Automatica 112 (2020) 108655

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Secure trajectory planning against undetectable spoofing attacks[☆]

Yin-Chen Liu, Gianluca Bianchin [*], Fabio Pasqualetti

Department of Mechanical Engineering, University of California, Riverside, United States of America

ARTICLE INFO

Article history:
Received 3 December 2018
Received in revised form 29 September 2019
Accepted 3 October 2019
Available online xxxx

Keywords:
Secure trajectory planning
Spoofing attacks
Undetectable attacks
Cyber–physical security
Nonlinear systems

ABSTRACT

This paper studies, for the first time, the trajectory planning problem in adversarial environments, where the objective is to design the trajectory of a robot to reach a desired final state despite the unknown and arbitrary action of an attacker. In particular, we consider a robot moving in a two-dimensional space and equipped with two sensors, namely, a Global Navigation Satellite System (GNSS) sensor and a Radio Signal Strength Indicator (RSSI) sensor. The attacker can arbitrarily spoof the readings of the GNSS sensor and the robot control input so as to maximally deviate its trajectory from the nominal precomputed path. We derive explicit and constructive conditions for the existence of undetectable attacks, through which the attacker deviates the robot trajectory in a stealthy way. Conversely, we characterize the existence of secure trajectories, which guarantee that the robot either moves along the nominal trajectory or that attacks remain detectable. We show that secure trajectories can only exist between a subset of states, and provide a numerical technique to compute them. We illustrate our findings through several numerical studies, and show that our methods are applicable to different models of robot dynamics, including unicycles. More generally, our results show how control design affects security in systems with nonlinear dynamics.

© 2019 Elsevier Ltd. All rights reserved.

1. Introduction

Autonomous robots have rapidly been adopted in a broad range of applications, including delivery, exploration, surveillance, and search and rescue. Autonomous robots rely on sensory data to make decisions, plan their trajectories, and apply controls. Yet, as demonstrated by recent studies and real world incidents, sensory data can be accidentally and maliciously compromised, thus undermining the effectiveness of autonomous operations in critical and adversarial applications.

Despite recent advances in understanding and enhancing the security of cyber–physical systems, security tools for autonomous systems are still of limited applicability and effectiveness. In this paper we formulate and solve a *secure trajectory planning* problem, where the objective is to design the trajectory of a robot to reach a desired final state despite unknown and arbitrary attacks. We consider a robot equipped with a Global Navigation Satellite System (GNSS) sensor and a Radio Signal Strength Indicator (RSSI) sensor, and focus on attackers capable of simultaneously spoofing the GNSS readings and sending falsified control inputs to the robot. We show how the attacker can generate undetectable attacks that maximally deviate the robot from the nominal and precomputed path, and study how the trajectory planner can exploit the RSSI readings to reveal certain attacks. Moreover, we demonstrate the existence of secure trajectories between certain initial and final configurations, and propose a technique to determine the corresponding control inputs. We remark that, because of the nonlinearity of RSSI sensor readings, existing security methods based on linear models are inapplicable in our setting. In fact, our results show for the first time that the security of a system with nonlinear dynamics can be improved by appropriately designing its control inputs.

Related work Security of cyber–physical systems is, by now, a widely studied topic across the controls and computer science communities, among others. Yet, most methods are applicable to static systems or systems with linear dynamics (Bai, Pasqualetti, & Gupta, 2017; Hamza, Tabuada, & Diggavi, 2011; Lun, D'Innocenzo, Smarra, Malavolta, & Benedetto, 2019; Mo & Sinopoli, 2010; Pasqualetti, Dörfler, & Bullo, 2013), and theoretical results and tools for the security of systems with nonlinear dynamics are still critically lacking. Few exceptions are Hespanha and Bopardikar (2019), which considers the problem of controlling a system under attack in a game-theoretic framework, Shoukry et al. (2015), which focuses on nonlinear systems satisfying differential flatness properties, and the recent articles

[☆] This material is based upon work supported in part by ARO, United States award 71603NSYIP, and in part by National Science Foundation, United States award CNS-1646641. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Andrey V. Savkin under the direction of Editor Ian R. Petersen.

[*] Corresponding author.

E-mail addresses: yliu@engr.ucr.edu (Y.-C. Liu), gianluca@engr.ucr.edu (G. Bianchin), fabiopas@engr.ucr.edu (F. Pasqualetti).

https://doi.org/10.1016/j.automatica.2019.108655
0005-1098/© 2019 Elsevier Ltd. All rights reserved.

(Hu, Fooladivanda, Chang, & Tomlin, 2018; Kim, Lee, Shim, Eun, & Seo, 2019), which are however restricted to state the estimation problem in the presence of attacks modifying the system measurements only. Instead, in this work we focus on characterizing detectability of attacks modifying both the measurements and the input of the system, on quantifying their effects on the trajectories, and on the problem of designing nominal control inputs to restrict or prevent undetectable attacks.

The literature on GNSS spoofing attack mechanisms and their detection is also related to this paper. Existing approaches to identify and prevent spoofing attacks can be divided into two categories: filtering-based and redundancy-based techniques. Filtering-based detection techniques rely on signal processing methods to reveal compromised streams of sensory data (e.g., see Broumandan, Jafarnia-Jahromi, Dehghanian, Nielsen, & Lachapelle, 2012; Jiang, Zhang, Harding, Makela, & Domínguez-García, 2013). Redundancy-based techniques, instead, rely on the availability of measurement from multiple types of sensors to reveal inconsistency in the data (e.g., see Montgomery, Humphreys, & Ledvina, 2009; Psiaki, O'Hanlon, Bhatti, Shepard, & Humphreys, 2013; Psiaki et al., 2014; Radin, Swaszek, & Seals, 2015; Swaszek, Pratz, Arocho, Seals, & Hartnett, 2014; Zou, Huang, Lin, & Cong, 2016). The methods developed in this work combine these two principles. In fact, detection is achieved by processing the sensory data over time, thus ensuring compatibility between the measurements and the robot dynamical model, and by processing the measurements of two or more sensors, thus exploiting redundancy across the two channels.

Paper contribution This paper features four main contributions. First, we demonstrate the existence and characterize the form of undetectable attacks, that is, coordinated attack inputs that deviate the robot trajectory from the nominal path and cannot be detected using the GNSS and RSSI readings. Second, we demonstrate how an attacker can design optimal undetectable attacks that maximally deviate the robot from its nominal path while maintaining undetectability. Third, we show the existence of secure trajectories where, independently of the intensity of the attack, the robot either follows the nominal precomputed path or readily detects the attack. Fourth, we formulate and solve the secure trajectory planning problem, which asks for the design of open-loop control inputs that allow the robot to securely navigate from a given initial configuration to a certain final position. As a minor contribution, we study and characterize undetectable attacks and secure trajectories for robots with unicycle dynamics, thus showing that our techniques are in fact applicable to different nonlinear dynamical robot models and sensors. More generally, our results show that secure trajectories can be substantially different from minimum-time trajectories, and demonstrate that the security of systems with nonlinear dynamics depends upon the inputs adopted for control.

Paper organization The remainder of the paper is organized as follows. Section 2 presents our problem setup and attack model. Section 3 contains our notion of undetectability and our characterization of undetectable attacks. Section 4 and Section 5 contain, respectively, the design of optimal undetectable attacks and of secure trajectories. Finally, Section 6 contains an extension of our results to the case of robots with unicycle dynamics, and Section 7 concludes the paper.

2. Problem setup and preliminary notions

We consider a robot with double-integrator dynamics,

$$\underbrace{\begin{bmatrix} \dot{p}_{\mathrm{n}} \\ \dot{v}_{\mathrm{n}} \end{bmatrix}}_{\dot{x}_{\mathrm{n}}} = \underbrace{\begin{bmatrix} 0_2 & I_2 \\ 0_2 & 0_2 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} p_{\mathrm{n}} \\ v_{\mathrm{n}} \end{bmatrix}}_{x_{\mathrm{n}}} + \underbrace{\begin{bmatrix} 0_2 \\ I_2 \end{bmatrix}}_{B} u_{\mathrm{n}}, \tag{1}$$

where $p_{\mathrm{n}} : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ denotes the robot position, $v_{\mathrm{n}} : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ the robot velocity, and $u_{\mathrm{n}} : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ the nominal control input that actuates the acceleration of the robot. The control input u_{n} is the design parameter that is used to plan the nominal robot trajectory between two desired configurations. We assume that u_{n} is piecewise continuous, and that

$$\|u_{\mathrm{n}}\| \leq u_{\max},$$

where $u_{\max} \in \mathbb{R}_{>0}$. We let the robot be equipped with two noiseless sensors: a GNSS receiver that provides an absolute measure of the position, and a RSSI sensor that provides a measure of the relative distance between the robot and a base station located at the origin of the reference frame. Specifically, the sensor readings are

$$y_{\mathrm{n}}^{\mathrm{GNSS}} = p_{\mathrm{n}}, \quad \text{and} \quad y_{\mathrm{n}}^{\mathrm{RSSI}} = p_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}}. \tag{2}$$

Although our results can be extended to include different sensors, we focus on GNSS and RSSI sensors because they are available in many practical applications (Jun & D'Andrea, 2003).

We consider scenarios where the robot operates in an adversarial environment, where adversaries can simultaneously (i) spoof the GNSS signal $y_{\mathrm{n}}^{\mathrm{GNSS}}$, and (ii) compromise the control input u_{n}. The robot dynamics in the presence of attacks are

$$\underbrace{\begin{bmatrix} \dot{p} \\ \dot{v} \end{bmatrix}}_{\dot{x}} = \underbrace{\begin{bmatrix} 0_2 & I_2 \\ 0_2 & 0_2 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} p \\ v \end{bmatrix}}_{x} + \underbrace{\begin{bmatrix} 0_2 \\ I_2 \end{bmatrix}}_{B} u, \tag{3}$$

where $u \in \mathbb{R}^2$ denotes the attacked control input that obeys the bound on the maximum acceleration $\|u\| \leq u_{\max}$, and

$$y^{\mathrm{GNSS}} = p + u^{\mathrm{GNSS}}, \quad \text{and} \quad y^{\mathrm{RSSI}} = p^{\mathsf{T}} p, \tag{4}$$

where $u^{\mathrm{GNSS}} : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ denotes the GNSS spoofing signal. Finally, we make the practical assumption that, at time $t = 0$, the nominal and attacked configurations satisfy $x_{\mathrm{n}}(0) = x(0)$.

In the remainder of this paper, we will denote the state by $x = [p^{\mathsf{T}}, v^{\mathsf{T}}]^{\mathsf{T}}$ or p and v interchangeably, depending on the context. In particular, we let $x = [x_1, x_2, x_3, x_4]^{\mathsf{T}}$, and $p = [p^x, p^y]^{\mathsf{T}} = [x_1, x_2]^{\mathsf{T}}$, $v = [v^x, v^y]^{\mathsf{T}} = [x_3, x_4]^{\mathsf{T}}$.

Remark 1 (*Spoofing Attack Mechanism*)**.** Well-known vulnerabilities of GNSS are conventionally associated with the lack of appropriate encryption in the signals that are broadcast by the satellite system. A typical framework to cast spoofing attacks consists in a receiver-spoofer antenna (Shepard, Humphreys, & Fansler, 2012) that is capable of sensing the authentic GNSS signals and of rebroadcasting falsified streams of information at a higher signal intensity. The retransmitted signals are typically designed in a way to induce the GNSS receiver to resynchronize with the spoofed information, for instance by gradually increasing the intensity of the retransmission. Once the onboard receiver has resynchronized with the falsified signals, an attacker can arbitrarily decide the GNSS data received by the robot, resulting in (4). A more in-depth discussion of common spoofing schemes and the required hardware can be found in e.g. Kerns, Shepard, Bhatti, and Humphreys (2014) and Shepard et al. (2012).

In common mobile robotic applications, robots communicate wirelessly with a ground control station, that is responsible to compute the actions and control inputs to be executed by the robot. The use of wireless communication constitutes a possible vulnerability that can be modeled as in (3). See Hartmann and Steup (2013) for a discussion of common vulnerabilities of wireless communication in commercial Unmanned Aerial Vehicles (UAV). □

In this work we consider two problems that formalize the contrasting objectives of an attacker, that is, to deviate the robot trajectory while remaining undetected, and the trajectory planner, that is, to design a trajectory between two configurations that is robust to attacks. We refer to the latter problem to as the *secure trajectory planning* problem. In particular, the attacker aims to design the attack inputs (u, u^{GNSS}) so that

(i) the deviation between the robot nominal trajectory and the actual (attacked) trajectory is maximized; and
(ii) the attack remains undetected (as defined below).

Instead, the secure trajectory planning problem asks for a nominal control input u_{n} to guarantee that

(iii) in the absence of attacks, u_{n} allows the robot to reach a desired final state; and
(iv) in the presence of attacks, attacks are detectable (see below) by processing the signals u_{n}, y^{GNSS}, and y^{RSSI}.

Two observations are in order. First, although the problem of trajectory planning has a long history in robotics (e.g., see LaValle, 2006), the problem of designing trajectories in adversarial environments has not been studied before. Second, the large body of literature on detection and mitigation of attacks in cyber–physical systems with linear dynamics (e.g., see Bai et al., 2017; Pasqualetti et al., 2013) is not applicable to the considered secure trajectory planning problem, since the system model is nonlinear due to (4). As we show later in this paper, and differently from the case of systems with linear dynamics, attack detectability for nonlinear systems depends also on the control input adopted by the trajectory planner.

We next formalize the notion of attack undetectability.

Definition 2 (*Undetectable Attack*)**.** The attack (u, u^{GNSS}) is undetectable if the measurements satisfy, at all times,

$$y^{\text{GNSS}} = y_{\text{n}}^{\text{GNSS}}, \quad \text{and} \quad y^{\text{RSSI}} = y_{\text{n}}^{\text{RSSI}},$$

and it is detectable otherwise. □

Loosely speaking, an attack is undetectable if the measurements generated by the attacker are compatible with their nominal counterparts and with the robot dynamics at all times. On the other hand, if the conditions in Definition 2 are not satisfied, then the attack is readily detected by simple comparison between the nominal and actual measurements.

Remark 3 (*Attack Detectability in the Presence of Noise*)**.** In this work we characterize undetectable attacks and secure trajectories for deterministic systems. When the dynamics or the sensors are driven by noise, different and more relaxed notions of attack detectability should be adopted, as done for instance in Bai et al. (2017) for the case of linear dynamics. Loosely speaking, undetectable attacks are easier to cast in stochastic systems, because an attacker has the additional possibility of hiding its action within the noise limits. Thus, the conditions derived in this paper for deterministic systems serve as fundamental limitations also for stochastic systems. □

Finally, we combine the objectives of the attacker and of the trajectory planner into an optimization problem of the general form:

$$\begin{aligned} \max_{u,u^{\text{GNSS}}} \ \min_{u_{\text{n}},T} \quad & \int_0^T L(x_{\text{n}}, x, t)\, dt + V(x_{\text{n}}(T), x(T)), \\ \text{subject to} \quad & \text{Dynamics (1) and (3)}, \\ & (u, u^{\text{GNSS}}) \text{ is undetectable}, \end{aligned} \tag{5}$$

where $T \in \mathbb{R}_{>0}$ represents the planning horizon, $L : \mathbb{R}^4 \times \mathbb{R}^4 \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is an integral cost, and $V : \mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}_{\geq 0}$ is a terminal cost that is chosen to penalize deviations between the nominal and attacked trajectories at the final time. The optimization problem (5) captures the general class of problems that can be solved with the framework proposed in this paper, and will be further specified and discussed in the following sections.

We observe that (5) is composed of two sequential phases. In the first phase, the trajectory planner designs the nominal control input u_{n} and the control horizon T (inner minimization problem) to satisfy the objectives (iii) and (iv). In the second phase, the attacker designs the attack inputs (u, u^{GNSS}) given the nominal input u_{n} (outer maximization problem) to satisfy objectives (i) and (ii). Further, we note that (5) can be interpreted as a Stackelberg game (Başar & Olsder, 1999), where undetectable attacks represent the best response among all strategies that can be adopted by the attacker, and secure trajectories represent the strategy that maximizes the payoff of the trajectory planner, anticipating the fact that the attacker will adopt its best response.

Remark 4 (*Control Mechanism and Attacker Information*)**.** Our formulation (5) reflects a control framework where the trajectory of the robot is planned in an open-loop fashion at the beginning of the control horizon by a remote control station, and the resulting control parameters are then transmitted in batch to the robot (Jun & D'Andrea, 2003). Our assumptions are motivated by the vulnerabilities of wireless communication, through which an attacker can intercept the information transmitted to the robot. Thus, to successfully cast undetectable attacks, the attacker is required to know the robot dynamics and the nominal trajectory ahead of time. These requirements can be relaxed in the case of single integrator dynamics (Bianchin, Liu, & Pasqualetti, 2019). □

Remark 5 (*Undetectability with GNSS Sensor*)**.** In scenarios where GNSS is the only sensor for detection, an adversary can deliberately alter the control input while remaining undetected. To see this, notice that the effect of any attack u can be canceled from the GNSS reading by selecting $u^{\text{GNSS}} = p_{\text{n}} - p$. Thus, secure trajectories for the considered attack model do not exist if the robot has no redundancy to combine with the GNSS readings. □

3. Characterization of undetectable attacks

In this section we characterize the class of undetectable attacks and the resulting attacked trajectories. First, we establish a relationship between the nominal and attacked instantaneous position and velocity. Then, we derive an explicit expression of undetectable attacks, and demonstrate how an attacker can readily design attacks that escape detection. The following result relates attack trajectories with their nominal counterparts.

Lemma 6 (*Undetectable Trajectories*)**.** *Let (u, u^{GNSS}) be an undetectable attack. Then,*

$$p^{\mathsf{T}} p = p_{\text{n}}^{\mathsf{T}} p_{\text{n}}, \ \text{and} \ v^{\mathsf{T}} p = v_{\text{n}}^{\mathsf{T}} p_{\text{n}}.$$

Proof. The first equality in the statement follows by substitution of (2) and (4) into Definition 2. Further, by taking the time-derivative on both sides of the equality $p^{\mathsf{T}} p = p_{\text{n}}^{\mathsf{T}} p_{\text{n}}$, and by using the assumption $x_{\text{n}}(0) = x(0)$, we obtain $2\dot{p}^{\mathsf{T}} p = 2\dot{p}_{\text{n}}^{\mathsf{T}} p_{\text{n}}$ at all times, from which the statement follows. ■

From Lemma 6, trajectories generated by undetectable attacks are characterized by two features: at all times, (i) the distance $p^{\mathsf{T}} p$ between the attacked position and the RSSI-base station must

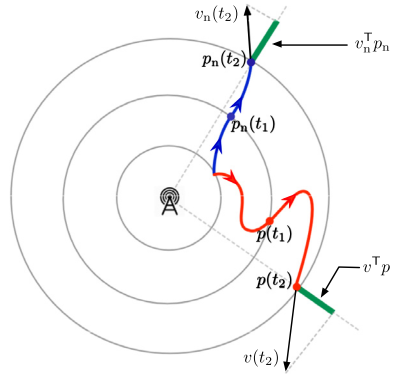


Fig. 1. Nominal (blue) and undetectable attack (red) trajectories. At all times, the two trajectories have identical relative distance from the base station, and equal velocity components along the direction of the instantaneous position (green segments). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

equal the distance $p_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}}$ in the nominal trajectory, and (ii) the component of the velocity v along the position p must equal the component of the nominal velocity v_{n} along p_{n}. These two geometric properties are illustrated in Fig. 1. Next, we give an implicit characterization of undetectable attacks.

Theorem 7 (*Implicit Characterization of Undetectable Attacks*)**.** *The attack* (u, u^{GNSS}) *is undetectable if and only if*

$$u^{\mathsf{T}} p = u_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}} + \|v_{\mathrm{n}}\|^2 - \|v\|^2, \ \text{and } u^{\mathrm{GNSS}} = p_{\mathrm{n}} - p. \tag{6}$$

Proof. (*Only if*) By substitution of (2) and (4) into Definition 2 we readily obtain $p + u^{\mathrm{GNSS}} = p_{\mathrm{n}}$, from which the second identity in the statement follows. To show the first identity, we note that for every undetectable attack u the identity $y^{\mathrm{RSSI}} - y_{\mathrm{n}}^{\mathrm{RSSI}} = 0$ holds. We then make explicit the dependence on the control input in the above identity by taking the second-order derivative with respect to time. This yields $\ddot{y}^{\mathrm{RSSI}} - \ddot{y}_{\mathrm{n}}^{\mathrm{RSSI}} = 0$. Then,

$$0 = \ddot{y}^{\mathrm{RSSI}} - \ddot{y}_{\mathrm{n}}^{\mathrm{RSSI}} = 2u^{\mathsf{T}} p + 2v^{\mathsf{T}} v - 2u_{\mathrm{n}}^{\mathsf{T}} u_{\mathrm{n}} - 2v_{\mathrm{n}}^{\mathsf{T}} v_{\mathrm{n}},$$

from which (6) follows. We emphasize that the functions $\dot{y}^{\mathrm{RSSI}}$, $\ddot{y}^{\mathrm{RSSI}}$, $\dot{y}_{\mathrm{n}}^{\mathrm{RSSI}}$, $\ddot{y}_{\mathrm{n}}^{\mathrm{RSSI}}$ are piecewise continuous functions, since the signals y^{RSSI} and $y_{\mathrm{n}}^{\mathrm{RSSI}}$ are continuous and twice differentiable at all times. To see this, we combine the piecewise continuity assumption on u_{n} and u with the dynamical equations (1) and (3), and note that the velocities v_{n} and v and the positions p_{n} and p are continuous and differentiable functions of time.

(*If*) Let $u^{\mathrm{GNSS}} = p_{\mathrm{n}} - p$. Substituting into (4) yields

$$y^{\mathrm{GNSS}} - y_{\mathrm{n}}^{\mathrm{GNSS}} = p + u^{\mathrm{GNSS}} - p_{\mathrm{n}} = 0,$$

from which the first condition in Definition 2 follows. To prove RSSI undetectability, let u satisfy (6). Then,

$$\ddot{y}^{\mathrm{RSSI}} - \ddot{y}_{\mathrm{n}}^{\mathrm{RSSI}} = 2u^{\mathsf{T}} p + 2v^{\mathsf{T}} v - 2u_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}} - 2v_{\mathrm{n}}^{\mathsf{T}} v_{\mathrm{n}} = 0,$$

from which we readily obtain the identity $\ddot{y}^{\mathrm{RSSI}} - \ddot{y}_{\mathrm{n}}^{\mathrm{RSSI}} = 0$. Since the functions y^{RSSI} and $y_{\mathrm{n}}^{\mathrm{RSSI}}$ are continuous and twice differentiable, and the initial conditions satisfy $p(0) = p_{\mathrm{n}}(0)$ and $v(0) = v_{\mathrm{n}}(0)$ we conclude that $\dot{y}^{\mathrm{RSSI}} - \dot{y}_{\mathrm{n}}^{\mathrm{RSSI}} = 0$ and $y^{\mathrm{RSSI}} - y_{\mathrm{n}}^{\mathrm{RSSI}} = 0$. Thus, $y^{\mathrm{RSSI}} = y_{\mathrm{n}}^{\mathrm{RSSI}}$ at all times, which implies undetectability of the attack u and concludes the proof. ■

Finally, we exploit Theorem 7 to give an explicit and comprehensive characterization of undetectable attacks.

Corollary 8 (*Explicit Characterization of Undetectable Attacks*)**.** *The attack* (u, u^{GNSS}) *is undetectable if and only if it satisfies*

$$u = a_{\mathrm{r}} p + w \ \text{and } u^{\mathrm{GNSS}} = p_{\mathrm{n}} - p, \tag{7}$$

whenever $\|p\| \neq 0$, *where* $w^{\mathsf{T}} p = 0$ *and*

$$a_{\mathrm{r}} = \frac{u_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}} + \|v_{\mathrm{n}}\|^2 - \|v\|^2}{\|p\|^2}.$$

Corollary 8 provides a systematic way to design undetectable attacks by designing the attack inputs (u, u^{GNSS}). We also note that the input w can be arbitrarily selected by the attacker and it does not affect detectability of the attack. Finally, it should be noticed that a_{r} corresponds to the radial acceleration of the robot, that is, the projection of u along p, and that the attack input u is unconstrained when $\|p\| = 0$ (see also Theorem 7).

4. Design of optimal undetectable attacks

In this section we design undetectable attacks that introduce maximal deviations between the nominal and attacked trajectories. Assuming that the attacker knows the nominal control input, we address the optimal control problem

$$\begin{aligned}
\max_{w} \quad & \|p(T) - p_{\mathrm{n}}(T)\|, \\
\text{subject to} \quad & \dot{x} = Ax + Bu, && \text{(8a)} \\
& u = a_{\mathrm{r}} p + w, && \text{(8b)} \\
& a_{\mathrm{r}} = (u_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}} + \|v_{\mathrm{n}}\|^2 - \|v\|^2)\|p\|^{-2}, && \text{(8c)} \\
& \|u\| \leq u_{\max}. && \text{(8d)}
\end{aligned}$$

In the maximization problem (8), constraint (8a) corresponds to the attacked dynamics (3), while (8b)–(8c) enforce attack-undetectability from Corollary 8. We next characterize the optimality conditions of the problem (8). Let e_i denote the ith canonical vector of appropriate dimension, and let sgn( ) denote the sign function.

Theorem 9 (*Attack Optimality Conditions*)**.** *Let* a_{r} *be as in* (8c), *and let* w^* *be an optimal solution to* (8). *Then,*

$$w^* = a_{\mathrm{t}} W x,$$

where

$$a_{\mathrm{t}} = -\operatorname{sgn}(\lambda^{\mathsf{T}} B \mathrm{W} x)\sqrt{u_{\max}^2/\|p\|^2 - a_{\mathrm{r}}^2},$$
$$W = \begin{bmatrix} -e_2 & e_1 & 0_2 & 0_2 \end{bmatrix},$$

and λ *and* x *satisfy*

$$\dot{x} = Ax + a_{\mathrm{r}} B p + B w^*,$$
$$-\dot{\lambda} = (A^{\mathsf{T}} \lambda + a_{\mathrm{r}} \tilde{P} + a_{\mathrm{t}} \tilde{W})\lambda + (x^{\mathsf{T}} \tilde{P} \lambda + 2 a_{\mathrm{r}} \nu \|p_{\mathrm{n}}\|^2)\nabla_x a_{\mathrm{r}},$$

with boundary conditions

$$x(0) = x_{\mathrm{n}}(0), \ \text{and } \lambda(T) = -2[(p(T) - p_{\mathrm{n}}(T))^{\mathsf{T}} \ 0_2^{\mathsf{T}}]^{\mathsf{T}},$$

where $\tilde{P} = P^{\mathsf{T}} B^{\mathsf{T}}$, $\tilde{W} = W^{\mathsf{T}} B^{\mathsf{T}}$, $\nabla_x a_{\mathrm{r}} = 2\|p\|^{-2}[0_2^{\mathsf{T}} \ v^{\mathsf{T}}]^{\mathsf{T}}$, *and* $\nu = -\frac{\lambda^{\mathsf{T}} B \mathrm{W} x}{2 a_{\mathrm{t}} \|p\|^2}$.

Proof. To formalize the result, we make use of the fact that any undetectable attack (7) can be written in the form

$$u = a_{\mathrm{r}} \mathrm{P} x + a_{\mathrm{t}} \mathrm{W} x, \tag{9}$$

where $\mathrm{P} = [e_1 \ e_2 \ 0 \ 0] \in \mathbb{R}^{2\times 4}$, $\mathrm{W} = [-e_2 \ e_1 \ 0 \ 0] \in \mathbb{R}^{2\times 4}$, and $a_{\mathrm{t}} : \mathbb{R}_{\geq 0} \to \mathbb{R}$. Following expression (9), the function a_{t} represents the new design parameter in the optimization problem. To derive the optimality conditions for (8), we use the Pontryagin's Maximum

Principle (Gelfand, Silverman, et al., 2000), combined with the direct adjoining method for mixed state-input constraints (Hartl, Sethi, & Vickson, 1995). We incorporate (8b) and (9) into (8a) and define the *Hamiltonian*

$$\mathcal{H}(x, a_{\mathrm{t}}, \lambda, t) = \lambda^{\mathsf{T}}(Ax + B(a_{\mathrm{r}}\mathrm{P}x + a_{\mathrm{t}}\mathrm{W}x)),$$

where $\lambda : [0, T] \to \mathbb{R}^4$ is a vector function of system costates, with the additional constraints

$$x(0) = x_{\mathrm{n}}(0),\ a_{\mathrm{r}} = \frac{u_{\mathrm{n}}^{\mathsf{T}} p_{\mathrm{n}} + \|v_{\mathrm{n}}\|^2 - \|v\|^2}{\|p\|^2},\ \|u\| \le u_{\max}.$$

We then use (9) to rewrite the bound $\|u\| \le u_{\max}$ as

$$a_{\mathrm{r}}^2\|p_{\mathrm{n}}\|^2 + a_{\mathrm{t}}^2\|p_{\mathrm{n}}\|^2 \le u_{\max}^2,$$

and form the Lagrangian by adjoining the Hamiltonian with the considered state constraint:

$$\mathcal{L}(x, a_{\mathrm{t}}, \lambda, t, \nu) = \mathcal{H}(x, a_{\mathrm{t}}, \lambda, t) + \nu(a_{\mathrm{r}}^2\|p_{\mathrm{n}}\|^2 + a_{\mathrm{t}}^2\|p_{\mathrm{n}}\|^2 - u_{\max}^2),$$

where $\nu : [0, T] \to \mathbb{R}$ is the Lagrange multiplier associated with the state constraint.

By application of the Maximum Principle (Hartl et al., 1995), the optimal control input a_{t}^* minimizes the Hamiltonian over the set $U(x) = \{a_{\mathrm{t}} : a_{\mathrm{r}}^2\|p\|^2 + a_{\mathrm{t}}^2\|p\|^2 \le u_{\max}^2\}$, that is, $a_{\mathrm{t}}^* = \arg\min_{a_{\mathrm{t}} \in U(x)} \mathcal{H}(x, a_{\mathrm{t}}, \lambda, t)$. This fact yields the optimal control law

$$a_{\mathrm{t}}^* = -\operatorname{sgn}(\lambda^{\mathsf{T}} B\mathrm{W}x)\sqrt{u_{\max}^2/\|p\|^2 - a_{\mathrm{r}}^2}.$$

Moreover, it follows from the Maximum Principle that there exists a vector function of system costates λ that satisfies the following system of equations

$$\begin{aligned}
\dot{x} = \frac{\partial \mathcal{L}}{\partial \lambda} &\Rightarrow \quad \dot{x} = Ax + B(a_{\mathrm{r}}\mathrm{P}x + a_{\mathrm{t}}\mathrm{W}x),\\
-\dot{\lambda} = \frac{\partial \mathcal{L}}{\partial x} &\Rightarrow \quad -\dot{\lambda} = A^{\mathsf{T}}\lambda + a_{\mathrm{r}}P^{\mathsf{T}}B^{\mathsf{T}}\lambda + x^{\mathsf{T}}P^{\mathsf{T}}B^{\mathsf{T}}\lambda\nabla_x a_{\mathrm{r}} + \\
&\qquad\qquad a_{\mathrm{t}}W^{\mathsf{T}}B^{\mathsf{T}}\lambda + 2a_{\mathrm{r}}\nu\|p_{\mathrm{n}}\|^2\nabla_x a_{\mathrm{r}}\\
0 = \frac{\partial \mathcal{L}}{\partial a_{\mathrm{t}}} &\Rightarrow \quad 0 = \lambda^{\mathsf{T}}BWx + 2\nu a_{\mathrm{t}}\|p\|^2,
\end{aligned}$$

where $\nabla_x a_{\mathrm{r}}$ denotes the gradient of a_{r} with respect to x, and with boundary conditions

$$x(0) = x_{\mathrm{n}}(0), \text{ and } \lambda(T) = \frac{\partial}{\partial x}\|p(T) - p_{\mathrm{n}}(T)\|.$$

The statement of the theorem follows by substituting the expression of the gradient $\nabla_x a_{\mathrm{r}} = 2\|p\|^{-2}[0\ 0\ v^{\mathsf{T}}]^{\mathsf{T}}$. ■

From Theorem 9, optimal undetectable attacks can be computed by solving a two-point boundary value problem (Keller, 2018). This class of problems is typically solved numerically, and it may lead to numerical difficulties for general cases (Keller, 2018). To conclude this section and provide some intuition in the design of optimal undetectable attacks, we next present an example where optimal attacks can be characterized explicitly.

Example 10 (*Undetectable Trajectories for Idle Robots*). Let $p_{\mathrm{n}}(0) = [1\ 0]^{\mathsf{T}}$, $v_{\mathrm{n}}(0) = 0$, and $u_{\mathrm{n}} = 0$, so that the robot remains at position $p_{\mathrm{n}}(0)$ at all times. Let $u_{\max} = 1$ and $T = 5$. Under these assumptions, the following control inputs satisfy the optimality conditions in Theorem 9:

$$a_{\mathrm{t}}^* = \begin{cases} \zeta\sqrt{u_{\max}^2 - a_{\mathrm{r}}^2}, & t \in [0, \tau],\\ -\zeta\sqrt{u_{\max}^2 - a_{\mathrm{r}}^2}, & t \in [\tau, T], \end{cases} \quad \text{and } a_{\mathrm{r}} = -\|v\|^2, \tag{10}$$

where $\tau = 3.475$, and $\zeta \in \{-1, 1\}$. It is worth noting that, because at every time the radial acceleration is proportional to the square of the magnitude of the velocity, the control input (10) leads the attacked robot to perform a circular motion around the origin (see Fig. 2). Notice that $\zeta = -1$ and $\zeta = 1$ achieve counterclockwise and clockwise motion, respectively. Finally, (10) is an optimal solution to the optimization problem (8) since the deviation $\|p(T) - p_{\mathrm{n}}(T)\|$ is maximized, as illustrated in Fig. 2.

To derive the value of the final time τ,we can explicitly derive an expression for the magnitude of the velocity vector $n := \|v\|$, that reads $\dot{n} = \sqrt{u_{\max}^2 - n^2}$, where we have substituted the expression for a_{r} into a_{t}^*, and used the fact that n is independent of a_{r}. To obtain the value of τ, we seek for the time needed to steer $n(t)$ from $u_{\max}$ to a full stop, by letting $n(0) = u_{\max}$ and $n(\tau) = 0$. □

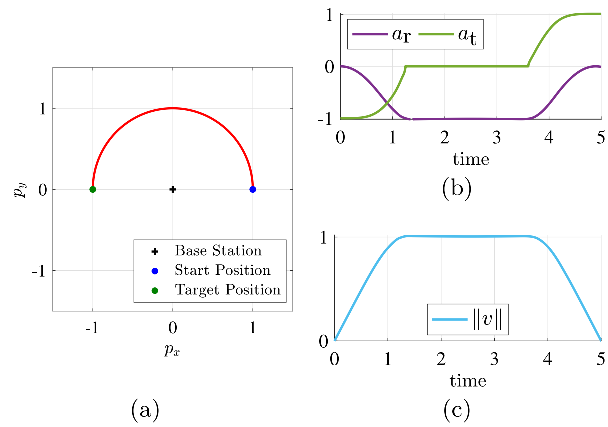


Fig. 2. For an idle robot at position (1, 0) (blue dot), (a) shows an optimal undetectable attack trajectory, which maintains a distance equal to 1 from the base station and maximizes the distance from the nominal position. Fig. (b) shows the radial and tangential components of the acceleration. Fig. (c) shows the velocity of the attacked robot, which becomes zero when the robot reaches the final point (−1, 0). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

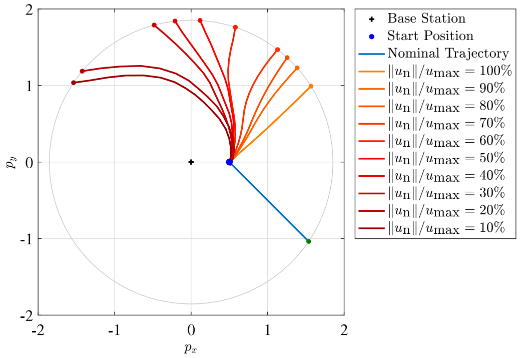


Fig. 3. For a nominal straight line trajectory (blue), the figure shows the undetectable attack trajectories obtained from Theorem 9 for different values of the nominal acceleration $\|u_{\mathrm{n}}\|/u_{\max}$. As the nominal acceleration decreases, the deviation induced by an optimal attack increases. Simulation parameters: $T = 1.5$, $v(0) = 0$, and $u_{\mathrm{n}} = [1, -1]^{\mathsf{T}}$ at all times. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

We show in Fig. 3 a set of simulations that illustrate the effects of optimal attacks (red) when the nominal trajectory is the shortest path between the initial and the final position (blue). In particular, the figure demonstrates that increasing levels of deviation are achieved by the attacker when the trajectory planner employs control inputs with decreasing magnitude (i.e., different and decreasing fractions of $u_{\max}$).

5. Design of secure trajectories

In this section we address the secure trajectory planning problem. First, we characterize the existence of secure trajectories as a function of the initial and final configurations of the robot. Then, we formulate and solve an optimization problem to design control inputs that generate secure trajectories to reach a desired final configuration. We start with some necessary definitions. We say that a trajectory x_{n} is *secure* if, independently of the attack u, one of the following mutually exclusive conditions is satisfied:

(C1) $p = p_{\mathrm{n}}$ at all times; or
(C2) if $p \neq p_{\mathrm{n}}$ at some time, the attack u is detectable.

Similarly, a control input is *secure* if it generates a secure trajectory. We next characterize secure control inputs explicitly.

Theorem 11 (*Secure Control Inputs*). *Let x_{n} be the trajectory generated by u_{n}. Then, u_{n} is secure if and only if the following conditions hold simultaneously:*

(1) there exists a function $\kappa : \mathbb{R}_{\geq 0} \to \{-1, 1\}$ satisfying

$$u_n = \kappa \frac{p_n}{\|p_n\|} u_{\max}, \tag{11}$$

(2) the trajectory x_{n} satisfies $p_n \neq 0$ at all times.

Proof. *If* We assume (1)–(2) and show that either (C1) or (C2) is satisfied. We distinguish among two cases.
(Case 1) The attack (u, u^{GNSS}) does not satisfy the undetectability condition (6). Then, (C2) follows.
(Case 2) The attack (u, u^{GNSS}) satisfies the undetectability condition (6). Under this assumption we now show that (1)–(2) imply (C1). We first consider the time instant $\tau = 0$. By using the assumption $x_{\mathrm{n}}(\tau) = x(\tau)$, which yields $p_{\mathrm{n}}(\tau) = p(\tau)$ and $\|v_{\mathrm{n}}(\tau)\| = \|v(\tau)\|$, and by substituting into (6) we obtain the following undetectability condition valid at time τ:

$$u_{\mathrm{n}}^{\mathsf{T}}(\tau) p_{\mathrm{n}}(\tau) = u^{\mathsf{T}}(\tau) p(\tau). \tag{12}$$

By taking the 2-norm on both sides of the above equality, and by substituting the expression (11) we obtain

$$u_{\max} \|p_{\mathrm{n}}(\tau)\| = |u_{\mathrm{n}}(\tau)^{\mathsf{T}} p_{\mathrm{n}}(\tau)| = |u^{\mathsf{T}}(\tau) p(\tau)| \leq u_{\max} \|p(\tau)\|,$$

where we used the Cauchy–Schwarz inequality. Since exact equality must hold, the vectors $u(\tau)$ and $p(\tau)$ are linearly dependent and $\|u(\tau)\| = u_{\max}$, that is,

$$u(\tau) = \gamma(\tau) \frac{p(\tau)}{\|p(\tau)\|} u_{\max},$$

where $\gamma(\tau) \in \{-1, 1\}$. Finally, we note that $\gamma(\tau) \neq \kappa(\tau)$ results in a violation of (12), and therefore $u(\tau) = u_{\mathrm{n}}(\tau)$. As a result, $p_{\mathrm{n}}(\tau^{+}) = p(\tau^{+})$. To conclude the proof, we iterate the above reasoning for all $\tau \in [0, T)$, from which (C1) follows.

(*Only if*) We show that (C1)–(C2) imply (1)–(2) or, equivalently, if (1)–(2) do not simultaneously hold, then (C1)–(C2) are not satisfied. We distinguish two cases.
(Case 1) Let $\bar{u}_{\mathrm{n}}$ be any control input that does not satisfy (11). That is, there exists $\bar{t} \in [0, T]$, such that

$$\bar{u}_{\mathrm{n}}(t) = u_{\mathrm{n}}(t) \text{ for all } t \in [0, \bar{t}), \qquad \text{and} \qquad \bar{u}_{\mathrm{n}}(\bar{t}) \neq u_{\mathrm{n}}(\bar{t}).$$

Let $\bar{u}$ be an attack input, with $\bar{u} = \bar{a}_{\mathrm{r}} p + \bar{w}$ as in Corollary 8. We take the absolute value of (7) and use the relationship $\|v_{\mathrm{n}}(\bar{t})\| = \|v(\bar{t})\|$ to obtain the inequality

$$|\bar{a}_{\mathrm{r}}(\bar{t})| = \frac{|\bar{u}_{\mathrm{n}}^{\mathsf{T}}(\bar{t}) p_{\mathrm{n}}(\bar{t})|}{\|p(\bar{t})\|} < u_{\max},$$

where strict inequality follows from the assumption $\bar{u}_{\mathrm{n}}(\bar{t}) \neq u_{\mathrm{n}}(\bar{t})$. As a result, any vector $\bar{w}$ that satisfies $\|\bar{a}_{\mathrm{r}}(\tau) p(\tau) + \bar{w}(\tau)\| = u_{\max}$, is a nonzero undetectable attack that violates (C1) and (C2).
(Case 2) There exists $\bar{t} \in [0, T]$, such that $\|p_{\mathrm{n}}(\bar{t})\| = 0$. It follows from (6) that whenever $p_{\mathrm{n}}(\bar{t}) = 0$ any attack input is unconstrained at time instant $\bar{t}$. As a result, any u with $u(t) = u_{\mathrm{n}}(t)$ for all $t \in [0, \bar{t})$ and $u(\bar{t}) \neq u_{\mathrm{n}}(\bar{t})$ is undetectable and violates (C1) and (C2). ■

Theorem 11 provides an explicit characterization of secure control inputs, and it shows that any secure control input has maximum magnitude $u_{\max}$ at all times, and its direction is aligned with the direction of the positioning vector. We next show that any secure trajectory evolves on an invariant manifold of the state space that is uniquely defined by the initial state of the robot.

Lemma 12 (*Invariant Manifold of Secure Trajectories*). *Let x_{n} be the trajectory generated by the secure control input u_{n}. Then, $x_{\mathrm{n}} \in \mathcal{S}$ at all times, where*

$$\mathcal{S} = \{x \;:\; x_1 x_4 - x_2 x_3 = x_1(0) x_4(0) - x_2(0) x_3(0)\}.$$

Proof. Let $x_{\mathrm{n}} = [x_1 \ x_2 \ x_3 \ x_4]^{\mathsf{T}}$ denote the solution to (1) with initial condition $x_{\mathrm{n}}(0)$, subject to control inputs that satisfy (1)–(2) in Theorem 11. To prove that $x_{\mathrm{n}} \in \mathcal{S}$, we equivalently show that the quantity $x_1 x_4 - x_2 x_3$ is time-invariant, that is, $\frac{d}{dt}(x_1 x_4 - x_2 x_3) = 0$. In fact,

$$\dot{x}_1 x_4 + x_1 \dot{x}_4 - \dot{x}_2 x_3 - x_2 \dot{x}_3 = 0,$$

where the last equality follows by substitution of (1). ■

Lemma 12 shows that secure trajectories are constrained to evolve on a manifold that is defined by the initial state of the robot, and it implies that only a subset of the state space can be reached via secure trajectories. These observations are illustrated in the next example.

Example 13 (*Reachable Configurations*). Let $x_{\mathrm{n}}(0) = [\bar{x}_1 \ 0 \ \bar{x}_3 \ 0]^{\mathsf{T}}$, where $\bar{x}_1 \in \mathbb{R}_{>0}$ and $\bar{x}_3 \in \mathbb{R}$, that is, let the robot at time $t = 0$ be located on the horizontal axis, with initial velocity in the horizontal direction. From Lemma 12, every secure trajectory satisfied $x_{\mathrm{n}} \in \mathcal{S}$ at all times, with

$$\mathcal{S} = \{x \;:\; x_1 x_4 - x_2 x_3 = 0\}.$$

It should be observed, however, that secure trajectories may in fact be constrained on a strict subset of $\mathcal{S}$. In fact, by combining the system dynamics (1) with the secure control input (11), we obtain

$$x_1 > 0, \quad x_2 = 0, \quad x_4 = 0,$$

which is a strict subset of $\mathcal{S}$. Notice that the above equations imply that the motion of the robot under secure control inputs is constrained on the positive x-axis. □

To determine a secure trajectory from the initial position p_{I} with given velocity v_{I} towards the final position p_{F}, we consider the optimization problem[1]

$$\begin{aligned} \min_{\kappa, T} \quad & T + \|p_{\mathrm{n}}(T) - p_{\mathrm{F}}\|, \\ \text{subject to} \quad & \dot{x}_{\mathrm{n}} = A x_{\mathrm{n}} + B u_{\mathrm{n}}, \\ & p_{\mathrm{n}}(0) = p_{\mathrm{I}}, \ v_{\mathrm{n}}(0) = v_{\mathrm{I}}, \\ & u_{\mathrm{n}} = \kappa \frac{p_{\mathrm{n}}}{\|p_{\mathrm{n}}\|} u_{\max}, \end{aligned} \tag{13}$$

[1] In the optimization problem, we allow a free final velocity to ensure that the final configuration achieved belongs to the invariant manifold that constraints the secure trajectory.

which aims to find a secure control input that minimizes a weighted combination of the distance to the desired final position and the time needed to reach such position. The following result characterizes the solutions to the optimization problem (13).

Theorem 14 (*Optimality Conditions for Secure Control Inputs*). *Let κ^* and T^* be an optimal solution to* (13). *Then,*

$$\kappa^* = -\operatorname{sgn}(\lambda^\mathsf{T} B p_\mathrm{n}), \ \ \textit{and } T^* = \xi,$$

where $\xi \in \mathbb{R}_{>0}$, x_n, and λ satisfy

$$\begin{aligned} \dot{x}_\mathrm{n} &= \xi(A x_\mathrm{n} + \frac{\kappa^* \, u_\mathrm{max}}{\|p_\mathrm{n}\|} B p_\mathrm{n}), \\ -\dot{\lambda} &= \xi(A^\mathsf{T}\lambda + \frac{\kappa^* \, u_\mathrm{max}}{\|p_\mathrm{n}\|^3} \Phi(p_\mathrm{n}) B^\mathsf{T} \lambda), \\ \dot{\xi} &= 0, \end{aligned} \tag{14}$$

for all $t \in [0, 1]$, with boundary conditions

$$\begin{aligned} & x_\mathrm{n}(0) = x_0, \\ & \lambda(1) = 2[(p(T) - p_\mathrm{n}(T))^\mathsf{T} 0_2^\mathsf{T}]^\mathsf{T}, \\ & \lambda(0)(A x_0 + B\kappa^*(0) \frac{p_n(0)}{\|p_n(0)\|} u_{max}) = -1, \end{aligned}$$

and

$$\Phi(p_\mathrm{n}) = \left(\|p_\mathrm{n}\|^2 I_2 - 2 p_\mathrm{n} p_\mathrm{n}^\mathsf{T}\right) \begin{bmatrix} I_2 & 0_2 \\ 0_2 & 0_2 \end{bmatrix}.$$

Proof. To determine the unknown final time T we employ a technique similar to Aly and Chan (1974) and let $t = \xi\tau$, where $\xi \in \mathbb{R}_{>0}$ is a constant unknown parameter, and τ is the new temporal variable, with $0 \leq \tau \leq 1$. We then use The Pontryagin's Maximum Principle (Gelfand et al., 2000) to derive the optimality conditions for the optimization problem (13), and consider the Hamiltonian

$$\mathcal{H}(x_\mathrm{n}, \kappa, \lambda) = 1 + \lambda^\mathsf{T} \xi (A x_\mathrm{n} + B u_\mathrm{n}),$$

where λ is the vector function of system costates. By application of the Maximum Principle (Gelfand et al., 2000), the optimal control input and corresponding trajectory satisfy the following optimality conditions

$$\begin{aligned} \dot{x}_\mathrm{n} &= \frac{\partial \mathcal{H}}{\partial \lambda} \Rightarrow \ \ \dot{x}_\mathrm{n} = \xi(A x_\mathrm{n} + B u_\mathrm{n}), \\ -\dot{\lambda} &= \frac{\partial \mathcal{H}}{\partial x_\mathrm{n}} \Rightarrow -\dot{\lambda} = \xi(A^\mathsf{T}\lambda + \frac{\partial u_\mathrm{n}}{\partial x_\mathrm{n}} B^\mathsf{T} \lambda), \end{aligned}$$

with boundary conditions $x_\mathrm{n}(0) = x_0$ and $\lambda(1) = \frac{\partial V}{\partial x}(x(1))$, where we used the fact $0 \leq \tau \leq 1$. To derive an expression for the partial derivative of u_n with respect to x_n we let $\mathrm{P} = [e_1 \ e_2 \ 0 \ 0] \in \mathbb{R}^{2\times 4}$ and rewrite (11) as

$$u_\mathrm{n} = \kappa \frac{\mathrm{P} x_\mathrm{n}}{\|\mathrm{P} x_\mathrm{n}\|} u_\mathrm{max},$$

which yields

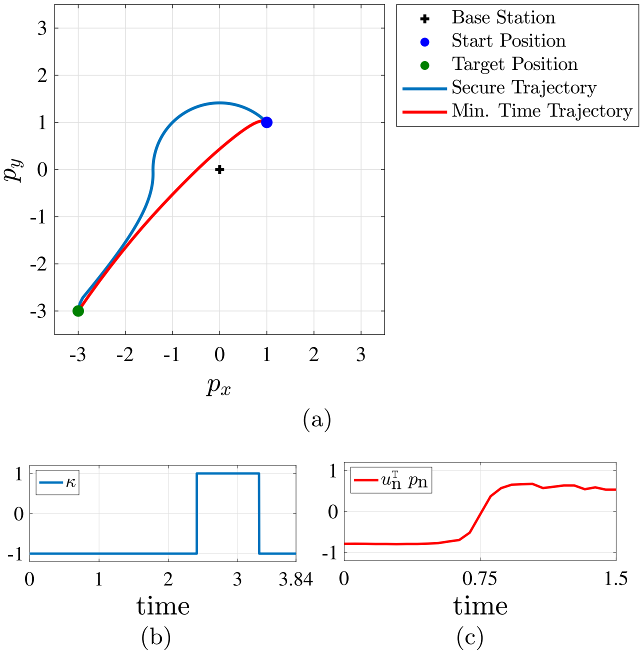
$$\frac{\partial u_\mathrm{n}}{\partial x_\mathrm{n}} = \frac{\kappa u_\mathrm{max}}{\|p_\mathrm{n}\|} \mathrm{P} - 2 \frac{\kappa u_\mathrm{max}}{\|p_\mathrm{n}\|^3} \mathrm{P} x_\mathrm{n} x_\mathrm{n}^\mathsf{T} \mathrm{P}^\mathsf{T} \mathrm{P}.$$

Hence, the expression for $\Phi(p_\mathrm{n})$ follows by substitution.

To determine the unknown final time, we consider the additional differential equation $\dot{\xi} = 0$, and let ξ be an unknown parameter. In particular, to determine the additional boundary condition we use the fact that the Hamiltonian is independent of time and the final time is free. Thus, the Hamiltonian is a first integral along optimal trajectories (Gelfand et al., 2000), i.e., $\mathcal{H}(x_\mathrm{n}, \kappa, \lambda) = \text{const.}$, with $\mathcal{H}(x_\mathrm{n}, \kappa, \lambda)|_{t=0} = 0$, which yield the claimed boundary conditions and the statement follows. ■

Table 1
Details for minimum-time and secure trajectories in Fig. 4.

	(Time) T	(Attack deviation) $\max_{w} \|p(T) - p_\mathrm{n}(T)\|$
Min. time trajectory	1.5	8.49
Secure trajectory	3.84	0



(a)

(b)

(c)

Fig. 4. (a) Secure (blue) and minimum time (red) trajectories between $p_\mathrm{I} = (1, 1)$ and $p_\mathrm{F} = (-3, -3)$, with $v(0) = [-1, 1]^\mathsf{T}$ and $u_\mathrm{max} = 1$. (b) and (c) Corresponding control inputs. Note that for minimum time trajectories, vectors u_n and p_n are not aligned at all times. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Theorem 14 allows us to compute secure control inputs by solving a two-point boundary value problem (Keller, 2018). We propose in Fig. 4 (see also corresponding data in Table 1) a comparison between a secure trajectory and a minimum time trajectory (non secure). In particular, a minimum-time trajectory is obtained by numerically solving the following optimization problem

$$\begin{aligned} \min_{u_\mathrm{n}, T} \quad & T \ + \ \|p_\mathrm{n}(T) - p_\mathrm{F}\|, \\ \text{subject to} \quad & \dot{x}_\mathrm{n} = A x_\mathrm{n} + B u_\mathrm{n}, \\ & p_\mathrm{n}(0) = p_\mathrm{I}, \ v_\mathrm{n}(0) = v_\mathrm{I}, \end{aligned}$$

Expectedly, the simulation shows that secure trajectories require longer control horizons as compared to commonly-adopted minimum-time trajectories, but have the benefit of preventing the existence of attacks.

6. Undetectable attacks and secure trajectories for robots with unicycle dynamics

The goal of this section is to characterize undetectable attacks and secure trajectories for robots with unicycle dynamics, so as to illustrate that the methods developed in this paper are applicable to a broad and general class of robot models. A robot with unicycle dynamics has one steerable drive wheel (Fantoni, Lozano, & Spong, 2000), and is modeled through the dynamical

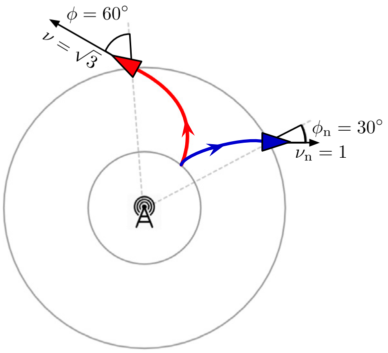


Fig. 5. Nominal (blue) and undetectable attack (red) trajectories. As discussed in Theorem 15, the illustrated vectors satisfy $v\cos(\phi) = v_n\cos(\phi_n)$ to guarantee undetectability. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

equations

$$\dot{p}_n^x = v_n\cos(\theta_n),\ \dot{p}_n^y = v_n\sin(\theta_n),\ \dot{\theta}_n = \omega_n,$$

where $p_n = [p_n^x\ p_n^y] : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ denotes the robot position, $\theta_n : \mathbb{R}_{\geq 0} \to [0, 2\pi)$ denotes the steering angle, $v_n : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ and $\omega_n : \mathbb{R}_{\geq 0} \to \mathbb{R}$ denote the wheel velocity and steering control, respectively. We assume that v_n is differentiable, ω_n is piecewise continuous, and that $v_n \leq v_{\max}$ and $|\omega_n| \leq \omega_{\max}$, where $v_{\max} \in \mathbb{R}_{>0}$ and $\omega_{\max} \in \mathbb{R}_{>0}$. Similarly to (3), we model the unicycle dynamics in the presence of attacks as

$$\dot{p}^x = v\cos(\theta),\ \dot{p}^y = v\sin(\theta),\ \dot{\theta} = \omega,$$

where $p = [p^x\ p^y] : \mathbb{R}_{\geq 0} \to \mathbb{R}^2$ and $\theta : \mathbb{R}_{\geq 0} \to [0, 2\pi)$ denote, respectively, the position and steering angle of the robot under attack, while $v : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ and $\omega : \mathbb{R}_{\geq 0} \to \mathbb{R}$ denote the attacked wheel velocity and steering control. As described in Section 2, we assume that the robot is equipped with a GNSS and an RSSI sensor, whose measurements are as in (2) in the absence of attacks, and as in (4) in the presence of attacks.

Using the notions in Definition 2, we next characterize undetectable attacks against robots with unicycle dynamics. In the remainder of this section, we let angle(v, w) denote the angle between the vectors v and w, that is

$$\text{angle}(v, w) = \arccos\left(\frac{v^\mathsf{T} w}{\|v\|\|w\|}\right),$$

with angle$(0, w) = $ angle$(v, 0) = 0$.

Theorem 15 (*Undetectable Attacks for Unicycle Dynamics*). *Let $\phi_n = \text{angle}(p_n, \dot{p}_n)$ and $\phi = \text{angle}(p, \dot{p})$. The attack $(v, \omega, u^{\text{GNSS}})$ is undetectable if and only if*

$$v\cos(\phi) = v_n\cos(\phi_n),\ \text{and}\ u^{\text{GNSS}} = p_n - p. \tag{15}$$

Proof. The proof follows by extending the proof of Theorem 7 to the considered unicycle dynamics. ■

An example where the condition in Theorem 15 holds is illustrated in Fig. 5. Next, we provide a characterization of secure control inputs for unicycle dynamics.

Theorem 16 (*Secure Control Inputs for Unicycle Dynamics*). *Let $\phi_n = \text{angle}(p_n, \dot{p}_n)$. The control input (v_n, ω_n) is secure if and only if the following conditions hold simultaneously:*

(1) $\phi_n(0) \in \{0, \pi\}$, and $p_n \neq 0$ at all times,
(2) $v_n = v_{max}$ and $\omega_n = 0$ at all times.

Proof. *If* We assume (1)–(2) and show that either (C1) or (C2) is satisfied. We distinguish among two cases.
(Case 1) The attack $(v, \omega, u^{\text{GNSS}})$ does not satisfy (15). Then, (C2) immediately follows.
(Case 2) The attack $(v, \omega, u^{\text{GNSS}})$ satisfies (15). We first focus on the time instant $\tau = 0$, and take the absolute value on both sides of the undetectability condition (15) to obtain the identity

$$|v_n(0)\cos(\phi_n(0))| = |v(0)\cos(\phi(0))|. \tag{16}$$

By substituting (1)–(2) into the left-hand side of (16) we obtain

$$|v_n(0)\cos(\phi_n(0))| = v_{\max}.$$

On the other hand, by applying the Cauchy–Schwarz inequality to the right-hand side of (16) we have

$$|v(0)\cos(\phi(0))| \leq |v(0)||\cos(\phi(0))| \leq v_{\max}.$$

By application of (16), exact equality must hold in the above bound, and thus we necessarily have $v(0) = v_{\max}$ and $|\cos(\phi(0))| = 1$. Finally, we use the fact that ϕ is a differentiable function of time to obtain $\phi(0) = \phi_n(0)$. To conclude the proof, we use the fact that $\omega_n = 0$ at all times, which implies $\phi_n(\tau) = \phi_n(0)$ for all τ (a formal proof of this fact can be done by leveraging the change of variables (17)), and iterate the above reasoning for all $\tau \in [0, T)$ to obtain $v = v_n$ and $\phi = \phi_n$ at all times, from which condition (C1) follows.

(*Only if*) We now show that (C1)–(C2) imply (1)–(2) or, equivalently, if (1)–(2) do not hold, then (C1)–(C2) are not verified. We distinguish among four cases.
(Case 1) The robot initial conditions are such that $\theta_n(0) \neq \{0, \pi\}$, and the nominal control inputs satisfy $v_n = v_{\max}$ and $\omega_n(t) = 0$ at all times. We consider the attack (v, ω), with

$$\dot{v} = \frac{1}{\cos\phi}\left(v_n\dot{\phi}_n\sin\phi_n - v\dot{\phi}\sin\phi\right),\ \text{and}\ \omega \neq 0,$$

and show that such attack is undetectable and violates (C1)–(C2). To prove undetectability, we use the fact that $x_n(0) = x(0)$, and equivalently show the identity between the time derivatives of (15), which yields

$$-v_n\dot{\phi}_n\sin\phi_n = \dot{v}\cos\phi - v\dot{\phi}\sin\phi,$$

where we used the relationship $\dot{v}_n = 0$ at all times. As a result, undetectability of (v, ω) follows by substitution. To conclude, we observe that (v, ω) is undetectable and violates (C1) and (C2).
(Case 2) There exists $\bar{t} \in [0, T]$ such that $\|p_n(\bar{t})\| = 0$. It follows from (15) that, when $p_n(\bar{t}) = 0$, angle$(0, \dot{p}_n(\bar{t})) = 0$. As a result, attack inputs are unconstrained at time $\bar{t}$, and any ω such that $\omega(t) = \omega_n(t)$ for all $t \in [0, \bar{t})$, and $\omega(\bar{t}) \neq \omega_n(\bar{t})$, is undetectable and violates (C1)–(C2).
(Case 3) Nominal control inputs satisfy $v_n = v_{\max}$ at all times, $\omega_n(t) = 0$ for all $t \in [0, \bar{t})$, and $\omega_n(\bar{t}) \neq 0$, $\bar{t} \in [0, T]$. We perform a change of variables (Siciliano, Sciavicco, Villani, & Oriolo, 2010)

$$\rho = \sqrt{p_x^2 + p_y^2},$$
$$\phi = \text{Atan2}(p_y, p_x) - \theta + \pi,$$
$$\delta = \phi + \theta, \tag{17}$$

which leads to the following dynamical equation $\dot{\phi} = \frac{\sin\phi}{\|p\|} - \omega$ that relates ϕ to the control inputs v and ω (see Siciliano et al., 2010). We then let $v = v_n$ at all times, and

$$\omega = \begin{cases} \omega_n, & \text{if } t \in [0, \bar{t}), \\ -\omega_n, & \text{if } t \in [\bar{t}, T], \end{cases}$$

from which we obtain

$$\dot{\phi} = \frac{\sin\phi}{\|p\|} - \omega = -\frac{\sin\phi_n}{\|p_n\|} + \omega_n = -\dot{\phi}_n,$$

for all $t \in [\bar{t}, T]$. By combining the above relationship with $\phi_{\mathrm{n}}(\bar{t}) = \phi(\bar{t})$ we obtain $\phi(t) = -\phi_{\mathrm{n}}(t)$ for all $t \in [\bar{t}, T]$. To conclude, we note that the given choice of (v, ω) leads to an undetectable attack that satisfies (15) and that violates (C1)–(C2).
(Case 4) Nominal control inputs satisfy $\omega_{\mathrm{n}} = 0$ at all times, $v_{\mathrm{n}}(t) = v_{\max}$ for all $t \in [0, \bar{t})$, and $v_{\mathrm{n}}(\bar{t}) < v_{\max}$, $\bar{t} \in [0, T]$. Under these assumptions, we consider the attack (v, ω) with $v(t) = v_{\mathrm{n}}(t)$ and $\omega(t) = \omega_{\mathrm{n}}(t)$ for all $t \in [0, \bar{t})$, and

$$\dot{v} = \frac{1}{\cos\phi}\left(\dot{v}_{\mathrm{n}} + v\dot{\phi}\sin\phi\right), \text{ and } \omega \neq 0,$$

for all $t \in [\bar{t}, T]$. To prove undetectability of the considered attack, we observe that $x_{\mathrm{n}}(\bar{t}) = x(\bar{t})$, and equivalently show the identity between the time derivatives of (15) for all $t \in (\bar{t}, T]$, which reads

$$\dot{v}_{\mathrm{n}} = \dot{v}\cos\phi - v\dot{\phi}\sin\phi,$$

where we used the relationships $\cos\phi_{\mathrm{n}} = 1$ and $\sin\phi_{\mathrm{n}} = 0$ at all times. As a result, undetectability of the given attack follows by substitution, which shows that (v, ω) is undetectable and violates (C1) and (C2). ■

From Theorem 16, a secure trajectory exists only if initial position, final position, and the origin are collinear. We conclude by observing that this aspect is consistent with the similar conclusions previously drawn in Theorem 11 and Lemma 12.

Remark 17 (*Generality of Our Methods*)**.** The approach presented in this work for the characterization of undetectable attacks and the resulting effects on the robot trajectories can be generalized to a wider class of nonlinear systems and attacks. The approach consists of three main steps, namely, the characterization of undetectable trajectories by studying the Lie derivatives of the measurement equations, the characterization of undetectable inputs and secure trajectories by solving a set of nonlinear algebraic equations akin to (6) and (15), and the study of the submanifold of the state space that can be reached by undetectable attacks. While systematic tools may exist to solve the first two steps for a broad class of dynamics, the problem of nonlinear constrained controllability in the third step, which is solved in this paper via numerical optimization, requires the development of novel control theories and tools. □

7. Conclusions

In this paper we introduce and study the problem of secure trajectory planning, that is, the design of trajectories to guarantee the navigation between two desired configurations despite the action of an attacker. We focus on the case where the robot has a GNSS sensor and a RSSI sensor, and provide an explicit characterization of secure trajectories, undetectable attacks, and their effects on the nominal trajectory. Further, we provide numerical algorithms to determine secure trajectories and optimal attacks, and we illustrate our findings through a set of examples. To the best of our knowledge, this work constitutes a first step towards understanding the fundamental limitations of attack-detection algorithms for systems with nonlinear dynamics. Several aspects are left as the subject of future investigation, including the extension of the methods to different classes of sensors and attacks, the development of robust control mechanisms to operate the system despite the presence of attacks, and the study of secure trajectories in the presence of sensing and actuation noise.

References

Aly, G. M., & Chan, W. C. (1974). Numerical computation of optimal control problems with unknown final time. *Journal of Mathematical Analysis and Applications*, *45*(2), 274–284.

Bai, C.-Z., Pasqualetti, F., & Gupta, V. (2017). Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. *Automatica*, *82*, 251–260.

Başar, T., & Olsder, G. J. (1999). *Dynamic noncooperative game theory* (2nd ed.). SIAM.

Bianchin, G., Liu, Y.-C., & Pasqualetti, F. (2019). Secure navigation of robots in adversarial environments. *IEEE Control Systems Letters*, *4*(1), 1–6.

Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., & Lachapelle, G. (2012). GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *ION position, location and navigation symposium* (pp. 479–487).

Fantoni, I., Lozano, R., & Spong, M. W. (2000). Energy based control of the pendubot. *IEEE Transactions on Automatic Control*, *45*(4), 725–729.

Gelfand, I. M., Silverman, R. A., et al. (2000). *Calculus of variations*. Courier Corporation.

Hamza, F., Tabuada, P., & Diggavi, S. (2011). Secure state-estimation for dynamical systems under active adversaries. In *Allerton conf. on communications, control and computing* (pp. 337–344). Monticello, IL, USA.

Hartl, R. F., Sethi, S. P., & Vickson, R. G. (1995). A survey of the maximum principles for optimal control problems with state constraints. *SIAM Review*, *37*(2), 181–218.

Hartmann, K., & Steup, C. (2013). The vulnerability of UAVs to cyber attacks - an approach to the risk assessment. In *International conference on cyber conflict* (pp. 1–23).

Hespanha, J. P., & Bopardikar, S. D. (2019). Output-feedback linear quadratic robust control under actuation and deception attacks. In *American control conference* (pp. 489–496). Philadelphia, PA, USA.

Hu, Q., Fooladivanda, D., Chang, Y. H., & Tomlin, C. J. (2018). Secure state estimation and control for cyber security of the nonlinear power systems. *IEEE Transactions on Automatic Control*, *5*(3), 1310–1321.

Jiang, X., Zhang, J., Harding, B. J., Makela, J. J., & Domínguez-García, A. D. (2013). Spoofing GPS receiver clock offset of phasor measurement units. *IEEE Transactions on Power Systems*, *28*(3), 3253–3262.

Jun, M., & D'Andrea, R. (2003). Path planning for unmanned aerial vehicles in uncertain and adversarial environments. In *Cooperative control: Models, applications and algorithms* (pp. 95–110). USA: Springer.

Keller, H. B. (2018). *Numerical methods for two-point boundary-value problems*. Courier Dover Publications.

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, *31*(4), 617–636.

Kim, J., Lee, C., Shim, H., Eun, Y., & Seo, J. H. (2019). Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors. *IEEE Transactions on Automatic Control*, *64*(3), 1162–1169.

LaValle, S. M. (2006). *Planning algorithms*. Cambridge University Press, Available at http://planning.cs.uiuc.edu.

Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., & Benedetto, M. D. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software*, *149*(2019), 174–216.

Mo, Y., & Sinopoli, B. (2010). Secure control against replay attacks. In *Allerton conf. on communications, control and computing* (pp. 911–918). Monticello, IL, USA.

Montgomery, P. Y., Humphreys, T. E., & Ledvina, B. M. (2009). Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In *ION international technical meeting* (pp. 124–130).

Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, *58*(11), 2715–2729.

Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic System*, *49*(4), 2250–2267.

Psiaki, M. L., O'Hanlon, B. W., Powell, S. P., Bhatti, J. A., Wesson, K. D., Humphreys, T. E., et al. (2014). GNSS spoofing detection using two-antenna differential carrier phase. In *International technical meeting of the satellite division of the institute of navigation* (pp. 2776–2800). Tampa, FL.

Radin, D. S., Swaszek, P. F., & Seals, K. C. (2015). GNSS spoof detection based upon pseudoranges from multiple receivers. In *International technical meeting of the institute of navigation* (pp. 657–671). Dana Point, CA.

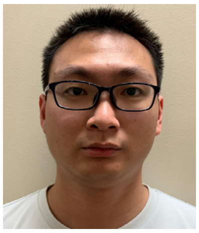
Shepard, D. P., Humphreys, T. E., & Fansler, A. A. (2012). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, *5*(3–4), 146–153.

Shoukry, Y., Nuzzo, P., Bezzo, N., Sangiovanni-Vincentelli, A. L., Seshia, S. A., & Tabuada, P. (2015). Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving. In *IEEE conf. on decision and control* (pp. 3804–3809).

Siciliano, B., Sciavicco, L., Villani, L., & Oriolo, G. (2010). *Robotics: modelling, planning and control*. Springer Science & Business Media.

Swaszek, P. F., Pratz, S. A., Arocho, B. N., Seals, K. C., & Hartnett, R. J. (2014). GNSS spoof detection using shipboard IMU measurements. In *International technical meeting of the satellite division of the institute of navigation* (pp. 745–758). Tampa, FL.

Zou, Q., Huang, S., Lin, F., & Cong, M. (2016). Detection of GPS spoofing based on UAV model estimation. In *Annual conference of the IEEE industrial electronics society* (pp. 6097–6102).



Yin-Chen Liu received the B.Sc. degree in Mechanical Engineering from the National Taipei University of Technology, Taiwan, in 2013, and the M.Sc. in Mechanical Engineering from the University of California, Riverside, in 2017. His main research interests are in the area of control systems, with applications to mobile robotics and cyber-physical security.

Gianluca Bianchin is a Ph.D. Candidate in the Department of Mechanical Engineering at the University of California, Riverside. He received the Laurea degree in Information Engineering and the Laurea Magistrale degree (Summa Cum Laude) in Controls Engineering from the University of Padova, Padova, Italy, in 2012 and 2014, respectively. In 2018 and 2019 he joined the Pacific Northwest National Laboratory and the Bosch Research Center as a Research Intern, respectively. His main research interests are in the modeling, analysis, and control of large-scale interconnected systems, with a focus on transportation networks and security of cyber-physical systems.

Fabio Pasqualetti is an Associate Professor in the Department of Mechanical Engineering, University of California at Riverside. He completed a Doctor of Philosophy degree in Mechanical Engineering at the University of California, Santa Barbara, in 2012, a Laurea Magistrale degree (M.Sc. equivalent) in Automation Engineering at the University of Pisa, Italy, in 2007, and a Laurea degree (B.Sc. equivalent) in Computer Engineering at the University of Pisa, Italy, in 2004. His main research interests include the analysis and control of complex networks, security of cyber-physical systems, distributed control, and network neuroscience. He has received several awards, including a Young Investigator Research Program award from AFOSR in 2020, a Young Investigator Program award from ARO in 2017, and the 2016 TCNS Outstanding Paper Award from IEEE CSS. He is a member of IEEE and SIAM.