A Decentralized Control Strategy for Resilient Connectivity Maintenance in Multi-Robot Systems Subject to Failures

Cinara Ghedini and Carlos H. C. Ribeiro and Lorenzo Sabattini

Abstract This paper addresses the problem of topology control for dealing with node failures in networks of multiple robots. While connectivity maintenance has been widely addressed in the literature, issues related to failures are typically not considered in such networks. However, physical robots can fail (i.e. stop working) due to several reasons. It is then mandatory to consider this aspect, as connectivity maintenance is usually critical. In fact, failures of a small fraction of robots — in particular on those that play a crucial role in routing information through the network — can lead to connectivity loss. In this paper, we present a decentralized estimation procedure for letting each robot a) assess its degree of robustness w.r.t. to connectivity maintenance under the occurrence of failures in its neighborhood, and b) take actions to improve it when needed. This estimation is combined with a connectivity maintenance control law, thus providing a mechanism that ensures, in the absence of failures, both the network connectivity and an improvement in the overall robustness to failures. In addition, for failures scenarios, the mechanism is able to postpone, or even avoid network fragmentation, as verified through a set of validation experiments.

Cinara Ghedini
Computer Science Division, Aeronautics Institute of Technology, São José dos Campos, SP, Brazil
e-mail: cinara@ita.br

Carlos H. C. Ribeiro
Computer Science Division, Aeronautics Institute of Technology, São José dos Campos, SP, Brazil
e-mail: carlos@ita.br

Lorenzo Sabattini
Department of Sciences and Methods for Engineering (DISMI), University of Modena and Reggio Emilia, Italy e-mail: lorenzo.sabattini@unimore.it

1 Introduction

Applications based on groups of self-organized mobile robots are becoming pervasive in communication, monitoring, traffic and transportation systems. Groups of mobile robots, if equipped with appropriate communication devices, can be exploited to create an infrastructure network to provide communication services. For instance, interconnected mobile robots can provide rescuing, acting as devices in an exploration task, or serving clients (e.g., mobile phones, laptops, tablets, etc.) in a network, with the advantage of doing so without the existence of a previously defined infrastructure and with a high degree of autonomy (Figure 1). In fact, these features are the key requirements for extending a pressing issue nowadays: how to provide the communication infrastructure that makes it possible for generic clients to access the Internet, cloud technologies, and communication services in several unstructured environments and situations. Thus, the applicability of interconnected mobile robots is expanding from the classical monitoring and exploration tasks to an essential technology that supports several kinds of services to be available everywhere and at any time. In particular, the Internet, considered as an indispensable part of the critical information infrastructure for many personal and business applications, is now expected to be always available, offering uninterrupted service regardless of domain constraints [1–3].

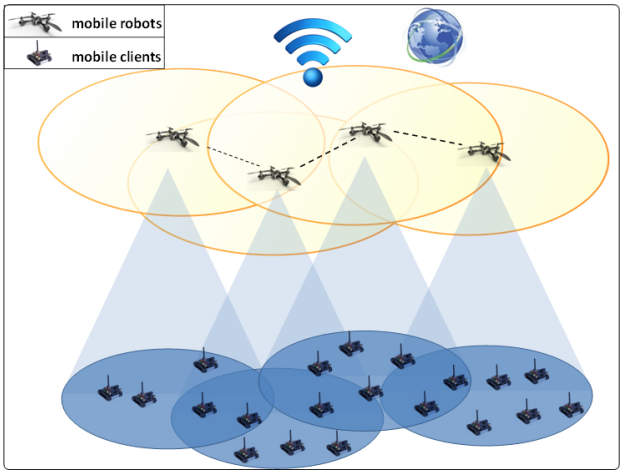
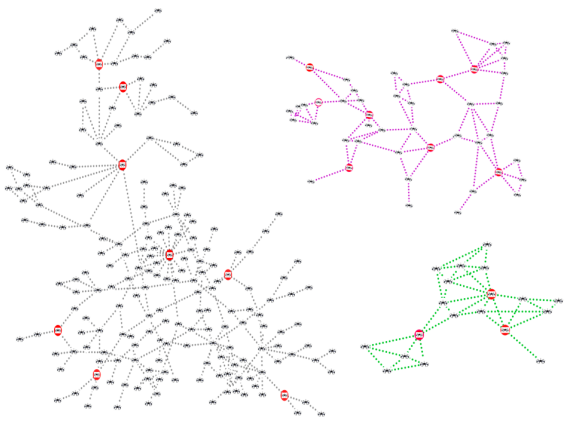
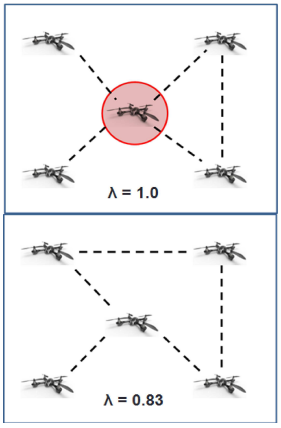


Fig. 1: Example of an application scenario.

In this sense, a critical aspect of providing network services for unstructured environments employing interconnected mobile robotic systems is that robots are prone to failures due to hardware or communication issues, and — as it is well known from the literature on Complex Networks — successive or cascading failures, particularly of agents playing a central role in the network topology, may easily result in inoperative or reduced services [4–8].



(a) Random network topologies. Failures in highlighted nodes can negatively affect the network connectivity, thus producing inoperative or reduced communication services.



(b) A network with larger algebraic connectivity (top) is more affected w.r.t. central node failure.

Fig. 2: Failures affect the connectivity of the network.

Figure 2(a) illustrates random network topologies highlighting some agents whose failures can strongly affect the network connectivity, characterizing vulnerable topological configurations. In the context of this work, a vulnerable topological configuration means that the network is potentially able to fragment if some nodes fail. Thus, we define the *resilience* of the multi-robot systems regarding its *robustness to failures*, that is the system's capacity to mitigate the effects of node failures through predictive actions that avoid topological configurations vulnerable to such effects.

Detecting such vulnerable configurations is not trivial because the topology emergent from these applications is dynamic; thus, its size and properties are most of the time unknown, costly to estimate and time varying. These features impose constraints on the design of solutions, such as a need for relying mostly on information that is locally available and straightforward to obtain, compute and update. Being a fundamental issue in multi-robot systems, the connectivity maintenance problem has been widely addressed in the literature. Therefore, several approaches can be found that ensure that, if the communication graph is initially connected, then it will remain connected as the system evolves [9–17]. In particular, the control strategy proposed in [16] ensures the network connectivity maintenance through a decentralized estimation of the algebraic connectivity, using the well-known property that the algebraic connectivity approaches 0 when the network is poorly connected. It is worth noting, however, that the algebraic connectivity *per se* is not effective as an indicator of the overall network fragility. A representative example of this fact is depicted in Figure 2(b): the network on the top has a larger algebraic connectivity (λ) than the network on the bottom, but it is more affected by a central node failure that might disconnect it into three subgraphs.

We, therefore, argue that, despite the algebraic connectivity being an estimator of how well a network is globally connected, it is not a suitable indicator to detect local vulnerable configurations and, thus, does not provide enough information to produce a more resilient network topology. On the other hand, connectivity is a crucial requirement in decentralized multi-robot systems: in order to achieve a common objective robots may need to exchange information. Thus, enhancing the robustness to failures is a fundamental requirement to be addressed in connectivity maintenance approaches. In this sense, a recent work proposes mechanisms, based on locally available information, for detecting and mitigating vulnerable topological configurations, consequently increasing the network resilience [18].

The contribution of this paper is the definition of a novel combined control law that, in the absence of failures, guarantees connectivity maintenance while improving the network robustness to failure and ensuring collision avoidance of robots with obstacles among them. It is important to emphasize that there is no way of guaranteeing that networks will remain connected in case of failures because the failure probability distribution is usually unknown and failures are not controllable. Hence, the central aspect of providing more resilient networks is to improve their capacity to tolerate disturbance without fragmenting. More generally, a resilient network is expected to exhibit the ability to react to undesirable states or unpredictable events through adaptive processes.

The proposed control law is validated comparing its performance regarding different parameterizations of gains in the presence of failures. The results demonstrate that the combined control law is able to increase the resilience of the system by adapting the network topology to accommodate failures, postponing or even avoiding network disconnection.

The rest of this paper is organized as follows. The necessary background on network properties is presented in Section 2. Section 3 discusses in details the problem of connectivity maintenance considering failures. Section 4 describes the proposed combined model, and Section 5 presents the simulation model and discusses the results. Concluding remarks are given in Section 6.

2 Background on network properties

We will hereafter define some quantities that can be useful for evaluating node and network connectivity, and robustness to failures.

Consider an undirected graph $\mathcal{G}$, where $\mathcal{V}(\mathcal{G})$ and $\mathcal{E}(\mathcal{G}) \subset \mathcal{V}(\mathcal{G}) \times \mathcal{V}(\mathcal{G})$ are the node set and the edge set, respectively. Moreover, let $W \in \mathbb{R}^{N \times N}$ be the weight matrix: each element w_{ij} is a positive number if an edge exists between nodes i and j, zero otherwise. Since $\mathcal{G}$ is undirected, then $w_{ij} = w_{ji}$.

Now, let $\mathcal{L} \in \mathbb{R}^{N \times N}$ be the Laplacian matrix of graph $\mathcal{G}$ and $D = \mathrm{diag}(\{k_i\})$ be the degree matrix of $\mathcal{G}$, where k_i is the degree of the i-th node of $\mathcal{G}$, i.e. $k_i = \sum_{j=1}^{N} w_{ij}$. The (weighted) Laplacian matrix of $\mathcal{G}$ is then defined as $\mathcal{L} = D - W$.

As is well known from algebraic graph theory, the Laplacian matrix of an undirected graph exhibits some remarkable properties regarding its connectivity [19]. Let λ_i, $i = 1,\dots,N$ be the eigenvalues of the Laplacian matrix, then:

- The eigenvalues are real, and can be ordered such that $0 = \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_N$.
- Define now $\lambda = \lambda_2$. Then, $\lambda > 0$ if and only if the graph is connected. Therefore, λ is defined as the **algebraic connectivity** of the graph.
- Considering a weighted graph, λ is a non-decreasing function of each edge weight.

In addition, we want to evaluate the number of node failures a network can stand before disconnecting. It is well-known that failures of nodes playing a central role in the network communication are likely to affect most its connectivity. In particular, referring to connectivity maintenance, we consider the concept of *Betweenness Centrality* (*BC*) for ranking the network nodes [20]. For a given node i and pair of nodes j,l, the importance of i as a mediator of the communication between j and l can be established as the ratio between the number of shortest paths linking nodes j and l that pass through node i ($g_{jl}(i)$), and the total number of shortest paths connecting nodes j and l (g_{jl}). Then, the *BC* of a node i is simply the sum of this value over all pairs of nodes, not including i:

$$BC(i) = \sum_{j<l} \frac{g_{jl}(i)}{g_{jl}}. \tag{1}$$

Once the *BC* has been computed for all the nodes, it is possible to order them from the *most central* (i.e. the node with highest value of *BC*) to the *less central* (i.e. the node with lowest value of *BC*). Hence, let $[v_1,\dots,v_N]$ be the list of nodes ordered by descending value of *BC*.

We therefore introduce the following definition of *Robustness level*.

Definition 1 (Robustness level [18]) *Consider a graph $\mathscr{G}$ with N nodes, and let $[v_1,\dots,v_N]$ be the list of nodes ordered by descending value of BC. Let $\varphi < N$ be the minimum index $i \in [1,\dots,N]$ such that, removing nodes $[v_1,\dots,v_i]$ leads to disconnecting the graph, that is, the graph including only nodes $\left[v_{\varphi+1},\dots,v_N\right]$ is disconnected. Then, the* robustness level *of $\mathscr{G}$ is defined as:*

$$\Theta(\mathscr{G}) = \frac{\varphi}{N}. \tag{2}$$

The robustness level defines the fraction of central nodes that need to be removed from the network to obtain a disconnected network. Small values of $\Theta(\mathscr{G})$ imply that a small fraction of node failures may fragment the network. Therefore, increasing this value means increasing the network robustness to failures. Notice that $\Theta(\mathscr{G})$ is only an estimate of how far the network is from getting disconnected w.r.t. the fraction of nodes removed. In fact, it might be the case that different orderings of nodes with the same *BC* produce different values of $\Theta(\mathscr{G})$.

From a local perspective, a heuristic for estimating the magnitude of the topological vulnerability of a node by means of information acquired from its 1-hop

and 2-hops neighbors is proposed in [18]. Let $d(v,u)$ be the shortest path between nodes v and u, i.e., the minimum number of edges that connect nodes v and u. Subsequently, define $\Pi(v)$ as the set of nodes from which v can acquire information:

$$\Pi(v) = \{u \in V(G) : d(v,u) \leq 2\}.$$

Moreover, let $|\Pi(v)|$ be the number of elements of $\Pi(v)$. In addition, define $\Pi_2(v) \subseteq \Pi(v)$ as the set of the 2-hop neighbors of v, that comprises only nodes whose shortest path from v is exactly equal to 2 hops, namely

$$\Pi_2(v) = \{u \in V(G) : d(v,u) = 2\}.$$

Now define $L(v,u)$ as the *number of paths* between nodes v and u, and let $Path_\beta(v) \subseteq \Pi_2(v)$ be the set of v's 2-hop neighbors that are reachable through at most β paths, namely

$$Path_\beta(v) = \{u \in \Pi_2(v) : L(v,u) \leq \beta\}.$$

Thus, β defines the threshold for the maximal number of paths between a node v and each of its u neighbors that are necessary to include u in $Path_\beta(v)$. Therefore, using a low value for β allows to identify the most weakly connected 2-hop neighbors. Hence, the value of $|Path_\beta(v)|$ is an indicator of the magnitude of node fragility w.r.t. connectivity, and **the vulnerability level of a node regarding failures** is given by $P_\theta(v) \in (0,1)$:

$$P_\theta(v) = \frac{|Path_\beta(v)|}{|\Pi(v)|}. \tag{3}$$

where $|\Pi(v)|$ is the number of v's 1-hop and 2-hops neighbors, and $|Path_\beta(v)|$ is the number of nodes that are exactly at 2-hops from node v and relying on at most β 2-hops paths to communicate with v.

3 Problem statement

Consider a multi-robot system composed of N robots that are able to communicate with other robots within the same communication radius R. The resulting communication topology can be represented by an undirected graph $\mathcal{G}$ where each robot is a node of the graph, and each communication link between two robots is an edge of the graph. Let each robot's state be its position $p_i \in \mathbb{R}^m$, and let $p = \left[p_1^T \dots p_N^T\right]^T \in \mathbb{R}^{N \times m}$ be the state vector of the multi-robot system. Let each robot be modeled as a single integrator system, whose velocity can be directly controlled, namely

$$\dot{p}_i = u_i, \tag{4}$$

where $u_i \in \mathbb{R}^m$ is a control input[1]. In order to guarantee the connectivity of $\mathscr{G}$, [16] proposes an approach to solve the connectivity maintenance problem in a decentralized manner, utilizing the algebraic connectivity property. For this purpose, consider a weighted graph, where the edge weights w_{ij} are defined as follows:

$$w_{ij} = \begin{cases} e^{-\left(\|p_i - p_j\|^2\right)/\left(2\sigma^2\right)} & \text{if } \|p_i - p_j\| \leq R \\ 0 & otherwise. \end{cases} \quad \text{with} \quad e^{-\left(R^2\right)/\left(2\sigma^2\right)} = \Delta \tag{5}$$

where Δ is a small predefined threshold[2].

Define now $\varepsilon > 0$ to be the desired lower-bound for the value of λ. The control strategy is then designed to ensure that the value λ never goes below ε. As in [16], the following *energy function* can then be utilized for generating the decentralized connectivity maintenance control strategy:

$$V(\lambda) = \begin{cases} \coth(\lambda - \varepsilon) & \text{if } \lambda > \varepsilon \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

The control design drives the robots to perform a gradient descent of $V(\cdot)$, in order to ensure connectivity maintenance. Namely, considering the dynamics of the system introduced in (4), the control law is defined as follows:

$$u_i = u_i^c = -\frac{\partial V(\lambda)}{\partial p_i} = -\frac{\partial V(\lambda)}{\partial \lambda}\frac{\partial \lambda}{\partial p_i}. \tag{7}$$

The connectivity maintenance framework can be enhanced to consider additional objectives. In particular, as shown in [15], the concept of *generalized connectivity* can be utilized for simultaneously guaranteeing **connectivity maintenance and collision avoidance** with environmental obstacles and among the robots. This is achieved considering the following *generalized edge weights*:

$$\omega_{ij} = w_{ij}\gamma_{ij}, \tag{8}$$

$\forall i, j = 1, \ldots, N$. In particular, the edge weights w_{ij} represent the standard connectivity property. The multiplicative coefficients γ_{ij} represent the *collision avoidance edge weights*:

Definition 2 *The collision avoidance edge weights γ_{ij} exhibits the following properties, $\forall i, j = 1, \ldots, N$:*

(P1) $\gamma_{ij} = \gamma_{ij}\left(\|p_i - p_j\|\right) \geq 0$.
(P2) $\gamma_{ij} = 0$ *if* $\|p_i - p_j\| = 0$, *and* $\gamma_{ij} = 1$ *if* $\|p_i - p_j\| \geq d_s$.

[1] It is worth remarking that, by endowing a robot with a sufficiently good cartesian trajectory tracking controller, it is possible to use this simple model to represent the kinematic behavior of several types of mobile robots, like wheeled mobile robots [21], and UAVs [22].

[2] This definition of the edge–weights introduces a discontinuity in the control action, that can be avoided introducing a smooth bump function, as in [23]. However, from an implementation viewpoint, the effect of the discontinuity can be made negligible by defining the threshold Δ sufficiently small.

(P3) $\gamma_{ij}(d)$ *is non-decreasing w.r.t. its argument* d.

The parameter $d_s > 0$ represents the *safety distance*: if the distance between two robots is larger than δ_s, then the collision avoidance action is not necessary. As shown in [15], the same formalism can be exploited for avoiding collisions with environmental obstacles as well.

Utilizing the generalized edge weights ω_{ij} defined in (8), we can compute the *generalized Laplacian matrix* $\mathscr{L}^G$, whose second smallest eigenvalue φ represents the *generalized connectivity* of the graph. As shown in [15], guaranteeing positiveness of the generalized connectivity φ simultaneously guarantees maintenance of the algebraic connectivity (i.e. it ensures that λ remains positive) and collision avoidance. This can then be achieved using the control law (7) replacing λ with φ, namely

$$u_i = u_i^c = -\frac{\partial V(\varphi)}{\partial p_i} = -\frac{\partial V(\varphi)}{\partial \varphi}\frac{\partial \varphi}{\partial p_i}. \tag{9}$$

Since φ and its gradient are global quantities, the proposed control law is centralized. Decentralized implementation can be achieved replacing φ and its gradient with their estimates, computed by each robot in a decentralized manner applying the procedure proposed in [16].

This methodology does not consider the fact that robots can unexpectedly fail, thus stopping their activity due to mechanical, electrical or software issues. As described in the introduction, it is necessary to reduce the effects of robot failures on the overall network connectivity, avoiding vulnerable topological configurations. In this paper we address the following problem:

Problem *Given a multi-robot system, design a local estimation procedure that allows each robot to assess its vulnerability level, based on locally available information, and subsequently exploit this estimate for controlling the motion.*

4 Combined control law

This section describes the unified model that aims at improving the robustness of networks to failures while, in the absence of failures, maintaining connectivity and avoiding collisions. In particular, considering the dynamics introduced in (4), we define the following control law:

$$u_i = \sigma u_i^c + \psi u_i^r, \tag{10}$$

where u_i^c is the generalized connectivity maintenance control law introduced in (9), and u_i^r is the additional control law that will be hereafter defined for improving robustness to failures. Moreover, $\sigma, \psi \geq 0$ are design parameters, that represent control gains. Setting either σ or ψ equal to zero leads to removing the effect of one of the control laws. Conversely, if both parameters are greater than zero, both control actions are simultaneously active.

Based on the vulnerability level definition, given in (3), the purpose of the control strategy is to increase the number of links of a potentially vulnerable node i towards its 2-hop neighbors that are in $Path_\beta(i)$, for a given value of β. Hence, define $x_\beta^i \in \mathbb{R}^m$ as the barycenter of the positions of the robots in $Path_\beta(i)$, namely

$$x_\beta^i = \frac{1}{|Path_\beta(i)|} \sum_{j \in Path_\beta(i)} p_j. \tag{11}$$

Considering the dynamics of the system introduced in (4), the control law is defined as follows:

$$u_i^r = \xi_i \frac{x_\beta^i - p_i}{\left\| x_\beta^i - p_i \right\|} \alpha(t), \tag{12}$$

where $\alpha(t) \in \mathbb{R}$ is the linear velocity of the robots[3]. The parameter ξ_i is introduced to take into account the vulnerability state of a node i, i.e. $\xi_i = 1$ if node i identify itself as vulnerable or $\xi_i = 0$ otherwise. As we aim at setting as vulnerable those robots i exhibiting high values for $P_\theta(i)$, ξ_i is defined as follows:

$$\xi_i = \begin{cases} 1 \text{ if } P_\theta(i) > r \\ 0 \text{ otherwise} \end{cases} \tag{13}$$

where $r \in (0,1)$ is a random number drawn from a uniform distribution. Namely, if $P_\theta(i) > r$, then the i-th robot considers itself as vulnerable. It is worth noting that (3) provides a decentralized methodology for each robot to evaluate its vulnerability level.

Summarizing, this control law drives vulnerable robots towards the barycenter of the positions of robots in their $Path_\beta$, thus decreasing their distance to those robots and eventually creating new edges in the communication graph. We will hereafter analyze the performance of the proposed combined control law introduced in (10). In particular, the control law u_i^c was proven in [15, 16] to guarantee positiveness of the generalized connectivity in a disturbance free environment. The following theorem extends these results considering the presence of the additional robustness improvement control law u_i^r.

Theorem 1 *Consider the dynamical system described by* (4)*, and the control laws described in* (9)*,* (10) *and* (12)*. Then, if the initial value of $\varphi(t)$, namely $\varphi(0)$, is greater than ε, then the value of $\varphi(t)$ will remain positive, as the system evolves, thus implying algebraic connectivity maintenance and collision avoidance.*

Proof. It is possible to show that, under the proposed control law, for constant values of P_θ, the energy function $V(\varphi(p))$ in (6) does not increase over time. As a consequence, it is possible to conclude that the generalized connectivity φ remains

[3] We would like to remark that pathological situations exist in which (12) is not well defined, namely when $p_i = x_\beta^i$. However, this corresponds to the case where the i-th robot is in the barycenter of its weakly connected 2-hop neighbors: hence, in practice, this never happens when a robot detects itself as vulnerable.

greater than zero, as the system evolves. Considering the definition of the generalized edge weights ω_{ij} in (8), this implies that the algebraic connectivity λ will remain positive, while avoiding collisions. This result can be extended to the case where P_θ is time-varying, assuming that variations are sufficiently slow. The proof is analogous to that of [16], and is then omitted due to space limitations. ■

5 Simulations

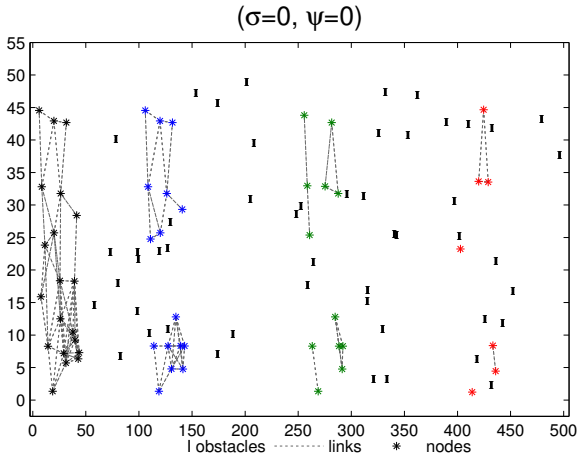
The proposed control strategy was validated using a simulation model, developed in MATLAB®. The initial network topologies were generated over a bounded area of size $\mathscr{A}$ in $\mathbb{R}^2$, through a random positioning of N robots, connected according to the communication radius R. For this simulation we consider $N = 20$, $\mathscr{A} = 50$ and $R = 16$. The experimental setup also considers a set of randomly generated failure times, distributed during the total simulation time of 80 seconds. At every 1 second, the vulnerability level estimation and the network properties were computed. We utilized the following model parametrization: $\varepsilon = 0.25$, $\beta = 1$, and $\sigma, \psi = \{0, 0.1, 0.5, 1\}$. Moreover, we considered a constant linear velocity $\alpha(t) = 0.25R/s$.

For evaluation purposes, at the specific times, a disturbance is introduced into the network by removing its most central node according to the updated *BC* ranking, as defined in (1). Given an initial network topology and the combined control law, it is expected that the proposed mechanism significantly reduces the impact of failures on the network connectivity, providing robots with means not only for accommodating but also for responding to failures, adapting the interconnection topology.

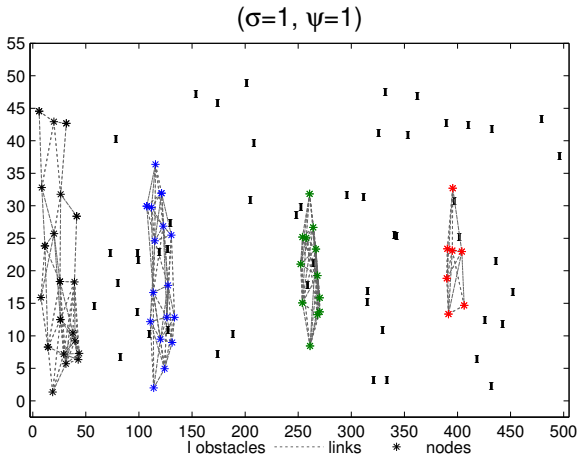
For demonstrating the fragility of random networks to failures of elements, Figure 3(a) exhibits snapshots of a network during the simulation process without the proposed control law (i.e. $\psi = 0$ and $\sigma = 0$). These snapshots correspond to simulation time $t = 0$, $t = 20$, $t = 50$ and $t = 80$, depicted by black, blue, green and red nodes, respectively. Notice that at $t = 20$ the network fragmented into two clusters, and as the simulation evolves the number of clusters increases. Of course, different failure distribution might accelerate or delay the network fragmentation. However, cascading failures or a high vulnerable topological configuration are surely harmful to the network connectivity and, as a consequence, to its operation.

Consider now the performance of the combined control law for the same scenario ($\psi = 1$ and $\sigma = 1$), illustrated in Figure 3(b). The resulting network topology is still connected at the end of the simulation despite failures of central elements, emphasizing the effectiveness of the combined control law to produce a more resilient network. As already mentioned, the connectivity can not always be guaranteed, but postponing the network fragmentation or increasing the number of elements in the largest connected component are significant achievements for those applications where connectivity is crucial.

As a proof of concept, the experiments were performed for 50 different network topologies. For each gain combination, the averaged results for the algebraic con-



(a) Performance **without** the control law.



(b) Performance **with** the control law.

Fig. 3: Snapshots of a network topology at $t = 0$ (black), $t = 20$ (blue) , $t = 50$ (green) and $t = 80$ (red) simulation times.

nectivity and the robustness level are illustrated in Figures 4 and 5, respectively. The vertical axis represents the initial scores for the respective property and its evolution when exposed to continuous failures through the fraction f of nodes removed from the network (horizontal axis).

As expected, networks were heavily affected by failures in scenarios where the robustness improvement mechanism was not significantly active ($\psi = 0$ and $\psi = 0.1$), as the algebraic connectivity approaches 0 with a few node failures. Notice that the robustness to failure level increases according to ψ gain setting. On the other hand, it is not significantly affected by the σ gain setting, i.e., improving the weight of the connectivity maintenance control through the algebraic connectivity estimation does not mean improving the robustness to failures. These findings sup-

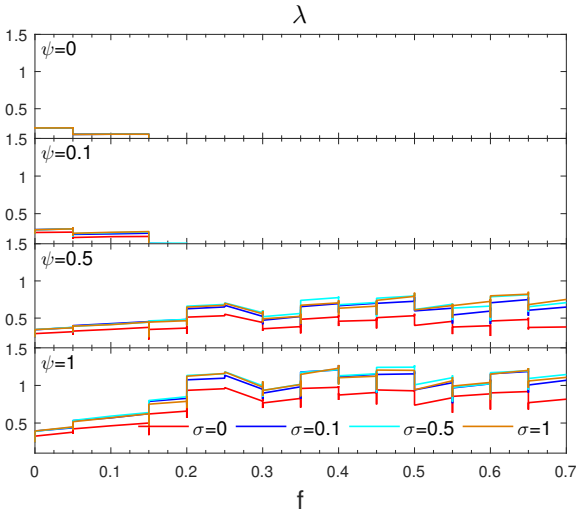


Fig. 4: Control law performance - The algebraic connectivity (λ).

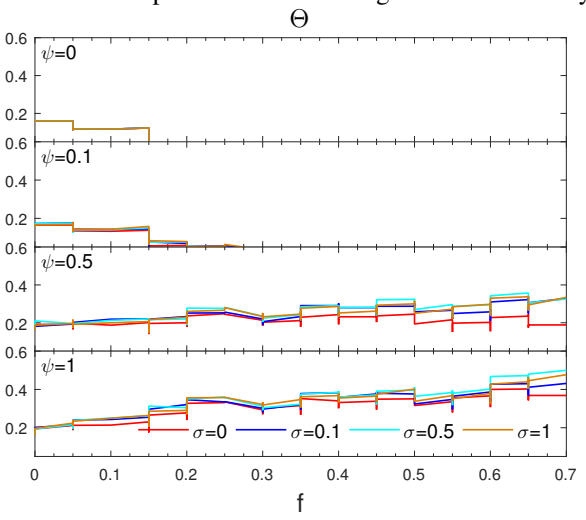


Fig. 5: Control law performance - The robustness level (Θ).

port the claim that the algebraic connectivity is not a suitable property for supporting mechanisms to produce more robust networks.

In contrast to the robustness level evolution, the algebraic connectivity exhibits a slight improvement as the ψ value increases, i.e., improving the robustness to failures implies increasing the overall network connectivity. It is important to highlight that the algebraic connectivity control law plays an important role: when there are no vulnerable nodes in the network the connectivity must be ensured.

In general, the experiments demonstrate the impact of failures on the network connectivity and, mainly, the feasibility of combining connectivity maintenance and

robustness to failures improvement mechanisms, even in the presence of obstacles. Besides, the gain modeling allows the design of tools for adaptively setting gains according to the application requirements and the devices/network states (e.g., battery level, sensor feedbacks, failure occurrences), which can result in a desirable control law behavior. Some additional examples can be freely viewed online on `https://youtu.be/ueo7nYEAm24`.

6 Conclusions

Multi-robot applications that require deploying services in unstructured domains should remain operative, regardless of the possibility of device failures, as service availability is a crucial requirement for most applications. In this paper, we present a model, based on local procedures, that combines control laws for both connectivity maintenance and failure effect mitigation in multi-robot networks, thus allowing a robust operation of the robotic network. The control laws are combined as a weighted sum, and failure mitigation is achieved by a vulnerability assessment that is also performed locally. The results demonstrate the feasibility of the model: the tested networks were able to postpone disconnection or to maintain the network connected even in scenarios of frequently occurring failures. Current work aims at implementing the proposed methodology on real robotic systems, to evaluate its performance in operational scenarios. Moreover, we are investigating the impact of different failure time distributions on the mechanism performance. For future work, we aim at developing methodologies for achieving online adaptation of the gains according to the network configuration and the application requirements, as a means of improving the overall performance. Finally, we aim at considering the presence of additional control objectives, such as formation control or environmental coverage.

References

1. P. K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "The resilience of wdm networks to probabilistic geographical failures," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 1521–1529.
2. S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah, "Fast local rerouting for handling transient link failures," *IEEE/ACM Trans. Netw.*, vol. 15, no. 2, pp. 359–372, Apr. 2007. [Online]. Available: http://dx.doi.org/10.1109/TNET.2007.892851
3. J. Rak, *Resilient Routing in Communication Networks*, 1st ed., ser. Computer Communications and Networks, S. I. P. Switzerland, Ed. Springer International Publishing, 2015.
4. R. Albert, H. Jeong, and A.-L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, July 2000.
5. L. Dall'Asta, A. Barrat, M. Barthelemy, and A. Vespignani, "Vulnerability of weighted networks," *Theory and Experiment*, vol. 2006, p. 04006, 2006.
6. C. Ghedini and C. H. C. Ribeiro, "Rethinking failure and attack tolerance assessment in complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 23–24, pp. 4684–4691, November 2011.

7. Z. He, S. Liu, and M. Zhan, "Dynamical robustness analysis of weighted complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 18, pp. 4181 – 4191, 2013.
8. M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle, "Endurance: A new robustness measure for complex networks under multiple failure scenarios," *Computer Networks*, vol. 57, no. 17, pp. 3641 – 3653, 2013.
9. M. Ji and M. Egerstedt, "Distributed coordination control of multiagent systems while preserving connectedness," *IEEE Transactions on Robotics*, 2007.
10. G. Notarstefano, K. Savla, F. Bullo, and A. Jadbabaie, "Maintaining limited–range connectivity among second–order agents," in *Proceedings of the American Control Conference*, 2006, pp. 2134–2129.
11. Y. Cao and W. Ren, "Distributed coordinated tracking via a variable structure approach – part I: consensus tracking. part II: swarm tracking," in *Proceedings of the American Control Conference*, 2010, pp. 4744–4755.
12. M. A. Hsieh, A. Cowley, V. Kumar, and C. J. Talyor, "Maintaining network connectivity and performance in robot teams," *Journal of Field Robotics*, vol. 25, no. 1, pp. 111–131, 2008.
13. A. Ajorlou, A. Momeni, and A. G. Aghdam, "A class of bounded distributed control strategies for connectivity preservation in multi–agent systems," *IEEE Transactions on Automatic Control*, vol. 55, pp. 2828–2833, 2010.
14. D. V. Dimarogonas and K. H. Johansson, "Bounded control of network connectivity in multi–agent systems," *IET Control Theory & Applications*, vol. 4, pp. 1751–8644, 2010.
15. P. Robuffo Giordano, A. Franchi, C. Secchi, and H. H. Bülthoff, "A passivity-based decentralized strategy for generalized connectivity maintenance," *The International Journal of Robotics Research*, vol. 32, no. 3, pp. 299–323, 2013.
16. L. Sabattini, N. Chopra, and C. Secchi, "Decentralized connectivity maintenance for cooperative control of mobile robotic systems," *The International Journal of Robotics Research (SAGE)*, vol. 32, no. 12, pp. 1411–1423, October 2013.
17. L. Sabattini, C. Secchi, and N. Chopra, "Decentralized estimation and control for preserving the strong connectivity of directed graphs," *IEEE Transactions on Cybernetics*, 2014.
18. C. Ghedini, C. Secchi, C. H. C. Ribeiro, and L. Sabattini, "Improving robustness in multi-robot networks," in *Proceedings of the IFAC Symposium on Robot Control (SYROCO)*, Salvador, Brazil, aug. 2015.
19. C. Godsil and G. Royle, *Algebraic Graph Theory*. Springer, 2001.
20. S. Wasserman, K. Faust, and D. Iacobucci, *Social Network Analysis : Methods and Applications (Structural Analysis in the Social Sciences)*. Cambridge University Press, November 1994.
21. R. Soukieh, I. Shames, and B. Fidan, "Obstacle avoidance of non-holonomic unicycle robots based on fluid mechanical modeling," in *Proceedings of the European Control Conference*, Budapest, hungary, 2009.
22. D. Lee, A. Franchi, H. Son, C. Ha, H. Bulthoff, and P. Robuffo Giordano, "Semiautonomous haptic teleoperation control architecture of multiple unmanned aerial vehicles," *IEEE/ASME Transactions on Mechatronics*, vol. 18, no. 4, pp. 1334–1345, Aug 2013.
23. K. D. Do, "Formation tracking control of unicycle–type mobile robots with limited sensing ranges," *IEEE Transactions on Control Systems Technology*, vol. 16, pp. 527–538, 2008.