String Stability Analysis of Cooperative Adaptive Cruise Control Under Jamming Attacks

Amir Alipour-Fanid*, Monireh Dabaghchian*, Hengrun Zhang† and Kai Zeng*
*Electrical and Computer Engineering Department,
† Computer Science Department
George Mason University, Fairfax, Virginia 22030
Email: {aalipour*, mdabaghc*, hzhang18†, kzeng2*}@gmu.edu

***Abstract*—Cooperative Adaptive Cruise Control (CACC) is considered as a key enabling technology to automatically regulate the inter-vehicle distances in a vehicle platooning while maintaining the string stability. Although the cyber and physical parts in the existing CACC systems are integrated in one control framework, the research on realistic modeling and security issues of these systems are still largely open. A good modeling of cyber characteristics and awareness of cyber attacks impact on the CACC operation leads to a better understanding of system design and defense mechanisms. In this paper, we conduct a comprehensive analysis on the vehicle string stability by considering a realistic wireless channel under a mobile reactive jamming attack. We examine the stability of the platoon under attacks by conducting extensive simulations for a wide range of realworld lead vehicle's acceleration profiles. We utilize time-domain definition of string stability to delineate the impact of the jamming attacks on the CACC system's functionality and string stability. We also examine the attacker's possible locations at which it can destabilize the string.**

I. Introduction

Vehicular Cyber-physical systems (CPS) expand the capabilities of the vehicles through the integration of computation, communication, and control [1]. Vehicle platooning is one of the important vehicular CPS applications that operates based on tight coupling of wireless communication and physical processes. Cooperative Adaptive Cruise Control (CACC) system as an extension of Adaptive Cruise Control (ACC) is proposed to constitute vehicle platooning formation [2], [3].

Based on CACC, each vehicle in the platoon uses two sources of information, absolute relative distance measured by the radar and acceleration information of the preceding vehicle received through the wireless channel established apriori.

Connected vehicles equipped with CACC systems are able to adjust inter-vehicle distances such that the traffic throughput is increased by running as close as possible to each other with safety guarantee. In addition, this technology reduces fuel consumption and provides more comfort to the users in comparison to solely human control of vehicles [4].

However, despite tremendous benefits attained by integrating the cyber (wireless communication) and physical processes in the CACC systems, there are several critical challenges remained.

First, considering tight coupling of cyber and control parts, the practical modeling of these parts play an important role to evaluate the performance of CACC system before a real implementation. Second, the CACC systems are highly susceptible to cyber attacks that can create significant disturbances in safe and efficient operation of these systems [5].

In a CACC enabled vehicle platoon, the distance between vehicles may change depending on the lead vehicle's behavior and spacing policy [6]. This variation in inter-vehicle distance affects the wireless channel conditions which further affects the received-signal-strength (RSS) and packet delivery ratio. However, in most of the existing literature, this coupling between the system state (inter-vehicle distance) and wireless channel conditions is ignored [2], [3], [7], [8].

In this paper, we consider a two-ray ground-reflection model (Line-of Sight and ground-reflected propagation) between the transmitters and the receivers and study the path loss impact on the CACC system's functionality [9], [10]. Furthermore, with the assumption of two-ray ground-reflection model for the wireless channel, we study the string stability of the CACC system under a mobile reactive jamming attack. The attacker jams the wireless channel established among the vehicles in order to prevent the receivers from decoding the transmitted packet with the purpose of destabilizing the platoon. If the attacker is successful to jam the packet, the CACC system will not work on the normal status until the next packet is received successfully. We evaluate the jamming attack impact on the string stability by employing the time-domain definition of string stability.

We compare the string stability of two basic cases: CACC with memory and memoryless. In the case with memory, the follower vehicle remembers the last successfully received acceleration information from the immediate preceding vehicle and feeds it to the feed-forward controller. In the memoryless case, whenever the acceleration information is lost due to jamming or channel fading, the following vehicle just assumes it is zero (the preceding vehicle maintains the same velocity).

Finally, by employing string stability criteria, we aim to find the best locations for the attacker to launch jamming attacks. Along the string, we examine the possible attacking locations at which the attacker can destabilize the platoon.

We summarize the contributions of this paper as follows:

- We study the path loss and ground-reflected signal effects on the CACC performance by modeling the wireless channel as a two-ray ground-reflected propagation.
- We consider a mobile reactive jamming attack on the wireless channels and investigate the impact of jamming attack on the CACC functionality for the two cases of CACC with and without memory.

- We examine the attacker's possible locations along the string at which it can destabilize the string.
- We conduct extensive simulations to analyze the string stability by utilizing its time-domain definition.

Our simulation results show that the CACC based platoon system is highly sensitive to jamming attacks and its performance can be compromised by a reactive jammer. In addition, we identify that the location being close to the second vehicle following the lead vehicle is the best location for the mobile jamming attacker to destabilize the platoon.

II. Related Work

Existing works [2], [3], [11] consider normal operation of CACC system without any possibility of the packet loss due to wireless channel condition or outsider attacker. Therefore, the frequency response of the system is derivable in these cases and the string stability can be analyzed in a fairly nice format in the frequency-domain. Necessary and sufficient conditions for string stability of a heterogeneous platoon are studied by Naus et al. [2]. Network delay and sampling effects are introduced in the string stability analysis in [3]. The delay is assumed identical in all the communication links and string stability is investigated based on different sampling interval and headway-time. In [7], the robustness of a CACC system to communication delays is studied and an upper bound on the delay is derived such that the string maintains its stability. However, the impact of distance variation between vehicles on the channel conditions is not considered in the aforementioned works.

There are few works focusing on the security of vehicle platooning in terms of attacking on wireless communication or control components. In [12], an insider attacker attacks on controller gains of a vehicle in the platoon. The attacker has the capability of modifying the gains such that it can destabilize the platoon. In [13], mass-spring-damper follower dynamics model is considered for studying the platoon performance under attack. The new class of the attack proposed in this paper is based on vehicle misbehavior. This work shows that the attacker is effective when the attacker is near the rear of the platoon. However, this work is different from our work in terms of platoon modeling, attacker's nature, the purpose of the attacker and the evaluation method employed to measure the impact of the attack. In another work [5], various security vulnerabilities on the CACC system have been identified. Message falsification and radio jamming attack's effects are studied through Vehicular Network Open Simulator. However, the CACC control structure and jamming attacking strategies are considered as a black box in the simulation environments. The coupling between the system state and wireless communication channel condition is not well modeled.

III. System Model

We consider a platoon of multiple vehicles. Each vehicle has a direct communication with its immediately following and preceding vehicle using Dedicated Short Range Communication (DSRC) technology. There is a mobile jammer (e.g., a drone), attacking on the wireless communication channel among the vehicles.

A. Vehicle String

We consider a platoon of vehicles consisting of n homogenous vehicles (identical longitudinal dynamic properties) shown in Fig 1. Each vehicle is equipped with a CACC system. In other words, each vehicle is equipped with a radar in front of the vehicle to measure the absolute relative distance from the vehicle ahead of it and a DSRC technique to transmit its acceleration information to its following vehicle.

B. Wireless Channel

Each vehicle in the platoon is equipped with DSRC system based on which acceleration information of each vehicle is sent every 100ms to the following vehicle. DSRC operates in the spectrum frequency of 75MHz in the 5.9 GHz band. For the wireless channel, we assume it is subject to Additive White Gaussian Noise (AWGN). We consider a two-ray propagation channel model, Line-Of-Sight (LOS) and ground-reflected wave propagation model [10]. By this modeling, we will be able to consider ground-reflected ray effect in addition to free space path loss impact on the received-signal-strength (RSS).

C. Attacker

We consider a mobile jamming attacker. The jammer is mounted on a drone flying over the platoon. Since the power source of the drone is limited, we assume a reactive jammer [14]. Reactive jammer has the capability of sensing channels and launching its jamming signal whenever the vehicles transmit their acceleration information through the wireless medium to their immediately following vehicles. All legitimate established wireless links among each pair of transmitters and receivers in the platoon are under jamming attack.

IV. Problem Formulation

A. Longitudinal Vehicle Dynamics

The common linearized third-order state space representation used for modeling longitudinal vehicle dynamics is as follows [3]:

$$\dot{q}_i(t) = v_i(t), \quad \dot{v}_i(t) = a_i(t), \quad \dot{a}_i(t) = -\eta_i^{-1} + \eta_i^{-1} u_i(t) \tag{1}$$

Where $q_i(t)$, $v_i(t)$ and $a_i(t)$ are absolute position, velocity and acceleration of the ith vehicle, respectively. η_i and $u_i(t)$ represent the internal actuator dynamics and the commanded acceleration, respectively. The transfer function of the longitudinal vehicle dynamics $G_i(s)$ is derived as follows:

$$G_i(s) = \frac{Q_i(s)}{U_i(s)} = \frac{1}{s^2(\eta_i s + 1)} \tag{2}$$

Where $Q_i(s) = \mathcal{L}(q_i(t))$ and $U_i(s) = \mathcal{L}(u_i(t))$ represent the Laplace transformation of the absolute position and the commanded acceleration for the ith vehicle, respectively.

B. CACC Control Structure and State Space Representation

The structure of a CACC system is shown in Fig. 2. In this model, $H_i(s) = 1 + h_d s$ represents the spacing policy dynamics. Headway-time constant, h_d, indicates the time that it takes vehicle i to arrive at the same position as its preceding vehicle $(i-1)$. Several spacing policies have been studied

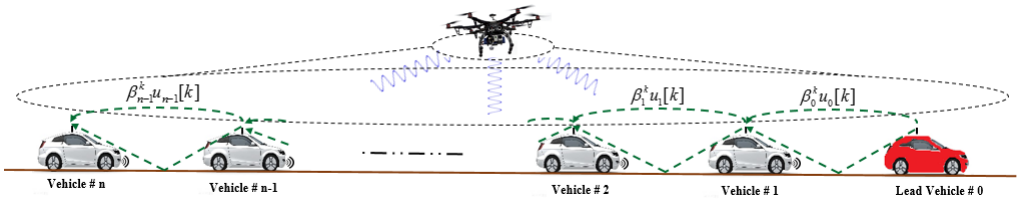


Figure 1: Vehicle Platoon Under Mobile Jamming Attacker

in the literature [2]. The spacing policy considered in this paper is based on the velocity-dependent spacing policy [2]. That is, the distance between the two vehicles increases if the velocity of the preceding vehicle increases, and vice versa. The string stability requirement is highly influenced by the value of headway-time h_d; as a result this parameter plays a crucial role in operating a safe and efficient CACC system.

In this structure, $K_i(s) = k_{pi} + k_{di}s$ is a feedback (PD) controller where k_{di} is the bandwidth of the controller and is chosen such that $k_{di} << 1/\eta_i$ [3]. The PD controller parameters k_{pi} and k_{di} are set up in such a way that the internal stability of the vehicle dynamics is satisfied. In [2], the feed-forward controller $F_i(s) = (H_i(s)G_i(s)s^2)^{-1}$ has been designed such that the zero steady state spacing error ($e_i(t) = 0$ as $t \to \infty$) is achievable. $u_{b,i}$ and $u_{f,i}$ also represent the controllers' output, respectively. The summation of these two outputs provide the commanded acceleration u_i for the ith vehicle.

Considering velocity-dependent spacing policy, the desired distance is defined as $h_d v_i(t)$. Therefore, spacing error, $e_i(t)$, at each time instant t can be determined by the difference between the actual relative distance, $q_{i-1}(t) - q_i(t)$, measured by the radar, and the desired distance, $h_d v_i(t)$, as follows:

$$e_i(t) = q_{i-1}(t) - q_i(t) - h_d v_i(t) \tag{3}$$

State space representation of the CACC control structure in Fig. 2 of the ith vehicle is given as follows [3]:

$$\begin{aligned} \dot{e}_i(t) &= v_{i-1}(t) - v_i(t) - h_d a_i(t) \\ \dot{v}_i(t) &= a_i(t) \\ \dot{a}_i(t) &= -\eta_i^{-1} a_i(t) + \eta_i^{-1} u_i(t) \\ \dot{u}_{f,i}(t) &= -h_d^{-1} u_{f,i}(t) + h_d^{-1} \tilde{u}_{i-1}(t) \end{aligned} \tag{4}$$

The acceleration of the $(i-1)$th vehicle, $u_{i-1}(t)$, is transmitted through the established wireless channel to the ith vehicle. The received acceleration information is denoted by $\tilde{u}_{i-1}(t)$ at the receiver of the following vehicle, i. From (4) we see that the output of the feed-forward controller, $u_{f,i}(t)$, depends on the received acceleration, $\tilde{u}_{i-1}(t)$, of the $(i-1)$th vehicle. For simplicity, we omit the continuous-time domain representation t in the remained article. By defining the state vector $x_i^T = [e_i \quad v_i \quad a_i \quad u_{f,i}]$, the state space variables are augmented in one variable and from (4) the continuous-time CACC vehicle dynamics is represented as follows:

$$\dot{x}_i = A_i x_i + A_{i-1} x_{i-1} + B_s u_i + B_c \tilde{u}_{i-1} \tag{5}$$

Due to limited space we refer the reader to [3] for the values of A_i, A_{i-1}, B_s, B_c matrices and vectors.

C. Vehicles String State Space Representation

The state space representation of the CACC control structure in a vehicle string is as follows [3]:

$$\dot{\bar{x}}_n = \bar{A}_n \bar{x}_n + \bar{B}_c \tilde{u}_{n-1} + \bar{B}_s u_l \tag{6}$$

Where $\dot{\bar{x}}_n = [x_1^T \quad x_2^T \quad ... \quad x_n^T]^T$ represents the augmented state space variables of the vehicles in the string. $\tilde{u}_{n-1} = [\tilde{u}_0 \quad \tilde{u}_1 \quad ... \quad \tilde{u}_{n-1}]^T$ is a vector where its elements denote the received acceleration information of the associated vehicle in its immediately following vehicle and u_l is an arbitrary commanded acceleration taken by the lead vehicle. The time-invariant matrices $\bar{A}_n$, $\bar{B}_c$ and $\bar{B}_s$ with constant entities can be found in [3]. Now we drive the discrete-time representation for the continuous-time system in (6) as follows:

$$\begin{aligned} x_n[k+1] &= \mathbf{A_n} x_n[k] + \mathbf{B_c} \tilde{u}_{n-1}[k] + \mathbf{B_s} u_l[k] \\ \mathbf{A_n} = e^{\bar{A}_n h}, \mathbf{B_s} &= \int_0^h e^{\bar{A}_n \nu} d\nu . \bar{B}_s, \mathbf{B_c} = \int_0^h e^{\bar{A}_n \nu} d\nu . \bar{B}_c \end{aligned} \tag{7}$$

Where h is the sampling interval.

D. String Stability

The lead vehicle's acceleration and deceleration will produce spacing error e_i between each pair of vehicles in the the platoon. String stability requires spacing error attenuation along the vehicle string. This can be shown as follows [7]:

$$\|e_n\|_\infty < \|e_{n-1}\|_\infty < ... < \|e_2\|_\infty < \|e_1\|_\infty \tag{8}$$

Hence, the time domain definition of the string stability will be:

$$\begin{aligned} \max_t |e_n(t)| < \max_t |e_{n-1}(t)| < ... \\ ... < \max_t |e_2(t)| < \max_t |e_1(t)| \end{aligned} \tag{9}$$

When the transfer function of CACC system is drivable, the string stability is evaluated by the frequency domain definition and string will be stable if the following condition is satisfied [2]:

$$|\Gamma(j\omega)| = \left| \frac{E_i(j\omega)}{E_{i-1}(j\omega)} \right| \leq 1 \quad \forall \omega, \quad i = 1, ..., n \tag{10}$$

In the next section, we will incorporate jamming attack and wireless channel condition effects to the equation (7) in order to analyze the string stability.

V. Jamming Attack on CACC

A. Wireless Channel and Attack Impact

Considering two-ray channel modeling, received signal's signal-to-noise ratio (SNR) alters as the vehicle's distance varies with the preceding vehicle. Moreover, the SNR drops dramatically at some distances due to the carrier phases cancellation of the two paths (LOS and ground-reflected) signal. Consequentially, the SNR level attenuation due to LOS path loss and signal cancellation due to opposite carrier phases received from two paths, affect the successful packet delivery ratio (PDR) in the long run and degrade the performance of the CACC system.

A reactive jammer mounted on a drone flying over the platoon emits its jamming signal over the wireless network whenever it senses that the communication traffic is happening in the network. Due to the stochastic nature of the noise and jamming signals' effect in the channel, the attacker's success is probabilistic at time k in each link between a pair of vehicles in the platoon. We consider a signal to interference plus noise ratio (SINR) model to derive the probability of successful packet delivery. In this model, the jamming signal is considered as the interference signal.

We determine vector $p^k = [p_0^k \quad p_1^k \quad ... \quad p_{n-1}^k]^T$ such that p_{i-1}^k, $i = 1, ..., n$, denotes the probability of successful packet delivery of the $(i-1)$th vehicle at the ith vehicle's receiver at time k. Thus, the PDR is defined as follows:

$$p_{i-1}^k = \mathbf{P}\left(\frac{P_t}{L_p(d_{i-1}^k)(N_0 + I)} \geq SINR_0\right) \quad i = 1, ..., n \tag{11}$$

Where $\mathbf{P}$ denotes the probability. P_t and N_0 are the signal and noise powers, respectively. I denotes the jamming signal power and $SINR_0$ represents some constant threshold. d_{i-1}^k denotes the actual distance between ith vehicle and its preceding vehicle $(i-1)$th at discrete time k. $L_p(d_{i-1}^k)$ indicates the path-loss value at a given distance and time.

Now, we define a Bernoulli random variable β_{i-1}^k to indicate the packet successful delivery which is defined as follows.

$$\beta_{i-1}^k = \begin{cases} 1, & p_{i-1}^k \\ 0, & 1 - p_{i-1}^k \end{cases} \tag{12}$$

For $k = 1, 2, ...$ and $i = 1, 2, ..., n$. Vector $\beta^k = [\beta_0^k \quad \beta_1^k \quad ... \quad \beta_{n-1}^k]^T$ shows the random variables of successful packet delivery among each pair of vehicles at time k and the vector $p^k = [p_0^k \quad p_1^k \quad ...p_{n-1}^k]^T$ indicates the corresponding probabilities.

B. Memory Block

To comply with the DSRC standard protocol, the preceding vehicle's acceleration information, u_{i-1} is sampled with sampling time $t_k = kh$ where $k = 1, 2, ...$and $h = 100$ms, Fig 2. These information, $u_{i-1}[k]$, for $k = 1, 2, ...$ in the form of packets are sent over a wireless channel to the following vehicle, i. As the packets are transmitted through the channel, they are subject to the channel condition and jamming attack impact. To show this, the vector $\beta^k = [\beta_0^k \quad \beta_1^k \quad ... \quad \beta_{n-1}^k]^T$

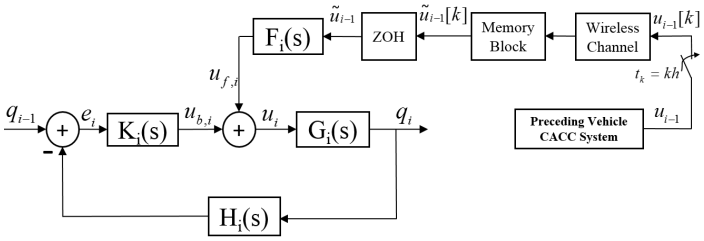


Figure 2: CACC Control Structure with Memory and ZOH

which has been determined in (12) as a Bernoulli random variable is multiplied by the transmitted information. Then at the output of the wireless channel we will have $\beta_{i-1}^k u_{i-1}[k]$. Now before feeding the received information to the feed-forward controller, we use a memory block in the following vehicle's CACC control structure, Fig 2. The low-cost memory has the capacity for saving only one packet information. Each time if the memory receives the packet successfully, it updates the memory, otherwise it keeps the last successful received information in the memory. The following model shows how the feed-forward controller uses the stored information in the memory as its input:

$$\tilde{u}_{i-1}[k] = \beta_{i-1}^k u_{i-1}[k] + (1 - \beta_{i-1}^k)\tilde{u}_{i-1}[k-1] \tag{13}$$

For $i = 1, 2, ..., n$ where $\tilde{u}_{i-1}[k]$ is the received acceleration of the $i-1$th vehicle at the receiver of ith vehicle, subject to the jamming attack and wireless channel condition impact at time k. As it can be realized, in case of successful packet reception $(\beta_{i-1}^k = 1)$, the output of the memory block will be $u_{i-1}[k]$. However, if the packet is jammed successfully or dropped due to path loss or ground-reflected signal effect $(\beta_{i-1}^k = 0)$, the output of the memory block will be the last successful received packet $\tilde{u}_{i-1}[k-1]$. Then we use ZOH (Zero Order Holder) to convert the discrete-time signal $\tilde{u}_{i-1}[k]$ to the continuous-time signal $\tilde{u}_{i-1}$ which will be fed into the feed-forward controller $F_i(s)$ shown in Fig 2. Now we substitute (13) in (7) to obtain the string state space representation of the platoon under reactive jamming attack and wireless channel condition impact. Then we have

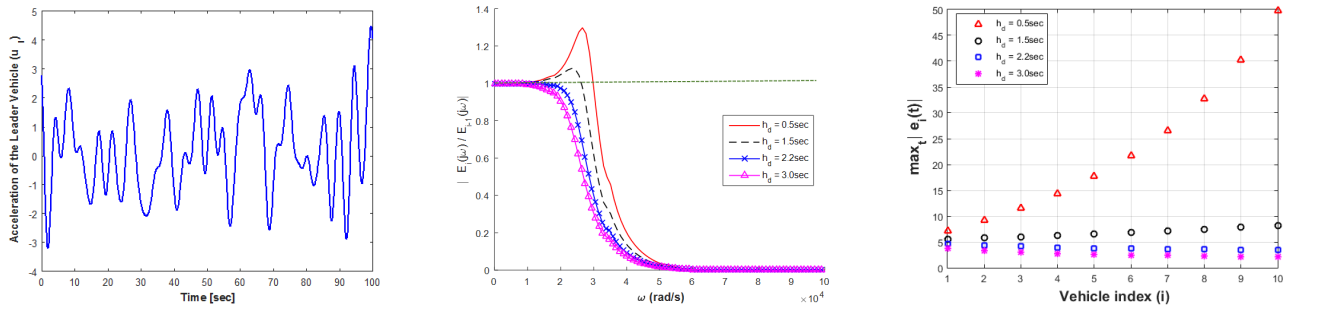
$$\begin{aligned} x_n[k+1] = \mathbf{A_n} x_n[k] + \mathbf{B_c}\beta_{n-1}^k u_{n-1}[k] \\ + \mathbf{B_c}(1 - \beta_{n-1}^k)\tilde{u}_{n-1}[k-1] + \mathbf{B_s} u_l[k] \end{aligned} \tag{14}$$

In order to analyze the string stability in the frequency-domain using $\Gamma(j\omega)$ in (10), the string state space equation needs to be deterministic. However, due to the presence of stochastic variable β_{i-1}^k in (14), the derived string state space is probabilistic at each given time k. Therefore, we adapt the time-domain definition of string stability for analyzing the string state space equation derived in (14), discussed in the next section.

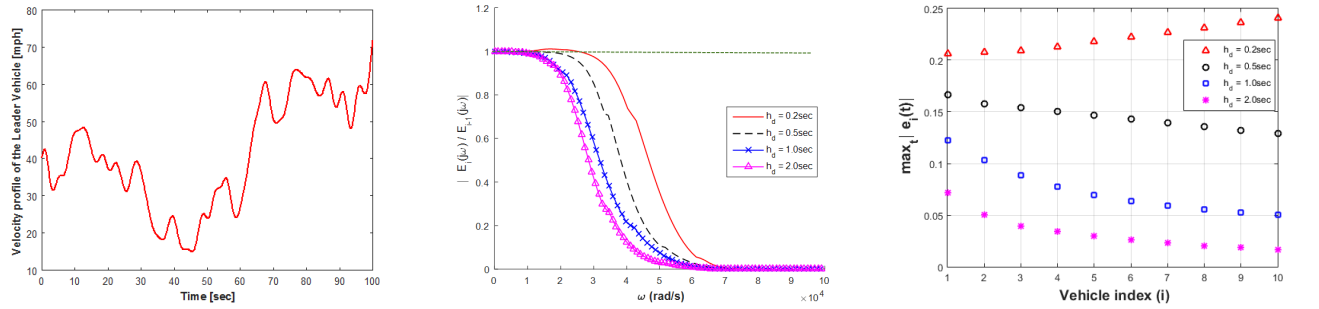
VI. String Stability Analysis

A. Simulation Setting

We consider a platoon constructed with $n = 11$ vehicles. The lead vehicle's index is zero and the rest of the vehicles are ordered from one to ten moving down the platoon. We assume that the vehicles are homogenous and the internal



(a) A sample lead vehicle's acceleration profile (b) Frequency-domain string stability for ACC mode (c) Time-domain string stability for ACC mode



(d) A sample lead vehicle's velocity profile (e) Frequency-domain string stability for CACC mode (f) Time-domain string stability for CACC mode

Figure 3: Simulation results I

actuator dynamics are identical for all vehicles in the platoon ($\eta_i = \eta = 0.1$ for $i = 1, 2, ..., n$). $k_{di} = k_d = 0.5 << 1/\eta$ and $k_{pi} = k_p = k_d^2 = 0.5$ for $i = 1, ..., n$ are chosen to satisfy the internal stability of the vehicle dynamics. We generate $1,000$ acceleration profiles using the random phase multi-sine signal generation method [15]. These acceleration profiles model the lead vehicle's real-world actions. One sample of lead vehicle's acceleration and the corresponding velocity profile up to 100 seconds are shown in Fig. 3(a) and 3(d), respectively. For each acceleration profile, we compute the maximum spacing error produced during 500 seconds at each vehicle. Then, we average over all the maximum errors of each vehicle to find the average maximum errors of each vehicle. We also assume that the signal transmission power for all vehicles is fixed and identical all the time for all scenarios. The mobile jammer's vertical distance from the horizontal platoon and its jamming signal power is also fixed all the time for all scenarios.

B. Validity of Time-Domain String Stability Analysis

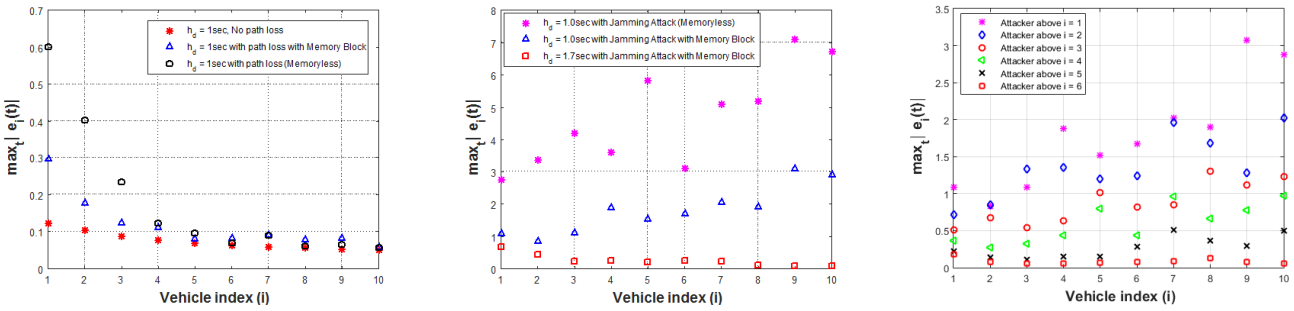
Existing string stability analysis are based on frequency-domain techniques. For our modeling in (14), this method cannot be applied because of time-varying probabilistic packet successful delivery at each receiver in the platoon. In order to tackle this challenge, for the first time, we analyze the time-domain string stability under a mobile jamming attacker. We validate our analysis through comparing frequency-domain and time-domain approaches for the case of perfect channel condition, no attack and normal operation of the platoon. Figures 3(b) and 3(c) illustrate the string stability analysis of ACC (CACC without V2V communication) systems in the frequency and time domains, respectively. By comparing the figures, we observe that in both domains for the headway-time 0.5 seconds and 1.5 seconds string is unstable. However, string is stable when the headway-time is set to 2.2 seconds and 3 seconds. Also, for CACC systems, Figures 3(e) and 3(f) show that in both domains for the headway-time 0.2 seconds string is unstable. However, for the headway-time 0.5 seconds, 1 second and 2 seconds string is stable. As a result, string stability analysis of both frequency-domain and time-domain are highly consistent and endorse each other.

C. Two-ray Channel Modeling Impact and No Attack

We consider a two-ray propagation model for the wireless channels among the vehicles. We assume if the received signal's SNR is below the threshold $SNR_0 = 20dB$, the packet is dropped, otherwise it is decoded successfully being fed into the feed-forward controller. We investigate channels' condition impact by examining string stability with and without utilizing the memory block. In case of memoryless (without the memory block), if the packet gets lost, the vehicle considers its preceding vehicle maintains the same velocity (zero acceleration). Figure 4(a) illustrates that overall the path loss degrades the performance of CACC by incrementing the magnitude of the spacing error. But the CACC controllers can prevent those errors from getting amplified upstream, thus still maintain the string stability.

D. Jamming Attack Impact

We consider a jammer above the second vehicle ($i = 1$) with a constant vertical distance from it. The jammer emits its signal over the platoon wireless ad-hoc network when it senses communication traffic. Fig. 4(b) shows the capability of



(a) Two-ray channel modeling impact on string stability (b) Jamming attack impact on string stability with memory block and different headway-time (c) Attacker's location impact on string stability

Figure 4: Simulation results II

the reactive attacker to destabilize the platoon. However, when the memory block is utilized, the magnitude of the propagated error is reduced, although the string is still unstable. From Fig. 4(b), it can also be observed that the error in the presence of the attacker does not propagate upstream the string, if the headway-time is increased from 1 second to 1.7 seconds. Note that as illustrated in Fig. 3(c), for the ACC mode the minimum headway-time to have a stable string is 2.2 seconds, however the string under attack is stable for the headway-time 1.7 seconds in the CACC mode with memory block.

E. Attacker's Location Impact on String Stability

We assume the head-way time is fixed to 1 second and the memory block is used in the control structure. As Fig. 4(c) shows, when the attacker is above the second vehicle ($i = 1$), not only the error propagates upstream the string, but also the magnitude of errors are high in comparison to the no attack scenarios Fig. 3(f). Also, in Fig. 4(c), we show that as the attacker moves toward down in the platoon, its ability to destabilize the platoon is diminished. This is because as the attacker goes far away from the lead vehicle, the produced spacing error magnitude for the front vehicles are decreased since the packet delivery ratio is increased. As a result, as the attacker goes away from the lead vehicle the more spacing error is corrected by the CACC controllers such that when the attacker is above the sixth vehicle in the platoon the string becomes stable. As a result the more the attacker is close to the lead vehicle the more effective it will be in terms of destabilizing the platoon. Therefore, we conclude that the best location for the attacker to launch its jamming signal is above the second vehicle ($i = 1$).

VII. Conclusions

In this paper, we studied the string stability of interconnected vehicles equipped with CACC systems under two-ray propagation model for the channel and mobile jamming attacker. We incorporated channel condition and jamming attack impact on the string state space representation and analyzed string stability through extensive simulations. We show that signal's power attenuation due to two-ray path loss model degrades the performance of the CACC system. Also, the analysis indicates that jamming attack can adversely destabilize the string. However, by increasing the headway-time and using the memory block, the stability can be improved. Finally, we discovered that the best possible location for the attacker to destabilize the string is above the second vehicle and as the attacker moves down in the string, its impact in terms of destabilizing the platoon is diminished.

References

[1] D. B. Rawat, C. Bajracharya, and G. Yan. Towards intelligent transportation cyber-physical systems: Real-time computing and communications perspectives. In *SoutheastCon 2015*, pages 1–6, April 2015.

[2] G. J. L. Naus, R. P. A. Vugts, J. Ploeg, M. J. G. van de Molengraft, and M. Steinbuch. String-stable cacc design and experimental validation: A frequency-domain approach. *IEEE Transactions on Vehicular Technology*, 59(9):4268–4279, Nov 2010.

[3] S. Öncü, J. Ploeg, N. van de Wouw, and H. Nijmeijer. Cooperative adaptive cruise control: Network-aware analysis of string stability. *IEEE Transactions on ITS*, 15(4):1527–1537, 2014.

[4] J. Ma, F. Zhou, and M. J. Demetsky. Evaluating mobility and sustainability benefits of cooperative adaptive cruise control using agent-based modeling approach. In *Systems and Information Design Symposium (SIEDS), 2012 IEEE*, pages 74–78, April 2012.

[5] M. Amoozadeh, A. Raghuramu, C. n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, June 2015.

[6] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura. Cooperative adaptive cruise control in real traffic situations. *IEEE Transactions on ITS*, 15(1):296–305, Feb 2014.

[7] Xiangheng Liu, A. Goldsmith, S. S. Mahal, and J. K. Hedrick. Effects of communication delay on string stability in vehicle platoons. In *Intelligent Transportation Systems, IEEE*, pages 625–630, 2001.

[8] J. Ploeg, D. P. Shukla, N. van de Wouw, and H. Nijmeijer. Controller synthesis for string stability of vehicle platoons. *IEEE Transactions on Intelligent Transportation Systems*, 15(2):854–865, April 2014.

[9] C. Sommer, S. Joerer, and F. Dressler. On the applicability of two-ray path loss models for vehicular network simulation. In *Vehicular Networking Conference (VNC), 2012 IEEE*, pages 64–69, Nov 2012.

[10] J.W. Mark and W. Zhuang. *Wireless Communications and Networking*. Prentice Hall, 2003.

[11] E. Shaw and J. K. Hedrick. String stability analysis for heterogeneous vehicle strings. In *2007 American Control Conference (ACC)*.

[12] Soodeh Dadras, Ryan M. Gerdes, and Rajnikant Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, pages 167–178, New York, NY, USA, 2015.

[13] Ryan M. Gerdes, Chris Winstead, and Kevin Heaslip. Cps: An efficiency-motivated attack against autonomous vehicular transportation. In *Proceedings of the 29th*, ACSAC '13, pages 99–108, New York, NY, USA, 2013. ACM.

[14] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on MobiHoc*, MobiHoc '05, pages 46–57, NY, USA, 2005. ACM.

[15] Jarosław Figwer. Multisine transformation — properties and applications. *Nonlinear Dynamics*, 35(4):331–346, 2004.