Evaluations of Cyberattacks on Cooperative Control of Connected and Autonomous Vehicles at Bottleneck Points

H M Sabbir Ahmad
Boston University
sabbir92@bu.edu

Ehsan Sabouni
Boston University
esabouni@bu.edu

Wei Xiao
Massachusetts Institute of Technology
weixy@mit.edu

Christos G. Cassandras
Boston University
cgc@bu.edu

Wenchao Li
Boston University
wenchao@bu.edu

***Abstract*—In this paper we analyze the effect of cyberattacks on cooperative control of connected and autonomous vehicles (CAVs) at traffic bottleneck points. We focus on three types of such bottleneck points including merging roadways, intersections and roundabouts. The coordination amongst CAVs in the network is achieved in a decentralized manner whereby each CAV formulates its own optimal control problem and solves it onboard in real time. A roadside unit is introduced to act as the coordinator that communicates and exchanges relevant data with the CAVs through wireless V2X communication. We show that this CAV setup is vulnerable to various cyberattacks such as Sybil attack, jamming attack and false data injection attack. Results from our simulation experiments call attention to the extent to which such attacks may jeopardize the coordination performance and the safety of the CAVs.**

I. Introduction

The emergence of connected and automated vehicles (CAVs) along with new traffic infrastructure technologies [1], [2] over the past decade have brought the promise of resolving long-lasting problems in transportation networks such as accidents, congestion, and unsustainable energy consumption along with environmental pollution [3]–[5]. Meeting this goal heavily depends on effective traffic management, specifically at the bottleneck points of a transportation network such as intersections, roundabouts, and merging roadways [6].

To date, both centralized [7], [8] and decentralized [9]–[11] methods have been proposed to tackle the control and coordination problem of CAVs in conflict points. In decentralized methods, as opposed to centralized ones, each CAV is responsible for its own on-board computation with information from other vehicles limited to a set of neighbors [12]. This paper emphasizes on decentralized algorithms as they provide manifold benefits including added security as an attacker can only target a limited number of agents, whereas in the centralized scheme an attack on the central entity can potentially compromise every agent/CAV. There has been extensive research on cybersecurity of CAVs summarized in [13]–[15]. The attacks can be categorized into in-vehicle network attacks and attacks on (V2V or V2X) communication network. In this paper, *we present the first study of a novel class of security problems concerning coordination and control of CAVs through numerous traffic bottleneck points*. There has been extensive research done from a control point of view with the aim of designing smart and efficient control and coordination algorithms for real world implementation. However, security for these next generation of CAV algorithms have received virtually no attention with only two papers found based on our survey.

One class of cooperative algorithms for autonomous vehicles which has been studied extensively from a security point-of-view is Cooperative Adaptive Cruise Control (CACC). The authors in [16] consider in vehicle network attack targeting sensors by manipulating sensor data, injecting false sensor data and jamming the onboard radar by injecting noise to the measurements. In [17], the authors focus on a replay attack targeting vehicle sensor network/controller using malware compromising the sensor readings and data received over DSRC. In terms of attacks on the wireless communication, [18] addresses Sybil/impersonation attack, [19] investigates mutation, denial of delivery, masquerading and false data injection (FDI) attack, [20] looks at signal jamming attack, and [21] looks into stealthy/covert attacks.

As mentioned previously, the research on security of CAVs in coordinated settings at bottleneck points is still at its embryonic stage [22]. The authors in [22] consider the decentralized algorithm in [23] and propose a vehicle authentication protocol based on public key cryptography by comparing between elliptic-curve cryptography (ECC) and RSA cryptography schemes. In [24] the authors assessed the cybersecurity risks on cooperative ramp merging by targeting the V2I communication with road-side units (RSU). Additionally, there is literature that considers cyberattacks on connected vehicles and investigates their effects on intersections [25], [26] and freeway [27] control system; however, with the fundamental difference that they do not consider the security of cooperative control of CAVs.

This work was supported in part by ONR grant N00014-19-1-2496, NSF under grants ECCS-1931600, DMS-1664644, CNS-1645681, CNS-2149511, by AFOSR under grant FA9550-19-1-0158, by ARPA-E under grant DE-AR0001282, by the MathWorks, by the Red Hat-Boston University Collaboratory, and by NPRP grant (12S-0228-190177) from the Qatar National Research Fund, a member of the Qatar Foundation (the statements made herein are solely the responsibility of the authors).

Symposium on Vehicles Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23082
www.ndss-symposium.org

Our aim in this paper is to present these problems with twofold objectives: (i) encourage the research community to take security into consideration and design resilient security-aware algorithms, and (ii) provide a knowledge base for the future stakeholders designing the technologies for implementing these algorithms. The main contributions of our paper are summarized below:

1) Provide an attack taxonomy for CAVs in cooperative environment.
2) Identify the main risks due to cyberattacks on cooperative control of CAVs at bottleneck points.
3) Analyze the main shortcomings from security points-of-view in the existing cooperative control algorithms for CAVs by using various simulated attack (not the worst possible) scenarios.

The paper is organized in five sections. In the following section, we present a decentralized cooperative control problem formulation for CAVs at the aforementioned bottleneck points. In section III, we present an attack taxonomy for V2X communication and identify the main threats on the coordination of CAVs at bottleneck points. In section IV, we present the results of various attack cases from computer simulation and deduce the main shortcomings of the existing cooperative control algorithms. Finally, we conclude our findings and offer future directions in Section V.

II. Cooperative Control at Bottleneck Points

We focus on the existing decentralized control approaches proposed in [28]–[30] for our study. The approach utilizes a roadside unit (RSU) which receives and stores information from all CAVs using V2X communication and ensures safe coordination by communicating to each CAV information about the other "relevant" CAVs in the network which they might come in collision with. We focus on three types of networks, which are: i. merging roadways [28], ii. signal-free intersections [29], and iii. roundabouts [30]; and briefly present the definition of each of the problems.

A. Merging roadway:

The merging problem arises when traffic from two different roads, usually associated with a main lane and a merging lane needs to be merged together, as shown in Fig. 1. The traffic comprises of CAVs randomly arriving from two lanes joined at the Merging Point (MP) M, where collisions may occur. The RSU coordinator maintains a First-In-First-Out (FIFO) queue of CAVs based on the arrival time at the CZ and uses real-time communication with the CAVs that are in the CZ as well as the last one leaving the CZ (see Fig. 1), to safely merge the traffic from the two lanes.

B. Multi-lane signal-free intersections:

Fig. 2 shows a typical intersection with multiple lanes. Here, the CZ is the area within the outer red circle and the length of each CZ segment is L which is initially assumed to be the same for all entry points to the intersection. Red dots show all MPs where potential collisions may occur. It is assumed that the motion trajectory of each CAV in the intersection is determined upon its entrance to the CZ (see grey lines in Fig. 1). Based on these trajectories, all MPs in the intersection are fixed and can be easily determined. However,

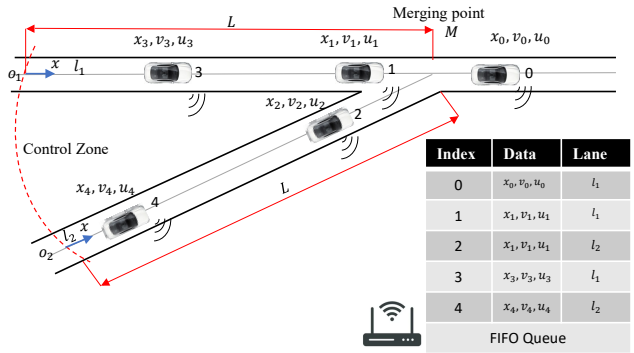

Fig. 1: Illustration of the merging roadway.

CAVs are allowed to change lanes in the CZ while they are in the "lane-changing zone",i.e., an area between the two red lines shown in Fig. 2. Due to lane-changing, apart from the fixed MPs in the intersection, some "floating" MPs may also appear in lane-changing zones which are not fixed in space.

All CAVs have three possible movements: going straight, turning left, and turning right. Thus, some CAVs must change their lanes so as to execute a movement, e.g., left-turning CAV 6 in l_8 in Fig. 2. Due to such lane-changing behavior, a new MP $M_{6,7}$ is generated since a conflict of CAV 6 with a CAV in l_7 may arise. Similarly, possible MPs may also appear in other lanes when vehicles perform lane-changing maneuvers, as the red dots $(M_{i,1}, M_{i,2}, \cdots,$ and $M_{i,8})$ indicate in Fig. 2. The coordinator (RSU) stores all individual CAV information and maintains the crossing sequence using FIFO queue.

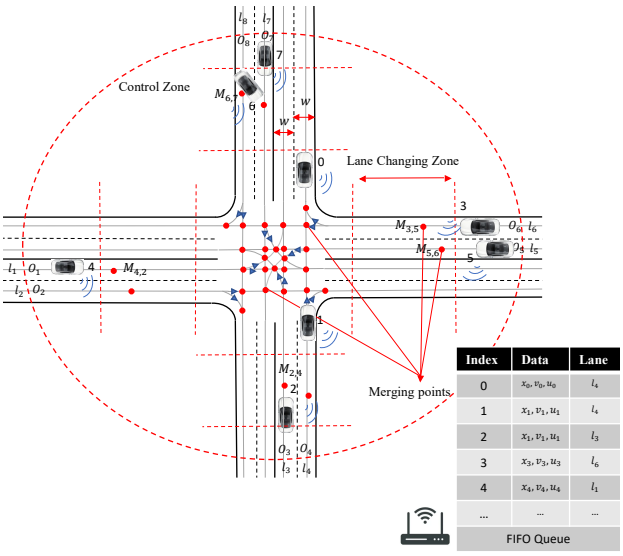

Fig. 2: The multi-lane intersection problem. Collisions may happen at the MPs (red dots shown in above figure).

C. Roundabout:

Fig. 3 depicts a roundabout with three entries and three exits.It is assumed that each road segment has a single lane. The entries are labeled as l_j with the origin O_j, where $j \in \{1, 2, 3\}$. CAVs randomly enter the roundabout from three different origin points O_1, O_2 and O_3 and have randomly

assigned exit points E_1, E_2 and E_3. The entry road segments are connected with the circular part at the three Merging Points (MPs) labeled as M_1, M_2 and M_3 where CAVs from different road segments may potentially collide with each other. The circular part of the roundabout is further divided into three road segments labeled from l_4 to l_6.

For all of three networks, the coordinator maintains a table of CAVs in the CZ under a unique index, assigned based on the passing sequence policy used along with their data, for every time t as shown in Fig. 1, 2 and 3. let $S(t)$ be the set of CAV indices in the coordinator queue table at time t whose cardinality is $N(t)$. Under FIFO passing sequence, when a new CAV arrives, it is allocated the index $N(t)+1$. Similarly, each time a CAV i leaves the CZ, it is dropped from the table and all CAV indices larger than i decrease by one. Whilst in the CZ, each CAV has to stay safe to the CAV that is physically proceeding it immediately and from the CAV that will pass immediately before it at every MPs it will traverse through in the CZ. This is done by imposing constraints namely rear end constraint (for staying safe from physically preceding CAV) and merging constraint (for avoiding collision at the MPs). The coordinator identifies the constraints for every CAV based on crossing sequence policy used (e.g. FIFO queuing policy) by checking the queue table.

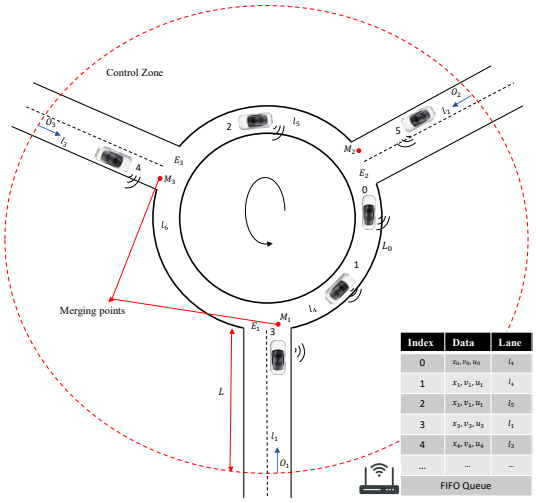

Fig. 3: Illustration of the roundabout problem.

D. Decentralized Optimal Control Problem formulation.

The vehicle dynamics for each CAV $i \in S(t)$ take the following form

$$\begin{bmatrix} \dot{x}_i(t) \\ \dot{v}_i(t) \end{bmatrix} = \begin{bmatrix} v_i(t) \\ u_i(t) \end{bmatrix}, \tag{1}$$

where $x_i(t)$ denotes the distance from the origin at which CAV i arrives, $v_i(t)$, and $u_i(t)$ denotes the velocity and control input (acceleration/deceleration) of CAV i, respectively. Let t_i^0 and t_i^f denote the time that CAV i arrives at the origin and leaves the CZ at its exit point, respectively. Constraints for any conflict area can be listed as follows:

Constraint 1 (Rear-End Safety Constraint): Let i_p denote the index of the CAV which physically immediately precedes CAV i in the CZ (if one is present). It is required that the distance $z_{i,i_p}(t) := x_{i_p}(t) - x_i(t)$ be constrained as follows:

$$z_{i,i_p}(t) - \varphi v_i(t) - \delta \geq 0, \quad \forall t \in [t_i^0, t_i^f] \tag{2}$$

where φ denotes the reaction time and δ is a given minimum safe distance. z_{i,i_p} is defined to be the distance from the center of CAV i to the center of CAV i_p, and δ depends on the length of these two CAVs.

Constraint 2 (Safe Merging Constraint): Whenever a CAV crosses a MP, a lateral collision is possible, and there must be adequate safe space for the CAV to avoid such collision, i.e.,

$$z_{i,i_c}(t_i^m) - \varphi v_i(t_i^m) - \delta \geq 0, \tag{3}$$

where i_m is the index of the CAV that may collide with CAV i at the merging points $m = \{1, ..., n_i\}$ where n_i is the total number of MPs that CAV i passes in the CZ. The determination of CAV i_m depends on the policy adopted for sequencing CAVs through the CZ.

Constraint 3 (Lateral Safety Constraint): In the roundabout problem, the moment generated by the centrifugal force needs to be smaller than the one generated by gravity in order to avoid rollover that is imposed as:

$$\kappa\left(x_i(t)\right) v_i^2(t) h \leq w_h g \tag{4}$$

where h is the height of the CAV, w_h is the half width of the CAV (for simplicity, both assumed to be the same for all CAVs), and g is the gravity constant.

Constraint 4 (Vehicle limitations): Finally, there are constraints on the speed and acceleration for each $i \in S(t)$:

$$v_{min} \leq v_i(t) \leq v_{max}, \forall t \in [t_i^0, t_i^f] \tag{5}$$

$$u_{min} \leq u_i(t) \leq u_{max}, \forall t \in [t_i^0, t_i^f] \tag{6}$$

where $v_{\max} > 0$ and $v_{\min} \geq 0$ denote the maximum and minimum speed allowed in the CZ, $u_{\min} < 0$ and $u_{\max} > 0$ denote the minimum and maximum control, respectively.

The control goal is to determine a control law jointly minimizing the travel time and energy consumption subject to constraints (2), (3), (4) (for roundabout only), (5) and (6) for each $i \in S(t)$ governed by the dynamics (1). Expressing energy through $\frac{1}{2}u_i^2(t)$ and normalizing travel time and energy, we use the weight $\alpha \in [0, 1]$ to construct a convex combination as follows:

$$\min_{u_i(t), t_i^f} J_i(u_i(t), t_i^f) := \beta(t_i^f - t_i^0) + \int_{t_i^0}^{t_i^f} \frac{1}{2} u_i^2(t) dt, \tag{7}$$

where $\beta := \frac{\alpha \max\{u_{max}^2, u_{min}^2\}}{2(1-\alpha)}$ is an adjustable weight to penalize travel time relative to the energy cost of CAV i. Additionally, in roundabout problem in [30] another objective is added to the optimal control problem to maximize centrifugal comfort given as following:

$$J_{i,3} = \int_{t_i^0}^{t_i^f} \kappa\left(x_i(t)\right) v_i^2(t) dt \tag{8}$$

where $\kappa\left(x_i\right)$ is the curvature of the road at position x_i. As the aim is to minimize the centrifugal force of the vehicle,

the curvature $\kappa(x_i)$ has the form of $\frac{1}{r(x_i)}$, where $r(x_i)$ is the radius of the road at position x_i.

The solution is *decentralized* in the sense that CAV i requires information only from CAVs that are relevant to it due to one or both constraints in (2) and (3).

The OCBF approach [11]. Firstly, Control Barrier Functions (CBFs) that ensure the constraints (2), (3), (4) (for roundabout only), (5) and (6) and (5) are derived, subject to the vehicle dynamics in (1) by defining $f(\boldsymbol{x}_i(t)) = [v_i(t), 0]^T$ and $g(\boldsymbol{x}_i(t)) = [0, 1]^T$. Each of these constraints can be easily written in the form of $b_q(\boldsymbol{x}(t)) \geq 0$, $q \in \{1, ..., n\}$ where n stands for the number of constraints only dependent on state variables and $\boldsymbol{x}(t) = [\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), ..., \boldsymbol{x}_{N(t)}(t)]$. The CBF method (details provided in [31]) maps a constraint $b_q(\boldsymbol{x}(t)) \geq 0$ onto a new constraint which is *linear* in the control input and takes the general form

$$L_f b_q(\boldsymbol{x}(t)) + L_g b_q(\boldsymbol{x}(t)) u_i(t) + \gamma(b_q(\boldsymbol{x}(t))) \geq 0. \quad (9)$$

Additionally, a Control Lyapunov Function (CLF) is used to track the CAV speed to a desired value $v_i^{ref}(t)$ setting $V(\boldsymbol{x}_i(t)) = (v_i(t) - v_i^{ref}(t))^2$ and expressing the CLF constraint as follows:

$$L_f V(\boldsymbol{x}_i(t)) + L_g V(\boldsymbol{x}_i(t)) \boldsymbol{u}_i(t) + c_3 V(\boldsymbol{x}_i(t)) \leq e_i(t), \quad (10)$$

where $e_i(t)$ makes this a soft constraint.

Finally, the OCBF problem is formulated as follows:

$$\min_{u_i(t), e_i(t)} J_i(u_i(t), e_i(t)) := \int_{t_i^0}^{t_i^f} \big[\frac{1}{2}(u_i(t) - u_i^{ref}(t))^2 + \lambda e_i^2(t)\big] dt \quad (11)$$

subject to vehicle dynamics (1), the CBF constraints (9), $\forall q = \{1, ..., n\}$ and CLF constraint. In this approach ,(i) u_i^{ref} is generated by solving the unconstrained optimal control problem in (7), (ii) the resulting u_i^{ref} is optimally tracked such that constraints including the CBF constraints (9) $\forall q = \{1, ..., n\}$ is satisfied, (iii) this tracking optimal control problem is efficiently solved by discretizing time and solving a simple QP at each discrete time step.

More concretely, we can solve this dynamic optimization problem by discretizing $[t_i^0, t_i^f]$ into intervals $[t_i^0, t_i^0 + \Delta], ..., [t_i^0 + k\Delta, t_i^0 + (k+1)\Delta], ...$ with equal length Δ and solving (11) over each time interval through solving a QP at each time step:

$$\min_{u_{i,k}, e_{i,k}} [\frac{1}{2}(u_{i,k} - u_i^{ref}(t_{i,k}))^2 + \lambda e_{i,k}^2] \quad (12)$$

subject to the CBF constraints (9), $\forall q = \{1, ..., n\}$, CLF constraint (10) and dynamics (1), where all constraints are linear in the decision variables.

III. Attack taxonomy and associated threats

Our first step is to generate an initial attack taxonomy, which is done by reviewing existing literature on CAV security and CACC security (as summarized in section I). For the road networks the systems assets are the RSU and the CAVs in the CZ. The information assets are: i. Queue table in the roadside coordinator (as the information in the table has to be always protected for safe coordination of CAVs) and ii. state information of the every CAV along with information of other CAVs that are relevant to it (communicated by the coordinator), communication bus associated to low-level controller responsible for driving the vehicle, its associated sensors and the actuators. Following that, we updated initial taxonomy by focusing specifically on V2X communication. Although adversaries can target the RSU and the CAV inter-vehicle network, we consider the RSU as a trusted entity; and primarily focus on V2X communication network security. It is important to note that the risks on the coordination performance of CAVs is the same for communication network attacks and attacks targeting road network infrastructure and/or CAVs. The attack taxonomy for the V2X communication networks is tabulated in table II.

TABLE I: Risks due to cyberattacks on the coordination and control performance of CAVs.

Threat type	Cause
Accident	Violation of rear-end/merging safety constraint
Traffic jam	Abnormally slow moving CAV/spoofed CAV.
Excessive energy usage causing environmental pollution	Rapid acceleration or deceleration (jerk).
Passenger discomfort	Rapid acceleration or deceleration (jerk).

As part of our study, we simulated various attacks on the aforementioned road networks. In the remainder of this section, we present the models of these attacks. The studied algorithms make the following assumptions:

Assumption 1: The road network contains homogeneous CAVs i.e., their parameters are the same.

Assumption 2: The cooperative control algorithms we studied have been designed assuming a perfect communication network, i.e., no packet loss and latency in the network.

The cooperative control algorithms considered require that each CAV has the data of CAVs that are relevant to it in real time to provably guarantee satisfaction of the safety constraints, and hence, assumption 2 introduces an additional shortcoming in these proposed algorithms.

A. Sybil attack:

Definition 1: (Spoofed Client) A single malicious client (could be a CAV or attacker nearby the CZ) may generate multiple unique identities, each with a fabricated position and velocity. Each generated, or "spawned" identity is considered a spoofed client/CAV. We assume at any time t, there are two groups of CAVs in CZ: i. Normal CAVs and ii. Spoofed CAVs. Let $\{\boldsymbol{x_1}(t), \ldots, \boldsymbol{x_m}(t)\}$ denote the set of normal CAV states where $\boldsymbol{x}_i \in \mathbb{R}^2$ includes the position and velocity of CAV i, and $\{u_1(t), \ldots, u_m(t)\}$ denote the set of control inputs for each of the normal CAVs where $u_i \in \mathbb{R}$ is the control input, that are communicated to the RSU by each CAV; and $S_x(t)$ is the set of their indices in the FIFO queue in the RSU coordinator unit. Let, $\{\tilde{\boldsymbol{x}}_1(t), \ldots, \tilde{\boldsymbol{x}}_s(t)\}$ is the set of the spoofed CAV states where $\tilde{\boldsymbol{x}}_i \in \mathbb{R}^2$ includes the position and velocity of spoofed CAV i, and $\{\tilde{u}_1(t), \ldots, \tilde{u}_s(t)\}$ is the set of the control inputs of the spoofed CAVs where $\tilde{u}_i \in \mathbb{R}$ is the acceleration input, that are communicated by the attacker

TABLE II: Attack taxonomy of V2X Communication of CAVs at bottleneck points

Attack category	Attack type	Network security requirements			
		Confidentiality	Integrity	Availability	Authenticity
Main-in-the-Middle attacks	Replay attack [14]		×		
	False data injection attack [13], [14]		×		
	Slight Attack [14], [32]		×		
Communication hijacking attacks	DoS attack [13], [33]			×	
	Timing attack [34]			×	
	Flooding attack [35]			×	
	Black hole attack [36]			×	
	Grey hole attack [37]			×	
	Wormhole attack [38]			×	
Spoofing attacks	Sybil attack [39]				×
	Impersonation attack [14]				×
Eavesdropping attack [14], [40]		×			
	Interception attack [41]	×			

at every time instant; and $S_{\tilde{x}}(t)$ is the set of their indices in the FIFO queue. Therefore the total number of CAVs in control zone at any time $t, N(t) = |S_x(t)| + |S_{\tilde{x}}(t)|$. There can be one or more spoofed clients/CAVs in the CZ at any time t.

Definition 2: (Sybil Attack) A set of normal and spoofed CAVs $S(t)$ are present in the CZ at any time t, where a subset of the clients $S_{\tilde{x}}(t)$ are spoofed and the remaining $S_x(t)$ are normal CAVs. It is assumed that th set $S(t)$ is located in the FIFO queue of the coordinator but the knowledge of which clients are spoofed (i.e., $S_{\tilde{x}}(t)$) is unknown. This attack is called a "Sybil Attack."

Let $[t_s^i, t_e^i]$ be the duration when attacker spoofs CAV $i \in S_{\tilde{x}}(t)$ in the network. We assume three types of attacker models:

1) Non-informed attacker: Attacker possesses no knowledge of the infrastructure and vehicle dynamics, and, hence the information sent by the attacker is modeled as follows:
$$\begin{bmatrix} \tilde{\boldsymbol{x}}_{i,k} \\ \tilde{u}_{i,k} \end{bmatrix} \in \mathbb{R}^3,\ \forall t_k \in [t_s^i, t_e^i],\ k \in [1, 2, 3 \dots] \tag{13}$$
2) Infrastructure aware attacker: Has knowledge about the data packet structures, coordination requirements (constraints), and vehicle dynamics and limitations. Thus, the data sent by the adversary is modeled as follows:
$$\begin{bmatrix} \tilde{\boldsymbol{x}}_{i,k} \\ \tilde{u}_{i,k} \end{bmatrix} = \begin{bmatrix} (f(\tilde{\boldsymbol{x}}_{i,k-1}) + g(\tilde{\boldsymbol{x}}_{i,k-1})\tilde{u}_{i,k})\, dt \\ \tilde{u}_i^k \end{bmatrix}$$
$$\forall t_k \in [t_s^i, t_e^i],\ k \in [1, 2, 3 \dots] \tag{14}$$
where dt is the sampling period and $\tilde{u}_i^k \in \mathbb{R}$ s.t. rear end (2), merging constraint (3) and vehicle limitations in (5) and (6) are satisfied. This attacker model is intended to model the situation when an adversary decides to be covert in pursuit of imparting damage to the network without getting detected by trivial checks.
3) Strategic attacker: This model is intended to emulate the scenario when the adversary's aim is to cause havoc in the traffic network in the shortest time possible before getting detected. Hence, the data is generated using the same model as in (14) except that the constraints in (2), (3), (5) and (6) are not always satisfied.

Definition 3: (FDI Attack) Given there are $N(t)$ CAVs in the CZ at any time t. In case of this attack, it is assumed that one or more CAVs are targeted by MiTM attack. Let $[t_{ei}, t_{ef}]$ be the start and end time of the FDI attack and $S_{FDI}(t) \subset S(t)$ be the set of CAVs targeted by the attack whereby the adversary is able to manipulate the data sent by the CAVs to the RSU, or the data sent by the RSU to the CAVs containing state information of the relevant CAVs, or both of them. We define $\boldsymbol{y_i}(t)$ where $t \in [t_{ei}, t_{ef}]$ and $i \in S_{FDI}(t)$ be the data (of CAV i, or data for CAV i containing the information of the relevant CAVs) injected by the adversary during the attack; and $\boldsymbol{z_i}(t)$ where $t \in [t_{ei}, t_{ef}]$ be the actual data (of CAV i sent to the RSU or data for CAV i containing the information of the relevant CAVs sent by the RSU). Then, during the FDI attack, $\boldsymbol{y_i}(t) = g(\boldsymbol{z_i}(t))\ \forall t \in [t_{ei}, t_{ef}]$ where g is the mapping used by the adversary to generate the false data.

Definition 4: (Timing attack) Under normal condition, every CAV i in the CZ receives data about the relevant CAVs from the RSU. During a timing attack on CAV i, it receives the updated state information of the relevant CAVs in the CZ after a period of delay and hence uses the last available information for computing the control command; hence the attack is modelled as following:
$$\tilde{\boldsymbol{z}}_i(k) = \begin{cases} \boldsymbol{z_i}(k) & k \notin T_a \\ (1 - D_s(k))\, \boldsymbol{z_i}(k) + D_s(k)\boldsymbol{z_i}(k-n) & k \in T_a \end{cases} \tag{15}$$
where $\boldsymbol{z_i}(k)$ and $\tilde{\boldsymbol{z}}_i(k)$ are the actual data and data due to timing attack, respectively, n is the packet delay as a count of number of sampling periods after which the packet arrives at the destination (CAV/RSU), T_a is the attack horizon, D_s a binary index that takes a value of 1 to resemble a scenario when a packet is delayed by a timing attack and becomes 0 to resemble a scenario when a packet is not delayed.

IV. Results and Discussion

We first present the results for various attacks simulated for the three aforementioned road networks. Besides the simulated attacks, all attacks in Table II can be used to target each of the three bottleneck points. The simulations were done in Matlab. The parameters for the simulation are listed in Table III where L represents the length of road entries to intersections, merging points and roundabouts. The presented results further highlight the necessity of addressing the security aspect of these cooperative control algorithms for CAVs.

TABLE III: Simulation parameters.

u_{max} (m/s^2)	u_{min}(m/s^2)	v_{max} (m/s)	v_{min} (m/s)	δ (s)	φ (s)	α	λ	Δ (s)	c_3	L (m)
5.98	-5.98	30	0	3.74	1.8	0.9	10	0.1	2	400

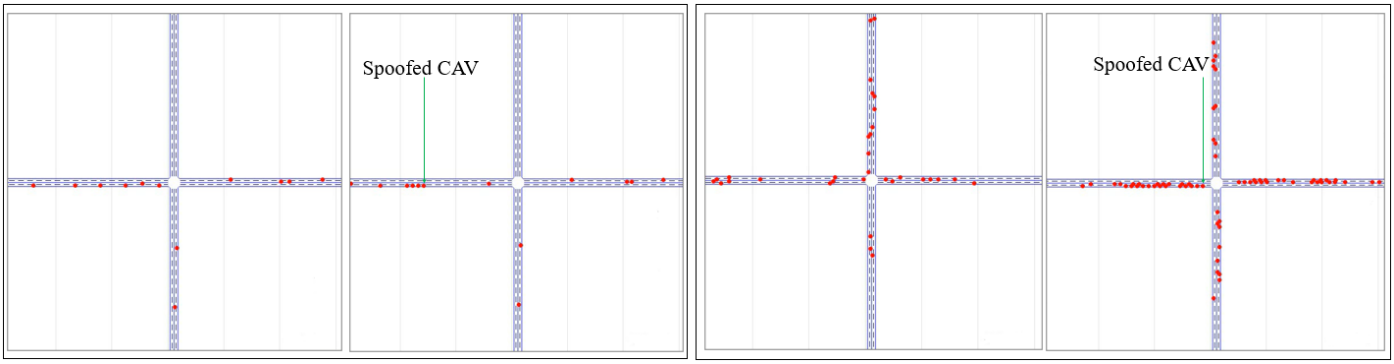

Fig. 4: Result for a Sybil attack with a single Spoofed CAV for intersection problem. The left pair compares the traffic volume in the absence of attack with the adversarial scenario after 30 seconds from the start of simulation. The right pair compares traffic volume between the normal and adversarial scenario after 7 minutes of simulation.

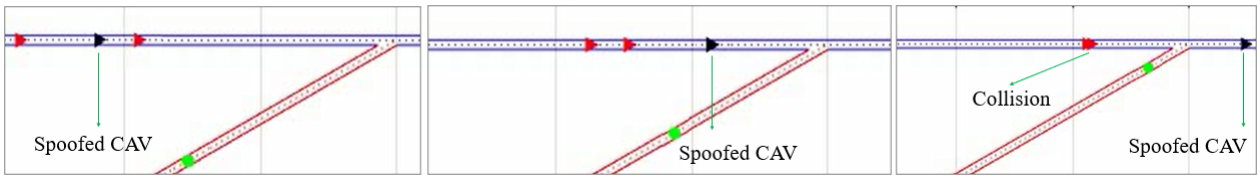

Fig. 5: Result for Sybil attack with a single Spoofed CAV for merging problem. From left to right: Plot showing Spoofed CAV position over time along with the effect of the attack on genuine CAVs.

A. *Sybil Attack:*

1) Adversarial objective: create congestion: During this attack the adversary spawns a fake CAV and registers it in the coordinator queue table. We consider an adversary who is aware of the infrastructure and, hence, generates data (including state and control input information) conforming to all the constraints. However, the adversary creates a scenario where the spoofed CAV is going abnormally slow despite not being physically constrained by a preceding CAV, which causes build up of traffic in the network, as evident from the result in Fig. 4. The presence of a single spoofed CAV not only causes traffic build up in the road it is located at (virtually) but also at other roads due to the cooperative nature of the algorithm which queues CAVs from multiple roads together, thus further highlighting the shortcoming of the FIFO queuing passing policy from security perspective.

2) Adversarial objective: create collision: As part of this attack we consider a strategic adversary who wants to cause havoc in the network in the shortest span of time. With that aim, the adversary spoofs a fake CAV and derives its control input by solving (12), however by setting $u_{ref}(t) = u_{max}$ in the objective and $v_{ref}(t) = v_{max}$ with the aim of maximally accelerating to full speed in shortest span of time, and, to avoid being constrained by any physically preceding CAV the adversary strategically chooses the position of the physically preceding CAV $x_{ip}(t)$ much larger than the true value. The result for the attack is presented in Fig. 5 and Fig. 6 respectively.

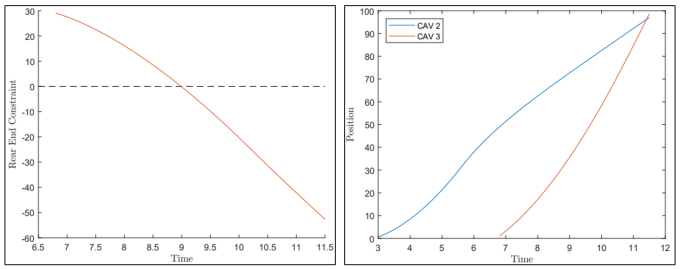

Fig. 6: Result for Sybil attack with a single Spoofed CAV for merging problem. left: plot of rear end safety constraint (negative value denotes collision). right: plot of position of 2nd and 3rd CAV in the presence of a single Spoofed CAV.

From the results, it can be seen that, with the chosen control strategy the spoofed CAV overtakes the CAV ahead of it in the FIFO queue violating its rear end constraint and ultimately creating collision between the CAV physically ahead of it and the CAV it physically precedes. This is also confirmed from the plot of the rear end constraint (Fig. 6) of CAV 3 (the CAV physically following the spoofed CAV in the main lane) given by (2) which becomes negative and is violated as a result of the attack.

B. *FDI attack:*

In the simulated scenario, there are two CAVs in the roundabout that have a common MP. The sequencing is based

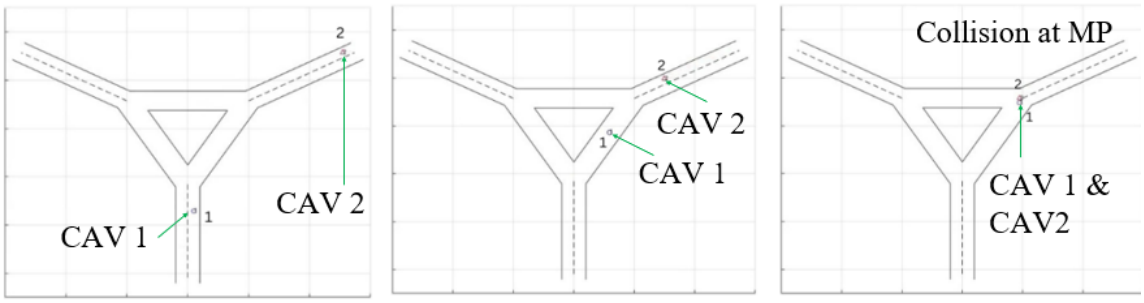

Fig. 7: Result for false data injection attack for roundabout problem. During the attack, the adversary manipulates the data (CAV 1 information) sent by the RSU to CAV 2 by adding a constant bias term to the values resulting in an accident.

on a FIFO queue. The attack was injected by launching a MiTM attack whereby the relevant CAV data sent to CAV 2 (i.e., CAV 1 data as they have a common MP) by the RSU was manipulated by adding a constant bias to true CAV 1 data (including state and acceleration input information), which caused the violation of the merging constraint and resulted in a collision at the MP as shown in Fig. 7.

C. Timing attack:

The attack was simulated for a merging roadway by introducing a delay in the CAV 1 data sent by the RSU to CAV 2, which causes it to decelerate rapidly to avoid violating the rear-end safety constraint due to usage of old information. This causes the CAV immediately following CAV 2 (i.e., CAV 3) to decelerate, and the effect is subsequently propagated to all the CAVs behind it. Upon receiving the updated information of CAV 1, CAV2 accelerates, and the CAVs physically preceding it follow suit. The attack further highlights the security vulnerability of the FIFO queue, which causes the effect of attacks to propagate across the network.

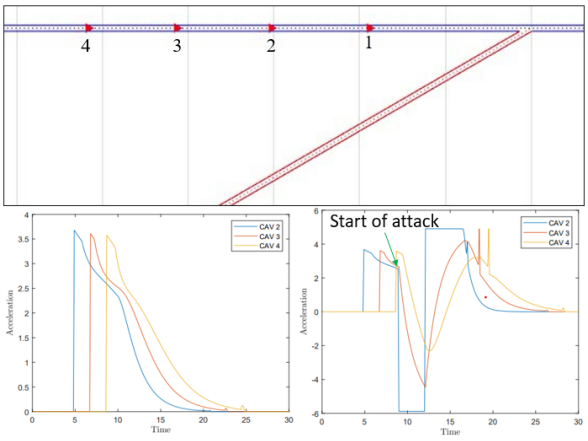

Fig. 8: Result for timing attack for merging problem. The attack was injected by adding a delay to CAV 1 data by 3 seconds which causes CAV 2 to decelerate rapidly, and this causes the CAVs following it to decelerate as well.

V. Conclusion

To conclude, cooperative control algorithms offer many attractive features for addressing traffic congestion at bottleneck points. In this work, we primarily looked at decentralized control algorithms that mainly require V2X communication between CAVs in the network and an RSU unit for safe coordination. We find that the formulation of the coordination problem inherently introduces shortcomings from a security prospective, as summarized below.

1) The lack of a dynamic re-sequencing policy introduces a vulnerability from a security perspective, as demonstrated from the results of a Sybil attack.
2) The coordination formulation lacks any metric that is used as feedback to assess how well traffic from each road is coordinated in the CZ. Hence, if any CAV located in some road in the CZ is targeted by an attack, the effect will be propagated through the whole CZ across all roads.
3) Another shortcoming of the proposed approaches is that the cooperative control algorithms are designed assuming perfect communication.

In addition, we provide an attack taxonomy for V2X communication at bottleneck points, demonstrated through various attack scenarios in simulation that show how the safety and performance of CAVs could be compromised by adversarial attacks. Our future plans include using more realistic simulators in our study, relaxing the assumption of perfect communication and incorporating attack detection and mitigation techniques as well as making the algorithms resilient to cyberattacks.

References

[1] D. W. L. Li and D. Yao, "A survey of traffic control with vehicular communications," *IEEE Trans. on Intelligent Transportation Systems*, vol. 15, no. 1, pp. pp. 425–432, 2013.

[2] C. Gao, G. Wang, W. Shi, Z. Wang, and Y. Chen, "Autonomous driving security: State of the art and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7572–7595, 2022.

[3] D. de Waard, C. Dijksterhuis, and K. Brookhuis, "Merging into heavy motorway traffic by young and elderly drivers," *Accident Analysis & Prevention*, vol. 41, no. 3, pp. pp. 588–597, 2009.

[4] T. L. D. Schrank, B. Eisele and J. Bak, "2015 urban mobility scorecard," 2015.

[5] I. Kavalchuk, A. Kolbasov, K. Karpukhin, A. Terenchenko *et al.*, "The performance assessment of low-cost air pollution sensor in city and the prospect of the autonomous vehicle for air pollution reduction," in *IOP Conference Series: Materials Science and Engineering*, vol. 819, no. 1. IOP Publishing, 2020, p. 012018.

[6] V. A. van den Berg and E. T. Verhoef, "Autonomous cars and dynamic bottleneck congestion: The effects on capacity, value of time and preference heterogeneity," *Transportation Research Part*

B: Methodological, vol. 94, pp. 43–60, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0191261515300643

[7] J. Liu, W. Zhao, and C. Xu, "An efficient on-ramp merging strategy for connected and automated vehicles in multi-lane traffic," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 6, pp. 5056–5067, 2022.

[8] H. Xu, S. Feng, Y. Zhang, and L. Li, "A grouping-based cooperative driving strategy for cavs merging problems," *IEEE Trans. on Vehicular Technology*, vol. 68, no. 6, pp. pp. 6125–6136, 2019.

[9] F. Xu and T. Shen, "Decentralized optimal merging control with optimization of energy consumption for connected hybrid electric vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 6, pp. 5539–5551, 2022.

[10] W. Xiao and C. G. Cassandras, "Decentralized optimal merging control for connected and automated vehicles with optimal dynamic resequencing," in *2020 American Control Conference (ACC)*, 2020, pp. 4090–4095.

[11] W. Xiao, C. G. Cassandras, and C. A. Belta, "Bridging the gap between optimal trajectory planning and safety-critical control with applications to autonomous vehicles," *Automatica*, vol. 129, p. 109592, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109821001126

[12] J. Rios-Torres, A. Malikopoulos, and P. Pisu, "Online optimal control of connected vehicles for efficient traffic flow at merging roads," in *2015 IEEE 18th International Conf. on Intelligent Transportation Systems*. IEEE, 2015, pp. 2432–2437.

[13] R. M. Shukla and S. Sengupta, "Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction application," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, 2018, pp. 688–694.

[14] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (cavs)," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6240–6259, 2022.

[15] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Computers Security*, vol. 109, p. 102269, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821000936

[16] P. Lu, L. Zhang, B. B. Park, and L. Feng, "Attack-resilient sensor fusion for cooperative adaptive cruise control," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 3955–3960.

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

[18] R. A. Biroon, P. Pisu, and Z. Abdollahi, "Real-time false data injection attack detection in connected vehicle systems with pde modeling," in *2020 American Control Conference (ACC)*, 2020, pp. 3267–3272.

[19] S. Boddupalli, A. S. Rao, and S. Ray, "Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–18, 2022.

[20] A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Impact of jamming attacks on vehicular cooperative adaptive cruise control systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 12 679–12 693, 2020.

[21] F. Farivar, M. Sayad Haghighi, A. Jolfaei, and S. Wen, "On the security of networked control systems in smart vehicle and its adaptive cruise control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3824–3831, 2021.

[22] A. Jarouf, N. Meskin, S. Al-Kuwari, M. Shakerpour, and C. G. Cassanderas, "Security analysis of merging control for connected and automated vehicles," in *2022 IEEE Intelligent Vehicles Symposium (IV)*, 2022, pp. 1739–1744.

[23] W. Xiao and C. G. Cassandras, "Decentralized optimal merging control for connected and automated vehicles with safety constraint guarantees," *Automatica*, vol. 123.109333, 2021.

[24] X. Zhao, A. Abdo, X. Liao, M. Barth, and G. Wu, "Evaluating cybersecurity risks of cooperative ramp merging in mixed traffic environments," *IEEE Intelligent Transportation Systems Magazine*, pp. 2–15, 2022.

[25] S. Huang, Y. Feng, W. Wong, Q. A. Chen, Z. Mao, and H. Liu, "Impact evaluation of falsified data attacks on connected vehicle based traffic signal control systems," 01 2021.

[26] Q. A. Chen, Y. Yin, Y. Feng, Z. Mao, and H. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," 01 2018.

[27] J. Reilly, S. Martin, M. Payer, and A. M. Bayen, "Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security," *Transportation Research Part B: Methodological*, vol. 91, pp. 366–382, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0191261516303307

[28] W. Xiao, C. Belta, and C. G. Cassandras, "Decentralized merging control in traffic networks: A control barrier function approach," ser. ICCPS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 270–279. [Online]. Available: https://doi.org/10.1145/3302509.3311054

[29] H. Xu, W. Xiao, C. G. Cassandras, Y. Zhang, and L. Li, "A general framework for decentralized safe optimal control of connected and automated vehicles in multi-lane signal-free intersections," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 17 382–17 396, 2022.

[30] K. Xu, C. G. Cassandras, and W. Xiao, "Decentralized time and energy-optimal control of connected and automated vehicles in a roundabout with safety and comfort guarantees," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–16, 2022.

[31] W. Xiao and C. Belta, "Control barrier functions for systems with high relative degree," in *Proc. of 58th IEEE Conference on Decision and Control*, Nice, France, 2019, pp. 474–479.

[32] Y. Li, Y. Tu, Q. Fan, C. Dong, and W. Wang, "Influence of cyber-attacks on longitudinal safety of connected and automated vehicles," *Accident Analysis Prevention*, vol. 121, pp. 148–156, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0001457518306341

[33] S. Kumar and K. S. Mann, "Prevention of dos attacks by detection of multiple malicious nodes in vanets," in *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, 2019, pp. 89–94.

[34] Y. Zhang and C. G. Cassandras, "A decentralized optimal control framework for connected automated vehicles at urban intersections with dynamic resequencing," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 217–222.

[35] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870517300562

[36] S. S. Albouq and E. M. Fredericks, "Lightweight detection and isolation of black hole attacks in connected vehicles," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2017, pp. 97–104.

[37] K. C. Purohit, S. C. Dimri, and S. Jasola, "Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad-hoc network (vanet)," *Wirel. Pers. Commun.*, vol. 97, no. 4, p. 5099–5114, dec 2017. [Online]. Available: https://doi.org/10.1007/s11277-017-4770-6

[38] P. Kumar, S. Verma *et al.*, "Detection of wormhole attack in vanet," *National Journal of System and Information Technology*, vol. 10, no. 1, p. 71, 2017.

[39] Y. Shoukry, S. Mishra, Z. Luo, and S. Diggavi, "Sybil attack resilient traffic networks: A physics-based trust propagation approach," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*, 2018, pp. 43–54.

[40] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, "Modeling and analysis of eavesdropping attack in 802.11ad mmwave wireless networks," *IEEE Access*, vol. 7, pp. 70 355–70 370, 2019.

[41] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, p. 101823, 2019, recent advances on security and privacy in Intelligent Transportation Systems. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870518309260