Sensor and Threshold Selection for Safe Fault Detection

Andrew Clark and Shiyu Cheng

***Abstract*— Control systems can be severely impacted by node faults due to natural failures or malicious attacks. This paper considers two design problems for unknown input observer (UIO)-based fault detection schemes. First, we consider the problem of choosing optimal detection thresholds to ensure the fault is detected before safety violations occur while avoiding false alarms. We derive bounds on the thresholds to ensure that any constant-magnitude fault can be detected. Second, we investigate the problem of ensuring that the fault detector has adequate information to detect and isolate faults. We derive sufficient conditions for the existence of a UIO as a function of the available sensors, and prove that the problem of selecting a minimum-size set of neighbors is equivalent to matroid intersection, enabling polynomial-time approximation algorithms. Our simulation results confirm that our approach is able to detect faults before safety violations occur.**

I. Introduction

Control systems are prone to faults, in which one or more system states deviates from its prescribed dynamical model. These failures occur due to equipment failure, environmental disturbances, or deliberate attacks, and may jeopardize stability and performance. Fault-tolerant control focuses on ensuring desired system behavior in the presence of disruptions such as actuator failures [1]. Fault-tolerant control often involves detection mechanisms, in which an estimator attempts to detect, localize, and mitigate failures to preserve stability [2]–[4].

One such detection method is based on the widely-studied approach of unknown input observers (UIO) [5]. Under this approach, the detector constructs a UIO for each fault mode. The UIO is designed to ensure that the state estimate is decoupled from the corresponding fault mode. Hence, when that fault mode occurs, the error of the corresponding UIO will remain low, while all other estimators will experience high errors, thus enabling the monitor to detect and localize the fault. This approach can then be combined with mitigation mechanisms to restore the stability of the system.

This paper presents two contributions towards the development of UIO-based fault detection. We first consider the problem of selecting optimal detection thresholds. Setting the threshold too high may result in the monitor failing to raise an alarm before a safety violation occurs, while a low threshold may cause false alarms due to noise and environmental disturbances. Current approaches to threshold selection are based on domain knowledge or heuristic methods [5], [6]. We propose a systematic approach that bounds the detection time and then selects a minimum threshold to ensure that detection occurs before a safety constraint on the norm of the system state is reached.

Our second contribution concerns the design of the observer itself. The existence of a UIO relies on having sufficient sensor measurements to decouple the fault and reconstruct the true system state. We propose an approach for selecting a minimum-cost set of sensors to guarantee existence of a UIO. We prove that this problem is equivalent to a minimum-cost matroid intersection problem, which can be approximately solved up to a provable optimality bound that is linear in the number of matroids. We evaluate our approach through a numerical study and find that the number of sensors remains constant as the system dimension grows (reflecting the local nature of the fault detection problem).

The paper is organized as follows. Section II presents the system model. Section III presents our problem formulation and proposed approach. Section IV presents simulation results. Section V concludes the paper.

II. Model and Preliminaries

This section presents the system and fault models we consider in this paper. We also present background on unknown input observers and matroids.

A. System and Fault Models

The dynamics of $\mathbf{x}(t)$ are given by $\dot{\mathbf{x}}(t) = A\mathbf{x}(t)+Gd(t)$, where $\mathbf{d}(t) \in \mathbb{R}^p$ is a disturbance with $||\mathbf{d}(t)||_2 \leq \overline{d}$ for all t and some $\overline{d} > 0$. We assume that there is a safety constraint of the form $||\mathbf{x}(t)||_2 \leq \xi$ for some given constant $\xi > 0$ which must hold for all time t. The sensor data at time t is given by $y(t) \in \mathbb{R}^m$ where $y(t) = C\mathbf{x}(t)$.

The fault modes are indexed in a set $\mathcal{F} = \{1, \ldots, M\}$. For the fault mode $k \in \mathcal{F}$, the corresponding system dynamics are

$$\dot{\mathbf{x}} = A\mathbf{x} + E_k f_k + Gd.$$

We consider single-state faults where E_k is an n-dimensional column vector with $(E_k)_i = 1$ if i is the failed state in mode k and $(E_k)_i = 0$ otherwise.

B. Unknown Input Observers

The system maintains an observer for each fault pattern k, which computes a time-varying state estimate $\hat{x}_k(t) \in \mathbb{R}^n$. Following the approach in [6], the observer for fault mode k has internal state $q_k(t)$ and dynamics

$$\dot{q}_k(t) = F_k q_k(t) + K_k y(t) \quad (1)$$

$$\hat{x}_k(t) = q_k(t) + H_k y(t) \quad (2)$$

for matrices F_k, K_k, and H_k of appropriate dimension.

A. Clark and S. Cheng are with the Department of Electrical and Systems Engineering, Washington University in St. Louis, St. Louis, MO, USA. Email: {andrewclark,cheng.shiyu}@wustl.edu

The estimator is an unknown input observer (UIO) for fault k if $\lim_{t\to\infty} ||\mathbf{x}(t) - \hat{\mathbf{x}}_k(t)||_2 = 0$ for any value of the fault signal $f_k(t)$ when $d(t) \equiv 0$. The following result gives sufficient conditions for (1)–(2) to define a UIO.

Proposition 1 ([6]): Suppose that F_k^i is Hurwitz and

$$K_k = K_1 + K_2,\ F_k = A - H_kCA - K_1C$$
$$K_2 = F_kH_k,\ T_k^i = I - H_kC$$
$$(H_kC - I)E_k = 0$$

Then (1)–(2) is a UIO.

We denote the error $z_k(t) = \mathbf{x}(t) - \hat{\mathbf{x}}_k(t)$. The existence of matrices satisfying the conditions of Proposition 1 depends on the choice of monitoring nodes. The following gives conditions for existence of a UIO based on the fault matrix E_k and the monitoring matrix C.

Proposition 2 ([6]): For the system with dynamics (1), the sufficient and necessary condition to ensure the existence of a UIO using the measurements of a single node i decoupled from a faulty node p is

$$\text{rank}(CE_k) = \text{rank}(E_k)$$
$$\text{rank}\begin{bmatrix} sI - A & E_k \\ C & 0 \end{bmatrix} = n + \text{rank}(E_k)$$

for all $s \in \mathcal{C}$ with nonnegative real parts.

C. Background on Matroids

In what follows, we give background results on matroids, which can be found in [7].

Definition 1: A matroid $\mathcal{M} = (V, \mathcal{I})$ is defined by a finite set V and a collection $\mathcal{I}$ of subsets of V satisfying: (i) $\emptyset \in \mathcal{I}$, (ii) if $B \in \mathcal{I}$, then $A \in \mathcal{I}$ for all $A \subseteq B$, and (iii) if $A, B \in \mathcal{I}$ and $|A| < |B|$, then there exists $v \in B \setminus A$ such that $(A \cup \{v\}) \in \mathcal{I}$.

A *basis* of $\mathcal{M}$ is a maximal independent set, i.e., a set $A \in \mathcal{I}$ such that there is no set $B \in \mathcal{I}$ that contains A. The rank of a matroid is equal to the cardinality of a basis of the matroid. The rank function of a matroid $\rho : 2^V \to \mathbb{Z}_{\geq 0}$ is defined by

$$\rho(A) = \max\{|T| : T \in \mathcal{I}, T \subseteq A\}$$

with $\rho(A) = |A|$ iff $A \in \mathcal{I}$. The following lemma enables us to construct matroids from rank functions.

Lemma 1: Suppose that V is a finite set and $\rho : 2^V \to \mathbb{Z}_{\geq 0}$ satisfies: (i) $\rho(\emptyset) = 0$, (ii) $(\rho(A \cup \{v\}) - \rho(A)) \in \{0, 1\}$ for all $A \subseteq V$ and $v \in V$, and (iii) for any $A \subseteq B \subseteq V$ and $v \in V$, we have $\rho(A \cup \{v\}) - \rho(A) \geq \rho(B \cup \{v\}) - \rho(B)$ (submodularity). Then the tuple $\mathcal{M} = (V, \mathcal{I})$ with $A \in \mathcal{I}$ iff $\rho(A) = |A|$ is a matroid.

We denote a matroid $\mathcal{M}$ constructed from a function ρ satisfying the conditions of Lemma 1 as the matroid induced by ρ.

Consider a collection of vectors $\{v_1, \ldots, v_n\} \subseteq \mathbb{R}^m$. We can define a matroid $\mathcal{M} = (V, \mathcal{I})$ with $V = \{1, \ldots, n\}$ and $A \in \mathcal{I}$ if the collection of vectors $\{v_i : i \in A\}$ is linearly independent. The rank function $\rho(A)$ of this matroid is equal to the rank of the matrix with columns $\{v_i : i \in A\}$.

Finally, if $\mathcal{M} = (V, \mathcal{I})$ is a matroid, then define $\mathcal{M}^* = (V, \mathcal{I}^*)$ with $A \in \mathcal{I}^*$ if $(V \setminus A)$ is a basis of $\mathcal{M}$. It can be shown that $\mathcal{M}^*$ is a matroid, which is referred to as the *dual* of matroid $\mathcal{M}$.

III. Problem Formulation

We consider the following policy [4] for UIO-based fault detection and identification. We maintain a bank of observers $\hat{\mathbf{x}}_k(t)$, $k = 1, \ldots, M$, as described in Section II-B. We let $r_k(t) = y(t) - C\hat{\mathbf{x}}_k(t)$. Fault k is detected at time t if $||r_k(t)|| \leq \psi_k$ and $||r_m(t)|| \geq \psi_m$ for all $m \neq k$. This approach is motivated by the fact that, if fault k occurs, the signal $r_k(t)$ associated with UIO k is unaffected, since that UIO is decoupled from k. On the other hand, all other estimators are not decoupled from fault k, and hence will experience high values of r (Fig. 1).

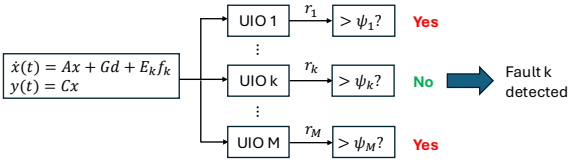


Fig. 1: Schematic illustration of our approach.

This section presents the formulation and solution approach for the two problems considered in this paper, namely selecting monitoring thresholds and choosing the set of nodes to act as observers. For the latter problem, we consider a scenario where the system is unable to construct a UIO using only the available sensor measurements, and must place additional sensors to construct the observer and detect the fault.

A. Selection of Observer Thresholds

Definition 2: The UIO-based FDI scheme described above is *safe* if (i) $f_k(t) \equiv 0$ for all k implies that $||r_k(t)|| \leq \psi_k$ for all t, k; (ii) $f_k(t) \equiv \overline{f}_k$ for $t \geq 0$ and some $\overline{f}_k$ with $|\overline{f}_k| \leq f_{max}$ implies that $||r_k(t)|| \leq \psi_k$ and either $||\mathbf{x}(t)|| \leq \xi$ for all t, or there exists time $t' \geq 0$ such that $||r_m(t')|| \geq \psi_m$ for all $m \neq k$, and $||\mathbf{x}(t)|| \leq \xi$ for all $t \in [0, t']$.

Property (i) implies that there are no false alarms in the detection, while property (ii) implies that, if there is a constant fault of any magnitude, then the fault is detected correctly before the state $\mathbf{x}(t)$ enters the unsafe region. Constant faults with known maximum amplitude could occur, for example, when a fault causes an actuator to be stuck in a fixed position, which is bounded by physical device constraints. Based on the above definition, we have the following problem formulation.

Problem 1: Given a collection of unknown input observers as described in Section II-B, choose thresholds ψ_k, $k = 1, \ldots, M$ such that the resulting FDI scheme is safe.

We make the following assumptions about the state and estimator dynamics.

Assumption 1: The matrix A is symmetric and negative definite with largest eigenvalue $-\lambda$, where $\lambda > 0$. The zero-state L_∞ gain from $d(t)$ to $r_k(t)$ is bounded above by $\gamma^k > 0$. The matrix F_k is Hurwitz for all k and satisfies $||e^{F_k t}z|| \leq e^{-\beta_k t}||z||$ for all z. The initial states and estimation error satisfy $||\mathbf{x}(0)|| \leq \phi$ and $||z_k(0)|| \leq \theta_k$. for some positive constants ϕ and θ_k, $k = 1, \ldots, M$. We assume that $\xi \geq \phi$, i.e., this system is initialized in a safe state.

Under these assumptions, the following theorem gives conditions for selecting the thresholds to ensure safety.

Theorem 1: Let the conditions of Assumption 1 hold. Suppose that for each k, we have $\gamma^k \overline{d} \leq \psi_k$. Define $g_{k,m}(w)$ by

$$g_{k,m}(w) = \left(\frac{\xi + \frac{1}{\lambda}||E_m||w + \frac{1}{\lambda}||G||\overline{d}}{\phi + \frac{1}{\lambda}||E_m||w + \frac{1}{\lambda}||G||\overline{d}} \right)^{-\beta_k/\lambda}$$

and define $g_{k,m}(w)$ by

$$h_{k,m}(w) = ||C(F_k)^{-1}T_k E_m||w - ||C||g_{k,m}(w)(||C(F_k)^{-1}T_k E_m||w + \theta_k).$$

Suppose that $h_{k,m}(w) - \gamma_k \overline{d} \geq \psi_k$ for all $w \in \left[\frac{\xi\lambda - ||G||\overline{d}}{||E_m||}, f_{max}\right]$ and all $m, k \in \{1, \ldots, M\}$ with $k \neq m$. Then the UIO-based FDI scheme is safe.

Proof: The approach of the proof is to derive a lower bound W on the first time t when $||\mathbf{x}(t)||_2 = \xi$ under fault mode m. We will then show that $||r_k(W)|| \geq \psi_k$ for all $k \neq m$, thus proving that condition (ii) of Definition 2 holds.

As a preliminary, we let $x^* = -A^{-1}E_m\overline{f}_m$ denote the equilibrium of the network dynamics under the constant fault $\overline{f}_m$, and let $(z_k)^* = (F_k)^{-1}T_k E_m \overline{f}_m$ denote the equilibrium of the estimation error z_k. Next, we define $\hat{z}_k = z_k - (z_k)^*$, so that

$$\dot{\hat{z}}_k = F_k \hat{z}_k + T_k G d.$$

We first derive an upper bound on $||\mathbf{x}(t)||$. We have

$$\begin{aligned}
&||\mathbf{x}(t)|| \\
&\leq ||e^{At}\mathbf{x}(0)|| + || \int_0^t e^{A(t-\tau)}E_m \, d\tau|||f_m| \\
&\quad + || \int_0^t e^{A(t-\tau)}Gd(\tau) \, d\tau|| \\
&\leq e^{-\lambda t}||\mathbf{x}(0)|| + \int_0^t ||e^{A(t-\tau)}E_m|| \, d\tau|f_m| \\
&\quad + \left(\int_0^T ||e^{A(t-\tau)}G \, d\tau \right) \overline{d} \\
&\leq e^{-\lambda t}||\mathbf{x}(0)|| + \left(\int_0^t e^{\lambda(t-\tau)} \, d\tau \right) (||E_m|||f_m| + ||G||\overline{d}) \\
&= e^{-\lambda t}(\phi - \frac{1}{\lambda}||E_m|||f_m| - \frac{1}{\lambda}||G||\overline{d}) \\
&\quad + \frac{1}{\lambda}(||G||\overline{d} + ||E_m|||f_m|) \triangleq \bar{x}(t)
\end{aligned}$$

It follows that $\overline{x}(t)$ is monotone nondecreasing if $\frac{1}{\lambda}(||E_m|||f_m| + ||G||\overline{d}) \geq \phi$ and monotone decreasing otherwise with $\overline{x}(0) = \phi$, implying that we can restrict our attention to the case $|f_m| \geq \frac{\phi\lambda - ||G||\overline{d}}{||E_m||}$. Furthermore, note that $\lim_{t\to\infty} \overline{x}(t) = \frac{1}{\lambda}(||G||\overline{d} + ||E_m|||f_m|)$, which gives an upper bound on $||\mathbf{x}(t)||$ for all t. Hence in order to guarantee the safety property, it suffices to detect the fault when $\frac{1}{\lambda}(||G||\overline{d} + ||E_m|||f_m|) \geq \xi$, i.e., when $|f_m| \geq \frac{\xi\lambda - ||G||\overline{d}}{||E_m||}$.

Now, let $W \geq 0$ satisfy $\bar{x}(W) = \xi$. Rearranging terms yields

$$W = \frac{1}{\lambda} \log \left\{ \frac{\xi + \frac{1}{\lambda}||E_m|||f_m| + \frac{1}{\lambda}||G||\overline{d}}{\phi + \frac{1}{\lambda}||E_m|||f_m| + \frac{1}{\lambda}||G||\overline{d}} \right\}.$$

Since $||\mathbf{x}(W)|| \leq \bar{x}(W)$, we must have $||\mathbf{x}(W)|| \leq \xi$. Hence if $||r_k(W)|| \geq \psi_k$ for all k, then condition (ii) for safety holds. We have that

$$\begin{aligned}
&||r_k(W)|| \\
&= ||Cz_k(W)|| = ||C((z_k)^* + \hat{z}_k(W))|| \\
&\geq ||Cz_k^*|| - ||C\hat{z}_k(W)|| \\
&\geq ||C(F_k)^{-1}T_k E_m|||f_m| - ||Ce^{F_k W}\hat{z}_k(0)|| - \gamma^k\overline{d} \\
&\geq |C(F_k)^{-1}T_k E_m|||f_m| - ||C||e^{-\beta W}||\hat{z}_k(0)|| - \gamma^k\overline{d}
\end{aligned}$$

Substituting the value of W yields

$$\begin{aligned}
&||r^k(W)|| \\
&\geq ||C(F_k)^{-1}T_k E_m|||f_m| - \gamma_i^k\overline{d} \\
&\quad -||C|| \left(\frac{\xi + \frac{1}{\lambda}||E_m|||f_m| + \frac{1}{\lambda}||G||\overline{d}}{\phi + \frac{1}{\lambda}||E_m|||f_m| + \frac{1}{\lambda}||G||\overline{d}} \right)^{-\beta/\lambda} ||\hat{z}_k(0)|| \\
&= ||C(F_k)^{-1}T_k E_m|||f_m| - ||C||g_{k,m}(|f_m|)||\hat{z}_k(0)|| - \gamma^k\overline{d}
\end{aligned}$$

Now, we have $||\hat{z}_k(0)|| = ||z_k(0) - (z_k)^*|| \leq ||z_k(0)|| + ||(z_k)^*||$. Hence we have

$$\begin{aligned}
||r^k(W)|| \geq\ &||C(F_k)^{-1}T_k E_m|||f_m| - \gamma^k\overline{d} \\
&-||C||g_{k,m}(|f_m|)(||C(F_k)^{-1}T_k E_m|||f_m| + \theta_k)
\end{aligned}$$

Thus the conditions of the theorem imply that the FDI scheme is safe. ■

We can therefore ensure safety if we select the threshold ψ_k to ensure that $h_{k,m}(w) - \gamma_k\overline{d} \geq \psi_k$ for all $w \in \left[\frac{\xi\lambda - ||G||\overline{d}}{||E_m||}, f_{max}\right]$. This can be checked by iterating over possible values of w within the interval $\left[\frac{\xi\lambda - ||G||\overline{d}}{||E_m||}, f_{max}\right]$. In the case where the fault magnitude is insufficient to cause safety violations, our proposed approach may still be able to detect the fault, although it is not guaranteed by Theorem 1.

B. Selection of Monitoring Nodes

The preceding analysis assumed that a UIO could be constructed based on the available sensor measurements. However, this approach may fail if the set of measurements is insufficient to enable a decoupled observation of the fault k, as characterized by Proposition 2. In this scenario, we can place additional sensors to recover more data. In what follows, we formulate the problem of choosing a minimum-cost set of sensors in order to ensure the decoupling property. Unlike the preceding section, the following results do not make any assumptions on the fault signals f_k.

Formally, we let μ_j be the cost to add a sensor for state j. We let S denote the set of sensors, and let $C(S)$ denote the induced observation matrix.

Problem 2: Select a set of nodes S in order to minimize $\sum_{j\in S}\mu_j$ while satisfying the conditions of Proposition 2.

Our approach to addressing Problem 2 leverages the following sufficient condition.

Lemma 2 ([8]): There exists a UIO for system (1) that is decoupled from faulty node k if (i) $\text{rank}(C(S)E_k) = \text{rank}(E_k)$ and (ii) $(A-HC(S)A, C(S))$ is a detectable pair, for some matrix H satisfying $(I-HC(S))E_k = 0$.

One challenge of applying the preceding lemma is that the matrix H is itself part of the UIO design. We give a construction for H as follows.

Lemma 3: Let k be a faulty node with $k \in S$. Without loss of generality, suppose the first row of $C(S)$ has a 1 in the k-th entry and 0s elsewhere. Then the matrix H with $H_{k1} = 1$ and all other entries 0 satisfies $(I-HC)E_k = 0$.

Proof: By definition of the matrices H and $C(S)$, we have the (j,l)-entry is given by

$$(HC(S))_{jl} = \begin{cases} 1, & j = k, l = k \\ 0, & \text{else} \end{cases}$$

Hence, we have that $(I-HC(S))$ is a diagonal matrix with a 0 in the (k,k) entry and 1's elsewhere. Since E_k is a vector with a 1 in the k-th entry and 0's elsewhere, the we have $(I-HC(S)) = 0$. ∎

Let $Z_k(S)$ denote the value of $HC(S)$ under this choice of H. Then $(Z_k(S))_{kk} = 1$ and all other entries of $(Z_k(S))$ are zero, regardless of the other nodes in S. We therefore omit S and write $HC(S) = Z_k$, and the condition of Lemma 2 is equivalent to $(A - Z_kA, C(S))$ being detectable.

Next, letting $\lambda_1, \ldots, \lambda_L$ denote the eigenvalues of $(A - Z_kA)$ with nonnegative real parts, we define functions $\rho_{k,0}, \ldots, \rho_{k,L} : 2^{\mathcal{V}} \to \mathbb{Z}$ as

$$\rho_{k,0}(S) = \text{rank}(C(S)E_k)$$
$$\rho_{k,j}(S) = \text{rank}\begin{pmatrix} A - Z_kA - \lambda_j I \\ C(S) \end{pmatrix} - \text{rank}(A - Z_kA - \lambda_j I)$$

By convention, let $\rho_{k,0}(\emptyset) = 0$.

Lemma 4: The functions $\rho_{k,0}, \ldots, \rho_{k,L}$ are matroid rank functions.

Proof: We need to show that for each $j \in \{0, \ldots, L\}$, $\rho_{kj}(S)$ satisfies (i) $\rho_{kj}(\emptyset) = 0$, (ii) for any v, $(\rho_{kj}(S \cup \{v\}) - \rho_{kj}(S)) \in \{0, 1\}$. We consider the cases $j = 0$ and $j \in \{1, \ldots, L\}$, and (iii) $\rho_{kj}(S)$ is submodular separately.

$j = 0$: If $S = \emptyset$ then $C(S) = 0$ and hence $\rho_{k0}(S) = 0$. We have that $\text{rank}(C(S\cup\{v\})E_k) - \text{rank}(C(S)E_k)$ is equal to 0 if $C(\{v\})E_k$ is in the span of the rows of $C(S)E_k$ and 1 otherwise, implying property (ii). Finally, if $C(\{v\})E_k$ is in the span of the rows of $C(S)E_k$, then $C(\{v\})E_k$ is in the span of the rows of $C(T)E_k$ for any T with $S \subseteq T$. Hence ρ_{k0} is a matroid rank function.

$j \in \{1, \ldots, L\}$: If $S = \emptyset$, then by definition $\rho_{k,j} = 0$. We also have that $\rho_{kj}(S \cup \{v\}) - \rho_{kj}(S) = 0$ if $C(\{v\})$ is in the row space of

$$\begin{pmatrix} A - Z_kA - \lambda_j I \\ C(S) \end{pmatrix}$$

and is equal to 1 otherwise. This implies (ii) and (iii). ∎

We let $\mathcal{M}_{k,0}, \ldots, \mathcal{M}_{k,L}$ denote the matroids induced by rank functions $\rho_{k,0}, \ldots, \rho_{k,L}$. We can then describe the necessary and sufficient conditions for existence of UIO in terms of matroid constraints on S.

Theorem 2: There exists a UIO decoupled from fault mode k if, for each $j \in \{0, \ldots, L\}$ there exists $T_j \subseteq S$ such that T_j is a basis for the matroid $\mathcal{M}_{k,j}$.

Proof: We have that a set T is a basis for a matroid $\mathcal{M}$ with rank function ρ iff $\rho(T) = |T|$ and $|T|$ is equal to the maximum value of ρ. We first consider $\mathcal{M}_{k,0}$. Note that $\rho_{k0}(S) = \text{rank}(C(S)E_k) \leq \text{rank}(E_k)$. Hence the first condition of Proposition 2 holds iff $\rho_{k0}(S) = \text{rank}(\mathcal{M}_{k0})$, which is satisfied iff S contains a basis of $\mathcal{M}_{k0}$.

Next, we consider $j \in \{1, \ldots, L\}$. We have that

$$\text{rank}\begin{pmatrix} A - Z_kA - \lambda_j I \\ C(S) \end{pmatrix} \leq n$$

Hence the second condition of Proposition 2 holds iff $\rho_{kj}(S) = \text{rank}(\mathcal{M}_{kj})$ for $j = 1, \ldots, L$, i.e., if S contains a basis of $\mathcal{M}_{kj}$ for $j = 1, \ldots, L$. ∎

The following corollary will allow us to develop an equivalent matroid optimization formulation for Problem 2.

Corollary 1: There exists a UIO decoupled from fault mode k if and only if $(V \setminus S) \in \mathcal{M}^*_{k0} \cap \cdots \cap \mathcal{M}^*_{kL}$.

Proof: The condition that S contains a basis of $\mathcal{M}_{kj}$ is equivalent to $V \setminus S$ lying in the dual matroid $\mathcal{M}^*_{kj}$. The result then follows from Theorem 2. ∎

From Corollary 1, Problem 2 is equivalent to

$$\begin{array}{ll} \text{minimize} & \sum_{j\in S}\mu_j \\ \text{s.t.} & (V \setminus S) \in \mathcal{M}^*_{k0} \cap \cdots \cap \mathcal{M}^*_{kL} \end{array} \tag{3}$$

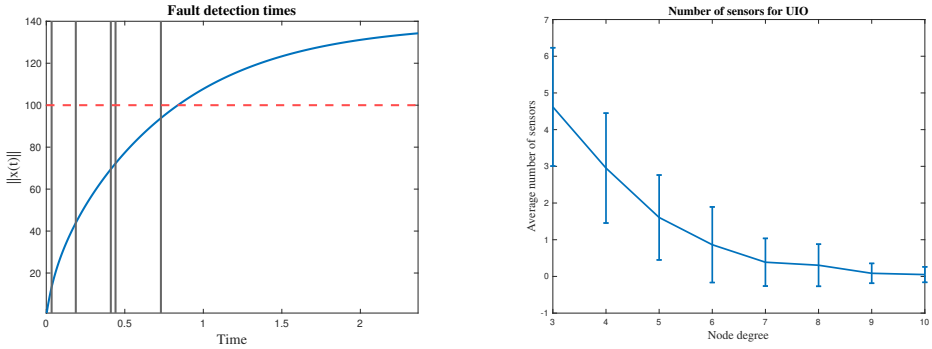
which, by setting $R = V \setminus S$ is equivalent to

$$\begin{array}{ll} \text{maximize} & \sum_{j\in R}\mu_j \\ \text{s.t.} & R \in \mathcal{M}^*_{k0} \cap \cdots \cap \mathcal{M}^*_{kL} \end{array} \tag{4}$$

Eq. (4) is a *maximum matroid intersection* problem. While NP-hard in general, efficient approximation algorithms exist. One such approach is given in Algorithm 1. Letting $\mu(S) = \sum_{j\in S}\mu_{ij}$, the following gives optimality bounds for Algorithm 1.

Proposition 3 ([9], Corollary 3.1): Algorithm 1 returns a set S satisfying $\mu(S) \geq \frac{1}{L}\mu(S^*)$, where S^* is the optimal solution to (4).

Furthermore, if $L = 1$ (i.e., there is only a single unstable mode), then (4) is a matroid intersection problem that can be solved in polynomial time [9].



(a) (b)

Fig. 2: (a) Example of our proposed fault detection approach. We computed the thresholds using the method of Theorem 1. (b) Number of sensors needed as a function of node degree.

Algorithm 1 Matroid intersection algorithm to solve (4)

Initialize: $v \leftarrow \arg\max \mu_j$, $S \leftarrow \{v\}$ $b \leftarrow 1$.
while $b == 1$ **do**
  $b \leftarrow 0$
  if $\exists S'$ with $|S' \setminus S| \leq 2, |S \setminus S'| \leq 2(L+1), \mu(S') \geq \left(1 + \frac{\epsilon}{n(L+2)}\right) \mu(S)$ **then**
    $b \leftarrow 1$, $S \leftarrow S'$
  end if
end while
Return S

IV. Simulation Study

We simulated our approach on a linear system described as follows. Each node i followed grounded Laplacian consensus dynamics given by

$$\dot{x}_i(t) = \begin{cases} -\sum_{j \in N(i)} W_{ij}(x_i(t) - x_j(t)) - 3x_i(t), \\ \qquad i \in \{1, \ldots, 5\} \\ -\sum_{j \in N(i)} W_{ij}(x_i(t) - x_j(t)), \\ \qquad i \in \{6, \ldots, n\} \end{cases}$$

with weights W_{ij} chosen uniformly at random from $[0, 10]$ with $W_{ij} = W_{ji}$. The additional term $-3x_i(t)$ for $i \in \{1, \ldots, 5\}$ ensures that the system matrix A is negative definite. The network topology G was chosen as a geometric random graph, in which each node had a position chosen uniformly at random within a deployment area in $Y \subset \mathbb{R}^2$ independent of all other nodes, and an edge existed between two nodes if they were within distance 1 of each other. The area $|Y|$ of Y was varied in order to ensure a desired average node degree via the formula $d_{avg} = \frac{\pi}{|Y|} n$.

For each simulation, the safety threshold was chosen as $\xi = 100$, maximum disturbance $\overline{d} = 0.01$, $\phi = 0.1$, and $\theta_k = 0.1$ for all k. We first simulated our proposed approach for setting the detection threshold in a network of 10 nodes with a highly connected topology (average degree equal to 8). We considered two fault modes with $\mathcal{V}^1 = \{5\}$, and $\mathcal{V}^2 = \{6\}$. We chose the UIO parameters to ensure that the matrix F_k was Hurwitz for each k with eigenvalues ranging from -1 to -10. The maximum fault amplitude was set to $f_{max} = 1000$. Our proposed approach selected thresholds that detected the faults when $f_{max} \geq 10$. For smaller values of the fault magnitude, the faults were insufficient to cause safety violations.

The results are shown as Fig. 2(a). The blue curve indicates the norm $||x(t)||$, while the red dashed line shows the safety threshold. Each vertical black line shows the detection time for one of the monitoring nodes for the faulty node when $k = 6$. All monitoring nodes detect the fault before the safety violation occurs.

We next examined the effect of the network topology on the number of sensors needed to ensure existence of a UIO. This enabled us to evaluate the practicality of our approach, as well as determine which network parameters influenced the effectiveness of the fault detection. We considered a network of $n = 20$ nodes. Using Algorithm 1, we determined the average number of sensors needed to detect each fault as a function of the average node degree. Each data point represents an average over 50 independent random trials. We found that the total number of sensors was roughly 6-7.

We also studied the number of sensors needed as a function of network size when the average node degree was equal to 4. We found that there was no clear relationship between the number of nodes in the network and the average number of sensors, suggesting that detecting faulty nodes is primarily a local phenomenon, and hence is determined by local network connectivity.

V. Conclusion

This paper studied the problem of fault detection in LTI systems. We investigated an unknown input observer (UIO)-based approach, with a focus on two design decisions. First, we formulated the problem of selecting detection thresholds in order to ensure that faults are identified before safety violations occur, while avoiding false alarms. We constructed thresholds with provable safety guarantees for LTI systems. Second, we formulated the problem of selecting a minimum-cost set of sensors to ensure existence of a UIO. We proved that our derived conditions are equivalent

to a matroid intersection problem and proposed polynomial-time approximation algorithms. A simulation result revealed that our threshold selection ensured detection prior to a safety violation. Future works should explore formulations for nonlinear systems. We will also consider distributed consensus-based UIO in our future work.

REFERENCES

[1] W. Zeng and M.-Y. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems," *IEEE transactions on cybernetics*, vol. 44, no. 11, pp. 2038–2049, 2014.

[2] X. Liu, X. Gao, and J. Han, "Distributed fault estimation for a class of nonlinear multiagent systems," *IEEE transactions on systems, man, and cybernetics: systems*, vol. 50, no. 9, pp. 3382–3390, 2018.

[3] S. Li, Y. Chen, and P. X. Liu, "Distributed fault detection and dynamic event-triggered consensus for heterogeneous multiagent systems under deception attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 8, pp. 3294–3304, 2023.

[4] S. X. Ding, *Model-based fault diagnosis techniques: design schemes, algorithms, and tools*. Springer Science & Business Media, 2008.

[5] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," *International Journal of control*, vol. 63, no. 1, pp. 85–105, 1996.

[6] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE transactions on cybernetics*, vol. 44, no. 11, pp. 2024–2037, 2014.

[7] J. G. Oxley, *Matroid theory*. Oxford University Press, USA, 2006, vol. 3.

[8] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, 2011.

[9] J. Lee, M. Sviridenko, and J. Vondrák, "Submodular maximization over multiple matroids via generalized exchange properties," *Mathematics of Operations Research*, vol. 35, no. 4, pp. 795–806, 2010.