# Generation of Time-Varying Feedback-Based Wheel Lock Attack Policies with Minimal Knowledge of the Traction Dynamics

Alireza Mohammadi[1*] and Hafiz Malik[1]

[1]University of Michigan-Dearborn, Dearborn MI 48128, USA,
[*]Corresponding Author: amohmmad@umich.edu,

**Abstract.** There are a variety of ways, such as reflashing of targeted electronic control units (ECUs) to hijacking the control of a fleet of wheeled mobile robots, through which adversaries can execute attacks on the actuators of mobile robots and autonomous vehicles. Independent of the source of cyber-physical infiltration, assessing the physical capabilities of an adversary who has made it to the last stage and is directly controlling the cyber-physical system actuators is of crucial importance. This paper investigates the potentials of an adversary who can directly manipulate the traction dynamics of wheeled mobile robots and autonomous vehicles but has a very limited knowledge of the physical parameters of the traction dynamics. It is shown that the adversary can exploit a new class of closed-loop attack policies that can be executed against the traction dynamics leading to wheel lock conditions. In comparison with a previously proposed wheel lock closed-loop attack policy, the attack policy in this paper relies on less computations and knowledge of the traction dynamics. Furthermore, the proposed attack policy generates smooth actuator input signals and is thus harder to detect. Simulation results using various tire-ground interaction conditions demonstrate the effectiveness of the proposed wheel lock attack policy.

**Keywords:** Cyber-Physical Systems, Robotics

## 1 Introduction

The past decade has witnessed the proliferation of mobility-related cyber-physical systems [10] ranging from vehicles with autonomous and connected features [29] to small UAVs for inspecting critical infrastructures and agricultural robotics [20].

The interconnected and autonomous features associated with mobility-related cyber-physical systems have been demonstrated to accompany serious security threats as evidenced by several recent successful attacks such as the wireless hack of a Tesla vehicle CAN bus [36] or successful adversarial hijacking of drones [39]. These risks span a plethora of scenarios such as exploitation of the critical vulnerabilities of in-vehicle networks by adversaries that try to take over the self-driving features of target vehicles [21], jamming/spoofing the GPS signals used

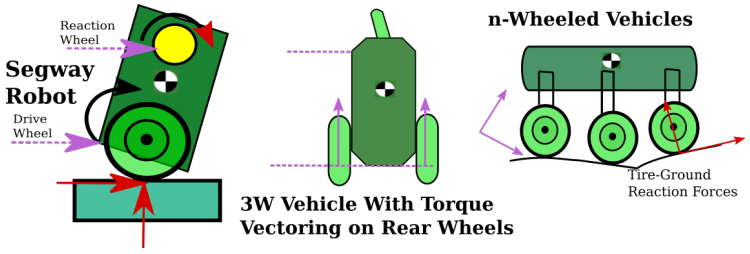


Fig. 1: Various class of wheeled mobile platforms where traction, through the longitudinal friction force between the ground and the wheels, slow or accelerate the motion: (left) a two-wheeled segway robot [16]; (middle) a 3-wheeled mobile platform with rear wheel torque vectoring [1]; and (right) an $n$-wheeled vehicle on uneven terrain [15]. In attacks against the traction dynamics, the adversary seeks to induce wheel lock conditions with a minimal knowledge of the tire-ground physical interaction characteristics.

by a fleet of service UAVs [41], and attacks against onboard charging systems of electric vehicles [9], to name a few.

Impact of cyber-attacks, as assessed in information security risk management [19, 46], is often concerned with the information/cyber system damage ranging from denying critical service functionality to sensitive information disclosure. In a cyber-physical system, on the other hand, attacks on the system constituents can also induce potential damage extending beyond the cyber-realm and impacting the physical components of the system [3, 47], as documented by infamous malwares such as Triton and Industoyer (see, e.g., [23]). Accordingly, physics-based impact assessment of cyber-attacks on physical processes has become one of the emerging aspects of security analysis in the cyber-physical systems literature [14, 33].

An important aspect of being able to assess the risk of cyberattacks on smart mobility applications is to search the space of attack policies through which adversaries can induce physical damage on their target systems [46]. In other words, the physical implications of cyberattacks against smart mobility systems, such as remotely steering a vehicle into a ditch as discussed by Miller [30], lead to the natural question posed by Fröschle and Stühring [11]: "Once an attacker has made it to the last stage, what exactly are his capabilities?"

The traction dynamics of vehicles and mobile robots, through which the wheels move with respect to the tangential ground surface (see Figure 1), can be attacked in a variety of ways such as spoofing attacks against the anti-lock braking system, reflashing the brake ECUs, and sending malicious brake commands through the CAN bus of the vehicle, amongst others (see, e.g. [13, 17, 18, 21, 22, 28, 40, 43]). Independent from the source of cyber-physical vulnerability, a frightening feature of vehicular cyberattacks on steering and braking actuators (see, e.g., [30–32]) is that they are forensically scentless (i.e., leaving no forensic evidence behind) and are almost invisible to the driver. Accordingly, it is of crucial importance to search and assess the space of attack policies through which an adversary can induce maximum physical damage on their target system.

The first steps on assessing the physical capabilities of an adversary manipulating the vehicular traction dynamics has been taken in [34, 35], where the authors model the cyber-physical threat of an adversary as a closed-loop attack policy design problem, which can be executed on the vehicle braking actuators. To demonstrate the physical capabilities of an adversary who has a limited knowledge of the vehicle traction dynamics and the tire-ground interaction characteristics, the authors utilized a predefined-time controller [42] and a nonlinear disturbance observer [26] to design a brake attack policy that will induce wheel lockup conditions in a finite time interval. A drawback of the proposed attack policies in [34, 35] is the reliance on the nonlinear disturbance observer feedforward computations, which compensate for the lack of adversarial knowledge about the physical parameters of the traction dynamics. Furthermore, the generated attack signals in [34, 35] might be non-smooth and therefore easier to detect through anomaly detection algorithms [12]. Finally, the overall effect of such wheel lock attacks were not investigated in terms of their impact on the overall motion of the vehicle under attack.

This paper demonstrates that the adversary with a very limited knowledge of tire-ground interaction characteristics can induce wheel lock conditions through a properly designed closed-loop attack policy against the traction dynamics. Unlike a previously designed wheel lock attack policy in [34, 35], the new attack policy does not rely on the computation of nonlinear disturbance observer-based feedforward terms. Furthermore, the new feedback control input is generated through a time-varying controller with prescribed convergence time [44] that can cause wheel lockups even when the physical parameters of the traction dynamics are not known *a priori* (see Figure 2). Finally, the attack signals generated by the policy in this paper are guaranteed to be smooth and hence harder detect through anomaly detection algorithms for monitoring the actuator signals [12].

**Contributions of the paper.** This paper proposes a new class of traction dynamics attack policies that can be executed against mobile robots and autonomous vehicles. In comparison with an existing result in [34, 35], the proposed attack policy in this article, which relies on time-varying feedback control schemes with prescribed convergence time, relies on *less computations*. Furthermore, the proposed attack policy is guaranteed to generate smooth actuator input signals and thus is harder to detect. Moreover, the effectiveness of the proposed attack policy is demonstrated in terms of its impact on the overall motion of the mobile platform under attack through various simulation scenarios.

The rest of this paper is organized as follows. First, we present the vehicle traction dynamics and formulate the wheel lock attack policy objective in terms of these dynamics in Section 2. Thereafter, in Section 3, we present our attack policy that is based on using time-varying feedback controllers with prescribed convergence time. Next, we validate the effectiveness of the proposed attack policy using various ground conditions and demonstrate the destabilizing effect of such wheel lock attacks on the overall motion of a 4-wheeled vehicle through simulations in Section 4. Finally, we conclude the paper with future research directions and final remarks in Section 5.

## 2 Traction Dynamics

In this section, we briefly present the single-wheel model of traction dynamics. This dynamical model can effectively capture the steady and transient tractive performance while demonstrating how a vehicle or wheeled mobile robot can end up in a wheel lock condition (see, e.g., [45,48] for the wheel slip dynamics of wheeled mobile robots and [6,27] for that of the vehicles). Often, the states of the traction dynamical system are selected to be the forward mobile robot/vehicle speed and tire/wheel rate of rotation. The dynamics that govern the states of the traction dynamical system are given by (see, e.g., [6])

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

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

where the parameters $M$, $r$, and $J$ are the vehicle/mobile robot mass, wheel radius, and wheel inertia, respectively. Additionally, during deceleration, the mobile robot/vehicle speed $v$ and the wheel rotational speed $\omega$ vary within the set

$$\mathcal{D}_b := \{(v,\omega) | v > 0,\ 0 \leq r\omega \leq v\}. \tag{2}$$

In the dynamics given by (1), the torque $T_a$, resulting from either the electric motors of the mobile robot or the vehicle brakes, is the input to the dynamical system in (1). Furthermore, the longitudinal slip $\lambda$ that determines whether the wheel is locked is given by

$$\lambda := \frac{v - r\omega}{\max(v, r\omega)}. \tag{3}$$

While the traction input actuators are engaged, we have $\lambda = \frac{v-r\omega}{v}$ and $(v,\omega) \in \mathcal{D}_b$. Accordingly, the longitudinal slip value $\lambda$ belongs to the closed interval $[0,1]$ during deceleration. Given the ground slope $\alpha$, we denote the tangential acceleration $g\cos(\alpha)$ by $g_\alpha$. 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 tractive unmodeled dynamics, respectively.

There are numerous ways to represent the nonlinear friction coefficient function $\mu(\cdot)$ including the Burckhardt equation (see, e.g., [5]). For instance, equations like Burckhardt model (see, e.g., [7]) where

$$\mu(\lambda) = c_1(1 - \exp(-c_2\lambda)) - c_3\lambda, \tag{4}$$

are empirical equations, which are based on coefficient curve fitting, and are widely employed in modeling the tire/ground interaction. The longitudinal force on the tire arising from this interaction is computed by $-\mu(\lambda)g_\alpha$. In this paper, no particular closed-form representation is assumed for the function $\mu(\cdot)$.

In accordance with the traction dynamics control literature (see, e.g., [6]), we assume that the unknown disturbance acting on the speed dynamics, i.e.,

$\Delta_v(t,v)$, and the unknown disturbance acting on the wheel angular speed dynamics, i.e., $\Delta_w(t,\omega)$, respect the following inequalities

$$|\Delta_v(t,v)| \leq \bar{\Delta}_v,\ |\Delta_w(t,\omega)| \leq \bar{\Delta}_\omega,$$
$$\text{for all } (t,v,\omega) \in [0,\infty) \times \mathcal{D}_b. \tag{5}$$

As it has been noted by Olson *et al.* in [37], it is more beneficial to change the coordinates of the traction dynamics in (1) from the pair of longitudinal speed-wheel angular speed, i.e., $(v,\omega)$, to the pair of longitudinal speed-longitudinal slip, i.e., $(v,\lambda)$. After the change of coordinates, the longitudinal dynamics read as

$$\dot{v} = -g_\alpha \mu(\lambda) - \frac{\Delta_v(t,v)}{M}, \tag{6a}$$
$$\dot{\lambda} = \frac{g_\alpha}{v}\big\{(\lambda - 1 - \nu)\mu(\lambda) + \Upsilon_a + \Upsilon_{\Delta,w} + (\lambda - 1)\Upsilon_{\Delta,v}\big\}, \tag{6b}$$

where $\nu := \frac{MR^2}{J}$ denotes a dimensionless ratio, $\Upsilon_a := \frac{r}{Jg_\alpha}T_a$ is the dimensionless traction dynamics control input, and $\Upsilon_{\Delta,w} := \frac{r}{Jg_\alpha}\Delta_w(t,\omega)$, $\Upsilon_{\Delta,v} := \frac{\Delta_v(t,v)}{Mg_\alpha}$ are the dimensionless force and torque disturbances affecting the speed and the longitudinal slip dynamics, respectively.

The dynamical system given by (1) and (6) take into account the inter-coupling between the wheel slip $\lambda$ and the mobile platform speed $v$ in (6), or the wheel angular speed $\omega$ dynamics and the mobile platform speed $v$ in (1). In the coordinates given by $(v,\lambda)$, the set $\mathcal{D}_b$ in (2), which is the state space of the traction dynamics, can be written as

$$\mathcal{D}_b = \big\{(v,\lambda) | v > 0,\ \lambda \in \Lambda := [0,1]\big\}. \tag{7}$$

Both the literature of automotive cybersecurity (see, e.g., [11,30]) and mobile robotics cybersecurity (see, e.g., [2,25]) outline a plethora of threats through which an adversary can manipulate the traction dynamics. This cyber-physical threat capability of an adversary can be formulated as a closed-loop attack policy design for the vehicle/mobile robot traction dynamics actuators (see Figure 2). To assess the physical capabilities of the adversary who can manipulate the traction dynamics of the mobile platform by utilizing the tractive control input $\Upsilon_a$, we consider the case where the adversary desires to induce unstable tractive behavior by wheel locks. To consider the most severe case of wheel lock, i.e., when the longitudinal slip satisfies $\lambda = 1$, we define the lockup manifold in the following way

$$\mathcal{W}_b^L := \big\{(v,\lambda) \big| v > 0,\ \lambda = 1\big\}. \tag{8}$$

It is remarked that the wheel lockup manifold was originally defined by Olson *et al.* in [37] to study the stability of vehicular traction dynamics. Furthermore, we remark that the adversary can set the slip reference value $\lambda^{\mathrm{r}}$, belonging to the closed interval $[0,1]$, *a priori*. The closer the reference slip value $\lambda^{\mathrm{r}}$ to one, the closer the wheel to the lock condition. We assume, without loss of generality, that $\lambda^{\mathrm{r}} = 1$.

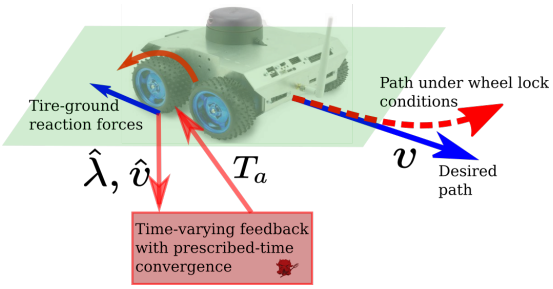


Fig. 2: This paper assesses the physical capabilities of an adversary who has infiltrated the control system associated with the traction dynamics. Despite having a limited knowledge of the underlying physical parameters, the adversary is trying to induce wheel lock using the input actuators, e.g., electric motors of mobile robot wheels or vehicle brake actuators.

## 3 Design of Traction Dynamics Wheel Lock Attack Policy

In this section, we present a wheel lock closed-loop attack policy that can be executed against the traction dynamics of vehicles and various wheeled mobile robots (see Figure 1). Our closed-loop attack policy *merely* relies on a feedback control action. In contrast to the previous line of work in [34, 35], no additional feedforward control action computation is required in this proposed attack policy. The attack input is designed based on a time-varying feedback control framework with prescribed convergence in finite time [44]. The proposed attack can induce wheel lock conditions *even if the wheel-ground interaction characteristics and other relevant parameters in the vehicle traction dynamics are not known.*

Following the control design framework in [44], we consider the mapping $\mu_K : t \mapsto \mu_K(t)$ where

$$\mu_K(t - t_0) = \frac{T^{1+m_0}}{\left(T + t_0 - w(\frac{t-t_0}{T})\right)^{1+m_0}}, \; t \in [t_0, t_0 + T). \tag{9}$$

In (9), $m_0$ is a positive integer and the real numbers $t_0$ and $T$ are non-negative and positive, respectively. Furthermore, the function $w : \tau \mapsto w(\tau)$ is any smooth and monotonically increasing function such that $w(0) = 0$ and $w(1) = t_0 + T$.

In the context of the wheel lock attack policy, $t_0$ in (9) represents the time of the onset of the attack. Furthermore, $T$ is the finite settling time associated with the attack by which the wheel longitudinal slip will converge to the adversary's desired slip value. The time-warping function $w(\cdot)$ controls the transient convergence behavior of the states of the traction dynamics to the wheel lockup manifold $\mathcal{W}_b^L$ given by (8). In its simplest form, the monotonic function $w(\cdot)$ can be chosen to be $w(\tau) = \tau$ as in [44]. As shown later, we choose this function to be a Bézier polynomial of order two.

Finally, we define the wheel lockup error as

$$e_L = \lambda - 1. \tag{10}$$

Hence, if the wheel lockup error satisfies $e_L = 0$ while the wheeled mobile platform speed is positive, i.e., $v > 0$, the wheel is in a locked stated. Using the closed-loop attack policy in this paper, the wheel will be locked in finite time. Therefore, the wheeled robot speed will satisfy

$$v \in [v_{\min}, v_{\max}], \tag{11}$$

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

**Closed-loop attack policy for inducing wheel lock in finite time.** Consider the wheeled mobile platform traction dynamics in (6). We propose using the following wheel lock attack policy

$$\Upsilon_a = \frac{v}{g_\alpha} u_{\text{np}}^{\text{a}}(e_L, t), \tag{12}$$

where

$$u_{\text{np}}^{\text{a}}(e_L, t) = -(k_0 + \frac{1 + m_0}{T})\mu_K(t) e_L. \tag{13}$$

In (13), the time-varying feedback gain function $\mu_K(\cdot)$ is given by (9). Furthermore, the time-warping function $w(\cdot)$ used in (9) is given by the second order Bézier polynomial

$$w(\tau) = p_1 + (1 - \tau)^2(p_0 - p_1) + \tau^2(p_2 - p_1), \tag{14}$$

where $p_0 = 0$ and $p_2 = t_0 + T$ are constant parameters. Furthermore, the constant parameter $p_1$ is chosen at the adversary's discretionary to control the transient behavior of the traction dynamics state trajectories during the wheel lock attack. It can be shown that the wheel slip error dynamics take the form

$$\dot{e}_L = u_{\text{np}}^{a}(e_{\text{L}}, t) + \Delta_e'(t, e_L), \tag{15}$$

where $\Delta_e'(t, e_L)$ denotes the lumped disturbance that lump the effect of all unknown parameters, unknown disturbances such as $\Delta_v(\cdot)$, $\Delta_w(\cdot)$, and the unknown wheel-ground friction coefficient function $\mu(\cdot)$ in the traction dynamics given by (6). The time-varying feedback control input $u_{\text{np}}^{a}(e_{\text{L}}, t)$, which is adopted from [44], ensures the rejection of these unknown disturbances and convergence to the lockup manifold $\mathcal{W}_b^L$ given by (8) in finite time $t_0 + T$ from the onset of the attack at time $t_0$. Indeed, it is because of the superior disturbance rejection capabilities of the time-varying feedback input $u_{\text{np}}^{a}(e_{\text{L}}, t)$ that there is no need for additional real-time computations of feedforward disturbance compensation terms as in [34,35]. In other words, the time-varying feedback control input $u_{\text{np}}^{a}(e_{\text{L}}, t)$ removes the need for additional estimation computations.

In the proposed attack policy in (12), we are assuming that the adversary has the knowledge and/or can estimate the wheeled mobile platform speed as well as the attacked wheel longitudinal slip. Clark *et al.* [4] and Lacava *et al.* in [24] enumerate several ways through which the firmware/OS on the microprocessor of the robotic devices can be infiltrated and exploited later for performing attacks on the actuation system of the robot. Furthermore, as demonstrated in

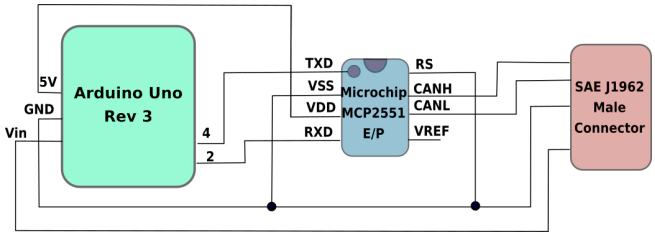


Fig. 3: The inexpensive attacking device proposed by Palanca *et al.* [38] for accessing the CAN bus through the OBD-II port.

experimental wireless attacks against Tesla electric vehicles [36], reprogramming the firmware of ECUs through the Unified Diagnostic Services (UDS) enables the adversary to read live data, such as speed or engine rpm, from the in-vehicle network. Finally, as demonstrated by Palanca *et al.* in [38], it is possible to craft an inexpensive attacking device consisting of an an SAE J1962 Male Connector, a Microchip MCP2551 E/Pa Microchip MCP2551 E/P, and Arduino Uno Rev 3, which can be powered by a simple 12V battery. This device, which was experimentally tested on a 2012 Alfa Romeo Giulietta, could be physically plugged into the OBD-II port of the target vehicle and access the various ECUs in the vehicle through the CAN bus (see Figure 3).

## 4 Simulation Results

In this section we first present numerical simulation results associated with the wheel lock attack policy in (12) using various wheel-ground interaction conditions. Next, we will present numerical simulation results demonstrating the impact of the presented wheel lock attack policy on the overall stability of the motion of a 4-wheeled vehicle.

In the wheel lock attack numerical simulations, we consider four different wheel-ground interaction conditions; namely, interaction with dry asphalt, wet asphalt, dry cobblestone, and wet cobblestone. The nonlinear friction coefficient function is modeled using the three-parameter Burckhardt model in (4). In the simulations, the adversary *has no knowledge* of the nonlinear friction coefficient function as it is evident from the closed-loop attack policy given by (12). The friction coefficient function is based on the Burckhardt tire model and the associated parameters are taken from [8]. The wheeled vehicle parameters are taken from [6]. The parameters of the wheel lock attack policy in (13) are chosen to be $m_0 = 1$, $T = 2.5$, $t_0 = 0$, and $p_1 = 2.38$.

Figure 4 presents the speed, wheel slip, and the traction dynamics state space trajectories from the simulations. As it can be seen from the figure, the time-varying feedback-based attack policy manages to induce wheel lock conditions in all four scenarios. Figure 5 depicts the lumped disturbance $\Delta'_e(t, e_L)$ time profile

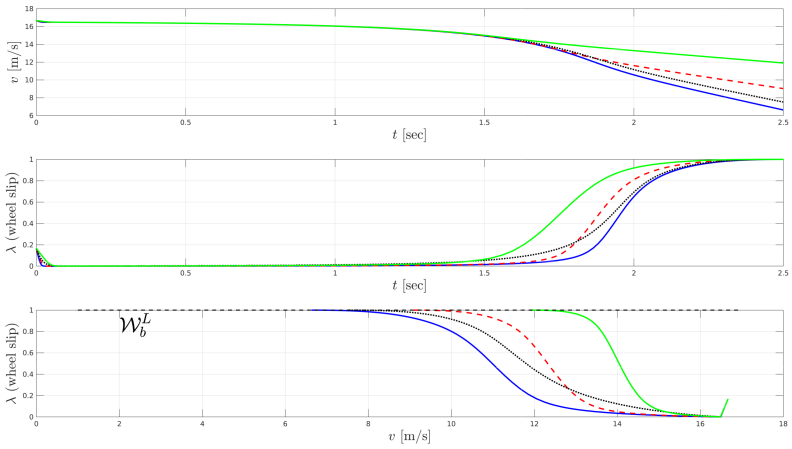


Fig. 4: Time profiles of the simulation results: (top) speed time profile on various ground conditions; (middle) wheel slip time profile on various ground conditions; and (bottom) state space trajectories of the traction dynamics in (6). In all four scenarios, finite-time convergence to the wheel lockup manifold $\mathcal{W}_b^L := \{(v, \lambda) | v > 0, \lambda = 1\}$ takes place without the need for estimating the lumped disturbance time profiles $\Delta_e'(t, e_L)$.

associated with the wheel lock attack numerical simulations. Despite being non-zero and time-varying, the closed-loop attack policy given by (12) manages to reject their effect on the wheel slip tracking dynamics without the need for additional computations to estimate this unknown lumped disturbance term.

To study the effect of the proposed closed-loop attack policy on the overall motion and stability of mobile platforms (including mobile robots and autonomous vehicles), one needs to study the attack impact on an individual basis. For instance, a wheel lock attack on a 3W mobile robot [1] or a 4-wheeled vehicle [49, 50] might result in lateral motion instability. The same attack on a segway robot [16] might result in loss of balance. In this paper, we study the overall impact of the wheel lock attacks by using the dynamical model developed by Yi, Tseng, and collaborators (see, e.g., [49,50]). The model in [49,50], which is based on a hybrid physical/dynamic tire/road friction mode, captures the coupling effect between longitudinal and lateral vehicle motions. As demonstrated by Figure 6, after the wheel lock attack policy in (12) is executed on the front wheels of the vehicle interacting with dry asphalt, wet asphalt, dry cobblestone, and wet cobblestone, the vehicle loses its lateral stability in all four scenarios.

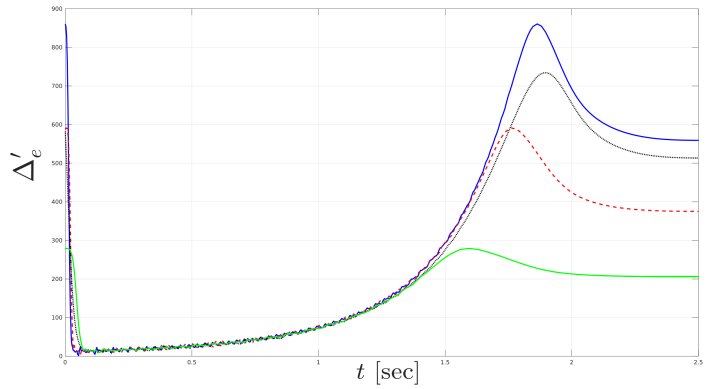


Fig. 5: The lumped disturbance $\Delta'_e(t, e_L)$ time profile associated with the wheel lock attack numerical simulations. The lumped disturbance captures the effect of all unknown parameters, unknown disturbances such as $\Delta_v(\cdot)$, $\Delta_w(\cdot)$, and the unknown wheel-ground friction coefficient function $\mu(\cdot)$ in the traction dynamics given by (6) and manifests itself in the tracking error dynamics in (15). The time-varying feedback control input $u^a_{\text{np}}(e_{\text{L}}, t)$ given by (13) guarantees the convergence of trajectories of the traction dynamics with the need for estimation of $\Delta'_e(t, e_L)$.

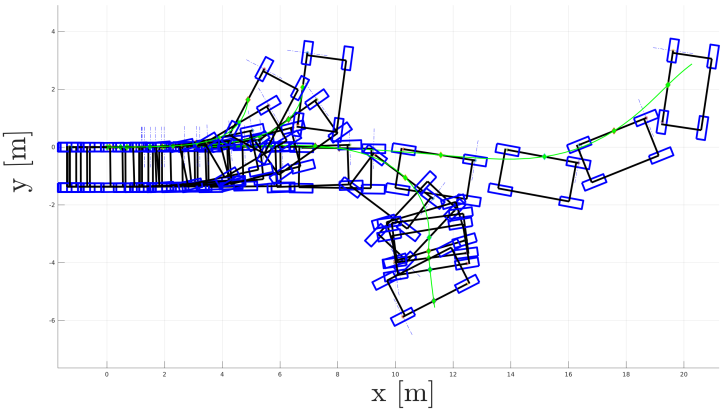


Fig. 6: The overall impact of the wheel lock attacks on the stability of a 4-wheeled vehicle modeled using the approach by Yi, Tseng, and collaborators [49, 50].

## 5 Concluding Remarks and Future Research Directions

In this paper, the potentials of an adversary who can directly manipulate the traction dynamics of wheeled mobile robots and autonomous vehicles were investigated. It was assumed that the adversary has a very limited knowledge of the physical parameters of the traction dynamics. Using a class of time-varying feed-

back control inputs with prescribed finite time convergence, this paper showed that the adversary can exploit this class of attack policies against the traction dynamics inducing wheel lock conditions. Simulation results using various tire-ground interaction conditions demonstrated the effectiveness of the proposed wheel lock attack policy.

## Acknowledgments

This work is supported by NSF Award CNS-2035770 (Division of Computer and Network Systems).

## References

1. Ataei, M., Khajepour, A., Jeon, S.: Reconfigurable integrated stability control for four-and three-wheeled urban vehicles with flexible combinations of actuation systems. IEEE/ASME Transactions on Mechatronics 23(5), 2031–2041 (2018)
2. Balsa-Comerón, J., Guerrero-Higueras, Á.M., Rodríguez-Lera, F.J., Fernández-Llamas, C., Matellán-Olivera, V.: Cybersecurity in autonomous systems: hardening ros using encrypted communications and semantic rules. In: Iberian robotics conference. pp. 67–78. Springer (2017)
3. Chong, M.S., Sandberg, H., Teixeira, A.M.: A tutorial introduction to security and privacy for cyber-physical systems. In: 2019 18th European Control Conference (ECC). pp. 968–978. IEEE (2019)
4. Clark, G.W., Doran, M.V., Andel, T.R.: Cybersecurity issues in robotics. In: 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA). pp. 1–5. IEEE (2017)
5. De Castro, R., Araujo, R., Freitas, D.: Optimal linear parameterization for on-line estimation of tire-road friction. IFAC Proc. Vol. (1), 8409–8414 (2011)
6. De Castro, R., Araújo, R.E., Tanelli, M., Savaresi, S.M., Freitas, D.: Torque blending and wheel slip control in EVs with in-wheel motors. Veh. Syst. Dyn. 50(sup1), 71–94 (2012)
7. De Wit, C.C., Horowitz, R., Tsiotras, P.: Model-based observers for tire/road contact friction prediction. In: New Directions in nonlinear observer design, pp. 23–42. Springer (1999)
8. Dousti, M., Baslamısli, S.C., Onder, E.T., Solmaz, S.: Design of a multiple-model switching controller for abs braking dynamics. Transactions of the Institute of Measurement and Control 37(5), 582–595 (2015)
9. ElHussini, H., Assi, C., Moussa, B., Atallah, R., Ghrayeb, A.: A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid. ACM Transactions on Internet of Things 2(2), 1–21 (2021)
10. Elshenawy, M., Abdulhai, B., El-Darieby, M.: Towards a service-oriented cyber–physical systems of systems for smart city mobility applications. Future Generation Computer Systems 79, 575–587 (2018)
11. Fröschle, S., Stühring, A.: Analyzing the capabilities of the CAN attacker. In: Eur. Symp. Res. Comput. Secur. pp. 464–482 (2017)
12. Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N.O., Sandberg, H., Candell, R.: A survey of physics-based attack detection in cyber-physical systems. ACM Computing Surveys (CSUR) 51(4), 1–36 (2018)

13. Hodge, C., Hauck, K., Gupta, S., Bennett, J.C.: Vehicle cybersecurity threats and mitigation approaches. Tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States) (2019)
14. Huang, K., Zhou, C., Tian, Y.C., Yang, S., Qin, Y.: Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Transactions on Industrial Electronics 65(10), 8153–8162 (2018)
15. Iagnemma, K., Dubowsky, S.: Traction control of wheeled robotic vehicles in rough terrain with application to planetary rovers. The International Journal of Robotics Research 23(10-11), 1029–1040 (2004)
16. Jones, D.R., Stol, K.A.: Modelling and stability control of two-wheeled robots in low-traction environments. In: Australasian Conference on Robotics and Automation, Brisbane, Australia (2010)
17. Kang, L., Shen, H.: Attack detection and mitigation for sensor and CAN bus attacks in vehicle anti-lock braking systems. In: 2020 29th International Conference on Computer Communications and Networks (ICCCN). pp. 1–9. IEEE (2020)
18. Kang, L., Shen, H.: Detection and mitigation of sensor and CAN bus attacks in vehicle anti-lock braking systems. ACM Transactions on Cyber-Physical Systems (TCPS) 6(1), 1–24 (2022)
19. Kaplan, S., Garrick, B.J.: On the quantitative definition of risk. Risk Analysis 1(1), 11–27 (1981)
20. Kim, J., Kim, S., Ju, C., Son, H.I.: Unmanned aerial vehicles in agriculture: A review of perspective of platform, control, and applications. IEEE Access 7, 105100–105115 (2019)
21. Kim, K., Kim, J.S., Jeong, S., Park, J.H., Kim, H.K.: Cybersecurity for autonomous vehicles: Review of attacks and defense. Comput. Secur. p. 102150 (2021)
22. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., et al.: Experimental security analysis of a modern automobile. In: The Ethics of Information Technologies, pp. 119–134. Routledge (2020)
23. Kshetri, N., Voas, J.: Hacking power grids: A current problem. Computer 50(12), 91–95 (2017)
24. Lacava, G., Marotta, A., Martinelli, F., Saracino, A., La Marra, A., Gil-Uriarte, E., Vilches, V.M.: Cybsersecurity issues in robotics. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 12(3), 1–28 (2021)
25. Lee, S., Min, B.C.: Distributed direction of arrival estimation-aided cyberattack detection in networked multi-robot systems. In: 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). pp. 1–9. IEEE (2018)
26. Li, S., Yang, J., Chen, W.H., Chen, X.: Disturbance observer-based control: methods and applications. CRC press (2014)
27. Li, W., Zhu, X., Ju, J.: Hierarchical braking torque control of in-wheel-motor-driven electric vehicles over CAN. IEEE Access 6, 65189–65198 (2018)
28. Liu, J., Corbett-Davies, J., Ferraiuolo, A., Ivanov, A., Luo, M., Suh, G.E., Myers, A.C., Campbell, M.: Secure autonomous cyber-physical systems through verifiable information flow control. In: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. pp. 48–59 (2018)
29. Lu, N., Cheng, N., Zhang, N., Shen, X., Mark, J.W.: Connected vehicles: Solutions and challenges. IEEE Internet of Things Journal 1(4), 289–299 (2014)
30. Miller, C.: Lessons learned from hacking a car. IEEE Design & Test 36(6), 7–9 (2019)
31. Miller, C., Valasek, C.: Adventures in automotive networks and control units. Def Con 21(260-264), 15–31 (2013)

32. Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015(S 91) (2015)
33. Mohammadi, A., Malik, H.: Vehicle lateral motion stability under wheel lockup attacks. In: Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022. San Diego, CA (2022), doi:10.14722/autosec.2022.23010
34. Mohammadi, A., Malik, H., Abbaszadeh, M.: Generation of CAN-based wheel lockup attacks on the dynamics of vehicle traction. In: Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022. San Diego, CA (2022), doi: 10.14722/autosec.2022.23025
35. Mohammadi, A., Malik, H., Abbaszadeh, M.: Generation of wheel lockup attacks on nonlinear dynamics of vehicle traction. In: 2022 American Control Conference (ACC). pp. 1994–1999 (2022)
36. Nie, S., Liu, L., Du, Y.: Free-fall: Hacking Tesla from wireless to CAN bus. Briefing, Black Hat USA 25, 1–16 (2017)
37. Olson, B., Shaw, S., Stépán, G.: Nonlinear dynamics of vehicle traction. Veh. Syst. Dyn. 40(6), 377–399 (2003)
38. Palanca, A., Evenchick, E., Maggi, F., Zanero, S.: A stealth, selective, link-layer denial-of-service attack against automotive networks. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. pp. 185–206. Springer (2017)
39. Petnga, L., Xu, H.: Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks. In: 2016 International Conference on Unmanned Aircraft Systems (ICUAS). pp. 811–819. IEEE (2016)
40. Pollicino, F., Stabili, D., Bella, G., Marchetti, M.: SixPack: Abusing ABS to avoid misbehavior detection in VANETs. In: 2021 IEEE 93rd Vehicular Technology Conference. pp. 1–6. IEEE (2021)
41. Salamh, F.E., Karabiyik, U., Rogers, M.K., Matson, E.T.: A comparative UAV forensic analysis: Static and live digital evidence traceability challenges. Drones 5(2), 42 (2021)
42. Sánchez-Torres, J.D., Sanchez, E.N., Loukianov, A.G.: Predefined-time stability of dynamical systems with sliding modes. In: 2015 American Contr. Conf. (ACC). pp. 5842–5846 (2015)
43. Shoukry, Y., Martin, P., Tabuada, P., Srivastava, M.: Non-invasive spoofing attacks for anti-lock braking systems. In: International Conference on Cryptographic Hardware and Embedded Systems. pp. 55–72. Springer (2013)
44. Song, Y., Wang, Y., Krstic, M.: Time-varying feedback for stabilization in prescribed finite time. Int. J. Robust Nonlin. Contr. 29(3), 618–633 (2019)
45. Stonier, D., Cho, S.H., Choi, S.L., Kuppuswamy, N.S., Kim, J.H.: Nonlinear slip dynamics for an omniwheel mobile robot platform. In: Proceedings 2007 IEEE International Conference on Robotics and Automation. pp. 2367–2372. IEEE (2007)
46. Teixeira, A., Sou, K.C., Sandberg, H., Johansson, K.H.: Secure control systems: A quantitative risk management approach. IEEE Control Systems Magazine 35(1), 24–45 (2015)
47. Teixeira, A.M.: Optimal stealthy attacks on actuators for strictly proper systems. In: 2019 IEEE 58th Conference on Decision and Control (CDC). pp. 4385–4390. IEEE (2019)
48. Tian, Y., Sidek, N., Sarkar, N.: Modeling and control of a nonholonomic wheeled mobile robot with wheel slip dynamics. In: 2009 IEEE Symposium on Computational Intelligence in Control and Automation. pp. 7–14. IEEE (2009)

49. Yi, J., Li, J., Lu, J., Liu, Z.: On the stability and agility of aggressive vehicle maneuvers: a pendulum-turn maneuver example. IEEE Trans. Contr. Syst. Technol. 20(3), 663–676 (2011)
50. Yi, J., Tseng, E.H.: Nonlinear stability analysis of vehicle lateral motion with a hybrid physical/dynamic tire/road friction model. In: ASME Dyn. Syst. Contr. Conf. (DSCD). vol. 48920, pp. 509–516 (2009)