IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 25, 2019, accepted December 11, 2019, date of publication December 19, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2961002

Security of Vehicle Platooning: A Game-Theoretic Approach

MOHAMMAD HOSSEIN BASIRI[1], MOHAMMAD PIRANI[2], NASSER L. AZAD[3], AND SEBASTIAN FISCHMEISTER[1]

[1]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[2]Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S, Canada
[3]Department of Systems Design Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Corresponding author: Mohammad Hossein Basiri (mh.basiri@uwaterloo.ca)

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

ABSTRACT In this paper, we study the security of a vehicle platoon exposed to cyber attacks using a game-theoretic approach. The platoon topologies under investigation are directed (called predecessor following) or undirected (bidirectional) weighted graphs. The edge weights specify the quality of the communication links between the vehicles in both the unidirectional/bidirectional data transfer environments. The attacker-detector game is defined as follows. The attacker targets some vehicles in the platoon to attack and the detector deploys monitoring sensors on the vehicles. The attacker's objective is to be as stealthy to the sensors as possible while the detector tries to place the monitoring sensors to detect the attack impact as much as it can. The existence of Nash Equilibrium (NE) strategies for this game is investigated based on which the detector can choose specific vehicles to put his sensors on and increase the security level of the system. Moreover, we study the effect of adding (or removing) communication weights between vehicles on the game value. The simulation and experimental results conducted on a vehicle platoon setup using Robotic Operating System (ROS) demonstrate the effectiveness of our analyses.

INDEX TERMS Game theory, graph theory, Nash equilibrium, security, sensor placement.

I. INTRODUCTION

A. MOTIVATION

Safe and secure driving experience is one of the most significant objectives in recently emerging intelligent transportation systems [1], [2]. Evolution of smart and autonomous vehicles has highlighted this concern much more than the past decades [3]. On the other hand, the possibility of featuring the connectivity and cooperation of vehicles has led to the emergence of strings of connected vehicles, namely *platoons*. Platoons have provided the opportunity to enhance the driving safety, ecological performance, road throughput, and comfort level [4]–[7]. Current standards for vehicular communications enable cars to exchange data, such as inter-vehicular distance, speed, and acceleration among each other through different communication environments, namely Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Cloud (V2C), and Vehicle-to-Broadband (V2B) [8], [9]. V2V communications can provide direct data transfer with a much lower delay compared to radars [10] and enable vehicles to drive closely with short inter-vehicular distances. This will increase the amount of road throughput and reduce the need for developing more road network. In this context, Cooperative Adaptive Cruise Control (CACC) has been widely developed which aims to enhance the fuel efficiency, safety, driving comfort, and road throughput [10]–[18].

Despite plenty of benefits resulting from the use of wireless communications in a platoon, it is naturally vulnerable to cyber attacks. Different types of attacks on a platoon can be generally classified into three classes, namely application layer attacks, network layer attacks, and privacy leakage attacks [19]. All these attacks can potentially endanger the string stability of the platoon. Moreover, the attacker could be an external or an internal malicious agent performing each of the above-mentioned attacks [20]. For details of the aforementioned attacks, the reader is referred to [19]. False data injection attack (message falsification/tampering), replay attack, jamming attack, eavesdropping attack, Man-in-the-Middle attack, GPS spoofing, impersonation attack, masquerading attack, and Denial of Service (DoS) are some of

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu.

the possible real-world attacks on vehicle platoons [21]–[24]. In this paper, we will focus on bias injection attack as a common form of disruption attacks [25], [26]. Another attack classification in literature splits the attacks into control algorithm modification and sensor reading tampering classes [20]. Control algorithm modification attacks include destabilizing attacks [27], high-speed collision induction attacks [28], and traffic flow instability attacks [29], [30]. Sensor reading tampering attacks consist of false data injection [31] and efficiency-motivated attacks [23].

It is notable that the vulnerability of a platoon against attacks can also arise from insecure individual vehicles participating in the platoon. Therefore, securing single vehicles individually is also essential to ensure the security of the connected vehicles in a platoon. In this respect, a means of attacks on a single vehicle is to exploit the vulnerability of a component of the vehicle allowing access to its CAN bus. For instance, in several real car attacks occurred recently, the infotainment component of the vehicle that required no authentication and could be accessed anonymously, was exploited aiming at getting access to the CAN bus of the vehicle thereby attaining control on different operations of the car, such as steering wheel, engine, and braking system. For a comprehensive list of real-world attacks happened on vehicles from 2010 up to 2017 together with several countermeasures, the reader is referred to [32].

Back to the platoons, an adversarial attacker can target one or several vehicles to physically/remotely manipulate the sensors of the vehicles which can eventually cause hazardous actions or even accidents. This signifies the importance of security of the vehicle platoons against external malicious attacks. Hence, the need for monitoring systems capable of detecting the attackers' action is highly sensible [33]–[39]. One of the important aspects of deployed monitoring sensors is their location regarding the possible locations of injected attacks. Consequently, it is largely essential to have a systematic procedure based on which the detector can place its sensors on specific locations to increase the security level of the system.

B. RELATED WORK

Recently, much research has been done in investigating the security of networked control systems from various perspectives [40]–[44]. Communication-related protection methods, such as encryption of wireless channels, are techniques to avoid receiving compromised data via the wireless infrastructures [9]. On the other hand, control-oriented concepts, such as game-theoretic methods are also among the leading methodologies which address the security issue of general cyber-physical systems with a considerable amount of care [45], [46]. Various approaches, such as Nash or Stackelberg formulations, demonstrate the conflicting decisions between the players (attackers and defenders) [47], [48]. The existence of an equilibrium state for this game is a solution based on which the detector can decide about its sensor placement strategy. Cooperative games are some other recent approaches aiming at modeling networked control systems [49]. Based on these games, robustness analysis of the system against malicious attacks has also been studied [50]–[52]. With respect to securing communication protocols used in platoons, secure communication protocols for VANETs based on game theory have been proposed either for multimedia transmission [53] or for communications exposed to specific attacks [54]. Network-aware control methods have also been proposed to handle possible communication failures through the platoon. Those approaches mainly consider random communication failures with an emphasis on the control/stability performance of the whole platoon without considering intelligent cyber attacks [55]–[57]. Despite the above-mentioned works and to the best of the authors' knowledge, a general procedure for investigation of security of vehicle platoons under cyber attacks in which the quality of communications among the vehicles are different is missing and has not been addressed yet. Game-theoretic approaches provide a powerful tool to tackle the attacker-detector conflicting actions as an attacker-detector game and study the security of a platoon based on various decisions made by the adversarial and the defender. Hence, in this paper, we will formulate the security problem of a general platoon, which is under cyber attacks, as a game where both the attacker and the defender attempt to face each other in opposite ways. Moreover, the communication links between different vehicles can have different qualities and both the unidirectional and bidirectional data transfer structures are taken into account in this work. More rigorously, the adversary tries to attack specific vehicles of the platoon such that he remains undetected while the defender endeavors to locate his sensors on specific vehicles such that the detectability of the attacker is maximized, hence, increases the security level of the system.

C. CONTRIBUTIONS

In this paper, we focus on optimal sensor placement on specific nodes in a vehicle platoon which is assumed to be exposed to cyber attacks. This sensor placement problem is investigated through a game-theoretic approach based on graph-theoretic properties of directed and undirected platoons. The attacker's objective is to attack f vehicles in a platoon while being minimally visible and the detector's strategy is to place f sensors on specific nodes in order to maximize the visibility of the attacker. We benefit from the system L_2-gain from the attack signal to the sensor measurements vector to characterize the cost function introduced in the game. Explicitly, our contributions in this paper are as follows,

- For both predecessor-following (directed) platoon and symmetric (undirected) platoon, we investigate the existence of a Nash Equilibrium (NE) strategy for an attacker-detector game based on which the detector can place its sensors on specific nodes increasing the security level of the system. We consider the case of single attacked vehicle, $f = 1$, as well as multiple attacked vehicles, $f > 1$, where f is the number of attacked nodes and deployed sensors on the network (Theorem 1, Theorem 2, Theorem 3, Theorem 4).

- We study the effects of adding or removing communication links (or weights) to (or from) the platoon on the game pay-off. Both undirected and directed scenarios will be investigated in this study, and we show that the behaviour of the game value in response to such topology variations is different for directed and undirected networks (Theorem 5, Theorem 6).
- The security level of a platoon equipped with undirected communication links among its vehicles will be compared to that of a platoon equipped with directed communication links. Our results show that using undirected data transfer increases the security level of the system which is consistent with the fact that the two-way data transfer between the pairs of vehicles lets them receive the attack signal from multiple ways instead of a single path, hence, resulting in a more reliable platoon (Proposition 2).

D. VEHICULAR COMMUNICATION STANDARDS AND DSRC

In vehicle platooning, there have been some studies that investigated interaction protocols and standards for data sharing [58], [59]. Other researches have also considered degradation and communication loss of data transfers affecting the CACC performance [60], [61]. Generally, several important variants of wireless data transfer systems exploited in connected vehicles include DSRC, VANET, and MANET [62], [63]. DSRC, which was developed by the American Society for Testing and Materials (ASTM), has been leveraged as one of the communication methods for V2X communications as an inter-vehicular communication infrastructure, and is largely based on IEEE 802.11p, which uses Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. It was initially developed to operate on a 912 MHz bandwidth channel in 1992. In 2002 and 2003, it was improved as the particular standard used in Intelligent Transportation Systems (ITS) using IEEE 802.11a operating on the 5.9 GHz band denoted by E2203-02 and E2203-03, respectively [64]. Recently, this protocol, which is also called the Wireless Access in the Vehicular Environment (WAVE), is established to manage the data transfers in the 5.9 GHz band on seven different channels of 75 MHz bandwidth [65], [66]. Each channel is 10 MHz wide along with 5 MHz reserved before the channels. For more details of DSRC and other protocols, the reader is referred to [65], [66] and references therein.

E. ORGANIZATION OF THE PAPER

This paper is organized as follows. Sec. II defines the problem formulation of a platoon under cyber attacks. The attacker-detector game is defined and the system and attack modeling are presented in this section. In Sec. III we perform the equilibrium analysis for both the weighted undirected and directed data transfer scenarios where the attacker attacks one node and the detector places one sensor on a node. Sec. IV extends the results to the case where more than one nodes are attacked and more than one monitoring sensors are supposed to be deployed. In Sec. V effects of adding extra communication links to a platoon are studied. Security level of a platoon with bidirectional versus unidirectional communication links is investigated in Sec. VI. Sec. VII presents the simulation and experimental results. Finally, Sec. VIII concludes the paper.

II. PROBLEM FORMULATION

First of all, we present the notations and definitions used in the rest of the paper for the sake of legibility.

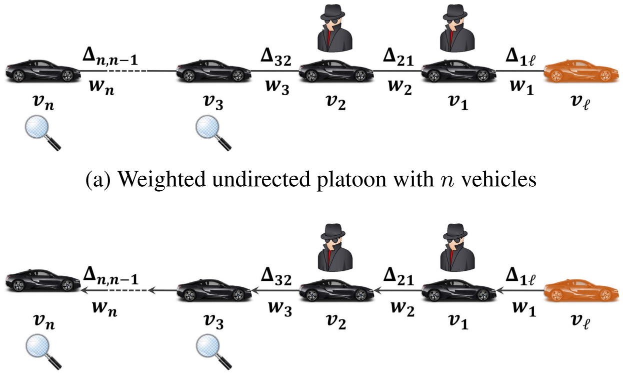
A. NOTATIONS AND DEFINITIONS

We denote a weighted undirected graph by $\mathcal{G}_u(\mathcal{V}, \mathcal{W})$ where $\mathcal{V}$ is the set of nodes (vertices) and $\mathcal{W}$ is the set of undirected edge weights. Assume $|\mathcal{V}| = n$. We note that $w_{ij} \geq 0$ for all $i, j = 1, 2, \ldots, n$ and $w_{ii} = 0$ for all $i = 1, 2, \ldots, n$. We say that (v_i, v_j) is an edge if and only if $w_{ij} > 0$. The leader node in a path graph is denoted by v_ℓ. For simplicity we define the weight of edge (v_i, v_j) by w_j if v_i is closer to the leader node. We denote a weighted directed graph by $\mathcal{G}_d(\mathcal{V}, \mathcal{W})$. We assume only unidirectional edges for the directed graphs, i.e., if there exists a directed edge from v_i to v_j in $\mathcal{G}_d$, then there is no directed edge from v_j to v_i. The adjacency matrix of $\mathcal{G}_d$ is $A_{n\times n}$ where $A_{ij} = w_i$ if and only if there is an edge from v_j to v_i. The *neighbor* nodes of vertex $v_i \in \mathcal{V}$ in $\mathcal{G}_d$ are determined by the set $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid (v_j, v_i) \in \mathcal{G}_d\}$. The in-degree of node v_i (degree for undirected networks) is determined by $d_i = \Sigma_{v_j \in \mathcal{N}_i} A_{ij}$. The Laplacian matrix of a general graph $\mathcal{G}$ is defined as $L = D - A$, where $D = \text{diag}(d_1, \ldots, d_n)$. It is noteworthy that since we consider a general weighted graph, the degree matrix does not measure the number of outgoing and incoming edges, hence, does not only take values from the natural domain. In this paper, we denote a vector which has a one in the i^{th} position and zero elsewhere by $\mathbf{e}_i$.

B. SYSTEM MODELING

Let us consider a string of n connected vehicles in a platoon modeled by a weighted path graph $\mathcal{G}(\mathcal{V}, \mathcal{W})$. The edge weights are to model the communication quality between the vehicles. In practice, different scenarios could occur affecting the quality of data transfer between the vehicles.[1] It is notable that in DSRC-based communications, it is common to normalize the communication perfection of signals versus the sent power or distance. Hence, from a practical point of view, the edge weights used in this paper can be normalized based on the above concepts to let the weight values lie in the $[0, 1]$ range; however, this is out of the scope of this paper. Let p_i denote the position of vehicle v_i. The objective is for each vehicle to maintain a specific distance from its neighbors. The desired vehicle formation will be formed by a specific constant distance Δ_{ij} between vehicles v_i and v_j, which should

[1] For instance, entering the platoon in a long tunnel may degrade the proper data transfer among the vehicles [67]–[70].



(a) Weighted undirected platoon with n vehicles

(b) Weighted directed platoon with n vehicles

FIGURE 1. Undirected and directed platoons with *n* vehicles and sample attackers and monitoring sensors.

satisfy $\Delta_{ij} = \Delta_{ik} + \Delta_{kj}$ for every triple $\{v_i, v_k, v_j\} \subset \mathcal{V}$. Considering the fact that each vehicle v_i has access to its own position, the positions of its neighbors, and the desired inter-vehicular distances Δ_{ij}, the control law for vehicle v_i is [71]

$$\ddot{p}_i(t)=\sum_{j\in\mathcal{N}_i} k_p\left(p_j(t)-p_i(t)+\Delta_{ij}\right)+k_v\left(\dot{p}_j(t)-\dot{p}_i(t)\right)+\zeta_i(t), \tag{1}$$

where $k_p, k_v > 0$ are control gains and $\zeta_i(t)$ models the injected attacks. Physically, this means that the attacker adds a traction acceleration (or brake) to vehicle v_i. Dynamics (1) in matrix form become

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\begin{bmatrix}\mathbf{0}_n & I_n\\ -k_pL_g & -k_vL_g\end{bmatrix}\boldsymbol{x}(t)+\begin{bmatrix}\mathbf{0}_{n\times 1}\\ k_p\Delta\end{bmatrix}+\begin{bmatrix}\mathbf{0}_n\\ B\end{bmatrix}\boldsymbol{\zeta}(t),\\ \boldsymbol{y}(t)=\begin{bmatrix}C & 0\end{bmatrix}\boldsymbol{x}(t),\end{cases} \tag{2}$$

where $\boldsymbol{x} = [\mathbf{P}\ \ \dot{\mathbf{P}}]^\mathsf{T} = [p_1, p_2, \ldots, p_n, \dot{p}_1, \dot{p}_2, \ldots, \dot{p}_n]^\mathsf{T}$, $\Delta = [\Delta_1, \Delta_2, \ldots, \Delta_n]^\mathsf{T}$ in which $\Delta_i = \sum_{j\in\mathcal{N}_i} \Delta_{ij}$. Here L_g is the grounded Laplacian matrix which is the reduced Laplacian matrix by removing the row and the column corresponding to the leader node, $\boldsymbol{y}(t)$ is the sensor measurements vector, and $\boldsymbol{\zeta}(t)$ is the attack vector. Matrices B and C represent the attacker and detector decisions, respectively. For instance, let us consider a specific vehicle platoon with $n = 4$ vehicles subject to cyber attacks shown in Fig. 1. Suppose that the attacker targets vehicles v_1 and v_2 while the detector places its sensors on vehicles v_3 and v_4. This gives $B = \begin{bmatrix}1\ 0\ 0\ 0\\ 0\ 1\ 0\ 0\end{bmatrix}^\mathsf{T}$ and $C = \begin{bmatrix}0\ 0\ 1\ 0\\ 0\ 0\ 0\ 1\end{bmatrix}$. The reason that the positions of vehicles are our output of interest is that we need the vehicles' positions to guarantee the desired inter-vehicular distance in terms of safety of the platoon. These data are available through both GPS and on-board sensors of the vehicles. In order to prevent a possible misconception that might arise due to the usage of the word "sensor" for the defender's action, we state that this is the exact same means to measure the output of the system. Based on (6), the output of the system is the relative position of the vehicles. To measure the position of the ego-vehicle, this quantity can be measured by the sensors mounted on it such as a GPS. To measure the relative position of the other vehicles, different commonly used sensors can be utilized such as radar and Light Detection and Ranging (LIDAR) sensor. An example of undirected and directed platoons of n vehicles subject to two attacks and equipped with two monitoring detectors are shown in Fig. 1.

For the rest of our analysis, we derive a model for the error dynamics of the system (2). Let us denote the desired position of vehicle v_i in steady state by $p_i^*(t)$ and define the following tracking error

$$\tilde{p}_i(t) \triangleq p_i(t) - p_i^*(t). \tag{3}$$

Obviously, the desired formation of the platoon has to satisfy $p_i^*(t) = p_j^*(t) + \Delta_{ij}$ [72]. Substituting (3) in (1) yields

$$\begin{aligned}&\ddot{\tilde{p}}_i(t) + \ddot{p}_i^*(t)\\ &\quad= \sum_{j\in\mathcal{N}_i} k_p\left(\tilde{p}_j(t) + p_j^*(t) - \tilde{p}_i(t) - p_i^*(t) + \Delta_{ij}\right)\\ &\qquad + k_v\left(\dot{\tilde{p}}_j(t) + \dot{p}_j^*(t) - \dot{\tilde{p}}_i(t) - \dot{p}_i^*(t)\right) + \zeta_i(t),\end{aligned} \tag{4}$$

Now respecting the fact that in the steady state formation the vehicles' velocities have to be equal, we observe that $\dot{p}_i^*(t) - \dot{p}_j^*(t) = 0$. Furthermore, in the steady state formation the vehicles' velocities reach constant values which results in $\ddot{p}_i^*(t) = 0$. Hence, (4) is reduced to the following error dynamics model

$$\ddot{\tilde{p}}_i(t) = \sum_{j\in\mathcal{N}_i} k_p(\tilde{p}_j(t) - \tilde{p}_i(t)) + k_v\left(\dot{\tilde{p}}_j(t) - \dot{\tilde{p}}_i(t)\right) + \zeta_i(t), \tag{5}$$

The above error dynamics can be written in the matrix form as follows

$$\begin{cases}\dot{\tilde{\boldsymbol{x}}}(t) = \begin{bmatrix}\mathbf{0}_n & I_n\\ -k_pL_g & -k_vL_g\end{bmatrix}\tilde{\boldsymbol{x}}(t) + \begin{bmatrix}\mathbf{0}_n\\ B\end{bmatrix}\boldsymbol{\zeta}(t),\\ \tilde{\boldsymbol{y}}(t) = \begin{bmatrix}C & 0\end{bmatrix}\tilde{\boldsymbol{x}}(t),\end{cases} \tag{6}$$

where $\tilde{\boldsymbol{x}} = [\tilde{\mathbf{P}}\ \ \dot{\tilde{\mathbf{P}}}]^\mathsf{T} = [\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_n, \dot{\tilde{p}}_1, \dot{\tilde{p}}_2, \ldots, \dot{\tilde{p}}_n]^\mathsf{T}$ and the other variables are the same as in (2).

C. ATTACK MODELING: BIAS INJECTION ATTACKS

For our particular application under study, i.e., vehicle platooning, we assume that the attacker does not inject a high frequency signal to the system. In fact, due to the large inertia of the vehicles, the attacker can not change the vehicle's acceleration abruptly. Hence, a high frequency attack signal which targets at changing the vehicle's acceleration can be immediately detected through receiving the information from the surrounding vehicles. Based on this fact, we consider a slowly time varying attack signal, namely a *bias injection attack*. Consequently, the L_2-gain of the system which equals the $\mathcal{H}_\infty$-norm of the system [73] can be calculated at the zero frequency.

Based on (6), the following proposition, formulates the system L_2-gain from the attack vector $\boldsymbol{\zeta}(t)$ to the output measurements vector $\tilde{\mathbf{y}}(t)$.

Proposition 1: The system L_2-gain from the attack vector $\boldsymbol{\zeta}(t)$ to the output measurements vector $\tilde{\mathbf{y}}(t)$ of (6) is as follows

$$\sup_{\|\boldsymbol{\zeta}(t)\|_2 \neq 0} \frac{\|\tilde{\mathbf{y}}(t)\|_2}{\|\boldsymbol{\zeta}(t)\|_2} = \sigma_{\max}(G(0)) = \sigma_{\max}\left(\frac{1}{k_p} C L_g^{-1} B\right), \tag{7}$$

where $\sigma_{\max}$ is the maximum singular value and the L_2-norm of a signal $\boldsymbol{x}$ is $\|\boldsymbol{x}\|_2^2 \triangleq \int_0^\infty \boldsymbol{x}^\mathsf{T} \boldsymbol{x} dt$. □

Proof: Taking the Laplace transform from the second row of (6) yields

$$s^2 \tilde{P}(s) = -k_p L_g \tilde{P}(s) - s k_v L_g \tilde{P}(s) + B Z(s), \tag{8}$$

where $\tilde{P}(s)$ and $Z(s)$ are the Laplace transform of $\tilde{\mathbf{P}}$ and $\boldsymbol{\zeta}(t)$, respectively. Moreover, taking the Laplace transform from the second equation of (6) gives

$$\tilde{Y}(s) = C\tilde{P}(s) = \underbrace{C\left(s^2 I + (k_p + s k_v) L_g\right)^{-1} B}_{G(s)} Z(s), \tag{9}$$

which completes the proof. ■

We define an attacker-detector game as follows. The attacker chooses f vehicles to attack such that L_2-gain from attack signal to monitoring nodes is minimized. On the other hand the detector chooses f vehicles to monitor such that L_2-gain from attack signal to monitoring nodes is maximized.

Remark 1: It is common in the literature that the defender (here detector) knows an upper bound of the attacked nodes [74]. Here, we assume that f is an upper bound of the attacked nodes, and hence, the detector acts based on this worst-case scenario. □

Based on Proposition 1, the cost function that the attacker tries to minimize and the detector tries to maximize is defined as follows

$$J(B, C) = \sigma_{\max}(G(0)) = \frac{1}{k_p} \sigma_{\max}\left(C L_g^{-1} B\right). \tag{10}$$

It is proved in the literature that when the graph $\mathcal{G}$ is connected (which holds for a platoon that is a line graph), then L_g is nonsingular and L_g^{-1} is nonegative elementwise [75].

Remark 2: The proposed approach in this paper is basically considered as a centralized one. In particular, as in (10), the global knowledge of the variables of the Laplacian matrix need to be known for the game pay-off to be fully defined. The elements of L_g^{-1} are determined based on the special form of this matrix according to the exploited information flow topology. This will be explained in Lemma 2 and 3. □

The following lemma will be needed in the subsequent attacker-detector game analyses.

Lemma 1 ([76]): For a non-negative matrix, A, the largest singular value is a non-decreasing function of its elements. Besides, if A is irreducible, then the largest singular value is a strictly increasing function of its entries. □

III. SINGLE ATTACKED–SINGLE DETECTING VEHICLES

In this section, we investigate the existence of an equilibrium point of the attacker-detector game in both undirected and directed cases where there is only one attacked node. To this end, we first present explicit representations of L_g^{-1} for both of these scenarios in the two following lemmas, respectively. The proof of these results are presented in the Appendix.

Lemma 2: Suppose that $\mathcal{G}_u$ is a weighted undirected path graph and let $\mathcal{P}_{i\ell}$ be the set of nodes involved in the (unique) path from the leader node v_ℓ to v_i (including v_i). Then we have

$$[L_g^{-1}]_{ij} = \sum_{\ell \in \mathcal{P}_{i\ell} \cap \mathcal{P}_{j\ell}} \frac{1}{w_\ell}. \tag{11}$$

□

Lemma 3: Suppose that $\mathcal{G}_d$ is a weighted directed path graph with the leader node v_ℓ. Then, the entries of the matrix L_g^{-1} are given by

$$[L_g^{-1}]_{ij} = \begin{cases} \dfrac{1}{w_j} & \textit{if there is a directed path from } j \textit{ to } i, \\ 0 & \textit{if there is no directed path from } j \textit{ to } i. \end{cases} \tag{12}$$

□

Remark 3: In case $f = 1$ where the attacker attacks node j and the detector places its sensor on node i, i.e., $B = \mathbf{e}_j$ and $C = \mathbf{e}_i^\mathsf{T}$ for some $1 \leq i, j \leq n$, the game pay-off is reduced to the following simple form

$$\sigma_{\max}\left(\frac{1}{k_p} C L_g^{-1} B\right) = \sigma_{\max}\left(\frac{1}{k_p} \mathbf{e}_i^\mathsf{T} L_g^{-1} \mathbf{e}_j\right) = \frac{1}{k_p} [L_g^{-1}]_{ij}, \tag{13}$$

where $[L_g^{-1}]_{ij}$ is the ij^{th} element of L_g^{-1}. □

The following result presents the existence of an equilibrium point in a weighted undirected path graph.

Theorem 1: Let $\mathcal{G}_u$ be a weighted undirected path graph with v_ℓ as the leader node in one end of the graph. Assume that the weight of an incoming edge from v_ℓ to node i is w_i. The game between the attacker and the detector has at least one NE and the game value is $\frac{1}{w_1}$ where w_1 is the weight of the incoming edge to the leader's neighbor node v_1. □

Proof: The NE pertains to the scenario in which the attacker attacks the leader's neighbor node. This fact is easily derived based on Lemma 2. In fact, the attacker tries to minimize the game objective by attacking the nearest node to the leader so as to regardless of the detection node, the number of common nodes from the leader to the attacked and defended nodes is minimized (which will be 1 in this case). Hence, regardless of the detector's action, the game admits at least one NE with the same game value, i.e., $\frac{1}{w_1}$ where node 1 is the leader's neighbor. Besides, if the attacker chooses any other nodes, the game pay-off will be at least $\frac{1}{w_1}$. ■

Remark 4: In Theorem 1, one of the NEs happens where the detector places its sensor on the farthest node from the leader. This is a particular case on which we will focus in the rest of the paper. □

The following result presents the existence of an equilibrium point in a platoon equipped with directed communication links modeled by a weighted directed path graph.

Theorem 2: Let $\mathcal{G}_d$ be a weighted directed path graph with v_ℓ as the leader node in one end of the graph. Assume that the weight of an incoming edge from v_ℓ to node i is w_i. Then, the game between the attacker and the detector admits an NE in node $v_k = \arg\max_{i\in\mathcal{W}} w_i$. □

Proof: Without loss of generality, let us denote the ordering of the nodes starting from the leader and ending at the end of the platoon by $v_\ell, v_1, v_2, \ldots, v_n$. Having in mind that in the case of a directed graph, L_g^{-1} is a lower-triangular matrix, we try to find the equilibrium point of the attacker-detector game. We know that, based on Lemma 3, the last row of L_g^{-1} is $[L_g^{-1}]_{n,1\leq j\leq n} = \begin{bmatrix}\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_n}\end{bmatrix}$. One can perceive that for the detector to maximize the game objective, he definitely chooses the last row of L_g^{-1} to assure there is no zero entry in the chosen row. On the other hand, the attacker has no other way except choosing the minimum entry of the aforementioned row. This entry corresponds to the node with the maximum incoming weight which completes the proof. ■

IV. ATTACKER–DETECTOR GAME: $f > 1$ CASE

Due to the availability of redundant on-board sensors on most of the vehicles from one hand, and that the attacker typically tends to attack more than one vehicle of the platoon to achieve a higher level of devastation from the other hand, it is more crucial for the detector to benefit from the sensor redundancy and be prepared for such attacks. In these attacks, the attacker targets more than one vehicle, and the detector is supposed to deploy more than one monitoring sensor. Hence, we extend our previous results and analyze the existence of an equilibrium point of the attacker-detector game in both undirected and directed cases where there are more than one attacked nodes.

The following result presents the existence of an equilibrium point in a weighted undirected path graph with multiple attacked nodes and multiple deployed sensors.

Theorem 3: Let $\mathcal{G}_u$ be a weighted undirected path graph with v_ℓ as the leader node in one end of the path. Then for any $f > 1$, the attacker-detector game described by the game payoff (10) admits at least one NE happening when the attacker chooses f closest nodes to the leader and the detector chooses f farthest nodes from the leader. □

Proof: The structure of L_g^{-1} for a general undirected path graph shown in Fig. 1a, is as follows

$$L_g^{-1} = \begin{bmatrix} \frac{1}{w_1} & \frac{1}{w_1} & \cdots & \frac{1}{w_1} \\ \frac{1}{w_1} & \frac{1}{w_1}+\frac{1}{w_2} & \cdots & \frac{1}{w_1}+\frac{1}{w_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{w_1} & \frac{1}{w_1}+\frac{1}{w_2} & \cdots & \frac{1}{w_1}+\frac{1}{w_2}+\ldots+\frac{1}{w_n} \end{bmatrix} \tag{14}$$

Based on the specific structure of (14), i.e., the entries monotonically increase as we go further in rows/columns, the NE occurs when the attacker chooses the first f columns of L_g^{-1} and the detector chooses the last f rows of it. Denoting the so-called columns and rows by B^* and C^*, respectively, based on Lemma 1, one can easily see that (we omit the coefficient $\frac{1}{k_p}$ for convenience)

$$\sigma_{\max}(CL_g^{-1}B^*) \leq \sigma_{\max}(C^*L_g^{-1}B^*) \leq \sigma_{\max}(C^*L_g^{-1}B), \tag{15}$$

where, B and C are any combination of f columns and rows of L_g^{-1}, respectively. If the attacker chooses columns corresponding to B (instead of B^*), then the elements of $C^*L_g^{-1}B$ increase (compared to $C^*L_g^{-1}B^*$) which in turn results in increasing $\sigma_{\max}(C^*L_g^{-1}B)$ (based on Lemma 1). Furthermore, if $n \leq 2f$, then any unilateral deviation of the detector's decision decreases $\sigma_{\max}(CL_g^{-1}B^*)$. In the case where $n > 2f$, the unilateral deviation of the detector's decision may not change the elements of $CL_g^{-1}B^*$ which results in more than one NE with the same game value. ■

The following theorem represents the existence of an equilibrium point in a weighted directed path graph with $f > 1$ attacked nodes and $f > 1$ deployed sensors.

Theorem 4: Let $\mathcal{G}_d$ be a weighted directed path graph with v_ℓ as the leader node in one end of the path. Then for any $f > 1$, the attacker-detector game (7) admits an NE happening when the detector chooses f farthest nodes from the leader. □

Proof: The structure of L_g^{-1} for a general directed platoon shown in Fig. 1b, is as follows

$$L_g^{-1} = \begin{bmatrix} \frac{1}{w_1} & 0 & \cdots & 0 \\ \frac{1}{w_1} & \frac{1}{w_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_n} \end{bmatrix} \tag{16}$$

Based on the lower-triangular structure of (16), the game admits an NE when the detector chooses the last f rows of L_g^{-1}. Moreover, the attacker's decision is highly sensitive to the weight assignments. Particularly, based on the values of w_i, $1 \leq i \leq n$, the attacker has to solve a minimization problem to achieve the least value for the game value corresponding to his strategy. Different scenarios for this decision making will be explained in Sec. VII. ■

Remark 5 (Computational cost of the attacker): In a general weighted directed platoon where there are more than one attacked nodes, the attacker's decision is highly sensitive to weight assignments since the attacker has to solve a computationally complex optimization problem. Particularly, he has to calculate the game value for every combination of selecting f columns out of n columns of the Laplacian matrix. Mathematically, the cost of this computation is evaluating the maximum singular value of the resulting $f \times f$ matrix for *every $\binom{n}{f}$ selections. Depending on the values of f and n, this computation can be of high burden.* □

V. EFFECTS OF ADDING EXTRA COMMUNICATION LINKS TO A PLATOON

In real vehicle platoons, it might be the case that additional communication links either undirected or directed are added between the vehicles. This will clearly affect the existing communication environment between the vehicles and the security level of the new platoon. Hence, in this section, we discuss the impact of adding extra links to a path graph on the security level of the resulting graph in both undirected and directed cases.

A. UNDIRECTED CASE

We consider the general scenario in which an extra edge with weight w_i (modeling the added communication link) is added from node j to node i. In the undirected case, this extension can be generally formulated as follows

$$\tilde{L}_g = L_g + w_i \mathbf{e}_{ij}\mathbf{e}_{ij}^{\mathsf{T}}, \tag{17}$$

where, $\tilde{L}_g$ is the perturbed Laplacian matrix corresponding to the new graph, $\mathbf{e}_{ij} = \mathbf{e}_i - \mathbf{e}_j$, and $\mathbf{e}_i$ is a vector with 1 in the i^{th} position and 0 elsewhere. The following result presents the effect of adding an extra communication link between two nodes of vehicle platoon on its security level. The proof of the following theorem is presented in the Appendix.

Theorem 5: Let $\mathcal{G}_u$ denote a weighted undirected path graph. Then, adding an extra edge to $\mathcal{G}_u$ will decrease the game value. □

Theorem 5 indicates that adding new communication links to a platoon equipped by bidirectional communication links between the vehicles lessens the detectability (visibility) of the attack. In fact, the attack signal finds more ways to be distributed through the new links which in turn reduces its power (energy). Consequently, the attack becomes less visible and more difficult to be detected, creating a less secure platoon.

B. DIRECTED CASE

In the directed case, this extension can be generally formulated as follows

$$\tilde{L}_g = L_g + w_i \mathbf{e}_i\mathbf{e}_{ij}^{\mathsf{T}}, \tag{18}$$

Theorem 6: Let $\mathcal{G}_d$ denote a weighted directed path graph. Then, adding an extra edge to $\mathcal{G}_d$ which makes a cycle will increase the game value and adding an extra edge to $\mathcal{G}_d$ which does not make a cycle will decrease the game value. □

Proof: The proof will be given in the Appendix. ■

Remark 6: The results of this section make real sense from a practical point of view. Particularly, in a platoon equipped by unidirectional communication links (the directed case), when the extra link is added between two vehicles creating a cycle, this data flow cycle is created in which the attack signal is circulated and becomes more visible (detectable). It is worth noting that as this is a directed flow path, there is no power loss for the attacker while it is circulating. Hence, the game value, i.e., the detectability of the attacker increases. In the case where no cycle is made, there is no data flow path created for the attack to be propagated. This physically dampens the attack effect. Thus, the attacker becomes less visible in the new platoon, and naturally, the game value is decreased. The same reasoning holds for the undirected case. □

VI. SECURITY LEVEL OF A PLATOON WITH BIDIRECTIONAL VERSUS UNIDIRECTIONAL COMMUNICATION LINKS

In this section we briefly study the security level of a platoon equipped by either a bidirectional or unidirectional communication links. The following proposition establishes the result.

Proposition 2: Let $\mathcal{G}_u$ and $\mathcal{G}_d$ denote a weighted undirected and directed vehicle platoon, respectively. The game value corresponding to the attacker-detector game of the undirected platoon is larger than the directed one, hence, is more secure. □

Proof: Let us first consider the $f = 1$ case. Based on the general structure of L_g^{-1} for the undirected and directed cases given in (14) and (16), respectively, one can easily see that each element of (16) is not larger than the corresponding element of (14). This is basically due to the way that these matrices are formed based on Lemma 2 and Lemma 3. Now let us consider the $f > 1$ case. With the same argument, we can immediately perceive that all the elements of the $f \times f$ matrix $\left(CL_g^{-1}B\right)_{\text{directed}}$ are not larger than the corresponding elements of $\left(CL_g^{-1}B\right)_{\text{undirected}}$ for any attacker and detector decisions. This together with Lemma 1 complete the proof. ■

This result verifies that when a platoon is equipped by bidirectional communication links among the vehicles (the undirected case), each vehicle can send and receive more data from its both follower and preceding vehicles. This clearly causes a more secure platoon. In the directed case, i.e., the communication links are of the unidirectional type, each vehicle is only able to receive data from its preceding vehicle, hence, the detectability of the attacker might not be maximized compared to the undirected case. Hence, the security level of the latter platoon is lower than the first one.

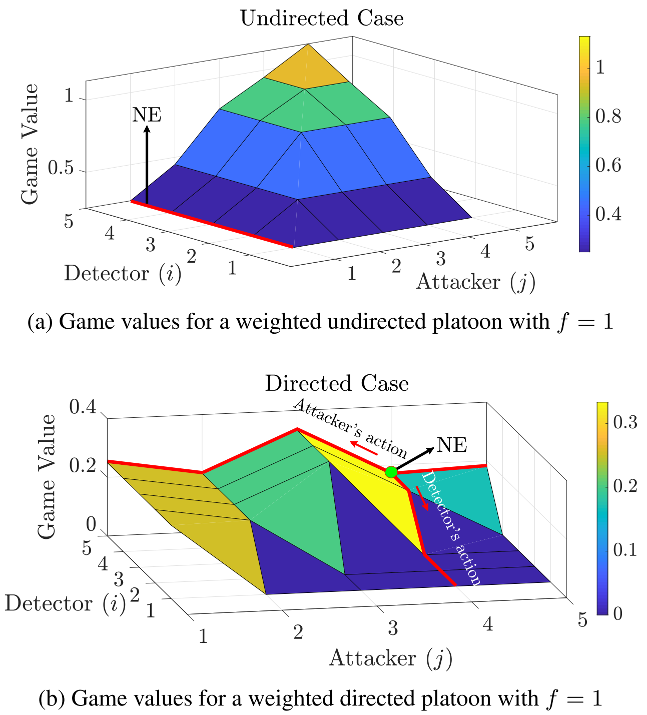
VII. SIMULATION AND EXPERIMENTAL RESULTS

A. SIMULATION RESULTS

Here, the application of the aforementioned results in a vehicle platoon subject to bias injection attacks in two different cases namely, undirected and directed platoons is investigated. In the considered platoon, we place the leader at one end of the path and keep the same labeling policy for the vehicles as before.

1) $f = 1$ CASE

In this case, we consider a weighted platoon formation in which the attacker attacks one vehicle and the detector places



(a) Game values for a weighted undirected platoon with $f = 1$

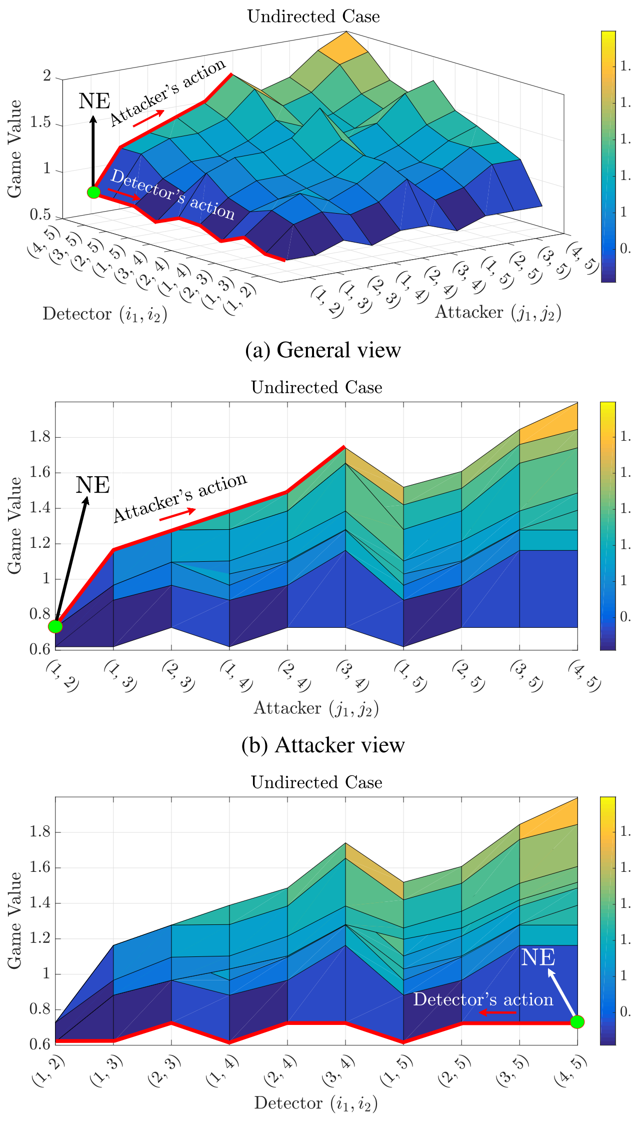
(b) Game values for a weighted directed platoon with $f = 1$

FIGURE 2. **Game values and NE for weighted undirected and directed platoons for $f = 1$.**

one sensor on a specified vehicle. This sensor placement has to be optimized based on NE of the attacker-detector game. We consider a platoon with 5 vehicles. The weights have been chosen as, $w_1 = 2, w_2 = 2.5, w_3 = 1.5, w_4 = 3$, and $w_5 = 2.75$. Fig. 2 shows the game values for both the undirected and directed cases where $f = 1$. For the undirected case (Fig. 2a), based on Theorem 1, the game has non-unique NEs happening in the leader's neighbor vehicle regardless of the detector's action. For the directed case (Fig. 2b), based on Theorem 2, the game has a unique NE in the vehicle with maximum incoming weight, which is w_4. From Fig. 2, one can easily see that in both undirected and directed cases, if the attacker chooses a vehicle other than the shown NE, the game value increases. Besides, if the detector chooses a vehicle other than the shown NE(s), the game value decreases. Hence, neither the attacker nor the detector are willing to change their strategies.

2) $f > 1$ CASE

In this case, we consider a similar platoon with 5 vehicles as in the previous case, and $f = 2$. The weights w_1 through w_5 are the same as before. In this case, the attacker attacks a pair of vehicles (j_1, j_2) and the detector places its sensors on a pair of vehicles (i_1, i_2). Fig. 3 shows the game values for the undirected case where $f = 2$. According to Theorem 3, the game admits at least one NE where the attacker attacks 2 closest vehicles to the leader, and the detector chooses the 2 farthest vehicles from the leader. In this case, since $n > 2f$, the game has non-unique NEs. These NEs occur when the attacker attacks 2 closest vehicles to the leader while the



(a) General view

(b) Attacker view

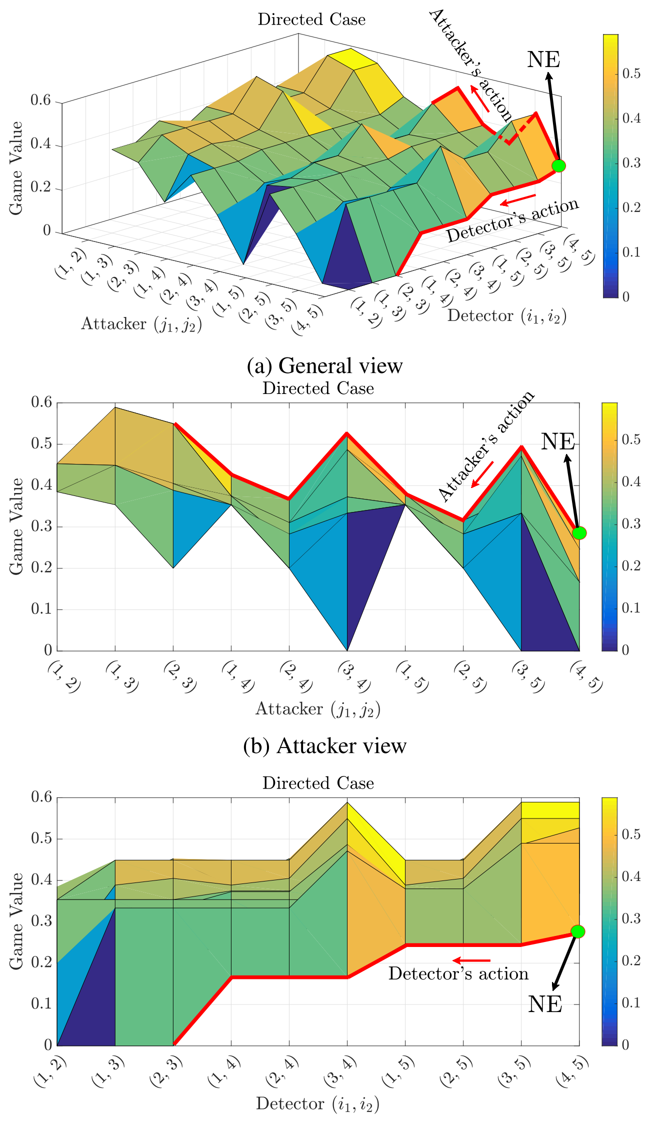
(c) Detector view

FIGURE 3. **Game values and NE for a weighted undirected platoon with 5 vehicles and $f = 2$.**

detector can choose any pair of vehicles such that they do not include the leader's neighbor vehicle. Fig. 3 shows one specific NE where the attacker attacks the pair (1, 2) (two closest vehicles to the leader) and the detector chooses the two farthest vehicles from the leader, which is the pair (4, 5). It is easily seen that neither the attacker nor the detector are willing to change their actions.

In the directed scenario, based on Theorem 4, there exists an NE which happens when the detector places two sensors in the farthest vehicles from the leader. Fig. 4 shows the game values for this scenario in which the game admits an NE where both the attacker and the detector choose the 2 farthest vehicles from the leader.

For the directed case, we present the following example showing that the attacker's decision is highly sensitive to weight assignments.



(a) General view

(b) Attacker view

(c) Detector view

FIGURE 4. Game values and NE for a weighted directed platoon with 5 vehicles and $f = 2$.

Example 1: Consider the weighted directed platoon shown in Fig. 1b with $n = 5$ vehicles, $f = 2$, and the following weights, $w_1 = 2000$, $w_2 = 0.1$, $w_3 = 0.05$, $w_4 = 0.1$, and $w_5 = 0.01$. Based on Theorem 4, there exists an NE where the detector chooses the 2 farthest vehicles from the leader. Fig. 5 shows the game value for this example. In this specific platoon, one can easily see that the game admits an NE which happens when the attacker attacks the 2 closest vehicles to the leader. Based on the lower-triangular structure of the Laplacian matrix, although there exists a zero element in the fifth column of L_g^{-1}, the attacker is willing to choose the first two columns (not choosing the fifth one at all) to achieve a lower game value. This example clearly verifies the high dependency of the attacker's decision on the weight assignments. □

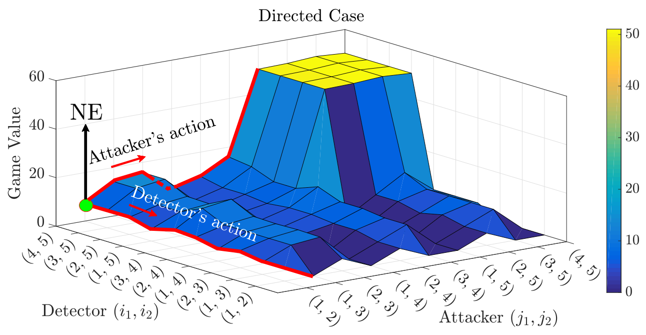


FIGURE 5. Game values for the specific weighted directed platoon in Example 1.

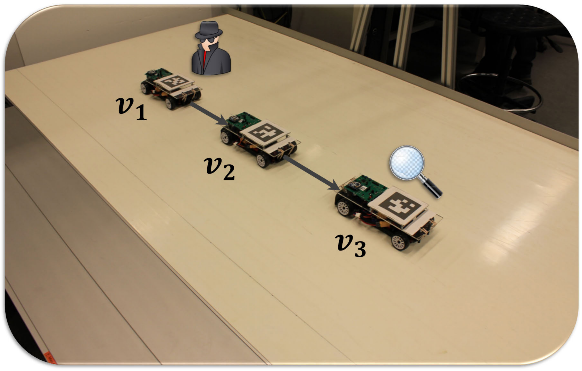


FIGURE 6. Vehicle platoon experimental setup.

B. EXPERIMENTAL RESULTS

We have conducted experimental tests on a vehicle platoon setup operated by Robotic Operating System (ROS).

1) EXPERIMENTAL SETUP CONFIGURATION

The setup is consisted of 3 vehicles driving on a treadmill (see Fig. 6). The vehicles' positions are captured by a central infrared camera detecting the specific Apriltags mounted on the vehicles. Here we consider a virtual leader specifying a desired speed profile, generated by the host PC, with 3 followers that have to follow this common profile. Each of the vehicles is equipped by a cascaded PID controller which commands the vehicle to follow the leader's speed profile and keep the desired safe distance with its preceding vehicle. The control signals are commanded based on the received data from the central ROS run on the host PC. In this setup, the data transfer between the vehicles is of directed predecessor-follower type, i.e., each vehicle can receive data from its predecessor. The data is exchanged between the host PC running the ROS and the vehicles through an IEEE 802.15.4-based 2.4GHz ZigBee wireless network protocol (see Fig. 7). The position, linear and angular velocity, steering and the throttle of the vehicles are measured in real-time via the ROS. Two different attack scenarios, namely an acceleration-brake attack and a brake-acceleration attack will be generated, and the results confirming our theoretical analyses will be demonstrated. It is noteworthy that our experimental results are in

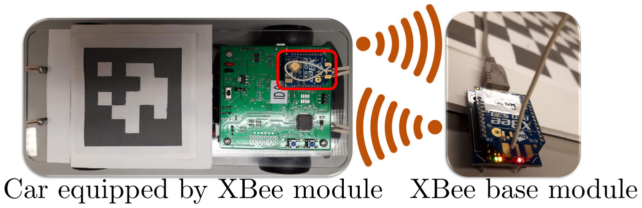


FIGURE 7. XBee network connection.

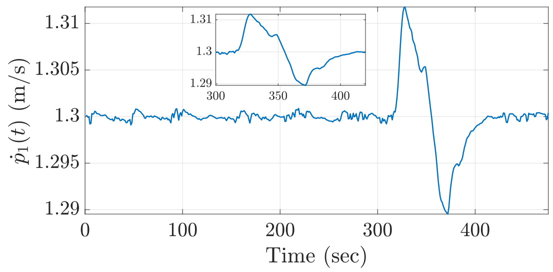
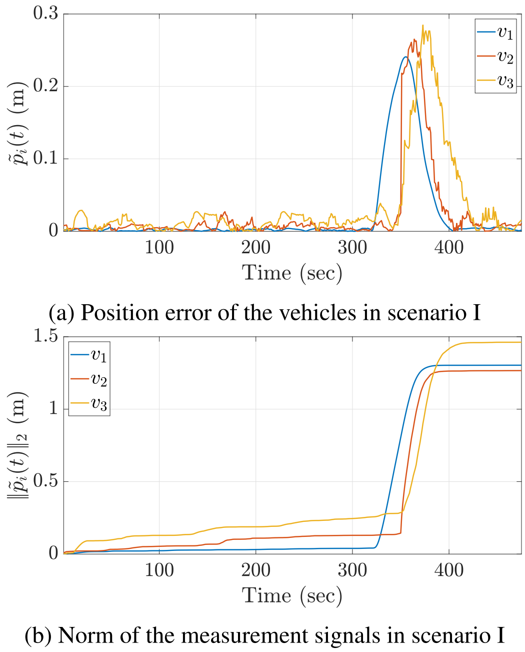


FIGURE 8. Velocity of the attacked car in scenario I.



(a) Position error of the vehicles in scenario I

(b) Norm of the measurement signals in scenario I

FIGURE 9. Position error and norm of the measurement signals of the follower vehicles in scenario I.

line with the string stability notion in vehicle platoons as well [77].

2) ATTACK SCENARIO I (ACCELERATION–BRAKE ATTACK)

In this experiment, we attack the first follower (vehicle v_1) by an acceleration followed by a brake (see Fig. 8). Hence, at the beginning, this vehicle accelerates forward and gets far from its desired position and then gets back to its original position. Subsequently, the other two followers have to accelerate first and then brake to keep the desired inter-vehicular distance among the platoon. Fig. 9 demonstrates the position error and the 2-norm of error signals for the followers. From Fig. 9a, it is obviously seen that the attack effect has been propagated through the upstream of the platoon with a time delay. Fig. 9b shows that the norm of the error signal of the last follower will eventually get the highest value in a finite time. As the norm of the attack signal is a fixed value, based on Proposition 1, the game value (detectability of the attacker) will get the highest value if the last vehicle in the platoon is monitored. Hence, the detector has to place his monitoring sensor on the last follower to increase the security level of the system. This clearly confirms our result for the detector strategy presented in Theorem 2.

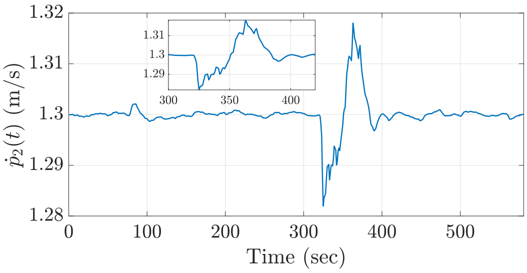
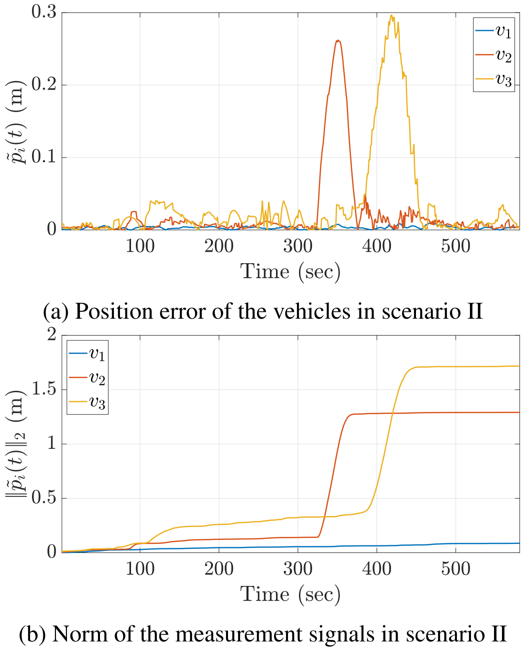


FIGURE 10. Velocity of the attacked car in scenario II.



(a) Position error of the vehicles in scenario II

(b) Norm of the measurement signals in scenario II

FIGURE 11. Position error and norm of the measurement signals of the follower vehicles in scenario II.

3) ATTACK SCENARIO II (BRAKE–ACCELERATION ATTACK)

In this scenario, we attack the second follower (vehicle v_2) by forcing it to have a brake followed by an acceleration (see Fig. 10). In a real platoon, this kind of attack could be of high significance as it can result in severe braking of the other followers resulting in a huge degradation of the driving comfort and safety. Fig. 11 shows the position error and the 2-norm of the error signals for the vehicles. As it can be seen from Fig. 11a, due to the unidirectional data transfer in the platoon, the attack occurred on v_2 does not affect v_1. Again the effect of the attack on v_2 propagates to v_3 with a short time delay. From Fig. 11b, similar to the first scenario, the detectability of the attacker is maximized if the detector places its sensor on the last follower which again verifies our previous theoretical results.

Remark 7: We can see from Fig. 8 and 10 that the attacks occurred in about 100 and 80 seconds in scenario I and II, respectively. Having been approximated the acceleration followed by a brake in scenario I (and the brake followed by an acceleration in scenario II) with a sinusoidal signal, they reflect approximately 0.01 – 0.02 Hz attacks. Hence, they can be reasonably captured as the low-frequency attacks. □

Remark 8: It is worth mentioning that according to our analytical results (Theorem 2), in a weighted directed platoon, the optimal strategy for the detector is to choose the farthest vehicle from the leader to place the monitoring sensor. Since in our experimental results the quality of the communication links among the vehicles are the same (the weights are all equal), the game admits more than one NE with the same game pay-off regardless of the attacker's action. This was the situation in the scenario I and II where different vehicles of the platoon were attacked. □

VIII. CONCLUSION AND FUTURE WORK

In this research, we have focused on security and robustness analysis of vehicle platoons based on a graph-theoretic approach. The vehicles have been assumed to be able to communicate data, such as inter-vehicular distance and speed among each other via wireless communication environments. Both the unidirectional and bidirectional data transfer have been studied. Moreover, the quality of communication links between the vehicles has been considered using edge weights of the underlying path graph topology. The platoon is assumed to be under cyber attacks, and a detector is supposed to choose a strategy to place his monitoring sensors on specific vehicles aiming at increasing the detectability of the attacker. An attacker-detector game has been defined based on which the existence of any possible NE points have been studied. Based on our results, the detector can decide about his sensor placement strategy to increase the security level of the system. Also, robustness analysis of a platoon against adding extra communication links between the vehicles has performed. Furthermore, our study verifies the fact that using a bidirectional communication environment forms a more secure platoon compared to the unidirectional counterpart. Our simulation and experimental results verified the effectiveness of our theoretical analyses. An open avenue for the current research is to extend the underlying graph topology such that it can handle dynamic platoon formations resulted from different vehicle maneuvers such as cut-in/cut-out actions, hence, studying the impacts of those movements on the security of vehicle platooning. Besides, the extension of this work to the dynamic game (with changing network topology) along with generalizing our method for possibly different vehicle dynamics in the platoon referred to as the "heterogeneous" case are left as our future studies.

APPENDIXES

APPENDIX A

PROOF OF LEMMA 2

Before proving Lemma 2 we need the following preliminary definition.

Definition 1 ([50]): A spanning subgraph of a graph $\mathcal{G}$ is called a 2-tree of $\mathcal{G}$, if and only if, it has two components each of which is a tree. In other words, a 2-tree of $\mathcal{G}$ consists of two trees with disjoint vertices which together span $\mathcal{G}$. One (or both) of the components may consist of an isolated node. We refer to $t_{ab,cd}$ as a 2-tree where vertices a and b are in one component of the 2-tree, and vertices c and d in the other. □

Based on the above definition, we prove Lemma 2.

Proof: The proof is based on the fact that $[L_g^{-1}]_{ij} = \frac{cof(L_g)_{ij,\ell,\ell}}{det(L_g)}$. Thus, it is sufficient to provide graph-theoretic definitions of the nominator and denominator of this fraction. For the denominator, based on the generalization of matrix tree theorem for weighted graphs, we have

$$det(L_g) = \prod_{i \in \mathcal{W}} w_i. \tag{19}$$

Moreover, for the nominator, the cofactor is equal to the sum of the impedance product of all 2-trees $t_{ij,\ell}$. Let us denote the set of edges in the path between nodes i and j by $\mathcal{R}_{ij}$. This path is unique since the graph is a tree. Defining $\mathcal{R}_{ij} = \{\mathcal{R}_{i\ell} \cup \mathcal{R}_{j\ell}\} \setminus \{\mathcal{R}_{i\ell} \cap \mathcal{R}_{j\ell}\}$ and $\pi_{\mathcal{R}} = \prod_{i \in \mathcal{R}_{ij}}$, we can write

$$\begin{aligned} &cof(L_g)_{ij,\ell,\ell} \\ &\;= \pi_{\mathcal{R}} w_2 w_3 \dots w_{|\mathcal{R}_{i\ell} \cap \mathcal{R}_{i\ell}|} \\ &\quad + \pi_{\mathcal{R}} w_1 w_3 \dots w_{|\mathcal{R}_{i\ell} \cap \mathcal{R}_{i\ell}|} \pi_{\mathcal{R}} w_1 w_2 w_4 \dots w_{|\mathcal{R}_{i\ell} \cap \mathcal{R}_{i\ell}|} + \dots \\ &\quad + \pi_{\mathcal{R}} w_2 \dots w_{|\mathcal{R}_{i\ell} \cap \mathcal{R}_{i\ell}|-1}. \end{aligned} \tag{20}$$

By dividing (20) by $det(L_g)$ from (19) the result will be obtained. ■

APPENDIX B

PROOF OF LEMMA 3

Proof: Due to the triangular structure of L_g and L_g^{-1}, we can obtain the elements of L_g^{-1} by solving each row of $L_g^{-1} L_g = I$ in a recursive manner and the elements of L_g^{-1} will be obtained. ■

APPENDIX C

PROOF OF THEOREM 5

Proof: Without loss of generality, we denote the ordering of the nodes in the path starting from the leader to the end of the path by $v_\ell, v_1, v_2, \dots, v_j, \dots, v_i, \dots, v_n$. For the case that an extra edge is added between nodes j and i, using Sherman-Morrison formula [78] and (17) results in

$$\tilde{L}_g^{-1} = L_g^{-1} - \frac{w_i L_g^{-1} \mathbf{e}_{ij} \mathbf{e}_{ij}^{\mathsf{T}} L_g^{-1}}{1 + w_i \mathbf{e}_{ij}^{\mathsf{T}} L_g^{-1} \mathbf{e}_{ij}}. \tag{21}$$

$$
\begin{aligned}
L_g^{-1}\mathbf{e}_i\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1} &= \begin{bmatrix}
\frac{1}{w_1} & 0 & \cdots & \overbrace{0}^{j^{\text{th}}} & \cdots & \overbrace{0}^{i^{\text{th}}} & \cdots & 0 \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_j} & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_j} & \cdots & \frac{1}{w_i} & \cdots & 0 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_j} & \cdots & \frac{1}{w_i} & \cdots & \frac{1}{w_n}
\end{bmatrix} \\
&\quad \times \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ \underbrace{1}_{i^{\text{th}}} \\ \vdots \\ 0 \end{bmatrix}
\begin{bmatrix} 0 \\ 0 \\ \vdots \\ \underbrace{-1}_{j^{\text{th}}} \\ \vdots \\ \underbrace{1}_{i^{\text{th}}} \\ \vdots \\ 0 \end{bmatrix}^{\mathsf{T}}
\begin{bmatrix}
\frac{1}{w_1} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_j} & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_j} & \cdots & \frac{1}{w_i} & \cdots & 0 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_j} & \cdots & \frac{1}{w_i} & \cdots & \frac{1}{w_n}
\end{bmatrix} \\
&= \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ \underbrace{\frac{1}{w_i}}_{i^{\text{th}}} \\ \vdots \\ \frac{1}{w_i} \end{bmatrix}
\begin{bmatrix} 0 & \cdots & \underbrace{0}_{j^{\text{th}}} & \frac{1}{w_{j+1}} & \frac{1}{w_{j+2}} & \cdots & \underbrace{\frac{1}{w_i}}_{i^{\text{th}}} & 0 & \cdots & 0 \end{bmatrix} \\
&= \begin{bmatrix}
0 & 0 & \cdots & \overbrace{0}^{j^{\text{th}}} & \overbrace{0}^{j+1^{\text{th}}} & \overbrace{0}^{j+2^{\text{th}}} & \cdots & \overbrace{0}^{i^{\text{th}}} & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots \\
0 & 0 & \cdots & 0 & \frac{1}{w_i w_{j+1}} & \frac{1}{w_i w_{j+2}} & \cdots & \frac{1}{w_i^2} & \cdots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots \\
0 & 0 & \cdots & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0
\end{bmatrix} \geq 0 \qquad (24)
\end{aligned}
$$

Now we have

$$L_g^{-1}\mathbf{e}_{ij}\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1}=\begin{bmatrix}[L_g^{-1}]_{1i}-[L_g^{-1}]_{1j}\\ [L_g^{-1}]_{2i}-[L_g^{-1}]_{2j}\\ \vdots\\ [L_g^{-1}]_{ni}-[L_g^{-1}]_{nj}\end{bmatrix}\begin{bmatrix}[L_g^{-1}]_{i1}-[L_g^{-1}]_{j1}\\ [L_g^{-1}]_{i2}-[L_g^{-1}]_{j2}\\ \vdots\\ [L_g^{-1}]_{in}-[L_g^{-1}]_{jn}\end{bmatrix}^{\mathsf{T}} \tag{22}$$

where $\mathbf{e}_{ij} = \mathbf{e}_i - \mathbf{e}_j$. The diagonal elements of (22) have the form $\left([L_g^{-1}]_{ki} - [L_g^{-1}]_{kj}\right)^2$, $1 \leq k \leq n$ as the L_g^{-1} is a symmetric matrix. We need to show that the off-diagonal elements of (22) are non-negative. Without loss of generality let us suppose the form of the off-diagonal elements as $\left([L_g^{-1}]_{ki} - [L_g^{-1}]_{kj}\right)\left([L_g^{-1}]_{il} - [L_g^{-1}]_{jl}\right)$ for any $1 \leq k, l \leq n$. If $1 \leq k \leq j$ or $1 \leq l \leq j$, then $\left([L_g^{-1}]_{ki} - [L_g^{-1}]_{kj}\right)\left([L_g^{-1}]_{il} - [L_g^{-1}]_{jl}\right) = 0$ (based on Lemma 2). Let us suppose $j \leq k \leq i$. In this case one can easily verify that for any value of l, i.e., either $j \leq l \leq i$, or $i \leq l \leq n$, $[L_g^{-1}]_{ki} - [L_g^{-1}]_{kj}$ and $[L_g^{-1}]_{il} - [L_g^{-1}]_{jl}$ have the same sign. Now let us suppose $i \leq k \leq n$. With the same argument we conclude that $\left([L_g^{-1}]_{ki} - [L_g^{-1}]_{kj}\right)\left([L_g^{-1}]_{il} - [L_g^{-1}]_{jl}\right) \geq 0$ for any $j \leq l \leq n$. It is now sufficient to show that $w_i\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1}\mathbf{e}_{ij} \geq 0$. We have $\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1}\mathbf{e}_{ij} = [L_g^{-1}]_{ii} - 2[L_g^{-1}]_{ij} + [L_g^{-1}]_{jj}$ which is the effective resistance of the added edge between nodes j and i and hence is positive [79]. Thus, the second term in (21) is a non-negative matrix. This implies that the elements of $\tilde{L}_g^{-1}$ are not larger than those of L_g^{-1}. This along with Lemma 1 complete the proof. ■

APPENDIX D
PROOF OF THEOREM 6

Proof: Without loss of generality, we denote the ordering of the nodes in the path starting from the leader to the end of the path the same as proof of Theorem 5. For the case that an extra edge is added from node j to node i (not making a cycle), using Sherman-Morrison formula [78] and (18) results in

$$\tilde{L}_g^{-1} = L_g^{-1} - \frac{w_i L_g^{-1}\mathbf{e}_i\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1}}{1 + w_i\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1}\mathbf{e}_i}. \tag{23}$$

Now, we have (24), as shown at the top of the previous page.

Furthermore,

$$w_i\mathbf{e}_{ij}^{\mathsf{T}}L_g^{-1}\mathbf{e}_i = w_i\left([L_g^{-1}]_{ii} - [L_g^{-1}]_{ji}\right) = w_i\left(\frac{1}{w_i} - 0\right) = 1 \tag{25}$$

Hence, the second term in (23) is a non-negative matrix. This implies that the elements of $\tilde{L}_g^{-1}$ are not larger than those of L_g^{-1}. This result along with Lemma 1 prove the claim.

For the case that an extra edge is added from node i to node j (making a cycle), with the same argument it can be easily shown that the second term in (23) is a non-positive matrix. This completes the proof. ■

REFERENCES

[1] M. A. Javed and E. B. Hamida, "On the interrelation of security, QoS, and safety in cooperative ITS," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 7, pp. 1943–1957, Jul. 2017.

[2] U. Lang and R. Schreiner, "Managing security in intelligent transport systems," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 48–53.

[3] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 1, pp. 90–96, Jan. 2017.

[4] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.

[5] S. Lam and J. Katupitiya, "Cooperative autonomous platoon maneuvers on highways," in *Proc. IEEE/ASME Int. Conf. Adv. Intell. Mechtron.*, Jul. 2013, pp. 1152–1157.

[6] K. Huang, X. Yang, Y. Lu, C. C. Mi, and P. Kondlapudi, "Ecological driving system for connected/automated vehicles using a two-stage control hierarchy," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2373–2384, Jul. 2018.

[7] G. Guo and Q. Wang, "Fuel-efficient en route speed planning and tracking control of truck platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 8, pp. 3091–3103, Aug. 2018.

[8] K. C. Dey, L. Yan, X. Wang, Y. Wang, H. Shen, M. Chowdhury, L. Yu, C. Qiu, and V. Soundararaj, "A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (CACC)," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 491–509, Feb. 2016.

[9] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape—Architectures, enabling technologies, applications, and development areas," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2391–2406, Aug. 2018.

[10] B. van Arem, C. J. G. van Driel, and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow characteristics," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 4, pp. 429–436, Dec. 2006.

[11] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 296–305, Feb. 2014.

[12] L. Guvenc, I. M. C. Uygan, K. Kahraman, R. Karaahmetoglu, I. Altay, M. Senturk, M. T. Emirler, A. E. H. Karci, B. A. Guvenc, and E. Altug, "Cooperative adaptive cruise control implementation of team Mekar at the grand cooperative driving challenge," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1062–1074, Sep. 2012.

[13] K. Lidström, K. Sjöberg, U. Holmberg, J. Andersson, F. Bergh, M. Bjäde, and S. Mak, "A modular CACC system integration and design," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1050–1061, Sep. 2012.

[14] B. Sakhdari and N. L. Azad, "Adaptive tube-based nonlinear MPC for economic autonomous cruise control of plug-in hybrid electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11390–11401, Dec. 2018.

[15] B. Sakhdari and N. L. Azad, "A distributed reference governor approach to ecological cooperative adaptive cruise control," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 5, pp. 1496–1507, May 2018.

[16] C. Nowakowski, S. E. Shladover, X.-Y. Lu, D. Thompson, and A. Kailas, "Cooperative adaptive cruise control (CACC) for truck platooning: Operational concept alternatives," California Partners Adv. Transp. Technol., UC Berkeley, Berkeley, CA, USA, 2015. [Online]. Available: https://escholarship.org/uc/item/7jf9n5wm#main

[17] Z. Wang, G. Wu, and M. J. Barth, "Developing a distributed consensus-based cooperative adaptive cruise control system for heterogeneous vehicles with predecessor following topology," *J. Adv. Transp.*, vol. 2017, Aug. 2017, Art. no. 1023654.

[18] C. Wang, S. Gong, A. Zhou, T. Li, and S. Peeta, "Cooperative adaptive cruise control for connected autonomous vehicles by factoring communication-related constraints," *Transp. Res. C, Emerg. Technol.*, to be published.

[19] 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 Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[20] S. Dadras and C. Winstead. (2018). *Insider Vs. Outsider Threats to Autonomous Vehicle Platooning*. [Online]. Available: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1773&context=researchweek

[21] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[22] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, and A. Kung, "Secure vehicular communication systems: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

[23] R. M. Gerdes, C. Winstead, and K. Heaslip, "CPS: An efficiency-motivated attack against autonomous vehicular transportation," in *Proc. 29th Annu. Comput. Secur. Appl. Conf.*, 2013, pp. 99–108.

[24] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016.

[25] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[26] J. Miloševič, T. Tanaka, H. Sandberg, and K. H. Johansson, "Analysis and mitigation of bias injection attacks against a Kalman filter," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8393–8398, 2017.

[27] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proc. 10th ACM Symp. Inf., Comput. Commun. Secur.*, 2015, pp. 167–178.

[28] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: A study of misbehavior in vehicular platoons," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2015, p. 22.

[29] D. D. Dunn, "Attacker-induced traffic flow instability in a stream of automated vehicles," Ph.D. dissertation, Utah State Univ., Logan, UT, USA, 2015. [Online]. Available: https://search.proquest.com/docview/1710737617/abstract/3DE6689E21AF46EBPQ/1?accountid=14906

[30] D. D. Dunn, S. A. Mitchell, I. Sajjad, R. M. Gerdes, R. Sharma, and M. Li, "Regular: Attacker-induced traffic flow instability in a stream of semi-automated vehicles," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 499–510.

[31] B. Biswas, "Analysis of false data injection in vehicle platooning," M.S. thesis, Dept. Elect. Eng., Utah State Univ., Logan, UT, USA, 2014.

[32] (2017). *A Brief History of Car Hacking 2010 to the Present*. [Online]. Available: https://smart.gi-de.com/2017/08/brief-history-carhacking-2010-present/

[33] R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *Proc. Annu. Amer. Control Conf. (ACC)*, 2018, pp. 5582–5587.

[34] L. Cui, J. Hu, B. B. Park, and P. Bujanovic, "Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: Assessing cooperative adaptive cruise control under cyber attack," *Transp. Res. C, Emerg. Technol.*, vol. 97, pp. 1–22, Dec. 2018.

[35] E. Mousavinejad, F. Yang, Q.-L. Han, Q. Qiu, and L. Vlacic, "Cyber attack detection in platoon-based vehicular networked control systems," in *Proc. IEEE 27th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2018, pp. 603–608.

[36] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes, "Attack mitigation in adversarial platooning using detection-based sliding mode control," in *Proc. 1st ACM Workshop Cyber-Phys. Syst.-Secur. Privacy*, 2015, pp. 43–53.

[37] R. G. Dutta, F. Yu, T. Zhang, Y. Hu, and Y. Jin, "Security for safety: A path toward building trusted autonomous vehicles," in *Proc. Int. Conf. Comput.-Aided Design*, 2018, p. 92.

[38] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[39] H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in *Proc. 51st IEEE Conf. Decis. Control (CDC)*, Dec. 2012, pp. 3412–3417.

[40] S. Amin. A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. 12th Int. Conf. Workshop Hybrid Syst., Comput. Control (HSCC)*, San Francisco, CA, USA. Berlin, Germany: Springer-Verlag, Apr. 2009, pp. 31–45.

[41] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, 2009, pp. 911–918.

[42] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Dec. 2010, pp. 5967–5972.

[43] R. Chabukswar, B. Sinopoli, G. Karsai, A. Giani, H. Neema, and A. Davis, "Simulation of network attacks on scada systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 587–592.

[44] M. H. Basiri, J. G. Thistle, J. W. Simpson-Porco, and S. Fischmeister, "Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems," in *Proc. Annu. Amer. Control Conf. (ACC)*, 2019, pp. 3841–3848.

[45] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 45–65, Feb. 2015.

[46] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[47] A. Gupta, C. Langbort, and T. Basar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decis. Control*, Dec. 2010, pp. 1096–1101.

[48] M. Felegyhazi and J.-P. Hubaux, "Game theory wireless networks: A tutorial," EPFL, Lausanne, Switzerland, 2006. [Online]. Available: https://infoscience.epfl.ch/record/79715

[49] J. R. Marden, G. Arslan, and J. S. Shamma, "Cooperative control and potential games," *IEEE Trans. Syst., Man, Cybern. B. Cybern.*, vol. 39, no. 6, pp. 1393–1407, Dec. 2009.

[50] M. Pirani, E. Nekouie, H. Sandberg, and K. H. Johansson, "A game-theoretic framework for security-aware sensor placement problem in networked control systems," in *Proc. Annu. Amer. Control Conf. (ACC)*, 2019, pp. 114–119.

[51] P. N. Brown, H. Borowski, and J. R. Marden, "Security against impersonation attacks in distributed systems," 2017, *arXiv:1711.00609*. [Online]. Available: https://arxiv.org/abs/1711.00609

[52] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[53] W. Lobato, D. Rosario, M. Gerla, and L. A. Villas, "Platoon-based driving protocol based on game theory for multimedia transmission over VANET," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[54] Z. Xu and Q. Zhu, "A game-theoretic approach to secure control of communication-based train control systems under jamming attacks," in *Proc. 1st Int. Workshop Safe Control Connected Auton. Vehicles*, 2017, pp. 27–34.

[55] Y. A. Harfouch, S. Yuan, and S. Baldi, "An adaptive switched control approach to heterogeneous platooning with intervehicle communication losses," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1434–1444, Sep. 2018.

[56] 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.

[57] 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, Aug. 2014.

[58] E. S. Kazerooni and J. Ploeg, "Interaction protocols for cooperative merging and lane reduction scenarios," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 1964–1970.

[59] H. H. Bengtsson, L. Chen, A. Voronov, and C. Englund, "Interaction protocol for highway platoon merge," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2015, pp. 1971–1976.

[60] C. Lei, E. Van Eenennaam, W. K. Wolterink, G. Karagiannis, G. Heijenk, and J. Ploeg, "Impact of packet loss on CACC string stability performance," in *Proc. 11th Int. Conf. ITS Telecommun.*, Aug. 2011, pp. 381–386.

[61] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful degradation of CACC performance subject to unreliable wireless communication," in *Proc. 16th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2013, pp. 1210–1216.

[62] F. Qu, F.-Y. Wang, and L. Yang, "Intelligent transportation spaces: Vehicles, traffic, communications, and beyond," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 136–142, Nov. 2010.

[63] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A survey of inter-vehicle communication protocols and their applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 3–20, 2nd Quart., 2009.

[64] X. Xiang, W. Qin, and B. Xiang, "Research on a dsrc-based rear-end collision warning model," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 3, pp. 1054–1065, Jun. 2014.

[65] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems—5-GHz Band Dedicated Short—Range Communications (DSRC), Medium Access Control (MAC), and Physical Layer (PHY) Specifications*, Standard ASTM-E221, ASTM International, West Conshohocken, PA, USA, 2018.

[66] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[67] F. Bai, D. D. Stancil, and H. Krishnan, "Toward understanding characteristics of dedicated short range communications (DSRC) from a perspective of vehicular network engineers," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, 2010, pp. 329–340.

[68] D. Shin, K. Park, and M. Park, "Effects of vehicular communication on risk assessment in automated driving vehicles," *Appl. Sci.*, vol. 8, no. 12, p. 2632, 2018.

[69] V. Shivaldova, G. Maier, D. Smely, N. Czink, A. Paier, and C. Mecklenbräuker, "Performance analysis of vehicle-to-vehicle tunnel measurements at 5.9 GHz," in *Proc. URSI Gen. Assem. Sci. Symp.*, 2011, pp. 1–4.

[70] X. Wu, S. Subramanian, R. Guha, R. G. White, J. Li, K. W. Lu, A. Bucceri, and T. Zhang, "Vehicular communications using DSRC: Challenges, enhancements, and evolution," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 399–408, Sep. 2013.

[71] H. Hao and P. Barooah, "Stability and robustness of large platoons of vehicles with double-integrator models and nearest neighbor interaction," *Int. J. Robust Nonlinear Control*, vol. 23, no. 18, pp. 2097–2122, 2013.

[72] H. Hao, P. Barooah, and J. 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.

[73] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*, vol. 15. Philadelphia, PA, USA: SIAM, 1994.

[74] 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.

[75] M. Pirani and S. Sundaram, "On the smallest eigenvalue of grounded Laplacian matrices," *IEEE Trans. Autom. Control*, vol. 61, no. 2, pp. 509–514, Feb. 2016.

[76] P. V. Mieghem, *Graph Spectra for Complex Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[77] D. Swaroop and J. K. Hedrick, "String stability of interconnected systems," *IEEE Trans. Autom. Control*, vol. 41, no. 3, pp. 349–357, Mar. 1996.

[78] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C: The Art of Scientific Computin*. Cambridge, U.K.: Cambridge Univ. Press, 1986.

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

MOHAMMAD HOSSEIN BASIRI received the B.Sc. degree (Hons.) from the Isfahan University of Technology (IUT), Isfahan, Iran, and the M.Sc. degree (Hons.) from the Sharif University of Technology (SUT), Tehran, Iran, both in electrical engineering—systems and controls. As a joint member of Real-time Embedded Software Group (RESG) and the Smart Hybrid and Electric Vehicle Systems (SHEVS) Laboratory, he is currently pursuing the Ph.D. degree in electrical engineering–systems and controls with the ECE Department, University of Waterloo, ON, Canada. He also had honorable permission for simultaneous study in two majors, electrical engineering and industrial engineering as an Exceptional Talented Student and received several scholarships during his studies. He was the winner of the Travel Award Grant to CPSWeek, 2019, Montreal, QC, Canada. His research interests include cyber-physical systems, security, and control theory particularly with the application to connected and automated vehicles.

MOHAMMAD PIRANI received 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 Postdoctoral Researcher with the Department of Electrical and Computer Engineering, University of Toronto, ON, Canada. His research interests include resilient and fault tolerant control, networked control systems, and intelligent transportation systems. He is a member of the IEEE-CSS technical committee on smart cities.

NASSER L. AZAD was a Postdoctoral Fellow with the Vehicle Dynamics and Control Laboratory, Department of Mechanical Engineering, University of California, Berkeley, CA, USA. He is currently an Associate Professor with the Department of Systems Design Engineering, University of Waterloo, and also the Director of the Smart Hybrid and Electric Vehicle Systems (SHEVS) Laboratory. His primary research interests lie in control of connected hybrid and electric vehicles, autonomous cars, and unmanned aerial vehicle quadrotors. He is also interested in applications of artificial intelligence for solving different engineering problems. Due to his outstanding work, he received an Early Researcher Award in 2015 from the Ministry of Research and Innovation, ON, Canada.

SEBASTIAN FISCHMEISTER received the Dipl.-Ing. degree in computer science from the Vienna University of Technology, Austria, in March 2000, and the Ph.D. degree in computer science from the University of Salzburg, Austria, in December 2002. He continued working at the University of Salzburg as a Researcher and a Lecturer and was awarded the Austrian APART stipend in 2005. He subsequently worked at the University of Pennsylvania, USA, as a Post Graduate Research Associate until 2008. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He performs systems research at the intersection of software technology, distributed systems, and formal methods. His preferred application area includes distributed real-time embedded systems in the domain of automotive systems, avionics, and medical devices.