Preprints, 9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes
September 2-4, 2015. Arts et Métiers ParisTech, Paris, France

Structural Approach for Distributed Fault Detection and Isolation

Hamed Khorasgani * **Daniel Jung** ** **Gautam Biswas** *

* *Inst. of Software-integrated Systems, Vanderbilt Univ., USA, e-mail:* {hamed.g.khorasgani,gautam.biswas}@vanderbilt.edu
** *Dept. of Electrical Engineering, Linköping University, Sweden, e-mail:* daner@isy.liu.se

Abstract:
This paper presents a framework for distributed fault detection and isolation in dynamic systems. Our approach uses the dynamic model of each subsystem to derive a set of independent, local diagnosers. If needed, the subsystem model is extended to include measurements and model equations from its immediate neighbors to compute its diagnosis. Our approach is designed to ensure that each subsystem diagnoser provides the correct results, therefore, a local diagnosis result is equivalent to the results that would be produced by a global system diagnoser. We discuss the distribute diagnosis algorithm, and illustrate its application using a multi-tank system.

Keywords: distributed fault diagnosis, residual generation.

1. INTRODUCTION

Analytical redundancy methods have been applied extensively for model based fault detection and isolation (FDI) of dynamic systems (Gertler, 1998; Bregon et al., 2014). Traditional approaches develop centralized diagnosers, e.g., the Aircraft Diagnostic and Maintenance Systems (ADMS) used on modern aircraft systems (Spitzer, 2007). However, as the complexity and size of systems, such as aircraft, automobiles, power plants, and manufacturing processes, have grown, distributed approaches to fault detection and isolation in large dynamic systems with many subsystems have become important (Leger et al., 1999; Shum et al., 1988). Transferring all of the collected sensor information to a central fault detection and isolation unit can be expensive and error prone. Centralized diagnosers may also be less reliable because they provide a single point of failure. Networking delays can also affect the timeliness of diagnosis decisions.

The computational intractability of centralized diagnosers for large systems is another reason for developing distributed diagnosers. In this paper, we adopt the approach of building individual diagnosers for each subsystem, taking into account that interactions with neighboring subsystems may have to be modeled to achieve globally correct diagnosis for each diagnoser.

The Dulmage-Mendelsohn (DM) decomposition (Dulmage and Mendelsohn, 1958) is a popular structural approach for designing FDI systems (Flaugergues et al., 2009; Krysander et al., 2008). Krysander and Frisk (2008) have used DM decomposition to address the sensor placement problem. In this paper, we adapt the DM decomposition approach to design and implement local diagnosers for each subsystem of a large, complex dynamic system. Unlike (Lafortune, 2007; Debouk et al., 2000) this method does not use a centralized coordinator and reduces the communication between subsystems to a minimum while still producing globally correct diagnosis results. Moreover, in the design process we do not need to have access to the global model.

The outline of the paper is as follows. Basic definitions and the multi-tank system as a running example are presented in Section 2. Section 3 formulates the problem. Our approach to distributed fault detection is presented in Section 4. The extension of the method to distributed fault isolation is presented in Section 5. Section 6 applies the method to the running example, a four-tank system and Section 7 concludes the paper.

2. BASIC DEFINITIONS AND RUNNING EXAMPLE

We use a four tank system (see Fig. 1) as a running example to discuss our distributed diagnosis algorithms. We assume each subsystem contains a tank, $T_i; 1 \leq i \leq 4$, and the outlet pipe to its right $P_i; 1 \leq i \leq 4$. Two of the subsystems, 1 and 3, also have inflows sources into their tanks. The system has eight sensors. Three sensors measure the pressure of T_1, T_2 and T_4 (p_1, p_2 and p_4, respectively). Three sensors measure the flow rates of P_1, P_2 and P_3 (q_1, q_2 and q_3, respectively). Two sensors measure the input flow rates, q_{in1} and q_{in2}. We assume the subsystems are disjoint, i.e., they have no overlapping components.

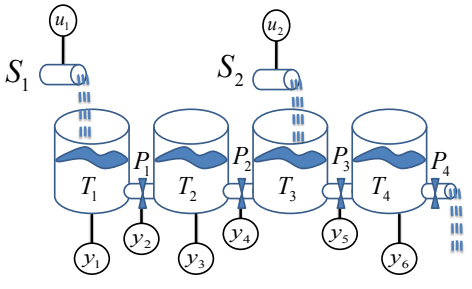

Fig. 1. Four-tanks system.

⋆ The work is partially supported by the Swedish Research Council within the Linnaeus Center CADICS.

More generally, we assume a system, S is made up of n of subsystems, $S_1, S_2, ...S_n$. Each subsystem is described by a dynamic system model.

Definition 1. (Subsystem model). A subsystem model M_i $(1 \leq i \leq n)$ is a tuple of (V_i, C_i, F_i), where V_i is the set of variables, C_i is the set of constraints and F_i is the set of system faults associated with the subsystem.

The overall set of system faults, $F = \bigcup_{i=1}^{n} F_i$, is the union of faults associated with each subsystem.

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

$$\begin{aligned} c_1 &: \dot{p}_1 = \frac{1}{C_{T1} + f_1}(q_{in1} - q_1) \\ c_2 &: q_1 = \frac{p_1 - p_2}{R_{P1} + f_2} \\ c_3 &: p_1 = \int \dot{p}_1 \, dt \end{aligned} \qquad \begin{aligned} c_4 &: q_{in1} = u_1 \\ c_5 &: p_1 = y_1 \\ c_6 &: q_1 = y_2. \end{aligned} \tag{1}$$

C_{Ti} is the nominal capacity of tank T_i, R_{Pi} is the nominal resistances of pipe P_i, $C_1 = \{c_1, c_2, c_3, c_4, c_5, c_6\}$ is the set of behavior constraints associated with this subsystem, $V_1 = \{\dot{p}_1, p_1, p_2, q_{in1}, q_1\}$ is the set of variables for the first subsystem model and $F_1 = \{f_1, f_2\}$ is the set of faults for this subsystem. Note that V_1 does not include known variables such as measurements, (u_1, y_1, y_2), or system parameters, (C_{T1}, R_{P1}).

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

$$\begin{aligned} c_7 &: \dot{p}_2 = \frac{1}{C_{T2} + f_3}(q_1 - q_2) \\ c_8 &: q_2 = \frac{p_2 - p_3}{R_{P2} + f_4} \\ c_9 &: p_2 = \int \dot{p}_2 \, dt \end{aligned} \qquad \begin{aligned} c_{10} &: p_2 = y_2 \\ c_{11} &: q_2 = y_4. \end{aligned} \tag{2}$$

For this subsystem the set of constraints is $C_2 = \{c_7, c_8, c_9, c_{10}, c_{11}\}$, the set of variable is $V_2 = \{\dot{p}_2, p_2, p_3, q_1, q_2\}$ and $F_2 = \{f_3, f_4\}$ is the set of faults. Note that the initial conditions for constraints c_3, c_9 and other integral equations in the paper are assumed to be known.

Definition 2. (Neighboring Subsystems). Two subsystems, and, therefore, their corresponding models, M_i and M_j are defined to be neighbors if and only if they have at least one shared variable.

In the running example, subsystem models M_1 and M_2 are neighbors and their shared variables are $V_1 \cap V_2 = \{p_2, q_1\}$.

The DM decomposition divides a system model into three parts: (1) under-determined, (2) exactly determined and (3) over-determined (Flaugergues et al., 2009). The over-determined part introduces redundancy in the system model and can be used for fault detection and isolation. Fig. 2 represents DM decomposition of the first subsystem. This subsystem model has a just determined part (${M_1}^0$) and an over-determined part (${M_1}^+$). The shared variables between a subsystem and the other subsystems in the running example are circled in the figures.

In this work, we assume every fault parameter, f is included in exactly one constraint equation, c_f. This is not a restricting assumption because if we have more than a fault in a constraint we can consider the other faults as new variables and then add new constraints for each of these new variables making the variable equal to the fault. Given that, the local detectability can be defined as:

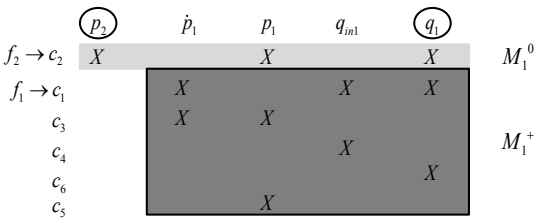

Fig. 2. DM decomposition of the first subsystem model.

Definition 3. (Locally detectable) A fault $f \in F_i$ is locally detectable if $c_f \in {M_i}^+$, where ${M_i}^+$ is the over-determined part of subsystem model M_i.

Consider *Definition* 3 and Fig. 2. Fault f_1 is locally detectable because $c_1 \in {M_1}^+$ but f_2 is not locally detectable since $c_2 \notin {M_1}^+$. To detect f_2, the diagnosis subsystem needs to have an extra constraint.

Definition 4. (Augmented subsystem model) Given subsystem model M_i and constraint $c_k \notin M_i$, the augmented subsystem model $M_{i_{c_k}} = (M_i | c_k)$ is $(V_{i_{c_k}}, C_{i_{c_k}}, F_{i_{c_k}})$, where $V_{i_{c_k}}$ is the union of V_i and variables appear in c_k, $C_{i_{c_k}}$ is the union of C_i and c_k and $F_{i_{c_k}}$ is the union of F_i and the possible fault associated with c_k.

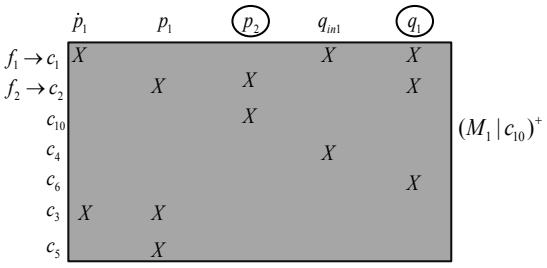

Fig. 3. DM decomposition of $M_{1_{c_{10}}} = (M_1 | c_{10})$.

For example in the running example $M_{1_{c_{10}}} = (M_1 | c_{10})$ is $(V_{1_{c_{10}}}, C_{1_{c_{10}}}, F_{1_{c_{10}}})$, where $V_{1_{c_{10}}} = \{\dot{p}_1, p_1, p_2, q_{in1}, q_1\}$, $C_{1_{c_{10}}} = \{c_1, c_2, c_3, c_4, c_5, c_6, c_{10}\}$ and $F_{1_{c_{10}}} = \{f_1, f_2\}$. Note that c_{10} did not add any new variables or faults to the subsystem model. Fig. 3 represents the DM decomposition of the augmented subsystem model $M_{1_{c_{10}}}$. This figure shows that $c_2 \in {M_{1_{c_{10}}}}^+$, and, therefore, f_2 is locally detectable for the augmented subsystem model $M_{1_{c_{10}}}$.

Definition 5. (Locally isolable) A fault $f_i \in F_i$ is locally isolable from fault $f_j \in F$ if $c_{f_i} \in (M_i \backslash c_{f_j})^+$, where $(M_i \backslash c_{f_j})^+$ is the over-determined part of subsystem model M_i without c_{f_j}.

Fig. 4 shows DM decomposition of the $M_{1_{c_{10}}} \backslash c_1$.

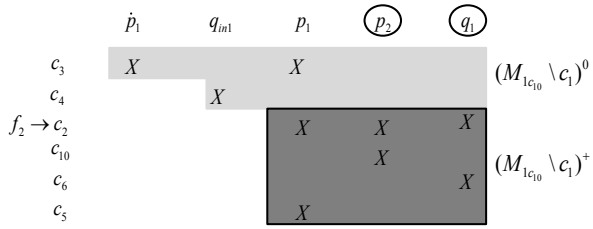

Fig. 4. DM decomposition of $M_{1_{c_{10}}} \backslash c_1$.

c_2 is in the overdetermined part of the augmented subsystem model, therefore f_2 is locally isolable from f_1 in the augmented subsystem model.

3. PROBLEM FORMULATION

We formulate the problem and solution approach for designing distributed diagnoser for a system, **S** made up of a number of subsystems, $S_1, S_2, \cdots S_n$, such that there is no overlap of components among the subsystems. However, the subsystems may share variables at their interface, e.g., liquid flowrate at outlet of pipe = liquid flowrate at input to connected tank. In the ideal case, each subsystem includes a sufficient number of measured variables, such that the ensuing redundancy is sufficient to detect and isolate all of its faults F_i locally. If so, we can associate an independent diagnoser D_i with each subsystem $S_i; 1 \leq i \leq n$, with no centralized control, and no exchange of information with other diagnosers. If the independence among diagnosers does not hold, then we have to consider the following additional cases:

(1) $f_k \in F_i$ is not locally detectable.
(2) $f_l \in F_i$ and $f_m \in F_i$ are not locally isolable from each other.
(3) $f_n \in F_i$ is not locally isolable from $f_o \in F_j$ and $f_o \notin F_i$.

Designing distributed diagnosers that account for these three scenarios is the focus of our work in this paper. After addressing each of these situations, we derive an integrated approach to distributed FDI, and derive algorithms that apply to complex, dynamic systems made up of a number of subsystems.

Given subsystems, $S_i; 1 \leq i \leq n$, with equation sets represented as a set of constraints, C_i. Associated with each subsystem are also a set of local fault candidates, F_i, such that $\bigcup_{i=1}^{n} F_i = F$. We may need to augment each subsystem with additional constraints that are typically acquired from the 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 constraints from a neighboring 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 n.

For each subsystem S_i with its model M_i, our goal is to find minimal sets of constraints from the neighboring subsystems that provide complete detectability and isolability to that subsystem. A set of constraints is minimal if there is no subset of constraints that provides the same detectability and isolability.

More formally, the problem for designing a diagnoser for a particular subsystem S_i can be described as follows:

Consider $\mathcal{M}_i = \{M_1, M_2, \ldots, M_l\}$ as the set of neighboring subsystem models to subsystem S_i. To address the three situations mentioned above, we need to develop an algorithm to find all the constraints sets c_o in $\mathcal{M}_i$ that guarantees maximal structural detectability and isolability for subsystems faults F_i and includes a minimal set of constraints from its neighbors, i.e.,

$$\begin{aligned} \min_{c_o \subseteq \mathcal{C}_n} \quad & |c_o| \\ & D(M_i|c_o) = D(M_i|\mathcal{C}_n), \\ & I(M_i|c_o) = I(M_i|\mathcal{C}_n), \end{aligned} \tag{3}$$

where $\mathcal{C}_n$ represents the set of all the constraints, D represent the set of detectable faults in F_i, and I represents the set of isolable faults in F_i from the system faults F.

Consider the first subsystem of the running example M_1, c_{10} makes f_1 and f_2 detectable and isolable from all the other faults in the system. Therefore, $A_1 = \{c_{10}\}$ is a minimal solution to the problem.

4. DISTRIBUTED APPROACH FOR FAULT DETECTION

In this section we present our approach to find all the minimal sets of constraints from the neighboring subsystem models to provide maximum possible fault detectability. We illustrate the procedure by solving this problem for subsystem model 2, and then develop a general algorithm to solve this problem.

Consider subsystem model 2 whose constraints are listed as equation (2). The corresponding structural decomposition of this subsystem is shown in Fig. 5. This sub-

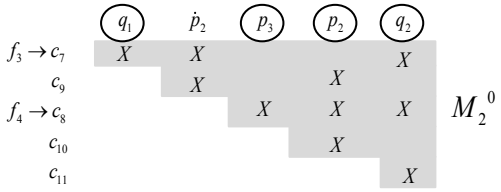

Fig. 5. DM decomposition of M_2.

system is just determined, therefore, none of the faults are locally detectable. However, q_1 is a shared variable with subsystem model 1, and p_3 is a shared variable with subsystem model 3. Therefore, we have to find constraints from one or both of the neighboring subsystems to make f_3 and f_4 detectable. It is straight forward to show that by adding a set of just determined constraints that include q_1, fault f_3 becomes detectable. However, this set of equations does not make f_4 detectable. Fig. 5 shows there is no path from c_7 to c_8, moving c_7 to an over-determined part does not affect c_8, and, therefore, this does not make f_4 detectable. However, augmenting the subsystem with a set of just determined constraints that contains p_3 makes f_4 detectable.

Krysander and Frisk (2008) present an algorithm that accepts a just determined subsystem and a set of measurement candidates and provides a minimal set of measurements that provide maximum detectability for the system. We skip the details of their algorithm in this paper, and assume, given the structure of the subsystem model and set of shared variables with the neighboring subsystems, we can derive a minimal set of variables that provides maximum detectability performance.

To make f_3 detectable, we have to find all of constraint sets that include q_1, and by adding them to M_2 we can make q_1 over-determined in this subsystem model. We start with all equations in M_1 that have q_1. These equations are c_1, c_2, and c_6 as it is shown in Fig. 6. Then for the additional variables in each equation that is not already in M_2^0 we need to add other equations. For c_1 we need to add two new constraints one with q_{in1} and the other one with $\dot{p}_1$. Finally we need to add a new constraint with p_1 and since $p_2 \in {M_2}^0$ we do not have to consider it.

To find the other minimal sets we keep adding the relative equations to the other sets using the same approach described above. As it is shown in Fig. 6, by adding constraints to the system we eventually achieve four sets of minimal constraints: $A_2 = \{c_1, c_2, c_3, c_4\}$, $A_3 = \{c_1, c_3, c_4, c_5\}$, $A_4 = \{c_2, c_5\}$, and $A_5 = \{c_6\}$.

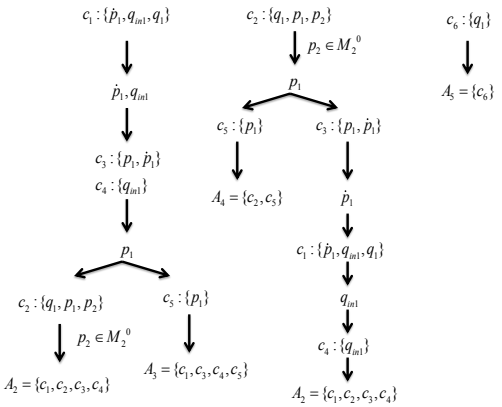

Fig. 6. Finding the minimal sets of constraints in M_1 to make f_3 locally detectable.

More formally, Fig. 6 represents a matching algorithm whose general form is presented as Algorithm 1. If we initialize the algorithm with the set of unknown variables − in this example q_1 is the unknown variable − it provides a set of complete matching of variables and constraints in the subsystem that includes the unknown variables.

Algorithm 1 Count-Matchings

1: **input:** current matching $\mathcal{M}$
2: **input:** sets of determined variables $\mathcal{D}$ and undetermined variables $\mathcal{U}$
3: **if** $U = \emptyset$ **then**
4: **return** $\mathcal{M}$ as a feasible (minimal) matching.
5: **for each** $x \in \mathcal{U}$ **do**
6: **for each** y which can determine x **do**
7: Let $\mathcal{M}'$ be $\mathcal{M} \cup \{x \to y\}$
8: Let $\mathcal{D}'$ be $\mathcal{D} \cup \{x\}$.
9: Let $\mathcal{U}'$ be $\mathcal{U} \setminus \{x\}$.
10: Add all the undetermined variables of y to $\mathcal{U}'$.
11: Count-Matchings$(\mathcal{M}', \mathcal{D}', \mathcal{U}')$

Fig. 7 shows that augmenting A_2 with M_2 makes f_3 detectable. Subsystem model 2 is just determined but a

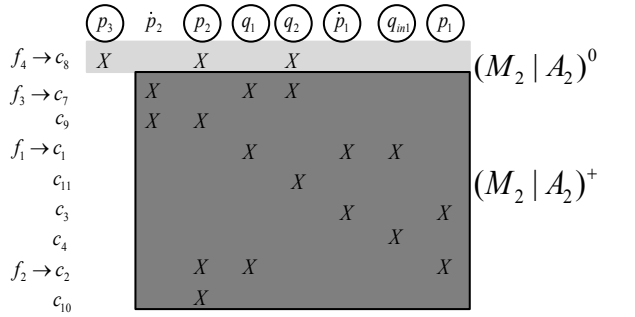

Fig. 7. DM decomposition of $(M_2|A_2)$.

subsystem can have an underdetermined part as well. For example consider subsystem model M_3 in equation (4).

$$
\begin{aligned}
c_{12} &: \dot{p}_3 = \frac{1}{C_{T3}}(q_{in2} + q_2 - q_3) \\
c_{13} &: q_3 = \frac{p_3 - p_4}{R_{P3} + f_5} \qquad\qquad c_{15} : q_{in2} = u_2 \\
c_{14} &: p_3 = \int \dot{p}_3 \, dt \qquad\qquad c_{16} : q_3 = y_5.
\end{aligned}
\tag{4}
$$

The DM decomposition of this subsystem model is shown in Fig. 8. f_5 is in the underdetermined part of the structure. q_{in2} and q_3 are in the just determined part of the

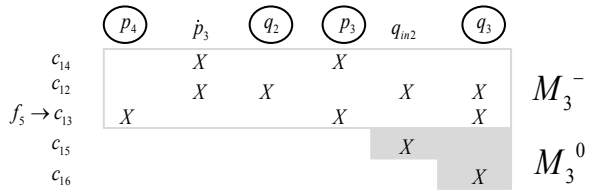

Fig. 8. DM decomposition of M_3.

system and we can compute them using c_{15} and c_{16}, respectively. However, to compute the other four variables in the subsystem, p_3, q_2, $\dot{p}_3$, and p_4, we only have three constraints, which makes complete matching between constraint and variables impossible. To make this part of the subsystem just determined, we need to augment a set of constraints from the neighboring subsystems. We use maximum weighted bipartite matching algorithm (West, 2001) to find the set of shared variables that are not already matched with a constraint. Maximum weighted matching is a polynomial algorithm and provides a matching with maximum sum of the values of the weights. We give shared variables in the under-determined part weight w_1 and non shared variables in the under-determined part weight $w_2 > w_1$. Therefore, the algorithm gives priority to match non shared variables with subsystem constraints and for the unmatched set of shared variables, we augment a set of constraints from the neighboring subsystems to match with them. Fig. 9 shows the matching results for subsystem model M_3.

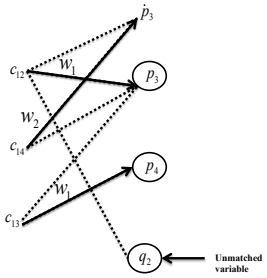

Fig. 9. Weighted matching of the under-determined part of M_3.

q_2 is the only unmatched variable in the under-determined part of the subsystem. Therefore, to make the subsystem just determined we need to augment a minimal set of just determined constraints that include q_2 from M_2 to M_3. Algorithm 2 summarizes the procedure.

Algorithm 2 UnderDetermined

1: **input:** under-determined part of subsystem model M_i^-
2: **input:** subsystem model shared variables V_s
3: Let w_1 be V_s weights
4: Let w_2 be $V \setminus V_s$ weights
5: Apply weighthed matching algorithm to M_i^-
6: $U =$ unmatched variables

It is shown in Fig. 10 that $A_6 = \{c_{11}\}$ is the only minimal set of constraint in M_2 that includes q_2. Therefore, we first need to augment M_3 with A_6 to make the system just determined and then apply the above method to make f_5 detectable. Consider subsystem model from equation (5) and structure of $(M_3|A_6)$ shown in Fig. 11.

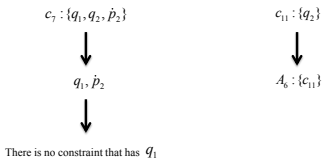

Fig. 10. Search for a minimal set of equation with q_2 in M_2.

$$\begin{aligned} c_{17} &: \dot{p}_4 = \frac{1}{C_{T4} + f_6}(q_3 - q_4) & c_{19} &: p_4 = \int \dot{p}_4 \, dt \\ c_{18} &: q_4 = \frac{p_4}{R_{P4}} & c_{20} &: p_4 = y_6. \end{aligned} \tag{5}$$

Using this structure and Algorithm 1, we know that $A_7 = \{c_{17}, c_{18}, c_{19}\}$ and $A_8 = \{c_{20}\}$ are the only minimal sets of equations that we can augment from M_4 to make the f_5 locally detectable.

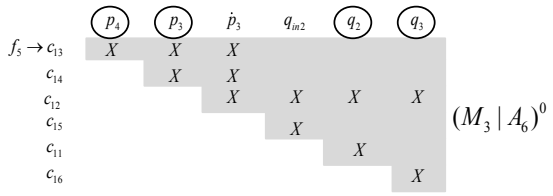

Fig. 11. DM decomposition of $(M_3|A_6)$.

Therefore, the minimal candidate sets that we can augment to M_3 are $A_9 = \{c_{11}, c_{17}, c_{18}, c_{19}\}$ and $A_{10} = \{c_{11}, c_{20}\}$. Fig. 12 shows DM decomposition of $(M_3|A_9)$. In some cases, it is possible that an augmented minimal

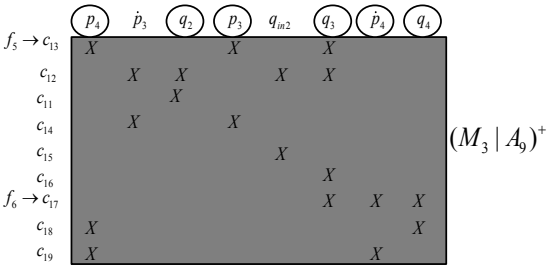

Fig. 12. DM decomposition of $(M_3|A_9)$.

set, A_i, adds a set of faults F_{A_i} to the subsystem model M_i too. These faults can be sensor faults or faults in other constraints. The following theorem states that these faults are locally detectable in subsystem model M_i.

Theorem 1. Consider local subsystem model $M_i = \{V_i, C_i, F_i\}$ and $C_{augments}$ a set of minimal constraints that makes set of faults F_i detectable in the augmented subsystem $(M_i|C_{augments}) = \{V_j, C_j, F_j\}$, then the set of faults F_j in the augmented subsystem $(M_i|C_{augments})$ are locally detectable.

Proof. The proof of this theorem is straight forward, since the minimal set makes a part of the system that includes the fault overdetermined, the set itself should be in the overdetermined part as well. This means the associated faults in the set are detectable.

For example, f_6 is locally detectable in $(M_3|A_9)$. Therefore, as long as we are focused on fault detection the augmented faults do not cause any problem. The fault detection algorithm is summarized as Algorithm 3 below.

Algorithm 3 Detectability

```
C = {}
input: subsystem model M_i
subsystem model shared variables V_s
input: subsystem model neighbors M
if ∀f ∈ F_i ∴ c_f ∈ M_i^+ then
    return
if ∃f ∈ F_i and f ∈ M_i^− then
    U = UnderDetermined(M_i^−, V_s)
    D = V_i \ U
    C = Count-Matchings (M, D, U)
U = minimal set of shared variables that makes all the
    faults over-determined
D = V_i \ U
C = Count-Matchings (M, D, U) ∪ C
```

5. DISTRIBUTED APPROACH FOR FAULT ISOLATION

In this section we assume the set of minimal constraints to make all the faults locally detectable have been derived based on the method presented in Section 4. It is clear that the locally detectable faults in each subsystem are locally isolable from the faults in the other subsystems.

Theorem 2. Consider local subsystem model $M_i = \{V_i, C_i, F_i\}$ if $f_i \in F_i$ is locally detectable in M_i, then f_i is locally isolable form f_j if $f_j \notin F_i$.

Proof. Since f_i is detectable we have $c_{f_i} \in {M_i}^+$ and since $f_j \notin F_i$ we can say $c_{f_j} \notin {M_i}^+$. Therefore, ${M_i}^+ = (M_i \backslash c_{f_j})^+$ and $c_{f_i} \in (M_i \backslash c_{f_j})^+$

For example, in subsystem model $(M_3|A_9)$, f_5 is isolable from f_1, f_2, f_3, and f_4 because they are not in the subsystem model and f_5 is detectable in this subsystem model. Considering Theorem 2, it is straight forward to address the isolability problem. For each fault $f_i \in F_i$, we remove the associated equation c_{f_i} from C_i and all the neighboring subsystems. Then we use Algorithm 1 to make all the remaining faults in F_i detectable. For example, consider $(M_3|A_9)$. To make f_5 isolable from f_6, we remove c_{17} from $(M_3|A_9)$ and M_4. DM decomposition of $(M_3|A_9)\backslash c_{17}$ is:

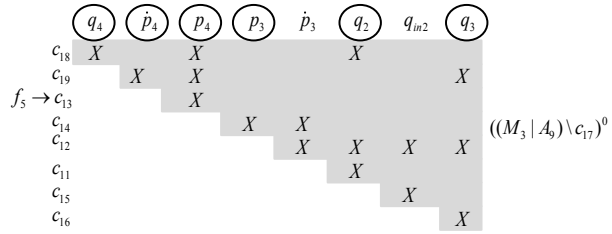

Fig. 13. DM decomposition of $(M_3|A_9)\backslash c_{17}$.

Considering Fig. 13, each of variables q_4, $\dot{p}_4$ and p_4 can make f_5 detectable. Applying Algorithm 1 to $M_4 \backslash c_7$ for each of them gives us: $\{c_{18}, c_{20}\}$, $\{c_{19}, c_{20}\}$, and $\{c_{20}\}$, respectively. Therefore, we can say the augmented subsystem $(M_3|A_9, c_{20})$ will detect f_5 and isolate it from all the other faults in the global system M. The following algorithm summarizes the method discussed above.

The proposed approach considers the neighboring subsystems M of subsystem M_i and augment minimal constraints from the M to maximize diagnosability. If the set neighboring subsystems M does not have required redundancies to achieve maximum diagnosability we have to expand the search process to the next higher order of

Algorithm 4 Diagnosability

input: subsystem model M_i
input: subsystem model neighbors M
C = Detectability(M_i, M)
for each $c \in C$ **do**
  $M^{'} = (M_i|c)$
  for each $f \in M^{'}$ **do**
    $\bar{M}_i^{'} = M^{'} \setminus (f \text{ and } c_f)$
    $\bar{c}$ = Detectability($\bar{M}_i^{'}$, $M \setminus c$)
    $c = \bar{c} \cup c$
Delete non-minimal constraint sets in C

neighborings subsystems of M. The expansion process will stop when the distributed approach achieves maximum diagnosability. Therefore, it is guaranteed that the method has the same diagnosability performance as the best centralized diagnoser for the same set of measurements.

In the case that there is no independent subsystem diagnosers can be derived using our distributed approach, the solution gradually expands to include all subsystems and eventually derives the centralized diagnoser. Algorithm 5 summarizes this approach.

Algorithm 5 DistributedDiagnosis

input: subsystem model M_i
input: subsystem model neighbors M
C = Diagnosability(M_i, M)
for each $c_o \in C$ **do**
  if $D(M_i|c_o) = D(M_i|\mathcal{C}_n)$ and $I(M_i|c_o) = I(M_i|\mathcal{C}_n)$ **then**
    return
  $\mathcal{M} = M \cup$ (neighboring subsystems of M)
  DistributedDiagnosis(M_i, $\mathcal{M}$)

6. DISTRIBUTED DIAGNOSIS FOR FOUR TANK SYSTEM

Table 1 shows the set of constraints that we need from its neighbors to augment each subsystem model to achieve maximum possible detectability and isolability. In the cases that there were more than one possible minimal set of constraints, we considered the one with minimum number of constraints.

Table 1. Set of augmented constraints to each subsystem model

Subsystem Model	Set of augmented constraints
M_1	c_{10}
M_2	c_6, c_{12}, c_{14}, c_{15}, c_{16}
M_3	c_{11}, c_{20}
M_4	c_{16}

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, with a global diagnostic method we can detect and isolate all the faults in the running example. However, using the original subsystems for distributed diagnosis does not provide the same results as the centralized global diagnoser. In fact, only f_1 can be detected and isolated from the other faults. Using the augmented subsystems in Table 1 we will have the same performance as the global model. This demonstrates that the distributed approach has the same performance with the centralized approach for fault detection and isolation in the running example.

7. CONCLUSIONS

A distributed approach to the problem of fault detection and isolation is presented in this paper. The proposed algorithm provides the maximum possible detectability and isolability that can be achieved. The contribution of work is that not only do not need a global model in 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 very feasible for complex systems, such as aircraft and power plants where the global systems models are likely to be unavailable or unknown.

In future work, we will consider the effect of model uncertainty in the residuals (Khorasgani et al. (2014)) and will extend the proposed method to robust distributed fault detection and isolation.

REFERENCES

Bregon, A., Biswas, G., Pulido, B., Alonso-Gonzalez, C., and Khorasgani, H. (2014). A common framework for compilation techniques applied applied to diagnosis of linear dynamic systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(7).

Debouk, R., Lafortune, S., and Teneketzis, D. (2000). Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic System: Theory and Applications*, 10(1-2), 33–86.

Dulmage, A.L. and Mendelsohn, N.S. (1958). Coverings of bipartite graphs. *Canadian Journal of Mathematics*, 10(4), 516–534.

Flaugergues, V., Cocquempot, V., Bayart, M., and Pengov, M. (2009). Structural analysis for fdi: a modified, invertibility-based canonical decomposition. In *Proceedings of the 20th International Workshop on Principles of Diagnosis, DX09*, 59–66. Citeseer.

Gertler, J. (1998). *Fault detection and diagnosis in engineering systems*. CRC press.

Khorasgani, H., Jung, D., Biswas, G., Frisk, E., and Krysander, M. (2014). Robust residual selection for fault detection. *Decision and Control (CDC), IEEE 53rd Annual Conference on*, 5764–5769.

Krysander, M., Åslund, J., and Nyberg, M. (2008). 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).

Krysander, M. and Frisk, E. (2008). Sensor placement for fault diagnosis. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 38(6), 1398–1410.

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

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

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

Spitzer, C. (2007). Honeywell primus epic aircraft diagnostic and maintenance. *Digital Avionics Handbook*, 2223.

West, D.B. (2001). *Introduction to graph theory*. Prentice Hall.