Anomaly Detection and String Stability Analysis in Connected Automated Vehicular Platoons

Yiyang Wang[a], Ruixuan Zhang[b], Neda Masoud[a,*] , Henry X. Liu[a]

[a] *Department of Civil and Environmental Engineering, University of Michigan, Ann Arbor, MI 48109*

[b] *Department of Civil and Urban Engineering, New York University, New York, NY 11201*

Abstract: In this study, we develop a comprehensive framework to model the impact of cyberattacks on safety, security, and head-to-tail stability of connected and automated vehicular platoons. First, we propose a general platoon dynamics model with heterogeneous time delays that may originate from the communication channel and/or vehicle onboard sensors. Based on the proposed dynamics model, we develop an augmented state extended Kalman filter (ASEKF) to smooth the sensor reading, and use it in conjunction with an anomaly detector to detect sensor anomalies. Specifically, we consider two detectors: a parametric detector, the χ^2-detector, and a learning-based detector, the one class support vector machine (OCSVM). We investigate the detection power of all combinations of vehicle dynamics models (EKF and ASEKF) and detectors (χ^2 and OCSVM). Furthermore, we introduce a novel concept in string stability, namely, pseudo string stability, to measure a platoon's string stability under cyberattacks and model uncertainties. We demonstrate the relationship between the pseudo string stability of a platoon and its detection rate, which enables us to identify the critical detection sensitivity/recall that the platoon's members should meet for the platoon to remain pseudo string stable.

Anomaly detection, connected and automated vehicles, cybersecurity, Kalman filter, platoon, stability, time delay, vehicle dynamics model

1. Introduction

In the past few years, with the continuous advancement in perception technologies and the maturity of communications technologies, autonomous driving features and connectivity are gradually appearing in more and more vehicles. A connected and automated vehicle (CAV), which combines automated and connected vehicle technologies, is envisioned to improve the mobility, safety, comfort, and environmental sustainability of the transportation sector (Masoud and Jayakrishnan 2017; Wyk, Khojandi, and Masoud 2019; Abdolmaleki, Masoud, and Yin 2019; Abdolmaleki et al. 2021).

Although CAVs offer promising benefits, they are prone to various security and privacy risks. In particular, the security risk escalates with increasing levels of connectivity and automation as CAVs expose more attack surfaces to malicious hackers. CAVs leverage cameras and Light Detection and Ranging (LiDAR) sensors to construct a high resolution 3D map of their surrounding environment to facilitate safe automated driving. Meanwhile, the connectivity between the CAVs and smart infrastructures also necessitates various types of sensors to communicate state information and situational awareness. Hence, anomalous information due to either malicious cyberattacks or faulty vehicle sensors can pose safety risks to road users, and possibly cause fatal crashes. For example, recently

* Corresponding author
Email addresses: yiyangw@umich.edu (Yiyang Wang), ruixuan.zhang@nyu.edu (Ruixuan Zhang), nmasoud@umich.edu (Neda Masoud), henryliu@umich.edu (Henry X. Liu)

there have been demonstrated cyberattacks on vehicle sensors in (Cao, Xiao, Cyr, et al. 2019; Cao, Xiao, Yang, et al. 2019), where the authors use optimization-based approaches to fool the LiDAR sensors aboard vehicles.

Moreover, as vehicles and infrastructures become more interconnected, a malicious attack on a single individual node (e.g., vehicle, traffic control device, etc.) can easily propagate throughout the system and affect other components. For instance, (Y. Feng et al. 2018) conducted falsified data injection attacks to actuated and adaptive signal control systems and showed using simulations that such attacks can effectively increase total system delay. Hence, cybersecurity solutions, especially for sensor security, have become increasingly more necessary in recent years in order to ensure the reliability and safety of the transportation system.

In order to ensure that a CAV can safely and effectively navigate the network, it needs access to robust and accurate data streams. As a result, any anomalous sensor data, if undetected, can greatly imperil the decision making process of CAVs. Either a malicious cyberattack or a sensor fault can result in an anomaly in CAV sensors. Moreover, with the presence of measurement noise, it is crucial to detect any anomalous sensor readings in real-time and accurately estimate the true state of the CAV meanwhile to ensure the safety of the CAV driving.

Anomalous sensor readings can be caused by a variety of reasons and manifest in different ways. In this paper, we adopt the taxonomy of sensor failure/attack provided by (Van Wyk et al. 2019; Y. Wang, Masoud, and Khojandi 2020b, 2020a; Watts et al. 2021) includes 'bias', 'gradual drift', 'noise', 'short', and 'miss'. Specifically, 'bias' and 'gradual drift' impose a constant offset and a gradual drift from the actual sensor readings, respectively. The anomaly type 'noise' represents a duration of change of variance in the observed readings. The anomaly type 'short' refers to a abrupt and short-lived change, and 'miss' is a short- or long-term missed observation in the sensor readings. The 'miss' anomaly type can be viewed as a special case of either 'short' or 'bias' anomaly types, depending on its duration, with the sensor reading being zero.

Meanwhile, connectivity enables a CAV to receive information from its surrounding vehicles and infrastructures. However, wireless communications and some forms of cyberattacks (e.g., the jamming attack) can introduce time delays to the receiver, which can significantly impact the state estimation accuracy and traffic stability, causing delay and chaos, and even leading to fatal crashes. Therefore, it is imperative to take time delay into consideration during state estimation and anomaly detection processes, and investigate the potential impacts of cyberattacks on traffic stability.

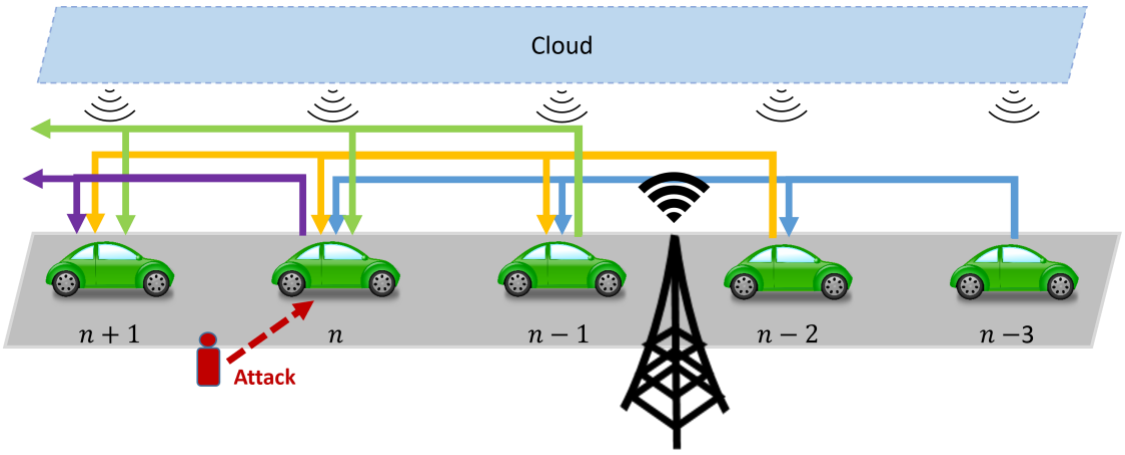


Figure 1: An example of platoon with 3-predecessor following information flow topology and with cloud information.

Figure 1 shows an illustrative scenario for this study of platoon with 3-predecessor following information flow topology. Other topologies discussed in (S. Feng et al. 2019) such as predecessor following, predecessor leader following, etc. can also be addressed in our framework. A malicious attacker can conduct cyberattacks to one or multiple vehicles in the platoon by manipulating the sensor reading of the compromised vehicle. We assume each vehicle is equipped with an anomaly detector and is capable of recovering the true sensor reading from the cloud once it successfully detects an abnormal sensor reading. The information from the cloud used for the recovery of anomalous sensor readings can be obtained from a road side unit (RSU), when possible, which monitors the vehicle trajectory and is assumed to be free from attacks.

In this study, we develop a holistic detection framework to improve the safety and security of CAV systems. Our framework combines sensor signal filtering and observer-based anomaly detection methods. Specifically, we consider anomaly detection in a platoon, where the ego vehicle can receive information from multiple sources, including other platoon members. We develop a general platooning framework for modeling a CAV's longitudinal dynamics under different types of cyberattacks. We use an augmented state extended Kalman filter (ASEKF) to estimate vehicle states from observed sensor readings of a CAV based on a nonlinear platooning model. In using the platooning model, the ego vehicle (i.e., the following CAV) leverages information from its leading vehicles to detect sensor anomalies by utilizing a set of offline-trained One Class Support Vector Machine (OCSVM) models. Stochastic and heterogeneous communication time delay factors are considered in the platoon dynamics to make it more congruent with real-world applications. Furthermore, we propose a novel definition of string stability, namely pseudo string stability, which represents the degree of string stability under model uncertainty. We establish the relationship between cyberattack detection rate and pseudo string stability, and identify the critical detection rate for maintaining pseudo string stability.

The contributions of this study can be summarized as threefold:

1. We extend the longitudinal platoon dynamics from Wang et al. (P. Wang, Wu, and He 2020), by considering a more realistic setting that accounts for heterogeneous time delay instead of a homogeneous time delay in previous literature. With heterogeneous time delay, we assume that the onboard sensor readings, i.e., the state vector, and the communication channel, i.e., the input vector, may experience different time delays. More specifically, we propose a modelling framework that supports a comprehensive analysis of CAV platoon performance under cyberattacks, including the false injection attack, the jamming attack, etc. We further consider the stochastic time delay setting and investigate its impact.

2. We convert the platoon dynamics into a state-space model, and apply an ASEKF combined with a detector to smooth the sensor measurement as well as to detect sensor anomalies. For the detector side, we consider both the χ^2-detector and OCSVM. An augmented state formulation is considered in order to compensate for the bias in the state-transition model, which can be caused by stochastic time delay or model inaccuracy. We show using numerical experiments that OCSVM outperforms the χ^2-detector both with and without the augmented state formulation. As we demonstrate in the experiments, however, OCSVM does not necessarily benefit from the augmented state formulation. Experiments also demonstrate that we obtain a significant improvement in detection performance by combining the ASEKF model with a χ^2-detector compared with χ^2-detector without augmented state formulation.

3. One of main advantages of forming platoons is their capability to maintain string stability. Therefore, we conduct a comprehensive stability analysis of platoons under various types of cyberattacks. We define the concept of pseudo string stability to capture the degree of string stability in expectation given an imperfect fault detector. To the best of our knowledge, this is the first string stability analysis of platoons under cyberattacks and model uncertainty. We demonstrate the relationship between the detection sensitivity of the detector and the platoon pseudo string stability, and identify the critical detection sensitivity for maintaining a pseudo stable string.

The remaining of this paper is organized as follows: In section 2, we review the literature on platooning technology and its cybersecurity concerns. In section 3, we provide the details of ASEKF and detection models, and conduct stability analysis of the platoon with and without attacks. In section 4, we perform extensive numerical experiments. Lastly, we conclude the paper in section 5.

2. Literature Review

CAVs can provide safety, mobility, and sustainability benefits by enabling the formation of platoon. Platoons can increase road capacity, improve traffic stability, and curb fuel consumption (Van Arem, Van Driel, and Visser 2006; Ploeg et al. 2011; Liu et al. 2020, 2022). A CAV platoon is enabled by using V2V and/or V2I technologies. It has been demonstrated that the destabilization effect of communication delay is suppressed by the

stabilization effect of multi-anticipations (i.e. more cooperative vehicles) of platoon (Ngoduy 2015). Platooning can also reduce fuel consumption, which is significantly influenced by air resistance, through shorter following gaps. It has been shown that tightly coupled platooning can improve fuel economy for both passenger cars (Liu et al. 2020; Shida and Nemoto 2009) and trucks (Alam 2011; Sun 2020). One application of platooning is cooperative adaptive cruise control (CACC). CACC extends the adaptive cruise control (ACC) by utilizing the V2V communication technology, which provides the ACC system with more and higher-quality information about its immediate following vehicle. With information of this type, the CACC controller will be able to better anticipate challenges ahead, and maneuver in a safer way while at the same time making the ride more comfortable for vehicle occupants. CACC systems with V2V communications enable a reduction in the mean following time gap/headway from about 1.4 seconds in manual driving to approximately 0.6 seconds (Nowakowski et al. 2010).

There has been a considerable amount of literature over the past few years on network-aware modeling of a platoons and improving the string stability of platoon-based vehicular systems. For instance, the effects of communication delays on string stability of a longitudinal dynamic model is addressed in (Zhang and Orosz 2016; Sykora et al. 2020). Longitudinal platoon control via communication channels with packet loss is studied in (Guo and Wen 2015; Molnár et al. 2015). In (Molnár et al. 2017), Molnár et al. further investigated the impact of network delay integrated with packet loss on the platoon stability. Although there has been a variety of literature considering network-induced phenomena in the vehicular platoon, there exits much fewer studies considering the detection of cyberattack and their impact on platoon stability. Since the platoon control model heavily relies on the external dynamical information, such as location, velocity, and headway, of other vehicles, when the vehicle communication network is under attack, transmitted messages will be contaminated or lost, rendering the platoon incapable of achieving the expected performance.

Previous literature have considered the impact of cyberattacks on vehicular platoons via simulation (Cui et al. 2018; Khattak, Smith, and Fontaine 2021), but they did not rigorously investigate the effect of cyberattacks on platoon stability. In (Ngoduy 2015), a car-following model was designed to receive the velocity and location of a fixed number of cooperative vehicles with constant information transmission time delays. Following this direction, in (P. Wang, Wu, and He 2020), Wang et al. extended the framework by incorporating a communication range to dynamically adjust the number of cooperative vesicles. In (Alipour-Fanid et al. 2017), Alipour-Fanid et al exemplified a CACC model where an UAV imposed jamming attacks on the wireless channel. Based on the CACC framework, other types of cyberattacks have been studied recently. In (Mousavinejad et al. 2019), Mousavinejad et al. considered the attacks on not only the inter-vehicle signals, but also the onboard sensor measurement outputs. (Biron, Dey, and Pisu 2018) focused on detecting the Denial of Service (DoS) attack using CACC model and estimating the effect on the CAV system if attacks occurred. While these studies provided valuable insights on vehicular platoon performance under cyberattacks, the traditional CACC model, which mostly only utilizes one leading vehicle's information for each ego vehicle, cannot fully leverage the Vehicle-to-Everything (V2X) capability, which is key in addressing future challenges in

dynamics control and fuel consumption reduction. Therefore, an advanced platoon vehicle dynamics model should be deployed.

To mitigate the risk of being attacked, both detection and recovery techniques are necessary to safeguard platoon operations. Little attention has been paid to cyberattack detection. (Mousavinejad et al. 2018) proposed a cyberattack detection algorithm that is capable of detecting attacks that violate both measurements and control command data in platoon-based vehicular systems. In (Biroon, Biron, and Pisu 2021), Biroon et al. developed a partial differential equation model for detection and isolation of cyberattacks. They considered a specific type of attack, which is modeled as a ghost vehicle being injected into the connected vehicles network to disrupt the performance of the entire system. In (Ju, Zhang, and Tan 2020), Ju et al. proposed a distributed Kalman filter with a modified generalized likelihood ratio algorithm to detect deception attacks. However, all of aforementioned studies only considered a specific platoon dynamic model and a rather specific attack model, which may limit the generalizability of their conclusions in practice. Moreover, none of them considered the time delay effect. This study aims to bridge this gap by proposing a general framework describing platoon dynamic, which considers the heterogeneous time delay effect as well as multiple types of sensor anomalies resulted from either sensor faults or cyberattacks.

3. System Modelling and Solution Methodology

In this section, we first propose a general model to describe the longitudinal dynamics of CAVs in a platoon. Then, we discuss how to reconfigure the platooning model to a state-space model, which includes a continuous state-transition model with heterogeneous time delays in an augmented state formulation, and a discrete measurement model. The continuous state-transition model represents the intrinsic nature of vehicle motion, and the discrete measurement model represents the discrete nature of sensor sampling. Based on the derived state-space model, we propose a filtering and anomaly detection method, which combines ASEKF with an anomaly detector. For the anomaly detector, we adopt a semi-supervised learning model, namely, OCSVM. We also introduce a χ^2-detector and later compare its performance with OCSVM in section 4. Finally, we conduct string stability analysis of the proposed platooning model under cyberattacks, and propose a novel definition of string stability under cyberattacks and model uncertainty.

3.1 Platooning Vehicle Dynamics with Heterogeneous Time Delay

We consider an extended version of the platoon dynamics model proposed by Wang et al. (P. Wang, Wu, and He 2020). Specifically, the CAV platoon dynamics in the absence of cyberattacks can be modeled as follows:

$$\dot{v}_n(t) = f\big(v_n(t-\tau_1), \alpha_{n1} w_{n1}(t-\tau_1) g_n(t-\tau_1) + \sum_{j=2}^{M} \alpha_{nj}\, w_{nj}(t-\tau_2) g_{n-j+1}(t-\tau_2), \\ \beta_{n1} w_{n1}(t-\tau_1) \Delta v_n(t-\tau_1) + \sum_{j=2}^{M} \beta_{nj}\, w_{nj}(t-\tau_2) \Delta v_{n-j+1}(t-\tau_2)\big) \tag{1}$$

where $v_n(t)$ represents the velocity of n-th vehicle; $x_n(t)$ is the location of the n-th vehicle; $g_n(t)$ represents the clearance gap between the n-th vehicle and $(n-1)$-th vehicle, which is defined as $g_n(t) := x_{n-1}(t) - x_n(t) - l_{n-1}$; l_{n-1} represents the length of $(n-1)$-th vehicle; $\Delta v_n(t)$ is the relative velocity between n-th vehicle and $(n-1)$-th vehicle defined as $\Delta v_n(t) := v_n(t) - v_{n-1}(t)$; α_{nj} and β_{nj} represent the weighting coefficients associated with the clearance gap and relative velocity between vehicle pair $n-j$ and $n-j+1$; M represents the number of cooperative leading vehicles; τ_1 and τ_2 represents the time delay of onboard measurement and communication channel, respectively; $w_{nj}(t)$ is the row-n-column-$(n-j+1)$ element of the adjacency matrix $\mathbf{W}(t)$, and $w_{nj}(t) = 1$ if vehicle n receives information from vehicle $n-j+1$ at time t and $w_{nj}(t) = 0$ otherwise. For example, considering a platoon of N vehicles indexed from 0 to $N-1$, when assuming each vehicle in the platoon only receives information from its leading/preceding vehicles, the adjacency matrix $\mathbf{W}(t)$ will be a lower triangular matrix and can be represented as:

$$\mathbf{W}(t) = \begin{bmatrix} 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ w_{11}(t) & 0 & \cdots & 0 & \cdots & 0 & 0 \\ w_{21}(t) & w_{22}(t) & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ w_{n1}(t) & w_{n2}(t) & \cdots & w_{nn}(t) & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ w_{(N-1)1}(t) & w_{(N-1)2}(t) & \cdots & w_{(N-1)j}(t) & \cdots & w_{(N-1)(N-1)}(t) & 0 \end{bmatrix} \tag{2}$$

By defining the n-th vehicle as the ego vehicle, the platooning model in equation (1) takes three inputs, namely, velocity of the ego vehicle, weighted average of clearance gaps, and weighted average of relative velocities between each pair of its cooperative vehicles. The platooning model determines the acceleration of the ego vehicle. Note that we consider two heterogeneous time delay factors, one for onboard measurements and one for the communication channel. To be specific, a time delay factor τ_1 incurs on all onboard measurements of the ego vehicle, including its velocity, the clearance gap and the relative velocity between the ego vehicle and its immediate leading vehicle. Meanwhile, another time delay factor τ_2 is imposed to the rest of the inputs of model (1), which are obtained via the communication channel. For a complete list of notations, see Table 1.

Table1: Table of notation

$f(\cdot)$	$\triangleq$	general platooning model
N	$\triangleq$	number of vehicles in platoon
$\mathbf{W}(t)$	$\triangleq$	adjacency matrix at time t
τ_1	$\triangleq$	time delay of onboard measurements
τ_2	$\triangleq$	time delay of the communication channel
l_n	$\triangleq$	length of vehicle n
$v_n(t)$	$\triangleq$	velocity of vehicle n in the platoon at time t
$x_n(t)$	$\triangleq$	position of vehicle n in the platoon at time t
$g_n(t)$	$\triangleq$	clearance gap between the preceding vehicle $n-1$ and vehicle n at time t
$\Delta v_n(t)$	$\triangleq$	relative velocity between vehicle n and its preceding vehicle $n-1$ at time t
α_{nj} /β_{nj}	$\triangleq$	weighting coefficients associated with the clearance gap/relative velocity from vehicle $n-j$ to vehicle $n-j+1$

3.2 State-Space Model

We define a state-space model which includes a continuous state-transition model and a discrete measurement model. Define the state vector $s_n(t)$ as the location and the velocity of the ego vehicle, i.e.,

$$s_n(t) = [x_n(t), v_n(t)]^\intercal \qquad (3)$$

where $\intercal$ represents transpose. Also define the input vector as $u_n(t;\tau_1,\tau_2)$, which associates with two time delay factors τ_1 and τ_2 and includes the clearance gap and the relative velocity,

$$u_n(t;\tau_1,\tau_2) = \begin{bmatrix} \alpha_{n1} w_{n1} g_n(t-\tau_1) + \sum_{j=2}^{M} \alpha_{nj}\, w_{nj}(t-\tau_2) g_{n-j+1}(t-\tau_2) \\ \beta_{n1} w_{n1}(t-\tau_1)\Delta v_n(t-\tau_1) + \sum_{j=2}^{M} \beta_{nj}\, w_{nj}(t-\tau_2)\Delta v_{n-j+1}(t-\tau_2) \end{bmatrix} \qquad (4)$$

The platoon dynamics (1) can be therefore recast into a state-transition model as follows,

$$\begin{aligned} \dot{s}_n(t) &= \begin{bmatrix} \dot{x}_n(t) \\ \dot{v}_n(t) \end{bmatrix} \\ &= \begin{bmatrix} e_2^\intercal s_n(t) \\ f\left(e_2^\intercal s_n(t-\tau_1), e_1^\intercal u_n(t|\tau_1,\tau_2), e_2^\intercal u_n(t|\tau_1,\tau_2)\right) \end{bmatrix} \end{aligned} \qquad (5)$$

where e_i represents a base vector with its i-th element being 1, and other elements set to 0.

When $\tau_1 = 0$, the state-transition model (5) satisfies the Markovian property, allowing for applying an extended Kalman filter (EKF). However, because of the time required for data processing and computations, in practice τ_1 can be non-zero. Similarly, communication delay may cause τ_2 to be non-zero. Under such circumstances, the Kalman filer cannot be directly applied to equation (5). Instead, we approximate the state-transition model by using an augmented state formulation. Specifically, assuming each vehicle has a bounded acceleration range, we can obtain a delay differential equation (DDE), describing the delayed state-transition model:

$$\begin{aligned}
\dot{s}_n(t) &= \begin{bmatrix} \dot{x}_n(t) \\ \dot{v}_n(t) \end{bmatrix} \\
&= \begin{bmatrix} e_2^{\intercal} s_n(t-\tau_1) + \int_{t-\tau_1}^{t} a_n(r)dr \\ f\left(e_2^{\intercal} s_n(t-\tau_1), e_1^{\intercal} u_n(t|\tau_1,\tau_2), e_2^{\intercal} u_n(t|\tau_1,\tau_2)\right) \end{bmatrix} \\
&= \begin{bmatrix} 1,0,1 \\ 0,1,0 \end{bmatrix} \times \begin{bmatrix} e_2^{\intercal} s_n(t-\tau_1) \\ f\left(e_2^{\intercal} s_n(t-\tau_1), e_1^{\intercal} u_n(t|\tau_1,\tau_2), e_2^{\intercal} u_n(t|\tau_1,\tau_2)\right) \\ \int_{t-\tau_1}^{t} a_n(r)dr \end{bmatrix} \\
&= \begin{bmatrix} 1,0,1 \\ 0,1,0 \end{bmatrix} \times \begin{bmatrix} e_2^{\intercal} \tilde{s}_n(t-\tau_1) \\ f\left(e_2^{\intercal} \tilde{s}_n(t-\tau_1), e_1^{\intercal} u_n(t|\tau_1,\tau_2), e_2^{\intercal} u_n(t|\tau_1,\tau_2)\right) \\ e_3^{\intercal} \tilde{s}_n(t-\tau_1) \end{bmatrix}
\end{aligned} \tag{6}$$

where we define the augmented state vector as

$$\tilde{s}_n(t) = [x_n(t), v_n(t), \delta_n(t)]^{\intercal} \tag{7}$$

with augmented state

$$\delta_n(t-\tau) = \begin{cases} \int_{t-\tau}^{t} a_n(r)dr & \text{if } \tau > 0 \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

The augmented state $\delta_n(t)$ is used to compensate potential bias caused by the time delay. Since $\delta_n(t)$ is unknown, we assume that at each time it is sampled from a random process with a small variance. Thus we have $\dot{\delta}_n(t) \approx 0$.

Then we can obtain the state-transition model with the augmented state vector $\tilde{s}_n(t)$ as follows:

$$\begin{aligned}\dot{\tilde{s}}_n(t) &= \begin{bmatrix}\dot{x}_n(t)\\ \dot{v}_n(t)\\ \dot{\delta}_n(t)\end{bmatrix}\\ &\approx \begin{bmatrix} e_2^{\mathrm{T}}\tilde{s}_n(t-\tau_1)\\ f\left(e_2^{\mathrm{T}}\tilde{s}_n(t-\tau_1), e_1^{\mathrm{T}}u_n(t;\tau_1,\tau_2), e_2^{\mathrm{T}}u_n(t;\tau_1,\tau_2)\right)\\ 0\end{bmatrix} + \theta(t)\\ &= \mathcal{T}\left(\tilde{s}_n(t-\tau_1), u_n(t;\tau_1,\tau_2)\right) + \theta(t)\end{aligned} \qquad (9)$$

where $\mathcal{T}(\cdot)$ is the state-transition model, and $\theta(t)$ is the process noise which accounts for the approximation error and model inaccuracy.

At each time epoch, the ego vehicle obtains its trajectory information from measurements by its onboard sensors. As such, using the new augmented state vector $\tilde{s}_n(t)$, we can obtain the state-space model with an augmented state vector as follows:

$$\begin{aligned}\dot{\tilde{s}}_n(t) &= \mathcal{T}\left(\tilde{s}_n(t-\tau_1), u_n(t;\tau_1,\tau_2)\right) + \theta(t)\\ z_n(t_k) &= \mathcal{M}\left(\tilde{s}_n(t_k)\right) + \eta(t_k),\ k \in \{0 \cup \mathbb{Z}^+\}\end{aligned} \qquad (10)$$

where $\mathcal{M}(\cdot)$ represents the measurement model, $z_n(\cdot)$ is sensor readings of the ego vehicle, $\eta(t_k)$ denotes the observation noise, which is assumed to be mutually independent from the process noise, $t_{k+1} = t_k + \Delta t,\ k \in \{0 \cup \mathbb{Z}^+\}$, and Δt is the sampling time interval for sensors.

3.3 Stochastic Time Delay of Input

We further consider a more general setting where the time delay factors τ_1 and τ_2 are not known constants, i.e., the input vector suffers from stochastic time delay. We assume the stochastic time delay obeys a linear model,

$$\begin{aligned}\tilde{\tau}_1 &= \tau_1 + \kappa_1\\ \tilde{\tau}_2 &= \tau_2 + \kappa_2\end{aligned} \qquad (11)$$

where κ_1 and κ_2 follow truncated normal distributions with mean 0 and variance σ_1^2 and σ_2^2, and within the intervals (a_1, b_1) and (a_2, b_2), respectively. That is, time delays $\tilde{\tau}_1$ and $\tilde{\tau}_2$ are within the range $(\tau_1 + a_1, \tau_1 + b_1)$ and $(\tau_2 + a_2, \tau_2 + b_2)$, respectively. The dynamics of the ego vehicle's most immediate leader can be simplified as a linear model,

$$\begin{cases}\dot{x}_{n-1}(t) = v_{n-1}(t)\\ \dot{v}_{n-1}(t) = a_{n-1}(t)\end{cases} \qquad (12)$$

where $a_{n-1}(t)$ is the acceleration of the $n-1$-th vehicle at time t. Then, we can obtain the following proposition:

Proposition 1. *Having stochastic time delays $\tilde{\tau}_1$ and $\tilde{\tau}_2$ is equivalent to adding noises into the input vector $u_n(t;\tau_1,\tau_2)$ with fixed time delays τ_1 and τ_2, i.e.,*

$$u_n(t;\tilde{\tau}_1,\tilde{\tau}_2) = u_n(t;\tau_1,\tau_2) + C(t) \qquad (13)$$

where $C(t)$ represents the noises caused by stochastic time delay.

Proof. Let us start by considering the communication delay, τ_2. For an arbitrary cooperative leader of the ego vehicle, i.e. $(n-j)$-th vehicle where $1 \le j \le M$, its clearance gap $g_{n-j}(t-\tilde{\tau}_2)$ is defined as $g_{n-j}(t-\tilde{\tau}_2) = x_{n-j-1}(t-\tilde{\tau}_2) - x_{n-j}(t-\tilde{\tau}_2) - l_{n-j-1}$. By integrating $\dot{x}_{n-j-1}(t-\tilde{\tau}_2)$, we have

$$\begin{aligned} x_{n-j-1}(t-\tilde{\tau}_2) &= \int_0^{t-\tilde{\tau}_2} v_{n-j-1}(\xi)d\xi \\ &= \int_0^{t-\tau_2-\kappa_2} v_{n-j-1}(\xi)d\xi \\ &= \int_0^{t-\tau_2} v_{n-j-1}(\xi)d\xi - \int_{t-\tau_2-\kappa_2}^{t-\tau_2} v_{n-j-1}(\xi)d\xi \\ &= x_{n-j-1}(t-\tau_2) + \epsilon_1(t-\tau_2;\kappa_2) \end{aligned} \tag{14}$$

where $\epsilon_1(t-\tau_2;\kappa_2) = -\int_{t-\tau_2-\kappa_2}^{t-\tau_2} v_{n-j-1}(\xi)d\xi$. Similarly, by integrating $x_{n-j}(t-\tilde{\tau}_2)$, we can obtain,

$$x_{n-j}(t-\tilde{\tau}_2) = x_{n-j}(t-\tau_2) + \epsilon_2(t-\tau_2;\kappa_2) \tag{15}$$

where $\epsilon_2(t-\tau_2;\kappa_2) = -\int_{t-\tau_2-\kappa_2}^{t-\tau_2} v_{n-j}(\xi)d\xi$.

Therefore, by combing (14) and (15), we obtain

$$\begin{aligned} g_{n-j}(t-\tilde{\tau}_2) &= x_{n-j-1}(t-\tau_2) - x_{n-j}(t-\tau_2) - l_{n-j-1} + \epsilon_1(t-\tau_2;\kappa_2) - \epsilon_2(t-\tau_2;\kappa_2) \\ &= g_{n-j}(t-\tau_2) + \epsilon_1(t-\tau_2;\kappa_2) - \epsilon_2(t-\tau_2;\kappa_2) \end{aligned} \tag{16}$$

Equation (16) shows that having stochastic time delay on the clearance gap is equivalent to adding a noise term $\epsilon_1(t-\tau_2;\kappa_2) - \epsilon_2(t-\tau_2;\kappa_2)$ into the clearance gap with a constant time delay. Note that we only consider the communication delay τ_2. However, similar results can be easily obtained for onboard measurement delay τ_1. Also note that the noise term is not necessarily zero mean with respect to κ_2, since it also depends on the vehicle velocity:

$$\begin{aligned} &\mathbb{E}_{\kappa_2}[\epsilon_1(t-\tau_2;\kappa_2) - \epsilon_2(t-\tau_2;\kappa_2)] = \mathbb{E}_{\kappa_2}[\epsilon_1(t-\tau_2;\kappa_2)] - \mathbb{E}_{\kappa_2}[\epsilon_2(t-\tau_2;\kappa_2)] \\ &= \int_{a_2}^{b_2} \tilde{\phi}(\iota;0,\sigma_2,a_2,b_2) \int_0^{-\iota} v_{n-j-1}(\xi+t-\tau_2)d\xi d\iota \\ &- \int_{a_2}^{b_2} \tilde{\phi}(\iota;0,\sigma_2,a_2,b_2) \int_0^{-\iota} v_{n-j}(\xi+t-\tau_2)d\xi d\iota \\ &= \int_{a_2}^{b_2} \tilde{\phi}(\iota;0,\sigma_2,a_2,b_2) \int_0^{-\iota} \Delta v_{n-j}(\xi+t-\tau_2)d\xi d\iota \end{aligned} \tag{17}$$

where $\tilde{\phi}(\iota;\mu,\sigma,a,b)$ represents the probability density function of truncated normal distribution,

$$\tilde{\phi}(\iota;\mu,\sigma,a,b)=\frac{1}{\sigma}\frac{\phi\left(\frac{\iota-\mu}{\sigma}\right)}{\Phi\left(\frac{b-\mu}{\sigma}\right)-\Phi\left(\frac{a-\mu}{\sigma}\right)} \qquad (18)$$

where $\phi(\cdot)$ and $\Phi(\cdot)$ are the probability density function and cumulative density function of the standard normal distribution, respectively.

Similarly, by integrating $v_{n-j-1}(t-\tilde{\tau}_2)$ and $v_{n-j}(t-\tilde{\tau}_2)$, we obtain

$$\begin{aligned} v_{n-j-1}(t-\tilde{\tau}_2) &= v_{n-j-1}(t-\tau_2)+\epsilon_3(t-\tau_2;\kappa_2) \\ v_{n-j}(t-\tilde{\tau}_2) &= v_{n-j}(t-\tau_2)+\epsilon_4(t-\tau_2;\kappa_2) \end{aligned} \qquad (19)$$

where $\epsilon_3(t-\tau_2;\kappa_2)=-\int_{t-\tau_2-\kappa_2}^{t-\tau_2} a_{n-j-1}(\xi)d\xi$ and $\epsilon_3(t-\tau_2;\kappa_2)=-\int_{t-\tau_2-\kappa_2}^{t-\tau_2} a_{n-j}(\xi)d\xi$. Then we have

$$\Delta v_{n-j}(t-\tilde{\tau}_2)=\Delta v_{n-j}(t-\tau_2)+\epsilon_3(t-\tau_2;\kappa_2)-\epsilon_4(t-\tau_2;\kappa_2) \qquad (20)$$

Therefore according to (16) and (20), having stochastic time delays is equivalent to adding noises into the input vector with the fixed time delays. □

When the time delays of the input vector are stochastic, according to Proposition 1, substituting equation (13) into (10) could induce a non-zero mean for the process noise $\theta(t)$, depending on the specific formulation of the platooning model. As mentioned in the next section, such a bias in $\theta(t)$ could negatively affect the performance of the classic χ^2-detector, whereas using ASEKF and OCSVM can mitigate this issue.

3.4 Augmented State Extended Kalman Filter with Anomaly Detector

Extended Kalman filter (EKF) is a well-known algorithm that takes a series of observed measurements and estimates the unknown state of a non-linear system in a timely and accurate manner (Ribeiro 2004). However, similar to other types of Kalman filter-based algorithms, it poses an assumption on both the process noise and the observation noise to be zero-mean Gaussian distributed. It has been shown that regardless of the Gaussian assumption, if the process covariance and measurement covariance are known, the Kalman filter is still the best possible linear estimator in the sense of minimum mean-squared-error (Humpherys, Redd, and West 2012). However, its performance can deteriorate significantly when there exits a background bias that is not incorporated in the model, as it violates the zero-mean assumption. In this study, in order to denoise CAV sensor measurements while compensating potential but unknown biases, we apply an augmented state extended Kalman filter (ASEKF) to the state-space model in (10) with three objectives: (i) to smooth the CAV sensor noise and estimate vehicle state in real time, (ii) to compensate potential but unknown bias caused by stochastic time delays or model inaccuracy, and (iii) to detect anomalous sensor readings by incorporating surrounding vehicles' information.

ASEKF includes two major stages to obtain the state estimation of $\tilde{s}_n(t_k)$ from the sensor input $z_n(t_k)$, namely, predict and update. Let $\hat{s}(k|k-1)$ and $P(t_k|t_{k-1})$ denote the state prediction and state covariance prediction at time t_k given the estimate at time t_{k-1}, respectively. Note that for ease of notation, we use state vector notation s instead of the

augmented state vector $\tilde{s}$, and we also omit subscript n for simplicity. Hence, given the state-space model in equation (10), the ASEKF consists of the following three steps:

Step 0 - Initialize state mean and covariance:

$$\begin{aligned} \hat{s}_{k|k-1} &= \mathbb{E}[s(t_0)] \\ P_{k|k-1} &= \mathrm{Var}[s(t_0)]. \end{aligned} \qquad (21)$$

Step 1 - Predict state and state covariance:

$$\begin{aligned} \text{Solve} \quad & \begin{cases} \dot{\hat{s}}(t) = \mathcal{T}\big(\hat{s}(t-\tau_1), u(t;\tau_1,\tau_2)\big), \\ \dot{P}(t) = F(t-\tau_1)P(t-\tau_1) + P(t-\tau_1)F(t-\tau_1)^{\intercal} + Q(t) \end{cases} \\ \text{with} \quad & \begin{cases} \hat{s}(t_{k-1}) = \hat{s}_{k-1|k-1} \\ P(t_{k-1}) = P_{k-1|k-1} \end{cases} \\ \Rightarrow \quad & \begin{cases} \hat{s}_{k|k-1} = \hat{s}(t_k) \\ P_{k|k-1} = P(t_k) \end{cases} \end{aligned} \qquad (22)$$

where $F(t-\tau_1) = \frac{\partial \mathcal{T}}{\partial s}|_{\hat{s}(t-\tau_1),u(t;\tau_1,\tau_2)}$ is the first-order approximation of the Jacobian matrix of state-transition model $\mathcal{T}(\cdot)$.

Step 2 - Update state and state covariance:

$$\begin{aligned} \nu_k &= z(t_k) - \mathcal{M}\big(\hat{s}_{k|k-1}\big) \\ S_k &= H(t_k)P_{k|k-1}H(t_k)^{\intercal} + R_k \\ K_k &= P_{k|k-1}H(t_k)^{\intercal}S_k^{-1} \\ \hat{s}_{k|k} &= \hat{s}_{k|k-1} + K_k\nu_k \\ P_{k|k} &= P_{k|k-1} - K_kH(t_k)P_{k|k-1} \end{aligned} \qquad (23)$$

where $H(t_k) = \frac{\partial \mathcal{M}}{\partial s}|_{\hat{s}_{k|k-1}}$, $Q(t)$ is the covariance matrix of the process noise at time t, $R_k = R(t_k)$ is the covariance matrix of the measurement noise at time t_k, and ν_k is innovation, which is the difference between the measurement and the prediction at time t_k.

One advantage of using ASEKF to estimate sensor data is that it can detect anomalies during the filtering procedure. One of the traditional anomaly detectors used in conjunction with Kalman filter is the χ^2-detector (Brumback and Srinath 1987; Bar-Shalom and Li 1995). Since ASEKF belongs to the family of Kalman filters, the χ^2-detector can be seamlessly applied. Specifically, it constructs a gate region by computing the χ^2 test statistics, and determines whether the new measurement falls into the gate region. The gate region is defined by the gate threshold γ, as shown in the following:

$$V_\gamma(k) = \{z: \quad \big(z - \hat{z}_{k|k-1}\big)^{\intercal} S_k^{-1} \big(z - \hat{z}_{k|k-1}\big) \leq \gamma\} \qquad (24)$$

where $\hat{z}_{k|k-1}$ is the predicted value of measurement at time t_k. The χ^2 test statistics for the anomaly detector is defined as

$$\chi^2(t_k) = \nu_k^{\intercal} S_k^{-1} \nu_k \qquad (25)$$

The χ^2-detector relies on the Gaussian assumption and zero-mean assumption of the ASEKF, as it essentially constructs a "spherical" decision boundary with the centroid of the origin point in the space of normalized innovation, which is defined as

$$\bar{v}(t_k) = S_k^{-\frac{1}{2}} \cdot v_k \qquad (26)$$

The normalized innovation instances falling outside this spherical decision boundary will be classified as anomalies. However, as we showed earlier in section 3.3, the process noise $\theta(t)$ may not be zero-mean under stochastic time delay, and the additive noise caused by the stochastic time delay does not follow a zero-mean Gaussian distribution. Moreover, the approximation step in (9) may also introduce such a bias. Therefore, we also consider a learning-based method, namely, one class Support Vector Machine (OCSVM), to actively learn the decision boundary in the normalized innovation space.

Consider L training data samples $\{\bar{v}(t_1), \ldots, \bar{v}(t_L)\}$ from a training set $\mathcal{L}$, which only contains normal data. Define a kernel mapping function $\mathcal{K}$ as $\mathcal{L} \to \mathcal{F}$, where $\mathcal{F}$ represents the feature space. OCSVM minimizes the following quadratic optimization problem:

$$\begin{aligned} &\min_{o \in \mathcal{F}, \boldsymbol{\psi} \in \mathbb{R}^L, \rho \in \mathbb{R}} \ \frac{1}{2} \| o \|^2 + \frac{1}{cL} \sum_j \psi_j - \rho \\ &\text{subject to} \ \ o \cdot \mathcal{K}\left(\bar{v}(t_j)\right) \geq \rho - \psi_j, \ \psi_j \leq 0 \end{aligned} \qquad (27)$$

where c is a constant parameter in the range of $(0,1)$. Decision variables o define a hyperplane and separate at least $1 - c$ percentage of the data points from the origin in the feature space $\mathcal{F}$ so as to maximize the distance from this hyperplane to the origin. This results in a region in the input space that encompasses at least $1 - c$ percentage of data points. Decision variables ψ_j are slack variables introduced to allow some data points violate the constraint $o \cdot \mathcal{K}\left(\bar{v}(t_j)\right) \geq \rho$.

Unlike the χ^2-detector which uses a decision boundary predefined by the threshold parameter γ, OCSVM learns the decision boundary from only non-anomalous training data, which can be collected easily without the need to enumerate all possible types of anomalies. It can also directly learn the potential bias from the training data, and is more robust. Furthermore, unlike the χ^2-detector, it does not impose distributional assumptions on the data.

3.5 String Stability Analysis

String stability reflects how platoons respond to imposed perturbations in longitudinal dynamics and stabilize back to the equilibrium state. String stability can be mathematically defined in both time-domain and frequency domain. String stability conditions are easy to verify, but hard to derive, in time-domain. Therefore, we conduct analysis in the frequency-domain. Note that in the presence of time delay, deploying power-series and the decay rate of perturbations to approximate the vehicle dynamics response and derive string stability conditions is not mathematically guaranteed for a non-linear dynamics model at high

angular frequency. To ensure the validity of the analysis, we pursue the transfer function approach instead. Obtaining inter-vehicle transfer functions under the standard definition of string stability is not trivial when their inputs and outputs are heavily correlated, i.e., one vehicle receiving information from multiple preceding vehicles as its control input. In this study, we adopt an extension of the standard string stability, namely, the head-to-tail string stability, originally proposed in (Jin and Orosz 2014) to address this problem:

Definition 1. *A platoon is called head-to-tail string stable if any perturbations that cause the first vehicle in the platoon (i.e., the platoon head) to deviate from its equilibrium state can be attenuated at the very last vehicle (i.e. the platoon tail).*

Head-to-tail string stability views a platoon of any size as a system with input (perturbation at the platoon head) and output (perturbation at the platoon tail). This input-output relationship between the platoon head and any vehicle following it can be established by truncating the platoon at the corresponding number of vehicles. This facilitates describing vehicle responses in complicated longitudinal dynamics, i.e., the vehicle takes outputs of multiple preceding vehicles, and its output serves as an input for other vehicles. Specifically, a transfer function that connects the input of the platoon head and the output of the platoon tail is called a head-to-tail transfer function, as described in (Jin and Orosz 2014). For a subject vehicle in the platoon, its correlated inputs can be neatly decoupled and represented in the form of head-to-tail transfer functions, using multiple transfer functions of any two vehicles between the platoon head and the subject vehicle itself. A detailed description will be provided later in this subsection. To better understand head-to-tail string stability and how it works with control dynamics, an example of vehicular communication topology is shown in Figure 2.

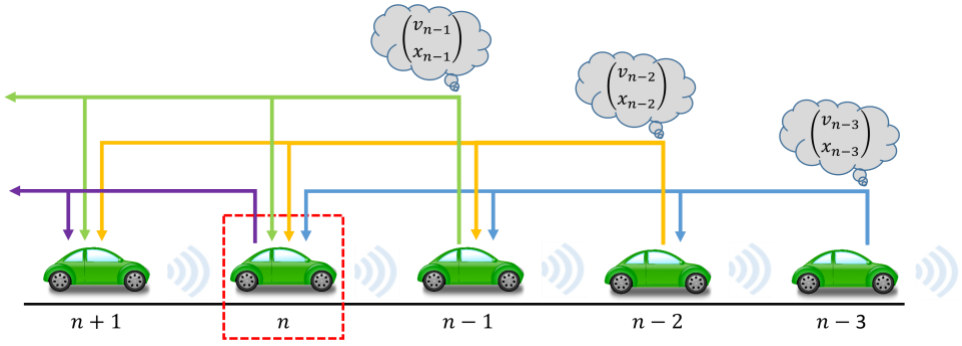


Figure 2: The topology in the above figure is called M-predecessor following (MPF), where here M=3 denotes the number of predecessors of vehicle n with communication capabilities. Vehicles n to $n-3$ are called a cooperative vehicle group. State information of position and velocity are transmitted via the vehicular network.

With the state space model defined earlier, the state of vehicle n at time t under flow equilibrium conditions is denoted as $s_n^*(t) = [x_n^*(t), v_n^*(t)]^\intercal$, where $x_n^*(t) = x_n(0) + t \cdot v_n^*(t)$ is the expected position of vehicle n at time t without perturbations. The actual position of vehicle n at time t is denoted as $x_n(t)$, and the vehicle length is l. One can easily obtain $g^* = x_{n-1}^*(t) - x_n^*(t) - l = x_{n-1}^*(0) - x_n^*(0) - l$, which is a constant determined by the initial condition of vehicle n. When perturbations are imposed at time t, the

relationship between the perceived position and velocity, the actual position and velocity, and perturbations can be formulated as follows:

$$\begin{aligned}\tilde{x}_n(t) &= x_n^*(t) - x_n(t)\\ \tilde{v}_n(t) &= v_n^*(t) - v_n(t)\end{aligned} \tag{28}$$

where $\tilde{x}_n(t)$ and $\tilde{v}_n(t)$ are the perturbations imposed on location and velocity, respectively. For vehicle n which utilizes information received from its cooperative leading vehicles, its longitudinal dynamics model can be linearized as follows:

$$\begin{aligned}\dot{\tilde{v}}_n(t) \quad &= f_n^v \tilde{v}_n(t-\tau_1) + f_n^g \left(\alpha_{n1} w_{n1}(t-\tau_1)\tilde{g}_n(t-\tau_1) + \sum_{j=2}^{M} \alpha_{nj}\, w_{nj}(t-\tau_2)\tilde{g}_{n-j+1}(t-\tau_2) \right)\\ &+ f_n^{\Delta v} \left(\beta_{n1} w_{n1}(t-\tau_1)\Delta\tilde{v}_n(t-\tau_1) + \sum_{j=2}^{M} \beta_{nj}\, w_{nj}(t-\tau_2)\Delta\tilde{v}_{n-j+1}(t-\tau_2) \right)\end{aligned} \tag{29}$$

where

$$f_n^v = \frac{\partial f}{\partial \tilde{v}_n}|_{s=s_n^*},\ f_n^g = \frac{\partial f}{\partial \tilde{g}_n}|_{s=s_n^*}, f_n^{\Delta v} = \frac{\partial f}{\partial \Delta\tilde{v}_n}|_{s=s_n^*} \tag{30}$$

The adjacency matrix **W** is omitted since the communication topology is fixed for M leading vehicles. We also denote α_{nj} and β_{nj} as α_j and β_j, respectively, for simplicity. The corresponding state space model can be formulated as:

$$\begin{aligned}\dot{\tilde{s}}_n(t) = \quad & \begin{bmatrix}\dot{\tilde{x}}_n(t)\\ \dot{\tilde{v}}_n(t)\end{bmatrix}\\ = \quad & \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} \cdot \begin{bmatrix}\tilde{x}_n(t)\\ \tilde{v}_n(t)\end{bmatrix} + \begin{bmatrix}0 & 0\\ -\alpha_1 f_n^g & f_n^v + \beta_1 f_n^{\Delta v}\end{bmatrix} \cdot \begin{bmatrix}\tilde{x}_n(t-\tau_1)\\ \tilde{v}_n(t-\tau_1)\end{bmatrix}\\ & + \sum_{j=1}^{M-1} \begin{bmatrix}0 & 0\\ (\alpha_j - \alpha_{j+1}) f_n^g & (\beta_{j+1} - \beta_j) f_n^{\Delta v}\end{bmatrix} \cdot \begin{bmatrix}\tilde{x}_{n-j}(t-\tau_2)\\ \tilde{v}_{n-j}(t-\tau_2)\end{bmatrix}\\ & + \begin{bmatrix}0 & 0\\ \alpha_M f_n^g & -\beta_M f_n^{\Delta v}\end{bmatrix} \cdot \begin{bmatrix}\tilde{x}_{n-M}(t-\tau_2)\\ \tilde{v}_{n-M}(t-\tau_2)\end{bmatrix}\\ y_n(t) = \quad & [0 \quad 1] \cdot \begin{bmatrix}\tilde{x}_n(t)\\ \tilde{v}_n(t)\end{bmatrix}\end{aligned} \tag{31}$$

After Laplace transformation of equation (31), the relationship between the output of vehicle n and its cooperative leading vehicles is shown as follows:

$$Y_n(s) = \begin{bmatrix}0 & 1\end{bmatrix} \cdot \left(sI - \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} - A_n^{\tau_1} \cdot e^{-s\tau_1}\right)^{-1} \cdot \left[\left(\sum_{j=1}^{M} B_{n-j}^{\tau_2} Y_{n-j}(s)\right) \cdot e^{-s\tau_2} \begin{bmatrix}1\\ \frac{1}{s}\\ 1\end{bmatrix}\right] \quad (32)$$

$$= \sum_{j=1}^{M} T_{n-j}(s) Y_{n-j}(s)$$

where

$$A_n^{\tau_1} = \begin{bmatrix}0 & 0\\ -\alpha_1 f_n^g & f_n^v + \beta_1 f_n^{\Delta v}\end{bmatrix}$$
$$B_{n-j}^{\tau_2} = \begin{bmatrix}0 & 0\\ (\alpha_j - \alpha_{j+1}) f_n^g & (\beta_{j+1} - \beta_j) f_n^{\Delta v}\end{bmatrix}, \ 1 \le j \le M-1 \quad (33)$$
$$B_{n-M}^{\tau_2} = \begin{bmatrix}0 & 0\\ \alpha_M f_n^g & -\beta_M f_n^{\Delta v}\end{bmatrix}$$

Here $T_{n-j}(s)$ represents the transfer function between vehicle $n-j$ and vehicle n. According to the definition, the head-to-tail transfer function is in the form of:

$$Y_n(s) = G_{n,0}(s) Y_0(s) \quad (34)$$

However, in this case, the head-to-tail transfer function is difficult to derive directly as the outputs of the leading vehicles are highly coupled within one vehicle group (vehicle n and its M cooperative leading vehicles). Inspired by the method proposed in (Zhang and Orosz 2016), we can derive the head-to-tail transfer function by iteration. By substituting equation (34) into equation (32), we can get:

$$G_{n,0}(s) = \sum_{j=1}^{M} T_{n-j}(s) G_{n-j,0}(s) \quad (35)$$

Rearrange the equation (35) to a transition model. It can be shown that:

$$\begin{bmatrix}G_{n,0}(s)\\ G_{n-1,0}(s)\\ G_{n-2,0}(s)\\ G_{n-3,0}(s)\\ \vdots\\ G_{n-M,0}(s)\end{bmatrix} = \begin{bmatrix}T_{n-1}(s) & T_{n-2}(s) & T_{n-3}(s) & \cdots & T_{n-M}(s) & 0\\ 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 1 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & 0\end{bmatrix} \cdot \begin{bmatrix}G_{n-1,0}(s)\\ G_{n-2,0}(s)\\ G_{n-3,0}(s)\\ G_{n-4,0}(s)\\ \vdots\\ G_{n-M-1,0}(s)\end{bmatrix} \quad (36)$$

From (36), for any two sequential vehicle groups, one with starting and ending vehicles $n-M$ and n, respectively, and the other with starting and ending vehicles $n-M-1$ and $n-1$, respectively, the relationship between the two groups of vehicles' head-to-tail transfer functions can be clearly established. Denote

$$\hat{P}_n(s) = \begin{bmatrix} T_{n-1}(s) & T_{n-2}(s) & T_{n-3}(s) & \cdots & T_{n-M}(s) & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

$$\mathcal{G}_n(s) = \begin{bmatrix} G_{n,0}(s) \\ G_{n-1,0}(s) \\ G_{n-2,0}(s) \\ G_{n-3,0}(s) \\ \vdots \\ G_{n-M,0}(s) \end{bmatrix} \quad (37)$$

where $\hat{P}_n(s)$ is the transfer matrix and $\mathcal{G}_n(s)$ is the vector containing head-to-tail transfer functions of vehicles from n to $n-M$. According to Theorem 2 in (Zhang and Orosz 2016), if $\| \mathcal{G}_n(s) \| < \| \mathcal{G}_{n-1}(s) \|$ for any two consecutive vehicle groups with leading vehicle n and $n-1$ respectively, then perturbations can be mitigated iteratively from the platoon head to the platoon tail, reaching head-to-tail string stability. We adopt this theorem to a platoon model with identical longitudinal vehicle dynamics. As a result, from equations (35)-(37), it requires that

$$\sup_{\forall \omega > 0} \left| \lambda_k \left(\hat{P}_n(i\omega) \right) \right| < 1, \quad k = 1,2,\ldots,M \quad (38)$$

where $\lambda_k \left(\hat{P}_n(i\omega) \right)$ is the k-th eigenvalue of the transfer matrix $\hat{P}_n(i\omega)$ with frequency ω.

3.6 Pseudo String Stability Analysis under Cybersecurity Uncertainties

In section 3.5, we conduct string stability analysis of the platooning model (1) in the attack-free scenario. In this section, we further extend the stability analysis under cyberattacks while taking the detection and recovery into account. Specifically, we aim to model the system with the ability to detect anomalies and fully recover the true measurements once the anomalies are detected. We assume the recovery can be achieved by utilizing other sources of information, e.g., road side units (RSUs). The detection sensitivity/recall may not always be 100%, meaning that there exists uncertainty in the platooning model where it switches between the compromised model and the normal model. Note that current tools for stability analysis do not consider such probabilistic models. Therefore, in this study, we define the concept of *pseudo string stability* for the case where the model is probabilistic.

We assume all platoon members will be affected by the attack. This can be achieved by a drone or a wireless device conducting false injection attacks or jamming attacks to affect either onboard measurements or the input vector. We also assume each platoon member is equipped with the same detector with detection sensitivity p, which is defined as the number of true positive anomaly detections, divided by the total number of anomalous instances. Then, the platoon model (1) becomes a probabilistic model,

$$\begin{aligned}\dot{v}_n(t) &= \eta_t f\left(v_n(t-\tau_1), \bar{g}_n(t;\tau_1,\tau_2), \bar{d}_n(t;\tau_1,\tau_2)\right) \\ &+(1-\eta_t)\cdot f\left(v_n(t-\tilde{\tau_1})+\tilde{A}, \bar{g}_n(t;\tilde{\tau}_1,\tilde{\tau}_2)+\tilde{B}, \bar{d}_n(t;\tilde{\tau}_1,\tilde{\tau}_2)+\tilde{C}\right)\end{aligned} \tag{39}$$

where

$$\begin{aligned}\bar{g}_n(t;\tau_1,\tau_2) &:= \alpha_1 g_n(t-\tau_1) + \sum_{j=2}^{M} \alpha_j\, g_{n-j+1}(t-\tau_2) \\ \bar{d}_n(t;\tau_1,\tau_2) &:= \beta_1 \Delta v_n(t-\tau_1) + \sum_{j=2}^{M} \beta_j\, \Delta v_{n-j+1}(t-\tau_2)\end{aligned} \tag{40}$$

and η_t is a Bernoulli random variable with $\mathbb{P}(\eta_t = 1) = \tilde{p} = p^N$ and $\mathbb{P}(\eta_t = 0) = 1-\tilde{p}$ given N vehicles in the platoon. Note that for the ease of stability analysis and for security concerns, we adopt the most conservative setting where if any platoon member fails to detect the attack, the whole platooning model becomes compromised with $\eta_t = 0$. The attack parameters are $\tilde{\tau}_1$, $\tilde{\tau}_2$, $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$, where $\tilde{\tau}_1$, $\tilde{\tau}_2$ can be affected by jamming attacks and the rest of three parameters can be affected by false injection attacks. Note that without abuse of notation we denote $\tilde{\tau}_1$ and $\tilde{\tau}_2$ as any time delays different from the single values τ_1 and τ_2, which can also account for stochastic time delays.

Since the platoon model in (39) is a probabilistic model, we define pseudo string stability under model uncertainty as follows:

Definition 2. *Consider a vehicle string with semi-infinite length in equilibrium state. Impose a transient perturbation on the head vehicle. The vehicle string is pseudo string stable if the perturbation eventually vanishes when reaching the tail vehicle in the string.*

Note that by Definition 1 the perturbation could be amplified for some time periods and a subset of vehicles. However, if the vehicle string is sufficiently long, the perturbation will vanish at the tail vehicle. Note that this is different from Definition 1, which requires perturbation attenuates at the end of the vehicle string even for a finite-length vehicle string.

Denote the transfer matrix of the compromised dynamic model as

$$\hat{P}_n(s;\Lambda) = \begin{bmatrix} T_{n-1}(s;\Lambda) & T_{n-2}(s;\Lambda) & \dots & T_{n-M}(s;\Lambda) & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix} \tag{41}$$

where Λ represents the set of attack parameters $\tilde{\tau}_1$, $\tilde{\tau}_2$, $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$. Denote the transfer matrix of the probabilistic platooning model (39) as $\hat{P}_n(s;\Lambda,\tilde{p})$. Then, given a detection sensitivity p, we can obtain the mean transfer matrix of the probabilistic platooning model (39),

$$\begin{aligned}\bar{\hat{P}}_n(s;\Lambda) &:= \mathbb{E}_{\tilde{p}}\left[\hat{P}_n(s;\Lambda,\tilde{p})\right] \\ &= \tilde{p}\cdot\hat{P}_n(s) + (1-\tilde{p})\cdot\hat{P}_n(s;\Lambda) \\ &= \begin{bmatrix} \bar{T}_{n-1}(s;\Lambda) & \bar{T}_{n-2}(s;\Lambda) & \dots & \bar{T}_{n-M}(s;\Lambda) & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}\end{aligned} \quad (42)$$

where $\bar{T}_i(s;\Lambda) = \tilde{p}\cdot T_i(s) + (1-\tilde{p})\cdot T_i(s;\Lambda)$.

Given a stochastic model $\mathcal{F}\left(\tilde{p},\hat{\xi}\right)$, it is pseudo string stable if it satisfies

$$\sup_{\forall\omega>0}\left|\lambda_k\left(\bar{\hat{P}}_n(i\omega;\Lambda)\right)\right| < 1, \quad k = 1,2,\dots,M \quad (43)$$

By formulas (41) and (42), we can validate whether a detection sensitivity can ensure a pseudo stable string given a set of attack parameters Λ.

After showing that the head-to-tail string stability is a function of detection sensitivity, as illustrated later in section 4, it is worthwhile and possible to find the critical detection sensitivity under a set of specific cyberattack parameters, such that if all detectors can successfully detect and recover from the attacks with a probability higher than the critical detection sensitivity, then the pseudo head-to-tail string stability can be maintained.

4. Numerical Experiments

In this section, we perform extensive numerical experiments to investigate the anomaly detection performance of our proposed methods in Section 3. First, we investigate the performance of the χ^2-detector and OCSVM under a mixed set of anomaly types introduced in Section 1, namely, 'short', 'noise', 'bias', 'gradual drift', and 'miss', with random attack magnitude and duration. This experiment explores the potential of using OCSVM and an augmented state formulation in the presence of sensor measurement and communication time delays. Next, we conduct sensitivity analysis on the attack parameters and investigate their impact on platoon string stability. This experiment demonstrates the stability of the platoon under different combinations of attack scenarios. Lastly, we analyze the relationship between the detection sensitivity/recall and the pseudo string stability of a platoon under cyberattacks. We further find the the critical detection sensitivity under which one can maintain a pseudo stable string.

We adopt a variant of the well-known intelligent driver model (IDM), originally proposed by Treiber et al. (Treiber and Kesting 2013), namely the cooperative intelligent driver model (CIDM) from (P. Wang, Wu, and He 2020) as our platooning model of choice, and implement our framework to compare the anomaly detection performance of the χ^2-detector and OCSVM in conjunction with EKF and AEKF. According to (Treiber and Kesting 2013), IDM is suitable for describing the characteristics of automated driving, e.g. ACC. Although IDM has no explicit reaction time, it can also be easily extended to capture the communication delay, as described in the literature (Y. Wang, Masoud, and Khojandi

2020b; P. Wang, Wu, and He 2020). Note that compared with the CIDM model in (P. Wang, Wu, and He 2020), in this paper we further extend the IDM model to the setting of heterogeneous time delay. The CIDM with heterogeneous time delay can be described as follows,

$$\dot{v}_n(t) = a^* \left(1 - \left(\frac{v_n(t)}{v_0} \right)^4 - \left(\frac{S^*\left(v_n(t), \bar{d}_n(t;\tau_1,\tau_2) \right)}{\bar{g}_n(t;\tau_1,\tau_2)} \right) \right) \quad \text{with} \tag{44}$$

$$S^*\left(v_n(t), \bar{d}_n(t;\tau_1,\tau_2) \right) = s_0 + T \cdot v_n(t) + \frac{v_n(t) \cdot \bar{d}_n(t;\tau_1,\tau_2)}{2\sqrt{a^* b^*}}$$

where $\bar{d}_n(t;\tau_1,\tau_2)$ and $\bar{g}_n(t;\tau_1,\tau_2)$ are defined in (39), a^*, b^* represent the maximum acceleration and the maximum comfortable deceleration respectively, v_0 represents the desired free-flow velocity, $S^*(\cdot)$ is the desired clearance gap, s_0 denotes the minimum clearance gap in jammed traffic, and T is the desired time headway to follow the immediate leading vehicle.

Table 2: CIDM parameters

v_0	33.33 m/s	Desired free-flow velocity
l	5 m	Vehicle length
T	1.1 s	Safety time headway
s_0	2	Minimum clearance gap
a^*	1 m/s^2	Maximum acceleration
b^*	2 m/s^2	Maximum comfortable deceleration

4.1 Detection Performance under a Single Vehicle Attack

To measure the effectiveness of our proposed detection methodologies, we conduct sensitivity analysis over the Kalman filter configuration (i.e., with and without augmented state formulation), the anomaly detection methodology (i.e., the χ^2-detector and OCSVM), and time delays τ_1 and τ_2. We calculate the area under the curve (AUC) of each receiver operating characteristic (ROC) curve which summarizes the trade-off between the true positive rate and false positive rate ($1 -$ specificity) for a predictive model at various threshold settings, by changing the values of γ of the χ^2-detector in (24), and parameter c of OCSVM in (27). Since we are using an imbalanced dataset in which the number of non-anomalous cases is substantially higher than the number of anomalous cases, we further calculate the AUC score of the precision-recall curve, which summarizes the trade-off between the true positive rate and the positive predictive value (PPV, or precision) for a predictive model at various threshold settings, and is more suitable for imbalanced dataset.

Our experiments are based on the Safety Pilot dataset from the Safety Pilot Model Deployment (SPMD) program (Bezzina and Sayer 2014) funded by the US department of Transportation, and collected in Michigan. The sampling frequency is 10 HZ (i.e. $\Delta t = 0.1$s).

We sample the in-vehicle speed from the SPMD dataset with 4000 samples (400 seconds) for training set and 2000 samples (200 seconds) for testing set.

The testing scenario contains a vehicle platoon with 10 vehicles and each vehicle except for the platoon leader adopts the CIDM model in (43), and each vehicle except for the first two vehicles receive two cooperative leading vehicles' information. For simplicity, we set $\alpha_1 = \beta_1 = 0.8$ and $\alpha_2 = \beta_2 = 0.2$. The measurement vector z_n includes the location and velocity of the n-th vehicle. The platoon leader's trajectory is extracted from SPMD dataset, and the trajectory of the rest of the platoon members are generated as the baseline based on the following rule:

$$\begin{aligned} x_n(k+1) = \;& x_n(k) + v_n(k) \cdot \Delta t \\ v_n(k+1) = \;& \Delta t \cdot f\big(v_n(k - \lfloor \tilde{\tau}_1/\Delta t \rfloor), \bar{g}_n(k; \lfloor \tilde{\tau}_1/\Delta t \rfloor, \lfloor \tilde{\tau}_2/\Delta t \rfloor)), \bar{d}_n(k; \lfloor \tilde{\tau}/\Delta t \rfloor, \lfloor \tilde{\tau}/\Delta t \rfloor)\big) \\ & + v_n(k) + \epsilon_k \end{aligned} \tag{45}$$

where ϵ_k is sampled from a random variable to represent the inaccuracy caused by the flooring operation, and ϵ_k is sampled from a uniform distribution within range $[-0.1, 0.1]$. After obtaining the baseline data, we add Gaussian white noise with a variance of 0.3 to the baseline data to represent the measurement noise. Random anomalies are generated with 10% anomaly rate and injected into the trajectory data of the 5-th vehicle in the platoon using algorithm 1 in (Y. Wang, Masoud, and Khojandi 2020b). The anomaly magnitude for each type of anomaly is uniformly distributed within range (0,1], and the anomaly durations are also uniformly distributed from 1 to 20 time epochs.

The experiments are separately implemented into four models for ablation study, where model 1 is composed of a χ^2-detector in conjunction with EKF, model 2 is composed of a χ^2-detector in conjunction with ASEKF, model 3 is composed of OCSVM in conjunction with EKF, and model 4 is composed of OCSVM in conjunction with ASEKF. The CIDM parameters are set according to Table 2. Table 3 shows the performance of three models under three testing scenarios with different time delay settings, i.e. 0 seconds, 0.5 seconds, and 1.5 seconds, where $\tau_1 = \tau_2 = 0$ for scenario 1. For scenario 2 and scenario 3, we consider stochastic time delay with $\mathbb{E}[\tilde{\tau}_1] = \mathbb{E}[\tilde{\tau}_2] = 0.5$ and $\mathbb{E}[\tilde{\tau}_1] = \mathbb{E}[\tilde{\tau}_2] = 1.5$, respectively, with bounds of stochastic time delays $a_1 = a_2 = -0.1$, and $b_1 = b_2 = 0.1$. The measurement function $\mathcal{M}(\cdot)$ of ASEKF in equation (10) is defined as:

$$\mathcal{M}(\tilde{s}) = \begin{bmatrix} 1,0,1 \\ 0,1,0 \end{bmatrix} \cdot \tilde{s} \tag{46}$$

Table 3: Detection performance of three models measuring on AUC scores of ROC curve and PR curve.

Time Delay	Scen 1: $\tau_1 = \tau_2 = 0$ s		Scen 2: $\mathbb{E}[\tilde{\tau}_1] = \mathbb{E}[\tilde{\tau}_2] =$ 0.5 s		Scen 3: $\mathbb{E}[\tilde{\tau}_1] = \mathbb{E}[\tilde{\tau}_2] =$ 1.5 s	
Metric	ROC AUC	PR AUC	ROC AUC	PR AUC	ROC AUC	PR AUC
χ^2 EKF	0.968 ± 0.018	0.922 ± 0.054	0.946 ± 0.018	0.895 ± 0.054	0.866 ± 0.016	0.820 ± 0.049
χ^2 ASEKF	0.968 ± 0.021	0.920 ± 0.056	0.953 ± 0.024	0.902 ± 0.060	0.938 ± 0.030	0.866 ± 0.068
OCSVM EKF	**0.977 ± 0.011**	**0.959 ± 0.020**	**0.974 ± 0.010**	**0.956 ± 0.019**	**0.964 ± 0.012**	**0.933 ± 0.019**
OCSVM ASEKF	0.970 ± 0.017	0.933 ± 0.019	0.966 ± 0.014	0.936 ± 0.026	0.959 ± 0.014	0.931 ± 0.024

and the measurement function $\mathcal{M}(\cdot)$ of EKF is defined as:

$$\mathcal{M}(s) = \begin{bmatrix} 1,0 \\ 0,1 \end{bmatrix} \cdot s \qquad (47)$$

The experiments indicate that the OCSVM with EKF fault detection method provides a significant improvement (up to 13.8% in PR AUC and 11.3% in ROC AUC) compared with the performance of the two χ^2-detector models, regardless of the value of time delay. Also, we observe that using augmented state formulation can significantly improve the performance of χ^2-detector under stochastic time delay (scenario 2 and scenario 3). However, when there is no time delay (scenario 1), using ASEKF does not lead to a better performance because there is no need to use the augmented state to compensate for potential bias caused by the time delay factors, and it introduces more uncertainties to the actual state which decreases the detection performance. Unlike the χ^2-detector, we observe a slight decrease of performance in OCSVM when it is combined with ASEKF. The reason is that OCSVM itself can learn the potential background bias in state-transition model and therefore the marginal benefit of using ASEKF is not prominent compared with the case for the χ^2-detector. Moreover, we observe that when using an augmented state formulation, the value of the augmented state is affected by the existence of anomalies and therefore the innovation distribution of the testing data is changed compared with that in

the training data, which makes it more difficult for the trained OCSVM classifier to detect anomalies. Additionally, we observe a systematic deterioration of the detection performance as we increase the time delays, due to the fact that the time delays decrease the estimation accuracy of both EKF and ASEKF and therefore affect the detection performance.

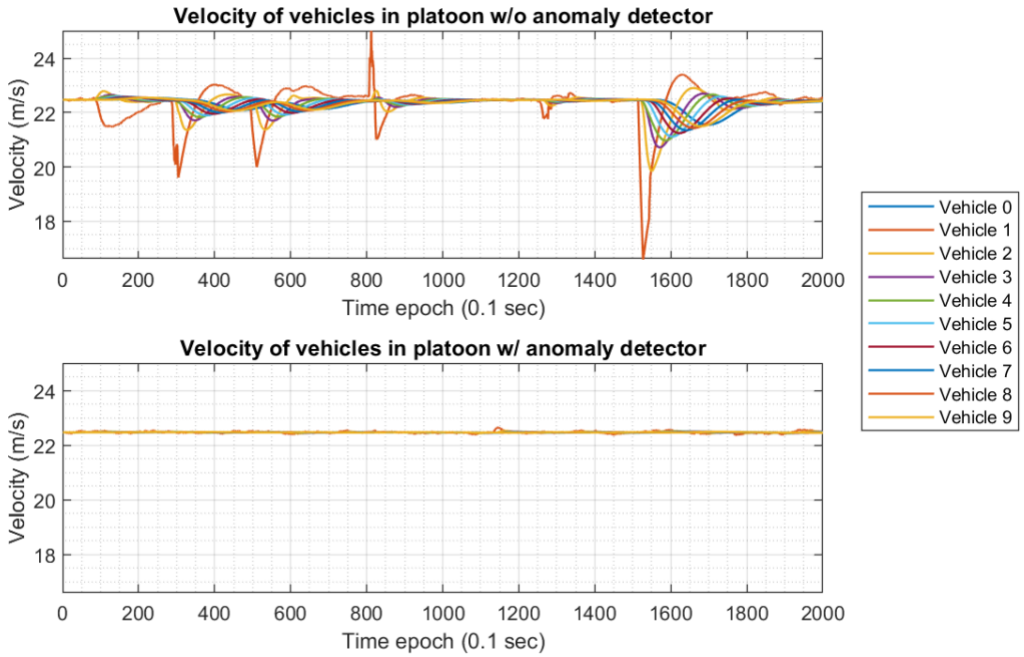


Figure 3: Vehicle velocity in platoon. Top: without detection and recovery. Bottom: with detection and recovery.

4.2 Detection Performance under Multiple Vehicle Attacks

Next, we investigate the impact of cyberattacks on multiple vehicles in the platoon, and the effect of the detection and recovery. We assume each individual platoon member is equipped with a detector and is able to recover the true state only if it successfully detects an anomaly. All platoon vehicles are initialized at the steady state, i.e. with equilibrium clearance gap of g^* and equilibrium velocity of v^*, which can be obtained by having all vehicles in the platoon travel with the same constant velocity v^*,

$$g^* = v^*(s_0 + Tv^*)\left(1 - \left(\frac{v^*}{v_0}\right)^4\right)^{-0.5} - g_0 \qquad (48)$$

where g_0 is the initial clearance gap between each pair of adjacent vehicles.

We consider a ten-vehicle platoon in a road-ring configuration (starting from ID 0 to ID 9). Each vehicle receives information from its immediate three leading vehicles, with $\alpha_1 = \beta_1 = 0.7$, $\alpha_2 = \beta_2 = 0.2$, and $\alpha_3 = \beta_3 = 0.1$. Again, we use the same parameters in CIDM as presented in Table 1. The time delay is set to a fixed value of 0.5 seconds for both τ_1 and τ_2. A mixed set of anomaly types with anomaly rate of 10% were applied to five vehicles in the

platoon, starting from the second vehicle to the sixth vehicle. The left and right subfigures in Figure 3 show the vehicle velocity with and without anomaly detection and recovery, respectively. We can observe a significant fluctuation of velocity under the attack scenario without detection and recovery, and conversely much smoother trajectories after detection and recovery.

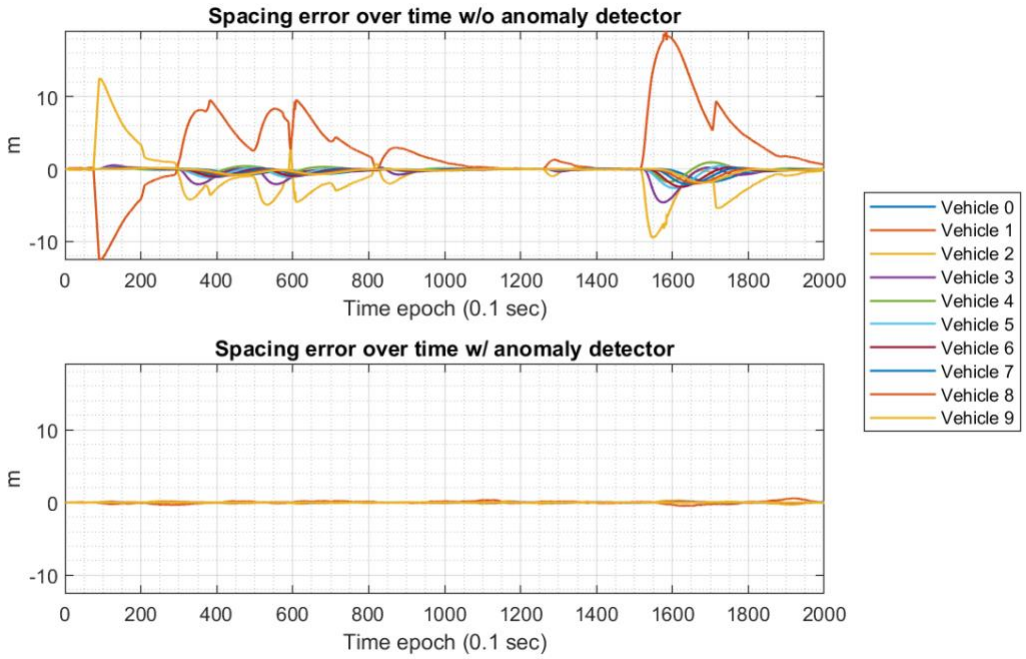


Figure 4: Spacing error over time under cyberattacks. Top: without anomaly detection and recovery. Bottom: with anomaly detection and recovery.

Figure 4 shows the spacing error between each pair of adjacent vehicles in the platoon in the span of 200 seconds. The top subfigure shows the spacing error without anomaly detection, and the bottom subfigure shows the spacing error with anomaly detection and recovery. The spacing error $\Delta g_n(t)$ for the n-th vehicle at time t is defined as

$$\Delta g_n(t) = g_n(t) - g^* \qquad (49)$$

and becomes zero when all vehicles in the platoon are in the equilibrium state. We can observe that when the platoon is under attack, there exist a lot of perturbations in terms of spacing error if no detector is deployed. Such perturbations are greatly reduced when using a detector, followed with a recovery step.

Figure 5 further shows the maximum spacing error with and without anomaly detection and recovery. The maximum spacing error is defined as $\max_t|\Delta g_n(t)|$. According to Definition 1, the head-to-tail string stability can also be described in time domain:

$$\max_t|\Delta g_{N-1}(t)| <\ldots< \max_t|\Delta g_n(t)| <\ldots< \max_t|\Delta g_0(t)| \qquad (50)$$

In Figure 5 we can observe an unstable vehicle string when there is no detector. However, the platoon stabilizes with detection and recovery.

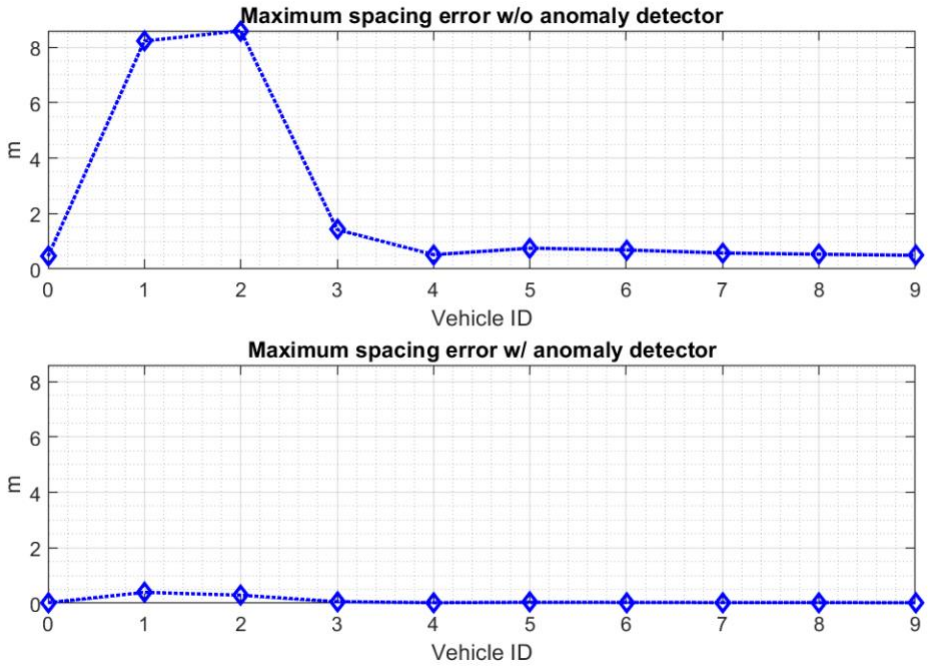


Figure 5: Maximum absolute spacing error under cyberattacks. Top: without anomaly detection. Bottom: with anomaly detection and recovery.

4.3 Sensitivity Analysis on the Attack Parameters

We further conduct sensitivity analysis to study the effect of attack parameters on the platoon's string stability. Specifically, we analyze the effects of attack parameters $\tilde{A}, \tilde{B}, \tilde{C}, \tilde{\tau}_1$, and $\tilde{\tau}_2$ on the platooning model without anomaly detection:

$$\dot{v}_n(t) \quad = f\big(v_n(t-\tilde{\tau_1}) + \tilde{A}, \bar{g}_n(t;\tilde{\tau}_1,\tilde{\tau}_2) + \tilde{B}, \bar{d}_n(t;\tilde{\tau}_1,\tilde{\tau}_2) + \tilde{C}\big) \qquad (51)$$

In our simulations so far, the three attack parameters (noise terms) $\tilde{A}, \tilde{B}, \tilde{C}$ have been fixed. To further investigate the influence of attack intensity on platoon string stability, we experiment with multiple sets of attack parameters and keep the rest of parameters fixed, as in Table 2. We keep the same topology, where each vehicle will receive information from three predecessors, as shown in Figure 2, and $\alpha_1 = \beta_1 = 0.7$, $\alpha_2 = \beta_2 = 0.2$, and $\alpha_3 = \beta_3 = 0.1$. The attack parameters tested for sensitivity analysis are listed in Table 2.

Table 4: Sensitivity Analysis Parameters

Parameter	Lower Bound	Upper Bound	Step Size
$\tilde{A}$	-15 m/s	15 m/s	0.2 m/s
$\tilde{B}$	-15 m	15 m	0.2 m
$\tilde{C}$	-15 m/s	15 m/s	0.2 m/s

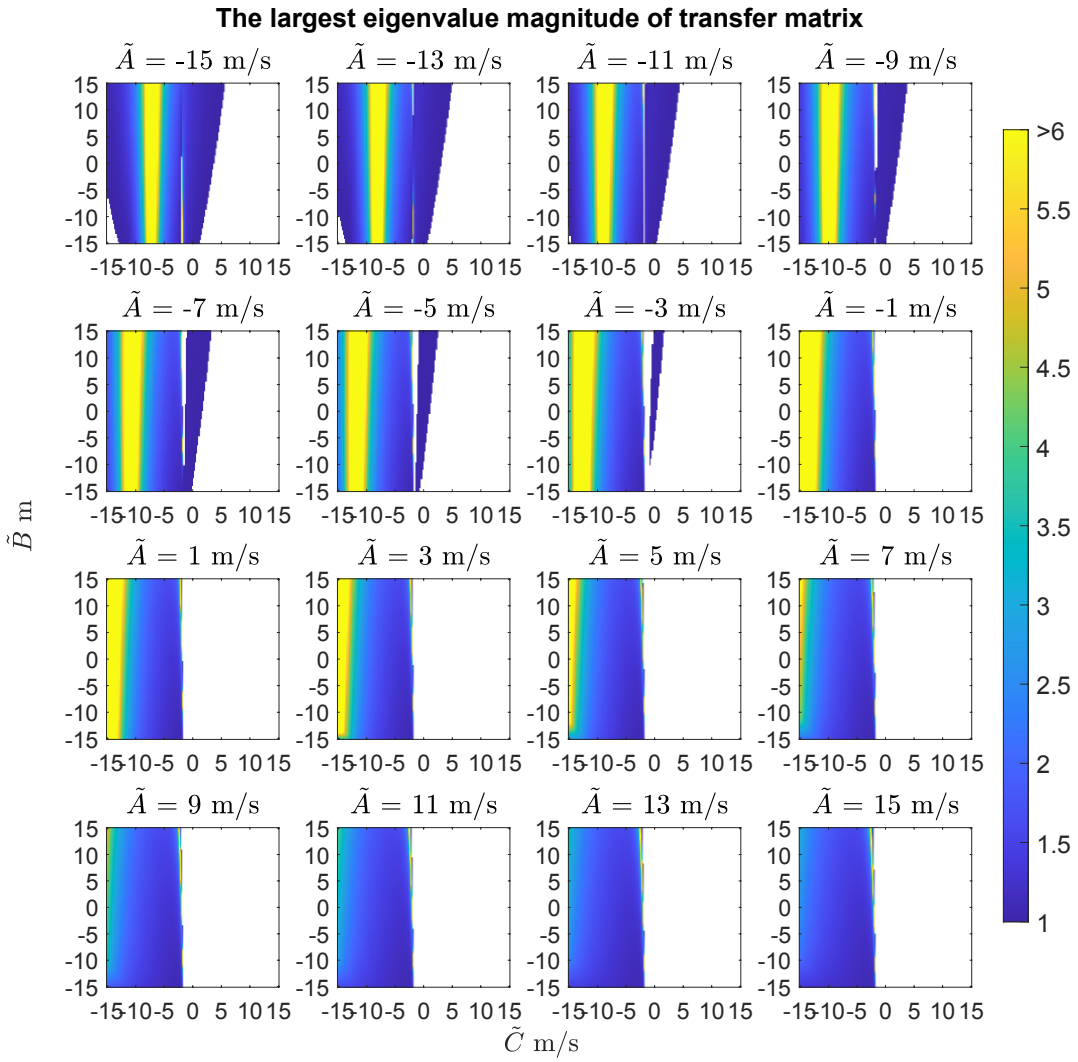


Figure 6: The white area in each subplot represents that given the set of attack parameters, the platoon can remain string stable. The color bar indicates the value of the largest eigenvalue of the transfer matrix.

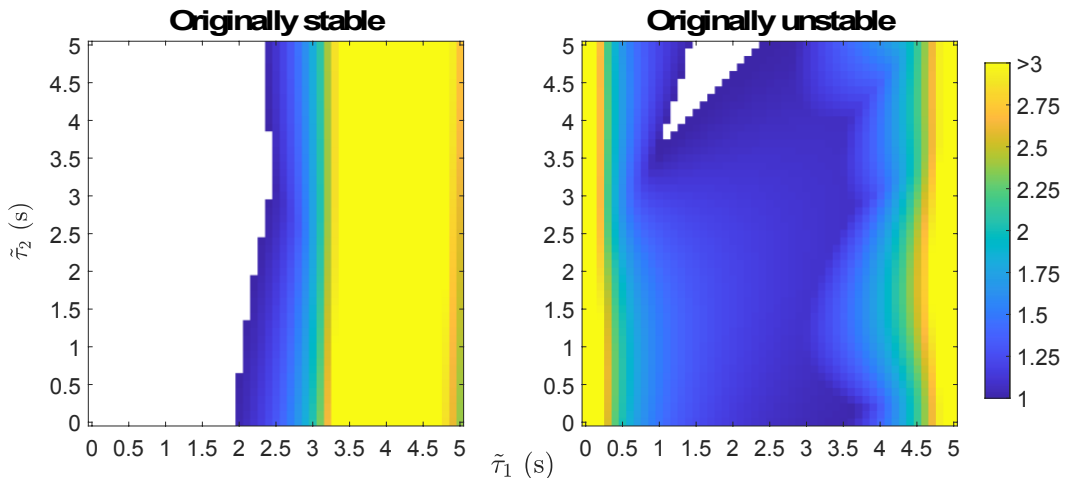


Figure 7: The left plot indicates the influence of the manipulated onboard time delay, $\tilde{\tau}_1$, and the manipulated communication time delay $\tilde{\tau}_2$ on platoon string stability when $\tilde{A} = \tilde{B} = \tilde{C} = 0$. The right plot shows the influence of $\tilde{\tau}_1$ and $\tilde{\tau}_2$ when the platoon is string unstable even in the absence of any attacks, and with $\tilde{A} = -3$ m/s, $\tilde{B} = -5$ m, $\tilde{C} = -11$ m/s. As a reference, the initial largest magnitude of eigenvalues of the transfer matrix when $\tilde{\tau}_1 = \tilde{\tau}_2 = 0$ is 5.2835. The maximum magnitude of eigenvalues with time delays is 5.3288. The white color represents the string stable region.

Figure 6 shows the heat map of the largest eigenvalue of the transfer matrix given the combination of attack parameters $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$. The color white indicates that the platoon will remain head-to-tail string stable for the given parameter combinations, while the colored region indicates loss of head-to-tail string stability. The color intensity indicates the magnitude of perturbation amplifications when the platoon is string unstable.

It can be observed that as $\tilde{A}$ increases from negative values to positive values, the unstable region shifts to the left. In an unstable platoon, when fixing the distance-targeted attack parameter $\tilde{B}$, to achieve the same level of peak amplification of perturbations in the platoon, the other two velocity-targeted attack parameters, $\tilde{A}$ and $\tilde{C}$, should be adjusted in opposite directions, i.e., increasing (decreasing) $\tilde{A}$, but decreasing (increasing) $\tilde{C}$. One explanation is that by increasing $\tilde{A}$, the ego vehicle falsely perceives its velocity higher than its actual velocity. Meanwhile if we do not change (or increase) $\tilde{C}$, which affects the relative velocity between the ego vehicle and its cooperative leaders, this indicates that the cooperative leaders are moving in higher velocities. Therefore within the current range of attack parameters, an attack that erroneously leads to a perceived higher velocity of leaders in the platoon compensates the damage done by an attack that erroneously leads to a perceived higher velocity of the ego vehicle, and could make the platoon more stable for some ranges of these attack parameters.

The relationship between the distance-targeted attack parameter and the two velocity-targeted attack parameters is even more complicated. However, we notice that when $\tilde{A} > -3$, there is a trend that when fixing $\tilde{C}$, to make the platoon achieve the same level of peak amplification of perturbations requires $\tilde{A}$ and $\tilde{B}$ to change in the same direction, i.e., increasing (decreasing) $\tilde{A}$ and $\tilde{B}$ together. One possible explanation is that, under the

current range of attack parameters, by increasing $\tilde{A}$, the ego vehicle perceives its velocity higher than its actual velocity. Increasing $\tilde{B}$, which affects the perceived clearance gap between the ego vehicle and its cooperative leaders, could illude the ego vehicle to actually drive faster, thereby making the platoon more unstable.

The influence of two time delay terms, $\tilde{\tau}_1$ and $\tilde{\tau}_2$, are also studied after fixing attack parameters $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$. We use the same communication topology as shown in Figure 2 with $\alpha_1 = \beta_1 = 0.7$, $\alpha_2 = \beta_2 = 0.2$, and $\alpha_3 = \beta_3 = 0.1$. The time delays and attack parameters are set as follows: we first set $\tilde{\tau}_1 = 0$ and $\tilde{\tau}_2 = 0$, where no time delays exist in the system. For the first set of parameters, which create stable conditions, we set $\tilde{A} = \tilde{B} = \tilde{C} = 0$ such that the platoon becomes string stable without any time delay. In the second set of attack parameters, which provide unstable conditions, we set $\tilde{A} = -3$ m/s, $\tilde{B} = -5$ m, and $\tilde{C} = -11$ m/s to make the platoon string unstable even without any time delays. All combinations of $(\tilde{\tau}_1, \tilde{\tau}_2)$ are then tested in the range of $[0,\ 5]$ seconds with a step size of 0.1 seconds. The results are shown in Figure 7.

From Figure 7, we observe that when the dynamics model is attack-free, onboard time delay $\tilde{\tau}_1$ has more power in affecting platoon stability compared to the communication time delay $\tilde{\tau}_2$, as we can always find an unstable region by fixing τ_2 and adjusting $\tilde{\tau}_1$, but not vice versa. Furthermore, it appears that there is a threshold value $\tilde{\tau}_1^*$ ($\tilde{\tau}_1^* = 2$ seconds in this case) such that the platoon will remain string stable as long as $\tilde{\tau}_1 < \tilde{\tau}_1^*$, when $\tilde{\tau}_2$ is smaller than 5 seconds. An extreme case is when $\tilde{\tau}_2 = \infty$, where the platoon is under a pure car-following model. In this case, $\tilde{\tau}_1$ represents the delay from the ego vehicle's onboard measurements, which in addition to the status of the ego vehicle provides information about its immediate leading vehicle. On the right subplot, we observe a more complex pattern. When fixing $\tilde{\tau}_2$, the peak amplification of perturbations can be altered greatly by changing $\tilde{\tau}_1$. However, except for the stable region in the upper part of figure, $\tilde{\tau}_2$ seems to have a more subtle impact on the peak amplification of perturbations. One interesting finding is that if the platoon is originally string unstable, increasing $\tilde{\tau}_1$ from 0 to 2.5 seconds can achieve a lower peak amplification of perturbations. This suggests that, when the platoon is unstable to begin with, the peak amplification of perturbations can be reduced by a slight increase of latency in onboard measurement. However, there may exist different trends for a broader range of attack parameters, because of the complex nature of the mutual impact of different attack parameters on the characteristics of stability region, which is characterized by the eigenvalues of the transfer matrix. Moreover, introducing larger time delays can eventually cause a crash, which is not reflected in stability analysis.

4.4 Pseudo String Stability Analysis

In this section, we conduct pseudo string stability analysis on model (39). One major contribution of this work is to bridge the gap between anomaly detection and platoon string stability. Since in practice the detection sensitivity/recall is not always 100%, as discussed in Section 3.6, the platoon model becomes a probabilistic model under detection uncertainties. Therefore, it is critical to find a minimum required detection sensitivity/recall such that any detector with a higher detection sensitivity can make the

platoon maintain pseudo string stability. Here we present several case studies to find the desired detection rate that determines the pseudo string stability of the platoon.

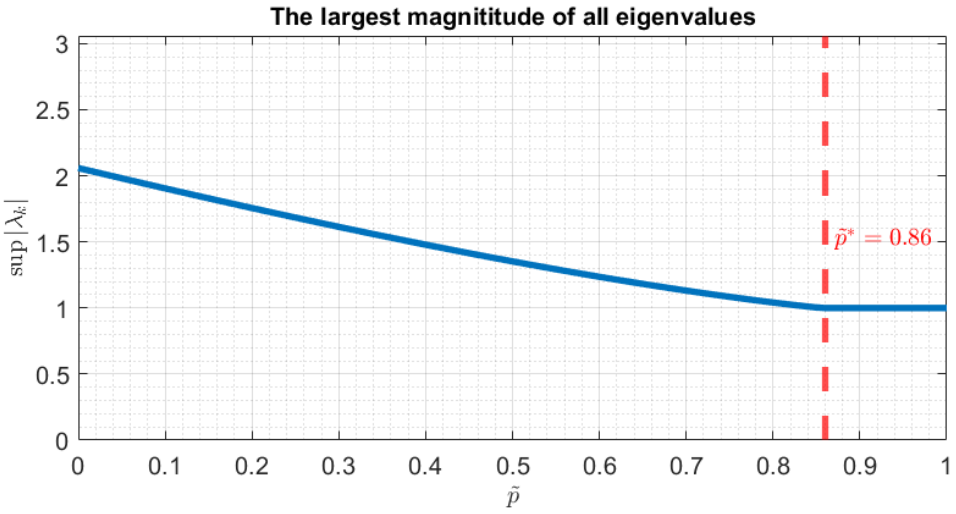
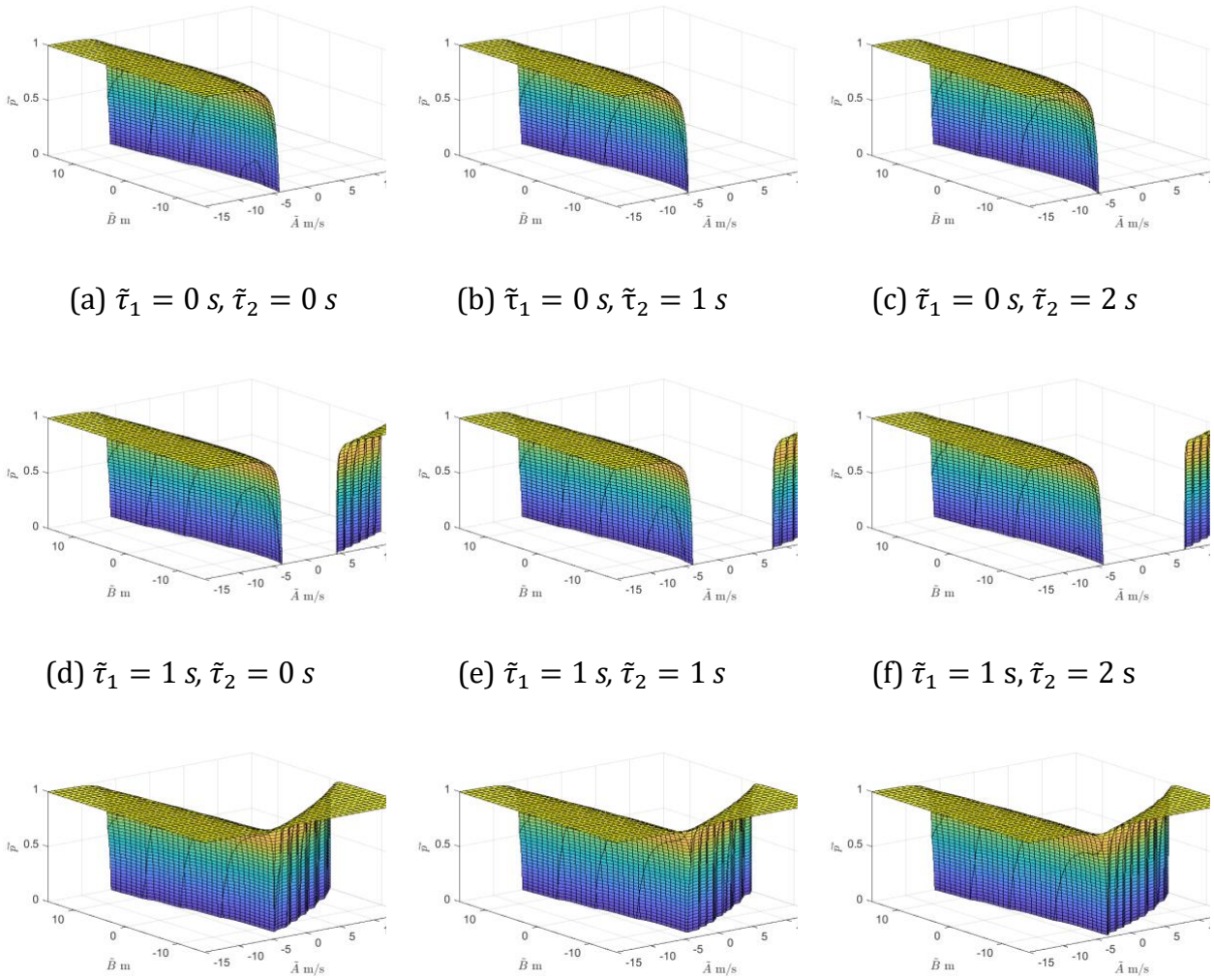


Figure 8: The blue curve represents the largest magnitude of all eigenvalues of the mean transfer matrix under detection uncertainties, i.e., $\tilde{p}$. The red dashed line indicates the critical point $\tilde{p}^* = (p^*)^{10} = 0.86$, when the largest magnitude becomes exactly 1, denoting a pseudo string stable platoon of 10 vehicles.

First, in order to investigate the existence and characteristics of such critical detection sensitivity, we conduct sensitivity analysis on the pseudo string stability of a platoon with 10 vehicles under different detection sensitivities. We use the same communication topology as shown in Figure 2 with $\alpha_1 = \beta_1 = 0.7$, $\alpha_2 = \beta_2 = 0.2$, and $\alpha_3 = \beta_3 = 0.1$. According to inequality (42), to maintain pseudo string stability, one needs to make sure that the largest magnitude of eigenvalues of the transfer matrix is always smaller or equal to 1 across all frequency values. In this experiment, the parameters selected for CIDM remain the same as shown in Table 1. Time delays take values of $\tilde{\tau}_1 = 0$ and $\tilde{\tau}_2 = 0.5$. The attack parameters use $\tilde{A} = -5$ m/s, $\tilde{B} = 15$ m, and $\tilde{C} = -6$ m/s. From Figure 8, we can see that given the existing topology of three predecessors in a ten-vehicle platoon, as the anomaly detection sensitivity increases from 0 to 1, the platoon will incrementally reach pseudo string stability with the critical detection sensitivity $p^* = \sqrt[10]{\tilde{p}^*} \approx 0.985$.



(a) $\tilde{\tau}_1 = 0\ s, \tilde{\tau}_2 = 0\ s$ (b) $\tilde{\tau}_1 = 0\ s, \tilde{\tau}_2 = 1\ s$ (c) $\tilde{\tau}_1 = 0\ s, \tilde{\tau}_2 = 2\ s$

(d) $\tilde{\tau}_1 = 1\ s, \tilde{\tau}_2 = 0\ s$ (e) $\tilde{\tau}_1 = 1\ s, \tilde{\tau}_2 = 1\ s$ (f) $\tilde{\tau}_1 = 1\ \mathrm{s}, \tilde{\tau}_2 = 2\ \mathrm{s}$

(g) $\tilde{\tau}_1 = 2\ s, \tilde{\tau}_2 = 0\ s$ (h) $\tilde{\tau}_1 = 2\ \mathrm{s}, \tilde{\tau}_2 = 1\ \mathrm{s}$ (i) $\tilde{\tau}_1 = 2\ \mathrm{s}, \tilde{\tau}_2 = 2\ \mathrm{s}$

Figure 9: Critical detection sensitivity $\tilde{p}^*$ under different attack parameters $\tilde{A} \in [-15, 15]$ m/s and $\tilde{B} \in [-15, 15]$ m by fixing $\tilde{B} = -1$ m/s. Each subfigure contains a hyperplane which represents the critical detection sensitivity $\tilde{p}^*$ under different time delay factors $\tilde{\tau}_1$ and $\tilde{\tau}_2$ in range $\{0,1,2\}$ seconds.

In order to further investigate how attack parameters affect the critical detection sensitivity value, we conduct sensitivity analysis by varying the different attack parameters, including $\tilde{A}$, $\tilde{B}$, $\tilde{\tau}_1$, and $\tilde{\tau}_2$, and calculating the corresponding critical $\tilde{p}^*$. Specifically, we consider a platoon with 10 vehicles and with 3 predecessors, where $\alpha_1 = \beta_1 = 0.7$, $\alpha_2 = \beta_2 = 0.2$, and $\alpha_3 = \beta_3 = 0.1$, following the CIDM parameters in Table 2. Figure 9 shows the critical detection sensitivity $\tilde{p}^*$ that maintains pseudo string stability of the platoon. In each subfigure, the hyperplane represents $\tilde{p}^*$ in z-axis for a range of $\tilde{A} \in [-15,15]$ in x-axis and $\tilde{B} \in [-15,15]$ in y-axis by fixing $\tilde{C} = -1$. We generate 9 subfigures

by considering all combinations of $\tilde{\tau}_1 \in \{0,1,2\}$ seconds and $\tilde{\tau}_2 \in \{0,1,2\}$ seconds. We first observe that in the given range of parameters, both attack parameters $\tilde{A}$ and $\tilde{B}$ determine the value of $\tilde{p}^*$, whereas the effect of destabilization is more prominent for the attack parameter $\tilde{A}$ when $\tilde{\tau}_1 = 0$. From subfigures 9c-9i, when $\tilde{A} > -3$ m/s, we observe the same trend as in Figure 6, i.e., when $\tilde{A} > -3$ m/s, in order to maintain the same level of peak amplification of perturbations, one needs to increase (decrease) $\tilde{A}$ and $\tilde{B}$ together. Each column of the subfigures in Figure 9 indicates that as we increase the value of $\tilde{\tau}_1$, we obtain a larger pseudo unstable region where we have non-zero critical detection sensitivity $\tilde{p}^*$. The destabilization effect of $\tilde{\tau}_2$ is less prominent than $\tilde{\tau}_1$, as we only observe a minimal change of hyperplane distribution in each row of Figure 9, which works in concert with our observation in Figure 7.

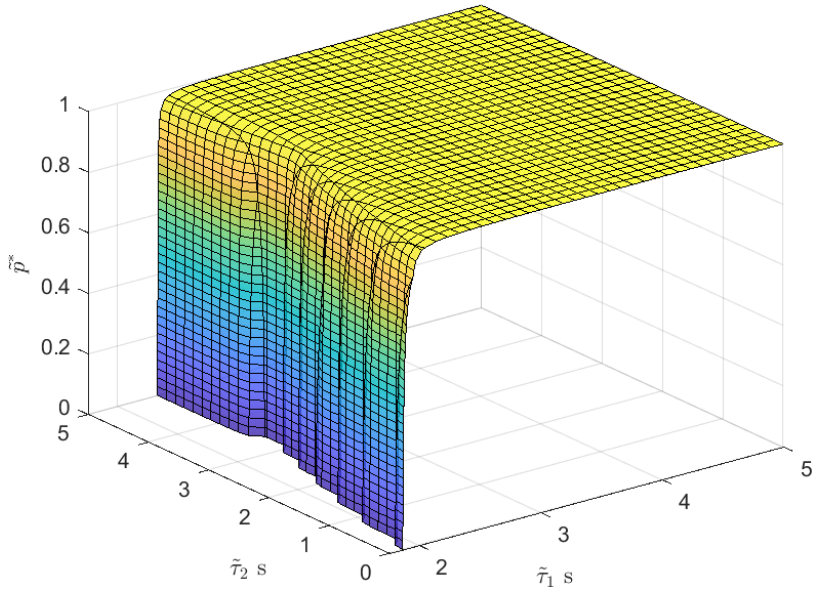


Figure 10: Critical detection sensitivity $\tilde{p}^*$ under different attack parameters $\tilde{\tau}_1$ and $\tilde{\tau}_2$ by fixing the values of $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$ to be 0.

In Figure 10, we investigate the standalone impact of manipulated delay factors $\tilde{\tau}_1$ and $\tilde{\tau}_2$ on the critical detection sensitivity. Figure 10 represents the critical detection sensitivity $\tilde{p}^*$ (z-axis) that maintains the pseudo string stability under different time delay factors $\tilde{\tau}_1 \in [0,5]$ seconds (x-axis) and $\tilde{\tau}_2 \in [0,5]$ seconds (y-axis), where we fix the values of $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$ to 0. Note that the projection of the hyperplane on the x-y plane is equivalent to the left figure in Figure 7 when $\tilde{\tau}_1$ and $\tilde{\tau}_2$ are within [0,3] seconds, which indicates the pseudo unstable region of the platoon when we do not use any anomaly detector.

Conclusion

CAVs can receive and utilize information from multiple sources to form vehicular platoons. However, literature has demonstrated that a CAV is more vulnerable to cyberattacks, as it has more attack surfaces. Existing literature either only investigates the impact of cyberattacks on platoons or defense methodologies, such as detection and protocol design.

Instead, in this study, we develop a comprehensive framework to model the impact of cyberattacks on platoons and to detect sensor measurement anomalies caused by either malicious attacks or sensor faults. Specifically, we propose a general platoon dynamics model under heterogeneous time delays, and design a state-space model for filtering and anomaly detection by utilizing cooperative vehicles' information. We further extend this model to consider stochastic time delays and show its impact on the state-space model. In order to investigate the impact of cyberattacks on platoons, we first conduct string stability analysis of the proposed platoon dynamics model. To the best of our knowledge, this is the first head-to-tail string stability analysis under heterogeneous time delay. Next, we propose a new definition for string stability under cyberattacks and model uncertainties, which we call pseudo string stability.

For vehicle state estimation, we show that under stochastic time delay, there may exist potential bias in the process noise of our proposed state-space model. To compensate for this, we propose an augmented state extended Kalman filter (ASEKF) for vehicle state estimation. For anomaly detection in the vehicle sensor measurements, we adopt two anomaly detectors, namely the χ^2-detector and the one class support vector machine (OCSVM), in conjunction with ASEKF. We conduct extensive experiments to demonstrate the effectiveness of our proposed detection framework. Specifically, we conduct an ablation study showing that an extended Kalman filter with an OCSVM detector achieves the best performance, whereas an augmented state formulation can significantly boost the performance of the χ^2-detector under time delay. Our experiments also show a negative impact of the time delay on the overall anomaly detection performance.

To study the impact of cyberattacks on the platoon's string stability, we conduct sensitivity analysis on the attack parameters. We observe certain relationships between the distance- and velocity-targeted attack parameters in affecting the peak amplification of perturbations in the platoon. In our experiments, we further investigate the pseudo string stability of platoons under different detection sensitivities and obtain the critical detection sensitivity to ensure a pseudo stable vehicle string.

The study is subject to certain limitations. In our experiments, similar to previous studies in the literature, due to the paucity of real-world anomalous CAV data, the anomalous instances in the sensor data are simulated with a mix of five types of anomalies. This implicitly imposes an assumption on the characteristics of the anomalous data. To partially address this limitation, we adopt a OCSVM model to learn the detection threshold by merely learning from normal data. It may be beneficial to test for novel anomaly types using real-world anomalous data to more accurately measure the effectiveness of our proposed detection methods.

Acknowledgements

This work has been supported by Center for Connected and Automated Transportation, a Region 5 University Transportation Center funded by the US Department of Transportation through grant #69A3551747105. We would like to extend our gratitude to Prof. Gabor Orosz for his invaluable feedback on this work.

References

Abdolmaleki, Mojtaba, Neda Masoud, and Yafeng Yin. 2019. "Vehicle-to-Vehicle Wireless Power Transfer: Paving the Way Toward an Electrified Transportation System." *Transportation Research Part C: Emerging Technologies* 103: 261–80.

Abdolmaleki, Mojtaba, Mehrdad Shahabi, Yafeng Yin, and Neda Masoud. 2021. "Itinerary Planning for Cooperative Truck Platooning." *Transportation Research Part B: Methodological* 153: 91–110.

Alam, Assad. 2011. "Fuel-Efficient Distributed Control for Heavy Duty Vehicle Platooning." PhD thesis, KTH Royal Institute of Technology.

Alipour-Fanid, Amir, Monireh Dabaghchian, Hengrun Zhang, and Kai Zeng. 2017. "String Stability Analysis of Cooperative Adaptive Cruise Control Under Jamming Attacks." In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, 157–62. IEEE.

Bar-Shalom, Yaakov, and Xiao-Rong Li. 1995. *Multitarget-Multisensor Tracking: Principles and Techniques*. Vol. 19. YBs Storrs, CT.

Bezzina, D, and J Sayer. 2014. "Safety Pilot Model Deployment: Test Conductor Team Report." *Report No. DOT HS* 812: 171.

Biron, Zoleikha Abdollahi, Satadru Dey, and Pierluigi Pisu. 2018. "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems." *IEEE Transactions on Intelligent Transportation Systems* 19 (12): 3893–3902.

Biroon, Roghieh A, Zoleikha Abdollahi Biron, and Pierluigi Pisu. 2021. "False Data Injection Attack in a Platoon of CACC: Real-Time Detection and Isolation with a PDE Approach." *IEEE Transactions on Intelligent Transportation Systems*.

Brumback, B, and M Srinath. 1987. "A Chi-Square Test for Fault-Detection in Kalman Filters." *IEEE Transactions on Automatic Control* 32 (6): 552–54.

Cao, Yulong, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z Morley Mao. 2019. "Adversarial Sensor Attack on Lidar-Based Perception in Autonomous Driving." In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2267–81.

Cao, Yulong, Chaowei Xiao, Dawei Yang, Jing Fang, Ruigang Yang, Mingyan Liu, and Bo Li. 2019. "Adversarial Objects Against Lidar-Based Autonomous Driving Systems." *arXiv Preprint arXiv:1907.05418*.

Cui, Lian, Jia Hu, B Brian Park, and Pavle Bujanovic. 2018. "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." *Transportation Research Part C: Emerging Technologies* 97: 1–22.

Feng, Shuo, Yi Zhang, Shengbo Eben Li, Zhong Cao, Henry X Liu, and Li Li. 2019. "String Stability for Vehicular Platoon Control: Definitions and Analysis Methods." *Annual Reviews in Control* 47: 81–97.

Feng, Yiheng, Shihong Huang, Qi Alfred Chen, Henry X Liu, and Z Morley Mao. 2018. "Vulnerability of Traffic Control System Under Cyberattacks with Falsified Data." *Transportation Research Record* 2672 (1): 1–11.

Guo, Ge, and Shixi Wen. 2015. "Communication Scheduling and Control of a Platoon of Vehicles in VANETs." *IEEE Transactions on Intelligent Transportation Systems* 17 (6): 1551–63.

Humpherys, Jeffrey, Preston Redd, and Jeremy West. 2012. "A Fresh Look at the Kalman Filter." *SIAM Review* 54 (4): 801–23.

Jin, I Ge, and Gábor Orosz. 2014. "Dynamics of Connected Vehicle Systems with Delayed Acceleration Feedback." *Transportation Research Part C: Emerging Technologies* 46: 46–64.

Ju, Zhiyang, Hui Zhang, and Ying Tan. 2020. "Distributed Deception Attack Detection in Platoon-Based Connected Vehicle Systems." *IEEE Transactions on Vehicular Technology* 69 (5): 4609–20.

Khattak, Zulqarnain H, Brian L Smith, and Michael D Fontaine. 2021. "Impact of Cyberattacks on Safety and Stability of Connected and Automated Vehicle Platoons Under Lane Changes." *Accident Analysis & Prevention* 150: 105861.

Liu, Xiangguo, Neda Masoud, Qi Zhu, and Anahita Khojandi. 2022. "A Markov Decision Process Framework to Incorporate Network-Level Data in Motion Planning for Connected and Automated Vehicles." *Transportation Research Part C: Emerging Technologies* 136: 103550.

Liu, Xiangguo, Guangchen Zhao, Neda Masoud, and Qi Zhu. 2020. "Trajectory Planning for Connected and Automated Vehicles: Cruising, Lane Changing, and Platooning." *arXiv Preprint arXiv:2001.08620*.

Masoud, Neda, and R Jayakrishnan. 2017. "Autonomous or Driver-Less Vehicles: Implementation Strategies and Operational Concerns." *Transportation Research Part E: Logistics and Transportation Review* 108: 179–94.

Molnár, Tamás G, Wubing B Qin, Tamás Insperger, and Gábor Orosz. 2015. "Predictor Design for Connected Cruise Control Subject to Packet Loss." *IFAC-PapersOnLine* 48 (12): 428–33.

———. 2017. "Application of Predictor Feedback to Compensate Time Delays in Connected Cruise Control." *IEEE Transactions on Intelligent Transportation Systems* 19 (2): 545–59.

Mousavinejad, Eman, Fuwen Yang, Qing-Long Han, Xiaohua Ge, and Ljubo Vlacic. 2019. "Distributed Cyber Attacks Detection and Recovery Mechanism for Vehicle Platooning." *IEEE Transactions on Intelligent Transportation Systems* 21 (9): 3821–34.

Mousavinejad, Eman, Fuwen Yang, Qing-Long Han, Quanwei Qiu, and Ljubo Vlacic. 2018. "Cyber Attack Detection in Platoon-Based Vehicular Networked Control Systems." In *2018 IEEE 27th International Symposium on Industrial Electronics (ISIE)*, 603–8. IEEE.

Ngoduy, Dong. 2015. "Linear Stability of a Generalized Multi-Anticipative Car Following Model with Time Delays." *Communications in Nonlinear Science and Numerical Simulation* 22 (1-3): 420–26.

Nowakowski, Christopher, Jessica O'Connell, Steven E Shladover, and Delphine Cody. 2010. "Cooperative Adaptive Cruise Control: Driver Acceptance of Following Gap Settings Less Than One Second." In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 54:2033–37. 24. SAGE Publications Sage CA: Los Angeles, CA.

Ploeg, Jeroen, Bart TM Scheepers, Ellen Van Nunen, Nathan Van de Wouw, and Henk Nijmeijer. 2011. "Design and Experimental Evaluation of Cooperative Adaptive Cruise Control." In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, 260–65. IEEE.

Ribeiro, Maria Isabel. 2004. "Kalman and Extended Kalman Filters: Concept, Derivation and Properties." *Institute for Systems and Robotics* 43: 46.

Shida, Mitsuhisa, and Yoshiaki Nemoto. 2009. "Development of a Small-Distance Vehicle Platooning System." In *16th ITS World Congress and Exhibition on Intelligent Transport Systems and ServicesITS AmericaERTICOITS Japan*.

Sun, Xiaotong. 2020. "Facilitating Cooperative Truck Platooning for Energy Savings: Path Planning, Platoon Formation and Benefit Redistribution." PhD thesis.

Sykora, Henrik T, Mehdi Sadeghpour, Jin I Ge, Dániel Bachrathy, and Gábor Orosz. 2020. "On the Moment Dynamics of Stochastically Delayed Linear Control Systems." *International Journal of Robust and Nonlinear Control* 30 (18): 8074–97.

Treiber, Martin, and Arne Kesting. 2013. "Traffic Flow Dynamics." *Traffic Flow Dynamics: Data, Models and Simulation, Springer-Verlag Berlin Heidelberg*, 983–1000.

Van Arem, Bart, Cornelie JG Van Driel, and Ruben Visser. 2006. "The Impact of Cooperative Adaptive Cruise Control on Traffic-Flow Characteristics." *IEEE Transactions on Intelligent Transportation Systems* 7 (4): 429–36.

Van Wyk, Franco, Yiyang Wang, Anahita Khojandi, and Neda Masoud. 2019. "Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles." *IEEE Transactions on Intelligent Transportation Systems* 21 (3): 1264–76.

Wang, Pengcheng, Xinkai Wu, and Xiaozheng He. 2020. "Modeling and Analyzing Cyberattack Effects on Connected Automated Vehicular Platoons." *Transportation Research Part C: Emerging Technologies* 115: 102625.

Wang, Yiyang, Neda Masoud, and Anahita Khojandi. 2020a. “Anomaly Detection in Connected and Automated Vehicles Using an Augmented State Formulation.” In *2020 Forum on Integrated and Sustainable Transportation Systems (FISTS)*, 156–61. IEEE.

———. 2020b. “Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors.” *IEEE Transactions on Intelligent Transportation Systems* 22 (3): 1411–21.

Watts, Jeremy, Franco van Wyk, Shahrbanoo Rezaei, Yiyang Wang, Neda Masoud, and Anahita Khojandi. 2021. “A Dynamic Deep Reinforcement Learning-Bayesian Framework for Anomaly Detection.” *ResearchGate Preprint: DOI: 10.13140/RG.2.2.35285.55526*.

Wyk, Franco van, Anahita Khojandi, and Neda Masoud. 2019. “A Path Towards Understanding Factors Affecting Crash Severity in Autonomous Vehicles Using Current Naturalistic Driving Data.” In *Proceedings of SAI Intelligent Systems Conference*, 106–20. Springer.

Zhang, Linjun, and Gábor Orosz. 2016. “Motif-Based Design for Connected Vehicle Systems in Presence of Heterogeneous Connectivity Structures and Time Delays.” *IEEE Transactions on Intelligent Transportation Systems* 17 (6): 1638–51.