



Article

Secure State Estimation for Motion Monitoring of Intelligent Connected Vehicle Systems

Xiulan Song , Xiaoxin Lou, Junwei Zhu and Defeng He 

College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China; lxx@zjut.edu.cn (X.L.); junweizhu1001@zjut.edu.cn (J.Z.); hdfzj@zjut.edu.cn (D.H.)

* Correspondence: songxl2008@zjut.edu.cn

Received: 21 January 2020; Accepted: 19 February 2020; Published: 25 February 2020



Abstract: This paper considers the state estimation problem of intelligent connected vehicle systems under the false data injection attack in wireless monitoring networks. We propose a new secure state estimation method to reconstruct the motion states of the connected vehicles equipped with cooperative adaptive cruise control (CACC) systems. First, the set of CACC models combined with Proportion-Differentiation (PD) controllers are used to represent the longitudinal dynamics of the intelligent connected vehicle systems. Then the notion of sparseness is employed to model the false data injection attack of the wireless networks of the monitoring platform. According to the corrupted data of the vehicles' states, the compressed sensing principle is used to describe the secure state estimation problem of the connected vehicles. Moreover, the L_1 norm optimization problem is solved to reconstruct the motion states of the vehicles based on the orthogonal decomposition. Finally, the simulation experiments verify that the proposed method can effectively reconstruct the motion states of vehicles for remote monitoring of the intelligent connected vehicle system.

Keywords: connected vehicles; cooperative adaptive cruise control; state estimation; remote monitoring; cyber-attack

1. Introduction

With the rapid increase in the number of road vehicles, the problems of traffic congestion, exhaust emissions and safety are becoming more and more serious in big cities and/or urban areas [1,2]. Intelligent transportation systems (ITS) technology is one of the potential solutions to lessen these problems [3–6]. Benefiting from the development of the wireless communication technology, the intelligent connected vehicle system is one of such ITS that can potentially reduce the risk of accidents and increase traffic throughput by resorting the Internet of Vehicles (IoV), e.g., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-road (V2R) communication, etc. However, due to the open nature of wireless communication and the high-mobility of moving vehicles, the IoV communication networks are vulnerable to packet dropping, communication time-delay and malicious cyber-attack [7]. Especially, the malicious cyber-attack, e.g., false data injection attack, will cause mistakes in the decision makers of ITS that may lead to serious traffic accidents [7]. Hence, it is necessary to realize the secure estimation of vehicle motion states in the remote monitoring platform of intelligent connected vehicle systems.

The intelligent connected vehicle system contains many on-board sensors, controllers, actuators and other units, and integrates modern wireless communication and network technologies. It can realize intelligent information exchange between moving vehicles and X (i.e., cars, roads, people, clouds, etc.) and can real-time sense the complex surroundings. Based on IoV and intelligent sensing, the intelligent connected vehicle system makes intelligent decisions in real time to help drivers to achieve collaborative control of a group of connected vehicles, and ultimately achieve automated

intelligent driving with safety, efficiency, ride comfort and energy-saving [5–8]. However, there are some inherent weakness in wireless IoV, such as communication delays and packet dropping. Moreover, because of the openness of wireless networks, there may be artificial attacks in intelligent connected vehicle systems [9–13]. In the past decades, many efforts have been directed at the study of the issues of wireless networked control of connected vehicle systems and rich control methods to compensate network defects such as packet dropping and communication delay have been proposed. For example, Ploeg et al. [14] and [15] proposed the L_p norm-based string stabilizing control method and discussed the string stability of cooperative adaptive cruise control (CACC) systems in unreliable communication networks. Ploeg et al. [16] considered the communication delay problem of IoV and achieved the stability of the intelligent connected vehicle systems using CACC approaches [12,13]. Moreover, when communication delay and packet loss occur simultaneously, the CACC system of connected vehicles will actively degrade to the traditional adaptive cruise control (ACC) system [5] while ensuring string stability that is better than the one of the ACC system [17].

In recent years, the cyber-security issue has increasingly gained attention in the automotive and academic communities due to widely used wireless communication networks of IoV and very dangerous results caused by cyber-attacks. For example, in July 2015, the "white hat hackers" Miller and Wallacek demonstrated how to "hijack" remote command methods by invading Chrysler Uconnect vehicle systems when driving, and eventually caused a "roll over" [8]. This remote cyber-attack event has made many scholars investigate the cyber-security problem in the field of intelligent connected vehicle system with various embedded CACC systems. For instance, Biron et al. [18] proposed a sliding mode observer algorithm for detecting the occurrence of denial of service (DOS) attacks in the networks and estimating the magnitude of the delay. Amoonzadeh et al. [19] studied the effects of the tampered sensors, which seriously affects the string stability of connected vehicle platooning systems. Dadras et al. [20] studied the ability of an attacker to invade a networked vehicle by remote attack and showed that attackers can remotely control the individual position and speed of networked vehicles. Liu et al. [21] showed the serious impacts of the cyber-attack on automated platoon systems and proposed a design approach for safe platooning controllers. Following the method in [21], the safe inter-vehicle distance is greatly shortened. Alipour-Fanid et al. [22] conducted a comprehensive analysis of stability and safety for vehicle strings over wireless Rician fading channels under jamming attacks. They showed that fading channels degrade the performance of CACC systems through rich simulation experiments under various attacked scenarios. In addition, Li et al. [23] summarized the influences of cyber-attacks on longitudinal safety of connected and automated vehicles via extensive simulations and sensitivity analysis.

Due to the significant threat of cyber-attacks to the safety of persons and property, in the automotive and academic communities more and more scholars have studied the safety and security problems of connected and networked vehicles under cyber-attack. For example, Massoumnia et al. [24] and Blanke et al. [25] proposed the residual test method to detect the false data injection attack for networked systems including connected and networked vehicles. Since each measured value has a residual signal, the measured value is considered to be attacked if the residual value is greater than a given threshold. However, if an attacker sets the special data so that the residual is still less than the threshold, this method cannot be applied well. Another method to again cyber-attack is to use the idea of robust control. It can achieve stability of uncertain systems when the system is destroyed by some unknown disturbances. However, in this method perturbations are assumed to be bounded by some ranges [26]. For instance, Schenato et al. [27] considered the disturbance as a certain random process if the wireless channel is interfered and analyzed the control and estimation problems of networked control systems. Lately, Lu and Yang [28] designed a Luenberger-like observer and used a new projection operator method to reconstruct the states from a series of continuous measurements of cyber-physical systems. Wu et al. [29] proposed a sliding mode observer for estimating the system states from the measurement data of contaminated sensors. Fawzi et al. [30] and Hwan et al. [31]

assumed that the attacked states satisfied sparseness and then proposed the use of L_1 norm optimization to reconstruct the states of cyber-physical systems including connected vehicle systems.

Aiming at the problem of secure state estimation of intelligent connected vehicle systems under the attack of false data injection in the wireless monitoring networks, this paper proposes a secure state estimation method to reconstruct the motion states of the connected and networked vehicles equipped with CACC systems. The main idea of the method is to use the principle of compressed sensing based on the notion of sparseness. By adopting Proportion-Differentiation (PD) controllers, e.g., [12,13], the set of CACC models is used to represent the longitudinal dynamics of the intelligent connected vehicle systems. Due to adversarial attack to the intelligent connected vehicle system, the number of attacked sensors is assumed to be less than the half of the total sensors. Then the attacked vector can be regarded as a sparse vector and transformed into an L_1 norm optimization problem for secure state reconstruction. Finally, the simulation experiments verify that the proposed method can effectively reconstruct the motion states of vehicles for remote monitoring of the intelligent connected vehicle system.

The remaining of this paper is organized as follows: In Section 2, the set of CACC models and false data injection attack models are formulated. In Section 3, we present the secure state estimation approach and verify the applicability of the approach. Then we demonstrate the proposed approach through some classical simulations in Section 4. Finally, we conclude the paper in Section 5.

2. Problem Description

To increase the efficiency of ITS, road vehicles are generally arranged into a vehicle platoon to reduce the risk of accidents and increase traffic throughput. Here a group of vehicles is assumed to be controlled by some stabilizing CACC systems to form a vehicle platoon with guaranteed string stability. From the department of transportation, it is necessary to remotely monitor the real motion states of each vehicle in the connected platoon system by the monitoring platforms of ITS. The motion state information of each vehicle includes the position, velocity, acceleration, etc. The monitoring platform can also use the estimated states to do such tasks as trajectory planning of vehicles or adjusting traffic scene and so on. However, the wireless communication of IoV is vulnerable to be attacked due to its openness. Thus, the vehicle states that the monitoring platform received may be corrupted by special cyber-attackers. Aiming at the problem, we now establish the CACC models of the connected vehicle system and the false data injection attack models.

2.1. CACC Models for Connected Vehicles

Consider a CACC system of connected and networked vehicles, as shown in Figure 1.

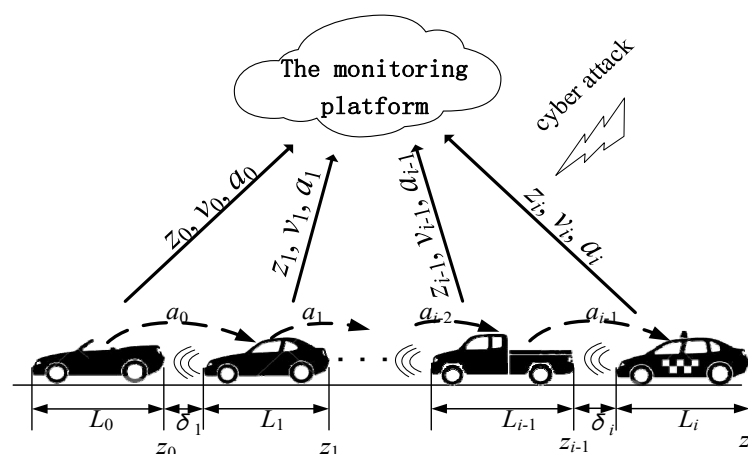


Figure 1. A schematic of intelligent connected vehicle systems with cooperative adaptive cruise control (CACC) and cyber-attack.

There are $n + 1$ vehicles running on a single lane being level with no effects of the wind speed. In this paper, we assume that the leading vehicle ($i = 0$) is running at a constant speed. For each vehicle $i = 1, \dots, n$, the desired spacing error is defined as:

$$\delta_i = z_{i-1} - z_i - \delta_d - L_i \quad (1)$$

where δ_i is the desired spacing error, z_i and L_i separately represent the absolute position and length of the i th vehicle and δ_d is the desired safe inter-vehicle distance (spacing).

For each vehicle $i = 1, \dots, n$, the longitudinal dynamics is described by [10,11]:

$$m_i a_i(t) = F_i(t) - \sigma A_i c_{di} v_i^2(t) / 2 - d_{mi} \quad (2)$$

where m_i represents the mass of the vehicle, a_i represents the acceleration, F_i is the driving force, σ is the density of air quality, A_i is the windshield area, c_{di} is the resistance coefficient, v_i is the velocity, d_{mi} is the mechanical resistance. Moreover, due to focusing on the CACC system, in this paper the vehicular throttle and braking pedal units are assumed to have desired dynamics [11], which is:

$$\dot{F}_i(t) = (-F_i(t) + c_i(t)) / \tau_i \quad (3)$$

where $\tau_i > 0$ is the constant lag time of the internal actuator dynamics and c_i is the input of the throttle or pedal of the i th vehicle. Substituting (2) into (3), we have that:

$$\dot{F}_i(t) = -\frac{1}{\tau_i} \left(m_i a_i(t) + \frac{\sigma A_i c_{di}}{2} v_i^2(t) + d_{mi} \right) + \frac{c_i(t)}{\tau_i} \quad (4)$$

Dividing m_i on both sides of (4) and then substituting it into the derivative of Equation (2), it is obtained the dynamics of the acceleration variable of the i th vehicle is:

$$\dot{a}_i(t) = -\frac{1}{\tau_i} \left(a_i(t) + \frac{\sigma A_i c_{di}}{2 m_i} v_i^2(t) + \frac{d_{mi}}{m_i} \right) - \frac{\sigma A_i c_{di} v_i(t) a_i(t)}{m_i} + \frac{c_i(t)}{\tau_i m_i} \quad (5)$$

For the nonlinear Equation (5), the feedback linearization controller is designed as:

$$c_i(t) = \frac{1}{m_i \tau_i} [u_i(t) - q(v_i(t), a_i(t))] \quad (6)$$

where u_i is the CACC input to be calculated by using the desired spacing error, relative velocity and acceleration between the host vehicle and the front one, and nonlinear term $q(v_i, a_i)$ is:

$$q(v_i, a_i) = -\frac{1}{\tau_i} \left(a_i + \frac{\sigma A_i c_{di}}{2 m_i} v_i^2 + \frac{d_{mi}}{m_i} \right) - \frac{\sigma A_i c_{di} v_i a_i}{m_i} \quad (7)$$

Then the kinematics equation of the i th vehicle can be represented as:

$$\begin{bmatrix} \dot{z}_i(t) \\ \dot{v}_i(t) \\ \dot{a}_i(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/\tau_i \end{bmatrix} \begin{bmatrix} z_i(t) \\ v_i(t) \\ a_i(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1/\tau_i \end{bmatrix} u_i(t). \quad (8)$$

In this paper, the CACC controller of each vehicle $i = 1, \dots, n$ is designed as an output feedback Proportion-Differentiation (PD) controller:

$$u_i(t) = K_i y_i(t), \quad t \geq 0 \quad (9)$$

where the controller gain $K_i = [k_{z_i}, k_{v_i}, k_{a_i}]$ and the output vector $y_i = [z_{i-1} - z_i, v_{i-1} - v_i, a_{i-1} - a_i]^T$. In CACC systems, PD controllers are the widely used due to simplicity and efficiencies [12–17]. Here

the gain K_i is assumed to be calculated using the spired spacing error, relative velocity and relative acceleration to ensure the string stability of the CACC system [13]. In CACC, the output y_i can be measured by the onboard sensors, e.g., radars, Lidar, etc., and the acceleration of the front vehicle is transmitted by wireless IoV communication.

We stack the state vector of the connected vehicle platoon, i.e., $x = [z_1, v_1, a_1, \dots, z_n, v_n, a_n]^T$. Then the closed-loop CACC system of the connected vehicle platoon has the compact form of:

$$\dot{x}(t) = \hat{A}x(t) + \hat{G}, t \geq 0 \quad (10)$$

where the matrices are:

$$\hat{A} = \begin{bmatrix} D & 0 & \cdots & 0 & 0 \\ H_1 & 0 & \cdots & 0 & 0 \\ 0 & D & \cdots & 0 & 0 \\ H'_2 & H_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & D \\ 0 & 0 & \cdots & H'_n & H_n \end{bmatrix}, \hat{G} = \begin{bmatrix} 0 \\ H'_1 \begin{bmatrix} z_0 & v_0 & a_0 \end{bmatrix}^T \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

$$\begin{cases} H_i = \begin{bmatrix} -k_{z,i}/\tau_i & -k_{v,i}/\tau_i & -(k_{z,i} + 1)/\tau_i \end{bmatrix} \\ H'_i = \begin{bmatrix} k_{z,i}/\tau_i & k_{v,i}/\tau_i & k_{a,i}/\tau_i \end{bmatrix} \end{cases}, D = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for $i = 1, \dots, n$. In order to securely estimate the motion states of the vehicle CACC system (10) by the sampled output measurements, the CACC system is discretized with a sampling time $T > 0$. Namely, the discrete-time state space model of the closed-loop CACC system of the connected vehicle platoon is represented as:

$$x(k+1) = Ax(k) + G(k), k = 0, 1, 2 \dots \quad (11)$$

where matrices $A = E + \bar{A}T$, $G = \hat{G}T$, and E is an identity matrix with appropriate dimension.

2.2. False Data Injection Attack Models

In this paper, we consider the class of cyber-attack which is occurred in the communication layer linking the vehicles with the monitoring platform. The wireless channels, which deliver the vehicle's state information from the CACC system to the monitoring platform, are attacked by cyber attackers (see Figure 1). In this way, the attackers can cheat the monitoring platform by tampering the data of the motion states of the vehicles in the intelligent connected vehicle system. Consequently, the monitors in the remote monitoring platform may make wrong decisions.

There are many kinds of cyber-attack such as denial of service (DoS), interference attack, false data injection attack and so on [21–23]. In this section we consider the false data injection attack. The attacker firstly attacks the wireless networks through truncating the package of the cruise states and modifying the payload, and then delivers the corrupted package to the monitoring platform. This may cause the monitoring platform to make incorrect judgments about the real operation of the CACC system and ultimately interfere with the normal operation of the monitoring platform.

In this scenario, every vehicle of the vehicle CACC system delivers the information such as absolute position, velocity and acceleration to the remote monitoring platform. Once the data package is in the communication layer linking the vehicles with the monitoring platform, the related data are modified by cyber attackers. It has been shown that the real cruise states cannot be reconstructed if the attacked node (state) is more than the half of the total quantity [30,31]. Hence, here we assume that the attacked date is no more than half of the total quantity of the state of the connected vehicle platoon at each time instant. The assumption is reasonable because the malicious attackers always want to be hidden and their abilities are limited by the economic capability. In other words, there is no

way to reconstruct the motion states of vehicles if an attacker has an ability to truncate all packages transmitted to the monitoring networks, and even the attacker can simulate any vehicles running scenarios but cannot be detected.

Now we establish the false data injection attack model of the vehicle CACC system (11). From the viewpoint of the monitoring platform, the vehicle's state space model is selected as (11). If the wireless channels linking the vehicles with the monitoring platform are not attacked and the data is received correctly by the monitoring platform, then the data is obtained by:

$$y(k) = Cx(k) \quad (12)$$

where $y(k)$ is the received data on the monitoring platform, and C is the observation matrix being identity matrix with appropriate dimension.

However, if the false data injection attack is occurred, the received data $y(k)$ will be introduced an unknown value compared to the actual states. For the monitoring platform, the attacked values are added to the state which are then delivered through the wireless channels. Hence, we present the false data injection attack model as:

$$y(k) = Cx(k) + \Gamma e(k) \quad (13)$$

where $\Gamma = \text{diag}(\lambda_1, \dots, \lambda_t)$ represents the attack selection matrix, the i th data is attacked if $\lambda_i = 1$; otherwise, $\lambda_i = 0$, and the signal $e(k)$ represents the attack values injected to the vehicle's state information which is delivered through the wireless channels to the monitoring platform.

3. Secure State Estimation

In order to reconstruct the initial states of the vehicle CACC system (11), let we first consider the principle of compressive sensing [32]:

$$\min_x \|x\|_0 \text{ s.t. } b = Px \quad (14)$$

where $b \in R^m$ is the measurements, $P \in R^{m \times n}$ is a sensing matrix and $\|x\|_0$ denotes the number of nonzero elements for the vector x . If the sparse vector x meets $\|x\|_0 = q \leq m/2$ and all subsets of $2q$ columns of P are full rank, then the solution to (14) is unique [32].

To reconstruct the states attacked through the above compression sensing method, we integrates the attacked CACC system of the connected vehicles described by (11)–(13) as:

$$\begin{cases} x(k+1) = Ax(k) + G(k) \\ y(k) = Cx(k) + \Gamma e(k) \end{cases} \quad (15)$$

where the diagonal matrix Γ corresponds with the data package which is under attacking.

To solve the problem of reconstructing the state at the initial time using the compressive sensing method, now we consider the set of output measured values $y(k)$, $k = 0, \dots, M-1$, which are destroyed at successive M times. From the model (15), we stacked the M output measurements as:

$$Y = \begin{bmatrix} y(0) & y(1) & \dots & y(M-1) \end{bmatrix}^T = \Phi x(0) + E + \hat{Y} \quad (16)$$

where the coefficient matrices are:

$$\Phi = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{M-1} \end{bmatrix}, E = \begin{bmatrix} \Gamma e(0) \\ \Gamma e(1) \\ \vdots \\ \Gamma e(M-1) \end{bmatrix}, \hat{Y} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ C & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CA^{M-2} & CA^{M-3} & \dots & 0 \end{bmatrix} \begin{bmatrix} G(0) \\ G(1) \\ \vdots \\ G(M-1) \end{bmatrix}.$$

Moving the term \hat{Y} to the left of equation (16), we have:

$$\bar{Y} = \Phi x(0) + E \quad (17)$$

where $\bar{Y} = Y - \hat{Y}$.

In order to resolve the problem of the state estimation, we should determine the value of M . From the results in [30,31], the value of M is equal to the number of states if the attacked states are fixed; but if the attacked states are varying, M may be greater than the number of states in some cases. Through the simulation experiments (see later), under the condition of varying attacked states, the states also can be reconstructed successfully if M is equal to the number of the states. As a result, we can estimate the error vector E firstly and next we reconstruct the initial state $x(0)$ through the estimated value of E .

In order to achieve the purpose of estimating E , we use the orthogonal decomposition to the matrix $\Phi \in R^{pM \times 3n}$, where p , M and n represents the number of the sensors, measurements and vehicles of the CACC system, respectively. Consider the orthogonal decomposition of Φ as:

$$\Phi = \begin{bmatrix} Q_1 & Q_2 \end{bmatrix} \begin{bmatrix} R_1 \\ 0 \end{bmatrix} \quad (18)$$

where $[Q_1 \ Q_2]$ is an orthogonal matrix with $Q_1 \in R^{pM \times 3n}$ and $Q_2 \in R^{pM \times (pM - 3n)}$ and $R_1 \in R^{3n \times 3n}$ is an upper triangular matrix with full rank.

Substituting Equation (18) into Equation (17), we can obtain that:

$$\bar{Y} = \begin{bmatrix} Q_1 & Q_2 \end{bmatrix} \begin{bmatrix} R_1 \\ 0 \end{bmatrix} x(0) + E. \quad (19)$$

Because the matrix $[Q_1 \ Q_2]$ is the orthogonal matrix. Multiplying the matrix $[Q_1 \ Q_2]^T$ on both sides of (19), it is obtained that:

$$\begin{bmatrix} Q_1^T \\ Q_2^T \end{bmatrix} \bar{Y} = \begin{bmatrix} R_1 \\ 0 \end{bmatrix} x(0) + \begin{bmatrix} Q_1^T \\ Q_2^T \end{bmatrix} E. \quad (20)$$

Simplifying (20), it is derived that:

$$Q_1^T \bar{Y} = R_1 x(0) + Q_1^T E \quad (21)$$

$$Q_2^T \bar{Y} = Q_2^T E \quad (22)$$

Since the number of attacked states is less than $p/2$, where p represents the number of the delivered states at each moment, the solution to Equation (22) is unique from the principle of compressive sensing in Equation (14). Because the intelligent connected vehicle system consists of n vehicles with together the leader vehicle and every vehicle has three state variables, then the number of the attacked states are up to $\lfloor 3n/2 \rfloor$ at each time instant.

Now we use the compressive sensing method to estimate the attack vector E by solving the following optimization problem:

$$\hat{E} = \min_E \|E\|_{L_0} \text{ s.t. } Q_2^T \bar{Y} = Q_2^T E. \quad (23)$$

Note that the solution of Equation (23) involves the L_0 norm but the L_0 norm optimization is an NP hard problem. As a result, the computational burden of solving Equation (23) is too heavy to efficiently solve the problem. To this end, we can transform the L_0 norm optimization to L_1 norm optimization as the L_1 norm is the optimal convex approximation of the L_0 norm:

$$\hat{E} = \min_E \|E\|_{L_1} \text{ s.t. } Q_2^T \bar{Y} = Q_2^T E. \quad (24)$$

We can obtain the estimation \hat{E} by computing Equation (24). Clearly, this approximation greatly reduces the computing burden of solving the estimation of the attack vector E . Moreover, substituting \hat{E} into (21) and simplifying the equation, we derive the initial state $x(0)$ by:

$$x(0) = R_1^{-1} Q_1^T (\bar{Y} - \hat{E}). \quad (25)$$

Then the actual motion states of each vehicle in the intelligent connected vehicle system can be evaluated real-time by iterative computing Equation (11).

It is noted that from the compressive sensing method [30,31], it is ensured that the solution of \hat{E} is unique. Because the matrix R_1 is an upper triangular matrix with full rank, the initial state $x(0)$ is also unique. Therefore, in the remote monitoring platform the presented secure state estimate method is used to real-time obtain the actual motion states of each vehicle in the intelligent connected vehicle system even under cyber-attack of false data injection.

4. Simulation Results

In this section, we show the validity of the presented secure state estimate method of the intelligent connected vehicle system. The simulation scene here considers a group of four heterogeneous vehicles running in a single lane, where all vehicles are equipped with the PD-type CACC controllers. Moreover, the vehicle CACC system is stable and string stable. There is the remote monitoring layer which monitors the vehicular motion states through wireless IoV communication (see Figure 1). The wireless channels may be maliciously attacked by the false data injection from cyber attackers. Using the presented secure state estimate method to recover the corrupted received data, the remote monitoring platform can achieve normal operation.

In this simulation study, the vehicles' parameters are selected as $L_i = 4$ m for $i = 0, 1, 2, 3$, $\tau_0 = 0.20$ s, $\tau_1 = 0.25$ s, $\tau_2 = 0.20$ s, $\tau_3 = 0.25$ s and $\delta_d = 2$ m. Note that the subscript "0" represents the leading vehicle and the others represent the following vehicles. For the wireless channels which link the vehicles to the remote monitoring layer, the observation matrix C is chosen as a nine-order identity. Moreover, the PD-type CACC controllers are calculated by the method in [12] and the controllers' gains are selected as $K_1 = [0.2284, 0.7740, 0.1961]$, $K_2 = [0.2181, 0.7456, 0.1466]$ and $K_3 = [0.2360, 0.8084, 0.2280]$. In addition, the simulation scenario is initialized such the case that the leading vehicle is running at the position of 40 m with the velocity of 20 m/s. Because the leading vehicle is running with the constant velocity, the motion state-space model of the leading vehicle is given as:

$$\begin{bmatrix} \dot{z}_0(t) \\ \dot{v}_0(t) \\ \dot{a}_0(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} z_0(t) \\ v_0(t) \\ a_0(t) \end{bmatrix} \quad (26)$$

where z_0 , v_0 and a_0 represents the absolute position, velocity and acceleration of the leading vehicle. The matrix G in (11) is calculated through the leading vehicle's states. At the initial time instant, the three following vehicles stop at the position of 25 m, 10 m and 0 m, and the velocity and acceleration are zero, that is, $x(0) = [25, 0, 0, 10, 0, 0, 0, 0, 0]^T$. Because the number of the states of the vehicle CACC system is 9, then the number of measurements of the system is selected at least as $M = 9$.

In the simulation experiment, it is assumed that attackers want to maliciously interfere with the normal operation of the remote monitoring platform of the intelligent connected vehicle system. Hence, they randomly attack the data packets in the remote monitoring networks. In this scene, it is assumed that the second following-vehicle is under attacking. The data delivered to the monitoring platform is injected by the false data from malicious attackers, which is shown in Figure 2. Note that this attack is launched randomly to the three states of this vehicle in this study. It is observed from Figure 2 that the three states of this vehicle are attacked and the other vehicles' states are not attacked. In Figure 2, the red dashed and dot-dashed lines represent the real and the attacked states of the following vehicles,

respectively. Then we use the presented secure state estimate method to estimate the time real states of the vehicle platoon. The secure state estimate results are shown in Figures 3–5.

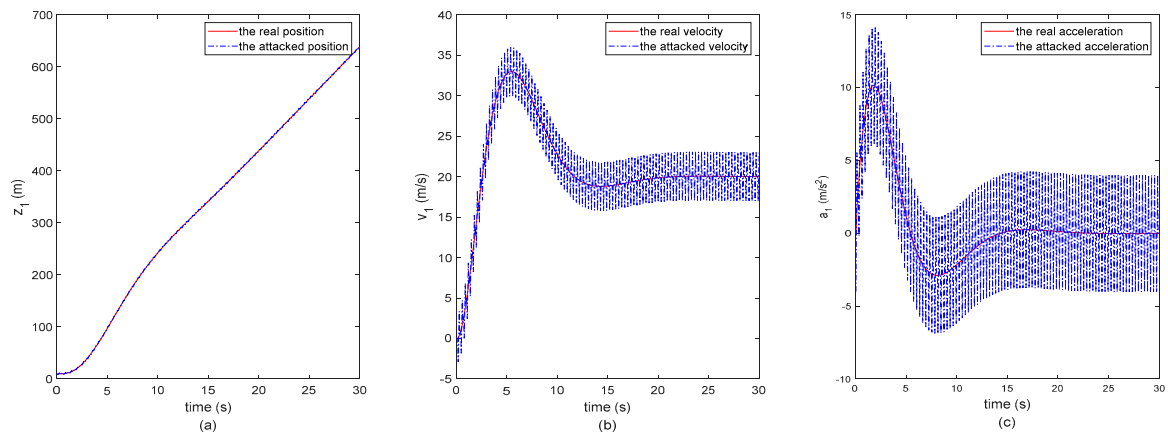


Figure 2. The second following-vehicle’s real states and attacked states. (a) The absolute position, (b) The velocity, (c) The acceleration.

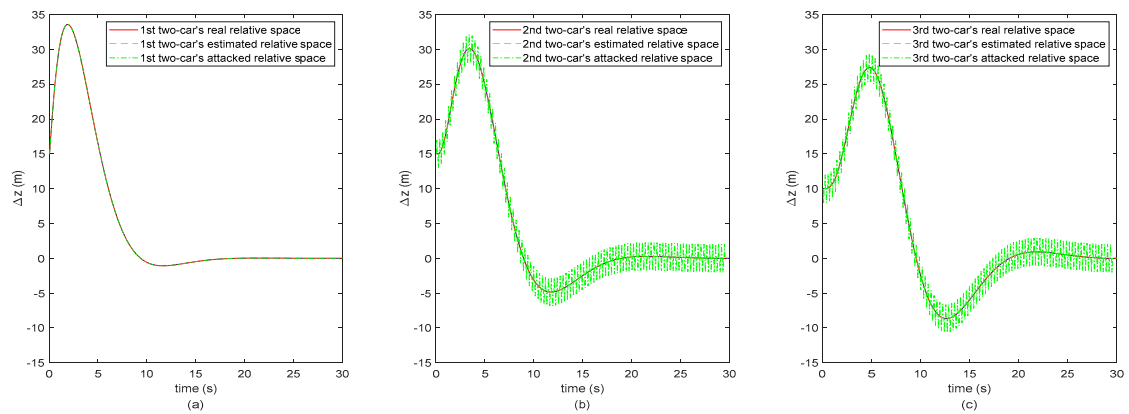


Figure 3. The three 2-cars’ spacing. (a) The 1st two-car, (b) The 2nd two-car, (c) The 3rd two-car.

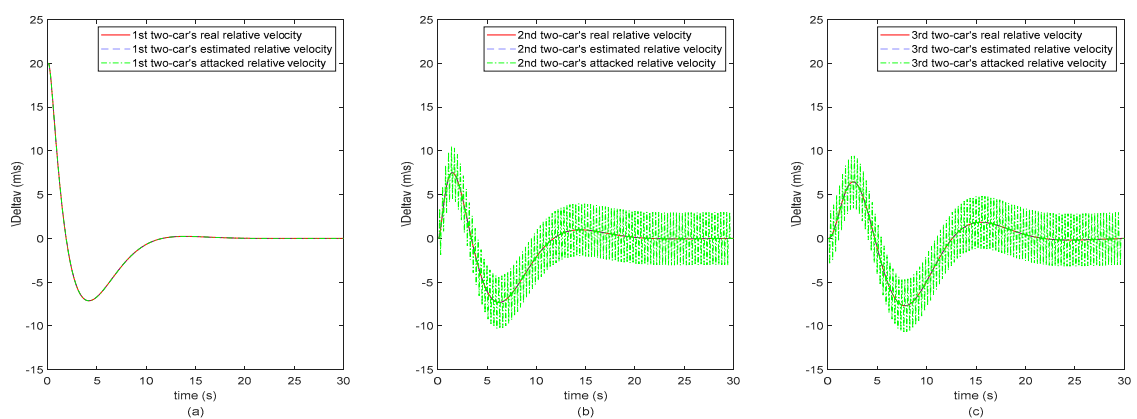


Figure 4. The three 2-cars’ relative velocity. (a) The 1st two-car, (b) The 2nd two-car, (c) The 3rd two-car.

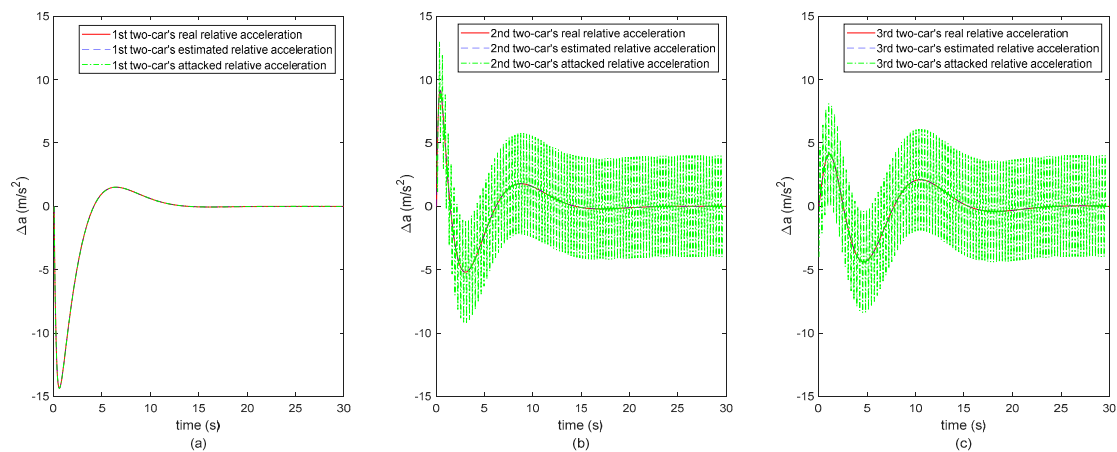


Figure 5. The three 2-cars' relative acceleration. (a) The 1st two-car, (b) The 2nd two-car, (c) The 3rd two-car.

In order to clearly analyze the results on secure state estimation of the vehicle CACC system, we use the spacing, relative velocity and acceleration profiles of the adjacent two vehicles to replace the absolute position, velocity and acceleration profiles. Hence, the subplots (a) of Figures 3–5 represent the 1st two-car's inter-vehicle distance, relative velocity and relative acceleration profiles, respectively, and subplots (b) and (c) represent the 2nd two-cars' and the 3rd two-cars', respectively. Note that the second following-vehicle is under attacking and the ranges of attack are as shown in Figure 2. As the CACC system (11) used in the remote monitoring platform is dependent on the inter-vehicle distance, relative velocity and acceleration between adjacent vehicles, the monitoring motion states of the third following-vehicle are also negatively, indirectly affected by the attack launched to the second following-vehicle. Hence, in Figures 3–5, the 2nd and 3rd two-cars' green dot-dashed lines are different from the 1st two-cars', which represent the values after attacking.

It is observed from Figures 3–5 that the red dashed lines and the blue dotted lines almost coincide, where the two sets of lines represent the real states and the estimated motion states of the vehicle CACC system, respectively. The estimated motion states of the vehicle CACC system are calculated from the attacked states by applying the proposed secure state estimation method. In other words, the motion states of the vehicle CACC system are estimated successfully in the context that the states of the second following-vehicle are under attacking randomly. Note that the attack launched here is hidden in the sense that it is intermittent to inject false data to the states of the second following-vehicle and the number of the attacked states is limited and may change over the time. Hence, the simulation results illustrate the effectiveness of the proposed secure state estimation method for remote monitoring of intelligent connected vehicle systems under the false data injection attack. The proposed estimation method increases the resilient ability of the remote monitoring platform of connected vehicles against to cyber-attack.

5. Conclusions

In this paper, we considered the false data injection attack on the wireless networks of intelligent connected vehicle systems and presented the secure state estimation method to reconstruct the motion states of the connected and networked vehicles equipped with the CACC systems. Applying the principle of compressed sensing, the optimization-based state estimation method was proposed to reconstruct the initial state of the vehicle. The simulation results demonstrated the effectiveness of the secure state estimation approach for remote monitoring motion of connected vehicles against to the false data injection attack. In the future, distributed secure state estimation with consideration of process and measurement noises is the pursuing work in order to more effectively reconstruct the motion states of connected vehicles against to cyber-attacks.

Author Contributions: Conceptualization, X.S.; methodology, X.S. and D.H.; validation, X.L. and J.Z.; formal analysis, X.S. and X.L.; investigation, X.L.; writing—original draft preparation, X.L.; writing—review and editing, X.S., J.Z. and D.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Natural Science Foundation of China under grant number 61803336 and Zhejiang Provincial Natural Science Foundation under grant number LR17F030004.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Milanés, V.; Shladover, S.E. Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data. *Trans. Res. Part C* **2014**, *48*, 285–300. [[CrossRef](#)]
2. Jia, D.; Lu, K.; Wang, J. A survey on platoon-based vehicular cyber-physical systems. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 263–284. [[CrossRef](#)]
3. Hu, C.; Wang, Z.; Taghavifar, H.; Na, J.; Qin, Y.; Guo, J.; Wei, C. MME-EKF-based path-tracking control of autonomous vehicles considering input saturation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 5246–5259. [[CrossRef](#)]
4. Hu, C.; Wang, Z.; Qin, Y.; Huang, Y.; Wang, J.; Wang, R. Lane keeping control of autonomous vehicles with prescribed performance considering the rollover prevention and input saturation. *IEEE Trans. Intell. Trans. Syst.* **2019**, 1–13. [[CrossRef](#)]
5. He, D.; Shi, Y.; Li, H.; Du, H. Multi-objective predictive cruise control for connected vehicle systems on urban conditions with InPA-SQP algorithm. *Optim. Control Appl. Methods* **2019**, *40*, 479–498. [[CrossRef](#)]
6. He, D.; Qiu, T.; Luo, R. Fuel efficiency-oriented platooning control of connected nonlinear vehicles: A distributed economic MPC approach. *Asian J. Control* **2019**, *21*, 1–11. [[CrossRef](#)]
7. Willke, T.L.; Tientrakool, P.; Maxemchuk, N.F. A survey of inter-vehicle communication protocols and their applications. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 3–20. [[CrossRef](#)]
8. Li, J. *Intelligent Connected Car Information Security White Paper*; China Academy of Automotive Engineering, Beijing Institute of Aeronautics and Astronautics: Beijing, China, 2016.
9. Yang, X.; Liu, L.; Vaidya, N.H. A vehicle-to-vehicle communication protocol for cooperative collision warning. In Proceedings of the 1st Annual International Conference Mobile and Ubiquitous Systems, Networking and Services, Cambridge, MA, USA, 22–26 August 2004; p. 26.
10. Biron, Z.A.; Dey, S.; Pisu, P. Resilient control strategy under denial of service in connected vehicles. In Proceedings of the 2017 American Control Conference, Seattle, WA, USA, 24–26 May 2017; pp. 4971–4976.
11. Yin, X.; Ma, X.; Trivedi, K.S. Performance and reliability evaluation of BSM broadcasting in DSRC with multi-channel schemes. *IEEE Trans. Comput.* **2014**, *63*, 3101–3113. [[CrossRef](#)]
12. Qin, W.B.; Gomez, M.M.; Orosz, G. Stability analysis of connected cruise control with stochastic delays. In Proceedings of the American Control Conference, Portland, OR, USA, 4–6 June 2014; pp. 4624–4629.
13. Song, X.; Lou, X.; Meng, L. Time-delay feedback cooperative adaptive cruise control of connected vehicles by heterogeneous channel transmission. *Meas. Control* **2019**, *52*, 369–378. [[CrossRef](#)]
14. Ploeg, J.; Shukla, D.P.; Nathan, V.D.W. Controller synthesis for string stability of vehicle platoons. *IEEE Trans. Intell. Trans. Syst.* **2014**, *15*, 854–865. [[CrossRef](#)]
15. Ploeg, J.; Nathan, V.D.W.; Nijmeijer, H. Lp string stability of cascaded systems: Application to vehicle platooning. *IEEE Trans. Control Syst. Technol.* **2014**, *22*, 786–793. [[CrossRef](#)]
16. Ploeg, J.; Elham, S.K.; Guido, L. Graceful degradation of cooperative adaptive cruise control. *IEEE Trans. Intell. Trans. Syst.* **2015**, *16*, 488–497. [[CrossRef](#)]
17. Vughts, R.P.A. String-stable CACC design and experimental validation. *Dept. Mech. Eng. Control Syst. Technol. Group Tech. Univ.* **2010**, *59*, 4268–4279.
18. Biron, Z.A.; Dey, S.; Pisu, P. Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Trans. Intell. Trans. Syst.* **2018**, *19*, 3893–3902. [[CrossRef](#)]
19. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [[CrossRef](#)]
20. Dadras, S.; Gerdes, R.M.; Sharma, R. Vehicular platooning in an adversarial environment. In Proceedings of the IEEE 2018 Annual American Control Conference, Milwaukee, WI, USA, 27–29 June 2018; pp. 167–178.

21. Liu, J.; Ma, D.; Weimerskirch, A. A functional do-design towards safe and secure vehicle platooning. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Abu Dhabi, UAE, 2 April 2017; pp. 81–90.
22. Alipour-Fanid, A.; Dabaghchian, M.; Zeng, K. Platoon stability and safety analysis of cooperative adaptive cruise control under wireless Rician fading channels and jamming attacks. *arXiv* **2017**, arXiv:1710.08476v1.
23. Li, Y.; Tu, Y.; Fan, Q.; Dong, C.; Wang, W. Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. *Accid. Anal. Prev.* **2018**, *121*, 148–156. [[CrossRef](#)]
24. Massoumnia, M.A.; Verghese, G.C.; Willsky, A.S. Failure detection and identification. *IEEE Trans. Autom. Control* **1989**, *34*, 316–321. [[CrossRef](#)]
25. Blanke, M.; Kinnaert, M.; Lunze, J. *Fault Diagnosis and Fault-Tolerant Control*; Springer: New York, NY, USA, 2006.
26. Qiu, L. *Essentials of Robust Control*; Prentice Hall: Upper Saddle River, NJ, USA, 1998; p. 38.
27. Schenato, L.; Sinopoli, B.; Franceschetti, M. Foundations of control and estimation over lossy networks. *Proc. IEEE* **2007**, *95*, 163–187. [[CrossRef](#)]
28. Lu, A.Y.; Yang, G.H. Secure Luenberger-like observers for cyber-physical systems under sparse actuator and sensor attacks. *Automatica* **2018**, *98*, 124–129. [[CrossRef](#)]
29. Wu, C.; Hu, Z.; Liu, J. Secure estimation for cyber-physical systems via sliding mode. *IEEE Trans. Cybern.* **2018**, *48*, 3420–3431. [[CrossRef](#)]
30. Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 1454–1467. [[CrossRef](#)]
31. Hwan, C.Y.; Qie, H.; Tomlin, C.J. Secure estimation based Kalman filter for cyber-physical systems against sensor attacks. *Automatica* **2018**, *95*, 399–412.
32. Candes, E.J.; Tao, T. Decoding by linear programming. *IEEE Trans. Inf. Theor.* **2005**, *51*, 4203–4215. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).