Minimal Structurally Overdetermined Sets Selection for Distributed Fault Detection

Hamed Khorasgani[1] **Gautam Biswas**[1] and **Daniel Jung**[2]
[1]Institute of Software Integrated Systems, Vanderbilt University, USA
e-mail: {hamed.g.khorasgani,gautam.biswas}@vanderbilt.edu
[2]Dept. of Electrical Engineering, Linkoping University, Sweden
e-mail: daner@isy.liu.se

Abstract

This paper discusses a distributed diagnosis approach, where each subsystem diagnoser operates independently without a coordinator that combines local results and generates the correct global diagnosis. In addition, the distributed diagnosis algorithm is designed to minimize communication between the subsystems. A Minimal Structurally Overdetermined (MSO) set selection approach is developed as a Binary Integer Linear Programming (BILP) optimization problem for subsystem diagnoser design. For cases, where a complete global model of the system may not be available, we develop a heuristic approach, where individual subsystem diagnosers are designed incrementally, starting with the local system MSOs and progressively extending the local set to include MSOs from the immediate neighbors of the subsystem. The inclusion of additional neighbors continues till the MSO set ensures correct global diagnosis results. A multi-tank system is used to demonstrate and validate the proposed methods.

1 Introduction

The Minimal Structurally Overdetermined (MSO) sets approach has been used extensively for designing model based fault detection and isolation (FDI) schemes for complex systems [Krysander *et al.*, 2008a; Krysander *et al.*, 2008b; Svard *et al.*, 2012]. However, for large complex systems such as aircraft and other transportation systems, manufacturing processes, supply chain and distribution networks, and power generation and the power grid it is becoming imperative to develop distributed approaches to monitoring and diagnosis to overcome the need for complete global models, while also addressing computational complexity and reliability problems for the diagnosers [Leger *et al.*, 1999; Shum *et al.*, 1988; Deb *et al.*, 1998; Lanigan *et al.*, 2011].

Unlike centralized approaches, distributed approaches are more reliable because they avoid single points of failure. In addition, they can reduce the problems of noise, corruption, and losses that can occur when transmitting signals from individual subsystems to a centralized fault diagnosis unit. Measurement noise and signal corruption can significantly affect diagnoser robustness and accuracy [Ferrari *et al.*, 2012]. Transmission delays not only increase detection time, but can also affect the order of detection, which can further affect diagnostic accuracy. Detection time is important for the safe and reliable operation of safety-critical systems. Faster fault detection and isolation enables accompanying fault tolerant control units to react in a timely manner, thus reducing damage and down time of systems [Roychoudhury *et al.*, 2009; Daigle *et al.*, 2007; Duarte Jr and Nanya, 1998; Rish *et al.*, 2005; Bregon *et al.*, 2014]. The computational intractability of building centralized diagnosers for the large systems is another important reason to develop distributed solutions for FDI problems.

In this paper, we formulate the distributed minimal structurally overdetermined set selection as a binary integer linear programming (BILP) problem [Wolsey, 1998]. The approach efficiently picks a minimal number of measurements from a subsystem and its neighboring subsystems to develop a local diagnoser for each subsystem of the larger, complex dynamic system. We start with an efficient algorithm designed by [Krysander *et al.*, 2008a] for finding minimally overdetermined sets of constraints to generate the minimal structurally overdetermined (MSO) sets for designing the diagnoser. Other researchers have employed binary integer programming and binary linear integer programming for optimal sensor placement for fault detection and isolation [Sarrate *et al.*, 2007; Rosich *et al.*, 2009]. In this paper, we utilize BILP for distributed MSO selection to facilitate an efficient distributed diagnosis approach.

Our method is designed in a way that the subsystem diagnosers, once designed can operate independently with no communication with the other subsystem diagnosers (other than a minimal number of shared measurements), but still provide globally correct diagnosis results. Unlike [Lafortune, 2007; Debouk *et al.*, 2000; Indra *et al.*, 2012] this method does not require the use of a centralized coordinator during on-line operations. Therefore, we avoid the single point-of-failure problem of centralized diagnosers. Our method assumes the availability of a global system model from which the set of MSOs for the system can be derived. The independent subsystem diagnosers are designed to minimize the sharing of measurements across subsystems, thus decreasing the cost, and increasing the reliability of the overall system diagnosis.

However, global models of a complex system are hard to construct and may not be readily available. Subsystems are often provided by different manufacturers, who are not willing to pass along all of the intellectual property associated with the subsystem to the system integrator. Therefore, to avoid the unrealistic assumption that the complete model of the complex system is available for subsystem diagnoser de-

sign, we propose a second algorithm that constructs the individual subsystem diagnosers without assuming the availability of a global model. The modified algorithm is computationally more efficient, but we cannot guarantee that the shared measurements between the subsystems is minimal globally (i.e., across the entire system).

The rest of this paper is organized as follows. The background material, definitions and the running example, a four-tank system, are presented in Section 2. The distributed diagnosis problem formulation is presented in Section 3. Algorithm 1 for distributed MSO set selection is described in Section 4. The heuristic modifications to Algorithm 1 given the global model is not available is presented in Section 5 as the incremental algorithm. Section 6 discusses the contributions of the paper in relation to previous work, and presents the conclusion of the paper.

2 Background

This section introduces the basic concepts associated with MSO set selection for structural diagnosis of dynamic systems. The system model S is defined as follows.

Definition 1 (System model)**.** *A system model S is a four-tuple: (V, M, E, F), where V is the set of variables, M is the set of measurements, E is the set of equations and F is the set of system faults.*

We use a configured four tank system, shown in Figure 1, as a running example throughout this paper to describe the problem, and to illustrate the algorithms for distributed MSO set selection. We assume each tank, and the outlet pipe to its right, constitute a subsystem. Therefore, this system has four subsystems. Two of the subsystems, 1 and 3, also have inflows into their tanks. We assume the subsystems are disjoint, i.e., they have no overlapping components. Associated with each subsystem are a set of measurements that are shown as encircled variables in the figure.

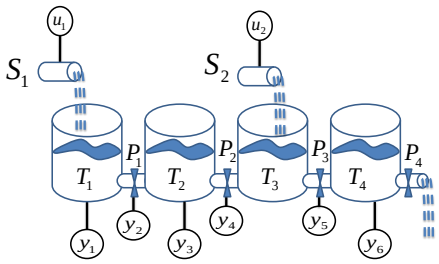

Figure 1: Running example: Four Tank System.

More generally, we assume the system, S has n predefined subsystems, $S_1, S_2, ...S_n$. Each subsystem model is defined as:

Definition 2 (Subsystem model)**.** *A subsystem model of system model S, S_i $(1 \leq i \leq k)$ is also a four-tuple: (V_i, M_i, E_i, F_i), where $V_i \subseteq V$, $M_i \subseteq M$, $E_i \subseteq E$ and $F_i \subseteq F$. Also, $S_1 \cup S_2 \cup ....S_k = S$.*

For illustration, the first subsystem in our running example is described by the following set of equations:

$$
\begin{aligned}
e_1 &: \dot{p}_1 = \frac{1}{C_{T1} + f_1}(q_{in1} - q_1) & e_4 &: q_{in1} = u_1 \\
e_2 &: q_1 = \frac{p_1 - p_2}{R_{P1} + f_2} & e_5 &: p_1 = y_1 \\
e_3 &: p_1 = \int \dot{p}_1 \, dt & e_6 &: q_1 = y_2.
\end{aligned}
\tag{1}
$$

Therefore, $E_1 = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ defines the set of equations, $V_1 = \{\dot{p}_1, p_1, p_2, q_{in1}, q_1\}$ defines the set of variables, $M_1 = \{u_1, y_1, y_2\}$ defines the set of subsystem measurements, and $F_1 = \{f_1, f_2\}$ defines the set of faults associated with this subsystem model.

Similarly, the second subsystem model is defined by the following equations:

$$
\begin{aligned}
e_7 &: \dot{p}_2 = \frac{1}{C_{T2} + f_3}(q_1 - q_2) & & \\
e_8 &: q_2 = \frac{p_2 - p_3}{R_{P2} + f_4} & e_{10} &: p_2 = y_3 \\
e_9 &: p_2 = \int \dot{p}_2 \, dt & e_{11} &: q_2 = y_4.
\end{aligned}
\tag{2}
$$

For this subsystem the set of equations is $E_2 = \{e_7, e_8, e_9, e_{10}, e_{11}\}$, the set of variable is $V_2 = \{\dot{p}_2, p_2, p_3, q_1, q_2\}$, the set of measurements is $M_2 = \{y_2, y_4\}$, and $F_2 = \{f_3, f_4\}$ is the set of faults.

In this paper, we assume there are no overlapping components among the subsystems. However, the subsystems may share variables at their interface. For example, the liquid flowrate at outlet pipe of subsystem $q_i = q_{i\prime}$, the liquid flowrate at input to connected tank $i + 1$.

Definition 3 (First Order Connected Subsystems)**.** *Two subsystems, S_i and S_j are defined to be first order connected if and only if they have at least one shared variable.*

In the running example, subsystems S_1 and S_2 are first order connected and their shared variables are $V_1 \cap V_2 = \{p_2, , q_1\}$. The two other subsystems in the running example are:

$$
\begin{aligned}
e_{12} &: \dot{p}_3 = \frac{1}{C_{T3}}(q_{in2} + q_2 - q_3) & & \\
e_{13} &: q_3 = \frac{p_3 - p_4}{R_{P3} + f_5} & e_{15} &: q_{in2} = u_2 \\
e_{14} &: p_3 = \int \dot{p}_3 \, dt & e_{16} &: q_3 = y_5.
\end{aligned}
\tag{3}
$$

$$
\begin{aligned}
e_{17} &: \dot{p}_4 = \frac{1}{C_{T4} + f_6}(q_3 - q_4) & e_{19} &: p_4 = \int \dot{p}_4 \, dt \\
e_{18} &: q_4 = \frac{p_4}{R_{P4}} & e_{20} &: p_4 = y_6.
\end{aligned}
\tag{4}
$$

In more general terms, ith order connected subsystem models are defined as follows.

Definition 4 (ith Order Connected Subsystems)**.** *Two subsystems, S_k and S_j are defined to be ith order connected if and only if there exists a subsystem model S_m that is $(i-1)th$ order connected to S_k, and is first-order connected to S_j, or S_m is $(i-1)th$ order connected to S_j, and is first-order connected to S_k .*

For example in the four tank system, S_1 and S_3 are second order connected because both of them are first order connected to S_2.

In this paper, we use MSO sets [Krysander *et al.*, 2008b] as the primary conceptual approach for fault detection and isolation. The formal definitions of Structurally Overdetermined (SO) and MSO sets are:

Definition 5. *(Structural Overdetermined Set) Consider a set of equations and its associated variables, measurements, and faults:* (E, V, M, F). *This set of equations is structurally overdetermined (SO) if the cardinality of the set* $\{E\}$ *is greater than the cardinality of set* $\{V\}$, *i.e.* $|E| > |V|$.

Definition 6. *(Minimal Structurally Overdetermined Set) A set of over determined equations is minimal structurally overdetermined (MSO) if it has no subset of structurally overdetermined equations.*

Consider subsystem S_1 of the four tank system in equation (1). Using the software developed by [Krysander *et al.*, 2008a], we can compute the only minimal structurally overdetermined set in this subsystem as $MSO_{11} = (E_{11}, V_{11}, M_{11}, F_{11})$, where $E_{11} = \{e_1, e_3, e_4, e_5, e_6\}$, $V_{11} = \{\dot{p}_1, p_1, q_{in1}, q_1\}$, $M_{11} = \{u_1, y_1, y_2\}$ and $F_{11} = \{f_1\}$. For the sake of brevity and simplification we simply say a specific equation, variable, measurement, or fault is a member of a MSO in the rest of the paper. For example, we say $f_1 \in MSO_{11}$.

MSOs represent the redundancies in the system and can form the basis for fault detection and isolation. Global and Local fault detectability are defined as:

Definition 7. *(Globally detectable fault) A fault* $f \in F$ *is globally detectable in system* S *if there is a minimal structurally overdetermined set* MSO_i *in the system, such that* $f \in MSO_i$.

Definition 8. *(Locally detectable fault) A fault* $f \in F_i$ *is locally detectable in subsystem* S_i *if there is a minimal structurally overdetermined set* MSO_i *in the subsystem that* $f \in MSO_i$.

Consider *Definition* 8 and equation (1). Fault f_1 is locally detectable because $f_1 \in MSO_{11}$ but f_2 is not locally detectable since there is no MSO in this subsystem that includes f_2. To detect f_2 locally, the diagnosis subsystem needs to include additional measurements. Global and Local fault isolability are defined as:

Definition 9. *(Globally isolable fault) A fault* $f_i \in F$ *is globally isolable from fault* $f_j \in F$ *if there exists a minimal structurally overdetermined set* MSO_i *in the system* S, *such that* $f_i \in MSO_i$ *and* $f_j \notin MSO_i$.

Definition 10. *(Locally isolable fault) A fault* $f_i \in F_i$ *is locally isolable from fault* $f_j \in F$ *if there exists a minimal structurally overdetermined set* MSO_i *in subsystem* S_i, *such that* $f_i \in MSO_i$ *and* $f_j \notin MSO_i$.

Note that if a fault f_i is locally detectable in a subsystem S_i, it is globally detectable too, and if a fault f_i is locally isolable from a fault f_j, it is globally isolable from f_j as well. The problem of MSO selection is presented as a binary integer linear programming (BILP) problem in this paper. BILP is a special case of the integer linear programming problem (ILP), where the unknowns to be solved for are binary variables.[1]

[1]See definition in Wikipedia: `https://en.wikipedia.org/wiki/Integer_programming`.

Definition 11. *(Binary integer linear programming problem (BILP)) A Binary integer linear programming problem is a special case of an integer linear programming (ILP) optimization problem in which some or all the unknown variables to be solved for are required to be binary, and the constraints in the problem and the objective function, like ILP, are linear.*

The mathematical formulation of BILP is as follows.

$$\begin{aligned} \min c^T x \\ Ax \leq b \\ \exists x_b \subset x \\ \forall x_k \in x_b \Rightarrow x_k \in \{0, 1\}, \end{aligned} \tag{5}$$

where vector c is the cost weights and matrix A and vector b define linear constraints, x represents the variables, and x_b represents the binary variables [Wolsey and Nemhauser, 2014].

3 Problem Formulation

Designing a set of distributed diagnosers that together have the same diagnosability as a centralized diagnoser is the focus of our work in this paper. In the ideal case, each subsystem includes sufficient redundancies, such that its set of MSOs is sufficient to detect and isolate all of its faults, F_i uniquely and unambiguously. In that case, we can associate an independent diagnoser D_i with each subsystem $S_i; 1 \leq i \leq k$, and each diagnoser operates with no centralized control, and no exchange of information with other diagnosers. If the independence among diagnosers does not hold, then the subsystems need to communicate some of their measurements to other subsystems to detect and isolate the faults. To address this problem in an efficient way, we derive an integrated approach to select a set of MSOs for each subsystem that guarantee full diagnosability and minimum exchange of measurements among subsystems.

Given subsystems, $S_i; 1 \leq i \leq k$, with a set of local fault candidates, F_i, such that $\bigcup_{i=1}^{k} F_i = F$. We may need to augment each subsystem with additional measurements that are typically acquired from the (nearest) neighbors of the subsystem, such that all of the faults associated with the extended model of this subsystem are detectable and isolable. In the worst case, all of the measurements from another subsystem may have to be included to make the current subsystem diagnosable. When such a situation occurs, we say the two subsystems are merged and represented by a common diagnoser, therefore, the total number of independent distributed diagnosers may be less than k.

Each MSO is sensitive to a set of faults and, therefore can be used to detect them and isolate them from the other faults in the system. For each subsystem S_i, our goal is to find a minimal set of MSOs that provide maximum detectability and isolability to that subsystem. A set of MSOs is minimal if there is no subset of MSOs that provides the same detectability and isolability. To achieve distributed fault diagnosis, we also want each subsystem to use the minimum number of measurements from the other subsystems. In other words, we want to minimize communication or the amount of data (measurements) to be transmitted between the subsystems. More formally, the problem for designing a diagnoser for a particular subsystem S_i can be described as follows:

Consider $\mathcal{MSO} = \{MSO_1, MSO_2, \ldots, MSO_r\}$ as the set of possible MSOs for the subsystem S_i. We need to develop an algorithm to select a minimal subset of $\mathcal{MSO}$ that guarantees maximal structural detectability and isolability for faults F_i associated with the subsystem, and include a minimum number of measurements from the other subsystems in the system to assure the equivalence of local and global diagnosability , i.e.,

$$\begin{array}{rl} \forall S_i; & 1 \leq i \leq k \\ Select & MSO_{Si} \subset \mathcal{MSO} \\ s.t. & \min\limits_{M_o \subseteq M} |M_o| \\ & D_i(M_i \cup M_o) = D_i(M), \\ & I_i(M_i \cup M_o) = I_i(M), \end{array} \tag{6}$$

where M_o represents the set of measurement we need to communicate to the subsystem S_i along with the set of measurements, M_i associated with the subsystem S_i. M represents the set of all measurements in the system. For a given set of measurements, X, $D_i(X)$ represents the set of detectable faults in F_i, and $I_i(X)$ represents the set of isolable faults in F_i from the system faults, F.

In the next section we formulate the problem as a BILP problem. Formulating the problem as a BILP, enables us to use a number of well-developed tools like branch and bound algorithms [Land and Doig, 1960] and branch and cut algorithms [Mitchell, 2002] to solve the problem. However, much like integer linear programming, the general BILP solution is exponential.

4 MSOs Selection for Distributed Fault Detection Using Global Model

In this section, we present our algorithm to select a minimal set of residuals for each subsystem of a system whose global model is available as a set of equations. In the next section, we modify this algorithm to make it applicable to much larger systems, where a compiled global model is not available.

For the situation in which the global model is known, M in equation (6) is the set of all system measurements. Assume we have l measurements in the system: $M = \{m_1, m_2, ..., m_l\}$. The measurements imply redundancies in the system model that form the basis for generating MSOs. Let us assume we can generate r MSOs given M: $\mathcal{MSO} = \{MSO_1, MSO_2, \ldots, MSO_r\}$. Our goal is to design an algorithm that selects $\mathcal{MSO}_i \subseteq \mathcal{MSO}$ in a way that we add a minimum number of measurements $M_o \subseteq M, M_i \cap M_o = \emptyset$, i.e., measurements from the system not belonging to subsystem i, to a subsystem to make all its faults globally diagnosable. Note that this is equivalent to the set covering problem and, therefore, any algorithm for finding the minimal measurements is exponential, in general. In the past, we have adopted heuristic search methods for solving this problem. Our approach for designing subsystem diagnosers used the Temporal Causal Graph (TCG) approach [Roychoudhury *et al.*, 2009]. In this paper, we formulate the search for minimal sensors as a BILP problem. The general formulation of BILP is presented in (5), and there are several tools available for solving this problem.[2]

To formulate the problem (6) as a BILP problem we define a binary variable $x(k)$: $1 \leq k \leq l$, for measurement m_k in the system as follows:

$$x(k) = \begin{cases} 1 & if \quad m_k \in M_i \cup M_o \\ 0 & if \quad m_k \notin M_i \cup M_o, \end{cases} \tag{7}$$

where M_o is the answer to problem (6). We also define $x(k+l)$: $1 \leq k \leq r$, for MSO MSO_k in the system as follows.

$$x(k+l) = \begin{cases} 1 & if \quad MSO_k \in \mathcal{MSO}_i \\ 0 & if \quad MSO_k \notin \mathcal{MSO}_i. \end{cases} \tag{8}$$

To minimize the number of measurements from the other subsystems, we develop the following cost function c as:

$$c(k) = \begin{cases} 0 & if \quad m_k \in M_i \\ 1 & if \quad m_k \in M \backslash M_i \\ 0 & if \quad l < k \leq l + r, \end{cases} \tag{9}$$

where l is the number system measurements and r is the number of MSOs in the system. Using the algorithm proposed in [Krysander *et al.*, 2008a] 165 MSOs are generated for the running example, the four tank system. Since there are 8 measurements in the system c is a vector with 173 elements for this example.

Consider subsystem S_i with local faults F_i and the set of system faults, F. Each local fault $f_j \in F_i$ has to be locally detectable. Given definition 8, we can guarantee local detectability of all the faults $f_j \in F_i$ with the following constraints in the optimization problem (5).

$$A(j,k) = \begin{cases} 0 & if & k < l \\ -1 & if & f_j \in MSO_{k-l} \\ 0 & otherwise. & \end{cases} \tag{10}$$

Note that l is the number of measurements in the system. By considering $b(j) = -1$ for $1 \leq j \leq g$, where g is the number of faults in F_i, we make sure that we have selected at least one MSO to detect each fault.

To address isolability requirement we follow the same procedure. To isolate $f_j \in F_i$ from any other fault in system, i.e., $f_h \in F$ we need to have:

$$A(j+g,k) = \begin{cases} 0 & k < l \\ -1 & f_j \in MSO_{k-l}, f_h \notin MSO_{k-l} \\ 0 & otherwise. \end{cases} \tag{11}$$

Setting $b(j) = -1$ for $g < j \leq g * h$, where h is the number of faults in the system, $h = |F|$, we make sure that there is at least one MSO to isolate each of the subsystem faults from the other faults in the system.

In addition to the constraints that guarantee maximum detectability and isolability for the distributed diagnosis system, we need a set of constraints that capture the relationship between the measurements and MSOs in the distributed diagnosis system. Using a MSO is equivalent to using the measurements that are included in the MSO, and we need to include this in the optimization problem. For example, consider MSO_{11}, it has three measurements $M_{11} = \{u_1, y_1, y_2\}$. Using MSO_{11} in a local diagnosis subsystem means we need to communicate these measurement streams to that subsystem to achieve global diagnosability for the

[2] For example, see `http://www.mathworks.com/help/optim/ug/mixed-integer-linear-programming-algorithms.html` in the Matlab™ linear integer programming toolbox.

faults that belong to that subsystem. The following equation represents this constraint.

$$-x(1) - x(2) - x(3) + |M_1|x(7) \leq 0, \qquad (12)$$

where $|M_1| = 3$ is the cardinality number of M_1 and $x(1)$, $x(2)$, $x(3)$ and $x(7)$ are binary variables that are 1 if we use u_1, y_1, y_2 and MSO_{11} in the diagnosis system and are zero otherwise. This constraint implies that if we use MSO_1: $x(7) = 1$, its associated measurements are used by the subsystem too: $x(1) = x(2) = x(3) = 1$.

Equation (13) represents these set of constraints in A matrix.

$$A(j + g * h, k) = \begin{cases} -1 & if \quad m_k \in MSO_j \\ |M_j| & if \quad k = j + |M| \\ 0 & otherwise, \end{cases} \qquad (13)$$

where $|M_j|$ is the cardinality number of set of measurements in MSO_j and $|M|$ is the cardinality number of set of all the measurements in the system. Setting $b(j) = 0$ for $g * h < j \leq g * h + n$, where n is the number of MSOs in the system. The optimization problem takes into account the relationship between measurements and MSOs. For the running example we generated 165 MSOs, there are also 3 measurements in the subsystem 1, and 8 measurements for the entire system. Similarly, subsystem 1 has two faults of interest, and the goal is to be able to isolate them from any of the 6 faults in the complete system. Therefore, to solve the optimization problem (5) for subsystem 1, matrix A has 177 rows (equal to the number of constraints: 2 constraints to guarantee the local detectability of f_1 and f_2, 10 constraints to guarantee the local isolability of f_1 and f_2 from the other faults, and 165 constraints to capture the relationship between the MSOs and the measurements) and 173 columns (equal to the number of binary variables: 8 for the measurements and 165 for the MSOs) and b is a vector with 177 elements (equal to the number of constraints).

Table 1 shows the set of measurements that we need to add for each of the subsystem diagnosers to achieve maximum possible detectability and isolability using our proposed algorithm. To find the optimum measurements, we solved the optimization problem (5) for each subsystem.

Table 1: Set of augmented measurements to each subsystem model

Subsystem	Set of augmented measurements
S_1	y_3
S_2	u_2, y_2, y_6
S_3	y_4, y_6
S_4	y_5

Considering the expanded measurement set the schematic of the four tank system with the four distributed diagnosers is shown in Figure 2. The figure shows the complete set of measurements required by the four subsystem diagnosers to achieve global detectability and isolability for the set of faults they contain. For example subsystem 1 includes three measurements $M_1 = \{u_1, y_1, y_2\}$, and to achieve global diagnosability for its faults, y_3 must be communicated to its diagnoser from subsystem 2. Subsystem 2 is the only subsystem that shares a variable with a second order connected subsystem, all the other subsystems only need to communicate with their first order connected subsystems. Note that communicated measurements typically will incur additional cost and may lower reliability of the system diagnoser. But keeping them to a minimum (see results in Table 1) reduces that cost and uncertainty, while maintaining global diagnosability.

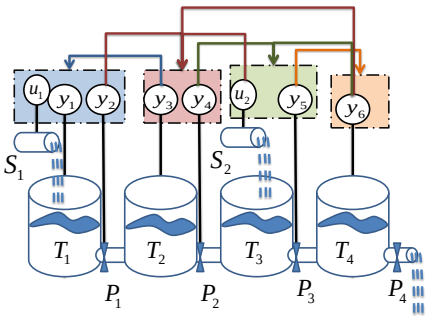

Figure 2: Distributed diagnosis subsystems.

A common way to validate a distributed fault detection and isolation approach is to compare the result with the maximum global detectability and isolability. Adopting the exoneration assumption, Table 2 shows the detectability and isolability performance of the centralized approach. An X in the table shows that the fault in the row and the fault in the column are not isolable from each other. An X in the first column (NF) means the fault in the corresponding row is not isolable from NF (No Fault) or simply it is not detectable. Table 2 shows that with a centralized approach we can detect and isolate all the faults.

Table 2: Fault isolability table for running example using centralized approach

	NF	f_1	f_2	f_3	f_4	f_5	f_6
f_1		X					
f_2			X				
f_3				X			
f_4					X		
f_5						X	
f_6							X

However, Table 3 shows that using the original subsystems for distributed diagnosis does not provide the same results as the centralized global diagnoser.

Table 3: Fault isolability table for running example using distributed approach for the original subsystems

	NF	f_1	f_2	f_3	f_4	f_5	f_6
f_1		X					
f_2	X		X	X	X	X	X
f_3	X		X	X	X	X	X
f_4	X		X	X	X	X	X
f_5	X		X	X	X	X	X
f_6	X		X	X	X	X	X

In fact, only f_1 can be detected and isolated from the other faults. Using the augmented subsystems in Table 1

Table 4: Fault isolability table for running example using distributed approach for the augmented subsystems

	NF	f_1	f_2	f_3	f_4	f_5	f_6
f_1		X					
f_2			X				
f_3				X			
f_4					X		
f_5						X	
f_6							X

(Figure 2) we achieve the same performance as the global diagnoser as shown in Table 4.

This demonstrates that the distributed approach can achieve the same performance with the centralized approach for fault detection and isolation in the running example. In general, the worst case scenario for a system with strongly connected subsystems (i.e., all subsystems are connected to each other) will typically require a large number of measurements from other subsystems to be communicated to each subsystem diagnoser. In those situations, subsystem diagnosers just get rid of the single point of failure, but each subsystem diagnoser may require a large number of measurements to be communicated to it from all of the other subsystems.

In our case study, the four tank system model included 165 MSOs, which means for each subsystem there was 2^{165} different MSO candidate sets. This creates a very large search space (in general the search space is exponential in the number of MSOs, and generating all MSOs is in itself an exponential problem. This justifies the formulation of the problem as a BILP problem that provides efficient tools, like the *bintprog* function in Matlab™(see earlier footnote), to solve it. However, given the exponential nature of the solution, this method will not scale up for larger systems, even if the subsystem diagnoser design is performed off-line. In addition to the computational complexity, the availability of global models for large, complex systems is unlikely because of the issues discussed in Section 1. To overcome this problem, we sacrifice minimality of the solution to some extent, and propose an incremental algorithm for designing the subsystem diagnosers.

5 MSOs Selection for Distributed Fault Detection Using Neighboring Subsystems

The proposed approach in the previous section used the global model of the system to generate the residuals, and then derived the subsystem diagnosers using the BILP algorithm run on the global MSO set. In this section, we achieve global diagnosability of a subsystem diagnoser by incrementally adding a minimum number of measurements from the neighbors of this subsystem till the global diagnosability property is established. The algorithm starts with the set of equations for the subsystem whose diagnoser is being designed, and if global diagnosability is not achieved using this model, it expands to include equation sets that correspond to the models of its immediate neighbors. If global diagnosability is achieved, the algorithm terminates, otherwise the algorithm expands to use the next higher order of neighbors and repeats the search for minimal MSOs to achieve complete diagnosability. The process of including successively higher order neighbors is shown in Figure 3. In the worst case, this process continues, till the complete set of system equations are required to generate all possible MSOs, and establish global diagnosability for the subsystem. Therefore, it is guaranteed that the method has the same diagnosability performance as the best centralized diagnoser for the same set of measurements. Algorithm 1 describes the algorithm for our proposed method.

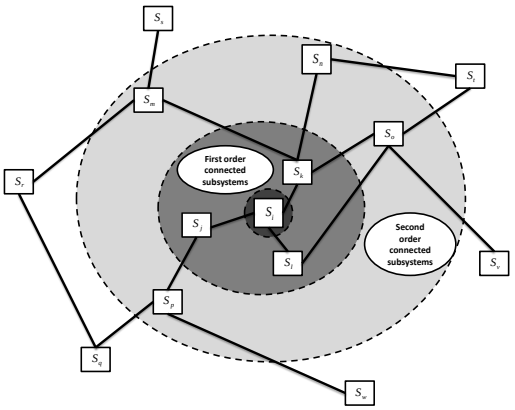

Figure 3: Expanding the search environment to the higher order connected subsystems.

Algorithm 1 Incremental Algorithm

1: **for each** $S_i \in S$ **do**
2: $SS = S_i$
3: $j = 0$
4: **while** $D_i(SS) \neq D_i(S)$ or $I_i(SS) \neq I_i(S)$ **do**
5: $j = j + 1$
6: $SS = SS \cup (j$th order connected subsystems of $S_i)$
7: Generate all the MSOs for SS
8: Use equation (9) to compute cost function for SS
9: Use equations (10), (11), and (13) to generate A matrix for SS
10: Generate vector b for SS
11: Use $bintprog(c, A, b)$ to solve the problem and compute $D_i(SS)$ and $I_i(SS)$

Consider the running example. To design the diagnosis system for the first subsystem, we start with its set of equations and we can only generate one MSO which is not enough to detect subsystem faults and isolate them from the system faults. We then augment the subsystem model with the model from its nearest neighbor subsystem 2, and generate the set of MSOs for the augmented model. The total number of MSOs for the augmented subsystem (Subsystem 1 + subsystem 2) is 11 which leads to 2^{11} MSO set candidates which is much smaller than 2^{165} candidates. Solving the optimization problem presented in this section gives the same result with the global method for this subsystem, but the computation time is reduced significantly. Using the same approach for every subsystem, the set of measurements that we need to transfer to each subsystem of the running example are presented in Table 5.

Figure 4 shows that for the four tank case study, all the subsystems share variables with their first order connected subsystems. This provides a practical advantage to this al-

Table 5: Set of augmented measurements to each subsystem model

Subsystem	Set of augmented measurements
S_1	y_3
S_2	u_2, y_2, y_5
S_3	y_4, y_6
S_4	y_5

gorithm because usually the subsystems with shared variables are physically closer to each other (corresponding to our definition of nearest neighbors) and, therefore, we do not need to transfer data over long distances, which, as discussed earlier, can be costly and error-prone.

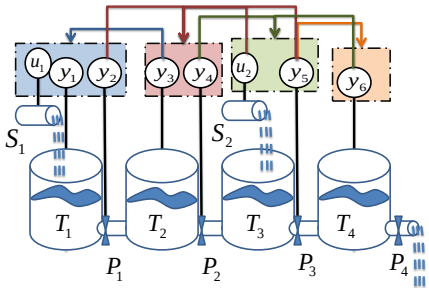

Figure 4: Distributed diagnosis subsystems using incremental algorithm.

Table 6 shows that this distributed diagnosis system provides the same diagnosability performance as the centralized diagnosis method.

Table 6: Fault isolability table for running example using the incremental algorithm

	NF	f_1	f_2	f_3	f_4	f_5	f_6
f_1		X					
f_2			X				
f_3				X			
f_4					X		
f_5						X	
f_6							X

The proposed algorithm provides the maximum possible detectability and isolability that can be achieved. The advantage of this algorithm is that not only we do not need a global model for detecting and isolating the faults, but also we do not use the global model in the design process of the supervisory system. This makes the approach suitable for large, complex systems, such as aircraft and power plants where the global systems models are likely to be unavailable or unknown.

6 Discussion and Conclusions

A distributed approach to the problem of fault detection and isolation is presented in this paper. We proposed two algorithms for MSOs selection for the distributed diagnosis. The proposed algorithms provide the maximum possible detectability and isolability that can be achieved for a system given a set of measurements. The first algorithm also guarantees that the subsystems share the minimum number of measurements, implying that we minimize the communication of measurement streams across subsystems of the global system. This is important because sending the data to other subsystems is costly in large scale systems. On the other hand, the second algorithm does not need to use the global model in the design process of the supervisory system . This makes the algorithm more practical, specially for the complex systems. However, the second algorithm does not guarantee that the number of shared variables among the subsystems are globally minimum.

Unlike previous work, such as [Bregon *et al.*, 2014; Daigle *et al.*, 2007] this method directly works with MSOs generated from subsystem and system equations, and therefore, does not need to use the temporal response and event ordering in the diagnosis, all of which are derived properties, and, therefore, require additional computation. Using a purely structural approach, reduces the overall diagnosability of the system for the given set of measurements. However, it also reduces the number of assumptions we need to make about the fault characteristics, order of events in the diagnoses subsystems (which can be error-prone), and we dot have to analyze in detail the subsystem dynamics.

Moreover, in the incremental algorithm we do not need to have the full global model to design the individual subsystem diagnosers. This is an important practical contribution of this paper in comparison to our previous work (e.g., [Roychoudhury *et al.*, 2009]). Requiring the global model may render the approach to be impractical for the large-scale complex systems, such as aircraft and power plants where the global systems models are likely to be unavailable or unknown.

Finally, in the proposed methods, we generate the MSOs first to design our subsystem diagnosers. The total number of MSOs is exponential in terms of the system measurements. This increases the computational cost of the problem. To make our diagnoser derivation process more efficient, we used BILP framework. On the other hand, having all the MSOs beforehand, makes robustness analysis [Khorasgani *et al.*, 2014a; Khorasgani *et al.*, 2014b] possible for robust distributed MSOs selection. In future work, we will consider noise and uncertainty in the system and will extend the proposed method to robust distributed fault detection and isolation.

References

[Bregon *et al.*, 2014] Anibal Bregon, Matthew Daigle, Indranil Roychoudhury, Gautam Biswas, Xenofon Koutsoukos, and Belarmino Pulido. An event-based distributed diagnosis framework using structural model decomposition. *Artificial Intelligence*, 210:1–35, 2014.

[Daigle *et al.*, 2007] M. J. Daigle, X. D. Koutsoukos, and G. Biswas. Distributed diagnosis in formations of mobile robots. *Robotics, IEEE Transactions*, 23(2):353–369, 2007.

[Deb *et al.*, 1998] S. Deb, A. Mathur, P. K. Willett, and K. R. Pattipati. Decentralized real-time monitoring and diagnosis. *In Systems, Man, and Cybernetics. IEEE International Conference*, 3:2998–3003, 1998.

[Debouk *et al.*, 2000] R. Debouk, S. Lafortune, and D. Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete*

Event Dynamic System: Theory and Applications, 10(1-2):33–86, 2000.

[Duarte Jr and Nanya, 1998] E. P Duarte Jr and T. Nanya. A hierarchical adaptive distributed system-level diagnosis algorithm. *Computers, IEEE Transactions*, 47(1):34–45, 1998.

[Ferrari *et al.*, 2012] Riccardo MG Ferrari, Thomas Parisini, and Marios M Polycarpou. Distributed fault detection and isolation of large-scale discrete-time nonlinear systems: An adaptive approximation approach. *Automatic Control, IEEE Transactions on*, 57(2):275–290, 2012.

[Indra *et al.*, 2012] Saurabh Indra, L. Trave-Massuyes, and Elodie Chanthery. Decentralized diagnosis with isolation on request for spacecraft. Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (Safeprocess), Mexico City, 2012.

[Khorasgani *et al.*, 2014a] Hamed Khorasgani, Daniel E. Jung, Gautam Biswas, Erik Frisk, and Mattias Krysander. Off-line robust residual selection using sensitivity analysis. International Workshop on Principles of Diagnosis (DX-14), Graz, Austria, 2014.

[Khorasgani *et al.*, 2014b] Hamed Khorasgani, Daniel E. Jung, Gautam Biswas, Erik Frisk, and Mattias Krysander. Robust residual selection for fault detection. Decision and Control (CDC), IEEE 53rd Annual Conference on, 2014.

[Krysander *et al.*, 2008a] Mattias Krysander, Jan Åslund, and Mattias Nyberg. An efficient algorithm for finding minimal overconstrained subsystems for model based diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 38(1), 2008.

[Krysander *et al.*, 2008b] Mattias Krysander, Jan Aslund, and Mattias Nyberg. An efficient algorithm for finding minimal overconstrained subsystems for model-based diagnosis. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 38(1):197–206, 2008.

[Lafortune, 2007] S. Lafortune. On decentralized and distributed control of partially-observed discrete event systems. in advances in control theory and applications. *Springer Berlin Heidelberg*, pages 171–184, 2007.

[Land and Doig, 1960] A. H. Land and A. G. Doig. An automatic method of solving discrete programming problems. *Econometrica: Journal of the Econometric Society*, pages 497–520, 1960.

[Lanigan *et al.*, 2011] Patrick E. Lanigan, Soila Kavulya, and Priya Narasimhan. Diagnosis in automotive systems: A survey. *Technical Report CMU-PDL-11-110, Carnegie Mellon University PDL*, 2011.

[Leger *et al.*, 1999] J. B. Leger, B. Iung, A. Ferro De Beca, and J. Pinoteau. An innovative approach for new distributed maintenance system: application to hydro power plants of the remafex project. *Computers in industry*, 38(2):131–148, 1999.

[Mitchell, 2002] John E. Mitchell. Branch-and-cut algorithms for combinatorial optimization problems. *Handbook of applied optimization*, pages 65–77, 2002.

[Rish *et al.*, 2005] I. Rish, M. Brodie, S. Ma, N. Odintsova, A. Beygelzimer, G. Grabarnik, and K Hernandez. Adaptive diagnosis in distributed systems. *Neural Networks, IEEE Transactions*, 16(5):1088–1109, 2005.

[Rosich *et al.*, 2009] Albert Rosich, Ramon Sarrate, and Fatiha Nejjari. Optimal sensor placement for fdi using binary integer programming. International Workshop on Principles of Diagnosis, 2009.

[Roychoudhury *et al.*, 2009] Indranil Roychoudhury, Gautam Biswas, and Xenofon Koutsoukos. Designing distributed diagnosers for complex continuous systems. *Automation Science and Engineering, IEEE Transactions on*, 6(2):277–290, 2009.

[Sarrate *et al.*, 2007] Ramon Sarrate, Puig Vicenc, Escobet Teresa, and Rosich Albert. Optimal sensor placement for model-based fault detection and isolation. pages 2584–2589. 46th IEEE Conference In Decision and Control, 2007.

[Shum *et al.*, 1988] S. K. Shum, J. F. Davis, W. F. Punch III, and B. Chandrasekaran. An expert system approach to malfunction diagnosis in chemical plants. *Computers and chemical engineering*, 12(1):27–36, 1988.

[Svard *et al.*, 2012] C. Svard, M. Nyberg, and J. Stoustrup. Automated design of an fdi system for the wind turbine benchmark. *JCSE Journal of Control Science and Engineering*, 2012.

[Wolsey and Nemhauser, 2014] Laurence A. Wolsey and George L Nemhauser. *Integer and combinatorial optimization*. John Wiley and Sons, 2014.

[Wolsey, 1998] Laurence A. Wolsey. *Integer programming*, volume 42. Wiley, New York, 1998.