UNIVERSITY OF CALIFORNIA
RIVERSIDE

RSSI-Aided Secure Trajectory Planning in the Presence of Spoofing

A Thesis submitted in partial satisfaction
of the requirements for the degree of

Master of Science

in

Mechanical Engineering

by

Yin-Chen Liu

June 2017

Thesis Committee:

Dr. Fabio Pasquiletti, Chairperson
Dr. Wei Ren
Dr. Qi Zhu

The Thesis of Yin-Chen Liu is approved:

Committee Chairperson

University of California, Riverside

Acknowledgments

I am grateful to my advisor, without whose help, I would not have been here.

To my parents for all the support.

ABSTRACT OF THE THESIS

RSSI-Aided Secure Trajectory Planning in the Presence of Spoofing

by

Yin-Chen Liu

Master of Science, Graduate Program in Mechanical Engineering
University of California, Riverside, June 2017
Dr. Fabio Pasquiletti, Chairperson

Global Navigation Satellite System (GNSS) is widely adopted in most applications requiring autonomous navigation, as it provides accurate measurements of a robots position with limited hardware and computation requirements. Yet, recent studies and real world incidents have demonstrated that GNSS readings can be easily corrupted, for instance, by jamming the receiver unit or spoofing the transmitted measurements via unauthorized GNSS transmissions. In the presence of attacks, success of autonomous navigation is not guaranteed in most scenarios. In this paper we put forth the idea of planning a robots trajectory and exploiting additional sensors to account and limit the effect of attacks against autonomous robots. In particular, we consider a robot equipped with a GNSS sensor and a Radio Signal Strength Indicator (RSSI) antenna, which provides the robot with an estimate of its distance to a radio station. We consider an attacker capable of arbitrarily spoofing the GNSS measurements and altering the robots input commands. We analytically characterize the class of undetectable attacks, that is, the attack signals that alter the robots nominal trajectory and that produce GNSS and RSSI measurements compatible with the robots nominal trajectory. We quantify the largest perturbation induced by an undetectable attack, and we show how the robots nominal trajectory should be designed to guarantee secure navigation in the presence of attacks.

Contents

List of Figures

Chapter 1

Introduction

In recent years autonomous robotic systems have been employed in a variety of engineering applications requiring advanced level of flexibility, adaptability, and accuracy, including surveillance and coverage control, search and rescue missions, and containment of hazardous materials. Yet, despite tremendous advances in sensing and communication technologies, fundamental vulnerabilities exist that undermine the correct and trustworthy operation of autonomous robots, as recently demonstrated by research studies [3, 11] and real-world incidents [7, 1]. New sophisticated methods are needed to guarantee the success of autonomous missions.

One of the most common attacks against autonomous systems consists of spoofing the Global Navigation Satellite System (GNSS), so as to provide the autonomous robot with falsified position information and induce large navigation errors. As a matter of fact, spoofing the GNSS readings can be easily achieved in civilian unencrypted devices [11], and it is also possible in more sophisticated systems. To implement such an attack, the attacker gradually overlays a spoofing GNSS signal to the nominal readings from the true GNSS satellites, so that the receiver eventually synchronizes with the falsified signal. At its core, vulnerability of the GNSS technology lies in the fact that the signal is broadcasted to all receiving units, making it possible to first mimic and then modify the information contained in the received signal. This type of attack has been used, for

instance, in the incidents of December 2011 [15], where a military drone was captured by the enemy due to relying on falsified position information.

Countermeasures to spoofing attacks have been studied. Existing approaches primarily rely on either analyzing the power spectrum of the received signal, so as to identify compromised transmissions [2, 6], or on creating measurements redundancy by combining GNSS measurements with those received by other sensors, such as the inertial measurement units [16, 18, 14, 13, 12, 8]. This work falls in the second category, as we employ a RSSI sensor to detect spoofing attacks against the GNSS system.

In this work, we focus on a situation where the UAV is under a combined attack, where the attacker is concurrently spoofing the GNSS signal and tampering with the control input of the robot. The contributions of this work are threefold. First, we formally characterize detectability of the combined GNSS-input attack from the sensors available on the UAV, specifically, GNSS and RSSI sensors. Second, we thoroughly characterize the class of attack strategies that are undetectable. We show that undetectable attack inputs depend not only on the dynamical model of the robot and its measurements, but also on the nominal control input and thus on the nominal trajectory of the UAV. This dependency is due to the non-linearity of the RSSI measurement model, and it distinguishes our study from prior works on the security of linear cyber-physical systems [9, 5]. Third, we characterize the region that the UAV can reach when driven by undetectable attacks, and we quantify the largest deviation between the nominal and attack trajectories induced by undetectable attacks. Finally, we illustrate our findings through simulations and experiments using the ROS platform.

The remainder of this thesis is organized as follows. Section 2 contains our formalism and problem definition. Section 3 characterize attack detectability and formalizes the competitive optimization problem solved by the attacker and the UAV. Section 4 quantifies the deviation introduced by undetectable attacks, and characterizes the region that the UAV can reach when driven by undetectable attacks. Finally, Section 5 contains the results of our simulations and experiments, and Section 6 concludes the thesis.

Chapter 2

Problem setup

2.1 Robot model

We consider a robot with single-integrator dynamics:

$$\dot{x}^{\text{nom}} = u, \tag{2.1}$$

where $x^{\text{nom}} : \mathbb{R} \to \mathbb{R}^2$ is the map describing the position of the robot over time, and $u : \mathbb{R} \to \mathbb{R}^2$ denotes the robot's control input. We assume that the robot moves with speed bounded by $u_{\max}$.

We let the robot be equipped with two noiseless sensors: a Global Navigation Satellite System (GNSS) receiver, which measures the robot's position, and a Radio Signal Strength Indicator (RSSI) sensor, which measures the distance between the robot and a base station located at the origin of the reference frame. The readings from the sensors are modeled as

$$\begin{aligned} {y_1}^{\text{nom}} &= x^{\text{nom}}, \\ {y_2}^{\text{nom}} &= (x^{\text{nom}})^{\mathsf{T}} x^{\text{nom}}, \end{aligned} \tag{2.2}$$

where $y_1 : \mathbb{R} \to \mathbb{R}^2$ and $y_2 : \mathbb{R} \to \mathbb{R}^2$ are the outputs of the GNSS and RSSI sensors at time $t \in \mathbb{R}_{\geq 0}$,

respectively.

2.2 Attack model

We consider a scenario where the robot moves in an adversarial environment, with an attacker capable of (i) spoofing the GNSS signal and (ii) arbitrarily modifying the robot's control input. Attacks are practically implemented by spoofing the GNSS signal [17] and by intercepting the control signal. In particular, in the presence of an attack the actual robot's dynamics read as

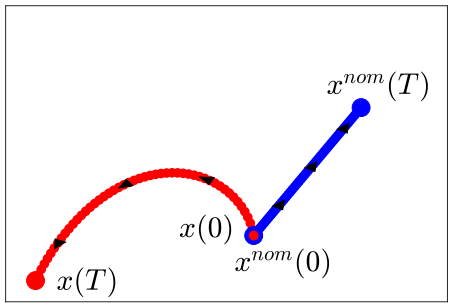
$$\begin{aligned} \dot{x} &= u + a_x, \\ y_1 &= x + a_y, \\ y_2 &= x^{\mathsf{T}} x, \end{aligned} \tag{2.3}$$

where $a_x : \mathbb{R} \to \mathbb{R}^2$ and $a_y : \mathbb{R} \to \mathbb{R}^2$ are the errors introduced by the attacker. The attack signals a_x and a_y are unknown and unmeasurable by the robot. Signal a_y is arbitrary, while a_x must satisfy the robot's velocity constraint, that is, $\|u + a_x\| \leq u_{\max}$ at all times $t \in \mathbb{R}_{\geq 0}$.

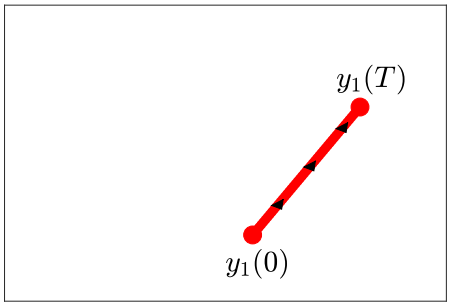
2.3 Problem Formulation

In this work we are interested in secure open-loop trajectory planning, where the robot's trajectory, which is determined by the nominal control input u, is pre-determined and executed by the robot without feedback information. We will say that an attack, described by the pair (a_x, a_y), is undetectable from sensors y_1 and y_2 if the output signals y_1 and y_2 are compatible with each other and with the nominal control input u (see section 3 for formal definition of attack detectibility). Thus, loosely speaking, we are interested in characterizing the robot's control input u that guarantees the following two properties:

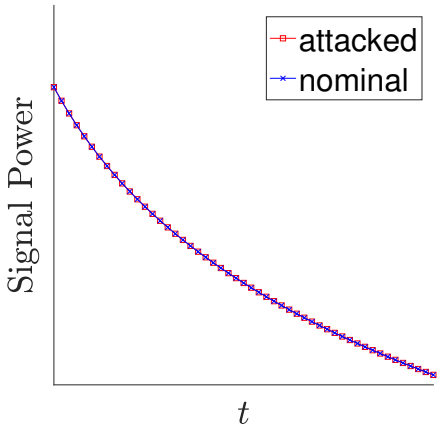
(i) in the absence of attacks, the input u allows the robot to reach a desired final state at a desired



(a)



(b)



(c)

Figure 2.1: Undetectable attack such that the designed trajectory and the trajectory under attack showed as the blue and red trajectory respectively in (a), while GNSS sensor reading (b) shows the same trajectory as the nominal trajectory and the RSSI sensor reading (c) shows no differences between the nominal trajectory and the attacked one.

time, and

(ii) in the presence of attacks, the input u and the measurements y_1, y_2 allow the robot to detect that its final position differs from the desired one, and that this deviation is as small as possible.

Conversely, the attacker's goal is to design the signals a_x and a_y in a way that

(iii) the robot's final position is as far as possible from the desired final location, and

(iv) the robot believes that the actual final position coincides with the desired one.

Tasks (i)-(iv) can be formalized through an optimization problem as follows :

$$\begin{aligned} \max_{a_x, a_y} \quad \min_{u} \quad & \|x^{\text{nom}}(T) - x(T)\|, \\ \text{subject to} \quad & \text{the attack } (a_x, a_y) \text{ is undetectable}, \\ & \|u + a_x\| \leq u_{\max}, \end{aligned} \tag{2.4}$$

where $T \in \mathbb{R}_{\geq 0}$ is the time horizon of the planning problem. In the optimization problem (2.4) the minimization over u represents the defender's objective to minimize the deviation caused by the attacker. Conversely, the attacker uses a_x, and a_y to maximize the distance between the nominal and the actual final position of the robot while remaining undetected. Notice that the optimization is of the form of a *minimax* problem, often used in decision and game theories [4].

Chapter 3

Undetectability of Attacks

In this section we formalize the notion of undetectable attacks, describe necessary conditions for undetectablility, and formalize the feasible set of problem (2.4). We consider scenarios where detection is performed (i) using GNSS readings only and (ii) using GNSS an RSSI data combined. We will show that when detection is based on the GNSS signal only, an attacker can steer the robot to any desired final location in the range bounded by only $x(0)$, $u_{\max}$ and T, along any trajectory while remain undetected. On the other hand, when detection is performed using both GNSS and RSSI readings, the class of undetectable trajectories limits the attacker capabilities in a way that we characterize.

3.1 GNSS-based attack detection

The following definition formalizes the notion of undetectable attacks to signals that make the GNSS output compatible with the corresponding nominal readings.

Definition 1 *(**Undetectable attack through** y_1) For the robot's dynamical model* (2.3)*, an attack is undetectable through* y_1 *if*

$$y_1 = y_1^{\text{nom}}, \tag{3.1}$$

at all times $t \in \mathbb{R}_{\geq 0}$*, where* y_1^{nom} *is an output of the nominal model* (2.2) *with input* u *and initial position* $x^{\text{nom}}(0)$*.* □

By using the dynamical model (2.1), (2.2) and (2.3), Definition 1 leads to the following condition for undetectability of attack: $\frac{d}{dt} y_1^{\text{nom}} = u$. Thus, Definition 1 is equivalent to

$$\begin{aligned} y_1(0) &= y_1^{\text{nom}}(0), \text{ and} \\ \dot{y}_1 &= u. \end{aligned} \tag{3.2}$$

The following result characterizes the class of attacks that are undetectable through y_1.

Lemma 2 *(**Undetectability through GNSS only**) Consider a robot with dynamics* (2.3)*. The attack* (a_x, a_y) *is undetectable through* y_1 *if and only if*

$$a_y(0) = 0, \text{ and } \dot{a}_y = -a_x, \tag{3.3}$$

at all times $t \in \mathbb{R}_{\geq 0}$*.*

Proof. For the proof we use equivalent conditions (3.2). The first condition in (3.2) can equivalently be rewritten as $x^{\text{nom}}(0) + a_y(0) = x^{\text{nom}}(0)$, which proves the first condition in the lemma. To prove the second condition we use the definition of $\dot{y}_1$ in (2.3), and rewrite it as

$$\dot{y}_1 = \dot{x} + \dot{a}_y = u + a_x + \dot{a}_y.$$

The second condition in the lemma follows by equating the above expression with the second con-

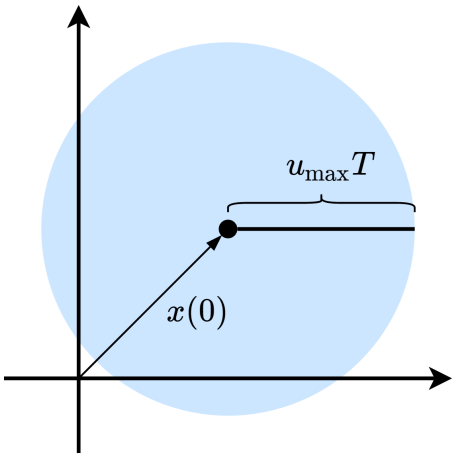


Figure 3.1: Region that can be reached by an attacked robot for a given initial position x_0. This is the area that is delimited by the circular region where the robot can be controlled using $\dot{x}(t) = u_{\max}$.

dition in (3.2). ■

Lemma 2 has some important implications. First, for an undetectable attack,the perturbation of y_1 at time $t+0$ must be zero. Second, for any attack input a_x to the dynamics, there exists a spoofing signal a_y that makes the attack undetectable independently of the control input. Consequently, the region the attacker can reach, for a given $u_{\max}$ and T, is a function of the attacked initial position $x(0)$ and is independent of the nominal control input. The relation between the region reachable by an attacked robot, its initial position $x(0)$, and the parameters $u_{\max}$ and T is geometrically illustrated in Fig. 3.1.

3.2 RSSI-aided attack detection

As discussed above, an attacker can easily evade detection when only the GNSS sensor is used. In this section we characterize the class of undetectable attacks when both GNSS and RSSI measurements are used.

Definition 3 *(**Undetectable attack through** y_1 **and** y_2**)** For the robot's dynamical model (2.3), an attack is undetectable through y_1 and y_2 if

$$\begin{aligned} y_1 &= y_1^{\text{nom}}, \text{ and} \\ y_2 &= y_2^{\text{nom}}, \end{aligned} \tag{3.4}$$

at all times $t \in \mathbb{R}_{\geq 0}$, where ${y_1}^{\text{nom}}$ and ${y_2}^{\text{nom}}$ are the outputs of the nominal model (2.2) with input u and initial position $x^{\text{nom}}(0)$. □

In other words, an attack is undetectable through y_1 and y_2 combined if (i) the attack is undetectable through y_1 only, and (ii) the output y_2 is consistent with its nominal counterpart. A straightforward implication of the second condition in Definition 3 is

$$\|x\| = \|x^{\text{nom}}\|, \tag{3.5}$$

for all $t \in \mathbb{R}_{\geq 0}$. Thus, any undetectable trajectory must feature the same relative distance to the RSSI tower as the nominal trajectory. To fully characterize the class of undetectable attacks through y_1 and y_2 we will make use of the following decomposition for $\dot{x}$ and $\dot{y}$:

$$\begin{aligned} \dot{x} &= v_{\parallel}(x)e_{\parallel}(x) + v_{\perp}(x)e_{\perp}(x), \\ \dot{y} &= v_{\parallel}(y)e_{\parallel}(y) + v_{\perp}(y)e_{\perp}(y), \end{aligned} \tag{3.6}$$

where for any differentiable function $r : \mathbb{R} \to \mathbb{R}^2$ and any function $p : \mathbb{R} \to \mathbb{R}^2$ satisfying $r^{\mathsf{T}}p = 0$ at all times, the maps $v_{\parallel} : \mathbb{R}^2 \to \mathbb{R}^2$, $e_{\parallel} : \mathbb{R}^2 \to \mathbb{R}^2$, $v_{\perp} : \mathbb{R}^2 \to \mathbb{R}^2$ and $e_{\perp} : \mathbb{R}^2 \to \mathbb{R}^2$ are defined as

$$\begin{aligned} v_{\parallel}(r) &= \frac{\dot{r}^{\mathsf{T}}r}{\|r\|}, \qquad e_{\parallel}(r) = \frac{r}{\|r\|}, \\ v_{\perp}(r) &= \frac{\dot{r}^{\mathsf{T}}p}{\|p\|}, \qquad e_{\perp}(r) = \frac{p}{\|p\|}, \end{aligned}$$

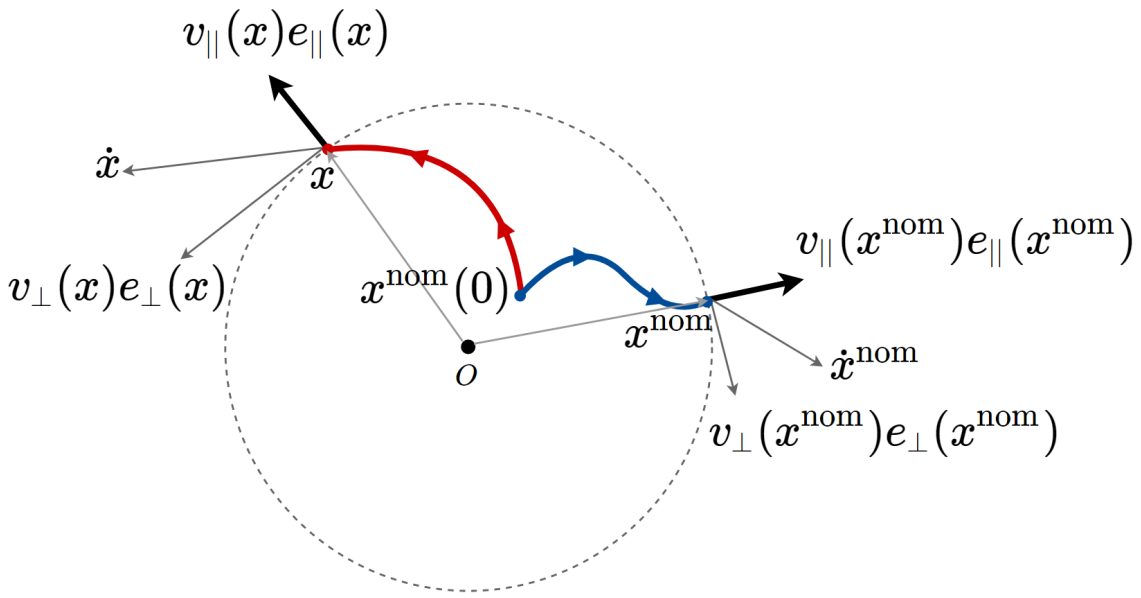


Figure 3.2: An attack is not detectable if the redial velocity of the true trajectory $v_{\parallel}(x)$ is the same as the nominal counterpart $v_{\parallel}(x^{\text{nom}})$. As showed here the attacker trajectory is in red and nominal trajectory in blue, with both of the initial condition at $x^{\text{nom}}(0)$, the attack input is undetectable if and only if the magnitude of the two balded velocities, that is $v_{\parallel}(x)$ and $v_{\parallel}(x^{\text{nom}})$, remains the same at all time.

In other words, $v_{\parallel}(r)$ and $v_{\perp}(r)$ represent radial and tangential components of the function r, respectively, and $e_{\parallel}(r)$ and $e_{\perp}(r)$ are the unit vectors parallel and normal to the function, respectively. [1] This decomposition will be applied to the trajectory of the robot. We next use the decomposition (3.6) to characterize the undetectibility through y_1 and y_2.

Lemma 4 *(**Undetectability through** y_1 **and** y_2**)** *For the robot's dynamical model* (2.3)*, the attack* (a_x, a_y) *is undetectable through* y_1 *and* y_2 *if and only if the following conditions hold at all times* $t \in \mathbb{R}_{\geq 0}$*:*

$$a_y(0) = 0,$$

$$\dot{a}_y = -a_x, \text{ and}$$

$$v_{\parallel}(x) = v_{\parallel}(x^{\text{nom}}).$$

[1] For sake of notation we will choose orthogonal vectors and pointing in a counterclockwise direction.

Proof. According to definition 3, an attack is undetectable through y_1, y_2 and u combined if it is undetectable from y_1 only. This yields the first and second condition. The second condition in definition 3 can be rewritten as the two conditions

$$y_2(0) = y_2^{\text{nom}}(0), \tag{3.7}$$

$$\dot{y}_2 = \dot{y}_2^{\text{nom}}. \tag{3.8}$$

Now, (3.7) is a straightforward consequence of the third condition in the Lemma. To prove the fourth condition we can rewrite (3.8) as

$$2\dot{x}^{\mathsf{T}}x = 2(\dot{x}^{\text{nom}})^{\mathsf{T}}(x^{\text{nom}})$$

where we used $y_2 = x^{\mathsf{T}}x$ and $y_2^{\text{nom}} = (x^{\text{nom}})^{\mathsf{T}}(x^{\text{nom}})$. We can now use 3.5, and rewrite

$$\frac{\dot{x}^{\mathsf{T}}x}{\|x\|} = \frac{(\dot{x}^{\text{nom}})^{\mathsf{T}}(x^{\text{nom}})}{\|x^{\text{nom}}\|},$$

or, equivalently $v_{\parallel}(x) = v_{\parallel}(x^{\text{nom}})$. ■

From Lemma 4 we concluded that (i) undetectability through y_1 is only necessary for undetectability through y_1 and y_2, and (ii) the radial component of the velocity of the nominal trajectory and of the attacked trajectory must be equal at all times. Fig. 3.2 geometrically illustrates the conditions in Lemma 4. It is now possible to rewrite the optimization problem (2.4) by incorporating

the undetectability conditions derived in Lemma 2 and Lemma 4 as follows:

$$\begin{aligned} \max_{a_x, a_y} \quad \min_{u} \quad & \|x^{\mathrm{nom}}(T) - x(T)\| \\ \text{subject to} \quad & a_y(0) = 0, \\ & \dot{a}_y = -a_x, \\ & v_{\parallel}(x) = v_{\parallel}(x^{\mathrm{nom}}). \end{aligned} \tag{3.9}$$

Chapter 4

Undetectable trajectories

In this section we study and solve the optimization problem (3.9). To this aim, we exploit the undetectibility conditions (3.9) and rewrite the cost function in a more convenient way. Referring to Fig 4.1, the undetectibility condition (3.5) implies that x^{nom} and x must lie on the same circle at all times. Thus, the vector $x(t)$ can be written as a function of $x^{\text{nom}}(t)$ and the angle angle θ_t

Lemma 5 ***(Angular description of position deviation)***

Let the attack (a_x, a_y) be undetectable from y_1, y_2 and u. Then, the cost function in (3.9) *can be rewrite as follows,*

$$\|x - x^{\text{nom}}\| = 2\|x^{\text{nom}}\| \left|\sin(\frac{\theta_t}{2})\right|, \tag{4.1}$$

$$\textit{where} \qquad \theta_t = \int_0^t \frac{v_\perp(x(s)) - v_\perp(x^{\text{nom}}(s))}{\|x^{\text{nom}}(s)\|} ds. \tag{4.2}$$

Proof. According to (3.5) an attack is undetectable if and only if $\|x\|$ remains the same as the nominal counterpart $\|x^{\text{nom}}\|$ at all time, thus as showed on Fig.4.1 the distance $\|x - x^{\text{nom}}\|$ can be described as (4.1). The angle traveled by x could be described as the integral of the angular velocity $\frac{v_\perp(x)}{\|x\|}$, and the same equation is also valid for x^{nom}. Since $\|x\| = \|x^{\text{nom}}\|$ and $x(0) = x^{\text{nom}}(0)$, thus we can describe the angle difference between x and x^{nom} as (4.2). ■

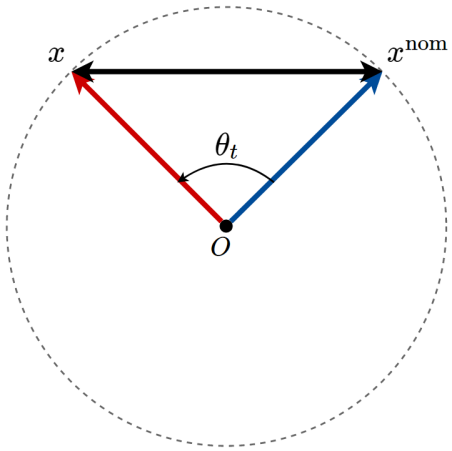


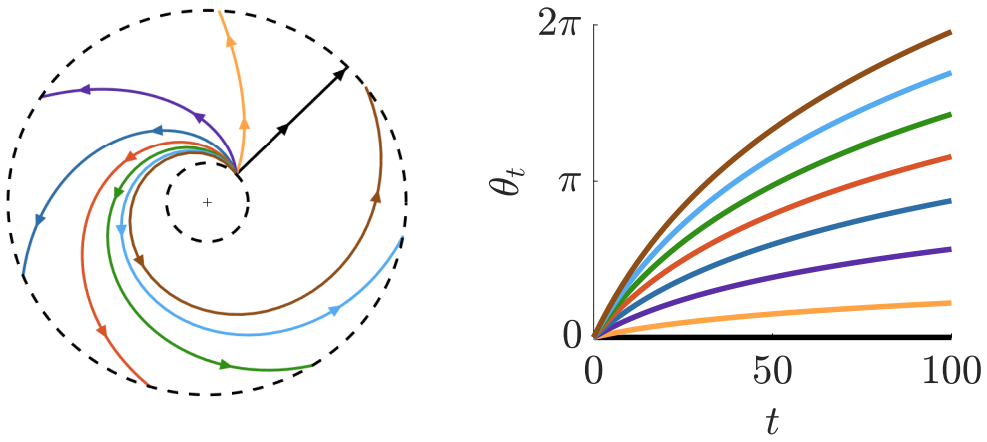
Figure 4.1: Deviation between $x(t)$ and $x^{\text{nom}}(t)$ is a function of the angle θ_t between the two vectors as showed in (4.1).

Lemma 5 shows that the attacker needs to maximize $|\sin(\frac{\theta_t}{2})|$ in order to maximize the deviation between the nominal and actual positions while remaining undetected. Because the speed of the robot is bounded, the maximum deviation introduced by an undetectable attack is limited and can be quantified as follows.

Theorem 6 ***(Upper bound on position deviation)***

Let $\theta_T^{\text{nom}} = atan2(x^{\text{nom}}(T)) - atan2(x^{\text{nom}}(t))$*, and attack* (a_x, a_y) *be undetectable from* y_1 *and* y_2*. Then,*

$$\|x(T) - x^{\text{nom}}(T)\| = 2\|x^{\text{nom}}(T)\| \left|\sin(\frac{\theta_T}{2})\right| \leq 2\|x^{\text{nom}}(T)\| \left|\sin(\frac{\theta_T^*}{2})\right|. \tag{4.3}$$



(a) (b)

Figure 4.2: The maximum angle traveled by the robot θ_t is strictly related to the radial speed $v_{\parallel}(x^{\text{nom}})$ chosen by the defender

where

$$\theta_T^* = min\left(\left|\int_0^T \frac{d\sqrt{u_{max}^2 - v_{\parallel}(x^{\text{nom}}(s))^2} - v_{\perp}(x^{\text{nom}}(s))}{\|x^{\text{nom}}(s)\|} ds\right|, \pi\right),$$

and

$$d = \begin{cases} -1 & \text{if} \quad 0 \leq \theta_T^{\text{nom}} \leq \pi \\ 1 & \text{otherwise} \end{cases} \tag{4.4}$$

Proof. According to (4.1), the deviation will be larger as $|\theta_t|$ gets larger until $|\theta_t|$ reaches π where the maximum deviation is achieved. According to (4.2), since $\|x^{\text{nom}}\|$ is positive for all times, maximizing $|\theta_t|$ is the same as maximizing $v_{\perp}(x)$ and ensuring its sign opposite from θ_T^{nom}. Since an attacker can utilize maximum speed until reaching π deviation to θ_T^{nom} and then remain zero in $v_{\perp}(x)$ for the remaining time to achieve maximum deviation thus concludes the proof. ■

Theorem 6 has some important consequences: the maximum instantaneous deviation from

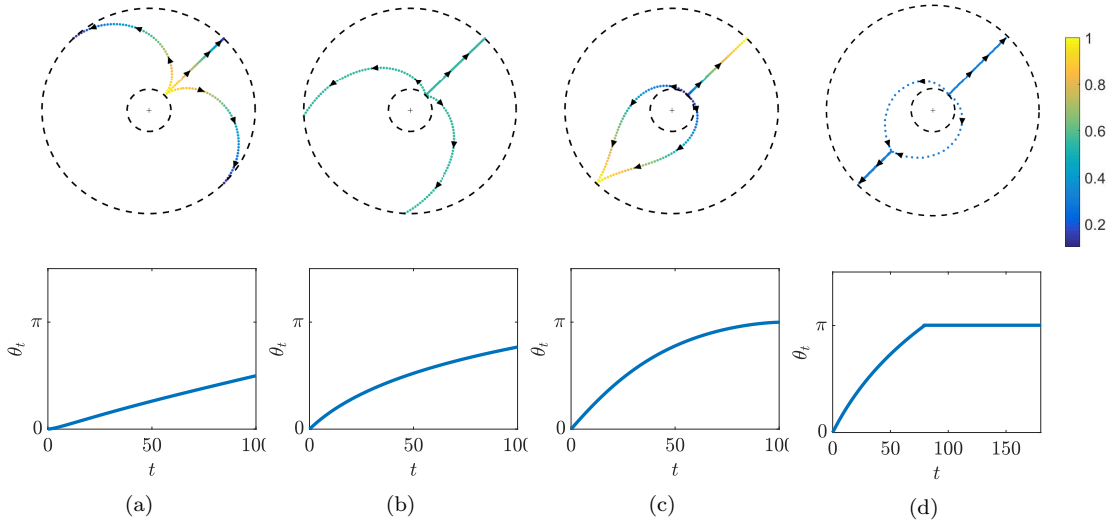


Figure 4.3: Undetectable trajectories for different choices of $v_{\parallel}(x^{\text{nom}})$, when $v_{\perp}(x)$ is chosen as in Algorithm (1) and $v_{\perp}(x^{\text{nom}}) = 0$. (a) $v_{\parallel}(x^{\text{nom}}) = (0.1 + 0.01t)u_{\max}$. (b) $v_{\parallel}(x^{\text{nom}}) = 0.55u_{\max}$. (c) $v_{\parallel}(x^{\text{nom}}) = (1 - 0.01t)u_{\max}$. (d) $v_{\parallel}(x^{\text{nom}}) = 0.3u_{\max}$. Notice that a longer simulation time is required to reach an equivalent radial distance because of a lower radial speed is chose than in Fig. 4.3(b).

the nominal trajectory is obtained when the tangential component of the velocity is chosen to maximize the speed of the robot. Moreover, when the final position at time T of the nominal trajectory is known to the attacker, it is possible to design the attack input so that the final deviation $\|x(T) - x^{\text{nom}}(T)\|$ is maximized. Algorithm 1 proposes a solution to the described problem, and the simulation result is depicted as Fig.4.3 for different choices of u.

Following the idea presented in Algorithm 1, the attacker can change the target location in Algorithm 1 to go through different position on the plane, one can identify the planar region where an attacked robot can be steered by an attacker, without being detected. These reachable regions are depicted in Fig. 4.4.

It is worth noting that, as testified by (4.4), the maximum angular deviation θ_t is related to $v_{\parallel}(x^{\text{nom}})$ and therefore the deviation is strictly related to the radial component of the velocity of the nominal trajectory $v_{\parallel}(x^{\text{nom}})$. Indeed, the largest $v_{\parallel}(x^{\text{nom}})$, the more constrained $v_{\perp}(x)$ is, according to the assumption on maximum velocity of the robot. Fig. 4.3 illustrates the effects of

Algorithm 1: Maximize $\|x(T) - x^{\text{nom}}(T)\|$

Data: u,x,$u_{\max}$,$x^{\text{nom}}(0)$,$x^{\text{nom}}(T)$
Result: a_x,a_y
integrate control input u to get position x^{nom};
$a_y = x^{\text{nom}} - x$;
$\theta_T^{\text{nom}} = \text{atan2}(x^{\text{nom}}(T))$;
$v_{\parallel}(x^{\text{nom}}) = \frac{u^{\mathsf{T}} x^{\text{nom}}}{\|x^{\text{nom}}\|}$;
if $\frac{x}{\|x\|} = \frac{-x^{\text{nom}}(T)}{\|x^{\text{nom}}(T)\|}$ **then**
  $v_{\perp}(x) = 0$;
else
  $v_{\perp}(x) = -\text{sign}(\theta_T^{\text{nom}})\sqrt{u_{\max}^2 - v_{\parallel}(y)^2}$;
calculate $e_{\perp}(x)$;
calculate $e_{\parallel}(x)$;
$\dot{x} = v_{\parallel}(x^{\text{nom}})e_{\parallel}(x) + v_{\perp}(x)e_{\perp}(x)$;
$a_x = \dot{x} - u$;
return

different choices for the function $v_{\parallel}(x^{\text{nom}})$.

4.1 Special case: Spoofing attack only

We now consider a class of attacks where the attacker can compromise the GNSS and relocate the initial position. Yet we do not allow the attacker to modify the robot's control input. The robot's dynamics are.

$$\begin{aligned} \dot{x} &= u, \\ x(0) &= x^{\text{nom}}(0) + a_0, \\ y_1 &= x + a_y, \\ y_2 &= x^{\mathsf{T}} x, \end{aligned} \tag{4.5}$$

where $a_0 \in \mathbb{R}^2$ is the displacement introduced by the attacker at time $t = 0$.

The undetectability condition can be stated as follows

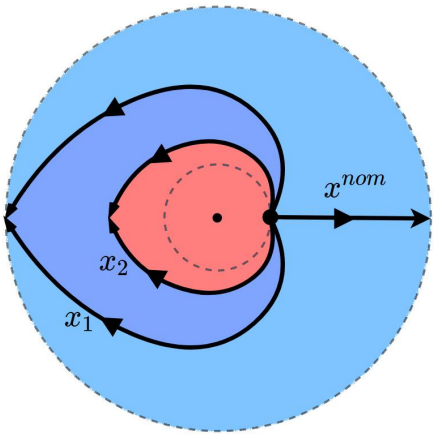


Figure 4.4: Reachable region for different choices of $v_{\parallel}(x^{\text{nom}})$ and nominal trajectory x^{nom}, as demonstrated on Fig. 4.3(b) and Fig.4.3(d), smaller $v_{\parallel}(x^{\text{nom}})$ will let the attacker to travel on trajectory x_2 instead of x_1, where x_2 has a larger reachable region as the dark blue and the light blue area compare to x_1 which has only the light blue area as the reachable region

Lemma 7 *(**Undetectability for spoofing only**) For the robot's dynamical model* (4.5)*, the attack* (a_y, a_0) *is undetectable through* y_1 *and* y_2 *if and only if the following terms hold at all times* $t \in \mathbb{R}_{\geq 0}$

$$\begin{aligned} a_y &= -a_0, \\ \|x(0)\| &= \|x^{\text{nom}}(0)\|, \\ u^{\mathsf{T}} a_y &= 0. \end{aligned} \tag{4.6}$$

Proof. Based on the proof of Lemma 4, the first condition in Definition 3 can be equivalent to

$$\begin{aligned} x^{\text{nom}} + a_0 + a_y(0) &= x^{\text{nom}}, \text{ and} \\ u + \dot{a}_y &= u, \end{aligned} \tag{4.7}$$

where the first condition implies that for an undetectable attack the initial condition of a_y is equal to $-a_0$. And the second condition implies that $\dot{a}_y$ should remain zero for undetectability, combined with the first condition about the initial value of a_y, thus we acquire the first condition in (4.7). According to the proof of Lemma4, the second condition in Definition 3 is satisfied when (3.7) and

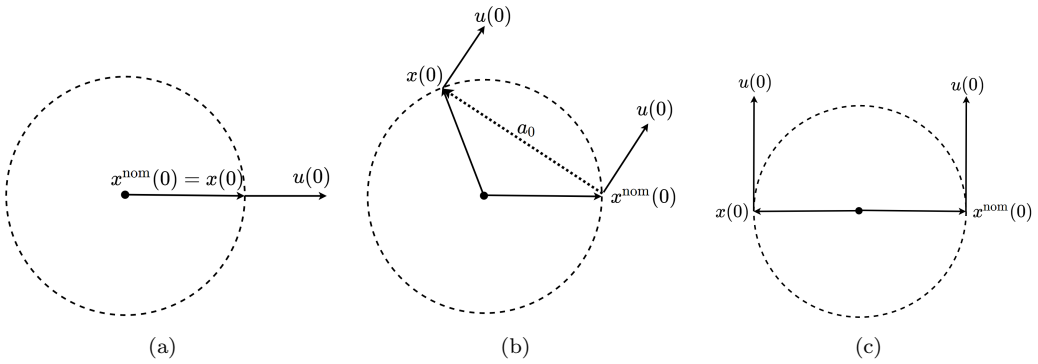


Figure 4.5: Final deviation an undetectable attack can introduce when $a_x = 0$, undetectable attack exists only when control input u remains on the same direction, and the final deviation depends solely on the direction of u, with maximum deviation $\|x(T) - x^{\text{nom}}(T)\| = 2\|x^{\text{nom}}(0)\|$ as (c), and minimum deviation $\|x(T) - x^{\text{nom}}(T)\| = 0$ as (a).

(3.8) are satisfied, which base on dynamic model (4.5) is equivalent to

$$x(0)^{\mathsf{T}} x(0) = x^{\text{nom}}(0)^{\mathsf{T}} x^{\text{nom}}(0), \text{ and}$$

$$2\dot{x}^{\mathsf{T}} x = 2(\dot{x}^{\text{nom}})^{\mathsf{T}} (x^{\text{nom}}),$$

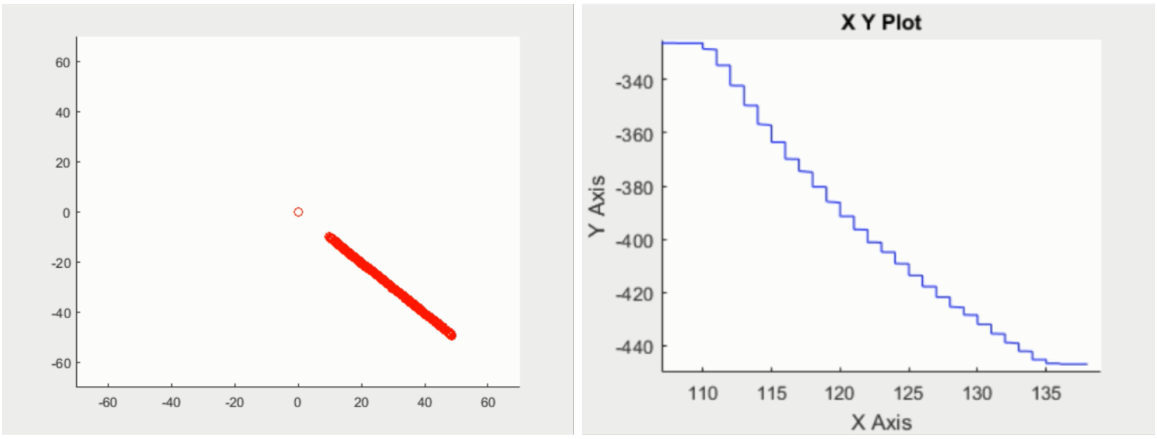
which conclude the proof. ■

Some comments about Lemma 7 are in order. The first condition in (4.7) indicates that a_y needs to be a constant and equal to $-a_0$ at all time to allow undetectibility. This implies that the final deviation $\|x(T) - x^{\text{nom}}(T)\|$ will be equal to the initial displacement $\|a_0\|$. Further, vector a_0 needs to satisfy the second condition in (4.7), that is, the new location $x(0)$ must have the same distance to the origin as $x^{\text{nom}}(0)$. Thus the maximum final deviation will be equal to $2\|x(0)\|$ as showed on Fig. 4.5(c). Finally, the attack input a_y must be orthogonal to the control input u at all times for undetectability. This is possible only if the control input u satisfies $u = g(t)u_0$, where $g : \mathbb{R} \to \mathbb{R}^2$ and $u_0 \in \mathbb{R}^2$ is a constant vector. Moreover, the maximum final deviation $2\|x(0)\|$ is achieved only when $u_0^{\mathsf{T}} x(0) = 0$. This discussion is illustrated in Fig.4.5.

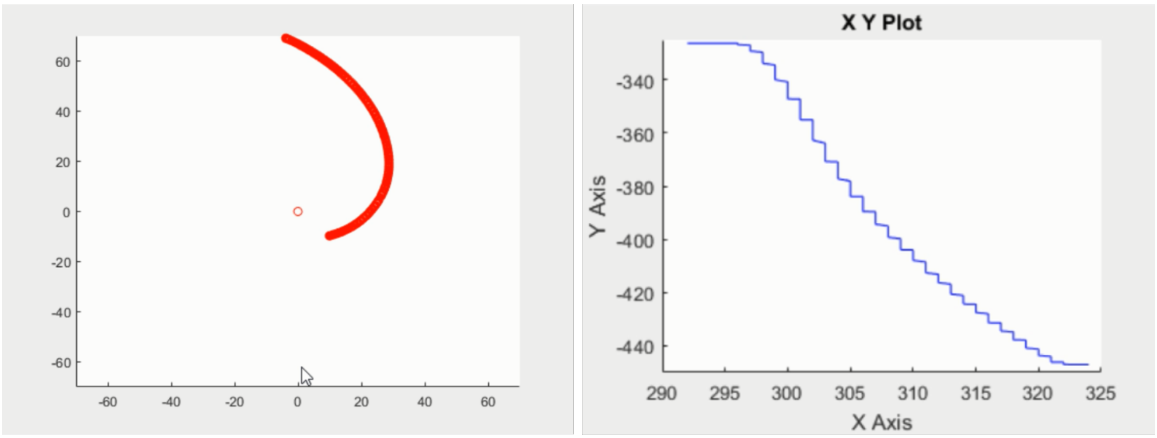
Chapter 5

Examples and experimental results

Experiment has been conducted in a simulated environment to testify the undetectability of the attacked trajectory presented in this paper. We produced two different trajectories, one is the nominal trajectory and the other one is the attacked trajectory produced by algorithm 1. A simulated environment and a simulated drone with physical engine is established through Gazebo simulator and the communication between the simulated drone and Matlab is established using Robot Operating System (ROS). Two trajectories have been converted into two sets of way points and sent to the simulated drone with the same frequency to simulate the result of the nominal trajectory and the attacked one. The simulation result is as showed in Fig.5.1, where it is shown that the two different trajectories actually produce the same behavior (small deviations are due to model uncertainties and numerical errors) on the RSSI sensor which showed on the right side. This demonstrated the undetectability of the attacker signal produced by algorithm 1.



(a)



(b)

Figure 5.1: Two sets of results for different choices of trajectories, figure on the left show the trajectory of the robot while on the right side is the RSSI sensor reading respect to time. Trajectory in (a) is predesigned while trajectory in (b) is calculated through algorithm 1. As showed in (a) and (b), the RSSI readings are almost identical, which indicated that the attack is truly undetectable through RSSI sensor.

Chapter 6

Conclusions

We study a secure trajectory generation for autonomous UAVs subjects to attacks. With extra information from the RSSI sensor, we have determined the undetectability condition for this kind of attacks. We proposed the characteristic of the undetectable attacks and the trajectory produced by undetectable attacks. We also presented the mapping between the maximum deviation brought by the attacker and the nominal control input, which makes us possible to minimize the final deviation. Simulations has also been made to support the undetectability condition presented in this paper. At last, we introduce a special case where the attacker is only changing the position data, and proposed the solution for a secure trajectory in this situation.

Bibliography

[1] Jahshan Bhatti and T Humphreys. Hostile control of ships via false gps signals: Demonstration and detection. *Navigation*, 2016.

[2] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. Gnss spoofing detection in handheld receivers based on signal spatial correlation. In *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*, pages 479–487. IEEE, 2012.

[3] D A Divis. Scientists document possible drone jamming. *Inside Unmanned Systems*, page 14, 2015.

[4] Ding-Zhu Du and Panos M Pardalos. *Minimax and applications*, volume 4. Springer Science & Business Media, 2013.

[5] Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. 59(6):1454–1467, 2014.

[6] Xichen Jiang, Jiangmeng Zhang, Brian J Harding, Jonathan J Makela, Alejandro D Domı, et al. Spoofing gps receiver clock offset of phasor measurement units. *IEEE Transactions on Power Systems*, 28(3):3253–3262, 2013.

[7] Andrew J Kerns, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[8] Paul Y Montgomery, Todd E Humphreys, and Brent M Ledvina. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer. In *Proceedings of the ION International Technical Meeting*, pages 124–130, 2009.

[9] F. Pasqualetti, F. Dörfler, and F. Bullo. Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems. 35(1):110–127, 2015.

[10] Fabio Pasqualetti, Florian Dorfler, and Francesco Bullo. Control-theoretic methods for cyber-physical security: Geometric principles for optimal cross-layer resilient control systems. *IEEE Control Systems*, 35(1):110–127, 2015.

[11] Mark L Psiaki and Todd E Humphreys. Gnss spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, 2016.

[12] Mark L Psiaki, Brady W O'Hanlon, Jahshan A Bhatti, Daniel P Shepard, and Todd E Humphreys. Gps spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, 49(4):2250–2267, 2013.

[13] Mark L Psiaki, Brady W O'hanlon, Steven P Powell, Jahshan A Bhatti, Kyle D Wesson, and Todd E Humphreys. Gnss spoofing detection using two-antenna differential carrier phase. 2014.

[14] David S Radin, Peter F Swaszek, KC Seals, et al. Gnss spoof detection based upon pseudoranges from multiple receivers. In *International technical meeting of the Institute of Navigation*, 2015.

[15] Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle, 8 2012.

[16] Peter F Swaszek, Scott A Pratz, Benjamin N Arocho, Kelly C Seals, and Richard J Hartnett. Gnss spoof detection using shipboard imu measurements. 2014.

[17] Kexiong (Curtis) Zeng, Yuanchao Shu, Shinan Liu, Yanzhi Dou, and Yaling Yang. A Practical GPS Location Spoofing Attack in Road Navigation Scenario. In *ACM HotMobile*, 2017.

[18] Qiang Zou, Sunan Huang, Feng Lin, and Ming Cong. Detection of gps spoofing based on uav model estimation. In *Industrial Electronics Society, IECON 2016-42nd Annual Conference of the IEEE*, pages 6097–6102. IEEE, 2016.