon = 2Z \lceil \sqrt{Z-1} \rceil + 1$. The system noise covariance matrix is set to be $W = I_{3m+1}$. The measurement noise covariance matrix is set as $V = \sigma_v^2 \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \frac{1}{\varepsilon^2} I_\tau \end{bmatrix}$. The sensor selection cost vector is set as $b = \mathbf{1}_{\tau+1}$, and the sensor selection budget is set as $B = m+1$. Note that the sensor selection vector for this instance is denoted by $\mu \in \{0, 1\}^{\tau+1}$. For the above construction, since

the only nonzero eigenvalue of A is λ_1 , we know from Lemma 3(a) that $\sum_{i=2}^{3m+1} (\Sigma(\mu))_{ii} = \sum_{i=2}^{3m+1} W_{ii} = 3m$ for all μ .

We claim that algorithm \mathcal{A} will return a sensor selection vector μ such that $\text{trace}(\Sigma(\mu)) \leq K(m+1)(\sigma_v^2 + 3)$ if and only if the answer to the $X3C$ problem is “yes”.

We prove the above claim as follows. Suppose that the answer to the instance of the $X3C$ problem is “yes”. Then $G^T x = \mathbf{1}_{3m}$ has a solution such that x has m nonzero entries. Denote the solution as x^* and denote $\text{supp}(x^*) = \{i_1, \dots, i_m\}$. Define $\tilde{\mu}$ to be the sensor selection vector that indicates selecting the first and the $(i_1 + 1)$ th to the $(i_m + 1)$ th sensors, i.e., sensors that correspond to rows $C_1, C_{i_1+1}, \dots, C_{i_m+1}$ from (22). Since $G^T x^* = \mathbf{1}_{3m}$, we have $[1 \ -\varepsilon x^{*T}]C = \mathbf{e}_1$ for C defined in Eq. (22). Noting that $\text{supp}(x^*) = \{i_1, \dots, i_m\}$, it then follows that $\mathbf{e}_1 \in \text{rowspan}(C(\tilde{\mu}))$. We can then perform elementary row operations on $C(\tilde{\mu})$ (which does not change the steady state *a priori* error covariance matrix of the corresponding Kalman filter) and obtain $\Gamma C(\tilde{\mu}) \triangleq \tilde{C}(\tilde{\mu}) = \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & * \end{bmatrix}$ with the corresponding measurement noise covariance $\Gamma V(\mu) \Gamma^T \triangleq \tilde{V}(\tilde{\mu}) = \begin{bmatrix} \sigma_v^2(m+1) & * \\ * & * \end{bmatrix}$, where $\Gamma = \begin{bmatrix} 1 & -\varepsilon \mathbf{1}_m^T \\ \mathbf{0} & I_m \end{bmatrix}$. Let $\tilde{\Sigma}$ denote the error covariance obtained from sensing matrix $(\tilde{C}(\tilde{\mu}))_1 = \mathbf{e}_1$ with measurement noise variance $\tilde{\sigma}_v^2 \triangleq \sigma_v^2(m+1)$, which corresponds to the first sensor in $\tilde{C}(\tilde{\mu})$. We then know from Lemma 4(a) that

$$\tilde{\Sigma}_{11} = \frac{1 + \tilde{\sigma}_v^2 \lambda_1^2 - \tilde{\sigma}_v^2 + \sqrt{(\tilde{\sigma}_v^2 - \tilde{\sigma}_v^2 \lambda_1^2 - 1)^2 + 4\tilde{\sigma}_v^2}}{2},$$

which further implies

$$\begin{aligned} \tilde{\Sigma}_{11} &\leq \frac{1 + \sqrt{(\tilde{\sigma}_v^2(1 - \lambda_1^2))^2 - 2\tilde{\sigma}_v^2(1 - \lambda_1^2)} + 1 + 4\tilde{\sigma}_v^2}{2} \\ &\leq \frac{1 + \sqrt{(\tilde{\sigma}_v^2(1 - \lambda_1^2))^2 + 1 + 4\tilde{\sigma}_v^2}}{2} \\ &\leq \frac{1 + \sqrt{\tilde{\sigma}_v^4 + 4\tilde{\sigma}_v^2 + 4}}{2} \leq \frac{1 + \tilde{\sigma}_v^2 + 2}{2}. \end{aligned} \quad (23)$$

Using similar arguments to those above, we have that $\sum_{i=2}^{3m+1} \tilde{\Sigma}_{ii} = 3m$. We then obtain from (23) that

$$\text{trace}(\tilde{\Sigma}) \leq \tilde{\sigma}_v^2 + 3 + 3m = (m+1)(\sigma_v^2 + 3). \quad (24)$$

Since adding more sensors does not increase the MSEE of the corresponding Kalman filter, we have from (24) that $\text{trace}(\Sigma(\tilde{\mu})) \leq (m+1)(\sigma_v^2 + 3)$, which further implies $\text{trace}(\Sigma(\mu^*)) \leq (m+1)(\sigma_v^2 + 3)$, where μ^* is the optimal sensor selection of the priori KFSS problem. Since \mathcal{A} has approximation ratio K , it returns a sensor selection μ such that $\text{trace}(\Sigma(\mu)) \leq K(m+1)(\sigma_v^2 + 3)$.

Conversely, suppose that the answer to the $X3C$ instance is “no”. Then, for any union of $l \leq m$ ($l \in \mathbb{Z}_{\geq 0}$) subsets in \mathcal{C} , denoted as \mathcal{C}_l , there exist $\kappa \geq 1$ ($\kappa \in \mathbb{Z}$) elements in D that are not covered by \mathcal{C}_l , i.e., for any $l \leq m$ and $\mathcal{L} \triangleq \{i_1, \dots, i_l\} \subseteq \{1, \dots, \tau\}$, $G_{\mathcal{L}} \triangleq [g_{i_1} \ \dots \ g_{i_l}]^T$ has $\kappa \geq 1$ zero columns. We then show that $\text{trace}(\Sigma(\mu)) > K(m+1)(\sigma_v^2 + 3)$ for all sensor selections μ (that satisfy the budget constraint). We divide our arguments into two cases.

First, for any sensor selection μ_1 that does not select the first sensor, the first column of $C(\mu_1)$ is zero (from the form of C defined in Eq. (22)). We then know from Lemma 3(b) that $(\Sigma(\mu_1))_{11} = \frac{1}{1-\lambda_1^2}$. Hence, by our choice of λ_1 , we have

$$\begin{aligned} (\Sigma(\mu_1))_{11} &= \frac{Z^2}{Z-1/4} > Z \geq K(m+1)(\sigma_v^2 + 3) \\ \Rightarrow \text{trace}(\Sigma(\mu_1)) &> K(m+1)(\sigma_v^2 + 3), \end{aligned} \quad (25)$$

where (25) follows from $\sum_{i=2}^{3m+1} (\Sigma(\mu_1))_{ii} = 3m > 0$ for all possible sensor selections.

Second, consider sensor selections μ_2 that select the first sensor. To proceed, we first assume that the measurement noise covariance is $V = \mathbf{0}_{(\tau+1) \times (\tau+1)}$. Denote $\text{supp}(\mu_2) = \{1, i_1, \dots, i_l\}$, where $l \leq m$ and define $G(\mu_2) = [g_{i_1-1} \ \dots \ g_{i_l-1}]^T$. We then have

$$C(\mu_2) = \begin{bmatrix} 1 & \varepsilon \mathbf{1}_{3m}^T \\ \mathbf{0} & G(\mu_2) \end{bmatrix},$$

where $G(\mu_2)$ has $\kappa \geq 1$ zero columns. As argued in Lemma 6, there exists an orthogonal matrix $E \in \mathbb{R}^{(3m+1) \times (3m+1)}$ of the form $E = \begin{bmatrix} 1 & 0 \\ 0 & N \end{bmatrix}$ such that

$$\tilde{C}(\mu_2) \triangleq C(\mu_2)E = \begin{bmatrix} 1 & \varepsilon\gamma & \varepsilon\beta \\ \mathbf{0} & \mathbf{0} & \tilde{G}(\mu_2) \end{bmatrix}.$$

In the above expression, $\tilde{G}(\mu_2) \in \mathbb{R}^{l \times r}$ is of full column rank, where $r = \text{rank}(G(\mu_2))$. Furthermore, $\gamma \in \mathbb{R}^{1 \times (3m-r)}$ and at least κ of its elements are 1's, and $\beta \in \mathbb{R}^{1 \times r}$. We then perform a similarity transformation on the system with E , which does not affect the trace of the steady state *a priori* error covariance matrix of the corresponding Kalman filter,³ and does not change A , W and V . We further perform additional elementary row operations to transform $\tilde{C}(\mu_2)$ into the matrix

$$\tilde{C}'(\mu_2) = \begin{bmatrix} 1 & \varepsilon\gamma & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \tilde{G}(\mu_2) \end{bmatrix}.$$

Since A and W are both diagonal, and $V = \mathbf{0}$, we can obtain from Eq. (4) that the steady state *a priori* error covariance corresponding to the sensing matrix $\tilde{C}'(\mu_2)$, denoted as $\tilde{\Sigma}'(\mu_2)$, is of the form

$$\tilde{\Sigma}'(\mu_2) = \begin{bmatrix} \tilde{\Sigma}'_1(\mu_2) & \mathbf{0} \\ \mathbf{0} & \tilde{\Sigma}'_2(\mu_2) \end{bmatrix},$$

where $\tilde{\Sigma}'_1(\mu_2) \in \mathbb{R}^{(3m+1-r) \times (3m+1-r)}$ satisfies

$$\begin{aligned} \tilde{\Sigma}'_1(\mu_2) &= A_1 \tilde{\Sigma}'_1(\mu_2) A_1^T + W_1 - \\ &\quad A_1 \tilde{\Sigma}'_1(\mu_2) \tilde{C}^T (\tilde{C} \tilde{\Sigma}'_1(\mu_2) \tilde{C}^T)^{-1} \tilde{C} \tilde{\Sigma}'_1(\mu_2) A_1^T, \end{aligned}$$

where $A_1 = \text{diag}(\lambda_1, 0, \dots, 0) \in \mathbb{R}^{(3m+1-r) \times (3m+1-r)}$, $\tilde{C} = [1 \ \varepsilon\gamma]$ and $W_1 = I_{3m+1-r}$. Denoting $\alpha^2 = \varepsilon^2 \|\gamma\|_2^2 \geq \kappa \varepsilon^2 \geq \varepsilon^2$, we then obtain from Lemma 4(a) that

$$\begin{aligned} (\tilde{\Sigma}'(\mu_2))_{11} &= \frac{1 + \alpha^2 \lambda_1^2 - \alpha^2 + \sqrt{(\alpha^2 - \alpha^2 \lambda_1^2 - 1)^2 + 4\alpha^2}}{2} \\ &\geq \frac{1 + \varepsilon^2 \lambda_1^2 - \varepsilon^2 + \sqrt{(\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 + 4\varepsilon^2}}{2}. \end{aligned} \quad (26)$$

³This can be easily verified using Eq. (4) as E is an orthogonal matrix.

By our choices of λ_1 and ε , we have the following:

$$\begin{aligned} \varepsilon^2 &> 4Z^2(Z-1) \Rightarrow (1 - \frac{Z-1/4}{Z})\varepsilon^2 > Z^2 - Z \\ \Rightarrow \varepsilon^2 &> Z^2 + Z\varepsilon^2 \frac{Z-1/4}{Z^2} - Z \\ \Rightarrow \varepsilon^2 &> Z^2 + Z(\varepsilon^2(1-\lambda_1^2) - 1) \\ \Rightarrow (\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 &+ 4\varepsilon^2 > \\ &(\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 + 4Z^2 + 4Z(\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1) \\ \Rightarrow (\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 &+ 4\varepsilon^2 > (2Z + \varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 \\ \Rightarrow \sqrt{(\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 + 4\varepsilon^2} &> 2Z + \varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1 \\ \Rightarrow \frac{1 + \varepsilon^2 \lambda_1^2 - \varepsilon^2 + \sqrt{(\varepsilon^2 - \varepsilon^2 \lambda_1^2 - 1)^2 + 4\varepsilon^2}}{2} &> Z. \end{aligned} \quad (27)$$

Since $Z \geq K(m+1)(\sigma_v^2 + 3)$, (26) and (27) imply $(\tilde{\Sigma}'(\mu_2))_{11} > K(m+1)(\sigma_v^2 + 3)$, which further implies $\text{trace}(\tilde{\Sigma}'(\mu_2)) > K(m+1)(\sigma_v^2 + 3)$. Since $\text{trace}(\tilde{\Sigma}'(\mu_2)) = \text{trace}(\Sigma(\mu_2))$ as argued above, we obtain that $\text{trace}(\Sigma(\mu_2)) > K(m+1)(\sigma_v^2 + 3)$. We then note the fact that the MSEE of the Kalman filter with noiseless measurements is no greater than that with any noisy measurements (for fixed A , W and C), when the system noise and the measurement noise are uncorrelated. Therefore, for $V = \sigma_v^2 \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \frac{1}{\varepsilon^2} I_\tau \end{bmatrix}$, we also have that $\text{trace}(\Sigma(\mu_2)) > K(m+1)(\sigma_v^2 + 3)$ for all μ_2 .

It then follows from the above arguments that $\text{trace}(\Sigma(\mu)) > K(m+1)(\sigma_v^2 + 3)$ for all sensor selections μ , which implies that algorithm \mathcal{A} would also return a sensor selection μ such that $\text{trace}(\Sigma(\mu)) > K(m+1)(\sigma_v^2 + 3)$. This completes the proof of the converse direction of the claim above.

Hence, it is clear that algorithm \mathcal{A} can be used to solve the $X3C$ problem by applying it to the above instance of the priori KFSS problem. Since $X3C$ is NP-complete, there is no polynomial-time algorithm for it if $P \neq NP$, and we get a contradiction. This completes the proof of the theorem. ■

Proof of Corollary 1:

We have shown in Theorem 1 that for any polynomial-time algorithm \mathcal{A} for the priori KFSS problem and any $K \in \mathbb{R}_{\geq 1}$, there exist instances of the priori KFSS problem such that $r_{\mathcal{A}}(\Sigma) > K$ (unless $P = NP$). Suppose that there exists a polynomial-time constant-factor approximation algorithm \mathcal{A}' for the posteriori KFSS problem, i.e., $\exists K' \in \mathbb{R}_{\geq 1}$ such that $r_{\mathcal{A}'}(\Sigma^*) \leq K'$ for all instances of the posteriori KFSS problem, where $r_{\mathcal{A}'}(\Sigma^*)$ is defined in Eq. (12). We consider an instance of the priori KFSS problem constructed in the proof of Theorem 1. We then set the instance of the posteriori KFSS problem to be the same as the constructed instance of the priori KFSS problem. Since $A = \text{diag}(\lambda_1, 0, \dots, 0) \in \mathbb{R}^{(3m+1) \times (3m+1)}$ and $W = I_{3m+1}$, where $0 < \lambda_1 < 1$, we have from Eq. (5) that

$$(\Sigma(\mu))_{11} = \lambda_1^2 (\Sigma^*(\mu))_{11} + 1, \forall \mu. \quad (28)$$

Since we know from Lemma 3(a) that $(\Sigma(\mu))_{ii} = 1, \forall i \in \{2, \dots, 3m+1\}$ and $\forall \mu$, it then follows from Eq. (28) that

$$\text{trace}(\Sigma(\mu)) = \lambda_1^2 (\Sigma^*(\mu))_{11} + 3m + 1, \forall \mu. \quad (29)$$

We also know from Lemma 3(a) that $0 \leq (\Sigma^*(\mu))_{ii} \leq 1$, $\forall i \in \{2, \dots, 3m+1\}$ and $\forall \mu$, which implies that

$$\text{trace}(\Sigma^*(\mu)) \leq (\Sigma^*(\mu))_{11} + 3m, \forall \mu. \quad (30)$$

We then obtain from Eqs. (29)-(30) that

$$\begin{aligned} \text{trace}(\Sigma^*(\mu)) &\leq \frac{3m\lambda_1^2 + \text{trace}(\Sigma(\mu)) - 3m - 1}{\lambda_1^2} \\ &\leq \frac{\text{trace}(\Sigma(\mu))}{\lambda_1^2}, \forall \mu, \end{aligned} \quad (31)$$

where the second inequality follows from the fact that $0 < \lambda_1 < 1$. Denote the optimal sensor selections of the priori and the posteriori KFSS problems as μ_1^* and μ_2^* , respectively. Denote the sensor selection returned by algorithm \mathcal{A}' as μ' . Note that $\Sigma_{opt} = \Sigma(\mu_1^*)$ and $\Sigma_{opt}^* = \Sigma^*(\mu_2^*)$ and $\Sigma_{\mathcal{A}'}^* = \Sigma^*(\mu')$. We then have the following:

$$\begin{aligned} \text{trace}(\Sigma_{\mathcal{A}'}^*) &\leq K' \text{trace}(\Sigma_{opt}^*) \\ \Rightarrow (\Sigma^*(\mu'))_{11} + \sum_{i=2}^{3m+1} (\Sigma^*(\mu'))_{ii} &\leq K' \text{trace}(\Sigma^*(\mu_2^*)) \\ \Rightarrow \frac{(\Sigma(\mu'))_{11} - 1}{\lambda_1^2} &\leq K' \text{trace}(\Sigma^*(\mu_2^*)) \leq K' \text{trace}(\Sigma^*(\mu_1^*)) \end{aligned} \quad (32)$$

$$\Rightarrow (\Sigma(\mu'))_{11} - 1 \leq K' \text{trace}(\Sigma(\mu_1^*)) \quad (33)$$

$$\Rightarrow \text{trace}(\Sigma(\mu')) \leq K' \text{trace}(\Sigma(\mu_1^*)) + 3m + 1 \quad (34)$$

$$\Rightarrow \frac{\text{trace}(\Sigma(\mu'))}{\text{trace}(\Sigma(\mu_1^*))} \leq K' + \frac{3m+1}{\text{trace}(\Sigma(\mu_1^*))} \leq K' + 1, \quad (35)$$

where the first inequality in (32) follows from Eq. (28) and $(\Sigma^*(\mu'))_{ii} \geq 0, \forall i$ (from Lemma 3(a)), the second inequality in (32) follows from the fact that μ_2^* is the optimal sensor selection for the posteriori KFSS problem, (33) follows from (31), (34) follows from the fact that $\sum_{i=2}^{3m+1} (\Sigma(\mu'))_{ii} = 3m$ (from Lemma 3(a)), and the second inequality in (35) uses the fact that $\text{trace}(\Sigma(\mu_1^*)) \geq 3m+1$ (from Lemma 3(a)). Thus, we have from (35) that $r_{\mathcal{A}'}(\Sigma) \leq K' + 1$, which contradicts the fact that the priori KFSS problem cannot have a polynomial-time constant-factor approximation algorithm for instances of the given form, and completes the proof of the corollary. ■

APPENDIX C

Proof of Theorem 2:

Assume that there exists such a polynomial-time constant-factor approximation algorithm \mathcal{A} , i.e., $\exists K \in \mathbb{R}_{\geq 1}$ such that $r_{\mathcal{A}}(\tilde{\Sigma}) \leq K$ for all instances of the priori KFSA problem, where $r_{\mathcal{A}}(\tilde{\Sigma})$ is defined in Eq. (13). We will show that \mathcal{A} can be used to solve the $X3C$ problem, leading to a contradiction.

Consider any instance of the $X3C$ problem to be a finite set $D = \{d_1, \dots, d_{3m}\}$ and a collection $\mathcal{C} = \{c_1, \dots, c_\tau\}$ of 3-element subsets of D , where $\tau \geq m$. Recall in the proof of Theorem 1 that we use a column vector $g_i \in \mathbb{R}^{3m}$ to encode which elements of D are contained in c_i , where $(g_i)_j = 1$ if $d_j \in D$ is in c_i , and $(g_i)_j = 0$ otherwise, for $i \in \{1, 2, \dots, \tau\}$ and $j \in \{1, 2, \dots, 3m\}$. The matrix $G \in \mathbb{R}^{\tau \times 3m}$ was defined in the proof of Theorem 1 as $G = [g_1 \ \dots \ g_\tau]^T$. In this

proof, we will make use of the matrix $F \triangleq G^T$; note that each column of F contains exactly three 1's.

Given the above instance of the $X3C$ problem, we then construct an instance of the priori KFSA as follows. Denote $Z = \lceil K \rceil (\tau + 2)(\delta_v^2 + 1)$, where we set $\delta_v = 1$. Define the system dynamics matrix as $A = \text{diag}(\lambda_1, 0, \dots, 0) \in \mathbb{R}^{(\tau+1) \times (\tau+1)}$, where $\lambda_1 = \frac{Z-1/2}{Z}$. Note that $Z \in \mathbb{Z}_{>1}$ and $0 < \lambda_1 < 1$. The set \mathcal{Q} consists of $3m + \tau$ sensors with collective measurement matrix

$$C = \begin{bmatrix} \mathbf{1}_{3m} & \rho F \\ \mathbf{0} & I_\tau \end{bmatrix}, \quad (36)$$

where F is defined above and I_τ is used to encode the collection \mathcal{C} , i.e., e_j represents $c_j \in \mathcal{C}$ for all $j \in \{1, 2, \dots, \tau\}$. The constant ρ is chosen as $\rho = 2Z \lceil \sqrt{m(Z-1)} \rceil + 1$. The system noise covariance matrix is set to be $W = I_{\tau+1}$. The measurement noise covariance is set as $V = \delta_v^2 \begin{bmatrix} I_{3m} & \mathbf{0} \\ \mathbf{0} & \frac{1}{\rho^2} I_\tau \end{bmatrix}$. The sensor attack cost vector is set as $\omega = \mathbf{1}_{3m+\tau}$, and the sensor attack budget is set as $\Omega = m$. Note that the sensor attack vector is given by $\nu \in \{0, 1\}^{3m+\tau}$. For the above construction, since the only nonzero eigenvalue of A is λ_1 , we know from Lemma 3(a) that $\sum_{i=2}^{\tau+1} (\Sigma(\nu^c))_{ii} = \sum_{i=2}^{\tau+1} W_{ii} = \tau$ for all ν .

We claim that algorithm \mathcal{A} will return a sensor attack vector ν such that $\text{trace}(\Sigma(\nu^c)) > (\tau + 2)(\delta_v^2 + 1)$ if and only if the answer to the $X3C$ problem is “yes”.

We prove the above claim as follows. Suppose that the answer to the $X3C$ problem is “yes”. Similarly to the proof of Theorem 1, we first assume that $V = \mathbf{0}_{(3m+\tau) \times (3m+\tau)}$. Denote an exact cover as $\mathcal{C}' = \{c_{j_1}, \dots, c_{j_m}\}$, where $\{j_1, \dots, j_m\} \subseteq \{1, 2, \dots, \tau\}$. Define $\tilde{\nu}$ to be the sensor attack such that $\text{supp}(\tilde{\nu}) = \{3m + j_1, \dots, 3m + j_m\}$. We then renumber the states of the system from state 2 to state τ such that for all $i \in \{1, 2, \dots, m\}$, the columns of the submatrix I_τ of C in Eq. (36) representing c_{j_i} in \mathcal{C}' , i.e., the columns of I_τ that correspond to $\text{supp}(\tilde{\nu})$, come first. Note that renumbering the states does not change the trace of the steady state *a priori* error covariance of the corresponding Kalman filter. We then have from Eq. (36) that

$$C(\tilde{\nu}^c) = \begin{bmatrix} \mathbf{1}_{3m} & \rho F_1 & \rho F_2 \\ \mathbf{0} & \mathbf{0} & I_{\tau-m} \end{bmatrix}, \quad (37)$$

where $F_1 \in \mathbb{R}^{3m \times m}$ and $F_2 \in \mathbb{R}^{3m \times (\tau-m)}$ satisfy $F = [F_1 \ F_2]$, and $I_{\tau-m}$ is the submatrix of I_τ that corresponds to $\text{supp}(\tilde{\nu}^c) \cap \{3m+1, \dots, 3m+\tau\}$, i.e., the elements of \mathcal{C} that are not in \mathcal{C}' .⁴ Since the sensor attack $\tilde{\nu}$ targets the rows of C that correspond to the elements of the exact cover \mathcal{C}' for D , we have that F_1 , after some row permutations of $C(\tilde{\nu}^c)$, is given by $F_1 = [e_1^T \ e_1^T \ e_1^T \ \dots \ e_m^T \ e_m^T \ e_m^T]^T$. We perform additional elementary row operations and merge identical rows (which does not change the steady state *a priori* error covariance matrix of the corresponding Kalman filter) to transform $C(\tilde{\nu}^c)$ into the matrix

$$\tilde{C}(\tilde{\nu}^c) = \begin{bmatrix} \mathbf{1}_m & \rho I_m & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{\tau-m} \end{bmatrix}. \quad (38)$$

⁴Note that if the submatrix of I_τ corresponding to $\text{supp}(\tilde{\nu}^c) \cap \{3m+1, \dots, 3m+\tau\}$ is not identity, we can always permute the rows of $C(\tilde{\nu}^c)$ to make it identity.

Since A and W are both diagonal, and $V = \mathbf{0}$, we can obtain from Eq. (4) that the steady state *a priori* error covariance corresponding to $\tilde{C}(\tilde{\nu}^c)$, denoted as $\tilde{\Sigma}(\tilde{\nu}^c)$, is of the form

$$\tilde{\Sigma}(\tilde{\nu}^c) = \begin{bmatrix} \tilde{\Sigma}_1(\tilde{\nu}^c) & \mathbf{0} \\ \mathbf{0} & \tilde{\Sigma}_2(\tilde{\nu}^c) \end{bmatrix},$$

where $\tilde{\Sigma}_1(\tilde{\nu}^c) \in \mathbb{R}^{(m+1) \times (m+1)}$ satisfies

$$\begin{aligned} \tilde{\Sigma}_1(\tilde{\nu}^c) &= A_1 \tilde{\Sigma}_1(\tilde{\nu}^c) A_1^T + W_1 - \\ &A_1 \tilde{\Sigma}_1(\tilde{\nu}^c) \tilde{C}^T (\tilde{C} \tilde{\Sigma}_1(\tilde{\nu}^c) \tilde{C}^T)^{-1} \tilde{C} \tilde{\Sigma}_1(\tilde{\nu}^c) A_1^T, \end{aligned}$$

where $A_1 = \text{diag}(\lambda_1, 0, \dots, 0) \in \mathbb{R}^{(m+1) \times (m+1)}$, $\tilde{C} = \begin{bmatrix} \mathbf{1}_m & \rho I_m \end{bmatrix}$ and $W_1 = I_{m+1}$. We then know from Lemma 4(b) that $(\Sigma(\tilde{\nu}^c))_{11} = (\tilde{\Sigma}(\tilde{\nu}^c))_{11}$ satisfies

$$(\Sigma(\tilde{\nu}^c))_{11} = \frac{\lambda_1^2 \rho^2 + m - \rho^2 + \sqrt{(\rho^2 - \lambda_1^2 \rho^2 - m)^2 + 4m\rho^2}}{2m}. \quad (39)$$

By our choices of λ_1 and ρ , we have

$$\begin{aligned} \rho^2 &> 4Z^2 m(Z-1) \Rightarrow (1 - \frac{Z-1/4}{Z})\rho^2 > Z^2 m - Zm \\ \Rightarrow \rho^2 &> mZ^2 + Z\rho^2 \frac{Z-1/4}{Z^2} - Zm \\ \Rightarrow 4m\rho^2 &> 4m^2 Z^2 + 4mZ(\rho^2(1 - \lambda_1^2) - m) \\ \Rightarrow (\rho^2 - \lambda_1^2 \rho^2 - m)^2 &+ 4m\rho^2 \\ &> 4m^2 Z^2 + 4mZ(\rho^2 - \lambda_1^2 \rho^2 - m) + (\rho^2 - \lambda_1^2 \rho^2 - m)^2 \\ \Rightarrow (\rho^2 - \lambda_1^2 \rho^2 - m)^2 &+ 4m\rho^2 > (2mZ + \rho^2 - \lambda_1^2 \rho^2 - m)^2 \\ \Rightarrow \sqrt{(\rho^2 - \lambda_1^2 \rho^2 - m)^2 + 4m\rho^2} &> 2mZ + \rho^2 - \lambda_1^2 \rho^2 - m \\ \Rightarrow \frac{\lambda_1^2 \rho^2 + m - \rho^2 + \sqrt{(\rho^2 - \lambda_1^2 \rho^2 - m)^2 + 4m\rho^2}}{2m} &> Z. \end{aligned} \quad (40)$$

Noting that $Z \geq K(\tau+2)(\delta_v^2+1)$, we then know from (39) and (40) that $(\Sigma(\tilde{\nu}^c))_{11} > K(\tau+2)(\delta_v^2+1)$, which further implies that $\text{trace}(\Sigma(\tilde{\nu}^c)) > K(\tau+2)(\delta_v^2+1)$. Following the same arguments as those in the proof of Theorem 1, we have that for $V = \delta_v^2 \begin{bmatrix} I_{3m} & \mathbf{0} \\ \mathbf{0} & \frac{1}{\rho^2} I_\tau \end{bmatrix}$, $\text{trace}(\Sigma(\tilde{\nu}^c)) > K(\tau+2)(\delta_v^2+1)$ also holds, which implies $\text{trace}(\Sigma(\nu^*{}^c)) > K(\tau+2)(\delta_v^2+1)$, where ν^* is the optimal sensor attack for the priori KFSA problem. Since algorithm \mathcal{A} has approximation ratio K , it would return a sensor attack ν such that $\text{trace}(\Sigma(\nu^c)) > (\tau+2)(\delta_v^2+1)$.

Conversely, suppose the answer to the $X3C$ problem is “no”. For any union of $l \leq m$ ($l \in \mathbb{Z}_{\geq 0}$) subsets in \mathcal{C} , denoted as \mathcal{C}_l , there exists at least one element in D that is not covered by \mathcal{C}_l . We then show that $\text{trace}(\Sigma(\nu^c)) \leq (\tau+2)(\delta_v^2+1)$ for all sensor attacks ν (that satisfy the budget constraint). We split our discussion into three cases.

First, consider any sensor attack ν_1 that targets l sensors merely from C_1 to C_{3m} in Eq. (36), i.e., $|\text{supp}(\nu_1)| = l$ and $\text{supp}(\nu_1) \subseteq \{1, \dots, 3m\}$, where $l \leq m$. We then obtain

$$C(\nu_1^c) = \begin{bmatrix} \mathbf{1}_{3m-l} & \rho F(\nu_1^c) \\ \mathbf{0} & I_\tau \end{bmatrix},$$

where $F(\nu_1^c) \in \mathbb{R}^{(3m-l) \times \tau}$ is defined to be the submatrix of F that corresponds to $\text{supp}(\nu_1^c) \cap \{1, \dots, 3m\}$, i.e., the rows

of F that are left over by ν_1 . We perform elementary row operations to transform $C(\nu_1^c)$ into

$$\tilde{C}(\nu_1^c) \triangleq \Psi C(\nu_1^c) = \begin{bmatrix} \mathbf{1}_{3m-l} & \mathbf{0} \\ \mathbf{0} & I_\tau \end{bmatrix} \quad (41)$$

with the corresponding measurement noise covariance

$$\begin{aligned} \tilde{V}(\nu_1^c) &\triangleq \Psi V(\nu_1^c) \Psi^T \\ &= \delta_v^2 \begin{bmatrix} I_{3m-l} + F(\nu_1^c)(F(\nu_1^c))^T & -\frac{1}{\rho} F(\nu_1^c) \\ -\frac{1}{\rho} (F(\nu_1^c))^T & \frac{1}{\rho^2} I_\tau \end{bmatrix}, \end{aligned} \quad (42)$$

where $\Psi = \begin{bmatrix} I_{3m-l} & -\rho F(\nu_1^c) \\ \mathbf{0} & I_\tau \end{bmatrix}$. Since there are at most τ nonzero elements (which are all 1's) in the first row of $F(\nu_1^c)$, it follows that $(F(\nu_1^c)(F(\nu_1^c))^T)_{11}$ (i.e., the element in the first row and first column of the matrix $F(\nu_1^c)(F(\nu_1^c))^T$) is at most τ . We then have from Eq. (42) that $(\tilde{V}(\nu_1^c))_{11}$, denoted as $\tilde{\delta}_v^2(\nu_1^c)$, satisfies

$$\tilde{\delta}_v^2(\nu_1^c) \leq (\tau+1)\delta_v^2. \quad (43)$$

Second, consider any sensor attack ν_2 that targets l sensors merely from C_{3m+1} to $C_{3m+\tau}$ in Eq. (36), i.e., $|\text{supp}(\nu_2)| = l$ and $\text{supp}(\nu_2) \subseteq \{3m+1, \dots, 3m+\tau\}$, where $l \leq m$. Via similar arguments to those for obtaining Eqs. (37), (41) and (42), we can perform elementary row operations to transform

$$C(\nu_2^c) = \begin{bmatrix} \mathbf{1}_{3m} & \rho F'_1 & \rho F'_2 \\ \mathbf{0} & \mathbf{0} & I_{\tau-l} \end{bmatrix}$$

into

$$\tilde{C}(\nu_2^c) = \begin{bmatrix} \mathbf{1}_{3m} & \rho F'_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{\tau-l} \end{bmatrix}$$

with the corresponding measurement noise covariance $\tilde{V}(\nu_2^c) = \begin{bmatrix} \tilde{\delta}_v^2(\nu_2^c) & * \\ * & * \end{bmatrix}$, where

$$\tilde{\delta}_v^2(\nu_2^c) \leq (\tau-l+1)\delta_v^2. \quad (44)$$

Note that $F'_1 \in \mathbb{R}^{3m \times l}$ and $F'_2 \in \mathbb{R}^{3m \times (\tau-l)}$ satisfy $F = \begin{bmatrix} F'_1 & F'_2 \end{bmatrix}$. Recall that for any union of $l \leq m$ subsets in \mathcal{C} , denoted as \mathcal{C}_l , there exists at least one element in D that is not covered by \mathcal{C}_l . We can then assume without loss of generality that one such element is d_1 , which implies that the first row of F'_1 is zero.

Third, consider any sensor attack ν_3 that targets sensors from both C_1 to C_{3m} and C_{3m+1} to $C_{3m+\tau}$ in Eq. (36). Suppose that the attack ν_3 attacks l_1 sensors from C_1 to C_{3m} and l_2 sensors from C_{3m+1} to $C_{3m+\tau}$, i.e., $\text{supp}(\nu_3) = \{j'_1, \dots, j'_{l_1}, 3m+j''_1, \dots, 3m+j''_{l_2}\} \subseteq \{1, 2, \dots, 3m+\tau\}$, where $l_1, l_2 \in \mathbb{Z}_{\geq 1}$, $l_1 + l_2 = l \leq m$, $\{j'_1, \dots, j'_{l_1}\} \subseteq \{1, \dots, 3m\}$ and $\{j''_1, \dots, j''_{l_2}\} \subseteq \{1, \dots, \tau\}$. By similar arguments to those above, we can perform elementary row operations to transform

$$C(\nu_3^c) = \begin{bmatrix} \mathbf{1}_{3m-l_1} & \rho F_1(\nu_3^c) & \rho F_2(\nu_3^c) \\ \mathbf{0} & \mathbf{0} & I_{\tau-l_2} \end{bmatrix}$$

into

$$\tilde{C}(\nu_3^c) = \begin{bmatrix} \mathbf{1}_{3m-l_1} & \rho F_1(\nu_3^c) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{\tau-l_2} \end{bmatrix},$$

where $F_1(\nu_3^c) \in \mathbb{R}^{(3m-l_1) \times l_2}$ and $F_2(\nu_3^c) \in \mathbb{R}^{(3m-l_1) \times (\tau-l_2)}$ satisfy $F(\nu_3^c) = \begin{bmatrix} F_1(\nu_3^c) & F_2(\nu_3^c) \end{bmatrix}$ with $F(\nu_3^c)$ defined in

the same way as $F(\nu_1^c)$. Moreover, the measurement noise covariance corresponding to $\tilde{C}(\nu_3^c)$ is given by $\tilde{V}(\nu_3^c) = \begin{bmatrix} \tilde{\delta}_v^2(\nu_3^c) & * \\ * & * \end{bmatrix}$, where

$$\tilde{\delta}_v^2(\nu_3^c) \leq (\tau - l_2 + 1)\delta_v^2. \quad (45)$$

Since any l_2 subsets in \mathcal{C} can cover at most $3l_2$ elements in D , there are at least $3m - 3l_2$ elements in D that are not covered by the l_2 subsets in \mathcal{C} . Also note that

$$3m - 3l_2 - l_1 = 3m - 2l_2 - l = 2(m - l_2) + m - l > 0,$$

where the last inequality follows from the facts that $l_1 + l_2 = l \leq m$ and $l_1, l_2 \in \mathbb{Z}_{\geq 1}$. Hence, by attacking l_1 sensors from C_1 to C_{3m} and l_2 sensors from C_{3m+1} to $C_{3m+\tau}$, we have at least $3m - 3l_2 - l_1 > 0$ row(s) of $F_1(\nu_3^c)$ that are zero. Again, we can assume without loss of generality that the first row of $F_1(\nu_3^c)$ is zero.

In summary, for any sensor attack ν , we let $\hat{\Sigma}(\nu_i^c)$ denote the steady state *a priori* error covariance obtained from measurement matrix $(\tilde{C}(\nu_i^c))_1 = \mathbf{e}_1$ with measurement noise variance $\tilde{\delta}_v^2(\nu_i^c)$ (which corresponds to the first sensor in $\tilde{C}(\nu_i^c)$), $\forall i \in \{1, 2, 3\}$, where ν_1 , ν_2 and ν_3 are given as above. Following similar arguments to those for (23), we have $(\hat{\Sigma}(\nu_i^c))_{11} \leq \tilde{\delta}_v^2(\nu_i^c) + 2$, $\forall i \in \{1, 2, 3\}$. Since $\sum_{i=2}^{\tau+1} (\hat{\Sigma}(\nu_i^c))_{ii} = \sum_{i=2}^{\tau+1} W_{ii} = \tau$ holds for all $i \in \{1, 2, 3\}$ via similar arguments to those above, we obtain that

$$\text{trace}(\hat{\Sigma}(\nu_i^c)) \leq \tilde{\delta}_v^2(\nu_i^c) + 2 + \tau, \forall i \in \{1, 2, 3\}. \quad (46)$$

Again note that adding more sensors does not increase the MSEE of the corresponding Kalman filter, and the above operations performed on the sensing matrix C do not change the trace of the steady state *a priori* error covariance of the corresponding Kalman filter as well. We then have from Eqs. (43)-(46) that $\text{trace}(\Sigma(\nu^c)) \leq (\tau+1)\delta_v^2 + 2 + \tau \leq (\tau+2)(\delta_v^2 + 1)$ for all ν . It follows that algorithm \mathcal{A} would also return a sensor attack ν such that $\text{trace}(\Sigma(\nu^c)) \leq (\tau+2)(\delta_v^2 + 1)$. This proves the converse direction of the claim above.

Therefore, we know that \mathcal{A} can be used to solve the $X3C$ problem by applying it to the above instance of the priori KFSA problem. Since $X3C$ is NP-complete, there is no polynomial-time algorithm for it if $P \neq NP$, yielding a contradiction. This completes the proof of the theorem. ■

Proof of Corollary 2:

Note that the A and W matrices for the instance of KFSA that we constructed in the proof of Theorem 2 are the same as those for the instance of KFSS that we constructed in the proof of Theorem 1. We then follow the same arguments as those in the proof of Corollary 1. Suppose that there exists a polynomial-time constant-factor approximation algorithm \mathcal{A}' for the posteriori KFSA problem, i.e., $\exists K' \in \mathbb{R}_{\geq 1}$ such that $r_{\mathcal{A}'}(\tilde{\Sigma}^*) \leq K'$ for all instances of the posteriori KFSA problem, where $r_{\mathcal{A}'}(\tilde{\Sigma}^*)$ is defined in Eq. (14). We consider an instance of the priori KFSA problem as constructed in the proof of Theorem 2. We then set the instance of the posteriori KFSA problem to be the same as the constructed instance of the priori KFSA problem. Denote the optimal sensor attacks

of the priori and the posteriori KFSA problems as ν_1^* and ν_2^* , respectively. Denote the sensor attack returned by algorithm \mathcal{A}' as ν' . Note that $\tilde{\Sigma}_{opt} = \Sigma(\nu_1^{*c})$, $\tilde{\Sigma}_{opt}^* = \Sigma^*(\nu_2^{*c})$ and $\tilde{\Sigma}_{\mathcal{A}'}^* = \Sigma^*(\nu'^c)$. Also note that $\text{trace}(\Sigma^*(\nu_1^{*c})) \leq \text{trace}(\Sigma^*(\nu_2^{*c}))$, since ν_2^* is the optimal sensor attack for the posteriori KFSA problem. We then have the following:

$$\begin{aligned} \text{trace}(\Sigma^*(\nu_1^{*c})) &\leq \text{trace}(\Sigma^*(\nu_2^{*c})) \leq K' \text{trace}(\tilde{\Sigma}_{\mathcal{A}'}^*) \\ &\Rightarrow (\Sigma^*(\nu_1^{*c}))_{11} + \sum_{i=2}^{3m+1} (\Sigma^*(\nu_1^{*c}))_{ii} \leq K' \text{trace}(\Sigma^*(\nu'^c)) \\ &\Rightarrow \frac{(\Sigma(\nu_1^{*c}))_{11} - 1}{\lambda_1^2} \leq K' \text{trace}(\Sigma^*(\nu'^c)) \\ &\Rightarrow (\Sigma(\nu_1^{*c}))_{11} - 1 \leq K' \text{trace}(\Sigma(\nu'^c)) \\ &\Rightarrow \text{trace}(\Sigma(\nu_1^{*c})) \leq K' \text{trace}(\Sigma(\nu'^c)) + 3m + 1 \\ &\Rightarrow \frac{\text{trace}(\Sigma(\nu_1^{*c}))}{\text{trace}(\Sigma(\nu'^c))} \leq K' + \frac{3m + 1}{\text{trace}(\Sigma(\nu'^c))} \leq K' + 1, \end{aligned}$$

which implies $r_{\mathcal{A}'}(\tilde{\Sigma}) \leq K' + 1$, and yields a contradiction with the fact that the priori KFSA problem cannot have a polynomial-time constant-factor approximation algorithm for the instances of the form given as above. This completes the proof of the corollary. ■

APPENDIX D

Proof of Theorem 3:

We first prove that Algorithm 1 for the priori KFSS problem selects sensor 2 and sensor 3 in its first and second iterations, respectively. Since the only nonzero eigenvalue of A is λ_1 , we know from Lemma 3(a) that $(\Sigma(\mu))_{22} = 1$ and $(\Sigma(\mu))_{33} = 1$, $\forall \mu$, which implies that $(\Sigma_{gre})_{22} = 1$ and $(\Sigma_{gre})_{33} = 1$. Hence, we focus on determining $(\Sigma_{gre})_{11}$.

Denoting $\mu_1 = [1 \ 0 \ 0]^T$ and $\mu_2 = [0 \ 1 \ 0]^T$, we have $C(\mu_1) = [1 \ h \ h]$ and $C(\mu_2) = [1 \ 0 \ h]$. Using the result in Lemma 4(a), we obtain that $\sigma_1 \triangleq (\Sigma(\mu_1))_{11}$ and $\sigma_2 \triangleq (\Sigma(\mu_2))_{11}$ satisfy

$$\sigma_1 = \frac{2}{\sqrt{(1 - \lambda_1^2 - \frac{1}{2h^2})^2 + \frac{2}{h^2} + 1 - \lambda_1^2 - \frac{1}{2h^2}}},$$

and

$$\sigma_2 = \frac{2}{\sqrt{(1 - \lambda_1^2 - \frac{1}{h^2})^2 + \frac{4}{h^2} + 1 - \lambda_1^2 - \frac{1}{h^2}}},$$

respectively. Similarly, denoting $\mu_3 = [0 \ 0 \ 1]^T$, we obtain $C(\mu_3) = [0 \ 1 \ 1]$. Since the first column of $C(\mu_3)$ is zero, we know from Lemma 3(b) that $\sigma_3 \triangleq (\Sigma(\mu_3))_{11} = \frac{1}{1 - \lambda_1^2}$. If we view σ_2 as a function of h^2 , denoted as $\sigma(h^2)$, we have $\sigma_1 = \sigma(2h^2)$. Since we know from Lemma 4(a) that $\sigma(h^2)$ is a strictly increasing function of $h^2 \in \mathbb{R}_{>0}$ and upper bounded by $\frac{1}{1 - \lambda_1^2}$, we obtain $\sigma_2 < \sigma_1 < \sigma_3$, which implies that the greedy algorithm selects sensor 2 in its first iteration.

Denote $\mu_{12} = [1 \ 1 \ 0]^T$. We have $C(\mu_{12}) = \begin{bmatrix} 1 & h & h \\ 1 & 0 & h \end{bmatrix}$, on which we perform elementary row operations and obtain $\tilde{C}(\mu_{12}) = \begin{bmatrix} 0 & h & 0 \\ 1 & 0 & h \end{bmatrix}$. By direct computation from Eq. (4), we obtain $(\Sigma(\mu_{12}))_{11} = \sigma_2$. Moreover, we denote $\mu_{23} = [0 \ 1 \ 1]^T$

and obtain $C(\mu_{23}) = \begin{bmatrix} 1 & 0 & h \\ 0 & 1 & 1 \end{bmatrix}$. By direct computation from Eq. (4), we have $(\Sigma(\mu_{23}))_{11}$, denoted as σ_{23} , to be

$$\sigma_{23} = \frac{2}{\sqrt{(1 - \lambda_1^2 - \frac{2}{h^2})^2 + \frac{8}{h^2} + 1 - \lambda_1^2 - \frac{2}{h^2}}}.$$

Similarly to the argument above, we have $\sigma_{12} = \sigma(h^2)$ and $\sigma_{23} = \sigma(\frac{h^2}{2})$, where $\sigma(\frac{h^2}{2}) < \sigma(h^2)$, which implies that the greedy algorithm selects sensor 3 in its second iteration. Hence, we have $\text{trace}(\Sigma_{gre}) = \sigma_{23} + 2$.

Furthermore, it is easy to see that the optimal sensor selection (for the priori KFSS instance) is $\mu = [1 \ 0 \ 1]^T$, denoted as μ_{13} . Since if $\mu = \mu_{13}$, then $\mathbf{e}_1 \in \text{rowspan}(C(\mu))$ and thus we know from Lemma 3(a) and (c) that $\text{trace}(\Sigma(\mu)) = 3 = \text{trace}(W)$, which is also the minimum value of $\text{trace}(\Sigma(\mu))$ among all possible sensor selections μ . Combining the results above and taking the limit as $h \rightarrow \infty$ lead to Eq. (15).

We next prove that the greedy algorithm defined in Algorithm 1 for the posteriori KFSS problem selects sensor 2 and sensor 3 in its first and second iterations, respectively. Note that it is easy to obtain from Eq. (5) that $\Sigma(\mu)$ is of the form $\Sigma(\mu) = \text{diag}((\Sigma(\mu))_{11}, 1, 1)$, $\forall \mu$. Hence, we have from Eq. (6) that $\text{trace}(\Sigma^*(\mu_1)) = 2 + \frac{h^2}{\sigma_1 + h^2}(\sigma_1 - 1)$, $\text{trace}(\Sigma^*(\mu_2)) = 2 + \frac{h^2}{\sigma_2 + h^2}(\sigma_2 - 1)$ and $\text{trace}(\Sigma^*(\mu_3)) = 2 + \frac{1}{1 - \lambda_1^2} - 1$, where $\sigma_1 = \sigma(2h^2)$ and $\sigma_2 = \sigma(h^2)$ are defined above. Since $\sigma(h^2)$ is a strictly increasing function of $h^2 \in \mathbb{R}_{>0}$ with $\sigma(h^2) \geq 1$ and upper bounded by $\frac{1}{1 - \lambda_1^2}$, and it is easy to obtain that $\frac{\sigma_1}{2} < \sigma_2$, it then follows that Algorithm 1 for the posteriori KFSS problem selects sensor 2 in its first iteration.

Similarly, we have from Eq. (6) that $\text{trace}(\Sigma^*(\mu_{12})) = 1 + \frac{h^2}{\sigma_2 + h^2}(\sigma_2 - 1)$, $\text{trace}(\Sigma^*(\mu_{23})) = 1 + \frac{h^2}{2\sigma_{23} + h^2}(\sigma_{23} - 1)$ and $\text{trace}(\Sigma^*(\mu_{13})) = 1$, where $\sigma_{23} = \sigma(\frac{h^2}{2})$ is defined above. Since $\sigma(h^2)$ is strictly increasing in $h^2 \in \mathbb{R}_{>0}$ with $\sigma(h^2) \geq 1$ and upper bounded by $\frac{1}{1 - \lambda_1^2}$, and it is easy to check that $\sigma_2 < 2\sigma_{23}$, it follows that the greedy algorithm selects sensor 3 in its second iteration, and $\mu = \mu_{13}$ is the optimal sensor selection (for the posteriori KFSS instance). Combining the results above and letting $h \rightarrow \infty$, we obtain Eq. (16). ■

Proof of Theorem 4 :

We first analyze Algorithm 2 for the priori KFSA problem. Since the only nonzero eigenvalue of A is λ_1 , we know from Lemma 3(a) that $(\Sigma(\nu^c))_{22} = 1$ and $(\Sigma(\nu^c))_{33} = 1$, $\forall \nu$, which implies that $(\tilde{\Sigma}_{gre})_{22} = 1$ and $(\tilde{\Sigma}_{gre})_{33} = 1$. Hence, we only need to determine $(\tilde{\Sigma}_{gre})_{11}$.

First, denote $\nu_1 = [1 \ 0 \ 0 \ 0]^T$, $\nu_2 = [0 \ 1 \ 0 \ 0]^T$ and $\nu_3 = [0 \ 0 \ 1 \ 0]^T$. Then, it is easy to see that $C(\nu^c)$ is of full column rank for all $\nu \in \{\nu_1, \nu_2, \nu_3\}$. This implies that $\mathbf{e}_1 \in \text{rowspan}(C(\nu^c))$ for all $\nu \in \{\nu_1, \nu_2, \nu_3\}$. Thus, we know from Lemma 3(c) that $(\Sigma(\nu^c))_{11} = 1$, $\forall \nu \in \{\nu_1, \nu_2, \nu_3\}$. Moreover, denoting $\nu_4 = [0 \ 0 \ 0 \ 1]^T$, we have $C(\nu_4^c)$ (after some elementary row operations and merging identical rows) is of the form $C(\nu_4^c) = \begin{bmatrix} 1 & 0 & h \\ 0 & 1 & 0 \end{bmatrix}$. Using the results from the proof of Theorem 3, we obtain that $\sigma'_4 \triangleq (\Sigma(\nu_4^c))_{11}$ satisfies

$$\sigma'_4 = \frac{1 + h^2\lambda_1^2 - h^2 + \sqrt{(h^2 - h^2\lambda_1^2 - 1)^2 + 4h^2}}{2}.$$

If we view σ'_4 as a function of h^2 , denoted as $\sigma'(h^2)$, we know from Lemma 4(a) that $\sigma'(h^2)$ is a strictly increasing function of $h^2 \in \mathbb{R}_{\geq 0}$ with $\sigma'(0) = 1$, which implies $\sigma'_4 > 1$. Thus, Algorithm 2 for priori KFSA targets sensor 4 in its first iteration.

Second, denote $\nu_{14} = [1 \ 0 \ 0 \ 1]^T$, $\nu_{24} = [0 \ 1 \ 0 \ 1]^T$ and $\nu_{34} = [0 \ 0 \ 1 \ 1]^T$. We obtain that $C(\nu^c)$ (after some elementary row operations) is of the form $C(\nu^c) = \begin{bmatrix} 1 & 0 & h \\ 0 & 1 & 0 \end{bmatrix}$, for all $\nu \in \{\nu_{14}, \nu_{24}, \nu_{34}\}$. It follows that $(\Sigma(\nu^c))_{11} = \sigma'_4$ for all $\nu \in \{\nu_{14}, \nu_{24}, \nu_{34}\}$, which implies that $\text{trace}(\tilde{\Sigma}_{gre}) = \sigma'_4 + 2$.

Furthermore, the optimal sensor attack (for the priori KFSA instance) is $\nu = \nu_{12}$, where $\nu_{12} = [1 \ 1 \ 0 \ 0]^T$, since in this case we know from Lemma 3(a) and (b) that $(\Sigma(\nu^c))_{11} = \frac{1}{1 - \lambda_1^2}$, which is also the maximum value of $(\Sigma(\nu^c))_{11}$ that it can achieve, i.e., $\tilde{\Sigma}_{opt} = \frac{1}{1 - \lambda_1^2} + 2$. Combining the results above and taking the limit as $h \rightarrow 0$, we obtain Eq. (17).

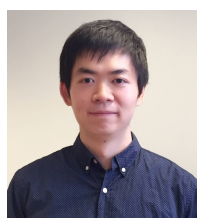
We next analyze Algorithm 2 for the posteriori KFSA problem. Since we know from previous arguments that $C(\nu^c)$ is of full column rank for all $\nu \in \{\nu_1, \nu_2, \nu_3\}$, it follows from Lemma 3(c) that $\text{trace}(\Sigma^*(\nu_1^c)) = \text{trace}(\Sigma^*(\nu_2^c)) = \text{trace}(\Sigma^*(\nu_3^c)) = 0$. Moreover, it is easy to obtain from Eq. (5) that $\Sigma(\nu^c)$ is of the form $\Sigma(\nu^c) = \text{diag}((\Sigma(\nu^c))_{11}, 1, 1)$, $\forall \nu$. We then have from Eq. (6) that $\text{trace}(\Sigma^*(\nu_4^c)) = 1 + \frac{h^2}{\sigma'_4 + h^2}(\sigma'_4 - 1)$, where $\sigma'_4 = \sigma'(h^2)$ is defined above. Since $\sigma'(h^2)$ is strictly increasing in $h^2 \in \mathbb{R}_{\geq 0}$ with $\sigma'(0) = 1$, it implies that Algorithm 2 for posteriori KFSA targets sensor 4 in its first iteration. Similarly, we have from Eq. (6) that $\text{trace}(\Sigma^*(\nu_{14}^c)) = \text{trace}(\Sigma^*(\nu_{24}^c)) = \text{trace}(\Sigma^*(\nu_{34}^c)) = 1 + \frac{h^2}{\sigma'_4 + h^2}(\sigma'_4 - 1)$, which implies $\text{trace}(\tilde{\Sigma}_{gre}) = 1 + \frac{h^2}{\sigma'_4 + h^2}(\sigma'_4 - 1)$.

Furthermore, denote $\nu_{23} = [0 \ 1 \ 1 \ 0]^T$ and $\nu_{13} = [1 \ 0 \ 1 \ 0]^T$. It is easy to show, via similar arguments to those above, that $\text{trace}(\Sigma^*(\nu^c)) = 1 + \frac{h^2}{\sigma'_4 + h^2}(\sigma'_4 - 1)$ for all $\nu \in \{\nu_{34}, \nu_{24}, \nu_{23}, \nu_{14}\}$, $\text{trace}(\Sigma^*(\nu_{13}^c)) = 1$, and $\text{trace}(\Sigma^*(\nu_{12}^c)) = 1 + \frac{1}{1 - \lambda_1^2} - 1$. Since $\sigma'_4 = \sigma'(h^2)$ is strictly increasing in $h^2 \in \mathbb{R}_{\geq 0}$ with $\sigma'(0) = 1$, and upper bounded by $\frac{1}{1 - \lambda_1^2}$, it follows that the optimal sensor attack (for the posteriori KFSA instance) is $\nu = \nu_{12}$. Combining the results above and taking the limit as $h \rightarrow 0$, we obtain Eq. (18). ■

REFERENCES

- [1] M. Van De Wal and B. De Jager, "A review of methods for input/output selection," *Automatica*, vol. 37, no. 4, pp. 487–510, 2001.
- [2] A. Olshevsky, "Minimal controllability problems," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 3, pp. 249–258, 2014.
- [3] X. Liu, B. M. Chen, and Z. Lin, "On the problem of general structural assignments of linear systems through sensor/actuator selection," *Automatica*, vol. 39, no. 2, pp. 233–241, 2003.
- [4] S. Joshi and S. Boyd, "Sensor selection via convex optimization," *IEEE Transactions on Signal Processing*, vol. 57, no. 2, pp. 451–462, 2009.
- [5] V. Tzoumas, M. A. Rahimian, G. J. Pappas, and A. Jadbabaie, "Minimal actuator placement with bounds on control effort," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 1, pp. 67–78, 2016.
- [6] T. H. Summers, F. L. Cortesi, and J. Lygeros, "On submodularity and controllability in complex dynamical networks," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 1, pp. 91–101, 2016.
- [7] A. Olshevsky, "On (non) supermodularity of average control energy," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1177–1181, 2018.
- [8] F. Lin, M. Fardad, and M. R. Jovanović, "Design of optimal sparse feedback gains via the alternating direction method of multipliers," *IEEE Transactions on Automatic Control*, vol. 58, no. 9, pp. 2426–2431, 2013.

- [9] T.-S. Yoo and S. LaFortune, "NP-completeness of sensor selection problems arising in partially observed discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 47, no. 9, pp. 1495–1499, 2002.
- [10] Y. Mo, R. Ambrosino, and B. Sinopoli, "Sensor selection strategies for state estimation in energy constrained wireless sensor networks," *Automatica*, vol. 47, no. 7, pp. 1330–1338, 2011.
- [11] L. F. Chamon, G. J. Pappas, and A. Ribeiro, "Approximate supermodularity of Kalman filter sensor selection," *IEEE Transactions on Automatic Control*, 2020.
- [12] M. P. Vitus, W. Zhang, A. Abate, J. Hu, and C. J. Tomlin, "On efficient sensor scheduling for linear dynamical systems," *Automatica*, vol. 48, no. 10, pp. 2482–2493, 2012.
- [13] M. F. Huber, "Optimal pruning for multi-step sensor scheduling," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1338–1343, 2012.
- [14] S. T. Jawaid and S. L. Smith, "Submodularity and greedy algorithms in sensor scheduling for linear dynamical systems," *Automatica*, vol. 61, pp. 282–288, 2015.
- [15] N. K. Dhingra, M. R. Jovanović, and Z.-Q. Luo, "An ADMM algorithm for optimal sensor and actuator selection," in *Proc. IEEE Conference on Decision and Control*, 2014, pp. 4039–4044.
- [16] C. Yang, J. Wu, X. Ren, W. Yang, H. Shi, and L. Shi, "Deterministic sensor selection for centralized state estimation under limited communication resource," *IEEE Transactions on Signal Processing*, vol. 63, no. 9, pp. 2336–2348, 2015.
- [17] L. Ye, S. Roy, and S. Sundaram, "Optimal sensor placement for Kalman filtering in stochastically forced consensus network," in *Proc. IEEE Conference on Decision and Control*, 2018, pp. 6686–6691.
- [18] H. Zhang, R. Ayoub, and S. Sundaram, "Sensor selection for Kalman filtering of linear dynamical systems: Complexity, limitations and greedy algorithms," *Automatica*, vol. 78, pp. 202–210, 2017.
- [19] A. Krause, A. Singh, and C. Guestrin, "Near-optimal sensor placements in Gaussian processes: Theory, efficient algorithms and empirical studies," *Journal of Machine Learning Research*, vol. 9, no. Feb, pp. 235–284, 2008.
- [20] M. Shamaiah, S. Banerjee, and H. Vikalo, "Greedy sensor selection: Leveraging submodularity," in *Proc. IEEE Conference on Decision and Control*, 2010, pp. 2572–2577.
- [21] G. L. Nemhauser, L. A. Wolsey, and M. L. Fisher, "An analysis of approximations for maximizing submodular set functions," *Mathematical Programming*, vol. 14, no. 1, pp. 265–294, 1978.
- [22] A. Das and D. Kempe, "Submodular meets spectral: Greedy algorithms for subset selection, sparse approximation and dictionary selection," *arXiv preprint arXiv:1102.3975*, 2011.
- [23] J. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, p. 13, 2011.
- [24] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.
- [25] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2014.
- [26] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.
- [27] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.
- [28] 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.
- [29] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," in *Proc. IEEE Symposium on Security and Privacy*, 1997, pp. 208–223.
- [30] A. Laszka, Y. Vorobeychik, and X. Koutsoukos, "Resilient observation selection in adversarial settings," in *Proc. IEEE Conference on Decision and Control*, 2015, pp. 7416–7421.
- [31] V. Tzoumas, K. Gatsis, A. Jadbabaie, and G. J. Pappas, "Resilient monotone submodular function maximization," in *Proc. IEEE Conference on Decision and Control*, 2018, pp. 1362–1367.
- [32] V. Tzoumas, A. Jadbabaie, and G. J. Pappas, "Sensor placement for optimal Kalman filtering: Fundamental limits, submodularity, and algorithms," in *Proc. American Control Conference*, 2016, pp. 191–196.
- [33] L. Ye, S. Roy, and S. Sundaram, "On the complexity and approximability of optimal sensor selection for Kalman filtering," in *Proc. American Control Conference*, 2018, pp. 5049–5054.
- [34] A. Das and D. Kempe, "Algorithms for subset selection in linear regression," in *Proc. ACM Symposium on Theory of Computing*, 2008, pp. 45–54.
- [35] J. Lu and R. Niu, "Sparse attacking strategies in multi-sensor dynamic systems maximizing state estimation errors," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, 2016, pp. 3151–3155.
- [36] B. D. Anderson and J. B. Moore, *Optimal Filtering*. Dover Books, 1979.
- [37] D. E. Catlin, *Estimation, control, and the discrete Kalman filter*. Springer, 1989.
- [38] B. D. Anderson and J. B. Moore, *Optimal control: linear quadratic methods*. Courier Corporation, 2007.
- [39] M. R. Garey and D. S. Johnson, *Computers and intractability: a guide to the theory of NP-completeness*. Freeman, 1979.
- [40] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge University Press, 1985.
- [41] B. K. Natarajan, "Sparse approximate solutions to linear systems," *SIAM Journal on Computing*, vol. 24, no. 2, pp. 227–234, 1995.



Lintao Ye received the B.E degree in Material Science and Engineering from Huazhong University of Science and Technology, Wuhan, China, in 2015. He received the M.S degree in Mechanical Engineering from Purdue University in 2017. He is currently pursuing a Ph.D degree in Electrical and Computer Engineering at Purdue University. His research interests are in the areas of optimization, linear system and estimation theory, signal processing, and network science.



Nathaniel Woodford received the Bachelors of Science Degree in Astronautical Engineering from the United States Air Force Academy in 2017. He is currently a masters graduate student in the School of Electrical and Computer Engineering at Purdue University. His interests include fault-tolerant control, combinatorial optimization, and machine learning.



Sandip Roy works as Professor and Associate Director for the School of Electrical Engineering and Computer Science at Washington State University. His research is primarily focused on developing techniques for the sparse monitoring and control of dynamical networks, and using these techniques to support wide-area management of disruptions in large-scale infrastructure networks, including electric power and air transportation networks. Recently, he have also been interested in network analysis and design problems that arise in neurological and epidemiological processes. These research efforts have led to new models and algorithms, as well as software deployments, which are described in archival journal publications (about 65 in total) and peer-reviewed conference articles (about 125 in total).



Shreyas Sundaram is an Associate Professor in the School of Electrical and Computer Engineering at Purdue University. He received his PhD in Electrical Engineering from the University of Illinois at Urbana-Champaign in 2009. He was a Postdoctoral Researcher at the University of Pennsylvania from 2009 to 2010, and an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Waterloo from 2010 to 2014. He is a recipient of the NSF CAREER award. At Purdue, he received the HKN Outstanding Professor Award, the Outstanding Mentor of Engineering Graduate Students Award, the Hesselberth Award for Teaching Excellence, and the Ruth and Joel Spira Outstanding Teacher Award. His research interests include network science, analysis of large-scale dynamical systems, fault-tolerant and secure control, linear system and estimation theory, and game theory.