A Robust CACC Scheme Against Cyberattacks via Multiple Vehicle-to-Vehicle Networks

Tianci Yang, Member, IEEE, Carlos Murguia, Dragan Nešić, Fellow, IEEE, and Chen Lv, Senior Member, IEEE

Abstract—Cooperative Adaptive Cruise Control (CACC) is a vehicular technology that allows groups of vehicles on the highway to form in closely-coupled automated platoons to increase highway capacity and safety. The underlying mechanism behind CACC is the use of Vehicle-to-Vehicle (V2V) wireless communication networks to transmit acceleration commands to adjacent vehicles in the platoon. However, the use of V2V networks leads to increased vulnerabilities against faults and cyberattacks. Here, we address the problem of increasing the robustness of CACC schemes against cyberattacks by using multiple V2V networks and a data fusion algorithm. The idea is to transmit acceleration commands multiple times through different communication channels to create redundancy at the receiver side. We propose a data fusion algorithm to estimate of the true acceleration command, and isolate compromised channels. Finally, we propose a robust $H_{∞}$ controller that reduces the joint effect of fusion errors and sensor/channel noise in the platooning performance (tracking performance and string stability). Simulation results are presented to illustrate the performance of our approach.

Index Terms—CACC, data fusion, network redundancy, cyberattacks, robust control.

I. INTRODUCTION

For several decades, our society has been continuously confronted with the heavy traffic congestion caused by limited highway capacity. An effective way to increase road capacity is to decrease the inter-vehicle distance. Since this might threaten traffic safety if vehicles are human-driven, vehicle automation is required to guarantee safety [1]. Adaptive Cruise Control (ACC) is a technology that adapts the velocity of vehicles to enforce a desired safe distance to preceding vehicles for platooning. However, ACC induces large inter-vehicle distances [2] and amplifies disturbances (caused, e.g., by sudden acceleration variations of the lead vehicle) in the upstream direction of the platoon, i.e., ACC is string unstable [3]. Cooperative ACC (CACC) solves these challenges by using Vehicle-to-Vehicle (V2V) wireless communication networks to transmit acceleration commands to adjacent vehicles in the platoon. The usage of V2V wireless communications plays an essential role for CACC to guarantee string stability [3], [4], and increase traffic throughput [5]. However, with the surge of vehicle connectivity, new security challenges have emerged as wireless vehicular networks increasingly serve as new access points for adversaries trying to disrupt the vehicle dynamics, see, e.g., [6], [7], [8], [9], [10], [11], and references therein. In the so-called Jeep Cherokee attack [9], researchers were able to remotely stop the engine of the vehicle while it was driving down a busy highway. This forced Chrysler to issue a recall for 1.4 million vehicles of 7 different models leading to an immense financial burden. It is essential to realize that cyberattacks to network-connected vehicles pose a real threat to human life – one vehicle hack could lead to catastrophic loss of life of not only the driver and passengers, but also pedestrians and other drivers. It follows that strategic mechanisms to identify and deal with cyberattacks on connected vehicles are a pressing need in this hyper-connected world.

Most of the current literature on the security of autonomous/connected vehicles focuses on cryptography-based attack prevention solutions, i.e., it provides algorithmic results to design communication protocols for device authentication and data transmission, see, e.g., [12], [13]. Attack prevention indeed plays a very important role in security and deserves our attention. However, since it is impossible to perfectly predict attacker’s behaviors, anomalous intrusion cannot be totally prevented. The enormous financial loss in many incidents due to breached IT defenses has already warned us that attack prevention is far from enough to protect safety-critical Cyber-Physical Systems (CPSs), e.g., CAVs. Hence, secure estimation, attack detection and isolation techniques are essential for reducing the damages caused by attacks when intrusion already occurs. There are only a few results focusing on minimizing the potential performance degradation induced by cyberattacks on network-connected vehicles. In [14], Blockchain and machine-learning techniques are combined to enhance the efficiency of CACC and detecting cyberattacks. Exploiting sensor redundancy, detection and isolation algorithms for a single vehicle under sensor attacks are provided in [15], [16]. In [17], the problem of secure estimation for CAVs in the presence of malicious vehicles is addressed and solved. A sensor fusion algorithm is proposed in [18] for CAVs...
in a platoon under sensor attacks. Similarly, Unbiased Finite Impulse Response (UFIR) filters are used in [19] to address the attack detection and estimation problems in the presence of sensor attacks. The problem of achieving vehicle-consensus in the presence of replay attacks is solved in [20]. The authors in [21] and [22] provide a robust control scheme for platooning under Denial-of-Service (DoS) attacks. They achieve this by modeling DoS attacks as stochastic communication delays in the network. Similarly, a distributed model predictive control scheme is designed for vehicle platoons in the presence of DoS attacks. In [23], a variety of algorithms to detect replay attacks in connected vehicles equipped with CACC are provided. In [24], an algorithm based on set-membership filtering techniques is provided for detecting cyberattacks on connected vehicles. An attack-resilient sensor fusion algorithm is proposed in [25]. The authors use the concept of abstract sensors to obtain multiple measurements of the same physical variable. Each abstract sensor provides a set with all possible values of the true state. Then, an attack-free fused measurement is obtained by checking the intersections of these sets. In [11], the authors suggest switching from CACC to ACC as a potential countermeasure if any abnormal behavior is detected. Here, we provide an alternative solution by creating (and then exploiting) communication channel redundancy in connected vehicles.

In this manuscript, we address the problem of increasing robustness of CACC schemes against cyberattacks by using multiple Vehicle-to-Vehicle (V2V) wireless communication networks and a data fusion algorithm. The idea is to transmit acceleration commands multiple times through different communication networks to create redundancy at the receiver side. However, due to network-induced imperfections (e.g., channel noise and data dropouts) the received data from different channels, will, in general, be different even in the attack-free case. This makes it challenging to distinguish between healthy data coming from adjacent vehicles and corrupted data induced by cyberattacks. To overcome this challenge, we propose a data-fusion algorithm that takes data from all channels, returns an estimate of the true acceleration command, and isolates compromised channels. We provide estimation performance guarantees in terms of the level of uncertainty induced by the communication channels. We prove that our algorithm is guaranteed to work (i.e., it provides an attack-free estimate of acceleration commands), if less than half of the communication channels are under attack. This is a realistic assumption as the adversary may only extract the cypher keys of some of the channels [26], [27], or the attacker may have limited resources. Note that even if the adversary is able to compromise all the channels, she/he may not be able to attack them all at the same time as the power supply is usually limited [28]. We assume that the set of attacked channels is unknown and potentially time-varying. We remark that heavy traffic conditions might not allow a degradation from CACC to ACC since the latter requires a much larger relative distance between vehicles. Hence, the anomaly detection-based CACC scheme, e.g., [14], [19], [23], might have limited applications in some circumstances. Although V2V communication channel redundancy might be costly to create, this is the price to pay for avoiding such a degradation in the presence of cyberattacks.

Note, however, that using estimated acceleration commands for control introduces uncertainty into the loop and thus decreases performance. To minimize this performance degradation, we propose an algorithm that reduces the joint effect of estimation errors and sensor/channel noise in the platooning performance (tracking performance and string stability). In the presence of cyberattacks, we show that a separation principle between data fusion and control holds and the vehicle string can be stabilized by closing the loop with the fusion algorithm and the robust controller. We use Input-to-State Stability (ISS) [29] of the closed-loop system with respect to estimation errors to conclude the stability of the tracking dynamics. Note that compared with [21], [22], [30] where DoS attacks are considered, the results given in this manuscript is more general since it can be used to address any type of deception cyberattacks on V2V networks, e.g., DoS, replay, bias injection attacks etc. [31].

The core of our fusion scheme is inspired by the work in [32], where the problem of state estimation for general continuous-time linear time-invariant (LTI) systems is addressed. The authors propose a multi-observer estimator, using a bank of Luenberger observers, that provides a robust estimate of the state in spite of sensor attacks. The main idea behind their estimation scheme is to place extra sensors in systems to create redundancy. Exploiting sensor/actuator redundancy is a standard technique in the research area of secure estimation and control in cyber-physical systems, see, e.g., [32], [33], [34], [35], [36]. We remark, however, that sensor/actuator redundancy cannot protect connected vehicles from cyberattacks at inter-vehicle communication networks. Modern vehicles equipped with C-V2X communication tools are capable to communicate with each other via 3 G/4 G/5 G and DSRC communication networks [37], [38]. In these modern network channels, interference can be neglected as different frequency bands are allocated [39], [40]. The latter enables the possibility to create network redundancy as multiple copies of the same data can be transmitted via different communication channels. To the best of the authors’ knowledge, none of the existing results have taken advantage of the network redundancy in connected vehicles to improve their resilience to cyberattacks.

The contributions of this manuscript are threefold: 1) instead of degrading from CACC to ACC as suggested in [11], we propose to create V2V communication channel redundancy for mitigating cyberattacks, and propose a secure fusion algorithm that guarantees CACC performance in the presence of cyberattacks; 2) attack detection and isolation algorithms are provided for CAVs when system disturbances are bounded with known bounds; and 3) an optimal $H_{\infty}$ controller is designed for each CAV in the platoon so that the closed-loop dynamics stability is guaranteed and the effect of fusion errors and sensor noise on the CACC tracking and string stability performance is minimized.

The paper is organized as follows. In Section II, some preliminary results needed for the subsequent sections are presented. In Section III, the considered vehicle platoon system is described. In Section IV, we show that our fusion scheme provides robust
estimates of the transmitted signals despite attacks on vehicular networks. Algorithms for detecting and isolating attacked communication channels are presented in Section V. The robust CACC scheme and stability analysis are given in Section VI. Numerical examples are given in Section VII to demonstrate the performance of our methods. Finally, in Section VIII, concluding remarks are given.

II. PRELIMINARIES

We denote the set of natural numbers by \( \mathbb{N} \), the symbol \( \mathbb{R} \) stands for the real numbers, \( \mathbb{R}_{>0} \) (\( \mathbb{R}_{\geq 0} \)) denotes the set of positive (non-negative) real numbers, and \( \mathbb{R}^{n \times m} \) is the set of all \( n \times m \) real matrices, \( m, n \in \mathbb{N} \). For any vector \( v \in \mathbb{R}^n \), we denote \( v^\dagger \) the stacking of all \( v_i, i \in J, J \subset \{1, \ldots, n\} \), \( |v| = \sqrt{v^\dagger v}, ||v||_{\mathcal{L}_p}, \) the signal \( \mathcal{L}_p\)-norm, and \( \text{supp}(v) = \{ i \in \{1, \ldots, n\} | v_i \neq 0 \} \). We denote the cardinality of a set \( S \) as \( \text{card}(S) \). The binomial coefficient is denoted as \( \binom{c}{b} \), where \( a, b \) are non-negative integers. We denote a variable \( m \) uniformly distributed in the interval \( [z_1, z_2] \) as \( m \sim \mathcal{U}(z_1, z_2) \) and normally distributed with mean \( \mu \) and variance \( \sigma^2 \) as \( m \sim \mathcal{N}(\mu, \sigma^2) \). The \( n \times m \) matrices composed of only ones and only zeros are denoted by \( \mathbf{1}_{n \times m} \) and \( \mathbf{0}_{n \times m} \), respectively, or simply \( 1 \) and \( 0 \) when their dimensions are clear.

Definition 1 (Vehicle String Stability): [4] Consider a string of \( m \in \mathbb{N} \) interconnected vehicles. The string is said to be string stable if and only if

\[
||z_i(t)||_{\mathcal{L}_p} \leq ||z_{i-1}(t)||_{\mathcal{L}_p}, \quad \forall \ t \geq 0, \ 2 \leq i \leq m,
\]

(1)

where \( z_i(t) \) can either be the inter-vehicle tracking error \( e_i(t) \), the velocity \( v_i(t) \), or the acceleration \( a_i(t) \) of the \( i\)-th vehicle; \( z_i(0) = 0, \ 2 \leq i \leq m; \) and \( z_i(t) \in \mathcal{L}_p \) is an unknown input signal (e.g., acceleration commands of the lead vehicle in the string or disturbances). That is, a vehicle string is said to be string stable if inputs driving the lead vehicle (acceleration commands and/or disturbances) do not amplify throughout the string.

III. PROBLEM FORMULATION

Consider a platoon of \( m \) vehicles as depicted in Fig. 1. Let \( v_i \in \mathbb{R} \) denote the velocity of vehicle \( i \), and \( d_i \in \mathbb{R} \) be the distance between vehicle \( i \) and its preceding vehicle \( i - 1 \). The objective of each vehicle is to follow the preceding vehicle at the desired distance:

\[
d_{r,i}(k) := r_i + h_iv_i(k), \quad i \in S_m,
\]

(2)

where \( h_i \in \mathbb{R}_{>0} \) denotes the constant head time spacing policy of the \( i\)-th vehicle, and \( r_i \) represents the standstill distance. Define \( S_m := \{ i \in \mathbb{N} | 1 \leq i \leq m \} \) as the set of all vehicles in a platoon of length \( m \in \mathbb{N} \). Including the spacing policy term, \( h_i v_i(k) \), in the desired inter-vehicle distance is known to improve string stability [4], [41]. The spacing error \( e_i \in \mathbb{R} \) is then defined as

\[
e_i(k) := d_i(k) - d_{r,i}(k),
\]

\[
= (q_{i-1} - q_i - L_i) - (r_i + h_iv_i(k)), \quad (3)
\]

with \( q_i \in \mathbb{R} \) being the rear-bumper position of vehicle \( i \) and \( L_i \) its length. It has been proven that the dynamic controller proposed in [4] accomplishes the vehicle-following objective, \( \lim_{k \to \infty} e_i(k) = 0, \forall i \in S_m \), and guarantees string stability. Here, we propose a controller, inspired by the one in [4], that robustifies the platoon against cyberattacks.

As a basis for the controller design, the following vehicle model is adopted [4]:

\[
\begin{bmatrix}
\dot{d}_i \\
\dot{v}_i \\
\dot{a}_i
\end{bmatrix}
= \begin{bmatrix}
v_{i-1} - v_i \\
a_i \\
\frac{1}{\tau_r} a_i + \frac{1}{\tau_r} u_i
\end{bmatrix}, \quad i \in S_m,
\]

(4)

where \( a_i \) is the acceleration of vehicle \( i \), \( u_i \) is the vehicle controller (the desired acceleration), and \( \tau_r \) is a time constant representing the driveline dynamics. Consider the following dynamic controller:

\[
h_i u_i = -u_i + \xi_i,
\]

(5)

with

\[
\xi_i := K_i \begin{bmatrix}
e_i \\
\dot{e}_i \\
\ddot{e}_i
\end{bmatrix}, \quad i \in S_m,
\]

(6)

where \( K_i = [k_{pi} \ k_{di} \ k_{ddi}] \), and \( k_{ddi} = 0 \) (to avoid feedback of jerk). The term \( \ddot{u}_{i-1} \) denotes an estimate of the control input of the preceding vehicle, \( u_{i-1} \). We compute this estimate in real-time using multiple distorted copies of \( u_{i-1} \) (transmitted wirelessly by vehicle \( i - 1 \) via multiple communication networks). In [4], the authors assume that \( u_{i-1} \) can be transmitted directly to vehicle \( i \) free of noise and network effects. However, even in that idealized scenario, if \( u_{i-1} \) is tampered with by cyberattacks, safety cannot be guaranteed. Here, we robustify the controller by transmitting multiple distorted copies of \( u_{i-1} \) (to create redundancy and thus not depending on a single, possibly corrupted, signal) and using this redundant information to construct an estimate \( \ddot{u}_{i-1} \) of \( u_{i-1} \). We use \( \ddot{u}_{i-1} \) as a feedforward term to drive the controller in (6). By doing so, we do not rely on a single signal but we pay the price of working with estimates (thus introducing uncertainty) and having to devise a fusing algorithm that produces accurate approximations of \( u_{i-1} \) and ensure the stability of the platoon in closed-loop with controller (6).
Using (3)–(6), the following platoon model is obtained:

\[
\begin{bmatrix}
\dot{e}_i \\
\dot{v}_i \\
\dot{a}_i \\
\dot{u}_i
\end{bmatrix} =
\begin{bmatrix}
0 & -1 & -h_i & 0 \\
0 & 0 & 1 & 0 \\
k_{pi} & -k_{ai} & -k_{di} & 1/	au_i \\
k_{ai} & k_{ci} & -k_{ci} & -1/	au_i \\
\end{bmatrix}
\begin{bmatrix}
e_i \\
v_i \\
a_i \\
u_i
\end{bmatrix}
+ \begin{bmatrix}1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix}v_{i-1} \\
\dot{a}_{i-1}
\end{bmatrix}.
\]  

(7)

Without loss of generality, we assume \( r_i \) is equal to zero. Here, we assume \( v_{i-1} \) is obtained from on-board sensors of vehicle \( i \) that measure the velocity of vehicle \( i \) and the relative velocity between vehicles \( i \) and \( i - 1 \). We rewrite system (7) compactly in matrix form as follows:

\[
\dot{x}_i = A_{ci} x_i + B_{ci} e_i, 
\]

(8)

with \( x_i := [e_i, v_i, a_i, u_i]^\top \), \( e_i := [v_{i-1}, \dot{a}_{i-1}]^\top \), and matrices \( A_{ci} \) and \( B_{ci} \) defined according to (7).

We assume the first vehicle in the platoon (the leader) does not have a preceding vehicle. Instead, it follows a so-called virtual reference vehicle \( (i = 0) \), allowing the lead vehicle to employ the same controller as the other vehicles in the platoon. We rewrite the virtual vehicle dynamics in matrix form:

\[
\begin{bmatrix}
\dot{e}_0 \\
\dot{v}_0 \\
\dot{a}_0 \\
\dot{u}_0
\end{bmatrix} =
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & -1/\tau_0 & 1/\tau_0 \\
0 & 0 & 0 & 1/\tau_0 \\
\end{bmatrix}
\begin{bmatrix}
e_0 \\
v_0 \\
a_0 \\
u_0
\end{bmatrix} + \begin{bmatrix}0 \end{bmatrix} e_0
\]

(9)

where \( e_0 \) is the desired acceleration of the leader induced by the human driver. We can write the virtual vehicle dynamics in matrix form as follows:

\[
x_0 = A_{co} x_0 + B_{co} e_0, 
\]

(10)

with \( x_0 := [e_0, v_0, a_0, u_0]^\top \), and matrices \( A_{co} \) and \( B_{co} \) defined from (9).

We exactly discretize (7) and (9) at the sampling time instants, \( t = T_s k, k \in \mathbb{N} \), and assume a zero-order hold to implement control actions (see [42] for details) to obtain the following equivalent discrete-time systems:

\[
x_i(k+1) = A_i^d x_i(k) + B_i^d e_i(k), i \in S_m,
\]

(11)

and

\[
x_0(k+1) = A_0^d x_0(k) + B_0^d e_0(k),
\]

(12)

with \( x_i(k) := x_i(T_s k), e_i(k) := e_i(T_s k), k \in \mathbb{N} \), \( A_i^d = e^{A_i T_s} \), and \( B_i^d = (f_i^{T_s} e^{A_i(T_s - \cdot)} ds) B_i^e \), for \( i \in S_m \cup \{0\} \).

We assume the desired acceleration of vehicle \( (i - 1), u_{i-1} \), for \( i \in S_m \setminus \{1\} \), is transmitted from vehicle \( i - 1 \) to vehicle \( i \) through \( N_i \geq 3 \) different unsecured communication channels, i.e., at each time \( k \geq 0 \), vehicle \( i \) receives \( N_i \) distorted copies of

\[
u_{i-1}(k):
\]

\[
U_i(k) = \begin{bmatrix} U_{i1}(k) \\ U_{i2}(k) \\ \vdots \\ U_{iN_i}(k) \end{bmatrix} := \begin{bmatrix} u_{i-1}(k) + \nu_{i1}(k) + \eta_{i1}(k) \\ u_{i-1}(k) + \nu_{i2}(k) + \eta_{i2}(k) \\ \vdots \\ u_{i-1}(k) + \nu_{iN_i}(k) + \eta_{iN_i}(k) \end{bmatrix}
\]

where \( \nu_{ij} \in \mathbb{R}, \{\nu_{ij}(k)\} \in l_{\infty} \), denotes unknown additive perturbations in the \( j \)-th channel, and \( \eta_{ij} \in \mathbb{R}^{N_i} \) is the attack signal that can take any value specified by the attacker, \( j \in \{1, \ldots, N_i\} \). That is, if the \( j \)-th channel is compromised, then \( \eta_{ij}(k) \neq 0 \) for some \( k \geq 0 \); otherwise, \( \eta_{ij}(k) = 0 \) for all \( k \geq 0 \). We let \( W_i(k) \subset \{1, \ldots, N_i\} \) be the time-varying set of attacked communication channels between vehicles \( i \) and \( i - 1 \) at time \( k \), i.e.,

\[\text{supp}(\eta_i(k)) \subseteq W_i(k).\]

(14)

The vector of perturbations, \( \nu_i := (\nu_{i1}, \ldots, \nu_{iN_i}) \in \mathbb{R}^{N_i} \), encompass all network induced imperfections in the channels (e.g., noise, delays, packet dropouts, and quantization). In (13), we are implicitly assuming that the adversary takes full control of the channels in set \( W_i(k) \) by additively injecting a vector \( \eta_i := (\eta_{i1}, \ldots, \eta_{iN_i}) \in \mathbb{R}^{N_i} \), where \( \eta_{ij} \) can take any arbitrary value for \( j = 1, \ldots, N_i \).

Remark 1: The \( N_i \) different communication channels used for transmitting \( u_{i-1} \) can be 4 G, 5 G, and DSRC etc. Because of the large differences between their frequency bands used, every two channels are orthogonal to each other. On the other hand, in most cases, the attacker sends large-power attack signals to increase his/her damages. For instance, in order jam a communication channel, the attacker might need to send signals with the same frequency as the receiving equipment, but with enough large power to override any signal at the receiver [43], [44]. Hence, the interference among different V2V channels is small enough to be neglected.

A. Main Problems

We address and solve the following three problems:

Problem 1: Provide necessary and sufficient conditions under which \( u_{i-1}(k) \) can be reconstructed from \( U_i(k) \), for \( i \in S_m \setminus \{1\} \).

Problem 2: Construct a secure fusion algorithm capable of reconstructing an attack-free estimate of \( u_{i-1}(k) \) from \( U_i(k) \), for \( i \in S_m \setminus \{1\} \) and \( k \geq 0 \).

Problem 3: Design a robust CACC scheme that stabilizes closed-loop platoon dynamics and minimizes the joint effect of fusion errors and sensor noise on the tracking and platoon string stability performance.

The workflow of the proposed robust CACC scheme is shown in Fig. 2.

Remark 2: Different from existing results in the literature, e.g., [32], [33], [34], [35], [36], [45], [46], which assume the set of attacked nodes is time-invariant, here we slightly relax the assumption by allowing the set of attacked communication channels to be time-varying, i.e., the attacker can choose a
different set of communication channels to compromise at each time $k \geq 0$, [28], [47], [48].

IV. SECURE DATA FUSION FOR CONNECTED VEHICLES EQUIPPED WITH MULTIPLE NETWORKS

In this section, we propose a fusion algorithm that exploits communication channel redundancy in connected vehicles to construct a robust estimate $\hat{u}_{i-1}$ of the preceding vehicle’s acceleration commands. To implement the CACC controller (5)–(6), we need the estimate $\hat{u}_{i-1}$ of the acceleration $u_{i-1}$ of the preceding vehicle. What vehicle $i$ receives is the vector $U_i(k)$ containing $N_i$ corrupted copies of $u_{i-1}(k)$ (corrupted by network-induced perturbations and cyberattacks). Here, we seek to reconstruct $u_{i-1}(k)$ from $U_i(k)$ and implement the controller (5)–(6) that uses the reconstructed signal, $\hat{u}_{i-1}(k)$. Then, the first question to raise is whether $u_{i-1}(k)$ is actually reconstructible from $U_i(k)$ (in some appropriate sense).

Definition 2: Consider input $u_{i-1}(k)$ and the vector of distorted inputs $U_i(k)$ in (13) under $q_i$ attacks $\eta_i(k)$, $\supp(\eta_i(k)) \subseteq W_i(k)$. Input $u_{i-1}(k)$ is reconstructible from $U_i(k)$, if for every other input $\bar{u}_{i-1}(k)$ with corresponding $\bar{U}_i(k)$ under $q_i$ attacks and attack vector $\bar{\eta}_i(k)$, $\supp(\bar{\eta}_i(k)) \subseteq W_i(k)$, the following is satisfied:

$$ U_i(k) = \bar{U}_i(k) \implies u_{i-1}(k) = \bar{u}_{i-1}(k). $$

Definition 1 implies that for $u_{i-1}(k)$ and corresponding $U_i(k)$, there is no other $\bar{u}_{i-1}(k) \neq u_{i-1}(k)$ consistent with the received $U_i(k)$. That is, $u_{i-1}(k)$ is reconstructible if it can be uniquely determined from $U_i(k)$.

Theorem 1: For every integer $q_i \geq 0$, the following statements are equivalent:

i) $u_{i-1}(k)$ is reconstructible from $U_i(k)$ under $q_i$ attacks for $k \geq 0$.

Proof: See Appendix A.

From Theorem 1, it follows that the following assumption is needed for any reconstruction scheme to work.

Assumption 1: The number of attacked channels between vehicles $i$ and $(i-1)$ is smaller than $\frac{N_i}{2}$, i.e.,

$$ \text{card}(W_i(k)) \leq q_i < \frac{N_i}{2}. $$

Remark 3: Note that Assumption 1 allows for attacks on all the channels as long as, at every time-step, the number of injected attack signals are strictly less than $\frac{N_i}{2}$. That is, the set of compromised channels can be time-varying as long as a maximum of $q_i < \frac{N_i}{2}$ channels are attacked at every $k \in \mathbb{N}$. This limitation might result from hardware or energy constraints from the adversary’s point of view. For instance, a jamming attack may randomly select one channel to jam for a short period of time [47]; and channel-hopping and pulsed-noise jammers might jam different sets of channels at different time instants [28], [48].

**Corollary 1:** Under Assumption 1, among all $N_i$ communication channels, at least $N_i - q_i$ of them are attack-free; and among every set of $N_i - q_i$ communication channels, at least $N_i - 2q_i$ channels are attack-free.

**Corollary 1** follows trivially from **Assumption 1**.

A. Reconstruction Strategy

Before we present our reconstruction algorithm, we need to introduce some notation and mathematical machinery. For every subset $J \subset \{1, \ldots, N_i\}$ of communication channels and $k \geq 0$, define $\hat{u}_{i,j}(k)$ as the average value of all the data transmitted via $J$ channels at time $k$:

$$ \hat{u}_{i,j}(k) := \frac{\sum_{j \in J} U_{ij}(k)}{\text{card}(J)}; $$

and an (unknown) upper bound on all channel disturbances between vehicles $i$ and $(i-1)$:

$$ ||\nu_k||_\infty := \max_{j \in \{1, \ldots, N_i\}} \{||\nu_{ij}(k)||\}. $$

**Lemma 1:** If $\eta^j_k(k) = 0$, then

$$ |\hat{u}_{i,j}(k) - u_{i-1}(k)| \leq ||\nu_k||_\infty, $$

for all $k \geq 0$.

Proof: See Appendix B.

Under Assumption 1, there exists at least one subset $I(k) \subset \{1, \ldots, N_i\}$ with card($I(k)$) = $N_i - q_i$ such that $\eta^j_k(k) = 0$ for $k \geq 0$. Then, in general, the difference between $\hat{u}_{i,j}(k)$ and any $U_{ij}(k)$ (see (13)), $i \in I(k)$, will be less than the other subsets $J \subset \{1, \ldots, N_i\}$ with $\text{card}(J) = N_i - q_i$ and $\eta^j_k(k) \neq 0$. This motivates the following reconstruction algorithm.

For every subset $J \subset \{1, \ldots, N_i\}$ of channels with $\text{card}(J) = N_i - q_i$, define $\pi_{i,j}(k)$ as the largest difference between $\hat{u}_{i,j}(k)$ and $U_{ij}(k)$ for all $j \in J$, i.e.,

$$ \pi_{i,j}(k) := \max_{j \in J} |\hat{u}_{i,j}(k) - U_{ij}(k)|, $$

for all $k \geq 0$, and the sequence $\sigma_i(k)$ as

$$ \sigma_i(k) := \arg\min_{J \subset \{1, \ldots, N_i\} : \text{card}(J) = N_i - q_i} \pi_{i,j}(k). $$

Then, as proved below, the fused measurement indexed by $\sigma_i(k)$:

$$ \hat{u}_{i-1}(k) = \hat{u}_{\sigma_i(k)}(k), $$

is an attack-free measurement of $u_{i-1}(k)$. The following result uses the terminology presented above.

**Theorem 2:** Consider system (7), and the reconstruction algorithm (20)–(22). Define the reconstruction error $e_{\sigma_i(k)}(k) :=$
\[ \hat{u}_{\sigma_i}(k) - u_{i-1}(k), \] and let Assumption 1 be satisfied; then,
\[ |e_{\sigma_i}(k)| \leq 3||\nu_i||_{\infty}, \] (23)
for all \( k \geq 0. \)

**Proof:** See Appendix C.

**Remark 4:** Note that the fusion algorithm proposed here is
general enough to be applied in all deception cyberattack sce-
narios. Many types of well-known attacks, for instance, replay
attacks, bias injection attacks, DoS attacks can be modeled as
deception attacks [31], which are hence covered in this manuscript.

**Remark 5:** Using multiple V2V communication networks for
data transmission is the basis for our secure fusion algorithm.
Indeed, V2V network redundancy might be costly to create;
however, when signals can be corrupted by adversaries, secure
estimation and control are impossible to accomplish without
data redundancy – this has been rigorously proved by many
authors [32], [33], [34], [35], [36]. Note that CAVs are already
equipped with redundant sensors that provide ‘similar’ position
and orientation information, e.g., lidars, radars, IMUs, GPS, and
cameras. This sensor redundancy, although costly, must be used to
enforce security and safety. The use of extra resources to create
redundancy is not a waste, but the price to pay to guarantee a
high security level in safety-critical systems.

**Remark 6:** The problem that we address is the correct re-
construction of the transmitted signal under deception attacks
using multiple communication channels to create redundancy.
Adding more channels carrying the same information does not
create extra vulnerabilities from the integrity point of view as we
assume up front that the adversary can compromise the original
channel. So, the extra networks actually decrease the system
vulnerability as we might be able to discard all together the
channels corrupted by the adversary. It might create privacy
concerns as there are more copies of the transmitted signals in
the air. However, the kinematic/dynamics data transmitted for
platooning is usually not of private (sensitive) nature. That is,
we do not need to protect against inference attacks to this data
in practice.

V. DETECTION AND ISOLATION

In this section, we now assume bounds on the perturbations in
all channels are known, i.e., \( ||\nu_i||_{\infty} \) for \( j \in \{1, \ldots, N_i\} \),
and \( i \in S_m \setminus \{1\} \) is known. We first provide a simple technique
for detecting attacks on the communication channels. Then, we
use the fusion algorithm presented in Section IV to select the
attack-free channels and isolate the ones that are compromised.

**A. Detection Strategy**

If all the channels are attack-free, then the deviation between
the average value of all the transmitted data and the data trans-
mitted in each single channel will be small, i.e., the difference
between
\[ \sum_{j=1}^{N_i} \frac{U_{ij}(k)}{N_i} \] and \( U_{ij}(k) \), for all \( j \), will be small and
\[ \left| \sum_{j=1}^{N_i} \frac{U_{ij}(k)}{N_i} - U_{ij}(k) \right| \
\]
\[ \leq \left| \frac{\sum_{j=1}^{N_i} U_{ij}(k)}{N_i} - u_{i-1}(k) \right| + |\nu_{ij}(k)| \]
\[ \leq ||\nu_i||_{\infty} + ||\nu_{ij}||_{\infty}, \forall i \in \{1, \ldots, N_i\}. \] (24)

Define a threshold for each communication channel:
\[ \tau_{ij}^d := ||\nu_i||_{\infty} + ||\nu_{ij}||_{\infty}, \] (25)
\( j \in \{1, \ldots, N_i\}. \) Then, attacks are detected at time \( k \) if there
exists at least one channel \( j \in \{1, \ldots, N_i\} \) such that
\[ \left| \frac{\sum_{j=1}^{N_i} U_{ij}(k)}{N_i} - U_{ij}(k) \right| > \tau_{ij}^d, \] (26)
for some \( k \geq 0. \)

**B. Isolation Strategy**

From Section IV, we know that \( \sigma_i(k) \in \{1, \ldots, N_i\} \) is a
set of attack-free communication channels. For \( k \geq 0, \) we
randomly select one channel \( j^*(k) \in \sigma_i(k) \) and the corresponding
\( \eta_{ij^*(k)}(k) \) must satisfy \( \eta_{ij^*(k)}(k) = 0. \) For each \( j \in \{1, \ldots, N_i\} \)
and \( k \geq 0, \) we compute the difference between \( \hat{U}_{ij}(k) \) and \( U_{ij}(k). \) Then, if the \( j \)-th channel is attack-free, i.e., \( \eta_{ij}(k) = 0, \) we have
\[ |U_{ij^*(k)}(k) - U_{ij}(k)| \]
\[ = |U_{ij^*(k)}(k) - u_{i-1}(k) + u_{i-1}(k) - U_{ij}(k)| \]
\[ \leq |U_{ij^*(k)}(k) - u_{i-1}(k)| + |u_{i-1}(k) - U_{ij}(k)| \]
\[ \leq ||\nu_{ij^*(k)}||_{\infty} + ||\nu_{ij}||_{\infty}. \] (27)

For each \( j \in \{1, \ldots, N_i\}, \) define the threshold as follows:
\[ \tau_{ij}(k) := ||\nu_{ij^*(k)}||_{\infty} + ||\nu_{ij}||_{\infty}. \] (28)

Then, for \( k \geq 0, \) the \( j \)-th channel is isolated as an attacked one
if the threshold is crossed, i.e.,
\[ |U_{ij^*(k)}(k) - U_{ij}(k)| > \tau_{ij}(k). \] (29)

Then, the set of channels that are isolated as the attacked ones
at time \( k, \) which we denote as \( \hat{W}_i(k), \) is given as:
\[ \hat{W}_i(k) := \{ i \in \{1, \ldots, N_i\} ||U_{ij^*(k)}(k) - U_{ij}(k)| > \tau_{ij}(k) \}. \] (30)

VI. ROBUST CONTROLLER AND SECURE ESTIMATOR

We have shown that the error of the proposed fusion algo-
rithm is bounded independently of the attacks if the conditions of
Theorem 2 are satisfied. In this section, we assume that the
on-board sensors of each vehicle in the platoon are noisy as
well and each vehicle uses the estimates provided by the
fusion algorithm for control as shown in Fig. 3. For each ve-
vehicle in the platoon, we design a \( H_{\infty} \) controller to stabilize
its closed-loop dynamics while minimizing the effect of the
error introduced by the fusion algorithm and sensor noise on
string stability and tracking performance. We consider system
(7) and assume the on-board sensors of vehicle \( i \) that measure
relative distance and relative velocity are subject to noise \( \omega_{d1} \)
and \( \omega_{v1}, \) respectively. We assume a zero-order hold is used
We remark that the controllers we use are actually $(32) \tilde{A}_i, \tilde{B}_i, \tilde{C}_i$ as defined in Theorem 7. System constrained to satisfy $-\tilde{T}_i = \tilde{A}_i + \tilde{B}_i$ is used to drive the controller. Let $\tilde{\omega}_i = \tilde{u}_i - \tilde{v}_i$ characterizes the performance output, $\tilde{u}_i = e_{\sigma_i(k)} + e_{\sigma_i(k)}$ as defined in Theorem 2 for $t \in [kT_s, (k+1)T_s)$, for all $i \in S_m$. Then, the closed-loop dynamics can be written as follows:

$$\begin{bmatrix}
\dot{e}_i \\
\dot{v}_i \\
\dot{a}_i \\
\dot{u}_i
\end{bmatrix} =
\begin{bmatrix}
0 & -1 & -h_i & 0 \\
0 & 0 & 1 & 0 \\
-\frac{k_{pi}}{\nu_i} & -\frac{k_{di}}{\nu_i} & -k_{di} & -\frac{1}{\nu_i} \\
-\frac{k_{pi}}{\nu_i} & 0 & \frac{k_{di}}{\nu_i} & \frac{1}{\nu_i}
\end{bmatrix}
\begin{bmatrix}
e_i \\
v_i \\
a_i \\
u_i
\end{bmatrix}
+ \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
-\frac{k_{pi}}{\nu_i} & \frac{k_{di}}{\nu_i} & \frac{1}{\nu_i}
\end{bmatrix}
\begin{bmatrix}
\omega_{d_i} \\
v_{i-1} + \omega_{vi} \\
u_{i-1} + e_{\sigma_i(k)}
\end{bmatrix}. \quad (31)
$$

Let $\omega_i := [\omega_{d_i}, v_{i-1} + \omega_{vi}, u_{i-1} + e_{\sigma_i(k)}]^T$. To implement the design method provided in [49], we rewrite the system in the following way:

$$\begin{align*}
\dot{x}_i &= \tilde{A}_i x_i + \tilde{B}_i w_i + \tilde{B}_2 u_i, \\
z_i &= \tilde{C}_i x_i, \\
y_i &= \tilde{C}_2 x_i + \tilde{D}_2 w_i, \\
\tilde{u}_i &= K_i y_i,
\end{align*} \quad (32)$$

with

$$\begin{bmatrix}
0 & -1 & h_i & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & -\frac{1}{\nu_i} & \frac{1}{\nu_i} \\
0 & 0 & 0 & -\frac{1}{\nu_i}
\end{bmatrix}, \quad \tilde{C}_2 = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & -1 & -h_i & 0
\end{bmatrix},
$$

$$\begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
-\frac{k_{pi}}{\nu_i} & \frac{k_{di}}{\nu_i} & \frac{1}{\nu_i}
\end{bmatrix}, \quad \tilde{D}_2 = \begin{bmatrix}
0 \\
0 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{bmatrix},$$

$$K_i = \begin{bmatrix}
k_{pi} & k_{di}
\end{bmatrix} \quad (33)$$

where $z_i$ is the performance output we seek to optimize. To minimize the effect of $\omega_i$ on string stability and tracking performance, we let $\tilde{C}_{ii}$ in (32) be given as

$$\tilde{C}_{ii} = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{bmatrix}. \quad (34)$$

This choice of $\tilde{C}_{ii}$ characterizes the performance output, $z_i = \tilde{C}_{ii} x_i$, and let us weigh simultaneously the effect of $\omega_i$ on the tracking error, $e_i$, and the velocity of the vehicle, $v_i$, for string stability. We seek to synthesize the controller gains, $(k_{pi}, k_{di})$, to minimize the $H_\infty$ norm from the vector of disturbances, $\omega_i$, to the performance output, $z_i = \tilde{C}_{ii} x_i$. To obtain such optimal gains, we use the reformulation in (31)–(34) and Algorithms 3 and 4 in [49] to satisfy $k_{pi}, k_{di} > 0$, and $k_{di} > k_{pi} \tau_i$ to guarantee the vehicle following control objective [4]. This emulation-based controller is able to stabilize (7) when $T_s$ is sufficiently small [50].

**Remark 7:** We remark that the controllers we use are actually standard state feedback controllers. The switching aspect arises when selecting what communication channels we ‘trust’ are transmitting attack-free data (as we use this data to feed the controller). Because the set of trusted channels might change over time (due to network effects and attacks), the scheme creates a switching behaviour in the controller. Summarizing, the controller is not switching by itself, we take a standard (non-switching) controller from the literature, and change the data we use to drive it based on our switching fusion algorithm which selects attack-free channels.

### A. Stability Analysis

Here, we give a brief statement on the stability of the interconnected vehicles when the secure fused measurement given by (20)–(22) is used to drive the controller. Let $x_i = [e_i, v_i, a_i, u_i]^T$ and $\tilde{e}_i = [\omega_{d_i}, v_{i-1} + \omega_{vi}, u_{i-1} + e_{\sigma_i(k)}]^T$. System (31) can be written as:

$$\dot{x}_i = A_{ci} x_i + \tilde{B}_i \tilde{e}_i, \quad (35)$$

with

$$A_{ci} = \begin{bmatrix}
0 & -1 & h_i & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & \frac{1}{\nu_i} & \frac{1}{\nu_i} \\
0 & 0 & 0 & -\frac{1}{\nu_i}
\end{bmatrix}, \quad \tilde{B}_i = \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
-\frac{k_{pi}}{\nu_i} & \frac{k_{di}}{\nu_i} & \frac{1}{\nu_i}
\end{bmatrix}. \quad (36)$$

The closed-loop dynamics (35) is Input-to-State-Stable (ISS) with input $\tilde{e}_i$, because $A_{ci}$ is a Hurwitz matrix [29]. As we have proved in Theorem 2 that $e_{\sigma_i(k)}$ is bounded for all $k \geq 0$, if $||x_{i-1}||_{\infty}$ is bounded, then $||\tilde{e}_i||_{\infty}$ is bounded, which then implies the boundedness of $||x_i||_{\infty}$ since (35) is ISS. Therefore, the boundedness of $||x_{i-1}||_{\infty}$ implies the boundedness of $||x_i||_{\infty}$ for $i \in S_m$. From the fact that the state of the virtual reference vehicle is bounded, i.e., $||x_i||_{\infty}$ is bounded, we conclude the boundedness of $||x_i||_{\infty}$ for all $i \in S_m$ [29].

### VII. SIMULATION

In this section, numerical examples are used to illustrate the effectiveness of our approaches. In particular, in Examples 1 and 2, we test the performance of our data fusion and isolation schemes provided in Sections IV and V respectively by considering a simple case when the platoon consists of two vehicles and three communication channels are used between them. At each time instant, one of the communication channels is under attack.
We consider a platoon of 2 vehicles. We let $\nu \sim \nu \nu \hat{W}$ that the obtained estimates $\hat{W}$ are only sufficient conditions for the detection and isolation algorithms to work respectively. This might lead the proposed algorithms conservative due to the perturbations in the communication channels. Example 2 illustrates that the algorithms still detect and isolate attacked channels relatively well under reasonable conditions.

**Example 3:** We consider a homogeneous vehicle platoon consisting of 5 vehicles. We let $h_1 = 0.5$, $\tau_1 = 0.1$, for all $i \in \{1, 2, 3, 4, 5\}$. $T_s = 0.01$ seconds, and $N_i = 3$ communication channels between vehicles, $i \in \{2, 3, 4, 5\}$. Channel and sensor perturbations are taken as $\nu_{1i} \sim \mathcal{U}(-0.1, 0.1)$, $\nu_{12} \sim \mathcal{U}(-0.2, 0.2)$, $\nu_{13} \sim \mathcal{U}(-0.3, 0.3)$, and $\omega_{1i}, \omega_{i1} \sim \mathcal{U}(-0.1, 0.1)$. Let $e_0$ be given as in Table I. At each time step $k$, let one of the 3 communication channels between the two vehicles be randomly selected to be attacked, i.e., $W_3(k) = \{1\}$, $W_2(k) = \{1\}$, or $W_1(k) = \{1\}$ and let $\eta W_i(k) \sim \mathcal{N}(0, 5^2)$. Then, $||\nu||_\infty = 0.3$, and $||\nu_1||_\infty = 0.1, ||\nu_2||_\infty = 0.2, ||\nu_3||_\infty = 0.3$. From equation (25), we can compute $\tau_{21} = 0.4, \tau_{22} = 0.5, \tau_{23} = 0.6$ accordingly. For $k \in [1, 400]$, (25)–(26) are used for attack detection and it turns out that 371 out of 400 time steps our detection algorithm successfully detects the attacks. For $k \in [1, 20]$, (28)–(30) are used for isolating the attacked channels. The performance of our isolation algorithm is presented in Fig. 5, where it is shown that our algorithm successfully isolates the attacked channel 14 out of 20 time steps for the considered time-varying attacks.

**Remark 9:** Note that (26) and (29) are only sufficient conditions for the detection and isolation algorithms to work respectively. This might lead the proposed algorithms conservative due to the perturbations in the communication channels. Example 2 illustrates that the algorithms still detect and isolate attacked channels relatively well under reasonable conditions.

**Example 3:** We consider a homogeneous vehicle platoon consisting of 5 vehicles. We let $h_1 = 0.5$, $\tau_1 = 0.1$, for all $i \in \{1, 2, 3, 4, 5\}$. $T_s = 0.01$ seconds, and $N_i = 3$ communication channels between vehicles, $i \in \{2, 3, 4, 5\}$. Channel and sensor perturbations are taken as $\nu_{1i} \sim \mathcal{U}(-0.1, 0.1)$, $\nu_{12} \sim \mathcal{U}(-0.2, 0.2)$, $\nu_{13} \sim \mathcal{U}(-0.3, 0.3)$, and $\omega_{1i}, \omega_{i1} \sim \mathcal{U}(-0.1, 0.1)$. Let $e_0$ be given as in Table I. At each time step $k$, let one of the 3 communication channels between the two vehicles be randomly selected to be attacked, i.e., $W_i(k) = \{1\}$, $W_2(k) = \{1\}$, or $W_1(k) = \{1\}$ and let $\eta W_i(k) \sim \mathcal{N}(0, 5^2)$ for $i \in \{2, 3, 4, 5\}$. For all $k \geq 0$, the $i$-th vehicle $i \in \{2, 3, 4, 5\}$ attacked channels can be tolerated. In this case, our algorithm can still guarantee an attack-free estimate as long as Assumption 1 holds, as proved in Theorem 2.

![Fig. 4](image-url)  

**Fig. 4.** $u_{i-1}$ (black) and $\hat{u}_{i-1}$ (blue).

**Fig. 5.** Actual attacked channel (‘o’) and the isolated channel (‘x’).

| $e_0$ ($m/s^2$) | Time (seconds) |
|-----------------|----------------|
| -10             | 0.5            |
| 0               | 5.10           |
| -10             | 10.15          |
| 0               | 15.20          |

Table I

**Desired Acceleration of the Leader**
uses (20)–(22) for fusing measurements of $u_{i-1}(k)$, and the CACC switching controller (3)–(6) to close the loop.

We use algorithms 3 and 4 in [49] to design a robust controller for each vehicle in the platoon with the smallest achievable $H_\infty$ norm of $\gamma = 1.0198$, and corresponding optimal $k_{pi} = 5.002$ and $k_{di} = 305.1862$, for $i \in S_m$. The performance of the robust controller is shown in Figs. 6–7. For comparison, the performance of the controller in [4] with $k_{pi} = 0.2$, $k_{di} = 0.7$ is shown in Figs. 8–9. Note that the controller gains in [4] are selected with a comfort concern, and the $H_\infty$ gain from $\omega_i$ to $z_i$ is 5.1000. In Fig. 6, the peak speed values of vehicles 1–5 are strictly non-increasing, which obeys string stability. On the other hand, from Fig. 8, it can be seen that the peak speed value of vehicle 5 exceeds the one of vehicle 4, which violates string stability. Besides, the tracking errors of vehicles 1–5 in Figs. 7 are closed to zero, which are much smaller than the ones shown in Fig. 9. This shows that the $H_\infty$ controller provided here provides a more robust performance in the presence of system disturbances compared with the one given in [4].

VIII. CONCLUSION

We have addressed the problem of data fusion, attack detection and isolation, and robust control for connected vehicles whose communication channels are under (potentially unbounded) cyberattacks. We suggest creating redundancy of inter-vehicle communication channels for connected vehicles to enhance their resilience to cyberattacks so that degradation from CACC to ACC can be avoided. Exploiting network redundancy, we have proposed a data fusion framework that reconstructs the transmitted data via the networks with bounded errors independent of attacks on the communication networks. This fused information is then used to detect and isolate attacks and stabilize the closed-loop dynamics of each vehicle. An $H_\infty$ controller is designed for each vehicle in a platoon to stabilize its closed-loop dynamics while minimizing the effects of sensor noise and fusion errors on string stability and tracking performance.
APPENDIX A
PROOF OF THEOREM 1

(i) → (ii) We proceed by contraposition. Assume \( q_i \geq \frac{N_i}{2} \), then for all \( W_i(k) \subset \{1, \ldots, N_i\} \), with \( \text{card}(W_i(k)) = q_i \) and \( k \geq 0 \), there exists another set \( \tilde{W}_i(k) \subset \{1, \ldots, N_i\} \) with \( \text{card}(\tilde{W}_i(k)) = q_i \) such that \( W_i(k) \cup \tilde{W}_i(k) = \{1, \ldots, N_i\} \) since \( 2q_i \geq N_i \). Let \( I_i(k) = W_i(k) \cap \tilde{W}_i(k) \). For all \( u_{i-1}(k) \neq u_{i-1}(k) \), with corresponding \( \tilde{U}_i(k) = 1_{\tilde{u}_{i-1}(k)}(k) + v_{i-1}(k) + \tilde{\eta}_i(k) \) and \( U_i(k) = 1_{u_{i-1}(k)}(k) + v_{i-1}(k) + \eta_i(k) \), we seek \( \tilde{\eta}_i(k) \) and \( \eta_i(k) \) such that \( \tilde{U}_i(k) = U_i(k) \). If such attack vectors exist, we can conclude that \( q_i \geq \frac{N_i}{2} \) implies \( u_{i-1}(k) \) is not reconstructible from \( U_i(k) \) (according to Definition 1), and thus, by contraposition, \( q_i < \frac{N_i}{2} \) implies \( u_{i-1}(k) \) is reconstructible [51]. For \( \tilde{u}_{i-1}(k) = u_{i-1}(k) \), let

\[
j \in \{ \tilde{W}_i(k) \setminus I_i(k) \} : \begin{cases} \tilde{\eta}_j(k) = u_{i-1}(k) - \tilde{u}_{i-1}(k), \\ \eta_j(k) = 0, \\ \eta_j(k) = \tilde{u}_{i-1}(k) - u_{i-1}(k), \\ \eta_j(k) = 0, \\ \eta_j(k) = \tilde{u}_{i-1}(k) - u_{i-1}(k), \\ \eta_j(k) = \tilde{u}_{i-1}(k) - u_{i-1}(k). \end{cases}
\]

It is easy to verify that these particular \( \tilde{\eta}_i(k) \) and \( \eta_i(k) \) satisfy \( u_{i-1}(k) \neq \tilde{u}_{i-1}(k) \) and \( U_i(k) = \tilde{U}_i(k) \), for all \( k \geq 0 \), and the result follows.

(ii) → (i) Let \( q_i < \frac{N_i}{2} \). For all \( \eta_i(k) \) and \( \tilde{\eta}_i(k) \) with \( \text{card}(\text{supp}(\eta_i(k))) \leq q_i \) and \( \text{card}(\text{supp}(\tilde{\eta}_i(k))) \leq q_i \), the number of nonzero elements of the difference, \( \eta_i(k) - \tilde{\eta}_i(k) \), is less than or equal to \( 2q_i \), which is strictly less than \( N_i \). Therefore, there does not exist \( u_{i-1}(k) \neq \tilde{u}_{i-1}(k) \) such that

\[
\eta_i(k) - \tilde{\eta}_i(k) = \begin{bmatrix} u_{i-1}(k) - \tilde{u}_{i-1}(k) \\ u_{i-1}(k) - \tilde{u}_{i-1}(k) \\ \vdots \\ u_{i-1}(k) - \tilde{u}_{i-1}(k) \end{bmatrix} \geq \begin{bmatrix} u_{i-1}(k) - \tilde{u}_{i-1}(k) \\ u_{i-1}(k) - \tilde{u}_{i-1}(k) \\ \vdots \\ u_{i-1}(k) - \tilde{u}_{i-1}(k) \end{bmatrix},
\]

because the number of nonzero elements on the right side of (37) has to be strictly less than \( N_i \), which indicates that there does not exist \( u_{i-1}(k) \neq \tilde{u}_{i-1}(k) \) such that \( U_i(k) = \tilde{U}_i(k) \), i.e.,

\[
\begin{bmatrix} u_{i-1}(k) + \nu_{i1}(k) \\ u_{i-1}(k) + \nu_{i2}(k) \\ \vdots \\ u_{i-1}(k) + \nu_{iN}(k) \end{bmatrix} + \eta_i(k) = \begin{bmatrix} \tilde{u}_{i-1}(k) + \nu_{i1}(k) \\ \tilde{u}_{i-1}(k) + \nu_{i2}(k) \\ \vdots \\ \tilde{u}_{i-1}(k) + \nu_{iN}(k) \end{bmatrix} + \tilde{\eta}_i(k).
\]

Hence, \( u_{i-1}(k) \) is reconstructible from \( U_i(k) \) under \( q_i \) attacks (according to Definition 1).

APPENDIX B
PROOF OF LEMMA 1

By construction and the triangle inequality

\[
\sum_{j=1}^{n} \nu_{ij} = \sqrt{(\nu_{i1} + \nu_{i2} + \cdots + \nu_{in})^2} = \sqrt{\nu_{i1}^2 + \nu_{i2}^2 + \cdots + \nu_{in}^2 + 2(\nu_{i1}\nu_{i2} + \cdots + \nu_{i(n-1)}\nu_{in})}
\]

\[
\leq \sqrt{\nu_{i1}^2 + \nu_{i2}^2 + \cdots + \nu_{in}^2 + (\nu_{i1}^2 + \nu_{i2}^2 + \cdots + \nu_{i(n-1)}^2 + \nu_{in}^2)} = \sqrt{\left(1 + \left(\frac{1}{n-1}\right)\right)(\nu_{i1}^2 + \nu_{i2}^2 + \cdots + \nu_{in}^2)}
\]

\[
\leq \sqrt{n^2||\nu_i||_\infty^2} = n||\nu_i||_\infty.
\]

It follows that

\[
|\hat{\nu}_{ij}(k) - u_{i-1}(k)| = \frac{\sum_{j \in j} U_{ij}(k)}{\text{card}(J)} - u_{i-1}(k) \leq \frac{1}{\text{card}(J)} \sum_{j \in j} \nu_{ij}(k) \leq \frac{1}{\text{card}(J)} \text{card}(J)||\nu_i||_\infty = ||\nu_i||_\infty.
\]

APPENDIX C
PROOF OF THEOREM 2

Under Assumption 1, there exists at least one subset \( \tilde{I}(k) \subset \{1, \ldots, N_i\} \) with \( \text{card}(\tilde{I}(k)) = N_i - q_i \) such that \( \eta_{\tilde{I}(k)}(k) = 0 \) for \( k \geq 0 \). Then

\[
|\hat{\nu}_{\tilde{I}(k)}(k) - u_{i-1}(k)| \leq ||\nu_i||_\infty.
\]

Moreover, for all \( j \in I(k) \), \( \eta_j(k) = 0 \) and we have

\[
|U_{ij}(k) - u_{i-1}(k)| = ||\nu_{ij}(k)||.
\]

Then, we have

\[
\pi_{i\tilde{I}(k)}(k) = \max_{j \in I(k)} |\hat{\nu}_{\tilde{I}(k)}(k) - U_{ij}(k)| = \max_{j \in I(k)} |\hat{\nu}_{\tilde{I}(k)}(k) - u_{i-1}(k) + u_{i-1}(k) - U_{ij}(k)|
\]

\[
= |\hat{\nu}_{\tilde{I}(k)}(k) - u_{i-1}(k)| + \max_{j \in I(k)} |u_{i-1}(k) - U_{ij}(k)|
\]

\[
\leq ||\nu_i||_\infty + \max_{j \in I(k)} ||\nu_{ij}(k)||. \tag{43}
\]

From Corollary 1, among every \( N_i - q_i \) communication channels, at least one of the channels is attack-free since \( N_i - 2q_i \geq 1 \). Therefore, there exists at least one \( \tilde{j}(k) \in \sigma_i(k) \) such that \( \eta_{\tilde{j}(k)}(k) = 0 \) for \( k \geq 0 \) and

\[
|U_{\tilde{j}(k)}(k) - u_{i-1}(k)| = ||\nu_{\tilde{j}(k)}(k)||. \tag{44}
\]

From (21), we have \( \pi_{i\sigma_i}(k) \leq \pi_{i\tilde{I}(k)}(k) \). From (20), we have

\[
\pi_{i\sigma_i}(k) = \max_{j \in \sigma_i(k)} |\hat{\nu}_{\sigma_i(k)}(k) - U_{ij}(k)|
\]

\[
\geq |\hat{\nu}_{\sigma_i(k)}(k) - U_{\tilde{j}(k)}(k)|. \tag{45}
\]

Using the lower bound on \( \pi_{i\sigma_i}(k) \) and the triangle inequality, we have that

\[
|e_{\sigma_i(k)}(k)| = |\hat{\nu}_{\sigma_i(k)}(k) - u_{i-1}(k)|
\]
\[
\begin{align*}
&= \left| \dot{\sigma}_i(k) - U_{ij}(k) + U_{i\bar{j}}(k) - u_{i-1}(k) \right| \\
&\leq \pi_{\sigma_i}(k) + |\nu_{ij}(k)| \\
&\leq \pi_{\sigma_i}(k) + |\nu_{ij}(k)| \\
&\leq \|\nu|| + \max_{j \in [\bar{i}]} |\nu_{ij}(k)| + |\nu_{i\bar{j}}(k)| \\
&\leq 3\|\nu||. 
\end{align*}
\]

Inequality (46) is of the form (23) and the result follows.

REFERENCES

[1] C. Huang et al., “Personalized trajectory planning and control of lane-change maneuvers for autonomous driving,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 5511–5523, Jun. 2021.
[2] A. Vahidi and A. Eskandarian, “Research advances in intelligent collision avoidance and adaptive cruise control,” IEEE Trans. Intell. Transp. Syst., vol. 4, no. 3, pp. 143–153, Sep. 2003.
[3] G. J. L. Naas, R. P. A. Vugts, J. Ploeg, M. J. G. van De Molengraft, and M. Steinbuch, “String-stable CACC design and experimental validation: A frequency-domain approach,” IEEE Trans. Veh. Technol., vol. 59, no. 9, pp. 4268–4279, Nov. 2010.
[4] J. Ploeg, N. Van De Wouw, and H. Nijmeijer, “LP string stability of cascaded systems: Application to vehicle platooning,” IEEE Trans. Control System Technol., vol. 22, no. 2, pp. 786–793, Mar. 2014.
[5] B. Van Arem, C. J. Van Driel, and R. Versin, “The impact of cooperative adaptive cruise control on traffic-flow characteristics,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 1, pp. 300–311, Feb. 2017.
[6] Z. El-rewini, K. Sadatsharan, D. Flora, S. Jose, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” Veh. Commun., vol. 23, 2020, Art. no. 100214.
[7] C. Laurendeau and M. Barbeau, “Threats to security in DSRC/wave,” in Proc. IEEE 55th Conf. Decis. Control, pp. 7757–7762, Sep. 2016.
[8] J. Dofe, J. Frey, H. Pahlavanazadeh, and Q. Yu, “Strengthening simion implementation against intelligent fault attacks,” IEEE Embedded Syst. Lett., vol. 7, no. 4, pp. 113–116, Dec. 2015.
[9] Z. A. Biron, S. Dey, and P. Pisu, “Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control,” in Proc. IEEE Annu. Amer. Control Conf., 2018, pp. 5582–5587.
[10] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, “Distributed cyber attacks detection and recovery mechanism for vehicle platooning,” IEEE Trans. Intell. Transp. Syst., vol. 21, no. 9, pp. 3821–3834, Sep. 2020.
[11] R. Ivanov, M. Pajic, and I. Lee, “Attack-resistant sensor fusion for safety-critical cyber-physical systems,” ACM Trans. Embedded Comput. Syst., vol. 15, no. 1, pp. 1–24, 2016.
[12] A. Vahidi and A. Eskandarian, “Research advances in intelligent collision avoidance and adaptive cruise control,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 1, pp. 300–311, Feb. 2017.
[13] C. Huang et al., “Personalized trajectory planning and control of lane-change maneuvers for autonomous driving,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 5511–5523, Jun. 2021.
[14] G. Raja, K. Kottursamy, K. Dev, R. Narayanan, A. Raja, and K. B. V., “Remote exploitation of an unaltered passenger vehicle,” Black Hat USA, vol. 15, pp. 1–91, 2015.
[15] A. Greenberg, “Hackers remotely kill a jeep on the highway—with me in it,” Wired, vol. 7, p. 21, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[16] J. Petitt and S. E. Shladover, “Potential cyberattacks on automated vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546–556, Apr. 2015.
[17] M. Amoazadeh et al., “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” IEEE Commun. Mag., vol. 53, no. 6, pp. 126–132, Jul. 2015.
[18] C.-M. Chen, B. Xiang, Y. Liu and K.-H. Wang, “A secure authentication protocol for internet of vehicles,” IEEE Access, vol. 7, pp. 12047–12057, 2019.
[19] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibáñez, “Internet of vehicles: Architecture, protocols, and security,” IEEE Internet Things J., vol. 5, no. 5, pp. 3701–3709, Oct. 2018.
[20] L. Vlajic, L. Liu, L. Deng, S. Yin, and S. Wei, “Against double fault attacks: Injection effect model, space and time randomization based countermeasures for reconfigurable array architecture,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1151–1164, Jun. 2016.
[21] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: A survey,” Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197–215, 2014.
[22] E. D. Sontag, “Input to state stability: Basic concepts and results,” in Nonlinear and Optimal Control Theory, Berlin, Germany: Springer, 2008, pp. 163–220.
[23] M. H. Basiri, N. L. Azad, and S. Fischmeister, “Attack resilient heterogeneous vehicle platooning using secure distributed nonlinear model predictive control,” in Proc. IEEE 28th Mediterranean Conf. Control Automat., 2020, pp. 307–312.
[24] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” Automatica, vol. 51, pp. 135–148, 2015.
[25] M. S. Chong, M. Wakaiki, and P. Hespahna, “Observability of linear systems under adversarial attacks,” in Proc. IEEE Amer. Control Conf., 2015, pp. 2439–2444.
[26] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” IEEE Trans. Autom. Control, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.
[27] Y. Shoukry, P. Nuzzo, A. Paggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, “Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach,” IEEE Trans. Autom. Control, vol. 62, pp. 4917–4932, Oct. 2017.
[28] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, “Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems,” in Proc. IEEE 55th Conf. Decis. Control, 2016, pp. 1297–1302.
[29] T. Yang, C. Murguia, M. Kuijper, and D. Nešić, “A multi-observer based estimation framework for nonlinear systems under sensor attacks,” Automatica, vol. 119, 2020, Art. no. 109043.
[30] K. Abboud, H. A. Omar, and W. Zhuang, “Interworking of DSRC and cellular network technologies for V2X communications: A survey,” IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 9457–9470, Dec. 2016.
[31] E. Ghafar, A. Fuchs, D. Ehlenkamp, and D. N. Alòe, “A vehicular rooftop, shark-fin, multiband antenna for the GPS/LTE/cellular/DSRC systems,” in Proc. IEEE-APS Topical Conf. Antennas Propag. Wireless Commun., 2014, pp. 237–240.
[32] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, “Connected vehicle: Solutions and challenges,” IEEE Internet Things J., vol. 1, no. 4, pp. 289–290, Aug. 2014.
[33] E. Ezhilarasan and M. Dinakaran, “A review on mobile technologies: 3G, 4G and 5G,” in Proc. IEEE 2nd Int. Conf. Recent Trends Challenges Comput. Models, 2017, pp. 369–373.
[34] C. Paper and S. Darbha, “String stability of interconnected systems - automatic control,” IEEE Trans. Autom. Control, vol. 41, no. 3, pp. 349–357, Mar. 1996.
[35] K. J. Aström and B. Wittenmark, Computer-Controlled Systems, 3rd ed., Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1997.
YANG et al.: ROBUST CACC SCHEME AGAINST CYBERATTACKS VIA MULTIPLE VEHICLE-TO-VEHICLE NETWORKS

[43] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, “Jamming attacks on wireless networks: A taxonomic survey,” Int. J. Prod. Econ., vol. 172, pp. 76–94, 2016.

[44] S. Feng and S. Haykin, “Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks,” IEEE Trans. Veh. Technol., vol. 68, no. 10, pp. 9920–9934, Oct. 2019.

[45] M. Showkatbakhsh, Y. Shoukry, R. H. Chen, S. Diggavi, and P. Tabuada, “An SMT-based approach to secure state estimation under sensor and actuator attacks,” in Proc. IEEE 56th Annu. Conf. Decis. Control, 2017, pp. 157–162.

[46] T. Yang, C. Murguia, M. Kuijper, and D. Nelić, “A robust circle-criterion observer-based estimator for discrete-time nonlinear systems in the presence of sensor attacks,” in Proc. IEEE 57th Conf. Decis. Control, 2018, pp. 571–576.

[47] A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos, “Defending wireless sensor networks from jamming attacks,” in Proc. IEEE 18th Int. Symp. Pers., Indoor Mobile Radio Commun., 2007, pp. 1–5.

[48] R. Muraleedharan and L. A. Osadciw, “Jamming attack detection and countermeasures in wireless sensor network using ant system,” Proc. SPIE, vol. 6248, pp. 118–129, 2006.

[49] Y. He and Q.-G. Wang, “An improved ILMI method for static output feedback control with application to multivariable pid control,” IEEE Trans. Autom. Control, vol. 51, no. 10, pp. 1678–1683, Oct. 2006.

[50] M. Tabbara, D. Nelić, and A. R. Teel, “Networked control systems: Emulation-based design,” Networked Control Syst.: Theory Appl., pp. 57–94, 2008.

[51] N. A. Loehr, An Introduction to Mathematical Proofs. Boca Raton, FL, USA: CRC Press, 2019.

Tianci Yang (Member, IEEE) received the bachelor’s degree in engineering from Honors School, Harbin Institute of Technology, Harbin, China, in 2014, and the Ph.D. degree in electrical and electronic engineering from the University of Melbourne, Melbourne, VIC, Australia, in 2019. He is currently a Research Fellow with the School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore. His research interests include systems and control, attack detection/identification, resilient state estimation and control of cyber-physical systems.

Carlos Murguia received the Master of Science degree in electrical engineering from the Center for Research and Advanced Studies (CINVESTAV), Mexico City, Mexico, in 2010, the Ph.D. degree in mechanical engineering from the Eindhoven University of Technology, The Netherlands, from November 2010 to May 2015, he was affiliated with the Dynamics and Control group, Eindhoven University of Technology. He was a Postdoctoral research Fellow with the Singapore University of Technology and Design, Singapore, the University of Melbourne, Melbourne, VIC, Australia, and the University of California, Los Angeles, CA, USA. During his time as postdoctoral Fellow, he held visiting Scientist positions at Princeton University, the University of Texas at Austin, Austin, TX, USA, and the University of Texas at Dallas, Dallas, TX. Since March 2020, he has been an Assistant Professor with the Mechanical Engineering Department, Eindhoven University of Technology, The Netherlands. His main research strengths and interests include the nonlinear dynamics and control, distributed dynamical systems, fault isolation/mitigation, and security and privacy of cyber-physical systems.

Dragan Nešić (Fellow, IEEE) received the Bachelor of Mechanical Engineering degree from the University of Belgrade, Belgrade, Serbia, in 1990 and the Ph.D. degree from The Australian National University, Canberra, ACT, Australia, in 1997. He is currently a Professor with the Department of Electrical and Electronic Engineering, The University of Melbourne, Melbourne, VIC, Australia. His research interests include the broad area of control engineering including its mathematical foundations such as Lyapunov stability theory, hybrid systems, singular perturbations, averaging, and its applications to various areas of engineering, such as automotive control, optical telecommunications and science, such as neuroscience. More specifically, he has made significant contributions to the areas of nonlinear sampled-data systems, nonlinear networked control systems, event-triggered control, optimization-based control and extremum seeking control and he presented several keynote lectures on these topics at international conferences.

Chen Lv (Senior Member, IEEE) is currently a Nanyang Assistant Professor with the School of Mechanical and Aerospace Engineering, and the Cluster Director in Future Mobility Solutions, Nanyang Technological University, Singapore. His research interests include intelligent vehicles, automated driving, and human-machine systems, where he has contributed two books, more than 100 papers, and obtained 12 granted patents. He is an Associate Editor for IEEE T-ITS, IEEE TVT, and IEEE T-I. He was the recipient of the many awards and honors, selectively including IEEE IV Best Workshop/Special Session Paper Award in 2018, Automotive Innovation Best Paper Award in 2020, the winner of Waymo Open Dataset Challenges at CVPR 2021, and Machines Young Investigator Award in 2022.