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 realistic lead vehicle’s acceleration profiles. We suggest a simple estimator embedded in the CACC control model to mitigate the impact of jamming attacks. We utilize time-domain definition of string stability to delineate the impact of the jamming attacks and the estimator performance on the CACC system functionality and string stability. We also discover 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 operate 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 its preceding vehicle with safety guarantee. In addition, this technology reduces fuel consumption and provides more comfort for 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 behaviors and spacing policy [6]. This variation in inter-vehicle distance affects the wireless channel conditions which further affects received-signal-strength 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 CACC systems 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 power-constrained 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.

To mitigate the jamming attacks’ impact and channel condition impairments on the CACC system, we suggest a simple and low cost estimator embedded in the CACC control structure. In this case, the results of the string stability evaluation show that the estimator impedes the performance degradation of the string stability, making the CACC system jamming resilient to some degrees.

Finally, by employing string stability criteria, we aim to find the best locations for the attacker to launch jamming attacks. Along the string, we discover 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 power-constrained reactive jamming attack on the wireless channels and investigate the impact of jamming attack on the CACC functionality.
• We suggest using a simple, low cost and efficient estimator embedded in the control framework of CACC to mitigate the jamming attack impact on the CACC performance.
• We discover 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. We also show that incorporating a simple and efficient estimator mitigates the jamming attack impact and the stability of the string becomes more resilient to the attack. 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 (vehicles with different longitudinal dynamics) 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 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 [13], [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 [3] is as follows:

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

(1)

Where \( q_i(t), v_i(t) \) and \( a_i(t) \) are absolute position, velocity and acceleration of the \( i \)th vehicle, respectively. \( \eta_i \) 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:

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

(2)

Where \( Q_i(s) = L(q_i(t)) \) and \( U_i(s) = L(u_i(t)) \) represent the Laplace transformation of absolute position and commanded acceleration for the \( i \)th vehicle, respectively.

B. CACC Control Structure and State Space Representation

The structure of a CACC system is shown in Fig. 2. In this model, \( H_i(s) = 1 + h_{idt} \) represents the spacing policy dynamics. Headway-time constant, \( h_{i dt} \), 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.
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 $h_d$ and 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. $u_{f,i}$ and $u_{f,i}$ also represent the controllers’ output, respectively. The summation of these two outputs provide the commanded acceleration $u_i$ for the $i^{th}$ vehicle.

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

$$e_i(t) = q_i(t) - q_i(t) - h_d a_i(t)$$

State space representation of the CACC control structure in Fig. 2 of the $i^{th}$ vehicle is given in [3] as follows:

$$\dot{e}_i(t) = v_{i-1}(t) - v_i(t) - h_d a_i(t)$$

$$\dot{v}_i(t) = a_i(t)$$

$$\dot{a}_i(t) = -\eta_i^{-1} a_i(t) + \eta_i^{-1} u_i(t)$$

$$\dot{u}_{f,i}(t) = -h_d^{-1} u_{f,i}(t) + h_d^{-1} \dot{u}_{i-1}(t)$$

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

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

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]:

$$\dot{x}_n = \tilde{A}_n x_n + \tilde{B}_c \tilde{u}_{n-1} + \tilde{B}_s u_t$$

Where $\dot{x}_n = [x_0^T \ x_1^T \ ... \ x_n^T]^T$ represents the augmented state space variables of the vehicles in the string. $\tilde{u}_{n-1} = [\tilde{u}_1 \ \tilde{u}_2 \ ... \ \tilde{u}_n]^T$ is a vector where its elements denote the received acceleration information of the associated vehicle in its immediately following vehicle and $u_t$ is an arbitrary commanded acceleration taken by the lead vehicle. The time-invariant matrices $\tilde{A}_n$, $\tilde{B}_c$ and $\tilde{B}_s$ with constant entities can be found in [3]. Now we drive the discrete-time representation for the continuous-time system in (6) as follows:

$$x_n[k + 1] = A_n x_n[k] + B_c \tilde{u}_{n-1}[k] + B_s u_t[k]$$

$$A_n = e^{\tilde{A}_n h}, B_c = \int_0^h e^{\tilde{A}_n \nu} d\nu \tilde{B}_c, B_s = \int_0^h e^{\tilde{A}_n \nu} d\nu \tilde{B}_s$$

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 platoon. String stability requires spacing error attenuation along the vehicle string. This can be shown as follows [7]:

$$\|e_n\| \leq \|e_{n-1}\| \leq \ ... \leq \|e_2\| \leq \|e_1\|$$

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

$$\max_t |e_n(t)| \leq \max_t |e_{n-1}(t)| \leq \ ... \ \leq \ \max_t |e_2(t)| \leq \max_t |e_1(t)|$$

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]:

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

When string state space equations are not deterministic in time domain, the exact transfer function of $\Gamma(j\omega)$ is not derivable and as a result string stability cannot be analyzed using (10). We perform time-domain definition for analyzing the string stability under reactive jamming attacks. 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. PROPOSED JAMMING ATTACK STRATEGY AND ESTIMATOR

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. Consequently, 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 in the long run and degrade the performance of the CACC system. We define an indicator function $\alpha_i^k$ to represent this phenomena in terms of successful packet delivery or loss as follows:

$$\alpha_i^k = I\left(\frac{P_i}{L_p(d_i^k)N_0} \geq SNR_0\right) = \begin{cases} 1, & \frac{P_i}{L_p(d_i^k)N_0} \geq SNR_0 \\ 0, & \text{Otherwise} \end{cases}$$ (11)

Where $i$ indicates the index of the vehicle, $P_i$ and $N_0$ are the signal and noise powers, respectively, $SNR_0$ represents some constant threshold. $d_i^k$ denotes the actual distance between $i$th vehicle and its preceding vehicle $(i - 1)$ at discrete time $k$. $L_p(d_i^k)$ indicates the path-loss value at a given distance and time.

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 noise effect, the attacker’s success at time $k$ in each link between a pair of vehicles in the platoon is probabilistic. The successful attack probability is time variable and at each time is dependent on the attacker’s distance from each link and the noise power at the receiver. Thus, we decide vector $p_i^k = [p_1^k, p_2^k, ..., p_n^k]^T$ such that $p_i^k$ denotes the probability of successful packet delivery of the $i$th vehicle at the $(i - 1)$th vehicle’s receiver at time $k$ if the channel condition is perfect (No path loss effect and No ground-reflection). Now we incorporate the jamming attack and wireless channel condition impairments by defining a vector which its elements are Bernoulli random variables as $\beta_i^k = [\beta_1^k, \beta_2^k, ..., \beta_n^k]^T$ with success probabilities of $p_i^k = [p_1^k, p_2^k, ..., p_n^k]^T$ representing as follows:

$$\beta_i^k = \begin{cases} \alpha_i^k, & p_i^k \\ 0, & 1 - p_i^k \end{cases}$$ (12)

For $i = 1, 2, ..., n$ and $k = 1, 2, ..., n$ in (12).

B. Estimator

To comply with the DSRC standard protocol, the preceding vehicle’s desired acceleration information $u_{i-1}$ is sampled with sampling time $t_k = kh$ where $k = 1, 2, ..., h = 100ms$ 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 $\beta_i^k = [\beta_1^k, \beta_2^k, ..., \beta_n^k]^T$ 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 $\beta_i^k u_{i-1}[k]$.

Now before feeding the received information to the feed-forward controller, we suggest using a simple and profitable but effective estimator Fig 2. The output of the estimator is determined as follows:

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

For $i = 1, 2, ..., n$ where $\tilde{u}_{i-1}[k]$ is the received desired acceleration of the $i$th vehicle at the receiver of $i$th vehicle, subject to the jamming attack and wireless channel condition impact at time $k$. As it can be realized, in case of successful packet received ($\beta_i^k = 1$), the output of the estimator will be $u_{i-1}$[k]. However, if the packet is jammed successfully or dropped ($\beta_i^k = 0$) because of path loss or ground-reflected signal effect, the output of the estimator will be the previous received packet $\tilde{u}_{i-1}[k - 1]$. The estimator has a memory that can keep the last successful received packet information to use in case of packet loss. 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 $F_1(s)$ 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

$$x_n[k + 1] = A_n x_n[k] + B_c (\beta_{n-1} u_{n-1}[k])$$

+ $B_c (1 - \beta_{n-1}) u_{n-1}[k - 1] + B_u u_t[k]$ (14)

$$= A_n x[k] + B_c \beta_{n-1} u_{n-1}[k]$$

+ $(B_c - B_c \beta_{n-1}) u_{n-1}[k - 1] + B_u u_t[k]$ (14)

In the next section, we will analyze the string stability under a reactive mobile jammer based on the derived state space representation of the string under attacks in (14).

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 actuator dynamics are identical for all vehicles in the platoon ($\eta_i = \eta = 0.1$ for $i = 1, 2, ..., n$). $k_d = 0.5 < 1/\eta$ and $k_{ip} = k_{ip} = 0.5$ 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...
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. We consider a two-ray propagation model for the wireless channels among the vehicles. If the received signal’s SNR is below the threshold $SNR_0 = 20dB$, the packet is dropped ($\alpha_{ki} = 0$), otherwise it is decoded successfully ($\alpha_{ki} = 1$) being fed into the feed-forward controller. We investigate channels’ condition impact by examining string stability with and without utilizing the estimator. Without the estimator, 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 the reactive attacker to destabilize the platoon. However, when the estimator 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 second. Note that as illustrated in Fig. 3(c), for the ACC mode the minimum headway-time to have the string stable is 2.2 seconds, however the string under attack is stable for the headway-time 1.7 second using the estimator.

E. Attacker’s Location Impact on String Stability

We assume the head-way time is fixed to 1 second and the estimator is embedded in the control structure. We consider a mobile attacker to examine the attacker’s location impact on string stability. 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 cannot destabilize the string, although the CACC performance is degraded for some degrees. Also, the analysis indicates that jamming attack can adversely destabilize the string. However, by increasing the headway-time and using the estimator in the control structure of the CACC system, string can be maintained stable. 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