Distributed Anomaly Detection and Estimation over Sensor Networks: Observational-Equivalence and \( Q \)-Redundant Observer Design

Mohammadreza Doostmohammadian, Themistoklis Charalambous, Senior Member, IEEE

Abstract—In this paper, we study stateless and stateful physics-based anomaly detection scenarios via distributed estimation over sensor networks. In the stateful case, the detector keeps track of the sensor residuals (i.e., the difference of estimated and true outputs) and reports an alarm if certain statistics of the recorded residuals deviate over a predefined threshold, e.g., \( \chi^2 \) (Chi-square) detector. Instead, only instantaneous deviation of the residuals raises the alarm in the stateless case without considering the history of the sensor outputs and estimation data. Given (approximate) false-alarm rate for both cases, we propose a probabilistic threshold design based on the noise statistics. We show by simulation that increasing the window length in the stateful case may not necessarily reduce the false-alarm rate. On the other hand, it adds unwanted delay to raise the alarm. The distributed aspect of the proposed detection algorithm enables local isolation of the faulty sensors with possible recovery solutions by adding redundant observationally-equivalent sensors. We, then, offer a mechanism to design \( Q \)-redundant distributed observers, robust to failure (or removal) of up to \( Q \) sensors over the network.

Index Terms—Anomaly detection, networked estimation, observational-equivalence, \( q \)-redundant observability

I. INTRODUCTION

The recent advancements in wireless communication, high-performance networking, sensing, and processing devices, along with cloud-computing and Internet-of-Thing (IoT) [1], [2] have motivated localized (or distributed) estimation over sensor networks. Such localized setup, further, mandates distributed detection mechanisms to find possible anomalies (faults, failures, or malicious attacks) locally, with potential large-scale applications from social networks [3] to Cyber-Physical Energy Systems (CPES) [4], [5]. Such distributed methods are privileged with no single node of failure and outperform existing centralized detection [6]–[9].

The existing distributed methods either require (i) local system observability in the neighborhood of every sensor via high-traffic communication network with large quantity of data-transfer [2], or (ii) fast data-sharing and processing units to perform many iterations of consensus and communication between every two samples of system dynamics (double time-scale) [10], [11]. In this work, similar to [12]–[14], we consider single time-scale distributed estimation (i.e., iterations at the same time scale of system dynamics) with no assumption on local system observability at any sensor [4], [15] to relax the networking, communication, and computational needs. A challenge is to build distributed estimation networks robust to faults, anomalies, and even cyber-attacks. Such detection and mitigation techniques are wide-spread in centralized setup [16]. Some works propose preventive mechanisms as in privacy-preserving [17], and resilient estimation [18], [19], while many other use detection mechanisms, e.g., observer-based (or predictive) fault detection and isolation (FDI) [8], [9]. Machine learning and binary classification algorithms (e.g., support-vector-machine [20]) are also used to generate decision boundaries separating normal space of system states from abnormal space (operating with fault or anomaly) [7]. Graph-theoretic methods via structured systems theory are also adopted for generic design of detection/mitigation protocols irrespective of numerical parameter values and only based on system structure [21], [22]. What missing in the literature is a distributed algorithm to localize the detection, in both stateful and stateless setups, along with network design for redundant distributed observability (distributed fault-tolerant models).

Main contributions: We propose a local mechanism to detect possible bias/anomaly in system output while performing single time-scale distributed estimation. We design probabilistic detection thresholds in both stateless and stateful scenarios, define the false-alarm (false-positive) rate (FAR) and false-negative rate for each case, and compare the performance of both solutions in terms of FAR (and delay in raising the alarm). Further, in contrast to the full-rank model in [3], [12], this work considers distributed detection on (possibly) rank-deficient systems, known to require more information-sharing over the distributed estimation networks [15]. We specifically use constrained LMI gain design to isolate (faulty) sensor residuals. Another contribution is to design \( Q \)-redundant distributed observers, robust to failure or removal of any \( Q \) (failed or faulty) sensors. Using graph-theory (structural methods), we first define the set of observationally-equivalent sensors/state-outputs using strongly-connected-components (SCCs) and contractions in the system digraph. Then, using \( k \)-vertex-connected (or \( k \)-connected) graphs [23], we propose sensor-network structures resilient to \( Q \) sensor removals such that the remaining sensor-network successfully tracks the underlying system (which is not necessarily observable in the neighborhood of any sensor). The proposed algorithms are of polynomial-order complexity.

Paper organization: the problem is set up in Section II. The distributed detection mechanism and \( Q \)-redundant observer are proposed in Section III and IV. The simulations and conclusion are given in Section V and VI.
II. The Framework

A. System model

In this paper, we consider LTI systems in the form,
\[ x(k + 1) = Ax(k) + ν(k), \]
with \( k \) as the time index, \( A \) as the system matrix (possibly rank-deficient), \( x \in \mathbb{R}^n \) as the column-vector of states, i.e., \( x = [x_1; \cdots; x_n] \), and \( ν \sim \mathcal{N}(0, Σ_ν) \) as the Gaussian noise. The output vector at time \( k \) is in the form,
\[ y(k) = Cx(k) + ζ(k) + f(k), \]
with \( y = [y_1; \cdots; y_N] \in \mathbb{R}^N \), \( ζ \sim \mathcal{N}(0, Σ_ζ) \) as the output noise (with diagonal \( Σ_ζ \)), and \( f \in \mathbb{R}^N \) as the additive bias to the outputs (due to faults or anomalies) defined as,
\[
\begin{cases}
  f_k(k) = 0 & \text{no-fault at output } i \\
  f_k(k) \neq 0 & \text{faulty output } i
\end{cases}
\]
Without loss of generality, in this paper, we assign every sensor \( i \) with one state-output \( y_i \). Given the structural representation of \( A, C \) matrices (i.e., the system digraph \( \mathcal{G}_A \)), sufficient conditions for structural (or generic) \((A, C)\)-observability are given in [15], [24]. Such structural methods imply observability for almost all numerical values of non-zero system parameters. This is referred to as the linear-structure-invariant (LSI) model, where the structure is fixed and the non-zero entries in \( A \) and \( C \) can take almost any value (with non-admissible parameter values lying on an algebraic subspace with zero Lebesgue measure) [15].

B. Distributed consensus-based estimation

We consider a distributed estimation framework, where the (group of) sensors estimate the system locally via information-sharing over a sensor network to gain distributed observability (as defined later in Lemma 1). The following distributed estimator in single time-scale, proposed in [15], is considered at sensor \( i \).

\[ \hat{x}_i(k|k−1) = \sum_{j \in N_α(i)} W_{ij} A \hat{x}_j(k−1|k−1), \]
\[ \hat{x}_i(k|k) = \hat{x}_i(k|k−1) + K_i \sum_{j \in N_α(i)} C_j \left( y_j(k) − C_j^T \hat{x}_i(k−1|k−1) \right), \]
where \( \hat{x}_i(k|k−1) \) and \( \hat{x}_i(k|k) \) denote the priori and posteriori estimates via the received data up to time \( k−1 \) and \( k \), respectively. \( K_i \) is the local gain (to be designed), and \( N_α(i) \) and \( N_β(i) \) denote the in-neighborhood respectively over networks \( \mathcal{G}_α \) and \( \mathcal{G}_β \) (defined in Lemma 1), with 0-1 matrix \( U = [U_{ij}] \) and row-stochastic matrix \( W = [W_{ij}] \). Recall that \( N_α(i) \) includes the so-called \( α \)-sensors with outputs of rank-deficient part of the system [15], [21], where for \( j \in N_α(i) \) the entry \( U_{ij} = 1 \). The following assumption distinguishes this work from many literature on single time-scale distributed estimation and observer-based detection.

Assumption 1: The pair \((A, C)\) is observable and the pair \((A, C_j∈N_α(i))\) (with \( C_j∈N_α(i) \) representing outputs in \( α \)-neighborhood of \( i \)) is not necessarily observable at any sensor \( i \). In other words, we assume global observability at the group of all sensors and no local observability in the neighborhood of any sensor.

Remark 1: The proposed single time-scale protocol, similar to [12]–[14], is more suitable for large-scale, as compared to double time-scale methods [10], [11], in terms of needed communication traffic and computation loads on sensors. This is because, in the latter, sensors perform a large number of consensus/data-sharing iterations between steps \( k \) and \( k+1 \) of system dynamics, in contrast to only 1 iteration in single time-scale methods. See details in [4], [12], [15].

Define the estimation error as \( e_i(k) = \hat{x}_i(k|k) − x(k) \) and \( e = [e_1, \cdots, e_N] \). The error dynamics under (4)–(5) is,
\[ e(k+1) = (W ⊗ A)e(k) − KD_C(W ⊗ A)e(k) + η(k+1), \]
\[ η(k+1) = (I − KD_C)I_N ⊗ ν(k) − KD_Cζ(k+1) + f(k+1). \]
with \( η(k+1) \) containing the noise and fault terms, \( nN \times nN \) matrices \( D_C = \text{diag}[U_{ij}, C_j^T] \) and \( KD_C \), \( \hat{A} \), are cumulative LTI dynamics with system matrix \( \hat{A} \), where \( ρ(\hat{A}) \) determines the error stability (with \( ρ(·) \) as the spectral radius). Following the Kalman stability theorem, one can design block-diagonal gain matrix \( K = K_o ⊗ K _c = \text{diag}[K_i] \) (with \( K_c = I_N ⊗ I_{n×n}, I_N \) and \( I_{n×n} \) respectively as identity and ones matrix of size \( N, n \)) to stabilize [6] if the pair \((W ⊗ A, D_C)\) is observable. This is referred to as the distributed observability, with the sufficient conditions discussed in the next lemma.

Lemma 1 ([15]): The pair \((W ⊗ A, D_C)\) is observable if (i) \( \mathcal{G}_β \) is strongly-connected, and (ii) every \( α \)-sensor is a hub of \( \mathcal{G}_α \), where every sensor \( i \) with a system-output recovering structural rank-deficiency \( \rho(\cdot) \) is regarded as an \( α \)-sensor.

Then, the block-diagonal gain matrix \( K \) can be designed, e.g., via the LMI in [15], [26], such that the error dynamics is Schur stable, i.e., \( ρ(\hat{A}) < 1 \) for general (possibly unstable) \( A \). Define the steady state error variance as \( Σ_e = \lim_{k→∞} E(e_i(k)|e_i(k)) \). It is shown in [15], [26] that \( \lim_{k→∞} E(e_i(k)) = 0 \), and,
\[ ||Σ_e||_2 = \frac{a_1 N ||Σ_e||_2 + a_2 ||Σ_ζ||_2}{1 − b^2}, \]
with \( b := ||(W ⊗ A) − KD_C(W ⊗ A)||_2 < 1, a_1 := ||I_N − KD_C||_2^2, a_2 := ||K||_2^2, \)
\[ Σ_ζ := \text{diag}[\sum_{j \in N_β(i)} \sum_{j \in N_β(i)} C_j^2 Σ_j], \]
where \( Σ_ζ \) denotes the \( j \)th diagonal entry of \( Σ_ζ \).

III. MAIN RESULTS: LOCAL DETECTION OF ANOMALIES

A. Stateless Detector

Given the error dynamics (6)–(7), define the residual of sensor \( i \) (including possible anomaly/bias \( f_i \)) at time \( k \) as,
\[ r_i(k) = y_i(k) − C_i \hat{x}_i(k|k) = C_i e_i(k) + ζ_i(k) + f_i(k), \]
\[ = C_i \hat{A} e_i(k−1|k) + C_i \hat{N}_i(k) + ζ_i(k) + f_i(k). \]

1Later in Section IV, using the system graph representation, an \( α \)-sensor is defined as the sensor with output of an state node in a contraction component. We refer interested readers to [25] for more details.
Algorithm 1: Constrained iterative LMI gain design

1. Input: matrices $A$, $W$, $U$, $C$, scale factor $\epsilon$
2. Calculate $D_C = \text{diag}(U_jC_jC^T_j)$;
3. If $(W \otimes A, D_C)$ is not observable then
   Terminate;
4. Else
   Iteratively solve for $\hat{A} = W \otimes A - K D_C (W \otimes A)$
   $$\min \text{ trace}(XY)$$
   subject to $X, Y > 0$,
   $$K \leftarrow K \circ K$$
   $$\begin{pmatrix} X & \hat{A}^T \\ \hat{A} & Y \end{pmatrix} > 0,$$
   $$\begin{pmatrix} X & I \\ I & Y \end{pmatrix} > 0,$$
   $$|C_i K_i C^T_j| / (|1 - C_j K_j C^T_i|) < \epsilon, \forall j \in \mathcal{N}_\alpha(i), j \neq i$$
5. Output Block-diagonal gain matrix $K = K \circ \mathcal{K}$;

with
$$\zeta_i(k) + f_i(k) + C_i n_i(k) = \zeta_i(k) + f_i(k) + C_i \nu(k - 1)$$
$$- C_i K_i \sum_{j \in \mathcal{N}_\alpha(i)} (C^T_j \zeta_j(k) + C^T_j f_i(k) + C_j^T C_j \nu(k - 1)) \quad (10)$$

In steady-state (large enough $k$), the noise and (non-zero) fault terms in (10) mainly value the residual of sensor $i$. From (10), other than bias $f_i$, any fault in the $\alpha$-neighborhood of sensor $i$, say $f_j, j \in \mathcal{N}_\alpha(i)$, also appears in $r_i(k)$. This makes the fault isolation more challenging as compared to the full-rank system models [3], [12] in which the fault isolation more challenging as compared to the full-rank system models [3], [12] in which $\mathcal{N}_\alpha(i) = \{i\}$. To overcome this and isolate the faults on $j \in \mathcal{N}_\alpha(i), j \neq i$, from (10), we constrain the gain matrix $K_i$ such that
$$|C_i K_i C_j| \leq \epsilon |1 - C^T_j K_j C_j|, \forall j \in \mathcal{N}_\alpha(i), j \neq i \quad (11)$$
with $\epsilon < 1$ as a design constant, implying that the fault-related term $C^T_i K_i C_j f_j$ in the residual $r_i(k)$ due to fault $f_j$ is down-scaled by $\epsilon$ as compared to the fault-related term in $r_j(k)$ (of $\alpha$-sensor $j$ itself). The constraint (11) helps to isolate possible faults at $\alpha$-sensors in rank-deficient systems via Algorithm 1 as the modified version of the LMI gain design in [12]. This algorithm can be run either once centralized offline with $K_i$s given to the nodes after termination or iteratively over $k$. From (5) and results in [12], [27], one can define the confidence intervals for $r_i(k)$. First, note that from (9) for the case of no anomaly/fault $f_i(k) = 0, \forall i$ and
$$ \Sigma_r^i \leq \frac{|C_i||\Sigma_\epsilon||2\Sigma_\epsilon||2}{N} + \Sigma_\zeta^i$$
where, assuming one state measurement by every sensor $i$, $|C_i|^2 = |C_i|$. Then, the probability that the residual lies in the confidence interval $|r_i(k)| \leq \kappa \Sigma_r^i$ is erf($\sqrt{2}$) with erf($\cdot$) as the Gauss error function. One can similarly claim that the probability of $|r_i(k)| \geq \kappa \Sigma_r^i$ is $1 - \text{erf}(\sqrt{2})$ for zero additive bias $f_i(k) = 0$. Define the probabilistic threshold $\theta_p = \kappa \Sigma_r^i$. Then, the detection logic in this paper is as follows: for given FAR (or false-positive probability) $p$ define the threshold $\theta_p$ with $\kappa = \sqrt{2}\text{erf}^{-1}(1-p)$. If $|r_i(k)| \geq \theta_p$ raise the anomaly detection alarm (associated with FAR $p$).

Recall that we use absolute residual $|r_i(k)|$, and, thus, folded Gaussian distribution, i.e., to fold-over the probability mass to the RHS of 0 axis by taking the absolute value. Similarly, the probability of false negative can be defined as,
$$p = \frac{1 - \text{erf}(\kappa/\sqrt{2})}{2} - \frac{1 - \text{erf}(3\kappa/\sqrt{2})}{2} = \frac{\text{erf}(3\kappa/\sqrt{2}) - \text{erf}(\kappa/\sqrt{2})}{2} \quad (13)$$

For $\kappa \geq 2$, we have $1 - \text{erf}(3\kappa/\sqrt{2}) = 2e^{-10}$ and one can approximate $p$ by $\frac{\kappa}{2}$. This is better explained in Fig. 1. This detection logic uses the instant value of the $r_i(k)$ at every time $k$ with no use of residual history, known as the stateless mechanism. Next, we consider residual history for anomaly detection, which is known as the stateful mechanism.

B. Stateful Detector

Define distance measure $i^T(k)$ as,
$$i^T_r(k) = \sum_{m=k-T+1}^{k} \frac{r_i(m)^2}{\Sigma_r}. \quad (14)$$
over a sliding time-window of length $T$. It is known that the summation of squared random variables from normal distribution (i.e., $r_i(m)^2$) follows the so-called Chi-squared distribution with $T$ degrees of freedom (denoted by $\chi^2_T$) [3], [16], [28], where $\mathcal{E}(i^T_r) = T$. Following the same line of reasoning as in the stateless case, the probabilistic threshold on the variable $i^T_r$ (for given FAR $p$) can be defined as,
$$\theta_r^T = 2\Gamma^{-1}(1-p, \frac{T}{2}) \quad (15)$$
where $\Gamma^{-1}(\cdot, \cdot)$ denotes the inverse regularized lower incomplete gamma function. Weighted distance measure [6]
further can be considered to put more weights on the normalized residuals and less on the far past residuals as
\[
\tau_i(k) = \sum_{m=k-T+1}^{k} \frac{\mu^{k-m} \gamma_i(m)^2}{\gamma_i(k)}, \quad (16)
\]
with \(0 < \mu \leq 1\) as the weight factor. \(\tau_i\) is referred to as the weighted sum of Chi-squared distributions \([28]\). Although, \(\chi^2\)-distribution is typically defined for positive integer \(T\), one can find similar results for the weighted \(\chi^2\) given by \(16\) \([28]\), with the expected value of \(\tau_i\) and the probabilistic thresholds (for a pre-specified FAR \(p\)) similar to \(15\).

\[
\mathbb{E}(\tau_i) = \frac{1 - \mu^T}{1 - \mu}, \quad \theta_p^T = 2\Gamma^{-1}\left(1 - p, \frac{1 - \mu^T}{2} - 2\mu\right) \quad (17)
\]

For the stateful detectors \(15\) and \(17\), the FAR is a function of \(T\) and \(\mu\) using the CDF of the \(\chi^2\)-distribution,

\[
p = 1 - \frac{\gamma(\frac{T}{2}, \frac{T}{2})}{\Gamma(\frac{T}{2})}, \quad p = 1 - \frac{\gamma(\frac{T}{2}, \frac{1 - \mu^T}{2} - 2\mu)}{\Gamma(\frac{1 - \mu^T}{2} - 2\mu)} \quad (18)
\]

with \(\gamma(\cdot, \cdot)\) as the lower incomplete gamma function. Our fault detection logics are summarized in Algorithm 2 with either stateless (first \(i.e.\)) or stateful detection (second \(i.e.\)).

**Remark 2:** For the stateful case, longer time-window \(T\) results in less FAR; however, it also increases the false alarm delay [16]. A similar statement holds for the weight factor \(\mu\); greater \(\mu\) results in lower FAR and more-delayed alarm. In general, there is a trade-off between detection accuracy (lower FAR via increasing \(T\) and \(\mu\)) and detection delay in raising the alarm; see examples in Section [5].

**Remark 3:** The proposed detection logic in Algorithm 2 is localized at every sensor \(i\) with no need of centralized decision making. This is more feasible in large-scale applications as compared to the centralized detection methods \([7]-[9]\).

**IV. Q-REDUNDANT DISTRIBUTED OBSERVER DESIGN BASED ON STRUCTURAL OBSERVATIONAL EQUIVALENCE**

In this section, we provide Q-redundant version of the distributed estimator \([4]-[5]\) such that it tolerates removal (or isolation) of any \(Q\) (faulty) sensors while holding distributed observability over the remaining sensor-network. Thus, the other sensors can locally estimate the system and detect possible output bias/anomaly. This problem is twofold: (i) it provides sufficient outputs such that after removal of up to \(Q\) rows of matrix \(C\), the pair \((A, C)\) remains structurally observable (known as Q-redundant observability \([19]\)), and (ii) designs Q-redundant communication network such that the conditions in Lemma [1] hold after removing \(Q\) sensors and cutting their linking over the network. We address these via the notion of observational-equivalence \([25], [29]\).

**A. Q-redundant observability**

Given an observable pair \((A, C)\), two outputs \(y_i = C_i x\) and \(y_j = C_j x\) are observationally-equivalent if losing either of the two does not affect system observability, while removing both makes the system unobservable. Let \(C_i\) denote the output matrix after removing the row \(C_i\) from \(C\) (i.e., removing sensor \(i\)). Then, for observationally equivalent sensors/outputs \(i, j\), \((A, \overline{C_i})\) and \((A, \overline{C_j})\) are observable, but \((A, \overline{C_{ij}})\) is not observable. Consider the system digraph \(G_A = \{V, E\}\) with set \(V = \{1, \ldots, n\}\) denoting the state nodes and link set \(E\) denoting the state interactions. Define a contraction, \(C_i\), as the set of nodes such that \(|N(C_i)| < |C_i|\), where \(N(C_i) = \{j|(i, j) \in E, i \in C_i\}\) \([25], [30]\). Define an SCC, \(S_i\), as the set of nodes \(i, j \in V\) such that \(i \rightarrow\) and \(j \rightarrow\) are a parent SCC is, then, defined as an SCC with no outgoing link to any other SCC \([25]\). Output of parent SCCs are known to recover the output-connectivity of \(G_A\), and output of contractions are known to recover the cyclicity of \(G_A\) and rank of the system matrix \(A\) \([25]\).

**Lemma 2 ([15], [24]):** Given system digraph \(G_A\), outputs of one state node in every parent SCC \(S_i\) and every contraction \(C_i\) are sufficient for structural \((A, C)\)-observability, i.e., to satisfy Assumption [1].

The above lemma implies that the set of state nodes in a contraction \(C_i\) and a parent SCC \(S_i\) in \(G_A\) are observationally equivalent. In this direction, \(Q + 1\) different state-outputs from every contraction and parent-SCC are sufficient for Q-redundant observability. We assign these outputs to \(Q + 1\) sensors. Then, removing any \(Q\) sensors, the remaining ones include (at least) one output from every \(S_i\) and \(C_i\). Thus, from Lemma [2] the pair \((A, \overline{C_Q})\) (with \(\overline{C_Q}\) as the output matrix after removal of any \(Q\) rows) remains observable.

**B. Q-redundant distributed observer**

Given the outputs and sensors for Q-redundant observability, this section provides the Q-redundant distributed observer. Following Lemma [1] we improve the network-connectivity of \(\overline{G}_\beta\) and \(\overline{G}_\alpha\) to gain Q-redundant \((W \otimes A, D_C)\)-observability as follows,

1) Design \(\overline{G}_\beta\) to be Q-vertex-connected, e.g., via computationally-efficient algorithms in \([31]\). Recall that a Q-vertex-connected graph remains strongly-connected after cutting any Q (sensor) nodes from the network.

2) For the hub-network \(\overline{G}_\alpha\), following Lemma [1] every \(\alpha\)-sensor \(i\) (say \(\alpha_1\)) as a network hub, directly shares its
output with every other sensor $j$ not observationally equivalent with $i$, (all other sensors except $\alpha_2$). The above connectivity ensures that every sensor directly links from $Q + 1$ set of $\alpha$-sensors and $Q + 1$ paths to and from other sensors. Then, protocol (4)-(5) over these $Q$-redundant networks $G_{\beta}$ and $G_{\alpha}$ can tolerate failure/isolation of any $Q$ sensors without losing distributed observability over the network (from Lemma 2), i.e., a $Q$-redundant distributed estimator. In similar setup, $\bar{Q}$-edge-connectivity can be used for survivable network design [32] resilient to link removal.

C. Illustrative Example

To illustrate the $Q$-redundant results, consider the system digraph $G_A$ in Fig. 2 (Left), containing three parent SCCs $S_1 = \{x_1, x_2, x_3\}, S_2 = \{x_6, x_7, x_8\}, S_3 = \{x_9, x_{10}\}$ and one contraction $C_1 = \{x_4, x_5, x_3, x_7, x_9\}$. We aim to design a 1-redundant distributed observer, i.e., an observer robust to removal/isolation of any one output sensor. Following Section IV-A taking 4 outputs from $\{x_1, x_5, x_6, x_9\}$ the system digraph is structurally observable. By adding another set of 4 outputs from states $\{x_2, x_4, x_7, x_{10}\}$, the system is (structurally) 1-redundant observable. Following Section IV-B we design $G_{\beta}$ as the 2-vertex-connected graph and $G_{\alpha}$ as a hub-network shown in Fig. 2 (Right) to gain 1-redundant distributed observability. Then, in protocol (4)-(5), matrix $W$ (as the adjacency of $G_{\beta}$) is designed row-stochastic; for example, by considering random positive non-zero entries, and then, dividing each row by the row-sum. Matrix $U$ is the 0-1 adjacency matrix of $G_{\alpha}$. Then, block-diagonal $K$ can be designed via Algorithm 1. This distributed observer is robust to failure of 1 sensor, or, more precisely, to failure of 1 output from every parent SCC and contraction.

V. Simulation

For simulation, we consider the same example in Section IV-C representing a rank deficient system of $n = 10$ nodes with non-zero entries as the given link weights in Fig. 2 (Left). We consider $N = 4$ outputs from $\{x_1, x_6, x_9, x_5\}$ associated with sensors $\{\beta_1, \beta_2, \beta_3, \alpha_1\}$, satisfying Lemma 2 and Assumption 2. Network $G_{\alpha}$ includes direct links (with weight 1) from $\alpha_1$ to $\beta_1, \beta_2, \beta_3$, and $G_{\beta}$ is considered as a directed cycle $1 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$ with random row-stochastic link weights. The non-zero entries of the output matrix $C$ are set equal to 1. The gain matrix $K$ is designed via Algorithm 1 with $\epsilon = 0.14$. The mean-square error (MSE) under the proposed protocol (4)-(5) is bounded steady-state as shown in Fig. 3 (TopLeft) with $\nu \sim \mathcal{N}(0,0.01)$ and $\zeta \sim \mathcal{N}(0,0.01)$. To check the performance in the presence of faults or anomalies, we consider two bias $f_{\beta_1}(k \geq 60) = 2$ and $f_{\alpha_1}(k \geq 30) \sim \mathcal{N}(2,0.5)$. Our localized (or distributed) detection logic follows algorithm 2 for FAR $p = 32\%, 5\%, 0.3\%, 0.01\%$. For the stateless case, the residual $r_i$ at the faulty sensors $\beta_1$ and $\alpha_1$ are between the thresholds $\theta_{32\%}$ and $\theta_{5\%}$. Therefore, the local detector declares the fault probability of more than 68% and less than 95% at these sensors and no fault at the other two. For the stateful case, considering the distance measure $t_i^2$ in (14) with $T = 10$-steps and thresholds (15), the local detector declares higher probabilities of 99.7% and 99.99% respectively at sensors $\alpha_1$ and $\beta_1$, however with certain delay (about 10-steps delay as in Fig. 3 (BelowLeft)). One can reduce this alarm delay by weighting the residual history by $\mu$ as in (16), however via thresholds of higher FAR. For $\mu = 0.75$, the weighted distance measure $r_i$ and the thresholds (17) are shown in Fig. 3 (BelowRight). The detection probability with this logic is approximately 99.7% at sensor $\alpha_1$ and 95% at sensor $\beta_1$, with alarm delay reduced to 7 time-steps.

Next, we compare the performance of the stateful detectors for different values of $T$ and $\mu$. Consider a constant fault resulting in biased residual $r_i^2 = 2\Sigma_i$. For the stateless
As future research, one may consider possible time-delay in Fig. 4. (Left) FAR increases for different $T$ for different detector, the associated FAR is equal to 5%. For the stateful case, the threshold’s FAR can be defined via [18], shown in Fig. 4 (Left) for different $T$ and $\mu$ values. Clearly, for greater $\mu$, the FAR is lower; however, as discussed in Remark 2 and Fig. 4, large $\mu$ values result in longer delays to raise the alarm. Further, for smaller values, e.g., $\mu = 0.5, 0.6$, the FAR is almost constant for $T \geq 8$ and, thus, longer time windows do not improve the FAR. Fig. 4 (Right) shows the FAR versus $\frac{\sigma^2}{\Sigma}$ for different $\mu$ values (for $T = 8$). It is clear that as $\mu \rightarrow 1$ the FAR decreases (with $\mu = 1$ giving [15]).

VI. CONCLUSION AND FUTURE WORKS

Stateful and stateless local detection mechanisms over distributed estimation networks are considered with a trade-off between alarm delay and FAR. The stateful case shows lower FAR with possibly delayed alarm over long sliding time windows. The solutions are of polynomial-order complexity; for example, system digraph decomposition into parent SCCs and contractions is of complexity $O(n^{2.5})$ [30]. As future research, one may consider possible time-delay in the communication network [33], [34].

REFERENCES

[1] M. Doostmohammadian and H. R. Rabiee, “On the observability and controllability of large-scale IoT networks: Reducing number of unmatched nodes via link addition,” IEEE Control Systems Letters, vol. 5, no. 5, pp. 1747–1752, 2021.

[2] Y. Chen, S. Kar, and J. M. F. Moura, “The internet of things: Secure distributed inference,” IEEE Signal Process. Mag., vol. 35, no. 5, pp. 64–75, 2018.

[3] M. Doostmohammadian, T. Charalambous, M. Shafei-khah, N. Meskin, and U. A. Khan, “Simultaneous distributed estimation and attack detection/isolation in social networks: Structural observability, kronecker-product network, and chi-square detector,” in IEEE International Conference on Autonomous Systems, 2021, pp. 344–348.

[4] U. A. Khan and M. Doostmohammadian, “A sensor placement and network design paradigm for future smart grids,” in IEEE Workshop on Computational Adv. in Multi-Sensor Adap. Proc., 2011, pp. 137–140.

[5] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, “Modeling of future cyber–physical energy systems for distributed sensing and control,” IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol. 40, no. 4, pp. 825–838, 2010.

[6] D. Ummston, Tuning of anomaly detectors in the presence of sensor attacks, Ph.D. thesis, KTH Royal Institute of Technology, 2019.

[7] M. Abbaszadeh, “System and method for anomaly and cyber-threat detection in a wind turbine,” 2019, US Patent App. 15/988,515.

[8] M. Davoodi, N. Meskin, and K. Khorasani, “Event-triggered multiobjective control and fault diagnosis: A unified framework,” IEEE Trans. on Industrial Informatics, vol. 13, no. 1, pp. 298–311, 2016.

[9] M. Navi, N. Meskin, and M. Davoodi, “Sensor fault detection and isolation of an industrial gas turbine using partial adaptive KPCA,” Journal of Process Control, vol. 64, pp. 37–48, 2018.

[10] X. He, X. Ren, H. Sandberg, and K. H Johansson, “How to secure distributed filters under sensor attacks?” IEEE Transactions on Automatic Control, arXiv preprint arXiv:2004.05409, 2021.

[11] S. Battilotti, F. Cacace, and M. d’Angelo, “A stability with optimality analysis of consensus-based distributed filters for discrete-time linear systems,” Automatica, vol. 129, pp. 109589, 2021.

[12] M. Doostmohammadian and N. Meskin, “Sensor fault detection and isolation via networked estimation: Full-rank dynamical systems,” IEEE Trans. Control of Net. Systems, vol. 8, no. 2, pp. 987–996, 2021.

[13] L. Wang, J. Liu, A. S. Morse, and B. D. O. Anderson, “A distributed observer for a discrete-time linear system,” in 58th IEEE Conference on Decision and Control, 2019, pp. 367–372.

[14] D. Marelli, M. Zamani, M. Fu, and B. Ninness, “Distributed kalman filter in a network of linear systems,” Systems & Control Letters, vol. 116, pp. 71–77, 2018.

[15] M. Doostmohammadian and U. Khan, “On the genericity properties in distributed estimation: Topological design and sensor placement,” IEEE J. of Sel. Topics in Signal Processing, vol. 7, no. 2, pp. 195–204, 2013.

[16] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, “A survey of physics-based attack detection in cyber-physical systems,” ACM Computing Surveys (CSUR), vol. 51, no. 4, pp. 1–36, 2018.

[17] A. I. Rikos, T. Charalambous, K. H. Johansson, and C. N. Hadjicostis, “Privacy-preserving event-driven quantized consensus: Average consensus,” in IEEE Conference on Decision and Control, 2020, pp. 6246–6253.

[18] A. Mitra, F. Ghawash, S. Sundaram, and W. Abbas, “On the impacts of redundancy, diversity, and trust in resilient distributed state estimation,” IEEE Transactions on Control of Network Systems, 2021.

[19] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, “Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors,” IEEE Transactions on Automatic Control, vol. 64, no. 3, pp. 1162–1169, 2018.

[20] M. Doostmohammadian, A. Aghiasi, T. Charalambous, and U. Khan, “Distributed support vector machines over dynamic balanced directed networks,” IEEE Control Systems Lett., vol. 6, pp. 738 – 763, 2021.

[21] M. Doostmohammadian and U. A. Khan, “Vulnerability of CPS inference to DoS attacks,” in 48th Annual Allerton Conference on Signals, Systems, and Computers, 2014, pp. 2015–2018.

[22] S. Gracy, J. Milošević, and H. Sandberg, “Security index based on perfectly undetectable attacks: Graph-theoretic conditions,” Automatica, vol. 134, pp. 109925, 2021.

[23] D. Guichard, “An introduction to combinatorics and graph theory,” Whitman College-Creative Commons, 2017.

[24] S. Pequito, S. Kar, and A. P. Aguiar, “A structured systems approach for optimal actuator-sensor placement in linear time-invariant systems,” in American Control Conference, 2013, pp. 6123–6128.

[25] M. Doostmohammadian and U. A. Khan, “Measurement partitioning and observational equivalence in state estimation in IEEE Conference on Acoustics, Speech and Signal Processing, 2016, pp. 4855–4859.

[26] U. A. Khan and A. Jadbabaie, “Coordinated networked estimation and control for uniformly observable nonlinear systems,” in 49th IEEE Conference on Decision and Control, Orlando, FL, Dec. 2011, pp. 2112–2117.

[27] U. A. Khan and A. Jadbabaie, “Collaborative scalar-gain estimators for sensor attacks/isolation in social networks,” in IEEE Conference on Decision and Control, 2021, pp. 367–372.

[28] A. Mitra, F. Ghawash, S. Sundaram, and W. Abbas, “On the impacts of redundancy, diversity, and trust in resilient distributed state estimation,” IEEE Transactions on Control of Network Systems, 2021.

[29] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, “Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors,” IEEE Transactions on Automatic Control, vol. 64, no. 3, pp. 1162–1169, 2018.

[30] M. Doostmohammadian and N. Meskin, “Sensor fault detection and isolation via networked estimation: Full-rank dynamical systems,” IEEE Control Systems Lett., vol. 6, pp. 738–763, 2021.

[31] M. Doostmohammadian and U. A. Khan, “Vulnerability of CPS inference to DoS attacks,” in 48th Annual Allerton Conference on Signals, Systems, and Computers, 2014, pp. 2015–2018.

[32] S. Gracy, J. Milošević, and H. Sandberg, “Security index based on perfectly undetectable attacks: Graph-theoretic conditions,” Automatica, vol. 134, pp. 109925, 2021.

[33] D. Guichard, “An introduction to combinatorics and graph theory,” Whitman College-Creative Commons, 2017.

[34] S. Pequito, S. Kar, and A. P. Aguiar, “A structured systems approach for optimal actuator-sensor placement in linear time-invariant systems,” in American Control Conference, 2013, pp. 6123–6128.