On the Optimality of Linear Signaling to Deceive Kalman Filters over Finite/Infinite Horizons

Muhammed O. Sayin(✉) and Tamer Başar

Department of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
{sayin2,basar1}@illinois.edu

Abstract. In this paper, we address the problem of obtaining optimal deceptive signaling strategies between two agents, a sender and a receiver, over an ideal channel. Different from classical (cooperative) communication settings, here, the agents select their strategies under two different cost measures. For the case when these costs are quadratic, we analyze the Stackelberg equilibrium, where the sender leads the game by committing his/her strategies beforehand. This is an infinite-dimensional optimization problem, where the sender needs to anticipate the receiver's reaction while selecting his/her policy within the general class of stochastic kernels. The specific model we adopt for the underlying information of interest is a discrete-time Markov process generated by a vector-valued linear dynamical system, and at each instant, the information is a realization of a square integrable multivariate random vector. Over both finite and infinite horizons, we show the optimality of memoryless, "linear" signaling rules when the receiver uses a Kalman filter to estimate its information of interest. We develop algorithms that deliver the optimal signaling strategies. Numerical analysis shows that the performance of the sender degrades slightly when the receiver uses the best nonlinear estimator even when the information of interest is a Rademacher random variable rather than Gaussian.

Keywords: Stackelberg games · Security · Signaling · Deception · Semi-definite programming · Infinite-horizon

1 Introduction

We have trust in and rely on the power of informed decisions more and more as we are always observing its repeatedly proven empirical effectiveness. Therefore, intelligent agents seek to make the best decisions based on the information available to them. This yields that there is a direct relation between how an agent

M.O. Sayin—This research was supported in part by the U.S. Office of Naval Research (ONR) MURI grant N00014-16-1-2710, and in part by the U.S. Army Research Labs (ARL) under IoBT Grant 479432-239012-191100.

T. Alpcan et al. (Eds.): GameSec 2019, LNCS 11836, pp. 459–478, 2019.
https://doi.org/10.1007/978-3-030-32430-8_27

would act and the information available to him/her. By controlling/designing the information available, it can be possible to control/manipulate the actions of an intelligent agent. In an adversarial environment, the ability to control others' actions can play a pronounced role on the outcome.

Particularly, asymmetry of information is common due to the asymmetry of agents in adversarial environments. Agents can have access to certain information private to them. For example, a defender could have access to the state of a dynamical system, or the outputs of certain sensors monitoring the system, which an attacker would not have access to. Correspondingly, this asymmetry enables agents to control how much the other agents could know about the information private to them. To this end, the agent who has access to the private information could share/signal it strategically with the other agents in order to control their perception, and correspondingly to control the others' decisions/actions.

Recently, deception applications have attracted extensive attention in the field of security. A survey of these studies can be found in [12]. For example, obfuscation techniques can be used to corrupt the information available to other agents in order to deceive them [5,8,21]. However, strategic information transmission to control the others' perceptions can be viewed as a special type of deception that is based on signaling. It differs from the previous studies based on obfuscation techniques. Particularly, here, decision makers who have access to private information craft it strategically before sharing it with the others in order to *control the others' perceptions* rather than corrupting it.

Furthermore, in computer security, honey-X based defense strategies are also used widely to make the threats believable that honey-X is the real system rather than a trap [19]. For example, in [4], the authors have studied honeypots within the framework of binary signaling games. However, how a honeypot can be crafted so that it mimics a real system, or vice versa, is viewed as binary signals instead of addressing the crafting mechanism. On the other hand, here, our goal is to address the *optimal crafting* strategy within the general class of stochastic kernels for information of interest with continuum supports.

Deception applications have also attracted extensive attention in the field of communication and control. In [13], the authors study strategic information transmission of multivariate Gaussian information over an additive Gaussian noise channel for quadratic cost functions that are misaligned by a commonly known bias term under the solution concept of Nash equilibrium [3]. In [1] and [7], the authors study strategic information transmission for the scenarios where the bias term is private to the information provider, under the solution concept of Stackelberg equilibrium [3] where the information provider is the leader.

Previously, we have addressed strategic information transmission for multivariate Gaussian information in dynamic environments over a finite horizon [14,15,18]. For a discrete-time Gauss Markov process, we have shown in [14] the optimality of linear signaling rules within the general class of measurable policies and provided a semi-definite programming (SDP) based algorithm to compute the optimal signaling strategies numerically. For a non-cooperative linear quadratic Gaussian control problem, we have addressed in [15,18] derivation

of the optimal linear signaling strategies for a sensor who seeks to deceive a private-type controller in the settings where the distribution over the private type of the controller is, respectively, known or not known.

Different from previous studies reviewed above, in this paper, our goal is to address strategic information transmission for *general multivariate distributions* in dynamic environments over both *finite and infinite horizons*. We consider the scenario where there are two decision makers: a sender and a receiver. The sender has access to two separate multi-dimensional information: information of interest and some private information. The receiver seeks to learn the information of interest through a Kalman filter [2]. However, the sender wants to deceive the receiver to perceive the information of interest as that private information with respect to another quadratic cost measure. To this end, at each instant, the sender can construct a multidimensional signal based on all the previous information through a stochastic kernel map.

Under the solution concept of Stackelberg equilibrium, where the sender is the leader, we show that linear signaling strategies are optimal within the general class of stochastic kernels. To this end, we show that the problem faced by the sender depends only on the covariance of the linear estimate. We can obtain certain upper and lower bounds on that covariance in terms of linear matrix inequalities. We show that for any matrix that satisfies these bounds, there exists a linear signaling strategy such that the covariance of the linear estimate is equal to that matrix. This enables us to formulate an equivalent semi-definite programming (SDP) problem to compute the optimal signaling numerically. However, over the infinite horizon that equivalent SDP problem is also infinite dimensional. Therefore, we prove the existence of a solution for that infinite-dimensional SDP problem and formulate a way to compute the linear signaling rules that attain a performance within any ϵ-neighborhood of the optimal solution. We also conduct numerical analyses to examine how much the players' performances change if the receiver can use the best nonlinear estimator.

We note that in [7], the authors address how to signal *Gaussian* information to deceive a Kalman filter with respect to *myopic* quadratic objectives. Our study differs from [7] by addressing optimal signaling for general distributions with respect to quadratic objectives over finite as well as infinite horizons.

Our main contributions are therefore as follows:

- We show that the infinite-dimensional signaling problem, to deceive a Kalman filter, can be transformed into an equivalent SDP problem.
- We show the optimality of linear signaling strategies within the general class of stochastic kernels.
- We show the existence of a solution for the equivalent SDP problem over the infinite horizon and provide a method to approximate it.

The paper is organized as follows: In Sect. 2, we formulate the deceptive signaling problem over finite and infinite horizons. In Sects. 3 and 4, we compute the optimal signaling strategies over finite and infinite horizons, respectively. In Sect. 5, we provide illustrative numerical examples. We conclude the paper and

identify possible future research directions in Sect. 6. One appendix includes a proof of a lemma provided.

2 Problem Formulation

Consider a non-cooperative communication setting over an ideal channel between two decision makers: a sender ($\mathcal{P}_S$) and a receiver ($\mathcal{P}_R$). Over a discrete-time scale $k = 1, 2, \ldots$, only $\mathcal{P}_S$ gains access to the underlying information of interest and some private information. At instant k, the information of interest and the private information are, respectively, realizations of m-dimensional random vectors $\boldsymbol{x}_k$ and $\boldsymbol{\theta}_k$. The random vectors are defined on a common probability space $(\Omega, \mathcal{F}, \mathbf{P})$, where Ω is the outcome space, $\mathcal{F}$ is a proper σ-algebra, and $\mathbf{P}$ is the probability measure, i.e.,

$$(\Omega, \mathcal{F}, \mathbf{P}) \xrightarrow{\boldsymbol{x}_k} (\mathcal{X}, \mathcal{B}^m, \mathbf{P}_{x,k}), \tag{1}$$

$$(\Omega, \mathcal{F}, \mathbf{P}) \xrightarrow{\boldsymbol{\theta}_k} (\mathcal{X}, \mathcal{B}^m, \mathbf{P}_{\theta,k}). \tag{2}$$

where $\mathcal{X} \subset \mathbb{R}^m$. We note that $\mathcal{X}$ is not necessarily compact and it can be as large as the entire $\mathbb{R}^m$, e.g., the support of a multivariate Gaussian distribution. The information of interest and the private information evolve over the discrete-time scale $k = 1, 2, \ldots$, through first-order auto-regressive recursions as[1]

$$\boldsymbol{x}_{k+1} = A\,\boldsymbol{x}_k + \boldsymbol{w}_k, \tag{3}$$

$$\boldsymbol{\theta}_{k+1} = B\,\boldsymbol{\theta}_k + \boldsymbol{v}_k, \tag{4}$$

where $A, B \in \mathbb{R}^{m\times m}$, and $\boldsymbol{x}_0 = \boldsymbol{\theta}_0 = \mathbf{0}_m$. Each noise parameter $\boldsymbol{w}_k$ or $\boldsymbol{v}_k$ has zero-mean and is independent of all previous noise parameters, i.e., $\boldsymbol{w}_{1:k-1}$ and $\boldsymbol{v}_{1:k-1}$; however, $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ can be correlated.

Let $\mathcal{H}^{(m)}$ denote the Hilbert space of all square integrable m-dimensional random vectors with inner product:

$$(\boldsymbol{x}, \boldsymbol{y}) = \int_\Omega \boldsymbol{x}(\omega)'\boldsymbol{y}(\omega)\mathbf{P}(d\omega). \tag{5}$$

Correspondingly, we use the induced norm, i.e., $\|\boldsymbol{x}\| = \sqrt{(\boldsymbol{x}, \boldsymbol{x})}$. We consider the scenarios where $\boldsymbol{x}_k, \boldsymbol{\theta}_k \in \mathcal{H}^{(m)}$ for all k, and $\|\boldsymbol{x}_k\|$ and $\|\boldsymbol{\theta}_k\|$ are uniformly bounded for all k, i.e., there exist $M_x, M_\theta \in \mathbb{R}$ such that $\|\boldsymbol{x}_k\|^2 \leq M_x$ and $\|\boldsymbol{\theta}_k\|^2 \leq M_\theta$ for all k.

In the dynamic environment, each decision maker makes a decision at each instant, and has perfect recall while selecting his/her[2] strategy[3] according to a

[1] For notational simplicity, we consider time-invariant matrices A and B; however, the results could be extended to the time-variant case rather straight-forwardly.

[2] We use the pronouns "he" and "she" while referring to $\mathcal{P}_S$ and $\mathcal{P}_R$, respectively, only for clear referral.

[3] We use the terms "strategy", "signaling/decision rule", and "policy" interchangeably.

distinct cost measure. For each instance of the underlying information, e.g., $\boldsymbol{x}_k \in \mathcal{H}^{(m)}$, $\mathcal{P}_S$ selects his strategy $\eta_k(\cdot)$ that is a "stochastic kernel" from $\mathcal{H}^{(2km)}$ to $\mathcal{H}^{(2m)}$ such that the signal sent, $\boldsymbol{s}_k \in \mathcal{H}^{(2m)}$, is a square-integrable $2m$-dimensional random vector, and is given by

$$\boldsymbol{s}_k = \eta_k(\boldsymbol{x}_{1:k}, \boldsymbol{\theta}_{1:k}) \text{ a.e. over } \mathcal{X} \times \mathcal{X}. \tag{6}$$

Let us denote the set of all such signaling rules by Υ_k, i.e., $\eta_k \in \Upsilon_k$. On the other side, after signal $\boldsymbol{s}_k \in \mathcal{H}^{(2\,m)}$ is received, $\mathcal{P}_R$ selects her strategy $\gamma_k(\cdot)$ that is a "linear" mapping from $\mathcal{H}^{(2km)}$ to $\mathcal{H}^{(m)}$ such that her estimate of the underlying information is given by

$$\boldsymbol{u}_k = \gamma_k(\boldsymbol{s}_{1:k}) \text{ a.e. over } \mathcal{X}. \tag{7}$$

At instant k, the strategy space of $\mathcal{P}_R$ is denoted by $\mathit{\Gamma}_k$, which is the set of all linear functions from $\mathcal{H}^{(2km)}$ to $\mathcal{H}^{(m)}$.

The decision makers have different cost measures. For the interactions over a finite horizon with length κ, $\mathcal{P}_S$ has the cost measure

$$\sum_{k=1}^{\kappa} \|\boldsymbol{\theta}_k - \boldsymbol{u}_k\|^2 \tag{8}$$

to be minimized via $\eta := \{\eta_k\}$ over $\mathit{\Upsilon} := \times_k \Upsilon_k$. On the other side, $\mathcal{P}_R$ has the quadratic cost measure

$$\sum_{k=1}^{\kappa} \|\boldsymbol{x}_k - \boldsymbol{u}_k\|^2, \tag{9}$$

to be minimized via $\gamma := \{\gamma_k\}$ over $\mathit{\Gamma} := \times_k \mathit{\Gamma}_k$. For the interactions over infinite horizon, $\mathcal{P}_S$ has the discounted cost measure

$$\lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \beta_S^k \|\boldsymbol{\theta}_k - \boldsymbol{u}_k\|^2 \tag{10}$$

to be minimized via $\eta \in \mathit{\Upsilon}$, where $\beta_S \in (0, 1)$ is the discount factor. The discount factor can be viewed as the probability that the information flow in-between $\mathcal{P}_S$ and $\mathcal{P}_R$ does not terminate permanently over the infinite horizon. Correspondingly, $\mathcal{P}_R$ has the cost measure

$$\lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \beta_R^k \|\boldsymbol{x}_k - \boldsymbol{u}_k\|^2, \tag{11}$$

to be minimized via $\gamma \in \mathit{\Gamma}$, where $\beta_R \in (0, 1)$ is the discount factor.

The misaligned cost measures can be viewed as $\mathcal{P}_R$ seeking to learn the underlying information $\{\boldsymbol{x}_k\}$ while $\mathcal{P}_S$ wants $\mathcal{P}_R$ to perceive the information of interest $\{\boldsymbol{x}_k\}$ as the private information $\{\boldsymbol{\theta}_k\}$ by designing the information available to $\mathcal{P}_R$ via strategic signaling. In other words, $\mathcal{P}_R$ makes her best possible decision selfishly according to her cost measure, yet the decision is based on the

information available to her. By making that information set biased, $\mathcal{P}_S$ seeks to deceive $\mathcal{P}_R$ to make a decision, inadvertently, in line with $\mathcal{P}_S$'s interest.

For formal analysis, we analyze the interaction between the decision makers under the solution concept of Stackelberg equilibrium [3], where $\mathcal{P}_S$ is the leader who commits to play his strategy beforehand and $\mathcal{P}_R$ is the follower who selects her strategy knowing the committed signaling rules $\{\eta_k\}$, i.e., knowing how biased her information set is. In the following, we provide an explicit definition of the game.

Definition 1 (Deceptive Signaling Game). *The deceptive signaling game* $\mathcal{G} := (\Upsilon, \Gamma, \{\boldsymbol{x}_k\}, \{\boldsymbol{\theta}_k\}, J_S(\cdot), J_R(\cdot))$ *is a Stackelberg game between the leader* $\mathcal{P}_S$ *and the follower* $\mathcal{P}_R$. *We let* $B(\eta) \in \Gamma$ *be the best reaction set of the follower* $\mathcal{P}_R$ *for a given strategy* $\eta \in \Upsilon$ *of* $\mathcal{P}_S$. *Then, the pair of the strategy and the best reaction set* $(\eta^*, B(\eta^*))$ *attains the Stackelberg equilibrium provided that*

$$\eta^* \in \operatorname*{argmin}_{\eta \in \Upsilon} \max_{\gamma \in B(\eta)} J_S(\eta, \gamma) \tag{12a}$$

$$B(\eta) = \operatorname*{argmin}_{\gamma \in \Gamma} J_R(\eta, \gamma). \tag{12b}$$

3 Deceptive Signaling over Finite Horizon

In this section, we first focus on the cost measures over a finite horizon, e.g., with length κ. We will address the equilibrium for the cost measures over the infinite horizon later in Sect. 4. To this end, we formulate $\mathcal{P}_R$'s best reaction set, which turns out to be an equivalence class of policies that lead to a unique $\boldsymbol{u}_k$. Incorporating that best response in $\mathcal{P}_S$'s cost measure, $\mathcal{P}_S$ faces an infinite-dimensional optimization problem that can be written in a compact form when we confine the impact of $\mathcal{P}_S$'s policy into certain symmetric matrices. Indeed, if $\mathcal{P}_R$'s policy space were the general class of measurable policies, then those matrices would correspond to covariance of the posterior estimate of the underlying information of interest given the signals sent. Then, we show that we can derive necessary and sufficient conditions over symmetric matrices such that any set of matrices satisfying the conditions can be realized via certain signaling rules. Furthermore, any signaling rule leads to a set of matrices that satisfy these conditions. This enables us to transform the infinite-dimensional optimization problem into a finite-dimensional one without loss of generality so that we can apply the powerful existing computational tools. We now provide the technical details of establishing that equivalence relationship.

We first observe that even though the players interact multiple times over a horizon, the information flows in a single direction from $\mathcal{P}_S$ to $\mathcal{P}_R$. In other words, $\mathcal{P}_S$'s strategy $\eta_k \in \Upsilon_k$ does not depend on $\mathcal{P}_R$'s strategy $\gamma_{1:k} \in \bigtimes_{j=1}^{k} \Gamma_j$. Therefore, the game can essentially be viewed as single shot (12) while the selected policies can have consequences over the horizon. Furthermore, $\mathcal{P}_R$'s cost measure (9) can be separated into sub-problems such that $\mathcal{P}_R$ selects her strategy $\gamma_k \in \Gamma_k$ in order to minimize

$$\|\boldsymbol{x}_k - \gamma_k(\boldsymbol{s}_{1:k})\|^2, \tag{13}$$

which is a linear mean square error estimation problem. And a minimizing linear strategy is given by

$$\gamma_k : \mathcal{H}^{(2km)} \to \mathcal{H}^{(m)} \tag{14}$$

$$\boldsymbol{s}_{1:k} \mapsto \mathbb{E}\{\boldsymbol{x}_k \boldsymbol{s}'_{1:k}\}\mathbb{E}\{\boldsymbol{s}_{1:k}\boldsymbol{s}'_{1:k}\}^{\dagger}\boldsymbol{s}_{1:k}, \tag{15}$$

where (and henceforth) the expectation is taken with respect to all the randomness. Since Γ_k is the set of all linear functions from $\mathcal{H}^{(2km)}$ to $\mathcal{H}^{(m)}$, given $\boldsymbol{s}_{1:k} \in \mathcal{H}^{(2km)}$, the set

$$\{\boldsymbol{u}_k \in \mathcal{H}^{(m)} \,|\, \exists \gamma_k \in \Gamma_k \ni \boldsymbol{u}_k = \gamma_k(\boldsymbol{s}_{1:k}) \text{ a.e.}\} \tag{16}$$

is a closed subspace of $\mathcal{H}^{(m)}$. Then, the Projection Theorem [10] yields that there is a unique minimizer $\boldsymbol{u}_k^*$ even though there can be multiple linear policies $\gamma_k \in \Gamma_k$ such that all lead to $\boldsymbol{u}_k^* = \gamma_k(\boldsymbol{s}_k)$, almost everywhere over $\mathcal{X}$, if $\mathbb{E}\{\boldsymbol{s}_{1:k}\boldsymbol{s}'_{1:k}\}$ is not invertible.

We note that if $\boldsymbol{x}_k$ and $\boldsymbol{s}_{1:k}$ were jointly Gaussian, then the linear policy (15) would minimize the mean square error. Furthermore, if $\mathcal{P}_R$'s policy space were not restricted to linear strategies, then the best reaction would be the conditional expectation of the information given the signal sent, i.e., $\mathbb{E}\{\boldsymbol{x}_k|\boldsymbol{s}_{1:k}\}$. Correspondingly, for notational simplicity, we introduce a linear estimation operator denoted by $\mathcal{E}(\cdot\,|\,\cdot)$. Particularly, for random vectors $\boldsymbol{a} \in \mathcal{H}^{(m_a)}$ and $\boldsymbol{b} \in \mathcal{H}^{(m_b)}$, the operator is given by

$$\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b}) := \underset{\boldsymbol{u}\in\mathcal{M}_{m_a}(\boldsymbol{b})}{\operatorname{argmin}} \|\boldsymbol{a}-\boldsymbol{u}\|^2, \tag{17}$$

where $\mathcal{M}_{m_a}(\boldsymbol{b})$ is a closed subspace of $\mathcal{H}^{(m_a)}$ and is given by

$$\mathcal{M}_{m_a}(\boldsymbol{b}) := \{\boldsymbol{\alpha} \in \mathcal{H}^{(m_a)} \ni \boldsymbol{\alpha} = K\boldsymbol{b} \text{ for some } K \in \mathbb{R}^{m_a \times m_b}\}. \tag{18}$$

The following lemma highlights some of the properties that $\mathcal{E}(\cdot\,|\,\cdot)$ enjoys. We will be using these properties while addressing the optimal deception rule.

Lemma 1. *Given random vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{H}^{(m_a)}$, and $\boldsymbol{c} \in \mathcal{H}^{(m_c)}$, let us decompose $\boldsymbol{b} = \tilde{\boldsymbol{b}} + \tilde{\boldsymbol{b}}^{\perp}$ such that*[4] *$\tilde{\boldsymbol{b}} \in \mathcal{M}_{m_a}(\boldsymbol{c})$ and $\tilde{\boldsymbol{b}}^{\perp} \in \mathcal{M}_{m_a}(\boldsymbol{c})^{\perp}$. Then, we have*[5]

(i) $\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b},\boldsymbol{c}) = \mathcal{E}(\boldsymbol{a}\,|\,\tilde{\boldsymbol{b}}^{\perp},\boldsymbol{c})$,
(ii) $\mathbb{E}\{\boldsymbol{a}\,\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})'\} = \operatorname{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})\}$,
(iii) $\mathbb{E}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b},\boldsymbol{c})\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})'\} = \operatorname{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})\}$,
(iv) $\operatorname{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b},\boldsymbol{c})\} = \operatorname{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\tilde{\boldsymbol{b}}^{\perp})\} + \operatorname{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})\}$.

Proof. The proof is provided in Appendix A. □

[4] Note that $\mathcal{M}_{m_a}(\boldsymbol{c})$ is a closed subspace of $\mathcal{H}^{(m_a)}$, and we have $\mathcal{H}^{(m_a)} = \mathcal{M}_{m_a}(\boldsymbol{c}) \oplus \mathcal{M}_{m_a}(\boldsymbol{c})^{\perp}$.

[5] With a slight abuse of notation, we define $\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b},\boldsymbol{c}) := \mathcal{E}\left(\boldsymbol{a}\,|\,\left[\boldsymbol{b}'\ \boldsymbol{c}'\right]'\right)$.

Substituting $\mathcal{P}_R$'s best reaction into $\mathcal{P}_S$'s cost measure (8), $\mathcal{P}_S$ faces the following infinite-dimensional optimization problem:

$$\min_{\eta\in\Upsilon} \sum_{k=1}^{\kappa} \|\boldsymbol{\theta}_k - \mathcal{E}(\boldsymbol{x}_k \,|\, \boldsymbol{s}_{1:k})\|^2. \tag{19}$$

In order to address this problem, we first seek to write (19) in a compact form. To this end, we define the auxiliary parameters:

$$\boldsymbol{z}_k := \begin{bmatrix} \boldsymbol{x}_k \\ \boldsymbol{\theta}_k \end{bmatrix}, C := \begin{bmatrix} A & \\ & B \end{bmatrix}, \text{ and } \boldsymbol{\nu}_k := \begin{bmatrix} \boldsymbol{w}_k \\ \boldsymbol{v}_k \end{bmatrix}. \tag{20}$$

Note that $\boldsymbol{z}_k, \boldsymbol{\nu}_k \in \mathcal{H}^{(2m)}$, and we have

$$\boldsymbol{z}_{k+1} = C\boldsymbol{z}_k + \boldsymbol{\nu}_k, \tag{21}$$

and $\boldsymbol{z}_0 = \mathbf{0}_{2m}$. We let $\Sigma_{z,k}, \Sigma_{\nu,k} \in \mathbb{S}^{2m}$ denote the covariance matrices of $\boldsymbol{z}_k$ and $\boldsymbol{\nu}_k$, respectively. Therefore, (21) yields that

$$\Sigma_{z,k+1} = C\Sigma_{z,k}C' + \Sigma_{\nu,k}. \tag{22}$$

For clear representation, we suppose that $\Sigma_{\nu,k} \succ O_{2m}$. The results could also be extended to the scenarios $\Sigma_{\nu,k} \succeq O_{2m}$ based on Lemma 3 in [16] straightforwardly.

After some algebra, the optimization problem faced by $\mathcal{P}_S$ (19) can be written in a compact form as

$$\min_{\eta\in\Upsilon} \sum_{k=1}^{\kappa} \mathrm{tr}\{H_k(\eta_{1:k})V\} + c_\kappa, \tag{23}$$

where the optimization argument $\eta \in \Upsilon$ has impact only on

$$H_k(\eta_{1:k}) := \mathrm{cov}\{\mathcal{E}(\boldsymbol{z}_k \,|\, \boldsymbol{s}_{1:k})\} \tag{24}$$

while $V \in \mathbb{S}^{2m}$ and $c \in \mathbb{R}$ are fixed deterministic parameters defined by

$$V := \begin{bmatrix} I_m & -I_m \\ -I_m & O_m \end{bmatrix} \text{ and } c_\kappa := \sum_{k=1}^{\kappa} \mathrm{tr}\left\{\mathrm{cov}\{\boldsymbol{\theta}_k\}\right\}.$$

Even though $\eta \in \Upsilon$ is an infinite-dimensional policy, its impact on the optimization objective is via the matrices $\{H_k(\eta_{1:k})\}$, which are finite dimensional. Therefore, we seek to derive the relationship between $\eta \in \Upsilon$ and $\{H_k(\eta_{1:k}) \in \mathbb{S}^{2m}\}$. Based on this relationship, we can obtain the necessary and sufficient conditions on the matrices over $\bigtimes_{k=1}^{\kappa} \mathbb{S}^{2m}$, i.e.,

$$\{\{S_k \in \mathbb{S}^{2m}\}_{k=1}^{\kappa} \,|\, \exists\, \eta \in \Upsilon \ni S_k = H_k(\eta_{1:k})\}. \tag{25}$$

If the corresponding necessary and sufficient conditions on matrices over $\mathbb{S}^{2m}$ turn out to be convex, then this infinite-dimensional optimization problem (23)

can be transformed into a finite-dimensional convex optimization problem with a linear optimization objective, which can be solved efficiently via existing powerful computational tools.

The following theorem provides the necessary and sufficient conditions on $\{S_k \in \mathbb{S}^{2m}\}$. Note that these conditions turn out to constitute a compact and convex set that can be described by the conventional partial ordering over symmetric matrices, e.g., for matrices $A, B \in \mathbb{S}^m$, we say that $A \succeq B$ if $A - B$ is a positive semi-definite matrix. Therefore, the infinite-dimensional optimization problem (23) is equivalent to a finite-dimensional SDP.

Theorem 1. *Given the random vector process $\{\boldsymbol{z}_k \in \mathcal{H}^{(2m)}\}$ as defined in (20), (21), and any stochastic kernel $\eta \in \Upsilon$, we have*

$$\Sigma_{z,k} \succeq H_k(\eta_{1:k}) \succeq C H_{k-1}(\eta_{1:k-1}) C', \tag{26}$$

where $H_k : \bigtimes_{l=1}^{k} \Upsilon_k \to \mathbb{S}^{2m}$ is as defined in (24). Furthermore, given the κ-tuple of symmetric matrices $\{S_k \in \mathbb{S}^{2m}\}$ satisfying[6]

$$\Sigma_{z,k} \succeq S_k \succeq C S_{k-1} C', \text{ for } k = 1, \ldots, \kappa, \tag{27}$$

*where $S_0 = O_{2m}$, we have that there exists a memoryless and probabilistic **linear-in-$\boldsymbol{z}_k$** signaling rule*

$$\eta_k(\boldsymbol{z}_{1:k}) = L_k \boldsymbol{z}_k + \boldsymbol{n}_k \ \ni \ H_k(\eta_{1:k}) = S_k, \tag{28}$$

where $L_k \in \mathbb{R}^{2m \times 2m}$, and $\boldsymbol{n}_k \in \mathcal{H}^{(2m)}$ has zero mean and is uncorrelated[7] *of $\boldsymbol{z}_{1:k}$ and $\boldsymbol{n}_{1:k-1}$.*

Given $\{S_k \in \mathbb{S}^{2m}\}$ satisfying (27), let us take the eigen-decomposition of

$$\Pi_k^{-1/2} (S_k - C S_{k-1} C') \Pi_k^{-1/2} = U_k \Lambda_k U_k', \tag{29}$$

where

$$\Pi_k := \Sigma_{z,k} - C S_{k-1} C'. \tag{30}$$

We have $\Lambda_k = \operatorname{diag}\{\lambda_{k,1}, \ldots, \lambda_{k,2m}\}$ with $\lambda_{k,i} \in [0,1]$. Then, the corresponding $L_k \in \mathbb{R}^{2m \times 2m}$ and $\operatorname{cov}\{\boldsymbol{n}_k\}$ are given by

$$L_k = \operatorname{diag}\{l_{k,1}, \ldots, l_{k,2m}\} U_k' \Pi_k^{-1/2}, \tag{31}$$

$$\operatorname{cov}\{\boldsymbol{n}_k\} = \operatorname{diag}\{\sigma_{n,k,1}^2, \ldots, \sigma_{n,k,2m}^2\}, \tag{32}$$

where the entries $l_{k,i}$ and $\sigma_{n,k,i}^2$ satisfy

$$\frac{l_{k,i}^2}{l_{k,i}^2 + \sigma_{n,k,i}^2} = \lambda_{k,i} \ \forall\, i = 1, \ldots, 2m. \tag{33}$$

[6] Note that $\Sigma_{z,k}$ satisfies (22).

[7] We say that two random vectors $\boldsymbol{a}, \boldsymbol{b}$ are uncorrelated if $\mathbb{E}\{\boldsymbol{a}\boldsymbol{b}'\} = \mathbb{E}\{\boldsymbol{a}\}\mathbb{E}\{\boldsymbol{b}\}'$. We also emphasize that uncorrelatedness is sufficient since the signal (28) is linear in $\boldsymbol{z}_k$ and $\boldsymbol{n}_k$.

Proof. Based on the properties of $\mathcal{E}(\cdot\,|\,\cdot)$ highlighted in Lemma 1, the proof follows from [17], where we show the sufficiency of (27) for multivariate Gauss-Markov processes even when the receiver's policy space is the general class of all measurable policies. □

Based on Theorem 1, we can solve the following SDP instead of (23):

$$\min_{\{S_k\}\in\Psi_\kappa} \sum_{k=1}^{\kappa} \mathrm{tr}\{S_k V\} + c_\kappa, \tag{34}$$

where

$$\Psi_\kappa := \{\{S_k \in \mathbb{S}^{2m}\}_{k=1}^{\kappa} \,|\, \Sigma_{z,k} \succeq S_k \succeq C S_{k-1} C', S_0 = O_{2m}\}. \tag{35}$$

Once we have the solution $\{S_k^*\}$, we can compute the corresponding signaling rule via Theorem 1. Note that the optimization objective in (34) is linear in the optimization arguments while the constraint set is compact and convex. Correspondingly, the solution (although it may not be unique) lies at the extreme points[8] of the constraint set (35), e.g., $\{S_k^e\}$, satisfies the following recursion:

$$S_k^e = C S_{k-1}^e C' + (\Sigma_{z,k} - C S_{k-1}^e C')^{1/2} P_k (\Sigma_{z,k} - C S_{k-1}^e C')^{1/2}, \tag{36}$$

for $k = 1, \dots, \kappa$, where $S_0^e = O_{2m}$ and $P_k \in \mathbb{S}^{2m}$ is a symmetric and idempotent matrix, i.e., $P_k = P_k^2$, which also implies that its eigenvalues are either 0 or 1.

Remark 1 (Noisy or Noiseless Signals). We emphasize that (36) yields that $\lambda_{k,i} \in \{0, 1\}$ for $k = 1, \dots, \kappa$ and $i = 1, \dots, 2m$ in (33). In particular, the optimal signaling rule is linear (i.e., there is no additional noise term) within the general class of stochastic kernels for the general class of square integrable distributions when $\mathcal{P}_R$'s strategy space is restricted to linear estimators.

Remark 2 (Versatility of Theorem 1). We also emphasize that the equivalence between (19) and (34) is not limited to equivalence at the optimum. Therefore, the equivalence would still hold when there are additional constraints on $H_k(\eta_{1:k})$ or if the optimization objective is not linear in $H_k(\eta_{1:k})$, which would imply that the solution may also not be an extreme point of the constraint set.

4 Deceptive Signaling over the Infinite Horizon

In this section, we address how to establish an equivalence relationship between problems with different computational complexity over the infinite horizon similar to the equivalence relationship between (19) and (34) over a finite horizon. However, even when such an equivalence relationship has been established, the

[8] We say that a point in a convex set is an extreme point if it cannot be expressed as a convex combination of any other two points in that set.

SDP counterpart of the original problem would still be an infinite-dimensional optimization problem, where $\mathcal{P}_S$ needs to design an infinite sequence of symmetric matrices. In order to mitigate that, we first show the existence of a solution and then provide an approach to approximate the solution with any approximation error. We next provide the technical details of this approximation.

We note that $\mathcal{P}_R$'s cost measure (11) can also be separated into sub-problems such that $\mathcal{P}_R$ selects her strategy $\gamma_k \in \Gamma_k$ in order to minimize (13). And the best reaction is also given by (15). Substituting $\mathcal{P}_R$'s best reaction into $\mathcal{P}_S$'s cost measure (10), $\mathcal{P}_S$ faces the following optimization problem:

$$\min_{\eta \in \Upsilon} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \beta_S^k \|\boldsymbol{\theta}_k - \mathcal{E}(\boldsymbol{x}_k \,|\, \boldsymbol{s}_{1:k})\|^2, \tag{37}$$

which can also be written in a compact form as

$$\min_{\eta \in \Upsilon} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \beta_S^k (\mathrm{tr}\{H_k(\eta_{1:k})V\} + \mathrm{tr}\{\Sigma_{\theta,k}\}). \tag{38}$$

The uniform boundedness conditions that $\|\boldsymbol{x}_k\|^2 \leq M_x$ and $\|\boldsymbol{\theta}_k\|^2 \leq M_\theta$ for all k yield that $\|\boldsymbol{z}_k\|^2 \leq M_z := M_x + M_\theta$. Therefore, by (26), we obtain

$$M_z I_{2m} \succeq \Sigma_{z,k} \succeq H_k(\eta_{1:k}) \succeq C H_{k-1}(\eta_{1:k-1}) C', \tag{39}$$

which implies that the largest eigenvalue of the positive semi-definite matrix $H_k(\eta_{1:k})$ can be as large as M_z. Furthermore, Von Neumann's trace inequality [11] says that for square matrices $A, B \in \mathbb{R}^{m \times m}$ with singular values $\sigma_{a,1} \geq \ldots \geq \sigma_{a,m}$ and $\sigma_{b,1} \geq \ldots \geq \sigma_{b,m}$, respectively, we have

$$|\mathrm{tr}\{AB\}| \leq \sum_{i=1}^{m} \sigma_{a,i} \sigma_{b,i}. \tag{40}$$

Correspondingly, we obtain

$$|\mathrm{tr}\{H_k(\eta_{1:k})V\}| \leq M_z \|V\|_*. \tag{41}$$

Furthermore, the uniform bound on $\|\boldsymbol{\theta}_k\|$ yields that $\mathrm{tr}\{\Sigma_{\theta,k}\} \leq M_\theta$. Since there is a bound on the absolute value of the term in parentheses and it is uniform over $k = 1, 2, \ldots$, the discount factor yields that the series in (38) is absolutely convergent. Since it is a series in $\mathbb{R}$, which is complete with respect to absolute value, the absolute convergence implies its convergence, and correspondingly, the limit in (38) exists. Therefore, (38) can also be written as

$$\min_{\eta \in \Upsilon} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \beta_S^k \mathrm{tr}\{H_k(\eta_{1:k})V\} + c \tag{42}$$

where

$$c := \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \beta_S^k \mathrm{tr}\{\Sigma_{\theta,k}\}. \tag{43}$$

Recall that the equivalence relationship in Theorem 1 holds for arbitrary length of horizon and its proof follows by forward induction. Therefore, (42) is equivalent to the following optimization problem:

$$\min_{\{S_k\}\in\Psi} \lim_{\kappa\to\infty} \sum_{k=1}^{\kappa} \beta^k \mathrm{tr}\{S_k V\} + c, \tag{44}$$

where

$$\Psi := \{\{S_k \in \mathbb{S}^{2m}\}_{k=1}^{\infty} \,|\, \Sigma_{z,k} \succeq S_k \succeq C S_{k-1} C', S_0 = O_{2m}\}. \tag{45}$$

If a solution exists, then given the solution $\{S_k^*\}$, we can compute the corresponding signaling rules via Theorem 1 in an iterative way. However, existence of a solution is not guaranteed in general. For example, closedness and boundedness of a set do not imply its compactness over infinite-dimensional spaces. However, a subset of a Banach space is compact if, and only if, it is closed, bounded and *flat*. We say that a set is flat if for every $\epsilon > 0$, the set is contained in the ϵ-neighborhood of some *finite*-dimensional linear subspace.

The following proposition shows that a solution exists by (i) showing that the problem can be transformed into an optimization problem over a certain Banach space without loss of generality; and then (ii) showing that the constraint set is bounded and flat; finally (iii) showing that the optimization objective is continuous, which enables us to invoke the Weierstrass Theorem [10] to conclude that a solution exists.

Proposition 1. *The infinite-dimensional optimization problem* (44) *admits a solution.*

Proof. Consider the linear vector space $\mathcal{S} \subset \times_{k=1}^{\infty} \mathbb{S}^{2m}$ with norm $\|\cdot\|_{\mathcal{S}}$. Particularly, each $s \in \mathcal{S}$ is an infinite sequence of symmetric matrices, i.e., $s := \{S_1, S_2, \ldots\}$, and

$$\|s\|_{\mathcal{S}} := \left(\sum_{k=1}^{\infty} \|S_k\|_F^2\right)^{1/2} < \infty. \tag{46}$$

Note that we can view $s \in \mathcal{S}$ as a sequence of real numbers with certain ordering within each symmetric matrix. For example, we can view

$$s = \left\{[S_1^{i,j}], [S_2^{i,j}], \ldots, \right\}, \tag{47}$$

where $S_k^{i,j} \in \mathbb{R}$ denotes the ith row and the jth column entry of the matrix $S_k \in \mathbb{S}^{2m}$, as

$$\{S_1^{1,1}, \ldots, S_1^{1,2m}, \ldots, S_1^{2m,1}, \ldots, S_1^{2m,2m}, S_2^{1,1}, \ldots\}. \tag{48}$$

The ℓ_2-norm of (48) is bounded if, and only if, $\|s\|_{\mathcal{S}}$ is bounded. Therefore, $\mathcal{S}$ is a subspace of ℓ_2-space, i.e., $\mathcal{S} \subseteq \ell_2$. Furthermore, given any $l \in \ell_2$, there exists

a unique sequence of symmetric matrices in $\mathcal{S}$. For example, $l := \{l_1, l_2, \ldots\}$ can be transformed into a sequence of symmetric matrices as

$$\left\{ \begin{bmatrix} l_1 & l_2 & l_4 & \cdots \\ l_2 & l_3 & & \\ l_4 & \ddots & & \\ \vdots & & l_{m(2m+1)} & \end{bmatrix}, \begin{bmatrix} l_{m(2m+1)+1} & \cdots \\ \vdots & \ddots \end{bmatrix} \cdots \right\},$$

and its $\mathcal{S}$-norm is bounded since $l \in \ell_2$. Therefore, ℓ_2-space is a subspace of $\mathcal{S}$, i.e., $\ell_2 \subseteq \mathcal{S}$. This yields that the normed spaces $\mathcal{S}$ and ℓ_2 are isometric. Correspondingly, $\mathcal{S}$ is also a Banach space since ℓ_2 is Banach.

Next, our goal is to show that the constraint set in (44) is a subset of $\mathcal{S}$ so that we can prove its compactness if we can show that the constraint set is flat in addition to being a bounded subset of the Banach space $\mathcal{S}$. Eventually, by showing that the optimization objective is continuous, we can invoke Weierstrass Theorem to conclude that a solution exists.

However, Ψ as defined in (45) is not a subset of $\mathcal{S}$. By inspecting the optimization objective, we observe that through a change of variable $\bar{S}_k := \alpha_S^k S_k$ for all k, where $\alpha_S := \sqrt{\beta_S} \in (0,1)$, (44) can be transformed into

$$\min_{\{\bar{S}_k\} \in \bar{\Psi}} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \alpha_S^k \mathrm{tr}\{\bar{S}_k V\} + c, \tag{49}$$

where

$$\bar{\Psi} := \{\{\bar{S}_k \in \mathbb{S}^{2m}\}_{k=1}^{\infty} \,|\, \alpha_S^k \Sigma_{z,k} \succeq \bar{S}_k \succeq \alpha_S C \bar{S}_{k-1} C', S_0 = O_{2m}\}. \tag{50}$$

In order to show that $\bar{\Psi} \subset \mathcal{S}$, let us take a look at the norm of any $\bar{s} := \{\bar{S}_k\} \in \bar{\Psi}$, which is given by

$$\begin{aligned} \|\bar{s}\|_{\mathcal{S}}^2 &= \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \|\bar{S}_k\|_F^2 \overset{(a)}{\leq} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \|\bar{S}_k\|_*^2 \\ &\overset{(b)}{=} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \mathrm{tr}\{\bar{S}_k\}^2 \overset{(c)}{\leq} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \alpha_S^{2k} M_z^2 4m^2 \\ &= \frac{4m^2 M_z^2 \alpha_S^2}{1 - \alpha_S^2} < \infty, \end{aligned} \tag{51}$$

where (a) follows since for a matrix S, the Frobenius norm $\|S\|_F = \sqrt{\sum_i \sigma_i(S)^2}$ while the trace norm $\|S\|_* = \sum_i \sigma_i(S)$, where $\sigma_i(S)$ refers to the ith singular value of S; and (b) follows since $\bar{S}_k$ is a positive semi-definite matrix and its singular values are the same with its eigenvalues; and (c) follows since we have $\alpha_S^k M_z I_{2m} \succeq \alpha_S^k \Sigma_{z,k} \succeq \bar{S}_k$ by the uniform boundedness condition on $\|\boldsymbol{z}_k\|$ and this implies that $\mathrm{tr}\{\bar{S}_k\} \leq \alpha_S^k M_z \mathrm{tr}\{I_{2m}\}$. Therefore, we have that $\bar{\Psi}$ is a bounded subset of $\mathcal{S}$.

In order to show that $\bar{\Psi}$ is flat, let us consider the following finite-dimensional space

$$\mathcal{F}_K := \{\{F_k\} \in \mathcal{S} \,|\, F_k = O_{2m} \text{ for } k > K\}.$$

Note that $\mathcal{F}_K \subset \mathcal{S}$. We define the distance of any $\bar{s} \in \bar{\Psi}$ to the space $\mathcal{F}_K$ by

$$d(\bar{s}, \mathcal{F}_K) = \inf\{\|\bar{s} - f\|_{\mathcal{S}}, f \in \mathcal{F}_K\}, \tag{52}$$

which can also be written as[9]

$$\begin{aligned} d(\bar{s}, \mathcal{F}_K) &= \inf_{f \in \mathcal{F}_K} \left(\sum_{k=1}^{\infty} \|\bar{S}_k - F_k\|_F^2 \right)^{1/2} \\ &\overset{(a)}{=} \inf_{f \in \mathcal{F}_k} \left(\underbrace{\sum_{k=1}^{K} \|\bar{S}_k - F_k\|_F^2}_{=0} + \sum_{k=K+1}^{\infty} \|\bar{S}_k\|_F^2 \right)^{1/2} \\ &= \left(\sum_{k=K+1}^{\infty} \|\bar{S}_k\|_F^2 \right)^{1/2} \leq \left(\sum_{k=K+1}^{\infty} \alpha_S^{2k} 4m^2 M_z^2 \right)^{1/2} \\ &= \frac{2mM_z \alpha_S^{(K+1)}}{\sqrt{1-\alpha_S^2}}, \end{aligned} \tag{53}$$

where (a) follows since $\{\bar{S}_1, \ldots, \bar{S}_K, O_{2m}, \ldots\} \in \mathcal{F}_K$. Therefore, we can ensure that the distance between any $\bar{s} \in \bar{\Psi}$ and finite-dimensional $\mathcal{F}_K$ is less than any $\epsilon > 0$ by selecting $K \in \mathbb{N}$ such that the upper bound on the distance, i.e., (53), is less than ϵ. This yields that $\bar{\Psi}$ is flat in addition to being a bounded subset of the Banach space $\mathcal{S}$. Hence $\bar{\Psi}$ is a compact set.

Furthermore, the optimization objective in (49) is a linear functional over $\mathcal{S}$. It is continuous if, and only if, it is bounded. And Von Neumann's trace inequality (40) yields that

$$\begin{aligned} \sup_{\|\bar{s}\|_{\mathcal{S}}=1} \lim_{\kappa \to \infty} \left| \sum_{k=1}^{\kappa} \alpha_S^k \text{tr}\{\bar{S}_k V\} \right| &\leq \sup_{\|\bar{s}\|_{\mathcal{S}}=1} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \alpha_S^k \left| \text{tr}\{\bar{S}_k V\} \right| \\ &\leq \sup_{\|\bar{s}\|_{\mathcal{S}}=1} \lim_{\kappa \to \infty} \sum_{k=1}^{\kappa} \alpha_S^k \sum_{i=1}^{2m} \sigma_i(\bar{S}_k) \sigma_i(V). \end{aligned} \tag{54}$$

Let us introduce two sequences of real numbers:

$$\begin{aligned} x &:= \{\sigma_1(\bar{S}_1), \ldots, \sigma_{2m}(\bar{S}_1), \sigma_1(\bar{S}_2), \ldots, \sigma_{2m}(\bar{S}_2), \ldots\} \\ y &:= \{\alpha_S \sigma_1(V), \ldots, \alpha_S \sigma_{2m}(V), \alpha_S^2 \sigma_1(V), \ldots, \alpha_S^2 \sigma_{2m}(V), \ldots\}. \end{aligned}$$

[9] Note that $\{\bar{S}_k - F_k\} \in \mathcal{S}$, which ensures that its $\mathcal{S}$-norm is bounded.

Then, the ℓ_2-norm of the sequences is given by $\|x\|_2 = 1$, due to the constraint $\|\bar{s}\|_{\mathcal{S}} = 1$, and $\|y\|_2 = (\alpha_S \|V\|_*)/\sqrt{1-\alpha_S^2}$. With the conventional inner-product of ℓ_2-Hilbert space, (54) can be written as

$$\sup_{\|x\|_2=1} (x, y), \tag{55}$$

while the Cauchy Schwarz inequality yields that

$$|(x, y)| \leq \|x\|_2 \|y\|_2 = \frac{\alpha_S \|V\|_*}{\sqrt{1-\alpha_S^2}}, \tag{56}$$

and the equality holds if, and only if, $x = \mu y$ for some $\mu \in \mathbb{R}$. Therefore, due to the norm constraint, the maximizing sequence x is given by $x = y/\|y\|$. Coming back to the original problem (54), we have

$$\sup_{\|\bar{s}\|_{\mathcal{S}}=1} \lim_{\kappa\to\infty} \sum_{k=1}^{\kappa} \alpha_S^k \sum_{i=1}^{2m} \sigma_i(\bar{S}_k)\sigma_i(V) \leq \frac{\alpha_S \|V\|_*}{\sqrt{1-\alpha_S^2}} \tag{57}$$

and the equality holds if, and only if, we have

$$\sigma_i(\bar{S}_k) = \alpha_S^{k-1}\sqrt{1-\alpha_S^2}\frac{\sigma_i(V)}{\|V\|_*}. \tag{58}$$

Hence, we obtain

$$\sup_{\|\bar{s}\|_{\mathcal{S}}=1} \lim_{\kappa\to\infty} \left| \sum_{k=1}^{\kappa} \alpha_S^k \mathrm{tr}\{\bar{S}_k V\} \right| = \frac{\alpha_S \|V\|_*}{\sqrt{1-\alpha_S^2}} \tag{59}$$

and the maximizing sequence of symmetric matrices is given by

$$\bar{S}_k = \frac{\alpha_S^{k-1}\sqrt{1-\alpha_S^2}}{\|V\|_*} V. \tag{60}$$

Therefore, the linear functional is bounded, and correspondingly continuous. This completes the proof. □

Even though a solution for (44) is guaranteed to exist, powerful computational tools to solve SDP cannot be applied since we seek to compute an infinite sequence of symmetric matrices. However, in the following theorem, we show how to approximate the solution with any approximation error.

Theorem 2. *For any given $\epsilon > 0$, let $K \in \mathbb{N}$ be such that*

$$M_z \|V\|_* \frac{\beta_S^{K+1}}{1-\beta_S} < \epsilon. \tag{61}$$

Furthermore, let $\{S_1^*, \ldots, S_K^*\}$ be the solution of

$$\min_{\{S_k\}\in\Psi_K} \sum_{k=1}^{K} \beta_S^k \mathrm{tr}\{S_k V\} + c. \tag{62}$$

Then, we have

$$\min_{\{S_k\}\in\Psi} \lim_{\kappa\to\infty} \sum_{k=1}^{\kappa} \beta_S^k \mathrm{tr}\{S_k V\} \geq \sum_{k=1}^{K} \beta_S^k \mathrm{tr}\{S_k^* V\} - \epsilon. \tag{63}$$

Proof. Note that for any $K \in \mathbb{N}$, we can write (44) as

$$\min_{\{S_k\}\in\Psi} \sum_{k=1}^{K} \beta_S^k \mathrm{tr}\{S_k V\} + \lim_{\kappa\to\infty} \sum_{k=K+1}^{\kappa} \beta_S^k \mathrm{tr}\{S_k V\} + c.$$

We seek to provide a bound on the absolute value of the second term. Particularly, for any $\{S_k\}_{k=K+1}^{\infty}$, we have

$$\begin{aligned} \lim_{\kappa\to\infty} \left| \sum_{k=K+1}^{\kappa} \beta_S^k \mathrm{tr}\{S_k V\} \right| &\leq \lim_{\kappa\to\infty} \sum_{k=K+1}^{\kappa} \beta_S^k |\mathrm{tr}\{S_k V\}| \\ &\overset{(a)}{\leq} \lim_{\kappa\to\infty} \sum_{k=K+1}^{\infty} \beta_S^k M_z \|V\|_* \leq M_z \|V\|_* \frac{\beta_S^{K+1}}{1-\beta_S}, \end{aligned} \tag{64}$$

where (a) follows by (41). Therefore, if (61) holds, we have (63), which completes the proof. □

5 Illustrative Examples

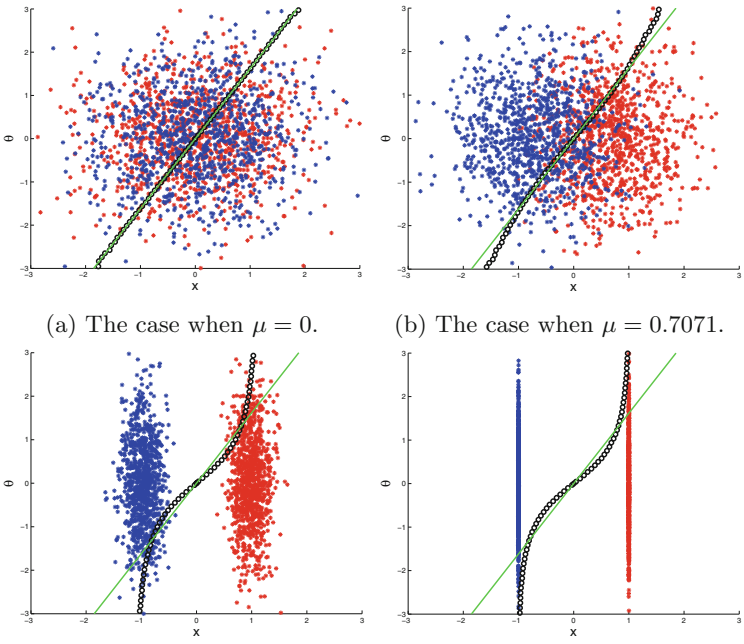
As an illustrative example, we consider the scenarios where there is only a single stage, and $\boldsymbol{x}_1$ and $\boldsymbol{\theta}_1$ are scalar random variables[10]. We suppose that $\boldsymbol{x}$ and $\boldsymbol{\theta}$ are independent of each other, have zero mean and unit variance. Indeed, the bias $\boldsymbol{\theta}$ is a standard normal random variable, i.e., $\boldsymbol{\theta} \sim \mathcal{N}(0,1)$. We, however, consider the scenarios where the information of interest $\boldsymbol{x}$ is not necessarily Gaussian, in order to examine the performances attained by the players in a more general setting, different from the previous studies [1,7,13–15,18]. Particularly, the information of interest $\boldsymbol{x}$ is given by

$$\boldsymbol{x} = \boldsymbol{b}\boldsymbol{x}_l + (1-\boldsymbol{b})\boldsymbol{x}_r, \tag{65}$$

almost everywhere over $\mathbb{R}$, where $\boldsymbol{b}, \boldsymbol{x}_l$, and $\boldsymbol{x}_r$ are random variables independent of each other and of the bias $\boldsymbol{\theta}$. Let $\boldsymbol{b}$ be a Bernoulli random variable and $\mathbf{P}\{\boldsymbol{b} = 1\} = 1/2$. And let $\boldsymbol{x}_l \sim \mathcal{N}(-\mu, \sigma^2)$ and $\boldsymbol{x}_r \sim \mathcal{N}(\mu, \sigma^2)$, where $\mu \in [0,1]$ and the variance σ^2 are such that $\mathrm{var}\{\boldsymbol{x}\} = 1$. In other words, the information of interest $\boldsymbol{x}$ is a Gaussian mixture with two components $\boldsymbol{x}_l$ and $\boldsymbol{x}_r$ at left and right, respectively.

By varying $\mu \in [0,1]$, we seek to examine the performances of the players. Note that when $\mu = 0$, $\boldsymbol{x}$ becomes a standard normal random variable as illustrated in Fig. 1a. Then, the best linear estimator attains the minimum mean

[10] Henceforth, we omit the subscript for notational simplicity.



(a) The case when $\mu = 0$. (b) The case when $\mu = 0.7071$.

(c) The case when $\mu = 0.9806$. (d) The case when $\mu = 1$.

Fig. 1. Color-coded samples of the augmented vector $\boldsymbol{z}$ for different values of $\mu \in [0, 1]$. For the best signaling rule to deceive a linear estimator, the best linear and nonlinear estimates are plotted via a green line and black circles, respectively. (Color figure online)

square error. However, for larger $\mu > 0$, the best linear estimator does not attain the best possible performance. $\mathcal{P}_R$ can attain better performance by using a nonlinear filter since the underlying information is no longer Gaussian when $\mu > 0$. Furthermore, when $\mu = 1$, which is the maximum possible value under the constraint that $\text{var}\{\boldsymbol{x}\} = 1$, the information of interest $\boldsymbol{x}$ becomes a Rademacher random variable as illustrated in Fig. 1d. Note that standard normal random variables have the maximum entropy while Rademacher random variables have the minimum entropy within the general class of random variables that have zero mean and unit variance [6].

We note that the augmented vector $\boldsymbol{z} = \begin{bmatrix}\boldsymbol{x}\ \boldsymbol{\theta}\end{bmatrix}' \in \mathbb{R}^2$ has zero mean and its covariance matrix is I_2, independent of $\mu \in [0, 1]$. Correspondingly, for all $\mu \in [0, 1]$, the solution for (34) is given by $S^* = uu'$, where $u = \begin{bmatrix}0.5257\ 0.8507\end{bmatrix}'$, as shown in [20]. And the optimal signal $\boldsymbol{s}^* = \begin{bmatrix}u'\boldsymbol{z}\ 0\end{bmatrix}'$, almost everywhere over $\mathbb{R}$. The optimal signal can be viewed as the projection onto the direction of the vector $u \in \mathbb{R}^2$. For a linear estimator, the projection, i.e., $\mathcal{E}(\boldsymbol{z} \mid u'\boldsymbol{z}) = uu'\boldsymbol{z}$, is the best estimate. However, for a nonlinear estimator, the best estimate is given by $\mathbb{E}\{\boldsymbol{z}|u'\boldsymbol{z}\}$, and it is not equal to the linear estimate in general.

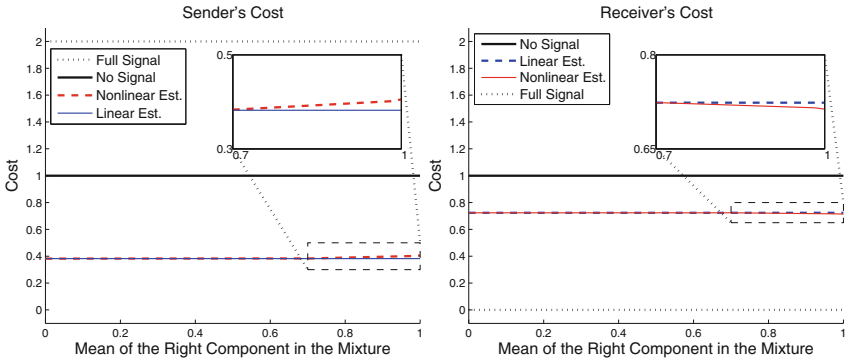


Fig. 2. Players' performances for null, full, and strategic signaling, and linear and nonlinear estimation strategies.

In Fig. 1, we plot about 500 samples of the augmented vector $\boldsymbol{z}$ for different values of $\mu \in [0,1]$ and color-code the samples drawn from different components of the mixture $\boldsymbol{x}$. We have conducted 10^7 independent trials of Monte Carlo simulations [9] in order to compute the best nonlinear estimate $\mathbb{E}\{\boldsymbol{z}|u'\boldsymbol{z}\}$ numerically. In Fig. 1, the best linear and nonlinear estimates for the signal $\boldsymbol{s} = u'\boldsymbol{z}$ are plotted via a green line and black circles, respectively, for different $\mu \in [0,1]$. Note that the best linear and nonlinear estimates match exactly for $\mu = 0$, i.e., for Gaussian information, while the deviation increases for larger μ. This deviation has different impact on players' performances. In other words, if $\mathcal{P}_R$ could use the best nonlinear estimator while $\mathcal{P}_S$ has selected his signaling rule considering the scenarios where $\mathcal{P}_R$ can only use the best linear estimator, e.g., Kalman filter; then $\mathcal{P}_S$ can have larger cost while the best nonlinear estimator can lead to smaller cost for $\mathcal{P}_R$. In Fig. 2, we compare the costs of the players for different scenarios:

(i) $\mathcal{P}_S$ does not share any signal, and correspondingly $\mathcal{P}_R$'s best linear/nonlinear estimate would be $\mathbb{E}\{\boldsymbol{z}\} = 0$;
(ii) $\mathcal{P}_S$ shares $\boldsymbol{z}$ completely, and correspondingly $\mathcal{P}_R$'s best linear/nonlinear estimate would be $\boldsymbol{z}$;
(iii) $\mathcal{P}_S$ shares $u'\boldsymbol{z}$ and $\mathcal{P}_R$ uses the best linear estimator;
(iv) $\mathcal{P}_S$ shares $u'\boldsymbol{z}$ yet $\mathcal{P}_R$ uses the best nonlinear estimator.

We note that the best deceptive signaling rule is not null or full information disclosure. And $\mathcal{P}_S$'s performance degrades slightly when he/she selects the signaling rule considering the scenarios where $\mathcal{P}_R$ uses the best linear estimator while $\mathcal{P}_R$ can use a nonlinear estimator even when the information of interest $\boldsymbol{x}$ is a Rademacher random variable as illustrated in Fig. 1d.

6 Conclusion

In non-cooperative environments, e.g., adversarial settings, an agent who has access to valuable information could seek to deceive other agents who seek to

make informed decisions. In this paper, we have addressed the optimal deceptive signaling of multivariate distributions over finite or infinite horizon. We have modeled the interaction between the agents under the solution concept of Stackelberg equilibrium, where the agent signaling is the leader. We have shown that the optimal signaling strategy to deceive a Kalman filter is linear within the general class of stochastic kernels over finite or infinite horizons. For problems over finite horizon, we have provided an SDP-based method to compute the optimal signaling numerically. Over the infinite horizon, the corresponding SDP is also infinite dimensional. We have shown the existence of a solution and provided a method to approximate the optimal performance within any given ϵ-neighborhood. Numerical analysis has shown that the performance of the sender degrades slightly when the receiver uses the best nonlinear estimator even for the scenarios where the information of interest is a Rademacher random variable rather than Gaussian. Some future research questions on this topic include: how much the sender's cost measure would increase/decrease if the receiver uses a particle filter instead of a Kalman filter; what the optimal signaling strategies are to deceive a particle filter; and what the optimal signaling strategies are for the scenarios with higher order cost measures other than quadratic cost.

A Proof of Lemma 1

In the following, we show each property one by one: Property (i) follows since $\mathcal{M}_{m_a}(\boldsymbol{b},\boldsymbol{c}) = \mathcal{M}_{m_a}(\tilde{\boldsymbol{b}}^{\perp},\boldsymbol{c})$. Property (ii) follows since

$$\mathbb{E}\{\boldsymbol{a}\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})'\} = \mathbb{E}\{\boldsymbol{a}(\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}\mathbb{E}\{\boldsymbol{c}\boldsymbol{c}'\}^{\dagger}\boldsymbol{c})'\} = \mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}\mathbb{E}\{\boldsymbol{c}\boldsymbol{c}'\}^{\dagger}\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}'. \tag{66}$$

Property (iii) follows since, by Property (i), we have

$$\mathbb{E}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b},\boldsymbol{c})\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})'\} = \mathbb{E}\{\mathcal{E}(\boldsymbol{a}\,|\,\tilde{\boldsymbol{b}}^{\perp},\boldsymbol{c})\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})'\}. \tag{67}$$

By taking a closer look at the right-hand-side, we obtain

$$\begin{bmatrix}\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}\\ \mathbb{E}\{\boldsymbol{a}\tilde{\boldsymbol{b}}^{\perp}\}\end{bmatrix}' \begin{bmatrix}\mathrm{cov}\{\boldsymbol{c}\} & \\ & \mathrm{cov}\{\tilde{\boldsymbol{b}}^{\perp}\}\end{bmatrix}^{\dagger} \begin{bmatrix}\mathbb{E}\{\boldsymbol{c}\boldsymbol{c}'\}\\ \mathbb{E}\{\tilde{\boldsymbol{b}}^{\perp}\boldsymbol{c}'\}\end{bmatrix} \mathrm{cov}\{\boldsymbol{c}\}^{\dagger}\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}'.$$

Since $\mathbb{E}\{\tilde{\boldsymbol{b}}^{\perp}\boldsymbol{c}'\} = O_{m_a\times m_c}$, it is equivalent to

$$\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}\mathrm{cov}\{\boldsymbol{c}\}^{\dagger}\mathrm{cov}\{\boldsymbol{c}\}\mathrm{cov}\{\boldsymbol{c}\}^{\dagger}\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}' = \mathrm{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})\},$$

which follows since the pseudo inverse of a matrix is a weak inverse for the multiplicative semi-group, i.e., $M^{\dagger}MM^{\dagger} = M^{\dagger}$. Property (iv) follows since $\mathrm{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{b},\boldsymbol{c})\}$ is equal to $\mathrm{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\tilde{\boldsymbol{b}}^{\perp},\boldsymbol{c})\}$. By taking a closer look at the right-hand-side, we obtain

$$\begin{bmatrix}\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}\\ \mathbb{E}\{\boldsymbol{a}\tilde{\boldsymbol{b}}^{\perp}\}\end{bmatrix}' \begin{bmatrix}\mathrm{cov}\{\boldsymbol{c}\} & \\ & \mathrm{cov}\{\tilde{\boldsymbol{b}}^{\perp}\}\end{bmatrix}^{\dagger} \begin{bmatrix}\mathbb{E}\{\boldsymbol{a}\boldsymbol{c}'\}\\ \mathbb{E}\{\boldsymbol{a}\tilde{\boldsymbol{b}}^{\perp}\}\end{bmatrix} = \mathrm{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\tilde{\boldsymbol{b}}^{\perp})\} + \mathrm{cov}\{\mathcal{E}(\boldsymbol{a}\,|\,\boldsymbol{c})\}. \tag{68}$$

References

1. Akyol, E., Langbort, C., Başar, T.: Information-theoretic approach to strategic communication as a hierarchical game. Proc. IEEE **105**(2), 205–218 (2017)
2. Anderson, B.D.O., Moore, J.B.: Optimal Filtering. Prentice Hall Inc., Upper Saddle River (1979)
3. Başar, T., Olsder, G.: Dynamic Noncooperative Game Theory. Society for Industrial and Applied Mathematics (SIAM) Series in Classics in Applied Mathematics (1999)
4. Carroll, T.E., Grosu, D.: A game theoretic investigation of deception in network security. Secur. Commun. Nets **4**(10), 1162–1172 (2011)
5. Clark, A., Zhu, Q., Poovendran, R., Başar, T.: Deceptive routing in relay networks. In: Grossklags, J., Walrand, J. (eds.) GameSec 2012. LNCS, vol. 7638, pp. 171–185. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34266-0_10
6. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley, Hoboken (2006)
7. Farokhi, F., Teixeira, A., Langbort, C.: Estimation with strategic sensors. IEEE Trans. Autom. Control **62**(2), 724–739 (2017)
8. Howe, D.G., Nissenbaum, H.: TrackMeNot: resisting surveillance in web search. In: Kerr, I., Lucock, C., Steeves, V. (eds.) On the Identity Trail: Privacy, Anonymity and Identity in a Networked Society. Oxford University Press, Oxford (2009)
9. Kroese, D.P., Brereton, T., Taimre, T., Botev, Z.I.: Why the Monte Carlo method is so important today. Wiley Interdisc. Rev. Comput. Stat. **6**(6), 386–392 (2014)
10. Luenberger, D.G.: Optimization by Vector Space Methods. Wiley, Hoboken (1969)
11. Mirsky, L.: A trace inequality of John von Neumann. Monatshefte für Mathematik **79**(4), 303–306 (1975)
12. Pawlick, J., Colbert, E., Zhu, Q.: A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. ArXiv:1712.05441 (2017)
13. Sarıtaş, S., Yüksel, S., Gezici, S.: Quadratic multi-dimensional signaling games and affine equilibria. IEEE Trans. Autom. Control **62**(2), 605–619 (2017)
14. Sayin, M.O., Akyol, E., Başar, T.: Hierarchical multi-stage Gaussian signaling games in noncooperative communication and control systems. Automatica **107**, 9–20 (2019)
15. Sayin, M.O., Başar, T.: Secure sensor design for cyber-physical systems against advanced persistent threats. In: Rass, S., An, B., Kiekintveld, C., Fang, F., Schauder, S. (eds.) Proceedings of International Conference on Decision and Game Theory for Security. LNCS, vol. 10575, pp. 91–111. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-68711-7_6
16. Sayin, M.O., Başar, T.: Dynamic information disclosure for deception. In: Proceedings of 57th IEEE Conference on Decision and Control (CDC), pp. 1110–1117 (2018)
17. Sayin, M.O., Başar, T.: Deception-as-defense framework for cyber-physical systems. arXiv:1902.01364 (2019)
18. Sayin, M.O., Başar, T.: Robust sensor design against multiple attackers with misaligned control objectives. arXiv:1901.10618 (2019)
19. Spitzner, L.: Honeypots: Tracking Hackers. Addison-Wesley Professional, Boston (2002)
20. Tamura, W.: A theory of multidimensional information disclosure. Working paper, available at SSRN 1987877 (2014)
21. Zhu, Q., Clark, A., Poovendran, R., Başar, T.: Deceptive routing games. In: Proceedings of IEEE Conference on Decision and Control, pp. 2704–2711 (2012)