Proceedings of the ASME 2019
Dynamic Systems and Control Conference
DSCC2019
October 9-11, 2019, Park City, UT, USA

DSCC2019-9096

RESILIENT CONTROL UNDER CYBER-ATTACKS IN CONNECTED ACC VEHICLES

Woongsun Jeon[1]
University of Minnesota
Minneapolis, MN, USA

Ali Zemouche
University of Lorraine
Cosnes et Romain, France

Rajesh Rajamani
University of Minnesota
Minneapolis, MN, USA

ABSTRACT

This paper focuses on the detection of cyber-attack on a communication channel and simultaneous radar health monitoring for a connected vehicle. A semi-autonomous adaptive cruise control (SA-ACC) vehicle is considered which has wireless communication with its immediately preceding vehicle to operate at small time-gap distances without creating string instability. However, the reliability of the wireless connectivity is critical for ensuring safe vehicle operation. The presence of two unknown inputs related to both sensor failure and cyber-attack seemingly poses a difficult estimation challenge. The dynamic system is first represented in descriptor system form. An observer with estimation error dynamics decoupled from the cyber-attack signal is developed. The performance of the observer is extensively evaluated in simulations. The estimation system is able to detect either a fault in the velocity measurement radar channel or a cyber-attack. Also, the proposed observer-based controller achieves resilient SA-ACC system under the cyber-attacks. The fundamental estimation algorithm developed herein can be extended in the future to enable cyber-attack detection in more complex connected vehicle architectures.

Keywords: Resilient control, observer, cyber-attack, sensor fault, and connected vehicle

1. INTRODUCTION

Vehicle-to-vehicle (V2V) and infrastructure-to-vehicle (I2V) communication can provide a number of benefits to future intelligent vehicle system. These benefits include improvements in fuel economy using knowledge of future vehicle trajectories, enhancement of safety by blocking of shock wave propagation, and improvements in traffic capacity by enabling closer vehicle following [1-3]. All of these benefits are obtained by enhancing currently available adaptive cruise control (ACC) systems using V2V and I2V communications [1-3].

One of the most basic connected vehicle architectures involves the ACC vehicle communicating with just one other vehicle, its immediate preceding vehicle in the same lane. Results published about 15 years ago show how string stability can be enhanced by this inter-vehicle communication [1]. Such a system was called a "semi-autonomous adaptive cruise control (SA-ACC)" system in [1]. Specifically, the allowable time-gap between vehicle h is normally required to be no smaller than the value

$$h > 2\tau \tag{1}$$

where τ is the time constant of the vehicle's lower loop dynamics involving the engine and driveline system [4]. However, if inter-vehicle communication from the immediately preceding vehicle is available (i.e., the preceding vehicle's acceleration is wirelessly transmitted to the ACC vehicle), then the time gap can be made much smaller and higher traffic flow can be achieved with no risk of shock wave propagation. This is because equation (1) no longer has to be satisfied.

This paper relates to SA-ACC systems and develops an estimation algorithm that can detect cyber-attacks on the communication channel with the preceding vehicle and can also monitor the health of the velocity measurement radar channel. An elegant solution that decouples the cyber-attack signal in the failures from the estimation error dynamics is developed.

It should be noted that potential attack threats on inter-vehicular communication systems and on sensor systems have been discussed previously in literature [5-7]. False data injection and denial of service attack can lead to significant problems in autonomous vehicles and connected vehicle systems that use inter-vehicular communication. Also, sensor faults can be a serious source of problems for many intelligent transportation systems. An attacker can obtain access to the internal system of the vehicle or transmit false data to the control system. Thus, it is necessary to have a resilient system for autonomous and/or connected vehicles that can be secure against cyber-attacks and sensor faults.

Recently, several researchers have focused on cyber-attacks

[1] Contact author: jeonx121@umn.edu

and sensor fault problems for connected vehicle systems. For an autonomous vehicle using an acceleration sensor and a radar, a sliding mode observer is used to detect sensor faults in [8]. In [9], two different observer techniques are proposed to estimate a vehicle's speed sensor fault. Authors in [10] proposed a sliding mode observer to detect and estimate denial of service attack for a connected vehicle. False data injection on acceleration information via V2V communication and sensor (LIDAR or radar) faults are considered and Hidden Markov Model-based attack detection method is proposed for cooperative adaptive cruise control applications in [11]. Most papers in literatures handle either cyber-attacks or sensor faults.

This paper is organized as follows. In the next section, a brief review of the SA-ACC system is provided. In Section 3, a model based on measurable states is developed from the SA-ACC system. An observer for cyber-attack and sensor fault estimation is proposed in Section 4. Results of simulation studies and discussion is presented in Section 5. Conclusions are presented in Section 6.

2. SA-ACC SYSTEM

The SA-ACC system aims to obtain high traffic capacity and small inter-vehicle spacing while using communication from only the preceding vehicle on the highway. The constant time gap spacing policy is utilized to design the controller of the SA-ACC system.

In the presence of actuator dynamics represented by a first-order lag, the vehicle model of the SA-ACC vehicle is described as

$$\tau \dddot{x}_i + \ddot{x}_i = u_{syn} \tag{2}$$

where τ is a lag constant associated with the lower dynamics of the vehicle, x_i is the i^{th} vehicle position and u_{syn} is the control input of the i^{th} vehicle. If the SA-ACC vehicle maintained a constant distance from the preceding vehicle, then the spacing error for the i^{th} vehicle in a string of vehicles would be defined as

$$\varepsilon_i = x_i - x_{i-1} + L_i \tag{3}$$

where L_i would be the desired constant spacing between vehicles.

However, a controller designed by using the constant spacing policy based on equation (3) would need wireless access to the lead vehicle speed and acceleration, in addition to preceding vehicle acceleration in order to maintain string stability in a string of autonomous vehicles. Therefore, in order to avoid requiring communication from the lead vehicle, the constant time-gap spacing policy is utilized to design a controller using only preceding vehicle information. The desired spacing between vehicles in the constant time-gap spacing policy is not constant but is linear function of speed:

$$\text{Desired spacing } = L_i + h\dot{x}_i \tag{4}$$

where L_i is a constant and h is time gap. The spacing error in the constant time-gap spacing policy is therefore

$$\bar{\varepsilon}_i = \varepsilon_i + h\dot{x}_i = x_i - x_{i-1} + L_i + h\dot{x}_i \tag{5}$$

Based on equation (5), the controller is given by

$$\begin{aligned} u_{syn} = &-k_1\ddot{x}_{i-1} + (k_1 + hk_1k_2)\ddot{x}_i \\ &-\frac{1}{h}(1 - hk_1k_2)\dot{\varepsilon}_i - \frac{k_2}{h}\varepsilon_i - k_2\dot{x}_i \end{aligned} \tag{6}$$

where $\ddot{x}_{i-1}$ is the acceleration of the preceding vehicle obtained by using inter-vehicle communication. k_1 and k_2 are controller design parameters. A detailed procedure to obtain the controller and determine its parameters can be found in [1].

3. NEW MODEL FOR SA-ACC SYSTEM

In this section, we develop a model incorporating relative motion between the preceding and following vehicle with the following vehicle using the SA-ACC system. The model is in terms of measurable variables (relative distance and velocity between the vehicles). Also, model for false data injection and denial of service cyber-attacks is presented.

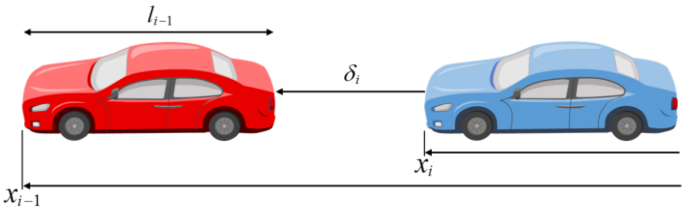

Figure 1: Preceding and following vehicles.

3.1 SA-ACC System Model

As shown in Figure 1, the radar-measured spacing distance for the i^{th} vehicle to the preceding vehicle can be defined as

$$\delta_i = x_{i-1} - x_i - l_{i-1} \tag{7}$$

where l_{i-1} is the length of the preceding vehicle. Then, we have

$$\begin{aligned} \dot{\delta}_i &= \dot{x}_{i-1} - \dot{x}_i \\ \ddot{\delta}_i &= \ddot{x}_{i-1} - \ddot{x}_i \\ \dddot{\delta}_i &= \dddot{x}_{i-1} - \dddot{x}_i \end{aligned} \tag{8}$$

By using equation (7) and (8), the controller becomes

$$
\begin{aligned}
u_{syn} = (hk_1k_2)\ddot{x}_{i-1} - k_2\dot{x}_i - (k_1 + hk_1k_2)\ddot{\delta}_i \\
+ \frac{1}{h}(1 - hk_1k_2)\dot{\delta}_i + \frac{k_2}{h}\delta_i \\
- \frac{k_2}{h}(L_i - l_{i-1})
\end{aligned}
\tag{9}
$$

Fortunately, the time lag constant associated with the preceding vehicle does not need to be known, since we directly obtain the acceleration information of the preceding vehicle using wireless communication. Thus, without considering its lower order dynamics, the preceding vehicle model can be represented as

$$
\begin{aligned}
\ddot{x}_{i-1} &= a_{i-1} \\
\dddot{x}_{i-1} &= 0
\end{aligned}
\tag{10}
$$

Substituting from equation (9) into equation (2) and using equation (10), we obtain

$$
\begin{aligned}
\dddot{\delta}_i = \frac{1}{\tau}(1 - hk_1k_2)a_{i-1} - \frac{1}{\tau}(1 - k_1 - hk_1k_2)\ddot{\delta}_i \\
- \frac{1}{\tau h}(1 - hk_1k_2)\dot{\delta}_i - \frac{k_2}{\tau h}\delta_i \\
+ \frac{k_2}{\tau}\dot{x}_i + \frac{k_2}{\tau h}(L_i - l_{i-1})
\end{aligned}
\tag{11}
$$

Finally, with a state vector $x = [\delta_i \quad \dot{\delta}_i \quad \ddot{\delta}_i]^T$, we have state space model:

$$
\begin{aligned}
\begin{bmatrix} \dot{\delta}_i \\ \ddot{\delta}_i \\ \dddot{\delta}_i \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -\frac{k_2}{\tau h} & -\frac{k_3}{\tau h} & \frac{(k_1 - k_3)}{\tau h} \end{bmatrix} \begin{bmatrix} \delta_i \\ \dot{\delta}_i \\ \ddot{\delta}_i \end{bmatrix} + \\
\begin{bmatrix} 0 \\ 0 \\ k_2/\tau \end{bmatrix} \dot{x}_i + \begin{bmatrix} 0 \\ 0 \\ k_3/\tau \end{bmatrix} a_{i-1} + \begin{bmatrix} 0 \\ 0 \\ k_2(L_i - l_{i-1})/h \end{bmatrix} \frac{1}{\tau}
\end{aligned}
\tag{12}
$$

where k_3 is $1 - hk_1k_2$. $\dot{x}_i$ can be easily obtained by using sensors on the vehicle and a_{i-1} is obtained by using inter-vehicle communication that can be the subject of cyber-attack.

Since a radar measures the relative distance and velocity, we have output equation as

$$
y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \delta_i \\ \dot{\delta}_i \\ \ddot{\delta}_i \end{bmatrix}
\tag{13}
$$

Equation (12) and (13) can be represented by the following compact form:

$$
\begin{aligned}
\dot{x} &= Ax + Bu + Fa_{i-1} + \mathit{\Delta} \\
y &= Cx
\end{aligned}
\tag{14}
$$

where

$$
\begin{aligned}
A &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -k_2/\tau h & -k_3/\tau h & (k_1 - k_3)/\tau \end{bmatrix}, \\
B &= \begin{bmatrix} 0 \\ 0 \\ k_2/\tau \end{bmatrix}, \quad F = \begin{bmatrix} 0 \\ 0 \\ k_3/\tau \end{bmatrix}, \\
\mathit{\Delta} &= \begin{bmatrix} 0 \\ 0 \\ k_2(L_i - l_{i-1})/\tau h \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}
\end{aligned}
\tag{15}
$$

Now, we also consider the model for two classes of cyber-attacks (false data injection and denial of service attacks) on the inter-vehicle wireless communication.

3.2 Cyber-Attack Model

We introduce a new variable μ as the signal (transmitted data: acceleration of preceding vehicle) obtained from inter-vehicle communication. Thus, the system model becomes

$$
\begin{aligned}
\dot{x} &= Ax + Bu + F\mu + \Delta \\
y &= Cx
\end{aligned}
\tag{16}
$$

False data injection attacks transmit false data to the control system or modify the transmitted data in the control system. Since the transmitted data can be corrupted by the false data injection attack, μ is defined as

$$
\mu = a_{i-1} + f_a
\tag{17}
$$

Denial of Service (DoS) attacks can keep the inter-vehicle communication network busy and can cause delays and congestions in the inter-vehicle communication channel. Therefore, the denial of service attacks can be modeled as the delay signal:

$$
\mu(t) = a_{i-1}(t - \tau_d)
\tag{18}
$$

where τ_d is unknown delay. By applying Taylor's theorem to equation (18) and assuming higher order terms negligible, the delay signal can be approximated as

$$
\mu(t) \approx a_{i-1}(t) - \tau_d \dot{a}_{i-1}(t)
\tag{19}
$$

Using the notation $f_d = -\tau_d \dot{a}_{i-1}(t)$ and omit time variable t for the sake of simplicity, the delay signal can be presented as

$$\mu = a_{i-1} + f_d \tag{20}$$

It is noted that equation (20) has the same structure as equation (17). Therefore, the two classes of the cyber-attacks can be modeled as

$$\mu = a_{i-1} + f_c \tag{21}$$

where f_c is either f_a or f_d. It is noted that f_c is assumed to be a constant or slowly varying.

4. OBSERVER AND CONTROLLER FOR RESILIENT SA-ACC SYSTEM

Instead of using the system model (16), we develop a model for the detection of cyber-attacks and sensor faults. The model involves cyber-attack and sensor fault terms. As a result, an observer designed corresponding the model can be developed to estimate the unknown cyber-attack and sensor fault terms so as to detect the cyber-attacks and sensor faults. The model is derived based on two assumptions.

First, we assume that the system is not corrupted by cyber-attacks (the system rejects cyber-attacks).

Second assumption is that sensor fault occurs only at the velocity measurement channel of the radar.

Based on the assumptions and using equation (21), the model (16) can be presented with unknown inputs f_c and f_s

$$\begin{aligned} \dot{x} &= Ax + Bu + F\mu + \Delta - Ff_c \\ y &= Cx + Df_s \end{aligned} \tag{22}$$

where $D = [0 \quad 1]^T$. By estimating unknown inputs f_c and f_s, the cyber-attack and sensor fault can be detected.

An unknown input observer that can estimate states and unknown inputs will be presented. Then, resilient control method under the cyber-attack will be proposed.

For unknown input estimation, a number of observer design methods have been proposed in literature. A proportional-integral observer was proposed to estimate the states and unknown inputs in [12]. An unknown input estimation method based on nonlinear observer design and dynamic model inversion is proposed in [13]. Another approach is designing observer for descriptor system that adding unknown input to the state vector [14]. In this paper, an observer design method based on descriptor systems is proposed to detect and estimate the unknown inputs due to cyber-attacks and sensor faults.

4.1 Descriptor System for Radar Sensor Fault

In order to deal with the radar sensor fault, f_s is considered as a state of the system. Using the new state vector, original system is converted to the descriptor system form. The state vector with f_s is defined as

$$\xi = [\delta_i \quad \dot{\delta}_i \quad \ddot{\delta}_s \quad f_s]^T \tag{23}$$

With the state vector (23), the system (22) is rewritten under the descriptor from:

$$\begin{aligned} E\dot{\xi} &= A_e\xi + Bu + F\mu + \Delta - Ff_c \\ y &= C_e\xi \end{aligned} \tag{24}$$

Detailed matrices in equation (24) are defined as

$$\begin{aligned} &E = [I_{n_x} \quad 0], \;\; A_e = [A \quad 0], \\ &C_e = [C \quad D] \end{aligned} \tag{25}$$

where I_{n_x} is the identity matrix of dimension n_x (size of state vector x).

Since the matrix D is full column rank, the following condition holds:

$$rank\left(\begin{bmatrix} E \\ C_e \end{bmatrix}\right) = rank\left(\begin{bmatrix} I_{n_x} & 0 \\ C & D \end{bmatrix}\right) = n_\xi \tag{26}$$

4.2 Unknown Input Observer for Cyber-Attack and Sensor Fault Estimation

Let us consider the following observer structure to estimate states and unknown inputs simultaneously:

$$\begin{aligned} \dot{z} &= Nz + Ly + Mu + G\mu + T\hat{f}_c + P_z\Delta \\ \hat{\xi} &= z + Q_z y \\ \dot{\hat{f}}_c &= H(y - \hat{y}) \end{aligned} \tag{27}$$

The matrices N, L, M, G, T, P_z, Q_z and H are observer parameters to be designed such that the estimation error $\tilde{\xi} = \xi - \hat{\xi}$ converges towards zero.

By using equation (24) and (27), the estimation error is

$$\tilde{\xi} = (I - Q_zC_e)\xi - z \tag{28}$$

From the rank condition (26), there exist matrices P_z and Q_z such that

$$P_zE + Q_zC_e = I_{n_\xi} \tag{29}$$

Also, P_z and Q_z can be computed as follow:

$$[P_z \quad Q_z] = \left(\begin{bmatrix} E \\ C_e \end{bmatrix}^T \begin{bmatrix} E \\ C_e \end{bmatrix}\right)^{-1} \begin{bmatrix} E \\ C_e \end{bmatrix}^T \tag{30}$$

Therefore, the estimation error dynamics can be written as

$$\dot{\tilde{\xi}} = P_z E \dot{\xi} - \dot{z} \tag{31}$$

Theorem 1: Consider the system (24) and observer (27). If there exist the symmetric matrix $P > 0$ and the matrix R of appropriate dimensions such that

$$\begin{aligned} N &= P_z A_e - K C_e \\ L &= K + N Q_z \\ M &= P_z B \\ G &= P_z F \\ T &= -P_z F \end{aligned} \tag{32}$$

and

$$\begin{aligned} &\begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix}^T P + P \begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix} \\ &-[C_e \quad 0]^T R - R^T [C_e \quad 0] + 2\alpha P \leq 0 \end{aligned} \tag{33}$$

then, the observer gain $[K \quad H]^T$ is given by

$$[K \quad H]^T = P^{-1} R^T \tag{34}$$

and with this value of the observer gain, the estimation error of the observer (27) converges exponentially towards zero. Therefore, the observer can estimate both unknown inputs due to the cyber-attacks and sensor faults simultaneously.

Proof: Using the system (24) and observer (27), the estimation error dynamics (31) is rewritten as

$$\begin{aligned} \dot{\tilde{\xi}} = N\tilde{\xi} + (P_z A_e - N - L C_e + N Q_z C_e)\xi \\ + (P_z B - M)u + (P_z F - G)\mu \\ - P_z F f_c - T \hat{f}_c \end{aligned} \tag{35}$$

The observer parameters are defined as (32). Then, equation (35) becomes

$$\dot{\tilde{\xi}} = (P_z A_e - K C_e)\tilde{\xi} - P_z F \tilde{f}_c \tag{36}$$

Using the observer (27) and the assumption that $\dot{f}_c = 0$, we have augmented system:

$$\begin{bmatrix} \dot{\tilde{\xi}} \\ \dot{\tilde{f}}_c \end{bmatrix} = \begin{bmatrix} (P_z A_e - K C_e) & -P_z F \\ -H C_e & 0 \end{bmatrix} \begin{bmatrix} \tilde{\xi} \\ \tilde{f}_c \end{bmatrix} \tag{37}$$

Rearrange equation (37), then we have

$$\begin{bmatrix} \dot{\tilde{\xi}} \\ \dot{\tilde{f}}_c \end{bmatrix} = \left[\begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} K \\ H \end{bmatrix} [C_e \quad 0] \right] \begin{bmatrix} \tilde{\xi} \\ \tilde{f}_c \end{bmatrix} \tag{38}$$

It should be noted that the estimation error dynamics is decoupled from u and μ. Thus, the observer (27) is allowed to estimate the state of the system and unknown inputs independently of the signal that may be corrupted by cyber-attacks or sensor faults.

In order to find a gain for the exponential stable system for equation (38), we require that the following differential inequality is satisfied:

$$\dot{V} \leq -2\alpha V \tag{39}$$

where V is the Lyapunov function candidate defined as

$$V = \begin{bmatrix} \tilde{\xi} \\ \tilde{f}_c \end{bmatrix}^T P \begin{bmatrix} \tilde{\xi} \\ \tilde{f}_c \end{bmatrix} \tag{40}$$

for observer design and α is a positive constant. The inequality (39) implies the exponential stability of the system [15]. By calculating the derivative of the Lyapunov function, we have

$$\dot{e}^T P e + e^T P \dot{e} + 2\alpha e^T P e \leq 0 \tag{41}$$

where $e = [\tilde{\xi} \quad \tilde{f}]^T$. Equation (41) is satisfied when following condition is satisfied:

$$\begin{aligned} &\left[\begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} K \\ H \end{bmatrix} [C_e \quad 0] \right]^T P + \\ &P \left[\begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} K \\ H \end{bmatrix} [C_e \quad 0] \right] + 2\alpha P \leq 0 \end{aligned} \tag{42}$$

By introducing a new variable $R = [K \quad H]P$, Equation (42) becomes

$$\begin{aligned} &\begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix}^T P + P \begin{bmatrix} P_z A_e & -P_z F \\ 0 & 0 \end{bmatrix} \\ &-[C_e \quad 0]^T R - R^T [C_e \quad 0] + 2\alpha P \leq 0 \end{aligned} \tag{43}$$

■

4.3 Cyber-Attack and Sensor Fault Detection

In this section, we discuss how to detect cyber-attacks and sensor faults based on the estimated terms $\hat{f}_c$ and $\hat{f}_s$ from the proposed unknown input observer.

If there are no cyber-attack and sensor fault i.e., the model (22) is the same as actual system (14), estimated unknown inputs $\hat{f}_c$ and $\hat{f}_s$ converge to zero. If cyber-attack exists ($f_c \neq 0$), $\hat{f}_c$

becomes non-zero and cyber-attack can be detected. It is noted that $\hat{f}_c$ may not converge to true value due to discrepancy between the actual system and the system model for the observer. However, still $\hat{f}_c$ can be used to detect the cyber-attack since $\hat{f}_c$ cannot be zero under the cyber-attack.

If sensor fault occurs, non-zero value of $\hat{f}_s$ is obtained from the observer. It is noted that $\hat{f}_c$ may not be zero due to discrepancy between the actual system and the system model for the observer even though cyber-attack does not occur.

As a result, we propose two-step approach to detect cyber-attacks or sensor faults. First, the system checks the value of $\hat{f}_s$ to find if there exist any sensor faults. If the value of $\hat{f}_s$ exceeds certain threshold, i.e., sensor fault occurs at velocity channels of the radar, the system alerts the driver and changes to manual driving from SA-ACC operation. Second, if there is no sensor fault, the system checks the value of $\hat{f}_c$. If the value of $\hat{f}_c$ exceeds certain threshold, i.e., cyber-attack occurs, the system switches the controller and can achieve resilient control for SA-ACC system, as shown in Figure 2.

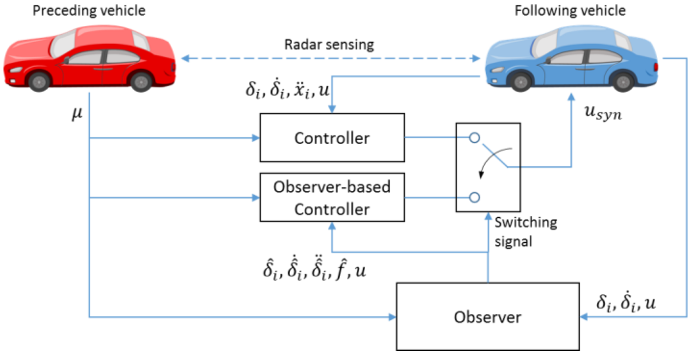
Preceding vehicle
Following vehicle
Radar sensing
$\delta_i, \dot{\delta}_i, \ddot{x}_i, u$
μ
u_{syn}
Controller
Observer-based Controller
Switching signal
$\hat{\delta}_i, \dot{\hat{\delta}}_i, \ddot{\hat{\delta}}_i, \hat{f}, u$
$\delta_i, \dot{\delta}_i, u$
Observer

Figure 2: Resilient control for SA-ACC system.

4.4 Controller for Resilient SA-ACC System

Resilient control for SA-ACC system can be accomplished by utilizing the controller follow, instead of using the controller (6):

$$\begin{aligned} u_{syn} = (hk_1k_2)\mu - k_2\dot{x}_i - (k_1 + hk_1k_2)\ddot{\hat{\delta}}_i \\ + \frac{1}{h}(1 - hk_1k_2)\dot{\hat{\delta}}_i + \frac{k_2}{h}\hat{\delta}_i \\ - \frac{k_2}{h}(L_i - l_{i-1}) - (hk_1k_2)\hat{f}_c \end{aligned} \tag{44}$$

This controller leads the actual system to exact match with the model (22). Hence, the proposed unknown input observer with the controller (44) guarantees that the estimation error of states and unknown inputs converges exponentially towards zero, and accomplishes resilient control for SA-ACC under the cyber-attack.

5. SIMULATION STUDIES AND DISCUSSION

The developed observer based on the descriptor system for the cyber-attack and sensor fault detection and controllers described in the previous section has been evaluated using simulations. For the SA-ACC system the system and controller parameters are $\tau = 0.4$, $l_{i-1} = 5$, $L_i = 7.3$, $h = 0.5$, $k_1 = -0.8$, $k_2 = 2.5$ and $k_3 = 2$.

We solve equation (32) – (34) for the observer gain using the LMI toolbox in MATLAB. The observer gain is with the exponential stability parameter $\alpha = 3.5$:

$$K = \begin{bmatrix} 17.3524 & 4.5678 \\ 237.1617 & 64.2509 \\ 271.4056 & 69.4228 \\ -244.0019 & -60.2509 \end{bmatrix} \tag{45}$$
$$H = [-762.0394 \quad -196.6185]$$

The preceding vehicle is initially driving with 10m/s and the following vehicle is stopped and the initial distance between the preceding and following vehicles is 10m. Gaussian noise $\sim\mathcal{N}(0, 6^2[cm])$ and $\sim\mathcal{N}(0, 60^2[cm/s])$ are added to the range and velocity measurements respectively. The upper and lower values of the thresholds for sensor fault and cyber-attack detection are set as ± 3. In practice, the threshold can be set based on the sensor noise. If the system switches the controller to equation (44) for resilient control under cyber-attacks, we utilize 1 for the value of h.

5.1 Simulation Results with Sensor Faults

we evaluate the performance of the proposed observer for the radar sensor fault detection. The sensor fault is modeled by adding false data f_v to the velocity measurement respectively. We consider the sensor fault in the velocity measurement channel of the radar. The sensor fault is generated as

$$f_v = \begin{cases} 10, & t \geq 10 \\ 0, & \text{otherwise} \end{cases} \tag{46}$$

Due to the sensor fault, the following vehicle perceives an abrupt increase of the velocity of the preceding vehicle. As shown in Figure 3, the following vehicle is controlled to increase the velocity of the vehicle to maintain the desired distance based on the wrong information. As a result, collision ($\delta_i \leq 0$) occurs at 19.28 seconds as shown in Fig. 3. Fig. 4 shows the results of the proposed observer. The proposed observer successfully estimates the false data due to the sensor fault in the velocity channel of the radar and detect the fault immediately at 10 seconds.

5.2 Simulation Results with Cyber-Attacks

First, false data injection cyber-attack on the acceleration information is simulated, as shown in Figure 5 and 6. The inter-vehicle communication is attacked by injecting follow values on the acceleration information of the preceding vehicle:

$$f_a = \begin{cases} 3(t-10), & t \geq 10 \\ 0, & \text{otherwise} \end{cases} \tag{47}$$

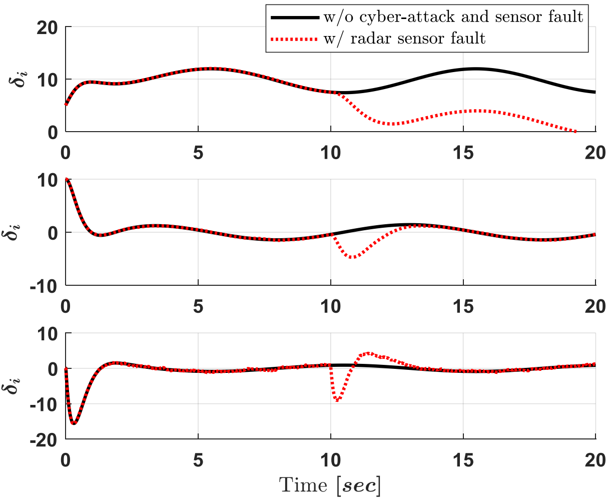

Figure 3: Behavior of SA-ACC system in the presence of the sensor fault in the velocity measurement channel of the radar.

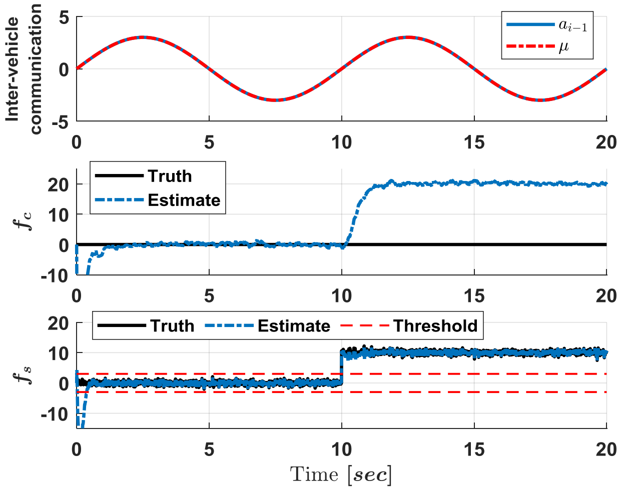

Figure 4: Acceleration of the preceding vehicle, cyber-attack estimation and sensor fault estimation in the presence of the sensor fault in the velocity measurement channel of the radar.

Due to the cyber-attack, the following vehicle receives wrong information such that the preceding vehicle is accelerating as shown in Figure 5. This will likely result in a collision. Figure 6 shows the performance of the controller with the proposed observer. Once the cyber-attack is detected at 11.23 seconds in Figure 5, the system switches to the controller based on the proposed observer as shown in Figure 2 and maintains the desired distance with larger time gap while the cyber-attack exists as shown in Figure 6. Also, it is shown that the proposed observer estimates the injected false data f_a successfully.

Simulation studies also conducted to evaluate the SA-ACC system with the proposed observer in the presence of the DoS cyber-attack. DoS attack on the inter-vehicle communication channel is considered and it causes communication delay. We

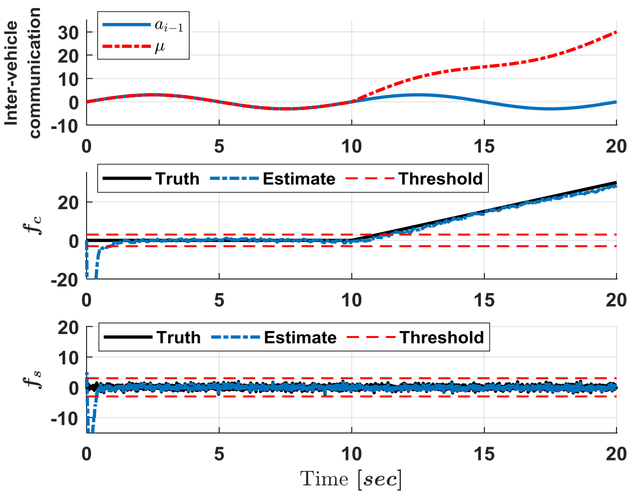

Figure 5: Acceleration of the preceding vehicle, cyber-attack estimation and sensor fault estimation in the presence of the false data injection cyber-attack on the communication channel.

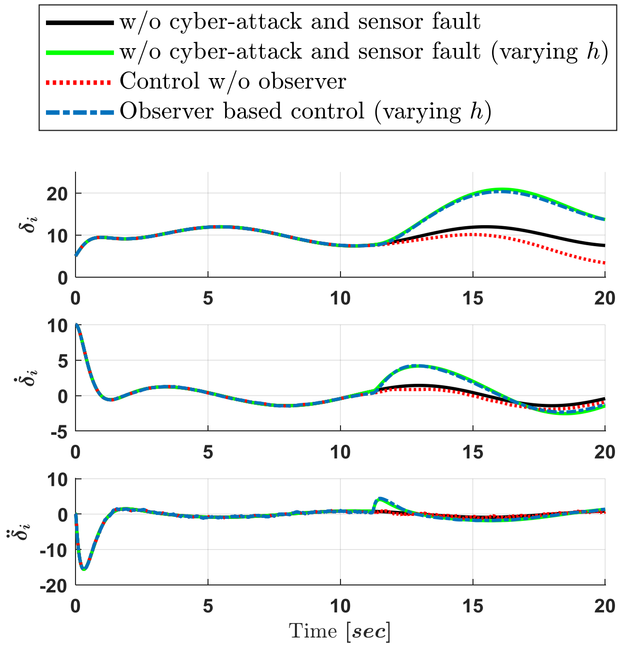

Figure 6: Behavior of SA-ACC system in the presence of the false data injection cyber-attack on the communication channel.

assume that the following vehicle receives the signal $\mu(t)$ as follows:

$$\mu(t) = \begin{cases} a_{i-1}(t), & t \leq t_1 \\ a_{i-1}(t_1), & t_1 \leq t \leq t_1 + \tau_d \\ a_{i-1}(t-\tau_d), & t \geq t_1 + \tau_d \end{cases} \tag{48}$$

where $t_1 = 10$ and $\tau_d = 5$. The true acceleration of the preceding vehicle and the delay signal due to DoS attack are shown in Figure 7. The preceding vehicle starts to decelerate at

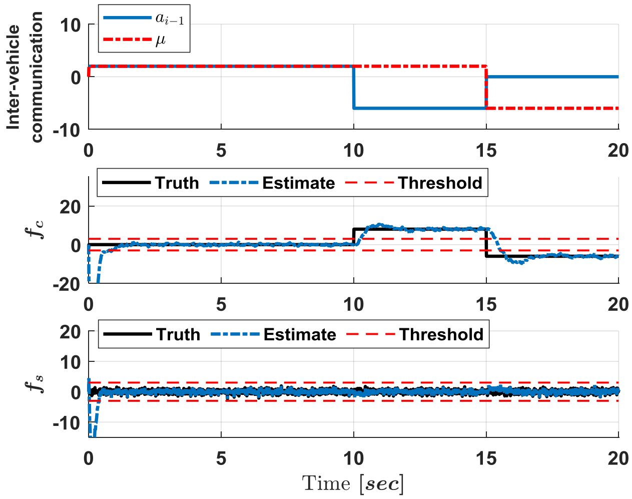

Figure 7: Acceleration of the preceding vehicle, cyber-attack estimation and sensor fault estimation in the presence of the denial of service cyber-attack on the communication channel.

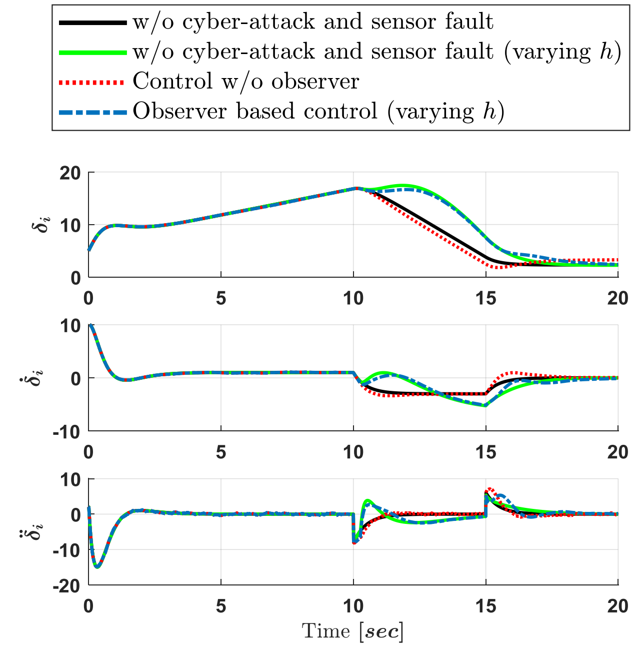

Figure 8: Behavior of SA-ACC system in the presence of the denial of service cyber-attack on the communication channel.

10 seconds. However, because of the DoS cyber-attack, the following vehicle receives delay signal and cannot perceive the deceleration of the preceding vehicle. As a result, the SA-ACC system without using the proposed controller and observer cannot maintain desired distance between the preceding and following vehicles as shown in Figure 8. This may lead to fail to maintain of string stability. The proposed observer estimates false data due to the DoS cyber-attack successfully and detect the DoS attack at 10.26 seconds as shown in Figure 7. Furthermore, Figure 8 shows that the following vehicle maintains desired distance to the preceding vehicle even in the presence of DoS cyber-attack using the proposed observer-based controller.

6. CONCLUSION

This paper developed an observer for detection of cyber-attack on a communication channel while also simultaneously monitoring the health of the velocity measurement radar channel for a connected vehicle. A semi-autonomous adaptive cruise control (SA-ACC) vehicle was considered which used wireless communication with its immediately preceding vehicle in the same lane. The wireless connectivity enabled the vehicle to operate at small time-gap distances without creating string instability. However, the reliability of the wireless connectivity was critical for ensuring safe vehicle operation and a cyber-attack in this channel needed to be detected autonomously. The presence of two unknown inputs related to both sensor failure and cyber-attack seemingly posed a difficult estimation challenge.

The dynamic system was first represented in descriptor system form. Then an observer with estimation error dynamics decoupled from the cyber-attack signal was developed.

The performance of the observer was extensively evaluated in simulations. Simulation results showed that the estimation system was able to detect either a fault in the velocity measurement radar channel or a cyber-attack. Also, the proposed observer-based controller achieves resilient SA-ACC system under the cyber-attacks. The fundamental estimation algorithm developed herein can be extended in the future to enable cyber-attack detection in more complex connected vehicle architectures.

ACKNOWLEDGEMENTS

This research was supported in part by a research grant from the National Science Foundation (NSF Grant PFI-1631133).

REFERENCES

[1] R. Rajamani and C. Zhu, "Semi-autonomous adaptive cruise control systems," in *IEEE Transactions on Vehicular Technology*, vol. 51, no. 5, pp. 1186-1192, Sept. 2002.

[2] J. E. Siegel, D. C. Erb and S. E. Sarma, "A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391-2406, Aug. 2018.

[3] D. Lang, T. Stanger, and L. d. Re, “Opportunities on fuel economy utilizing v2v based drive systems,” *SAE Technical Paper*, no. 2013-01-0985, 2013.

[4] R. Rajamani, *Vehicle dynamics and control*, Springer Science & Business Media, 2011

[5] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546-556, April 2015.

[6] R. van der Heijden, T. Lukaseder and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (CACC)," *2017 IEEE Vehicular Networking Conference (VNC)*,

Torino, 2017, pp. 45-52.

[7] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898-2915, Nov. 2017.

[8] K. Oh, S. Park, J. Lee, and K. Yi. "Functional perspective-based probabilistic fault detection and diagnostic algorithm for autonomous vehicle using longitudinal kinematic model." *Microsystem Technologies*, pp. 1-11, 2018.

[9] M. Boukhari, A. Chaibet, M. Boukhnifer, and S. Glaser. "Proprioceptive Sensors' Fault Tolerant Control Strategy for an Autonomous Vehicle." *Sensors* 18, no. 6, 2018.

[10] Z. Abdollahi Biron, S. Dey and P. Pisu, "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems," in *IEEE Transactions on Intelligent Transportation Systems*.

[11] M. Jagielski, N. Jones, CW. Lin, C. Nita-Rotaru, and S. Shiraishi, "Threat Detection for Collaborative Adaptive Cruise Control in Connected Cars." *11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pp. 184-189, ACM, 2018.

[12] F. Bakhshande, D. Söffker, Proportional-Integral-Observer: A brief survey with special attention to the actual methods using ACC Benchmark, *IFAC-PapersOnLine*, vol. 48, issue 1, pp. 532-537, 2015.

[13] G. Phanomchoeng and R. Rajamani, "Real-Time Estimation of Rollover Index for Tripped Rollovers With a Novel Unknown Input Nonlinear Observer," in *IEEE/ASME Transactions on Mechatronics*, vol. 19, no. 2, pp. 743-754, April 2014.

[14] G. Phanomchocng, A. Zemouche, W. Jeon, R. Rajamani and F. Mazenc, "H_∞ Observer for Descriptor Nonlinear Systems with Nonlinear Output Equations," *2018 Annual American Control Conference (ACC)*, Milwaukee, WI, pp. 5952-5956, 2018.

[15] H. K. Khalil, *Nonlinear Systems*, Prentice Hall, Upper Saddle River, NJ, USA, 3rd edition, 2002.