A Decision Support System for Improving Resiliency of Cooperative Adaptive Cruise Control Systems

Shirin Noei\textsuperscript{a*}, Arman Sargolzaei\textsuperscript{b}, Alireza Abbaspour\textsuperscript{c}, Kang Yen\textsuperscript{c}

\textsuperscript{a}Department of Civil and Coastal Engineering, University of Florida, Gainsville, FL, USA
\textsuperscript{b}Department of Electrical Engineering, Florida Polytechnic University, Lakeland, FL, USA
\textsuperscript{c}Department of Electrical and Computer Engineering at Florida International University, Miami, FL, USA

Abstract

Advanced driver assistance systems (ADASs) enhance transportation safety and mobility, and reduce impacts on the environment and economical costs, through decreasing driver errors. One of the main features of ADASs is cruise control system that maintains the driver's desired speed without intervention from the driver. Adaptive cruise control (ACC) systems adjust the vehicle's speed to maintain a safe following distance to the vehicle in front. Adding vehicle-to-vehicle and vehicle-to-infrastructure communications (V2X) to ACC systems, result in cooperative adaptive cruise control (CACC) systems, where each vehicle has trajectory data of all other vehicles in the same lane. Although CACC systems offer advantages over ACC systems in increasing throughput and average speed, they are more vulnerable to cyber-security attacks. This is due to V2X communications that increase the attack surface from one vehicle to multiple vehicles. In this paper, we inject common types of attack on the application layer of connected vehicles to show their vulnerability in comparison to autonomous vehicles. We also proposed a decision support system that eliminates risk of inaccurate information. The microscopic work simulates a CACC system with a bi-objective PID controller and a fuzzy detector. A case study is illustrated in detail to verify the system functionality.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology

Keywords: Adaptive Cruise Control; Cooperative Adaptive Cruise Control; Cyber Attacks; Resiliency; Autonomous Vehicles; Connected Vehicles; Decision Support System; Bi-objective PID Controller; Fuzzy Detector

* Corresponding author. Tel.: +1-305-766-0556
E-mail address: noei.shirin@gmail.com
1. Cooperative adaptive cruise control

The purpose of advanced driver assistance systems (ADASs) is that driver error is reduced or even eliminated, and efficiency in transport is enhanced. Benefits of ADASs implementations are potentially considerable because of a significant decrease in human suffering, economical costs, and environmental pollution [1].

One of the main features of ADASs is cruise control system that accurately maintains the driver's desired set speed, without intervention from the driver.

Adaptive cruise control (ACC) systems are advanced cruise control systems, which enable the drivers to set a desired cruising speed as well as a desired gap with respect to a lead vehicle. If a lead vehicle is present, the system automatically adjusts the vehicle’s speed to maintain a safe following distance to the vehicle in front. Otherwise, the system works as a conventional cruise control system [2].

ACC systems use LiDAR sensors to measure the distance to the back of the preceding vehicle and also to sense rate of change in the measured distance to take proper actions in response to the acceleration and deceleration of the target vehicle. These systems have a considerable high response delay in detecting changes to the trajectory data of the lead vehicle that results in a large threshold for the minimum safe gap [3].

Adding wireless vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to ACC systems result in cooperative adaptive cruise control (CACC) systems. CACC systems have faster response to the predecessor’s gas and brake pedal actuator, which allows a significant reduction in the safe gap between the rear end of the target vehicle and the front of the host vehicle [4].

ACC features are compatible with autonomous vehicles (AVs), where each vehicle is not subject to any additional input from other vehicles or infrastructure. This limits the ability of ACC systems to follow the target vehicle accurately and respond to speed changes of the leading vehicle in a timely manner. This can also negatively affect the traffic flow capacity and stability.

Connected vehicles (CVs) involve some level of coordination between the vehicles and the roadway infrastructure, where each vehicle is not entirely independent. Adding communication systems to ACC systems make any vehicle possible to follow the leading vehicle with higher accuracy and faster response to changes. This can improve traffic throughput, reduce traffic congestion, increase average speed, and enhance the flow’s string stability, without compromising safety or expanding roadway infrastructure [5].

2. Problem statement

ADASs rely on a range of sensing and communication systems. Such dependencies make vehicular platforms vulnerable to a multitude of cyber-security threats, which have the potential to endanger passengers’ safety [6].

AVs are capable of navigating themselves without human input. AVs use different combination of elements including sensors, laser, GPS, map, and stereo cameras to perceive the environment. These integrated components can form potential attack surfaces [7].

On the other hand, CVs use V2V and V2I communications (V2X) to get trajectory data of all other vehicles in a specific segment. Although the additional information can provide supplementary tools to verify the vehicles’ status, they can provide attackers with additional attack surface [8].

To propose a robust CACC system, we assumed a platoon of three vehicles driving at a specific following distance. Although the gap between the vehicles is dependent on the trajectory data of the two proceeding vehicles, it is more secure to use the distance measurements from sensing technologies.

To develop a decision support system (DSS), the microscopic work simulates a CACC system with a bi-objective PID controller, where inputs to the controller are distance error and speed error, and output is acceleration or braking. If the measured distance is less than the desired gap, the speed of the host vehicle changes to the speed of the target vehicle. To ensure system resiliency, a fuzzy detector is proposed that predicts the speed of the leader vehicle using state estimator and adjusts the safe distance.

The main contribution of this paper is to develop a DSS to address security issues at the application layer of a system of CVs. This is done through designing a control strategy that detects possible threats and takes proper actions to prevent subsequent incidents.
3. System setup

Consider a platoon of three vehicles that use wireless V2V communications to send their current state including location, speed, and acceleration/deceleration, and receive the same data from other vehicles in the same lane (Fig. 1). For the ease of calculations, the vehicles are numbered starting with the platoon leader as vehicle 1, its follower as vehicle 2, and the last one as vehicle 3.

![Fig. 1. Cooperative adaptive cruise control system.](image)

Dedicated short-range communication (DSRC) is a wireless communication system that provides transmission of data between the vehicles and the roadside or between the vehicles and other vehicles. This source of data is not robust enough to cyber threats [9]. To enhance the system resiliency, the distance between the two proceeding vehicles is measured using LiDAR sensors. However, it is less accurate to use this measurement for calculating the trajectory data of the target vehicle [10].

4. System setup

Let’s consider a vehicle with mass \( m \) and velocity \( v \). \( u \) represents the force generated at the tire interface in the opposite or the same direction of the vehicle’s speed. From the Newton’s second law of motion, a state-space model of a cruise control system can be obtained as in Equation (1).

\[
\begin{bmatrix}
    \dot{x}_i(t) \\
    \dot{v}_i(t)
\end{bmatrix} =
\begin{bmatrix}
    v_i(t) \\
    u_i(t) + \frac{b_i}{m_i} v_i(t)
\end{bmatrix}
\]

where \( v \) is the vehicle’s velocity, \( b \) is the friction force between the road and the tire, \( i \) is the vehicle ID, and \( u \) is the driving force of the vehicle’s engine. After rearranging the Laplace transform function in Equation (2), the transfer function of the open-loop cruise control system for each of the vehicles can be obtained as Equation (3).

\[
m_i s V_i(s) - b_i V_i(s) = U_i(s)
\]

\[
\frac{V_i(s)}{U_i(s)} = \frac{1}{m_i s + b_i}
\]

5. System dynamics under attack

Although CVs benefit from communication of data, which allows them to have faster responses and considerable shorter vehicle-following gaps, a system of CVs is vulnerable to different types of cyber-security attacks on its physical layer, application layer, and network layer (Fig. 2) [11]. Physical-layer and privacy-leakage attacks are related to the hardware or software of each vehicle. Application-layer attacks affect particular functions of the system such as CACC. Main examples of this type of attack are message falsification, spoofing, and replay attacks.
In network-layer attacks, adversary targets multiple applications functionality. Denial-of-Service (DoS) attack and spoof jamming are common examples.

The state space model of the system of CVs under attack is modeled as the following equation.

\[
\begin{bmatrix}
\dot{x}_i(t) \\
\dot{v}_i(t)
\end{bmatrix} = \begin{bmatrix}
\frac{\tilde{v}_i(t)}{u_i(t) + \frac{b_i}{m_i}\tilde{v}_i(t)}
\end{bmatrix}
\]

where \(\tilde{v}_i(t)\) is the fault speed injected to the system.

\[
\tilde{v}_i(t) = \begin{cases} 
v_i(t) & \text{otherwise} \\
\alpha v_i(t) + \beta & \text{attack}
\end{cases}
\]

\(\alpha\) and \(\beta\) are zero for DoS attack, and are random values for false data injection (FDI) attack.

6. Control methodology

Consider a system of three CVs driving in the same lane. These vehicles use V2X communications for exchange of data. Our control system consists of a bi-objective PID controller and a fuzzy detector (Fig. 3). When distance between the two preceding vehicles drops below the safe threshold, our proposed controller is engaged to maintain the desired gap and speed.

6.1. Bi-objective PID controller

The bi-objective PID controller has speed error and distance error as inputs and braking/acceleration actuation as output. Speed error is defined as the difference between the desired speed and the speed of the subject vehicle. When no leading vehicle is detected, the desired speed is the same as the reference cruise speed. Otherwise, this value is equal to the speed of the target vehicle. On the other hand, distance error is the difference in the gap measured using LiDAR sensors and the safe desired distance.

CACC drivers can choose a safe headway from 0.6 to 1.1 sec, in contrast to the available ACC settings from 1.1 to 2.2 sec [12]. The distance corresponding to this time gap is clearance that is product of the headway and the
subject vehicle’s speed. To address the initial space between the two vehicles, a minimum safe distance of 2 ft is added to the clearance value.

6.2. Fuzzy detector

In CACC systems, the lead vehicle trajectory data are transmitted to the follower vehicles through DSRC wireless communication. These data are vulnerable to cyber-security threats and are not reliable enough to be used directly in the control system. To propose a robust controller, the lead vehicle’s motion is estimated using a state estimator [13].

As shown in Fig. 4, values of the membership function are assigned to the linguistic variables using three fuzzy subsets called low, medium, and high [14, 15]. Inputs to the proposed fuzzy detector are speed of the follower vehicle and the difference between the actual and the estimated speed of the lead vehicle. Output is the additional safe distance added to the current gap to prevent possible incidents.

Fig. 4. Inputs and output of the proposed fuzzy detector.
Nine fuzzy rules are generated with the knowledge base of the system (Table 1). Where L, M, and H are add low, add medium, and add high positive values to the minimum safe distance between the two vehicles.

<table>
<thead>
<tr>
<th>Table 1. Fuzzy rules.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
</tr>
<tr>
<td>Speed:num</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>

7. Results

In this section, a series of scenarios are performed to test performance of the designed controller under a range of representative driving conditions. Fig. 5 shows a scenario, in which the lead vehicle makes repeated accelerate and decelerate maneuvers, while the subject vehicle follows it if the distance is less than gap distance otherwise follows its own desired speed. The proposed PID controller can smoothly track changes in the reference speed. Note that the follower PID controller is designed to response faster to changes compared with leader PID controller.

Fig. 5 (a) shows deceleration of the lead vehicle after two-step acceleration. In the first 30 seconds, the vehicle is speeding up. But at the end of this time, the vehicle starts slowing down. With the feed-forward information from wireless communications, CACC controller of the host vehicle reacts very quickly to the speed changes of the target vehicle and brakes in a timely manner to avoid rear-end collisions (Fig. 5 (b)). It should be noted that the follower vehicle reference speed increases at 10 seconds which is 5 seconds later than leading vehicle. As shown in Fig. 5 (c), the minimum safe distance between the two vehicles is well regulated at 2 ft.

(a) Solid line is the reference speed and dashed line is actual vehicle speed
(b) Solid line is the reference speed and dashed line is actual vehicle speed
The second scenario evaluates performance of the system under FDI or DoS attack. The proposed fuzzy detector constantly compares the lead vehicle’s speed obtained from DSRC communication with the estimated speed of the lead vehicle using the state estimator. When this value exceeds a specified fuzzy threshold, safe distance between the two vehicles must be increased with respect to the follower vehicle’s speed.

As shown in Fig 6 (a), an adversary injects a fault data to the system at time 31 sec. This threat transmits a false value of 20 mi/h to the follower vehicle. In absence of a resilient control system, the subject vehicle assumes that the target vehicle is driving at the speed of 20 mi/h. This results in rear-end collisions that may endanger passengers’ safety (Fig. 6 (d)). To propose a resilient control system, the controller adds an additional distance of approximately 4.5 ft to the minimum safe distance to prevent subsequent incidents (Fig. 6 (b) and Fig. 6 (c)).
8. Conclusion

Autonomous vehicles (AVs) use sensing technologies to detect presence of the vehicle ahead in addition to the following gap and rate of change in the distance measurements. Sensing a change in the lead vehicle’s motion increases the response duration and limits the ability of AVs to react quickly and accurately to the target vehicle’s deceleration.

Connecting vehicles via wireless communication allows for faster and more accurate response to changes. From this perspective, connected vehicles (CVs) are better able to dampen shock waves in the traffic stream. Although AVs are resilient in terms of cyber-security attacks due to their on-board control systems and less attack surface, CVs are less robust due to the data transmission between the vehicles.

In this paper, we proposed a bi-objective PID controller that adjusts the subject vehicle’s speed with respect to the deceleration of the leading vehicle and error in the distance measurements. To address security issues of a system of CVs, a fuzzy detector is also introduced that detects possibility of a cyber threat and takes proper actions in response to the specific attack.

Results clearly show that our designed controller works well under both secure and unsecure conditions. The control system can detect any adversary access to the system and can prevent subsequent crashes by adjusting the safe following distance.

References