Fault Tolerant Stabilizability of Multi-Hop Control Networks

M.D. Di Benedetto, A. D’Innocenzo, and E. Serra

Department of Electrical and Information Engineering,
Center of Excellence DEWS, University of L’Aquila - L’Aquila, Italy.

Abstract: A Multi-hop Control Network (MCN) consists of a plant where the communication between sensor, actuator and computational unit is supported by a wireless multi-hop 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., Akyildiz, I.F. and Kasimoglu, I.H. (2004), Song et al. (2008a), Song et al. (2008b)). Although multi-hop networks 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 systems. The design of the control system has to take into account 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. Using a wireless communication medium, new issues such as fading and time-varying throughput in communication channels have to be addressed, and communication delays and packet losses may occur. Moreover, 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. While most of the research on networked control systems is on direct networking, we focus on multi-hop networks. In Section 2 we relate our research to the existing scientific literature on Networked Control Systems. In particular, the modeling and stability verification problem for a MIMO LTI plant embedded in a multi-hop control network (MCN) when the controller is already designed has been addressed in Alur et al. (2009). 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). The mathematical framework defined in Alur et al. (2009) is compositional, namely it is possible to exploit compositional operators of automata to design scalable scheduling and routing for multiple control loops closed on the same multi-hop control network.

In this paper, starting from the mathematical framework developed in Alur et al. (2009), we address the novel issue of characterizing controllability and observability of a continuous-time SISO LTI plant embedded in a MCN that implements scheduling and routing protocols, and where failures of communication links may occur. We motivate the exploitation of redundancy in data communication (i.e., sending sensing and actuation data through multiple paths) with the aim of rendering the system robust with respect to link failures (e.g., when the battery of a node discharges or a communication channel goes down), and to mitigate the effect of packet losses (e.g., transmission errors). In Section 3 we extend the model in Alur et al. (2009) to model redundancy, by defining a weight function that specifies how the duplicate information transmitted through the multi-hop network is merged, and by defining a semantics of the redundant data flow through the network. Of course, all results stated in this paper also apply to MCN that do not exploit redundancy.

We remark that the differences introduced in this paper with respect to the model in Alur et al. (2009) do not
invalidate compositionality of the framework. As a first result of this paper, given a MCN, we state in Section 4 necessary and sufficient controllability and observability conditions on the plant dynamics and on the scheduling and routing of the communication network. As a second result, given a MCN and a set of failures configurations of the communication nodes, we state in Section 5 necessary and sufficient conditions on the plant dynamics, on the scheduling and routing of the communication network, and on the set of failures configurations, such that there exists a scheduling and routing configuration that guarantees reachability and observability conditions of the MCN for each failures configuration. Since we adopt a constructive proof, we provide a methodology to configure scheduling and routing of a MCN, in order to satisfy controllability and observability of the closed loop system for any fault occurrence in a given set of failures configurations. An extended version of this paper can be found in M.D. Di Benedetto et al. (2011).

2. RELATED WORK

There exists a wide literature on Networked Control Systems, see for example Zhang et al. (2001), Walsh, G.C. and Ye (2001), Antsaklis and Basillieul (2004), Hespanhua, J.P. et al. (2007) and references therein. The literature on robust stability of networked control systems (see e.g. Lin et al. (2003), Cloosterman et al. (2006), Shi et al. (2006)) generally addresses stability analysis in presence of packet loss and variable delays, but does not take into account the non-idealities introduced by scheduling and routing communication protocols of multi-hop control networks. When relating our paper with the current research about the interaction of control networks and communication protocols, most efforts in the literature focus on scheduling message and sampling time assignment for sensors/actuators and controllers interconnected by wired common-bus networks, e.g. Aström and Wittenmark (1997), Walsh, G.C. et al. (2002), Yook, J.K. et al. (2002), Tabbara and Nesić (2007), Tabbara et al. (2007). The authors in Witrant et al. (2007) use model predictive control to stabilize a plant over a multi-hop control network, by only considering delay introduced by the routing policy. However, what is needed for modeling and analyzing control protocols on multi hop control networks is an integrated framework for analyzing/co-designing network topology, scheduling, routing, transmission errors and control. To the best of our knowledge, the only formal model of multi-hop wireless sensor and actuator networks is reported in Andersson et al. (2005). In this paper, a simulation environment that facilitates simulation of computer nodes and communication networks interacting with the continuous-time dynamics of the real world is presented. The main difference between the work presented in Andersson et al. (2005) and this work is that here we provide results on a formal mathematical model that takes into account plant dynamics and scheduling-routing dynamics. At the best of our knowledge, our work is pioneering in addressing the controller design problem for multi-hop control networks that implement standardized scheduling and routing communication protocols, in order to enable co-design of controller, scheduling and routing.

3. MODELING OF MCNS

The challenges in modeling multi-hop control networks are best explained by considering the recently developed wireless industrial control protocols, such as WirelessHART and ISA-100. These standards allow designers of wireless control networks to distribute a synchronous communication schedule to all communication nodes of a wireless network. For each working frequency, time is divided into slots of fixed time length $\Delta$ (see Figure 1). A periodic scheduling composed by $\Pi$ time slots allows each node to transmit data only in a subset of time slots and frequencies, i.e. a mixed TDMA and FDMA MAC protocol is used. The standard specifies a syntax for defining schedules and a mechanism to apply them. However, the issue of designing schedules and routing remains a challenge for the engineers, and is currently done using heuristic rules. To allow systematic methods for designing schedules that preserve controllability and observability of a plant, a mathematical model of the effect of scheduling and routing on the control system is needed. The MCN model we propose in this paper allows modeling multi-hop control networks that implement the protocols WirelessHART and ISA-100, but it is much more general: it allows modeling general routing and scheduling 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.

Fig. 1. Time-slotted structure of the scheduling period.

Definition 1. A SISO Multi-hop control network (MCN) is a tuple $\mathcal{N} = (\mathcal{P}, \mathcal{G}_R, \eta_R, \mathcal{G}_O, \eta_O, \Delta)$ where:

- $\mathcal{P} = (A, B, C)$ models a plant dynamics in terms of matrices of a continuous-time SISO LTI system.
- $\mathcal{G}_R = (V_R, E_R, W_R)$ is the controllability radio connectivity acyclic graph, where the vertices correspond to the nodes of the network, and an edge from $v_i$ to $v_j$ means that $v_j$ can receive messages transmitted by $v_i$ through the wireless communication link $(v_i, v_j)$. We denote $v_{s_i}$ the special node of $V_R$ that corresponds to the controller, and $v_{a_i} \in V_R$ the special node that corresponds to the actuator of the input $u$ of $\mathcal{P}$. The weight function $W_R : E_R \rightarrow \mathbb{R}^+ \cup \{0\}$ associates to each link a positive constant. The semantics of $W_R$ will be clear in the following definition of $\eta_R$.
- $\eta_R : \{1, \ldots, \Pi\} \rightarrow 2^{E_R}$ is the controllability communication scheduling function, that associates to each time slot $k \in \{1, \ldots, \Pi\}$ a set of edges of the controllability radio connectivity graph. The integer constant $\Pi$ is the period of the reachability communication scheduling. The semantics of $\eta_R$ is that $(v_i, v_j) \in \eta(k)$ if and only if at time slot $k$ the data content of the node $v_i$ is transmitted to the node $v_j$, multiplied for the weight $W_R(v_i, v_j)$.
- $\mathcal{G}_O = (V_O, E_O, W_O)$ is the observability radio connectivity acyclic graph, and is defined similarly to $\mathcal{G}_R$.

1 We denote by $\mathbb{R}^+$ the set of strictly positive reals.
The above definitions can be given similarly for observability graph $G_o$ and scheduling $\eta_o$. The semantics of a MCN $\mathcal{N}$ can be modeled by the interconnection of $N$ blocks as in Figure 2. The block $P_T$ is characterized by the transfer function $G_R(z)$ of the discrete-time plant $P_T$, obtained by discretizing $P(s) = C(sI - A)^{-1}B$ with sampling time $T = \Pi\Delta$ equal to the scheduling period duration. The block $G_R$ models the dynamics introduced by the data flow of the actuation data through the network $G_R$ according to the applied controllability scheduling $\eta_R$. In order to define the dynamical behavior of $G_R$, we need to define the semantics of the data flow through the network, according to the scheduling $\eta_R$. We associate to the controller node $v_c$ a real value $\mu_c(kT)$ at time $k$, and we assume that $\mu_c$ is periodically updated with a new control command at the beginning of each scheduling period and holds this value for the whole time duration of the scheduling period. Formally, $\mu_c(kT) = \bar{u}(kT)$. The dynamics of the other nodes needs to be defined at the level of the time slots. We associate to each other node $v_j \in V_R \setminus \{v_c\}$ a real value $\mu_{ij}(h)$ at time slot $h$, for each node $v_i$ belonging to the set $\text{inc}(v_j) = \{v_i \in V_R : (v_i, v_j) \in E_R\}$ of edges incoming in $v_j$. Formally: $\mu_{ij}(h) = \sum_{v_i \in \text{inc}(v_j)} \mu_i(h)$ is the sum of the variables associated to node $v_i$ in the time slot $h$. When the link from $v_i$ to $v_j$ is scheduled at time slot $h$, the variable of node $v_i$ is updated with the sum of the variables of node $v_i$ multiplied for the link weight $W_R(v_i, v_j)$. Formally, for each $v_j \in V_R \setminus \{v_c\}$ and for each time slot $h \in \{1, \ldots, N\}$:

$$\mu_{ij}(h + 1) = \left\{ \begin{array}{ll}
\mu_{ij}(h) + W_R(v_i, v_j) \mu_i(h) & \text{if } (v_i, v_j) \notin \eta_R(h), \\
W_R(v_i, v_j) \mu_i(h) & \text{if } (v_i, v_j) \in \eta_R(h).
\end{array} \right.$$

Finally, the actuator node $v_a$ periodically actuates a new actuation command at the beginning of each scheduling period on the basis of its variable $\mu_a$, and holds this value for the whole time duration of the scheduling period. Formally: $u(kT) = \mu_a(kT) = \sum_{v_i \in \text{inc}(v_a)} \mu_i(kT)$. On the basis of the semantics defined above, it is possible to model the dynamical behavior of $G_R$ as follows.

**Proposition 1.** Given $G_R$ and $\eta_R$, the block $G_R$ can be modeled as a discrete time SISO LTI system with sampling time equal to the scheduling period duration $T = \Pi\Delta$, and characterized by the following transfer function:

$$G_R(z) = \sum_{i=1}^{D_R} \gamma_R(i), \quad \gamma_R(i) = \sum_{\rho \in \mathbb{R}^T} W_R(\rho),$$

with $\gamma_R(D_R) \neq 0$, $\forall i \in \{1, \ldots, D_R - 1\}$, $\gamma_R(i) \in \mathbb{R}^T \cup \{0\}$.

We consider a single-path scenario for the controllability radio connectivity graph and scheduling. $P = (A, B, C)$ represents a continuous-time SISO LTI plant characterized by the following transfer function:

$$P(s) = \frac{1}{(s^2 - 69.3\Delta s + 25880)(s^2 + 24670)}$$

On the basis of the above reasoning, it is possible to model the semantics of a MCN $\mathcal{N}$ as in Figure 3, where each block is a discrete time SISO LTI system with sampling time equal to the scheduling period duration, characterized by the transfer functions $G_R(z)$, $P_T(z)$ and $G_O(z)$. The following example motivates the use of redundancy in MCNs characterized by failures in links.

**Example 1.** Consider a MCN $\mathcal{N}_1 = (P, G_R, \eta_R, G_O, \eta_o, \Delta)$. We remark that, since we are addressing controllability analysis, we do not consider the effect of observability radio connectivity graph and scheduling. $P = (A, B, C)$ represents a continuous-time SISO LTI plant characterized by the following transfer function:

$$P(s) = \frac{1}{(s^2 - 69.3\Delta s + 25880)(s^2 + 24670)}$$

We consider a single-path scenario for the controllability radio connectivity graph $G_R$ as shown in Figure 4, where $v_c = v_1$ and $v_a = v_3$. Let us define two schedules on $G_R$, which convey actuation data from $v_c$ to $v_a$: we define $\eta_R$ as the string $\langle \{v_1, v_2\} \rangle$, $\{v_2, v_3\}$, and $\eta'_R$ as the string $\langle \{v_1, v_2\} \rangle$, $\{v_3, v_2\}$, $\{v_1, v_3\}$, $\{v_2, v_3\}$, $\{v_1, v_2\}$, $\{v_3, v_2\}$, $\{v_1, v_3\}$, $\{v_3, v_2\}$. Both scheduling have period $I = 2$. Let $\Delta$ be the duration in seconds of a single time slot of the scheduling, for example 10 ms as in WirelessHART: then the duration of the whole scheduling period is given by $T = \Pi\Delta = 2 \cdot 10$ ms = 20 ms. If we apply $\eta'_R$, the block $G_R$ introduces a delay equal to 1 scheduling period, i.e. $u(kT) = \bar{u}((k - 1)T)$. In fact, using $\eta'_R$, the value of $\bar{u}$ is conveyed first to $v_2$ and then to $v_3$ in just one scheduling period. Thus, the block $G_R$ is characterized by the transfer function $G_R(z) = \frac{1}{z}$. If we apply $\eta''_R$, the
block $G_R$ introduces a delay equal to 2 scheduling periods, i.e. $u(kT) = ˜u((k − 2)T)$. In fact, using $η''_R$, the value of $u$ is conveyed to $v_2$ in the first period, and to $v_3$ in the second period. Thus, the block $G_R$ is characterized by the transfer function $G_R(z) = \frac{1}{T}$. It is easy to verify that, in both cases, the cascade of systems $G_R$ and $P_T$ always satisfies the controllability condition because $G_R(z)$ does not have any zeros, so its interconnection to $P_T(z)$ can not introduce any pole cancelation. However, if one of the links of $G_R$ is damaged, then $G_R(z) = 0$ and the MCN does not satisfy the controllability condition. Moreover, an error in one of the data transmissions between $v_1$, $v_2$ and $v_3$ is totally transferred to the input of the plant. □

The above example motivates the exploitation of redundancy, for instance by sending control data through multiple paths in the same scheduling period and then merging these components in the actuator node. We call this approach redundancy by static multi-path routing. An alternative is sending control data through a single-path (route) for each scheduling period, and dynamically updating this route in order to avoid faulty nodes in the new route. We call this approach redundancy by dynamic single-path routing. At the best of our knowledge, although there exist several algorithms for static (e.g. Dijkstra and Bellman-Ford) and dynamic routing Ash (1997) of multi-hop networks, none of them have been designed to address control specifications. In this paper, we only address the problem of designing redundancy by static multi-path routing, in order to preserve controllability and observability structural properties of a MCN. The Pros of applying redundancy by static multi-path routing are the following: first, controllability of the MCN is robust to failures of links; and second, the effect of data transmission errors on a single link is alleviated when averaging all the components received from the multiple paths. It is worth to remark that, although protocols such as WirelessHART and ISA-100 are oriented to single-path routing (i.e. sensing and actuation data are sent to the controller via a unique path of wireless nodes), it is possible to implement redundancy of sensing and actuation data by appropriately defining the scheduling in order to achieve multi-path routing. The Cons of redundancy by static multi-path routing are the following: first, it increases data traffic in the network, but this is a necessary investment to improve robustness with respect to link failures when we apply static routing: second, sending control data through multiple paths and then merging them the actuator node generates dynamics that might invalidate controllability conditions, as illustrated in the following example.

Example 2. Let define a MCN $N_p = (∏, G_R, η_R, G_C, η_C, Δ)$. As above, we do not consider the observability radio connectivity graph and scheduling. $∏ = (A, B, C)$ represents a continuous-time SISO LTI plant characterized by the transfer function $P(s)$ adopted in the previous example. We consider a multi-path scenario for the controllability radio connectivity graph $G_R$ as shown in Figure 5 where $v_c = v_1$ and $v_a = v_3$. Differently from the controllability graph of Example 1, in this case some nodes receive actuation data from multiple links. We define the weight function $W_R$ so that all nodes equally weight the contribution of each incoming link. Let us define three schedules on $G_R$, which convey actuation data from $v_c$ to $v_a$ using multiple paths:

$η_R^a = \{((v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_5), (v_2, v_7), (v_3, v_5), (v_3, v_6), (v_4, v_6), (v_4, v_7), (v_5, v_7), (v_6, v_7))\};$

$η_R^b = \{((v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_5), (v_2, v_7)), ((v_3, v_5), (v_3, v_6), (v_5, v_7)), ((v_4, v_6), (v_4, v_7)), ((v_5, v_7)), ((v_6, v_7))\};$

$η_R^c = \{((v_1, v_2), (v_1, v_3), (v_1, v_4), (v_5, v_7), (v_6, v_7)), ((v_2, v_5), (v_2, v_7), (v_3, v_5), (v_3, v_6), (v_5, v_7), (v_6, v_7))\}.

The scheduling have periods $Π^a = 1$, $Π^b = 6$, and $Π^c = 2$. Let $Δ = 10 ms$ as above: then the durations of the scheduling periods are given by $T^a = 10 ms$, $T^b = 60 ms$, and $T^c = 20 ms$. Scheduling $a$ consists of only one time slot, where all nodes transmit simultaneously. This is a corner case, that is realistic e.g. if the MAC layer of the communication protocol implements CDMA. The scheduling $a$ produces the following dynamics for $u(kT_a)$:

$u(kT_a) = \frac{3}{5} \tilde{u}((k-2)T^a) + 2 \frac{2}{5} \tilde{u}((k-3)T^a).

Note that a delay of 2 scheduling periods of $η^a_R$ corresponds to an actuation delay of 2 : $T^a = 20 ms$. Scheduling $b$ consists of 6 time slots: in each time slot only one node transmits and the other nodes receive. This is also a corner case, that is realistic when the communication protocol implements TDMA (i.e. only one node is allowed to transmit for each time slot). The scheduling $b$ produces the following dynamics for $u(kT^b)$:

$u(kT^b) = \frac{3}{5} \tilde{u}((k-1)T^b).

Note that a delay of 1 scheduling period of $η^b_R$ corresponds to an actuation delay of 1 : $T^b = 60 ms$. As a comparison to the single-path scenario of Example 1, we can conclude that adding redundancy generally increases the actuation delay of the control input, and thus worsen responsiveness of the control algorithm. The only case when the actuation delay does not increase is when we dispose of a multi-hop network that allows simultaneous transmission of all links (scheduling $a$, e.g. using CDMA, $T^a = 10 ms$). Unfortunately, this is not generally the case for current specifications for wireless networks, e.g. WirelessHART and ISA-100 do not admit CDMA. In the worst scenario, only one node can transmit data for each time slot (scheduling $b$, e.g. using TDMA, $T^b = 60 ms$). In this case, the actuation delay strongly increases, in contrast with the

\[
\eta_R^c = \{((v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_5), (v_2, v_7), (v_3, v_5), (v_3, v_6), (v_4, v_6), (v_4, v_7), (v_5, v_7), (v_6, v_7))\};
\]
requirement of designing responsive control algorithms. In typical industrial scenarios, as illustrated in D'Innocenzo et al. (2009), if we do not admit simultaneous transmission of two nodes then it is not always possible to design a scheduling that satisfies constraints on the actuation delay guaranteeing the achievement of control specifications on the closed loop system. For this reason, we choose a scheduling that allows multiple transmissions on a subset of links, which do not interfere each other (scheduling c, e.g. using TDMA and FDMA, $T^c = 20 ms$). The schedule c has the advantage of introducing redundancy and only moderately increasing the actuation delay. Moreover, it is reasonably implementable since it requires simultaneous use of mixed TDMA and FDMA, which is standardized in existing communication protocols for wireless sensor networks such as WirelessHART and ISA-100. Using $η_R$, the system can be seen as the cascade of blocks $G_R$ and $P_T$. The latter block is characterized by the transfer function $P_T(z)$ obtained by discretizing $P(s)$ with sampling time $T^c$ as follows:

$$P_T(z) = 4.2932 \times 10^{-9} \frac{z + 1.189}{(z + 1)(z + 2)}$$

where the poles of $P_T(z)$ are $p_1 = -1$ and $p_2 = -2$. The block $G_R$ models the dynamics introduced by the data flow through the network $G_N$, according to the applied scheduling $η_R$. The block $G_R$ is characterized by the transfer function:

$$G_R(z) = \frac{2^z + 2}{z^2} \Rightarrow z = 2^{-\frac{2}{3}}$$

Thus, when no failures occur, the zero $z$ of $G_R(z)$ does not coincide with any of the poles of $P_T(z)$. Assume that a failure occurs in the link $(v_3, v_7)$, denoted by the failures configuration $f_1$. Then the following holds:

$$f_1 = \{(v_3, v_7)\} \Rightarrow G^f_R(z) = \frac{2^z + 2}{z^2} \Rightarrow z_{f_1} = -1.$$ 

Thus, when the fault $f_1$ occurs the zero $z_{f_1}$ of $G^f_R(z)$ coincides with the pole $p_1$ of $P_T(z)$. Assume that a failure simultaneously occurs in the links $(v_3, v_7)$ and $(v_5, v_7)$, denoted by the failures configuration $f_2$. Then the following holds:

$$f_2 = \{(v_3, v_7), (v_5, v_7)\} \Rightarrow G^f_R(z) = \frac{2^z + 2}{z^2} \Rightarrow z_{f_2} = -1$$

Thus, when the fault $f_2$ occurs, the zero $z_{f_2}$ of $G^f_R(z)$ does not coincide with any of the poles of $P_T(z)$. Assume that a failure simultaneously occurs in the links $(v_3, v_7)$ and $(v_2, v_7)$, denoted by the failures configuration $f_3$. Then the following holds:

$$f_3 = \{(v_3, v_7), (v_2, v_7)\} \Rightarrow G^f_R(z) = \frac{2^z + 2}{z^2} \Rightarrow z_{f_3} = -2.$$ 

Thus, when the fault $f_3$ occurs the zero $z_{f_3}$ of $G^f_R(z)$ coincides with the pole $p_3$ of $P_T(z)$. Note that, according to a generic set of faulty edges f and to the weight function $W_R$, some failures introduce dynamics in the block $G^f_R(z)$ that invalidate controllability of $P_T(z)$.

Example 2 motivates characterizing MCNs controllability conditions over the plant dynamics, the scheduling and the routing. We will address this problem in the next Section.

4. STABILIZABILITY OF MCNS

As discussed in Section 3, MCNs $N$ can be modeled by the interconnection $N$ of blocks as in Figure 3.

**Definition 4.** We say that a MCN $N$ is controllable (resp. observable) if and only if $N$ is controllable (resp. detectable). Moreover, we say that $N$ is stabilizable (resp. detectable) if and only if $N$ is controllable (resp. detectable).

**Theorem 1.** A MCN $N$ is controllable if and only if the following hold:

1. $(A, B)$ is controllable;
2. $G_R$ is jointly connected by $η_R$;
3. for each pole $p$ of $P_T(z)$, $\sum_{i=1}^{\gamma_R(i)} p^D_{R,i} \neq 0$;
4. for each zero $z$ of $P_T(z)$, $z \neq 0$.

Note that controllability of $(A, B)$ and connectivity of the controller and actuator nodes are necessary conditions, as suggested by the intuition, but they are not sufficient. In fact, the controllability scheduling may introduce dynamics that invalidate controllability. This issue generates Conditions 3 and 4 of Theorem 1, that provide together with Conditions 1 and 2 necessary and sufficient controllability conditions. Another interesting remark is that, in order to guarantee controllability, we do not need to design an ordered schedule, i.e. we can schedule links with any order. This is an interesting result, since it allows much more freedom in designing the scheduling. The main problem, as illustrated in Example 2, is the design of a weight function $W_R$ such that Condition 3 of Theorem 1 is satisfied: we address and solve this issue in the following Section. Note that designing both a scheduling function $η_R$ and a weight function $W_R$ that satisfy the conditions of the Theorem 1, corresponds to designing a scheduling and a multi-path routing of the communication protocol.

Theorem 1 can be easily extended to address stabilizability, observability, and detectability.

5. FAULT TOLERANT STABILIZABILITY OF MCNS

Given a MCN and a set $f \subseteq E_R \cup E_O$ of communication links subject to a failure, we define a faulty MCN.

**Definition 5.** Given MCN $N = (P, G_R, η_R, G_O, η_O, Δ)$, let $f \subseteq E_R \cup E_O$ be a set of faulty links. We define the faulty MCN $N_f = (P, G_R, η_R, G_O, η_O, Δ_f)$, where $\forall k \in \{1, \ldots, II\}$, $η_R^f(k) = η_R(k) \setminus (η_R(k) \cap f)$ and $η_O^f(k) = η_O(k) \setminus (η_O(k) \cap f)$.

In other words, the faulty MCN $N_f$ is obtained by removing the faulty links from the schedules, while keeping the original radio connectivity graphs and the weight functions. Let $F \subseteq F_R \cup F_O$ be a set of failures configurations. The empty set $∅$ always belong to $F$, and $N_E$ represents the MCN in absence of failures. As clearly illustrated in Section 4, the main issue in designing a MCN such that it is controllable even with link failures, is the choice of the weight function $W_R$. Since we are exploiting redundancy by static multi-path routing, we need to design a unique static weight function $W_R$ (which implicitly defines the weight of each routing path) such that $N_f$ is controllable for each $f \in F$. This problem is not trivial: as an example, notice that it is not always possible to arbitrarily assign the value $W_R(\rho)$ for each path of an acrylic graph that consists of more than 5 vertices, since the number of paths, which corresponds to the number of constraints, is greater than the number of edges, which corresponds to the number of edges in the graph.
free variables. The following Theorem provides necessary and sufficient conditions for guaranteeing, given a MCN and a set of failures configurations $\mathcal{F}$, the existence of a weight function $W_R$ such that $\mathcal{N}_f$ is controllable for each $f \in \mathcal{F}$, if and only if the following hold:

1. $(A, B)$ is controllable;
2. for each $f \in \mathcal{F}$, $G_R$ is jointly connected by $\mathcal{N}_f$;
3. for each zero $z$ of $P_f(z)$, $z \neq 0$.

In the particular case $\mathcal{F} = \emptyset$, Theorem 2 provides necessary and sufficient conditions for guaranteeing, given a non-faulty MCN $\mathcal{N}_\emptyset$, the existence of a weight function $W_R$ such that $\mathcal{N}_\emptyset$ is controllable, thus solving the design problem defined in the previous Section.

Theorem 2 can be easily extended to address stabilizability, observability, and detectability.

6. CONCLUSIONS

This work provides a novel methodology to design scheduling and routing of a communication network in order to preserve controllability and observability, for any set of failures configurations that at least preserve connectivity within the scheduling period between the controller and the plant, and vice-versa. In future extensions of this paper, we aim to address the same problem for MIMO systems. Moreover, we will address the issue of introducing dynamical routing in our model, and performing an optimal choice of scheduling and weight functions. Another interesting problem to be addressed is guaranteeing the existence of a unique LTI controller of a MCN, that guarantees stability of the closed loop although the switching dynamics introduced by failures.

REFERENCES


