Vehicle Lateral Motion Dynamics Under Braking/ABS Cyber-Physical Attacks

Alireza Mohammadi*, Hafiz Malik*, and Masoud Abbaszadeh†
*University of Michigan–Dearborn
†GE Global Research

***Abstract*—In face of an increasing number of automotive cyber-physical threat scenarios, the issue of adversarial destabilization of the lateral motion of target vehicles through direct attacks on their steering systems has been extensively studied. A more subtle question is whether a cyberattacker can destabilize the target vehicle lateral motion through improper engagement of the vehicle brakes and/or anti-lock braking systems (ABS). Motivated by such a question, this paper investigates the impact of cyber-physical attacks that exploit the braking/ABS systems to adversely affect the lateral motion stability of the targeted vehicles. Using a hybrid physical/dynamic tire-road friction model, it is shown that if a braking system/ABS attacker manages to continuously vary the longitudinal slips of the wheels, they can violate the necessary conditions for asymptotic stability of the underlying linear time-varying (LTV) dynamics of the lateral motion. Furthermore, the minimal perturbations of the wheel longitudinal slips that result in lateral motion instability under fixed slip values are derived. Finally, a real-time algorithm for monitoring the lateral motion dynamics of vehicles against braking/ABS cyber-physical attacks is devised. This algorithm, which can be efficiently computed using the modest computational resources of automotive embedded processors, can be utilized along with other intrusion detection techniques to infer whether a vehicle braking system/ABS is experiencing a cyber-physical attack. Numerical simulations in the presence of realistic CAN bus delays, destabilizing slip value perturbations obtained from solving quadratic programs on an embedded ARM Cortex-M3 emulator, and side-wind gusts demonstrate the effectiveness of the proposed methodology.**

I. Introduction

The existence of communication network protocols such as CAN and FlexRay, which are an integral component of the modern automotive networked control systems, and the proliferation of connected vehicles, which facilitate vehicle-to-everything (V2X) communications, have revealed an ever-increasing horizon of automotive cyber-physical threat scenarios [1], [2]. Given the safety-critical nature of braking, there is no wonder that cybersecurity researchers are interested in demonstrating cyber-physical vulnerabilities of modern vehicles through design of various attacks against their braking and anti-lock braking systems (ABS) (see, e.g., the line of literature [3]–[9]) while analyzing the capabilities of an adversary who "has made it to the last stage" [10].

This work is supported by NSF Award CNS-2035770. A. Mohammadi and H. Malik are with the Department of Electrical and Computer Engineering, University of Michigan-Dearborn, MI 48127 USA. M. Abbaszadeh is with GE Global Research, NY 12309 USA. Emails: {amohmmad,hmalik}@umich.edu, abbaszadeh@ge.com. Corresponding Author: A. Mohammadi.

Figure 1 depicts several possible attack vectors through which the adversaries can launch their malicious activities against a target vehicle. In general, attacks against the vehicle braking systems and ABS fall within two broad categories. In the first category, adversaries target the physical components of the braking systems through external attack vectors against the physical layer. For instance, Shoukry *et al.* [4] executed an ABS attack by injection of spoofing magnetic fields through an electromagnetic actuator in a vicinity of the ABS sensor.

In the second category of attacks against the braking system and ABS, the attackers target the CAN and/or FlexRay communication systems of the vehicle and subsequently inject false brake/ABS messages onto the in-vehicle network (IVN) bus. Another possibility for an adversary who chooses to use these types of CAN bus attacks is to reprogram a target brake/ABS electronic control unit (ECU). For instance, in a series of celebrated white-hat attacks, Miller and Valasek [11] managed to reprogram V850 chips to disable the braking system of a class of Fiat-Chrysler vehicles (for other types of attacks that directly target the brake/ABS ECUs, see, e.g., [10]). Furthermore, as demonstrated by [6], a compromised brake/ABS ECU can be exploited for executing closed-loop attack policies against the vehicle longitudinal traction dynamics. Through a proper closed-loop attack policy, the authors have shown that the adversary can drive the states of the vehicle traction dynamics to a vicinity of the lockup manifold in a finite time despite possessing a limited knowledge of the tire-road interaction characteristics [6].

A less investigated aspect of the impact of cyber-physical attacks against the vehicle braking/ABS systems is destabilizing the vehicle lateral motion. A conventional way for adversarial destabilization of a target vehicle lateral motion is through direct attacks on its steering system. Indeed, Valasek and Miller (see, e.g., [11], [12]) managed to steer a 2014 Jeep Cherokee into a ditch by taking over its steering system while leaving almost no forensic evidence behind. Another notable hack against the active steering system is proposed by Nekouei *et al.* [13], where the gains of the vehicle steering closed-loop controller are inferred by infiltrating the vehicular ad-hoc network. Nevertheless, in all of these scenarios, it is through the direct adversarial manipulation of the steering input that the lateral motion becomes unstable.

Given the well-documented literature on attacks against ABS/braking systems [3]–[9], this paper investigates the following questions: (1) is it possible for a braking system/ABS

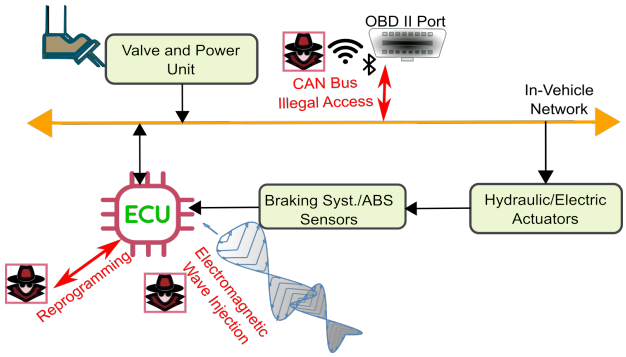


Fig. 1: Several possible vectors through which attacks can be executed against the braking system/ABS of the target vehicle.

attacker to induce lateral motion instability through varying the longitudinal slips of the wheels?; (2) what is the minimum amount of longitudinal slip perturbations that makes the lateral motion dynamics unstable?; and, (3) is it possible to devise an algorithm, which can be efficiently computed in real-time (preferably with the modest computational capabilities of a commercial ECU), for monitoring the lateral motion dynamics of the vehicles against potential braking system/ABS attacks?

To answer these three questions (see, also, Section II-A for the contributions of the paper), we demonstrate that if a braking system/ABS attacker manages to continuously vary the longitudinal slips of the wheels, they can violate certain conditions for asymptotic stability of an underlying LTV dynamical model that governs the vehicle lateral motion under small slip angles (Propositions 3, 4, and Corollary 6). Furthermore, we provide a distance-to-instability metric for the lateral dynamics with frozen-time eigenvalues and derive the minimal perturbations of the wheel longitudinal slips resulting in lateral motion instability under fixed slip values (Propositions 7, 8, and the quadratic programming (QP) problem formulated in (34)). Finally, we devise a real-time algorithm for monitoring the vehicle lateral dynamics against braking/ABS cyber-physical attacks (Algorithm 1 and Propositions 12 and 14). This algorithm monitors the vehicle lateral dynamics for potential unstable behavior due to time-varying longitudinal slip values under braking/ABS attacks and issues warning signals to higher-level supervisory modules for taking further actions. The algorithm, which can be run using the modest computational resources of commercial ECUs (through the closed-form solutions outlined in V-A1, V-A2, and V-A3), can be utilized along with other intrusion detection techniques (see, e.g., [14]) to infer an attack.

The rest of this paper is organized as follows. We first highlight *the contributions of this paper* in Section II-A. After reviewing some preliminaries about the vehicle dynamics and the impact of road/tire lateral forces using a hybrid physical/dynamic friction model, we present the resulting LTV dynamics under varying longitudinal slips in Section II-B. Next, in Section III, we present the conditions under which the adversary can violate certain conditions for asymptotic stability of the lateral motion. Thereafter, we find the minimal perturbations of the wheel longitudinal slip values that result in an unstable lateral motion under fixed slip conditions in Section IV. Afterwards, we present a real-time algorithm that can be used for monitoring the lateral motion of vehicles for inferring potential cyber-physical attacks on the vehicle braking systems/ABS in Section V. After presenting the simulations in Section VI and providing some further remarks and discussion about the scalability of the proposed approach in Section VII, we conclude this paper in Section VIII.

Notation. Given an integer N, we denote the identity matrix of size N by $\mathbf{I}_N$. Given a square matrix $\mathbf{A}$, we denote its trace and determinant by $\det(\mathbf{A})$ and $\mathrm{tr}(\mathbf{A})$, respectively. Additionally, we let $\mathrm{eig}(\mathbf{A})$ denote the collection of eigenvalues of $\mathbf{A}$. Given the integers m, n and the matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$, we denote the transpose of the matrix by $\mathbf{B}^\top$.

II. Literature Review and Preliminaries

In this section we first provide an outline of the paper contributions and its highlights with respect to the existing literature. Next, we review some preliminaries about the vehicle dynamics and the impact of road/tire lateral forces using a hybrid physical/dynamic friction model.

A. Contributions of the Paper

With respect to the vehicle dynamics and control literature, this work provides a formal analysis of the lateral motion stability under braking/ABS cyber-physical attacks in an adversarial setting where the longitudinal slip values of the wheels can change over time due to the adversary's exploitation of the braking/ABS systems. Remarkably, the interest within the traditional vehicle dynamics and control literature is in maximizing the traction forces and operating within a close vicinity of a constant reference friction coefficient (see, e.g., [15], [16]). Due to the emerging cyber-physical threat scenarios, there is a need to investigate the less-studied stability issues under time-varying longitudinal slip values with an emphasis on finding conditions that lead to instability.

The conditions of *linear time invariant (LTI) lateral motion instability* with *fixed* wheel longitudinal slip values have already been investigated in the line of work by Yi, Tseng, and collaborators (see, e.g., [17]–[19]). An extension of their work in [7] utilizes Mikhailov plots from the robust stability analysis literature to find the intervals on which the lateral motion stability with *fixed wheel longitudinal slip values* is guaranteed. This paper extends these previous results by extending the analysis to time-varying longitudinal slip values and computing minimally destabilizing longitudinal slip perturbations as outlined in what follows.

As another contribution, this article adds to the body of knowledge on cyber-physical attack generation in autonomous and connected vehicles. In particular, by utilizing the concept of the distance of a given stable LTI system from its nearest unstable dynamics of the same order (see, e.g., [20]–[22]), we provide a method for computing the minimal perturbations of the longitudinal slip values that result in lateral motion instability. These results are related to the body of literature on designing cyber-physical attacks where the intent of the adversary is to drive the targeted system to an unsafe operating region (see, e.g., [23]–[26]). Additionally, a majority of the previous cyber-physical attack generation literature has an

exclusive focus on plants with time-invariant dynamics. In contrast, our results focus on a *time-varying setting*, where we demonstrate that a braking system/ABS attacker, who manages to continuously vary the longitudinal slips of the wheels, can violate the necessary conditions for asymptotic stability of the underlying lateral motion LTV dynamics. One of the few similar results is due to Pessim and Lacerda [27], where feedback schemes for cyber-physical linear parameter varying systems under DoS attacks is designed.

There are a number of theoretical and practical challenges associated with monitoring the stability of LTV systems in real-time. The LTV dynamics stability results with the exception of few works such as [28], which are suitable for a real-time monitoring setting, are very scarce in the literature (see, [29]–[31] on some recent results about the stability of LTV dynamical systems). Furthermore, despite the existence of conclusive theories and abundance of tools for assessing the stability of LTI systems, investigating the properties of LTV systems is still an open quest (see, e.g., [29], [30] for some recent theoretical results and the earlier pioneering works by Rosenbrock [32], [33] and Desoer [34], respectively).

The underlying assumption of a majority of previous results in the LTV stability literature is completely knowing the state transition matrix as a function of time. However, possessing such a knowledge is not realistic when the adversary is manipulating the dynamics at his/her own will. Accordingly, the emerging automotive cyberthreat scenarios necessitate the development of *real-time monitoring tools* to infer whether a vehicle is undergoing a braking system/ABS attack.

By modifying the framework proposed by Mullhaupt *et al.* [28] in a way that is suitable for implementation in automotive embedded settings for the first time, we devise a real-time algorithm for monitoring the lateral motion dynamics against braking/ABS cyber-physical attacks. In particular, through *two extensions*, we are making the results of [28] applicable to real-time settings. First, since the numerical procedures in [28] rely on solving matrix Lyapunov equations and multivariable optimization problems as well as orthonormal diagonalization of real symmetric matrices, they are not suitable for implementation in embedded applications with modest computational resources. We provide closed-form solutions to the numerical subproblems that are needed for running the algorithm in real-time. Second, we provide a condition on the sampling times of the monitoring algorithm ensuring that the stability results of [28] can be invoked in a sampled-data setting.

B. Modeling

In this section we present a brief overview of the important kinematic relationships, the bicycle model for vehicle dynamics, the tire/road interaction forces under small slip conditions, and the resulting LTV dynamics under time-varying longitudinal slip profiles. We assume, without loss of generality, that the front wheel is braking while the rear wheel is in traction. The reader is referred to the respective vehicle dynamics and control references for further details on the presented modeling approach (see, e.g., [17]–[19]). Unless otherwise stated, we use

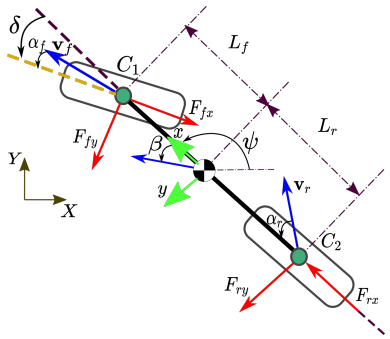


Fig. 2: Bicycle model schematic.

the subscripts r and f to denote the variables associated with the rear and front wheels of the vehicle, respectively.

1) Kinematic Relationships: In this section we briefly present the important kinematic relationship in the vehicle bicycle model. Table I provides the list of variables utilized in the bicycle model along with their descriptions. Additionally, Figure 2 provides a schematic view of the bicycle model. A variable that plays an important role in analyzing the lateral motion stability besides the vehicle yaw rate, i.e., $\omega_\psi := \dot{\psi}$, can be defined using the side slip angle β as follows

$$\sigma := \tan\beta = \frac{v_{Gy}}{v_{Gx}}. \tag{1}$$

TABLE I: Bicycle Model Kinematic and Dynamic Variables.

Variable	Description
X, Y x, y	Ground-fixed and body-fixed coordinate systems.
F_{fx}, F_{fy} F_{rx}, F_{ry}	The front and rear wheel contact forces.
$\mathbf{v}_f$, $\mathbf{v}_r$ $\mathbf{v}_G = [v_{Gx}, v_{Gy}]^\top$	The Front and rear wheel contact point velocity vectors. The velocity vector of the COM.
ω_f, ω_r α_f, α_r λ_f, λ_r	The front and rear wheel angular velocities. The front and rear wheel slip angles. The front and rear wheel longitudinal slip values.
ψ, $\dot{\psi}$ δ	The vehicle yaw angle and angular yaw rate. Front wheel steering angle.
β $\sigma = \tan(\beta)$	Vehicle side slip angle. Side slip angle variable.
g m I_z L_f, L_r	The gravitational acceleration. The vehicle total mass. The moment of inertia about the z-axis. The distances between the COM and the front and rear wheel contact points.

Two other important relationships can be used to describe the front and rear wheel slip angles α_f and α_r in terms of the other kinematic variables. In particular, we have

$$\tan(\delta - \alpha_f) = \frac{v_{fy}}{v_{fx}} = \frac{v_{Gy} + L_f\dot{\psi}}{v_{Gx}} = \sigma + \frac{L_f\dot{\psi}}{v_{Gx}}, \tag{2}$$

and

$$\tan(\alpha_r) = -\frac{v_{ry}}{v_{rx}} = -\frac{v_{Gy} - L_r\dot{\psi}}{v_{Gx}} = -\sigma + \frac{L_r\dot{\psi}}{v_{Gx}}. \quad (3)$$

The kinematic relationships (2) and (3), under small slip angle conditions, can be further simplified to

$$\alpha_f = \delta - \sigma - \frac{L_f\dot{\psi}}{v_{Gx}},\ \alpha_r = -\sigma + \frac{L_r\dot{\psi}}{v_{Gx}}. \quad (4)$$

To describe the kinematic relationships between the rear and front wheel contact point velocities and the vehicle COM velocity, one can use the slip angles α_f and α_r as follows

$$v_{rx} = v_r\cos(\alpha_r) = v_{Gx},\ v_{ry} = -v_{rx}\tan(\alpha_r), \quad (5)$$

and

$$v_{fx} = v_f\cos(\delta - \alpha_f) = v_{Gx},\ v_{fy} = v_{fx}\tan(\delta - \alpha_f). \quad (6)$$

Consequently, the relative velocity of the front and rear wheel contact points with respect to the ground are

$$v_{R_f} = \sqrt{v_{fx}^2 + v_{fy}^2} = v_{Gx}\sqrt{1 + \sin(\delta - \alpha_f)^2}, \quad (7a)$$

$$v_{R_r} = \sqrt{v_{rx}^2 + v_{ry}^2} = v_{Gx}\sqrt{1 + \tan(\alpha_r)^2}. \quad (7b)$$

Under small slip angle conditions and zero front wheel steering angle, i.e., $\delta = 0$, the magnitudes of the relative velocity of the front and rear wheel contact points given by (7) get simplified to

$$v_{R_f} = v_{R_r} = v_{Gx}. \quad (8)$$

In addition to the slip angles α_f and α_r, it is possible to define the front and rear wheel longitudinal slips as

$$\lambda_f := \frac{v_f\cos(\alpha_f) - r_f\omega_f}{v_f\cos(\alpha_f)},\ \lambda_r := \frac{v_{Gx} - r_r\omega_r}{v_{Gx}}, \quad (9)$$

respectively. Similarly, under small slip angle conditions and zero front wheel steering angle, the longitudinal slip values given by (9) get simplified to

$$\lambda_f = \frac{v_{Gx} - r_f\omega_f}{v_{Gx}},\ \lambda_r = \frac{v_{Gx} - r_r\omega_r}{v_{Gx}}. \quad (10)$$

2) Bicycle Model of Vehicle Dynamics: In this section we present the bicycle model for vehicle dynamics, the tire/road interaction forces under small slip angle conditions, and the resulting LTV dynamics under time-varying longitudinal slip profiles. We assume that $F_{fx} - F_{rx} = 0$ and that $\delta = 0$. In the vehicle dynamics and control literature (see, e.g., [17], [18]), where the coupling between the lateral and longitudinal dynamics are investigated, it is customary to assume a constant COM velocity, i.e., $v_{Gx} = V_0$, which is equivalent to $F_{fx} - F_{rx} = 0$. Under these assumptions, the nonlinear dynamics of the vehicle lateral motion are

$$\dot{\sigma} = -(1 + \sigma^2)\omega_\psi + \frac{F_{fy} + F_{ry}}{mV_0}, \quad (11a)$$

$$\dot{\omega}_\psi = \frac{1}{I_z}(F_{fy}L_f - F_{ry}L_r). \quad (11b)$$

The nonlinear dynamics given by (11) can effectively capture the effect of tire/road friction forces on the lateral stability

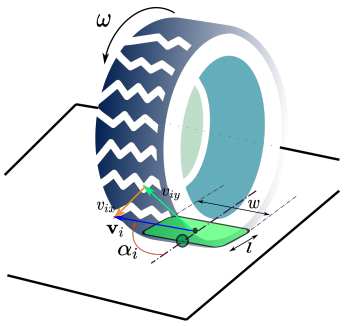


Fig. 3: The tire contact patch geometry and its motion kinematics.

of the vehicle (see, e.g., [17], [18]). To model the tire/road friction forces, we assume a contact patch with rectangular geometry between the tire and the road (see Figure 3). Under this contact patch geometry and small slip angle conditions, the steady-state tire/road lateral forces using a hybrid physical/dynamic tire/road friction model (see, e.g., [17]–[19]) are

$$F_{yi} = \frac{l_i\hat{\sigma}_{0yi}F_{ni}}{2}\big(1 - \frac{l_i\hat{\sigma}_{0yi}}{2g_{iy}(v_{Ri})}\lambda_i\big)\alpha_i,\ i = r, f, \quad (12)$$

where l_i and $\hat{\sigma}_{0yi}$, $i = r, f$, are contact patch length and normalized tire bristle elastic stiffness, respectively (see Figure 3 for the tire/road contact patch geometry). Furthermore, F_{ni}, $i = r, f$, is the tire normal load, where the relationship $F_{ni} = \frac{L_i}{L}mg$ holds under a static normal load distribution. Finally, the nonlinear mapping $g_{iy}(\cdot)$, which captures the impact of the tire/road distributed LuGre dynamic model on lateral forces in steady state, can be expressed as

$$g_{iy}(v_{Ri}) = \mu_{Ci} + (\mu_{Si} - \mu_{Ci})\exp\big(-\sqrt{\frac{v_{Ri}}{v_{si}}}\big). \quad (13)$$

In (13), the parameters v_{si}, μ_{Ci}, and μ_{Si}, $i = r, f$, are the Stribeck velocity, the Coulomb friction coefficient, and the static friction coefficient, respectively. As it is demonstrated by [17], the tire lateral forces in (12) can be written as

$$F_{yi} = b_i g_{iy}(v_{Ri})F_{ni}\big(1 - b_i\lambda_i\big)\alpha_i,\ i = r, f, \quad (14)$$

where $b_i := \frac{l_i\hat{\sigma}_{0yi}}{2g_{iy}(v_{Ri})}$, and the slip angles are given by (4). It is possible to model the effect of environmental disturbances acting on the vehicle lateral dynamics as discussed in Section VI. Such environmental disturbance modeling not only makes the utilized physics-based models more accurate but also helps to understand the capabilities of sophisticated adversaries when they time their cyber-physical attacks with environmental factors to induce more damage (see, e.g., the work by Kott *et al.* [35]).

Linearizing the nonlinear dynamics given by (11) under the lateral tire forces in (14) about the equilibrium $\mathbf{x}_e = [\sigma,\ \psi]^\top = [0, 0]^\top$ (see [17] for the derivation details), we arrive at the LTV dynamical model

$$\dot{\sigma} = A_{11}(t)\sigma + A_{12}(t)\omega_\psi, \quad (15a)$$

$$\dot{\omega}_\psi = A_{21}(t)\sigma + A_{22}(t)\omega_\psi, \quad (15b)$$

under time-varying longitudinal slips $\lambda_i(t)$, $i = r,\, f$, where

$$A_{11}(t) = \frac{-g}{LV_0}\Big\{b_f g_{fy}(V_0)(1 - b_f\lambda_f(t))L_r + b_r g_{ry}(V_0)(1 - b_r\lambda_r(t))L_f\Big\}, \tag{16a}$$

$$A_{12}(t) = -1 - \frac{gL_fL_r}{LV_0^2}\Big\{b_f g_{fy}(V_0)(1 - b_f\lambda_f(t)) - b_r g_{ry}(V_0)(1 - b_r\lambda_r(t))\Big\}, \tag{16b}$$

$$A_{21}(t) = \frac{-gL_fL_r}{I_zL}\Big\{b_f g_{fy}(V_0)(1 - b_f\lambda_f(t)) - b_r g_{ry}(V_0)(1 - b_r\lambda_r(t))\Big\}, \tag{16c}$$

$$A_{22}(t) = \frac{-gL_fL_r}{LV_0}\Big\{b_f g_{fy}(V_0)(1 - b_f\lambda_f(t))L_f - b_r g_{ry}(V_0)(1 + b_r\lambda_r(t))L_r\Big\}. \tag{16d}$$

In summary, under small slip angle conditions and zero steering angle input, the linearized lateral dynamics about the equilibrium $\mathbf{x}_e = [\sigma,\, \psi]^\top = [0, 0]^\top$ under time-varying longitudinal slip profiles take the following LTV form

$$\dot{\mathbf{x}} = \mathbf{A}_\ell(t)\mathbf{x}, \tag{17}$$

where $\mathbf{x} := [\sigma,\, \omega_\psi]^\top$ is the state vector. Also, the entries of the state transition matrix $\mathbf{A}_\ell(t) \in \mathbb{R}^{2\times 2}$ are given by (16).

When the longitudinal slip values of the wheels do not change with time, namely, when $\lambda_f(t) = \lambda_f^*$ and $\lambda_r(t) = \lambda_r^*$ for some constant values λ_f^* and λ_r^*, we arrive at

$$\dot{\mathbf{x}} = \mathbf{A}_\ell^*\mathbf{x}, \tag{18}$$

where $\mathbf{A}_\ell^*$ is the state transition matrix of the LTI dynamics in (18) under $\lambda_f(t) = \lambda_f^*$ and $\lambda_r(t) = \lambda_r^*$.

The trace of the matrix $\mathbf{A}_\ell(t)$, which will play an important role in our subsequent developments, is given by $\mathrm{tr}(\mathbf{A}_\ell(t)) = A_{11}(t) + A_{22}(t)$. Using (16), it can be seen that

$$\mathrm{tr}(\mathbf{A}_\ell(t)) = \kappa_f\big(1 - b_f\lambda_f(t)\big) + \kappa_r(1 - b_r\lambda_r(t)\big), \tag{19}$$

where the constant parameters κ_f and κ_r, which are dependent on the kinematic parameters of the vehicle and the tire-road interaction characteristics, are given by

$$\kappa_f = \frac{-gL_rb_f g_{fy}(V_0)}{LV_0}\big(1 + L_f^2\big), \tag{20a}$$

$$\kappa_r = \frac{-gL_fb_r g_{ry}(V_0)}{LV_0}\big(1 + L_r^2\big). \tag{20b}$$

Remark 1. *There are various ways for estimating the state transition matrix $\mathbf{A}_\ell(t)$ thanks to the mature technologies and algorithms developed for commercial vehicles such as utilizing unknown input observers and lateral tire force sensors (see, e.g., [36]–[38]).*

III. Cyber-Physical Threat Analysis Under Time-Varying Longitudinal Slip Values

In this section we present the conditions under which the adversary can endanger the vehicle lateral motion stability through improper engagement of the braking system/ABS by continuously changing the longitudinal slip values.

Our analysis in this section is independent of the source of intrusion into the braking system/ABS and the only assumption is that the attacker is changing the longitudinal slip values with time. A special case of such a scenario is when the attacker causes wheel lockups (see, e.g., [6]), which can be considered as one of the most severe types of attacks with a potential for catastrophic road injuries [39]. Nevertheless, such a sophisticated attacker needs to execute closed-loop attack policies on the vehicle traction dynamics while having full disclosure and disruption resources simultaneously. Here, we relax such an assumption and provide more general conditions under which the attacker can induce lateral motion instability. For instance, the attacker might be using the simple and inexpensive electromagnetic spoofing device proposed by [4].

We first present the following proposition that establishes the equivalency between the local exponential stability of the equilibrium $\mathbf{x}_e = [0, 0]^\top$ for the lateral motion nonlinear time-varying dynamics and its LTV linearized model.

Proposition 2. *Consider the vehicle lateral motion dynamics given by* (11) *and its linearized LTV model about the equilibrium $\mathbf{x}_e = [\sigma,\, \psi]^\top = [0, 0]^\top$ given by* (17)*. The equilibrium $\mathbf{x}_e$ is locally uniformly exponentially stable for the nonlinear dynamics in* (11) *if and only if the LTV dynamics in* (17) *are uniformly asymptotically stable.*

Proof. The uniform exponential stability of $\mathbf{x}_e$ for the nonlinear dynamics (11) is equivalent to the uniform exponential stability of $\mathbf{x}_e$ for the LTV dynamics (17) (see, e.g., Theorem 4.15 in [40]). Furthermore, the uniform exponential stability of the LTV dynamics given by (17) is equivalent to its uniform asymptotic stability (see, e.g., Lemma 1 in [29]). □

The following proposition provides a necessary condition for asymptotic stability of the lateral motion LTV dynamics that can get violated due to improper engagement of the vehicle brakes/ABS by an adversary.

Proposition 3. *Consider the lateral motion LTV dynamics under time-varying longitudinal slip values given by* (17)*, where the entries of $\mathbf{A}_\ell(t)$ are given by* (16)*. A necessary condition for asymptotic stability of the vehicle lateral dynamics is*

$$\lim_{t\to\infty}\int_{t_0}^{t}\big[\kappa_f\big(1 - b_f\lambda_f(t)\big) + \kappa_r(1 - b_r\lambda_r(t))\big]\,dt = -\infty. \tag{21}$$

Proof. The trace of the state transition matrix $\mathbf{A}_\ell(t)$ is given by (19). According to Theorem 1 given by [41], if the LTV dynamics in (17) are asymptotically stable, then it is necessary that for any $t > t_0$, $\int_{t_0}^{t}\mathrm{tr}(\mathbf{A}_\ell(t))\,dt \to -\infty$, as $t \to \infty$. □

The following proposition provides a sufficient condition for instability of the lateral motion LTV dynamics.

Proposition 4. *Consider the lateral dynamics in the statement of Proposition 3. A sufficient condition for instability is*

$$\lim_{t\to\infty}\int_{t_0}^{t}\big[\kappa_f\big(1-b_f\lambda_f(t)\big)+\kappa_r(1-b_r\lambda_r(t))\big]\,dt=\infty. \quad (22)$$

Proof. The proof follows from a straightforward application of Theorem 2 given by [41] and noting that the trace of the state transition matrix $\mathbf{A}_\ell(t)$ is given by (19). □

Remark 5. *In the special case of fixed longitudinal slip values resulting in the LTI dynamics in* (18)*, we have* $\int_{t_0}^{t}\operatorname{tr}(A_\ell(t))\,dt=\operatorname{tr}(A_\ell^*)(t-t_0)$*. Therefore, if* $\operatorname{tr}(A_\ell^*)>0$*, then the sufficient condition in* (22) *holds and instability of the vehicle lateral motion follows, which is in agreement with the results obtained by [7], [17].*

The following corollary is an immediate result of Proposition 4 when the wheel longitudinal slip values change periodically under the adversary's actions.

Corollary 6. *Consider the lateral dynamics in the statement of Proposition 4. Assume that the wheel longitudinal slip values are periodically time-varying with period* T_0*. A sufficient condition for instability of the vehicle lateral dynamics is*

$$\kappa_f+\kappa_r>\kappa_f b_f\bar{\lambda}_f+\kappa_r b_r\bar{\lambda}_r, \quad (23)$$

where $\bar{\lambda}_i=\frac{1}{T_0}\int_{t_0}^{t_0+T_0}\lambda_i(\tau)d\tau$*,* $i=r,\,f$*, is the longitudinal slip value average over one period for any arbitrary* $t_0>0$*.*

According to Proposition 3 if the attacker changes the longitudinal slip values such that the equality in (21) is violated, then a necessary condition for asymptotic stability of the lateral motion LTV dynamics will not hold anymore. Furthermore, Proposition 4 and Corollary 6 provide sufficient conditions for time-varying wheel slip profiles that will result in lateral motion instability. The reader is referred to Section VI-A for the simulation results associated with time-varying longitudinal slip value profiles.

IV. Distance to the Nearest Unstable Lateral Motion Dynamics

In this section we utilize the concept of the distance between a given stable LTI dynamical system and its nearest unstable dynamics using the frozen-time eigenvalues of (17) (see, e.g., [20]–[22] for various approaches to develop a metric for this concept). In particular, we find the distance between the lateral motion dynamics under fixed wheel longitudinal slip values to its nearest unstable LTI dynamics. Furthermore, we provide a method for computing the minimal perturbations of the wheel longitudinal slip values that result in lateral motion instability under fixed slip conditions. These derivations are important from two different perspectives. From the adversary's perspective, it might be appealing to know about the minimal engagement of the brakes/ABS to cause lateral instability. From a defender's perspective, as discussed in the next section (Remark 10), the derived distance metric appears in certain parts of the real-time monitoring algorithm.

Let us consider an arbitrary time instant $t^*>0$. The frozen-time eigenvalues of $\mathbf{A}_\ell(t)$ given by (17) at $t=t^*$ play an important role for computing the instantaneous distance to instability. At $t=t^*$, the state transition matrix $\mathbf{A}_\ell(t)$ gives rise to the LTI dynamics

$$\dot{\mathbf{x}}=\mathbf{A}_\ell(t^*)\mathbf{x}. \quad (24)$$

The characteristic polynomial of $\mathbf{A}_\ell(t^*)$ in (24) is given by the second-order monic polynomial

$$f(z)=\det(z\mathbf{I}_2-\mathbf{A}_\ell(t^*))=z^2-\operatorname{tr}(\mathbf{A}_\ell(t^*))z+\det(\mathbf{A}_\ell(t^*)). \quad (25)$$

The LTI dynamics given by (24) are asymptotically stable if and only if the frozen-time eigenvalues of $\mathbf{A}_\ell(t)$ at $t=t^*$ lie in the left half complex plane. Since the trace and the determinant of $\mathbf{A}_\ell(t^*)$ are equal to the product and sum of the frozen-time eigenvalues of $\mathbf{A}_\ell(t)$ at $t=t^*$, asymptotic stability holds if and only if

$$\operatorname{tr}(\mathbf{A}_\ell(t^*))<0,\ \det(\mathbf{A}_\ell(t^*))>0. \quad (26)$$

Assuming asymptotic stability of (24), we would like to find the minimal real-valued perturbations to the coefficients of (25) such that the dynamics given by (24) become unstable. Furthermore, we would like to compute the distance of (24) to the nearest unstable LTI dynamics of the same order, namely, with a second-order characteristic polynomial. To find such perturbations, we follow the procedure due to Hitz and Kaltofen [21]. Let us consider the first-order polynomial

$$P_\Delta(z)=\Delta_0+\Delta_1 z, \quad (27)$$

where Δ_0 and Δ_1 are real constant values. The polynomial $P_\Delta(z)$ in (27) yields the perturbed monic polynomial

$$\begin{aligned}\tilde{f}(z):=&f(z)-P_\Delta(z)=z^2-(\operatorname{tr}(\mathbf{A}_\ell(t^*))+\Delta_1)z\\&+(\det(\mathbf{A}_\ell(t^*))-\Delta_0).\end{aligned} \quad (28)$$

Additionally, the distance between $f(\cdot)$ and $\tilde{f}(\cdot)$ is given by

$$d(f,\tilde{f}):=\sqrt{\Delta_0^2+\Delta_1^2}. \quad (29)$$

The following proposition can be used for computing the nearest unstable polynomial $\tilde{f}$ with real coefficients from a stable lateral motion characteristic polynomial of the form (25).

Proposition 7. *Consider the vehicle lateral motion LTI dynamics given by* (24) *and its associated characteristic polynomial in* (25)*. Assume that the dynamics in* (24) *are asymptotically stable, where the inequalities* (26) *are satisfied. Denote the nearest second-order monic polynomial to the stable lateral motion characteristic polynomial in* (25) *by* $\tilde{f}(z)$*. The polynomial* $\tilde{f}(z)$*, which has at least one root on the imaginary axis, is of the form* (28)*. The nearest unstable polynomial* $\tilde{f}(z)$ *to* $f(z)$ *can be obtained through the parametric perturbations* $\Delta_0(\zeta)=-\zeta^2+\det(\mathbf{A}_\ell(t^*))$ *and* $\Delta_1(\zeta)=-\operatorname{tr}(\mathbf{A}_\ell(t^*))$*. Furthermore, the square norm* $\mathcal{N}_m(\zeta):=\operatorname{tr}(\mathbf{A}_\ell(t^*))^2+\big(\zeta^2-\det(\mathbf{A}_\ell(t^*)\big)^2$ *gets minimized at* $\zeta=\pm\sqrt{\det(\mathbf{A}_\ell(t^*))}$ *resulting in the minimum distance*

$$d^*_{\mathbf{A}_\ell(t^*)}=-\operatorname{tr}(\mathbf{A}_\ell(t^*)). \quad (30)$$

Proof. The statement of the proposition directly follows from the application of Theorem 3 in [21] to the second-order stable monic polynomial given by (25). □

We now utilize Proposition 7 to find the minimal perturbations of the wheel longitudinal slip values that result in lateral motion instability. First, it is remarked that a perturbed wheel longitudinal slip vector of the form

$$\tilde{\boldsymbol{\lambda}} = \begin{bmatrix} \lambda_f(t^*) + \Delta\lambda_f \\ \lambda_r(t^*) + \Delta\lambda_r \end{bmatrix}, \tag{31}$$

at time $t = t^*$ results in a perturbed state transition matrix $\tilde{\mathbf{A}}_\ell(t)$ whose trace is given by

$$\operatorname{tr}(\tilde{\mathbf{A}}_\ell(t^*)) = \operatorname{tr}(\mathbf{A}_\ell(t^*)) - \kappa_f b_f \Delta\lambda_f(t) - \kappa_r b_r \Delta\lambda_r(t). \tag{32}$$

We have the following lemma regarding the wheel longitudinal slip vector perturbations that minimize the distance of the stable characteristic polynomial in (25) to its nearest unstable second-order monic polynomial.

Lemma 8. *Consider the vehicle lateral motion LTI dynamics given by* (24) *and its associated characteristic polynomial in* (25)*. Assume that the dynamics in* (24) *are asymptotically stable, where the inequalities* (26) *are satisfied. The wheel longitudinal slip vector perturbation* $\Delta\boldsymbol{\lambda} := [\Delta\lambda_f,\, \Delta\lambda_r]^\top$ *that minimizes the distance of* (25) *to the nearest unstable monic second-order polynomial satisfies the equality constraint*

$$\Delta\boldsymbol{\lambda}^\top \boldsymbol{\nu} - \operatorname{tr}(\mathbf{A}_\ell(t^*)) = 0, \tag{33}$$

where $\boldsymbol{\nu} := [\kappa_f b_f,\, \kappa_r b_r]^\top$.

Proof. According to Proposition 7, the perturbation $P_\Delta(z) = -\operatorname{tr}(\mathbf{A}_\ell(t^*))z$ will minimize the distance of (25) to the nearest unstable characteristic polynomial. Such a perturbation will result in a perturbed state transition matrix $\tilde{\mathbf{A}}_\ell(t^*)$ satisfying (32). Rewriting the Equation (32) by using an inner product between $\Delta\boldsymbol{\lambda}$ and $\boldsymbol{\nu}$ concludes the proof. □

Using Lemma 8, we can numerically search for the wheel longitudinal slip vector perturbations $\Delta\boldsymbol{\lambda} := [\Delta\lambda_f,\, \Delta\lambda_r]^\top$ of minimum norm, which minimize the distance between the asymptotically stable characteristic polynomial in (25) and the family of unstable characteristic polynomials of order two. In particular, we can form the following QP problem

$$\begin{aligned} \min_{\Delta\boldsymbol{\lambda}} \quad & \Delta\boldsymbol{\lambda}^\top \Delta\boldsymbol{\lambda} \\ \text{s.t.} \quad & \Delta\boldsymbol{\lambda}^\top \boldsymbol{\nu} - \operatorname{tr}(\mathbf{A}_\ell(t^*)) = 0 \\ & -\lambda_i(t^*) \le \Delta\lambda_i \le 1 - \lambda_i(t^*),\ i = r,\, f, \end{aligned} \tag{34}$$

where the equality constraint in the constrained QP is the condition given by (33) in Lemma 8. The reader is referred to Section VI-B for the simulation results associated with the minimal destabilizing longitudinal slip value perturbations.

Remark 9. *The QP in* (34) *can be solved in embedded settings using alternating direction method of multipliers (ADMM)-based algorithms (see, e.g., [42], [43]). One such algorithm is presented in Appendix A and its real-time performance is benchmarked through processor-in-the-loop (PIL) simulations on an ARM Cortex processor emulator in Section VI.*

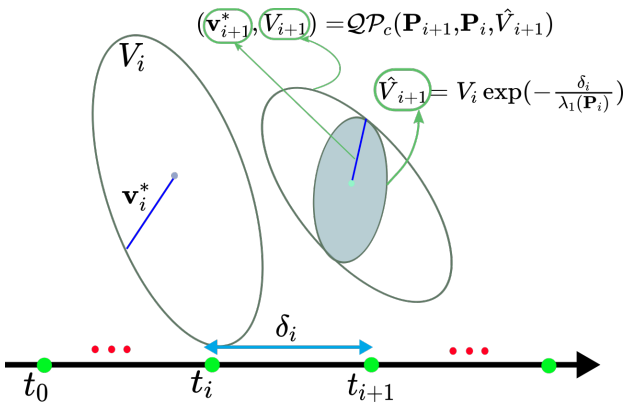


Fig. 4: Using the incoming stream of matrices $\mathbf{A}_\ell(t_{i+1})$, Algorithm 1 keeps generating a sequence of tube widths $\{V_0, V_1, \cdots\}$ through the following three numerical procedures: (1) tube width estimation (computing $\hat{V}_{i+1}$); (2) tube shape construction (computing $\mathbf{P}_{i+1} = \mathcal{LY}(\mathbf{A}_\ell(t_{i+1}))$); and, (3) tube junction (computing V_{i+1} and $\mathbf{v}^*_{i+1}$). By inspecting the numerical properties of the generated sequence $\mathcal{S} = \{V_i\}_{i=0}^{\infty}$ by Algorithm 1, one can infer stability of the vehicle lateral motion LTV dynamics.

V. Monitoring the Lateral Motion Dynamics against Braking System/ABS Attacks

In this section we adapt the theoretical framework in [28] to real-time settings for devising an algorithm to monitor the lateral motion dynamics of vehicles against braking/ABS cyber-physical attacks. This is the first time that Mullhaupt *et al.*'s theoretical results [28] are adapted to a cyber-physical monitoring application. In particular, through *two extensions*, we are making the results of [28] applicable to a real-time setting. First, since the numerical procedures in [28] rely on solving matrix-based equations and numerical optimizations, they are not suitable for implementation on embedded processors with limited resources (see Remark 11). We provide closed-form solutions to the numerical subproblems that are needed for running the algorithm in real-time. Second, we provide a condition on the sampling times of the monitoring algorithm that upholds the stability results of [28] in the case of a sampled-data setting (see Remark 13).

A. The Algorithm and Its Numerical Implementation

Algorithm 1 is a re-statement of the numerical procedures presented by [28] with extensions for making it suitable for automotive embedded settings. In particular, while Mullhaupt *et al.*'s method [28] is not suitable for real-time implementation on automotive embedded processors, Algorithm 1 in this article merely relies on the four fundamental arithmetic operations and some trigonometric function calculations as outlined in V-A1–V-A3. Indeed, Algorithm 1 is suitable for embedded settings with limited computational resources (Remark 11).

Algorithm 1 can be described as follows (see, also, Figure 4). First, the initialization step is carried out through the closed-form solution presented in V-A1 at time t_0. In the next sampling instants t_{i+1}, where $i = 0, 1, \cdots$, Algorithm 1 reads the lateral dynamics state transition matrix $\mathbf{A}_\ell(t_{i+1})$

Algorithm 1: Real-Time Monitoring of the Vehicle Lateral Motion LTV Dynamics

Data: A constant threshold V_{max} and sampled LTV state transition matrices $\mathbf{A}_\ell(t_i)$ at sampling instants $t_i > 0$, $i = 0, 1, \cdots$
Result: A sequence of tube widths $\{V_0, V_1, \cdots\}$
Initialization: Set $i = 0$ and read $\mathbf{A}_\ell(t_0)$;
if $\mathrm{tr}(\mathbf{A}_\ell(t_0)) < 0$ ***AND*** $\det(\mathbf{A}_\ell(t_0)) > 0$ **then**
  Choose $V_0 > 0$ and compute $\mathbf{P}_0 = \mathcal{LY}(\mathbf{A}_\ell(t_0))$ using (36) and (37) as outlined in V-A1;
else
  Issue a warning signal;
  return;
end
while $\sup_i V_i < V_{max}$ **do**
  Wait for the next sample of $\mathbf{A}_\ell(t)$ at $t = t_{i+1}$;
  Compute the elapsed time $\delta_i = t_{i+1} - t_i$ between the two readings;
  if $\mathrm{tr}(\mathbf{A}_\ell(t_i)) < 0$ ***AND*** $\det(\mathbf{A}_\ell(t_i)) > 0$ **then**
    (1) Estimate the tube width:
    Compute $\lambda_1(\mathbf{P}_i)$ using (40) as outlined in V-A2 and $\hat{V}_{i+1} = V_i \exp(-\frac{\delta_i}{\lambda_1(\mathbf{P}_i)})$;
    (2) Construct the tube shape:
    Compute $\mathbf{P}_{i+1} = \mathcal{LY}(\mathbf{A}_\ell(t_{i+1}))$ using (36) and (37) as outlined in V-A1;
    (3) Perform the tube junction:
    Compute $(\mathbf{v}^*_{i+1}, V_{i+1}) = \mathcal{QP}_c(\mathbf{P}_{i+1}, \mathbf{P}_i, \hat{V}_{i+1})$ using (46) as outlined in V-A3;
    $i \leftarrow i + 1$
  else
    Issue a warning signal;
    return;
  end
  Issue a warning signal;
  return;
end

(see Remark 1). Using the incoming stream of matrices $\mathbf{A}_\ell(t_{i+1})$, the algorithm keeps generating a sequence of tube widths $\{V_0, V_1, \cdots\}$ through the following three numerical calculations: (1) tube width estimation (through the closed-form solution presented in V-A2); (2) tube shape construction (through the closed-form solution presented in V-A1); and, (3) tube junction (through the closed-form solution presented in V-A3). Figure 4 provides a schematic of the computational steps within each iteration of running the algorithm.

For now, we assume that the sequence of tube widths $\{V_0, V_1, \cdots\}$ keeps getting generated with no interruption and that $\sup_i V_i \leq V_{\max}$. We will discuss the situations when $\mathrm{tr}(\mathbf{A}_\ell(t_i)) > 0$, $\det(\mathbf{A}_\ell(t_i)) < 0$, or when $\sup_i V_i > V_{\max}$ later in this section (see Remark 15). The closed-form solutions for implementing the Algorithm are outlined as follows.

1) Closed-form solution to two-dimensional Lyapunov equations: We define the function $\mathcal{LY} : \mathbf{B} \mapsto \mathbf{X}$ to be the mapping whose domain is the collection of constant real square matrices $\mathbf{B} \in \mathbb{R}^{2\times 2}$ with eigenvalues belonging to the left half complex plane. The mapping $\mathcal{LY}(\cdot)$ maps each matrix $\mathbf{B}$ in its domain to a unique symmetric matrix $\mathbf{X} \in \mathbb{R}^{2\times 2}$ that is the solution to the Lyapunov equation

$$\mathbf{B}^\top \mathbf{X} + \mathbf{X}\mathbf{B} = -\mathbf{I}_2. \tag{35}$$

In (35), if we denote the columns of the matrix $\mathbf{B}$ by $\mathbf{b}_1$ and $\mathbf{b}_2$, namely, if $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2]$, then the unique solution $\mathbf{X}$ to (35) takes the closed-form

$$\mathbf{X} = \mathcal{LY}(\mathbf{B}) = \begin{bmatrix} x_{11}(\mathbf{B}) & x_{12}(\mathbf{B}) \\ x_{21}(\mathbf{B}) & x_{22}(\mathbf{B}) \end{bmatrix}, \tag{36}$$

where

$$x_{11}(\mathbf{B}) = -\frac{|\mathbf{b}_2|^2 + \det(\mathbf{B})}{2\,\mathrm{tr}(\mathbf{B})\det(\mathbf{B})}, \tag{37a}$$

$$x_{12}(\mathbf{B}) = x_{21}(\mathbf{B}) = \frac{\mathbf{b}_1^\top \mathbf{b}_2}{2\,\mathrm{tr}(\mathbf{B})\det(\mathbf{B})}, \tag{37b}$$

$$x_{22}(\mathbf{B}) = -\frac{|\mathbf{b}_1|^2 + \det(\mathbf{B})}{2\,\mathrm{tr}(\mathbf{B})\det(\mathbf{B})}. \tag{37c}$$

Remark 10. *The entries of $\mathcal{LY}(\mathbf{A}_\ell(t_i))$, which need to be computed for tube shape construction at each time instant, are proportional to $\frac{1}{d^*_{\mathbf{A}_\ell(t_i)}}$. This is due to Proposition 7 stating that the smallest distance-to-instability is given by $d^*_{\mathbf{A}_\ell(t_i)} = -\mathrm{tr}(\mathbf{A}_\ell(t_i)) > 0$.*

2) Closed-form orthonormal diagonalization of two-dimensional symmetric matrices: We define the functions $\mathcal{D} : \mathbf{Z} \mapsto \mathcal{D}(\mathbf{Z})$ and $\mathcal{O} : \mathbf{Z} \mapsto \mathcal{O}(\mathbf{Z})$ that take in constant real symmetric square matrices $\mathbf{Z} \in \mathbb{R}^{2\times 2}$ and map them to $\mathcal{D}(\mathbf{Z}) \in \mathbb{R}^{2\times 2}$ and $\mathcal{O}(\mathbf{Z}) \in \mathbb{R}^{2\times 2}$ such that

$$\mathbf{Z} = \mathcal{O}(\mathbf{Z})\mathcal{D}(\mathbf{Z})\mathcal{O}(\mathbf{Z})^\top. \tag{38}$$

Therefore, the matrices $\mathcal{D}(\mathbf{Z})$ and $\mathcal{O}(\mathbf{Z})$ provide an orthonormal diagonalization of $\mathbf{Z}$ given by (38). The closed-form expression for the diagonal matrix $\mathcal{D}(\mathbf{Z})$ is given by

$$\mathcal{D}(\mathbf{Z}) = \begin{bmatrix} \lambda_1(\mathbf{Z}) & 0 \\ 0 & \lambda_2(\mathbf{Z}) \end{bmatrix}, \tag{39}$$

where $\lambda_i(\mathbf{Z})$, $i = 1, 2$, are the eigenvalues of $\mathbf{Z}$. These eigenvalues can be computed according to

$$\lambda_i(\mathbf{Z}) = \frac{1}{2}\left\{ \mathrm{tr}(\mathbf{Z}) + (-1)^{i-1}\sqrt{(z_{11} - z_{22})^2 + 4z_{12}^2} \right\}. \tag{40}$$

Also, the orthonormal matrix $\mathcal{O}(\mathbf{Z})$ is the rotation matrix

$$\mathcal{O}(\mathbf{Z}) = \begin{bmatrix} \cos\theta_{\mathbf{Z}} & -\sin\theta_{\mathbf{Z}} \\ \sin\theta_{\mathbf{Z}} & \cos\theta_{\mathbf{Z}} \end{bmatrix}, \tag{41}$$

where

$$\theta_{\mathbf{Z}} = \frac{1}{2}\mathrm{atan2}(\sin(2\theta_{\mathbf{Z}}), \cos(2\theta_{\mathbf{Z}})), \tag{42a}$$

$$\sin(2\theta_{\mathbf{Z}}) = \frac{2z_{12}}{\sqrt{(z_{11} - z_{22})^2 + 4z_{12}^2}}, \tag{42b}$$

$$\cos(2\theta_{\mathbf{Z}}) = \frac{z_{11} - z_{22}}{\sqrt{(z_{11} - z_{22})^2 + 4z_{12}^2}}. \tag{42c}$$

3) Closed-form solution to two-dimensional quadratic programs subject to quadratic equality constraints: We define the mapping $\mathcal{QP}_c : (\mathbf{X}, \mathbf{Y}, v_0) \mapsto (\mathbf{v}^*, v^*)$ that takes in triplets of the form $(\mathbf{X}, \mathbf{Y}, v_0)$ consisting of two positive definite matrices $\mathbf{X}, \mathbf{Y} \in \mathbb{R}^{2\times 2}$ and a positive real number v_0. The mapping $\mathcal{QP}_c(\cdot)$ maps the triplet $(\mathbf{X}, \mathbf{Y}, v_0)$ to a vector $\mathbf{v}^* \in \mathbb{R}^2$ and a real value v^* such that

$$\begin{aligned} v^* = \max_{\mathbf{v}} \quad & \mathbf{v}^\top \mathbf{X}\mathbf{v} \\ \text{s.t.} \quad & \mathbf{v}^\top \mathbf{Y}\mathbf{v} - v_0 = 0, \end{aligned} \tag{43}$$

and $\mathbf{v}^*$ is the vector that maximizes the quadratic cost function $\mathbf{v}^\top \mathbf{X}\mathbf{v}$ while satisfying the equality constraint in (43).

Considering the mapping $\mathcal{QP}_c : (\mathbf{X}, \mathbf{Y}, v_0) \mapsto (\mathbf{v}, v^*)$, it can be shown that (see, e.g., Lemma 2 in [28])

$$\mathbf{v} = \sqrt{\frac{v_0}{\lambda_2}} \mathcal{O}(\mathbf{X}) \mathcal{D}(\mathbf{X})^{-\frac{1}{2}} \mathbf{m}_2, \; v^* = \mathbf{v}^\top \mathbf{X}\mathbf{v}, \tag{44}$$

where $\mathcal{D}(\mathbf{X})$ and $\mathcal{O}(\mathbf{X})$ are obtained from applying the mappings $\mathcal{D}(\cdot)$ in (39)–(40) and $\mathcal{O}(\cdot)$ in (41)–(42) to $\mathbf{X}$, respectively. Furthermore, λ_2 is the smallest eigenvalue of

$$\mathbf{\Gamma} := \mathcal{D}(\mathbf{X})^{-\frac{1}{2}} \mathcal{O}(\mathbf{X})^\top \mathbf{Y} \mathcal{O}(\mathbf{X}) \mathcal{D}(\mathbf{X})^{-\frac{1}{2}}, \tag{45}$$

and the vector $\mathbf{m}_2$ is the orthonormal vector associated with λ_2. To compute λ_2 and $\mathbf{m}_2$, one needs to apply the mappings $\mathcal{D}(\cdot)$ in (39)–(40) and $\mathcal{O}(\cdot)$ in (41)–(42) to $\mathbf{\Gamma}$, respectively. The second element on the diagonal of $\mathcal{D}(\mathbf{\Gamma})$ is equal to λ_2 and the second column of $\mathcal{O}(\mathbf{\Gamma})$ is equal to the vector $\mathbf{m}_2$. Therefore, the closed-form solution to (44) takes the following form

$$\mathbf{v} = \sqrt{\frac{v_0}{\lambda_2(\mathbf{\Gamma})}} \begin{bmatrix} \frac{-\sin(\theta_{\mathbf{X}} + \theta_{\mathbf{\Gamma}})}{\sqrt{\lambda_1(\mathbf{X})}} \\ \frac{\cos(\theta_{\mathbf{X}} + \theta_{\mathbf{\Gamma}})}{\sqrt{\lambda_2(\mathbf{X})}} \end{bmatrix}, \; v^* = \mathbf{v}^\top \mathbf{X}\mathbf{v}, \tag{46}$$

where $\theta_{\mathbf{X}}$ and $\theta_{\mathbf{\Gamma}}$ can be computed from (42).

Remark 11. *Computing the closed-form solutions as outlined in V-A1– V-A3 merely relies on computing some trigonometric functions and performing the four fundamental arithmetic operations. The trigonometric expressions in* (41) *and* (42) *can be effectively calculated using CORDIC algorithms (see, e.g., [44]), which are well-suited for implementation on embedded processors. In contrast, the numerical procedures presented by [28] rely on solving matrix Lyapunov equations (to construct the tube shapes) and multivariable optimization problems as well as orthonormal diagonalization of real symmetric matrices (to perform the tube junction). Consequently, they are not suitable for implementation in automotive embedded applications with modest computational resources.*

B. Stability Guarantees of the Monitoring Algorithm

In this section we present the theoretical underpinnings of Algorithm 1. The theoretical framework of Mullhaupt *et al.* [28] is based on successive ellipsoidal approximations for checking the asymptotic stability of LTV Hurwitz systems, where the underlying continuous-time LTV state transition matrices are evaluated at discrete time instants. The following proposition, which constrains the sampling times, will enable us to invoke the stability results from [28].

Proposition 12. *Consider the vehicle lateral motion LTV dynamics under time-varying wheel longitudinal slip values given by* (17)*, where the entries of the state transition matrix* $\mathbf{A}_\ell(t)$ *are given by* (16)*. Assume that* $\mathbf{A}_\ell(t)$ *is Hurwitz for all times* t *and that the inequality*

$$t - t_i \leq \Big| \int_{t_i}^{t} \beta_i(\tau)\, d\tau \Big|, \; i = 0,\, 1,\, \cdots, \tag{47}$$

is satisfied for all time intervals $[t_i, t_{i+1}]$*,* $i = 0,\, 1,\, \cdots$*. In* (47)*,* $\beta_i(t) = \max\big\{ \operatorname{eig}\big(\mathbf{A}_\ell^\top(t)\mathbf{P}_i + \mathbf{P}_i\mathbf{A}_\ell(t)\big)\big\}$ *and* $\mathbf{P}_i = \mathcal{LY}(\mathbf{A}_\ell(t_i))$*, where* $\mathcal{LY}(\cdot)$ *is defined in V-A1. Furthermore, consider the sequence of tube widths* $\{V_i\}_{i=0}^{\infty}$ *generated by Algorithm 1. Then, the lateral dynamics state trajectories* $\mathbf{x}(t) = [\sigma(t), \omega_\psi(t)]^\top$ *satisfying* (17) *will be confined to the tubes* $\mathcal{T}_i := \{\mathbf{w} | \mathbf{w}^\top \mathbf{P}_i \mathbf{w} \leq V_i\}$ *for all* $t \in [t_i, t_{i+1}]$*,* $i = 1,\, 2,\, \cdots$*, provided that* V_0 *is chosen such that* $\mathbf{x}_0^\top \mathbf{P}_0 \mathbf{x}_0 \leq V_0$*.*

Remark 13. *Due to the restrictions of the sampled-data setting in automotive embedded applications, the tube width estimates in Algorithm 1 presented in this paper, i.e.,* $\hat{V}_{i+1} = V_i \exp(-\frac{\delta_i}{\lambda_1(\mathbf{P}_i)})$*, where* $\delta_i = t_{i+1} - t_i$*, are different from the tube width estimates in Mullhaupt* et al.*'s work [28]. Indeed, they utilize* $\hat{V}_{i+1} = V_i \exp(-\frac{\int_{t_i}^{t_{i+1}} \beta_i(\tau)\, d\tau}{\lambda_1(\mathbf{P}_i)})$ *with* $\beta_i(t) = \max\big\{ \operatorname{eig}\big(\mathbf{A}_\ell^\top(t)\mathbf{P}_i + \mathbf{P}_i\mathbf{A}_\ell(t)\big)\big\}$*. Proposition 12 guarantees that the results of [28] can be utilized in this paper.*

Proof. The inequality given by (47) guarantees that $\hat{V}(t) := V_i^* \exp\big(\frac{\int_{t_i}^{t} \beta_i(\tau) d\tau}{\lambda_1(\mathbf{P}_i)}\big) \leq \hat{V}^s(t)$, where $V_i^* = \mathbf{x}(t_i)^\top \mathbf{P}_i \mathbf{x}(t_i)$ and $\hat{V}^s(t) := V_i^* \exp\big(\frac{-(t-t_i)}{\lambda_1(\mathbf{P}_i)}\big)$. Using Equation (6) in the proof of Theorem 1 stated by [28], it follows that for all $t \in [t_i, t_{i+1}]$, $\mathbf{x}(t) \in \{\mathbf{w} \big| \mathbf{w}^\top \mathbf{P}_i \mathbf{w} \leq \hat{V}(t) \leq \hat{V}^s(t)\}$. The rest follows verbatim the proof of Theorem 1 stated by [28]. □

As a direct consequence of (47), the inequality

$$\delta_i \leq \Big| \int_{t_i}^{t_{i+1}} \beta_i(\tau)\, d\tau \Big|, \tag{48}$$

provides an upper bound on the sampling times to ensure that the state trajectories of the vehicle lateral dynamics are contained within the tubes $\mathcal{T}_i$ whose widths are given by the sequence $\{V_i\}_{i=0}^{\infty}$ generated by Algorithm 1. As affirmed by the following proposition, which is a direct consequence of Proposition 12 in this paper, Corollary 1, and Corollary 2 in [28], we can infer uniform stability and/or uniform asymptotic stability of the lateral dynamics of a monitored vehicle by inspecting the numerical properties of the sequence $\mathcal{S} = \{V_i\}_{i=0}^{\infty}$ generated by Algorithm 1. In Section VI, we will benchmark the performance of Algorithm 1 in the presence of delays in CAN bus using experimental data reported in the literature (see, e.g., [45], [46]).

Proposition 14. *Assume the conditions in the statement of Proposition 12 and consider the sequence* $\mathcal{S} = \{V_i\}_{i=0}^{\infty}$ *generated by Algorithm 1. If there exists a finite integer* M_0 *such that* $V_{M_0} < \infty$ *and* $V_i \leq V_{M_0}$ *for all* $V_i \in \mathcal{S}$*, then vehicle lateral LTV dynamics are uniformly stable. Furthermore, if there exists an ordered subsequence* $\mathcal{S}^* \subset \mathcal{S}$ *that is monotonically*

strictly decreasing, then the vehicle lateral LTV dynamics are uniformly asymptotically stable.

Proof. Under the assumptions of Proposition 12, the proof follows verbatim the proof of Corollaries 1 and 2 of [28]. □

Remark 15. *When the conditions* $\mathrm{tr}(\mathbf{A}_\ell(t_i)) < 0$ *or* $\det(\mathbf{A}_\ell(t_i)) > 0$ *are violated at* t_i, $i = 0, 1, \cdots$, *then no tube width estimate will be generated by Algorithm 1. Indeed, since the frozen-time eigenvalues of* $\mathbf{A}_\ell(t_i)$ *do not fall within the left-half complex plane, a warning signal will be issued to a higher-level supervisory module such as the security supervisor proposed by Lima* et al. *[47] for further actions. Moreover, when* $\sup_i V_i$ *is non-decreasing, then the conditions in Proposition 14 for uniform stability and/or uniform asymptotic stability of* $\mathbf{A}_\ell(t)$ *do not hold and a warning signal is issued to the higher-level supervisory module.*

The reader is referred to Section VI-C for the simulation results associated with the real-time monitoring algorithm.

VI. Simulation Results

In the numerical simulations that will follow, we are using the nonlinear dynamics given by (11) and its linearized LTV model in (15) under tire/road lateral forces given by (12). In our numerical simulations, we have chosen the parameter values to be given by $\hat{\sigma}_{0y} = 54$ 1/m, $\mu_S = 4.7$, $\mu_C = 0.14$, $v_s = 0.3$ m/s, and $l = 0.29$ m, for the front tire. Furthermore, we have chosen the parameter values $\hat{\sigma}_{0y} = 55$ 1/m, $\mu_S = 3.4$, $\mu_C = 0.06$, $v_s = 0.2$ m/s, and $l = 0.28$ m, for the rear tire. Additionally, we have chosen the vehicle mass to be $m = 1500$ kg, its mass moment of inertia to be $I_z = 3000$ kg.m^2, and the distances between the front and rear wheel contact points and the COM to be $L_f = 1.2$ m and $L_r = 1.3$ m, respectively. Finally, we have chosen the vehicle velocity component $v_{Gx} = V_0$, where $V_0 = 25$ m/s is a fixed value unless otherwise stated. These values have also been used in the numerical simulations presented by [17].

Our assumption regarding the attacker is that they can change the longitudinal slip values with time through improper engagement of the brakes/ABS. For instance, a sophisticated attacker who has managed to reprogram the braking/ABS ECUs can either induce wheel lock conditions (see, e.g., [6]) or can make the wheel slip values to follow a desired reference trajectory (see, e.g., [48]).

Modeling the Environmental Disturbances: In our simulations, the environmental disturbance effects on the lateral dynamics of the vehicle such as side-wind gusts can be modeled. Such environmental disturbance modeling not only makes the utilized physics-based models more accurate but also helps to understand the capabilities of sophisticated adversaries when they time their cyber-physical attacks with environmental factors to induce more damage. Following Cerone *et al.* [49], a side wind of velocity with time profile $v_w(t)$ will exert the force $F_w(t) = \frac{2.5\pi}{2} v_w(t)^2$ and the moment $M_w(t) = \frac{L_f - L_r}{2} F_w(t) + \left(\frac{2.5\pi}{2} - \frac{3.3\pi^3}{8}\right) v_w(t)^2$ on the vehicle. Therefore, in (11), the wind gust-induced disturbances manifest themselves as time-varying inputs getting added to dynamical equations. In particular, $\frac{F_{fy}+F_{ry}}{mV_0}$ should be changed to $\frac{F_{fy}+F_{ry}+F_w(t)}{mV_0}$ and $\frac{1}{I_z}(F_{fy}L_f - F_{ry}L_r)$ should be changed to $\frac{1}{I_z}(F_{fy}L_f - F_{ry}L_r + M_w(t))$. Furthermore, the LTV dynamics given by (17) take the following form $\dot{\mathbf{x}} = \mathbf{A}_\ell(t)\mathbf{x} + \mathbf{d}_w(t)$, where $\mathbf{d}_w(t) := [\frac{F_w(t)}{mV_0}, \frac{M_w(t)}{I_z}]^\top$ is the vector of environmental disturbances due to side-wind gusts.

Modeling the CAN Bus Delay: To benchmark the performance of Algorithm 1 in the presence of realistic CAN bus delays, we use experimental data reported in the literature. In particular, the work by De Andrade *et al.* [46] provides experimental measurements of the CAN bus worst-case message delay versus CAN bus load, where CAN bus loads of 19.49%, 29.62%, 49.88%, and 70.13% correspond to CAN bus delays of approximately 1 ms, 2.5 ms, 10 ms, and 21 ms, respectively. Using a second-order polynomial fit, we arrive at

$$\delta_{\text{CAN}} = 5.14\times10^{-3}x_{\text{busload}}^2 - 6.176\times10^{-2}x_{\text{busload}} + 1.002\times10^{-1}, \tag{49}$$

where δ_{CAN}, which is the CAN bus delay in milliseconds, can be expressed as a function of x_{busload}, which is the bus load (in percents). Figure 5 depicts the second-order polynomial given by (49) and the data reported by De Andrade *et al.* [46].

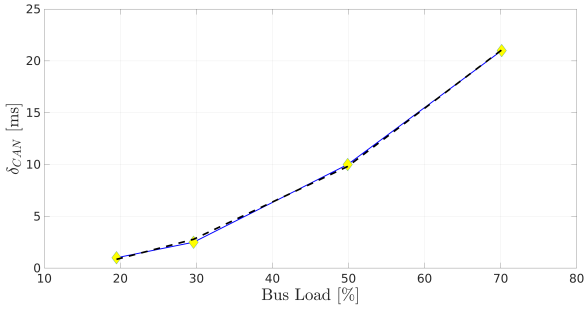


Fig. 5: The second-order polynomial fit (dashed black) to bus delay-bus load data (yellow diamonds) reported by De Andrade *et al.* [46]. The blue line segments represent the piecewise linear interpolation of the data.

A. Simulations Under Time-Varying Longitudinal Slip Profiles

Figure 6 depicts the phase portrait of the asymptotically stable lateral motion dynamics under $\lambda_f = \lambda_r = 0$.

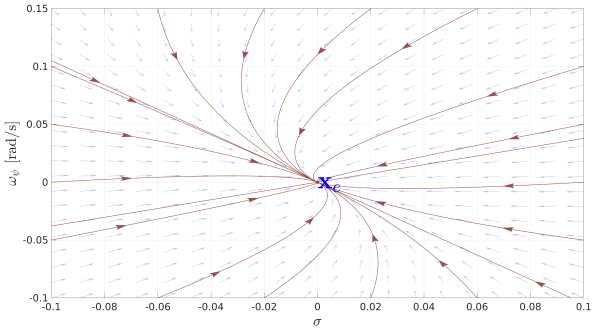


Fig. 6: The phase portrait of the asymptotically stable lateral motion dynamics under $\lambda_f = \lambda_r = 0$ and $v_{Gx} = 25.0$ m/s.

We now assume that the attacker is periodically varying the longitudinal slip values according to $\lambda_r = 0$ and $\lambda_f(t) = \alpha\cos(t)^2$, where $\alpha = 0.075$. Since the inequality $\kappa_f b_f \frac{\alpha}{2} < \kappa_f + \kappa_r$ is satisfied for all $\alpha > 0.072$, we should expect from Corollary 6 that the vehicle will lose its lateral stability. This is indeed the case where the upper plot in Figure 7 depicts the unstable time profiles of $\omega_\psi(t)$ and $\sigma(t)$ starting from $\sigma(0) = 0.1$ and $\omega_\psi(0) = -0.05$. The lower plot in Figure 7 depicts the locus of the frozen-time eigenvalues of $\mathbf{A}_\ell(t)$.

Figure 8 depicts the vehicle trajectories under $\lambda_f = \lambda_r = 0$ (upper plot) and the periodically time-varying longitudinal slip profiles $\lambda_f(t) = 0.2\cos(t)^2$, $\lambda_r(t) = 0$ (lower plot). The initial conditions for the vehicle have been chosen to be $\dot{\omega}_\psi(0) = -0.05$ rad/s and $v_{Gy}(0) = 2.5$ m/s. Remarkably, the attacker does not need to induce wheel lockups (i.e., either $\lambda_f = 1$ or $\lambda_r = 1$) to cause lateral motion instability.

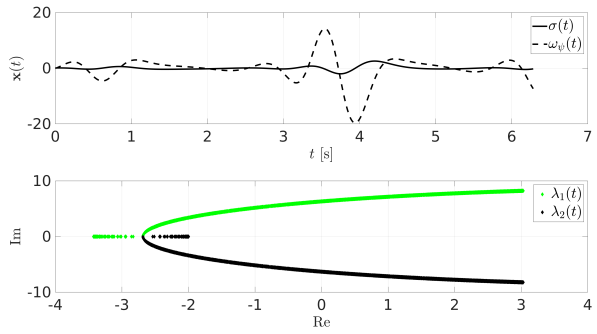


Fig. 7: (Upper) The time profiles of $\omega_\psi(t)$ and $\sigma(t)$ under periodically time-varying longitudinal time profiles $\lambda_r = 0$ and $\lambda_f(t) = \alpha\cos(t)^2$ with $\alpha = 0.075$ and $\sigma(0) = 0.1$, $\omega_\psi(0) = -0.05$. (Lower) The locus of the frozen-time eigenvalues of $\mathbf{A}_\ell(t)$ over one period.

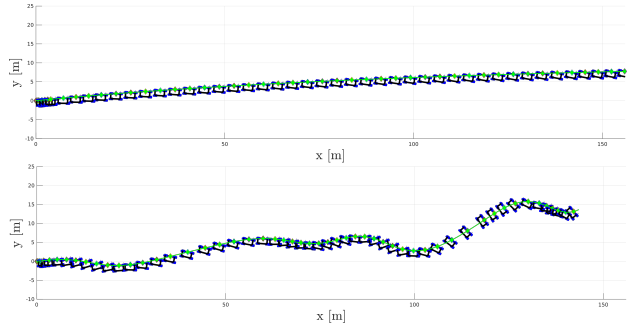


Fig. 8: The trajectories of the vehicle under $\lambda_f = \lambda_r = 0$ (upper plot), and $\lambda_f(t) = 0.2\cos(t)^2$, $\lambda_r(t) = 0$ (lower plot), with initial conditions $\dot{\omega}_\psi(0) = -0.05$ rad/s and $v_{Gy}(0) = 2.5$ m/s.

B. Simulations Under Minimal Slip Value Perturbations

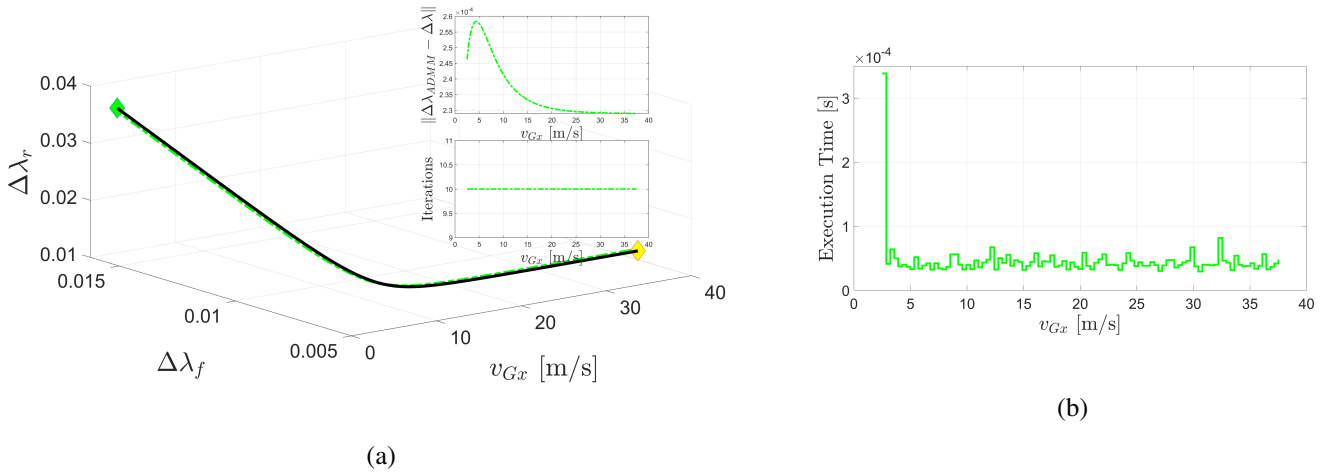
Computing the minimal perturbation vectors $\Delta\boldsymbol{\lambda} = [\Delta\lambda_f,\, \Delta\lambda_r]^\top$ versus the velocity profiles v_{Gx} for destabilizing the vehicle lateral motion dynamics is important from both a cyber-physical safety and a lateral motion stability perspective. While one can utilize the constrained QP given by (34) with conventional QP solvers, it is of crucial importance to solve (34) in an embedded setting. For this purpose, we will utilize an ADMM-based embedded algorithm for finding the minimal destabilizing perturbations (see Algorithm 2 in Appendix A) and benchmark its real-time performance through processor-in-the-loop (PIL) simulations on ARM Cortex processors (in particular, ARM Cortex-M3 processor [50]). ARM Cortex-M3 is an automotive grade processor utilized in various cybersecurity applications (see, e.g., [51] and [52]).

The black curve in the 3D plot in Figure 9 depicts the profile of the minimal perturbation vector components for destabilizing the vehicle lateral dynamics from $\lambda_f = \lambda_r = 0$ (obtained from MATLAB `quadprog` solver). The green and yellow diamonds on the black curve are associated with $v_{Gx} = 2.5$ m/s and $v_{Gx} = 37.5$ m/s, respectively. As it can be clearly seen from Figure 9, the required destabilizing minimal perturbations to the longitudinal slip values keep decreasing as the vehicle speed v_{Gx} increases. Therefore, an attacker who manages to engage the vehicle brakes at a higher speed can destabilize the vehicle lateral motion with smaller amounts of longitudinal slip value perturbations.

Embedded Benchmarking: To benchmark the embedded ADMM-based algorithm (Algorithm 2 in Appendix A) for solving (34), we utilize the MATLAB interface for embedded benchmarking of codes on ARM Cortex-M3 QEMU Emulator [53]. The dash-dotted green curve in the 3D plot in Figure 9(a) depicts the profile of the solutions obtained from the embedded ADMM algorithm with $\epsilon_{\text{dual}} = \epsilon_{\text{primal}} = 5 \times 10^{-4}$. The smaller upper plot in Figure 9(a) demonstrates the profiles of the error norm $\|\Delta\boldsymbol{\lambda} - \Delta\boldsymbol{\lambda}_{\text{ADMM}}\|$ versus the vehicle speed, where $\Delta\boldsymbol{\lambda}$ and $\Delta\boldsymbol{\lambda}_{\text{ADMM}}$ are the solutions obtained from the MATLAB `quadprog` solver and the ADMM-based algorithm run on the ARM Cortex-M3 emulator, respectively. The smaller lower plot in Figure 9(a) demonstrates the number of needed iterations for convergence of the embedded ADMM solver. Finally, Figure 9(b) demonstrates an execution time profile on the ARM Cortex-M3 processor versus the vehicle speed.

Figure 10 depicts the phase portrait of the destabilized lateral motion dynamics by applying the minimal perturbations $\Delta\lambda_f = 6.4 \times 10^{-3}$ and $\Delta\lambda_r = 13.4 \times 10^{-3}$ to the nominal wheel longitudinal slip values $\lambda_f = \lambda_r = 0$ with velocity $v_{Gx} = 25.0$ m/s (compare this phase portrait with the one depicted in Figure 6).

We now present the trajectories of the vehicle under side-wind gust using the dynamical modeling approach discussed earlier in this section in two attack scenarios. In the first attack scenario, we assume that the attacker can solve the QP in (34) via an accurate solver. In the second attack scenario, we assume that the attacker is using the embedded real-time solver on an ARM Cortex-M3 processor to obtain the solutions to (34). We assume that the side-wind gust speed is $v_w = 6$ km/h and the vehicle initial velocity vector components are $v_{Gx}(0) = 10.28$ m/s and $v_{Gy}(0) = 0$ m/s. Additionally, it is assumed that $\omega_\psi(0) = 0$ rad/s. Figure 11 depicts the trajectories of the vehicle under $\lambda_f = \lambda_r = 0$ (upper plot), the



(a) (b)

Fig. 9: (a) The trajectory of the minimal perturbation vectors $\Delta\boldsymbol{\lambda} = [\Delta\lambda_f, \Delta\lambda_r]^\top$ versus various vehicle speeds v_{Gx} for destabilizing the lateral motion dynamics under $\lambda_f = \lambda_r = 0$: (black) obtained from MATLAB `quadprog` solver; and, (dash-dotted green) obtained from the embedded ADMM optimization on ARM Cortex-M3 QEMU Emulator with $\epsilon_{\text{dual}} = \epsilon_{\text{primal}} = 5 \times 10^{-4}$. The green and yellow diamonds on the black curve are associated with $v_{Gx} = 2.5$ m/s and $v_{Gx} = 37.5$ m/s, respectively. The smaller upper plot demonstrates the profile of the error norm $\|\Delta\boldsymbol{\lambda} - \Delta\boldsymbol{\lambda}_{\text{ADMM}}\|$ versus vehicle speed. The smaller lower plot demonstrates the number of needed iterations for convergence of the embedded ADMM solver. (b) An execution time profile for computing the minimal destabilizing perturbation vector on the ARM Cortex-M3 processor versus the vehicle speed.

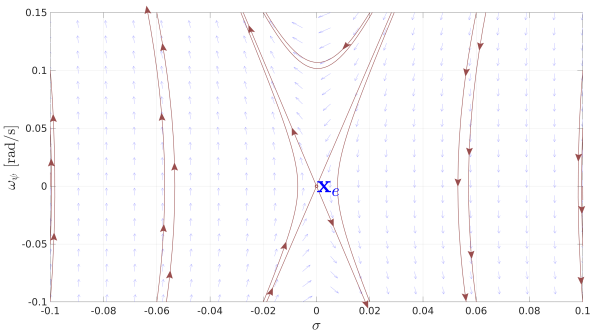


Fig. 10: The phase portrait of the destabilized lateral motion dynamics by applying the minimal perturbations $\Delta\lambda_f = 6.4 \times 10^{-3}$ and $\Delta\lambda_r = 13.4 \times 10^{-3}$ to nominal wheel longitudinal slip values $\lambda_f = \lambda_r = 0$ with velocity $v_{Gx} = 25.0$ m/s.

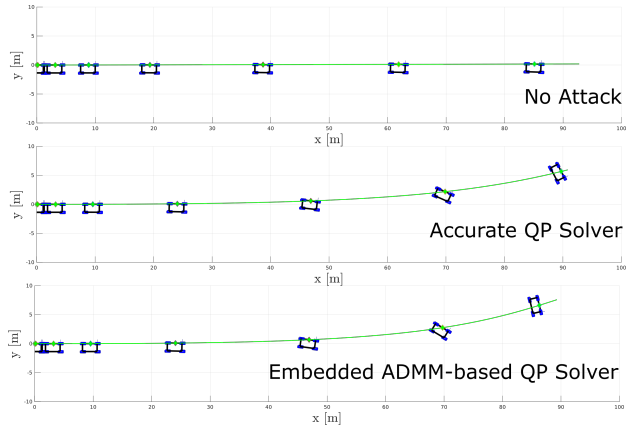


Fig. 11: The trajectories of the vehicle under $\lambda_f = \lambda_r = 0$ (most upper plot), $\lambda_f = 6.464 \times 10^{-3}$, $\lambda_r = 14.119 \times 10^{-3}$ (middle plot), and $\lambda_f = 7.339 \times 10^{-3}$, $\lambda_r = 13.718 \times 10^{-3}$ (bottom plot), with initial conditions $\omega_\psi(0) = 0$ rad/s, $v_{Gx}(0) = 10.28$ m/s, and $v_{Gy}(0) = 0$ m/s. In all of these cases, a side-wind gust with a constant speed $v_w = 6$ km/h is assumed.

perturbed longitudinal slip values in the first attack scenario (middle plot), and the perturbed longitudinal slip values in the second attack scenario (bottom plot). Remarkably, the attacker does not need to induce wheel lockups (i.e., either $\lambda_f = 1$ or $\lambda_r = 1$) to cause lateral motion instability. Furthermore, despite the fact that the attacker is using an embedded processor in the second scenario where it takes about 50 microseconds for the iterative ADMM algorithm to converge to the approximate solution (see Figure 9(b)), the motion of the vehicle gets destabilized.

C. The Real-Time Monitoring Algorithm Simulations

In this section we investigate the performance of the monitoring algorithm (Algorithm 1) under various simulation scenarios and CAN bus load profiles. Using the polynomial fit in (49), which has been found by fitting a second-order polynomial to the experimental data reported by De Andrade *et al.* [46], we consider three different CAN bus load probability distributions in each simulation scenario resulting in different CAN bus delay profiles. In particular, the first, the second, and the third CAN bus delay profiles are obtained by assuming a fixed bus load of 50%, a uniformly distributed bus load varying between 0% and 100%, and a normally distributed bus load with a mean of 50% and a standard deviation of 20%.

Figure 12 depicts the sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 0$ and $\lambda_f(t) = 0.02\cos^2(\sqrt{10}t) + 0.005$ with the fixed CAN bus delay profile. It is remarked that the monitoring algorithm does not have any knowledge of the lateral dynamics state transition matrix $\mathbf{A}_\ell(t)$ except for discrete readings of this matrix at each

sampling time. Therefore, the only way that Algorithm 1 manages to predict uniform stability or uniform asymptotic stability of the vehicle lateral motion dynamics is through checking the sequence of the tube widths V_i and invoking Proposition 14. Figures 13 and 14 depict the sequence of the tube widths generated by Algorithm 1 under the same longitudinal slip profiles but with the uniformly and normally distributed CAN bus load profiles, respectively. As it can be seen in both cases, there exists a subsequence of tube widths that is monotonically strictly decreasing during the simulation. Therefore, according to Proposition 14, the algorithm does not issue any warning signals through the simulation.

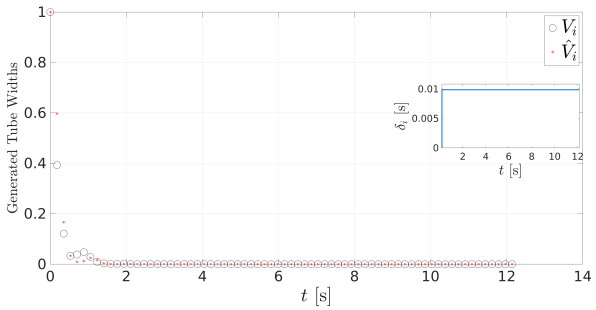


Fig. 12: The sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 0$ and $\lambda_f(t) = 0.02\cos^2(\sqrt{10}t)+0.005$. The inner plot depicts the CAN bus delay δ_i versus time resulting from a fixed bus load of 50%.

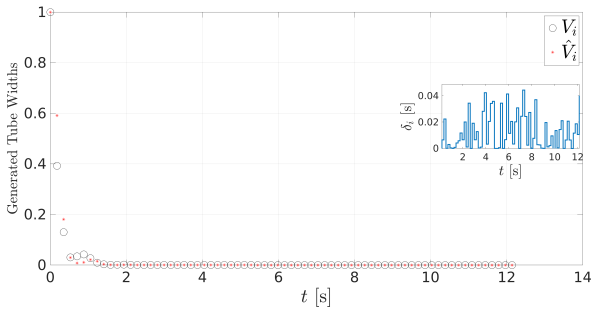


Fig. 13: The sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 0$ and $\lambda_f(t) = 0.02\cos^2(\sqrt{10}t)+0.005$. The inner plot depicts the CAN bus delay δ_i versus time resulting from a uniformly distributed bus load varying between 0% and 100%.

Figures 15, 16, and 17 depict the sequence of the tube widths generated by Algorithm 1 up to time $t \approx 4.2$ sec under $\lambda_r(t) = 1.5 \times 10^{-3}\sin^2(10t)$ and $\lambda_f(t) = 10^{-3}(t - \frac{\pi}{2})^2\cos^4(\sqrt{40}t)\mathbf{u}(t - \frac{\pi}{2})$, where $\mathbf{u}(\cdot)$ is the unit step function, with the fixed, uniformly distributed, and normally distributed CAN bus delay profiles, respectively. In all these scenarios, as it can be seen from their respective figures, $\sup_i V_i$ keeps increasing as the time goes on. The upper plot in Figure 18 depicts the trajectory profile $[\omega_\psi(t),\, \sigma(t)]^\top$ up to time $t \approx 8.5$ sec while the lower plot in the same figure demonstrates the

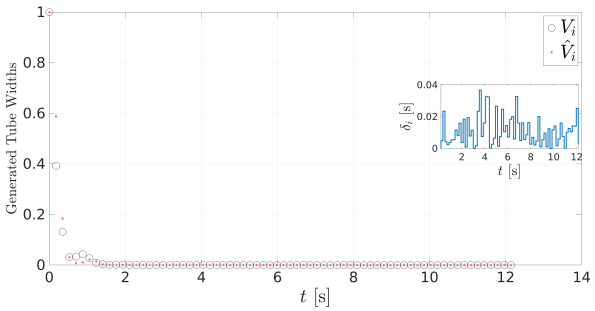


Fig. 14: The sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 0$ and $\lambda_f(t) = 0.02\cos^2(\sqrt{10}t)+0.005$. The inner plot depicts the CAN bus delay δ_i versus time resulting from a normally distributed bus load with a mean of 50% and a standard deviation of 20%.

locus of the frozen-time eigenvalues up to time $t \approx 8.5$ sec. It is notable that the monitoring algorithm has been generating a sequence of tube widths with increasing $\sup_i V_i$ well before the frozen-time eigenvalues become unstable around $t \approx 7.5$ sec. Therefore, the higher-level supervisory module can be informed well ahead for taking a decision on the issued warning signal.

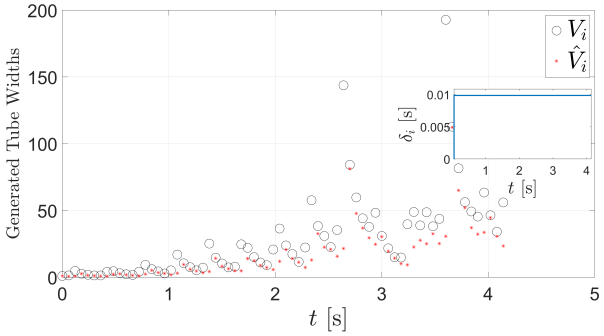


Fig. 15: The sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 1.5 \times 10^{-3}\sin^2(10t)$ and $\lambda_f(t) = 10^{-3}(t - \frac{\pi}{2})^2\cos^4(\sqrt{40}t)\mathbf{u}(t - \frac{\pi}{2})$. The inner plot depicts the CAN bus delay δ_i versus time resulting from a fixed bus load of 50%.

VII. Further Remarks and Discussion

The Impact of Environmental Disturbances on Algorithm 1: As long as the environmental disturbances acting on the lateral dynamics of the vehicle (e.g., due to side-wind gusts as discussed in Section VI) manifest themselves as a time-varying additive input in the form

$$\dot{\mathbf{x}} = \mathbf{A}_\ell(t)\mathbf{x} + \mathbf{d}_e(t), \tag{50}$$

the monitoring Algorithm 1 is capable of attributing the anomalies in $\mathbf{A}_\ell(t)$ to a cyber-physical attack targeting the

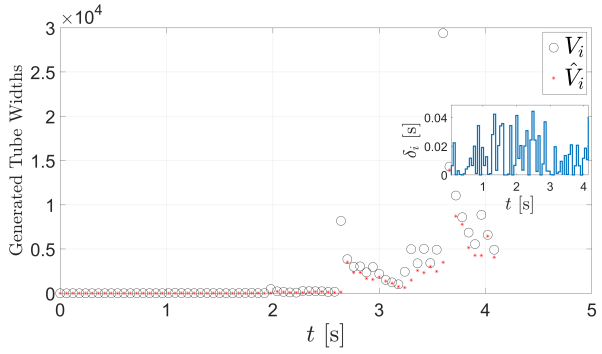


Fig. 16: The sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 1.5 \times 10^{-3}\sin^2(10t)$ and $\lambda_f(t) = 10^{-3}(t-\frac{\pi}{2})^2\cos^4(\sqrt{40}t)\mathbf{u}(t-\frac{\pi}{2})$. The inner plot depicts the CAN bus delay δ_i versus time resulting from a uniformly distributed bus load varying between 0% and 100%.

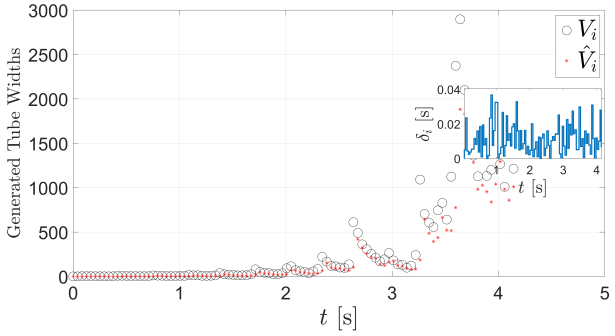


Fig. 17: The sequence of the tube widths V_i, $\hat{V}_i$ generated by Algorithm 1 under $\lambda_r(t) = 1.5 \times 10^{-3}\sin^2(10t)$ and $\lambda_f(t) = 10^{-3}(t-\frac{\pi}{2})^2\cos^4(\sqrt{40}t)\mathbf{u}(t-\frac{\pi}{2})$. The inner plot depicts the CAN bus delay δ_i versus time resulting from a normally distributed bus load with a mean of 50% and a standard deviation of 20%.

braking/ABS system of the vehicle without even the need for knowing $\mathbf{d}_e(t)$ (recall that Algorithm 1 only needs the samples $\mathbf{A}_\ell(t_i)$). Nevertheless, variations in the road conditions, which perturb the entries of $\mathbf{A}_\ell(t)$ and result in destabilization of the lateral dynamics, will only lead to issuance of warning signals by Algorithm 1. To provide a definitive answer to whether there exists a cyber-physical threat against the braking/ABS system in such a scenario, on-board road condition monitoring systems relying on additional sensor readings such as dashcam videos and GPS/IMU sensors along with machine learning algorithms (see, e.g., [54]–[56]) should work concurrently with Algorithm 1. For instance, one can utilize an additional artificial neural network-based algorithm, which has been trained on various road condition datasets. If no change in road conditions is detected, then a warning signal issued by Algorithm 1 will be indicative of a cyber-physical attack against the braking/ABS system.

Extensions to Electric Vehicles: When utilized for anti-lock braking or traction control, the dynamic performance of on-board electric powertrains can be affected by the torsional dynamics of the half-shafts, which connect the motor and

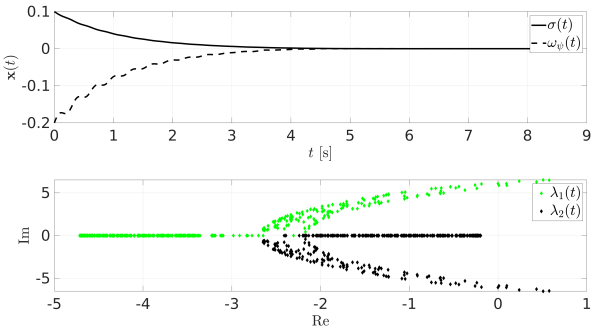


Fig. 18: (Upper) The time profiles of $\omega_\psi(t)$ and $\sigma(t)$ under periodically time-varying longitudinal time profiles $\lambda_r(t) = 1.5 \times 10^{-3}\sin^2(10t)$ and $\lambda_f(t) = 10^{-3}(t-\frac{\pi}{2})^2\cos^4(\sqrt{40}t)\mathbf{u}(t-\frac{\pi}{2})$ with $\sigma(0) = 0.1$, $\omega_\psi(0) = -0.2$. (Lower) The locus of the frozen-time eigenvalues of $\mathbf{A}_\ell(t)$.

transmission to the wheels. Therefore, to extend the method of analysis in this paper to electric vehicles, one should additionally take into account wheel slip dynamics that impact on-board electric drivetrain layouts with significant torsional dynamics (see, e.g., [57], [58] for further details).

Extensions to Autonomous Vehicles: To increase the safety of autonomous vehicle operations, fail safe technologies such as using dual winding (DW) motors in integrated electric brake (IEB) systems have been proposed in the literature (see, e.g., [59]). Under cyber-physical attack scenarios against IEB system of autonomous vehicles, the dynamics of DW motors and their overheating under successful attacks should be additionally taken into consideration.

VIII. Conclusion

This paper investigated the safety-critical issue of indirect destabilization of a target vehicle lateral motion under braking system/ABS attacks, where the adversary is improperly engaging the braking system/ABS. We demonstrated that if an attacker manages to continuously vary the longitudinal slips of the wheels, they can violate the necessary conditions for asymptotic stability of the vehicle lateral motion LTV dynamics. Furthermore, we derived the minimal perturbations of the wheel longitudinal slips that result in lateral motion instability under fixed longitudinal slip values. Such a minimal perturbation enables the braking/ABS attacker to destabilize the lateral motion of the vehicle without having to induce wheel lockup conditions. Finally, we devised a real-time algorithm for monitoring the lateral motion dynamics of vehicles against braking/ABS cyber-physical attacks. This numerical algorithm, which can be efficiently computed using the modest computational resources of automotive embedded processors, can inform higher-level supervisory modules of the vehicle about impending instability of the vehicle lateral motion due to the time-varying behavior of the longitudinal wheel slip values induced by a braking system/ABS attacker. This real-time monitoring algorithm can be utilized along with other intrusion detection techniques to infer whether a vehicle braking system/ABS is experiencing a cyber-physical attack.

Future research should consider integration of the developed control theory-based real-time monitoring algorithm in this paper with physical finger printing-based intrusion detection techniques (see, e.g., [60], [61]) and CAN bus traffic/load monitoring-based security tools (see, e.g., [62]) from the cybersecurity forensics literature.

APPENDIX A
ADMM-BASED EMBEDDED ALGORITHM FOR QP (34)

We follow [42] to derive our embedded solver algorithm. One first needs to define and compute the matrices and vectors

$$\mathbf{F}_e = [\nu_1,\, \nu_2]^\top \in \mathbb{R}^{2\times 1}, \tag{51a}$$

$$\mathbf{g}_e = [\lambda_f(t^*),\, 1-\lambda_f(t^*),\, \lambda_r(t^*),\, 1-\lambda_r(t^*)]^\top \in \mathbb{R}^{4\times 1}, \tag{51b}$$

$$\mathbf{G}_e = \begin{bmatrix} -1 & 0 \\ 1 & 0 \\ 0 & -1 \\ 0 & 1 \end{bmatrix} \in \mathbb{R}^{4\times 2}, \tag{51c}$$

$$\mathbf{A}_e = \begin{bmatrix} \mathbf{G}_e \\ \mathbf{F}_e^\top \end{bmatrix} \in \mathbb{R}^{5\times 2}, \tag{51d}$$

$$\mathbf{B}_e = \begin{bmatrix} \mathbf{I}_4 \\ \mathbf{0} \end{bmatrix} \in \mathbb{R}^{5\times 4}, \tag{51e}$$

$$\mathbf{c}_e = [\mathbf{g}_e^\top,\, \mathrm{tr}\left(\mathbf{A}_\ell(t^*)\right)]^\top \in \mathbb{R}^{5\times 1}, \tag{51f}$$

$$\bar{\mathbf{M}} = -\rho(\mathbf{I}_2 + \rho\mathbf{A}^\top\mathbf{A})^{-1}\mathbf{A}^\top \in \mathbb{R}^{2\times 5} \tag{51g}$$

where the parameter ρ, which determines the convergence rate of the ADMM iterative algorithm, needs to be computed according to the following procedure. Recall that $[\nu_1,\, \nu_2]^\top := [\kappa_f b_f,\, \kappa_r b_r]^\top$. Therefore, $\mathbf{F}_e$, $\mathbf{g}_e$, and $\mathrm{tr}\left(\mathbf{A}_\ell(t^*)\right)$ are physically meaningful quantities, which play a fundamental role in the stability of the lateral dynamics of the vehicle as discussed in II-B. The matrices/vectors in (51) need to be *computed only once* in each call of the ADMM Algorithm 2.

Calculating ρ: According to [42], the constant $\rho > 0$, should be chosen such that the nonzero eigenvalues of $\rho\mathbf{A}_e(\mathbf{I}_2 + \rho\mathbf{A}_e^\top\mathbf{A}_e)^{-1}\mathbf{A}_e^\top$ are as close to $\frac{1}{2}$ as possible. Thankfully, in the case of the matrices in (51), the two aforementioned non-zero eigenvalues can be computed analytically. These two eigenvalues are equal to $\frac{2\rho}{2\rho+1}$ and $1-\frac{1}{\rho\nu_1^2+\rho\nu_2^2+2\rho+1}$, respectively. Therefore, the optimal ρ minimizing $\left(\frac{1}{2}-\frac{2\rho}{2\rho+1}\right)^2 + \left(\frac{1}{2}-\frac{1}{\rho\nu_1^2+\rho\nu_2^2+2\rho+1}\right)^2$ can be computed to be equal to $\rho^\star = 0.5$.

The iterative Algorithm 2 is well-suited for implementation on embedded processors (e.g., microprocessors and FPGAs). It takes as input the matrices/vectors defined in (51) and two constant tolerances ϵ_{dual}, ϵ_{primal}. In Algorithm 2, k is the counter, $\mathbf{z}_k$ is the vector of slack variables for taking into account the inequalities $-\lambda_i(t^*) \le \Delta\lambda_i \le 1-\lambda_i(t^*)$ in (34), and $\boldsymbol{\tau}_k := [\boldsymbol{\tau}_k^{g\top},\, \tau_k^f]^\top$ is the vector of the scaled dual variables, where $\boldsymbol{\tau}_k^g$ is the vector of $\boldsymbol{\tau}_k$ first four elements.

Algorithm 2: ADMM-based Algorithm for Solving the QP in (34)

Data: The matrices and vectors given by (51) and residual and primal tolerances ϵ_{dual}, ϵ_{primal}
Result: Minimal destabilizing perturbation vector $\Delta\boldsymbol{\lambda}$ (solution to (34))
Initialization: $\Delta\boldsymbol{\lambda}_0 \in \mathbb{R}^2$, $\mathbf{z}_0 \in \mathbb{R}^4$, and $\boldsymbol{\tau}_0 \in \mathbb{R}^5$, $k = 0$ (cold start)
while $\|\mathbf{A}_e\Delta\boldsymbol{\lambda}_k + \mathbf{B}_e\mathbf{z}_k - \mathbf{c}_e\| \ge \epsilon_{primal}$ ***OR*** $\|\rho\mathbf{A}_e^\top\mathbf{B}_e(\mathbf{z}_{k+1}-\mathbf{z}_k)\| \ge \epsilon_{dual}$ **do**

$$\Delta\boldsymbol{\lambda}_{k+1} = -\bar{\mathbf{M}}_e\mathbf{c}_e + \bar{\mathbf{M}}_e\left(\begin{bmatrix}\mathbf{z}_k \\ 0\end{bmatrix} + \boldsymbol{\tau}_k\right)$$

$$\mathbf{z}_{k+1} = \max\left\{\mathbf{0}, -\mathbf{G}_e\Delta\boldsymbol{\lambda}_{k+1} - \boldsymbol{\tau}_k^g + \mathbf{g}_e\right\}$$

$$\boldsymbol{\tau}_{k+1} = \boldsymbol{\tau}_k + \mathbf{A}_e\Delta\boldsymbol{\lambda}_{k+1} + \mathbf{B}_e\mathbf{z}_{k+1} - \mathbf{c}_e$$

end

REFERENCES

[1] J. Huang, M. Zhao, Y. Zhou, and C.-C. Xing, "In-vehicle networking: Protocols, challenges, and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 92–98, 2018.

[2] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Comput. Secur.*, p. 102150, 2021.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Secur. Symp.*, vol. 4. San Francisco, 2011, pp. 447–462.

[4] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Int. Conf. Cryptogr. Hardw. Embed. Syst.* Springer, 2013, pp. 55–72.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *The Ethics of Information Technologies*. Routledge, 2020, pp. 119–134.

[6] A. Mohammadi, H. Malik, and M. Abbaszadeh, "Generation of wheel lockup attacks on nonlinear dynamics of vehicle traction," in *2022 American Contr. Conf.* IEEE, 2022, pp. 1994–1999.

[7] A. Mohammadi and H. Malik, "Vehicle lateral motion stability under wheel lockup attacks," in *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022*, San Diego, CA, 2022, doi: https://dx.doi.org/10.14722/autosec.2022.23010.

[8] L. Kang and H. Shen, "Detection and mitigation of sensor and CAN bus attacks in vehicle anti-lock braking systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 6, no. 1, pp. 1–24, 2022.

[9] A. Sarker, H. Shen, C. Qiu, H. Uehara, and K. Zhang, "Brake signal-based driver's location tracking in usage-based auto insurance programs," *IEEE Internet Things J.*, 2023, doi:10.1109/JIOT.2023.3237759.

[10] S. Fröschle and A. Stühring, "Analyzing the capabilities of the CAN attacker," in *Eur. Symp. Res. Comput. Secur.*, 2017, pp. 464–482.

[11] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.

[12] C. Miller, "Lessons learned from hacking a car," *IEEE Des. Test*, vol. 36, no. 6, pp. 7–9, 2019.

[13] E. Nekouei, M. Pirani, H. Sandberg, and K. H. Johansson, "A randomized filtering strategy against inference attacks on active steering control systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 16–27, 2021.

[14] R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 1727–1736, 2020.

[15] G. A. Magallan, C. H. De Angelo, and G. O. Garcia, "Maximization of the traction forces in a 2WD electric vehicle," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 369–380, 2010.

[16] E. Dinçmen, B. A. Güvenç, and T. Acarman, "Extremum-seeking control of abs braking in road vehicles with lateral force improvement," *IEEE Trans. Contr. Syst. Technol.*, vol. 22, no. 1, pp. 230–237, 2012.

[17] J. Yi and E. H. Tseng, "Nonlinear stability analysis of vehicle lateral motion with a hybrid physical/dynamic tire/road friction model," in *Dyn. Syst. Contr. Conf.*, vol. 48920, 2009, pp. 509–516.

[18] J. Yi, J. Li, J. Lu, and Z. Liu, "On the stability and agility of aggressive vehicle maneuvers: a pendulum-turn maneuver example," *IEEE Trans. Contr. Syst. Technol.*, vol. 20, no. 3, pp. 663–676, 2011.

[19] J. Li, Y. Zhang, and J. Yi, "A hybrid physical-dynamic tire/road friction model," *J. Dyn. Syst. Meas. Contr.*, vol. 135, no. 1, p. 011007, 2013.

[20] S. C. Johnson, M. Wicks, M. Žefran, and R. A. DeCarlo, "The structured distance to the nearest system without property $\mathcal{P}$," *IEEE Trans. Automat. Contr.*, vol. 63, no. 9, pp. 2960–2975, 2018.

[21] M. A. Hitz and E. Kaltofen, "Efficient algorithms for computing the nearest polynomial with constrained roots," in *Proc. 1998 Int. Symp. Symb. Algebr. Comput.*, 1998, pp. 236–243.

[22] V. Katewa and F. Pasqualetti, "On the real stability radius of sparse systems," *Automatica*, vol. 113, p. 108685, 2020.

[23] R. Zhang and P. Venkitasubramaniam, "Stealthy control signal attacks in linear quadratic gaussian control systems: Detectability reward tradeoff," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1555–1570, 2017.

[24] E. Kontouras, A. Tzes, and L. Dritsas, "Impact analysis of a bias injection cyber-attack on a power plant," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 11 094–11 099, 2017.

[25] X. Wang, X. Luo, X. Pan, and X. Guan, "Detection and location of bias load injection attack in smart grid via robust adaptive observer," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4454–4465, 2020.

[26] A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, and A. Youssef, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 10.

[27] P. S. Pessim and M. J. Lacerda, "State-feedback control for cyber-physical LPV systems under DoS attacks," *IEEE Contr. Syst. Lett.*, vol. 5, no. 3, pp. 1043–1048, 2020.

[28] P. Mullhaupt, D. Buccieri, and D. Bonvin, "A numerical sufficiency test for the asymptotic stability of linear time-varying systems," *Automatica*, vol. 43, no. 4, pp. 631–638.

[29] B. Zhou, "On asymptotic stability of linear time-varying systems," *Automatica*, vol. 68, pp. 266–276, 2016.

[30] R. Vrabel, "A note on uniform exponential stability of linear periodic time-varying systems," *IEEE Trans. Automat. Contr.*, vol. 65, no. 4, pp. 1647–1651, 2019.

[31] X.-M. Zhang, Q.-L. Han, A. Seuret, F. Gouaisbaut, and Y. He, "Overview of recent advances in stability of linear systems with time-varying delays," *IET Contr. Theory Appl.*, vol. 13, no. 1, pp. 1–16, 2019.

[32] H. Rosenbrock, "The stability of linear time-dependent control systems," *Int. J. Electronics*, vol. 15, no. 1, pp. 73–80, 1963.

[33] ——, "A Lyapunov function for some naturally-occurring linear homogeneous time-dependent equations," *Automatica*, vol. 1, no. 2-3, pp. 97–109, 1963.

[34] C. Desoer, "Slowly varying system $\dot{x} = A(t)x$," *IEEE Trans. Automat. Contr.*, vol. 14, no. 6, pp. 780–781, 1969.

[35] A. Kott, B. Blakely, D. Henshel, G. Wehner, J. Rowell, N. Evans, L. Muñoz-González, N. Leslie, D. W. French, D. Woodard *et al.*, "Approaches to enhancing cyber resilience: report of the North Atlantic Treaty organization (NATO) workshop IST-153," *arXiv preprint arXiv:1804.07651*, 2018.

[36] S. Mammar, S. Glaser, and M. Netto, "Vehicle lateral dynamics estimation using unknown input proportional-integral observers," in *2006 American Contr. Conf.* IEEE, 2006, pp. 4658–4663.

[37] R. Rajamani, G. Phanomchoeng, D. Piyabongkarn, and J. Y. Lew, "Algorithms for real-time estimation of individual wheel tire-road friction coefficients," *IEEE/ASME Trans. Mechatron.*, vol. 17, no. 6, pp. 1183–1195, 2011.

[38] K. Nam, H. Fujimoto, and Y. Hori, "Lateral stability control of in-wheel-motor-driven electric vehicles based on sideslip angle estimation using lateral tire force sensors," *IEEE Trans. Veh. Technol.*, vol. 61, no. 5, pp. 1972–1985, 2012.

[39] M. J. Giummarra, B. Beck, and B. J. Gabbe, "Classification of road traffic injury collision characteristics using text mining analysis: Implications for road injury prevention," *PLOS One*, vol. 16, no. 1, p. e0245636, 2021.

[40] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Upper Saddle River, New Jersey: Prentice Hall, 2002.

[41] M.-Y. Wu, "On stability of linear time-varying systems," *Int. J. Syst. Sci.*, vol. 15, no. 2, pp. 137–150, 1984.

[42] T. V. Dang, K. V. Ling, and J. M. Maciejowski, "Embedded ADMM-based QP solver for MPC with polytopic constraints," in *2015 Eur. Control Conf. (ECC)*. IEEE, 2015, pp. 3446–3451.

[43] J. L. Jerez, P. J. Goulart, S. Richter, G. A. Constantinides, E. C. Kerrigan, and M. Morari, "Embedded online optimization for model predictive control at megahertz rates," *IEEE Trans. Autom. Contr.*, vol. 59, no. 12, pp. 3238–3251, 2014.

[44] M. Garrido, P. Källström, M. Kumm, and O. Gustafsson, "CORDIC II: a new improved CORDIC algorithm," *IEEE Trans. Circuits Syst. II: Express Br.*, vol. 63, no. 2, pp. 186–190, 2015.

[45] K. Tindell, H. Hanssmon, and A. J. Wellings, "Analysing real-time communications: controller area network (CAN)," in *1994 Proc. Real-Time Syst. Symp. (RTSS)*. IEEE, 1994, pp. 259–263.

[46] R. De Andrade, K. N. Hodel, J. F. Justo, A. M. Laganá, M. M. Santos, and Z. Gu, "Analytical and experimental performance evaluations of CAN-FD bus," *IEEE Access*, vol. 6, pp. 21 287–21 295, 2018.

[47] P. M. Lima, M. V. Alves, L. K. Carvalho, and M. V. Moreira, "Security of cyber-physical systems: Design of a security supervisor to thwart attacks," *IEEE Trans. Autom. Sci. Eng.*, vol. 19, no. 3, pp. 2030–2041, 2021.

[48] H. Mirzaeinejad and M. Mirzaei, "A novel method for non-linear control of wheel slip in anti-lock braking systems," *Contr. Eng. Pract.*, vol. 18, no. 8, pp. 918–926, 2010.

[49] V. Cerone, M. Milanese, and D. Regruto, "Yaw stability control design through a mixed-sensitivity approach," *IEEE Trans. Contr. Syst. Technol.*, vol. 17, no. 5, pp. 1096–1104, 2009.

[50] S. Sadasivan, "White Paper: An Introduction to the ARM Cortex-M3 Processor," Arm Ltd., Tech. Rep., 10 2006.

[51] M. Dunne and S. Fischmeister, "Powertrace-based fuzzing of CAN connected hardware," in *2022 IEEE Int. Conf. Cyber Secur. Resil. Technol. (CSR)*. IEEE, 2022, pp. 239–244.

[52] F. Pollicino, D. Stabili, L. Ferretti, and M. Marchetti, "Hardware limitations to secure C-ITS: Experimental evaluation and solutions," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12 946–12 959, 2021.

[53] Mathworks. (2023) Build and run executable on ARM Cortex-M3 QEMU emulator. Accessed on: 06/12/2023. [Online]. Available: https://www.mathworks.com/help/supportpkg/armcortexm/ug/build-and-run-executable-on-arm-cortex-m-processors.html

[54] M. Simoncini, D. C. de Andrade, S. Salti, L. Taccari, F. Schoen, and F. Sambo, "Two-stream neural architecture for unsafe maneuvers classification from dashcam videos and GPS/IMU sensors," in *2020 IEEE 23rd Int. Conf. Intell. Transp. Syst. (ITSC)*. IEEE, 2020, pp. 1–6.

[55] N. Xu, Z. Tang, H. Askari, J. Zhou, and A. Khajepour, "Direct tire slip ratio estimation using intelligent tire system and machine learning algorithms," *Mech. Syst. Signal Process.*, vol. 175, p. 109085, 2022.

[56] E. Ranyal, A. Sadhu, and K. Jain, "Road condition monitoring using smart sensing and artificial intelligence: A review," *Sensors*, vol. 22, no. 8, p. 3044, 2022.

[57] S. De Pinto, C. Chatzikomis, A. Sorniotti, and G. Mantriota, "Comparison of traction controllers for electric vehicles with on-board drivetrains," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 6715–6727, 2017.

[58] F. Bottiglione, A. Sorniotti, and L. Shead, "The effect of half-shaft torsion dynamics on the performance of a traction control system for electric vehicles," *Proc. Inst. Mech. Eng. D: J. Automob. Eng.*, vol. 226, no. 9, pp. 1145–1159, 2012.

[59] K.-y. Hwang, S.-i. Kim, and B.-k. Song, "Single winding type determination of dual winding three-phase motor considering overheat problem in integrated electric braking system of autonomous vehicles," *IEEE Trans. Transp. Electrif.*, 2022.

[60] P. M. S. Sánchez, J. M. J. Valero, A. H. Celdrán, G. Bovet, M. G. Pérez, and G. M. Pérez, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 2, pp. 1048–1077, 2021.

[61] M. L. Han, B. I. Kwak, and H. K. Kim, "Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2941–2956, 2021.

[62] M. Marchetti and D. Stabili, "READ: Reverse engineering of automotive data frames," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 1083–1097, 2018.