This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

Robustness of synchronization to additive noise: how vulnerability depends on dynamics

Maurizio Porfiri, *Senior Member, IEEE,* Mattia Frasca, *Senior Member, IEEE*

***Abstract*—From biological to technological networks, scientists and engineers must face the question of vulnerability to understand evolutionary processes or design resilient systems. Here, we examine the vulnerability of a network of coupled dynamical units to failure or malfunction of one of its nodes. More specifically, we study the effect of additive noise that is injected at one of the network sites on the overall synchronization of the coupled dynamical systems. In the context of mean square stochastic stability, we present a mathematically-principled approach to illuminate the interplay between dynamics and topology on network robustness. Through the new theoretical construct of robust metric, we uncover a complex and often counterintuitive effect of dynamics. While networks are more robust to noise injected at their hubs for a classical consensus problem, these hubs could become the most vulnerable nodes for higher order dynamics, such as second-order consensus and Rössler chaos. From the exact treatment of star networks and the systematic application of perturbation techniques, we offer a mechanistic explanation of these surprising results and lay the foundation for a theory of dynamic robustness of networks.**

***Index Terms*—Consensus, information centrality, mean square, nonlinear, perturbation, stochastic stability.**

I. Introduction

From the brain to the Internet, the question of vulnerability is pervasive to biological and technological networks [1], [2], [3]. Just as the neuroscience community seeks to elucidate the relationship between clinical outcomes and focal brain lesions, so engineers attempt at predicting how the failure of one or multiple routers could challenge the functionality of the Internet. Across a wide range of applications, we have learnt that localized faults of a single or a few nodes might trigger a dramatic cascading process that could lead to the failure of a large portion of the network [4], [5], [6], [7]. When and how these avalanches occur have been investigated through a number of complementary methodologies, searching for answers in the topology of the network and the dynamics of its constituting units.

Topology is certainly the most common lens to investigate network vulnerability and, its counterpart, network robustness. In algebraic graph theory, structural measures of connectivity [8], [9], [10] and related topological concepts, such as fault diameter [11], expansion parameter [12], and isoperimetric number [13], have been systematically leveraged to characterize robustness, measured as the ability of the network to withstand accidental events. In statistical physics and complex networks, several efforts have been devoted to elucidate the effect of the removal of a fraction of nodes or links on salient properties of the network, such as its diameter, largest component, and efficiency [14], [15], [16], [17]. Another important direction in the study of network robustness entails the concepts of graph resistance and Kemeny constant [18], which are particular relevant in the context of networks distributing flows of critical resources, such as electricity, water, and gas networks [19]. These concepts have been also applied to network routing problems, prompting the definition of criteria for robust network design and optimization [20]. In sum, these studies have shed light on the role of topological heterogeneity on the robustness of the network to targeted or random attacks, suggesting that heterogeneous, scale-free, networks are robust against random attacks and fragile to the removal of their hubs, while homogenous networks are resilient to targeted attacks.

A less explored research avenue has examined the role of dynamics on network robustness. Contrary to topological approaches where attacks are typically modeled through the removal of nodes or links, studying the dynamics of the network allows for describing attacks in a more general context. For example, attacks at network nodes have been modeled through changes in their dynamics [21], partial malfunctioning [22], and additive noise [23]. Across these modeling choices, numerical simulations reveal a rich and complex interplay between dynamics and topology. Surprisingly, those low-degree nodes that would be dismissed in a targeted attack based on a topological lens could be the most critical sites to hamper or destroy the collective dynamics of the entire network.

Here, we seek to establish a mathematically-principled framework to explain the role of the node dynamics on the network robustness. We tackle the problem within the modeling framework that we have proposed in [23], in which the synchronization of a network of coupled dynamical systems is hindered by additive noise at one of the network sites. Through numerical simulations on random networks with different chaotic dynamics, in [23], we have found that hubs could perform better or worse than low-degree nodes and have proposed a semiempirical approach to apprehend the interplay between dynamics and topology. We have successfully demonstrated the approach on real data on power grids [24] and offered experimental evidence for its practicality on electrical circuits [25]. Yet, our previous work does not bring forward the mathematical foundations for a general understanding of network robustness.

Interestingly, the setup is similar to recent studies on the selection of leaders to maximize the performance of a network of integrators tasked with reaching consensus in the presence

M. Porfiri is with the Department of Mechanical and Aerospace Engineering, New York University Tandon School of Engineering, Brooklyn, New York 11201, USA e-mail: mporfiri@nyu.edu.
M. Frasca is with the Department of Electrical, Electronics and Computer Engineering, Università degli Studi di Catania, Catania, 95125, Italy
Manuscript received December 28, 2017

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

of stochastic disturbances [26], [27], [28], [29], [30]. It is this very similarity that prompted us to reexamine the problem and attempt at a focused mathematical treatment in the context of mean square stochastic stability, upon which these recent studies are framed. Different from these recent studies, where all but one of the nodes are noisy, in our setup only one node is subject to additive noise. Most importantly, our analysis applies to general time-varying dynamics, rather than to scalar integrators in a consensus protocol. We comment that a complementary line of approach to study the robustness of a networked system consists of examining the effect of system uncertainty rather than stochastic disturbance, as recently proposed in [31].

Toward a theory of network robustness, we formulate the problem in terms of the variational dynamics about the synchronous solution, such that we focus on the forced response of a linear time-varying system subject to a stochastic input. We study the evolution of the synchronization error in a mean square sense to establish a time-varying matrix Lyapunov equation for the correlation matrix associated with the variational dynamics. Through modal analysis, we reduce this high-dimensional Lyapunov equation into a low-dimensional master equation, from which we define a robust metric that encapsulates the role of dynamics on robustness. The robustness metric disentangles dynamics from topology: it can be computed once for all, irrespective of the network topology and the location of the node where noise is injected. Once the robustness metric is determined and a specific network is assigned, the overall synchronization error can be computed for any choice of the node where noise is injected.

For a star network, we evaluate in closed-form the synchronization error for the case noise is injected at the center or at a peripheral node to illustrate the process through which the robustness metric operates on the spectrum of the graph Laplacian and clarify the key role of the node degree. For a generic network, we tap into perturbation methods to gain a similar insight and shed light on the concurrent role of the node degree and robustness metric on vulnerability. Through the analysis of the classical consensus problem, second-order consensus algorithms, and Rössler chaos, we demonstrate a complex dependence of the robustness metric on the underlying dynamics. While a network may be more vulnerable to added noise at low-degree nodes for a given dynamics, the opposite may hold true for another dynamics, thereby offering compelling evidence for a key role of dynamics on robustness.

II. Problem statement

We build on the mathematical framework posited in [23], where the failure of a node in the network is modeled by injecting noise into the dynamics of that particular node. With slightly different notation from [23], we consider a network of N dynamical systems whose time evolution is given by the following set of coupled stochastic differential equations:

$$\dot{x}_i(t) = F(x_i(t)) - \kappa \sum_{j=1}^{N} L_{ij} H_x(x_j(t)) + \nu_i H_\eta \eta(t) \qquad (1)$$

for $i = 1, \ldots, N$ and $t \in \mathbb{R}^+$. Here, $x_i \in \mathbb{R}^n$ is the state of the ith node, F is a smooth function describing the individual dynamics of each node, $\kappa \in \mathbb{R}^+$ is the coupling constant, L_{ij}'s are the entries of the graph Laplacian $L \in \mathbb{R}^{N\times N}$ of the network, H_x is a smooth coupling function, ν_i is an indicator which is equal to one if the ith node is subject to additive noise and is zero otherwise, H_η is a constant vector specifying how noise enters the dynamics of a node, and η is a zero-mean Gaussian white noise of variance $\frac{\theta}{2}$. The solutions of the stochastic differential equations involved in our study should be interpreted in Stratonovich sense, such that the mathematical derivations are based on properties stemming from the Stratonovich integral definition [32], [33], [34].

The graph Laplacian is defined as $L = \mathcal{D} - \mathcal{A}$, where $\mathcal{D}$ is the degree matrix and $\mathcal{A}$ is the adjacency matrix. The degree matrix is a diagonal matrix, whose elements are the degree of the nodes, while the adjacency matrix encodes the links between the nodes such that its entries are equal to one in correspondence of connected nodes and are zero otherwise. By construction, L is a zero row-sum matrix [35].

We linearize the dynamics of each node about the synchronous solution $s(t)$ – common to all the network nodes – such that $\dot{s}(t) = F(s(t))$. By introducing the ith variation $\xi_i(t) = x_i(t) - s(t)$ and recalling that L is zero row-sum, we obtain the following set of variational equations:

$$\dot{\xi}_i(t) = A(t)\xi_i(t) - \kappa \sum_{j=1}^{N} L_{ij} B(t)\xi_j(t) + \nu_i H_\eta \eta(t) \qquad (2)$$

for $i = 1, \ldots, N$. Here, $A(t)$ and $B(t)$ are the Jacobians of F and H_x evaluated along the synchronous solution, such that $A(t) = \frac{\partial F(x)}{\partial x}|_{x=s(t)}$ and $B(t) = \frac{\partial H_x(x)}{\partial x}|_{x=s(t)}$. These matrices are generally assumed to be piecewise continuous, such that the elegant machinery of linear time-varying systems applies.

We write the linearized dynamics (2) using Kronecker algebra (see for, example, [36]) toward a more compact representation of the perturbed synchronization problem. We aggregate the variations of all the dynamical systems in a single error vector of length equal to Nn, such that, $\xi(t)^{\mathrm{T}} = \left[\xi_1(t)^{\mathrm{T}}, \ldots, \xi_N(t)^{\mathrm{T}}\right]$, where T indicates matrix transposition. Thus, (2) becomes

$$\dot{\xi}(t) = [I_N \otimes A(t) - \kappa L \otimes B(t)]\xi(t) + [\nu \otimes H_\eta]\eta(t) \qquad (3)$$

where $\otimes$ is the Kronecker product, I_N is the identity matrix in $\mathbb{R}^{N\times N}$, and $\nu \in \mathbb{R}^N$ has all zeros except of a one in correspondence of the node where noise in injected.

The chief objective of this work is to provide a thorough mathematical treatment of (3), toward an improved understanding of how topology and dynamics together determine the overall effect of noise on synchronization. Topological aspects pertain to both the structure of the network, encapsulated by the graph Laplacian L, and to the location of the node where noise is injected, encoded by the vector ν. Our approach applies to a wide class of coupled dynamical systems, including the classical consensus problem in which $n = 1$, $A(t) = 0$, and $B(t) = 1$; second-order consensus algorithms where $n = 2$ and $A(t)$ and $B(t)$ are constant

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

matrices; and chaotic oscillators in which $n \geq 3$ and $A(t)$ and $B(t)$ will vary in time as the synchronous solution covers the invariant manifold. We present our theory in a general setting and then specialize our claims to few relevant applications that help illustrate the complex interplay between topology and dynamics on robustness.

III. Analysis

We articulate the analysis of (3) as follows. First, we introduce the instantaneous synchronization error, which quantifies the overall discrepancy between the network nodes and the synchronous solution. Second, we specialize the results to the case of noiseless synchronization, recovering the classical master stability function by Pecora and Carroll [37]. Third, we study the error dynamics in a mean square sense and establish a deterministic governing equation for the error dynamics. Fourth, we diagonalize the deterministic dynamics to establish a robustness metric that can be used to shed light on the interplay between topology and dynamics on robustness. The formal derivation of such a metric is the objective of the final subsection, which summarizes our main results in a proposition.

A. Synchronization error

As a first step in the analysis, we introduce the metric by which we ascertain the robustness of the network to injected noise. Specifically, by writing the state variable of the generic ith node $x_i(t)$ as the sum of the variation $\xi_i(t)$ and the synchronous solution $s(t)$, the instantaneous synchronization error [23]

$$\mathcal{E}(t) = \frac{1}{N(N-1)} \sum_{i,j=1}^{N} \|x_i(t) - x_j(t)\|^2 \tag{4}$$

takes the following form:

$$\mathcal{E}(t) = \frac{1}{N(N-1)} \sum_{i,j=1}^{N} \|\xi_i(t) - \xi_j(t)\|^2 \tag{5}$$

where, without loss of generality, we have used the Euclidean norm. The dynamical systems are synchronized if their states are equal, such that the synchronization error vanishes. Note that, with respect to [23], we have dropped the square root in the definition of the synchronization error.

Through simple algebra, it is easy to verify that

$$\mathcal{E}(t) = \frac{2}{N-1} \sum_{i=1}^{N} \|\xi_i(t) - \overline{\xi}(t)\|^2 \tag{6}$$

which uses the average mismatch with respect to the synchronous solution, defined by

$$\overline{\xi}(t) = \frac{1}{N} \sum_{i=1}^{N} \xi_i(t) \tag{7}$$

Thus, the synchronization error can be expressed in terms of the difference between the variation at each node and the average mismatch in the network, without the need of incorporating the synchronous solution, which, however, enters the equations through $A(t)$ and $B(t)$. The latter two matrices vary in time with the evolution of the synchronous solution $s(t)$, about which we perform the linearization.

The synchronization error in (6) can be compactly written through the Kronecker representation in (3) by using the matrix $R \in \mathbb{R}^{N \times N}$, defined as

$$R = I_N - \frac{1}{N} 1_N 1_N^{\mathrm{T}} \tag{8}$$

where 1_N is the vector in $\mathbb{R}^N$ of all ones. As detailed in [38], the matrix R is an orthogonal projection onto $(\mathrm{Span}\{1_N\})^{\perp}$ as it is symmetric, idempotent, and $\mathrm{Ker}(R) = \mathrm{Span}\{1_N\}$. Specifically, using R, we may write the instantaneous synchronization error in terms of $\xi(t)$ as

$$\mathcal{E}(t) = \frac{2}{N-1} \parallel (R \otimes I_n)\xi(t) \parallel^2 \tag{9}$$

This expression for the instantaneous synchronization error hints at looking at the linearized dynamics in terms of the projected variable

$$z(t) = (R \otimes I_n)\xi(t) \tag{10}$$

which quantifies the variational dynamics in the transverse manifold, orthogonal to $\mathrm{Span}\{1_N\}$. Through the lens of z, a common mismatch of all the network nodes with respect to the synchronous solution will be automatically mapped into the zero vector.

At any time, the variation $\xi(t)$ can be obtained from $z(t)$ and $\overline{\xi}(t)$ through

$$\xi(t) = z(t) + 1_N \otimes \overline{\xi}(t) \tag{11}$$

and the variational dynamics can be written in terms of two decoupled equations for z and $\overline{\xi}$, by replacing (11) into (3). Specifically, we left multiply the equation by $R \otimes I_n$ to obtain the dynamics of z, namely,

$$\dot{z}(t) = [R \otimes A(t) - \kappa L \otimes B(t)]z(t) + (R\nu \otimes H_\eta)\eta(t) \tag{12}$$

where we have used (11) in the right-hand-side of the equation and we have accounted for the facts that $RL = L$ and $L1_N = 0$. Similarly, we left multiply (3) by $1_N \otimes I_n$ to derive the following equation for the average mismatch between the nodes:

$$\dot{\overline{\xi}}(t) = A(t)\overline{\xi}(t) + \frac{1}{N} H_\eta \eta(t) \tag{13}$$

where we have accounted for the fact that noise is injected at a single node in the network, such that, $\nu^{\mathrm{T}} 1_N = 1$.

Equation (12) completely determines the stochastic evolution of the synchronization error in (9), and its study in the mean square sense (see, for example, [39]) is the objective of the following analysis. On the other hand, (13) plays no role on the synchronization error, but it determines how the average mismatch in the network stochastically evolves in time along the synchronization manifold. The coupling does not enter the dynamics of the average mismatch, which is a function only of the overall intensity of the noise injected in the network and the individual dynamics of a node. From a control perspective, we have no ability to modulate this dynamics, which simply sets a common level of mismatch between the network nodes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

and the synchronous solution, without impacting the extent of synchrony of the nodes.

For example, for a classical consensus problem, we would find $\dot{\bar{\xi}}(t) = \frac{1}{N}\eta(t)$, which corresponds to a Langevin equation with null relaxation. In this case, the effect of the noise will build up in time, leading to large variations in the average mismatch, although one may tackle the design a coupling network such that the nodes are very close to each other at all times, as further discussed in what follows. More precisely, $\bar{\xi}(t) - \bar{\xi}(0)$ is a Gaussian random variable with zero mean and with variance proportional to the time variable t.

B. Deterministic dynamics in the absence of additive noise

In the absence of noise, that is, for $\theta = 0$, we obtain the classical synchronization problem for a network of coupled identical dynamical systems, which has been extensively studied in the technical literature, as exemplified by a large number of thorough technical reviews (see, for example, [40], [41]). In this case, the problem admits an elegant treatment by projecting the variational dynamics on the eigenvectors of the graph Laplacian. Here, we summarize this treatment to provide useful notation for our main claims on dynamic robustness and familiarize the reader with the notion of modal analysis.

Specifically, let V be the orthogonal matrix whose ith column is the eigenvector v_i of L with corresponding eigenvalue λ_i, where $\lambda_1 = 0$ and $v_1 = \frac{1}{\sqrt{N}}1_N$. Also, let Λ be the corresponding diagonal matrix of eigenvalues, such that $L = V\Lambda V^{\mathrm{T}}$. From V, we construct the $\mathbb{R}^{nN\times nN}$ orthogonal matrix $\tilde{V} = V \otimes I_n$, which we utilize to simplify the study of the variational dynamics.

Setting $\eta(t) = 0$ in (12), left multiplying by $\tilde{V}^{\mathrm{T}}$, and applying elementary properties of Kronecker algebra, we obtain the following chain of equalities:

$$\begin{aligned}\dot{\tilde{z}}(t) &= \left(V^{\mathrm{T}} \otimes I_n\right)\left[R \otimes A(t) - \kappa L \otimes B(t)\right] z(t)\\ &= \left[V^{\mathrm{T}}R \otimes A(t) - \kappa V^{\mathrm{T}}L \otimes B(t)\right] z(t)\\ &= \left[V^{\mathrm{T}}RVV^{\mathrm{T}} \otimes A(t) - \kappa V^{\mathrm{T}}LVV^{\mathrm{T}} \otimes B(t)\right] z(t)\\ &= \left[\tilde{R} \otimes A(t) - \kappa\Lambda \otimes B(t)\right](V^{\mathrm{T}} \otimes I_n)z(t)\\ &= \left[\tilde{R} \otimes A(t) - \kappa\Lambda \otimes B(t)\right]\tilde{z}(t)\end{aligned} \tag{14}$$

where we have introduced the modal coordinates $\tilde{z}(t) = \tilde{V}^{\mathrm{T}}z(t)$ and $\tilde{R} = V^{\mathrm{T}}RV$. The latter matrix is simply equal to $\tilde{R} = I_N - e_1e_1^{\mathrm{T}}$, where e_1 is the first vector of the natural basis $\{e_i\}_{i=1}^N$, since $Rv_1 = 0$ and $Rv_i = v_i$ for $i = 2, \ldots, N$. Equation (14) corresponds to a system of N decoupled differential equations in $\mathbb{R}^n$, such that,

$$\dot{\tilde{z}}_1(t) = 0 \tag{15a}$$

$$\dot{\tilde{z}}_i(t) = [A(t) - \kappa\lambda_i B(t)]\tilde{z}_i(t) \tag{15b}$$

for $i = 2, \ldots, N$.

Since $\tilde{z}_1(0) = 0$ by construction, see (10), the asymptotic synchronization of the network is equivalent to the asymptotic stability of the following master equation for $N-1$ values of the nonnegative parameter $\alpha \in \{\kappa\lambda_2, \ldots, \kappa\lambda_N\}$:

$$\dot{y}(t) = [A(t) - \alpha B(t)]y(t) \tag{16}$$

where $y(t) \in \mathbb{R}^n$ is the master state variable. Therefore, the synchronization of a network of N coupled systems reduces to the study of a single master stability equation in $\mathbb{R}^n$, as originally established in [37].

C. Mean square dynamics of the synchronization error

From (9), we write the expected synchronization error at time t as

$$\mathsf{E}[\mathcal{E}(t)] = \frac{2}{N-1}\mathsf{E}\left[z(t)^{\mathrm{T}}z(t)\right] = \frac{2}{N-1}\mathrm{Tr}\left(\mathsf{E}\left[z(t)z(t)^{\mathrm{T}}\right]\right) \tag{17}$$

where the expectation is computed with respect to the σ-algebra induced by the noise. Thus, the analysis of the effect of noise injected at one of the network nodes reduces to the study of the time of evolution of the trace of the correlation matrix $\Sigma(t) = \mathsf{E}[z(t)z(t)^{\mathrm{T}}]$ – a symmetric and positive semidefinite matrix.

By taking the time derivative of $\Sigma(t)$, applying the chain rule of differentiation, and using (12), we obtain

$$\begin{aligned}\dot{\Sigma}(t) &= [R \otimes A(t) - \kappa L \otimes B(t)]\Sigma(t)\\ &\quad + \Sigma(t)\left[R \otimes A(t)^{\mathrm{T}} - \kappa L \otimes B(t)^{\mathrm{T}}\right]\\ &\quad + (R\nu \otimes H_\eta)\mathsf{E}\left[\eta(t)z(t)^{\mathrm{T}}\right] + \mathsf{E}\left[\eta(t)z(t)\right]\left(\nu^{\mathrm{T}}R \otimes H_\eta^{\mathrm{T}}\right)\end{aligned} \tag{18}$$

To compute the latter two summands on the right hand side of the equation above, we replace $z(t)$ with the solution of (12), which reads

$$z(t) = \Phi_z(t,0)z(0) + \int_0^t \Phi_z(t,\tau)R\nu \otimes H_\eta\eta(\tau)\mathrm{d}\tau \tag{19}$$

where $z(0)$ is the initial condition and $\Phi_z(t,\tau)$ is the transition matrix associated with the state matrix $[R \otimes A(t) - \kappa L \otimes B(t)]$. By recalling that the noise is hypothesized to be white, such that $\mathsf{E}[\eta(t)\eta(\tau)] = \frac{\theta}{2}\delta(t-\tau)$ where $\delta(t)$ is the Dirac distribution, we obtain the following time-varying Lyapunov equation for the time evolution of the correlation matrix:

$$\begin{aligned}\dot{\Sigma}(t) &= [R \otimes A(t) - \kappa L \otimes B(t)]\Sigma(t)\\ &+ \Sigma(t)[R \otimes A(t)^{\mathrm{T}} - \kappa L \otimes B(t)^{\mathrm{T}}] + \theta[R\nu\nu^{\mathrm{T}}R \otimes H_\eta H_\eta^{\mathrm{T}}]\end{aligned} \tag{20}$$

whose initial condition is $\Sigma(0) = z(0)z(0)^{\mathrm{T}} = (R \otimes I_n)\xi(0)\xi(0)^{\mathrm{T}}(R \otimes I_n)$.

D. Modal analysis of the mean square dynamics

Toward the objective of crafting a master equation to examine dynamic robustness, we perform a modal analysis of the correlation dynamics on the eigenspaces of the Laplacian matrix, similar to the classical analysis for noiseless systems reviewed in Section III-B. By left multiplying the governing equation for the dynamics of the correlation matrix in (20) by $\tilde{V}^{\mathrm{T}}$ and right multiplying by $\tilde{V}$, we find

$$\begin{aligned}\dot{\tilde{\Sigma}}(t) &= [\tilde{R} \otimes A(t) - \kappa\Lambda \otimes B(t)]\tilde{\Sigma}(t)\\ &\quad + \tilde{\Sigma}(t)\left[\tilde{R} \otimes A(t)^{\mathrm{T}} - \kappa\Lambda \otimes B(t)^{\mathrm{T}}\right]\\ &\quad + \theta\left(V^{\mathrm{T}}R\nu\nu^{\mathrm{T}}RV \otimes H_\eta H_\eta^{\mathrm{T}}\right)\end{aligned} \tag{21}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

where we have introduced $\tilde{\Sigma}(t) = \tilde{V}^{\mathrm{T}}\Sigma(t)\tilde{V}$.

Our next step is to write $\tilde{\Sigma}$ as the summation of N^2 matrices in $\mathbb{R}^{n\times n}$, such that

$$\tilde{\Sigma}(t) = \sum_{i,j=1}^{N} e_i e_j^{\mathrm{T}} \otimes \tilde{\sigma}_{ij}(t) \tag{22}$$

where $\tilde{\sigma}_{ij}(t)$ corresponds to the ijth block of $\tilde{\Sigma}(t)$. By replacing (22) in (21), we obtain N^2 decoupled systems of matrix differential equations in $\mathbb{R}^{n\times n}$. Specifically, we determine the following set of modal equations:

$$\dot{\tilde{\sigma}}_{1j}(t) = -\kappa\lambda_j\tilde{\sigma}_{1j}(t)B(t)^{\mathrm{T}} \tag{23a}$$

$$\dot{\tilde{\sigma}}_{i1}(t) = -\kappa\lambda_i B(t)\tilde{\sigma}_{i1}(t) \tag{23b}$$

for $i, j = 1, \ldots, N$, together with

$$\begin{aligned}\dot{\tilde{\sigma}}_{ij}(t) &= [A(t) - \kappa\lambda_i B(t)]\tilde{\sigma}_{ij}(t) \\ &+ \tilde{\sigma}_{ij}(t)\left[A(t)^{\mathrm{T}} - \kappa\lambda_j B(t)^{\mathrm{T}}\right] + \theta\left(v_i^{\mathrm{T}}\nu\right)\left(v_j^{\mathrm{T}}\nu\right)H_\eta H_\eta^{\mathrm{T}}\end{aligned} \tag{24}$$

for $i, j = 2, \ldots, N$. Notably, the initial condition for (21) is $\tilde{\Sigma}(0) = (V^{\mathrm{T}}R \otimes I_n)\xi(0)\xi(0)^{\mathrm{T}}(RV \otimes I_n)$, such that $\tilde{\sigma}_{1j}(0) = \tilde{\sigma}_{i1}(0) = 0$ for $i, j = 1, \ldots, N$. As a result, (23) implies that $\tilde{\sigma}_{1j}(t)$ and $\tilde{\sigma}_{i1}(t)$ remain zero for all times. On the other hand, (24) will in general yield nontrivial dynamics, associated with the modes of the correlation matrix on the transverse manifold.

Since we are interested in the trace of $\Sigma(t)$ and the trace is invariant under a similarity transformation, like the one elicited by $\tilde{V}$ (see, for example, [42]), our entire problem reduces to the solution of $N-1$ independent systems of differential equations

$$\begin{aligned}\dot{\tilde{\sigma}}_{ii}(t) &= [A(t) - \kappa\lambda_i B(t)]\tilde{\sigma}_{ii}(t) + \tilde{\sigma}_{ii}(t)[A(t) - \kappa\lambda_i B(t)]^{\mathrm{T}} \\ &+ \theta\left(v_i^{\mathrm{T}}\nu\right)^2 H_\eta H_\eta^{\mathrm{T}}\end{aligned} \tag{25}$$

for $i = 2, \ldots, N$ with initial conditions given by

$$\tilde{\sigma}_{ii}(0) = (v_i^{\mathrm{T}} \otimes I_n)\xi(0)\xi(0)^{\mathrm{T}}(v_i \otimes I_n) \tag{26}$$

From the solution of these equations we ultimately evaluate the expectation of the synchronization error in (17) as

$$\mathsf{E}[\mathcal{E}(t)] = \frac{2}{N-1}\sum_{i=2}^{N}\mathrm{Tr}\tilde{\sigma}_{ii}(t) \tag{27}$$

E. Master equation and robustness metric

Given that the coupling enters (25) through the eigenvalue λ_i and the component of the eigenvector $v_i^{\mathrm{T}}\nu$ corresponding to the location of the node where noise is injected, we posit a master equation for the master correlation matrix $\zeta(t) \in \mathbb{R}^{n\times n}$ of the form

$$\dot{\zeta}(t) = [A(t) - \alpha B(t)]\zeta(t) + \zeta(t)[A(t) - \alpha B(t)]^{\mathrm{T}} + \theta u^2 H_\eta H_\eta^{\mathrm{T}} \tag{28}$$

where α and u should be treated as arbitrary nonnegative parameters. The study of this time-varying Lyapunov equation allows for an exhaustive analysis of the interplay between topology and dynamics on robustness.

It may be convenient to transform the Lyapunov equation into a linear system in terms of a vector assembled from the components of $\zeta(t)$ by utilizing Kronecker algebra. Thus, we may write (28) as

$$\begin{aligned}\mathrm{Vec}\dot{\zeta}(t) &= [A(t) - \alpha B(t)] \oplus [A(t) - \alpha B(t)]\mathrm{Vec}\zeta(t) \\ &+ \theta u^2 \mathrm{Vec}\left(H_\eta H_\eta^{\mathrm{T}}\right)\end{aligned} \tag{29}$$

where $\oplus$ is the Kronecker sum and Vec indicates matrix vectorization. The solution of (29) can be written using the transition matrix $\Phi_{\mathrm{Vec}\zeta}(t,\tau)$ associated with the state matrix $[A(t) - \alpha B(t)] \oplus [A(t) - \alpha B(t)]$ as follows:

$$\begin{aligned}\mathrm{Vec}\zeta(t) &= \Phi_{\mathrm{Vec}\zeta}(t,\tau)\mathrm{Vec}\zeta(0) \\ &+ \theta u^2 \int_0^t \Phi_{\mathrm{Vec}\zeta}(t,\tau)\mathrm{d}\tau \mathrm{Vec}\left(H_\eta H_\eta^{\mathrm{T}}\right)\end{aligned} \tag{30}$$

Therefore, the contribution to (27) from the mode with Laplacian eigenvalue equal to $\frac{\alpha}{\kappa}$ and eigenvector component at the node where noise is injected equal to u is

$$\mathcal{E}_{\alpha,u}(t) = \mathrm{Vec}\left(I_n\right)^{\mathrm{T}}\mathrm{Vec}\zeta(t) \tag{31}$$

such that

$$\mathsf{E}[\mathcal{E}(t)] = \frac{2}{N-1}\sum_{i=2}^{N}\mathcal{E}_{\kappa\lambda_i,|v_i^{\mathrm{T}}\nu|}(t) \tag{32}$$

By construction, the transition matrix $\Phi_{\mathrm{Vec}\zeta}(t,\tau)$ can be expressed as the Kronecker product of two identical matrices

$$\Phi_{\mathrm{Vec}\zeta}(t,\tau) = \Phi_y(t,\tau) \otimes \Phi_y(t,\tau) \tag{33}$$

Here, $\Phi_y(t,\tau)$ is the transition matrix of the master equation for noiseless synchronization in (16). Therefore, the contribution to the expectation of the synchronization error in (31) becomes

$$\begin{aligned}\mathcal{E}_{\alpha,u}(t) &= \mathrm{Vec}\left(I_n^{\mathrm{T}}\right)\Phi(t,0) \otimes \Phi(t,0)\mathrm{Vec}\zeta(0) \\ &+ \theta u^2 \mathrm{Tr}\int_0^t \Phi_y(t,\tau)H_\eta H_\eta^T \Phi_y(t,\tau)^{\mathrm{T}}\mathrm{d}\tau\end{aligned} \tag{34}$$

We assume that the network synchronizes in the absence of noise, such that the transition matrix vanishes in the limit of $t \to \infty$ for $\lambda \in \{\lambda_2, \ldots, \lambda_N\}$ – the asymptotic stability of the noiseless variational dynamics can be inferred from a master stability function constructed upon (16). Under the premise of asymptotic stability of (16), for sufficiently large times the free evolution in the right hand side of (34) vanishes and the contribution to the synchronization error approaches the steady-state solution

$$\mathcal{E}_{\alpha,u}^{\mathrm{ss}}(t) = \theta u^2 \rho(\alpha, t) \tag{35}$$

where the so-called robustness metric ρ is given by

$$\rho(\alpha, t) = \mathrm{Tr}\int_0^t \Phi_y(t,\tau)H_\eta H_\eta^T \Phi_y(t,\tau)^{\mathrm{T}}\mathrm{d}\tau \tag{36}$$

This function is independent of u and can be computed parametrically for any choice of α as a function of time.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

Through such a parametric analysis, we may ultimately write the expected synchronization error at the steady-state as

$$\mathsf{E}[\mathcal{E}^{\rm ss}(t)] = \frac{2\theta}{N-1}\nu^{\rm T}\left[\sum_{i=2}^{N}\rho(\kappa\lambda_i,t)v_i v_i^{\rm T}\right]\nu \qquad (37)$$

We formulate this result in the form of the following proposition for the linearized dynamics in (3):

Proposition 1: Consider the network of coupled linear systems (3), where L is the graph Laplacian of the network, $A(t)$ and $B(t)$ are piecewise continuous matrix functions in $\mathbb{R}^{n\times n}$, $\nu\in\mathbb{R}^N$ has all zeros except of the entry corresponding to the node where noise is injected, $H_\eta\in\mathbb{R}^N$ is a constant vector specifying how noise enters the dynamics of a node, and η is a zero-mean Gaussian white noise of variance 2θ. If the linear system asymptotically synchronizes in the absence of additive noise ($\lim_{t\to\infty}\|\xi_i(t)-\xi_j(t)\|=0$ for $i,j=1,\dots,N$ and any initial condition), then at steady-state the expected synchronization error $\frac{1}{N(N-1)}\sum_{i,j=1}^{N}\mathsf{E}\left[\|\xi_i(t)-\xi_j(t)\|^2\right]$ approaches (37), where v_i is the ith eigenvector of L whose corresponding eigenvalue is λ_i and the robustness metric $\rho(\kappa\lambda,t)$ is computed through (36), from the transition matrix of the master equation for noiseless synchronization in (16).

Through Proposition 1, we can systematically examine the interplay between topology and dynamics on robustness. All the information related to the network dynamics are encoded in the robustness metric $\rho(\alpha,t)$, which is independent of the topology of the network and the location of the node where noise is injected. Computation of the robustness metric requires only knowledge of the noiseless deterministic dynamics and the way noise enters the state of the network nodes via H_η. The network topology determines the numerical values of the eigenvalues and eigenvectors of the graph Laplacian, which, together with the robustness metric, shape the response of the network to additive noise. More specifically, from the topology and the robustness metric, we can evaluate the matrix $\sum_{i=2}^{N}\rho(\kappa\lambda_i,t)v_i v_i^{\rm T}$, which might be assimilated to a generalized function of the graph Laplacian. The diagonal entries of this generalized matrix function will ultimately reveal the vulnerability of the network to injected noise at specific nodes.

Proposition 1 offers some directions on how to expand the approach to network control. Toward minimizing the effect of noise on the networked dynamics, this proposition might inform the selection of nodes where localized interventions should be applied. For instance, knowledge about the nodes where noise injection yields the larger synchronization error may suggest where filters should be introduced to hamper noise, thereby reducing its impact on the overall networked system.

IV. Computation of the robustness metric

From a practical point of view, it may be difficult to compute the integral in (36) and one may opt for directly solving the time-varying Lyapunov equation in (28) or the associated linear system in (29) in the steady-state. Specifically, $\rho(\alpha,t)$ corresponds to the trace of the solution of (28) with zero initial conditions and $\theta=u=1$.

While for a general time-varying system the dependence of the robustness metric on time might not be discarded, in our treatment of time-invariant and chaotic systems we can focus on a robustness metric that depends only on α. In these cases, the steady-state solution should be independent of time.

Specifically, for linear time-invariant systems, we could directly set the left hand side of the equation to zero and solve the resulting algebraic Lyapunov equation to determine $\rho(\alpha)$. More specifically, for time-invariant systems, we solve the following equation for ζ:

$$(A-\alpha B)\zeta+\zeta(A-\alpha B)^{\rm T}+H_\eta H_\eta^{\rm T}=0 \qquad (38)$$

and set $\rho(\alpha)=\mathrm{Tr}\zeta$.

For chaotic systems, we exploit the ergodicity of the synchronous solution to tailor the definition of the robustness metric. Toward this aim, we solve (28), or (29), for a large time interval with $\theta=u=1$. Then, we compute the trace of the solution and average over an integration window to define a robustness metric that is only a function of α. A similar line of approach could be proposed for periodic systems, in which we would design the integration window on the basis of the period of the variational dynamics.

In what follows, we briefly examine three representative dynamics: classical consensus, second-order consensus, and Rössler chaos. These three exemplary cases help illustrate the complexity of the interplay of dynamics and topology on robustness.

A. Classical consensus

For the case of a classical consensus, $n=1$, $A(t)=0$, and $B(t)=1$ and (38) yields the simple expression

$$-2\alpha\zeta+1=0 \qquad (39)$$

Thus, the robustness metric is

$$\rho(\alpha)=\frac{1}{2\alpha} \qquad (40)$$

which is, obviously, a monotonically decreasing function of α.

B. Second-order consensus

As an example of second-order consensus, we consider

$$A=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\quad B=\begin{bmatrix}0 & 0\\ \beta & 1\end{bmatrix},\quad H_\eta=\begin{bmatrix}0\\ 1\end{bmatrix} \qquad (41)$$

where $\beta\in\mathbb{R}$. If we were to draw an analogy with mechanical systems, then the problem would correspond to an array of mass-spring systems of unit mass and unit stiffness, which are interconnected by springs of stiffness β and dampers of unit damping constant. If β is positive, (16) will be asymptotically stable for any positive α, but if α is negative then asymptotic stability will be lost for $\alpha>-\frac{1}{\beta}$. Through the lens of the mechanical analogy, a negative spring constant will cause the masses to be pushed away from their equilibrium, which can be contrasted by the restoring damping only up to a certain extent.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

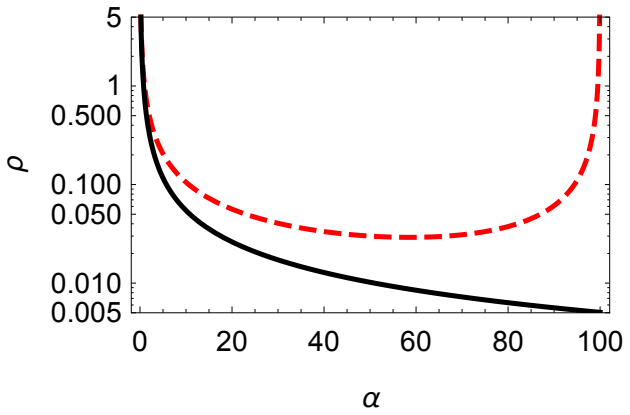

Fig. 1: Robustness metric for second-order consensus. Black solid curve identifies the case in which $\beta = 1$ and the system is asymptotically stable for any positive value of α. Red dashed curve refer to the case in which $\beta = -\frac{1}{100}$ and the system is asymptotically stable for $0 < \alpha < 100$.

Solving (38) for ζ, we find

$$\zeta = \begin{bmatrix} \frac{1}{2\alpha(1+\alpha\beta)} & 0 \\ 0 & \frac{1}{2\alpha} \end{bmatrix} \tag{42}$$

from which we define the robustness metric

$$\rho(\alpha) = \frac{2+\alpha\beta}{2\alpha(1+\alpha\beta)} \tag{43}$$

Fig. 1 illustrates the robustness metric for two exemplary instances of second-order consensus. For the case of $\beta > 0$, the metric is monotonically decreasing, thereby we expect an equivalent behavior to the classical consensus problem. On the other hand, for $\beta < 0$, a much more complex scenario emerges.

The robustness metric depends nonmonotonically on α and features two vertical asymptotes at 0 and $-\frac{1}{\beta}$. For an arbitrary linear system, it is tenable to anticipate a similar response, where the dependence of the robustness metric on α may be in general nonmonotonic and may feature multiple asymptotes that separate islands of synchronization in the absence of additive noise. As evidenced from (43), we expect the function $\rho(\alpha)$ to grow to infinity as α approaches the critical values at which the master stability equation loses stability. Interestingly, even the classical first-order consensus problem will display an equivalent behavior if formulated in a discrete-time setting, where stability of the noiseless protocol is only possible for a finite range of the coupling gains between the nodes [43].

C. Rössler chaotic oscillators

Next, we examine Rössler chaotic dynamics, whose nonlinear behavior is encoded in the three-dimensional nonlinear function $F(x) = \left[-x_2 - x_3, x_1 + \frac{1}{5}x_2, \frac{1}{5} + x_1 x_3 - 9x_3\right]^{\mathrm{T}}$, where x_1, x_2, x_3 are the three components of the state vector. As discussed in [44], the Lyapunov exponents for this oscillator are approximately -8.716, 0, and 0.080. We assume that the oscillators are coupled on the second variable, such that

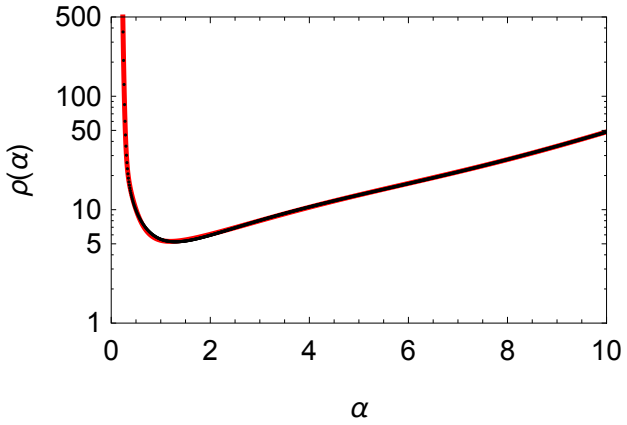

Fig. 2: Robustness metric for Rössler chaotic oscillators. Black markers are results from computer simulations and red solid curve is the empirical fit in (45).

$H_x(x) = x_2$. Thus, the time-varying matrices describing the system dynamics are

$$A = \begin{bmatrix} 0 & -1 & -1 \\ 1 & \frac{1}{5} & 0 \\ s_3(t) & 0 & s_1(t) - 9 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{44}$$

where $s(t) \in \mathbb{R}^3$ is the chaotic solution of an oscillator. As shown by [44], for this configuration, the master equation (16) is asymptotically stable for $\alpha > 0.157$.

Following our previous work [23], we consider noise injected on the first variable so that $H_\eta = [1, 0, 0]^{\mathrm{T}}$. To compute the robustness metric, we adopt the following approach. First, we integrate the original nonlinear dynamics of a single oscillator from $t = 0$ to $t = 1000$ from an initial condition with all the state variables at 1 to compute $s(t)$. Then, for any value of α, we integrate (29) in the same time window using homogenous initial conditions and $\theta = u = 1$. Then, we left multiply by $(\mathrm{Vec}I_3)^{\mathrm{T}}$, integrate in $[750, 1000]$, and scale the result by the length of the interval, 250. We repeat this process by varying α from 0.160 to 10.000 with a step of 0.010 for 1000 times. We perform the numerical integration using the MATHEMATICA® built-in function NDSOLVE.

Results of the computation are shown in Fig. 2 where we report the robustness metric as a function of α. As expected, the robustness metric has a vertical asymptote approximately in correspondence to the smallest value of α for which the master equation is asymptotically stable, that is, $\alpha = 0.157$. Interestingly, the order of the singularity identified from numerical fitting of the data seems larger than one, different from the linear time-invariant problems described above. As α increases, we see a minimum at approximately 1.293 and finally a polynomial growth in α, identified from the numerical data. As shown in Fig. 2, the robustness metric is accurately fitted by the following function:

$$\rho(\alpha) = \frac{0.0543}{(\alpha - 0.157)^4} - \frac{0.754}{(\alpha - 0.157)^3} + \frac{4.02}{(\alpha - 0.157)^2} - \frac{6.29}{(\alpha - 0.157)} + 10.3 - 3.27\alpha + 1.51\alpha^2 - 0.193\alpha^3 + 0.0114\alpha^4 \tag{45}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

V. Understanding the interplay between topology and dynamics

Here, we systematically apply Proposition 1 to clarify the relationship between robustness and both the network topology and dynamics. We start with the analysis of the classical consensus problem, for which we can compute in closed-form the synchronization error as a function of salient topological properties of the node where noise is inserted.

Closed-form computation of both the robustness metric and the resulting generalized matrix function of the Laplacian are unfortunately not feasible as we consider more general dynamics, like the second-order consensus protocol or Rössler chaotic oscillators. As a result, one may need to compromise on the class of networks to be examined to establish exact results for dynamic robustness or devise approximation methods that could help illuminate the relationship between dynamic robustness and the topological properties of the nodes under attack for general networks. Here, we explore both of these lines of approach. First, we examine a star graph and then we turn to general networks, for which we first present some useful analysis tools based on perturbation theory and then demonstrate the approach on an exemplary complex network.

A. Classical consensus

By assuming that the graph is connected, such that $\lambda_2 > 0$ (see, for example [35]), the integrators asymptotically reach consensus in the absence of noise. Thus, the error at steady-state in (37) takes the following form:

$$\mathsf{E}[\mathcal{E}^{\mathrm{ss}}] = \frac{\theta}{\kappa(N-1)} \nu^{\mathrm{T}} \left[\sum_{i=2}^{N} \frac{1}{\lambda_i} v_i v_i^{\mathrm{T}} \right] \nu \tag{46}$$

where we have used (40). Recalling the definition of the Moore-Penrose inverse of a matrix (see, for example, [45]), we can compactly write

$$\mathsf{E}[\mathcal{E}^{\mathrm{ss}}] = \frac{\theta}{\kappa(N-1)} \nu^{\mathrm{T}} L^{+} \nu \tag{47}$$

where L^{+} is the Moore-Penrose inverse of the graph Laplacian. Therefore, the error at steady-state is proportional to the diagonal entry of L^{+}, corresponding to the node where noise is injected.

From a topological point of view, the ith diagonal entry of the Moore-Penrose inverse of the graph Laplacian L_{ii}^{+} for $i = 1, \ldots, N$ can be related to the information centrality of the ith node, as demonstrated in [30] and concisely summarized in [29]. In the context of networks, the information encoded in a path between two nodes is defined as the inverse of the path length, such that information-rich paths would pertain to adjacent nodes and information would decay as the nodes become further and further away [46].

Specifically, from Eq. (8) in [29], we may write

$$L_{ii}^{+} = \frac{1}{c_i} - \frac{K_{\mathrm{f}}}{N^2} \tag{48}$$

where c_i is the information centrality of the ith node and K_{f} is the Kirchhoff index or total effective resistance of the network (see, for example, [47]). Information centrality is defined as the harmonic average of the total information between the ith node and any other network nodes, that is,

$$c_i = \left(\frac{1}{N} \sum_{j=1}^{N} \frac{1}{I_{i,j}^{\mathrm{tot}}} \right)^{-1} \tag{49}$$

where $I_{i,j}^{\mathrm{tot}}$ is the total information between nodes i and j, computed as the sum of the information in all paths connecting these two nodes. Thus, for the classical consensus problem, robustness is proportional to information centrality: the higher information centrality is, the lower will be the effect of the injected noise on the disagreement among the nodes. In other words, for a classical consensus problem, the network is most vulnerable to additive noise when injected from a node with low information centrality.

Information centrality is not entirely controlled by the degree, which only accounts for connections with nearest neighbors rather than nonlocal interactions that are built-in the definition of information centrality (see, for example, [48]). However, for several networks, large values of information centrality will typically map into large values of the degree, and, vice versa, nodes with low information centrality will correspond to nodes with low degree [49], [50].

Through numerical simulations, in [23], we in fact have found that dynamic robustness correlates with the node degree for scale-free and Erdős-Rényi networks. This is in sharp contrast with a purely topological view of network robustness which would suggest that the network is most vulnerable to attacks on the high-degree nodes.

B. Dynamic robustness beyond classical consensus: star networks

For a generic linear-time invariant or chaotic dynamics, it may be difficult or impossible to establish a precise connection between the network vulnerability and its topology, as we have done for the classical consensus problem. To illustrate the complexity of the problem, we examine a star network, in which node 1 corresponds to the center of degree $N-1$. The graph Laplacian has two nonzero eigenvalues 1 and $N-1$, with multiplicity equal to $N-2$ and 1, respectively. The eigenvector corresponding to the largest eigenvalue is $\frac{1}{\sqrt{N(N-1)}}(Ne_1 - 1_N)$ and the eigenspace of dimension $N-2$ associated with the unitary eigenvalue is simply $(\mathrm{Span}\{1_N, e_1\})^{\perp}$.

The steady-state synchronization error (37) becomes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2018.2825024, IEEE Transactions on Control of Network Systems

$$\mathsf{E}[\mathcal{E}^{\mathrm{ss-star}}] = \frac{2\theta}{N-1}\nu^{\mathrm{T}}\Bigg[\rho(\kappa)\left(I_N - \frac{1}{N-1}1_N 1_N^{\mathrm{T}} - \frac{N}{N-1}e_1 e_1^{\mathrm{T}} + \frac{1}{N-1}(e_1 1_N^{\mathrm{T}} + 1_N e_1^{\mathrm{T}})\right) + \rho(\kappa(N-1))\left(\frac{1}{N(N-1)}1_N 1_N^{\mathrm{T}} + \frac{N}{N-1}e_1 e_1^{\mathrm{T}} - \frac{1}{N-1}(e_1 1_N^{\mathrm{T}} + 1_N e_1^{\mathrm{T}})\right)\Bigg]\nu \quad (50)$$

where we have dropped the dependence on time given our focus on time-invariant and chaotic systems. We can specialize the synchronization error to the case in which we inject noise to the central node, $\nu = e_1$, or to any other node in the star, say $\nu = e_2$. In the former case, (50) yields

$$\mathsf{E}[\mathcal{E}^{\mathrm{ss-star}}] = \frac{2\theta}{N}\rho(\kappa(N-1)) \quad (51)$$

and in the latter, we find

$$\mathsf{E}[\mathcal{E}^{\mathrm{ss-star}}] = \frac{2\theta}{N-1}\left[\frac{N-2}{N-1}\rho(\kappa) + \frac{1}{N(N-1)}\rho(\kappa(N-1))\right] \quad (52)$$

Taking the ratio between (51) and (52), we define the following vulnerability ratio:

$$\mathrm{Vul}\left(\frac{\rho(\kappa)}{\rho(\kappa(N-1))}\right) = \frac{\frac{N-1}{N}}{\frac{N-2}{N-1}\frac{\rho(\kappa)}{\rho(\kappa(N-1))} + \frac{1}{N(N-1)}} \quad (53)$$

When the vulnerability ratio is less than one, then the star network is more robust at its center, and, vice versa, when the vulnerability ratio is more than one, then the center is the least robust node.

From a simple analysis of the function (53), we discover that the vulnerability ratio is equal to 1 when $\frac{\rho(\kappa)}{\rho(\kappa(N-1))} = 1$. Any value of $\frac{\rho(\kappa)}{\rho(\kappa(N-1))}$ less than 1 value will yield $\mathrm{Vul}\left(\frac{\rho(\kappa)}{\rho(\kappa(N-1))}\right) > 1$, and vice versa if the ratio is above 1, we will find $\mathrm{Vul}\left(\frac{\rho(\kappa)}{\rho(\kappa(N-1))}\right) < 1$.

For the classical consensus problem, $\rho(\alpha) = \frac{1}{2\alpha}$, such that $\frac{\rho(\kappa)}{\rho(\kappa(N-1))} = N-1$. Provided that $N > 2$, the vulnerability ratio will be less than 1 and the network will be more robust at its center, in agreement with the previous general results.

With respect to the second-order consensus problem with $\beta > 0$, a star network will be more vulnerable to attacks at the peripheral nodes. But for $\beta < 0$, the value of the coupling gain κ will shape the response of the networks to attacks at the center or peripheral nodes. As shown in Fig. 3 for three exemplary network sizes, for small values of κ, the ratio $\frac{\rho(\kappa)}{\rho(\kappa(N-1))}$ is larger than one, such that the network is more robust to attacks at its center. As κ increases, we have the opposite behavior and the network becomes more robust to attacks at its peripheral nodes. The qualitative dependence does not change with the size of the star network, which only reduces the range of admissible coupling gains given by $\kappa < -\frac{1}{(\beta(N-1))}$.

Rössler chaotic oscillators will show a similar behavior to second-order consensus with $\beta < 0$, such that we can switch

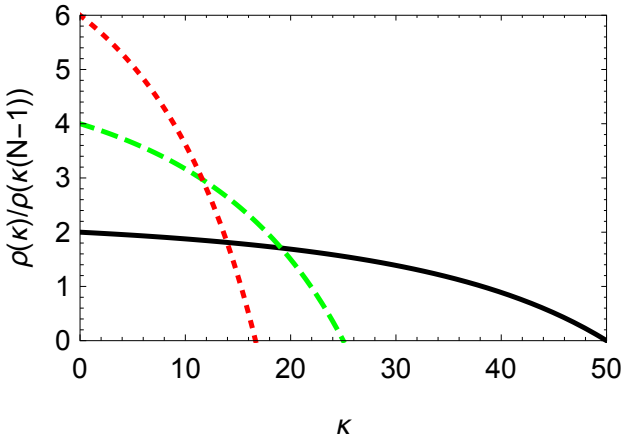

Fig. 3: Dependence of $\frac{\rho(\kappa)}{\rho(\kappa(N-1))}$ on the coupling gain and network size for second-order consensus over a star network with $\beta = -\frac{1}{100}$. Solid black curve refers to $N = 3$, green dashed curve to $N = 5$, and dotted red curve to $N = 7$.

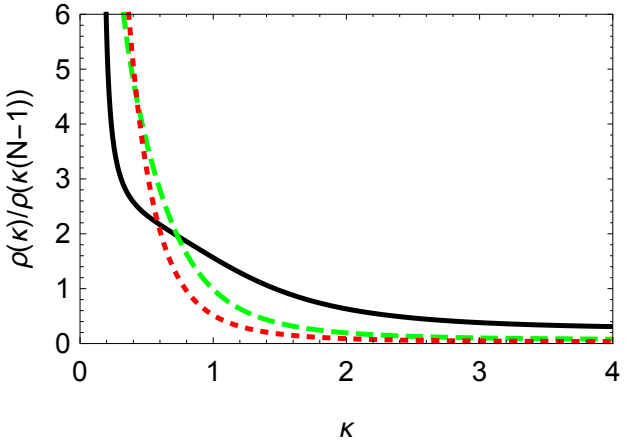

Fig. 4: Dependence of $\frac{\rho(\kappa)}{\rho(\kappa(N-1))}$ on the coupling gain and network size for Rössler chaotic oscillators interconnected by a star network. Solid black curve refers to $N = 3$, green dashed curve to $N = 5$, and dotted red curve to $N = 7$. Plots are generated using the empirical fit for the robustness metric in (45).

the relative vulnerability of the center and peripheral nodes by changing κ. More specifically, for small values of κ, the center is more robust to injected noise, and increasing the value of κ will lead to the peripheral nodes being more robust, as shown in Fig. 4.

C. Dynamic robustness beyond classical consensus: perturbation analysis on arbitrary networks

To enable the study of general networks, we posit an alternative approach based on perturbation theory. Specifically, by focusing on a compact interval of the stability region where the robustness metric is a smooth function we expand the function in a Taylor series and use the resulting polynomial approximation to write (37) in terms of a polynomial expansion of the Laplacian matrix.

For example, if the spectrum of the network is localized in an interval $[\lambda_2, \lambda_N]$ for which the function $\rho(\alpha)$ is monotonically increasing or decreasing, as a first approximation, we may propose $\rho(\alpha) \approx a_0 + a_1\alpha$. As a result, we may approximate the expected synchronization error in (37) as

$$\mathsf{E}[\mathcal{E}^{\rm ss}] \approx \frac{2\theta}{N-1}\nu^{\rm T}\left[\sum_{i=2}^{N}(a_0 + a_1\kappa\lambda_i)v_i v_i^{\rm T}\right]\nu \qquad (54)$$

which yields the following compact expression in terms of the graph Laplacian

$$\mathsf{E}[\mathcal{E}^{\rm ss}] \approx \frac{2\theta}{N-1}\left[a_0\left(1-\frac{1}{N}\right) + a_1\kappa\nu^{\rm T}L\nu\right] \qquad (55)$$

where we have used $\sum_{i=1}^{N} v_i v_i^{\rm T} = I_N$ and $\sum_{i=1}^{N}\lambda_i v_i v_i^{\rm T} = L$. This equation offers an important insight into the interplay between dynamics and topology on robustness. If $a_1 < 0$, then the synchronization error decreases with increasing values of $\nu^{\rm T}L\nu$, while the opposite holds for $a_1 > 0$. Since $\nu^{\rm T}L\nu$ is equal to the degree of the node where noise is being injected, then the sign of a_1 will determine whether the network is more vulnerable to additive noise injected at nodes with high or low degree.

In the context of the classical consensus problem, the robustness metric is a monotonically decreasing function, such that $a_1 < 0$. Thus, the affine approximation (55) predicts that dynamic robustness increases with node degree, in agreement with numerical predictions in [23]. The same behavior is expected for the second-order consensus algorithm with $\beta > 0$, while a richer landscape of robustness will characterize second-order consensus with $\beta < 0$ and Rössler chaotic oscillators.

Specifically, if $\{\kappa\lambda_i\}_{i=2}^{N}$ is concentrated around the origin for second-order consensus or around 0.157 for chaotic dynamics, then, the network will be more vulnerable to attacks at its low degree nodes. On the contrary, if $\{\kappa\lambda_i\}_{i=2}^{N}$ concentrates around the asymptote at $-\frac{1}{\beta}$ for second-order consensus or are larger than 1.293 for chaotic oscillators, the network will be more vulnerable when attacked at its high degree nodes. If $\{\kappa\lambda_i\}_{i=2}^{N}$ is somewhere in the central region where the robustness metric is nearly flat, then vulnerability will be largely independent of the degree of the nodes.

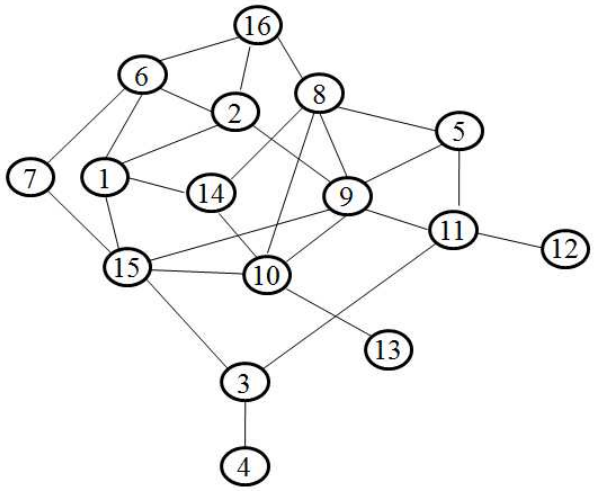

Fig. 5: Exemplary network of $N = 16$ nodes borrowed from [29] to illustrate the interplay of dynamics and topology. For this network, $\lambda_2 = 0.605$ and $\lambda_{16} = 8.030$.

We illustrate these claims on the network depicted in Fig. 5 for the cases of classical consensus, second-order consensus with $\beta = -\frac{1}{100}$, and Rössler chaos. The same network has been used to exemplify leader selection in consensus problems in [29]. For each type of dynamics, we fix $\theta = 1$ and evaluate the steady-state error $\mathsf{E}[\mathcal{E}^{ss}]$ in (37) generated by noise injected at one of the network nodes. In (37), the robustness metric is given by (40), (43), and (45) for classical consensus, second-order consensus, and Rössler chaotic dynamics, respectively. The node where noise is injected is systematically varied to cover the entire vertex set, thereby identifying the most vulnerable nodes in the network for each type of dynamics. Table I synoptically presents the results of the analysis, including side-by-side topological properties of the node where noise is injected and the corresponding steady-state error in the entire network.

For the classical consensus problem, our results indicate that the network is most vulnerable to attacks from node 12, which has, in fact, the lowest information centrality in the network. Very close values of $\mathsf{E}[\mathcal{E}^{ss}]$ are associated with two other nodes, that is, nodes 4 and 13. These are the other two nodes in the network that have the smallest degree of one.

For the second-order consensus algorithm, we consider two values of κ. The first one ($\kappa = 0.20$) corresponds to a scenario where $\{\kappa\lambda_i\}_{i=2}^{N}$ is close to the origin, such that the robustness metric will monotonically decrease and the problem be equivalent to the classical consensus. In agreement with our perturbation analysis, we find that the nodes which produce the larger error are those with the lowest degree. The second value of κ ($\kappa = 12.30$) portrays a different scenario, in which $\{\kappa\lambda_i\}_{i=2}^{N}$ concentrates around the asymptote at $-\frac{1}{\beta}$. In this case, the robustness metric monotonically increases and we confirm that the network is most vulnerable to attacks at the node with the highest degree, that is, node 9 with degree equal to six.

For Rössler chaotic oscillators, we consider three values

TABLE I: Topological properties of the network in Fig. 5, along with numerical values of the steady-state error induced by noise injected at one of the nodes for different dynamics. Each row lists the location of the injected noise (column 1), its degree (column 2), information centrality (column 3), and number of triangles (column 4), together with the steady-state errors in the entire network for different dynamics (column 5–10). For all the considered dynamics except of Rössler chaos with $\kappa = 0.65$, knowledge of the degree is sufficient to predict the most vulnerable network nodes. For Rössler chaos with $\kappa = 0.65$, knowledge of number of triangles is also required as shown in the very last column (column 11), where we present the theoretical prediction from the perturbation analysis based on both the degree and number of triangles in (59).

Node	d_i	c_i	t_i	Classical consensus	Second-order consensus, $\beta = -\frac{1}{100}$ and $\kappa = 0.20$	Second-order consensus, $\beta = -\frac{1}{100}$ and $\kappa = 12.30$	Rössler chaos, $\kappa = 0.32$	Rössler chaos, $\kappa = 1.00$	Rössler chaos, $\kappa = 0.65$	Rössler chaos, $\kappa = 0.65$ - prediction
1	4	1.227	2	0.021	0.210	0.006	109.759	1.546	1.066	1.234
2	5	1.311	3	0.017	0.175	0.012	103.189	2.021	1.267	1.443
3	4	1.209	0	0.022	0.218	0.007	85.833	1.556	1.080	1.004
4	1	0.587	0	0.080	0.802	0.014	569.280	0.886	1.395	1.445
5	3	1.118	2	0.026	0.263	0.006	10.849	1.162	0.871	1.184
6	4	1.163	2	0.024	0.240	0.006	181.081	1.561	1.122	1.234
7	2	0.903	0	0.040	0.405	0.008	167.336	0.905	0.861	1.063
8	4	1.250	1	0.020	0.200	0.008	31.926	1.546	1.033	1.119
9	6	1.465	2	0.012	0.122	0.029	2.604	2.609	1.438	1.351
10	4	1.224	0	0.021	0.211	0.009	17.725	1.564	1.067	1.004
11	4	1.176	1	0.023	0.233	0.008	145.030	1.569	1.112	1.119
12	1	0.580	0	0.082	0.817	0.014	948.156	0.914	1.462	1.445
13	1	0.591	0	0.079	0.795	0.014	160.080	0.875	1.365	1.445
14	4	1.266	1	0.019	0.193	0.007	56.030	1.542	1.030	1.119
15	4	1.274	0	0.019	0.190	0.008	21.567	1.547	1.020	1.004
16	3	1.086	1	0.028	0.280	0.006	148.299	1.187	0.931	1.069

of κ: 0.32, 1.00, and 0.65. The first one ($\kappa = 0.32$) locates $\{\kappa\lambda_i\}_{i=2}^N$ close to the asymptote at 0.157 and produces a scenario similar to that of classical consensus, with higher vulnerability for nodes with low degree. The second one ($\kappa = 1.00$) places $\{\kappa\lambda_i\}_{i=2}^N$ in the region where $\rho(\alpha)$ monotonically increases with α. In this case, the correlation between vulnerability and degree is reversed: the network is more vulnerable to attacks at its high-degree nodes. Node 9 is where the network is most vulnerable, similar to the second-order consensus with $\kappa = 12.3$. For the third value of κ ($\kappa = 0.65$), the set $\{\kappa\lambda_i\}_{i=2}^N$ is between 0.193 and 2.570, which is around the minimum of the robustness metric at 1.293. In this case, vulnerability is not correlated with the degree, whereby injecting noise at nodes 4, 9, 12 and 13 yields equivalent errors in network synchronization, despite the large mismatch in the degree of these nodes ($d_4 = d_{12} = d_{13} = 1$ and $d_9 = 6$).

A potential line of approach to examine the last case in which the degree is not a predictor of vulnerability entails the use of higher order approximation for the robustness metric. Specifically, when the robustness metric is not changing monotonically, an affine approximation of the robustness metric is not suitable and one may contemplate retaining more terms in the expansion such that $\rho(\alpha) \approx \sum_{i=0}^m a_i \alpha^i$, where m is the order of the expansion. In this more general setting, the synchronization error in (37) will be approximated as

$$\mathsf{E}[\mathcal{E}^{\rm ss}] \approx \frac{2\theta}{N-1}\left[a_0\left(1-\frac{1}{N}\right) + \sum_{i=1}^m a_i \kappa^i \nu^{\rm T} L^i \nu\right] \tag{56}$$

The geometric interpretation of the powers of the graph Laplacian is not trivial since the degree matrix $\mathcal{D}$ and the adjacency matrix $\mathcal{A}$ do not generally commute. However, some meaningful insight can be garnered by considering the identities presented in [51] for low order powers of L, based on classical identities on the diagonal elements of the first three powers of the adjacency matrix, namely,

$$\mathcal{A}_{ii} = 0, \quad \left(\mathcal{A}^2\right)_{ii} = d_i, \quad \left(\mathcal{A}^3\right)_{ii} = 2t_i \tag{57}$$

where $i = 1, \dots, N$, $d_i = \mathcal{D}_{ii}$ is the degree of node i, and t_i is the number of triangles that touch node i. Based on these identities, we can compute

$$\left(L^2\right)_{ii} = d_i^2 + d_i \tag{58a}$$

$$\left(L^3\right)_{ii} = d_i^3 + 3d_i^2 - 6t_i \tag{58b}$$

Therefore, up to a third order approximation in the robustness metric, we propose the following expansion for the synchronization error in (37):

$$\mathsf{E}[\mathcal{E}^{\rm ss}] \approx \frac{2\theta}{N-1}\Bigg[a_0\left(1-\frac{1}{N}\right) + a_1\kappa d_{\hat{i}} + a_2\kappa^2\left(d_{\hat{i}}^2 + d_{\hat{i}}\right) + a_3\kappa^3\left(d_{\hat{i}}^3 + 3d_{\hat{i}}^2 - 6t_{\hat{i}}\right)\Bigg] \tag{59}$$

where we have identified the node where noise is injected as $\hat{i}$. Equation (59) indicates that as the order of the expansion of the robustness metric increases, the degree of a node is not sufficient to predict the degree of vulnerability of the network as a function of the dynamics and nonlocal measures of centrality, such as the number of triangles, become important.

Going back to our example of Rössler chaotic oscillators with $\kappa = 0.65$, by least-square fitting the robustness metric at

$\{\kappa\lambda_i\}_{i=2}^{N}$, we find $a_0 = 17.7$, $a_1 = -15.2$, $a_2 = 5.49$, and $a_3 = -0.523$. By applying (59), we successfully anticipate that the network is equivalently vulnerable to noise injected at nodes 4, 9, 12, and 13, as shown in the very last column of Table I .

VI. Conclusions

From biological to technological networks, the question of robustness to local attacks is pervasive to science and engineering. In this paper, we have examined how networks of coupled dynamical systems respond to additive noise injected at one of the network nodes. We have established a mathematical framework to quantify the effect of noise injected at one of the network nodes on the overall synchronization among the coupled dynamical systems. By studying the time evolution of the synchronization error in a mean square sense, we have formulated a robustness metric that disentangles the roles of dynamics and topology on the robustness of the network. The robustness metric can be computed once for all, for any network and any choice of the node where noise is injected. Through the analysis of representative linear and nonlinear dynamics, we have demonstrated a wide range of feasible behaviors for the robustness metric, which ultimately shape how networks respond to additive noise.

Once a specific network topology is assigned, the synchronization error is simply evaluated in terms of the spectral properties of the graph Laplacian, the robustness metric, and a vector encoding the node where noise is injected. For the classical consensus problem, we have established an elegant relationship between network robustness and information centrality, which echoes recent studies on the effect of leadership in noisy consensus protocols [29], [30]. The higher is the information centrality of a node, the more the network will be robust to noise injected at that node. In contrast with a topological view of robustness that would suggest to protect hubs from attacks to preserve connectivity, we have found that for the classical consensus problem an attack in the form of additive noise is more detrimental when implemented on the peripheral nodes of the network.

For second-order consensus algorithms and Rössler chaotic dynamics, it is difficult to establish a universal relationship between the topological properties of the nodes where noise is injected and the vulnerability of the network. To gain mathematical insight, we have put forward two complementary approaches. First, we have proposed an exact solution for a star network that clarifies how the selection of the dynamics determines whether the network is more vulnerable at its center or at its peripheral nodes. For second-order consensus and Rössler chaos, we have identified selections of model parameters and coupling strengths that lead the center to be the most vulnerable node, in contrast with the classical consensus problem. For arbitrary networks, we have proposed an approach based on perturbation theory to unravel the dependence of network robustness on node degree and higher order measures of centrality.

While the proposed mathematical framework builds on the growing body of literature on leadership in noisy consensus protocols [26], [27], [28], [29], [30], it offers several technical improvements that are needed for the study of network robustness. Specifically, our approach is not limited to the classical consensus problem of coupled scalar integrators, but it is formulated in a general setting to study higher order linear and nonlinear dynamics. Embracing nonlinear, higher order dynamics significantly complicates the mathematical treatment, leading to: i) the general study of a time-varying Lyapunov equation to examine the new construct of a robustness metric, and ii) the advancement of tailored approaches to clarify the role of topology on synchronization.

These contributions could, in turn, aid in extending the problem of leader selection to richer dynamics than the classical consensus, building on the recent work by [52] that addresses second-order consensus with $\beta = 1$ and small-world scale-free Koch networks. For example, it may be interesting to explore whether leadership selection exhibits also a rich dependence of dynamics, such that the effectiveness of a leader could depend on the specific dynamics that underlie the collective phenomenon. A visually alluring instance can be the example of a fish school. If fish were performing a simple consensus protocol on their heading, then one might expect leaders to place themselves in the center of the group where they could be most visible to others. Experimental evidence suggests that leaders instead could prefer to occupy frontal positions, hinting that perhaps dynamics could play a role in the position leaders choose to maximize their influence on the school [53].

Our results may also contribute to the synthesis of networked control strategies, by helping identify those nodes where filters should be introduced to enhance noise rejection of the overall system. With respect to the alluring example of a fish school, this may open the door to the integration of robotic fish that could influence the collective dynamics [54], against the effect of local perturbations.

One of the main limitations of our work is the linearized treatment of the synchronization problem. Future work should seek to extend the analysis beyond the variational dynamics explored in our work and clarify whether network robustness to large injected noise obeys similar laws as those established in our work. It is possible that large injected noise could push some of the coupled dynamical systems to leave the basin of attraction, destroying network synchronization. Whether parts of the network could still exhibit synchrony is an open question that could be addressed in future research.

Acknowledgments

This work was supported by the National Science Foundation under Grant no. CMMI 1561134, and the US Army Research Office under Grant No. W911NF-15-1-0267 with Drs. Samuel C. Stanton and Alfredo Garcia as the program managers. Views expressed herein are those of authors, and not of the funding agencies.

References

[1] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[2] A.-L. Barabási and Z. N. Oltvai, "Network biology: understanding the cell's functional organization," *Nature Genetics*, vol. 5, no. 2, pp. 101–113, 2004.

[3] E. Bullmore and O. Sporns, "Complex brain networks: graph theoretical analysis of structural and functional systems," *Nature Reviews Neuroscience*, vol. 10, no. 3, pp. 186–198, 2009.

[4] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, no. 4, p. 045104, 2004.

[5] J. Ø. H. Bakke, A. Hansen, and J. Kertész, "Failures and avalanches in complex networks," *EPL (Europhysics Letters)*, vol. 76, no. 4, p. 717, 2006.

[6] Y. Yang, T. Nishikawa, and A. E. Motter, "Vulnerability and cosusceptibility determine the size of network cascades," *Physical Review Letters*, vol. 118, no. 4, p. 048301, 2017.

[7] ——, "Small vulnerable sets determine large network cascades in power grids," *Science*, vol. 358, no. 6365, p. eaan3184, 2017.

[8] F. Harary, "Conditional connectivity," *Networks*, vol. 13, no. 3, pp. 347–357, 1983.

[9] A.-H. Esfahanian and S. L. Hakimi, "On computing a conditional edge-connectivity of a graph," *Information Processing Letters*, vol. 27, no. 4, pp. 195–199, 1988.

[10] G. Bauer and G. Bolch, "Analytical approach to discrete optimization of queueing networks," *Computer Communications*, vol. 13, no. 8, pp. 494–502, 1990.

[11] M. Krishnamoorthy and B. Krishnamurthy, "Fault diameter of interconnection networks," *Computers & Mathematics with Applications*, vol. 13, no. 5, pp. 577–582, 1987.

[12] N. Alon, "Eigenvalues and expanders," *Combinatorica*, vol. 6, no. 2, pp. 83–96, 1986.

[13] B. Mohar, "Isoperimetric numbers of graphs," *Journal of Combinatorial Theory, Series B*, vol. 47, no. 3, pp. 274–291, 1989.

[14] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," *Physical Review Letters*, vol. 85, no. 25, p. 5468, 2000.

[15] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the internet to random breakdowns," *Physical Review Letters*, vol. 85, no. 21, p. 4626, 2000.

[16] ——, "Breakdown of the internet under intentional attack," *Physical Review Letters*, vol. 86, no. 16, p. 3682, 2001.

[17] Y. Moreno, J.-B. Gómez, and A. Pacheco, "Instability of scale-free networks under node-breaking avalanches," *EPL (Europhysics Letters)*, vol. 58, no. 4, p. 630, 2002.

[18] X. Wang, J. L. A. Dubbeldam, and P. Van Mieghem, "Kemeny's constant and the effective graph resistance," *Linear Algebra and its Applications*, vol. 535, pp. 231–244, 2017.

[19] X. Wang, E. Pournaras, R. E. Kooij, and P. Van Mieghem, "Improving robustness of complex networks via the effective graph resistance," *The European Physical Journal B*, vol. 87, no. 9, p. 221, 2014.

[20] A. Ghayoori and A. Leon-Garcia, "Robust network design," in *Communications (ICC), 2013 IEEE International Conference on*. IEEE, 2013, pp. 2409–2414.

[21] G. Tanaka, K. Morino, and K. Aihara, "Dynamical robustness in complex networks: the crucial role of low-degree nodes," *Scientific reports*, vol. 2, p. 232, 2012.

[22] R. Gutiérrez, F. Del-Pozo, and S. Boccaletti, "Node vulnerability under finite perturbations in complex networks," *PLoS ONE*, vol. 6, no. 6, p. e20236, 2011.

[23] A. Buscarino, L. V. Gambuzza, M. Porfiri, L. Fortuna, and M. Frasca, "Robustness to noise in synchronization of complex networks," *Scientific Reports*, vol. 3, 2013.

[24] L. V. Gambuzza, A. Buscarino, L. Fortuna, M. Porfiri, and M. Frasca, "Analysis of dynamical robustness to noise in power grids," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2017.

[25] A. Buscarino, L. Fortuna, M. Frasca, M. Iachello, and V.-T. Pham, "Robustness to noise in synchronization of network motifs: Experimental results," *Chaos*, vol. 22, no. 4, p. 043106, 2012.

[26] B. Bamieh, M. R. Jovanovic, P. Mitra, and S. Patterson, "Coherence in large-scale networks: Dimension-dependent limitations of local feedback," *IEEE Transactions on Automatic Control*, vol. 57, no. 9, pp. 2235–2249, 2012.

[27] F. Lin, M. Fardad, and M. R. Jovanovic, "Algorithms for leader selection in stochastically forced consensus networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 7, pp. 1789–1802, 2014.

[28] S. Patterson, N. McGlohon, and K. Dyagilev, "Optimal k-leader selection for coherence and convergence rate in one-dimensional networks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 3, pp. 523–532, 2016.

[29] K. Fitch and N. E. Leonard, "Joint centrality distinguishes optimal leaders in noisy networks," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 4, pp. 366–378, 2016.

[30] I. Poulakakis, G. F. Young, L. Scardovi, and N. E. Leonard, "Information centrality and ordering of nodes for accuracy in noisy decision-making networks," *IEEE Transactions on Automatic Control*, vol. 61, no. 4, pp. 1040–1045, 2016.

[31] R. Pates and G. Vinnicombe, "Scalable design of heterogeneous networks," *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2318–2333, 2017.

[32] L. C. Evans, *An introduction to stochastic differential equations*. American Mathematical Soc., 2012, vol. 82.

[33] W. Moon and J. Wettlaufer, "On the interpretation of stratonovich calculus," *New Journal of Physics*, vol. 16, no. 5, p. 055017, 2014.

[34] B. Øksendal, *Stochastic differential equations*. Springer, 2003.

[35] C. Godsil and G. Royle, *Algebraic Graph Theory*. New York, NY: Springer-Verlag, 2001.

[36] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*. Cambridge, United Kingdom: Cambridge University Press, 1991.

[37] L. M. Pecora and T. L. Carroll, "Master stability functions for synchronized coupled systems," *Physical Review Letters*, vol. 80, no. 10, p. 2109, 1998.

[38] N. Abaid, I. Igel, and M. Porfiri, "On the consensus protocol of conspecific agents," *Linear Algebra and its Applications*, vol. 437, no. 1, pp. 221–235, 2012.

[39] H. J. Kushner, *Introduction to Stochastic Control*. New York: Holt, Rinehart and Winston, 1971.

[40] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Physics Reports*, vol. 366, no. 1, pp. 1–101, 2002.

[41] A. Arenas, A. Diaz-Guilera, J. Kurths, Y. Moreno, and C. Zhou, "Synchronization in complex networks," *Physics Reports*, vol. 469, no. 3, pp. 93–153, 2008.

[42] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, United Kingdom: Cambridge University Press, 1985.

[43] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[44] L. Huang, Q. Chen, Y.-C. Lai, and L. M. Pecora, "Generic behavior of master-stability functions in coupled nonlinear dynamical systems," *Physical Review E*, vol. 80, no. 3, p. 036204, 2009.

[45] A. Ben-Israel and T. N. E. Greville, *Generalized Inverses: Theory and Applications*. New York, USA: Springer, 2000.

[46] K. Stephenson and M. Zelen, "Rethinking centrality: Methods and examples," *Social Networks*, vol. 11, no. 1, pp. 1–37, 1989.

[47] A. Ghosh, S. Boyd, and A. Saberi, "Minimizing effective resistance of a graph," *SIAM Review*, vol. 50, no. 1, pp. 37–66, 2008.

[48] S. P. Borgatti and M. G. Everett, "A graph-theoretic perspective on centrality," *Social Networks*, vol. 28, no. 4, pp. 466–484, 2006.

[49] R. B. Rothenberg, J. J. Potterat, D. E. Woodhouse, W. W. Darrow, S. Q. Muth, and A. S. Klovdahl, "Choosing a centrality measure: epidemiologic correlates in the colorado springs study of social networks," *Social Networks*, vol. 17, no. 3-4, pp. 273–297, 1995.

[50] C. Li, Q. Li, P. Van Mieghem, H. E. Stanley, and H. Wang, "Correlation between centrality metrics and their application to the opinion model," *The European Physical Journal B*, vol. 88, no. 3, p. 65, 2015.

[51] V. M. Preciado and G. C. Verghese, "Low-order spectral analysis of the kirchhoff matrix for a probabilistic graph with a prescribed expected degree sequence," *IEEE Transactions on Circuits and Systems I*, vol. 56, no. 6, pp. 1231–1240, 2009.

[52] Y. Yi, Z. Zhang, L. Shan, and G. Chen, "Robustness of first-and second-order consensus algorithms for a noisy scale-free small-world Koch network," *IEEE Transactions on Control Systems Technology*, vol. 25, no. 1, pp. 342–350, 2017.

[53] A. J. King, D. D. Johnson, and M. Van Vugt, "The origins and evolution of leadership," *Current Biology*, vol. 19, no. 19, pp. R911–R916, 2009.

[54] S. Butail, N. Abaid, S. Macrì, and M. Porfiri, "Fish–robot interactions: robot fish in animal behavioral studies," in *Robot Fish*. Springer, 2015, pp. 359–377.

PLACE PHOTO HERE

Maurizio Porfiri Dr. Maurizio Porfiri is a Professor in the Department of Mechanical and Aerospace Engineering at New York University Tandon School of Engineering. He received M.Sc. and Ph.D. degrees in Engineering Mechanics from Virginia Tech, in 2000 and 2006; a Laurea in Electrical Engineering (with honours) and a Ph.D. in Theoretical and Applied Mechanics from the University of Rome La Sapienza and the University of Toulon (dual degree program), in 2001 and 2005, respectively. He is engaged in conducting and supervising research on dynamical systems theory, multiphysics modeling, and underwater robotics. Maurizio Porfiri is the author of more than 250 journal publications and the recipient of the National Science Foundation CAREER award. He has been included in the Brilliant 10 list of Popular Science and his research featured in all the major media outlets, including CNN, NPR, Scientific American, and Discovery Channel. Other significant recognitions include invitations to the Frontiers of Engineering Symposium and the Japan-America Frontiers of Engineering Symposium organized by National Academy of Engineering; the Outstanding Young Alumnus award by the college of Engineering of Virginia Tech; the ASME Gary Anderson Early Achievement Award; the ASME DSCD Young Investigator Award; and the ASME C.D. Mote, Jr. Early Career Award.

PLACE PHOTO HERE

Mattia Frasca Mattia Frasca graduated in Electronics Engineering in 2000 and received the Ph.D. in Electronics and Automation Engineering in 2003, at the University of Catania, Italy. Currently, he is associate professor at the University of Catania, where he also teaches Process control. His scientific interests include nonlinear systems and chaos, complex networks and bio-inspired robotics. He is involved in many research projects and collaborations with industries and academic centres. He is referee for many international journals and conferences. He was chair of the European Conference on Circuit Theory and Design ECCTD 2017, in the organizing committee of the 10th "Experimental Chaos Conference" and co-chair of the "4th International Conference on Physics and Control". He is coauthor of four research monographs (published by Springer and World Scientific) and two textbooks (published by CRC Press). He published more than 250 papers on refereed international journals and international conference proceedings and is co-author of two international patents. He is IEEE Senior and, since January 2018, President of the Italian Society for Chaos and Complexity (SICC).