Generation of CAN-based Wheel Lockup Attacks on the Dynamics of Vehicle Traction

A. Mohammadi[†],
H. Malik
University of Michigan-Dearborn
{amohmmad,hafiz}@umich.edu

M. Abbaszadeh
GE Global Research
abbaszadeh@ge.com

Abstract—**Recent automotive hacking incidences have demonstrated that when an adversary manages to gain access to a safety-critical CAN, severe safety implications will ensue. Under such threats, this paper explores the capabilities of an adversary who is interested in engaging the car brakes at full speed and would like to cause wheel lockup conditions leading to catastrophic road injuries. This paper shows that the physical capabilities of a CAN attacker can be studied through the lens of closed-loop attack policy design. In particular, it is demonstrated that the adversary can cause wheel lockups by means of closed-loop attack policies for commanding the frictional brake actuators under a limited knowledge of the tire-road interaction characteristics. The effectiveness of the proposed wheel lockup attack policy is shown via numerical simulations under different road conditions.**

I. Introduction

One of the most widely utilized bus types in in-vehicle networks through which electronic control units (ECUs) communicate with each other is called Controller Area Network (CAN) [1]. There exists a well-established line of work documenting how hackers/adversaries can access the CAN bus (see, e.g., [2]–[7]). Figure 1(left) depicts some possible scenarios through which hackers can access the CAN bus. Having access to the CAN bus, the adversary can easily sniff the CAN packets, which are broadcast to all components on the CAN bus, and/or inject CAN packets onto the CAN bus while masquerading as a legitimate car ECU [8]. Furthermore, there is the possibility of re-flashing the compromised ECUs by the adversaries (see, e.g., [9], [10] and the celebrated hack by Miller and Valasek [7]). A frightening feature of the attacks outlined by Miller and Valasek is that they are almost invisible to the driver while almost no forensic evidence is left behind [5]–[7].

The cyber-physical implications of the aforementioned threats, such as remotely steering a vehicle into a ditch as demonstrated by Miller and Valasek [5], [7], lead to the natural question posed by Fröschle and Stühring [8]: "Once an attacker has made it to the last stage, what exactly are his capabilities?" This paper provides an answer to this question by investigating the cyber-physical threat of an adversary through the lens of closed-loop attack policy design for the braking actuators. In particular, this paper investigates the capabilities of an adversary who has taken over the braking ECUs and is trying to induce wheel lockup during braking.

In this paper, we demonstrate that the adversary with a very limited knowledge of the tire-road interaction characteristics can induce wheel lockup through a properly designed closed-loop attack policy for the braking actuators. The attack policy utilizes a feedback and a feedforward control action simultaneously. The feedback control input is generated through a predefined-time controller [12] that can cause wheel lockups if the tire-road interaction characteristics and other relevant parameters in the vehicle traction dynamics are completely known. Against the lack of such information, it is shown that the adversary can employ an additional feedforward control input that is generated by a nonlinear disturbance observer (NDOB) (see, e.g., the references [13], [14]). The NDOB will compensate for the adversarial limited knowledge of the vehicle traction dynamics.

This paper adds to the body of literature on physical attack generation against nonlinear dynamical systems in the context of automotive cybersecurity as follows. Using the available results in the automotive cybersecurity literature, the cyber-physical threat of an adversary is modeled as a closed-loop attack policy design on the vehicle actuators (braking actuators in this paper). Moreover, this paper investigates the physical capabilities of an adversary who has a limited knowledge of the vehicle traction dynamics and the tire-road interaction characteristics in terms of inducing wheel lockup conditions in a finite time interval.

The rest of this paper is organized as follows. First, we present a variety of possible hacking scenarios from the literature for accessing the braking actuators in II. Next, we present the nonlinear dynamical model of the vehicle traction dynamics and a frictional brake actuator dynamical model in Section III. Then, we formulate the wheel lockup attack policy objective under uncertain tire-road friction characteristics in Section IV. Thereafter, in Section V, we present our attack policy based on using predefined-time controllers and NDOBs, which are validated through simulation results in Section VI.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, Virtual
ISBN 1-891562-75-4
https://dx.doi.org/10.14722/autosec.2022.23025
www.ndss-symposium.org

[†] A. Mohammadi is the corresponding author.

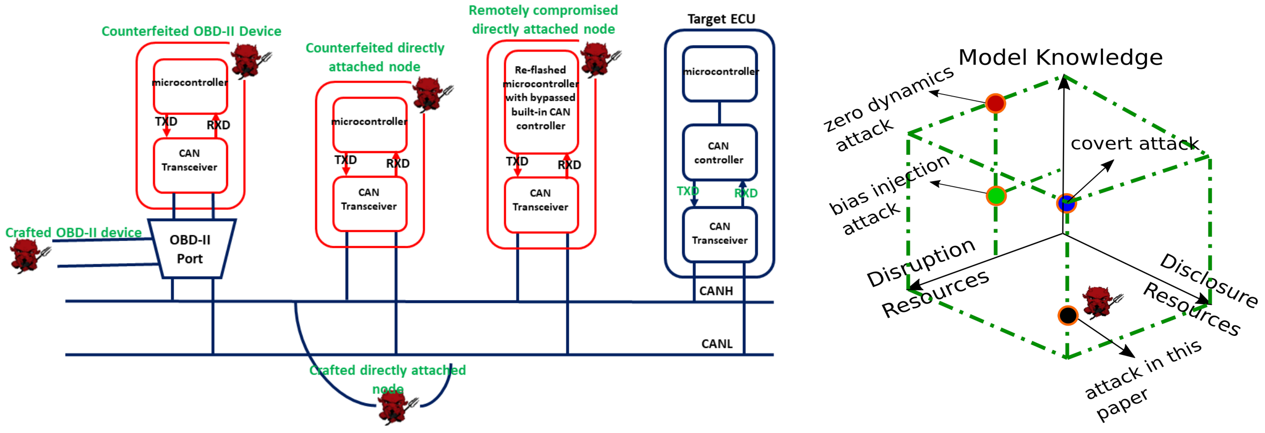

Fig. 1: Cyber-physical attacks on the CAN bus: (left) examples of attacking nodes architectures (recreated from [9]); (right) classification of the proposed braking actuator attack policy by locating it within the cyber-physical attack space due to Teixeira *et al.* [11].

Finally, we conclude the paper with further remarks and future research directions in Section VII.

II. Modeling the Physical Capabilities of a CAN Attacker as a Closed-Loop Attack Policy

In this section we briefly review a variety of security threats to automotive CAN networks that an adversary can exploit for targeting the braking ECUs (see, e.g., [7]–[9] for further details). This section also provides a justification for modeling the cyber-physical threat capabilities of an adversary as a closed-loop attack policy design for the vehicle actuators.

Under certain assumptions, Fröschle and Stühring [8] have outlined a collection of six possible attacks on the CAN bus with cyber-physical implications. These attacks include: (i) blocking messages by priority; (ii) disrupting the target network; (iii) silencing a target node by dominant bits; (iv) silencing a target node by collisions; (v) suppressing a target message; and (vi) modification attacks via either impersonating a target node or modifying target messages by suppress and inject. Through a combination of these six attacks, Fröschle and Stühring [8] investigate the cyber-physical implications for manipulation of steering and braking, e.g., steering a Jeep at any speed. The systemic investigation by Fröschle and Stühring [8] was motivated by the celebrated hack of Miller and Valasek [5], [7], in which remote re-flashing of the firmware of a target microcontroller was demonstrated.

Under the assumption of re-flashing the firmware of a target braking ECU, the adversary threat capability can be modeled by assuming complete authority over the brake actuators and full knowledge of the states of the vehicle traction dynamics by reading from the in-vehicle network, e.g., the CAN bus. *In essence, the adversary can act as a feedback controller by sending malicious commands to the brake actuators while using the sensed states of the vehicle for computing these commands.* In general, the adversary does have a very limited knowledge of the plant dynamics and its interactions with the ambient environment (vehicle traction dynamics and its interaction with the road). Consequently, the closed-loop attack policies on a vehicle actuator can be located within the cyber-physical attack space due to Teixeira *et al.* [11] according to Figure 1(right).

III. Vehicle Traction Dynamical Model

In this section, we provide a brief overview of the single-wheel model of rubber-tired vehicles that are subject to straight-ahead braking conditions. This single-wheel dynamic model can capture the steady and transient tractive performance while demonstrating how a vehicle can undergo lockup or stable braking [15]–[18]. The dynamic states are often chosen to be the tire/wheel rate of rotation and the forward vehicle speed. Hence, the quarter-car dynamics that govern the vehicle longitudinal motion during braking are given by (see, e.g., [16], [17])

$$\dot{v} = -g_\alpha \mu(\lambda) - \frac{\Delta_v(t,v)}{M}, \tag{1a}$$

$$\dot{\omega} = \frac{M g_\alpha r}{J}\mu(\lambda) - \frac{T_a}{J} - \frac{\Delta_w(t,\omega)}{J}, \tag{1b}$$

where the parameters M, r, and J are the quarter-car mass, wheel radius, and wheel inertia, respectively. Additionally, during braking, the vehicle speed v and the wheel rotational speed ω vary within in the set $\mathcal{D}_b := \{(v,\omega) | v > 0,\ 0 \leq r\omega \leq v\}$. The braking torque T_a is the input to the dynamical system in (1). Furthermore, the longitudinal slip λ that determines whether the wheel is locked is given by

$$\lambda := \frac{v - r\omega}{\max(v, r\omega)}. \tag{2}$$

While braking actuators are engaged, we have $\lambda = \frac{v - r\omega}{v}$ and $(v,\omega) \in \mathcal{D}_b$. It follows that $\lambda \in [0,1]$ during braking. We let the constant g_α denote $g\cos(\alpha)$ where α is the road slope. Finally, $\mu(\lambda)$, $\Delta_v(t,v)$, and $\Delta_w(t,\omega)$ denote the uncertain nonlinear friction coefficient, the force, and the torque disturbances resulting from unmodeled dynamics, respectively.

There are a variety of ways to represent the function $\mu(\cdot)$ including the Magic Formula and Burckhardt representation (see, e.g., [19]). For instance, equations like Burckhardt model (see, e.g., [20]) where

$$\mu(\lambda) = c_1(1 - \exp(-c_2\lambda)) - c_3\lambda, \tag{3}$$

are empirical equations based on fitting coefficients that are widely utilized for modeling the interaction between the road pavement and tire tread. The longitudinal force on the tire arising from this interaction is computed by $-\mu(\lambda)g_\alpha$.

In this paper, we do not assume any particular closed-form representation for the nonlinear friction coefficient function $\mu(\cdot)$ and only assume that $\mu : \Lambda \to \mathbb{R}$ is a continuous function on the closed interval $\Lambda := [0,1]$. Accordingly, $\mu(\cdot)$ attains its maximum μ_{max} and minimum μ_{min} on the closed interval Λ because of the well-known properties of continuous functions on compact sets.

It will be assumed that the disturbances $\Delta_v(t,v)$, and $\Delta_w(t,\omega)$ satisfy the following uniform bounds (see, e.g., [17])

$$\begin{aligned} |\Delta_v(t,v)| \leq \bar{\Delta}_v,\ |\Delta_w(t,\omega)| \leq \bar{\Delta}_\omega, \\ \text{for all } (t,v,\omega) \in [0,\infty) \times \mathcal{D}_b. \end{aligned} \tag{4}$$

It is possible to transform the longitudinal dynamics by a change of coordinates from (v,ω) to (v,λ). Under this change of coordinates, the longitudinal dynamics become (see, e.g., [15], [17] for the details of derivation)

$$\dot{v} = -g_\alpha \mu(\lambda) - \frac{\Delta_v(t,v)}{M}, \tag{5a}$$

$$\dot{\lambda} = \frac{g_\alpha}{v}\big\{(\lambda - 1 - \nu)\mu(\lambda) + \Upsilon_a + \Upsilon_{\Delta,w} + (\lambda - 1)\Upsilon_{\Delta,v}\big\}, \tag{5b}$$

where $\nu := \frac{MR^2}{J}$ is the dimensionless ratio of vehicle to wheel inertia, $\Upsilon_a := \frac{r}{J g_\alpha} T_a$ is the dimensionless brake torque, and $\Upsilon_{\Delta,w} := \frac{r}{J g_\alpha}\Delta_w(t,\omega)$, $\Upsilon_{\Delta,v} := \frac{\Delta_v(t,v)}{M g_\alpha}$ are the dimensionless force and torque disturbances acting on speed and slip dynamics, respectively.

The dynamical equations in (1) and (5) capture the coupling in-between the wheel slip λ dynamics with that of the vehicle speed v in case of (5), or the tire/wheel angular speed ω dynamics with that of the vehicle speed v in case of (1). In (v,λ) coordinates, the set $\mathcal{D}_b$ reads as

$$\mathcal{D}_b = \big\{(v,\lambda)\big|v > 0,\ \lambda \in \Lambda := [0,1]\big\}. \tag{6}$$

Using the brake input Υ_a, the adversary would like to induce unstable braking conditions corresponding to lockup. The most severe case of lockup happens when $\lambda = 1$. Therefore, following Olson *et al.* [15], we define **the lockup manifold** in the following way

$$\mathcal{W}_b^L := \big\{(v,\lambda)\big|v > 0,\ \lambda = 1\big\}. \tag{7}$$

Remark 3.1: It is remarked that the adversary can choose the slip reference value λ^{r} in advance, which can belong to the interval $[0,1]$. The closer λ^{r} to one, the closer the wheel to the condition of lockup. Without loss of generality, we assume that λ^{r} has been chosen to be equal to one.

To model the adversarial disruption resources, we assume that the reference malicious command generated by the attack policy $\hat{\Upsilon}_a$ passes through the following first-order delay system (see, e.g., [17], [18])

$$\tau_f \dot{\Upsilon}_a = -\Upsilon_a + \hat{\Upsilon}_a(t - \delta_f), \tag{8}$$

to generate the frictional braking torque response Υ_a, which then gets applied to the traction dynamics in (5). It is remarked that the attacker does not have any knowledge of either the friction brake time constant τ_f or the friction brake deadtime δ_f. In designing our attack policies in the next section, we assume that $\tau_f \approx 0$ and $\delta_f \approx 0$. However, the simulation results in Section VI demonstrate the effectiveness of the attack policies when these assumptions do not hold.

IV. Attack Policy Objectives

In this section we formulate the attack policy objectives and state our assumptions about the adversarial knowledge of the vehicle dynamical model.

Following the notation by Teixeira *et al.* [11], we denote the vehicle traction dynamics in (5) by $\mathcal{P}$. Moreover, we let the attacker's *a priori* knowledge model $\hat{\mathcal{P}}$ be given by

$$\dot{v} = -g_\alpha \hat{\mu}(\lambda), \tag{9a}$$

$$\dot{\lambda} = \frac{g_\alpha}{v}\big\{(\lambda - 1 - \hat{\nu})\hat{\mu}(\lambda) + \hat{\Upsilon}_a\big\}, \tag{9b}$$

where the adversary has no *a priori knowledge* of the dimensionless torque and force disturbances $\Upsilon_{\Delta,w}$, $\Upsilon_{\Delta,v}$. Furthermore, the adversary has only an approximate knowledge of the tire-road interaction characteristics given by $\hat{\mu}(\lambda)$. When the adversary does not have any knowledge of $\mu(\lambda)$, the friction coefficient $\hat{\mu}(\lambda)$ is set equal to 0 in $\hat{\mathcal{P}}$. We assume that the adversary knows and/or can compute the vehicle velocity as well as the wheel slip. This scenario corresponds to having complete access to disclosure resources in the cyber-attack space [11].

Wheel Lockup Attack Policy Objective. Given the vehicle longitudinal dynamics $\mathcal{P}$ in (5), the attacker's *a priori* knowledge $\hat{\mathcal{P}}$ in (9), and the braking response in (8), design an attack policy $\hat{\Upsilon}_a$ such that the trajectories of the vehicle longitudinal dynamics during braking converge to any sufficiently close neighborhood of the lockup manifold $\mathcal{W}_b^L$ within a finite time interval.

V. Attack Policy Design

In this section, we present an attack policy that can achieve the wheel lockup attack policy objective in the previous section. The proof of the stated propositions are removed for the sake of brevity. The attack policy relies on a feedback and a feedforward control action. The feedback control input is generated through a predefined-time controller [12] that can cause wheel lockups if the tire-road interaction characteristics and other relevant parameters in the vehicle traction dynamics are completely known. Against the lack of such information, it is shown that the adversary can employ an additional feedforward control input that is generated by a nonlinear disturbance observer.

Predefined-time controller design. Following the notation in [12], we let

$$\Phi_p(x) := \frac{\exp(|x|^p)}{p}|x|^{1-p}\text{sign}(x), \tag{10}$$

for any $x \in \mathbb{R}$ and some real constant $0 < p < 1$, and

$$\Phi_1(x) := \exp(|x|)\text{sign}(x), \tag{11}$$

for any $x \in \mathbb{R}$. Furthermore, we define the lockup error as

$$e_L := \lambda - 1. \tag{12}$$

Hence, if $e_L = 0$ and $v > 0$, the wheel is in a locked stated. As it will be demonstrated in this section, if the attack objective is met, the wheel will be locked in finite time. Hence, the vehicle speed will satisfy

$$v \in [v_{\text{min}}, v_{\text{max}}], \tag{13}$$

during a successful attack, for some positive v_{min} and v_{max}.

Proposition 5.1: Consider the vehicle longitudinal dynamics $\mathcal{P}$ in (5) with the attacker's *a priori* knowledge $\hat{\mathcal{P}}$ in (9) and the frictional braking response given by (8) with $\tau_f \approx 0$ and $\delta_f \approx 0$. Suppose $\Upsilon_{\Delta,w} = 0$, $\hat{\nu} = \nu$, and $\hat{\mu}(\cdot) = \mu(\cdot)$. Additionally, assume that the uniform bound on $\Delta_v(t, v)$ given by (4) holds. Given any positive constant T_c, the attack policy

$$\hat{\Upsilon}_a = \frac{v}{g_\alpha}u^a_{np}(e_{\text{L}}) + \hat{\nu}\hat{\mu}(\lambda), \tag{14}$$

with $u^a_{np}(e_{\text{L}}) = -(\frac{1}{T_c} + kp)\Phi_p(e_L)$, where $0 < p < 1$, $k \geq k^{*\prime} := \frac{Mg_\alpha\mu_{\text{max}}+\bar{\Delta}_v}{Mv_{\text{min}}}$, and $\Phi_p(\cdot)$ given by (10), makes the lockup manifold $\mathcal{W}^L_b$ globally finite-time stable with settling-time T_c.

Remark 5.2: Proposition 5.1 assumes an almost perfect knowledge of the vehicle's model, where the only unknown is the disturbance force $\Delta_v(t, v)$ acting on the vehicle speed dynamics in (5). The next proposition removes these restrictions further.

Proposition 5.3: Consider the stated assumptions in Proposition 5.1 with $\hat{\nu}$ arbitrary, and $\Delta_w(t, \omega)$, $\Delta_v(t, v)$ satisfying (4). Furthermore, assume that $\hat{\mu} : \Lambda \to \mathbb{R}$ is a continuous function. Then, given $0 < T_c < 1$, the attack policy (14) with $u^a_{np}(e_{\text{L}}) = -k_a\text{sign}(e_L) - \frac{1}{T_c}\Phi_p(e_L)$, $0 < p < 1$, $\Phi_p(\cdot)$ given by (10), and $k_a \geq k^*$ in which

$$k^* := \frac{Mg_\alpha\mu_{\text{max}} + \bar{\Delta}_v}{Mv_{\text{min}}} + \frac{g_\alpha}{v_{\text{min}}}\left(\hat{\nu}\hat{\mu}_{\text{max}} + \nu\mu_{\text{max}} + \frac{r\bar{\Delta}_w}{Jg_\alpha}\right), \tag{15}$$

makes the lockup manifold $\mathcal{W}^L_b$ globally finite-time stable with settling-time T_c.

The following proposition, whose proof is omitted for the sake of brevity, removes the restrictions on the settling-time in Proposition 5.3.

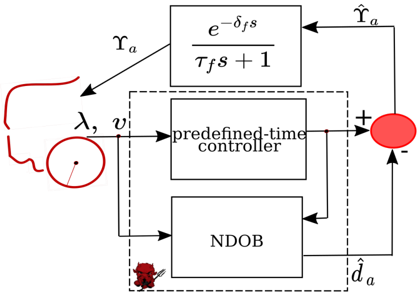
Υ_a
$\frac{e^{-\delta_f s}}{\tau_f s + 1}$
$\hat{\Upsilon}_a$
$\lambda,\ v$
predefined-time controller
+
-
NDOB
$\hat{d}_a$

Fig. 2: The proposed attack policy block diagram.

Proposition 5.4: Consider the stated assumptions in Proposition 5.3. Given any positive constant T_c, the attack policy

$$\hat{\Upsilon}_a = \frac{v}{g_\alpha}u^a_{n1}(e_{\text{L}}) + \hat{\nu}\hat{\mu}(\lambda), \tag{16}$$

with $u^a_{n1}(e_{\text{L}}) = -(\frac{1}{T_c} + k_a)\Phi_1(e_L)$, where $k_a \geq k^*$, k^* given by (15), and $\Phi_1(\cdot)$ given by (11), makes the lockup manifold $\mathcal{W}^L_b$ globally finite-time stable with settling-time $T_c > 0$.

Nonlinear disturbance observer design. Thus far, the presented family of attack policies in Propositions 5.1–5.4 depend on some *a priori* knowledge of the vehicle longitudinal dynamics $\mathcal{P}$ in (5). Against the lack of such information in realistic scenarios, we add a feedforward compensation term to the proposed attack policies. In particular, we extend the brake attack policies in (14) and (16) according to

$$\hat{\Upsilon}_a = \frac{v}{g_\alpha}u^a_{ni}(e_{\text{L}}) + \hat{\nu}\hat{\mu}(\lambda) - \hat{d}_a,\ i = 1, p, \tag{17}$$

where $\hat{d}_a \in \mathbb{R}$ is the output of the following NDOB (see, e.g., [14], [21] for details of derivation)

$$\dot{z}_a = -L_d z_a - L_d\big\{u^a_{ni} + \frac{g_\alpha}{v}(-\hat{d}_a + \hat{\nu}\hat{\mu}(\lambda) + p_a)\big\}, \tag{18a}$$

$$\hat{d}_a = z_a + p_a, \tag{18b}$$

where $z_a \in \mathbb{R}$ is the state of the NDOB, and the relationship $p_a = L_d e_L$ between L_d, namely, the NDOB gain, and p_a, namely, the NDOB auxiliary variable, holds. Therefore, it follows that $L_d = \frac{\partial p_a}{\partial e_L}$.

The convergence properties of the disturbance tracking error are well-studied in the literature (see, e.g., [13], [14], [21]) and for the sake of brevity we refer the readers to the aforementioned references.

Remark 5.5: The NDOB in (18) has only one dynamic state and it does not rely on having a particular representation such as the Burckhardt closed-form for the nonlinear friction coefficient function $\mu(\cdot)$. Indeed, whenever no knowledge of $\mu(\cdot)$ is available, the adversary can set $\hat{\mu}(\lambda)$ to be equal to zero in (18). This NDOB-based disturbance compensation technique is unlike the adaptive algorithms in [17], [18] where a particular representation of the friction coefficient function is needed and several parameters need to get updated simultaneously. As it will be seen in the simulations, even when $\hat{\mu}(\lambda)$ is set to zero, corresponding to a complete lack

Quarter-car parameters	Road parameters	Attack policy parameters
$M = 250$ kg	$\alpha = 0^{\text{deg}}$	$T_c = 0.95$
$\tau_f = 16$ ms	$c_1 = 1.28, c_1' = 0.86$	$p = 0.15$
$\delta_f = 15$ ms	$c_2 = 23.99, c_2' = 33.82$	$k = 0$
$J = 1.5$ kg.m^2	$c_3 = 0.52, c_3' = 0.35$	$L_d = 2.65$
$R = 0.3$ m	–	$\hat{\nu} = \nu = 15$
–	–	$\hat{\mu}(\lambda) = 0, \tau_f = 0, \delta_f = 0$

Fig. 3: Numerical simulation parameters.

of knowledge by the adversary, the attack policy using the NDOB will meet its objectives.

VI. Simulation Results

In this section we present several numerical simulation results associated with *five different attack policies* during braking in a straight road on both wet and dry asphalt. The simulation parameters are given in Table 3, where the quarter-car parameters are directly adopted from [17].

Since the adversary would like to induce an almost complete wheel lockup condition during braking, it is desired that the trajectories $(v(t), \lambda(t))$ of the vehicle nonlinear traction dynamics in (5) converge to a very near vicinity of the lockup manifold $\mathcal{W}_L^b$ defined in (7) within a relatively small amount of time (here, $T_c = 0.95$ seconds). Out of the five attack policies employed by the adversary, one of them corresponds to applying a constant brake torque to the wheel, which is indeed a naive attack based on the assumption that with a relatively large brake torque the adversary can induce lockup in the wheels. The other four attacks employ the presented predefined-time controllers in the paper, where two of them that are given by (14), with $p = 0.15$ and $T_c = 0.95$, do not possess any NDOB-based dynamic compensation mechanism. On the other hand, the last two predefined-time controllers, with $p = 0.15$ and $T_c = 0.95$, are employing the control policy in (17) with the disturbance estimate generated by the NDOB given by (17) with $L_d = 2.65$.

The nonlinear friction coefficient function is modeled using the three-parameter Burckhardt model in (3). It is assumed that the adversary *has no knowledge* of the nonlinear friction coefficient function. Accordingly, in all of the four non-constant adopted attack policies, $\hat{\mu}(\lambda)$ is set equal to zero. In Figure 3, the coefficients associated with dry and wet asphalt road conditions are given by c_i and c_i', $1 \leq i \leq 3$, respectively. Furthermore, it is assumed that the adversary *has no knowledge* of either the friction brake time constant τ_f or the friction brake deadtime δ_f. Finally, it is assumed that the adversary *has no knowledge* of the lower bounds $k^{*\prime}$ and k^* in Propositions 5.1 and 5.3. Therefore, k in all four cases is set equal to zero. Finally, in the presented simulations, the external disturbances not related to road-tire interaction forces, i.e., $\Delta_v(t, v)$ and $\Delta_w(t, \omega)$, are set equal to zero.

Figure 4 depicts the speed, wheel slip, and disturbance profiles from the simulations. As it can be seen from the Figure, in the three scenarios where the adversary does not employ the NDOB in (16), the attack objective is not met.

It remains an open question how an adversary can devise an attacking device for realizing the proposed wheel lockup attacks in this paper. An initial direction could be the line of work by Palanca *et al.* in [9], where they crafted an inexpensive attacking device that utilizes an Arduino Uno Rev 3, a Microchip MCP2551 E/P, and an SAE J1962 Male Connector. Their device, which was powered by a simple 12V battery, could be physically plugged into the OBD-II port of their target vehicle, namely, a 2012 Alfa Romeo Giulietta.

VII. Concluding Remarks and Future Research Directions

Motivated by the recent automotive hacking incidences, this paper investigated the capabilities of an adversary who is interested in engaging the car brakes at full speed and would like to cause wheel lockup conditions after infiltrating the CAN in-vehicle network. As stated by Miller in [7]: “no matter how hard we try and how complex we make the security solutions on vehicles, it is impossible to make something perfectly secure and unhackable.” Therefore, understanding the physical threats of a CAN attacker need to be thoroughly understood. This paper demonstrated that the physical capabilities of a CAN attacker can be studied through the lens of closed-loop attack policy design. In particular, it is demonstrated that the adversary can cause wheel lockups by means of closed-loop attack policies for commanding the frictional brake actuators. This line of investigation on generating vehicle brake attack policies leads us to further research avenues. First, this paper provides insights for the emerging area of attack generation against platoons of vehicles where string stability of a given platoon is of crucial importance. Second, this paper provides an urgent motivation for devising defensive ABS control policies that can protect the vehicle traction dynamics against such wheel lockup attacks. Finally, to have a better understanding of the safety implications under the proposed brake attack policies, the stability of vehicle lateral dynamics under such attacks needs to be thoroughly analyzed. The results in the paper [22] provide an initial analysis for the cyber-physical implications of wheel lockup attacks for the lateral stability.

ACKNOWLEDGMENT

This work is supported by NSF Award 2035770.

References

[1] P. Kleberger, T. Olovsson, and E. Jonsson, “Security aspects of the in-vehicle network in the connected car,” in *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011, pp. 528–533.

[2] 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.

[3] 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.

[4] O. Avatefipour and H. Malik, “State-of-the-art survey on in-vehicle network communication can-bus security and vulnerabilities,” *Int. J. Comput. Sci. Netw.*, pp. 720–727, 2017.

[5] C. Miller and C. Valasek, “Adventures in automotive networks and control units,” *Def Con*, vol. 21, no. 260-264, pp. 15–31, 2013.

[6] ——, “Remote exploitation of an unaltered passenger vehicle,” *Black Hat USA*, vol. 2015, no. S 91, 2015.

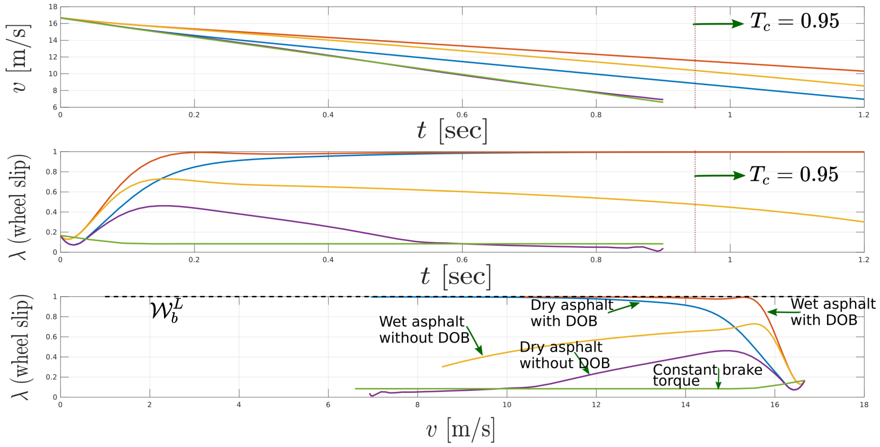

Fig. 4: Profiles of the simulation results: speed and wheel slip profiles under all five attack scenarios.

[7] C. Miller, “Lessons learned from hacking a car,” *IEEE Design & Test*, vol. 36, no. 6, pp. 7–9, 2019.

[8] S. Fröschle and A. Stühring, “Analyzing the capabilities of the can attacker,” in *Eur. Symp. Res. Comput. Secur.*, 2017, pp. 464–482.

[9] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, “A stealth, selective, link-layer denial-of-service attack against automotive networks,” in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2017, pp. 185–206.

[10] 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.

[11] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” *Automatica*, vol. 51, pp. 135–148, 2015.

[12] J. D. Sánchez-Torres, E. N. Sanchez, and A. G. Loukianov, “Predefined-time stability of dynamical systems with sliding modes,” in *2015 American Contr. Conf. (ACC)*, 2015, pp. 5842–5846.

[13] S. Li, J. Yang, W.-H. Chen, and X. Chen, *Disturbance observer-based control: methods and applications*. CRC press, 2014.

[14] W.-H. Chen, “Disturbance observer based control for nonlinear systems,” *IEEE/ASME Trans. Mechatron.*, vol. 9, no. 4, pp. 706–710, 2004.

[15] B. Olson, S. Shaw, and G. Stépán, “Nonlinear dynamics of vehicle traction,” *Veh. Syst. Dyn.*, vol. 40, no. 6, pp. 377–399, 2003.

[16] T. A. Johansen, I. Petersen, J. Kalkkuhl, and J. Ludemann, “Gain-scheduled wheel slip control in automotive brake systems,” *IEEE Trans. Contr. Syst. Technol.*, vol. 11, no. 6, pp. 799–811, 2003.

[17] R. De Castro, R. E. Araújo, M. Tanelli, S. M. Savaresi, and D. Freitas, “Torque blending and wheel slip control in EVs with in-wheel motors,” *Veh. Syst. Dyn.*, vol. 50, no. sup1, pp. 71–94, 2012.

[18] W. Li, X. Zhu, and J. Ju, “Hierarchical braking torque control of in-wheel-motor-driven electric vehicles over CAN,” *IEEE Access*, vol. 6, pp. 65 189–65 198, 2018.

[19] R. De Castro, R. Araujo, and D. Freitas, “Optimal linear parameterization for on-line estimation of tire-road friction,” *IFAC Proc. Vol.*, no. 1, pp. 8409–8414, 2011.

[20] C. C. De Wit, R. Horowitz, and P. Tsiotras, “Model-based observers for tire/road contact friction prediction,” in *New Directions in nonlinear observer design*. Springer, 1999, pp. 23–42.

[21] A. Mohammadi, H. J. Marquez, and M. Tavakoli, “Nonlinear disturbance observers: Design and applications to Euler-Lagrange systems,” *IEEE Contr. Syst.*, vol. 37, no. 4, pp. 50–72, 2017.

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