Diagnosability of Hybrid Dynamical Networks using Indicator Functions

Lachlan Blackhall * **Priscilla Kan John** ** **Alban Grastien** **
David J. Hill *

* *Research School of Information Sciences and Engineering, The Australian National University, Canberra, ACT, 0200, Australia (e-mail: lachlan.blackhall, david.hill@anu.edu.au).*
** *National Information and Communications Technology Australia (NICTA) and The Australian National University, Canberra, ACT, 0200, Australia (e-mail: priscilla.kanjohn@anu.edu.au, alban.grastien@nicta.com.au)*

Abstract: Results for the diagnosability of hybrid dynamical networks are presented. These results give the conditions for which arbitrary events (including faults) in hybrid networks can be detected and isolated using a general class of indicator functions. These results emerge from the overlap of the control theoretic fault detection and isolation (FDI) and diagnosis (DX) communities. The interaction of the many systems in the network is exploited to achieve diagnosability conditions dependent only on the number of events in the network rather than the number of interconnected systems. The algorithmic complexity of the diagnosability conditions and methods of choosing a minimal indicator set that guarantee diagnosability are also addressed.

1. INTRODUCTION

The physical interconnection of myriad types of dynamical systems is often referred to as a dynamical network. Understanding the operation of such networks in order to better manage them is becoming more important given the many real world dynamical networks in the engineering domain, of which electricity and information networks, like the Internet, are two examples.

The interconnection of many dynamical systems is known to lead to complex, emergent behavior not observed in the individual dynamic systems. The accurate diagnosis, that is the detection and isolation, of faults and other events in dynamical networks has thus emerged as an important problem in characterizing the operation of such networks.

This work extends the notion of diagnosability as studied in the field of Discrete Event Systems to Hybrid Systems. The Hybrid System framework, as developed in Blackhall and Kan John (2008), aims to augment diagnosis and control capabilities on such systems by combining Discrete Event System modeling and analysis techniques with control and system theoric methodologies. Diagnosability is significantly complicated in dynamical networks due to the interaction of the fault and event characteristics of the many interconnected systems.

Modeling electricity or information networks as hybrid dynamical networks therefore allows us to better characterise their behaviours which have both a discrete and a continuous component.

Diagnosability is presented here as the ability to detect the occurence of an event in a system given a model of the system and a set of observable indicators. Each indicator is an observation on a set of events.

We present here a very general characterization of the diagnosability conditions for the detection and isolation of multiple, arbitrary sequential or simultaneous events in hybrid dynamical networks.

2. PREVIOUS WORK

Diagnosability definitions are provided in a number of different works, including Sampath et al. (1995); Cordier et al. (2006); Pencolé (2004) and Bayoudh et al. (2006), in the model-based diagnosis literature. All relate to the ability to determine, given a system model and observations on the system, that a fault or set of faults have occured. Being able to distinguish between faults is an additional benefit. Our definition of diagnosability is close to the one presented in Bayoudh et al. (2006) and is explicitly defined in Section 8.1.

The study of hybrid systems is relatively recent and has emerged from the overlap of control theoretic fault detection and isolation and diagnosis methods. These approaches, as well as some supporting literature, are briefly reviewed here. A comparison of diagnosability is done in Cordier et al. (2006) where correspondences between concepts used in FDI and DX are clarified and the diagnosability problem as understood in both fields can be brought to one common formulation using the concept of

⋆ This research was supported by NICTA in the framework of the SuperCom project. NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program.

signatures. This common ground is what hybrid system diagnosis and diagnosability studies are based on.

FDI methodologies focus mainly on continuous systems with dynamical behaviour and have sought to ensure the robust operation of such systems in the presence of faults. Control and system theoric techniques are used to model uncertainties as well as process and measurement noise. A good overview of these methods can be found in Gissinger et al. (2000) Hou and Muller (1994), Frank (1996) and Luong et al. (1997). This area of work has generally focussed on specific examples or classes of systems and has typically used observers and residual generators to detect deviations of the observed system trajectory away from some nominal operating condition.

On the other hand the diagnosis community typically focusses on logical systems as in Reiter (1987). Within the diagnosis community there has been substantial work on the diagnosis of discrete event systems as in Cassandras and Lafortune (1999) and Sampath et al. (1995). An extension of the discrete diagnosis approach has been to perform diagnosis on hybrid systems as in Bayoudh et al. (2008), McIlraith et al. (2000), Yang et al. (2008) and Cocquempot et al. (2004). Hybrid systems allow both the continuous and the discrete dynamics of a system to be encapsulated, thus providing an accurate model for many real world systems.

What is needed from both an FDI and DX perspective is a more general framework that unifies techniques from the two fields in order to provide methods of addressing the more difficult problem of fault detection and isolation in hybrid dynamical networks. We use a similar unification approach as presented in Cordier et al. (2006) and extend on the concept of signatures. Additional supporting work used within this paper is drawn from the field of probing, an overview of which can be found in Brodie et al. (2002).

3. MOTIVATION

The motivation for this work is to develop tools to analyse power grids which are a type of complex dynamical networks. Most of the body of work available on electricity networks focus on their dynamical behaviour, Kinney et al. (2005); Hill and Chen (2006). One important representation they use is to model a network by using a graph. In Kinney et al. (2005), the nodes of the graph represent the substations and the edges represent the transmission lines. In more complicated models, we could take the nodes to represent other components (e.g. switches or transformers) on the network as well. In section 5, we present a simplified model of a system that could represent an electricity network or any similar network (e.g. the Internet).

The fact that networks have a graphical representation facilitates the bridging of methodologies from FDI and DX. In the DX community, it is common to extricate an automaton representation from the graph of a system. We then use the concept of signatures, where a signature is defined as in Cordier et al. (2006) as being a function associating a set of observables to each event, to link continuous and discrete behaviours. There can be different approaches in obtaining a fault signature. For example, in Bayoudh et al. (2006), Analytical Redundancy Relations (ARR) and residuals are used. We use direct detection of mode changes by regression techniques to get fault signatures as presented in Blackhall and Kan John (2008). A mode change corresponds to a change in signature. Essentially we are able to extract an overarching discrete automaton where each mode of the automaton has its own continuous dynamics (explained further in Section 6).

The term 'indicator function' in our work corresponds broadly to what is meant by 'event signature'. We define indicator functions in Section 7.

4. HYBRID DYNAMICAL NETWORKS

Dynamical networks emerge from the interconnection of many individual dynamical systems, where each dynamical system is a node in the network. Hybrid dynamical networks (subsequently referred to as networks) are networks where the individual dynamical systems have a hybrid characteristic as in Zhao and Hill (2008), that is, the fundamental dynamics of each dynamical system have a finite number of discrete operating modes. The governing dynamics for each node (N_k) of the hybrid dynamical network is given by:

$$\begin{aligned} \dot{\mathbf{x}}_\mathbf{k} &= f_{k_{\sigma_k}}(\mathbf{x}_\mathbf{k}, \mathbf{u}_{\mathbf{k}_{\sigma_\mathbf{k}}}) + \sum_j l_{kj_{\sigma_k}}(\mathbf{x}_\mathbf{k}, \mathbf{y}_\mathbf{j}) \\ \mathbf{y}_\mathbf{k} &= h_{k_{\sigma_k}}(\mathbf{x}_\mathbf{k}) \end{aligned} \tag{1}$$

for $k \in 1, 2, \cdots, K$ where σ_k is the mode switching signal taking values in $M_k = \{1, 2, \cdots, m_k\}$ where the value of the mode switching signal is assumed known at time t_0. At each node $\mathbf{x}_\mathbf{k} \in \mathbb{R}^{n_k}$ are the internal states, $\mathbf{u}_{\mathbf{k}_{\sigma_\mathbf{k}}} \in \mathbb{R}^{m_{k_{\sigma_k}}}$ are the local control inputs and $\mathbf{y}_\mathbf{k} \in \mathbb{R}^{p_k}$ are the measurable outputs. The internal dynamics at each node are given by $(f_{k_{\sigma_k}}(\mathbf{x}_\mathbf{k}, \mathbf{u}_{\mathbf{k}_{\sigma_\mathbf{k}}}) : \mathbb{R}^{n_k} \times \mathbb{R}^{m_{k_{\sigma_k}}} \rightarrow \mathbb{R}^{n_k})$ and the measurable output is given by $(h_{k_{\sigma_k}}(\mathbf{x}_\mathbf{k}) : \mathbb{R}^{n_k} \rightarrow \mathbb{R}^{p_k})$. The dynamical effect of the j-th node being connected to the k-th node is given by the interconnection dynamics $(l_{kj_{\sigma_k}}(\mathbf{x}_\mathbf{k}, \mathbf{y}_\mathbf{j}) : \mathbb{R}^{n_k} \times \mathbb{R}^{p_j} \rightarrow \mathbb{R}^{n_k})$.

When there is only a single system in the network we recover the usual definition for a single hybrid dynamical system. We assume that the state of the system is continuous and does not exhibit abrupt changes at the instant of switching mode. The entire internal, control and network dynamics of the network can be characterized by the K-tuple $([\sigma_1(t), \sigma_2(t), \cdots, \sigma_K(t)] \in \{M_1 \times M_2 \times \cdots \times M_K\})$. It should be noted that both the *Continuous* and *Discrete* faults detailed in Yang et al. (2008) can be analysed in the proposed hybrid systems framework.

5. RUNNING EXAMPLE

We present now an introduction to the example that will be presented throughout this paper. We have a simple four node, fully interconnected hybrid dynamical network as seen in Fig. 1. We are interested in determining the structural diagnosability of the network. The structural diagnosability refers to the ability to accurately detect node and/or link failures in this network.

A link failure occurs when a given link between two nodes fails and a node failure occurs when a node, and all its interconnections, are simultaneously removed from the

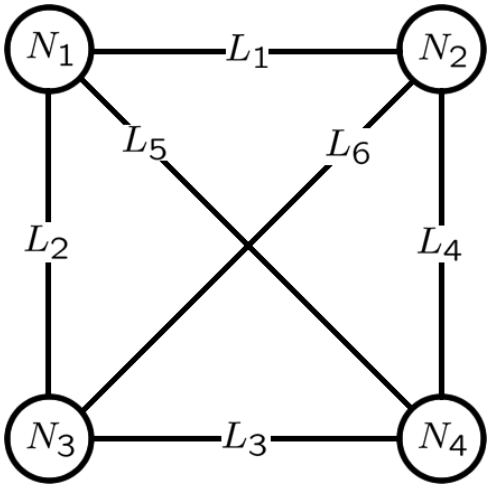

Fig. 1. The four node, six link complex network analyzed in this example.

network. These structural changes can be well codified in the theory of hybrid dynamical networks outlined earlier where a change in the interconnection structure of the k-th node corresponds to a different operational mode (σ_k) and thus different interconnection dynamics ($l_{kj_{\sigma_k}}(\mathbf{x_k}, \mathbf{y_j})$).

From this perspective there are ten distinct faults that can occur, corresponding to the four node failures and six link failures. A link failure between two nodes, caused by either a link or node failing, can be seen to impact both nodes to which it is connected. Hence, it is possible to determine the occurrence of the link failure from observing either of the connected nodes. It is of interest to determine the conditions under which these node and link failures are diagnosable. The example will be continued in the *Example Continued* sections throughout the paper.

6. MODES AND EVENTS

The discrete operating modes of each system in a hybrid dynamical network completely describe the operation of the network as a whole. These modes can correspond to arbitrary operating conditions, some nominal and some induced through the occurrence of a fault or other event in the network. We use the term events to be very general and include faults and other events of interest that can be characterized by a change in operating mode. We assume that there are a finite number of events (including faults) that can occur within the network and we can thus define the set (E) of n network events:

$$e_i \in E,\ \forall i \in \{1, 2, \cdots, n\} \tag{2}$$

representing all the possible events that can occur in the network. We then define the status of an event (e_i) as:

$$e_{i[t_\lambda, t_{\lambda+1})} = \begin{cases} 0 & \text{Event } e_i \text{ hasn't occurred in } [t_\lambda, t_{\lambda+1}). \\ 1 & \text{Event } e_i \text{ has occurred in } [t_\lambda, t_{\lambda+1}). \end{cases} \tag{3}$$

This representation, as we will see later, has important benefits for computing the diagnosability of the hybrid dynamical network. Additionally $[t_\lambda, t_{\lambda+1})$ is a sampling interval for arbitrary t_λ and $t_{\lambda+1}$ where $t_{\lambda+1} > t_\lambda$. We will see later that this sampling interval is necessary for the indicator functions of Section 7 to be robustly defined. There is an explicit assumption here that an event e_i can only occur once in the interval $[t_\lambda, t_{\lambda+1})$. The sampling interval can be varied depending on the requirements of the particular network and the sampling intervals cover the entire operational time of the network thus:

$$\bigcup_{\lambda \in \mathbb{Z}_+} [t_\lambda, t_{\lambda+1}) = [t_0, t_\infty) \tag{4}$$

where $\mathbb{Z}_+$ is the set of nonnegative integers.

We also define the set of active events $\Omega_{[t_\lambda, t_{\lambda+1})} \subseteq E$ to be the set of events that are occurring in the time interval $[t_\lambda, t_{\lambda+1})$:

$$\Omega_{[t_\lambda, t_{\lambda+1})} = \{e_i | e_{i[t_\lambda, t_{\lambda+1})} = 1\} \tag{5}$$

It should be noted that the true value of $e_{i[t_\lambda, t_{\lambda+1})}$ and $\Omega_{[t_\lambda, t_{\lambda+1})}$ is never known explicitly and this is what we seek to estimate with a given diagnosis.

The events that occur in the network cause a corresponding mode change in some or all of the hybrid systems in the network. It is common to represent the relationship between the network events and the discrete operating modes of the k-th system by a deterministic finite automaton as in Cassandras and Lafortune (1999). This gives:

Definition 1. (Deterministic Finite Automaton (DFA)). A deterministic finite automaton for the discrete behavior of the k-th hybrid system in the network is given by the tuple:

$$S_{k_{disc}} = \langle M_k, \bar{E}_k, \mathcal{T}_k \rangle \tag{6}$$

where for the k-th system M_k is the finite set of system modes, $\bar{E}_k \subseteq E$ is the set of events which cause a mode transition and $\mathcal{T}_k$ is the transition function that maps an event and mode into a new mode, $\mathcal{T}_k : M_k \times \bar{E}_k \to M_k$.

The DFA formalizes the relationship between the operating modes of each of the hybrid systems and the events that occur within the network. In large interconnected networks it is common that a single event will appear in the DFA for a number of systems in the network. This corresponds to a single event being responsible for mode changes in more than one hybrid system in the network. We can exploit this behavior to determine the operating mode of each system in the network without needing to determine the operating mode of each system explicitly. This can be shown by:

Lemma 2. (Hybrid System Mode Determination). Given the automaton ($S_{k_{disc}}$) and the initial operational mode ($\sigma_k(t_0)$) of the k-th system and assuming that no more than one event in $\bar{E}_k$ occurs in each sampling interval $[t_\lambda, t_{\lambda+1})$ then knowledge of $\Omega_{[t_\lambda, t_{\lambda+1})}$ (where $\Omega_{[t_\lambda, t_{\lambda+1})} \cap \bar{E}_k$ contains the relevant events for the k-th system) for all sampling intervals $[t_\lambda, t_{\lambda+1})$ will allow determination of $\sigma_k(t_{\lambda+1})$ for all $t_{\lambda+1}$.

Proof. Given $S_{k_{disc}}$ and $\sigma_k(t_\lambda)$ we can determine $\sigma_k(t_{\lambda+1})$ after the interval $[t_\lambda, t_{\lambda+1})$ using:

$$\sigma_k(t_{\lambda+1}) = \mathcal{T}_k(\sigma_k(t_\lambda), \Omega_{[t_\lambda, t_{\lambda+1})} \cap \bar{E}_k) \tag{7}$$

■

Remark 3. Although we require that only a single event occurs in a given sampling interval for each system, this does not restrict the possibility that multiple events can occur simultaneously as multiple events affecting different systems in the network may occur simultaneously. Additionally, assuming that the sampling interval is sufficiently

small compared to the fault occurrence interval then this assumption can be seen to be very unrestrictive.

From this we see that if every event in the network can be determined in each time interval then the K-tuple $([\sigma_1(t_{\lambda+1}), \sigma_2(t_{\lambda+1}), \cdots, \sigma_K(t_{\lambda+1})])$ can be reliably determined for all $t_{\lambda+1}$. For this reason the diagnosability of the operational mode of each system in the network can be reduced to the diagnosability of all the events in the network. Finding reliable methods of determining the events that are occurring in the network is the topic of the following section.

7. INDICATOR FUNCTIONS AND EVENT DETECTION

It is common in dynamical systems to have indicators; quantities that indicate the transition of a system between modes or that measure the occurrence of an event directly. An indicator thus represents the signature of an event.We saw in Section 6 that if it is possible to determine the occurrence of all events in the hybrid network then it is possible to know the operational mode of all systems in the network. In showing this we have effectively decoupled the problem of detecting and isolating network events and the determination of the operational mode of every system in the network which is the eventual goal. We can formalize the concept of indicator functions as follows.
We define the set (S) of m indicator functions as:

$$s_j \in S,\ \forall j \in \{1, 2, \cdots, m\}. \tag{8}$$

where:

$$s_j := \langle g_j, \Psi_j, E_{s_j}, \nu_j \rangle \tag{9}$$

is a tuple where $\Psi_j \subseteq Q_j \subseteq \mathbb{R}^{\kappa_j}$ and Ψ_j and Q_j are well-defined. The indicator function $g_j : \mathbb{R}^{q_j} \rightarrow Q_j \subseteq \mathbb{R}^{\kappa_j}$ is defined as:

$$g_j(Y_{j_{[t_\lambda, t_{\lambda+1})}}) \in \begin{cases} \Psi_j \subseteq Q_j & \text{if } E_{s_j} \cap \Omega_{[t_\lambda, t_{\lambda+1})} \neq \emptyset \\ Q_j \setminus \Psi_j & \text{if } E_{s_j} \cap \Omega_{[t_\lambda, t_{\lambda+1})} = \emptyset \end{cases} \tag{10}$$

where $Y_{j_{[t_\lambda, t_{\lambda+1})}} \in \mathbb{R}^{q_j}$ are an arbitrary combination of observations taken from the measurable outputs $(\mathbf{y_k})$ of any system in the network in the interval $[t_\lambda, t_{\lambda+1})$. $E_{s_j} \subseteq E$ is the set of events that can be detected by s_j resulting in the indicator returning a result in $\Psi_j \subseteq Q_j$. The value of indicator s_j is given by:

$$\nu_j = \begin{cases} 1 & g_j(Y_{j_{[t_\lambda, t_{\lambda+1})}}) \in \Psi_j \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

Essentially, the j-th indicator function will return a value in a well defined region (Ψ_j) of $\mathbb{R}^\kappa$ when one of a set of events (E_{s_j}) that is detectable by s_j occurs in the interval $[t_\lambda, t_{\lambda+1})$.

The generality of this approach can be seen in that a particular indicator function does not need to detect a given event with perfect certainty but rather that the indicator function will determine that one of a set of events has occurred with perfect certainty. This reduces considerably the burden placed on the designer of the indicator functions. The only assumption made here is that it is possible to create an indicator function with the required properties.

There are a number of methods of creating indicator functions and all can be suitable for use within the framework outlined. Existing work has generally focussed on residual indicators detecting a difference between the nominal and actual trajectory of the system as in Cocquempot et al. (2004). Recent work on the structural diagnosis of hybrid networks has shown that such indicators can work by detecting the mode changes directly as in Blackhall and Kan John (2008).

Indicator	N_1	N_2	N_3	N_4	L_1	L_2	L_3	L_4	L_5	L_6
s_1	0	1	0	0	1	0	0	0	0	0
s_2	0	0	1	0	0	1	0	0	0	0
s_3	0	0	0	1	0	0	0	0	1	0
s_4	1	0	0	0	1	0	0	0	0	0
s_5	0	0	1	0	0	0	0	0	0	1
s_6	0	0	0	1	0	0	0	1	0	0
s_7	1	0	0	0	0	1	0	0	0	0
s_8	0	1	0	0	0	0	0	0	0	1
s_9	0	0	0	1	0	0	1	0	0	0
s_{10}	1	0	0	0	0	0	0	0	1	0
s_{11}	0	1	0	0	0	0	0	1	0	0
s_{12}	0	0	1	0	0	0	1	0	0	0

Fig. 2. The fault signature matrix for the complete set of event indicators that are available in the four node hybrid network in this example.

7.1 Event Dependency/Fault Signature Matrix

An alternative simple representation of the events detectable by a given indicator function can be achieved using an event dependency matrix as in Brodie et al. (2002) or equivalently a fault signature matrix as in Travé-Massuyès et al. (2004) . We define this to be:

$$D_{S,E}(j,i) = \begin{cases} 1 & e_i \in E_{s_j} \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Here $D_{S,E}$ is an $m \times n$ matrix showing how events are detectable through indicator functions. The question that arises is what conditions on the matrix $D_{S,E}$ will allow us to guarantee that every event in the network is diagnosable in all time intervals $[t_\lambda, t_{\lambda+1})$, which is addressed in Section 8.1.

7.2 Example Continued - Fault Signature Matrix

In Blackhall and Kan John (2008) the diagnosis method presented is equivalent to having indicator functions that allow the node and link failures to be detected by directly measuring the change in the operational mode. The diagnosis could indicate either that the link itself had failed, or that the node at the end of the link had failed, thus each indicator could reduce the potential fault to one of two possible faults. If we assume that all possible event indicators can be implemented then each of the four nodes will have three unique event indicators corresponding to all the link and node failures that can be measured by that node. The corresponding fault signature matrix for these event indicators is shown in Fig. 2 and it is from this set of estimators that we must choose the indicator sets for both fault detection and fault isolation.

8. DIAGNOSABILITY OF HYBRID DYNAMICAL NETWORKS

We have shown, in Lemma 2, that for the hybrid dynamical network to be diagnosable we require the network events to be diagnosable in all time intervals $[t_\lambda, t_{\lambda+1})$. We now present the conditions under which the network events E are diagnosable in each time interval $[t_\lambda, t_{\lambda+1})$ with event indicators S. We present two preliminary definitions on diagnosability that formalize the results we seek.

8.1 Diagnosability

We consider two definitions of diagnosability that correspond to the fault detection and fault isolation problem. We refer to them as weak diagnosability and strong diagnosability respectively.

Definition 4. (Weakly Diagnosable). A network is weakly diagnosable with respect to a subset of events ($\bar{E} \subseteq E$) with a given set of event indicators ($\bar{S} \subseteq S$) if the set of event indicators is able to detect the occurrence of any event in the set ($\bar{E}$). we can write:
Weakly Diagnosable($\bar{E}$), $\bar{E} \subseteq E$, $\exists \bar{S} \subseteq S$, *where* $\bar{S} = \{s_{p_1}, \cdots, s_{p_d}\}$, $\bar{E} \subseteq \{E_{s_{p_1}}, \cdots, E_{s_{p_d}}\}$, *where* $1 \leq p_1 < \cdots < p_d \leq m$ *for* $d \leq m$.

Definition 5. (Strongly Diagnosable). A network is strongly diagnosable with respect to a subset of events ($\bar{E} \subseteq E$) with a given set of event indicators ($\bar{S} \subseteq S$) if the set of event indicators is able to detect the occurrence of any event in the set ($\bar{E}$) and if the diagnosed set of events (Ω_{diag}) is equal to the true event set (Ω). That is $\Omega = \Omega_{\text{diag}}$. We can write:
Strongly Diagnosable($\bar{E}$), $\bar{E} \subseteq E$, $\exists \bar{S} \subseteq S$, *where* $\bar{S} = \{s_{p_1}, \cdots, s_{p_d}\}$, $\bar{E} \subseteq \{E_{s_{p_1}}, \cdots, E_{s_{p_d}}\}$, *where* $1 \leq p_1 < \cdots < p_d \leq m$ *for* $d \leq m$. *We also have the additional requirement that* $\Omega = \Omega_{diag}$.

Remark 6. Within the definition of strong diagnosability it is possible for this to be for single faults or multiple faults. In the case of multiple faults there are $2^n - 1$ possible sets of faults corresponding to all possible combinations of faults occurring. Meeting the requirement of strong diagnosability for every possible set of faults can be seen as a very complicated problem. For this reason we say that a hybrid dynamical network is strongly diagnosable for a given set of faults. If, for example, we were interested in determining the simultaneous occurrence of pairs of events ((e_α, e_β) for all $\alpha, \beta \in 1, 2, \cdots, n$, such that $\alpha \neq \beta$) then we would say that the hybrid network is strongly diagnosable for all possible pairs of events.

We now present the conditions for fault detection and fault isolation; the conditions required to satisfy the strong and weak diagnosability conditions.

8.2 Weak Diagnosability - Fault Detection

The fault detection problem is to determine if the chosen indicator functions $s_j \in \bar{S}$ will ensure that the occurrence of any event(s) will result in one of the chosen event indicators being active ($\nu_j = 1$). Formally this gives us:

Theorem 7. Given the set of event indicators $\bar{S}$ and the set of events we wish to detect ($\bar{E}$) then the hybrid dynamical network is weakly diagnosable if:

$$\bigcup_{\{j|s_j \in \bar{S}\}} E_{s_j} = \bar{E} \tag{13}$$

This corresponds to there being a one in all columns of the corresponding fault signature matrix ($D_{\bar{S},\bar{E}}$).

Proof. It can be verified that this condition satisfies the weak diagnosability condition given in Def. 4. The corresponding proof for the fault signature matrix follows from Brodie et al. (2002) which first established the result in the context of probing. ∎

Example Continued - Fault Detection From the complete set of mode estimators given in Fig. 2 it is possible to determine if a given indicator set will satisfy the fault detection condition. Ignoring the method by which this set is chosen we are able to verify easily, using the earlier conditions, that the set in Fig. 3 satisfies the weak diagnosability condition. Subsequently isolating the location of the fault requires additional conditions to be satisfied and we address this in the following section.

8.3 Strong Diagnosability - Fault Isolation

The problem of fault isolation is to determine a set of event indicators such that each fault can be uniquely identified. We will address single fault and multiple fault isolation separately.

Single Fault Isolation The case of single fault isolation, where only a single fault is active at any given time ($|\Omega| = 1$), is the less general fault isolation problem but due to its connection with previous results in Brodie et al. (2002) it is presented independently. Formally we have:

Theorem 8. Given the set of event indicators $\bar{S}$ and the single fault we wish to detect ($e_i \in \bar{E}$) then the hybrid dynamical network will be single fault isolable if it is weakly diagnosable and

$$\Big(\bigcap_{\{j|s_j \in \bar{S}, e_i \in E_{s_j}\}} E_{s_j}\Big) \cap \Big(\bar{E} \setminus \bigcup_{\{j|s_j \in \bar{S}, e_i \notin E_{s_j}\}} E_{s_j}\Big) = e_i = \Omega \tag{14}$$

This corresponds to all the columns of the fault signature matrix ($D_{\bar{S},\bar{E}}$) being unique, with at least a one in every column.

Proof. We are taking the intersection of the possible events as determined by the active event indicators with the possible events as determined by the inactive indicators. We can verify that this condition satisfies the requirements of the strong diagnosability condition given in Def. 5. The corresponding proof for the fault signature matrix follows from Brodie et al. (2002) which first established the result in the context of probing. ∎

Example Continued - Single Fault Isolation From the complete set of mode estimators given in Fig. 2 it is possible to determine if a given indicator set will satisfy the single fault isolation condition. Ignoring the method by which this set is chosen we are able to verify easily, using the earlier conditions, that the set in Fig. 3 allows single fault isolation to occur. We now show the conditions for which multiple faults can be isolated presenting the most general case of the fault isolation condition.

Indicator	N_1	N_2	N_3	N_4	L_1	L_2	L_3	L_4	L_5	L_6
s_1	0	1	0	0	1	0	0	0	0	0
s_2	0	0	1	0	0	1	0	0	0	0
s_3	0	0	0	1	0	0	0	0	1	0
s_4	1	0	0	0	1	0	0	0	0	0
s_5	0	0	1	0	0	0	0	0	0	1
s_6	0	0	0	1	0	0	0	1	0	0
s_7	1	0	0	0	0	1	0	0	0	0
s_8	0	1	0	0	0	0	0	0	0	1
s_9	0	0	0	1	0	0	1	0	0	0

Fig. 3. One possible set of estimators that satisfy the fault detection and single fault isolation conditions presented earlier.

Multiple Fault Isolation When multiple faults occur (that is $|\Omega| \geq 1$) it is no longer possible to isolate the faults using the fault isolation condition defined previously. We now seek to isolate the occurrence of multiple faults by determining the events that are not occurring through exploiting our knowledge of the indicators that are not active. Formally this gives us:

Theorem 9. Given the set of event indicators $\bar{S}$ and the set of faults we wish to detect ($E_{\text{faults}} \subseteq \bar{E}$) then the hybrid dynamical network is multiple fault isolable for E_{faults} if it is weakly diagnosable and

$$\bar{E} \setminus \Big(\bigcup_{\{j | s_j \in \bar{S}, E_{\text{faults}} \cap E_{s_j} = \emptyset\}} E_{s_j} \Big) = E_{\text{faults}} = \Omega \qquad (15)$$

This corresponds to a one in every column of the fault signature matrix ($D_{\bar{S},\bar{E}}$) to satisfy weak diagnosability as well as a one in every column of the submatrix ($D_{\underline{S},\bar{E}\setminus E_{\text{faults}}} \subseteq D_{\bar{S},\bar{E}}$) where $\underline{S} = \{s_j | E_{\text{faults}} \cap E_{s_j} = \emptyset\}$ is the set of event indicators not sensitive to any of the fault events.

Proof. Again it is easy to verify that the condition presented satisfies the strong diagnosability condition of Def. 5. The corresponding condition for the fault signature matrix can be seen as simply the fault detection condition for those events that are not occurring. ■

The strong diagnosability condition for multiple faults is also applicable for single faults and is thus the most general diagnosability result presented in this work.

8.4 Example Continued - Multiple Fault Isolation

From the complete set of mode estimators given in Fig. 2 it is possible to determine if a given indicator set will satisfy the multiple fault isolation condition for a given fault set or class of fault sets. For clarity we focus on the isolation of the pair of faults when node N_4 and link L_1 fail. We are able to verify easily, using the earlier conditions, that the set in Fig. 4 satisfies the conditions for the multiple faults indicated. It should be noted that this set of indicators will not necessarily satisfy the multiple fault diagnosis condition for an arbitrary set of faults, highlighting the complexity of the arbitrary multiple fault isolation problem.

8.5 Complexity

In all cases in the preceding analysis it should be noted that the complexity of the algorithms is polynomial as it consists of checking a simple set theoretic or matrix condition.

Indicator	N_1	N_2	N_3	N_4	L_1	L_2	L_3	L_4	L_5	L_6
s_1	0	1	0	0	1	0	0	0	0	0
s_3	0	0	0	1	0	0	0	0	1	0
s_7	1	0	0	0	0	1	0	0	0	0
s_8	0	1	0	0	0	0	0	0	0	1
s_{10}	1	0	0	0	0	0	0	0	1	0
s_{11}	0	1	0	0	0	0	0	1	0	0
s_{12}	0	0	1	0	0	0	1	0	0	0

Fig. 4. The event indicators necessary to allow multiple fault diagnosability for node N_4 and link L_1 failures.

9. DETERMINING THE MINIMAL INDICATOR SET FOR DIAGNOSABILITY

We have thus far presented conditions that guarantee the diagnosability of a given hybrid dynamical network. It remains to show how to determine the minimal set of event indicators $S_{\min} \subseteq S$ such that the diagnosability conditions are satisfied. We will present a complexity analysis of each of these problems to guide the development of algorithms for finding such a minimum diagnosability set.

9.1 Complexity Analysis

Theorem 10. (Fault Detection Complexity). Fault detection is NP-hard

Proof. Fault detection is exactly the minimum set cover problem Karp (1972) which is known to be NP-hard. ■

Theorem 11. (Single Fault Isolation Complexity). Single fault isolation is NP-hard.

Proof. This was shown to be true in Brodie et al. (2002) using a reduction from the fault detection problem outlined previously. ■

Theorem 12. (Multiple Fault Isolation Complexity). Multiple fault isolation is NP-hard.

Proof. To satisfy the conditions for multiple fault diagnosis we see that we need to provide a minimum set cover for $\bar{E} \setminus E_{\text{faults}}$ from the set $\{s_j | E_{s_j} \cap E_{\text{faults}} = \emptyset\}$ and a minimum set cover for E_{faults} from the set $\{s_j | E_{s_j} \cap E_{\text{faults}} \neq \emptyset\}$. The union of these minimum set cover will necessarily be the minimum indicator set for multiple fault diagnosis. As both of these are the minimum set cover problem that was shown in Karp (1972) to be NP-hard the multiple fault isolation is clearly NP-hard. ■

Having shown the computational difficulty of each of these problems we see that finding the minimal set that guarantees diagnosability is a complicated task. Results for this minimum diagnosability set are beyond the scope this paper. The reader is directed to results in Brodie et al. (2002) and Cormen et al. (2001) for suitable polynomial time methodologies giving algorithms that would allow the near optimal minimum diagnosability set to be determined. Additional methods of finding such minimal diagnosability sets is an active area of future work.

10. CONCLUSION

In this paper we have presented a general framework for determining the diagnosability of hybrid dynamical networks using a general class of indicator functions. We show that determining the operational mode of each system in the network reduces to determining the occurrence of all events in the network. Weak and strong diagnosability results are hence presented in this context. The generality of the approach provides flexibility in designing appropriate indicator functions to exploit this result.

We have shown that determining if a given set of indicators satisfies the diagnosability conditions has polynomial complexity however choosing a minimum set of such indicators that still guarantees diagnosability is NP-hard. This suggests that future work in this area should focus on the development of algorithms that can recover a near optimal solution in polynomial time. These results would be directly applicable to the construction of minimum order diagnosis engines for a variety of real world hybrid dynamical networks.

REFERENCES

M. Bayoudh, L. Travé-Massuyès, and X. Olive. Hybrid systems diagnosability by abstracting faulty continuous dynamics. In *17th International Workshop on the Principles of Diagnosis*, 2006.

M. Bayoudh, L. Travé-Massuyès, and X. Olive. Towards active diagnosis of hybrid systems. In *International Workshop on Principles of Diagnosis*, 2008.

L. Blackhall and P. Kan John. Model-based diagnosis of hybrid dynamical networks for fault tolerant control. In *19th International Workshop on Principles of Diagnosis*, 2008.

M. Brodie, I. Rish, S. Ma, A. Beygelzimer, and N. Odintsova. Strategies for problem determination using probing. Technical report, IBM T.J. Watson Research Center, 2002.

C. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems.* Kluwer Academic Publishers, 1999.

V. Cocquempot, T. El Mezyani, and M. Staroswieckit. Fault detection and isolation for hybrid systems using structured parity residuals. In *5th Asian Control Conference*, 2004.

M-O. Cordier, L. Travé-Massuyès, and X. Pucel. Comparing diagnosability in continuous and discrete-event systems. In *17th International Workshop on the Principles of Diagnosis*, 2006.

T.M. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein. *Introduction to Algorithms, Second Edition.* MIT Press and McGraw-Hill, 2001.

P.M. Frank. Analytical and qualitative model-based fault diagnosis a survey and some new results. *European Journal of Control*, 1996.

G.L. Gissinger, M. Loung, and H.-F. Reynaund. Failure detection and isolation - optimal design of instrumentation system. In *IFAC Workshop SAFEPROCESS*, 2000.

D.J. Hill and G. Chen. Power systems as dynamic networks. In *Proceedings IEEE International Symposium on Circuits and Systems*, 2006.

M. Hou and P.C. Muller. Fault detection and isolation observers. *International Journal of Control*, 1994.

R. M. Karp. *Complexity of Computer Computations.* Plenum Press, 1972.

R. Kinney, P. Crucitti, R. Albert Contact, and V. Latora. Modeling cascading failures in the north american power grid. *The European Physical Journal B - Condensed Matter and Complex Systems*, 46(1):1555–1575, 2005.

M. Luong, D. Maquin, and Ragot J. Sensor network design for failure detection and isolation. In *3rd IFAC Symposium SICICA*, 1997.

S. McIlraith, G. Biswas, D. Clancy, and V. Gupta. Hybrid systems diagnosis. In *International Workshop On Hybrid Systems, Computation and Control*, 2000.

Y. Pencolé. Diagnosability analysis of distributed discrete event systems. In *European Conference on Artificial Intelligence (ECAI-04)*, 2004.

R. Reiter. A theory of diagnosis from first principles. *Artificial Intelligence Journal (AIJ)*, 32(1):57–95, 1987.

M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.

L. Travé-Massuyès, T. Escobet, S. Spanache, and X. Olive. Diagnosability analysis based on component supported analytical redundancy relations. *IEEE Transactions on Systems, Man and Cybernetics, Part A*, 2004.

H. Yang, B. Jiang, and V. Cocquempot. Qualitative fault tolerance analysis for a class of hybrid systems. *Nonlinear Analysis: Hybrid Systems*, 2:846–861, 2008.

J. Zhao and D. J. Hill. Dissipativity theory for switched systems. *IEEE Transactions on Automatic Control*, 53 (4):941 – 953, May 2008.