2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

Link Failure Detection in Multi-hop Control Networks

Alessandro D'Innocenzo, Maria Domenica Di Benedetto and Emmanuele Serra

***Abstract*— A Multi-hop Control Network (MCN) consists of a plant where the communication between sensors, actuators and computational unit is supported by a wireless multi-hop communication network, and data flow is performed using scheduling and routing of sensing and actuation data. We characterize the problem of detecting the failure of links of the radio connectivity graph and provide necessary and sufficient conditions on the plant dynamics and on the communication protocol. We also provide a methodology to *explicitly* design the network topology, scheduling and routing of a communication protocol in order to satisfy the above conditions.**

I. Introduction

Wireless networked control systems are spatially distributed control systems where the communication between sensors, actuators, and computational units is supported by a shared wireless communication network. Control with wireless technologies typically involves multiple communication hops for conveying information from sensors to the controller and from the controller to actuators. The use of wireless networked control systems in industrial automation results in flexible architectures and generally reduces installation, debugging, diagnostic and maintenance costs with respect to wired networks. The main motivation for studying such systems is the emerging use of wireless technologies in control systems (see e.g., [1], [2], and [3]).

Although Multi-hop Control Networks (MCNs) offer many advantages, their use for control is a challenge when one has to take into account the joint dynamics of the plant and of the communication protocol. Wide deployment of wireless industrial automation requires substantial progress in wireless transmission, networking and control, in order to provide formal models and verification/design methodologies for wireless networked control system. The design of the control system has to consider the presence of the network, as it represents the interconnection between the plant and the controller, and thus affects the dynamical behavior of the system. The analysis of stability, performance, and reliability of real implementations of wireless networked control systems requires addressing issues such as scheduling and routing using real communication protocols.

Recently, a huge effort has been made in scientific research on Networked Control Systems (NCSs), see [4], [5], [6], [7], and [8], and references therein for a general overview. However, the literature on NCSs usually does not take into account the non–idealities introduced by scheduling and routing communication protocols of Multi-hop Control Networks. In [9], a simulative environment of computer nodes and communication networks interacting with the continuous-time dynamics of the real world is presented. To the best of our knowledge, the only formal model of a Multi-hop Control Network has been presented in [10], [11], where the modeling and stability verification problem has been addressed for a MIMO LTI plant embedded in a MCN, when the controller is already designed. A mathematical framework has been proposed, that allows modeling the MAC layer (communication scheduling) and the Network layer (routing) of the recently developed wireless industrial control protocols, such as WirelessHART (`www.hartcomm2.org`) and ISA-100 (`www.isa.org`).

Consider the networked control architecture illustrated in Figure 1, that consists of a plant $\mathcal{P}$ interconnected to a controller $\mathcal{C}$ via two multi-hop wireless communication networks $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$. We proved in [12] that for any *time-invariant* topology i of $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$, characterized by at least one path between the controller and the plant, it is always possible to design a controller $\mathcal{C}_i$, a routing and a scheduling to arbitrarily assign the eigenvalues of the closed loop system. Consider the following two application scenarios. In the first scenario (e.g. the mine application investigated in [13]), an industrial plant is connected to a controller via a multi-hop wireless communication network: the graph topology of the wireless network is time-varying because of link failures and battery discharge of the communication nodes. In the second scenario, a plant is connected to a controller via a swarm of mobile agents (e.g. robots [14] or UAVs [15]) equipped with wireless communication nodes: the graph topology of the wireless network is time-varying because of motion of the agents. In both scenarios, the time-varying topology perturbs the dynamics of the interconnected system N, and the controller is required to detect the current topology i of $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$ to apply the corresponding control law $\mathcal{C}_i$.

In this paper we suppose that the topology of $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$ is *time-varying* because of link failures, and provide a methodology to detect the set of faulty links using Fault Detection and Identification (FDI) methods. In the taxonomy of fault diagnosis techniques, we leverage on the model-based approach introduced by the pioneering works in [16], [17] on observer-based FDI, later pursued in [18] for linear systems and in [19] for non-linear systems.

As can be inferred from the recent survey [20], fault tolerant control and fault diagnosis is one of the main issues addressed in the research on NCSs. However, most of the existing literature on NCSs fault diagnosis (e.g. [21], [15]) usually addresses communication delays, and does not consider the effect of the communication protocol introduced by a Multi-hop Control Network. In [22], a procedure to minimize the number and cost of additional sensors, required to solve the FDI problem for *structured systems*, is presented.

The authors are with the Department of Electrical and Information Engineering, University of L'Aquila. Address: Via G. Gronchi, 18 Nucleo Industriale di Pile, L'Aquila, 67100 Italy. Tel: +39 328 941 5922. Email: {mariadomenica.dibenedetto, alessandro.dinnocenzo, emmanuele.serra}@univaq.it. The research leading to these results has received funding from the European Union Seventh Framework Programme [FP7/2007-2013] under grant agreement n257462 HYCON2 Network of excellence.

978-1-61284-799-3/11/$26.00 ©2011 IEEE

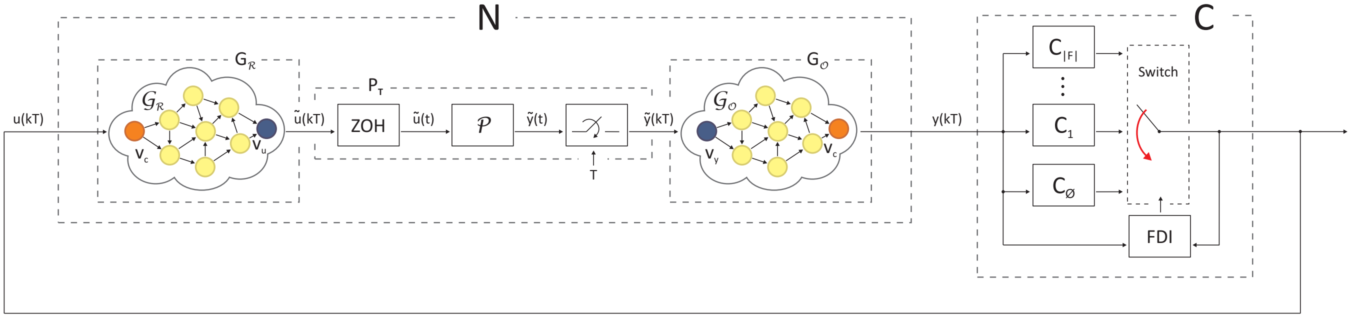

Fig. 1. Proposed control scheme of a MCN.

In [23], the design of an intrusion detection system is presented for a MCN, where the network *itself* acts as the controller. Our modeling framework differs from that developed in [23], since we model the MCN as an input-output system where the wireless networks *transfer* sensing and actuation data between a plant and a controller (they are *relay* networks), while in [23] the MCN is an autonomous system where the wireless network *itself* acts as a controller. Moreover, in our model we explicitly take into account the effect of the scheduling ordering of the node transmissions in the sensing and actuation data relay.

Our work differs from the existing literature since we characterize the communication link failures detection problem in a MCN as a FDI problem, and state necessary and sufficient conditions *on the plant dynamics* and *on the communication protocol*. Moreover, we provide a methodology to *explicitly* design the network topology, scheduling and routing of a communication protocol in order to satisfy link failure detection conditions of a MCN for any failure of communication links. The explicit design of scheduling and routing is a fundamental aspect of our contribution. In fact, as evidenced in [13], when applying a wireless industrial control protocol to the real scenario the topology of the wireless network introduces hard limitations in the choice of the scheduling. This is due to the fact that most of the wireless industrial control protocols suggest that the communication scheduling satisfies a specific ordering (see [13], [24] for more details). The results in [12] and in this paper mitigate these constraints, by proving that it is not required to perform scheduling according to a specific ordering. This allows to strongly reduce the scheduling length, as illustrated in [12]. An extended version of this paper can be found in [25].

In the paper we denote by $\mathbb{N}, \mathbb{R}, \mathbb{R}^+, \mathbb{R}_0^+$ respectively the sets of natural, real, positive real and non-negative real numbers. Given a matrix L, then $\mathcal{L}$, $\mathcal{N}(L)$ and $d(\mathcal{L})$ respectively denote the range of L, the Kernel of L and the dimension of $\mathcal{L}$. We denote by $\mathbf{e}_i$ the i-th column versor. We denote by $\mathbf{0}_{n\times m}$ the matrix of zeros with n rows and m columns, by $\mathbf{I}_n$ the identity matrix of dimension n, and by $\boldsymbol{\mathit{0}}$ the null space. Given a finite set F and a subset $f \subseteq F$, we define $F \setminus f$ the difference set and 2^F the power set.

II. Modeling of MCNs

The challenges in modeling MCNs are best explained by considering the recently developed wireless industrial control protocols, such as WirelessHART and ISA-100. These standards require that designers of wireless control networks define a communication scheduling for all communication nodes of a wireless network. For each working frequency, time is divided into slots of fixed duration Δ, and groups of Π time slots are called frames of duration $T = \Pi\Delta$ (see Figure 2). For each frame, a communication scheduling allows each node to transmit data only in a specified time slot and frequency, i.e. a mixed TDMA and FDMA MAC protocol is used. The communication scheduling is periodic with period Π, i.e. it is repeated in all frames. The standard specifies a syntax for defining scheduling and routing and a mechanism to apply them, but the issue of designing them remains a challenge for engineers and is currently done using heuristic rules. To allow systematic methods for designing the communication protocol configuration, a mathematical model of the effect of scheduling and routing on the control system is needed.

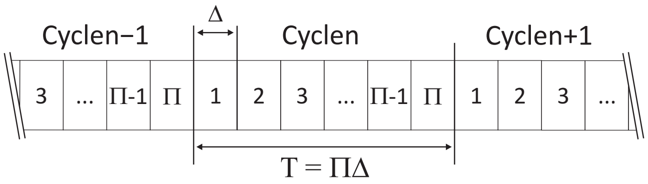

Fig. 2. Time-slotted structure of frames.

Definition 1: A SISO Multi-hop Control Network is a tuple $N = (\mathcal{P}, G_\mathcal{R}, \eta_\mathcal{R}, G_\mathcal{O}, \eta_\mathcal{O}, \Delta)$ where:

- $\mathcal{P} = (A^c_\mathcal{P}, B^c_\mathcal{P}, C^c_\mathcal{P})$ models a plant dynamics in terms of matrices of a continuous-time SISO LTI system.
- $G_\mathcal{R} = (V_\mathcal{R}, E_\mathcal{R}, W_\mathcal{R})$ is the controllability radio connectivity acyclic graph, where the vertices correspond to the nodes of the network, and an edge from v to v' means that v' can receive messages transmitted by v through the wireless communication link (v, v'). We denote v_c the special node of $V_\mathcal{R}$ that corresponds to the controller, and $v_u \in V_\mathcal{R}$ the special node that corresponds to the actuator of the input u of $\mathcal{P}$. The weight function $W_\mathcal{R} : E_\mathcal{R} \to \mathbb{R}^+$ associates to each link a positive constant. The role of $W_\mathcal{R}$ will be clear in the following definition of $\eta_\mathcal{R}$.
- $\eta_\mathcal{R}: \mathbb{N} \to 2^{E_\mathcal{R}}$ is the controllability communication scheduling function, that associates to each time slot of each frame a set of edges of the controllability

radio connectivity graph. Since in this paper we only consider a periodic scheduling that is repeated in all frames, we define the controllability communication scheduling function by $\eta_{\mathcal{R}} \colon \{1, \ldots, \Pi\} \to 2^{E_{\mathcal{R}}}$. The integer constant Π is the period of the controllability communication scheduling. The semantics of $\eta_{\mathcal{R}}$ is that $(v, v') \in \eta(h)$ if and only if at time slot h of each frame the data content of the node v is transmitted to the node v', multiplied by the weight $W_{\mathcal{R}}(v, v')$. We assume that each link can be scheduled only one time for each frame. This does not lead to loss of generality, since it is always possible to obtain an equivalent model that satisfies this constraint by appropriately splitting the nodes of the graph, as already illustrated in the memory slot graph definition of [11].

- $G_{\mathcal{O}} = (V_{\mathcal{O}}, E_{\mathcal{O}}, W_{\mathcal{O}})$ is the observability radio connectivity acyclic graph, and is defined similarly to $G_{\mathcal{R}}$. We denote with v_c the special node of $V_{\mathcal{O}}$ that corresponds to the controller, and $v_y \in V_{\mathcal{O}}$ the special node that corresponds to the sensor of the output y of $\mathcal{P}$.
- $\eta_{\mathcal{O}} \colon \{1, \ldots, \Pi\} \to 2^{E_{\mathcal{O}}}$ is the observability communication scheduling function, and is defined similarly to $\eta_{\mathcal{R}}$. We remark that Π is the same period as the controllability scheduling period.
- Δ is the time slot duration. As a consequence, $T = \Pi\Delta$ is the frame duration.

Definition 1 allows modeling communication protocols that specify TDMA, FDMA and/or CDMA access to a shared communication resource, for a set of communication nodes interconnected by an arbitrary radio connectivity graph. In particular, it allows modeling wireless multi-hop communication networks that implement protocols such as WirelessHART and ISA-100. Our MCN model differs from the framework developed in [11], since it allows modeling redundancy in data communication sending control data through multiple paths in the same frame and then merging these components according to the weight function. This kind of redundancy is called *multi-path routing* (or *flooding*, in the *communication* scientific community), and aims at rendering the MCN robust with respect to link failures and to mitigating the effect of packet losses.

For any given radio connectivity graph that models the communication range of each node, designing a scheduling function induces a communication scheduling (namely the time slot when each node is allowed to transmit) and a multipath routing (namely the set of paths that convey data from the input to the output of the connectivity graph) of the communication protocol. Since the scheduling function is periodic the induced communication scheduling is periodic, and the induced multi-path routing is static.

The dynamics of a MCN N can be modeled by the interconnection of blocks as in Figure 1. The block P_T is characterized by the discrete-time state space representation $(A_{\mathcal{P}}, B_{\mathcal{P}}, C_{\mathcal{P}})$ obtained by discretizing $(A^c_{\mathcal{P}}, B^c_{\mathcal{P}}, C^c_{\mathcal{P}})$ with sampling time $T = \Pi\Delta$. We assume that the plant $\mathcal{P}$ is stabilizable and detectable, and that $\mathcal{P} = (A^c_{\mathcal{P}}, B^c_{\mathcal{P}}, C^c_{\mathcal{P}})$ is the controllable and observable minimal representation. If this assumption does not hold, then even with an ideal interconnection between the controller and the plant it is clearly not possible to stabilize the closed loop system, and the control scheme in Figure 1 looses any interest.

The block $G_{\mathcal{R}}$ models the dynamics introduced by the data flow of the actuation data through the communication network represented by $G_{\mathcal{R}}$ according to the applied controllability scheduling $\eta_{\mathcal{R}}$. The following proposition proved in [12] characterizes the dynamics of $G_{\mathcal{R}}$ at the level of frames, induced by the data flow through the network at the level of time slots.

Proposition 1: [12] Given $G_{\mathcal{R}}$ and $\eta_{\mathcal{R}}$, the controllability graph can be modeled as a discrete time SISO LTI system with sampling time equal to the frame duration $T = \Pi\Delta$, and characterized by the following transfer function:

$$G_{\mathcal{R}}(z) = \sum_{d=1}^{D_{\mathcal{R}}} \frac{\gamma_{\mathcal{R}}(d)}{z^d},$$

where $D_{\mathcal{R}} \in \mathbb{N}$ is the maximum delay introduced by G_R, and $\forall d \in \{1, \ldots, D_{\mathcal{R}} - 1\}$, $\gamma_{\mathcal{R}}(d) \in \mathbb{R}_0^+$, $\gamma_{\mathcal{R}}(D_{\mathcal{R}}) \neq 0$.

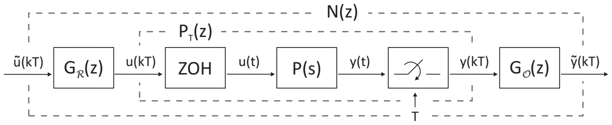

Fig. 3. Transfer function of the MCN interconnected system.

$G_{\mathcal{O}}(z)$ can be computed similarly. The dynamics of a MCN N can be modeled as in Figure 3, where each block is a discrete time SISO LTI system with sampling time equal to the frame duration, characterized by the transfer functions $G_{\mathcal{R}}(z)$, $P_T(z)$ and $G_{\mathcal{O}}(z)$.

Let $x_{\mathcal{O}} \in \mathbb{R}^{n_{\mathcal{O}}}$, $x_{\mathcal{P}} \in \mathbb{R}^{n_{\mathcal{P}}}$ and $x_{\mathcal{R}} \in \mathbb{R}^{n_{\mathcal{R}}}$ be respectively the states of the observability graph, of the plant, and of the controllability graph. We will denote by $x = \left[\begin{array}{ccc} x_{\mathcal{O}}^\top & x_{\mathcal{P}}^\top & x_{\mathcal{R}}^\top \end{array}\right]^\top$ the extended state of N, with $x \in \mathbb{R}^n$, and $n = n_{\mathcal{O}} + n_{\mathcal{P}} + n_{\mathcal{R}}$. The dynamics of N can also be described by the following state space representation:

$$\begin{aligned} x((k+1)T) &= Ax(kT) + Bu(kT), \\ y(kT) &= Cx(kT), \qquad u(kT),\ y(kT) \in \mathbb{R}, \end{aligned} \tag{1}$$

with:

$$A = \left[\begin{array}{ccc} A_{\mathcal{O}} & B_{\mathcal{O}}C_{\mathcal{P}} & \mathbf{0}_{n_{\mathcal{O}} \times n_{\mathcal{R}}} \\ \mathbf{0}_{n_{\mathcal{P}} \times n_{\mathcal{O}}} & A_{\mathcal{P}} & B_{\mathcal{P}}C_{\mathcal{R}} \\ \mathbf{0}_{n_{\mathcal{R}} \times n_{\mathcal{O}}} & \mathbf{0}_{n_{\mathcal{R}} \times n_{\mathcal{P}}} & A_{\mathcal{R}} \end{array}\right],$$

$$B = \left[\begin{array}{c} \mathbf{0}_{n_{\mathcal{O}} \times 1} \\ \mathbf{0}_{n_{\mathcal{P}} \times 1} \\ B_{\mathcal{R}} \end{array}\right], C = \left[\begin{array}{c} C_{\mathcal{O}}^\top \\ \mathbf{0}_{n_{\mathcal{P}} \times 1} \\ \mathbf{0}_{n_{\mathcal{R}} \times 1} \end{array}\right]^\top,$$

and

$$A_{\mathcal{R}} = \left[\begin{array}{lcr} 0 & \gamma_{\mathcal{R}}(D_{\mathcal{R}}) & \gamma_{\mathcal{R}}(D_{\mathcal{R}} - 1) \cdots \gamma_{\mathcal{R}}(2) \\ \mathbf{0}_{(D_{\mathcal{R}}-2) \times 1} & \mathbf{0}_{(D_{\mathcal{R}}-2) \times 1} & \mathbf{I}_{D_{\mathcal{R}}-2} \\ 0 & 0 & \mathbf{0}_{1 \times (D_{\mathcal{R}}-2)} \end{array}\right],$$

$$B_{\mathcal{R}} = \left[\begin{array}{l} \gamma_{\mathcal{R}}(1) \\ \mathbf{0}_{1 \times (D_{\mathcal{R}}-2)} \\ 1 \end{array}\right], C_{\mathcal{R}} = \left[\begin{array}{l} 1 \\ \mathbf{0}_{(D_{\mathcal{R}}-1) \times 1} \end{array}\right]^\top.$$

The matrices $(A_{\mathcal{O}}, B_{\mathcal{O}}, C_{\mathcal{O}})$ are defined similarly.

III. Fault Detection on MCNs

In this section we provide a methodology to detect the current dynamics of a MCN subject to link failures using Fault Detection and Identification (FDI) methods. The failure of a set of links $f \subseteq E_{\mathcal{R}} \cup E_{\mathcal{O}}$ on the dynamics (1) can be modeled as follows:

$$\begin{aligned} x((k+1)T) &= Ax(kT) + Bu(kT) + L_f m_f(kT) \\ y(kT) &= Cx(kT) \end{aligned} \qquad (2)$$

where $m_f(kT) : \mathbb{N} \to \mathbb{R}^{n+1}$ is an arbitrary function of time and $L_f\colon \mathbb{R}^{n+1} \to \mathbb{R}^n$ is called the failure signature map associated to the configuration of failures f. We define the failure signature maps as in Figure 4, where the d-th components $\delta_{\mathcal{R},f}(d)$ and $\delta_{\mathcal{O},f}(d)$ of the row vectors $\delta_{\mathcal{R},f} = \left[\begin{array}{ccc} \delta_{\mathcal{R},f}(D_{\mathcal{R}}) & \cdots & \delta_{\mathcal{R},f}(1) \end{array}\right]$ and $\delta_{\mathcal{O},f} = \left[\begin{array}{ccc} \delta_{\mathcal{O},f}(D_{\mathcal{O}}) & \cdots & \delta_{\mathcal{O},f}(1) \end{array}\right]$ are the perturbations introduced by the configuration of failures f in the paths of $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$ characterized by delay d. Since $\gamma_{\mathcal{R}}(d) \geq 0$ and $\gamma_{\mathcal{O}}(d) \geq 0$, and a failure of each path reduces the value of the corresponding component, then $\delta_{\mathcal{R},f}(d) \geq 0$ and $\delta_{\mathcal{O},f}(d) \geq 0$ for each $f \subseteq E_{\mathcal{R}} \cup E_{\mathcal{O}}$. In the absence of failures $L_{\varnothing} = \mathbf{0}_{n\times(n+1)}$.

The signal $m_f(kT)$ depends on the protocol applied by the communication nodes when the configuration of failures f occurs. By an appropriate choice of $m_f(kT)$, it is possible to model by (2) the dynamics of N when a failure occurs in the set of links f, for any protocol applied by the communication nodes in case of failure. As an example, if a node sets to 0 the data contribution incoming from a faulty link, then we can model this behavior by defining $m_f(kT) = \left[\begin{array}{cc} x(kT)^\top & u(kT)^\top \end{array}\right]^\top$. If a node uses the latest data received from a faulty link, then we can model this behavior by defining $m_f(kT) = \left[\begin{array}{cc} x(kT)^\top & u(kT)^\top \end{array}\right]^\top + \nu$, with $\nu \in \mathbb{R}^{n+1}$ a constant vector of real numbers.

To perform failure detection of a MCN with the aim of applying an appropriate control law for each dynamics induced by all failure configurations, we first need to define the set $\Phi \subseteq 2^{E_{\mathcal{R}} \cup E_{\mathcal{O}}}$ of failures we are interested in distinguishing. In fact, we need to distinguish two failures induced by sets of links f, f' only when they introduce different perturbations of the dynamics (1), namely when $L_f m_f(kT) \neq L_{f'} m_{f'}(kT)$. For this reason, we define Φ_Ω the set of equivalence classes $[f]$, each consisting of sets of links that affect the dynamics (1) by means of the same representative failure signal $L_f m_f(kT)$:

$$[f] = \{f' \subseteq E_{\mathcal{R}} \cup E_{\mathcal{O}} : \forall k \geq 0, L_{f'} m_{f'}(kT) = L_f m_f(kT)\}.$$

For simplicity of notation, we will denote in the following the equivalence class $[f]$ by a representative set of links $\varphi \in [f]$. In order to take into account simultaneous failures, we define the subset $\Phi_\Sigma \subset \Phi_\Omega$ of equivalence classes such that the perturbation introduced can be obtained as the sum of perturbations introduced by equivalence classes of Φ_Ω:

$$\Phi_\Sigma = \Bigg\{ f \in \Phi_\Omega : \Big(\exists\ p \in \mathbb{N}, \exists\ f_1, \ldots, f_p \in \Phi_\Omega \setminus f : \\ L_f m_f(kT) = \sum_{i=1}^{m} L_{f_i} m_{f_i}(kT) \Big) \Bigg\}.$$

Define the set of failures as $\Phi = \Phi_\Omega \setminus \Phi_\Sigma$. Φ always contains the equivalence class $\varnothing$, that corresponds to the absence of failures. It is easy to prove that the set Φ always exists and is unique. For this reason, we can associate to any given MCN N the corresponding unique set of failures Φ we are interested in distinguishing, and model their simultaneous occurrence as follows:

$$\begin{aligned} x((k+1)T) &= Ax(kT) + Bu(kT) + \sum_{\varphi \in \Phi} L_\varphi m_\varphi(kT), \\ y(kT) &= Cx(kT). \end{aligned} \qquad (3)$$

Given a MCN N and the corresponding faulty set Φ modeled by (3), we address the problem of detecting a failure $\varphi \in \Phi$ that is perturbing the dynamics of N by using the measures of the signals $u(\cdot)$, $y(\cdot)$. To this aim we leverage on the model-based approach developed in [18], which exploits a bank of LTI observer-like systems (called the residual generators) that take as input the signals $u(\cdot)$, $y(\cdot)$, and provides asymptotic estimates of $m_\varphi(kT)$ for any failure $\varphi \in \Phi$. This allows to identify which failures are affecting the dynamics of N. The problem of designing such residual generators with arbitrary asymptotic convergence rate on the model (3) is well known as the *Extended Fundamental Problem in Residual Generation* (EFPRG). Necessary and sufficient conditions for solving the EFPRG have been stated in [18]:

Theorem 2: Given the failure model (3), the EFPRG has a solution for the failure $\varphi \in \Phi$ if and only if:

$$\mathcal{S}^*(\bar{\mathcal{L}}_\varphi) \cap \mathcal{L}_\varphi = \boldsymbol{0},$$

where $\bar{\mathcal{L}}_\varphi := \sum_{\varphi' \in \Phi \setminus \varphi} \mathcal{L}_{\varphi'}$.

Given any $\mathcal{L} \subseteq \mathbb{R}^n$, the computation of $\mathcal{S}^*(\mathcal{L})$ can be performed by applying the (C,A)-Invariant Subspace Algorithm (CAISA) and the UnObservability Subspace Algorithm (UOSA), recursive algorithms provided in [26]. We define $\mathcal{W}^*(\mathcal{L})$ the fixed point of the following recursion (CAISA):

$$\mathcal{W}_{k+1}(\mathcal{L}) = \mathcal{L} + A\big(\mathcal{W}_k(\mathcal{L}) \cap \mathcal{N}(C)\big), \quad \mathcal{W}_0(\mathcal{L}) = \boldsymbol{0}.$$

We define $\mathcal{S}^*(\mathcal{L})$ the fixed point of the following recursion (UOSA):

$$\mathcal{S}_{k+1}(\mathcal{L}) = \mathcal{W}^*(\mathcal{L}) + A^{-1}\big(\mathcal{S}_k(\mathcal{L})\big) \cap \mathcal{N}(C), \quad \mathcal{S}_0(\mathcal{L}) = \mathbb{R}^n.$$

The following lemma provides a useful property of the CAISA and UOSA Algorithms.

Lemma 3: Let $\mathcal{L} \subseteq \mathcal{N}^\perp(C)$, then $\mathcal{W}^*(\mathcal{L}) = \mathcal{L}$, and $\mathcal{S}^*(\mathcal{L}) = \mathcal{L} + \mathcal{K}$ with $\mathcal{K} \subseteq \mathcal{N}(C)$. Moreover, if $\mathcal{L} = \big(\mathcal{N}(C)\big)^\perp$, then $\mathcal{S}^*(\mathcal{L}) = \mathbb{R}^n$.

For the sake of clarity, we address the link failure detection problem starting by two special cases. In the first case, we consider a multi-hop interconnection between the controller and the actuator and a single-hop interconnection between the sensor and the controller, namely the controllability graph $G_{\mathcal{O}}$ consists of two nodes connected by one link. In the second case, we consider a single-hop interconnection between the controller and the actuator, namely the controllability graph $G_{\mathcal{R}}$ consists of two nodes connected by one link, and a multi-hop interconnection between the sensor and the controller. In the third case, we consider the general case when both $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$ are multi-hop communication networks.

$$L_f = \begin{bmatrix} 0 & -\delta_{\mathcal{O},f} & \mathbf{0}_{1\times n_{\mathcal{P}}} & \mathbf{0}_{1\times n_{\mathcal{R}}} \\ \mathbf{0}_{(n_{\mathcal{O}}+n_{\mathcal{P}}-1)\times 1} & \mathbf{0}_{(n_{\mathcal{O}}+n_{\mathcal{P}}-1)\times n_{\mathcal{O}}} & \mathbf{0}_{(n_{\mathcal{O}}+n_{\mathcal{P}}-1)\times n_{\mathcal{P}}} & \mathbf{0}_{(n_{\mathcal{O}}+n_{\mathcal{P}}-1)\times n_{\mathcal{R}}} \\ 0 & \mathbf{0}_{1\times n_{\mathcal{O}}} & \mathbf{0}_{1\times n_{\mathcal{P}}} & -\delta_{\mathcal{R},f} \\ \mathbf{0}_{(n_{\mathcal{R}}-1)\times 1} & \mathbf{0}_{(n_{\mathcal{R}}-1)\times n_{\mathcal{O}}} & \mathbf{0}_{(n_{\mathcal{R}}-1)\times n_{\mathcal{P}}} & \mathbf{0}_{(n_{\mathcal{R}}-1)\times n_{\mathcal{R}}} \end{bmatrix}$$

Fig. 4. Matrix L_f.

A. $G_{\mathcal{R}}$ multi-hop and $G_{\mathcal{O}}$ single-hop

If $G_{\mathcal{O}}$ consists of a single-hop, then $n_{\mathcal{O}} = 1$, $A_{\mathcal{O}} = 0$, $B_{\mathcal{O}} = C_{\mathcal{O}} = 1$. As illustrated in [18], each L_φ can be assumed monic with no loss of generality, since when failures are not present the corresponding components of $m_\varphi(kT)$ are identically zero. For this reason, by an appropriate choice of $m_\varphi(kT)$, we define the L_φ in (3) as follows:

$$L_\varphi = \begin{bmatrix} \mathbf{0}_{(n_{\mathcal{O}}+n_{\mathcal{P}})\times n_{\mathcal{R}}} \\ -\delta_\varphi \\ \mathbf{0}_{(n_{\mathcal{R}}-1)\times n_{\mathcal{R}}} \end{bmatrix},$$

where $\delta_\varphi \in (\mathbb{R}_0^+)^{n_{\mathcal{R}}}$ is a row vector and $L_\varphi \colon \mathbb{R}^{n_{\mathcal{R}}} \to \mathbb{R}^n$. The following theorem states a negative result.

Theorem 4: Let a MCN N and the corresponding faulty set Φ be given, where $G_{\mathcal{R}}$ is multi-hop and $G_{\mathcal{O}}$ is single-hop. Then the EFPRG can be solved for each $\varphi \in \Phi$ if and only if $|\Phi| \le 2$.

The above theorem states that if the controllability graph is multi-hop and the observability graph is single-hop, then it is not possible to distinguish failures in a set Φ, unless Φ is trivial. In the following section, we will show that more can be done if the controllability graph is single-hop and the observability graph is multi-hop.

B. $G_{\mathcal{R}}$ single-hop and $G_{\mathcal{O}}$ multi-hop

If $G_{\mathcal{R}}$ consists of a single-hop, then $n_{\mathcal{R}} = 1$, $A_{\mathcal{R}} = 0$, $B_{\mathcal{R}} = C_{\mathcal{R}} = 1$. Using the same reasoning as in the above section, we can define a set Φ of equivalence classes of link failures that equally perturb the dynamics (3). Since in this case the failures occur in the observability graph, by an appropriate choice of $m_\varphi(kT)$ we define $L_\varphi : \mathbb{R}^{n_{\mathcal{O}}} \to \mathbb{R}^n$ the failure signature map associated to the equivalence classes $\varphi \in \Phi$:

$$L_\varphi = \begin{bmatrix} -\delta_\varphi \\ \mathbf{0}_{(n-1)\times n_{\mathcal{O}}} \end{bmatrix},$$

where $\delta_\varphi \in (\mathbb{R}_0^+)^{n_{\mathcal{O}}}$ is a row vector and each component $\delta_\varphi(d)$ is the perturbation introduced by a failure φ in the paths of $G_{\mathcal{O}}$ characterized by delay d. The following theorem motivates an extension of the model (3).

Theorem 5: Let a MCN N and the corresponding faulty set Φ be given, where $G_{\mathcal{R}}$ is single-hop and $G_{\mathcal{O}}$ is multi-hop. Then the EFPRG can be solved for each $\varphi \in \Phi$ only if the following condition holds:

$$d\Big(\big(\mathcal{N}(C)\big)^\perp\Big) \ge \sum_{\varphi\in\Phi} d(\mathcal{L}_\varphi) := n_\Phi.$$

The above theorem shows that it is not possible to design a residual generator for each $\varphi \in \Phi$ if the rank of the matrix C is smaller than n_Φ. In particular, in system (1) the rank of C is 1, and n_Φ is equal to 1 only if the set Φ is trivial, namely it contains the equivalence class $\varnothing$ and just one equivalence class φ. For this reason, we need to consider a more general model for the observability graph. More precisely, we consider observability graphs characterized by n_S terminating nodes $v_1, \ldots, v_{n_S}$, with $n_S \ge n_\Phi$. This can be modeled without loss of generality by redefining matrices $A_{\mathcal{O}}$, $B_{\mathcal{O}}$ and $C_{\mathcal{O}}$ as follows:

$$A_{\mathcal{O}} = \left[\begin{array}{cc|ccc} \mathbf{0}_{1\times n_S} & \gamma_1(D_{\mathcal{O}}) & \gamma_1(D_{\mathcal{O}}-1) & \cdots & \gamma_1(2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{1\times n_S} & \gamma_{n_S}(D_{\mathcal{O}}) & \gamma_{n_S}(D_{\mathcal{O}}-1) & \cdots & \gamma_{n_S}(2) \\ \hline \mathbf{0}_{(D_{\mathcal{O}}-2)\times n_S} & \mathbf{0}_{(D_{\mathcal{O}}-2)\times 1} & \multicolumn{3}{c}{\mathbf{I}_{D_{\mathcal{O}}-2}} \\ \mathbf{0}_{1\times n_S} & 0 & \multicolumn{3}{c}{\mathbf{0}_{1\times(D_{\mathcal{O}}-2)}} \end{array}\right],$$

$$B_{\mathcal{O}} = \begin{bmatrix} \gamma_1(1) & \cdots & \gamma_{n_S}(1) & \mathbf{0}_{1\times(D_{\mathcal{O}}-2)} & 1 \end{bmatrix}^\top,$$
$$C_{\mathcal{O}} = \begin{bmatrix} \mathbf{I}_{n_S} & \mathbf{0}_{n_S\times(D_{\mathcal{O}}-1)} \end{bmatrix}.$$

where $n_{\mathcal{O}} = D_{\mathcal{O}} + n_S - 1$ is the new dimension of the state space. The failure signature maps $L_\varphi \colon \mathbb{R}^{D_{\mathcal{O}}} \to \mathbb{R}^n$ are:

$$L_\varphi = \begin{bmatrix} -\delta_{\varphi,1} \\ \vdots \\ -\delta_{\varphi,n_S} \\ \mathbf{0}_{(n-n_S)\times D_{\mathcal{O}}} \end{bmatrix}, \tag{4}$$

where $\delta_{\varphi,i} \in (\mathbb{R}_0^+)^{D_{\mathcal{O}}}$ and each component $\delta_{\varphi,i}(d)$ is the perturbation introduced by a failure φ in the paths of $G_{\mathcal{O}}$ terminating with node v_i and characterized by delay d. The following theorem states necessary and sufficient conditions to solve the EFPRG when $G_{\mathcal{O}}$ is multi-hop and $G_{\mathcal{R}}$ is single-hop.

Theorem 6: Let a MCN N and the corresponding faulty set Φ be given, where $G_{\mathcal{R}}$ is single-hop and $G_{\mathcal{O}}$ is multi-hop with $n_S \ge n_\Phi$ terminating nodes. Then the EFPRG can be solved for each $\varphi \in \Phi$ if and only if the following condition holds:

$$d(\mathcal{L}_\Phi) = n_\Phi, \tag{5}$$

where the matrix $L_\Phi := \begin{bmatrix} L_{\varphi_1} & L_{\varphi_2} & \cdots & L_{\varphi_{|\Phi|}} \end{bmatrix}$ is the juxtaposition of all failure signature maps in Φ and has dimensions $n_S \times n_\Phi$.

The following theorem characterizes the relation between Condition (5) and the topology of $G_{\mathcal{O}}(\eta_{\mathcal{O}})$.

Theorem 7: Let a MCN N and the corresponding faulty set Φ be given, where $G_{\mathcal{R}}$ is single-hop and $G_{\mathcal{O}}$ is multi-hop with n_S terminating nodes. Then, $d(\mathcal{L}_\Phi) = n_\Phi$ if and only if $G_{\mathcal{O}}(\eta_{\mathcal{O}})$ is a tree, where v_y is the root node and $v_1, \ldots, v_{n_S}$ are the leaves.

Corollary 8: Let a MCN N and the corresponding faulty set Φ be given, where $G_{\mathcal{R}}$ is single-hop and $G_{\mathcal{O}}$ is multi-hop with n_S terminating nodes. If the EFPRG can be solved for each $\varphi \in \Phi$, then $n_S = n_\Phi$ and $\mathcal{L}_\Phi = \big(\mathcal{N}(C)\big)^\perp$.

The necessary and sufficient condition given in Theorem 7 provides a hard constraint on the topology of $G_{\mathcal{O}}(\eta_{\mathcal{O}})$ induced by the scheduling $\eta_{\mathcal{O}}$. This is not surprising, since we require to solve the EFPRG for the set Φ of *all* configurations of failures that perturb the dynamics (3). From an implementation point of view, this constraint can be both interpreted as hardware or software redundancy. In the former case, the tree structure of $G_{\mathcal{O}}(\eta_{\mathcal{O}})$ provides a hardware separation for all paths from v_y to the terminating nodes. However, a tree communication graph might be not always implementable in real cases: therefore, the constraint on $G_{\mathcal{O}}(\eta_{\mathcal{O}})$ can be implemented by using, for those communication nodes that receive data from multiple incoming links, separate memory slots for each of the incoming data. These nodes will transmit distinct data for each memory slot, thus providing a software separation for all paths from v_y to the terminating nodes. In general, a combination of the above approaches is reasonably implementable in a real communication network. An interesting future research direction is relating the properties of $G_{\mathcal{O}}(\eta_{\mathcal{O}})$ with Condition (5) when the number of simultaneous failures that can occur is bounded, or when failures can not occur in some *secure* paths of the communication network.

C. $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$ multi-hop

When both $G_{\mathcal{R}}$ and $G_{\mathcal{O}}$ are multi-hop, we need to define the set $\Phi = \Phi_{\mathcal{R}} \cup \Phi_{\mathcal{O}}$ of equivalence classes that equally perturb the dynamics (3). In this case, failures occur in both the controllability and observability graphs. Therefore, by an appropriate choice of $m_{\varphi}(kT)$, we define the failure signature maps associated to the equivalence classes $\varphi_{\mathcal{R}} \in \Phi_{\mathcal{R}}$ and $\varphi_{\mathcal{O}} \in \Phi_{\mathcal{O}}$ by:

$$L_{\varphi_{\mathcal{R}}} = \left[\begin{array}{c} \mathbf{0}_{(n_{\mathcal{O}}+n_{\mathcal{P}})\times n_{\mathcal{R}}} \\ -\delta_{\varphi_{\mathcal{R}}} \\ \mathbf{0}_{(n_{\mathcal{R}}-1)\times n_{\mathcal{R}}} \end{array} \right],\ L_{\varphi_{\mathcal{O}}} = \left[\begin{array}{c} -\delta_{\varphi_{\mathcal{O}}} \\ \mathbf{0}_{(n-n_{\mathcal{S}})\times n_{\mathcal{O}}} \end{array} \right],$$

with $\delta_{\varphi_{\mathcal{R}}} \in (\mathbb{R}_0^+)^{D_{\mathcal{R}}}$ a row vector, and $\delta_{\varphi_{\mathcal{O}}} \in (\mathbb{R}_0^+)^{n_{\mathcal{S}}\times D_{\mathcal{O}}}$ as defined in (4).

The following theorem states that it is not possible to detect failures in the controllability and observability graphs using the measurements of the observability graph.

Theorem 9: Let a MCN N and the corresponding faulty set Φ be given, where $G_{\mathcal{R}}$ is multi-hop and $G_{\mathcal{O}}$ is multi-hop with $n_{\mathcal{S}}$ terminating nodes. Then the EFPRG is not solvable for any $\varphi_{\mathcal{R}} \in \Phi_{\mathcal{R}}$ and any $\varphi_{\mathcal{O}} \in \Phi_{\mathcal{O}}$.

Theorem 9 states that, in order to detect failures in the observability graph, the controllability graph must not be subject to failures. By a practical point of view, the communication protocol in the controllability graph is required to implement failure detection using handshaking messages between nodes and inform the controller about the set of faulty links.

References

[1] I.F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, 2004.

[2] J. Song, S. Han, A.K. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control," in *RTAS*, 2008.

[3] J. Song, S. Han, X. Zhu, A.K. Mok, D. Chen, and M. Nixon, "A Complete WirelessHART Network," in *ACME*, 2008, pp. 381–382.

[4] W. Zhang, M.S. Branicky, and S.M. Phillips, "Stability of Networked Control Systems," *IEEE Control Systems Magazine*, vol. 21, no. 1, pp. 84–99, February 2001.

[5] G.C. Walsh and H. Ye, "Scheduling of Networked Control Systems," *IEEE Control Systems Magazine*, pp. 57–65, February 2001.

[6] P. Antsaklis and J. Baillieul, "Guest Editorial Special Issue on Networked Control Systems," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1421–1423, September 2004.

[7] J.P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A Survey of Recent Results in Networked Control Systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, January 2007.

[8] W.P.M.H. Heemels, A.R. Teel, N. van de Wouw, and D. Nešić, "Networked Control Systems With Communication Constraints: Tradeoffs Between Transmission Intervals, Delays and Performance," *IEEE Transactions on Automatic Control*, vol. 55, no. 8, pp. 1781 –1796, August 2010.

[9] M. Andersson, D. Henriksson, A. Cervin, and K. Arzen, "Simulation of Wireless Networked Control Systems," in *Proceedings of the 44th IEEE Conference on Decision and Control and European Control Conference*, 2005, pp. 476–481.

[10] R. Alur, A. D'Innocenzo, K.H. Johansson, G.J. Pappas, and G. Weiss, "Modeling and Analysis of Multi-Hop Control Networks," in *Proceedings of the 15th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2009.

[11] R. Alur, A. D'Innocenzo, K.H. Johansson, G.J. Pappas, and G. Weiss, "Compositional Modeling and Analysis of Multi-Hop Control Networks," *IEEE Transactions on Automatic Control*, 2011, accepted for publication as regular paper.

[12] M.D. Di Benedetto, A. D'Innocenzo, and E. Serra, "Fault Tolerant Stabilizability of Multi-Hop Control Networks," in *Proceedings of the 18th IFAC World Congress, Milan, Italy*, 2011, preprint available at arXiv:1103.4340v1.

[13] A. D'Innocenzo, G. Weiss, R. Alur, A.J. Isaksson, K.H. Johansson, and G.J. Pappas, "Scalable Scheduling Algorithms for Wireless Networked Control Systems," in *Proceedings of the 5th IEEE Conference on Automation Science and Engineering (CASE)*, 2009.

[14] M.M. Zavlanos and G.J. Pappas, "Distributed Connectivity Control of Mobile Networks," in *Proceedings of the 46th IEEE Conference on Decision and Control*, December 2007, pp. 3591 –3596.

[15] N. Meskin and K. Khorasani, "Actuator Fault Detection and Isolation for a Network of Unmanned Vehicles," *IEEE Transactions on Automatic Control*, vol. 54, no. 4, pp. 835 –840, April 2009.

[16] R. Beard, "Failure Accomondation in Linear Systems Through Self-Reorganization," Ph.D. dissertation, MIT, 1971.

[17] H. Jones, "Failure Detection in Linear Systems," Ph.D. dissertation, MIT, 1973.

[18] M.-A. Massoumnia, G.C. Verghese, and A.S. Willsky, "Failure Detection and Identification," *IEEE Transactions on Automatic Control*, vol. 34, no. 3, pp. 316 –321, Mar. 1989.

[19] C. De Persis and A. Isidori, "A Geometric Approach to Nonlinear Fault Detection and Isolation," *IEEE Transactions on Automatic Control*, vol. 46, no. 6, pp. 853 –865, June 2001.

[20] R. Gupta and M.-Y. Chow, "Networked Control System: Overview and Research Trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527 –2535, July 2010.

[21] Y. Wang, S.X. Ding, H. Ye, and G. Wang, "A New Fault Detection Scheme for Networked Control Systems Subject to Uncertain Time-Varying Delay," *IEEE Transactions on Signal Processing*, vol. 56, no. 10, pp. 5258 –5268, October 2008.

[22] C. Commault and J.-M. Dion, "Sensor Location for Diagnosis in Linear Systems: A Structural Analysis," *IEEE Transactions on Automatic Control*, vol. 52, no. 2, pp. 155 –169, February 2007.

[23] S. Sundaram, M. Pajic, C.N. Hadjicostis, R. Mangharam, and G.J. Pappas, "The Wireless Control Network: Monitoring for Malicious Behavior," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC)*, December 2010, pp. 5979 –5984.

[24] M.D. Di Benedetto, A. D'Innocenzo, and E. Serra, "Dynamical Power Optimization by Decentralized Routing Control in Multi-Hop Wireless Control Networks," in *Proceedings of the 18th IFAC World Congress, Milan, Italy*, 2011.

[25] A. D'Innocenzo, E. Serra, and M.D. Di Benedetto, "Link failure detection in multi-hop control networks," in *arXiv:1108.5316*, 2011.

[26] W.M. Wonham, *Linear Multivariable Control: a Geometric Approach*, 2nd ed., ser. Applications of Mathematics. Springer-Verlag, 1979.