Impact of Network Topology on the Resilience of Vehicle Platoons

Mohammad Pirani, Simone Baldi, *Senior Member, IEEE*, and Karl Henrik Johansson, *Fellow, IEEE*

***Abstract*— This paper presents a comprehensive study on the impact of information flow topologies on the resilience of distributed algorithms that are widely used for estimation and control in vehicle platoons. In the state of the art, the influence of information flow topology on both internal and string stability of vehicle platoons has been well studied. However, understanding the impact of information flow topology on cyber-security tasks, e.g., attack detection, resilient estimation and formation algorithms, is largely open. By means of a general graph theory framework, we study connectivity measures of several platoon topologies and we reveal how these measures affect the ability of distributed algorithms to reject communication disturbances, to detect cyber-attacks, and to be resilient against them. We show that the traditional platoon topologies relying on interaction with the nearest neighbor are very fragile with respect to performance and security criteria. On the other hand, appropriate platoon topologies, namely k-nearest neighbor topologies, are shown to fulfill desired security and performance levels. The framework we study covers undirected and directed topologies, ungrounded and grounded topologies, or topologies on a line and on a ring. We show that there is a trade-off in the network design between the robustness to disturbances and the resilience to adversarial actions. Theoretical results are validated via simulations.**

***Index Terms*— Resilience of vehicle platoons, graph theory, network connectivity, distributed algorithms.**

I. Introduction

CONNECTED vehicles are vehicles that use a number of different communication technologies to communicate with other vehicles on the road, e.g., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or with the driver. A typical connected vehicle test case often studied in the literature is platooning. Platooning is a method for driving a group of vehicles in a queue which is meant to increase the capacity of roads via an automated highway system.

A. Motivation

Due to the need to operate autonomously and in a wide range of situations, notions of *robustness* and *resilience* of connected vehicles naturally arise. An accepted definition of the robustness of control systems is their ability to withstand perturbation without the need for adaptation. On the other hand, resilience is referred to the ability of the system to respond to perturbation and restore full functionality (or a certain level of functionality). As compared to robustness, guaranteeing resilience demands larger complexity and computation. In large-scale systems, both notions of robustness and resilience highly depend on the structure of the underlying communication network and on the type of distributed algorithms operating in the large-scale system.

Distributed estimation and/or control algorithms are commonly operated in large-scale systems with interconnected processors. The algorithm is broken into parts and each part is operated concurrently and independently with a limited amount of information. These features make distributed algorithms suitable to operate connected vehicles. Distributed estimation and control algorithms, including consensus-based algorithms and distributed resource allocation, are pivotal in improving connected vehicles' safety, improving the traffic throughput, and optimizing the energy consumption [1]–[3]. In those problems, system-theoretic conditions are sought which ensure the effectiveness of the proposed algorithms. However, by increasing the scale of the vehicular network and the complexity of the interactions, cyber-security issues must be also taken into account. In this paper, we investigate the impact of the topology of vehicle platoons on the robustness and resilience of certain distributed estimation and control algorithms which are applicable in cooperative control of vehicle platoons.

B. Related Work

Concerns about the performance and resilience of distributed platooning algorithms against faults and adversarial behaviours have been an avenue of research in recent years [4]–[7]. In addition to systems and control tools, networks and graph theory have been also used to model various structures of connected vehicles. While these modeling tools have been in general studied independently, it is recognized that intelligent platoons require a tight relation between system-theoretic and network-theoretic approaches.

The relation between the network science and systems and control, which are entangled in networked control systems, has been an active line of research [8], [9]. This has been

Manuscript received 4 February 2021; revised 6 October 2021; accepted 14 December 2021. Date of publication 11 January 2022; date of current version 12 September 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62073074, in part by the Double Innovation Plan under Grant 4207012004, and in part by the Special Funding for Overseas under Grant 6207011901. The Associate Editor for this article was S. E. Li. *(Corresponding author: Simone Baldi.)*

Mohammad Pirani is with the Department of Mechanical and Mechatronics Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: mpirani@uwatreloo.ca).

Simone Baldi is with the School of Mathematics, Southeast University, Nanjing 210096, China, and also with the Delft Center for System and Control, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: s.baldi@tudelft.nl).

Karl Henrik Johansson is with the Division of Decision and Control Systems, KTH Royal Institute of Technology, 114 28 Stockholm, Sweden (e-mail: kallej@kth.se).

Digital Object Identifier 10.1109/TITS.2021.3137826

done by advancing interdisciplinary fields in applied mathematics and systems theory, e.g., algebraic graph theory and structured systems theory. There is a body of research on redefining system-theoretic notions from the network's perspective. In this direction, there are newly introduced notions such as *network coherence* [9], [10], which is a system-norm interpretation of a networked control system, and *network robustness* [11], which defines the ability of a network to bypass the adversaries during the operation of distributed algorithms. Moreover, resilient and secure estimation and control in networked systems have been studied from a graph-theoretic perspective in [12], [13]. Such an interplay between the two areas finds diverse applications in mobile ad-hoc networks and connected vehicles. Some works have investigated the impact of platoon topologies on the performance of cooperative adaptive cruise control algorithms: [14], [15] studied the impact of the platoon topology on the stability and string stability of a vehicle platoon formation; in [16], the influence of directed and bidirectional topologies on the robustness of platoon to communication disturbances was discussed; methods to compensate communication delay in a homogeneous cooperative adaptive cruise control systems were proposed in [17]; discussions on the impact of the topology on the robustness to time delay can be found in [1], showing a trade-off between making the platoon robust to time delay and to disturbances or additive faults.

C. Contribution

The current paper is among the few studies about the impact of the platoon topology on the resilience and security of distributed estimation and control algorithms [18], [19]. The contributions of this paper are:

- We discuss the resilience of several platoon topologies to the adversarial actions in different distributed estimation and control algorithms. We show that for every distributed algorithm, a certain network connectivity measure represents the resilience of that algorithm to adversaries.
- We show that traditional platoon topologies based on the interaction with the nearest neighbor are fragile with respect to performance and security criteria. On the other hand, appropriate platoon topologies, namely k-nearest neighbor topologies, are shown to fulfill desired security and performance levels.
- We show that there is a trade-off in the topology design between the robustness of vehicle platoons to disturbances and their resilience against attacks.

This work extend the preliminary study [20] in various directions: First, we investigate the resilience of a wider range of platoon topologies (Propositions 1, 2, 4 and 5, Lemma 1). Second, graph-theoretic conditions for anomaly detection in platoons are studied here (Section IV-D). Third, the trade-off between resilience and performance is presented. Finally, this work gives a proof for the network robustness in k-nearest neighbor platoons (Theorem 1).

D. Notations and Definitions

In this paper, a directed network (graph) is denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes (or vertices) and $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ is the set of edges. In particular, $(v_i, v_j) \in \mathcal{E}$ if and only if there exists a directed edge from v_i to v_j. When $(v_i, v_j) \in \mathcal{E}$ implies $(v_j, v_i) \in \mathcal{E}$, the graph is called undirected. Neighbors of node $v_i \in \mathcal{V}$ are indicated by the set $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid (v_j, v_i) \in \mathcal{E}\}$. The degree of each node v_i is denoted by $d_i = |\mathcal{N}_i|$ and the minimum and maximum degrees in graph $\mathcal{G}$ are denoted by $d_{\min}$ and $d_{\max}$, respectively. The adjacency matrix of the graph is a binary $n \times n$ matrix A, where element $A_{ij} = 1$ if $(v_j, v_i) \in \mathcal{E}$ and $A_{ij} = 0$ otherwise. The Laplacian matrix of the graph is $L \triangleq D - A$, where $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$. The eigenvalues of a symmetric Laplacian are nonnegative and are denoted by $0 = \lambda_1(L) \leq \lambda_2(L) \leq \ldots \leq \lambda_n(L)$ and $\lambda_2(L)$ is called the algebraic connectivity of the network [21]. For graph $\mathcal{G}$ with m edges, numbered as $e_1, e_2, \ldots, e_m$, its node-edge incidence matrix $\mathcal{B}(\mathcal{G}) \in \mathbb{R}^{n \times m}$ is defined as [21]

$$[\mathcal{B}(\mathcal{G})]_{kl} = \begin{cases} 1 & \text{if node } k \text{ is the head of edge } l, \\ -1 & \text{if node } k \text{ is the tail of edge } l, \\ 0 & \text{otherwise.} \end{cases}$$

The graph Laplacian satisfies $L = \mathcal{B}(\mathcal{G})\mathcal{B}(\mathcal{G})^{\mathsf{T}}$ [21]. For a given subset $\mathcal{S} \subset \mathcal{V}$ of nodes (which we term *grounded nodes*), the *grounded Laplacian* induced by $\mathcal{S}$ is denoted by $L_g(\mathcal{S})$ or simply L_g, and is obtained by removing the rows and columns of L corresponding to the nodes in $\mathcal{S}$. Given two subsets $\mathcal{X}_1, \mathcal{X}_2 \subset \mathcal{V}$, a set of r vertex disjoint paths, each with start vertex in $\mathcal{X}_1$ and end vertex in $\mathcal{X}_2$, is called an r-linking from $\mathcal{X}_1$ to $\mathcal{X}_2$ and is denoted by $\mathcal{L}_r(\mathcal{X}_1, \mathcal{X}_2)$. The largest integer less than a is denoted by $\lfloor a \rfloor$.

II. Graph Connectivity Measures

In this section, we introduce a set of connectivity measures that will be useful to quantify the resilience of various distributed algorithms performed on vehicle platoons.

A. Vertex and Edge Connectivity

A *vertex-cut* in a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a subset $\mathcal{S} \subset \mathcal{V}$ of vertices such that removing the vertices in $\mathcal{S}$ (and any resulting dangling edges) from the graph causes the remaining graph to be disconnected. A (j, i)*-cut* in a graph is a subset $\mathcal{S}_{ij} \subset \mathcal{V}$ such that if the nodes $\mathcal{S}_{ij}$ are removed, the resulting graph contains no path from vertex v_j to vertex v_i. Let κ_{ij} denote the size of the smallest (j, i)-cut between any two vertices v_j and v_i. The graph $\mathcal{G}$ is said to have *vertex connectivity* $\kappa(\mathcal{G}) = \kappa$ (or to be κ*-vertex-connected*) if $\kappa_{ij} = \kappa$ for all $i, j \in \mathcal{V}$. The *edge connectivity* $e(\mathcal{G})$ of a graph $\mathcal{G}$ is the minimum number of edges whose deletion disconnects the graph. For the vertex and edge connectivity and graph's minimum degree the following inequalities hold [22]

$$\kappa(\mathcal{G}) \leq e(\mathcal{G}) \leq d_{\min}(\mathcal{G}). \tag{1}$$

Due to inequality (1), in this paper we will focus on vertex connectivity, since it gives the minimum degree of connectivity in a network. From now, we simply use *k-connected* to indicate a k-vertex connected graph.

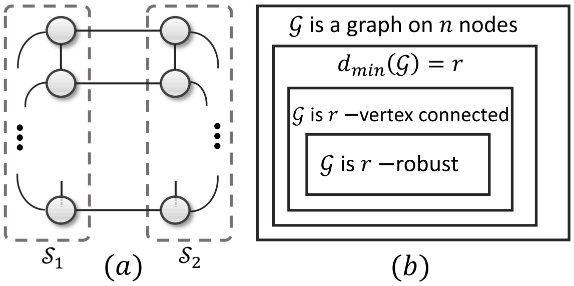

$\mathcal{S}_1$
(a)
$\mathcal{S}_2$
$\mathcal{G}$ is a graph on n nodes
$d_{min}(\mathcal{G}) = r$
$\mathcal{G}$ is r −vertex connected
$\mathcal{G}$ is r −robust
(b)

Fig. 1. (a) A graph with a large connectivity (n-vertex connected) but small robustness (1-robust), (b) Schematic set diagram of graph connectivities [23].

B. Graph Robustness

Let $r \in \mathbb{N}$. A subset $\mathcal{S} \subset \mathcal{V}$ of nodes in the graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is said to be *r-reachable* if there exists a node $v_j \in \mathcal{S}$ such that $|\mathcal{N}_j \setminus \mathcal{S}| \geq r$. A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is said to be *r-robust* if for every pair of nonempty, disjoint subsets of $\mathcal{V}$, at least one of them is r-reachable.

Note that r-robustness is a stronger notion than r-connectivity [11], as shown in the following example.

Example 1: The graph shown in Fig. 1 (a) is comprised of two complete graphs (i.e., there is an edge between each pair of nodes) on n nodes ($\mathcal{S}_1$ and $\mathcal{S}_2$) and each node in $\mathcal{S}_1$ has exactly one neighbor in $\mathcal{S}_2$ and vice-versa. The minimum degree and the vertex connectivity are both n; however, the network is only 1-robust. □

C. Algebraic Connectivity

For a subset of nodes $\mathcal{X} \subset \mathcal{V}$, its *edge-boundary* is $\partial\mathcal{X} \triangleq \{(v_i, v_j) \in \mathcal{E} \mid v_i \in \mathcal{X}, v_j \in \mathcal{V}\backslash\mathcal{X}\}$. The *isoperimetric constant* of $\mathcal{G}$ is defined as [24]

$$i(\mathcal{G}) \triangleq \min_{\mathcal{S}\subset\mathcal{V}, |\mathcal{S}|\leq\frac{n}{2}} \frac{|\partial\mathcal{S}|}{|\mathcal{S}|}, \tag{2}$$

where $\partial\mathcal{S}$ is the edge-boundary of a set of nodes $\mathcal{S} \subset \mathcal{V}$.

For an undirected graph, the algebraic connectivity is related to the isoperimetric constant by the following bounds [24]

$$\frac{i(\mathcal{G})^2}{2d_{\max}(\mathcal{G})} \leq \lambda_2(L) \leq 2i(\mathcal{G}). \tag{3}$$

Fig. 1 (b) schematically shows the strength of the connectivity measures in general graphs [23]. One can include the algebraic connectivity in (1) and get [21]

$$\lambda_2(L) \leq \kappa(\mathcal{G}) \leq e(\mathcal{G}) \leq d_{\min}(\mathcal{G}).$$

This shows that the algebraic connectivity is the strongest notion of connectivity, compared to the edge and vertex connectivity. For the relation between robustness and algebraic connectivity, we have $\lambda_2(L) \leq 2i(\mathcal{G})$ [24]. Based on this, if $\lambda_2(L) > r - 1$, then the network is at least $\lfloor\frac{r}{2}\rfloor$-robust [23]. However, $\lfloor\frac{r}{2}\rfloor$ provides a loose lower bound for the network robustness. An example is a star graph which is 1-robust with $\lambda_2(L) = 1$. Further research is needed to be done in this direction.

III. Platoon Topologies

In this section, we discuss classes of topologies popularly used in vehicle platoon problems and summarized in Fig. 2. Graph connectivity measures of these topologies are also discussed, whereas their resilience properties will be investigated later in the paper (Sect. IV).

A. Nearest Neighbor Topologies

The simplest and most well-known vehicle platoon topology is the nearest neighbor topology, in which every vehicle communicates with its immediate neighbors. There are two kinds of nearest neighbor topology: predecessor following (also called *directed*) and bidirectional (also called *undirected*). In bidirectional topology, every vehicle can send and receive information from the immediate vehicles in its front and back, Fig. 2(a), while in predecessor following topology, each vehicle receives information from the vehicle in its front, Fig. 2(b). Note that the notions of graph connectivity do not give much information in platoons with directed line topologies. Because in directed acyclic graphs, since there is always a pair (v_i, v_j) in which there is no path from v_i to v_j (which consequently implies zero connectivity). Hence, in this paper, we either study the connectivity measures of directed platoons on a ring (Proposition 4) or talk about vertex cuts between subsets of nodes in directed platoons on a line (Section IV-D).

An undirected nearest neighbor topology is clearly a 1-connected and 1-robust network. The isoperimetric constant of the platoon is $i(\mathcal{G}) = \frac{2}{n}$ and, based on (3), the algebraic connectivity of the graph is upper bounded by $\lambda_2(L) \leq \frac{4}{n}$. We will see in Section IV that these connectivity measures imply a low level of resilience of the nearest neighbor platoon against failures and adversarial behaviours.

B. Leader-to-All Topologies

A leader-to-all topology is a nearest neighbor topology where every vehicle is also connected to the leading vehicle in the head of the platoon. An advantage of this topology, compared to the nearest neighbor topology, is that each vehicle is able to receive information of the leading vehicle directly. Due to the peculiarity of this topology, it can appear in three forms: *undirected leader-to-all*; *undirected leader-to-all leader-tracking*; *directed leader-to-all leader-tracking*, as shown in Fig. 2(c)-(d)-(e), respectively. The term leader tracking refers to the fact that the communication between the leader and the other vehicles is unidirectional (i.e. the leader does not receive any communication and thus its control strategy is not affected by other vehicles in the platoon): then, as in Fig. 2(d)-(e), the vertex connectivity is the same as the nearest neighbor topology. When the communication between the leader and other vehicles is bidirectional, as in Fig. 2(c), it is intuitive that the connectivity is larger compared to the nearest neighbor platoons, as clarified below.

Proposition 1: An undirected leader-to-all topology is 2-connected and 2-robust. □

Proof: We first show 2-robustness. Suppose that we remove the leader and its incident edges. The remaining graph

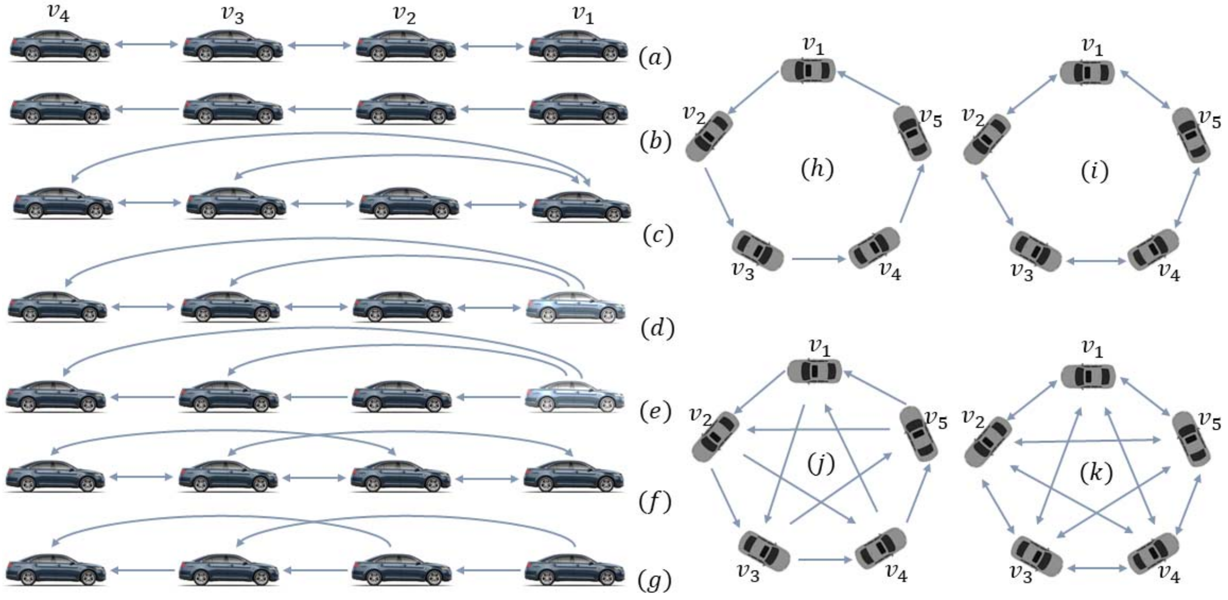


Fig. 2. (a) Undirected nearest neighbor, (b) Directed nearest neighbor, (c) Undirected leader-to-all, (d) Undirected leader-to-all leader tracking, (e) Directed leader-to-all leader tracking, (f) Undirected 2-nearest neighbor, (g) Directed 2-nearest neighbor, (h) Directed nearest neighbor ring, (i) Undirected nearest neighbor ring, (j) Directed 2-nearest neighbor ring, (k) Undirected 2-nearest neighbor ring.

is a nearest neighbor platoon which is 1-connected. Hence, based on Proposition 1 in [25], by adding the leader and connect it to all other vehicles the platoon with $n \geq 3$ vehicles is 2-robust. Increasing the length of the platoon, by adding vehicle $n+1$ to the end of the line with degree 2 (i.e., connected to vehicle n and the leader) maintains the robustness of the graph, based on Theorem 6 in [26]. Since robustness is stronger than connectivity, the platoon is at least 2-connected. Moreover, as the smallest degree of the graph is 2, according to (1), it is exactly 2-connected. ■

The following proposition provides bounds on the algebraic connectivity of the undirected leader-to-all topology.

Proposition 2: For the undirected leader-to-all topology we have $1 \leq \lambda_2(L) \leq 2$. □

Proof: The lower bound comes from the fact that a star topology, i.e., the topology that all nodes are connected to a single node, is a subgraph of the leader-to-all topology. For the star graph we have $\lambda_2(L) = 1$. Hence, since the algebraic connectivity is an increasing function of edge addition, the lower bound is obtained. The upper bound is due to $\lambda_2(L) \leq d_{\min}(\mathcal{G}) = 2$. ■

As shown in Proposition 1, the leader-to-all topology with bidirectional communication exhibits a higher connectivity level than the nearest neighbor topology. However, this connectivity is not scalable since it is always 2 for any platoon. In order to reach to larger connectivity levels, a scalable platoon topology is discussed in the following subsection.

C. k-Nearest Neighbor Topologies

The k-nearest neighbor platoon is a generalization of nearest neighbor topology. For positive integers $n, k \geq 1$ with $n > k$, a k-nearest neighbor topology, denoted by $\mathcal{P}(n, k)$, is a network comprised of n vehicles where each vehicle can communicate with its k nearest neighbors. In bidirectional topology, each vehicle communicates with its front k nearest neighbors and its back and k nearest neighbors ($k = 2$ in Fig. 2(f)). In the predecessor following topology, each vehicle receives data only from its front k nearest neighbors ($k = 2$ in Fig. 2(g)). Inspired from sensor networks, the value of k might depend on the limited sensing and communication range for each vehicle and the distance with the consecutive vehicles [1]. To formalize this point, it is convenient to look at $\mathcal{P}(n, k)$ as a geometric graph [27], as discussed below.

Undirected k-Nearest Neighbor Topology as a Geometric Graph: A one dimensional geometric graph $\mathcal{G}_{n,\rho,l} = (\mathcal{V}, \mathcal{E})$ is an undirected graph which is formed by placing n nodes (based on some procedure) in a 1-dimensional region $\Omega = [0, l]$. The position of node $v_i \in \mathcal{V}$ is denoted by $x(i) \in \Omega$. Nodes $v_i, v_j \in \mathcal{V}$ are connected by an edge if and only if $||x_i - x_j|| \leq \rho$ for some threshold ρ, where $|| \cdot ||$ is some vector norm (usually the standard Euclidean norm).

Based on the above definition, a bidirectional k-nearest neighbor topology can be seen as a geometric graph $\mathcal{G}_{n,\rho,l}$ with $\rho = \frac{lk}{n-1}$ and placing the nodes as follows: the first node, v_1, is placed on one end of the line and the i-th node is placed in distance $\frac{(i-1)l}{n-1}$ from v_1.

Lemma 1: A k-nearest neighbor platoon $\mathcal{P}(n, k)$ with $n \geq 2k-1$ is a k-vertex and a k-edge connected graph, i.e., $\kappa(\mathcal{G}) = e(\mathcal{G}) = k$. □

Proof: We prove using contradiction. Suppose that the k-nearest neighbor platoon is a ℓ-vertex connected graph, with $\ell < k$. Then, a minimum vertex cut $\mathcal{S}_{ij}$ exists between two vertices v_i and v_j in which $|\mathcal{S}_{ij}| = \ell$. We label the vertices from v_i to v_j as $v_i, v_{i+1}, \ldots, v_j$. Since $\ell < k$, there is a vertex $\bar{v}$ among $v_{i+1}, \ldots, v_{i+k}$ (which are directly connected to v_i) which does not belong to $\mathcal{S}_{ij}$. By replacing v_i with $\bar{v}$ in the above discussion, we will find a path from v_i to v_j which does not include vertices in $\mathcal{S}_{ij}$ and this contradicts the claim that $\mathcal{S}_{ij}$ is a vertex cut. Hence $\mathcal{P}(n, k)$ is a k-vertex connected graph. For the edge connectivity, we use (1) and considering that for $\mathcal{P}(n, k)$ we have $d_{\min} = k$. This completes the proof. ■

Theorem 1: A k-nearest neighbor platoon $\mathcal{P}(n, k)$ with $n \geq 2k - 1$ is k-robust. □

Proof: First, based on [26], we know that if $n < 2k-1$ the graph is not k-robust even if it is a complete graph. Moreover, for $k \leq 4$ the graph with $n = 2k - 1$ nodes, if we label the nodes as in Fig. 2, nodes $k - 1$, k, and $k + 1$ are connected to all other nodes in the graph. We collect these three nodes in set S. If we remove the nodes in set S and their incident edges, the resulting graph remains connected. Hence, based on Proposition 1 in [25], the graph with $n = 2k - 1$ nodes is k-robust. Increasing the length of the platoon happens by adding nodes, each with degree k, to the end of $\mathcal{P}(2k - 1, k)$. Thus, based on Theorem 6 in [26], the graph remains k-robust.

For k, we use complete (strong) induction. We use $k \leq 4$ as the base of induction, i.e., $\mathcal{P}(n, k)$ with $n = 2k - 1$ nodes is k-robust for $k \leq 4$. We assume that for any $k \leq \bar{k}$, $\mathcal{P}(n, k)$ with $n \geq 2k - 1$ nodes is k-robust. We must show that $\mathcal{P}(n, \bar{k} + 1)$ with $n \geq 2\bar{k}+1$ nodes is $\bar{k}+1$-robust. We prove for $n = 2(\bar{k}+1)-1 = 2\bar{k}+1$ and for $n > 2\bar{k}+1$, adding nodes with degree $\bar{k}+1$ just preserves the robustness. Similar to the case of $k \leq 4$, there exists set $S = \{v_{k-1}, v_k, v_{k+1}\}$ where each of these three nodes is connected to all nodes in the graph. We choose (any) two nodes from S, denoted by $\bar{S} \subset S$. We remove nodes in $\bar{S}$ and their incident edges from $\mathcal{P}(2\bar{k} + 1, \bar{k} + 1)$ and introduce $\bar{\mathcal{P}} = \mathcal{P} \setminus \bar{S}$ as the graph of size $2\bar{k} - 1$. Clearly, we can see $\bar{\mathcal{P}}$ as a $(\bar{k} - 1)$-nearest neighbor platoon of size $2\bar{k} - 1$ with some additional edges. If we remove nodes v_1 and $v_{2\bar{k}-1}$ and their incident edges from $\bar{\mathcal{P}}$, it becomes $\mathcal{P}(2\bar{k} - 3, \bar{k} - 1)$ which is, by induction assumption, $(\bar{k} - 1)$-robust. Hence, bringing back the nodes v_1 and $v_{2\bar{k}-1}$ preserves $(\bar{k} - 1)$-robustness of $\bar{\mathcal{P}}$. We use $(\bar{k}-1)$-robustness of $\bar{\mathcal{P}}$ to prove $(\bar{k}+1)$-robustness of $\mathcal{P}(2\bar{k}+1, \bar{k}+1)$. Let S_1 and S_2 be two non-empty disjoint subsets of nodes in $\mathcal{P}$ and $|S_1| < |S_2|$. We consider two cases: (i) $S_1 \cap \bar{S} \neq \emptyset$: In this case, there exists $v \in S_1 \cap \bar{S}$ and we have $|\mathcal{N}_v \setminus S_1| = 2\bar{k} - (|S_1| - 1)$. Since $1 \leq |S_1| \leq \bar{k}$, we have $|\mathcal{N}_v \setminus S_1| \geq \bar{k} + 1$. Thus, S_1 is $(\bar{k} + 1)$-reachable. (ii) $S_1 \cap \bar{S} = \emptyset$: In this case, $S_1 \subset \bar{\mathcal{P}}$. By design, each node in $\bar{\mathcal{P}}$, and consequently S_1, is connected to both nodes in $\bar{S}$. Moreover, since $\bar{\mathcal{P}}$ is $(\bar{k}-1)$-robust, then there is a node $v \in S_1$ for which $|\mathcal{N}_v \setminus S_1| = \bar{k} - 1 + 2 = \bar{k} + 1$ which shows that S_1 is $(\bar{k} + 1)$-reachable in $\mathcal{P}$. This completes the proof. ■

Using (3), we present the following bounds on the algebraic connectivity of bidirectional k-nearest neighbor platoons.

Proposition 3: Given a k-nearest neighbor platoon $\mathcal{P}(n, k)$ its algebraic connectivity is bounded by

$$\max\left\{2k - n + 2, \frac{k(k+1)^2}{4n^2}\right\} \leq \lambda_2(L) \leq \frac{2k(k+1)}{n}. \quad (4)$$

□

Proof: First we use bounds given in (3). For this, we should calculate the isoperimetric constant in $\mathcal{P}(n, k)$ by finding a set in $\mathcal{P}(n, k)$ which minimizes $\frac{|\partial S|}{|S|}$ with $|S| \leq \frac{n}{2}$. A set which contains consecutive $\lfloor \frac{n}{2} \rfloor$ nodes, starting from the head of the platoon, minimizes this function. Hence, the isoperimetric constant will be $i(\mathcal{G}) = \frac{1+2+...+k}{\lfloor \frac{n}{2} \rfloor} = \frac{k(k+1)}{2\lfloor \frac{n}{2} \rfloor}$. Substituting this value into (3) and considering the fact that $d_{\max} \leq 2k$ provides the upper bound and the lower bound $\frac{k(k+1)^2}{4n^2}$. The second lower bound comes from bound $2d_{\min} - n + 2 \leq \lambda_2(L)$ proposed in [28] and considering the fact that $d_{\min} = k$. The maximum over two lower bounds in (5) is due to the fact that for certain values of k one of the lower bounds is tighter than the other. For instance, for $k \leq \frac{n-2}{2}$ the left lower bound is zero or negative and the right lower bound is tighter. However, for $k = n - 1$ the left lower bound is tighter. ■

D. Ring Topologies

The topologies in Sects. III-A-III-C refer to vehicles running on a line. In recent years, vehicle platoons running on a ring have been studied, mostly motivated by the fact that performing experimental tests on a ring is easier than experiments on a line [29], [30]. From the theoretical point of view, this poses the interesting question on the generalizability of the results obtained on ring topologies to line topologies. With this in mind, in this paper we investigate the resilience of different platoon topologies on a ring and compare the results with the line topology. Similar to line topologies, we consider both directed and undirected ring topologies, and their k-nearest neighbor versions (Fig. 2(h)-(k)). According to [31], along with Theorem 1, we have the following result.

Proposition 4: A bidirectional k-nearest neighbor ring topology is $2k$-connected and k-robust. Moreover, a directed k-nearest neighbor ring is k-connected and at least $\lfloor \frac{k+2}{4} \rfloor$-robust. □

As a counterpart of k-nearest neighbor platoon topology, we have the following result for the algebraic connectivity of k-nearest neighbor ring topology. The proof is the same as that of Proposition 3 considering that for the ring topology we have $d_{\min} = d_{\max} = 2k$ and $i(\mathcal{G}) = \frac{2k(k+1)}{n}$.

Proposition 5: The algebraic connectivity of a k-nearest neighbor ring platoon is bounded by

$$\max\left\{4k - n + 2, \frac{k(k+1)^2}{n^2}\right\} \leq \lambda_2(L) \leq \frac{4k(k+1)}{n}. \quad (5)$$

□

The connectivity measures for different vehicle platoons with bidirectional communication are summarized in Table I.

Remark 1 (Trade-Off Between Connectivity Measures): According to the values in Table I, if k is sufficiently small, i.e., $k(k+1) \leq \frac{n}{2}$, the leader-to-all platoon has a larger algebraic connectivity than k-nearest neighbor platoon. On the other hand, for $k > 2$, the vertex connectivity of k-nearest neighbor platoon is always larger than the leader-to-all topology. Hence, there exists a trade-off in topology design between vertex and algebraic connectivity. We will revisit this trade-off later in Section IV. □

IV. Distributed Algorithms on Platoons

In this section, we show how the resilience properties of distributed estimation and control algorithms for vehicle

TABLE I

CONNECTIVITY MEASURES FOR DIFFERENT PLATOON TOPOLOGIES WITH BIDIRECTIONAL COMMUNICATIONS

Topology	Vertex Connectivity	Robustness	Algebraic Connectivity
Nearest Neighbor	1	1	$\lambda_2(L) \leqslant \frac{4}{n}$
Undirected Leader-to-all	2	2	$1 \leqslant \lambda_2(L) \leqslant 2$
Leader-tracking Leader-to-all	1	1	$\lambda_2(L) \leqslant \frac{4}{n}$
k-Nearest Neighbor	k	k	$\max\left\{2k-n+2, \frac{k(k+1)^2}{4n^2}\right\} \leqslant \lambda_2(L) \leqslant \frac{2k(k+1)}{n}$
k-Nearest Neighbor (ring)	$2k$	k	$\max\left\{4k-n+2, \frac{k(k+1)^2}{n^2}\right\} \leqslant \lambda_2(L) \leqslant \frac{4k(k+1)}{n}$

platoons are intrinsically related to the connectivity measures discussed in Section II.

A. $\mathcal{H}_\infty$ Norm Approach to Resilient Network Formation

In formation control, each agent (vehicle) tries to keep a safe distance from its neighbors. We denote the position and velocity of vehicle v_i by p_i and u_i, respectively. The desired safe distance between two vehicles v_i and v_j is Δ_{ij} which should satisfy $\Delta_{ij} = \Delta_{ik} + \Delta_{kj}$ for every triple $\{v_i, v_j, v_k\} \subset \mathcal{V}$. Considering the fact that each vehicle v_i has access to its own position and velocity, as well as the positions and velocities of its neighbors, and the desired inter-vehicular distances Δ_{ij}, the control law for vehicle v_i is [16]

$$\ddot{p}_i(t) = \sum_{j\in\mathcal{N}_i} k_p\left(p_j(t) - p_i(t) + \Delta_{ij}\right) + k_u\left(u_j(t) - u_i(t)\right) + w_i(t), \quad (6)$$

where $k_p, k_u > 0$ are control gains and $w_i(t)$ models communication disturbances.[1] Dynamics (6) in matrix form become

$$\dot{\boldsymbol{x}}(t) = \underbrace{\begin{bmatrix}\mathbf{0}_n & I_n\\ -k_pL & -k_uL\end{bmatrix}}_{A}\boldsymbol{x}(t) + \underbrace{\begin{bmatrix}\mathbf{0}_{n\times 1}\\ k_p\Delta\end{bmatrix}}_{B} + \underbrace{\begin{bmatrix}\mathbf{0}_n\\ I\end{bmatrix}}_{F}\boldsymbol{w}(t), \quad (7)$$

where $\boldsymbol{x} = [\mathbf{P}\ \dot{\mathbf{P}}]^\mathsf{T} = [p_1, p_2, \dots, p_n, \dot{p}_1, \dot{p}_2, \dots, \dot{p}_n]^\mathsf{T}$, $\boldsymbol{w}(t) = [w_1, w_2, \dots, w_n]^\mathsf{T}$ $\Delta = [\Delta_1, \Delta_2, \dots, \Delta_n]^\mathsf{T}$ in which $\Delta_i = \sum_{j\in\mathcal{N}_i}\Delta_{ij}$. The objective is to quantify the impact of the external disturbances $\boldsymbol{w}$ on the distances between consecutive vehicles. To do this, an appropriate output measurement $\mathbf{y} = \mathcal{B}^\mathsf{T}\mathbf{P}$ is chosen, where $\mathcal{B} \in \mathbb{R}^{n\times|\mathcal{E}|}$ is the incidence matrix associated with the network and $\mathbf{P} = [p_1, p_2, \dots, p_n]^\mathsf{T}$. With this output, we have the distance between neighbor vehicles, i.e., $y_{ij} = p_i - p_j$, as a measurement. The sensitivity of this measured output to disturbances is captured by an appropriate system norm. We choose the system $\mathcal{H}_\infty$ norm which represents the worst case amplification of the disturbances over all frequencies. This system norm is widely used in disturbance rejection in vehicle platoons [32].

Theorem 2: The system $\mathcal{H}_\infty$ norm of (7) from the external disturbances $\boldsymbol{w}(t)$ to $\mathbf{y} = \mathcal{B}^\mathsf{T}\mathbf{P}$ is

$$||G||_\infty = \begin{cases} \dfrac{2}{k_u\lambda_2(L)\sqrt{4k_p - k_u^2\lambda_2(L)}}, & \text{if } \dfrac{\lambda_2(L)k_u^2}{2k_p} \le 1,\\[2ex] \dfrac{1}{k_p\lambda_2^{\frac{1}{2}}(L)} & \text{otherwise,}\end{cases} \quad (8)$$

where $\lambda_2(L)$ is the algebraic connectivity of the underlying platoon topology. □

Proof: First we show that the system $\mathcal{H}_\infty$ norms of (7) from disturbance $\boldsymbol{w}$ to performance outputs $\mathbf{y} = \mathcal{B}^\mathsf{T}\mathbf{P}$ and $\mathbf{y} = L^{\frac{1}{2}}\mathbf{P}$ are the same. For the output measurement $\mathbf{y} = \mathcal{B}^\mathsf{T}\mathbf{P}$ we have $G^*G = F^\mathsf{T}(s^*I - A)^{-\mathsf{T}}\mathcal{B}\mathcal{B}^\mathsf{T}(sI - A)^{-1}F = F^\mathsf{T}(s^*I - A)^{-\mathsf{T}}L(sI - A)^{-1}F$. As system $\mathcal{H}_\infty$ norm is a function of the spectrum of G^*G, identical results will be obtained as if one used $\mathbf{y} = L^{\frac{1}{2}}\mathbf{P}$ instead of $\mathbf{y} = \mathcal{B}^\mathsf{T}\mathbf{P}$. Hence, it is sufficient to find the system $\mathcal{H}_\infty$ norm of (7) from disturbances to $\mathbf{y} = L^{\frac{1}{2}}\mathbf{P}$. Let $\Lambda = V^\mathsf{T}LV$ be the eigendecomposition of L, where V may be taken to be orthogonal. Consider the invertible change of states $\tilde{\boldsymbol{x}} = (V^\mathsf{T}\boldsymbol{x}, V^\mathsf{T}\dot{\boldsymbol{x}})$. Then, a straightforward computation shows that

$$\begin{aligned}\dot{\tilde{\boldsymbol{x}}} &= \begin{bmatrix}0 & I_n\\ -k_p\Lambda & -k_u\Lambda\end{bmatrix}\tilde{\boldsymbol{x}} + \begin{bmatrix}0\\ V^\mathsf{T}\end{bmatrix}w\\ y &= \begin{bmatrix}L^{\frac{1}{2}}V & 0\end{bmatrix}\tilde{\boldsymbol{x}}.\end{aligned} \quad (9)$$

The model (9) has the same transfer function as (7), and hence the same system norm. Now consider an input/output transformation on (9), where $\bar{y} = V^\mathsf{T}y$ and $\bar{w} = V^\mathsf{T}w$, knowing the fact that such input/output transformation preserves the system $\mathcal{H}_\infty$ norm [33]. Hence, the transformed system

$$\begin{aligned}\dot{\tilde{\boldsymbol{x}}} &= \begin{bmatrix}0 & I_n\\ -k_p\Lambda & -k_u\Lambda\end{bmatrix}\tilde{\boldsymbol{x}} + \begin{bmatrix}0\\ \underbrace{V^\mathsf{T}V}_{=I_n}\end{bmatrix}\bar{w}\\ \bar{y} &= \underbrace{\begin{bmatrix}V^\mathsf{T}L^{\frac{1}{2}}V & 0\end{bmatrix}}_{=\begin{bmatrix}\Lambda^{\frac{1}{2}} & 0\end{bmatrix}}\tilde{\boldsymbol{x}}\end{aligned} \quad (10)$$

has the same system norm as (9). The system (10) is comprised of n decoupled subsystems, each of the form

$$\begin{aligned}\dot{\tilde{\boldsymbol{x}}}_i &= \begin{bmatrix}0 & 1\\ -k_p\lambda_i & -k_u\lambda_i\end{bmatrix}\tilde{\boldsymbol{x}}_i + \begin{bmatrix}0\\ 1\end{bmatrix}\bar{w}_i\\ \bar{y}_i &= \begin{bmatrix}\lambda_i^{\frac{1}{2}} & 0\end{bmatrix}\tilde{\boldsymbol{x}}_i,\end{aligned} \quad (11)$$

with transfer functions

$$\tilde{G}_i(s) = \frac{\lambda_i^{\frac{1}{2}}}{s^2 + k_u\lambda_i s + k_p\lambda_i}, \qquad i \in \{1, \dots, n\},$$

which gives $\tilde{G}_1(s) = 0$. For $i \in \{2, \dots, n\}$, we have

$$|\tilde{G}_i(j\omega)|^2 = \tilde{G}_i(-j\omega)\tilde{G}_i(j\omega) = \frac{\lambda_i}{\underbrace{(k_p\lambda_i - \omega^2)^2 + k_u^2\lambda_i^2\omega^2}_{f(\omega)}}.$$

[1] It can also be a model of a failure or intrusion in inter-vehicular communication.

Maximizing $|\tilde{G}_i(j\omega)|^2$ with respect to ω is equivalent to minimizing $f(\omega)$. By setting $\frac{df(\omega)}{d\omega} = 0$ we get $\bar{\omega}_1 = 0$ and $\bar{\omega}_2 = (k_p\lambda_i - \frac{1}{2}k_u^2\lambda_i^2)^{\frac{1}{2}}$ as critical points. Here $\bar{\omega}_2$ is the global minimizer of $f(\omega)$, unless $\frac{k_u^2\lambda_i}{2k_p} > 1$. Substituting these critical values back into the formula for $|\tilde{G}_i(j\omega)|^2$, we find for $i \in \{2, \ldots, n\}$ that

$$||\tilde{G}_i||_\infty = \begin{cases} \dfrac{2}{k_u\lambda_i\sqrt{4k_p - k_u^2\lambda_i}}, & \text{if } \dfrac{\lambda_i k_u^2}{2k_p} \le 1, \\ \dfrac{1}{k_p\lambda_i^{\frac{1}{2}}} & \text{otherwise.} \end{cases} \quad (12)$$

Since $0 < \lambda_2 \le \lambda_3 \le \cdots \le \lambda_n$ and $||\tilde{G}_i||_\infty$ is a monotonically decreasing function of λ_i, the result follows. ■

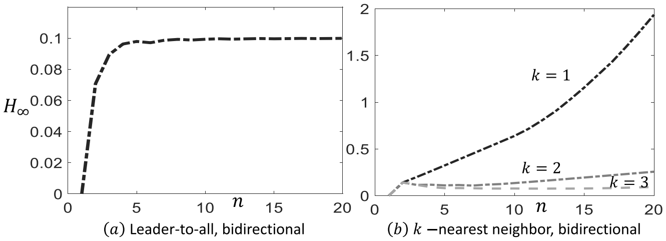
In leader-tracking situations, in addition to keeping safe distance from neighbor vehicles, each vehicle should follow the speed $\dot{p}_1(t)$ of the leading vehicle in the platoon, which is unaffected by the other vehicles. Hence, the graph Laplacian matrix L in (7) must be replaced by the grounded Laplacian matrix L_g in which the row and the column corresponding to the leader is removed. This matrix is positive definite [34] and the resulting $\mathcal{H}_\infty$ norm (13) turns out to be

$$||G||_\infty = \begin{cases} \dfrac{2}{k_u\lambda_1(L_g)\sqrt{4k_p - k_u^2\lambda_1(L_g)}}, & \text{if } \dfrac{\lambda_1(L_g)k_u^2}{2k_p} \le 1, \\ \dfrac{1}{k_p\lambda_1(L_g)^{\frac{1}{2}}} & \text{otherwise.} \end{cases} \quad (13)$$

The smallest eigenvalue of the grounded Laplacian matrix is an indicator of how well-connected the leader is to the rest of the network [9]. It is shown that $\lambda_1(L_g) \le \frac{d_\ell}{n-1}$, where d_ℓ is the degree of the leader vehicle. Similar to $\lambda_2(L)$, the eigenvalue $\lambda_1(L_g)$ is an increasing function of edge addition, i.e. it increases by increasing the network connectivity. The upper bound is attained for the leader-to-all platoon.

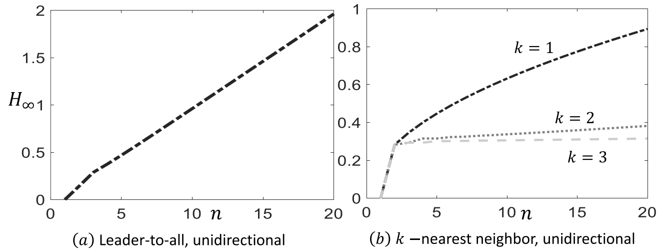
Discussion of the Results: Based on the graph-theoretic bounds presented in (5), undirected nearest neighbor platoon topologies ($k = 1$) do not perform well in disturbance rejection. However, as the network connectivity increases, e.g., k-nearest neighbor platoons for $k > 1$, the $\mathcal{H}_\infty$ norm decreases and the system becomes more robust. In Fig. 3 (a) the $\mathcal{H}_\infty$ norm for leader-to-all topology is shown and in Fig. 3 (b) the system norms for 1 and 2-nearest neighbor platoon are depicted (for $k_p = 5$ and $k_u = 10$). Based on these simulations, the leader-to-all topology is more robust than k-nearest neighbor, because each vehicle is directly connected to the leader and uses the information from the leader directly. This is what we expect to see based on Remark 1 which indicated that the leader-to-all topology has a larger algebraic connectivity compared to the k-nearest neighbor topology.

As mentioned before, for platoons with directed communications a closed form expression for $\mathcal{H}_\infty$ norms does not exist. Fig. 4 shows the positive impact of the network connectivity on the robustness of the platoon with directed communications. As shown in Fig. 4(a), the $\mathcal{H}_\infty$ norm of the leader-to-all topology with directed communication is larger than the nearest neighbor ($k = 1$), Fig. 4(b). This is because, unlike bidirectional communications, increasing the connectivity of directed communications does not always increase the robustness. This phenomenon was observed for the first time in [35], which also gives conditions under which increasing the connectivity in directed networks yields increased robustness.



(a) Leader-to-all, bidirectional (b) k −nearest neighbor, bidirectional

Fig. 3. $\mathcal{H}_\infty$ norms of platoons with bidirectional links: (a) leader-to-all topology and (b) k-nearest neighbor topology.



(a) Leader-to-all, unidirectional (b) k −nearest neighbor, unidirectional

Fig. 4. $\mathcal{H}_\infty$ norms of platoons with directed links: (a) leader-to-all topology and (b) k-nearest neighbor topology.

Remark 2 (Convergence Rate): The network topology also has a direct impact on the convergence rate of the distributed algorithms. In particular, for the control policy (7), the convergence rate is determined by the eigenvalue of A with the largest real part (i.e., smallest in magnitude). It can be easily shown that this eigenvalue is a function of the algebraic connectivity, i.e., $\lambda_2(L)$ [36]. Hence, our results on the influence of platoon topology on $\lambda_2(L)$ can be readily applied to the convergence rate of the distributed control algorithm. □

B. Resilient Distributed Calculation

In distributed calculation, each agent (here vehicle) in the network tries to retrieve (unavailable) quantities of all other agents via incomplete local measurements and cooperation with nearby agents. It has applications to multi-agent robotics and vehicular networks, specifically in fault detection [37].

The quantity that each vehicle tries to calculate from all other vehicles in the network can be a kinematic state (e.g., speed of other vehicles) or some spatial parameter, (e.g., road condition). For vehicle υ_j, this quantity is denoted by the scalar state $x_j[0]$. The objective is to enable any vehicle υ_i (which is not necessarily a neighbor of υ_j) to calculate this value. To do this, vehicle υ_i follows an updating rule (using its own and its neighbors' states) as

$$x_i[k+1] = w_{ii}x_i[k] + \sum_{j \in \mathcal{N}_i} w_{ij}x_j[k], \quad (14)$$

where $w_{ii}, w_{ij} > 0$ are some communication weights. Along with (14), v_i has direct access to its own state and those of its neighbors, i.e.,

$$y_i[k] = \mathcal{C}_i \boldsymbol{x}[k]. \tag{15}$$

Here, $\mathcal{C}_i$ is a $(d_i + 1) \times n$ matrix with a single 1 in each row that denotes the elements of the state $\boldsymbol{x}[k]$ available to v_i (i.e., positions correspond to vehicles that are neighbors of v_i, along with vehicle v_i itself). Let us now consider the faulty case when some vehicles fail to communicate with their neighbors in the prescribed way, i.e., they do not follow dynamics (14) to update their value. These faults are modeled by additive terms in the updating rule. Specifically, at some time step k, vehicle v_i updates its state different from (14) and adds an arbitrary value $\phi_i[k]$ to its updating policy. Hence, (14) becomes

$$x_i[k+1] = w_{ii} x_i[k] + \sum_{j \in \mathcal{N}_i} w_{ij} x_j[k] + \phi_i[k]. \tag{16}$$

If there are f of those faulty vehicles, for some $f \in \mathbb{N}$, the update (16) takes the following vector form

$$\boldsymbol{x}[k+1] = \mathcal{W}\boldsymbol{x}[k] + \underbrace{[\mathbf{e}_{i1} \quad \mathbf{e}_{i2} \quad \ldots \quad \mathbf{e}_{if}]}_{\mathcal{A}} \boldsymbol{\phi}[k], \tag{17}$$

where $\boldsymbol{x} = (x_1, \ldots, x_n)^{\mathsf{T}}$, $\mathcal{W} \in \mathbb{R}^{n \times n}$ is the matrix of communication weights w_{ij}, and $\boldsymbol{\phi}[k] = [\phi_1[k], \phi_2[k], \ldots, \phi_f[k]]^{\mathsf{T}}$. Here, $\mathbf{e}_i$ is the ith unit vector of the canonical basis. However, as the j-th faulty vehicle is not necessarily the j-th vehicle in the network, we use $\mathbf{e}_{ij}$ to denote its vector in $\mathcal{A}$. The exact number and the arrangement of faulty vehicles in the network is unknown to all vehicles (hence, matrix $\mathcal{A}$ is unknown). However, each vehicle knows an upper bound f for the number of faulty vehicles.

The following theorem provides a condition which ensures each vehicle to calculate the true quantity $x_j[0]$ of all other vehicles in the network, despite of the presence of a limited number of faulty vehicles. The algorithm design procedure is known in the literature and omitted here. See [38] for details.

Theorem 3 ([38]): Let $\mathcal{G}$ be a network and let f denote the maximum number of faulty vehicles. Then, regardless of the actions of the faulty vehicles, v_i can determine all of the initial values of linear iterative strategy (17) for almost[2] any choice of weights in the matrix $\mathcal{W}$ if $\mathcal{G}$ is at least $(2f+1)$-vertex connected. □

Discussion of the Results: Based on the above theorem, in case of a single failure, the platoon must be at least 3-connected to be able to perform the distributed calculation properly. Such a level of connectivity can not be found in nearest neighbor topologies and leader-to-all topologies. However, via using k-nearest neighbor platoons, one can perform the distributed calculation despite the existence of up to $\lfloor \frac{k-1}{2} \rfloor$ faulty vehicles. For the k-nearest neighbor platoon on a ring, as the connectivity is twice of the k-nearest neighbor on a line, one can perform the distributed calculation despite the existence of up to k faulty vehicles.

C. Resilient Distributed Consensus

In distributed consensus, vehicles try to reach to an agreement on a value, e.g., velocity or some spatio-temporal parameter, e.g., the road condition. Similar to distributed calculation algorithm, we expect the distributed consensus to operate reliably despite the existence of some fault or an adversarial action. The adversary's objective is usually to deviate the steady-state value from the consensus. With this in mind, the objective of the resilient consensus algorithm is to filter out the extreme values generated by adversaries such that the states of the vehicles remain in a safe region, i.e., inside the convex hull of initial conditions. We denote the state of vehicle v_i by $x_i[k]$. To yield this goal, an iteration policy, called Mean-Subsequence-Reduced (MSR) [11], is proposed. The details of MSR algorithm are discussed below.

MSR Algorithm: At each time step, every node knows an upper bound of the number of faulty vehicles, $f \in \mathbb{N}$, and ignores the largest and smallest f values in its neighborhood ($2f$ in total) and updates its state to be a weighted average of the remaining values. More formally, this yields

$$x_j[k+1] = w_{jj} x_j[k] + \sum_{p \in \mathcal{N}_j[k]} w_{jp} x_p[k], \tag{18}$$

where $\mathcal{N}_j[k]$ is the set of vehicles which are the neighbors of vehicle j and are not ignored at time step k.

In particular, if there exist f faulty vehicles, the dynamics is similar to (14), except the following two additional restrictions on matrix $\mathcal{W}$:

- $w_{jp} > 0, \qquad \forall v_p \in \mathcal{N}_j[k] \cup \{v_j\}, v_j \in \mathcal{V}$,
- $\sum_{p \in \mathcal{N}_j[k] \cup \{v_j\}} w_{jp} = 1, \quad \forall v_j \in \mathcal{V}$.

Denoting the maximum and minimum values of the normal vehicles at time-step k as $M[k]$ and $m[k]$, respectively, we have the following definition.

Definition 1 (f-Local Safe): The MSR algorithm is f-local safe if the states of all normal (not-faulty) nodes are always in the range $\big[m[0], M[0]\big]$ despite the actions of f faulty (or adversarial) nodes. □

Compared to the distributed calculation discussed in Section IV-B, distributed consensus requires *r-robustness* which a stronger notion of network connectivity as discussed in Section II. The following theorem provides necessary and sufficient conditions for MSR algorithm (18) to be f-local safe despite of the actions of faulty vehicles in the network.

Theorem 4: The MSR algorithm is f-local safe if the network $\mathcal{G}$ is $(2f+1)$-robust. Furthermore, for any $f > 0$, there exists a $2f$-robust network which fails to reach consensus using the MSR algorithm with parameter $2f$. □

Remark 3 Distributed Calculation vs. Distributed Consensus: In the distributed calculation algorithm discussed in Sect. IV-B, the objective is to find the initial state of all vehicles in the platoon. These initial conditions can be used to calculate the exact consensus (average) value. However, the algorithm is combinatorial and hard to solve in general. The resilient distributed consensus provides a simpler and computationally efficient algorithm to reach to agreement. However, the cost to be payed is that the exact average value

[2] The *almost* in Theorem 3 is due to the fact that the set of parameters for which the system is not observable has Lebesgue measure zero [39].

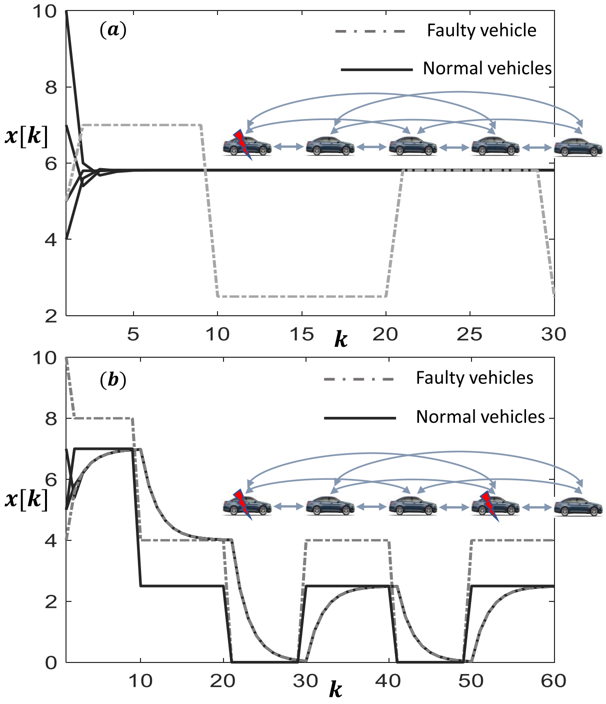


Fig. 5. A 3-nearest neighbor platoon of five vehicles with one faulty vehicle, plot (a), and two faulty vehicles, plot (b). The value of $x[k]$ here is the speed of each vehicle.

may not be reached and the consensus value is only guaranteed to be in the convex hull of initial conditions. □

Discussion of the Results: According to Theorem 4, the platoon must be at least 3-robust in order to tolerate a single faulty vehicle in distributed consensus. Such a level of robustness does not exists in nearest neighbor and leader-to-all topologies. However, for k-nearest neighbor platoons (for both line and ring topologies) the network structure allows us to perform the distributed consensus, even if there are up to $\lfloor \frac{k-1}{2} \rfloor$ faulty vehicles. A simulation example is shown in Fig. 5, where a platoon of 5 vehicles is trying to reach a distributed consensus on the velocity. The platoon is connected according to a 3-nearest neighbor topology. In Fig. 5(a) there is only a single faulty vehicle. The normal (non-faulty) vehicles can calculate the consensus velocity despite the existence of the faulty vehicle. For the same topology, when we increase the number of faulty vehicles to 2 (Fig. 5(b)), the vehicles can no longer calculate the consensus value correctly.

D. Anomaly Detection

Let $x_i[k]$ be the state of each vehicle which is used in a certain distributed algorithm, e.g., distributed calculation or consensus discussed in the previous sections. As discussed before, the attack or fault is modeled as an additive term to the updating rule of each vehicle. Note that we consider attacks in the application layer in this study. Attacks in the network layer require considering probabilistic packet losses. The objective of anomaly detection is to detect faults or attacks applied to some distributed algorithm. In order to detect the attacks, a centralized detector works using sensor measurements. There are few vehicles which are equipped with some sensors dedicated to detect anomalies.[3] We assume that centralized detector observes sensor measurements $\boldsymbol{y}[k]$ and is aware of matrices $\mathcal{W}$ in (17) and the output matrix C which is a binary matrix with single 1 in its i-th column if state x_i is measured. However, the detector is unaware of $\mathcal{A}$ in (17), i.e., the attacker's strategy. The detector uses the following linear filter [12]

$$\begin{aligned}\hat{\boldsymbol{x}}[k+1] &= (\mathcal{W} - KC\mathcal{W})\hat{\boldsymbol{x}}[k] + K\boldsymbol{y}[k+1],\\ z[k] &= \boldsymbol{y}[k] - C\mathcal{W}\hat{\boldsymbol{x}}[k-1],\end{aligned} \tag{19}$$

where $z[k]$ is called the residue. The gain K is designed such that $\mathcal{W} - KC\mathcal{W}$ is Schur stable. This residue signal is an indicator of an anomaly in the system. If the residues under normal operation and during an attack are the same, then an attack is called *perfect*. In this case, the centralized detector can not distinguish an attack from normal operation. In the coming result, we provide an algebraic interpretation of perfect attacks.

Definition 2: The generic normal rank of the matrix pencil

$$\boldsymbol{P}(z) = \begin{bmatrix} A - z\mathbf{I}_n & B_F \\ C & \mathbf{0} \end{bmatrix},$$

is the maximum rank of the matrix over all choices of free (nonzero) parameters in (A, B_F, C) and $z \in \mathbb{C}$. □

It is shown in that for a set of f attacked nodes, a perfect attack is equivalent to having rank$\boldsymbol{P}(z) < n + f$ [40]. The following result characterizes the generic normal rank of $\boldsymbol{P}(z)$ in terms of the graph $\mathcal{G}$.

Theorem 5 ([12], [41]): The generic normal rank of the matrix pencil $\boldsymbol{P}(z)$ is equal to $n + r$, where r is the size of the largest linking in $\mathcal{G}$ from the attacked nodes (vehicles) to the nodes with sensors. □

Theorem 5 implies that to prevent perfect attacks, parameter r has to be equal to the number of attacks f. Due to the fact that the attacked set is not known to the detector, there must be an f-linking from the set of vehicles with dedicated sensors to any other set of size f in the network. This is equivalent to have an f-connected graph. This fact is formally stated below.

Corollary 1: If the underlying graph is f-connected, then the linear filter (19) can detect any set of f attacks on the vehicle platoon.

Discussion of the Results: Consider a k-nearest neighbor platoon with bidirectional communications. As the graph is k-connected, by placing sensors on any set of k vehicles in the network, there exists a linking of size k from any set of attacked vehicles to the sensors. Thus, any set of k attacks can be detected. Now consider k-nearest neighbor platoon with directed communications. This graph is no longer k-connected. However, by placing sensors on the last k vehicles in the platoon, as shown in Fig. 6 (bottom), there exists a linking of size k which connects any set of attacked vehicles to the sensors, i.e., any combination of k attacks can be detected.

[3] They are different from sensors used for the state estimation, i.e. (15).

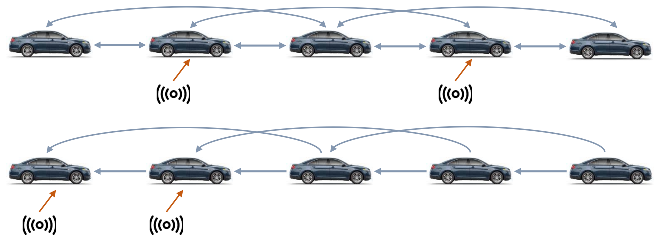


Fig. 6. Sensor placement on bidirectional (top) and directed (bottom) 2-nearest neighbor platoons for attach detection.

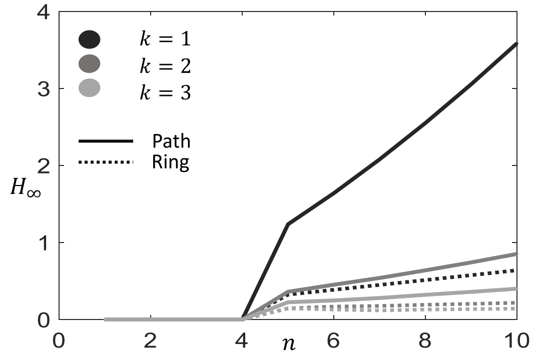


Fig. 7. $\mathcal{H}_\infty$ norm for bidirectional ring and line topologies.

V. Simulations

In this section, we present additional simulations to validate the theoretical results in the paper. In particular, we show how different platoon topologies exhibit different levels of resilience against adversaries.

According to Table I, k-nearest neighbor ring topology has a larger algebraic connectivity compared to k-nearest neighbor topology. Thus, it is expected that the k-nearest neighbor platoon on a ring shows a better $\mathcal{H}_\infty$ performance in formation control algorithms. Fig. 7 shows the $\mathcal{H}_\infty$ norm for k-nearest neighbor ring and line topologies with bidirectional communication and for different values of k. The feedback gains used are $k_p = 15$ and $k_u = 20$. According to this figure, by increasing the connectivity, k, the system $\mathcal{H}_\infty$ norm decreases, i.e., the platoon becomes more robust to disturbances. Moreover, since the ring topology has larger algebraic connectivity, it exhibits a better $\mathcal{H}_\infty$ performance, compared to the line.

Remark 4 (Considerations in Using Ring Topologies): In many experimental tests it is claimed that platoons on a ring can represent an approximation of line platoons. However, from the above observations we conclude that the $\mathcal{H}_\infty$ performance of the ring topology is an over-estimation of that of the line topology. Hence, extending the results on the $\mathcal{H}_\infty$ performance from the platoons on a ring to platoons on a line requires further subtleties. □

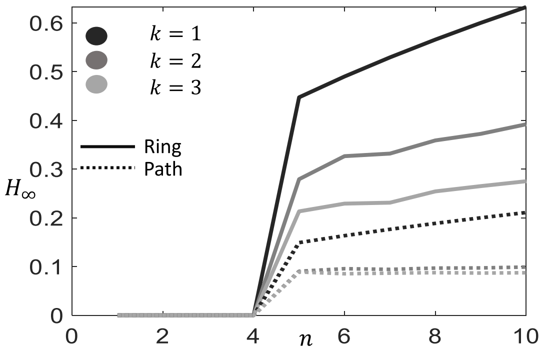


Fig. 8. $\mathcal{H}_\infty$ norm for unidirectional ring and line topologies.

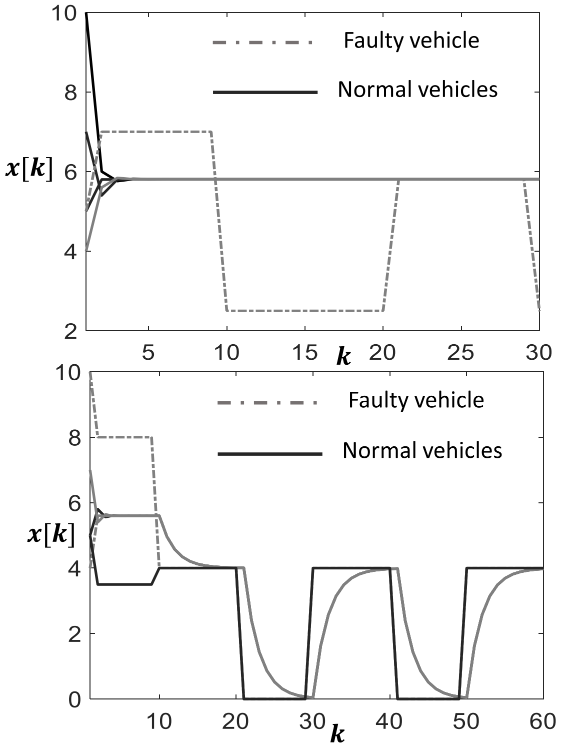


Fig. 9. State trajectories of a 3-nearest neighbor platoon on a ring with a single faulty vehicle (top) and two faulty vehicles (bottom).

Fig. 8 shows the $\mathcal{H}_\infty$ performance of the formation control on unidirectional k-nearest neighbor ring and line platoons. An important observation is that, unlike bidirectional topologies, the unidirectional line topology exhibits smaller $\mathcal{H}_\infty$ norm, i.e., better performance, compared to the ring topology. The above observation confirms the theoretical result in [35] in which directed cycles deteriorate the $\mathcal{H}_\infty$ performance in consensus dynamics. Physically, this phenomenon is explained by the fact that a disturbance can circulate continuously along directed cycles which results in its propagation in the network, while in a directed line this phenomenon does not happen.

Next simulations show the resilience of the consensus dynamics on ring topology. As shown in Fig. 9, the resilience of a 3-nearest neighbor platoon on a ring is similar to that of the line topology, i.e., Fig. 5. This supports the results of Table I, showing that despite the ring topology has a larger vertex connectivity and algebraic connectivity compared to the line topology, they have identical network robustness. Hence, a takeaway message is that ring and line topologies show the same levels of resilience to attacks in distributed consensus.

VI. Conclusion

This paper presented a comprehensive study on the impact of platoon topologies on the resilience of classes of distributed algorithms. We studied connectivity measures of various platoon topologies and showed how these measures affect the ability of distributed algorithms to reject communication disturbances, to detect cyber-attacks, and to be resilient against them. We showed that traditional platoon topologies relying on interaction with the nearest neighbor are very fragile with respect to performance and security criteria. We analyzed the ability of k-nearest neighbor platoons to fulfill desired security and performance levels. The framework we studied covers undirected and directed topologies, ungrounded and grounded topologies, line and ring topologies. We also discussed the trade-off in the network design between the robustness to disturbances and the resilience to adversarial actions.

Most of the graph-theoretic conditions discussed in this paper to overcome faulty vehicles in distributed algorithms demand higher network connectivity. However, in real-world ad-hoc networks, it is desired the topology to be sparse, with low connectivity. Modifying the distributed algorithms mentioned in the paper to be resilient against failures on sparse networks is therefore a relevant future research line.

Most results in the paper are independent on the vehicle model and on the control strategy since they are based on connectivity measures. The exception is the $\mathcal{H}_\infty$ control part. With respect to the vehicle model, we notice that the analysis done for second-order vehicle dynamics is amenable to higher-order vehicle models. For instance, we can treat the third-order vehicle model (a double integrator with a first order filter representing the driveline dynamics) as a perturbed version of the double integrator. The rationale is that the driveline time constant is in practice uncertain. By doing this, the proposed $\mathcal{H}_\infty$ performance can be intended as robustness to uncertain driveline dynamics. With respect to control strategies, we notice that the use of a linear control law allow us to derive an analytic form of the robustness bounds. The use of alternative control laws proposed in the literature, e.g. model predictive control (MPC), sliding mode or adaptive control, will usually require to evaluate such robustness bounds numerically, rather than analytically. Therefore, extensions of our robustness bounds to other control algorithms, specifically decentralized MPC [42], is another relevant future direction.

References

[1] M. Pirani, E. Hashemi, J. W. Simpson-Porco, B. Fidan, and A. Khajepour, "Graph theoretic approach to the robustness of K-nearest neighbor vehicle platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 3218–3224, Nov. 2017.

[2] V. Turri, B. Besselink, and K. H. Johansson, "Cooperative look-ahead control for fuel-efficient and safe heavy-duty vehicle platooning," *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 1, pp. 12–28, Jan. 2017.

[3] K. Liang, J. Mårtensson, and K. H. Johansson, "Heavy-duty vehicle platoon formation for fuel efficiency," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1051–1061, Apr. 2016.

[4] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commum. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[5] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security vulnerabilities of IEEE 802.11p and visible light communication based platoon," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–4.

[6] F. Acciani, P. Frasca, A. Stoorvogel, E. Semsar-Kazerooni, and G. Heijenk, "Cooperative adaptive cruise control over unreliable networks: An observer-based approach to increase robustness to packet loss," in *Proc. Eur. Control Conf. (ECC)*, Jun. 2018, pp. 1399–1404.

[7] V. S. Dolk, J. Ploeg, and W. P. M. H. Heemels, "Event-triggered control for string-stable vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 12, pp. 3486–3500, Dec. 2017.

[8] K. Fitch and N. E. Leonard, "Information centrality and optimal leader selection in noisy networks," in *Proc. 52nd IEEE Conf. Decis. Control*, Dec. 2013, pp. 7510–7515.

[9] M. Pirani, E. Moradi Shahrivar, B. Fidan, and S. Sundaram, "Robustness of leader–follower networked dynamical systems," 2016, *arXiv:1604.08651*.

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

[11] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, Apr. 2013.

[12] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[13] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation and consensus using linear iterative strategies," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 4, pp. 650–660, May 2008.

[14] Y. Zheng, S. E. Li, J. Wang, D. Cao, and K. Li, "Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 1, pp. 14–26, Jan. 2016.

[15] S. Öncü, J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Network-aware analysis of string stability," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1527–1537, Feb. 2014.

[16] H. Hao, P. Barooah, and J. J. P. Veerman, "Effect of network structure on the stability margin of large vehicle formation with distributed control," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Dec. 2010, pp. 4783–4788.

[17] H. Xing, J. Ploeg, and H. Nijmeijer, "Compensation of communication delays in a cooperative ACC system," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1177–1189, Feb. 2020.

[18] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Trans. Cybern.*, early access, May 25, 2021, doi: 10.1109/TCYB.2021.3074318.

[19] A. Petrillo, A. Pescapé, and S. Santini, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Trans. Cybern.*, early access, May 25, 2021.

[20] M. Pirani, E. Hashemi, B. Fidan, J. W. Simpson-Porco, H. Sandberg, and K. H. Johansson, "Resilient estimation and control on K-nearest neighbor platoons: A network-theoretic approach," in *Proc. IFAC Workshop Distrib. Estimation Control Netw. Syst.*, 2018, pp. 22–27.

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

[22] D. B. West, *Introduction to Graph Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.

[23] E. Moradi Shahrivar, M. Pirani, and S. Sundaram, "Spectral and structural properties of random interdependent networks," *Automatica*, vol. 83, pp. 234–242, Sep. 2017.

[24] F. Chung, *Spectral Graph Theory*. Providence, RI, USA: American Mathematical Society, 1997.

[25] L. Guerrero-Bonilla, A. Prorok, and V. Kumar, "Formations for resilient robot teams," *IEEE Robot. Autom. Lett.*, vol. 2, no. 2, pp. 841–848, Apr. 2017.

[26] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 3, pp. 310–320, Sep. 2015.

[27] M. Penrose, *Random Geometric Graphs*. Oxford, U.K.: Oxford Univ. Press, 2003.

[28] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak Math. J.*, vol. 23, no. 2, pp. 298–305, 1973.

[29] S. Cui, B. Seibold, R. Stern, and D. B. Work, "Stabilizing traffic flow via a single autonomous vehicle: Possibilities and limitations," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1336–1341.

[30] V. Giammarino, S. Baldi, P. Frasca, and M. L. D. Monache, "Traffic flow on a ring with a single autonomous vehicle: An interconnected stability perspective," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 4998–5008, Aug. 2021.

[31] J. Usevitch and D. Panagou, "r-robustness and (r, s)-robustness of circulant graphs," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Dec. 2017, pp. 4416–4421.

[32] I. Herman, D. Martinec, Z. Hurák, and M. Šebek, "Nonzero bound on Fiedler eigenvalue causes exponential growth of H-infinity norm of vehicular platoon," *IEEE Trans. Autom. Control*, vol. 60, no. 8, pp. 2248–2253, Aug. 2015.

[33] M. Pirani, J. W. Simpson-Porco, and B. Fidan, "System-theoretic performance metrics for low-inertia stability of power networks," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Dec. 2017, pp. 5106–5111.

[34] M. Pirani and S. Sundaram, "On the smallest eigenvalue of grounded Laplacian matrices," 2014, *arXiv:1406.2271*.

[35] M. Pirani, H. Sandberg, and K. H. Johansson, "A graph-theoretic approach to the H_∞ performance of leader–follower consensus on directed networks," *IEEE Control Syst. Lett.*, vol. 3, no. 4, pp. 954–959, Oct. 2019.

[36] W. Yu, G. Chen, and M. Cao, "Some necessary and sufficient conditions for second-order consensus in multi-agent dynamical systems," *Automatica*, vol. 46, no. 6, pp. 1089–1095, 2010.

[37] M. Pirani *et al.*, "Cooperative vehicle speed fault diagnosis and correction," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 783–789, Feb. 2018.

[38] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

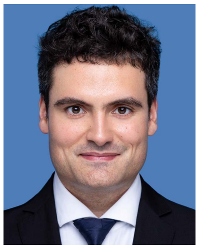
[39] K. Reinschke, *Multivariable Control: A Graph-Theoretic Approach*. New York, NY, USA: Springer-Verlag, 1987.

[40] H. Cam, P. Mouallem, Y. Mo, B. Sinopoli, and B. Nkrumah, "Modeling impact of attacks, recovery, and attackability conditions for situational awareness," in *Proc. IEEE Int. Inter-Disciplinary Conf. Cognit. Methods Situation Awareness Decis. Support (CogSIMA)*, Mar. 2014, pp. 181–187.

[41] J. W. van der Woude, "A graph-theoretic characterization for the rank of the transfer matrix of a structured system," *Math. Control, Signals Syst.*, vol. 4, no. 1, pp. 33–40, Mar. 1991.

[42] Y. Zheng, S. E. Li, K. Li, F. Borrelli, and J. K. Hedrick, "Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies," *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 3, pp. 899–910, Mar. 2017.

Mohammad Pirani received the B.Sc. degree in mechanical engineering from the Amirkabir University of Technology in 2011 and the M.A.Sc. degree in electrical and computer engineering and the Ph.D. degree in mechanical and mechatronics engineering from the University of Waterloo in 2014 and 2017, respectively. He is currently a Research Assistant Professor with the Department of Mechanical and Mechatronics Engineering, University of Waterloo. Before that, he held post-doctoral researcher positions at the KTH Royal Institute of Technology, Sweden, from 2018 to 2019, and the University of Toronto from 2019 to 2021. His research interests include resilient and fault-tolerant control, networked control systems, and multi-agent systems.



Simone Baldi (Senior Member, IEEE) received the B.Sc. degree in electrical engineering and the M.Sc. and Ph.D. degrees in automatic control engineering from the University of Florence, Italy, in 2005, 2007, and 2011, respectively. He is currently a Professor at Southeast University. He has a guest position at the Delft Center for Systems and Control, TU Delft, where he was an Assistant Professor. His research interests include adaptive and learning systems with applications in networked systems and intelligent vehicles. He was awarded the Outstanding Reviewer of *Applied Energy* in 2016 and *Automatica* in 2017. He is a Subject Editor of the *International Journal of Adaptive Control and Signal Processing* and an Associate Editor of IEEE CONTROL SYSTEMS LETTERS.

Karl Henrik Johansson (Fellow, IEEE) received the M.Sc. and Ph.D. degrees from Lund University. He has held visiting positions at UC Berkeley, Caltech, NTU, HKUST Institute of Advanced Studies, and NTNU. He is currently the Director of the Stockholm Strategic Research Area ICT The Next Generation and a Professor at the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology. His research interests are in networked control systems, cyber-physical systems, and applications in transportation, energy, and automation. He is a member of the IEEE Control Systems Society Board of Governors, the IFAC Executive Board, and the European Control Association Council. He has received several best paper awards and other distinctions. He is a fellow of the Royal Swedish Academy of Engineering Sciences. He has been awarded a Distinguished Professor with the Swedish Research Council and a Wallenberg Scholar. He has received the Future Research Leader Award from the Swedish Foundation for Strategic Research and the Triennial Young Author Prize from IFAC. He is a IEEE Distinguished Lecturer.