IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 19, 2021, accepted October 22, 2021, date of publication November 1, 2021, date of current version November 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3124547

Attack Detection and Defense System Using an Unknown Input Observer for Cooperative Adaptive Cruise Control Systems

YUDAI YAMAMOTO, NAOMI KUZE, (Member, IEEE), AND TOSHIMITSU USHIO, (Member, IEEE)
Graduate School of Engineering Science, Osaka University, Toyonaka 560-8531, Japan

Corresponding author: Naomi Kuze (kuze@sys.es.osaka-u.ac.jp)

This work was supported by Grant-in-Aid for Challenging Research of the SECOM Science and Technology Foundation.

ABSTRACT Cooperative adaptive cruise control (CACC) is a technology for the automated control of platoons of vehicles. CACC controls the behavior of vehicles based on information that is shared among the vehicles through vehicle-to-vehicle (V2V) communication. However, cyberattacks on V2V communication can degrade the control performance and may cause serious accidents such as vehicle collisions; therefore, it is important to improve the resilience against such attacks. In this paper, we propose a novel attack detection and defense mechanism for CACC. Our approach is based on an unknown input observer (UIO), which estimates vehicle states by treating the unreliable information obtained through V2V communication as unknown inputs. Attacks on V2V communication are detected from the estimated states. When an attack is detected, the control method is switched to a secure method. Through simulation experiments, we show that the proposed mechanism can detect attacks immediately and accurately, allowing the stability of the platoon to be maintained.

INDEX TERMS Attack detection, attack defense, cooperative adaptive cruise control (CACC), unknown input observer (UIO).

I. INTRODUCTION

Advances in information and control technologies have led to the development of intelligent transportation systems (ITSs). In particular, focus has been placed on automated vehicle control for improving the effectiveness and safety of transportation systems. Cooperative adaptive cruise control (CACC) [1] (Fig. 1) is one of the most promising technologies for the automated control of vehicle platoons (referred to simply as platoons in this paper). CACC controls the behavior of the vehicles in a platoon in an autonomous and cooperative manner based on information shared through vehicle-to-vehicle (V2V) communication to realize safe and effective cruising. In a platoon with CACC, each vehicle is equipped with a controller, a V2V communication device, and a sensor. The controller calculates the control inputs to the vehicle based on data obtained via V2V communication and the sensor. There have been many studies on CACC [1]–[7]. For example, in [2], the authors proposed a method for the longitudinal and lateral control of platoons. In [3], a control method was proposed for platoons with uncertain dynamics. In [4], [5], the authors proposed an ecological adaptive cruise control (Eco-CACC) strategy for improving the fuel economy of a heterogeneous platoon. In [6], the authors proposed a cooperative optimal power split (COPS) method for decreasing the energy consumption of a group of intelligent electric vehicles. In [7], the authors proposed a novel switched control strategy for a heterogeneous vehicle platoon based on multiple objectives (SCSHPM) and showed its effectiveness.

When designing a controller, one must consider the relevant resource limitations [8]. In [8], the capacities of memory and processors were discussed. Considering the limited nature of such resources, it is important to establish an attack detection and defense mechanism that takes the available computational resources into account.

For platoons using CACC, *string stability* [9] is a fundamental and important property. A platoon is string stable if range errors do not propagate from one vehicle to the following vehicle. In a platoon using CACC, the controller in each vehicle needs to be designed to enhance the string

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

stability even when the platoon is attacked [10]. In [10], the authors designed a decentralized controller for CACC considering string stability.

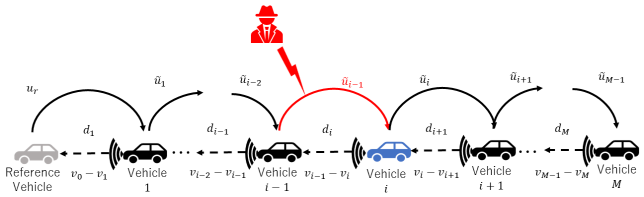


FIGURE 1. Cyberattack on V2V communications in a platoon with CACC.

Moreover, transmission delays exist in V2V communications, which may cause a loss of string stability. In [11], the string stability in the presence of delay was analyzed using the magnitude of the string stability transfer function in both the continuous-time and discrete-time domains.

Cyberattacks on V2V communications, in which attackers maliciously eavesdrop on, interfere with and/or tamper with V2V communication data, have become a serious problem [12], [13] in recent years. In platoons using CACC, such attacks can cause a loss of string stability [14]–[16]. In [14], the various types of attacks on platoons with CACC were discussed, and the author showed that attacks on V2V communications could cause a significant loss of string stability. More specifically, the range errors among the vehicles increase, which results in traffic congestion and, in the worst case, may cause vehicle collisions. The effects on string stability of attacks on V2V communications have been investigated in previous works [15], [16]. Improving the resilience against such attacks on V2V communications is an essential and challenging task.

The two main requirements for mitigating attacks are attack detection and defense. When a platoon with CACC is attacked, the attack needs to be detected quickly and with high accuracy, and many attack detection mechanisms have been proposed for CACC [17]–[21]. In [17], the authors focused on replay attacks on connected vehicles and proposed a replay attack detection mechanism based on a noisy control signal methodology. In [18], the authors used a partial differential equation model for detecting attacks. In [19], [20], an anomaly detection mechanism that utilizes the physical laws of kinematics and a data fusion technique was proposed. In [21], the authors introduced a sliding mode observer to detect and estimate cyberattacks.

Once an attack is detected, the vehicles need to defend against the damage caused by the attack [22]–[25]. Defense mechanisms against jamming attacks were proposed in [22], [23], and an attack-resilient controller was designed in [24]. One technology for attack defense is called fallback control [25]. In fallback control, the system is normally observed and controlled by a networked controller, but when an attack is detected, the controller is switched from the networked controller to a local controller to reduce the effect of the attack. However, these conventional defense approaches require the design and implementation of at least two controllers, one for normal situations and another for attack defense, which increases the overall complexity of the system.

To reduce the system complexity, we utilize an unknown input observer (UIO). UIOs are used to estimate the state of a system in the presence of unknown inputs. There are many studies on fault diagnosis using UIOs [26], [27]. In [26], [27], mechanisms were proposed for diagnosing faults accurately even when the information available from actuators or sensors is unreliable due to the faults. In these mechanisms, the UIO estimates the system state by treating the unreliable inputs from the actuators or sensors as unknown inputs. In recent years, UIOs have attracted attention as a promising approach for cyberattack detection [28], [29].

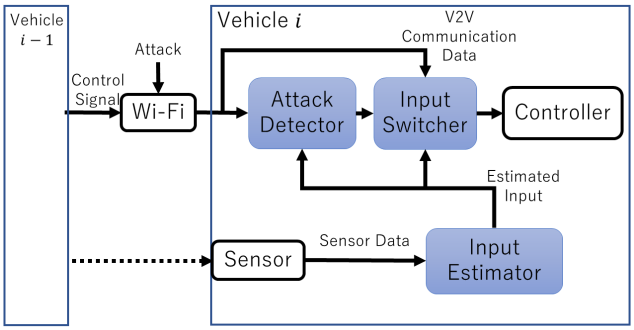


FIGURE 2. Architecture of the proposed mechanism.

In this paper, we propose an attack detection and defense mechanism using a UIO to improve the resilience of platoons with CACC against attacks on V2V communications. The architecture of the proposed mechanism is shown in Fig. 2. In this mechanism, each vehicle is equipped with a sensor (e.g., a radar unit or camera), a V2V communication device (a Wi-Fi device), an input estimator, an attack detector, an input switcher, and a controller. The input estimator estimates the control input of the preceding vehicle based on information obtained by the sensor. When V2V communications are attacked, the information obtained from the Wi-Fi device is not reliable, so the input estimator uses a UIO to estimate the state of the preceding vehicle by treating the unreliable information as unknown inputs. Based on the estimated input, the attack detector then decides whether the system is under attack. Accordingly, the input switcher selects and sends inputs to the controller in accordance with the attack detection results. When no attack is detected, the input switcher sends inputs calculated based on the information obtained through V2V communication. However, when an attack is detected, the input switcher sends inputs calculated based on state estimation. Note that in the proposed mechanism, the same controller is used regardless of whether an attack is detected, and it is only the inputs to this controller that are switched. This approach enables a simple control system design that contributes to reducing the management cost of the system. Moreover, such simplicity is important for vehicles with limited energy and computational power.

We also present simulation experiments conducted to elucidate the advantages and properties of the proposed mechanism. The simulations consider jamming and replay attacks on V2V communications, allowing the performance of the attack detection and defense mechanism under such attacks to be evaluated.

The contributions of this paper are as follows.

- To protect platoons from attacks on V2V communications, we propose an attack detection and defense mechanism using UIOs for platoons with CACC. The input estimator on each vehicle uses a UIO to estimate the state of the preceding vehicle without relying on unreliable communication data, which results in immediate and accurate attack detection.
- In the proposed attack defense mechanism, when an attack is detected, the input switcher sends inputs calculated based on the state estimation results of the input estimator, which protects the vehicle against the attack. Since only one controller is implemented regardless of whether an attack is detected, the control system is simple, and therefore, the management cost of the system is low.
- It is demonstrated through simulation experiments that the proposed mechanism can detect attacks with a 1-step delay and enhance the stability of the system, thereby reducing the loss in safety due to attacks. In the simulations, we consider jamming and replay attacks as typical attacks on V2V communications and show that the proposed mechanism is effective for both types of attacks.

The remainder of this paper is organized as follows. We review CACC in Section II. Section III then describes the proposed attack detection and defense mechanism. We evaluate the proposed mechanism on the basis of simulation experiments in Section IV. Finally, we conclude our study in Section V.

II. COOPERATIVE ADAPTIVE CRUISE CONTROL (CACC) SYSTEMS

Fig. 1 shows an overview of a cyberattack on V2V communications in a platoon with CACC. This paper uses the vehicle dynamics model proposed in [30].

Consider a platoon of M vehicles. The state of vehicle i is denoted by $x_i = \begin{bmatrix} q_i & v_i & a_i \end{bmatrix}^T$, where q_i, v_i, and a_i denote the absolute position, absolute velocity, and absolute acceleration, respectively, of vehicle i. Vehicle i is equipped with sensor i, V2V communication device i, and controller i. Under CACC, controller i first obtains the distance d_i of vehicle i from the preceding vehicle $i-1$ and the velocity v_{i-1} of the preceding vehicle $i-1$ from sensor i, and based on d_i, controller i then calculates the position q_{i-1} of the preceding vehicle. Furthermore, controller i obtains the input $\tilde{u}_{i-1}$ of the preceding vehicle $i-1$ through V2V communication. Controller i then calculates and sends the control input u_i to vehicle i. In this paper, we focus on attacks targeting V2V communications such as jamming and replay attacks.

In a platoon with CACC, there is a virtual vehicle called the *reference vehicle*, which has the role of leading the platoon. The state and control input of the reference vehicle are denoted by x_0 and u_r, respectively. The dynamics of the reference vehicle are described by (1).

$$\dot{x}_0(t) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\eta^{-1} \end{bmatrix} x_0(t) + \begin{bmatrix} 0 \\ 0 \\ \eta^{-1} \end{bmatrix} u_r(t). \quad (1)$$

x_0 and u_r can always be observed by vehicle 1 without V2V communication. In this paper, we assume that x_0 and u_r cannot be attacked, meaning that x_0 and u_r are reliable.

The dynamics of vehicle i ($1 \le i \le M$) are given by

$$\dot{x}_i(t) = A_c x_i(t) + B_c u_i(t), \quad (2)$$

where

$$A_c = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\eta^{-1} \end{bmatrix},$$

$$B_c = \begin{bmatrix} 0 \\ 0 \\ \eta^{-1} \end{bmatrix},$$

and u_i is the control input of vehicle i. Vehicle i calculates u_i using sensor data q_{i-1} and v_{i-1} combined with the control input $\tilde{u}_{i-1}(t)$ of vehicle $i-1$ as obtained through V2V communication. The output y_i of vehicle i is given by

$$y_i(t) = C x_i(t) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} x_i(t). \quad (3)$$

In CACC control, vehicle i receives control input from the preceding vehicle $i-1$ through V2V communication, and this control input is then provided as input to controller i. The control input received at time t is denoted by $\tilde{u}_{i-1}(t)$. In general, there is a transmission delay in V2V communication, denoted by θ, which leads to

$$\tilde{u}_{i-1}(t) = u_{i-1}(t-\theta). \quad (4)$$

The control input $u_i(t)$ is then calculated as

$$\dot{u}_i(t) = -\frac{1}{h}u_i(t) + \frac{1}{h}(k_p e_i(t) + k_d \dot{e}_i(t)) + \frac{1}{h}\tilde{u}_{i-1}(t), \quad (5)$$

where $e_i(t)$ is given by

$$\begin{aligned} e_i(t) &= d_i(t) - d_{r,i}(t) \\ &= (q_{i-1}(t) - q_i(t) - L) - (r + h v_i(t)). \end{aligned} \quad (6)$$

Here, L is the vehicle length, r is the ideal intervehicle distance when the vehicles are stopped, and k_p and k_d are design parameters. Note that when $i = 1$, $\tilde{u}_0(t) = u_r(t)$.

A block diagram of the closed-loop system for vehicle i is shown in Fig. 3, where

$$\begin{aligned} G(s) &= \frac{1}{s^2(\eta s + 1)}, \\ H(s) &= hs + 1, \\ K(s) &= k_p + k_d s, \\ D(s) &= e^{-\theta s}. \end{aligned}$$

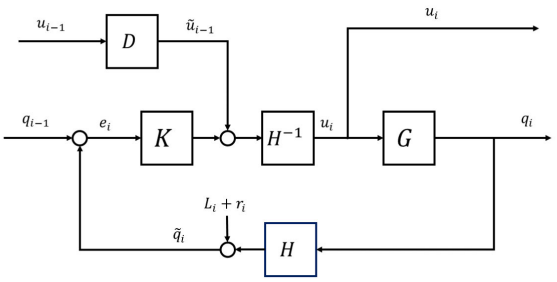


FIGURE 3. Block diagram of vehicle i.

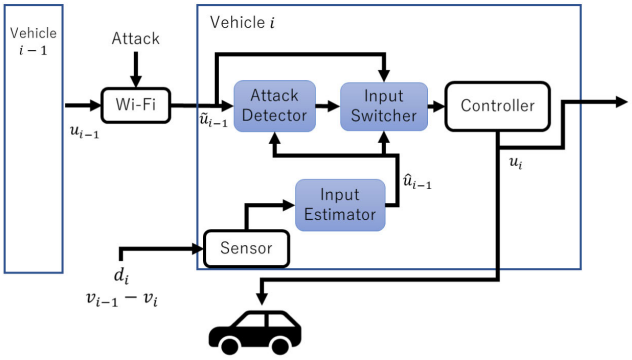


FIGURE 4. System architecture of the proposed mechanism.

String stability [9] is an important concept for the stability of CACC. In this paper, we consider *strong frequency-domain string stability (SFSS)*. A platoon exhibits SFSS if the transfer function $\Gamma_{i-1,i}$ between the outputs of vehicle i and its preceding vehicle $i-1$ satisfies

$$||\Gamma_{i-1,i}(s)||_{\mathcal{H}_\infty} \leq 1, \quad \forall i \in \{1, \ldots, M\}. \tag{7}$$

In this paper, we focus on the transfer function $\Gamma_{i-1,i}$ for velocity, as given in (8).

$$\begin{aligned}\Gamma_{i-1,i}(s) &= \frac{V_i(s)}{V_{i-1}(s)} = \frac{Q_i(s)}{Q_{i-1}(s)} \\ &= \frac{1}{H(s)} \frac{G(s)K(s) + D(s)}{1 + G(s)K(s)},\end{aligned} \tag{8}$$

where $V_i(s)$ and $Q_i(s)$ are the Laplace transforms of $v_i(t)$ and $q_i(t)$, respectively.

III. PROPOSED MECHANISM

For simplicity, the communication delay θ is set to 0 in this paper. In CACC platoons, the control inputs $\tilde{u}_i$ sent via V2V communication are not always reliable because $\tilde{u}_i$ can be tampered with by attackers. We therefore introduce a UIO into each vehicle to detect attacks and maintain vehicle stability. An overview of the proposed mechanism is shown in Fig. 4. In this mechanism, an *input estimator* first estimates the state of the preceding vehicle, and an *attack detector* then uses the estimated state to decide whether V2V communications are under attack. When an attack is detected, an *input switcher* switches the controller input to secure input.

To implement the attack detection and defense mechanism, we discretize the dynamics model described in Section II. The discrete-time model for vehicle i, which is the discretization of (2) and (3), is

$$\begin{cases} x_i[k+1] = A_d x_i[k] + B_d u_i[k], \\ y_i[k] = C_d x_i[k], \end{cases} \tag{9}$$

with

$$\begin{aligned} A_d &= e^{A_c T}, \\ B_d &= \int_0^T e^{A_c \tau} B_c d\tau, \\ C_d &= C, \end{aligned}$$

where T is the sampling period, and $u_i[k] = u_i(kT)$ (5) can also be rewritten as

$$\begin{aligned} u_i[k+1] = e^{-T/h} u_i[k] &+ \int_0^T e^{\tau/h} \frac{k_p}{h} d\tau e_{i,1}[k] \\ &+ \int_0^T e^{\tau/h} \frac{k_d}{h} d\tau e_{i,2}[k] + \int_0^T e^{\tau/h} \frac{1}{h} d\tau \tilde{u}_{i-1}[k], \end{aligned} \tag{10}$$

where $e_{i,1}[k]$ and $e_{i,2}[k]$ are given by

$$\begin{aligned} e_{i,1}[k] &= d_i[k] - d_{r,i}[k] \\ &= (q_{i-1}[k] - q_i[k] - L) - (r + hv_i[k]), \end{aligned} \tag{11}$$

$$e_{i,2}[k] = (v_{i-1}[k] - v_i[k]) - ha_i[k]. \tag{12}$$

In practice, the controller is implemented in discrete time as described in (10) because the position q_{i-1}, the velocity v_{i-1}, and the inputs $\tilde{u}_{i-1}$ are obtained in discrete time.

A. UNKNOWN INPUT OBSERVER (UIO)

We design a UIO i for each vehicle i.[1] UIO i estimates u_{i-1} by treating $\tilde{u}_{i-1}$ as an unknown input. The UIO is described as follows:

$$\begin{aligned} &\hat{x}_i[k+1] \\ &= (A_d - G_1 C_d A_d - G_2 C_d)\hat{x}_i[k] + (B_d (C_d B_d)^+ \\ &\quad + J[I_2 - C_d B_d (C_d B_d)^+])y_i[k+1] + G_2 y_i[k], \end{aligned} \tag{13}$$

where A_d, B_d, C_d, G_1, G_2, and J are design parameters. J affects the convergence speed of the state estimation process. Note that A^+ denotes the pseudoinverse of matrix A, i.e., $A^+ = [A^T A]^{-1} A^T$. Then, the estimated value $\tilde{u}_i$ of the control input is given by

$$\hat{u}_{i-1}[k] = B_d^+ (\hat{x}_{i-1}[k+1] - A\hat{x}_{i-1}[k]). \tag{14}$$

The model of the system must satisfy certain restrictions in terms of observability and detectability. If the system is observable, we can create a UIO with an arbitrary convergence rate. If the system is not observable but is detectable, the convergence rate cannot be set, but a UIO can be created

[1] In this paper, we assume that there are no actuator delays for simplicity. However, the proposed mechanism can be extended to platoons with actuator delays by suitably modifying (9) and (14).

such that the error converges to zero. Because this system is observable, the convergence rate can be adjusted by setting the pole configuration and J.

B. ATTACK DETECTION MECHANISM

We now propose a mechanism for detecting attacks using the UIO. In the attack detection mechanism, vehicle i detects attacks by comparing the estimated value $\hat{u}_i$ of the control input against the value $\tilde{u}_i$ obtained through V2V communication.

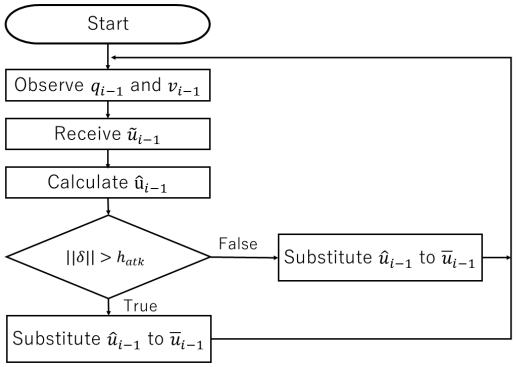


FIGURE 5. Flowchart of the attack detection and defense mechanism at vehicle i.

The process of attack detection at vehicle i is shown in Fig. 5. Vehicle i observes the distance d_i and the velocity difference $v_{i-1} - v_i$ between vehicles i and $i-1$ through its sensor. Vehicle i then uses these sensor data to calculate the position q_{i-1} and velocity v_{i-1} of vehicle $i-1$. The control input of vehicle $i-1$, denoted by $\tilde{u}_{i-1}$, is obtained through V2V communication. UIO i then calculates the estimated value $\hat{u}_{i-1}$ of the control input of vehicle $i-1$. Based on this estimated value, vehicle i detects whether an attack is occurring by comparing $\hat{u}_{i-1}$ against $\tilde{u}_{i-1}$.

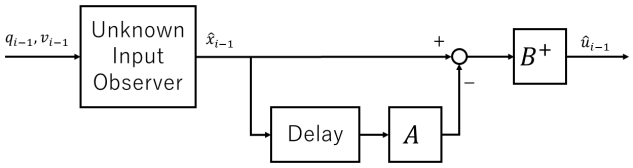


FIGURE 6. Block diagram of the estimation process for an unknown input u_{i-1}.

Fig. 6 presents a block diagram of the estimation process performed by UIO i. UIO i uses q_{i-1} and v_{i-1} to calculate the estimated state $\hat{x}_{i-1}$ of vehicle $i-1$. The difference between the estimation result and the value one step earlier multiplied by A is then calculated to obtain $B\hat{u}_{i-1}$, which is an estimate of the state change due to the input. By multiplying this by the pseudoinverse matrix B^+, we obtain an estimate of the input $\hat{u}_{i-1}$. In the proposed mechanism, not only the current estimated value but also previous estimated values are used to reduce the occurrence of false positives and false negatives in attack detection due to noise. In particular, we use the vectors $[\hat{u}_i[k], \cdots, \hat{u}_i[k-N+1]]^T$ and $\left[\tilde{u}_i[k], \cdots, \tilde{u}_i[k-N+1]\right]^T$. The detection result is expressed as

$$r_{detection,i}[k] = \begin{cases} 1, & \text{if } ||\delta[k]||_2 > h_{atk}, \\ 0, & \text{otherwise}, \end{cases} \tag{15}$$

where

$$\delta[k] = \begin{bmatrix} \Delta\hat{u}_{i-1}[k-1] \\ \vdots \\ \Delta\hat{u}_{i-1}[k-N] \end{bmatrix},$$
$$\Delta\hat{u}_{i-1}[k] = \hat{u}_{i-1}[k] - \tilde{u}_{i-1}[k], \tag{16}$$

N is the vector length, and h_{atk} is a threshold for attack detection. Note that $||\cdot||_2$ denotes the $\mathcal{L}_2$ norm of a vector. A detection result of 1 means that the attack detector decides that the input signal is under attack, and 0 means that the attack detector decides that the input signal is not under attack.

C. DEFENSE MECHANISM

We next propose a defense mechanism by which the stability of the system can be maintained even if the system is under attack. When an attack is detected by vehicle i, vehicle i switches to a secure mode. In the secure mode, vehicle i uses the estimated value $\hat{u}_{i-1}$ instead of $\tilde{u}_{i-1}$ when calculating the control input u_i according to (10). This allows vehicle i to mitigate the effects of attacks on V2V communications.

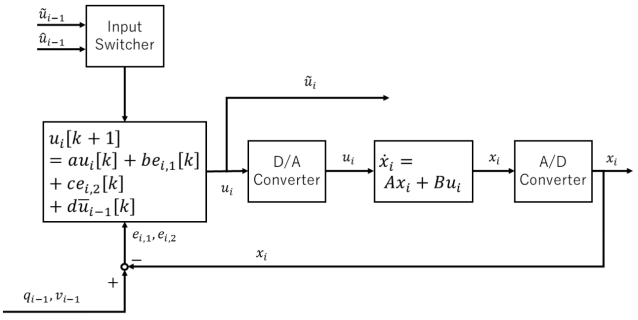


FIGURE 7. Defense process at vehicle i.

Fig. 7 shows a block diagram of the defense process at vehicle i. The *input switcher* receives $\tilde{u}_{i-1}$ and $\hat{u}_{i-1}$ and outputs

$$\bar{u}_{i-1}[k] = \begin{cases} \hat{u}_{i-1}[k-1], & \text{if } r_{detection,i}[k] = 1, \\ \tilde{u}_{i-1}[k], & \text{otherwise.} \end{cases} \tag{17}$$

If vehicle i decides that $\tilde{u}_{i-1}$ is not under attack (i.e., $\tilde{u}_{i-1}$ is reliable), then the input switcher outputs $\tilde{u}_{i-1}$ as $\bar{u}_{i-1}$. Otherwise, it outputs $\hat{u}_{i-1}$ as $\bar{u}_{i-1}$. Since the system uses $\hat{u}_{i-1}$ while $\tilde{u}_{i-1}$ is under attack, no compromised data are used, thus making the system resilient against attacks on V2V communications. A flowchart of the defense process at vehicle i is shown in Fig. 5.

Note that the estimation process conducted by the UIO causes a one-step delay. In step k, the UIO estimates the

control input in step $k-1$. Therefore, in the fallback mode, the input switcher outputs $\hat{u}_{i-1}[k-1]$ as $\bar{u}_{i-1}[k]$.

IV. SIMULATION AND DISCUSSION

We next report simulation experiments conducted to clarify the advantages and properties of the proposed mechanism. The simulations consider two typical V2V communication attack scenarios, namely, jamming and replay attacks. We first evaluate the proposed attack detection mechanism in Section IV-A and then evaluate the proposed attack defense mechanism in Section IV-B.

The simulations consider a platoon of 10 vehicles ($M = 10$). Each vehicle follows the preceding vehicle based on the CACC model described in Section II. Note that vehicle 1, that is, the lead vehicle, follows a virtual reference vehicle. We conducted simulation experiments using MATLAB 2018b [31], with a sampling period T of 0.01 s. We summarize the parameter settings of our simulations in Table 1. The parameters were determined experimentally.

TABLE 1. Parameter settings.

Parameter	Value
k_p	0.2
k_d	0.7
η	0.1
L	2.0
r	1.5
h	1.3
M	10

If there is no time delay, i.e., $\theta = 0$ in Eq. (8), then the Bode diagram of $\Gamma_{i-1,i}$ is as shown in Fig. 8. This figure shows that the platoon exhibits SFSS.

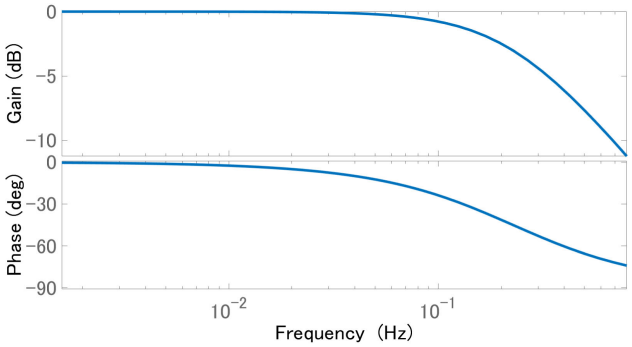


FIGURE 8. Bode diagram of $\Gamma_{i-1,i}$ without any delay.

The Bode diagram of $\Gamma_{i-1,i}$ with a 0.01 s delay, i.e., the one-step delay caused by switching the system from the normal operation mode to the defense mode, is shown in Fig. 9. As seen from this figure, even if there is a 0.01 s delay, the platoon still exhibits SFSS. This means that the proposed attack defense mechanism enhances the string stability of the platoon when the V2V communications of the platoon are attacked.

In our evaluation, the parameters of the discrete-time model for each vehicle were set as shown in the following equations.

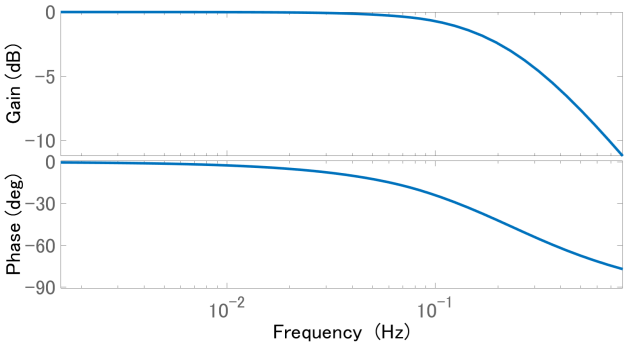


FIGURE 9. Bode diagram of $\Gamma_{i-1,i}$ with a 0.01 s delay.

$$A_d = \begin{bmatrix} 1 & 0.01 & 0 \\ 0 & 1 & 0.0095 \\ 0 & 0 & 0.9048 \end{bmatrix}, \tag{18}$$

$$B_d = \begin{bmatrix} 0 \\ 0.0005 \\ 0.0952 \end{bmatrix}. \tag{19}$$

The parameters of the UIOs were set as shown in the following equations.

$$J = \begin{bmatrix} 212500 & 212500 \end{bmatrix}, \tag{20}$$

$$G_1 = \begin{bmatrix} 2.1178 & -0.0071 \\ 2.1178 & -0.0071 \\ 2.1178 & -0.0052 \end{bmatrix} \times 10^5, \tag{21}$$

$$G_2 = \begin{bmatrix} -2.1178 & -0.0141 \\ -2.1179 & -0.0141 \\ -2.1179 & -0.0161 \end{bmatrix} \times 10^5. \tag{22}$$

The poles of the UIOs were set to 0.5, 0.2, and 0.1 based on these parameter matrices.

A. EVALUATION OF THE ATTACK DETECTION MECHANISM

We begin by evaluating the proposed attack detection mechanism. At the beginning of the simulation period, the 10 vehicles are stationary at 1.5 m intervals. In the first 0–100 s from the beginning of the simulation, the reference vehicle accelerates at 0.3 m/s^2. After 100 s, the reference vehicle continues moving at 30 m/s. The 10 vehicles follow their preceding vehicles based on the CACC model given in Section II. On this basis, we conducted simulation experiments of jamming and replay attack scenarios.

First, we evaluate the proposed attack detection mechanism in the case of a jamming attack. We consider attackers launching jamming attacks on the input signals $\tilde{u}_1$, $\tilde{u}_3$, and $\tilde{u}_7$ during the period of 90–150 s. When an input signal $\tilde{u}_i$ is attacked, noise appears in that input signal; that is, vehicle $i+1$ receives $u_i + s_{noise}$ instead of u_i. Here, s_{noise} is Gaussian noise that follows a standard normal distribution with mean 0 and variance 1.

To determine the detection threshold h_{atk} and the vector length N, we evaluated the detection performance, i.e., the

detection delay and accuracy, of the proposed mechanism while varying h_{atk} and N.

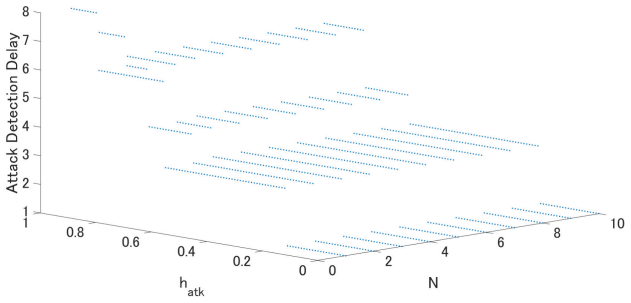


FIGURE 10. Attack detection delay versus h_{atk} and N.

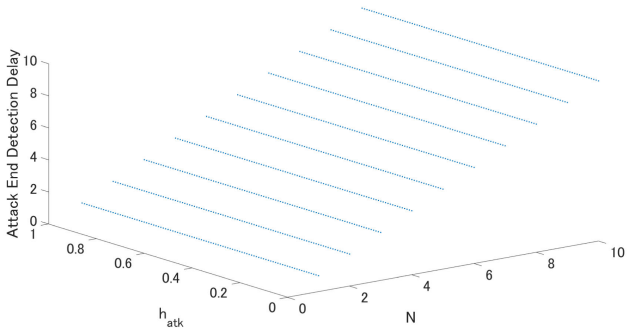


FIGURE 11. End-of-attack detection delay versus h_{atk} and N.

First, we focus on the detection delay of the proposed mechanism. Fig. 10 shows the delay in attack detection plotted versus h_{atk} and N. Regardless of the value of N, the detection delay is lower with a lower h_{atk}. In particular, when $h_{atk} \leq 0.2$, the detection delay is only 1 step. Fig. 11 shows the delay in detecting that an attack has stopped plotted versus h_{atk} and N. Regardless of the value of h_{atk}, the detection delay is lower with a lower N. As seen from these results, h_{atk} and N both need to be lower to decrease the delay in detecting that an attack has either started or stopped. However, when h_{atk} is too small, the attack detection results are vulnerable to disturbance and noise. Therefore, we set h_{atk} to 0.1.

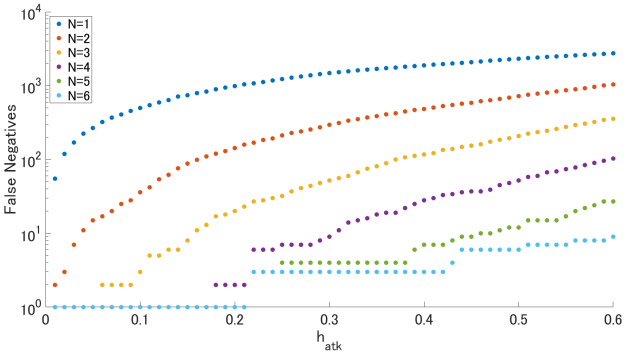


FIGURE 12. False negatives versus h_{atk} and N.

Second, we focus on the detection accuracy. Fig. 12 shows the number of false negatives plotted versus h_{atk} and N. When $h_{atk} = 0.1$, the number of false negatives is large when $N \leq 3$. As an example, the detection results with $h_{atk} = 0.1$ and $N = 1$ are shown in Fig. 13. As shown in this figure, when $N \leq 3$, attacks cannot always be detected. This is because when N is low, the proposed mechanism is vulnerable to temporal noise. When $N \geq 4$, the proposed detection mechanism detects attacks correctly. Thus, we set $h_{atk} = 0.1$ and $N = 4$ in the following evaluations.

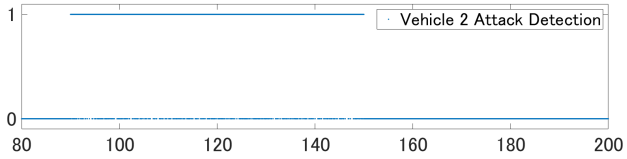


FIGURE 13. Attack detection results at vehicle 2 when $h_{atk} = 0.1$ and $N = 1$.

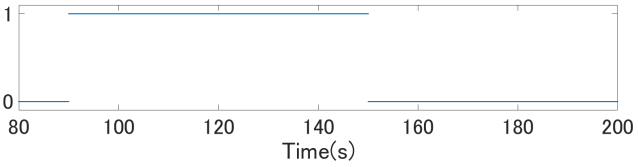


FIGURE 14. Attack detection results at vehicle 2.

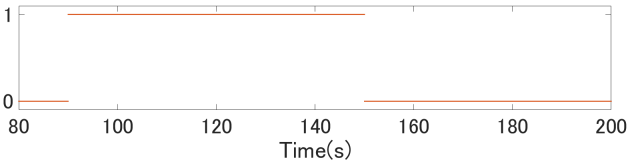


FIGURE 15. Attack detection results at vehicle 4.

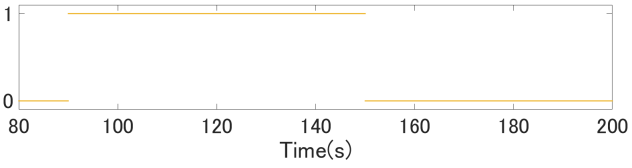


FIGURE 16. Attack detection results at vehicle 8.

The attack detection results at vehicles 2, 4, and 8 in the period of 80–200 s are shown in Figs. 14, 15, and 16, respectively. In these figures, a value of 1 means that the attack detector decides that the input signal is under attack, and 0 means that the attack detector decides that the input signal is not under attack, as defined in (15). The results show that attacks are detected immediately and accurately. Thus, the input estimator of each vehicle accurately estimates the state of the preceding vehicle even when information obtained through V2V communication is not reliable due to an attack. The attack detection time for each vehicle is only 1 step (i.e., 0.01 s). Moreover, when the attack ends, the attack detector in each vehicle decides that the input signal is no longer under attack within at most 0.04 s. This is because the proposed attack detection mechanism detects attacks based on the last 4 steps of information according

to (15). Therefore, the proposed attack detection mechanism can detect jamming attacks immediately and accurately by virtue of the introduction of a UIO.

Next, we evaluate the proposed attack detection mechanism in the case of a replay attack. The attackers execute a replay attack on the input signals $\tilde{u}_1$, $\tilde{u}_3$, and $\tilde{u}_7$ during the period of 110–170 s. The attack tampers with each attacked input signal $\tilde{u}_i$. More specifically, vehicle $i+1$ receives the input signal $u_i(t-90)$, which is the input signal from 90 s in the past, instead of $u_i(t)$ at time t. Thus, under this replay attack, vehicles 2, 4, and 8 receive input signals from 20–80 s during the period of 110–170 s. In the simulated scenario, the vehicles are intended to continue moving at a regular velocity during the period of 110–170 s, whereas the vehicles are accelerating in the period of 20–80 s. In other words, the attackers' purpose is to accelerate vehicles 2, 4, and 8 while the other vehicles continue to move at a constant velocity, which could lead to vehicle collisions.

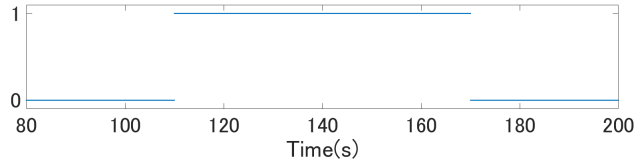


FIGURE 17. Attack detection results at vehicle 2.

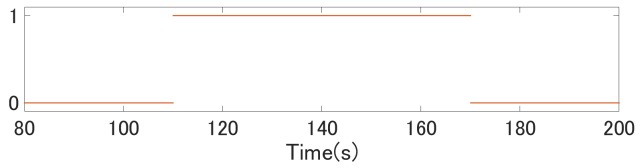


FIGURE 18. Attack detection results at vehicle 4.

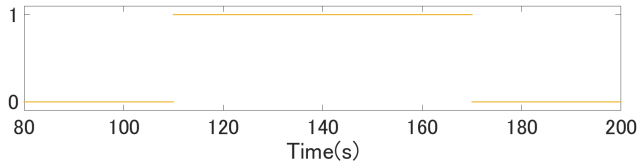


FIGURE 19. Attack detection results at vehicle 8.

The attack detection results at vehicles 2, 4, and 8 in the period of 80–200 s are shown in Figs. 17, 18, and 19, respectively. These results show that the attack is detected immediately and accurately. The attack detection time for each vehicle is only 1 step (i.e., 0.01 s). Moreover, when the attack ends, the attack detector of each vehicle decides that the input signal is no longer under attack within at most 0.04 s. The reason is that the attack and end-of-attack detection times are the same as for jamming attacks. Therefore, this evaluation shows the proposed attack detection mechanism can also detect replay attacks immediately and accurately by virtue of the introduction of the UIO.

B. EVALUATION OF THE ATTACK DEFENSE MECHANISM

We next evaluate the effectiveness of the proposed attack defense mechanism based on simulations of jamming and replay attack scenarios.

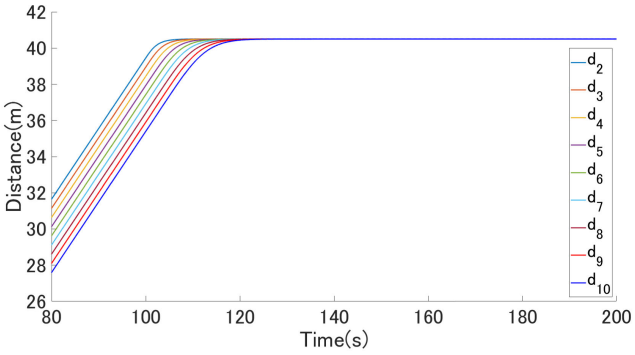


FIGURE 20. Intervehicle distances for all vehicles when not under attack.

First, we evaluate the proposed attack defense mechanism in the case of a jamming attack. The settings for the 10 vehicles are the same as in Section IV-A. The attackers conduct a jamming attack on the input signals $\tilde{u}_1$, $\tilde{u}_3$, and $\tilde{u}_7$ during the period of 90–150 s. When an input signal $\tilde{u}_i$ is attacked, noise appears in that input signal; that is, vehicle $i+1$ receives $u_i + s_{noise}$ instead of u_i. Here, s_{noise} is Gaussian noise following a standard normal distribution with mean 0 and variance 1.

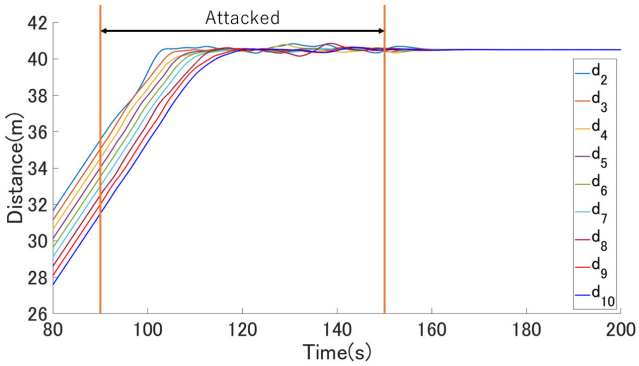


FIGURE 21. Intervehicle distances for all vehicles under a jamming attack without the proposed defense mechanism.

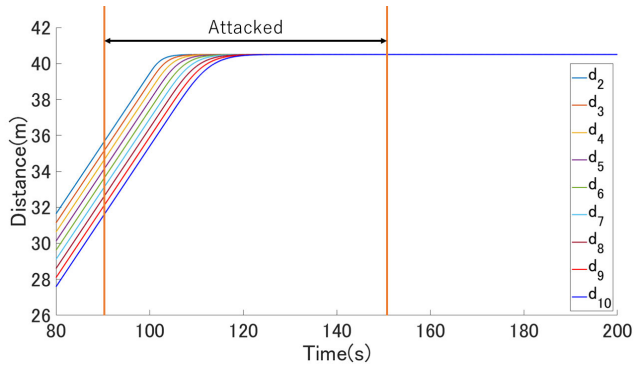


FIGURE 22. Intervehicle distances under a jamming attack with the proposed defense mechanism.

The intervehicle distances under this jamming attack without and with the proposed defense mechanism from 80 s

to 200 s are shown in Figs. 21 and 22, respectively. We also show the intervehicle distances when not under attack in Fig. 20 for comparison. As seen from Fig. 21, when the input signals are attacked (i.e., during the period of 90–150 s), the intervehicle distances are disturbed, which could lead to vehicle collisions. In contrast, in Fig. 22, the intervehicle distances are not disturbed and remain the same as in the case of no attack (Fig. 20) even when the input signals are attacked. The proposed mechanism immediately detects when the input signals are under attack and switches the inputs to the inputs calculated without using the attacked input signals. Even when the inputs are switched, the string stability of the platoon is enhanced, as shown in Fig. 9, and as a result, the intervehicle distance is not disturbed by the attack. Moreover, as shown in Section IV-A, the inputs are switched with a delay 0.01 s after the beginning of the attack. However, the impact of the attacked signals on the system is small enough that it affects only 1 step (i.e., 0.01 s). Moreover, the input delay caused by the input estimation process is 0.01 s, which is small enough that the platoon is controlled in almost the same way as in the normal mode. Thus, the proposed mechanism protects the platoon from jamming attacks.

Next, we evaluate the proposed attack defense mechanism in the case of a replay attack. The settings for the 10 vehicles are the same as in Section IV-A. The attackers conduct a replay attack on the input signals $\tilde{u}_1$, $\tilde{u}_3$, and $\tilde{u}_7$ during the period of 110–170 s. More specifically, vehicle $i+1$ receives the input signal $u_i(t-90)$, which is the input signal from 90 s in the past, instead of $u_i(t)$ at time t. In this scenario, the attackers intend to accelerate vehicles 2, 4, and 8 while the other vehicles continue to move at a constant velocity, which could lead to vehicle collisions.

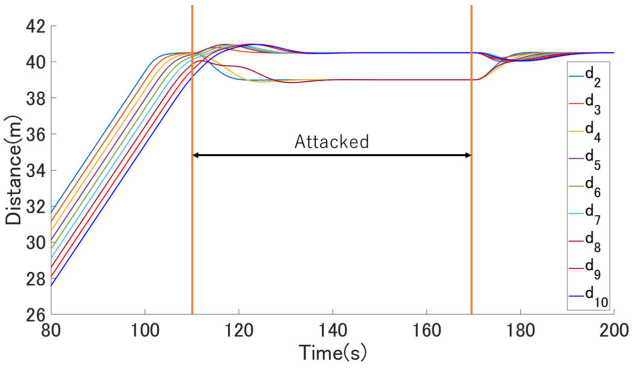


FIGURE 23. Intervehicle distances for all vehicles under a replay attack without the proposed defense mechanism.

The intervehicle distances under this replay attack without and with the proposed defense mechanism from 80 s to 200 s are shown in Figs. 23 and 24, respectively. Under the replay attack, the intervehicle distances are greatly disturbed without the defense mechanism, as shown in Fig. 23. However, Fig. 24 shows that even when the effect of the attack is large, the intervehicle distances are not disturbed under the proposed defense mechanism.

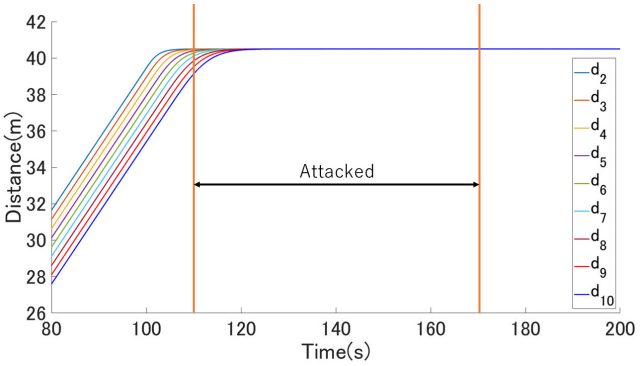


FIGURE 24. Intervehicle distances for all vehicles under a replay attack with the proposed defense mechanism.

To further investigate the effect of attacks, we conducted simulations of another situation, again considering the case of a replay attack. At the beginning of the simulation period, the velocities of the 10 vehicles are equal to 30 m/s, and the intervehicle distances are equal to 40.5 m. During the period of 50–150 s, the reference vehicle decelerates with an acceleration of -0.1 m/s^2. Accordingly, u_r is given by (23).

$$u_r(t) = \begin{cases} -0.1, & \text{if } 50 \le t \le 150, \\ 0, & \text{otherwise.} \end{cases} \tag{23}$$

The attackers conduct a replay attack on the input signals $\tilde{u}_1$, $\tilde{u}_3$, and $\tilde{u}_7$ during the period of $110 \le t \le 170$ s. The attacked signals are given by (24).

$$\tilde{u}_i(t) = \begin{cases} 0.4, & \text{if } 110 \le t \le 170,\ i \in \{1, 3, 7\}, \\ u_i(t), & \text{otherwise.} \end{cases} \tag{24}$$

This means that the attackers intend to accelerate vehicles 2, 4, and 8 while the other vehicles are decelerating, which is an extremely dangerous situation.

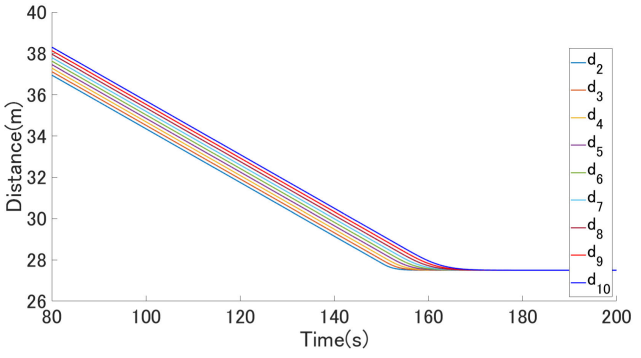


FIGURE 25. Intervehicle distances for the 10 vehicles when u_r follows (23).

The intervehicle distances under this replay attack without and with the proposed defense mechanism from 80 s to 200 s are shown in Figs. 26 and 27, respectively. We also show the intervehicle distances under no attack in Fig. 25 for comparison. Although the effect of the attack is extremely large, as shown in Fig. 26, the intervehicle distances are not disturbed when the proposed defense mechanism is used,

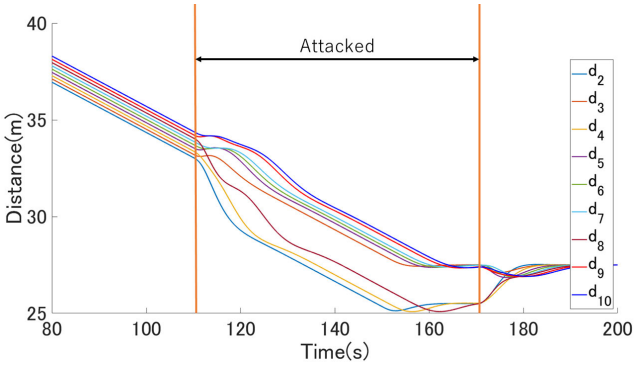


FIGURE 26. Intervehicle distances for the 10 vehicles without the proposed defense mechanism.

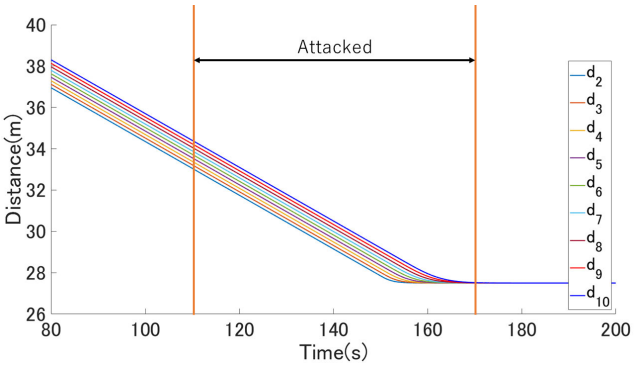


FIGURE 27. Intervehicle distances for the 10 vehicles with the proposed defense mechanism.

as shown in Fig. 27. Therefore, the proposed attack defense mechanism can protect the platoon from attacks even when the attack effect is large.

C. DISCUSSION

Many attack detection mechanisms have been proposed for CACC [17], [18]. However, these previous studies have only focused on single types of attacks or have not considered attack defense. The authors of [17] proposed a replay attack detection mechanism, and those of [18] proposed a real-time false injection attack detection mechanism. The authors of [19]–[21] focused on several kinds of attacks, but their proposals alone cannot defend vehicles from attacks. Our proposal can detect several kinds of attacks while also defending vehicles against attacks, making it advantageous compared to conventional mechanisms.

V. CONCLUSION

To improve the resilience of platoons using CACC against cyberattacks on V2V communications, we propose an attack detection and defense mechanism. By using a UIO, the state of the preceding vehicle can be estimated without using unreliable inputs obtained through V2V communication. Simulation experiments show that the proposed detection and defense mechanism can detect attacks with a 1-step delay and enhance the string stability of a platoon, reducing the loss in safety caused by attacks. It is a future work to analyze detection performances of the proposed mechanism theoretically.

In this paper, we assume that there are no failures in the on-board sensors and no delays in communication over the network and that the controller itself is operating normally based on the control signals. In future research, to more closely replicate real-world situations, it will be necessary to consider situations in which network delays occur at non-definite times and in which the controller itself is hijacked.

REFERENCES

[1] Z. Wang, G. Wu, and M. J. Barth, "A review on cooperative adaptive cruise control (CACC) systems: Architectures, controls, and applications," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 2884–2891.

[2] R. Rajamani, H.-S. Tan, B. K. Law, and W.-B. Zhang, "Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons," *IEEE Trans. Control Syst. Technol.*, vol. 8, no. 4, pp. 695–708, Jul. 2000.

[3] Y. Zhu, D. Zhao, and Z. Zhong, "Adaptive optimal control of heterogeneous CACC system with uncertain dynamics," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 4, pp. 1772–1779, Jul. 2019.

[4] C. Zhai, X. Chen, C. Yan, Y. Liu, and H. Li, "Ecological cooperative adaptive cruise control for a heterogeneous platoon of heavy-duty vehicles with time delays," *IEEE Access*, vol. 8, pp. 146208–146219, 2020.

[5] C. Zhai, F. Luo, Y. Liu, and Z. Chen, "Ecological cooperative look-ahead control for automated vehicles travelling on freeways with varying slopes," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1208–1221, Feb. 2019.

[6] C. Zhai, F. Luo, and Y. Liu, "Cooperative power split optimization for a group of intelligent electric vehicles travelling on a highway with varying slopes," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 29, Dec. 2021, doi: 10.1109/TITS.2020.3045264.

[7] C. Zhai, Y. Liu, and F. Luo, "A switched control strategy of heterogeneous vehicle platoon for multiple objectives with state constraints," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1883–1896, May 2019.

[8] P. Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems*. Cham, Switzerland: Springer, 2011.

[9] S. Feng, Y. Zhang, S. E. Li, Z. Cao, H. X. Liu, and L. Li, "String stability for vehicular platoon control: Definitions and analysis methods," *Annu. Rev. Control*, vol. 47, pp. 81–97, Mar. 2019.

[10] G. J. L. Naus, R. P. A. Vugts, J. Ploeg, M. J. G. van de Molengraft, and M. Steinbuch, "String-stable CACC design and experimental validation: A frequency-domain approach," *IEEE Trans. Veh. Technol.*, vol. 59, no. 9, pp. 4268–4279, Nov. 2010.

[11] S. Öncü, J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Network-aware analysis of string stability," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1527–1537, Aug. 2014.

[12] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[13] P. K. Singh, G. Saikamal Tabjul, M. Imran, S. K. Nandi, and S. Nandi, "Impact of security attacks on cooperative driving use case: CACC platooning," in *Proc. TENCON IEEE Region Conf.*, Oct. 2018, pp. 138–143.

[14] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commum. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[15] A. Alipour-Fanid, M. Dabaghchian, H. Zhang, and K. Zeng, "String stability analysis of cooperative adaptive cruise control under jamming attacks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, 2017, pp. 157–162.

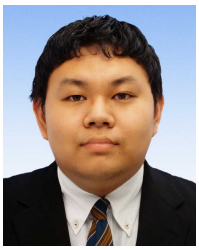
[16] A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Impact of jamming attacks on vehicular cooperative adaptive cruise control systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 12679–12693, Nov. 2020.

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

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

[19] F. Alotibi and M. Abdelhakim, "Anomaly detection in cooperative adaptive cruise control using physics laws and data fusion," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–7.

[20] F. Alotibi and M. Abdelhakim, "Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3468–3478, Jun. 2021.
[21] T. Keijzer and R. M. G. Ferrari, "A sliding mode observer approach for attack detection and estimation in autonomous vehicle platoons using event triggered communication," in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, Dec. 2019, pp. 5742–5747.
[22] G. Patounas, Y. Zhang, and S. Gjessing, "Evaluating defence schemes against jamming in vehicle platoon networks," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 2153–2158.
[23] T. Yang, C. Murguia, D. Nešić, and C. Lv, "A robust CACC scheme against cyberattacks via multiple vehicle-to-vehicle networks," 2021, *arXiv:2106.10448*.
[24] R. Merco, F. Ferrante, and P. Pisu, "A hybrid controller for DOS-resilient string-stable vehicle platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1697–1707, Mar. 2021.
[25] T. Sasaki, K. Sawada, S. Shin, and S. Hosokawa, "Fallback and recovery control system of industrial control system for cybersecurity," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 15247–15252, Jul. 2017.
[26] J. Chen and R. Patton, *Robust Model-Based Fault Diagnosis for Dynamic Systems*, 1999th ed. Dordrecht, The Netherlands: Springer, 1998.
[27] M. Witczak, *Fault Diagnosis and Fault-Tolerant Control Strategies for Non-Linear Systems: Analytical and Soft Computing Approaches*. Cham, Switzerland: Springer, 2016.
[28] H. Varmaziari and M. Dehghani, "Cyber-attack detection system of large-scale power systems using decentralized unknown input observer," in *Proc. Iranian Conf. Electr. Eng. (ICEE)*, May 2017, pp. 621–626.
[29] T. Yang, C. Murguia, M. Kuijper, and D. Nesic, "An unknown input multiobserver approach for estimation and control under adversarial attacks," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 475–486, Mar. 2021.
[30] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful degradation of CACC performance subject to unreliable wireless communication," in *Proc. IEEE 16th Int. Annu. Conf. Intell. Transp. Syst.*, Oct. 2013, pp. 1210–1216.
[31] MathWorks. *Matlab*. Accessed: Jul. 12, 2021. [Online]. Available: https://jp.mathworks.com/products/matlab.html?s_tid=hp_ff_p_matlab
[32] W. Chen and M. Saif, "Fault detection and isolation based on novel unknown input observer design," in *Proc. Amer. Control Conf.*, Jun. 2006, pp. 5129–5134.
[33] B. van Arem, C. J. G. van Driel, and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow characteristics," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 4, pp. 429–436, Dec. 2006.
[34] L. Xiao and F. Gao, "Practical string stability of platoon of adaptive cruise control vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1184–1194, Dec. 2011.
[35] K. Kalsi, S. Hui, and S. H. Zak, "Unknown input and sensor fault estimation using sliding-mode observers," in *Proc. Amer. Control Conf.*, Jun. 2011, pp. 1364–1369.
[36] I. H. Zohdy and H. Rakha, "Game theory algorithm for intersection-based cooperative adaptive cruise control (CACC) systems," in *Proc. 15th Int. IEEE Conf. Intell. Transp. Syst.*, Sep. 2012, pp. 1097–1102.
[37] J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Lp string stability of cascaded systems: Application to vehicle platooning," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 2, pp. 786–793, Mar. 2014.
[38] Z. Gao, X. Liu, and Z. Q. Chen, "Unknown input observer-based robust fault estimation for systems corrupted by partially decoupled disturbances," *IEEE Trans. Ind. Electron.*, vol. 63, no. 4, pp. 2537–2547, Apr. 2016.
[39] Z. Wang, G. Wu, P. Hao, K. Boriboonsomsin, and M. Barth, "Developing a platoon-wide Eco-cooperative adaptive cruise control (CACC) system," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1256–1261.
[40] E. Mousavinejad, F. Yang, Q. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2020.
[41] B. Tian, X. Deng, Z. Xu, Y. Zhang, and X. Zhao, "Modeling and numerical analysis on communication delay boundary for CACC string stability," *IEEE Access*, vol. 7, pp. 168870–168884, 2019.
[42] S.-Y. Han, J. Zhou, L. Wang, Y.-H. Chen, and N.-X. Cui, "Output-based centralized longitudinal CACC systems with wireless communication delay and actuator delay," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 2690–2695.
[43] Y. Qin and S. Li, "String stability analysis of mixed CACC vehicular flow with vehicle-to-vehicle communication," *IEEE Access*, vol. 8, pp. 174132–174141, 2020.
[44] R. G. Dutta, Y. Hu, F. Yu, T. Zhang, and Y. Jin, "Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 17, 2020, doi: 10.1109/TITS.2020.3036376.
[45] B. Alenezi, M. Zhang, S. Hui, and S. H. Zak, "Simultaneous estimation of the state, unknown input, and output disturbance in discrete-time linear systems," *IEEE Trans. Autom. Control*, early access, Feb. 24, 2021, doi: 10.1109/TAC.2021.3061993.
[46] L. Cui, J. Hu, B. B. Park, and P. Bujanovic, "Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: Assessing cooperative adaptive cruise control under cyber attack," *Transp. Res. C, Emerg. Technol.*, vol. 97, pp. 1–22, Dec. 2018.
[47] X. He, E. Hashemi, and K. H. Johansson, "Secure platooning of autonomous vehicles under attacked GPS data," 2020, *arXiv:2003.12975*.
[48] R. Rajamani and S. E. Shladover, "An experimental comparative study of autonomous and co-operative vehicle-follower control systems," *Transp. Res. C, Emerg. Technol.*, vol. 9, no. 1, pp. 15–31, 2001.



YUDAI YAMAMOTO is currently pursuing the bachelor's degree with Osaka University, Japan. His research interests include cybersecurity and control theory.

NAOMI KUZE (Member, IEEE) received the M.E. and Ph.D. degrees in information science and technology from Osaka University, in 2013 and 2016, respectively. In May 2018, she joined with the Graduate School of Engineering Science, Osaka University, as an Assistant Professor. Her research interests include self-organizing networks and security in cyber-physical systems.

TOSHIMITSU USHIO (Member, IEEE) received the B.S., M.S., and Ph.D. degrees from Kobe University, Japan, in 1980, 1982, and 1985. He was a Research Assistant at the UC Berkeley, in 1985. From 1986 to 1990, he was a Research Associate at Kobe University. He joined with Osaka University, in 1994, where he is currently a Professor. His research interests include control of discrete event and hybrid systems and analysis of nonlinear systems.