Transmissibility-Based Health Monitoring of the Future Connected Autonomous Vehicles Networks

Abdelrahman Khalil, Mohammad Al Janaideh, Khaled F. Aljanaideh, and Deepa Kundur

***Abstract*—Transmissibility is a mathematical model that relates a subset of a system's outputs to another subset of outputs of the same system without knowledge of the external excitation or the dynamics of the system. This study investigates fault detection, localization, and mitigation of connected autonomous vehicles (CAV) platoons using transmissibility operators. A CAV platoon is a network of connected autonomous vehicles that communicate together to move in a specific path with the desired velocity. Failure in a physical component of a vehicle, or failure in the form of an internal delay, a cyber-attack, or a communication time-delay affects the safety and security of the CAV platoons. In this paper, we use measurements from sensors available in CAV platoons to identify transmissibility operators, which are used for health monitoring, fault localization, and fault mitigation in the platoon. We first consider the case of vehicle-to-cloud communication (V2C) to monitor the platoon's health. Then, we assume that the platoon loses communication with the cloud, and we monitor the health of the platoon based on vehicle-to-vehicle (V2V) communication. We apply the proposed technique to a model of the platoon obtained using the bond graph approach, and an experimental setup consisting of three connected autonomous robots.**

***Index Terms*—Connected autonomous vehicles, fault detection, fault mitigation, transmissibility.**

I. Introduction

CONNECTED autonomous vehicles (CAV) platoons represent a new technology where a network of vehicles communicates together using wireless communication to achieve the desired speed and position of the vehicles in the network.

This new technology represents an emerging cyber-physical system (networking, computation, and physical processes) with significant potential to enhance traffic safety, ease congestion, and positively impact the environment through autonomous platoon control, see for example [1]–[3]. The cyber component of such a system incorporates the vehicle-to-vehicle (V2V) and vehicle-to-cloud (V2C) communication networks [4], while the physical component includes physical vehicle dynamics and human-driver responses. Within CAV, communication networks enable opportunities for greater situational awareness, collaborative decision-making, and improved control [5].

It is evident that as the technology and complexity of connected autonomous vehicles evolve, several grand research challenges need to be addressed. These include securing the connected autonomous vehicles from malicious cyberattacks that can affect the actuators and sensors in the CAV platoon, see for example [6], [7]. Other sources of failures include cyber-physical attacks, faults in sensors and actuators, and unknown nonlinear dynamics in the CAV [8].

Connected autonomous vehicles faults can lead to catastrophic losses [9]–[11]. The presence of cyberattacks can lead to faulty sensor measurements, faulty control signals, or delayed control signals that appear as cyber-physical attacks on actuators [6]. Moreover, disturbances can occur in the communication between two vehicles, as in [8]. Furthermore, each system is subjected to system jamming, that is, time delay in one or more of the cyber-physical components of the system [7], [12]. Time delay affects V2V communication and can lead to instability in the control system [7]. Time delay requires a high management level in a way that presents no significant effect on platoon string stability [13]. Therefore, there is a critical need to provide fault mitigation for different uncertainties that may affect the dynamics of the CAV. Since the CAV may include different uncertainties, then it is essential, from a practical point of view, for the fault mitigation technique to be able to perform under unknown dynamics of the CAV.

Developments in cyberattacks, however, require a new comprehensive methodology to mitigate these attacks [14]. In this paper, we use transmissibility operators, which are mathematical models that relate a sensor response to another sensor response in the same system to detect, localize, and mitigate faults in the CAV network. Transmissibility operators can detect faults in sensors or systems without the need to know the excitation signal or a model of the underlying system [15]–[17]. The input and output of transmissibility are referred to as *pseudo input* and *pseudo output*. Transmissibilities identified under healthy conditions can be used along with the pseudo input, to obtain a prediction of the pseudo output of the transmissibility. This predicted output can be used instead of the actual output from the sensor if the sensor has become faulty. Transmissibility-based fault detection was used for health monitoring of aircraft sensors [17], acoustic systems [15], and structural health monitoring [18]. This paper is the first to present a comprehensive transmissibility-based approach for fault detection, localization,

Manuscript received March 5, 2021; revised June 14, 2021 and October 25, 2021; accepted December 19, 2021. Date of publication February 14, 2022; date of current version May 2, 2022. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and in part by Quanser, Markham, ON, Canada. The review of this article was coordinated by Dr. Ricardo Pinto de Castro. *(Corresponding author: Mohammad Al Janaideh.)*

Abdelrahman Khalil and Mohammad Al Janaideh are with the Department of Mechanical Engineering, Memorial University, St. John's, NL A1B 3R5, Canada (e-mail: amkhalil@mun.ca; maljanaideh@mun.ca).

Khaled F. Aljanaideh is with the Department of Aeronautical Engineering, Jordan University of Science and Technology, Irbid 22110, Jordan (e-mail: kfaljanaideh@just.edu.jo).

Deepa Kundur is with The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: dkundur@ece.utoronto.ca).

Digital Object Identifier 10.1109/TVT.2022.3151326

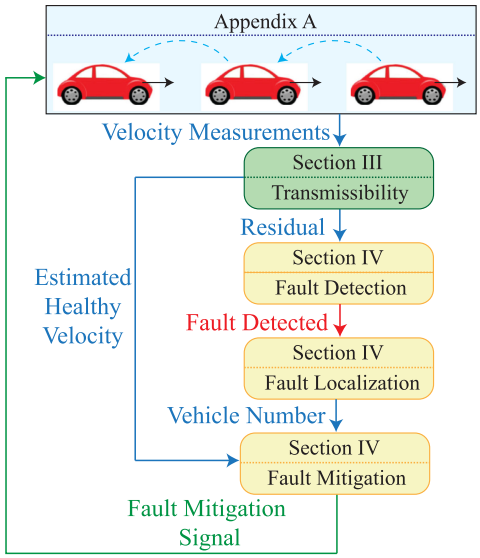


Fig. 1. Flow chart of the architecture of the paper. Only velocity measurements are used along with the transmissibility operators to obtain estimations of the healthy velocities. The discrepancy between the measured and estimated velocities are considered as faults indicators, and then the estimated velocity is used to mitigate faults. Fig. 3 presents the proposed approach in more details.

and mitigation in CAV platoons. We consider time-domain models of transmissibilities, where the differentiation operator $\mathbf{p} \triangleq \frac{\mathrm{d}}{\mathrm{d}t}$ is used to account for nonzero initial conditions [19]. Transmissibility operators can be unstable, noncausal, and of unknown order [15]. Thus, we use noncausal FIR models to identify transmissibilities [20]. These models can be used to represent systems that are unstable, noncausal, and of unknown order.

We consider two architectures of the platoon communications, namely, V2C and V2V communications. In the V2C communication architecture, each vehicle communicates with one preceding and one succeeding vehicle in addition to the cloud communication. In this case, transmissibilities and their related computations are stored in the cloud, while no computations are performed on the vehicle's level. In the V2V communication architecture, each vehicle communicates with two preceding and two succeeding vehicles while no cloud communication is considered. In this case, each vehicle is considered to have the transmissiblity operators between the vehicle itself and the vehicles that it communicates with stored in the vehicle's computer. Moreover, each vehicle is considered to perform its own computations.

We first consider the bond graph approach to simulate a set of platoons that operate with different conditions that can be hard to implement on an experimental setup. The bond graph approach, which is described in more detail in [21], uses energy and power propagation to model complex systems that consist of several electromechanical components. Then, we consider an experimental setup of a platoon consisting of three autonomous robots.

In this paper, we present a class of dynamic faults in CAV platoons, these faults include physical faults such as motor disturbances [22] and internal motor delay [23], along with cyber faults such as burst transmission [24] and denial-of-service [7]. A flow chart of the architecture of the paper is shown in Fig. 1. As shown in Fig. 1, the platoon dynamics produce velocity measurements from the vehicles, which are used for transmissibility identification (Section III). Then the identified transmissibilities are used for fault detection (Section V-A). After a fault is detected, the location of the fault is determined (Section V-B) and the fault is then mitigated (Section V-C). Section VI applies the proposed fault detection, localization, and mitigation algorithms to the platoon. Moreover, Sections VII and VIII apply the proposed fault detection, localization, and mitigation algorithms to the experimental setup for V2V and V2C communications, respectively.

A description of the gaps that this paper fills with respect to the state-of-the-art methods are discussed in Section II-B. The main contributions of this work are:

- We introduce an algorithm that uses output-only measurements available from CAV platoons sensors for fault detection, localization, and mitigation without the knowledge of the dynamics of the CAV platoons or the inputs that excite them.
- The proposed algorithm is applied to detect faults in CAV platoons including failures in vehicles' physical components, internal delay, excessive noise (disturbance), cyberattacks, and communication time delay.
- The proposed algorithm is applied to mitigate faults in CAV platoons including excessive noise (disturbance), cyberattacks, and communication time delay.
- The proposed algorithm is applied to a model of multiple CAV platoons obtained using the bond graph approach and an experimental setup of a CAV platoon with 3 mobile robots.

II. Related Work

A. Literature Review

Several studies have proposed fault detection and mitigation techniques for a class of faults and cyber-attacks to enhance the traffic safety of CAV. Observer-based fault detection and mitigation is the most common method used in the literature to monitor the health of CAV platoons [25]–[31]. Observer-based techniques require using a model of the platoon and the excitation signal acting on the platoon to estimate the vehicle states. The estimated states are then compared to the measured states obtained from the vehicles for fault detection. Accurate state estimation, which is required to obtain the fault detection residual or to implement observer-based control strategies, can be affected by several sources that excite the platoon such as road irregularities and platoon disturbances. A voting technique based on observer-based methods were used in [31]–[33]. A fault detection, localization, and mitigation algorithm for attacked GPS systems in CAV platoons was introduced in [34]. Two detectors were used to localize the faulty vehicle and then a local state observer was used on each vehicle to mitigate the attacked GPS system.

A fault detection algorithm for cyber-attacks that destabilize CAV platoons was considered in [35]. However, this algorithm cannot detect faults in the vehicles that can lead to malicious consequences on the network while maintaining the string stability. In [36], an adaptive control algorithm was used to secure a platoon that consists of both human-driven vehicles and autonomous vehicles without using a fault detection algorithm. An adaptive fault-tolerant control algorithm is used in [37] for

a class of CAV platoons with actuator faults based on spacing distance policies. This control scheme was developed by employing radial basis function neural networks and PID-type sliding mode control. An online identification algorithm was used to obtain a fault signature matrix in [11]. This algorithm uses active excitation of the system to obtain a fault detection residual, which can be explored to identify specific system faults. Real-time observers designed using sliding mode and adaptive estimation theory were used to detect denial-of-service cyber-attacks [38]. Distance and velocity controllers were used to avoid collisions and to guarantee string stability under communication delay in [39]. In [24], an algorithm that is based on a distributed function calculation was used to detect faults in the platoon's V2V communications between the two preceding and two succeeding vehicles.

A novel secure adaptive cooperative control approach was introduced in [31] to track the leading vehicle under the presence of security vulnerabilities. The leading vehicle information is assumed to be always available and precise. In fact, it is assumed in [31] that the first vehicle cannot be faulty. This dependency on the leading vehicle to secure CAV platoons highlights two matters. The first matter is in the fact that the first vehicle of the platoon is subject to different faults like any other vehicle in the platoon. And the second matter is the limited range of the V2V communication links, which makes the communication with more than two following vehicles not feasible. Moreover, the platoon dynamics are considered to be known.

Several other methods of fault detection and mitigation of CAV platoons considered using Kalman filtering [40] and particle filtering [41]. These filters represent a form of analytical redundancy that estimates vehicle kinematics and compares it with the measured kinematics. These model-based methods require knowledge of the vehicles' kinematic model and the excitation signal acting on the CAV platoon.

B. Contributions

The study of the recent literature highlighted several gaps that this paper aims to fill. These gaps include requiring knowledge of the dynamics of the platoon and the excitation signal, assuming that the leader vehicle is always healthy, requiring more than one detector for fault detection, and designing the fault detection algorithm to deal with specific types of fault or one communication topology.

The proposed approach does not require knowledge of the platoon dynamics or the excitation signal and does not assume that the leading vehicle in the platoon is always healthy. The proposed approach can also deal with a wide range of faults. This includes, but is not limited to, faults in the physical layer of the platoon (i.e. motor disturbances), faults that destabilize the platoon dynamics (i.e. motor internal delay), faults within the cyber layer of the platoon (i.e. burst transmission and denial-of-service), and any fault that changes the behavior of the platoon not necessarily leading to destabilizing the platoon dynamics. The proposed technique is also flexible with different communication topologies. Two different communication topologies are considered, and the proposed technique is shown to detect different classes of faults within the considered communication topologies. Furthermore, only one detector is used to detect, localize, and mitigate different classes of faults.

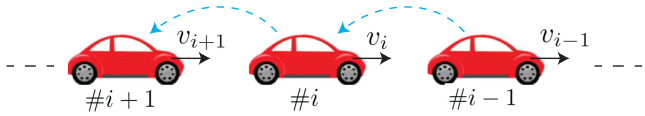


Fig. 2. Illustration of platoon portion with V2V communications.

Moreover, this work introduces developments in the transmissibility theory. Transmissibility operators are applied for systems with bounded nonlinearities, and the obtained transmissibility operators then are independent on the system nonlinearities. This allows us to simulate systems with unknown nonlinearities using linear models without linearizing the system or use multilinear models. Furthermore, the transmissibility-based health monitoring in this work is formulated to overcome the external disturbances by considering them as independent excitations on the system.

III. Transmissibility Identification of CAV

Transmissibility operators are mathematical objects that characterize the relationship between outputs of an underlying system. In this section, we introduce transmissibility operators for CAV platoons with an algorithm to identify them.

A. CAV Transmissibility Operators

Consider the platoon shown in Fig. 2 that is described by the following state space model

$$\dot{x}(t) = Ax(t) + B_v v_1^*(t) + B_f f(t,x) + B_w w(t), \quad (1)$$

$$v(t) = Cx(t) + \Delta(t), \quad (2)$$

where $A \in \mathbb{R}^{\mathfrak{n}\times\mathfrak{n}}$ is Hurwitz, $B_v \in \mathbb{R}^{\mathfrak{n}\times(m-2)}$, $B_f \in \mathbb{R}^{\mathfrak{n}\times 1}$ $B_w \in \mathbb{R}^{\mathfrak{n}\times 1}$, $C \in \mathbb{R}^{n\times\mathfrak{n}}$, $\mathfrak{n}$ is the model order, $n \geq 2$ is the number of vehicles, m is the number of independent excitations (inputs) on the system, $f(\cdot,\cdot)$ and w are bounded unknown unmodeled dynamics and bounded unknown excitations, respectively, $v(t) = [v_1(t) \quad \dots \quad v_n(t)]^{\mathrm{T}}$, $\Delta(t)$ is the measurements noise, for $i = 1,\dots,n$, v_i is the velocity of the ith vehicle. Then, define

$$v_{\mathrm{i},0}(t) \triangleq C_{\mathrm{i}} x(t) \in \mathbb{R}^p, \quad (3)$$

$$v_{\mathrm{o},0}(t) \triangleq C_{\mathrm{o}} x(t) \in \mathbb{R}^{n-p}, \quad (4)$$

to be two independent sets of noise-free velocity outputs, where p is the number of independent pseudo inputs, $C_{\mathrm{i}} \in \mathbb{R}^{p\times\mathfrak{n}}$, and $C_{\mathrm{o}} \in \mathbb{R}^{(n-p)\times\mathfrak{n}}$. Then the transmissibility whose pseudo input is $v_{\mathrm{i},0}$ and whose pseudo output is $v_{\mathrm{o},0}$, satisfies [42]

$$v_{\mathrm{o},0}(t) = \mathcal{T}(\mathbf{p}) v_{\mathrm{i},0}(t), \quad (5)$$

where

$$\mathcal{T}(\mathbf{p}) \triangleq \Gamma_{\mathrm{o}}(\mathbf{p})\Gamma_{\mathrm{i}}^{-1}(\mathbf{p}), \quad (6)$$

$$\Gamma_{\mathrm{i}}(\mathbf{p}) \triangleq C_{\mathrm{i}}\mathrm{adj}(\mathbf{p}I - A)B \in \mathbb{R}^{p\times p}[\mathbf{p}], \quad (7)$$

$$\Gamma_{\mathrm{o}}(\mathbf{p}) \triangleq C_{\mathrm{o}}\mathrm{adj}(\mathbf{p}I - A)B \in \mathbb{R}^{(n-p)\times p}[\mathbf{p}], \quad (8)$$

where $B = [\,B_v \;\; B_f \;\; B_w\,]$, $\mathbf{p} \triangleq \frac{\mathbf{d}}{\mathbf{d}t}$ is the differentiation operator, and $\mathrm{adj}\,\Gamma_{\mathrm{i}}$ denotes the adjugate matrix of Γ_{i}. The definition of B considers the signals v_1^*, f, and w as independent excitations. Then the transmissibility operator $\mathcal{T}$ is independent of

the platoon desired velocity v_1^*, the unmodeled dynamics $f(\cdot,\cdot)$, and the external disturbances w. Since sensor measurements are obtained in discrete time, we consider discrete-time transmissibility operators in the forward-shift operator $\mathbf{q}$, that is, we replace $\mathbf{p}$ in (6) by the forward shift operator $\mathbf{q}$ [43].

B. Identification of Transmissibilities

Replacing $\mathbf{p}$ in (5) with $\mathbf{q}$ yields, for all $k \geq 0$,

$$v_{\mathrm{o},0}(k) = \mathcal{T}(\mathbf{q}) v_{\mathrm{i},0}(k), \tag{9}$$

where

$$\mathcal{T}(\mathbf{q}) = \Gamma_{\mathrm{o}}(\mathbf{q})\Gamma_{\mathrm{i}}^{-1}(\mathbf{q}) \tag{10}$$

$$= \frac{1}{\det \Gamma_{\mathrm{i}}(\mathbf{q})} \Gamma_{\mathrm{o}}(\mathbf{q}) \mathrm{adj}\Gamma_{\mathrm{i}}(\mathbf{q}). \tag{11}$$

Note that if Γ_{i} has a nonminimum phase (unstable) zero, then $\mathcal{T}$ is unstable. Also, if Γ_{o} has more zeros than Γ_{i}, then $\mathcal{T}$ is noncausal. Moreover, transmissibilities are identified using the output measurements only with no information about the dynamics of the system, and thus, the order of the transmissibility is unknown. Therefore, to identify transmissibilities, we need to consider a model structure that can approximate noncausal and unstable transmissibilities with unknown order. In this paper, we consider noncausal FIR models, which are truncations of the Laurent expansion in an analytic annulus that contains the unit circle [20]. A noncausal FIR model of $\mathcal{T}$ is given by

$$\mathcal{T}(\mathbf{q}, \Theta_{r,d}^{\mathrm{FIR}}) = \sum_{i=-d}^{r} H_i \mathbf{q}^{-i}, \tag{12}$$

where r, d denote the order of the causal and noncausal parts of the FIR model of $\mathcal{T}$, respectively, $H_i \in \mathbb{R}^{(n-p)\times p}$ is the i-th coefficient of the Laurent expansion of $\mathcal{T}$ in the annulus that contains the unit circle, and $\Theta_{r,d}^{\mathrm{FIR}} \triangleq [H_{-d}, \ldots, H_r] \in \mathbb{R}^{(n-p)\times p(r+d+1)}$.

Next, let v_{i} and v_{o} denote measurements of $v_{\mathrm{i},0}$ and $v_{\mathrm{o},0}$ that are corrupted by sensor noise, process noise, or model uncertainties. Then, the least squares estimate $\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}$ of $\Theta_{r,d}^{\mathrm{FIR}}$ is given by

$$\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}} = \Psi_{v_{\mathrm{o}},\ell} \Phi_{r,d,\ell}^{\mathrm{T}} (\Phi_{r,d,\ell}^{\mathrm{T}} \Phi_{r,d,\ell})^{-1}, \tag{13}$$

where ℓ is the number of samples,

$$\Psi_{v_{\mathrm{o}},\ell} \triangleq \begin{bmatrix} v_{\mathrm{o}}(r) & \cdots & v_{\mathrm{o}}(\ell - d) \end{bmatrix}, \tag{14}$$

$$\Phi_{r,d,\ell} \triangleq \begin{bmatrix} \phi_{r,d}(r) & \cdots & \phi_{r,d}(\ell - d) \end{bmatrix}, \tag{15}$$

$$\phi_{r,d}(k) \triangleq \begin{bmatrix} v_{\mathrm{i}}(k+d)^{\mathrm{T}} & \cdots & v_{\mathrm{i}}(k-r)^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}}, \tag{16}$$

$\Psi_{v_{\mathrm{o}},\ell} \in \mathbb{R}^{(n-p)\times(\ell-r-d+1)}$, $\Phi_{r,d,\ell} \in \mathbb{R}^{(p(r+d+1))\times(\ell-r-d+1)}$, and $\phi_{r,d} \in \mathbb{R}^{p(r+d+1)\times 1}$. The residual of the identified transmissibility obtained using least squares with a noncausal FIR model at time k is defined by

$$e(k|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}) \triangleq v_{\mathrm{o}}(k) - \hat{v}_{\mathrm{o}}(k|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}), \tag{17}$$

where

$$\hat{v}_{\mathrm{o}}(k|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}) \triangleq \mathcal{T}(\mathbf{q}, \hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}) v_{\mathrm{i}}(k)$$

$$= \sum_{i=-d}^{r} \hat{H}_{i,\ell} v_{\mathrm{i}}(k-i), \tag{18}$$

$$\mathcal{T}(\mathbf{q}, \hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}) \triangleq \sum_{i=-d}^{r} \hat{H}_{i,\ell} \mathbf{q}^{-i}, \tag{19}$$

and $\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}} \triangleq [\hat{H}_{-d,\ell}, \ldots, \hat{H}_{r,\ell}] \in \mathbb{R}^{(n-p)\times p(r+d+1)}$.

The least-squares estimate $\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}$ is estimated from CAV velocities $v_1, \ldots, v_n$ under healthy conditions of the platoon. Next, the identified transmissibility operator $\mathcal{T}(\mathbf{q}, \hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}})$ is used along with measurements of $v_1, \ldots, v_n$ to obtain the predicted velocity $\hat{v}_{\mathrm{o}}(k|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}})$. As sensor measurements are prone to noise, the residuals of the transmissibilities will not be zero or constant but will be varying over a range that depends on the sensor noise. If the platoon faults occur, the level of the residuals will change significantly, which indicates that a fault has occurred. Based on the change in the residual we distinguish the system uncertainties from the system fault and conclude whether the system is healthy or faulty.

IV. CAV Health Monitoring

This section uses the transmissibility operators identified in the previous section for the purpose of fault detection, localization, and mitigation in CAV platoons. The transmissibility residual defined in (17) is used in this section to monitor the platoon health. Platoon faults such as the faults introduced in Appendix B result in the measured corrupted velocity $\tilde{v}_i$. Then the discrepancy between the measured and estimated velocities is implemented in this section as a fault detection indicator. After determining which vehicle is faulty, the faulty velocity is then replaced with the healthy estimated one in order to mitigate the faults. To protect against false alarms due to reasons such as outliers in the measurements, we consider the norm of the residuals (17) over a sliding window of w steps width. That is, for all $k \geq d$, we compute

$$E(k|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}, w) \triangleq \sqrt{\sum_{i=k}^{w+k} \|e(i|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}})\|}. \tag{20}$$

Assume that the system operates in a healthy manner for the first M steps, where $M \geq w + d$, and let η be the signal-to-noise ratio, then the threshold is defined as [44]

$$\mu(\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}, w, M) \triangleq \frac{\eta}{M+1} \sum_{i=d}^{M} E(i|\hat{\Theta}_{r,d,\ell}^{\mathrm{FIR}}, w). \tag{21}$$

To localize the fault we consider identifying multiple transmissibilities along the set of platoons. All transmissibilities that use the faulty velocity as pseudo input/output will result in high level of the norm of residual. For further explanation on how to localize the faulty vehicle, consider a system of m platoons each with n vehicles, then for all $j = 1, \ldots, m-1$, let $\mathcal{T}_j$ denote a transmissibility operator that relates the velocities of the fifth vehicle in each platoon as defined in Table II that considers a set of m platoons. Moreover, $\mathcal{T}_0$ and $\mathcal{T}_m$ are as defined in Table I. Using Algorithm 1 and Table II, the location of the fault can be determined. If $\mathcal{T}_0$ is faulty and $\mathcal{T}_j$ is healthy then platoon j

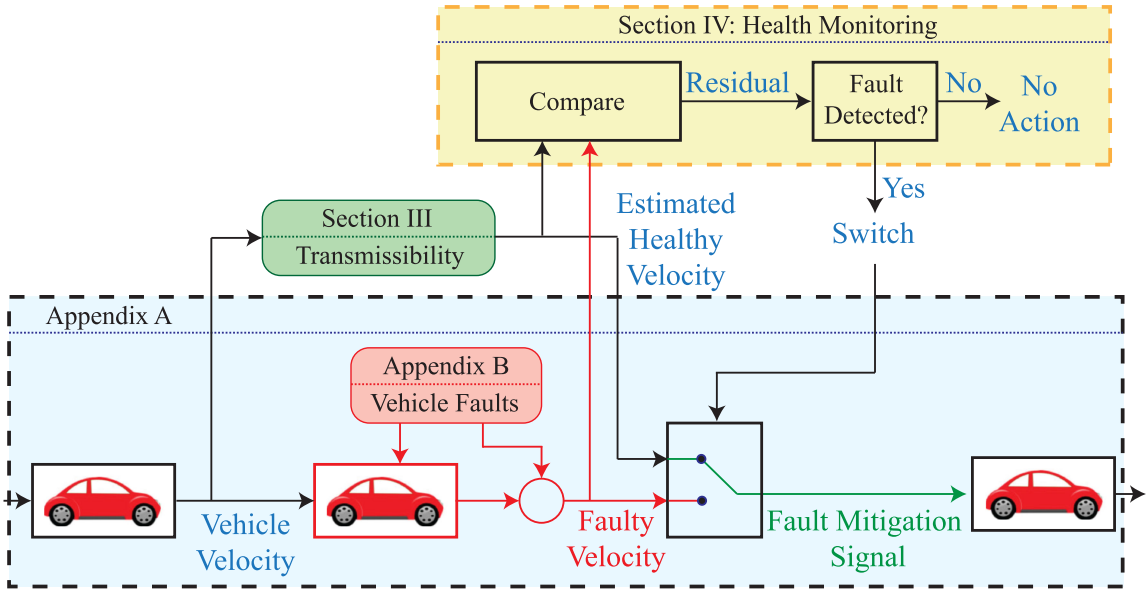


Fig. 3. Block diagram for the proposed transmissibility-based fault mitigation algorithm on a three vehicles platoon portion. The middle vehicle is faulty. The velocity of the front vehicle is used in the transmissibility to obtain the estimated healthy velocity. Then comparing the measured and estimated velocities gives a fault indicator. If the fault is detected, then the measured velocity is replaced with the estimated one to mitigate the faults effect transmitted to the next vehicle.

TABLE I
TRANSMISSIBILITY OPERATORS $\mathcal{T}_0, \ldots, \mathcal{T}_m$ ARE USED TO DETECT AND LOCALIZE THE FAULTY PLATOON IN THE SET OF PLATOONS. NEXT, THE TRANSMISSIBILITY OPERATORS $\mathcal{T}_{\tilde{j}}^i$, WHERE $i = 2, \ldots, 5$ ARE USED TO LOCALIZE THE FAULTY VEHICLE IN THE FAULTY PLATOON $\tilde{j}$. THESE TRANSMISSIBILITIES ARE USED IN ALGORITHM 1

Operator	Pseudo Inputs	Pseudo Output
$\mathcal{T}_0$	$\{v_5^1, v_5^2, \ldots, v_5^{m-1}\}$	v_5^m
$\mathcal{T}_j$	$\{v_5^1, v_5^2, \ldots, v_5^{m-1}\} \setminus \{v_5^j\}$	v_5^m
$\mathcal{T}_m$	$\{v_5^1, v_5^2, \ldots, v_5^{m-2}\}$	v_5^{m-1}
$\mathcal{T}_{\tilde{j}}^i$	$v_{i-1}^{\tilde{j}}$	$v_i^{\tilde{j}}$

TABLE II
PSEUDO INPUTS AND PSEUDO OUTPUTS OF THE TRANSMISSIBILITY OPERATORS $\mathcal{T}_1$ AND $\mathcal{T}_2$ USED FOR FAULT DETECTION AND LOCALIZATION IN THE EXPERIMENTAL SETUP SHOWN IN FIG. 16

Operator	Pseudo Inputs	Pseudo Outputs
$\mathcal{T}_1$	v_1 and v_2	v_3
$\mathcal{T}_2$	v_1	v_2

TABLE III
PSEUDO INPUTS AND PSEUDO OUTPUTS OF THE TRANSMISSIBILITY OPERATORS $\mathcal{T}_1, \mathcal{T}_2$, AND $\mathcal{T}_3$ USED FOR FAULT DETECTION, LOCALIZATION, AND MITIGATION IN THE EXPERIMENT

Operator	Pseudo Inputs	Pseudo Outputs
$\mathcal{T}_1$	v_1	v_2
$\mathcal{T}_2$	v_2	v_3
$\mathcal{T}_3$	v_1	v_3

TABLE IV
PARAMETERS DESCRIPTION AND VALUES FOR THE BOND GRAPH MODEL SHOWN IN FIG. 29

Symbol	Description	Value
R_i	Motor Resistance	$18m\Omega$
I_i	Motor Inductance	$252\mu H$
C_i	Motor Constant	$0.26\text{rad}/s.A$
S_i	Shaft moment of inertia	$0.2kg.m^2$
G_i	Transmission Ratio	0.2
r_i	Wheel Radius	$0.3m$
M_i	Vehicle gross mass	$1478kg$
F_i	Friction coefficient	0.6
$k_{P,i}$	Controller proportional gain	2.5
$k_{I,i}$	Controller integral gain	0.6
α_i	Constant in (A.1)	72.01
β_i	Constant in (A.1)	117.9
γ_i	Constant in (A.1)	46.72
δ_i	Constant in (A.1)	28.03

is faulty. Next, to localize the faulty vehicle, let $\tilde{j}$ denote the number of the faulty platoon, and $\mathcal{T}_{\tilde{j}}^i$ denote the transmissibility from v_{i-1} to v_i in in platoon $\tilde{j}$. If $\mathcal{T}_{\tilde{j}}^i$ is faulty, then vehicle i in platoon $\tilde{j}$ is faulty.

Next, to mitigate faults in vehicle i in platoon $\tilde{j}$, we replace the faulty velocity signal $\tilde{v}_i^{\tilde{j}}$ with the estimated healthy signal obtained from the transmissibility operator $\mathcal{T}_{\tilde{j}}^i$. Note that since $\mathcal{T}_{\tilde{j}}^i$ represents a reflect of vehicle i dynamics, the causal assumption for $\mathcal{T}_{\tilde{j}}^i$ is possible. The correction signal can be obtained for all $k \geq 0$ as

$$v_{i,\text{mit}}(k|\hat{\Theta}_{r,d,\ell}^{\text{FIR}}) \triangleq \begin{cases} v_i(k), & k < \hat{k}, \\ \hat{v}_i(k|\hat{\Theta}_{r,d,\ell}^{\text{FIR}}), & k \geq \hat{k}, \end{cases} \tag{22}$$

where $\hat{k}$ is the time sample at which we start using the fault mitigation algorithm, $\hat{v}_i$ is obtained using the transmissibility operator $\mathcal{T}_{\tilde{j}}^i$ along with v_{i-1}. The correction signal $v_{i,\text{mit}}$ replaces the faulty velocity measurement of vehicle i in platoon $\tilde{j}$ and thus is used as a reference for vehicle $i+1$ as shown in Fig. 3.

Algorithm 1 Fault Localization Algorithm for a Set of m Platoons, Each With n Autonomous Vehicles.

if $\mathcal{T}_0$ is healthy **then**
  All platoons are healthy
else
  if $\mathcal{T}_j$ is healthy, where $j = 1, \ldots, m$, **then**
    Platoon j is Faulty
    Set $\tilde{j} = j$
  end
  if $\mathcal{T}_{\tilde{j}}^i$ is faulty, where $i = 2, \ldots, n$, **then**
    Vehicle i in platoon $\tilde{j}$ is faulty
  else
    Vehicle 1 in platoon $\tilde{j}$ is faulty
  end
end

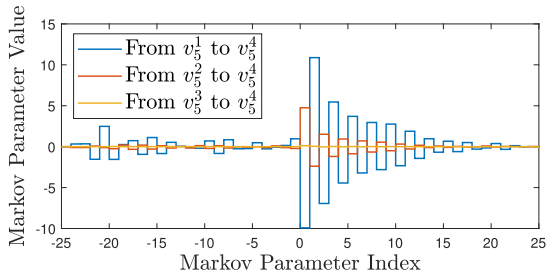


Fig. 4. Estimated Markov parameters from each pseudo input to the pseudo output for the transmissibility operator $\mathcal{T}_0$ defined in Table I. The estimated Markov parameters were obtained using least squares with a noncausal FIR model with $r = 25$ and $d = 25$.

V. Simulation Results

A. CAV Health Monitoring Depending on V2C

Consider four platoons, each with five identical vehicles with the parameters shown in Table IV. We model the platoons using the bond graph approach as shown in Appendix A. To identify the transmissibility operators defined in Table I with $m = 4$ and $n = 5$, we set the desired velocities of the platoons to Gaussian white noise with zero mean and unit variance. Algorithm 1 is then used to detect and localize the fault based on the change in the level of the residuals of the identified transmissibilities.

Fig. 4 shows the estimated Markov parameters of $\mathcal{T}_0$ from each pseudo input to the pseudo output obtained under healthy conditions. Then, the estimated transmissibility $\mathcal{T}_0$ is used with the measurements of v_5^1, v_5^2, and v_5^3 to obtain an estimate of v_5^4. Fig. 5 shows a plot of v_5^4 and the estimate of v_5^4, which are close to each other.

Next, we introduce the motor disturbances, motor delay, burst transmission, and DoS faults to the system separately as introduced in Appendix B. To emulate the motor disturbance fault, a band-limited white noise is added to the motor constant of the third vehicle in the second platoon. To emulate a motor delay, a 1-second delay is introduced to the input current of the motor of the third vehicle in the second platoon. To emulate a burst transmission fault, a band-limited white noise is added to the communication link between the third and the fourth vehicles in the second platoon. Moreover, to emulate communication-link time delay, a time delay of 2 seconds is introduced in the communication link between the third and fourth vehicles in the second platoon. Figs. 6 and 7 show the norm of the residuals of the transmissibility operators defined in Table I, where each fault is introduced separately at $t = 80$ seconds. The threshold limits are obtained by considering a signal-to-noise ratio of 20. Note from Fig. 6 that at $t = 90$ seconds the norm of the residuals of the transmissibility operators $\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_3$, and $\mathcal{T}_4$ increased. Moreover, since the level of the residuals of $\mathcal{T}_2$ in Fig. 6 did not change, then it follows from the Algorithm in 1 that platoon 2 is faulty, and thus $\tilde{j} = 2$. Note that at $t = 90$ seconds the norm of the residuals of the transmissibility operators $\mathcal{T}_2^2$, $\mathcal{T}_2^4$, and $\mathcal{T}_2^5$ did

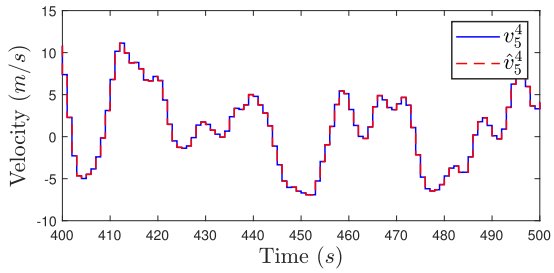


Fig. 5. Simulated output velocity v_5^4 and the predicted output velocity $\hat{v}_5^4$, where the predicted velocity is obtained using the identified transmissibility operator $\mathcal{T}_0$ and the measurements of v_1^5, v_2^5, and v_3^5.

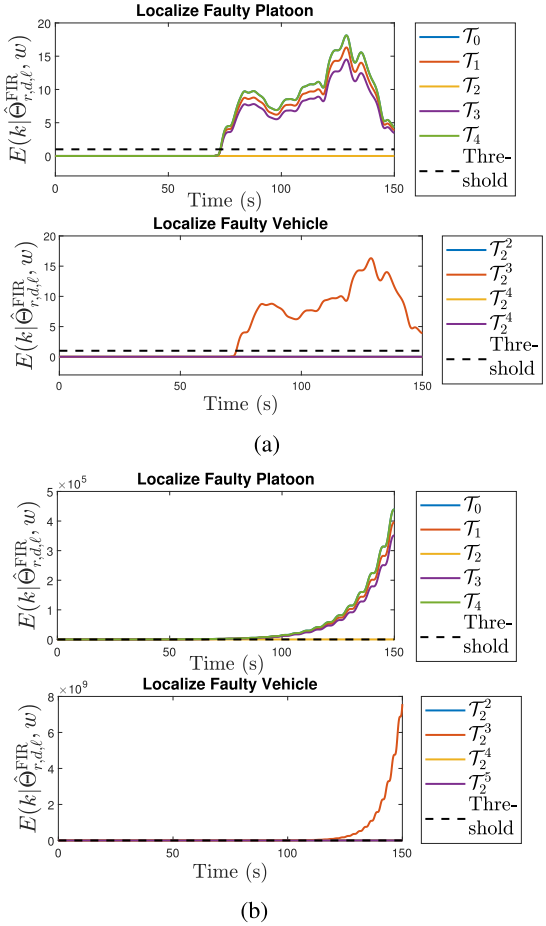


Fig. 6. Norm of the residuals of the transmissibilities $\mathcal{T}_0, \ldots, \mathcal{T}_4$ and $\mathcal{T}_2^2, \ldots, \mathcal{T}_2^5$ computed using. (20) with $w = 100$ steps for (a) Motor disturbances, and (b) Motor delay. We use Algorithm 1 to determine the faulty platoon and faulty vehicle. All faults are introduced separately at approximately $t = 80$ seconds.

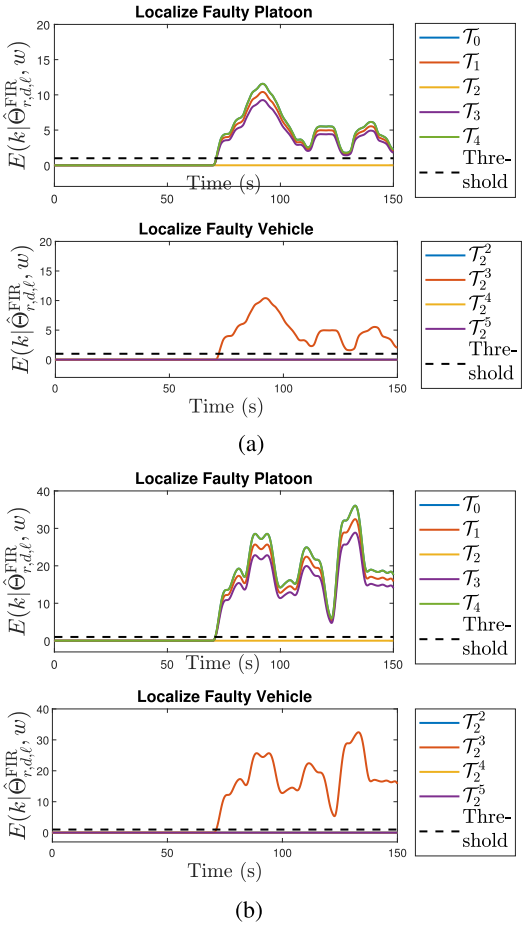


Fig. 7. Norm of the residuals of the transmissibilities $\mathcal{T}_0, \ldots, \mathcal{T}_4$ and $\mathcal{T}_2^2, \ldots, \mathcal{T}_2^5$ computed using (20) with $w = 100$ steps for (a) Burst transmission, and (b) DoS. We use Algorithm 1 to determine the faulty platoon and faulty vehicle. All faults are introduced separately at approximately $t = 80$ seconds.

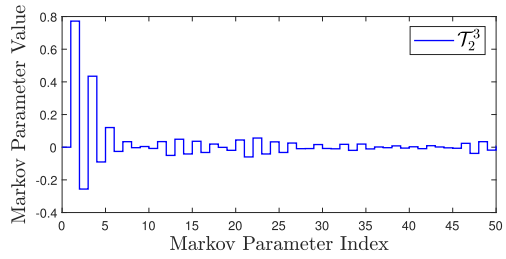


Fig. 8. Estimated Markov parameters for the transmissibility operator $\mathcal{T}_2^3$ obtained using least squares with a noncausal FIR model with $r = 50$ and $d = 0$.

not change, where the norm of residual of the transmissibility operators $\mathcal{T}_2^3$ increased. Therefore, using the Algorithm in 1 we conclude that the third vehicle in the second platoon is faulty. Similar results are shown for the motor delay, cyberattack, and time-delay faults in Figs. 6 and 7.

Next, we use the fault mitigation algorithm shown in Fig. 3 to replace the faulty signal from the faulty vehicle i with a healthy signal that will be used as a reference for the succeeding vehicle $i + 1$. Fig. 8 shows the estimated Markov parameters for the transmissibility operator $\mathcal{T}_2^3$ obtained using least squares with a noncausal FIR model with $r = 50$ and $d = 0$. Fig. 9 shows the velocity v_3^2 and the estimated velocity $\hat{v}_3^2$ obtained using the

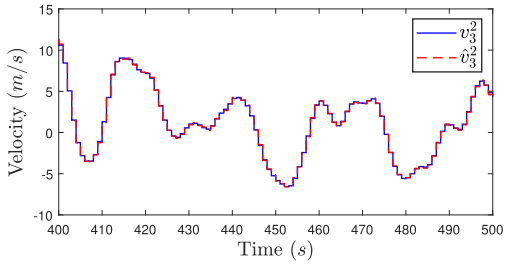


Fig. 9. Simulated output velocity and predicted output velocity of v_3^2, where the predicted velocity is obtained using the identified transmissibility $\mathcal{T}_2^3$ whose Markov parameters are shown in Fig. 8 along with the measurement of v_2^2. The predicted output $\hat{v}_3^2$ is used in the fault mitigation algorithm.

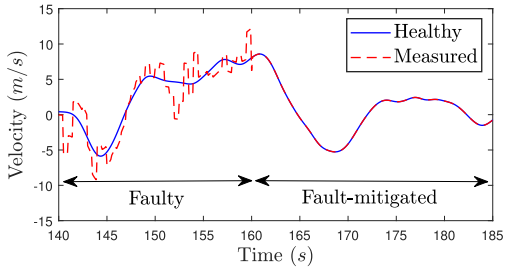


Fig. 10. Plot of the fourth vehicle velocity in the second platoon, v_4^2, before and after applying the fault mitigation algorithm, where the third vehicle in the same platoon is subject to a burst transmission. Note that, after applying the fault mitigation algorithm at $t = 160$, the fourth vehicle in the second platoon starts to operate in a healthy manner again.

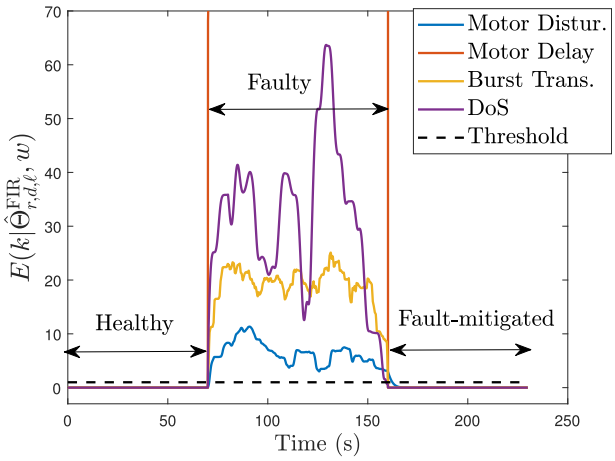


Fig. 11. Norm of the residuals of the transmissibility $\mathcal{T}_0$ introduced in Table I. Note that at approximately $t = 160$ sec, the fault mitigation based on transmissibilities implemented, which leads to a decrease in the norm of residuals for proposed faults.

identified transmissibility $\mathcal{T}_2^3$ along with the measurement of v_2^2. We use the estimate $\hat{v}_3^2$ to obtain the correction signal $v_{3,\text{mit}}$. Fig. 10 shows the fourth vehicle velocity in the second platoon while the third vehicle is subject to a burst transmission. Note from Fig. 10 that after applying the proposed fault mitigation algorithm at time $t = 160$ sec, the fourth vehicle in the second platoon starts to operate in a healthy manner again. The norm of the residual of the identified transmissibility $\mathcal{T}_0$ is shown in

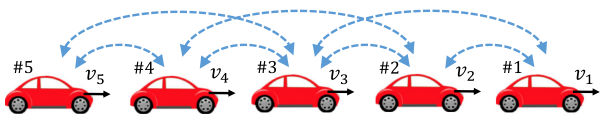


Fig. 12. Connected autonomous vehicles platoon, where each vehicle can communicate with two preceding and two succeeding vehicles.

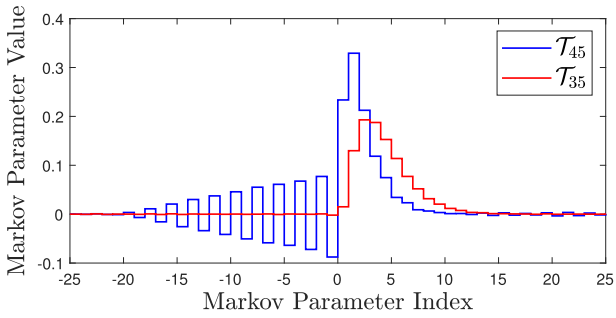


Fig. 13. Estimated Markov parameters of the transmissibilities associated with vehicle 5 in the V2V communication model shown in Fig. 12.

Fig. 11 for the motor disturbances, motor delay, burst transmission, and DoS faults. Note from Fig. 11 that at $t = 160$, the level of the residuals decreased due to utilizing the proposed fault mitigation algorithm.

B. V2V Communication Platoon Health Monitoring

V2V communication topologies have been proposed in the literature to improve the string stability [45]. In this section, we consider the architecture where the platoon loses communication with the cloud. We adopt the platoon communication model introduced in [24]. As shown in Fig. 12, in this model each vehicle within the platoon has a V2V communication with two preceding and two succeeding vehicles in the same platoon. The velocity of each vehicle follows the average of the two preceding vehicles. For fault detection, we consider single-input single-output transmissibilities between vehicles connected to each other via a V2V communication.

Consider a platoon with 5 vehicles. For $i = 1, \ldots, 5$ and $j = 1, \ldots, 5$, where $j \neq i$, let $\mathcal{T}_{ij}$ denote the transmissibility operator from vehicle i to vehicle j in this platoon. Since vehicle 5, for example, is connected to vehicle 3 and vehicle 4 only, then for vehicle 5 we can construct $\mathcal{T}_{35}$ and $\mathcal{T}_{45}$. We set the desired velocity of the platoon to a Gaussian white noise with zero mean and unit variance. Next, we use least squares with a noncausal FIR model with $r = d = 25$ to identify the transmissibilities $\mathcal{T}_{35}$ and $\mathcal{T}_{45}$. Fig. 13 shows the estimated Markov parameters of $\mathcal{T}_{35}$ and $\mathcal{T}_{45}$. Moreover, Fig. 14 shows the velocity v_5 and the predicted velocity $\hat{v}_5$ obtained using the identified transmissibility $\mathcal{T}_{35}$ and the measurement of v_3. Note from Fig. 14 that the true and estimated velocities are close to each other.

Next, we introduce a burst transmission fault between the fourth and fifth vehicles as introduced in Appendix B. Note that this will make both the fourth and fifth vehicles operate in a faulty manner. Fig. 15 shows the norm of the residuals of the transmissibilities defined for the platoon. Note from Fig. 15 that at $t = 80$ seconds, due to the presence of the cyberattack, the level of the residuals of the transmissibility operators $\mathcal{T}_{34}$, $\mathcal{T}_{45}$, $\mathcal{T}_{24}$ and $\mathcal{T}_{35}$ changes, where the levels of the residuals of all other transmissibilities do not change. Since the level of the norm of

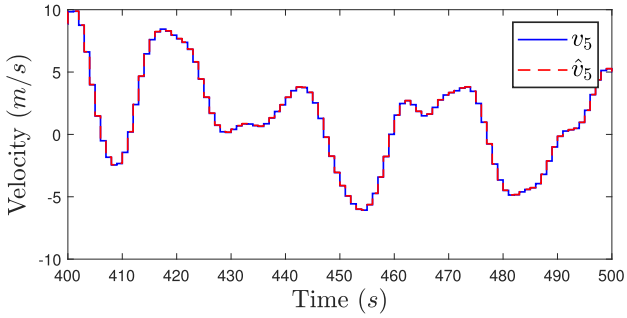


Fig. 14. Velocity v_5 and the predicted velocity $\hat{v}_5$ obtained using the identified transmissibility $\mathcal{T}_{35}$ and the measurement of v_3. Note that v_5 and $\hat{v}_5$ are close to each other.

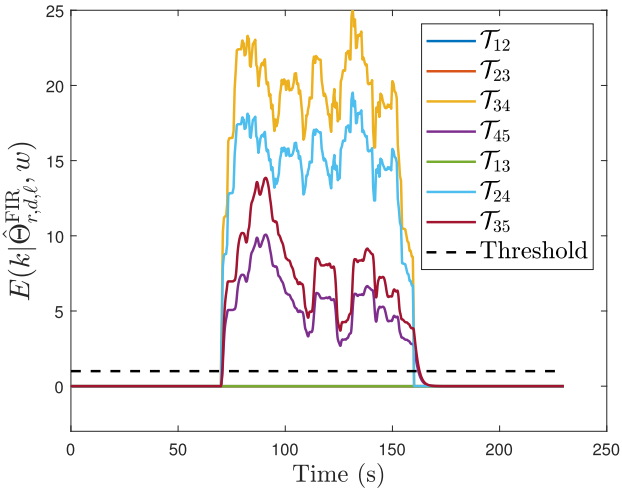


Fig. 15. Norm of the residuals of the transmissibilities $\mathcal{T}_{12}, \mathcal{T}_{23}, \mathcal{T}_{34}, \mathcal{T}_{45}, \mathcal{T}_{13}, \mathcal{T}_{24}$, and $\mathcal{T}_{35}$. Note that after applying the fault mitigation algorithm at $t = 160$ seconds, the norm of residuals of the transmissibilities decreased, which indicates that the platoon started to operate in a healthy manner after applying the fault mitigation algorithm.

residuals of all transmissibilities that are related to the fourth and fifth vehicles has changed, then we conclude from Fig. 15 that both the fourth and fifth vehicles are faulty.

Next, at $t = 160$ seconds we use the fault mitigation algorithm shown in Fig. 3, where vehicle 5 follows the average of v_3 and $v_{4,\mathrm{mit}}$, $v_{4,\mathrm{mit}}$ is computed using (22), and $\hat{v}_4$ is obtained using the identified transmissibility $\mathcal{T}_{34}$ and the measurement of v_3. Fig. 15 shows that at $t = 160$ seconds the norm of the residuals of all transmissibilities decreased, which indicates that the platoon started to operate in a healthy manner again after applying the fault mitigation algorithm.

VI. Experimental Health Monitoring With V2C Communication

We consider the experimental setup shown in Fig. 16 consisting of three autonomous Quanser robots called Qbots. Each Qbot consists of two coaxial wheels, where each wheel is driven by a DC motor. Qbots use closed-loop inverse kinematic controllers to obtain the DC motors commands for both wheels based on the desired linear and rotational velocities of the robot. The difference between the wheels' velocities results in an angular

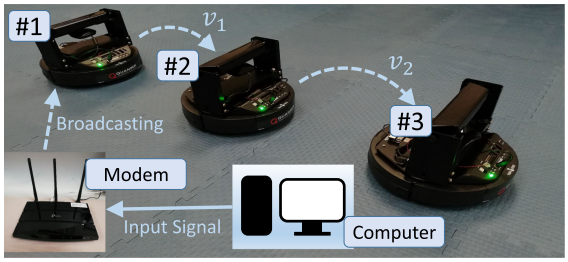


Fig. 16. Experimental setup of V2C communications: Qbot1 receives the desired velocity from the computer while Qbot2, and third Qbot3 receive the desired velocity from the preceding Qbot via V2V communication.

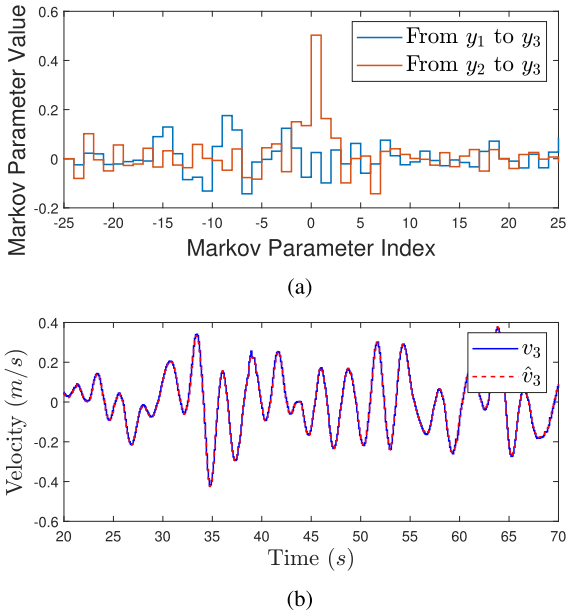


Fig. 17. Experimental results: (a) estimated causal Markov parameters from each pseudo input to the pseudo output for the transmissibility operator $\mathcal{T}_1$ defined in Table II, and (b) measured velocity and predicted velocity of Qbot3, where the predicted velocity is obtained using the identified transmissibility operator $\mathcal{T}_1$ whose parameters are shown in (a) and measurements of v_1 and v_2.

motion of the Qbot. If the desired angular velocity is zero, then both wheels velocities are equal and the Qbot moves forward or backward in a straight line. Qbot1 receives the excitation signal from a computer through wireless communication, and Qbot2 is connected with Qbot1 via a V2V communication channel. Similarly, Qbot3 is connected with Qbot2 via a V2V communication channel.

For health monitoring, we consider a one-dimensional motion for the platoon. We first run the setup by sending a zero-mean, unit variance, Gaussian random excitation signal to Qbot1. All Qbots run and move simultaneously depending only on V2V communications. We use least squares with a noncausal FIR model with $r = 25$ and $d = 25$ to identify the transmissibility operators $\mathcal{T}_1$ and $\mathcal{T}_2$ defined in Table II, where v_1, v_2, and v_3 denote the velocities of Qbot1, Qbot2, and Qbot3, respectively. The estimated Markov parameters of the transmissibility operator $\mathcal{T}_1$ is shown in Fig. 17(a). Moreover, Fig. 17(b) shows the measured velocity v_3 and the predicted velocity $\hat{v}_3$ of Qbot3, where the predicted velocity is obtained using the identified transmissibility and the measured velocities v_1 and v_2. Note that

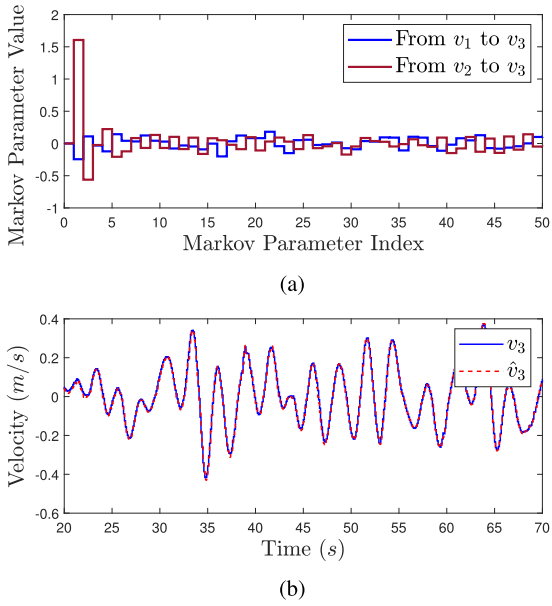


Fig. 18. Experimental results: (a) estimated Markov parameters from each pseudo input to the pseudo output for the transmissibility operator $\mathcal{T}_1$ defined in Table II, and (b) the measured velocity v_3 of Qbot3 and the predicted velocity $\hat{v}_3$ obtained using the identified transmissibility operator $\mathcal{T}_1$ whose parameters are shown in (a) and measurements of v_1 and v_2.

neither the dynamics of the network nor the excitation signal of the network is used to obtain the predicted velocity $\hat{v}_3$ of Qbot3.

Next, we identify causal models of the transmissibility operators defined in Table II to use them for fault mitigation. Fig. 18(a) shows the identified Markov parameters of the estimated transmissibility from each pseudo input to the pseudo output of the transmissibility operator $\mathcal{T}_1$ defined in Table II. Fig. 18(b) shows the measured velocity and the predicted velocity of Qbot3, where the predicted velocity is obtained using the identified transmissibility operator $\mathcal{T}_1$ shown in Fig. 18(a) along with measurements of v_1 and v_2.

A. Disturbance Fault

We consider injecting band-limited white noise in the command signal of the DC-motor that drives the right wheel of Qbot3 as represented in Fig. 19, which results in a physical fault similar to the motor disturbances introduced in Appendix B. This makes the velocities of the wheels in Qbot3 not equal, which results in a 2-D motion of Qbot3 (i.e. a physical fault). Fig. 20 shows the velocity of Qbot3 under healthy and faulty conditions. Fig. 21 shows the norm of residual for the transmissibility operators $E(k|\hat{\Theta}^{\text{FIR}}_{r,d,\ell}, w)$ defined in Table II. Note that at $t = 80$ sec, the norm of the residual of $\mathcal{T}_1$ increases, where the norm of the residual of $\mathcal{T}_2$ remains on the same level. Therefore, we conclude that Qbot3 is faulty. For fault mitigation, we use $\mathcal{T}_2$ and the measurements of v_1 to obtain the correction signal, which is used as a reference for Qbot3. Note from Fig. 21 that after applying the fault mitigation algorithm at approximately $t = 180$ seconds, the norm of residual of $\mathcal{T}_1$ decreased.

B. Internal Time Delay

We emulate the internal mechanical delay by considering a transport time delay in both command signals, which results in

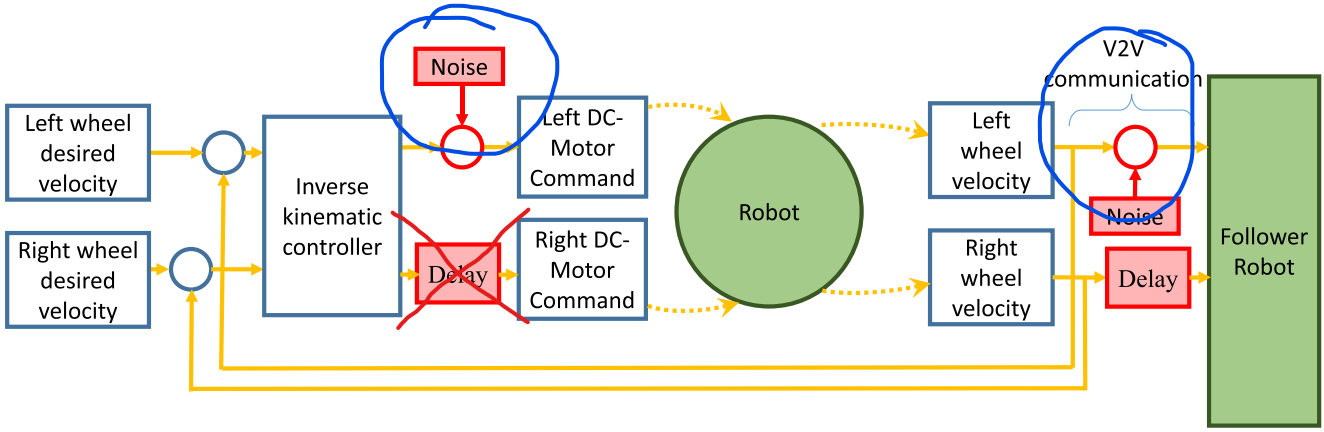


Fig. 19. Experimental emulation of the platoon faults. Four faults are considered separately, as represented by the red blocks. The physical faults include internal disturbances and internal mechanical delay within the closed loop control. The cyber faults are represented by injecting noise and delay to the information packet in the V2V communication link.

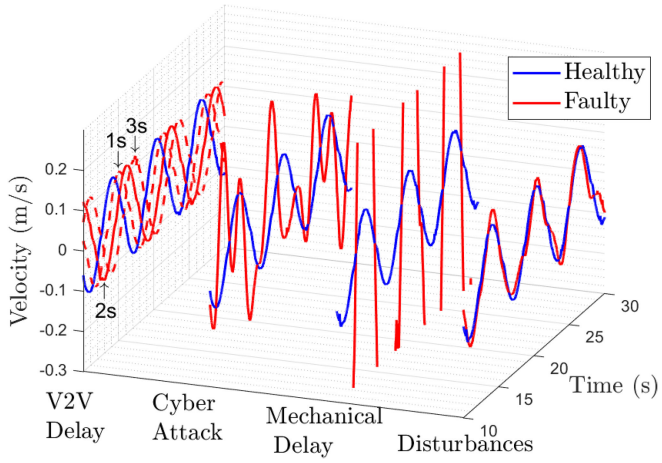


Fig. 20. Experimental results: The velocities of Qbot3 under healthy and faulty conditions, where the proposed faults are injected disturbance, mechanical (internal time) delay, cyberattack, and delay in the V2V communication link between Qbot2 and Qbot3.

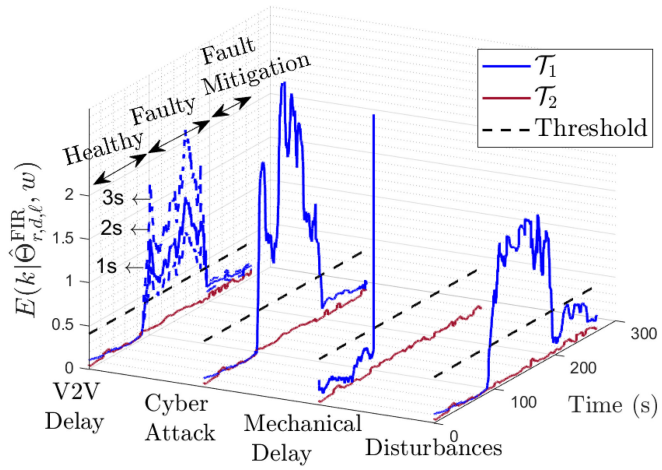


Fig. 21. Norm of the residuals of the transmissibilities $\mathcal{T}_1$ and $\mathcal{T}_2$ defined in Table II under the faults in Fig. 19. At $t = 80$ seconds, as $\mathcal{T}_1$ is faulty and $\mathcal{T}_2$ stays healthy, we conclude Qbot3 is faulty. After applying the fault mitigation algorithm at $t = 180$ the norm of the residual of $\mathcal{T}_1$ decreases. Note that since the mechanical delay is inherent in the robot, it cannot be mitigated using the proposed fault mitigation algorithm.

a similar fault to the motor delay introduced in Appendix B. That is a constant time delay between the controller and both actuators. Fig. 19 shows how the internal delay is emulated for the right actuator, which can be applied similarly to the left actuator. Fig. 20 shows the velocity of Qbot3 under healthy and faulty conditions. Fig. 21 shows the norm of residuals of the transmissibility operators defined in Table II. Note from Fig. 21 that at $t = 80$ seconds, the norm of the residual of $\mathcal{T}_1$ increases, where the norm of the residual of $\mathcal{T}_2$ remains on the same level. Therefore, we conclude that Qbot3 is faulty. Such a fault is inherent in the robot and cannot be mitigated using the proposed approach.

C. Cyber Attacks

Similar results can be obtained for the burst transmission and the DoS attacks as introduced in Appendix B, which we apply individually. For the burst transmission, a band-limited white noise signal is added to the velocity of Qbot2. The corrupted signal is then injected into the communication link between Qbot2 and Qbot3. For the communication time-delay fault, we consider individual cases of 1, 2, and 3 seconds of time delay in the communication link between Qbot2 and Qbot3. Fig. 19 shows a block diagram on how these faults are emulated. Fig. 20 shows Qbot3 velocity under healthy and faulty conditions. Fig. 21 shows the norm of the residuals for the transmissibility operators defined in Table II. Note that, for the proposed faults, at $t = 80$ seconds the norm of the residual of $\mathcal{T}_1$ increases, whereas the norm of the residual of $\mathcal{T}_2$ remains on the same level. Since measurements from Qbot3 were used to construct $\mathcal{T}_1$ but not $\mathcal{T}_2$, we can conclude that Qbot3 is faulty. For fault mitigation, we inject the correction signal obtained using $\mathcal{T}_2$ and the measurements of v_1 in the communication link between Qbot2 and Qbot3. Note from Fig. 21 that after applying the fault mitigation algorithm at approximately $t = 180$ the norm of the residual of $\mathcal{T}_1$ decreased.

VII. Experimental Health Monitoring With V2V Communications

In this section, we consider the experimental setup shown in Fig. 22 with V2V communications. Qbot1 leads the platoon

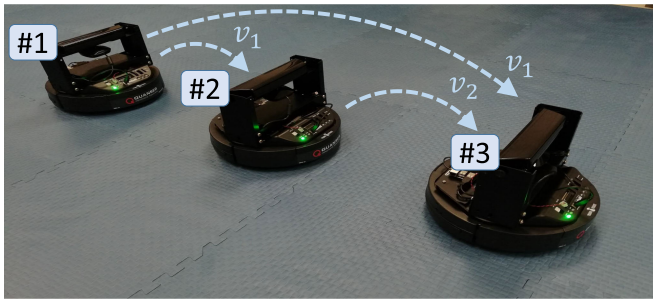


Fig. 22. Experimental setup: Qbot1 leads the platoon, Qbot2 receives the desired velocity from Qbot1 via V2V communications, and Qbot3 receives the desired velocities from Qbot2 and Qbot3 via two separate V2V communications, and follows the average of the two desired velocities.

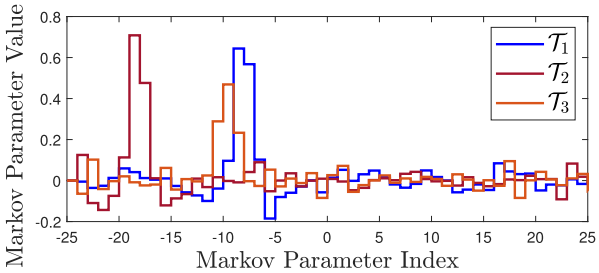


Fig. 23. Estimated Markov parameters for the transmissibility operators $\mathcal{T}_1$, $\mathcal{T}_2$, and $\mathcal{T}_3$ defined in Table III obtained using least squares with a noncausal FIR model with $r = d = 25$.

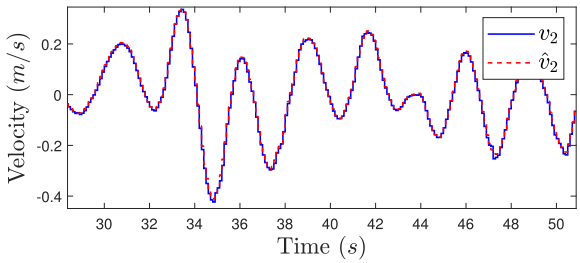


Fig. 24. Measured velocity v_2 and predicted velocity $\hat{v}_2$ of Qbot2, where $\hat{v}_2$ is obtained using the identified transmissibility operator $\mathcal{T}_1$ and measurements of v_1.

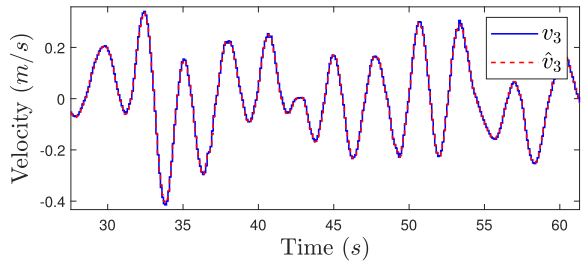


Fig. 25. Measured velocity v_3 and predicted velocity $\hat{v}_3$ of Qbot3, where $\hat{v}_3$ is obtained using the identified transmissibility operator $\mathcal{T}_3$ and measurements of v_1.

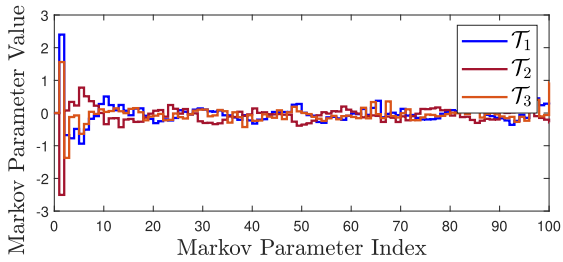


Fig. 26. Estimated Markov parameters for the transmissibility operators $\mathcal{T}_1$, $\mathcal{T}_2$, and $\mathcal{T}_3$ defined in Table III obtained using least squares with a noncausal FIR model with $r = 100$ and $d = 0$.

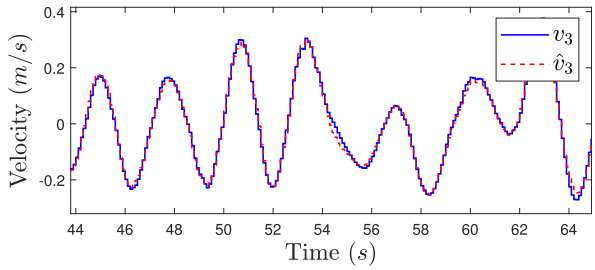


Fig. 27. Measured velocity and predicted velocity of Qbot3 obtained using the identified transmissibility operator $\mathcal{T}_3$ shown in Fig. 26.

and Qbot2 receives the desired velocity from Qbot1 via V2V communication. Qbot3 is connected with Qbot1 and Qbot2 via two separate V2V communications, and Qbot3 follows the average of the two velocities of Qbot1 and Qbot2.

For health monitoring, we consider a one-dimensional motion of the platoon. We first consider a zero-mean, unit variance, Gaussian random excitation signal for Qbot1. Consequently, Qbot 2 and Qbot3 move in response to the motion of Qbot1. We use least squares with a noncausal FIR model with $r = 25$ and $d = 25$ to identify the transmissibility operators shown in Table III, where v_1, v_2, and v_3 represent the velocities of Qbot1, Qbot2, and Qbot3, respectively. The estimated Markov parameters of the transmissibility operators $\mathcal{T}_1, \mathcal{T}_2$, and $\mathcal{T}_3$ are shown in Fig. 23. Figs. 24 and 25 show the measured velocities v_2 and v_3 and the predicted velocities $\hat{v}_2$ and $\hat{v}_3$ of Qbot2 and Qbot3, respectively, where $\hat{v}_2$ is computed using the identified transmissibility $\mathcal{T}_1$ and measurements of v_1, and $\hat{v}_3$ is computed using the identified transmissibility $\mathcal{T}_3$ and measurements of v_1. It is important to mention that neither the dynamics of the network and the robots nor the excitation signal of the transmissibility is used to obtain the predicted velocities of Qbot2 and Qbot3.

For fault mitigation, we identify causal models of the transmissibility operators defined in Table III. Fig. 26 shows the identified Markov parameters of the transmissibility operators $\mathcal{T}_1, \mathcal{T}_2$, and $\mathcal{T}_3$ defined in Table III obtained using least squares with a noncausal FIR model with $r = d = 25$. Fig. 27 shows the measured velocity and the predicted velocity of Qbot3, where the predicted velocity is obtained using the identified transmissibility $\mathcal{T}_3$ shown in Fig. 26 and measurements of v_1.

Next, we individually apply the internal disturbances, burst transmission, and communication time delay faults as introduced in Appendix B and detailed in Section VI. Fig. 28 shows the norm of the residual for the transmissibility operators defined in Table III. Note from Fig. 28 that for the disturbance, cyber attack, and time-delay faults, which occur at $t = 80$ seconds, the norms of the residual of $\mathcal{T}_2$ and $\mathcal{T}_3$ increase and the norm of the residual of $\mathcal{T}_1$ remains on the same level. Since measurements of

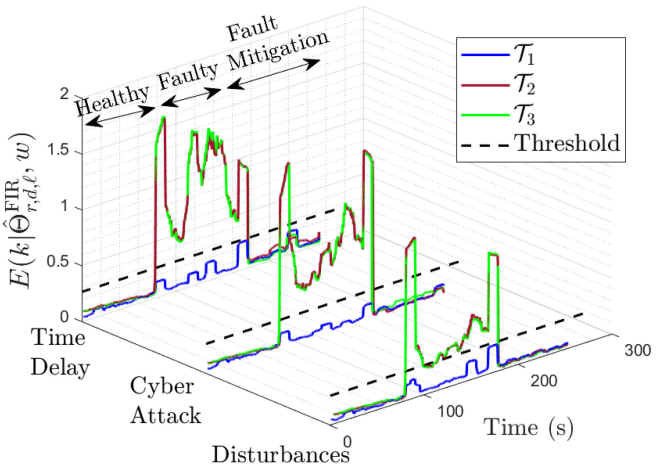


Fig. 28. Norm of the residuals of the $\mathcal{T}_1$, $\mathcal{T}_2$, and $\mathcal{T}_3$ transmissibilities introduced in Table III under disturbance, cyber-attack, and time delay faults proposed at approximately $t = 80$ sec. Since measurements of Qbot3 were used to identify $\mathcal{T}_2$ and $\mathcal{T}_3$ but not $\mathcal{T}_1$, we conclude that Qbot3 is faulty. After applying the fault mitigation algorithm at approximately $t = 180$ seconds the norm of the residuals of the transmissibilities $\mathcal{T}_1$ and $\mathcal{T}_3$ drops, which indicates that Qbot3 has become healthy again.

Qbot3 were used to identify $\mathcal{T}_2$ and $\mathcal{T}_3$ but not $\mathcal{T}_1$, we conclude that Qbot3 is faulty.

For fault mitigation, the reference velocity of Qbot3 is obtained using the identified $\mathcal{T}_3$ shown in Fig. 26 and the measurement of v_1 via the communication link between Qbot1 and Qbot3. Note from Fig. 28 that after applying the fault mitigation algorithm at approximately $t = 180$ seconds, the norms of the residuals of all transmissibilities drop, which indicates that Qbot3 has become healthy again.

VIII. Conclusion

In this paper, we used transmissibility operators for fault detection, localization, and mitigation in a set of platoons of connected autonomous vehicles. This approach uses sensor measurements available from vehicles in the platoon to identify transmissibility operators under healthy conditions of the platoon. Then, the identified transmissibilities are used along with the available sensor measurements for fault detection, localization, and mitigation. The proposed approach does not require knowledge of the dynamics of the platoon or the input that excites the platoon. We proposed a fault localization algorithm that determines both the faulty platoon and the faulty vehicle in the platoon. Then, the transmissibilities identified under healthy conditions were used along with measurements from healthy vehicles to mitigate the effect of the fault. The excitation signal that acts on the network and the dynamics of the network and the vehicles are assumed to be unknown. Networks with V2C and V2V communications were considered. Simulation results for a network with both V2C and V2V communications were shown. Moreover, the algorithm was tested on an experimental setup consisting of three mobile robots connected with V2C and V2V communication. Disturbance, internal time-delay, cyberattack, and communication time-delay faults were considered for both the simulation and experimental results. The proposed algorithm was able to detect the faulty vehicle and the faulty platoon, and mitigate the effect of the fault efficiently.

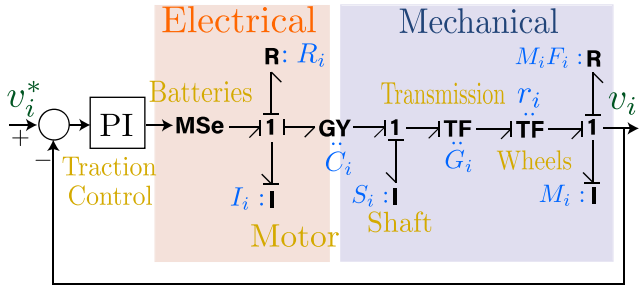


Fig. 29. Bond graph model of an electric vehicle used for the numerical results.

Appendix A
Platoon Modeling

In this appendix, we introduce an analytical bond graph model of the platoon. Although the proposed approach does not require knowledge of a model of the platoon, this model is used to a) apply the proposed approach of fault detection, localization, and mitigation to a numerical model, and b) apply the proposed approach to a set of realistic physical and cyber faults, which can affect real CAV and are difficult to implement experimentally. We consider modeling the CAV vehicle dynamics using the bond graph approach. This uses energy and power propagation to simulate systems that consist of several mechanical and electrical components.

A. Modeling of One Platoon of CAV

Consider a platoon of n identical connected autonomous vehicles with longitudinal motion. For all $i = 1, \ldots, n$, let v_i and v_i^* denote the velocity and the desired velocity of the i-th vehicle, respectively. All vehicles are assumed to be electric vehicles with the powertrain topology in [46]. Following [46], [47], we consider the drive motor as a Brushless DC Motor that extracts power from the batteries based on the traction control signal. The controller is assumed to be a PI controller to characterize the cruise-control traction with proportional gain $k_{P,i}$ and integral gain $k_{I,i}$.

Fig. 29 shows a bond-graph model of the considered electric vehicle, while parameters description and their numerical values are defined in Table IV. Following the formulation procedure in [21, Chapter 5, Section 5.3], the bond graph model of vehicle i can be formulated in the following differential equation

$$\dddot{v}_i(t) + \alpha_i \ddot{v}_i(t) + \beta_i \dot{v}_i(t) + \gamma_i v_i(t) = \delta_i \dot{v}_i^*(t) + \gamma_i v_i^*(t). \tag{A1}$$

where $\alpha_i = \kappa_i R_i[\eta_i + 1 + \frac{F_i I_i}{R_i}]$, $\beta_i = \kappa_i[\frac{C_i^2 \eta_i}{S_i} + F_i + \zeta_i k_{I,i}]$, $\gamma_i = \kappa_i \zeta_i$, $\delta_i = \gamma_i k_{I,i}$, $\kappa_i = \frac{1}{I_i(\eta_i+1)}$, and $\zeta_i = \frac{C_i k_{P,i}}{k_{I,i} G_i r_i M_i}$.

By setting the desired velocity of each vehicle to the velocity of the front vehicle, the platoon can be modeled on the state space form in (1), (2) where

$$A = \begin{bmatrix} A_1 & & \ldots & 0 \\ B_2 C_1 & A_2 & & \\ & \ddots & \ddots & \\ 0 & \ldots & B_n C_{n-1} & A_n \end{bmatrix},$$

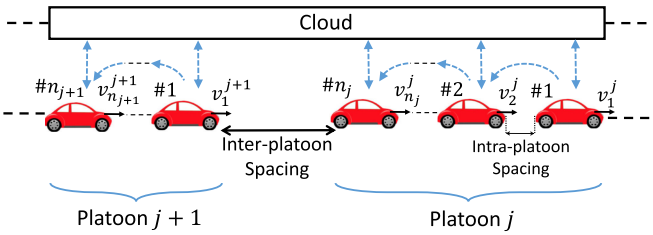


Fig. 30. An illustration of a set of platoons of CAVs. All vehicles within the V2V communications are considered as a platoon, and vehicles connected with each other via V2V are within the same set of platoons.

$$B = \begin{bmatrix} B_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, C = \begin{bmatrix} C_1 & \dots & 0 \\ \vdots & \ddots & \\ 0 & \dots & C_n \end{bmatrix},$$

$$A_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -\gamma_i & -\beta_i & -\alpha_i \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ \delta_i \\ \gamma_i - \alpha_i \delta_i \end{bmatrix},$$

$$C_i = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}.$$

B. Cyber Communications

V2V wireless information communication uses short-to-medium range communication. CAV platoons are expected to use the Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC-WAVE) as in [24], [48]. DSRC-WAVE covers up to 1 km in range with a rate of data transmission that is up to 27 Mbps, 5.9 GHz frequency, and a 75 MHz channel bandwidth.

For V2C communications, CAV platoons use a combination of the large-area street network and a cellular Long Term Evolution (LTE) [49]. According to [50], V2C communications allow CAVs to communicate with each other and conduct integration of cloud computing. LTE communication covers up to 2 km in the range between the vehicle and the roadside infrastructure antenna with a rate of data transmission that is up to 75 Mbps and a 2.6 GHz frequency with a 20 MHz channel bandwidth [51].

C. Modeling of a Set of Platoons of CAV

In this section, we extend the CAV model obtained earlier in this section to a set of CAV platoons as in [52]. Connected autonomous vehicles sets are sets of multi-platoons used to cooperate, split, or merge platoons [53]. Therefore, we assume that each vehicle has a vehicle-to-cloud wireless communication as shown in Fig. 30. For all $j = 1, \dots, m$, where m is the number of platoons, and for all $i = 1, \dots, n_j$, where n_j is the number of vehicles in the j-th platoon, let v_i^j denote the velocity of the i-th vehicle in platoon j. The intra-platoon spacing is the distance between vehicles in the same platoon, which is assumed to be a small separation distance compared to the inter-platoon spacing distance. That is, all vehicles that are within the vehicle-to-vehicle communication range are assumed to be in the same platoon. To connect these platoons, we assume that the first vehicle in each platoon receives the same desired velocity signal from the cloud.

APPENDIX B
FAULT MODELS

In this appendix, we introduce common physical and cyber fault models from the literature. The proposed technique is independent of the fault dynamics and considers any fault to result in the corrupted unknown velocity $\tilde{v}_i$.

A. Motor Disturbances

Brushless DC motors that are used in electric vehicles are subjected to vulnerable operating conditions including high magnetic force and severe weather conditions. Following [54], we introduce an additive fault to the motor's nominal value of the current-to-torque ratio C_i after motor loss of effectiveness occurs. The faulty motor constant is then given by

$$\tilde{C}_i(t) = 0.8C_i + \delta_{C_i}(t), \tag{B1}$$

where $\tilde{C}_i$ is the corrupted motor constant, and δ_{C_i} is the deviation from the original motor constant after the loss of effectiveness occurs.

B. Motor Delay

Internal delay in actuators can lead to poor control performance and potential instability [23], [55]. The motor internal delay can be modeled as a time delay between the motor electrical current and the output torque, that is,

$$\tilde{\rho}_i(t) = \rho_i(t - \tau_{e,i}(t)), \tag{B2}$$

where $\tilde{\rho}_i$ is the delayed current, ρ_i is the original current and $\tau_{e,i}$ is the time-variant motor delay.

C. Burst Transmission

Connected autonomous vehicles platoons have several spacing-distance policies as shown in [8], [56]. One possible cyberattack is burst transmission that can affect the system performance by adding bounded random disturbances to the spacing distance between two preceding vehicles [31]. This fault can lead to instabilities, inaccuracies, and oscillations in the system performance [14], [24], [32]. For all $i = 1, \dots, n$, let h_i denote the nominal spacing value between vehicle i and vehicle $i+1$, then for all $t \geq 0$,

$$\tilde{h}_i(t) = h_i(t) + \delta_{f,i}(t), \tag{B3}$$

where $\tilde{h}_i$ denotes the corrupted spacing distance, and $\delta_{f,i}$ denotes the deviation from h_i due to a cyberattack. Spacing distance fault can occur due to corrupted measurements of the velocities of the vehicles. Therefore, v_i can be represented by

$$\tilde{v}_i(t) = v_i(t) + \dot{\tilde{h}}_i(t), \tag{B4}$$

where for all $i = 1, \dots, n$, $\tilde{v}_i$ represents the corrupted measurements of the velocity of vehicle i, $\dot{\tilde{h}}_i$ denotes the deviation from v_i due to a cyberattack.

D. Denial-of-Service

Time delays in connected autonomous vehicles platoons can yield fatal faults [7]. One of the main malicious cyberattacks in vehicle platoons is the Denial-of-Service (DoS) attack [31]. DoS attack increases the service time in the communication link, which makes it busier and results in a communication time delay within the communication link. Note that, as the service time increases, the packet transmitted fades, which is known as the packet loss. In this paper, we consider small-time communication delays that cause the packet to arrive late. For all $i = 1, \ldots, n$, consider the velocity of the i-th vehicle v_i, then a delay in v_i yields the corrupted signal

$$\tilde{v}_i(t) = v_i(t - \tau_{v,i}(t)), \tag{B5}$$

where $\tau_{v,i}$ is a relatively small time-variant communication delay in v_i that does not cause any packet loss.

REFERENCES

[1] R. Hult, G. R. Campos, E. Steinmetz, L. Hammarstrand, P. Falcone, and H. Wymeersch, "Coordination of cooperative autonomous vehicles: Toward safer and more efficient road transportation," *IEEE Signal Process. Mag.*, vol. 33, no. 6, pp. 74–84, Nov. 2016.

[2] D. Bechtsis, N. Tsolakis, D. Vlachos, and J. S. Srai, "Intelligent autonomous vehicles in digital supply chains: A framework for integrating innovations towards sustainable value networks," *J. Cleaner Prod.*, vol. 181, pp. 60–71, 2018.

[3] S. E. Shladover, "Connected and automated vehicle systems: Introduction and overview," *J. Intell. Transp. Syst.*, vol. 22, pp. 190–200, 2018.

[4] S. Darbha, S. Konduri, and P. R. Pagilla, "Benefits of V2V communication for autonomous and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1954–1963, May 2019.

[5] A. H. Taylor, M. Droege, G. Shaver, J. Sandoval, S. Erlien, and J. Kuszmaul, "Capturing the impact of speed, grade, and traffic on class 8 truck platooning," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 10506–10518, Oct. 2020.

[6] X. Jin, W. M. Haddad, Z.-P. Jiang, and K. G. Vamvoudakis, "Adaptive control for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," in *Proc. IEEE Conf. Decis. Control*, Miami Beach, FL, USA, 2018, pp. 2810–2815.

[7] F. Li, D. Mikulski, J. R. Wagner, and Y. Wang, "Trust-based control and scheduling for UGV platoon under cyber attacks," SAE Tech. Paper 2019-01-1077, 2019, doi: 10.4271/2019-01-1077.

[8] P. Seiler, A. Pant, and K. Hedrick, "Disturbance propagation in vehicle strings," *IEEE Trans. Autom. Control*, vol. 49, no. 10, pp. 1835–1842, Oct. 2004.

[9] M. Sun, A. Al-Hashimi, M. Li, and R. Gerdes, "Impacts of constrained sensing and communication based attacks on vehicular platoons," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 4773–4787, May 2020.

[10] 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.

[11] A. Lopes and R. E. Araújo, "Active fault diagnosis method for vehicles in platoon formation," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 3590–3603, Apr. 2020.

[12] P. Fernandes and U. Nunes, "Platooning with IVC-enabled autonomous vehicles: Strategies to mitigate communication delays, improve safety and traffic flow," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 91–106, Mar. 2012.

[13] P. Fernandes and U. Nunes, "Platooning of autonomous vehicles with intervehicle communications in sumo traffic simulator," in *Proc. Int. IEEE Conf. Intell. Transp. Syst.*, 2010, pp. 1313–1318.

[14] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[15] K. F. Aljanaideh and D. S. Bernstein, "Experimental application of time-domain transmissibility identification to fault detection and localization in acoustic systems," *J. Vib. Acoust.*, vol. 140, 2018, Art. no. 021017.

[16] K. Aljanaideh, B. Coffer, D. Dionne, S. Kukreja, and D. Bernstein, "Sensor-to-sensor identification for the sofia testbed," in *Proc. AIAA Guid., Navig., Control Conf.*, Minneapolis, MN, USA, 2012, pp. 1–17.

[17] K. F. Aljanaideh and D. S. Bernstein, "Aircraft sensor health monitoring based on transmissibility operators," *J. Guid., Control, Dyn.*, vol. 38, pp. 1492–1495, 2015.

[18] A. Khalil and K. F. Aljanaideh, "Aircraft structural health monitoring using transmissibility identification," *IFAC-PapersOnLine*, vol. 51, pp. 969–974, 2018.

[19] K. F. Aljanaideh and D. S. Bernstein, "Initial conditions in time-and frequency-domain system identification: Implications of the shift operator versus the Z and discrete fourier transforms," *IEEE Control Syst. Mag.*, vol. 38, no. 2, pp. 80–93, Apr. 2018.

[20] K. F. Aljanaideh and D. S. Bernstein, "Closed-loop identification of unstable systems using noncausal FIR models," *Int. J. Control*, vol. 90, pp. 168–185, 2017.

[21] D. C. Karnopp, D. L. Margolis, and R. C. Rosenberg, *System Dynamics: Modeling, Simulation, and Control of Mechatronic Systems*. Hoboken, NJ, USA: Wiley, 2012.

[22] J. Chen and R. B. Randall, "Intelligent diagnosis of bearing knock faults in internal combustion engines using vibration simulation," *Mechanism Mach. Theory*, vol. 104, pp. 161–176, 2016.

[23] B. Li, X. Rui, W. Tian, and G. Cui, "Neural-network-predictor-based control for an uncertain multiple launch rocket system with actuator delay," *Mech. Syst. Signal Process.*, vol. 141, pp. 1–19, 2019.

[24] M. Pirani *et al.*, "Cooperative vehicle speed fault diagnosis and correction," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 783–789, Feb. 2019.

[25] A. D'Innocenzo, F. Smarra, and M. D. Di Benedetto, "Resilient stabilization of multi-hop control networks subject to malicious attacks," *Automatica*, vol. 71, pp. 1–9, 2016.

[26] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3432–3439, Dec. 2018.

[27] C.-H. Xie and G.-H. Yang, "Observer-based attack-resilient control for linear systems against FDI attacks on communication links from controller to actuators," *Int. J. Robust Nonlinear Control*, vol. 28, no. 15, pp. 4382–4403, 2018.

[28] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242–3251, May 2016.

[29] D. Ding, Z. Wang, D. W. Ho, and G. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 1936–1947, Aug. 2017.

[30] X. He, E. Hashemi, and K. H. Johansson, "Distributed control under compromised measurements: Resilient estimation, attack detection, and vehicle platooning," vol. 134, 2021, Art. no. 109953.

[31] A. Petrillo, A. Pescape, and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1134–1149, Mar. 2021.

[32] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative approach for improving the security of vehicular scenarios: The case of platooning," *Comput. Commun.*, vol. 122, pp. 59–75, 2018.

[33] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[34] E. Hashemi, X. He, and K. H. Johansson, "A dynamical game approach for integrated stabilization and path tracking for autonomous vehicles," in *Proc. Amer. Control Conf. (ACC)*, Denver, CO, 2020, pp. 4108–4113.

[35] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proc. ACM Symp. Inf., Comput. Commun. Secur.*, 2015, pp. 167–178.

[36] X. Jin, W. M. Haddad, Z.-P. Jiang, A. Kanellopoulos, and K. G. Vamvoudakis, "An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," *Int. J. Adaptive Control Signal Process.*, vol. 33, pp. 1788–1802, 2019.

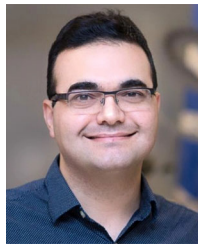
[37] G. Guo, P. Li, and L. Hao, "Adaptive fault-tolerant control of platoons with guaranteed traffic flow stability," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6916–6927, Jul. 2020.

[38] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

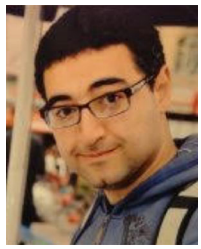
[39] J. Lunze, "Adaptive cruise control with guaranteed collision avoidance," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1897–1907, May 2019.

[40] Y. Fang, H. Min, W. Wang, Z. Xu, and X. Zhao, "A fault detection and diagnosis system for autonomous vehicles based on hybrid approaches," *IEEE Sensors J.*, vol. 20, no. 16, pp. 9359–9371, Aug. 2020.
[41] A. Petrillo, A. Picariello, S. Santini, B. Scarciello, and G. Sperli, "Model-based vehicular prognostics framework using big data architecture," *Comput. Ind.*, vol. 115, 2020, Art. no. 103177.
[42] K. F. Aljanaideh and D. S. Bernstein, "Time-domain analysis of sensor-to-sensor transmissibility operators," *Automatica*, vol. 53, pp. 312–319, 2015.
[43] R. H. Middleton and G. C. Goodwin, *Digital Control and Estimation: A Unified Approach*. Englewood Cliffs, NJ, USA:Prentice-Hall, 1990.
[44] A. Youssef, C. Delpha, and D. Diallo, "An optimal fault detection threshold for early detection using Kullback-Leibler divergence for unknown distribution data," *Signal Process.*, vol. 120, pp. 266–279, 2016.
[45] 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.
[46] B. Wang, M. Xu, and L. Yang, "Study on the economic and environmental benefits of different EV powertrain topologies," *Energy Convers. Manage.*, vol. 86, pp. 916–926, 2014.
[47] B. N. Kommula and V. R. Kota, "Performance evaluation of hybrid fuzzy PI speed controller for brushless DC motor for electric vehicle application," in *Proc. IEEE Conf. Power, Control, Commun. Comput. Technol. Sustain. Growth*, 2015, pp. 266–270.
[48] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Identifier Allocations*, IEEE Standard 1609.12–2016, U.D. Transportation, Queens, NY, 2013.
[49] J. Pillmann, B. Sliwa, J. Schmutzler, C. Ide, and C. Wietfeld, "Car-to-cloud communication traffic analysis based on the common vehicle information model," in *Proc. IEEE Veh. Technol. Conf.*, Toronto, Canada, 2017, pp. 1–5.
[50] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.
[51] L. Kong, M. K. Khan, F. Wu, G. Chen, and P. Zeng, "Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 62–68, Jan. 2017.
[52] D. Jia and D. Ngoduy, "Platoon based cooperative driving model with consideration of realistic inter-vehicle communication," *Transp. Res. Part C: Emerg. Technol.*, vol. 68, pp. 245–264, 2016.
[53] Y. Li, C. Tang, K. Li, X. He, S. Peeta, and Y. Wang, "Consensus-based cooperative control for multi-platoon under the connected vehicles environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 6, pp. 2220–2229, Jun. 2019.
[54] G. Zhang, H. Zhang, X. Huang, J. Wang, H. Yu, and R. Graaf, "Active fault-tolerant control for electric vehicles with independently driven rear in-wheel motors against certain actuator faults," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 5, pp. 1557–1572, Sep. 2016.
[55] D. Bresch-Pietri and M. Krstic, "Delay-adaptive predictor feedback for systems with unknown long actuator delay," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2106–2112, Sep. 2010.
[56] D. Swaroop, "String stability of interconnected systems: An application to platooning in automated highway systems," Ph.D. dissertation, Univ. California, Berkeley, CA, USA, 1994.

Abdelrahman Khalil received the B.Sc. degree in aeronautical engineering from the Jordan University of Science and Technology, Irbid, Jordan, in 2018. He is currently working toward the Ph.D. degree in mechanical engineering with the Memorial University of Newfoundland, St. John's, NL, Canada. His research interests include estimation and control of dynamic systems, fault detection and mitigation, and system identification.



Mohammad Al Janaideh received the M.A.Sc. degree in mechanical engineering and the Ph.D. degree in mechatronics and control from Concordia University, Montreal, QC, Canada, in 2005 and 2010, respectively. He was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada, and the Department of Aerospace Engineering, University of Michigan, Ann Arbor, MI, USA. He also was a Senior Mechatronics Engineer with ASML, CT, USA. Since 2017, he has been with the Department of Mechanical Engineering, Memorial University of Newfoundland, St. John's, NL, Canada. His research interests include design and control of micro- and nano-positioning systems, fault detection and mitigation of connected autonomous robotics networks, design and control of precision motion stages for semiconductor manufacturing machines, and control of systems with uncertain hysteresis nonlinearities. He is the Technical Editor of IEEE TRANSACTIONS ON MECHATRONICS, IEEE CONFERENCE OF DECISION AND CONTROL (CDC), and the American Control Conference (ACC).



Khaled F. Aljanaideh received the B.Sc. degree in mechanical engineering (top of class) from the Jordan University of Science and Technology, Irbid, Jordan, in 2009, the M.S.E. and M.Sc. degrees in aerospace engineering and applied mathematics and the Ph.D. degree in aerospace engineering,from the University of Michigan, Ann Arbor, MI, USA, in 2011, 2014, and 2015, respectively. He is an Assistant Professor with the Department of Aeronautical Engineering, Jordan University of Science and Technology. He was a Postdoctoral Research Fellow with the Department of Aerospace Engineering, University of Michigan, between 2015 and 2016, where he also was a part-time Visiting Assistant Professor between 2017 and 2019. He is currently with MathWorks, Natick, MA. His current research interests are in system identification and fault detection for aerospace and mechanical systems.

Deepa Kundur received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively. She is currently a Professor & Chair of The Edward S. Rogers Sr. Department of Electrical & Computer Engineering, University of Toronto. Her research interests include the interface of cybersecurity, signal processing, and complex dynamical networks. She is an author of more than 200 journal and conference papers and is also a recognized authority on cybersecurity issues. Professor Kundur has participated on several editorial boards. She currently serves on the Advisory Board of IEEE Spectrum. Professor Kundur's research was the recipient of the best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference and the 2015 IEEE Electrical Power and Energy Conference She is a Fellow of the Canadian Academy of Engineering and a Senior Fellow of Massey College.