Strategic Defense Against Deceptive Civilian GPS Spoofing of Unmanned Aerial Vehicles

Tao Zhang(✉) and Quanyan Zhu

Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, Brooklyn, NY 11201, USA
{tz636,qz494}@nyu.edu

Abstract. The Global Positioning System (GPS) is commonly used in civilian Unmanned Aerial Vehicles (UAVs) to provide geolocation and time information for navigation. However, GPS is vulnerable to many intentional threats such as the GPS signal spoofing, where an attacker can deceive a GPS receiver by broadcasting incorrect GPS signals. Defense against such attacks is critical to ensure the reliability and security of UAVs. In this work, we propose a signaling game framework in which the GPS receiver can strategically infer the true location when the attacker attempts to mislead it with a fraudulent and purposefully crafted signal. We characterize the necessary and sufficient conditions of perfect Bayesian equilibrium (PBE) of the game and observe that the equilibrium has a PLASH structure, i.e., pooling in low types and separating in high types. This structure enables the development of a game-theoretic security mechanism to defend against the civil GPS signal spoofing for civilian UAVs. Our results show that in the separating part of the PLASH PBE, the civilian UAV can infer its true position under the spoofing attack while in the pooling portion of the PLASH PBE, the corresponding equilibrium strategy allows the civilian UAV to rationally decide the position that minimizes the deviation from its true position. Numerical experiments are used to corroborate our results and observations.

Keywords: Game theory · Signaling game · GPS spoofing · Cybersecurity

1 Introduction

The unmanned aerial vehicle (UAV) is the next generation of aerial platform in various domains. Apart from the military applications, the civilian UAVs are anticipated to play an essential role in commercial applications including business to business (B2B) and business to consumer (B2C) purposes, especially for the delivery systems with logistics services and supply chain support. Prime Air, for example, is a delivery system, currently in development by Amazon, using fully autonomous GPS-guided UAVs to provide rapid parcel delivery (Fig. 1 shows an

S. Rass et al. (Eds.): GameSec 2017, LNCS 10575, pp. 213–233, 2017.
DOI: 10.1007/978-3-319-68711-7_12

Fig. 1. Illustration of a GPS-guided UAV conducts delivery mission between two locations. The attacker in the lower-right corner indicates that the mission is under threat.

example), showing a great potential to improve the efficiency and safety of the overall supply chain system [1].

Emerging applications that primarily depend on autonomous UAV requires a dependable and trustworthy navigation system. Global Positioning System (GPS) is the most common and popular navigation sensor used in the navigation system of UAVs to achieve high-performance flights. In military applications, GPS signals are encrypted to prevent unauthorized use and imitation. However, the current civilian GPS signal is transparent and easily accessible worldwide, which makes the civilian GPS-guided infrastructures vulnerable to different types of GPS spoofing attacks.

It has been shown by researchers in recent literature [22] that civilian UAVs can be easily spoofed. For example, in 2002 researchers from Los Alamos National Laboratory have successfully performed an simplistic GPS spoofing attack [24]. In 2012, Humphreys et al. have shown the spoofing of a UAV by sending the false positional data to its GPS receiver and thus misled the UAV to crash into the sand [7].

Therefore, it is imperative to develop an appropriate defense mechanism to make the civilian GPS dependable for UAVs. Cryptography is one prospective approach. However, the encryption of civilian GPS signals requires high level of secrecy, expense, and scalability. It will create a significant computational and communication overhead when widely used, which can be impractical and limit the scope of its applications. Moreover, the cryptographic keys can be leaked to or stolen by a stealthy adversary who launches an advanced persistent threat (APT) attacks that exploit zero-day exploits and human vulnerabilities. Therefore, an alternative protection mechanism is needed to build a trust mechanism that allows UAV to mitigate the risk of UAV by anticipating the spoof attacks.

To this end, we propose a two-player game-theoretic framework to capture the strategic behaviors of the spoofer and the GPS receiver in which the spoofer aims to inject a counterfeit signal to the UAV to mislead its command and control while the receiver aims to decide whether to estimate the true signal upon receiving the signal. In the two-player game, the receiver does not know the true

signal while the adversary knows the correct signal and is able to generate a counterfeit one. To capture the information asymmetry, we use a continuous-kernel signaling game model in which the receiver does not completely know its current location but can form a belief given the received GPS signal. The location of the UAV can be taken as the private information of the sender and hence it is taken as the type of the sender, which is a continuous variable unknown to the receiver. This treatment aligns with the literature in the games of incomplete information. The objective of the receiver is to estimate the correct location based on the received signal and the risk of trusting it. The spoofer, on the other hand, designs a deceptive scheme to manipulate the UAV to move toward an adversarial direction. The spoofer can act stealthily by carefully crafting a signal that takes into account the response of the receiver. The equilibrium analysis of the two-stage game with information asymmetry provides a fundamental understanding of the risk of a UAV under spoofing attacks and yields a strategic trust mechanism that can defend against a rational attacker.

Our results show that the perfect Bayesian equilibrium (PBE) of the game is pooling in low types and separating in high types (PLASH), known as a PLASH PBE. In the separating part of the PLASH PBE, the UAV can strategically infer its true position under the spoofing attack; while in the pooling part of the PLASH PBE, the civilian UAV could not infer its true position exactly, but the corresponding equilibrium strategy enables the civilian UAV to rationally decide the position that minimizes the deviation from its true position. When the deception cost is small enough relative to the level of deviation of aimed by the spoofer, the PLASH PBE becomes a fully pooling PBE (PPBE); while the deception cost is sufficiently large compared to the level of deviation, the PLASH PBE becomes a fully separating PBE (SPBE). These two PBEs coincide with the intuition that the spoofer prefers pooling (resp. separating) strategy when the deception cost is low (resp. high). The main contributions of this paper are summarized as follows:

(i) We model the deceptive spoofing using a continuous-kernel signal game framework and capture the information asymmetry between the sender and the receiver through the private type.
(ii) We develop a risk-based defense mechanism in which the GPS receiver can strategically trust the received messages by taking into account the spoofing threat that a civilian UAV is subject to.
(iii) We characterize the PLASH perfect Bayesian equilibrium (PBE) of the signaling game between the GPS spoofer and the UAV, which has implications in developing defense mechanisms.

1.1 Related Work

There have been a number of approaches based on cryptography proposed to defend against GPS spoofing attacks. For example, spreading code encryption (SCE) [6,18] is currently the only cryptographic technique in widespread use, exclusively in military applications [21]. Techniques based on SCE have provided

a very high degree of resistance to the GPS spoofing attacks; however, the high level of secrecy, expense, and scalability of such approach makes it impractical for the civilian GPS [21]. Kuhn et al. [12] have used short sequences of spread spectrum security codes to modify the GPS signal to suit the civilian application; however, the modification in the standard signal protocols makes it impractical to be widely use [21]. Other cryptographic techniques include the navigation message authentication (NMA) [18,25,27], which allows both the uncertified and certified GPS receivers to read navigation messages with different levels of security; however, it has shown that NMA can be fully circumvented by powerful spoofers [6,16].

There has also been a significant amount of work on GPS spoofing defense techniques based on signaling processing [5]. For example, receiver autonomous integrity monitoring (RAIM) is the most widely used approach to detecting GNSS spoofing attacks [8,13]; RAIM is successful in any spoofing attacks that confined to one or two aberrant satellites, but fails when the attacks are confined to the entire constellation [21]. Another line of anti-spoofing work lies in the correlation with other GNSS sources. For example, the external sources of position and timing information such as inertial measurement unit (IMU) is one of the possible sources for the verification of the GPS position data [8,13]. These techniques can accumulate errors due to the inaccuracy of external sources compared to the GPS signal, thereby causing a quick drift from the accurate information. There are also anti-spoofing techniques using machine learning. For example, Wang et al. [23] have developed a machine learning classifier to detect time synchronization attack in cyber-physical systems.

Game theory has been widely applied in the intrusion detection systems [31], and the cyber security systems in various fields, including wireless networks [10,20], mobile networks [19], and control systems [17,29,30]. Signaling game has attracted attention in the field of cyber security [2,3,28]. Xu et al. [28], for example, have proposed an impact-aware defense mechanism using a cyber-physical signaling game. Casey et al. [2] provided a game-theoretical model to simultaneously study systems properties and human incentives.

In this work, we use the signaling game to capture the strategic interactions between the sender and the receiver. The GPS receiver does not have complete location information and the spoofer aims to send signals to mislead the UAV to another location. The game-theoretic defense provides an algorithmic solution that can be implemented on the embedded system in the UAV against GPS spoofings.

1.2 Organization

This paper is organized as follows. Section 2 presents the problem statement and develops a signaling game model. In Sect. 3, we analyze signaling game, define the PLASH PBE, and provide the necessary and sufficient conditions of the equilibrium. The numerical results are shown in Sect. 4. Finally, Sect. 5 concludes the paper.

2 Problem Statement

In this section, we formulate the game-theoretic model for UAV spoofing. First, we describe the dynamic state-space control model of the UAV and show that the UAV can be manipulated by controlling the source of the position information. Then, we describe the GPS signal spoofing attack model. Finally, we develop a signaling game model for the strategic defence mechanism.

2.1 State-Space Model of UAV

Consider an autonomous UAV that conducts a delivery mission from the origin to the destination as shown in Fig. 1. Suppose that the navigation of the UAV is fully supported by the GPS, and there is no other infrastructure such as radar that can provide navigation information. For each specific mission, the UAV flies along a prescribed flight path. Without loss of generality, we assume that the UAV flies at the same altitude; thus we focus on the 2-dimensional (2-D) navigation model with longitude and latitude.

Let $t = [t_x, t_y]$, $v = [v_x, v_y]$ and $\lambda = [\lambda_x, \lambda_y]$ be position, velocity and acceleration of the UAV, respectively, where J_x and J_y are the x and y components of $J \in \{t, v, \lambda\}$. Note that we use t to denote the position, which is referred as the *type* in the signaling game or the incomplete information of the game. The linear state-space model for the UAV plant is described as:

$$\dot{\chi}_z = \Lambda \chi_z + B\lambda_z,$$

where $\dot{\chi}_z = \begin{bmatrix} v_z \\ \lambda_z \end{bmatrix}$, $\chi_z = \begin{bmatrix} t_z \\ v_z \end{bmatrix}$, for $z \in \{x, y\}$, $\Lambda = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Thus, the state χ is driven by an acceleration λ, which is the control input. The control objective of the UAV is to track a prescribed flight path. Let $\tilde{t} = [\tilde{t}_x, \tilde{t}_y]$, $\tilde{v} = [\tilde{v}_x, \tilde{v}_y]$, and $\tilde{\lambda} = [\tilde{\lambda}_x, \tilde{\lambda}_y]$ be the prescribed reference position, velocity, and acceleration, respectively. Similarly, the double integrator dynamics of the prescribed reference model is $\dot{\tilde{\chi}}_z = \Lambda \tilde{\chi}_z + B\tilde{\lambda}_z$, where $\dot{\tilde{\chi}}_z = \begin{bmatrix} \tilde{v}_z \\ \tilde{\lambda}_z \end{bmatrix}$, $\tilde{\chi}_z = \begin{bmatrix} \tilde{t}_z \\ \tilde{v}_z \end{bmatrix}$, for $z \in \{x, y\}$. We model the controller of the UAV by a Proportional-Derivative (PD) compensator $\lambda_z = -K(\chi_z - \tilde{\chi}_z)$, where $K = [K_p, K_d]$ is the gain matrix with K_p, $K_d > 0$ such that the closed-loop control system is stable. Thus, the continuous-time linear state space model of the UAV can be written as:

$$\begin{bmatrix} \dot{\chi}_z \\ \dot{\tilde{\chi}}_z \end{bmatrix} = \begin{bmatrix} \Lambda - BK & BK \\ 0 & \Lambda \end{bmatrix} \begin{bmatrix} \chi_z \\ \tilde{x}_z \end{bmatrix} + \begin{bmatrix} 0 \\ B \end{bmatrix} \tilde{\lambda}_z. \tag{1}$$

We consider the case when GPS is the only source of navigation information. Suppose the UAV receives a GPS signal indicating a current position $t = (t_x, t_y)$ that shows a deviation of the UAV from the prescribed flight path. The controller adjusts the velocity v and the acceleration λ according to the state space model (1) as: $v_z = (\Lambda + BK)t_z + BK\tilde{t}_z$, and $\lambda = (\Lambda - BK)v_z + BK\tilde{v}_z$, for $z \in \{x, y\}$.

As shown in Sect. 2.2, a GPS spoofer aims to mislead the UAV to a wrong destination via creating a reset flight path by GPS signaling spoofing. The GPS spoofer starts a spoofing attack by sending a fake GPS signal indicating a wrong position $t' = (t'_x, t'_y)$ that shows a fake deviation. The reset flight path is determined based on the first spoofing signal. In this paper, we only consider that once the reset flight path is determined, it is fixed during the entire delivery mission. If the UAV is naive, its controller completely accept $t' = (t'_x, t'_y)$. The corresponding v'_z and λ'_z are then obtained; the GPS spoofer continues spoofing the GPS signal based on the first spoofed signal to lead the UAV to fly on the reset flight path towarding the wrong destination while making the controller believe it is the original prescribed flight path. We model the communication between the GPS spoofer and the UAV by a signaling game, and show that the strategic acceptance of $t' = (t'_x, t'_y)$ will significantly reduce or completely avoid the damage that might be caused by the spoofing attack.

2.2 GPS Signal Spoofing

In this paper, we consider a GPS signal spoofer located from a distance as shown in Fig. 2. At time τ during one mission, the spoofer starts to launch an spoofing attack. The spoofer is capable of capturing the authentic navigation message for the UAV from all visible GPS satellites and sends the counterfeit navigation message to the UAV as shown in Fig. 2. The navigation message from GPS satellites does not directly reveal the 2D position; instead, the message contains the time and the orbital information of the GPS satellites for computing the 2D position by the GPS receiver of the UAV via 2D trilateration. The spoofer aims to make the GPS receiver of the UAV report the current location as the simulated position $t' = [t'_x, t'_y]$ while the true position is $t = [t_x, t_y]$.

Starting from time τ, the spoofer continuously sends the UAV the counterfeit navigation messages such that the UAV would be deceived to fly along the reset flight path as shown in Fig. 3. The deviation between the true path and the reset path depends on the simulated position chosen by the adversary at time τ.

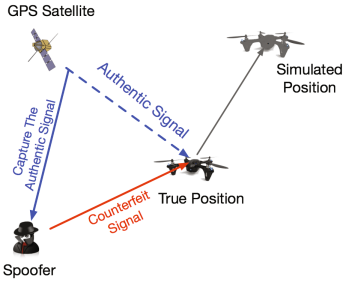


Fig. 2. Illustration of a GPS spoofing attack targeting a GPS-guided UAV.

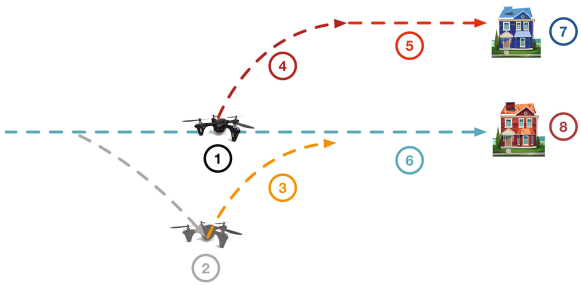


Fig. 3. Illustration of a complete GPS spoofing procedure. 1: True position of the UAV; 2: Counterfeit GPS signal makes the UAV think that its current position is deviated from the original path; 3: UAV control system adjusts the velocity and acceleration to return to the original path; 4: Actual move of the UAV; 5: Reset path; 6: Original path; 7: Wrong destination; 8: Correct destination.

2.3 Signaling Game

In this sub-section, we propose a game-theoretic cyber-security mechanism to capture the receiver's uncertainties on the received GPS signals, which can be either the true locations or the counterfeit ones. The analysis of the game yields a defense mechanism that allows the UAV to strategically minimize its risk and deal with the GPS signal spoofing without terminating the mission or resorting to other costly navigation infrastructures.

Signaling games are a class of the incomplete information games, in which one player has more information than the other. Specifically, the more informed player strategically decides to signal the private information called *type*, which is unknown to the opponent; the less informed player decides how to respond to the signal received [9,15]. In this paper, we model the communications between the GPS spoofer and the UAV by the signaling game and propose a game-theoretic approach to dealing with the GPS deception.

In our scenario, the role of GPS spoofer is the signal sender, denoted as S, and the role of GPS receiver of the UAV is the signal receiver, denoted as R. It is clear that the GPS spoofer is the more informed player and the UAV is the less informed counterpart. To capture the information asymmetry, we use the signaling game framework in which the navigation message (thus the position information) is only known to S. The position is viewed as type $t = [t_x, t_y] \in T$, where t_x and t_y are the latitude and longitude, respectively, in the form of decimal degrees, and $T = [t_x^m, t_x^M] \times [t_y^m, t_y^M]$ is the 2D location space with t_z^m and t_z^M are the minimum and maximum values of $z \in \{x, y\}$, respectively, which are determined based on the mission of the UAV. Note that the position or the type t takes a continuum of values in set T. Hence the game is a continuous-kernel signal game.

Let $m \in M$ be the navigation message sent by S. We denote $\Omega(m) = [\Omega_x(m), \Omega_y(m)] : M \to T$ as the 2D trilateration function to compute the 2D position. The output of the computation is $t' = [t'_x, t'_y] = \Omega(m)$ is the position

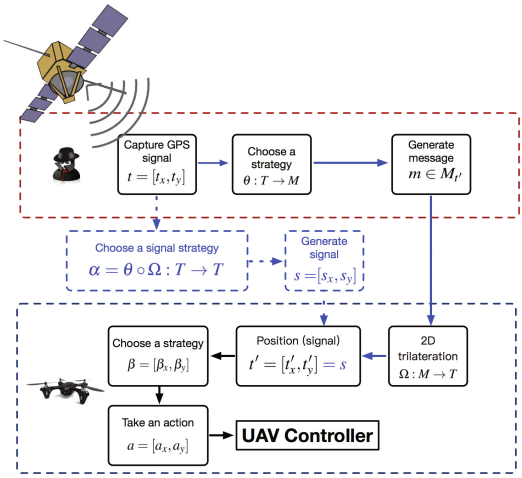


Fig. 4. Illustration of the signaling game model. The procedure represented by the solid blue line is equivalent to the procedure represented by the dashed blue line, i.e., the strategy θ generates a message m that tells R the position $t' = \Omega(m) = s$, where s is the signal generated by the signal strategy α.

claimed in message m. This process is illustrated in Fig. 4. The procedure of 2D trilateration is a pure mathematical computation and there is no strategic activity involved; thus, we can equivalently regard the action of generating message m as the action of generating a signal $s = [s_x, s_y] \in T$, i.e., choosing $s = t'$ means is equivalent to generating a message m that indicates $t' = [t'_x, t'_y] = \Omega(m)$.

The signaling game is played at τ, which is chosen by the spoofer, S. Since the choice of τ contains no strategic activity, we assume that τ is chosen according to a uniform distribution. Suppose a UAV, R, is flying at position $t = [t_x, t_y]$ at time τ. Here, we assume that t_x and t_y are drawn independently according to a uniform distribution over a credible interval to the receiver. After capturing the authentic navigation message for R from the GPS satellites, S generates a counterfeit message $m \in M$ leading to $t' = \Omega(m)$ or, equivalently, generates a signal $s = t'$. Then, S sends message m to R (equivalently sends signal s to R). Sender S tells the truth if $s = t$; otherwise, $s = t'$, for $t' \neq t$. Once s is observed by the receiver, R can strategically estimate the true location t by taking an action $a = [a_x, a_y] \in A$. It is natural to take $A = T$. The receiver then estimates the position of the UAV based on its belief and the received message. The navigation system of the UAV then adjusts the direction and speed according to the estimated position.

S has the cost function $C^S(a, t, s) = C^A(a, t) + k_1 C^D(t, s) : A \times T \times T \to \mathbb{R}$, where $C^A(a, t) : A \times T \to \mathbb{R}$ is the action-related cost, and $C^D(t, s) : T \times T \to \mathbb{R}$ is the deception cost, and $k_1 > 0$ is a constant scaling the intensity of the deception cost. The signal s (thus the message m) is only cost relevant to S in C^D. R has the cost function $C^R(a, t) : A \times T \to \mathbb{R}$. The goal of S is to choose a message to

minimize the cost function by anticipating the action of R, while the goal of R is to take an action to minimize the cost function based on the belief about the true type after observing the signal s.

Suppose that the true type is $t = [t_x, t_y]$. S chooses the message m claiming $t' = \Omega(m)$ based on the pure strategy, which is a measurable function $\theta(t) = [\theta_x(t_x), \theta_y(t_y)] : T \to M$. Equivalently, we define a measurable function $\alpha(t) = [\alpha_z(t_z), \alpha_z(t_z)] := T \to T$ as the signal strategy, based on which S chooses the signal s. The aforementioned relationship between s and m yields $\alpha(t) = t'$. The interpretation is that the signal strategy $\alpha(t)$ indicates the position S wants R to believe. R chooses its action $a = [a_x, a_y]$ using a pure strategy $\beta(\Omega(m)) : M \to T$. Based on the action, the strategically chosen position is sent to the UAV control system. The signaling game model is illustrated in Fig. 4.

Due to the fact that no GPS satellite is in a geostationary orbit, all the GPS satellites are moving all the time with respective to the ground; thus, there exists a message subspace M_t such that for each pair of different messages m_i, $m_j \in M_t$, we have $\Omega(m_i) = \Omega(m_j) = t$. Thus, every message $m \in M_t$ gives $\Omega(m) = t$. Clearly, $M = \cup_t M_t$ and $|M_t| = \infty$. Therefore, S can send an infinite number of messages for any strategy $\theta(t)$. Equivalently, we can claim that for every specific signal strategy $\alpha(t) = t'$, there is an infinite number of messages $m \in M_{t'}$ that S can choose.

3 Signaling Game Analysis

In this section, we define the cost functions of the sender S and the receiver R and analyze the solution of the signaling game based on the perfect Bayesian equilibrium (PBE).

3.1 Cost Function and Strategy

Let $C^A(a,t) = \| a - t - L \|^2$ and $C^D(t,m) = \| s - t \|^2 + \rho \| s \|^2$. The cost function of S is defined as:

$$\begin{aligned} C^S(a,t,s) &= C^A(a,t) + k_1 C^D(t,s) \\ &= \| a - t - L \|^2 + k_1 \big(\| s - t \|^2 + \rho \| s \|^2 \big) \\ &= \big[(a_x - t_x - l_x)^2 + k_1 \big((s_x - x)^2 + \rho s_x^2 \big) \big] \\ &\quad + \big[(a_y - t_y - l_y)^2 + k_1 \big((s_y - y)^2 + \rho s_y^2 \big) \big], \end{aligned} \tag{2}$$

where $L = (l_x, l_y)$ with $l_x, l_y > 0$ represents the malignity of S that models the conflict of interests between S and R. Therefore, the optimal action that minimizes the cost function of R leads to a strictly positive C^A, $\rho \| s \|^2$ with $\rho > 0$ models the other cost including message generation cost and transmission cost, and $k_1 > 0$ parameterizes the intensity of the cost C^D.

The cost function of R is defined as:

$$C^R(a,t) = k_2 \| a - t \|^2 = k_2 (a_x - t_x)^2 + k_2 (a_y - t_y)^2, \tag{3}$$

where $k_2 > 0$ is a constant. Let $C^{S,z} = (a_z - t_z - l_z)^2 + k_1\big((s_z - t_z)^2 + \rho s_z^2\big)$, for $z \in \{x, y\}$, and let $C^{R,x} = k_2(a_x - t_x)^2$and $C^{R,y} = k_2(a_y - t_y)^2$. Therefore, R chooses an action $a = (a_x, a_y)$ to solve the following problem

$$\min_{a \in A} C^R(a, t) := C^{R,x} + C^{R,y}. \tag{4}$$

S aims to choose a message m to solve the following problem

$$\min_{s \in T} C^S(a, t, s) := C^{S,x} + C^{S,y}. \tag{5}$$

Since t_x and t_y are generated independently. Thus, $\min_s C^{S,x}$ and $\min_s C^{S,y}$ are independent to each other and can be solved independently and so are $\min_{a_x} C^{R,x}$ and $\min_{a_y} C^{R,y}$. Therefore, $\min\limits_{a \in A} C^R(a, t) = \min\limits_{a_x} C^{R,x} + \min\limits_{a_y} C^{R,y}$, and $\min\limits_{s \in T} C^S(a, t, m) = \min\limits_{s_x} C^{S,x} + \min\limits_{s_y} C^{S,y}$. Then, (4) and (5) are equivalent to the following

$$\min_{a_z} C^{R,z}(a_z, t_z) = k_2(a_z - t_z)^2, \tag{6}$$

and $\min_{s_z} C^{S,z}(a_z, t_z, s_z) = C^{A,z}(a_z, t_z) + k_1 C^{D,z}(t_z, s_z)$, where $C^{A,z}(a_z, t_z) = (a_z - t_z - l_z)^2$ and $C^{D,z}(t_z, s_z) = (s_z - t_z)^2 + \rho s_z^2$, for $z \in \{x, y\}$ (hereafter). The function $C^{A,z}(\cdot, \cdot)$ and $C^{R,z}(\cdot, \cdot)$ are double differentiable at both arguments with $C_{12}^{A,z} < 0 < C_{11}^{A,z}$ and $C_{12}^{R,z} < 0 < C_{11}^{R,z}$; thus, $C^{A,z}$ and $C^{R,z}$ are convex in action a_z and super-modular in (a_z, t_z). Let $a_{R,z}^*(t_z) := \arg\min_{a_z} C^{R,z} = t_z$ and $a_{S,z}^*(t_z) := \arg\min_{a_z} C^{S,z} = t_z + l_z$, respectively, be the most preferred action (taken by R) for R and S with $\frac{da_{J,z}^*(t_z)}{dt_z} > 0$ for $J \in \{R, S\}$; and $a_{R,z}^*(t_z) < a_{S,z}^*(t_z)$ that coincides with the existence of conflict of interest. $C^{D,z}(\cdot, \cdot)$ is double differentiable for both arguments and $C_{12}^{D,z} < 0 < C_{11}^{D,z}$, which implies that given a type t_z, a larger s_z leads to a larger deception cost.

Based on the pure strategy $\alpha(t)$, S chooses a signal $s(t) = (s_x(t_x), s_y(t_y))$ and sends a corresponding message m. After observing the signal s_z, R updates its posterior belief about t_z, denoted as $g_z(t_z|s_z)$, using Bayes' rule. Using the pure strategy $\beta(s) = (\beta_x(s_x), \beta_y(s_y))$, R takes an action $a = (a_x, a_y)$. Let $p_z(t_z)$ be the prior belief of R about type t_z. Let $q^{S,z}(s_z)|t_z)$ and $q^{R,z}(a_z|s_z)$ be the probability distributions induced by $\alpha_z(t_z)$ and $\beta_z(s_z)$, respectively, which satisfy

$$\int_{s_z \in T} q^{S,z}(s_z|t_z)ds_z = 1, \quad \int_{a_z} q^{R,z}(a_z|s_z)da_z = 1.$$

Our solution concept to deal with the GPS signal deception in the signaling game model is the perfect Bayesian equilibrium, which is defined as follows.

Definition 1. *The strategy profile $(\alpha(t), \beta(s(t))$ with the belief $g_z(t_z|s(t))$ of the signaling game is a the perfect Bayesian equilibrium (PBE) if*

– *(Consistent belief) for all* s_z,

$$g_z(t_z|s_z) = \begin{cases} \frac{p_z(t_z)q^{S,z}(s_z|t_z)}{\int_{\hat{t}_z} p_z(\hat{t}_z)q^{S,z}(s_z|\hat{t}_z)d\hat{t}_z} & if \int_{\hat{t}_z} p_z(\hat{t}_z)q^{S,z}(s_z|\hat{t}_z)d\hat{t}_z > 0, \\ any\, distribution & otherwise. \end{cases}$$

– *(Sequential rationality)*

$$\alpha(t) \in \arg\min_{s \in T} C^S(\beta(s_z), t_z, s_z),$$

$$\beta_z(s_z) \in \arg\min_{a_z} \int_{t_z} g_z(t_z|s_z) C^{R,z}(a_z, t_z) dt_z.$$

Remark 1. There are two pure strategy equilibria. One is the separating PBE (SPBE), in which S chooses strategies for different types and the other one is the pooling PBE (PPBE), in which S uses the same strategy for different types.

3.2 Equilibrium Analysis

In this section, we characterize the equilibrium of the signaling game model. In our scenario of GPS signal deception, S aims to lead R to believe the type that is actually deviated from the true type. In this paper, we focus on the pure PBE strategy, and consider the case when $\frac{d\alpha_z(t_z)}{dt_z} \geq 0$.

First, we consider if there exists a SPBE. In any differentiable SPBE, the cost function $C^{S,z}$ and the signal strategy α_z have to satisfy the following necessary first-order condition for optimality based on the sequential rationality:

$$C_1^{S,z}(a^*_{R,z}(t_z), t_z, \alpha_z(t_z)) \frac{da^*_{R,z}(t_z)}{dt_z} + C_3^{S,z}(a^*_{R,z}(t_z), t_z, \alpha_z(t_z)) \frac{d\alpha_z(t_z)}{dt_z} = 0. \quad (7)$$

However, since $\frac{d\alpha_z(t_z)}{dt_z} \geq 0$ and $C_1^{S,z}(a^*_{R,z}(t_z), t_z, \alpha_z(t_z)) = 2(a^*_{R,z}(t_z) - t_z - l_z) = -2l_z$ is independent of $\alpha_z(t_z)$, there is no strategy such that $C_1^{S,z} \frac{da^*_{R,z}(t_z)}{dt_z} = 0$ when $C_3^{S,z} = 0$. Instead, we rearrange (7) and obtain the following differential equation:

$$\frac{d\alpha_z(t_z)}{dt_z} = -\frac{C_1^{S,z}(a^*_{R,z}(t_z), t_z, \alpha_z(t_z)) \frac{da^*_{R,z}(t_z)}{dt_z}}{C_3^{S,z}(a^*_{R,z}(t_z), t_z, \alpha_z(t_z))} = \frac{l_z}{k_1\big((1+\rho)\alpha_z(t_z) - t_z\big)},$$

to circumvent the case when $C_3^{S,z} = 0$. Let $\alpha^*(t) = \arg\min_s C^D$ be the signal strategy of choosing a signal $s^*(t) = (s^*_x(t_x), s^*_y(t_y))$ that minimizes the deception function. Then, $s^*_z(t_z) = \frac{t_z}{1+\rho} < t_z$ with $\frac{ds^*_z(t_z)}{dt_z} > 0$. We summarize the property of the strategy $\alpha_z(t_z)$ in any separating regime of the type space in the following lemma.

Lemma 1. *We say that in the type space* $(t_z^s, t_z^l) \subset [t_z^m, t_z^M]$*, the signaling game has a monotone SPBE with strategy* $\alpha_z(t_z)$ *if for each* $t_z \in (t_z^s, t_z^l)$*,* $\alpha_z(t_z) > s_z^*(t_z)$*, and*

$$\frac{d\alpha_z(t_z)}{dt_z} = \frac{l_z}{k_1\big((1+\rho)\alpha_z(t_z) - t_z\big)}. \tag{8}$$

Proof. See the proof in Appendix A.1.

Based on Lemma 1, we can conclude the following theorem.

Theorem 1. *There exists a unique SPBE portion* $[\hat{t}, t_z^M] \subseteq [t_z^m, t_z^M]$ *with initial condition* $\alpha_z^*(t_z^M) = t_z^M$*, where* $\alpha_z^*(t_z)$ *is the solution to (8).*

Proof. See the proof in Appendix A.2.

Since $\frac{d\alpha_z(t_z)}{dt_z} \geq 0$, $\frac{d\alpha_z^*(t_z)}{dt_z} > 0$, which means that in any separating region, the SPBE strategy of S is strictly increasing; thus, according to (8), we must have $\alpha_z^*(t_z) > \frac{t_z}{1+\rho} = s_z^*(t_z)$. Since S tells the truth if the type is t_z^M at the time τ (when S launches a spoofing attack), i.e., $\alpha_z(t_z^M) = t_z^M$, if t_z^M is in the separating region, $\alpha_z^*(t_z^M) = t_z^M$, which satisfies $\alpha_z^*(t_z^M) = t_z^M > \frac{t_z^M}{1+\rho}$. We summarize the existence of a full SPBE in the following corollary.

Corollary 1. *Let* $\alpha_z^*(t_z)$ *be the unique separating signal strategy given the initial condition* $\alpha_z^*(t_z^M) = t_z^M$*. There exists a single SPBE in the entire type space* $[t_z^m, t_z^M]$*, if* $\alpha_z^*(t_z^m) = t_z^m$*, which depends on the values of* l_z *and* k_1*.*

Proof. See the proof in Appendix A.2.

Corollary 1 shows that for certain values of l_z and k_1 there exists a unique single SPBE in the entire type space $[t_z^m, t_z^M]$. However, when there is no single SPBE existing, we are interested in a class of pooling strategy. For the separating region, Theorem 1 shows that there exists a continuous and increasing separating signal strategy function $\alpha_z^*(t_z)$ that solves (8) with initial condition $\alpha_z^*(t_z^M) = t_z^M$ for all $t_z \in [\hat{t}_z, t_z^M]$, where $\hat{t}_z \in (t_z^m, t_z^M)$ has a well-defined unique SPBE signal strategy $\alpha_z^*(\hat{t}_z) = t_z^m$. In this case, the maximal feasible interval of separating types is $[\hat{t}_z, t_z^M]$, while for all $t_z \in [t_z^m, \hat{t}_z]$, $\alpha_z(t_z) = t_z^m$. Before analyzing the pooling strategy, we first define the following equilibrium by introducing a boundary type $\bar{t}_z \in [\hat{t}_z, t_z^M]$.

Definition 2. *Let* $t^m = (t_x^m, t_y^m)$ *and* $t^* = (\alpha_x^*(t_x), \alpha_x^*(t_x))$*. A strategy* θ *and the corresponding signal strategy* α_z *is a PLASH (Pooling in Low types And Separating in High types) strategy if there exists a boundary type* $\bar{t}_z \in [\hat{t}_z, t_z^M]$ *such that:*

1. *(Pooling strategy)* $\theta(t) \in M_{t^m}$ *and* $\alpha_z(t_z) = t_z^m$ *for all* $t_z \in [t_z^m, \bar{t}_z)$*,*
2. *(Separating strategy)* $\theta(t) \in M_{t^*}$ *and* $\alpha_z(t_z) = \alpha_z^*(t_z)$ *for all* $t_z \in [\bar{t}_z, t_z^M]$*.*

In the pooling type interval, any type $t_z \in [t_z^m, \bar{t}_z]$ induces the equal deception cost since the signal strategy $\alpha_z(t_z) = t_z^m$ is chosen for all $t_z \in [t_z^m, \bar{t}_z]$. Therefore, we can regard the communication in $[t_z^m, \bar{t}_z]$ as a cheap talk [26]. However, as shown in Sect. 2.3, all the message $m \in M_{t_z^m}$ give the same value of signal $s_z = \Omega_z(m)$; then, it is possible for S to choose the same signal strategy $\alpha_z(t_z)$ but different message-related strategy θ so that R can choose distinct actions for different types in the pooling interval $[t_z^m, \bar{t}_z]$. Let $[t_z^{'}, t_z^{''}] \subseteq [t_z^m, \bar{t}_z]$. Suppose that based on the message m, R only knows that t_z lies in $[t_z^{'}, t_z^{''}]$ for each type $t_z \in [t_z^{'}, t_z^{''}]$. Let $\hat{a}_z(t_z^{'}, t_z^{''})$ be defined as follows:

$$\hat{a}_z(t_z^{'}, t_z^{''}) = \arg\max_{a_z} \int_{t_z^{'}}^{t_z^{''}} C^{R,z}(a_z, t_z) dt_z = \frac{t_z^{'} + t_z^{''}}{2}.$$

Thus, R takes the same action $\hat{a}_z(t_z^{'}, t_z^{''})$ for each type $t_z \in [t_z^{'}, t_z^{''}]$. Therefore, it is possible for R to choose $\hat{a}_z(t_z^{'}, t_z^{''})$ for different intervals $[t_z^{'}, t_z^{''}] \subseteq [t_z^m, \bar{t}_z]$.

Indeed, Crawford and Sobel [4] has shown that there exists a pooling-partition for $[t_z^m, \bar{t}_z]$. Specifically, for a boundary type $\bar{t}_z$, $[t_z^m, \bar{t}_z]$ can be partitioned into multiple pooling sub-intervals, which can be represented by a strictly increasing sequence $[t_z^0, t_z^1, ..., t_z^N]$, where $t_z^0 = t_z^m$ and $t_z^N = \bar{t}_z$. Thus, for all $n \in \{1, 2, ..., N-1\}$, the cost for S satisfies

$$C^{S,z}(\hat{a}_z(t_z^{n-1}, t_z^n), t_z^n, s_z(t_z^n)) = C^{S,z}(\hat{a}_z(t_z^n, t_z^{n+1}), t_z^n, s_z(t_z^n)). \tag{9}$$

Note that the deception cost is the same for every type $t_z \in [t_z^m, \bar{t}_z]$, (9) implies $C^{A,z}(\hat{a}_z(t_z^{n-1}, t_z^n), t_z^n) = C^{A,z}(\hat{a}_z(t_z^n, t_z^{n+1}), t_z^n)$. The interpretation is that, for each $t_z \in (t_z^{n-1}, t_z^n)$, S sends the same message $m_n \in M_{t_z^m}$, and R takes the same action $\hat{a}_z(t_z^{n-1}, t_z^n)$. S can send either m_n or m_{n+1} for the connecting type t_z^n. Note that $\alpha_z(t_z)$ is the same for all types $t_z \in [t_z^m, \bar{t}_z]$, but $m_n \neq m_j$ for $n \neq j$ and $m_j \in M_{t_z^m}$; thus S uses the same signal for all types $t_z \in [t_z^m, \bar{t}_z]$ but different messages for types in different pooling sub-intervals and all the messages are chosen from the set $M_{t_z^m}$.

The necessary and sufficient conditions for the existence of PLASH equilibrium are summarized in the following theorem.

Theorem 2 *(**Necessary condition**). In any PLASH equilibrium, there exists a boundary type $\bar{t}_z \in [\hat{t}_z, t_z^M]$ such that the pooling interval $[t_z^m, \bar{t}_z]$ can be partitioned into multiple pooling sub-intervals, denoted by a strictly increasing sequence $[t_z^0, t_z^1, ..., t_z^N]$ with $t_z^0 = t_z^m$ and $t_z^N = \bar{t}_z$, such that*

$$C^{A,z}(\hat{a}_z(t_z^{n-1}, t_z^n), t_z^n) = C^{A,z}(\hat{a}_z(t_z^n, t_z^{n+1}), t_z^n), \forall n \in \{1, ..., N-1\} \tag{10}$$

$$C^{S,z}(\hat{a}_z(t_z^{N-1}, \bar{t}_z), \bar{t}_z, t_z^m) = C^{S,z}(a_{R,z}^*(\bar{t}_z), \bar{t}_z, \alpha_z^*(\bar{t}_z)), if \bar{t}_z < t_z^M. \tag{11}$$

*(**Sufficient condition**). Given any boundary type and a pooling-partition shown in (10) and (11), and*

$$C^{S,z}(\hat{a}_z(t_z^{N-1}, \bar{t}_z), t_z^M, t_z^m) \leq C^{S,z}(a_{R,z}^*(t_z^M), t_z^M, t_z^M), if \bar{t}_z = t_z^M. \tag{12}$$

There exists a PLASH equilibrium.

In any PLASH equilibrium, both players must play on the equilibrium. Specifically, R chooses strategy $\beta_z(\Omega_z(m_n))$ and takes the action $\hat{a}_z(t_z^{n-1}, t_z^n)$ for any $m_n \in M_{t_z^m}$ with $\theta(t) = m_n$ and $t = [t_x, t_y]$ for all $t_z \in (t_z^{n-1}, t_z^n)$; while for any $t_z \in (\bar{t}_z, t_z^M]$, R chooses $\beta_z(\Omega_z(\theta(t))) = \alpha_{R,z}^*(t_z)$ with $t = [t_x, t_y]$. S chooses the signaling strategy $\alpha_z(t_z) = \alpha_z^*(t_z)$ for all $t_z \in (\bar{t}_z, t_z^M]$, and chooses $\alpha_z(t_z) = t_z^m$ for all $t_z \in [t_z^m, \bar{t}_z]$, and sends message $m_n \in M_{t_z^m}$ for any $t_z \in (t_z^{n-1}, t_z^n)$; for $t_z \in (t_z^{j-1}, t_z^j)$, S sends message $m_j \neq m_n$, but $\Omega_z(m_j) = \Omega_z(m_n) = t_z^m$.

Remark 2. In the separating PBE regime, S chooses the signal strategy $\alpha_z^*(t_z)$, which induces action $a_{R,z}^*$ of R; thus, the signal strategy $\alpha_z^*(t_z)$ reveals the true type; yet this signal strategy is costly since $\alpha_z^*(t_z) > s_z^*(t_z)$, which means that it does not minimize the deception cost $C^{D,z}$. However, if S chooses the least costly strategy $\alpha_z(t_z) = s_z^*(t_z)$, it would cause adverse inferences from R since R expects a certain degree of deception at separating PBE and rationally infers the true type.

4 Numerical Experiments

In this section, we simulate a simple scenario of GPS spoofing and construct a signaling game model in which the UAV plays the receiver (R) and the GPS spoofer plays the sender (S). In the numerical experiments, we set the minimum value and the maximum value of latitude or longitude as $t_z^m = 1$ and $t_z^M = 10$, respectively, and set the constant parameters $\rho = 1$ and $k_2 = 1$. The differential equation (8) becomes

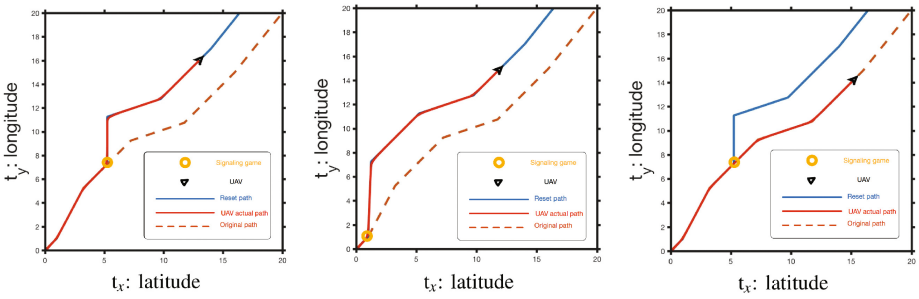
$$\frac{d\alpha_z(t_z)}{dt_z} = \frac{l_z}{k_1\big(2\alpha_z(t_z) - t_z\big)}. \tag{13}$$

Let $c = \frac{l_z}{k_1}$, $w = 2\alpha_z(t_z) - t_z$, then $w' = 2\alpha_z'(t_z) - 1$; thus $\frac{d\alpha_z(t_z)}{dt_z} = \frac{w'+1}{2}$; substituting w to (13) yields $\frac{w}{2c-w}dw = dt_z$, which can be integrated and yield the solution form $t_z + \sigma = -w - 2c\ln(2c - w)$, where σ is a constant to be found. We assume that when the UAV reaches the maximum value of latitude (longitude), the spoofer does not spoof on the value of latitude (longitude). Therefore, we have the initial condition $\alpha_z^*(10) = 10$, and then can determine $\sigma = -20 - 2c\ln(2c - 10)$. Thus, the solution of (13) α_z^* satisfies

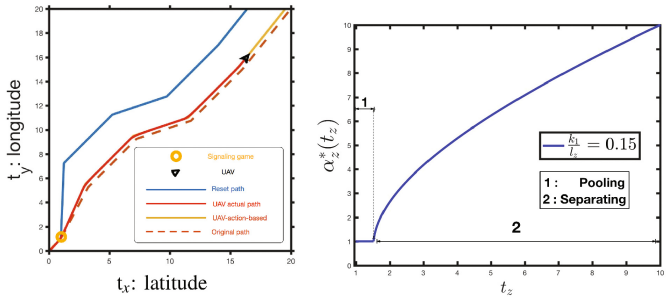
$$\frac{e^{\frac{-10k_1}{l_z}}k_1}{2l_z - 10k_1}\Big(\frac{2l_z}{k_1} - 2\alpha_z^*(t_z) + t_z\Big) = e^{\frac{-k_1}{l_z}\alpha_z^*(t_z)} \tag{14}$$

The solutions of (14) are shown in Fig. 5e–f. Since $\alpha_z^*(\hat{t}_z) = 1$, the value of $\hat{t}_z$ can be determined as

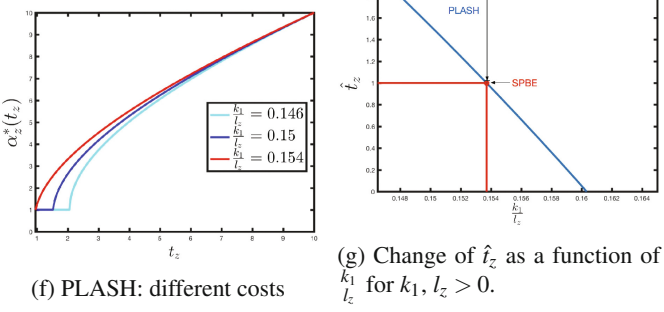
$$\hat{t}_z = \frac{2 - 10\frac{k_1}{l_z}}{\frac{k_1}{l_z}}e^{\frac{9k_1}{l_z}} + 2 - 2\frac{l_z}{k_1} \tag{15}$$



(a) Naive R. (b) Naive R. (c) Strategic R: SPBE



(d) Strategic R: PPBE (e) PLASH



(f) PLASH: different costs (g) Change of $\hat{t}_z$ as a function of $\frac{k_1}{l_z}$ for $k_1, l_z > 0$.

Fig. 5. 5**a**–**d:** Examples of UAV scenarios at PLASH equilibrium. The orange circle represents the place where both players take actions. (a) naive UAV (R) at the region where SPBE exists; (b) naive UAV at the region where PPBE exists; (c) strategic UAV at SPBE; (d) strategic UAV at PPBE. **5e**–**f:** Examples of UAV scenarios at PLASH equilibrium (e): PLASH strategies of the GPS spoofer: PLASH (f): PLASH strategies of the GPS spoofer with different deception costs (relative to the malignity of the sender). **5g:** Change of $\bar{t}_z$ as a function of $\frac{k_1}{l_z}$ for $k_1, l_z > 0$. PLASH equilibrium exists for all $1 < \bar{t}_z < 2$ (above the red line). (Color figure online)

Since $\alpha_z^*(\hat{t}_z) > \frac{\hat{t}_z}{2}$ is required in the separating region, $1 \leq \hat{t}_z < 2$. As shown in Fig. 5g, $\hat{t}_z$ decreases with respect to $\frac{k_1}{l_z}$, for all $k_1 > 0$ and $l_z > 0$. Also, $\hat{t}_z = 1$ if $\frac{k_1}{l_z} \approx 0.154$; it implies that a single SPBE exists if k is large enough relative to l_z ($\frac{k_1}{l_z} > 0.154$), and a single pooling PBE exists if k is small enough relative to l_z ($\frac{k_1}{l_z} \to 0$); the plot of $\hat{t}_z = 1$ coincides with the intuition that when the deception is cheap (resp. expensive) relative to the level of deviation aimed by the attacker, S prefers the pooling (separating) strategy.

From (10), we have: $t_z^n - t_z^{n-1} + 4l_z = t_z^{n+1} - t_z^n$; thus, $\bar{t}_z - t_z^{N-1} = t_z^n - t_z^{n-1} + 4(N-n)l_z$, for all $n \in \{1, 2, ..., N-1\}$. Equation (11) yields:

$$\Big(\frac{t_z^{N-1} - \bar{t}_z}{2} - l_z\Big)^2 - l_z^2 = k_1\Big((\alpha_z^*(\bar{t}_z) - \bar{t}_z)^2 - (1 - \bar{t}_z)^2 + \rho\big(1 - (\alpha_z^*(\bar{t}_z))^2\big)\Big),$$

if $\bar{t}_z < t_z^M = 10$. Also, from (12), we arrive at $t_z^{N-1} \geq 10 + 2l_z - 2\sqrt{l_z^2 + 18k_1}$, if $\bar{t}_z = t_z^M = 10$. Since $10 + 2l_z - 2\sqrt{l_z^2 + 18k_1} < t_z^M = 10$, $t_z^{N-1} < t_z^M$ is well defined. Thus, both the necessary and the sufficient conditions of Theorem 2 are satisfied. Therefore, there exists a PLASH equilibrium.

Figure 5a–d shows the behaviors of the UAV under different strategies. In each figure, the orange dashed line represents the planned flight path, the blue solid line represents the reset flight path created by the spoofer, and the red solid line represents the actual flight path of the UAV. The signaling game starts at the place marked by an orange circle, where the UAV and the GPS spoofer take actions. Based on the action of the GPS spoofer, the controller of the UAV strategically accepts the current position coordinates and adjusts the velocity v and λ according to (1). Figure 5a and b show the behaviors of a naive UAV in the regions where SPBE and PPBE, respectively, exist. A naive UAV is credulous, i.e., unconditionally trusting the received signal, s_z. Therefore, the controller of the naive UAV completely accept the literal current position coordinates according to the GPS signal, and the corresponding v and λ make the UAV deviate to the reset path (shown in blue) that is totally determined by the spoofed GPS signal. Figure 5c shows the behavior of a strategic UAV at the SPBE. Since the GPS spoofer's SPBE strategy $\alpha_z^*(t_z)$ reveals the true position in the SPBE, the controller of the UAV can obtain the correct current position coordinates $(a_{R,x}^*(t_x), a_{R,y}^*(t_y))$ based on the SPBE strategy, and the corresponding v and λ keep the UAV fly on the original flight path. Figure 5d shows the behavior of a strategic UAV at the PPBE. In the PPBE, the GPS spoofer plays the PPBE strategy $\alpha_z(t_z) = t_z^m$. However, in the PPBE region the spoofer can send different navigation messages $m_z \in M_{t_z^m}$ that induce the same value of signal $s_z = t_z^m$ (position coordinates) due to the existence of multiple pooling sub-intervals. The controller of the strategic UAV takes the current position coordinates as $(\hat{a}_x(t_x^{n-1}, t_x^n), \hat{a}_y(t_y^{n-1}, t_y^n))$ when the UAV is in the region (t_z^{n-1}, t_z^n), the corresponding v and λ make the UAV fly on a path shown in solid orange in Fig. 5d. As can be seen, the strategy of the UAV in the

multiple pooling region cannot always obtain the exactly true position but performs better than being credulous.

5 Conclusion

Civilian UAVs primarily guided by GPS have been shown to be readily spoofable by researchers. Failing to detect and defend the civil GPS spoofing could cause a significant hazard in the national airspace and sabotage the businesses primarily based on UAVs. Thus, it is critical to design a security mechanism. We have proposed a signaling game-based defense mechanism against the civil GPS spoofing attacks for the civilian UAVs. Our focus is on the case when the position information is spoofed while the velocity and the time are assumed to be accurate. However, our method can be further extended to the spoofing of the velocity and time information.

We have defined a perfect Bayesian equilibrium (PBE) pooling in low types and separating in high types (PLASH). We have also shown that there can be a unique full separating PBE if the deception cost is sufficiently small compared to the malice of the GPS spoofer. A full pooling PBE can exist if the deception cost is sufficiently large. We have also shown that the pooling portion of the PLASH can be partitioned into multiple pooling subintervals such that the GPS spoofer chooses messages to for different pooling subintervals.

The simulation results have shown that in the separating portion of the PLASH, the GPS spoofer chooses a strategy that yields the optimal action of the UAV that reveals the true position and completely defends the spoofing. In the pooling portion, the UAV cannot exactly infer its true position, but the equilibrium action can reduce the deviation between the estimated position and the true position, thus mitigating the potential loss caused by the spoofing.

Acknowledgement. This research is partially supported by NSF grants CNS-1544782, CNS-1720230 and the DOE grant DE-NE0008571.

A Appendix

A.1 Appendix A: Proof of Lemma 1

Proof. Since we require $\frac{d\alpha_z(t_z)}{dt_z} \geq 0$, the strategy $\alpha_z(t_z)$ in the separating portion must satisfy $\alpha_z(t_z) > s_z^*(t_z) = \frac{t_z}{1+\rho}$. Suppose that α_z is constant on some interval $\Phi \subseteq (t_z^s, t_z^l)$), then there exists some type $t_z \in \Phi$ such that S can send a signal $s_z(t_z+\delta)$ with $\delta > 0$ indicating a slightly higher type $t_z+\delta \in \Phi$ without inducing the additional deception cost, which contradicts the hypothesis of separating equilibrium in Lemma 1; therefore, α_z is strictly increasing on (t_z^s, t_z^l); thus, $\alpha_z \in (t_z^m, t_z^M)$ for any $t_z \in (t_z^s, t_z^l)$.

The incentive compatibility of SPBE requires that for any $t_z \in (t_z^s, t_z^l)$, $\alpha_z(t_z) \in \arg\min_{s_z} C^{S,z}(t_z, t_z, s_z)$. (8) is obtained by differentiating $C^{S,z}(t_z, t_z, s_z)$, which can be done only if $\alpha_z(t_z)$ is differentiable. In order to

prove that $\alpha_z(t_z)$ on (t_z^s, t_z^l), we first prove that $\alpha_z(t_z) > \arg\min_s C^{D,z}$ and $\alpha_z(t_z)$ is continuous for all $t_z \in (t_z^s, t_z^l)$.

We prove $\alpha_z(t_z) > s_z^* = \frac{t_z}{1+\rho}$ for all $t_z \in (t_z^s, t_z^l)$ in two steps as follows.

Step 1: Suppose $\alpha_z(\bar{\tau}_z) = s_z^*(\bar{\tau}_z) = \frac{\bar{\tau}_z}{1+\rho}$ for some $\bar{\tau}_z \in (t_z^s, t_z^l)$. Then, $C_2^{D,z}(t_z, \alpha_z(\bar{\tau}_z)) = 0$. Let $\delta > 0$ be a position constant with small enough $|\delta|$. Let $U(\delta)$ be the expected change in the cost for type $\bar{\tau}_z - \delta \in (t_z^s, t_z^l)$ by changing from $\alpha_z(\bar{\tau}_z - \delta)$ to $\alpha_z(\bar{\tau}_z)$. Then,

$$\begin{aligned} U(\delta) =& C^{S,z}(\bar{\tau}_z, \bar{\tau}_z - \delta, s_z^*(\bar{\tau}_z)) - C^{S,z}(\bar{\tau}_z - \delta, \bar{\tau}_z - \delta, \alpha_z(\bar{\tau}_z - \delta)) \\ =& \left[C^{A,z}(\bar{\tau}_z, \bar{\tau}_z - \delta) - C^{A,z}(\bar{\tau}_z - \delta, \bar{\tau}_z - \delta)\right] \\ &+ k_1\left[C^{D,z}(\bar{\tau}_z - \delta, s_z^*(\bar{\tau}_z)) - C^{D,z}(\bar{\tau}_z - \delta, \alpha_z(\bar{\tau}_z - \delta))\right]. \end{aligned}$$

Since $C^{A,z}(\bar{\tau}_z, \bar{\tau}_z - \delta) < C^{A,z}(\bar{\tau}_z - \delta, \bar{\tau}_z - \delta)$ and $C^{D,z}(\bar{\tau}_z - \delta, s_z^*(\bar{\tau}_z - \delta)) \leq C^{D,z}(\bar{\tau}_z - \delta, \alpha_z(\bar{\tau}_z - \delta))$, $U(\delta) < 0$, which implies that S strictly prefers to use the strategy $\alpha_z(\bar{\tau}_z)$ when the type is $\bar{\tau}_z - \delta$; this means that S uses the strategy $\alpha_z(\bar{\tau}_z)$ for both type $\bar{\tau}_z - \delta$ and type $\bar{\tau}_z$, which contradicts the hypothesis of SPBE for $\bar{\tau}_z$. Thus, $\alpha_z(\bar{\tau}_z) \neq s_z^*(\bar{\tau}_z)$.

Step 2: Suppose there exists a $\hat{\tau}_z \in (t_z^s, t_z^l)$ such that $\alpha_z(\hat{\tau}_z) < s_z^*(\hat{\tau}_z) < \hat{\tau}_z$. From (8), we have $\frac{d\alpha_z(\hat{\tau}_z)}{d\hat{\tau}_z} < 0$. Thus, the strict monotonicity of $\alpha_z(t_z)$ gives that $\alpha_z(\hat{\tau}_z - \delta) > \alpha_z(\hat{\tau}_z)$ for all $\delta > 0$. Then for small enough $\delta > 0$, we have $C^{D,z}(\hat{\tau}_z - \delta, \alpha_z(\hat{\tau}_z)) < C^{D,z}(\hat{\tau}_z - \delta, \alpha_z(\hat{\tau}_z - \delta))$. Also, we have $C^{A,z}(\hat{\tau}_z, \hat{\tau}_z - \delta) < C^{A,z}(\hat{\tau}_z - \delta, \hat{\tau}_z - \delta)$. As a result, $C^{S,z}(\hat{\tau}_z, \hat{\tau}_z - \delta, \alpha_z(\hat{\tau}_z)) < C^{S,z}(\hat{\tau}_z - \delta, \hat{\tau}_z - \delta, \alpha_z(\hat{\tau}_z - \delta))$. Therefore, S prefers to use the same strategy $\alpha_z(\hat{\tau}_z)$ for $\hat{\tau}_z - \delta$ as for $\hat{\tau}_z$, which contradicts the hypothesis of SPBE for $\hat{\tau}_z$. Thus, Step 1 and 2 yield that $\alpha_z(t_z) > s_z^*(t_z)$.

Now we prove the continuity of $\alpha_z(t_z)$ on $t_z \in (t_z^s, t_z^l)$. Suppose that there exists a discontinuity point at some $t_z \in (t_z^s, t_z^l)$. Let $\alpha_z(t_z) > \lim_{t_z \to t_z^-} = \hat{\alpha}_z$. Then,

$$\lim_{\delta \to 0+} \left[C^{A,z}(t_z - \delta, \alpha_z(t_z - \delta)) - C^{A,z}(t_z - \delta, \alpha_z(t_z))\right] = 0.$$

Since α_z is strictly increasing and $s_z^*(t_z) \leq \hat{\alpha}_z < \alpha_z(t_z)$, we also have

$$\lim_{\delta \to 0} \left[C^{D,z}(t_z - \delta, \alpha_z(t_z - \delta) - C^{D,z}(t_z - \delta, \alpha_z(t_z))\right] = C^{D,z}(t_z, \hat{\alpha}_z) - C^{D,z}(t_z, \alpha_z(t_z)) < 0.$$

Therefore, the cost of $\alpha_z(t_z - \delta)$ is less than $\alpha_z(t_z)$; thus, S prefers to use the same strategy $\alpha_z(t_z - \delta)$ for t_z as for $t_z - \delta$ for small enough $\delta > 0$, which contradicts the hypothesis of SPBE. Similar proof for the case $\alpha_z(t_z) < \lim_{t_z \to t_z^+} = \hat{\alpha}_z$ can show that S prefers to use the same strategy $\alpha_z(t_z + \delta)$ for t_z as for $t_z + \delta$ for small enough $\delta > 0$, contradicting the SPBE. Therefore, $\alpha_z(t_z)$ is continuous on (t_z^s, t_z^l).

Based on the same argument of the Proposition 2 in the Appendix of Mailath's work in [14] (also see the proof of [9]), α_z is differentiable. Therefore, Lemma 1 is proved.

A.2 Appendix B: Proof of Theorem 1

In this part, we prove that there exists a unique solution on $[\hat{t}, t_z^M]$ to (8) with initial condition $\alpha_z^*(t_z^M) = t_z^M = \hat{s}_z(t_z^M)$ and $\frac{d\alpha_z^*(t_z)}{dt_z} > 0$.

Proof. **Step 1: Local uniqueness and existence**
Let $B_z(t_z, s_z)$ be the inverse initial value problem and let $\eta_z(s_z)$ be the solution of $B_z(t_z, s_z)$. Then,

$$\eta_z' = B_z(\eta_z, s_z) = -\frac{C^{S,z}(\eta_z, \eta_z, s_z)_3}{C^{S,z}(\eta_z, \eta_z, s_z)_1}, \text{ with } \eta_z(s_z^*(t_z^M)) = t_z^M. \tag{16}$$

From the definition of $C^{S,z}$, B_z is Lipschitz continuous on $T \times T$. Then, from the existence and uniqueness theorems [11], we can find some $\delta > 0$ such that $\hat{s}_z(t_z) - \delta \geq s_z^*(t_z) = \frac{t_z}{1+\rho}$ and there exists a unique solution $\hat{\eta}_z$ to (16) on $[\hat{s}_z(t_z^M) - \delta, \hat{s}_z(t_z^M))$, and $\hat{\eta_z}$ is continuously differentiable on $[\hat{s}_z(t_z^M) - \delta, \hat{s}_z(t_z^M))$. From the definition of $\hat{s}_z(t_z^M)$, we have $B_z(t_z^M, \hat{s}_z(t_z^M)) > 0$, $B_z(t_z^M, s_z^*(t_z^M)) = 0$ and $\hat{s}_z^{-1}(t_z^M) = \frac{1}{\hat{s}_z(\hat{s}_z^{-1}(t_z^M))} > 0$; δ can be small enough such that $s_z < \hat{s}_z(\hat{\eta}_z(s_z))$ for all $s_z \in (\hat{s}_z(t_z^M) - \delta, \hat{s}_z(t_z^M)))$; and thus $\hat{\eta}_z'(s_z) > 0$. Let $\hat{\alpha}_z = \hat{\eta}_z^{-1}$ be a solution to 8 on $(\check{t}_z, t_z^M]$ for some $\check{t}_z < t_z^M$ with $\frac{d\hat{\alpha}_z}{dt_z} > 0$. Since the solution $\hat{\eta}_z$ to the inverse initial value problem is locally unique, the solution to the initial value problem (8) is locally unique.

Step 2: Suppose $\hat{\alpha}_z$ is the a solution to (8) with initial condition $\alpha_z^*(t_z^M) = t_z^M = \hat{s}_z(t_z^M)$ and $\frac{d\alpha_z^*(t_z)}{dt_z} > 0$, on $(t_z', t_z^M]$. Let $\bar{\alpha}_z = \lim_{t_z \to t_z'} \hat{\alpha}_z$. As been proved above, $\hat{\alpha}_z > s_z^*(t_z)$ for all $(t_z', t_z^M]$, and $\bar{\alpha}_z \geq s_z^*(t_z)$. Suppose $\bar{\alpha}_z = s_z^*(t_z)$. Then, $C_3^{S,z} = 0$, which yields $\lim_{t_z \to t_z'} = \infty$. Let $\zeta = \sup_{t_z \in [t_z', t_z^M]} (s_z^*(t_z))' = \frac{1}{1+\rho} < \infty$. Since $\hat{\alpha}_z'(t_z^M) > 0$ exists, there exists a $t_z^{''} > t_z'$ such that $\alpha_z(t_z^{''}) > \zeta$ for all $t_z \in [t_z', t_z^{''}]$. Let $\epsilon > 0$ such that $\hat{\alpha}_z(t_z^{''}) > s_z^*(t_z^{''}) + \epsilon$. Since $\bar{\alpha}_z = \lim_{t_z \to t_z'} \hat{\alpha}_z$, it follows

$$\begin{aligned}\bar{\alpha}_z = \hat{\alpha}_z(t_z^{''}) + \lim_{t_z \to t_z'} \int_{t_z}^{t_z^{''}} \alpha_z'(\tau) d\tau > s_z^*(t_z^{''}) + \epsilon + \int_{t_z'}^{t_z^{''}} \alpha_z'(\tau) d\tau \\ > s_z^*(t_z^{''}) + \int_{t_z'}^{t_z^{''}} \left(s_z^*(\tau)\right)' d\tau + \epsilon = s_z^*(t_z') + \epsilon,\end{aligned}$$

which contradicts that $\bar{\alpha}_z = s_z^*(t_z)$. Therefore, we have $\bar{\alpha}_z > s_z^*(t_z)$.

If the solution $\hat{\alpha}_z(t_z)$ is well defined on $(t_z', t_z^M]$ with $\lim_{t_z \to t_z'} \hat{\alpha}_z(t_z) > t_z^M$, then $-\frac{C_1^{S,z}}{C_3^{S,z}}$ is Lipschitz continuous and bounded in a neighborhood of $(\bar{\alpha}_z, t_z')$. According to the existence and uniqueness theorems, there exists a unique differentiable solution $\hat{\alpha}_z$ to (8) on $(t_z' - \epsilon', t_z^M]$ for some $\epsilon' > 0$ with $\lim_{t_z \to t_z' - \epsilon'} \hat{\alpha}_z(t_z) > s_z^*(t_z' - \epsilon')$ for $t_z' \in (t_z^m, t_z^M)$.

Clearly, $\hat{t}_z = \sup\{\hat{\tau}_z : \hat{\alpha}_z \text{ is well defined on } (\hat{\tau}_z, t_z^M]\}$, and setting $\hat{\alpha}_z(\hat{t}_z) = t_z^m$ finishes the proof of Theorem 1.

References

1. Amazon.com: Amazon prime air (2017). https://www.amazon.com/Amazon-Prime-Air/b?node=8037720011. Accessed 12 Apr 2017
2. Casey, W., Morales, J.A., Nguyen, T., Spring, J., Weaver, R., Wright, E., Metcalf, L., Mishra, B.: Cyber security via signaling games: toward a science of cyber security. In: Natarajan, R. (ed.) ICDCIT 2014. LNCS, vol. 8337, pp. 34–42. Springer, Cham (2014). doi:10.1007/978-3-319-04483-5_4
3. Casey, W.A., Zhu, Q., Morales, J.A., Mishra, B.: Compliance control: managed vulnerability surface in social-technological systems via signaling games. In: Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats, pp. 53–62. ACM (2015)
4. Crawford, V.P., Sobel, J.: Strategic information transmission. Econom. J. Econom. Soc. 1431–1451 (1982)
5. Curry, C., et al.: SENTINEL Project-Report on GNSS Vulnerabilities. Chronos Technology Ltd., Lydbrook (2014)
6. Hein, G., Kneissl, F., Avila-Rodriguez, J.A., Wallner, S.: Authenticating GNSS: proofs against spoofs, Inside GNSS **2**(5), 58–63 (2007). part 2
7. Humphreys, T.: Cockrell school researchers demonstrate first successful spoofing of UAVs (2012). https://www.engr.utexas.edu/features/humphreysspoofing. Accessed 5 Apr 2017
8. Infrastructure, Transportation: Vulnerability assessment of the transportation infrastructure relying on the global positioning system (2001)
9. Kartik, N.: Strategic communication with lying costs. Rev. Econ. Stud. **76**(4), 1359–1395 (2009)
10. Kashyap, A., Basar, T., Srikant, R.: Correlated jamming on mimo gaussian fading channels. IEEE Trans. Inf. Theor. **50**(9), 2119–2123 (2004)
11. Khalil, H.K.: Nonlinear Systems. Prentice Hall, Upper Saddle River (2002)
12. Kuhn, M.G.: An asymmetric security mechanism for navigation signals. In: Fridrich, J. (ed.) IH 2004. LNCS, vol. 3200, pp. 239–252. Springer, Heidelberg (2004). doi:10.1007/978-3-540-30114-1_17
13. Ledvina, B.M., Bencze, W.J., Galusha, B., Miller, I.: An in-line anti-spoofing device for legacy civil GPS receivers. In: Proceedings of the 2010 International Technical Meeting of the Institute of Navigation, pp. 698–712 (2001)
14. Mailath, G.J.: Incentive compatibility in signaling games with a continuum of types. Econom. J. Econom. Soc. 1349–1365 (1987)
15. Noe, T.H.: Capital structure and signaling game equilibria. Rev. Financ. Stud. **1**(4), 331–355 (1988)
16. Papadimitratos, P., Jovanovic, A.: GNSS-based positioning: attacks and countermeasures. In: Military Communications Conference, MILCOM 2008, pp. 1–7. IEEE (2008)
17. Pawlick, J., Zhu, Q.: Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. IEEE Trans. Inf. Forensics Secur. (2017)
18. Pozzobon, O.: Keeping the spoofs out: signal authentication services for future GNSS. Inside GNSS **6**(3), 48–55 (2011)
19. Raya, M., Manshaei, M.H., Félegyházi, M., Hubaux, J.P.: Revocation games in ephemeral networks. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 199–210. ACM (2008)
20. Sagduyu, Y.E., Berry, R., Ephremides, A.: MAC games for distributed wireless network security with incomplete information of selfish and malicious user types.

In: International Conference on Game Theory for Networks, GameNets 2009, pp. 130–139. IEEE (2009)
21. Schmidt, D., Radke, K., Camtepe, S., Foo, E., Ren, M.: A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Comput. Surv. (CSUR) **48**(4), 64 (2016)
22. Shepard, D.P., Bhatti, J.A., Humphreys, T.E., Fansler, A.A.: Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: Proceedings of the ION GNSS Meeting, vol. 3 (2012)
23. Wang, J., Tu, W., Hui, L.C., Yiu, S., Wang, E.K.: Detecting time synchronization attacks in cyber-physical systems with machine learning techniques. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 2246–2251. IEEE (2017)
24. Warner, J.S., Johnston, R.G.: A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. J. Secur. Adm. **25**(2), 19–27 (2002)
25. Wesson, K., Rothlisberger, M., Humphreys, T.: Practical cryptographic civil GPS signal authentication. Navigation **59**(3), 177–193 (2012)
26. Wikipedia: Cheap talk — wikipedia, the free encyclopedia (2017). https://en.wikipedia.org/w/index.php?title=Cheap_talk&oldid=771947821. Accessed 4 Apr 2017
27. Wullems, C., Pozzobon, O., Kubik, K.: Signal authentication and integrity schemes for next generation global navigation satellite systems. In: Proceedings of the European Navigation Conference GNSS (2005)
28. Xu, Z., Zhu, Q.: A cyber-physical game framework for secure and resilient multi-agent autonomous systems. In: 2015 IEEE 54th Annual Conference on Decision and Control (CDC), pp. 5156–5161. IEEE (2015)
29. Xu, Z., Zhu, Q.: A game-theoretic approach to secure control of communication-based train control systems under jamming attacks. In: Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles, pp. 27–34. ACM (2017)
30. Zhu, Q., Basar, T.: Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Syst. **35**(1), 46–65 (2015)
31. Zhu, Q., Fung, C., Boutaba, R., Basar, T.: A game-theoretical approach to incentive design in collaborative intrusion detection networks. In: International Conference on Game Theory for Networks, GameNets 2009, pp. 384–392. IEEE (2009)